

Radix Device Management User Guide

Radix Device Management Platform

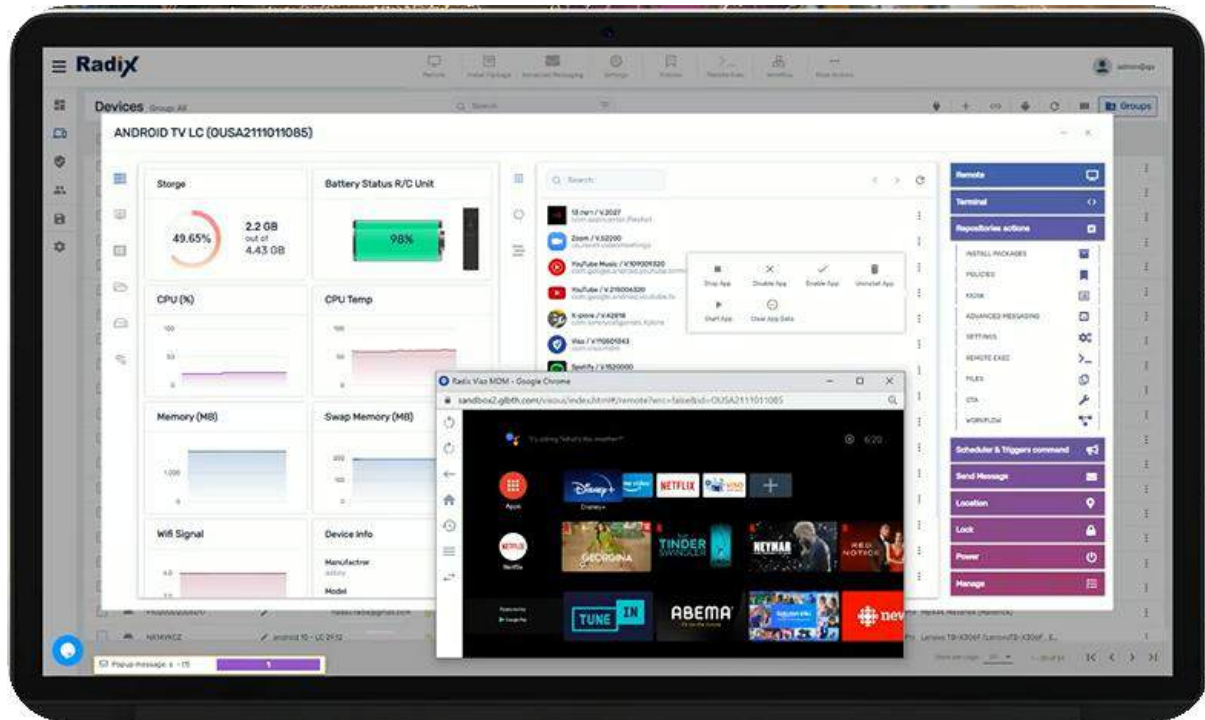


Table of Contents

Table of Contents	2
Chapter 1. Introduction	8
Chapter 2. Creating an Account and Logging In	9
2.1 Creating an Account.....	9
2.2 Logging into the Radix Device Management Platform	12
Chapter 3. Overview Dashboard.....	14
3.1 Overview Dashboard-Navigation Sidebar Menu.....	15
3.2 Overview Dashboard--Top Panes	19
3.3 Overview Dashboard—Middle Panes.....	19
3.4 Overview Dashboard—Bottom Panes	20
3.4.1 Last Commands Pane.....	21
Chapter 4. User Profile Menu.....	22
4.1 User Profile Settings Menu	23
4.1.1 Change User Password.....	23
4.1.2 Enable Two-Step Verification.....	24
4.2 Language Options	25
4.3 Dark Mode Options.....	26
4.4 Account Settings Menu	27
4.4.1 Remote Control Option	29
4.4.2 Pair with Organization Domain Option	31
4.4.3 Android for Work Registration.....	31
4.4.4 Device Pairing Option.....	34
4.4.5 Report Scheduling Option.....	35
4.4.6 Custom Columns Option.....	36
4.4.7 Health Check Thresholds Option.....	39
4.4.8 Import Tags and Labels	39
4.5 Billing History	44
4.5.1 Billing Data--Background	44
4.5.2 Fields of the Billing History screen	45
4.6 Users Management Menu.....	47
4.6.1 Adding a New User.....	48
4.6.2 Viewing a User's Profile	59
4.6.3 Changing the User's Interface Language	60

4.6.4	Granting Administrator Privileges to a User	60
4.6.5	Changing User Permissions.....	61
4.6.6	Deleting a User	64
4.7	Audit Logs	65
4.8	Sign out	66
Chapter 5.	Devices Table.....	67
5.1	Dynamic Groups Pane.....	68
5.1.1	Creating a New Group of Devices.....	69
5.1.2	Adding Devices to an Existing Group	82
5.1.3	Group Actions Options.....	84
5.1.4	Deleting a Group.....	85
5.1.5	Managing the New Devices Group.....	87
5.1.6	Summary of Remaining Group Commands	93
5.2	Top Action Bar.....	96
5.2.1	Enrolling a New Device	96
5.3	Group Status Bar.....	103
5.4	Bulk Actions Bar.....	105
5.5	Main Devices Table.....	106
5.6	Recent Commands Status bar	106
5.7	Main Devices Table in Detail	107
5.7.1	Devices Table Tabular Display	107
5.7.2	Device Usage Insights Display	114
5.7.3	Bulk Actions Options	116
5.7.4	Device Information Viewing Options	118
5.7.5	Who is Online?	119
5.7.6	Refresh	119
5.7.7	Filter Devices.....	120
5.7.8	Selecting Columns Option.....	125
5.8	Device Dashboard.....	127
5.8.1	Left Pane Icons-- Device Status Information	128
5.8.2	Center Pane Icons—App Management.....	129
5.8.3	Right Pane Options—Device Actions.....	131
Chapter 6.	List of Commands.....	147
6.1.1	Advanced Messaging/Messaging	147
6.1.2	Android for Work (AFW) install/uninstall	152

6.1.3	Change Agent Password.....	157
6.1.4	Clear Apps Cache.....	158
6.1.5	Clear Apps Data.....	160
6.1.6	Collect System Logs	161
6.1.7	Commands & Scripts	163
6.1.8	Device Settings	163
6.1.9	Direct Message	177
6.1.10	Disable/Enable apps	177
6.1.11	Export Device Data to CSV	179
6.1.12	Firmware Update.....	180
6.1.13	Install App/Install Package	180
6.1.14	Kiosk.....	187
6.1.15	Manage users.....	211
6.1.16	Messaging	213
6.1.17	Metrics	213
6.1.18	OTA	213
6.1.19	OTA Update Engine	215
6.1.20	Play Siren.....	218
6.1.21	Policies (Block Lists)	218
6.1.22	Remote Control	234
6.1.23	Remote Execute/Commands & Scripts	238
6.1.24	Remove Google Accounts from Device	246
6.1.25	Restart.....	247
6.1.26	Scheduler & Triggers Command.....	248
6.1.27	Screen Settings.....	255
6.1.28	Send Files.....	256
6.1.29	Shutdown	263
6.1.30	Smart Recovery	263
6.1.31	Standby	272
6.1.32	Tags.....	272
6.1.33	Terminal.....	274
6.1.34	Uninstall Packages	275
6.1.35	Views	276
6.1.36	Wake on LAN	281
6.1.37	Wake Up	284

6.1.38	Windows Update	284
6.1.39	Workflow	286
6.2	Warning Icons	290
6.2.1	Invalid Authentication Token Warning	291
6.2.2	Ad-Hoc Session	292
Chapter 7.	Libraries Menu	297
7.1	Deployment Options	297
7.1.1	Apps	297
7.1.2	Messaging	298
7.1.3	Commands and Scripts	298
7.1.4	OTA	299
7.1.5	OTA Update Engine	299
7.1.6	Files	300
7.1.7	Smart Recovery	300
7.2	Configurations Options	301
7.2.1	Device Settings	301
7.2.2	Block Lists	301
7.2.3	Kiosk Modes	301
7.2.4	Views	302
7.2.5	Android for Work	303
7.3	Automation Options	306
7.3.1	Workflows	306
7.3.2	Schedules & Triggers	307
Chapter 8.	Device Templates Console	308
8.1	Creating a New Template	308
8.1.1	Overview Panel	312
8.1.2	Population Panel	313
8.1.3	Content Panel	316
8.1.4	Command Status View and Delete Options	335
8.1.5	Roll-out Panel	337
8.2	Starting a Device Template	343
8.3	Stopping a Template	346
8.4	Editing a Template	348
8.5	Viewing a Previous Version of a Template	351
8.6	Setting the Priority of Templates	353

8.7	Deleting a Template	354
Chapter 9.	Device Health Console.....	356
9.1	Device Health Pane.....	356
9.1.1	Device Health Graphs	357
Chapter 10.	Command History Log	376
10.1	Types of Commands in the Command History Log	376
10.2	Command Search Options.....	376
10.3	Viewing the Status of a Particular Command.....	377
10.4	Executing Commands from the Command History Log.....	379
10.5	Use of the Persist Command for Groups.....	380
Chapter 11.	Further Resources.....	382
Chapter 12.	Appendices.....	383
	Appendix A—Alphabetical List of Commands	383
12.1	Methods of Accessing Commands.....	383
12.1.1	Advanced messaging	387
12.1.2	AFW Install/Uninstall.....	387
12.1.3	Block Lists (Policies)	387
12.1.4	Change Agent Password	387
12.1.5	Clear apps cache.....	388
12.1.6	Clear apps data	388
12.1.7	Collect system logs.....	388
12.1.8	Device Alert	388
12.1.9	Device Settings.....	389
12.1.10	Direct Message.....	390
12.1.11	Disable/Enable Apps	390
12.1.12	Export Device Data to CSV.....	390
12.1.13	Firmware update.....	391
12.1.14	Edit Group.....	391
12.1.15	Install App/Install Packages.....	391
12.1.16	Kiosk.....	392
12.1.17	Manage Users.....	392
12.1.18	Metrics	392
12.1.19	OTA (= Over-the-Air).....	392
12.1.20	OTA Update Engine	392
12.1.21	Policies/Block Lists	393

12.1.22	Remote Control	393
12.1.23	Commands & Scripts/Remote Execute	393
12.1.24	Remove Google Accounts from a Device	393
12.1.25	Restart.....	393
12.1.26	Scheduler & trigger command	394
12.1.27	Screen settings.....	394
12.1.28	Send Files/Files	394
12.1.29	Shutdown	394
12.1.30	Smart Recovery (Windows Devices Only).....	394
12.1.31	Siren/Sound Siren.....	395
12.1.32	Standby	395
12.1.33	Tags.....	395
12.1.34	Timeout.....	395
12.1.35	Uninstall Packages	395
12.1.36	Views	396
12.1.37	Wake on LAN	396
12.1.38	Wake Up	396
12.1.39	Windows Update	396
12.1.40	Workflow	396
12.2	Pinning and Unpinning Commands	397
Appendix B: General Devices Table Tile options.....		398
12.3	Repository Tile Command Editing Options	398
12.3.1	Pick Color	399
12.3.2	Pick Icon	399
12.3.3	Edit Icon.....	400
12.3.4	Clone.....	400
12.3.5	Delete.....	400
12.3.6	Pin to Top.....	401
Appendix C: List of All Commands.....		402
Appendix D: Smart Recovery Version Comparison		404
Appendix E: Remote Execute Command Reference		405

Chapter 1. Introduction

The Radix Device Management Platform is a comprehensive, SaaS turnkey solution to manage entire fleets of devices remotely, without the need to set up local servers. The Radix platform can be used on Android devices as well as devices running Windows, or ChromeOS. The latest release of the Radix Device Management Platform features a new UI that is faster, more feature-rich, and more secure.

Here is just a partial list of some of the things that the Radix Device Management Platform will allow you to do:

- Install several apps on an entire fleet of devices at once,
- Send files and important alerts to users on their devices,
- Assist users by adjusting settings on their devices,
- Block problematic software apps from devices,
- Allow only certain software apps, to operate a device in “Kiosk” mode,
- And much more.

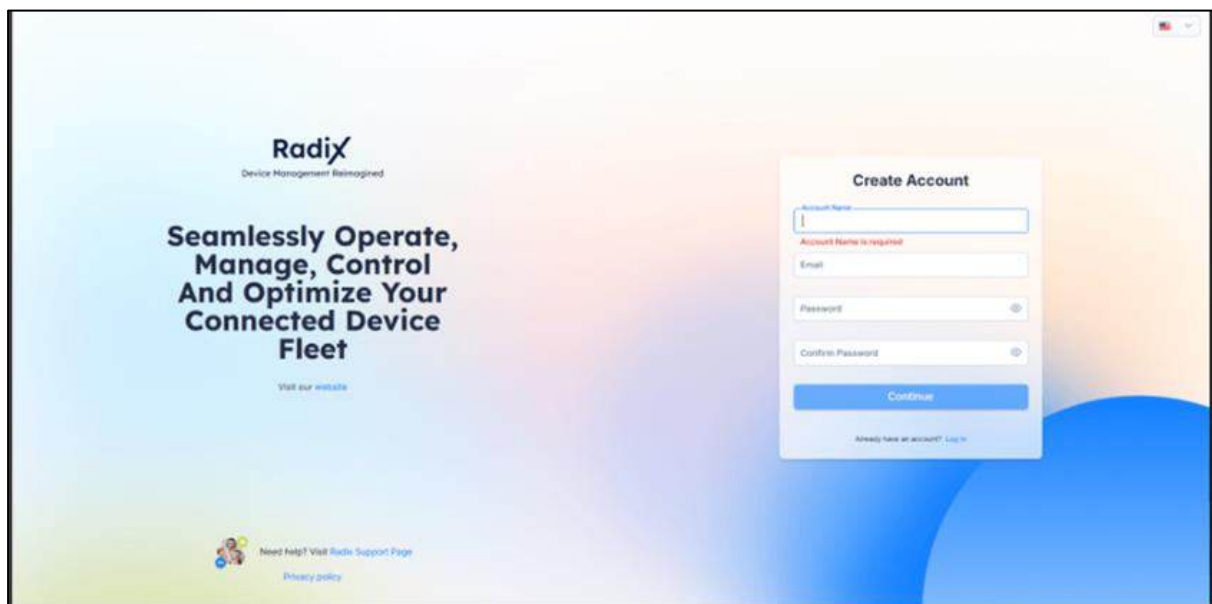
We will first go over the general layout of the Radix Device Management Platform. After that, we will step you through how to get the most out of its many features.

Chapter 2. Creating an Account and Logging In

2.1 Creating an Account

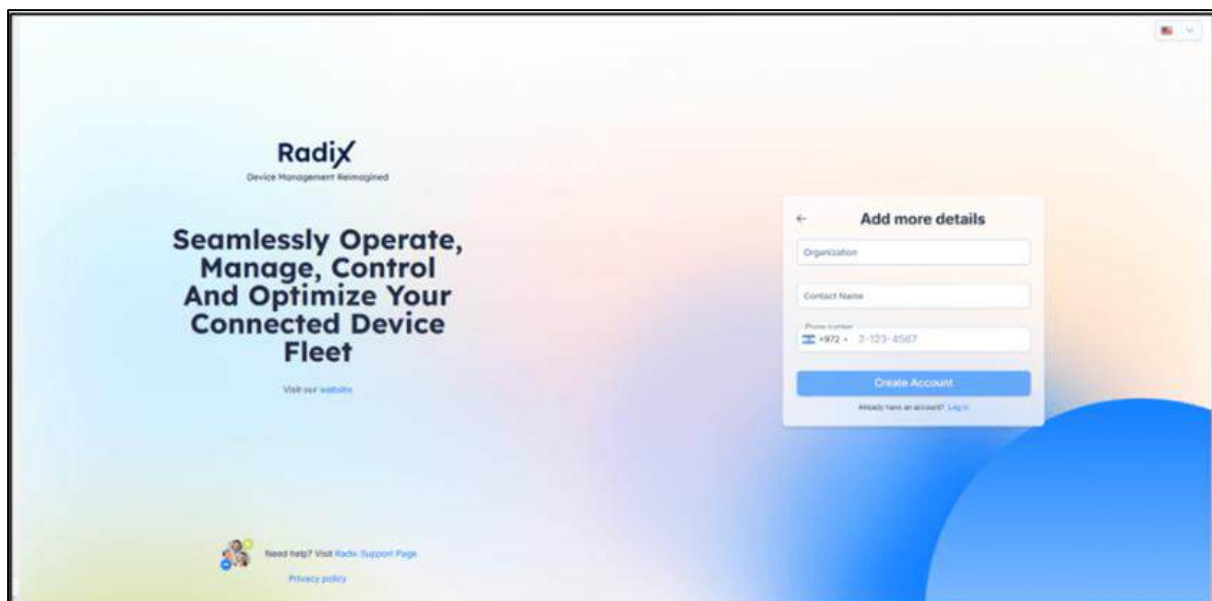
You can create an account in the Radix Device Management Platform, either as an administrator, user, or just “supporter” (where you can only request customer support).

1. [Click here](#) to register in the Radix Device Management Platform console. The following Registration Form window opens:



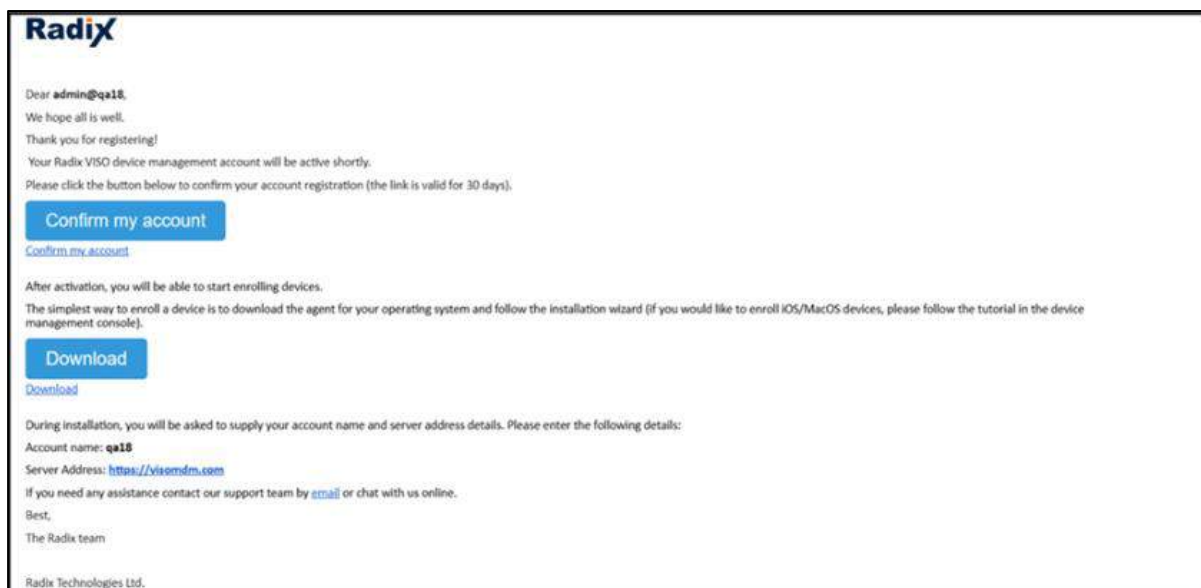
The screenshot shows the Radix Device Management Platform registration page. On the left, the Radix logo is at the top, followed by the tagline 'Device Management Reimagined'. Below this is the main heading 'Seamlessly Operate, Manage, Control And Optimize Your Connected Device Fleet' and a link 'Visit our website'. At the bottom left, there are links for 'Need help? Visit Radix Support Page' and 'Privacy policy'. On the right, a 'Create Account' form is displayed. The form has a title 'Create Account' and a back arrow. It contains four input fields: 'Account Name' (with a red error message 'Account Name is required'), 'Email', 'Password', and 'Confirm Password'. Below these fields is a blue 'Continue' button. At the bottom of the form, there is a link 'Already have an account? Log In'.

2. After you complete the details and click **Continue**, you will be requested to enter the details of your organization, contact name, and phone number:



The screenshot shows the Radix Device Management Platform 'Add more details' page. On the left, the Radix logo is at the top, followed by the tagline 'Device Management Reimagined'. Below this is the main heading 'Seamlessly Operate, Manage, Control And Optimize Your Connected Device Fleet' and a link 'Visit our website'. At the bottom left, there are links for 'Need help? Visit Radix Support Page' and 'Privacy policy'. On the right, an 'Add more details' form is displayed. The form has a title 'Add more details' and a back arrow. It contains three input fields: 'Organization', 'Contact Name', and 'Phone number' (with a pre-filled number '+972 2-123-4567'). Below these fields is a blue 'Create Account' button. At the bottom of the form, there is a link 'Already have an account? Log In'.

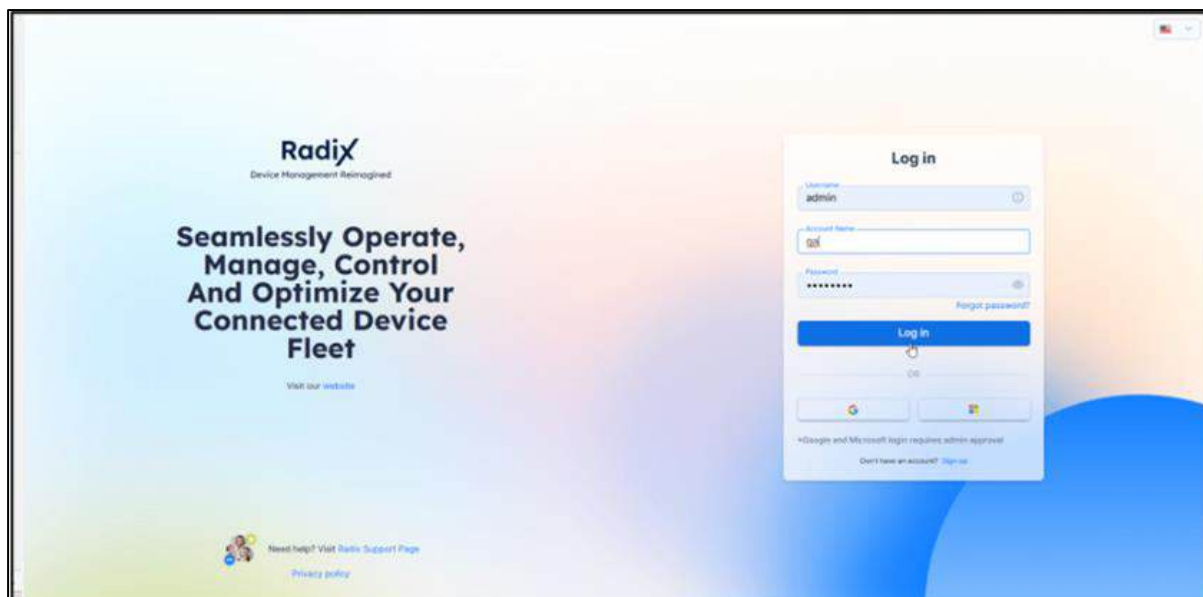
3. Upon clicking **Create Account**, you should receive an email containing an account activation link.



4. Make sure you click on **Confirm my account** to activate your account. The confirmation link is valid for 30 days after you register.
5. The EULA screen opens. Check the **I agree** checkbox and click **OK** to accept the terms and conditions.



6. Upon clicking **OK**, the Radix Device Management Platform login screen opens.



Once you have created an account, you can log in to your account using your Google or Microsoft account credentials as well.

1. If you add a user who with the option to log in with a Google/Microsoft account, a confirmation email will be sent to the user. The user will be able to log in after confirmation.

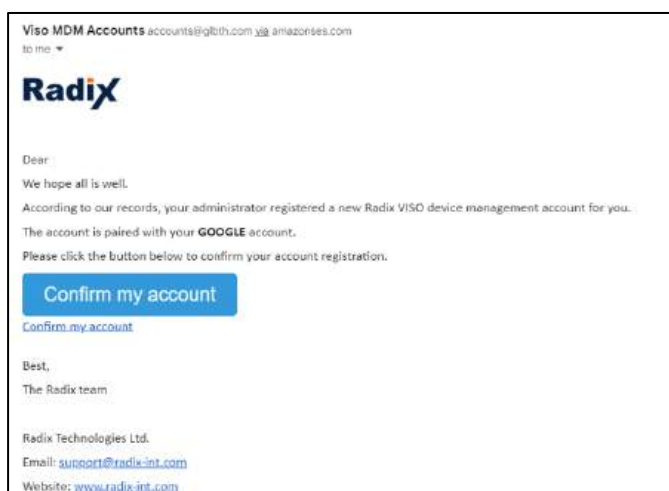


Figure 2-1: Google Confirmation E-mail

Upon your first login, you will see the End User License Agreement.

Terms and conditions

END USER LICENSE AGREEMENT

[Last Amended: May 11, 2025]

This End User License Agreement ("EULA") governs your engagement with Radix Technologies Ltd. ("Radix", "Company", "we", "us", "our"), with respect to the usage of Radix's Dashboard and Product (as defined herein).

Radix specializes in providing advanced device management solutions through a comprehensive, cloud-based platform designed to simplify the administration and security of various devices across diverse environments ("Product"). Our offerings support customers who have purchased the right to use our Products, whether directly from us or indirectly through any of our distributors and business partners ("Customer/s"). The Customers may include educational institutions, enterprises, and public sectors, using the Product to ensure their managed devices ("Device/s") remain healthy, secure, and optimally tuned to their mission. Key features of the product include centralized control over the Devices, remote installation and updates, and comprehensive security monitoring and management features. The Customer and its authorized users are able to control and operate those features through the use of a designated web interface ("Dashboard"), which is an integral part of the Product or provided otherwise by the Customer.

This EULA is a legally binding and enforceable agreement between Radix and you, a user of the Product ("End User" or "you"), whether you are the Customer itself or any of its authorized users. The End User and Radix shall each be referred to herein as a "party" and collectively as the "parties".

ACCEPTANCE OF THE TERMS: BY REGISTERING AND ACCESSING THE DASHBOARD OR OTHERWISE USING THE PRODUCT, OR BY OTHERWISE USING THE PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO THE TERMS OF THIS EULA. YOU AGREE TO BE BOUND BY THIS EULA AND TO COMPLY WITH ALL APPLICABLE LAWS AND REGULATIONS REGARDING YOUR USE OF THE PRODUCT. IF YOU DO NOT AGREE TO ALL OR PART OF THIS EULA PLEASE DO NOT REGISTER OR USE THE PRODUCT OR ITS FEATURES IN ANY MANNER.

1. REGISTRATION AND ACCOUNT

1.1 In order to use and access the Dashboard or the Product, you must have a registered account ("Account"), created for you independently or by the Customer. As part of the registration process, we will collect your name and a valid email address, and designate you with a personal username and password.

☐ I agree
 OK

2. Check the **I agree** checkbox and click **OK**.

Note: A user who logs in via a Google or a Microsoft account can be related to only one domain. If you would like to switch to another domain, the user will have to be removed from the previous domain.

2.2 Logging into the Radix Device Management Platform

1. To start using Radix Device Management Platform, go to the [login page](#). You will see the login screen on the right side, along with a brief description of the advantages of the Radix Device Management on the left.

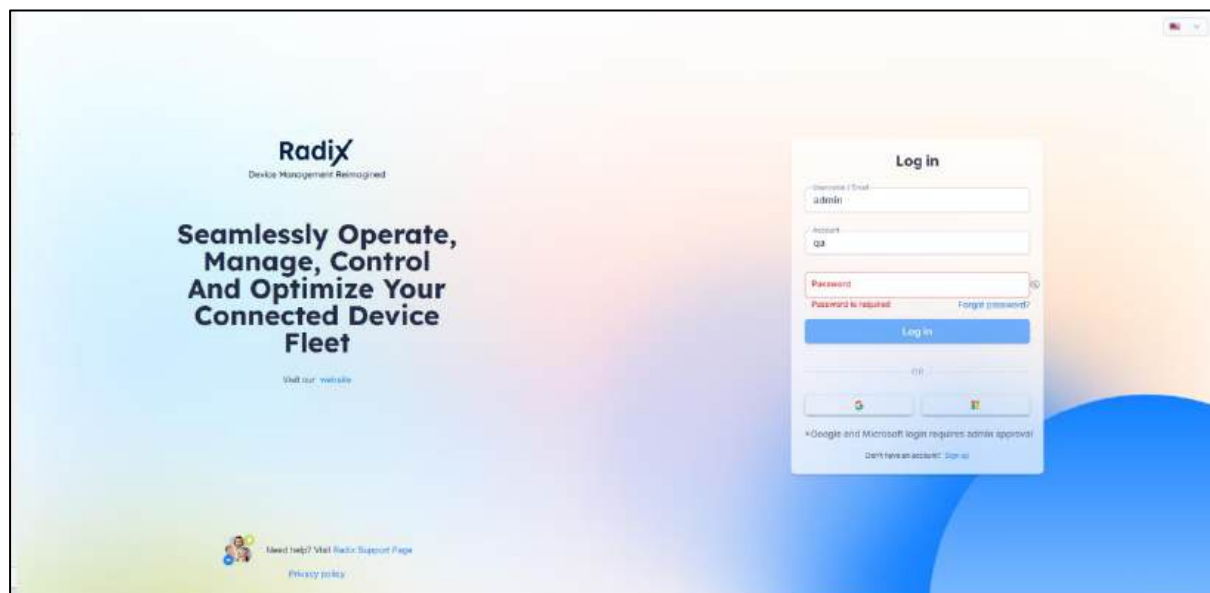
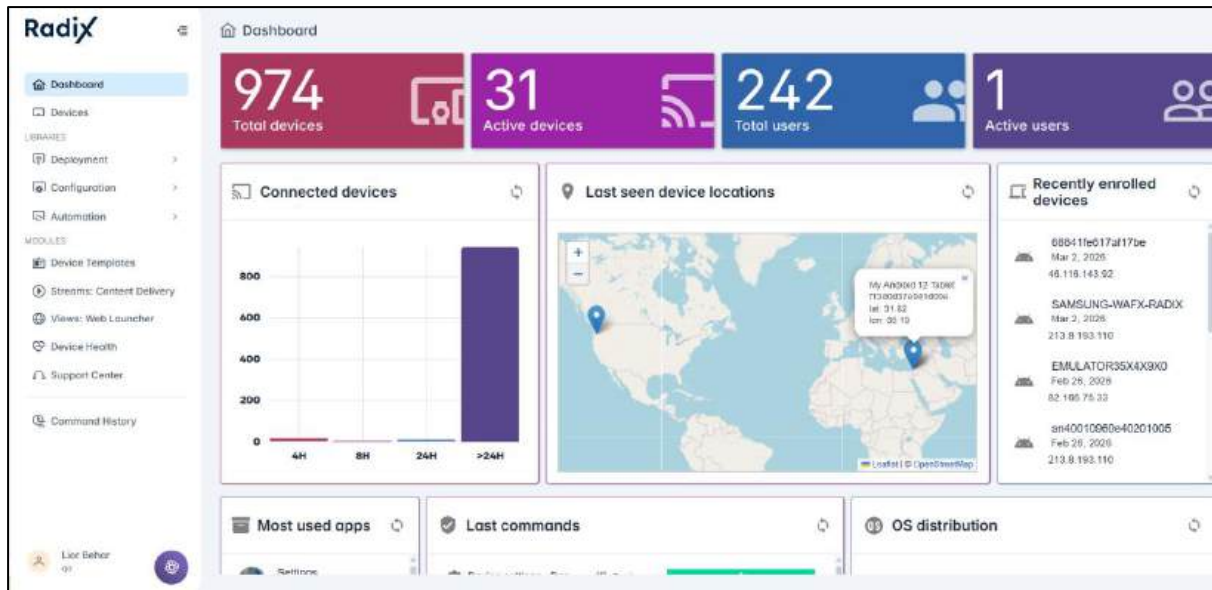


Figure 2-2: Radix Device Management Login Screen

2. Enter the username, account name, and password as you entered them when registering your account.
When you click **Log in**, the Overview Dashboard of the Radix Devices Table opens.



We will examine the sections of the Overview Dashboard in the next chapter.

Chapter 3. Overview Dashboard

After successfully logging in, you will see the **Overview Dashboard**, which gives information about the number of devices and users presently active, and which apps and operating systems they use the most.

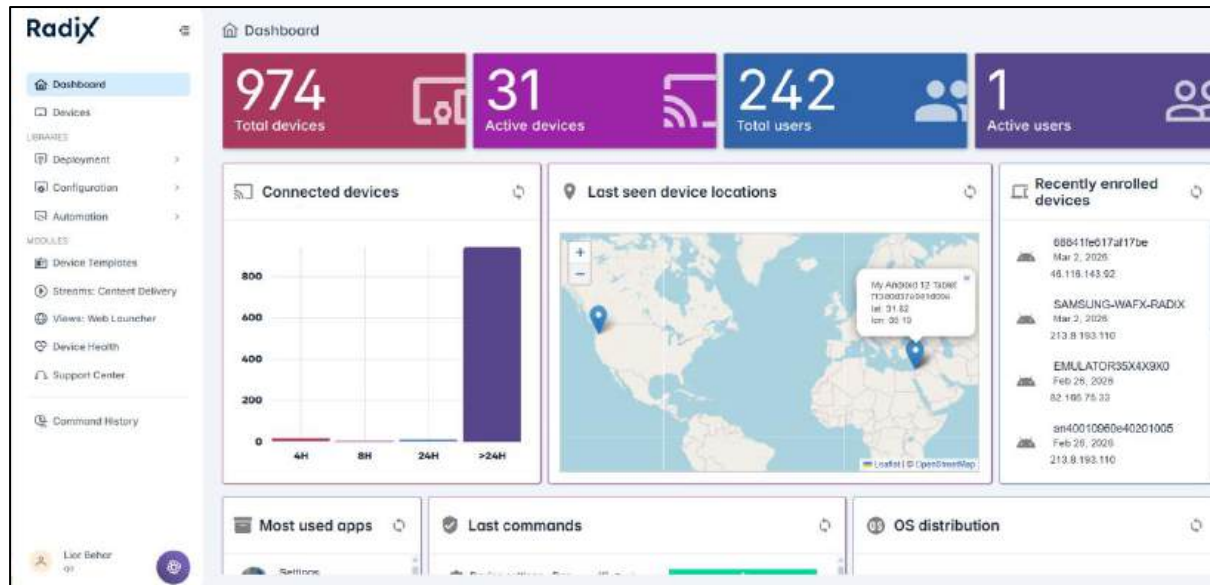


Figure 3-1: Overview Dashboard—Top Pane

You can collapse the sidebar menu on the left side of the screen by clicking on the “hamburger menu” on the upper left:

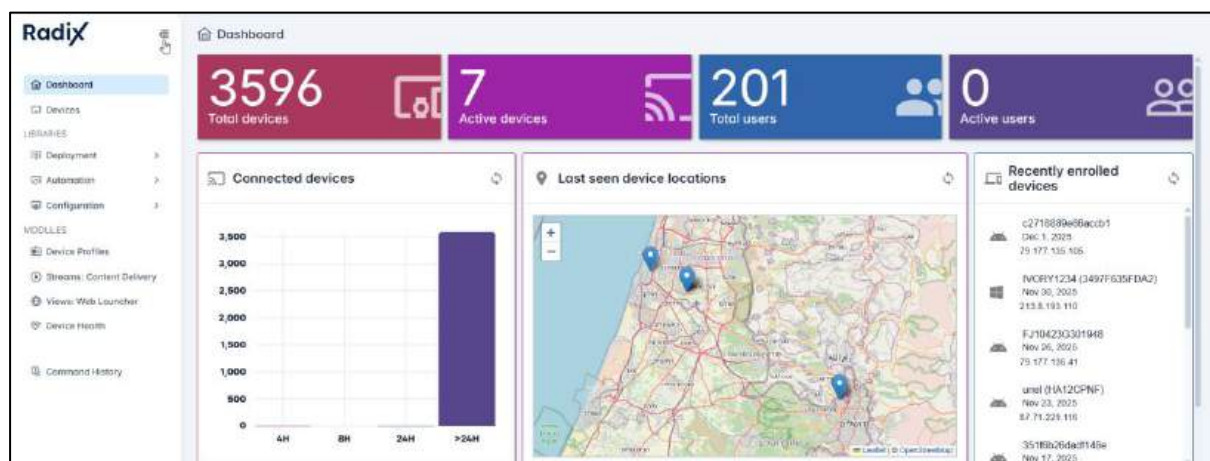
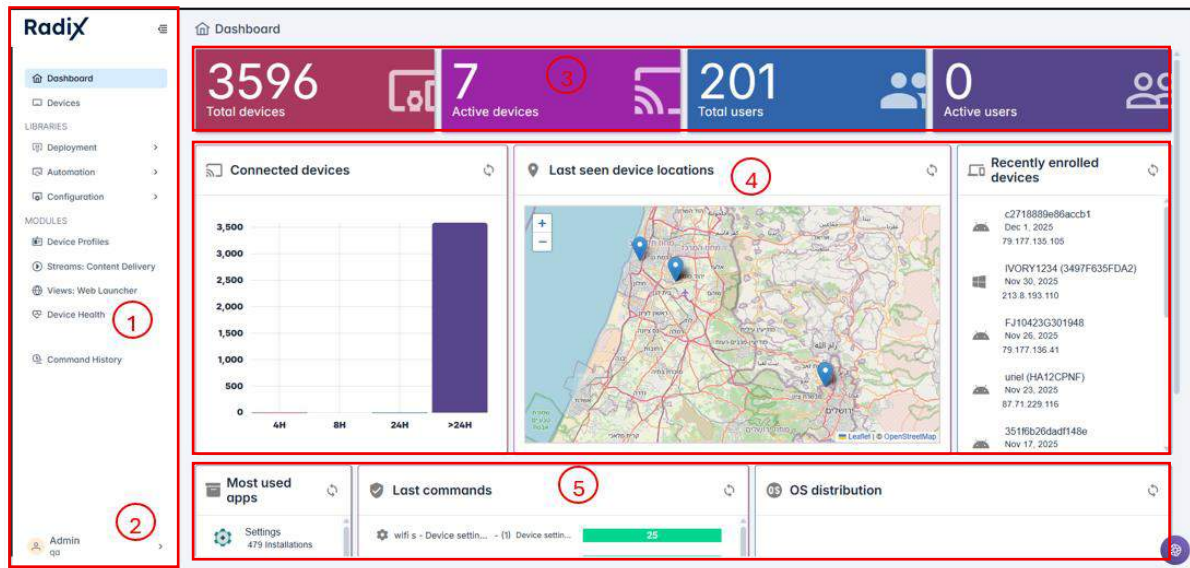


Figure 3-2: Overview Dashboard—Top Pane with Hamburger Menu expanded

We will explain the purpose of each section of the Overview Dashboard:

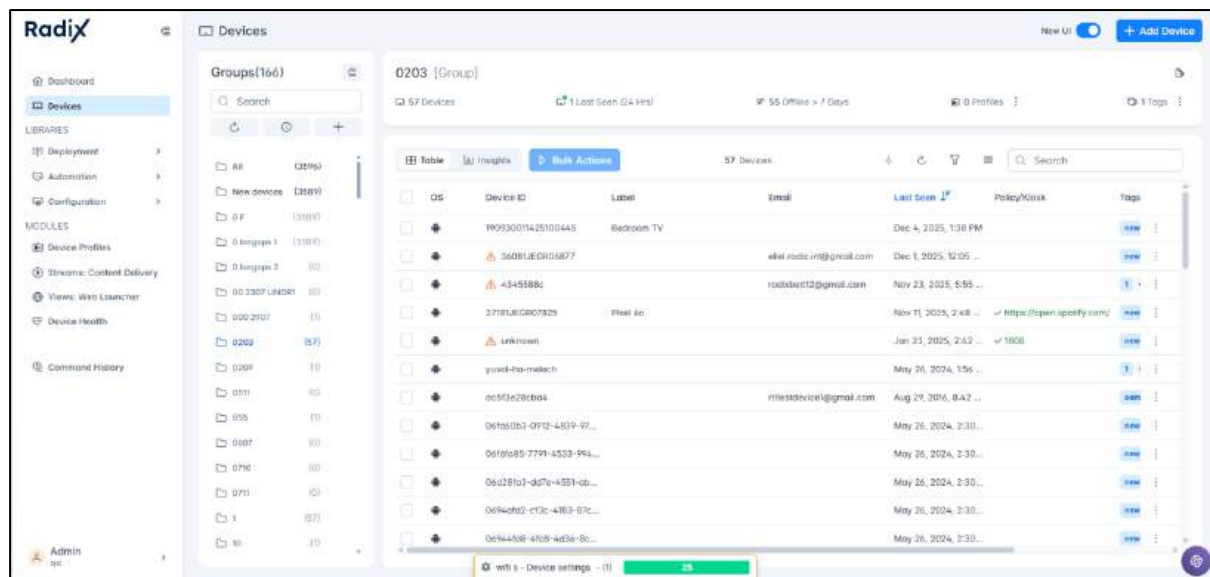


Item	Description
①	Navigation Sidebar Menu
②	User Account and Profile Menu
③	Device and User Summary
④	Device Location and Enrollment Summary
⑤	App Usage and Commands Summary

3.1 Overview Dashboard-Navigation Sidebar Menu

The Navigation sidebar menu on the side of the Radix Device Management Platform gives you access to all of the options in the Radix Device Management Platform. Here is a brief summary of each menu item:

- **Dashboard** displays information about the number of enrolled devices, their location, apps usage, and results of commands,
- **Devices** displays the Devices Table, where you can view information about all enrolled devices.

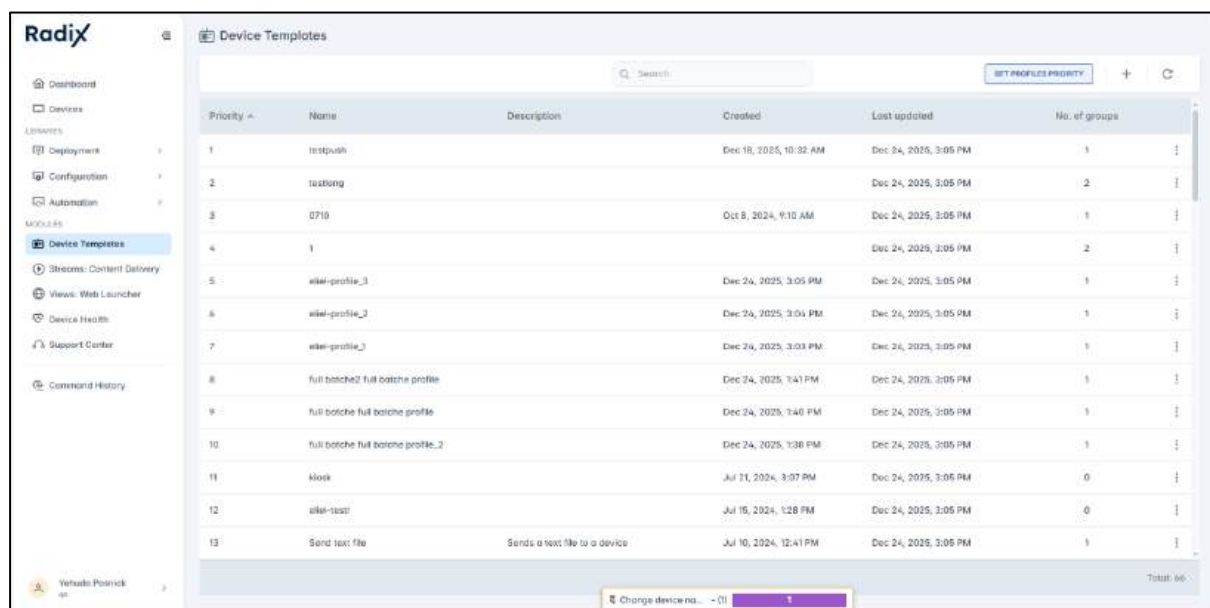


The **Libraries Section** gives a drop-down list of software and apps that can be sent to remote devices. It consists of the following menus:

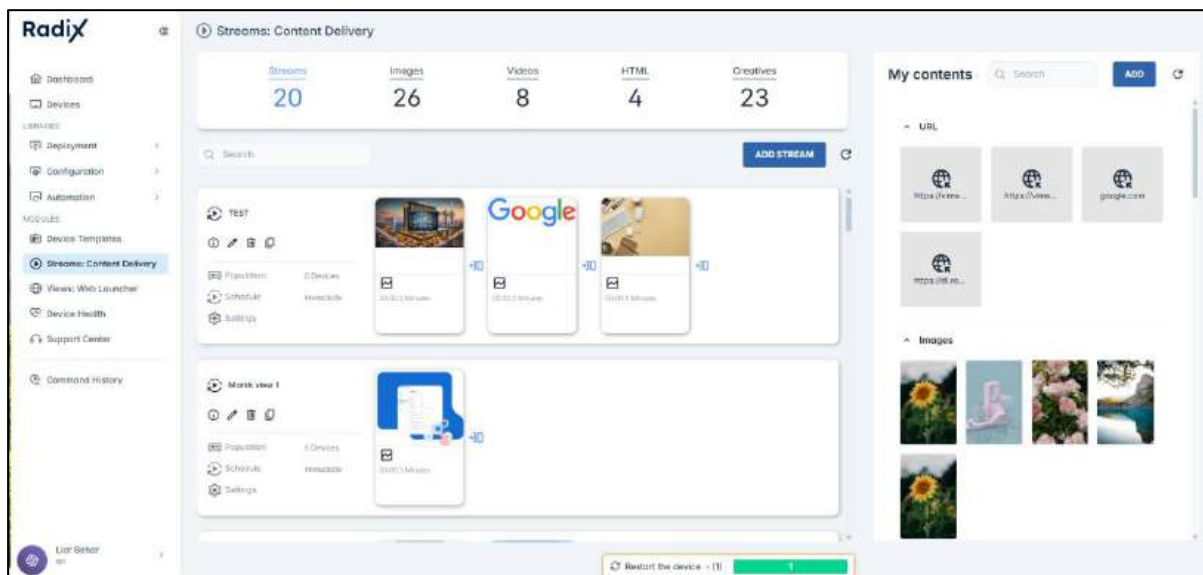
- The **Deployment** menu allows you to install apps, send messages and files, and run commands or scripts on remote devices,
- The **Automation** menu allows you to compose a workflow (a sequence of commands to be executed on remote devices), or to execute commands in accordance with a trigger,
- The **Configuration** menu gives a drop-down menu of commands to manage device settings as well as the apps that can be run on remote devices.

The **Modules Section** includes additional consoles that provide additional functionality and control over your fleet of remote devices. These consoles include:

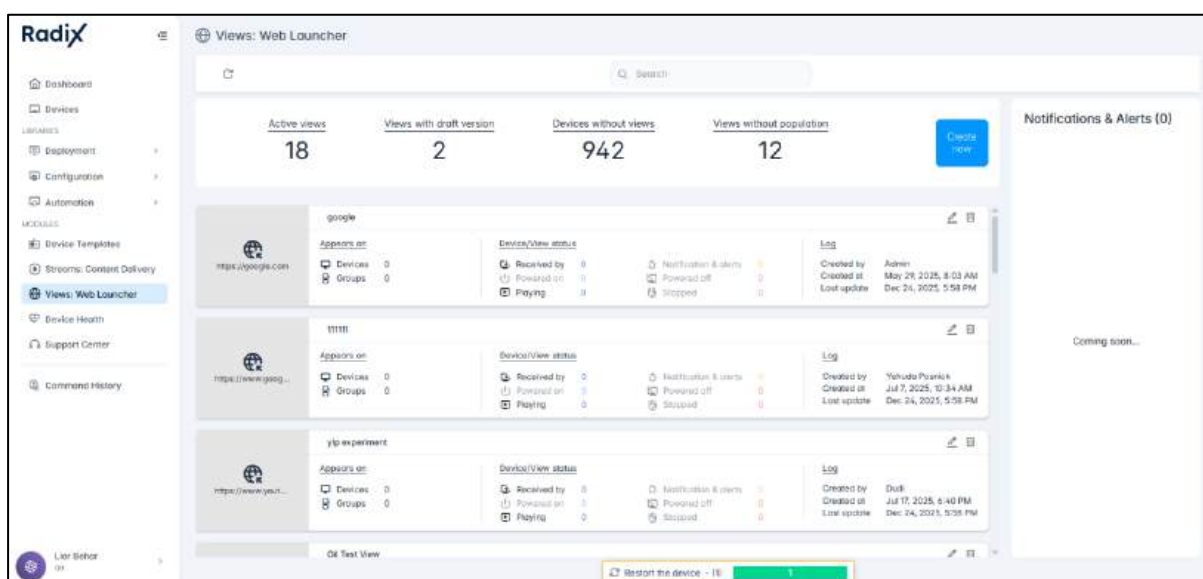
- **Device Templates** opens the **Device Templates** module, which allows you to configure content and apps on entire groups of devices.



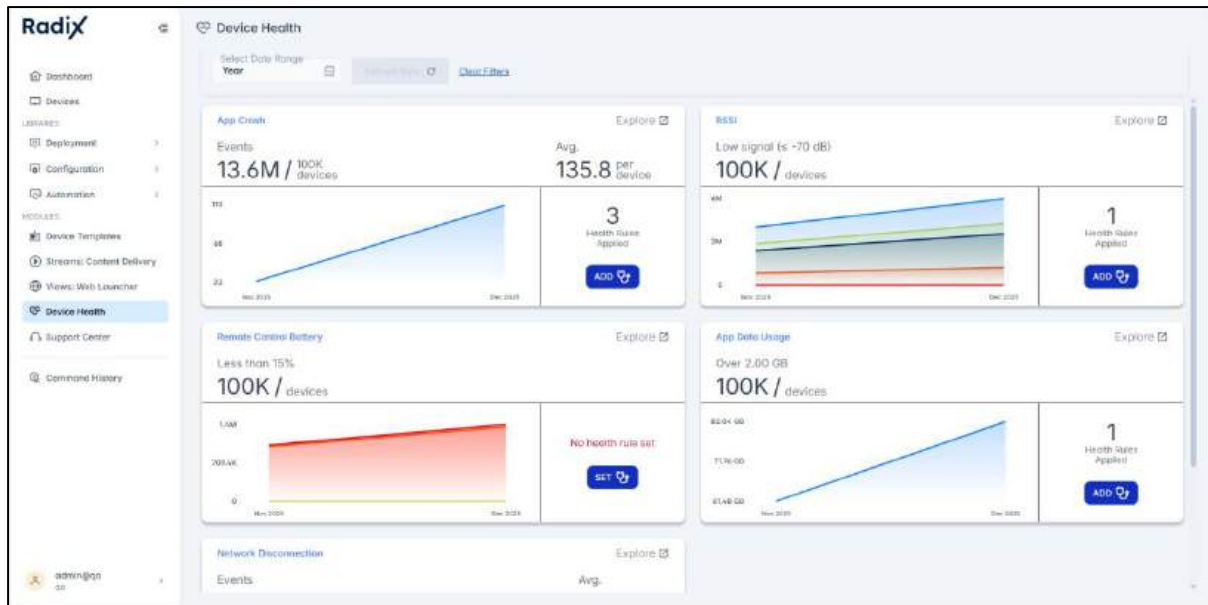
- **Streams: Content Delivery** opens the Streams Console, where the user can create a slideshow consisting of images, video clips, or creative content.



- **Views: Web Launcher** opens the Views Console, where the user can display a video clip from a URL on a group of devices.



- **Device Health** opens a console that displays data on app crashes, battery power, app usage, network disconnections, and low Wi-Fi signals to devices.

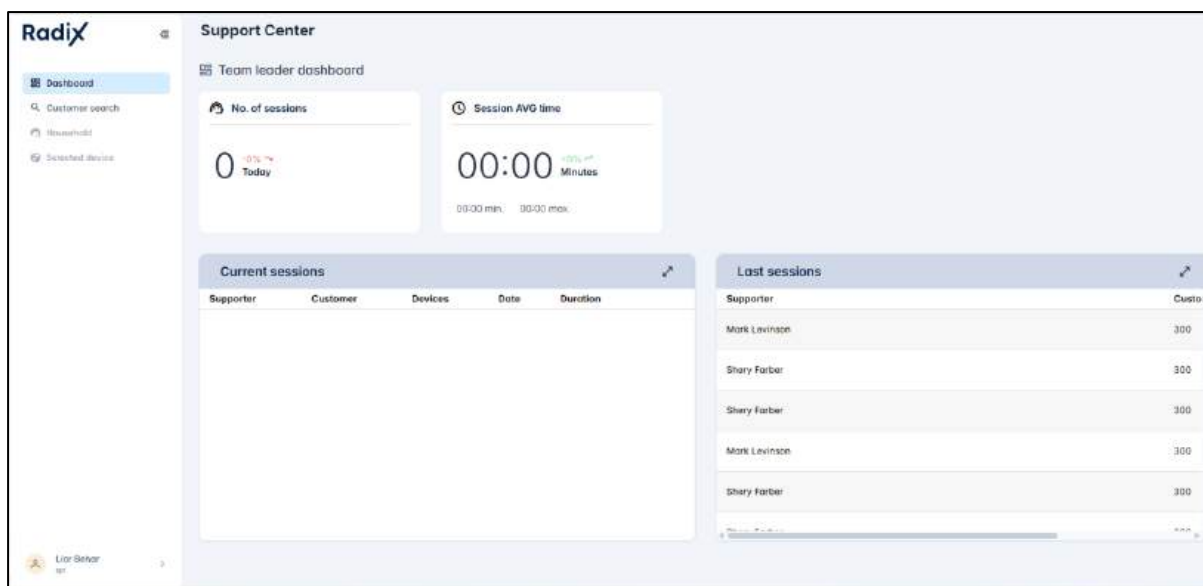


- **Command History Log** displays the Command History Log, showing all commands sent to devices and their results.

The Command History Log displays a list of commands sent to devices. The table has columns: Type, Description, Command, Group, Owner, and Creation time. The commands listed are:

Type	Description	Command	Group	Owner	Creation time
Ad-Hoc	Screen Settings Command	Screen settings command		na@vovni@ga	Dec 29, 2025, 7:24:22 PM
Ad-Hoc	Screen Settings Command	Screen settings command		na@vovni@ga	Dec 29, 2025, 7:24:05 PM
Ad-Hoc	Advanced Messaging : Youtube Fujitsu crash test	Advanced messaging		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:09:33 PM
Ad-Hoc	Advanced Messaging : Youtube Fujitsu crash test	Advanced messaging		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:08:49 PM
Ad-Hoc	Advanced Messaging : Youtube Fujitsu crash test	Advanced messaging		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:07:24 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:03:19 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:02:36 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 7:01:16 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 6:45:15 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 6:40:33 PM
Ad-Hoc	Device settings : ktc prometheus test	Device settings		U36403nFw6MAOQePyBuApLvcYrSF@ga	Dec 29, 2025, 6:39:40 PM

- **Support Center** opens an interface that shows data of customer support on devices.



3.2 Overview Dashboard--Top Panes

The banner at the top of the page displays the following information:

- **Total devices:** The total number of devices enrolled in the system.
- **Active devices:** The number of devices that are active in the last 24 hours.
- **Total users:** The total number of users enrolled in the system.
- **Active users:** The number of users who are presently using the system (excluding yourself).



Figure 3-3: Overview Dashboard--Top Panes

3.3 Overview Dashboard—Middle Panes

Underneath the top ribbon, you will see fields that show the number of devices that are presently connected and where they are located, as well as the ID of recently enrolled devices, with information about the operating system that they use, the Device ID, the enrollment date, and the device's IP address. Clicking on the **Reload** icon  in any of the fields will update the information.

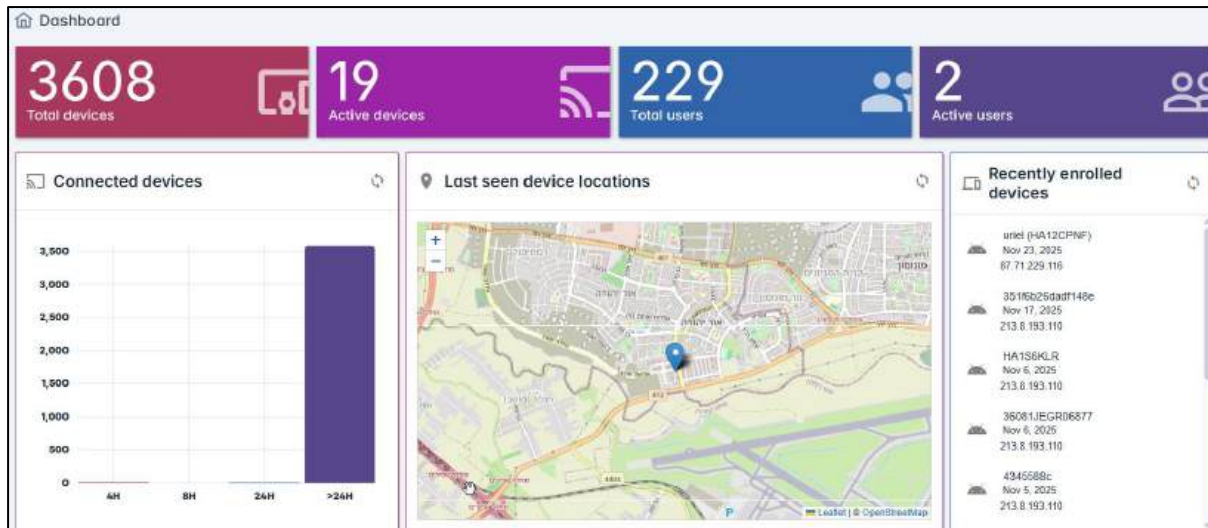


Figure 3-4: Overview Dashboard--Middle Panes

The middle panes display the following information:

- **Connected devices:** The total number of devices enrolled in the system, according to their last check-in time.
- **Last seen device locations:** The locations of the last devices who reported their connection to the domain. As we will see, this can be useful in locating a device, in a situation where a device is lost or stolen.
- **Recently enrolled devices:** The devices in your fleet that logged in most recently to the Radix Device Management Platform, as well as the date and IP address of the login.

3.4 Overview Dashboard—Bottom Panes

In the bottom section of the **Overview Dashboard**, you will see fields that display the most used apps among the active devices, the last commands that were used, and the distribution of operating systems among the active devices.

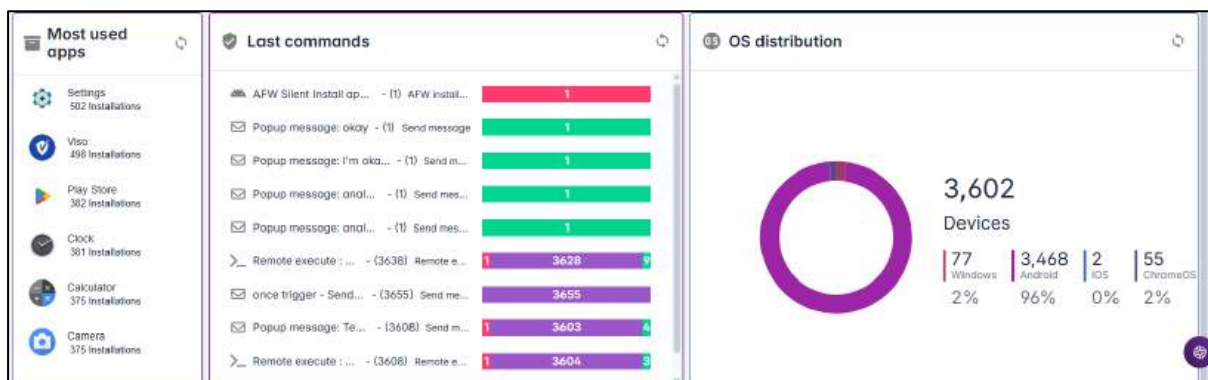


Figure 3-5: Overview Dashboard--Bottom Pane

The bottom panes display the following information:

- **Most-used apps:** Statistics regarding the most frequently used apps.
- **Last commands:** A list of the last-performed commands.

- **OS distribution:** A pie chart showing the distribution of operating systems among the devices.

3.4.1 Last Commands Pane

The **Last Commands** pane gives you information about the latest commands that you sent to a device or a fleet of devices. If you click on any particular command, the **Command Status** window opens, telling you when the command was sent to the device, and whether or not it was executed.

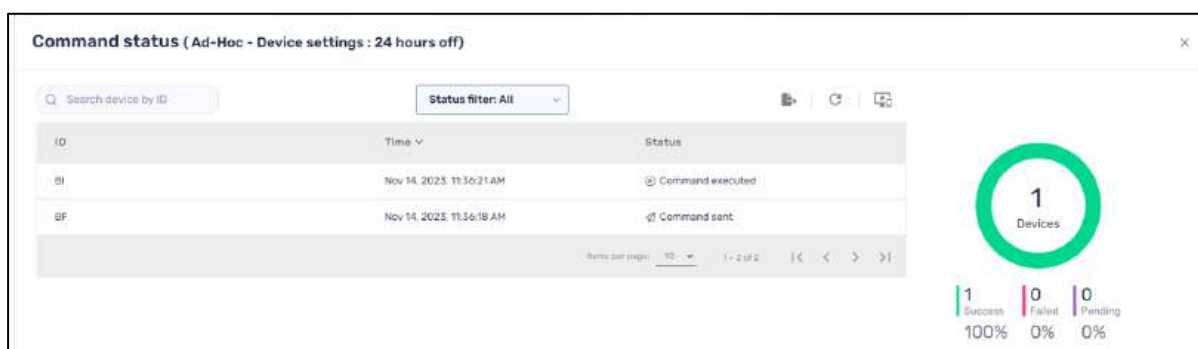


Figure 3-6: Command Status window, showing that the command was successfully executed

We will see the Command Status window when we discuss the Commands History Log (Chapter Chapter 10).

Chapter 4. User Profile Menu

When you click on the **User** icon  in the lower left of the Radix Device Management Dashboard, you will see the **User Profile Menu**. For Radix Device Management users with Admin privileges, it offers the following options:

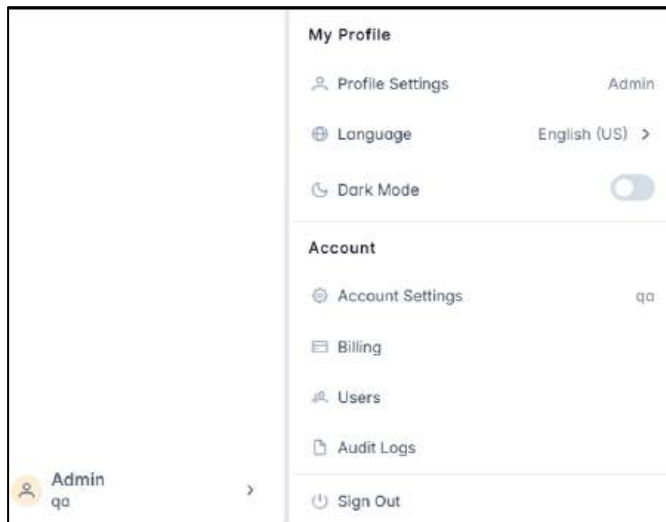


Figure 4-1: User Profile Menu, in lower left corner

My Profile Options

- **Profile Settings**, with user account options (**Section 4.1**)
- **Language**, for adjusting the interface language (**Section 4.2**)
- **Dark Mode**, to toggle between a white or dark background (**Section 4.3**)

Account Options

- **Account Settings**, which opens the Account Settings Menu (**Section 4.4**).
- **Billing**, displaying information about payments and credit balance (**Section 4.5**).
- **Users**, which opens the Users Management Menu, with a list of all users, their email addresses, level of authority, and status (**Section 4.6**).
- **Audit logs** allows you to view all of the commands sent by a user (**Section 4.7**).
- **Sign out**, to exit the system (**Section 4.8**).

Note: For Radix Device Management users with only User privileges, the User menu will not have the “Billing” option.

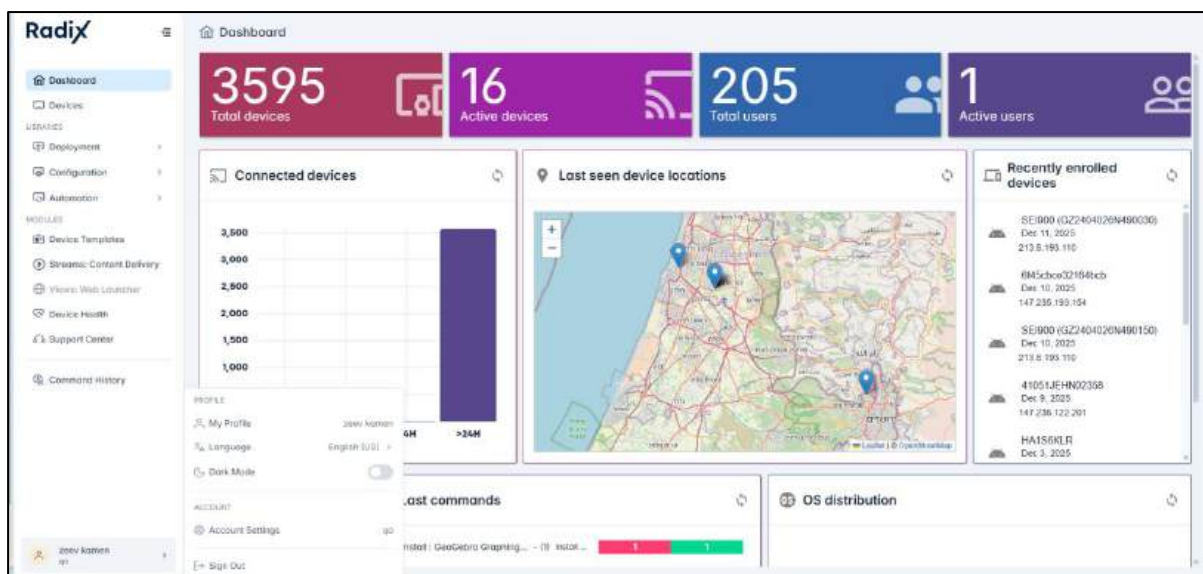


Figure 4-2: User Profile menu for non-Admin users. The Billing, Users, and Audit Logs options are missing.

We will go through the options in detail:

4.1 User Profile Settings Menu

The **My Profile** option in the drop-down menu displays your Username, Contact Name, Email address, and the current interface language. It also has options to change your user password or enable two-step verification on your account, to make the login process more secure.

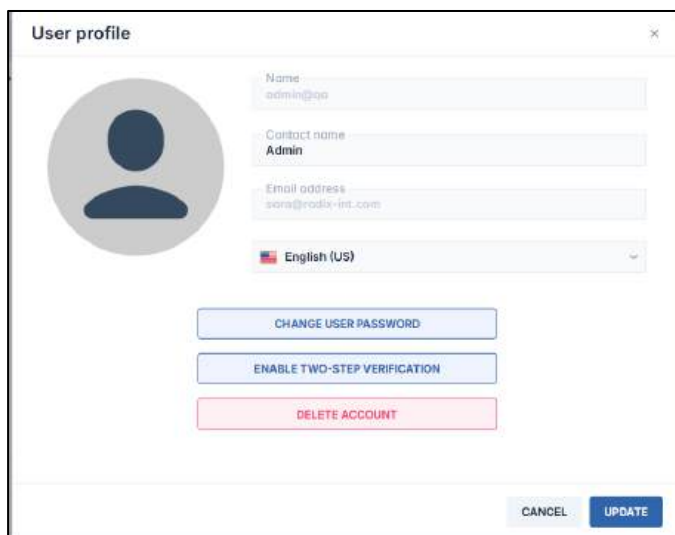
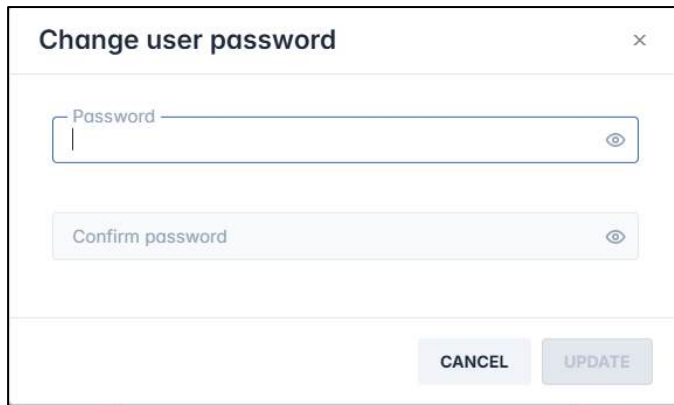


Figure 4-3: User Profile Screen, with options to change password, enable two-step verification, or delete an account

4.1.1 Change User Password

This allows the user to change the password they use to log in to the Radix Device Management Platform.

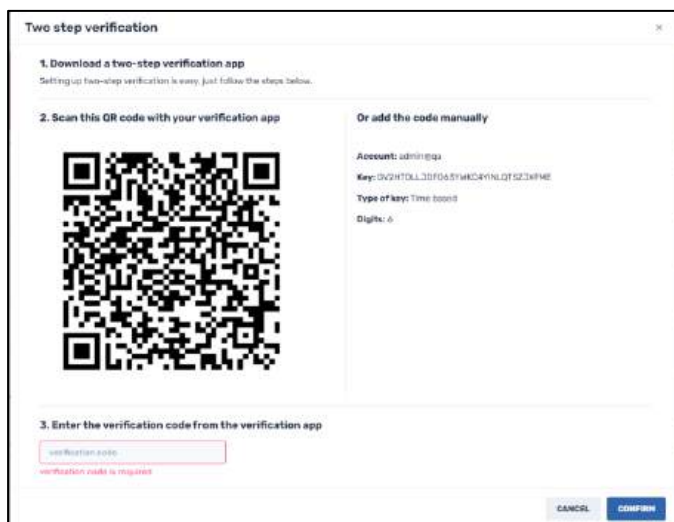


A dialog box titled "Change user password" with a close button (X) in the top right corner. It contains two input fields: "Password" and "Confirm password", both with eye icons for toggling visibility. At the bottom, there are two buttons: "CANCEL" and "UPDATE".

4.1.2 Enable Two-Step Verification

To enable two-step verification:

1. Download a two-step verification app, such as Google Authenticator or Microsoft Authenticator.
2. Perform the verification either by:
 - a. Scanning a QR code provided by the verification app, or
 - b. Manually entering the verification code that the verification app provides.



A dialog box titled "Two step verification" with a close button (X) in the top right corner. It contains three steps:

- Download a two-step verification app. Setting up two-step verification is easy. Just follow the steps below.
- Scan this QR code with your verification app. To the right, under "Or add the code manually", it shows account details: Account: admin@qa, Key: 0V2HTOLL3DF0A5YMK54YNLQF523K8WE, Type of key: Time based, Digits: 6.
- Enter the verification code from the verification app. A text input field is shown with a red border and the text "verification code is required" below it.

 At the bottom, there are two buttons: "CANCEL" and "CONFIRM".

Figure 4-4: Two-step verification options

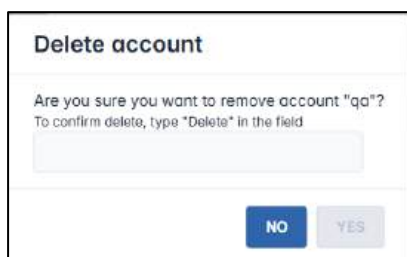
If you have Administrator privileges, you can also delete an account.



A dialog box titled "User profile" with a close button (X) in the top right corner. It displays user information: Email address: qa@radix-int.com, Language: English (US). Below this, there are three buttons: "CHANGE USER PASSWORD", "ENABLE TWO-STEP VERIFICATION", and "DELETE ACCOUNT" (highlighted in red). At the bottom, there are two buttons: "CANCEL" and "UPDATE".

To delete an account:

1. Click on **Delete Account**. The **Delete account** dialog box opens:

A dialog box titled "Delete account". It contains the text "Are you sure you want to remove account 'qa'?" and "To confirm delete, type 'Delete' in the field". Below the text is a text input field. At the bottom are two buttons: "NO" and "YES".

Delete account

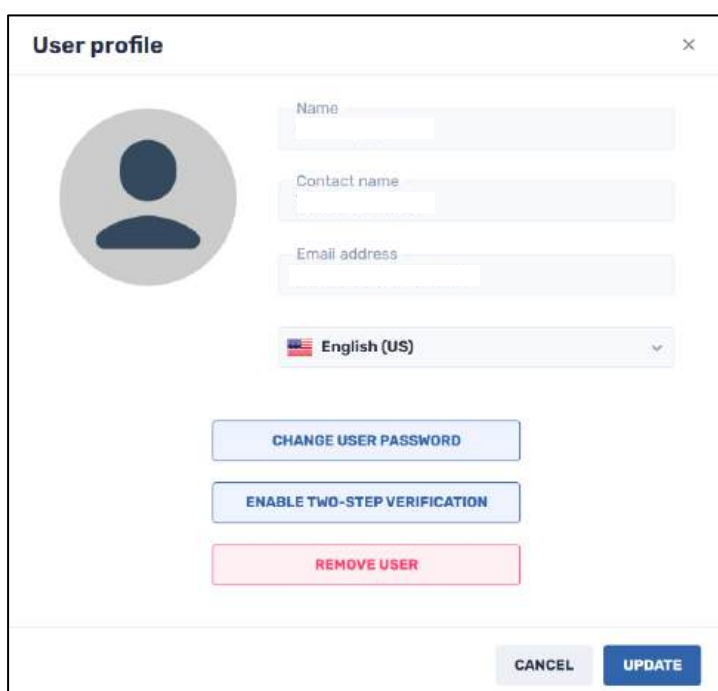
Are you sure you want to remove account "qa"?
To confirm delete, type "Delete" in the field

NO **YES**

2. Type "Delete" in the textbox and click **Yes** to delete the account.

Note: If you have Administrator privileges, clicking the **Delete Account** option will completely delete the account and all its records and log you out of the platform.

If you only have User privileges, the User Profile dialog box will appear as follows:

A dialog box titled "User profile" with a close button (X) in the top right corner. It features a circular profile picture placeholder on the left. To the right are input fields for "Name", "Contact name", and "Email address". Below these is a language dropdown menu showing "English (US)". At the bottom are three buttons: "CHANGE USER PASSWORD", "ENABLE TWO-STEP VERIFICATION", and "REMOVE USER" (highlighted in red). At the very bottom are "CANCEL" and "UPDATE" buttons.

User profile X



Name

Contact name

Email address

 English (US) ▼

CHANGE USER PASSWORD

ENABLE TWO-STEP VERIFICATION

REMOVE USER

CANCEL **UPDATE**

Figure 4-5: User Profile dialog box for regular client user

For someone with only User privileges, the procedure to remove a user is the same as for someone with Admin privileges. However, clicking **Delete User** will delete the user and log you out of the platform, but the user may still be able to access their records.

4.2 Language Options

The **Language** option allows you to select a different language for the user interface.

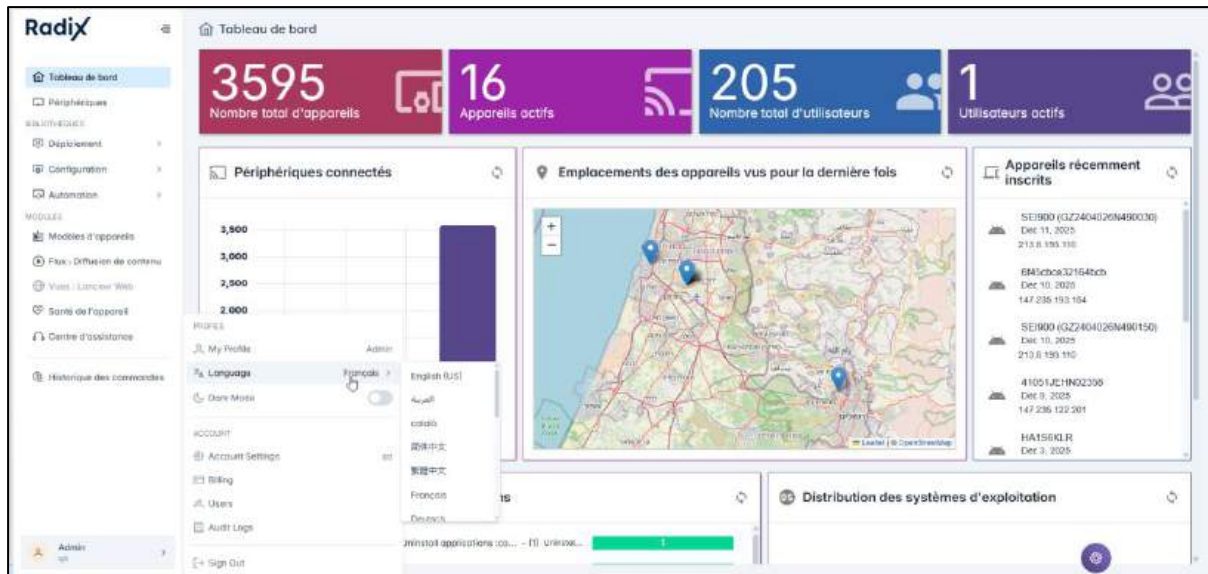


Figure 4-6: The Language option, with French selected as the interface language

This option is available for users without Administrator privileges. We will see in **Section 4.6.3** that a user with Administrator privileges can change the interface language for all users.

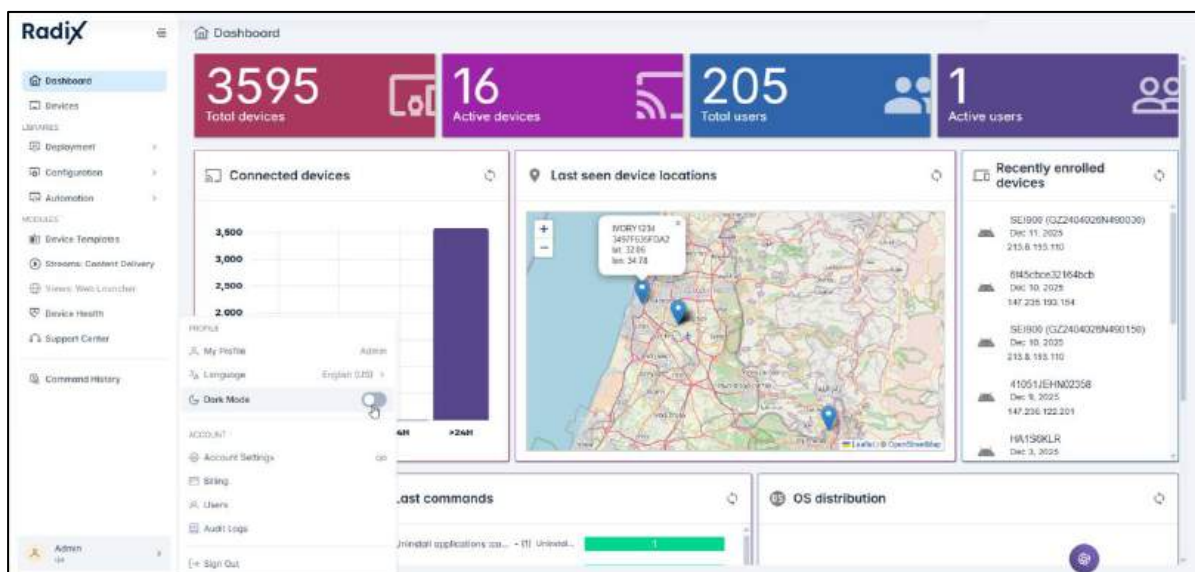
4.3 Dark Mode Options

When you log in to the Radix Device Management Platform, you may choose between two different display options: a white background, or a dark background.

When you first log in to the Radix Device Management Platform, everything will be displayed in the default white theme. If you find this to be too intense and would prefer a dark background, we recently added an option to switch to a dark theme.

To toggle between the different modes:

1. Click on the **Profile** icon in the lower left corner.



- Click on **Dark Mode** to change the display to dark mode.

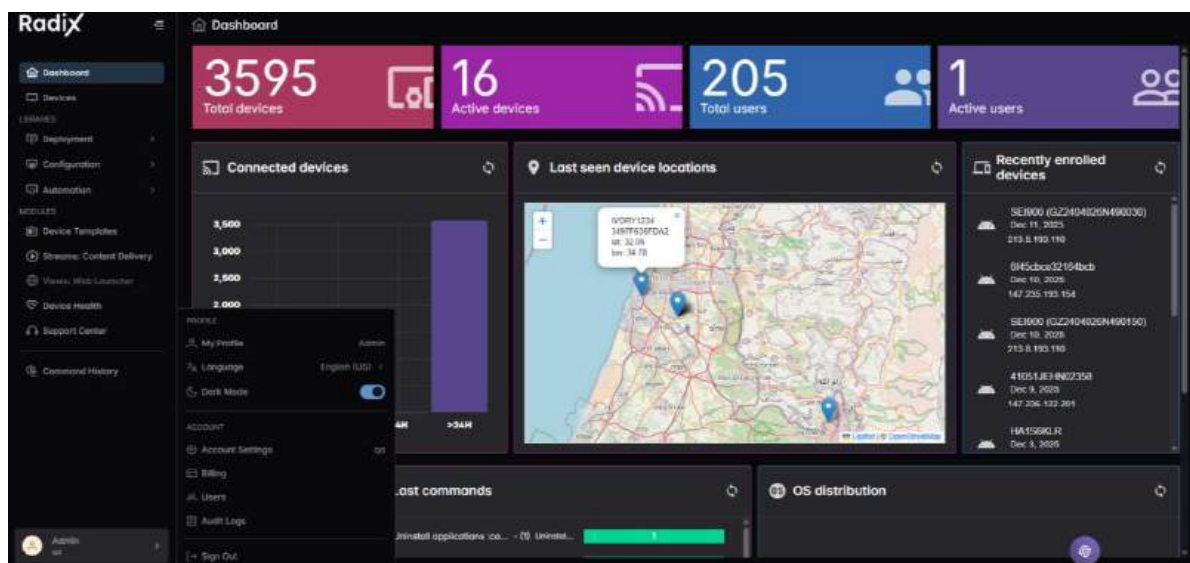


Figure 4-7: Dark Mode Overview Dashboard

4.4 Account Settings Menu

The **Account Settings Menu** will provide an administrator with options to perform changes to users' accounts.

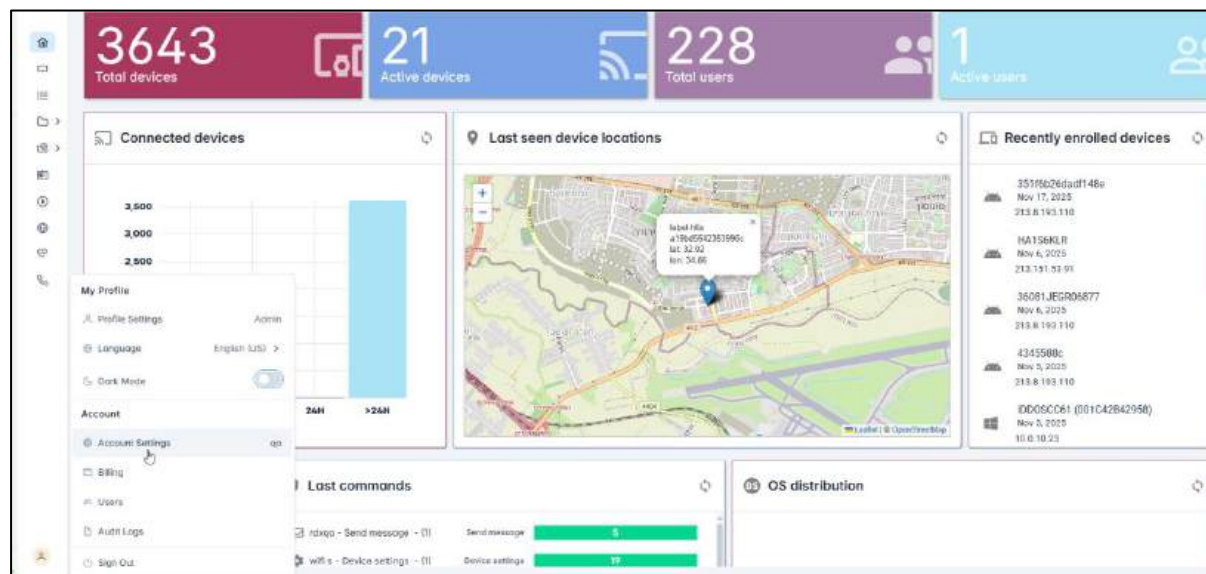


Figure 4-8: Account Settings icon in the Overview Dashboard

When you click on the Account Settings icon in the Overview Dashboard, the **Account Settings** window opens.

Account settings











Require users permission for remote control

Alerts mail

qa1@radix-int.com

SAVE

The left-hand side of the Account settings box contains the following options:

Table 4-1: Account Settings Options

Icon	Function
	Remote control
	Pair with organization domain
	Android for Work
	Device Pairing
	Report Scheduling
	Custom Columns
	Health Check Thresholds
	Import Tags
	Audit Logs

We will go through the options in order.

4.4.1 Remote Control Option

Clicking on the “Remote Control” icon  in the Account Settings Menu gives the Radix Device Management Platform administrator the option of being able to control a user’s device, with or without that user’s permission.

Selecting “**Requires users’ permission for remote control**” button means that you will only be able to engage with the user’s device after receiving permission.

In addition, you can supply a tag in the **Device tag** textbox. This will require that the remote user give permission for remote control for an entire group of devices, where every member of the group bears that identifying tag. In the example below, all of the devices with the tag “aep” will now require that the remote users explicitly allow remote control of their devices.

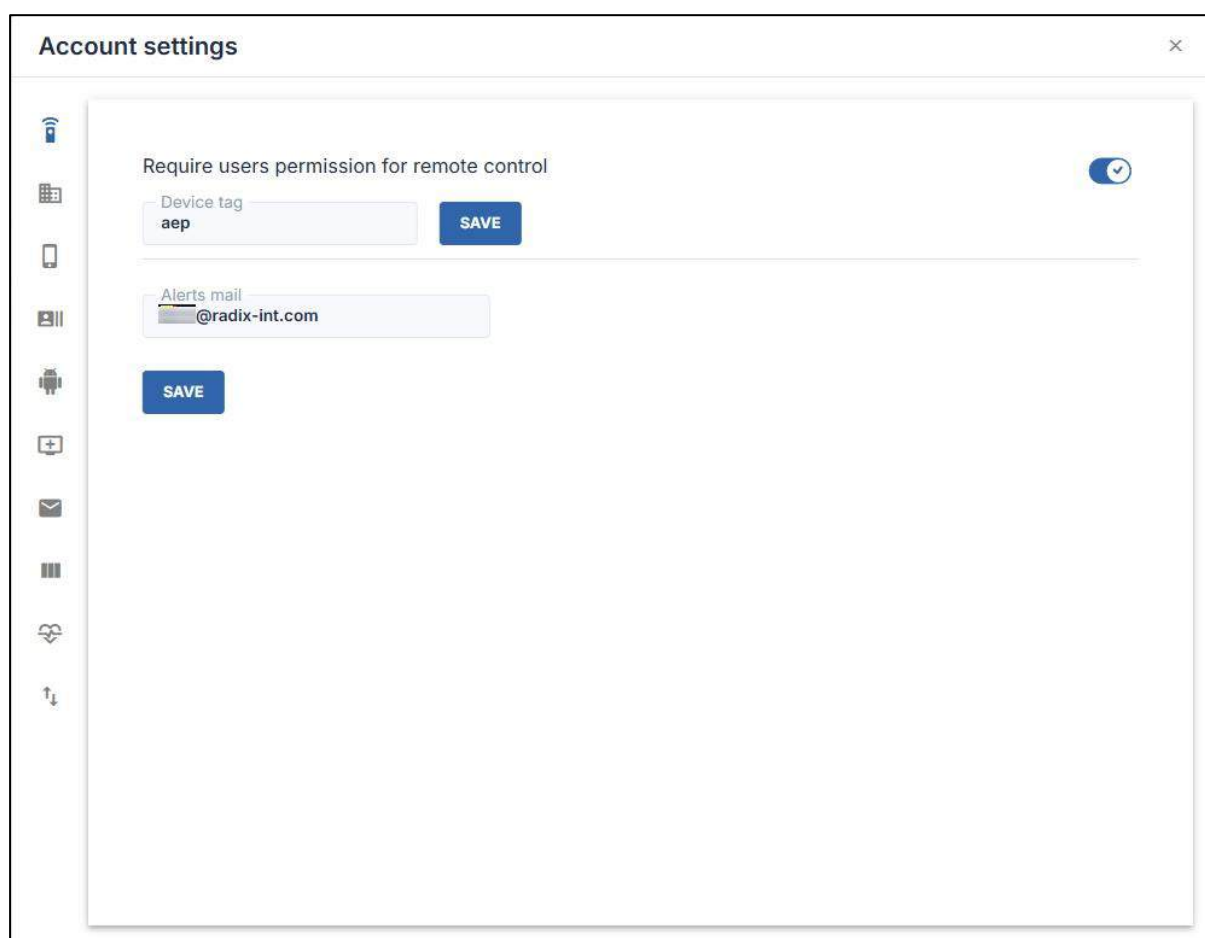


Figure 4-9: Account Settings Menu, with permission for remote control option selected

The user will receive a prompt on their device, asking them if they wish to allow remote control access:

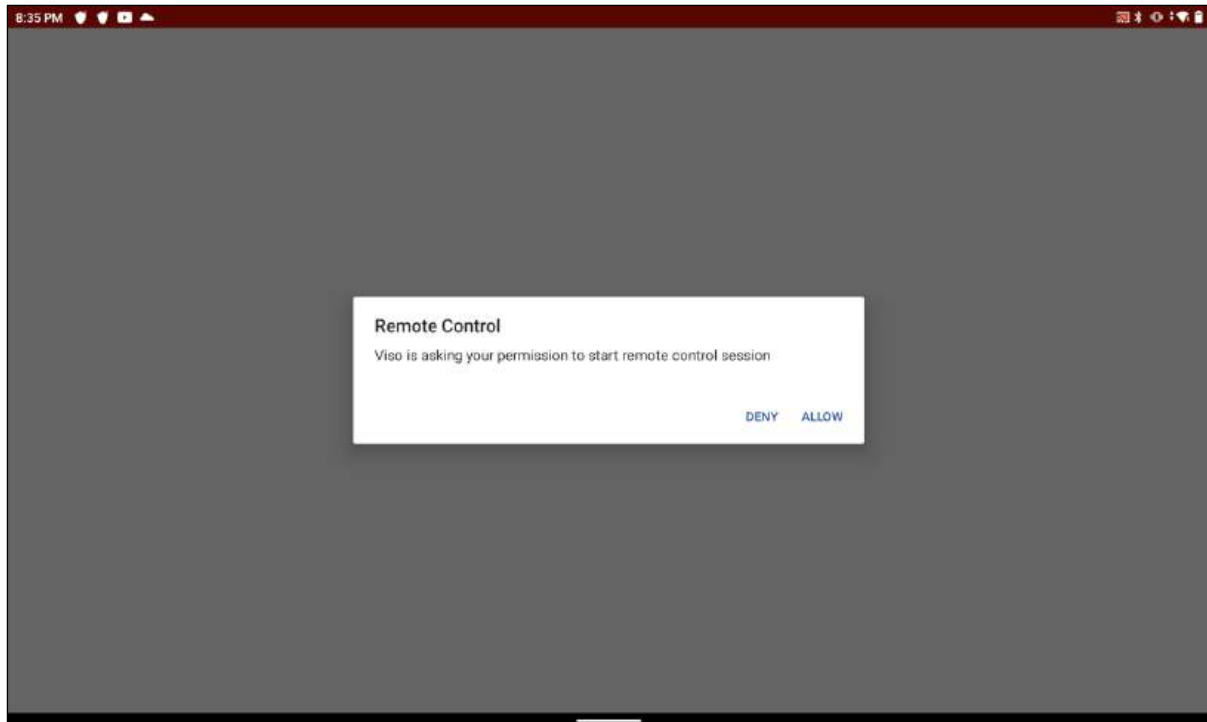


Figure 4-10: Prompt on the user's device, to allow remote control of a device

When you enable or disable requiring user permission, you will receive a pop-up notification in the lower right corner that the account settings have been changed:

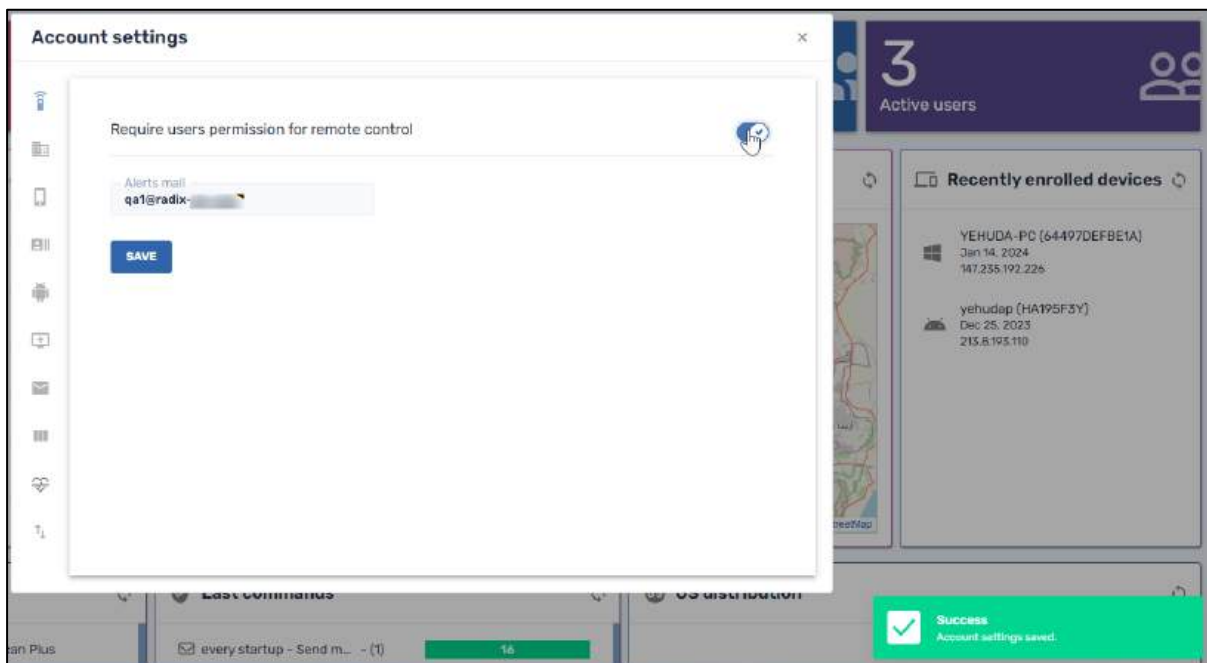


Figure 4-11: Notification of a successful change to the account

Note: This option is only for users with administrator privileges. If a regular user tries to change the account settings, they will receive an error message telling them that the account settings cannot be changed:

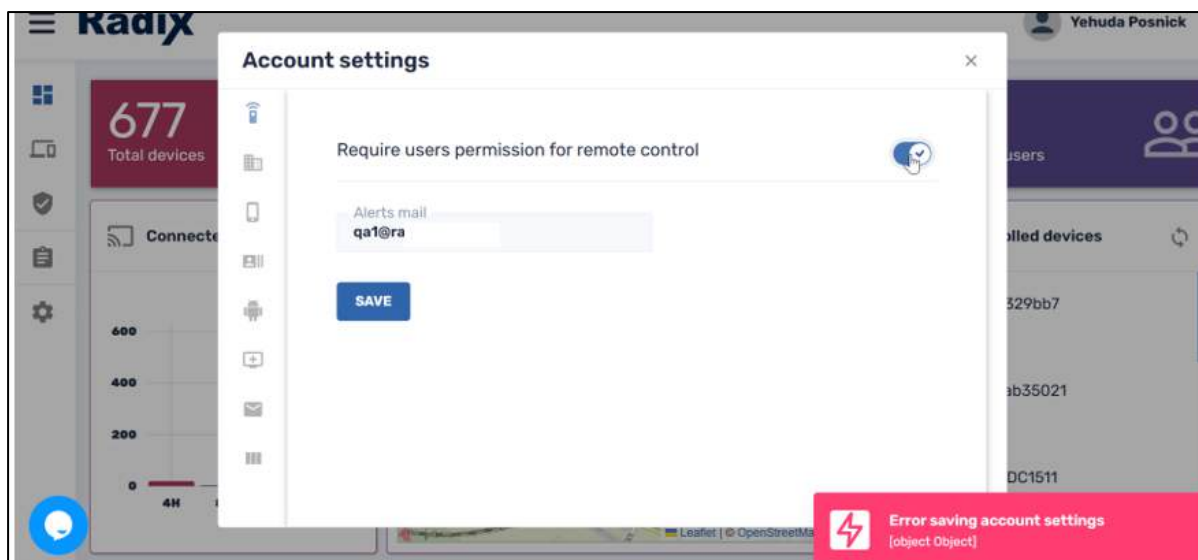


Figure 4-12: Error message for user without Admin privileges

4.4.2 Pair with Organization Domain Option

Clicking on the **Organization Domain** option tells you the present domain name. It allows you to change the domain name to another valid e-mail address in the organization.

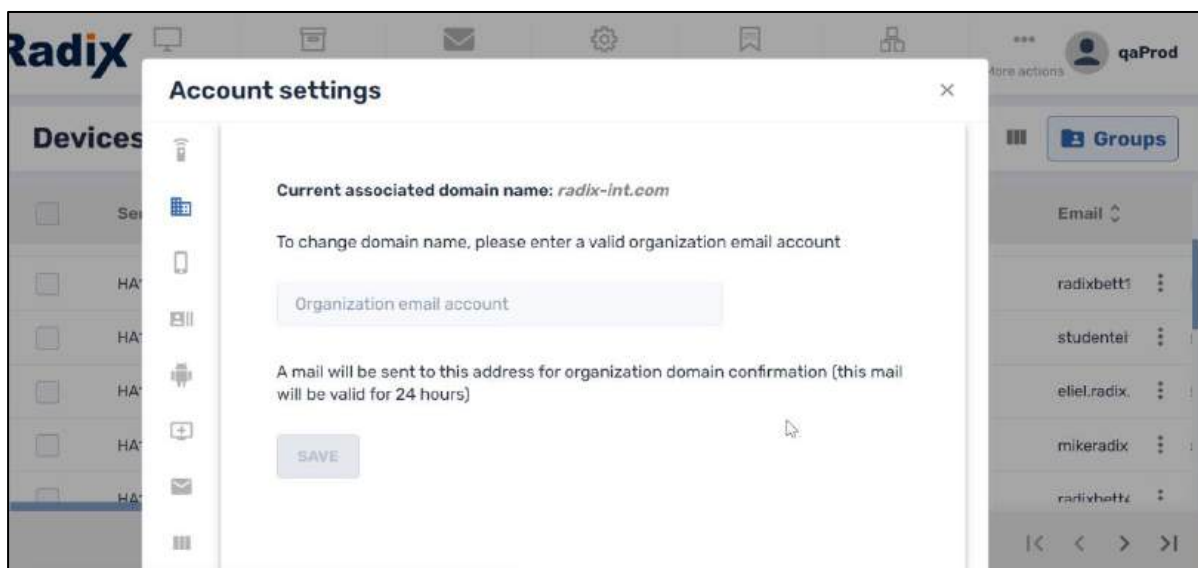
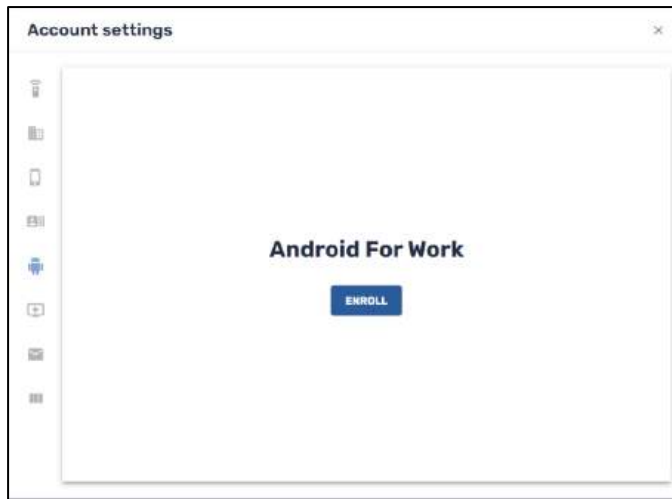


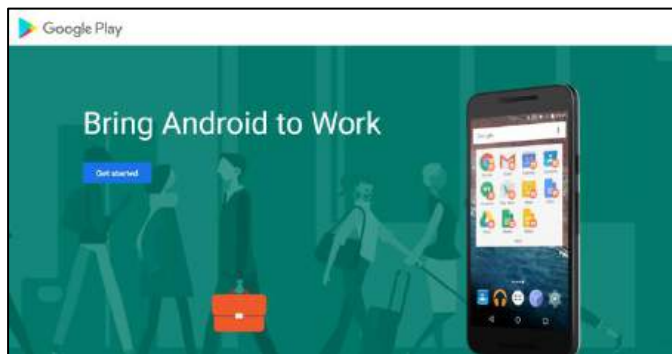
Figure 4-13: Dialog Box to select a domain

4.4.3 Android for Work Registration

When you click on the **Android for Work** icon, you get a prompt to register in Android Enterprise. This will enable you to use the Radix Mobile Device Management (=MDM) platform to securely install selected apps on remote Android devices that are also enrolled in Android for Work.



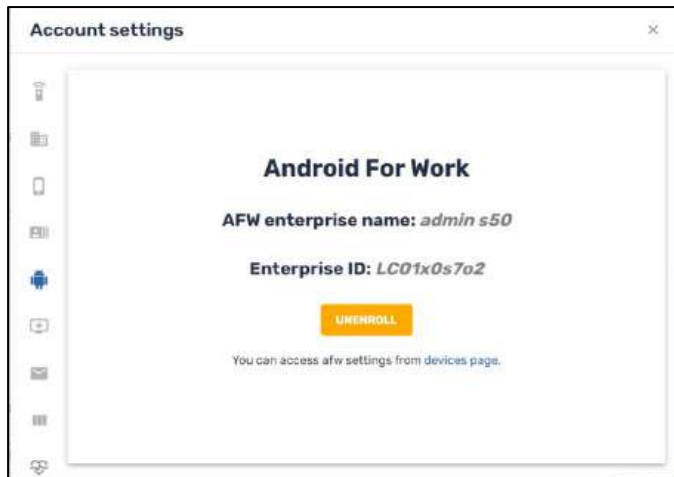
After you click on the **Enroll** prompt, the Google Play app opens:



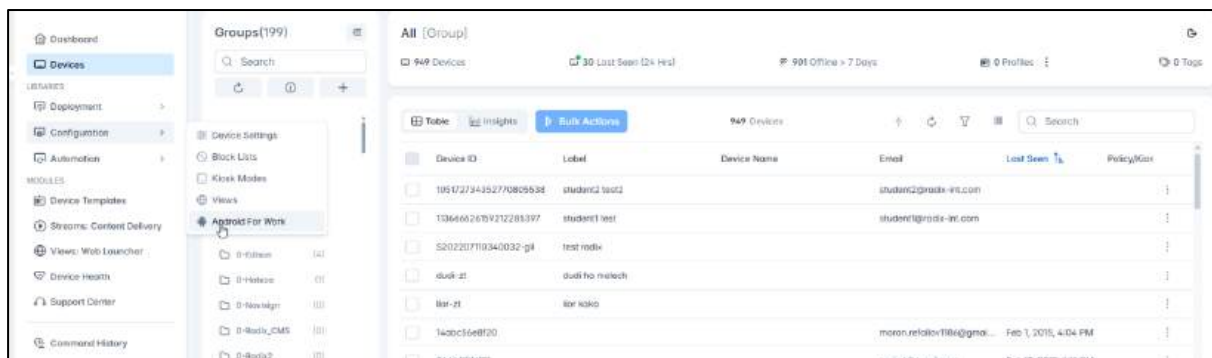
After clicking **Get Started**, you will be prompted for business details:

 A screenshot of a "Business details" form. The title "Business details" is at the top in large white letters. Below it, the text "We need some details about your business" is displayed. The form contains two input fields: "Domain name or Business name" with a placeholder "Your answer", and "Enterprise mobility management (EMM) provider" with the text "Radix Viso" entered. At the bottom right, there are two buttons: "Previous" (disabled) and "Next" (active).

Once a device is enrolled in Android for Work, you will see the following screen in the account settings:



After registering, you can proceed to select applications to be installed on remote devices. You select these apps by clicking on **Configuration>Android for Work** in the Devices Table sidebar menu:



See **Section 7.2.4** for details on how to select apps to be installed on remote devices enrolled in Android for Work.

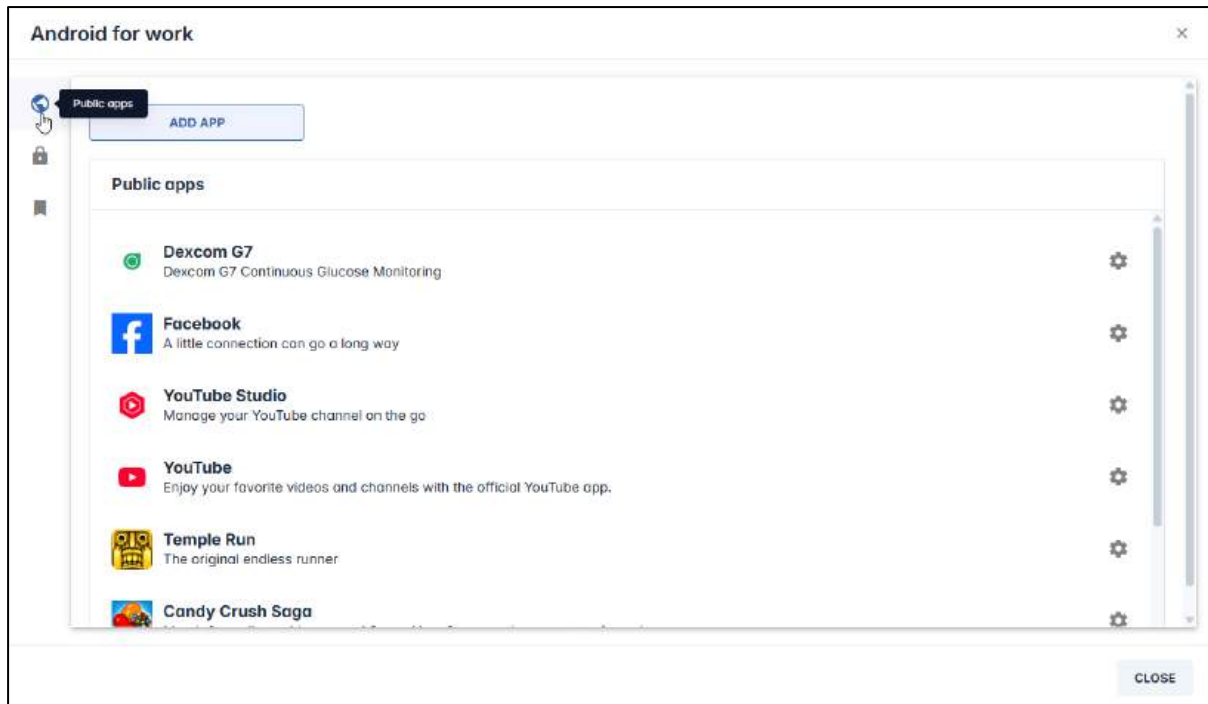


Figure 4-14: Selecting Android for Work apps for installing on remote devices

You can then install these selected apps on remote devices by following the procedure outlined in **Section 6.1.2 (Android for Work (AFW) install/uninstall)**.

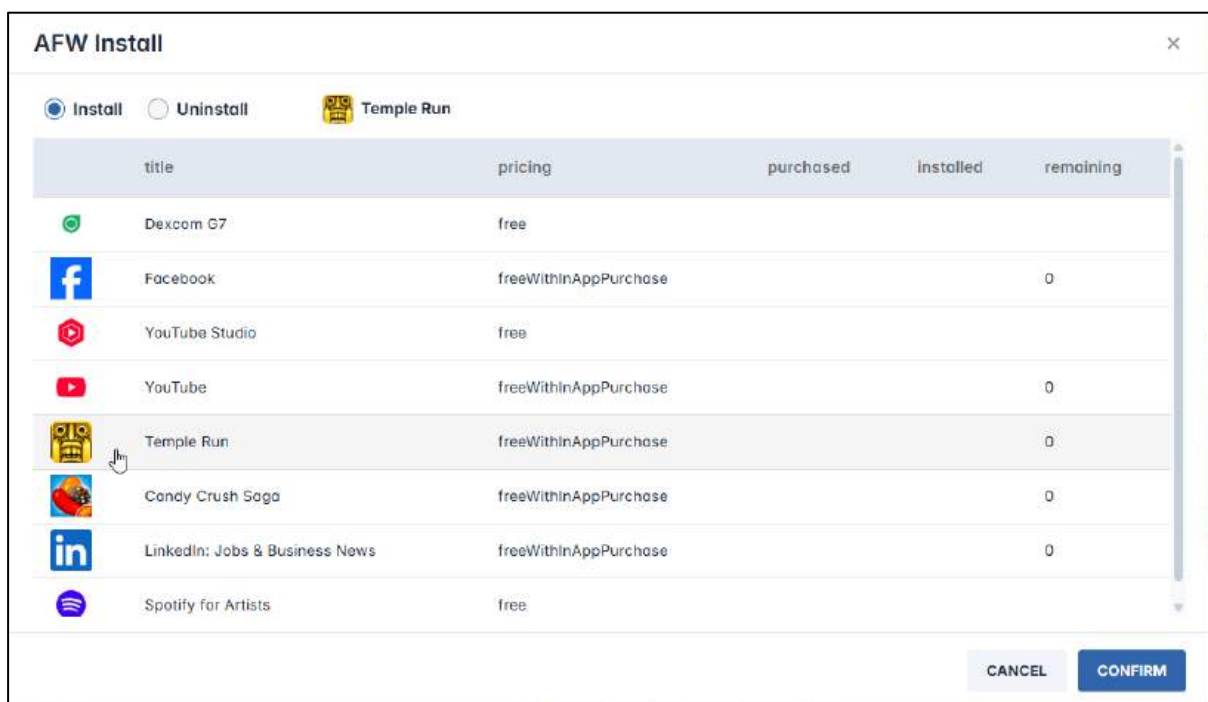
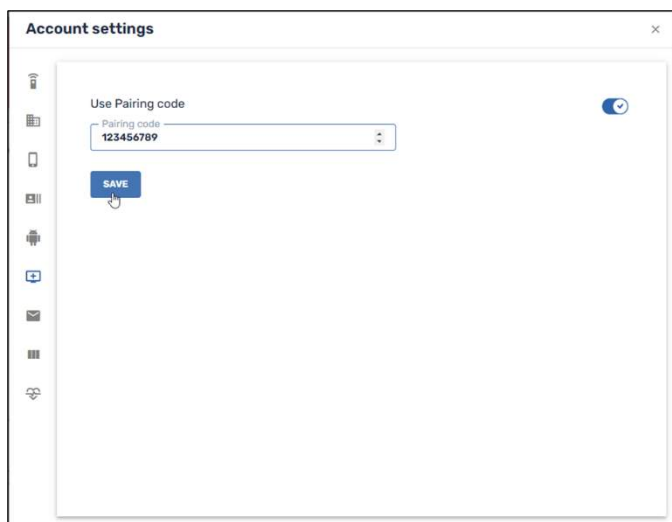


Figure 4-15: Installing an app ("Temple Run") on a remote device using Android for Work

4.4.4 Device Pairing Option

This option adds another level of security to remote devices. When the Radix Device Management Platform administrator creates a pairing code, the remote user will have to supply this code any time they wish to effect a change to the configuration of the Viso Agent

app. This feature lets you narrow down the users and devices, excluding anyone who does not have the pairing code from changing the configuration of the Viso Agent app.



When a remote user tries to make any changes to their installation of the Viso Agent app on their device, they are prompted for the device pairing code:

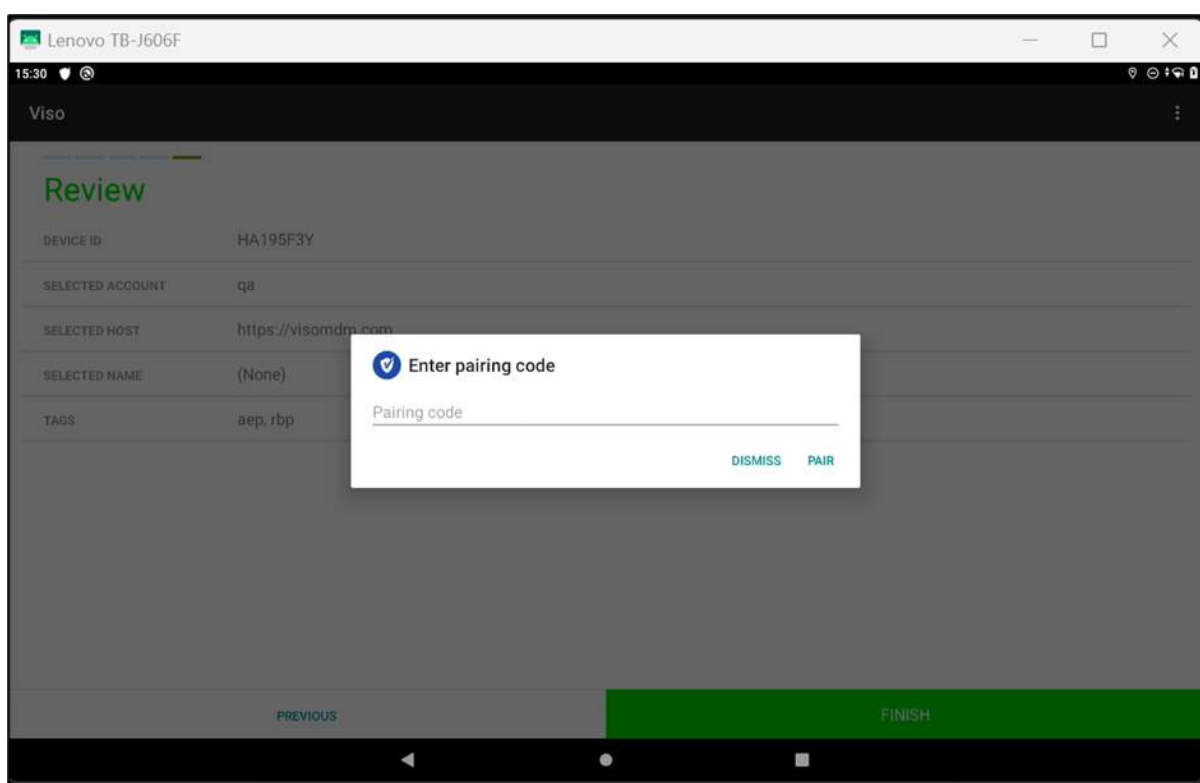


Figure 4-16: The user of the remote device will be prompted for the pairing code

4.4.5 Report Scheduling Option

This sends a weekly report of activity on particular devices to selected users. You can add several email addresses, as well as select a specific time and day of the week that the report will be sent.

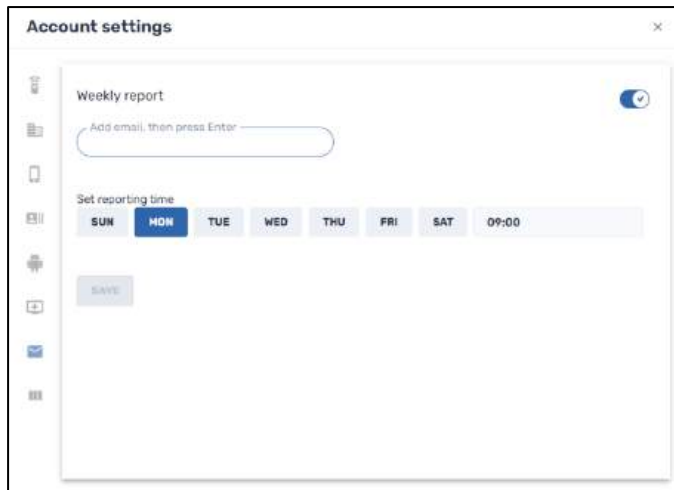


Figure 4-17: Interface to select email addresses, day, and time to send a weekly report

4.4.6 Custom Columns Option

This option allows you to add or delete columns to be displayed in the other consoles. You can create your own custom columns or select a new column heading from a list of apps.

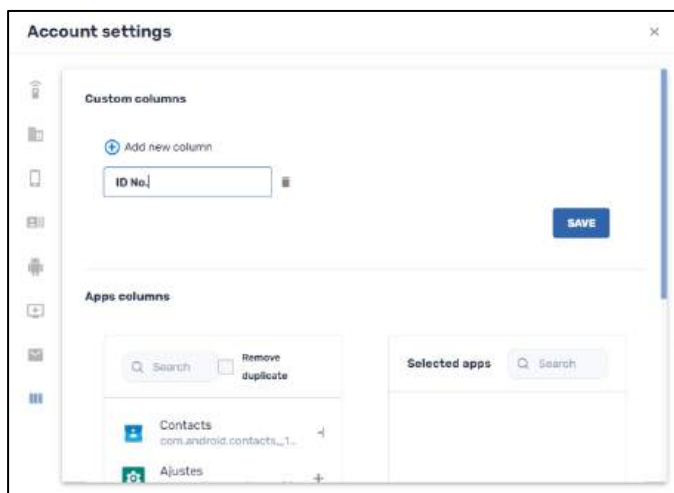


Figure 4-18: Window to select columns to be displayed

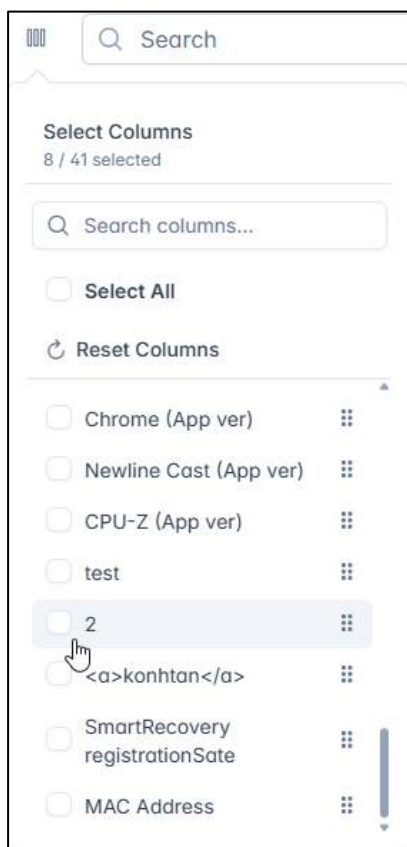
To add a new column heading:

1. Click on **Add new column**. The “Type the column name” textbox appears.



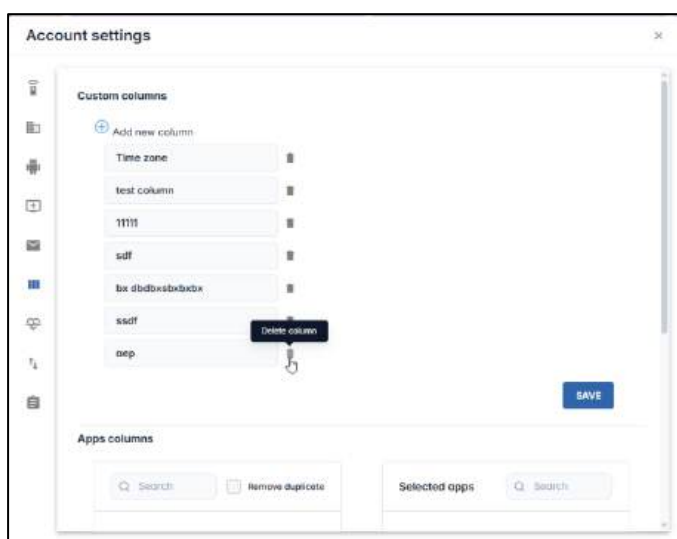
2. Type in the name for a new column heading and click **Save**.
The new column heading will now appear among the display options in the other consoles.

Note: This will allow you to add these optional columns in the Devices Table display. However, you will have to activate these optional columns with the **Configure columns** option in the Devices Table (**Section 5.7.8**).

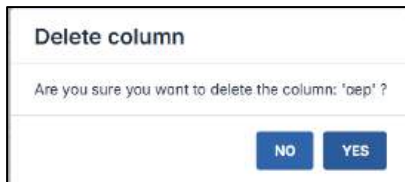


To delete a column that you have added:

1. Click on the **Delete Column** icon  next to the column heading that you wish to remove.

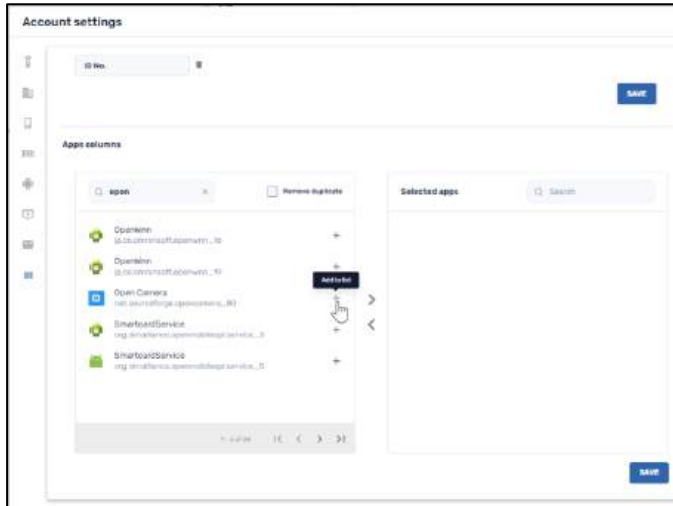


2. At the **Delete column** prompt, click **Yes**. The column name will be removed from the list of columns heading options.

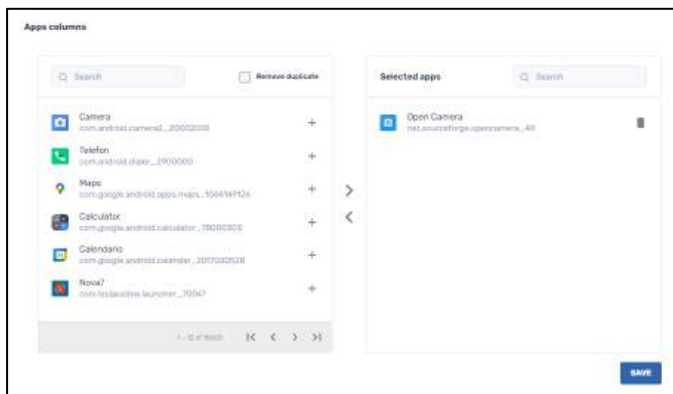


To add a new column from the list of selected apps:

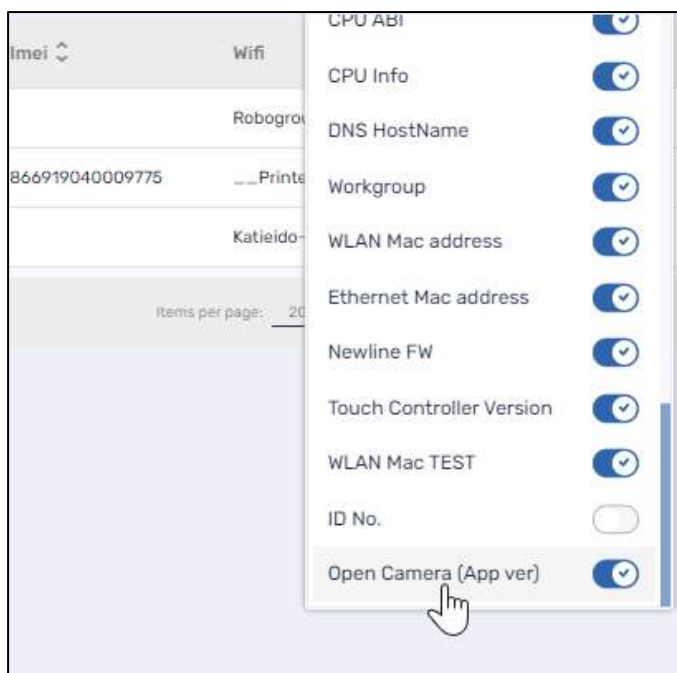
1. Search for the app from the list, either using the Search bar, or by scrolling through the options.



2. Click on the **Add to list** icon. The app will now appear in the **Selected apps** column.



3. Click **Save**. The new column option will appear in the Column list.



4.4.7 Health Check Thresholds Option

This allows you to define minimum values for battery charge, upload speed, and download speed.

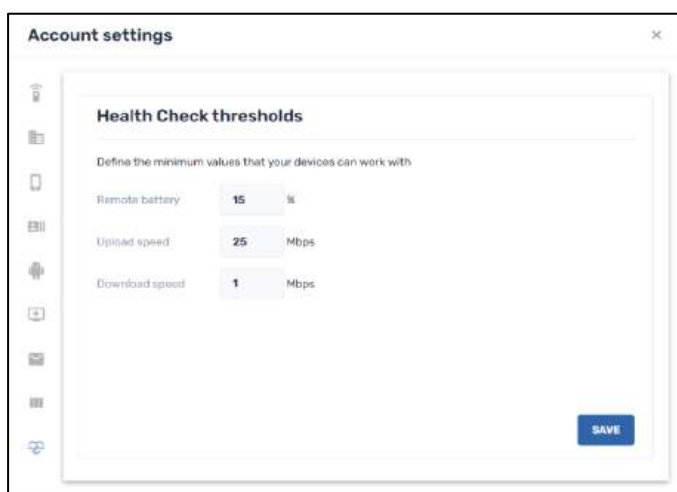


Figure 4-19: Health Check Thresholds Window

4.4.8 Import Tags and Labels

There is an option in the Radix Device Management Platform to import tags and labels to devices, by uploading a CSV file with these tags and labels. Depending on the syntax you use in the CSV file, you will be able to change:

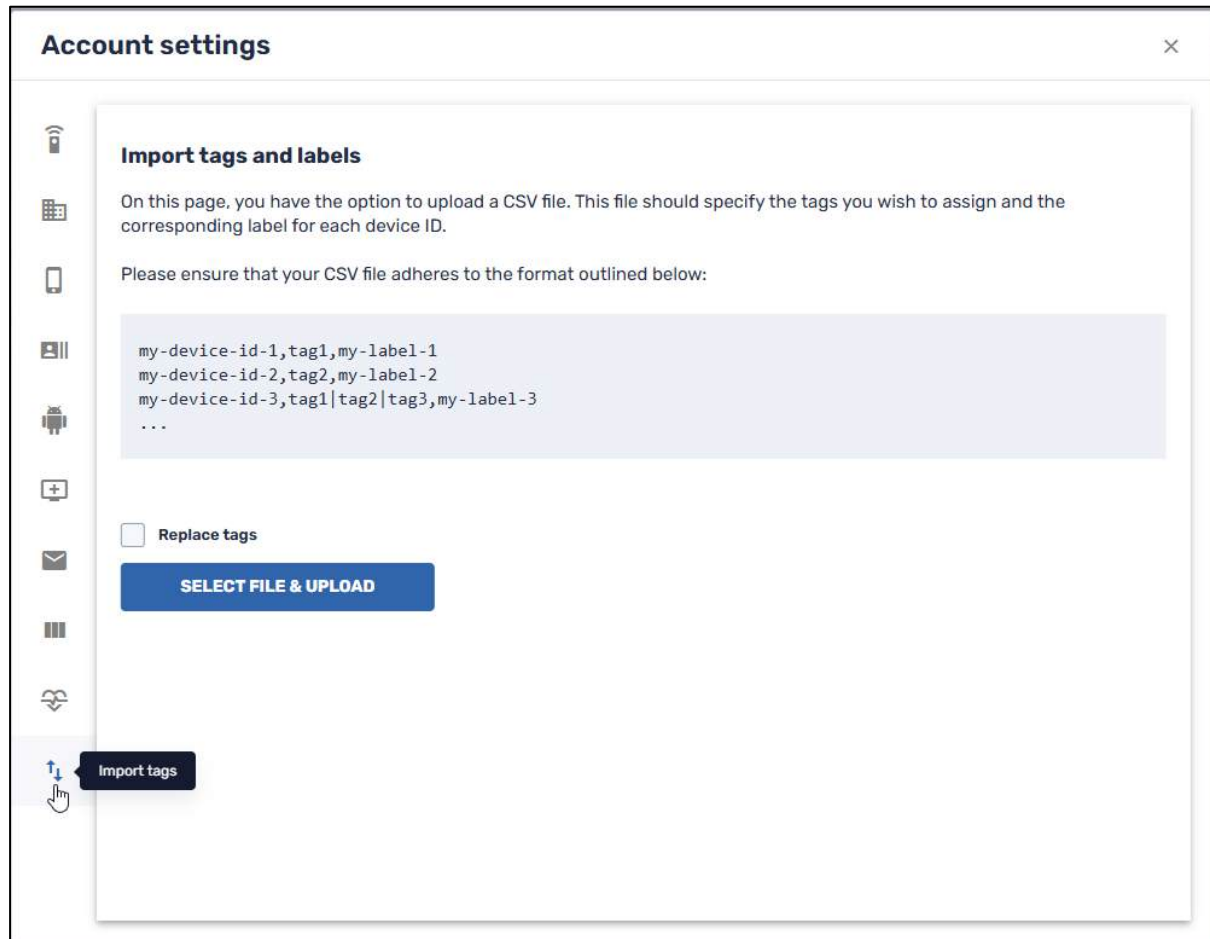
- Both the device name and its tags,
- Just the device names, or
- Just the tags.

The advantage of this method is that it allows you to change the names and tags on an entire fleet of devices with a single command.

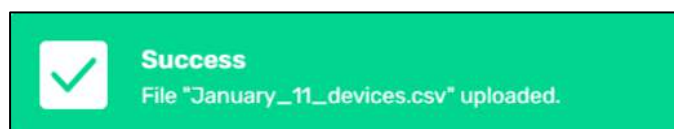
Note: This option may not appear in your particular implementation of the Radix Device Management Platform.

To import tags and labels to a device:

1. When you click on the **Import Tags** icon  in the sidebar menu, the following window opens:



2. Click **Select File & Upload**. You will be prompted to upload a CSV file from your computer. You should create the file using a simple text editor, such as Notepad, and save the file with the extension ".csv". (A file created using Word or Excel may not work, even if you save it as a .csv file.)
3. If the upload is successful, you will receive a notification that it succeeded in the lower right-hand corner.



4.4.8.1 Proper Format of the CSV File

For this command to work properly, you must ensure that the parameters in the file are in the correct format.

This table summarizes the syntax rules:

Action	Device ID	New Device Label	Tags to be Added	Syntax
Change the Device Label and Add Tags	my-device-id-1	my-label-1	tag1,tag2,tag3	my-device-id-1, tag1 tag2 tag3,my-label-1
Change the Device Label without adding tags	my-device-id-2	my-label-2		my-device-id-2,"",my-label-2
Add tags without changing the Device Label	my-device-id-3		tag1,tag2,tag3	my-device-id-3,tag1 tag2 tag3,

Make sure that:

- You separate the fields for **Device ID**, **Device Label**, and **Tags** with a comma. In the option where you only assign tags, remember to put a comma at the end of the list of tags, even though you do not intend to assign a label the device.
- There should be **no** spaces between the various parameters. Spaces are **not** ignored.

4.4.8.2 Practical Examples

4.4.8.2.1 Example 1: Adding Tags and Labels

To illustrate, we will take three devices, assign names, and add tags by means of the **Import Tags** option.

- We have created a group “AEP,” with the following three devices.

Device ID	OS	Name	Email	Agent version	Tags	Wifi	Local
HA195F3Y			ylposnick@gmail.com	251004135	new, aep	rdxqa	192.161
64f6bb92ac7b				250802560	new, aep	rdxqa	192.161
NAA200660686				250802560	new, aep	rdxqa	192.161

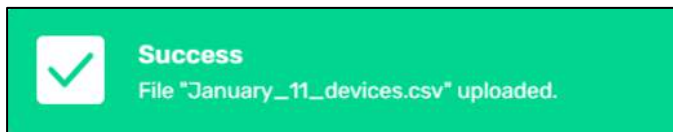
Initially, the data is as follows:

Device ID	Initial Device Label	Initial Device Tags
64f6bb92ac7b		new, aep
HA195F3Y		new, aep
NAA200660686		new, aep

- Using Notepad, we have created a CSV text file named Gauss.csv, that will change the Device Labels and add tags to the three devices in our group:

```
HA195F3Y,"",HA195Gauss
64497DEFBE1A,kappa|lambda|mu,Car1
NAA200660686,eta|theta|iota
```

- If the upload is successful, you will receive a notification that it succeeded in the lower right-hand corner.



After uploading the CSV file, the group of devices now appears as follows:

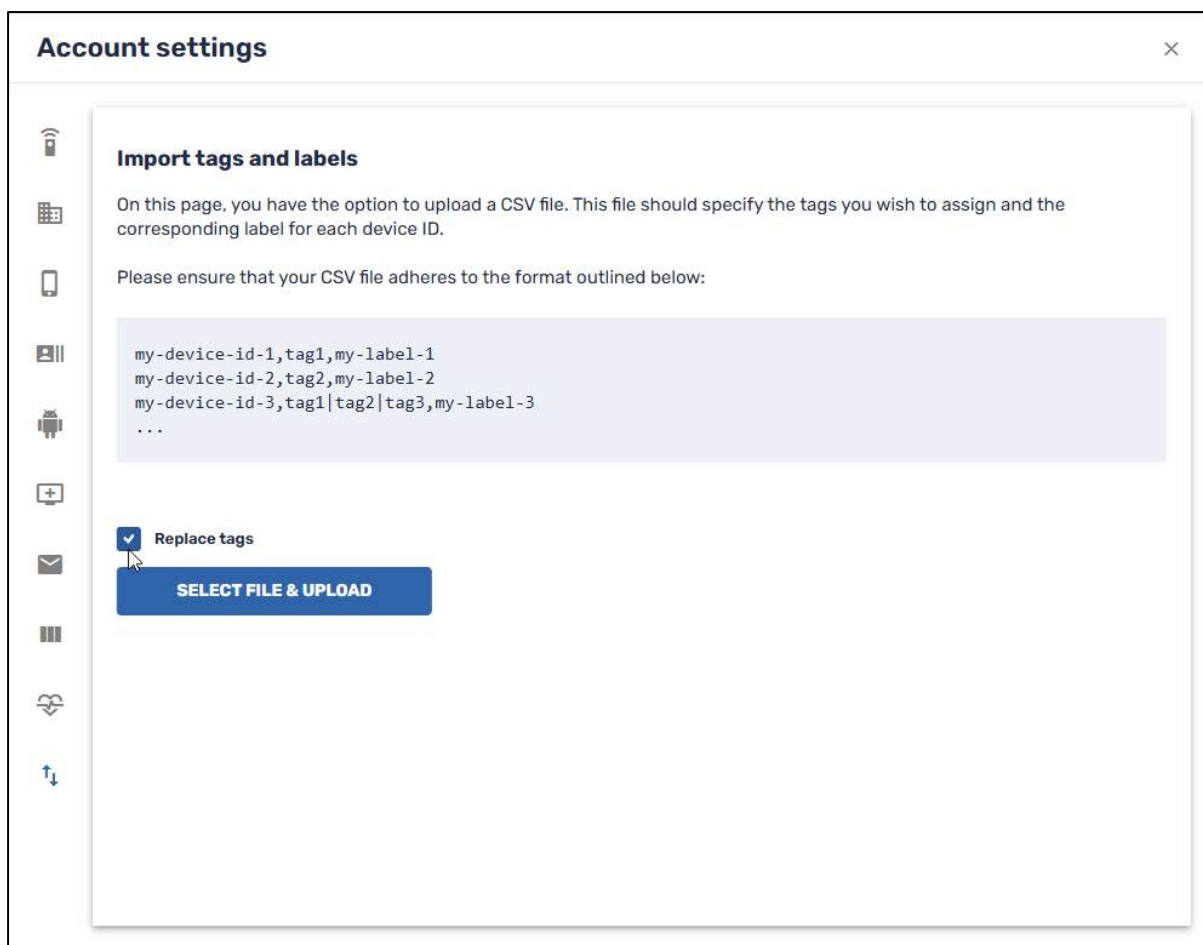
Device ID	OS	Name	Email	Agent version	Tags	Wifi	Local
NAA200660686				250802560	new, aep, eta, theta	rdxqa	192.161
64f6bb92ac7b		Carl		250802560	new, aep, kappa, lambda	rdxqa	192.161
HA195F3Y		HA195Gauss	yiposnick@gmail.com	251004135	new, aep	rdxqa	192.161

The labels and tags are now as follows:

Device ID	Final Device Label	Final Device Tags
64f6bb92ac7b	Carl	new, aep, kappa, lambda, mu
HA195F3Y	HA195Gauss	new, aep
NAA200660686		new, aep, eta, iota, theta

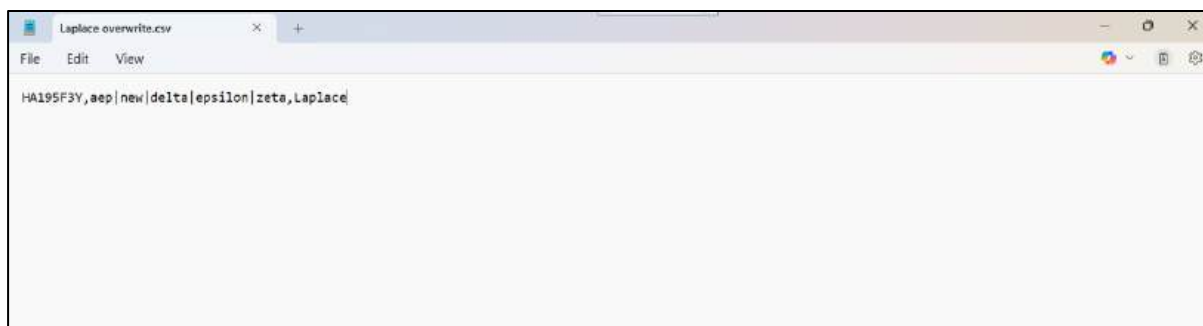
4.4.8.2.2 Example 2: Overwriting Tags and Labels

There is also an option to overwrite the existing tags on the devices, by clicking the **Replace Tags** box.



We will illustrate the use of the **Replace tags** option, by using the following file, named Laplace Overwrite.csv.

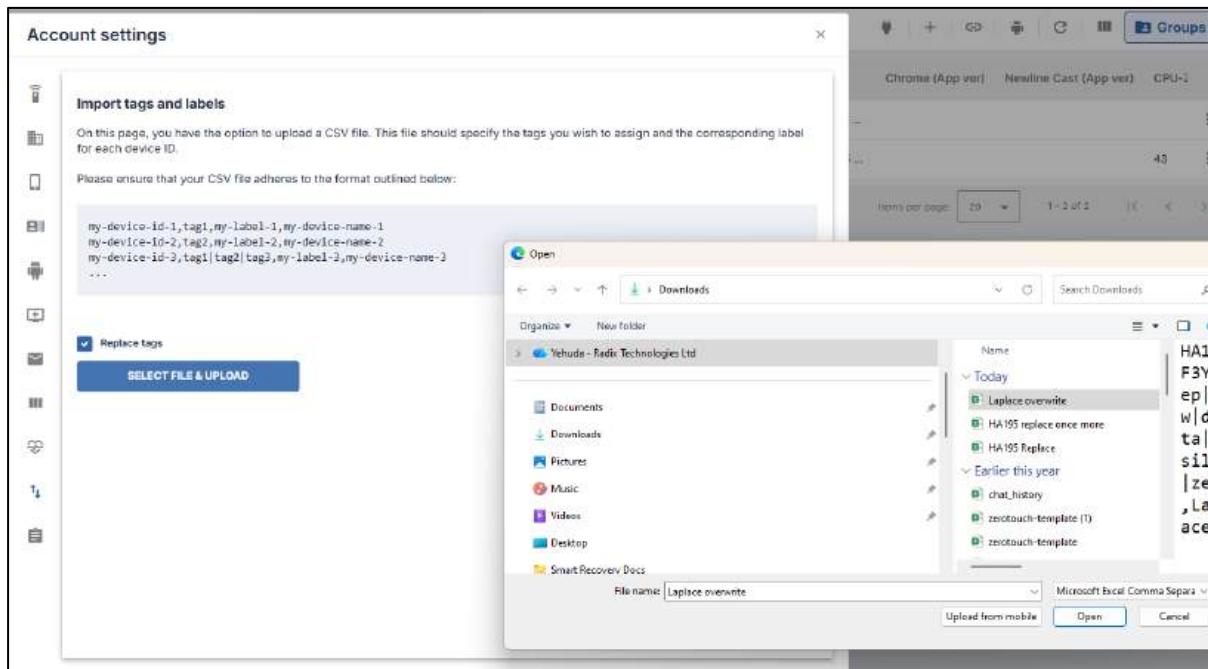
Note: We will have to retain the tags “new” and “AEP,” so that the device HA195F3Y will remain in the group AEP. If we overwrite the existing tags without including the “aep” tag, the device will lose the “aep” tag and will no longer be members of the AEP group.



Initially, the device HA195F3Y will appear as follows in the Radix Device Management Platform. It has the tags “new”, “aep”, “nu”, “omicron”, “pi”, and the Device Label “Lagrange”.



1. Check the “Replace tags” checkbox.
2. Click **Select File and Upload** and select the CSV file “Laplace overwrite.csv”.



After applying the overwrite, Device HA195F3Y will now appear as follows in the Radix Device Management Platform:

OS	Device ID	Label	Email	Last seen	Policy/Kiosk	Tags	First Register	Chrome (App ver)	Newsline Cast (App ver)	CPU-Z
	13F2618889538158		yipomick@gmail.com	Mar 31, 2025, 9:34		new	Mar 31, 2025, 9:46			
	HA195F3Y	Laplace	yipomick@gmail.com	Oct 15, 2025, 1:25		new, aep, delta, epsilon, zeta	Sep 28, 2025, 2:55			43

We see that the device now has the tags “new”, “aep”, “delta”, “epsilon”, “zeta”, and now has the Device Label “Laplace”.

4.5 Billing History

If you are logged in with Administrator privileges, you will be able to see your billing history by clicking on the **Billing** option in the drop-down menu. The billing history will include a list of credit events, the date on which they occurred, the number of credits in your balance, and more.

4.5.1 Billing Data--Background

When you create an account on the Radix Device Management Platform, you will purchase a certain number of credits, depending on the number of devices you wish to enroll in the system, and the number of years of your subscription. Presently, the minimum number of devices that you can enroll is five. There is also a one-time account setup fee. Every license has 365 credits, one credit for each day of the year. When you add a device to your Radix Device Management Platform account, it initiates a “countdown” to the number of credits, decreasing by one credit a day per device.

Radix Billing

Active Account status **Dec 7, 2021** Account created **599409431** Account credits **166734** Days remaining

Billing history Show device coupons

Credit event	Date	Credits	Credits before	Credits after	Notes	Code
purchase event	Jul 8, 2025	-100000000	700000000	600000000	online purchase	
purchase event	Jul 8, 2025	699993000	7000	700000000	online purchase	
purchase event	Jul 8, 2025	-8993000	9000000	7000	online purchase	
		-891000000	900000000	9000000	online purchase	
		1111112	88888888	90000000	online purchase	
		88793333	95555	88888888	online purchase	
		919180	36395	95555	online purchase	
		1	36394	36395	online purchase	
		299974492	25508	300009000	online purchase	

Redeem credits from coupon code

Coupon number

REDEEM

Credit calculator

Enter number of years:

Enter number of devices:

Total year credits needed:

BUY

Figure 4-20: Billing History Display

4.5.2 Fields of the Billing History screen

There are four fields to the **Billing History** screen:

- **Top Ribbon:** The top ribbon will display your account status, the date when your account was created, how many credits remain in your account, and how many days remain in your subscription.

Active Account status **Jul 12, 2022** Account created **186** Account credits **62** Days remaining

Figure 4-21: Top Ribbon of Billing History Screen

- **Billing History Spreadsheet:** This pane displays any transactions made on your account: how many credits were used or purchased, the date of the transaction, your balance, and the source of the transaction. By clicking on the **Show device coupons** button at the upper right , you can toggle between viewing all transactions, including credits from device coupons, or only credits from online purchases.

Credit event	Date	Credits	Credits before	Credit after	Notes	Code
purchase event	Dec 7, 2023	-680	472610	471930	device coupon	an400
purchase event	Nov 12, 2023	1095	488695	489790	device coupon	BFQAUEGNDAS030
purchase event	Nov 5, 2023	1825	491623	493448	device coupon	c55c389d611f0469
purchase event	Oct 29, 2023	1095	495268	496363	device coupon	6C0079B6A2
purchase event	Oct 26, 2023	1095	496204	497299	device coupon	000014ae85dc5fa2
purchase event	Oct 17, 2023	1825	500454	502279	device coupon	LTN6101003459
purchase event	Sep 21, 2023	-343	518227	517884	device coupon	6438428eb059ed5f
purchase event	Sep 7, 2023	1095	526489	527584	device coupon	6C0079B6A2
purchase event	Sep 7, 2023	1095	525394	526489	device coupon	000014ae85dc5fa2
purchase event	Sep 5, 2023	1095	525631	526726	device coupon	BFFS0CND60002

Figure 4-22: Billing History spreadsheet, including device coupons

Credit event	Date	Credits	Credits before	Credit after	Notes	Code
purchase event	Jul 12, 2023	365	558366	558731	credits from coupon	samsungjay
purchase event	Jul 12, 2023	365	558001	558366	credits from coupon	samsungkay
purchase event	Jul 10, 2023	1	559312	559313	credits from coupon	uriel
purchase event	Jul 10, 2023	1	559311	559312	online purchase	
purchase event	Oct 6, 2022	365	713306	713670	online purchase	
purchase event	Feb 12, 2022	-365	729972	729607	online purchase	
purchase event	Feb 10, 2022	2	730964	730966	credits from coupon	2
purchase event	Feb 10, 2022	1	730963	730964	credits from coupon	1
purchase event	Feb 10, 2022	365	730598	730963	online purchase	
purchase event	Jul 11, 2021	1	824555	824556	online purchase	
purchase event	Jul 11, 2021	21	824534	824555	credits from coupon	21

Figure 4-23: Spreadsheet of Purchase Events, excluding device coupons

- **Redeem Credits from Coupon Code**

The screen on the upper right allows you to enter a coupon code. The coupon will entitle you to an additional number of credits. Upon clicking the **Redeem** button, your account is credited with the specified number of credits in the coupon. Your balance before and after adding the coupon will appear on the **Billing History** screen.

Redeem credits from coupon code

Figure 4-24: Redeem Credits screen

- **Credit Calculator and Order Information**

The Credit Calculator tile in the lower right of the Billing History screen will allow you to make payments on your account, depending on the number of devices you wish to enroll.



Credit calculator

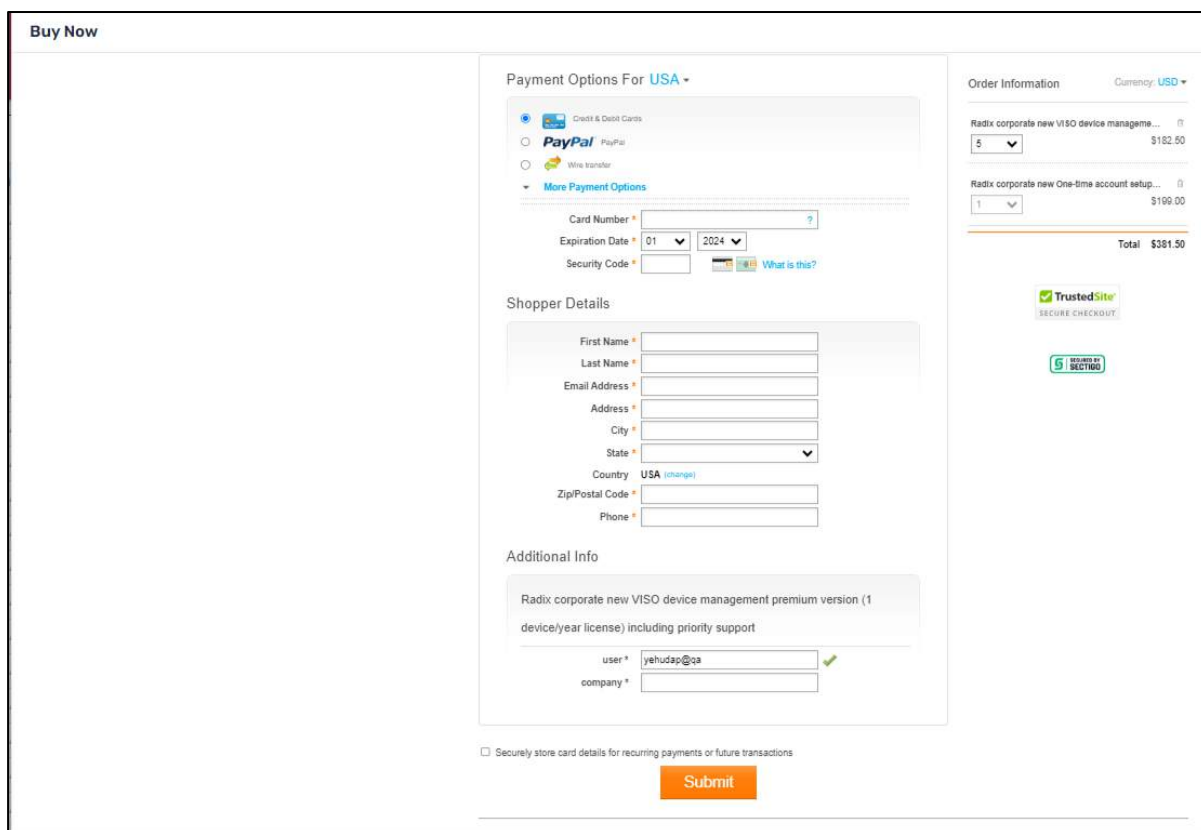
Enter number of years: 1

Enter number of devices: 6

Total year credits needed: 6

BUY

When you click on the **Buy** button in the Credit Calculator screen, the **Buy Now** screen opens:



Buy Now

Payment Options For **USA**

☒ Credit & Debit Cards

☐ PayPal

☐ Wire transfer

[More Payment Options](#)

Card Number *

Expiration Date * 01 2024

Security Code *

Shopper Details

First Name *

Last Name *

Email Address *

Address *

City *

State *

Country * USA [\(change\)](#)

Zip/Postal Code *

Phone *

Additional Info

Radix corporate new VISO device management premium version (1 device/year license) including priority support

user * ☒

company *

☐ Securely store card details for recurring payments or future transactions

Submit

Order Information

Currency: **USD**

Radix corporate new VISO device manage... 5 \$182.50

Radix corporate new One-time account setup... 1 \$100.00

Total \$381.50

TrustedSite
SECURE CHECKOUT

5 **SECURED BY** **SECURE**

Figure 4-25: "Buy Now" screen, allowing you to purchase additional credits

You can use your license for up to 1 year from the purchase date. As this is a SaaS model, the remaining balance will clear at the end of the license period, whether you utilize the Radix Device Management Platform service or not. Therefore, it is recommended to purchase the exact number of licenses that you require. You can always add more at any given time.

4.6 Users Management Menu

If you have Administrator status in the Radix Device Management Platform, you will be able to view all the users presently in the system, by means of the Users Management Menu.

Clicking on the **Users** option will display the Users Management Menu: a list of the current users in the system, as well as their email address, level of authorization (user or Admin status), and more.

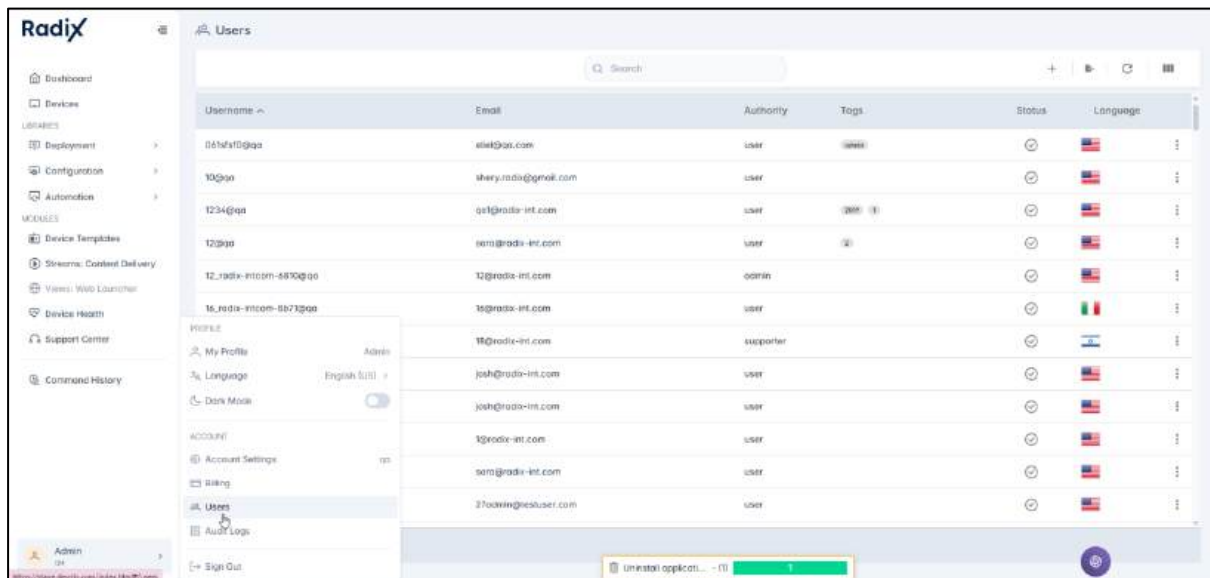
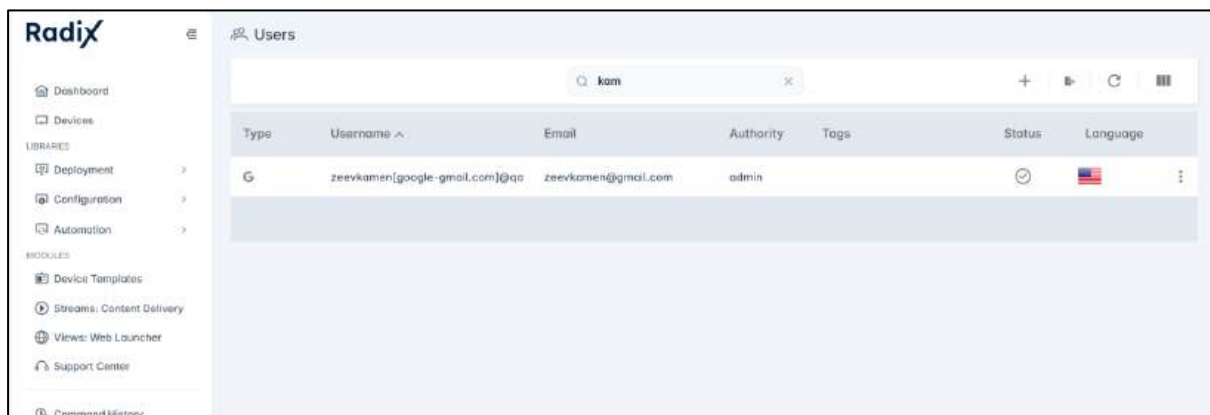


Figure 4-26: List of Users, as displayed in the Users Management Menu

There is a search bar that allows you to search for a particular user by name.



4.6.1 Adding a New User

If you have Admin privileges, you will be able to add new users to the Radix Device Management Platform.

To add a new user:

1. Click on the **Users** icon in the User Profile Menu. The Users Management Menu opens, displaying all existing users.

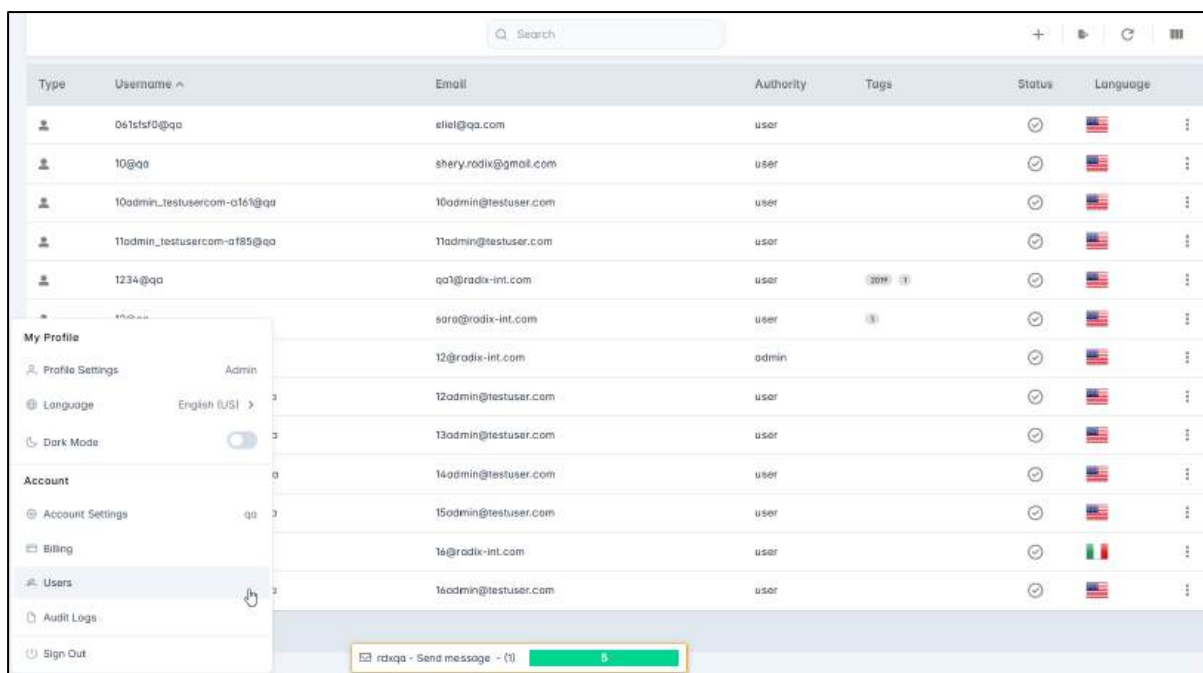


Figure 4-27: Users Management Menu Icon in Overview Dashboard

- In the upper right side of the Users Management Menu, click on the **Add New User** + icon.

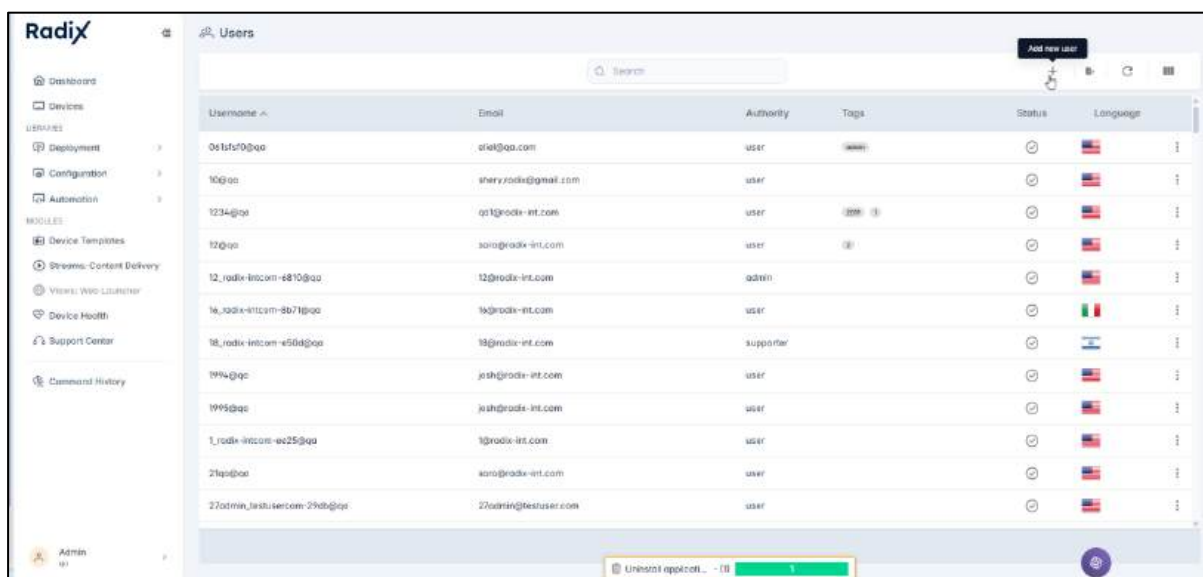
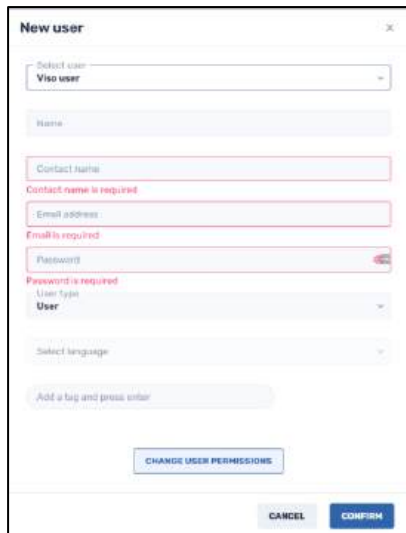


Figure 4-28: Placement of "Add New User" icon

The **New User** dialog box opens.

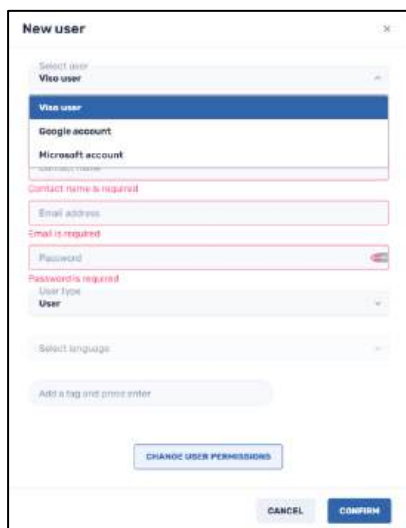


The screenshot shows the 'New user' form. At the top, there is a 'Select user' dropdown menu with 'Viso user' selected. Below this is a 'Name' input field. Then, there is a 'Contact name' input field with a red error message 'Contact name is required'. This is followed by an 'Email address' input field with a red error message 'Email is required', and a 'Password' input field with a red error message 'Password is required'. Below these is a 'User type' dropdown menu with 'User' selected. Then, there is a 'Select language' dropdown menu. At the bottom, there is a button 'Add a tag and press enter'. Below this is a button 'CHANGE USER PERMISSIONS'. At the very bottom, there are two buttons: 'CANCEL' and 'CONFIRM'.

You will have to supply the following information to add a new user:

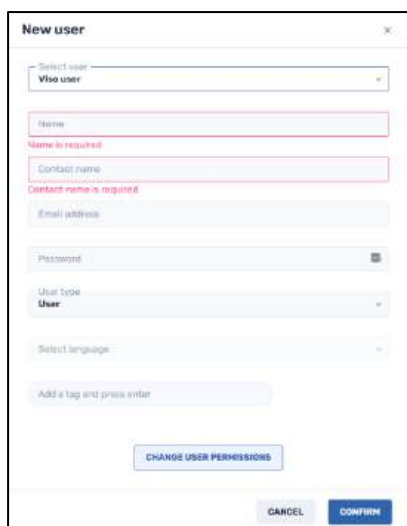
4.6.1.1 Select User

There are three options here:



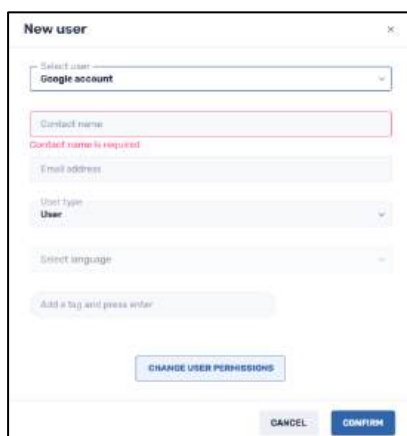
The screenshot shows the 'New user' form with the 'Select user' dropdown menu open. The dropdown menu has three options: 'Viso user', 'Google account', and 'Microsoft account'. The 'Viso user' option is highlighted. Below the dropdown menu, there is a 'Name' input field. Then, there is a 'Contact name' input field with a red error message 'Contact name is required'. This is followed by an 'Email address' input field with a red error message 'Email is required', and a 'Password' input field with a red error message 'Password is required'. Below these is a 'User type' dropdown menu with 'User' selected. Then, there is a 'Select language' dropdown menu. At the bottom, there is a button 'Add a tag and press enter'. Below this is a button 'CHANGE USER PERMISSIONS'. At the very bottom, there are two buttons: 'CANCEL' and 'CONFIRM'.

- **Viso user:** Note that if you use a Viso account, you will have to supply a name, contact name, email address, and password.



The screenshot shows the 'New user' form with the 'Select user' dropdown set to 'Viso user'. The form includes fields for Name, Contact name, Email address, Password, User type (set to 'User'), and Select language. There is a 'CHANGE USER PERMISSIONS' button and 'CANCEL' and 'CONFIRM' buttons at the bottom.

- **Google account:** If you add a new user by using their Google account, they will be sent a confirmation email. They will be in “Pending” status until they answer the confirmation email.



The screenshot shows the 'New user' form with the 'Select user' dropdown set to 'Google account'. The form includes fields for Contact name, Email address, User type (set to 'User'), and Select language. There is a 'CHANGE USER PERMISSIONS' button and 'CANCEL' and 'CONFIRM' buttons at the bottom.

After supplying the required information and clicking **Confirm**, the user’s account will appear in the Radix Device Management Platform Dashboard as being in “Pending” status.

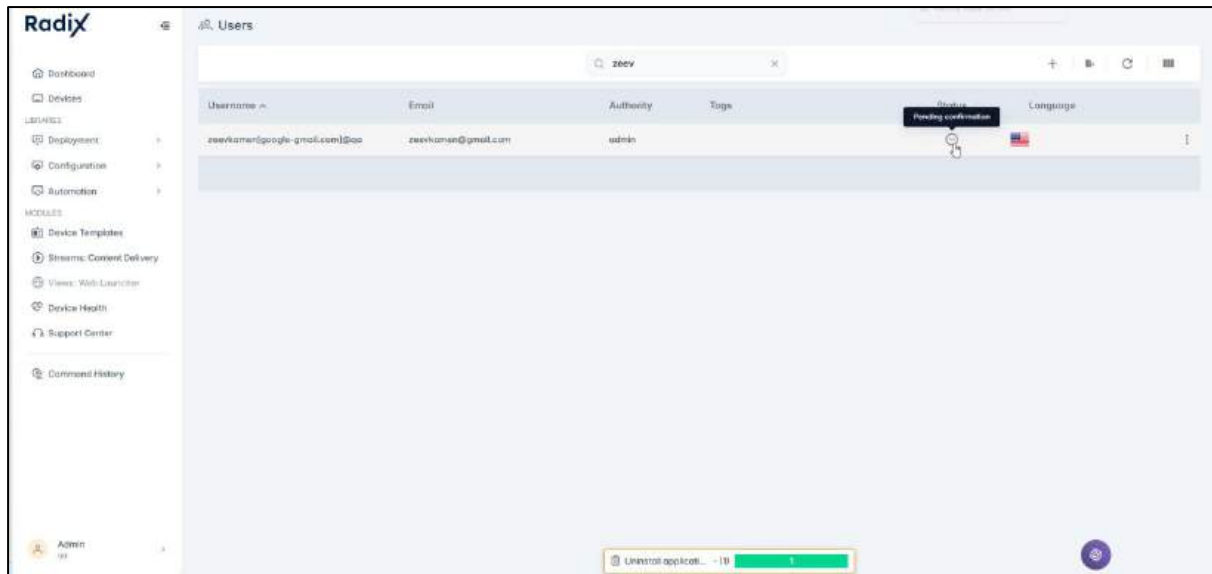


Figure 4-29: Appearance of user status, pending confirmation

The user will have to go to the email account that they provided, to click on the confirmation button.

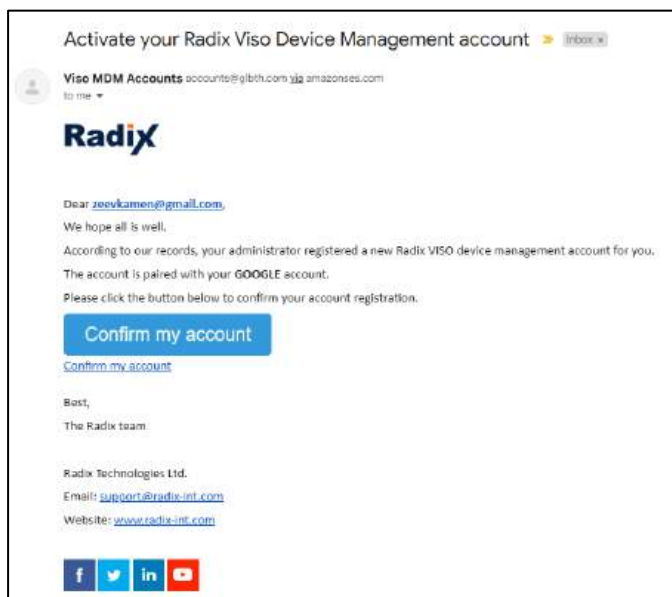
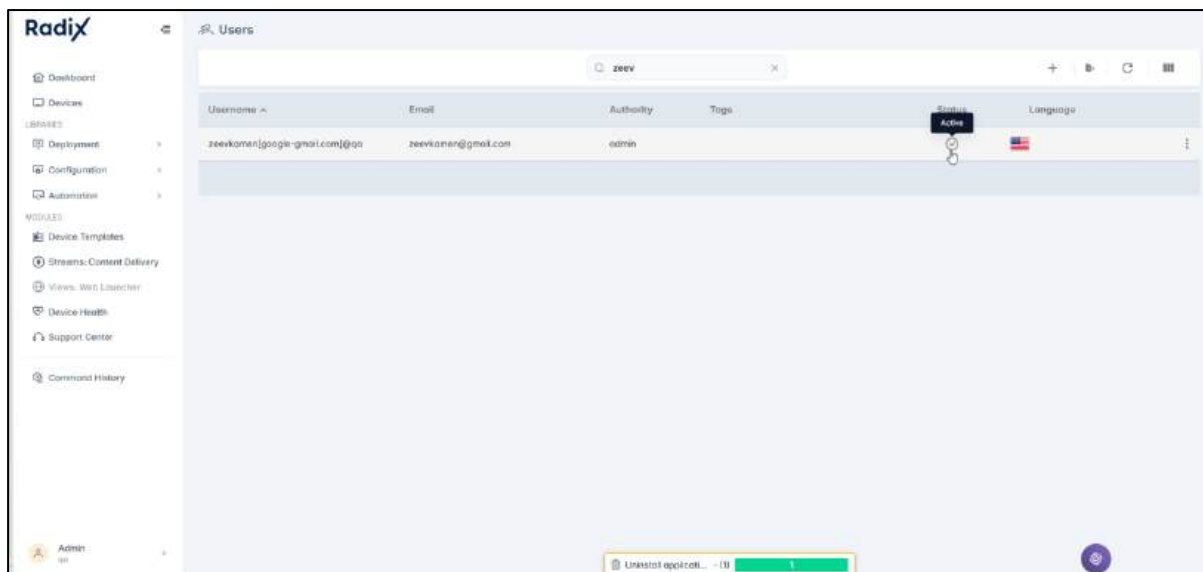
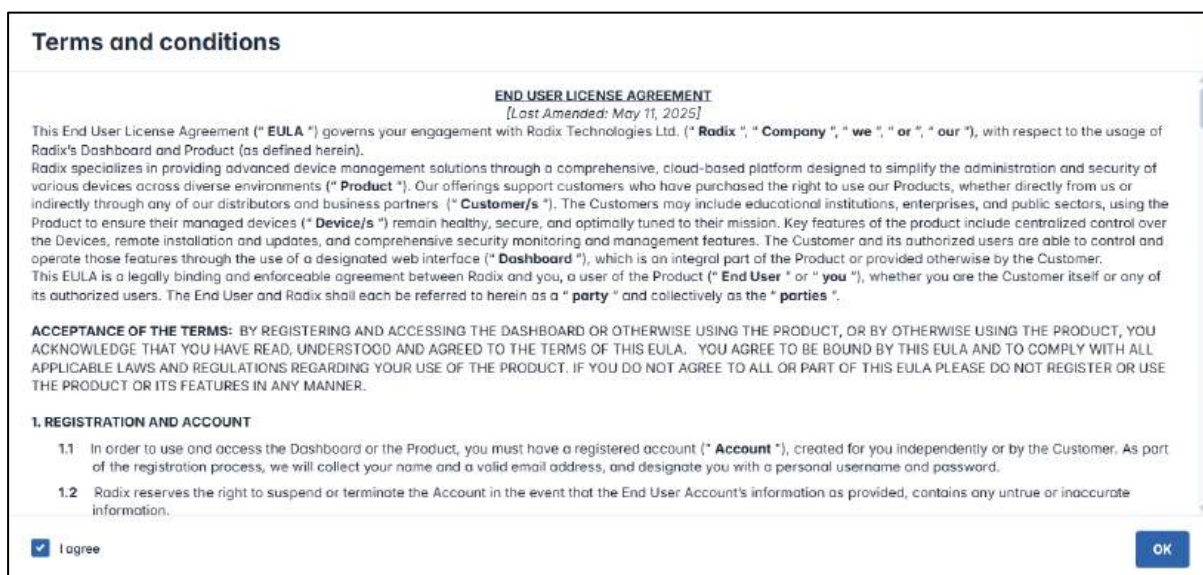


Figure 4-30: Google Account Confirmation E-mail

They will now appear in the Users Management Menu in “Active” status:



When the new user logs in for the first time, they will have to approve the EULA:



Zeev will now be seen as the user of the account:

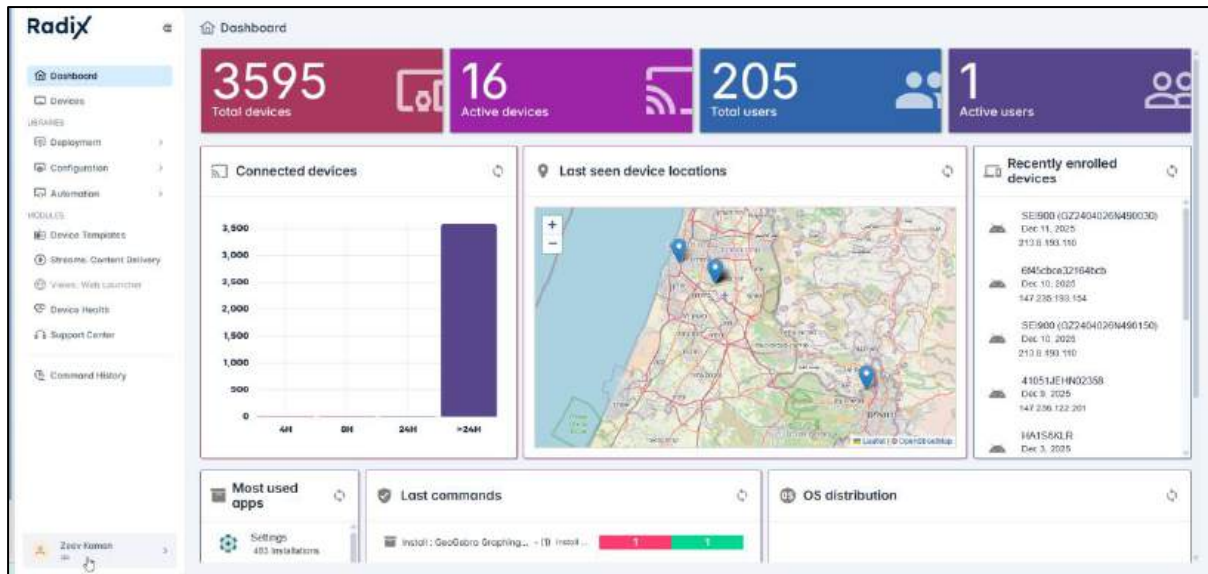


Figure 4-31: Zeev Kamen appears as the owner of the account

- **Microsoft account:** The sign-in requirements for a Microsoft account are similar to those for a Google account.

4.6.1.2 Contact Name

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

4.6.1.3 Email Address

The email address you supply will be used for alerts and messages to the user.

4.6.1.4 Password

Here you supply a password to enter your account. The password must be at least eight characters with a combination of letters, numbers, and symbols.

4.6.1.5 User Type

There are three user types, each with distinct levels of privileges:

- **Admin** – An administrator has full privileges. An administrator can view billing information and will also be able to view the other users in the Users Management Menu. Also, any user of the Radix Device Management Platform with “Admin” status

can edit any items that are set to “Read-only”. (Those with only “User” status can view and use these items but cannot edit them.)

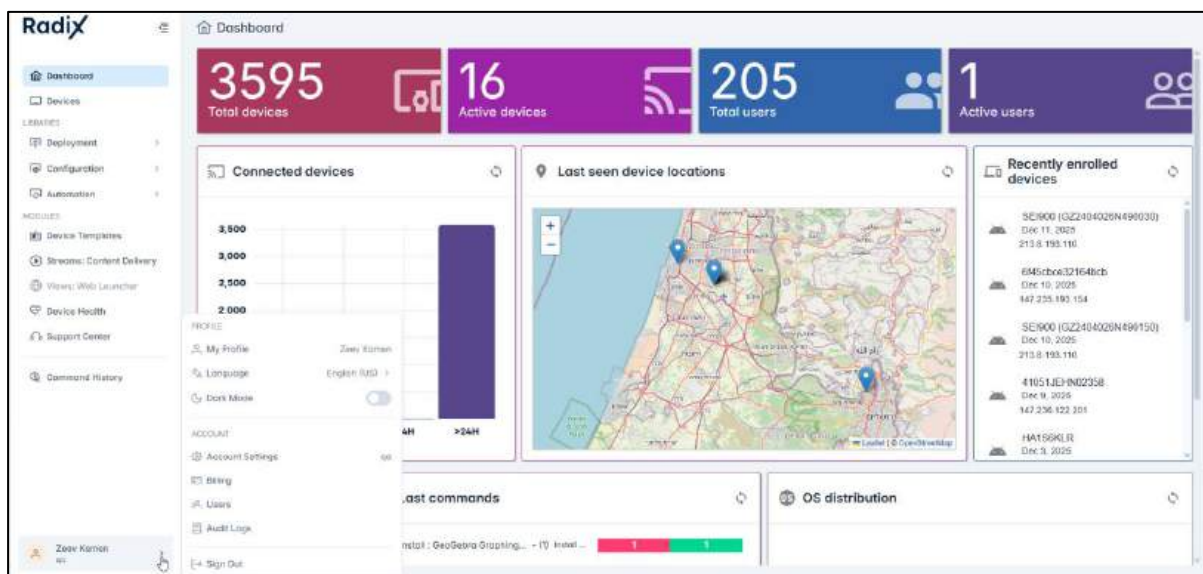


Figure 4-32: The interface of the user ("Zeev Kamen") with Admin privileges

- **User** – This means that the user has privileges for all functions, excluding that of managing users or viewing their billing information.

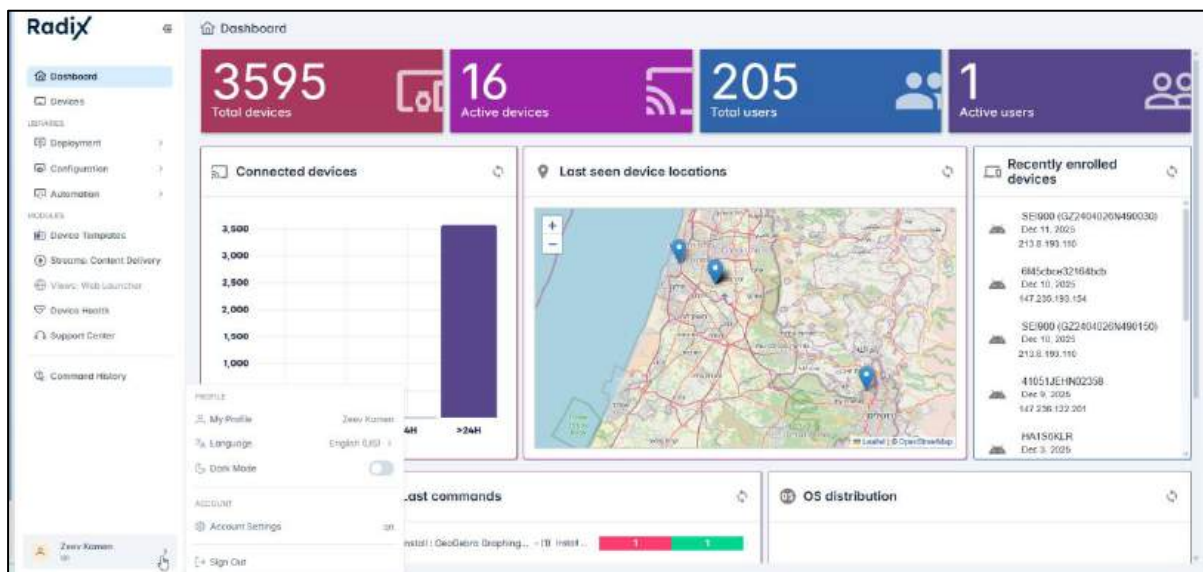


Figure 4-33: The same user as above, with only User privileges

- **Supporter** – This limits the user only to communicate with the Radix Support Center and changing the language of the Radix interface.

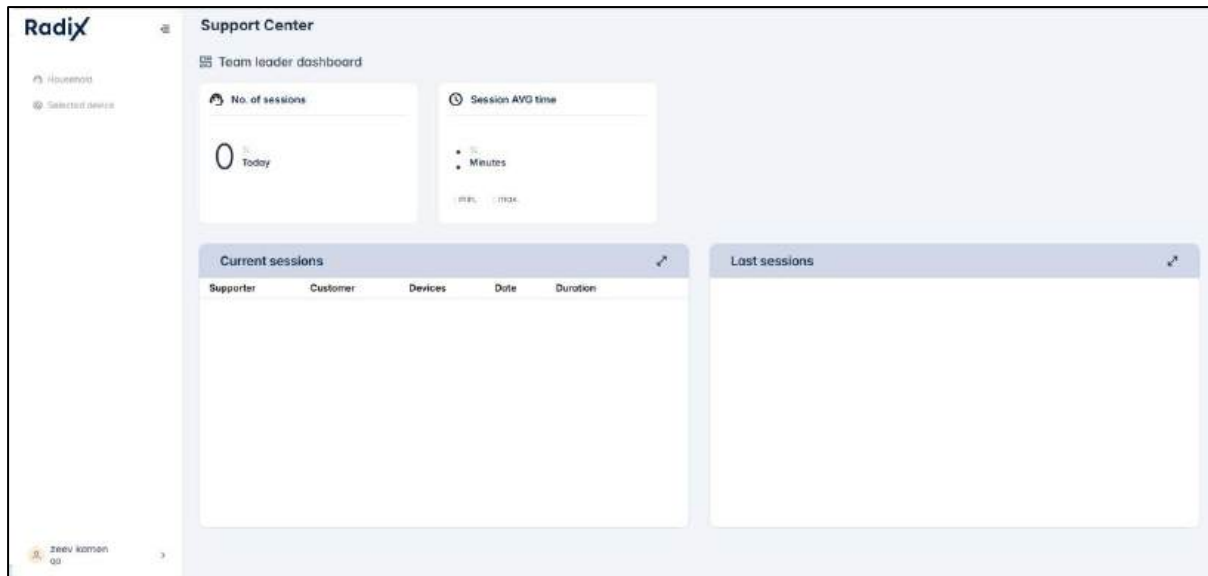


Figure 4-34: View of Display of User with only Supporter Privileges

4.6.1.6 Select Language

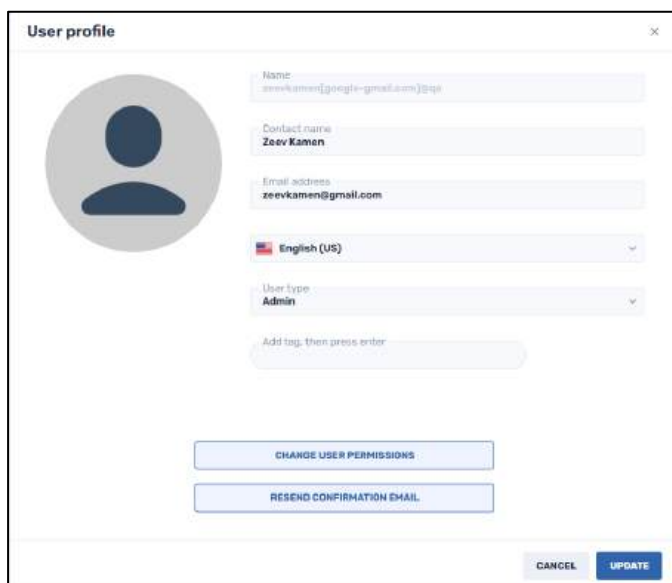
This allows you to select the default language in the user's Radix Device Management Platform user interface. The default language will be English.

4.6.1.7 Add a Tag

Tags are identifying names that you can assign to users or devices. By assigning tags to users, they will be able to see only devices with correlating tags. The devices must contain all the tags for the user to be able to see them.

4.6.1.7.1 Examples of Tags Applied to a User

- **Without tags:** If a user is not tagged at all, all devices enrolled are visible to the user. In the example below, the user has no tags associated with his account:



Therefore, when he logs into the Radix Device Management Platform, he will see all the devices presently enrolled:

OS	Device ID	Tags	Label	Email	Last seen	Policy-Kiosk	First Register
Android	97847a04770c644f	1234		Android Enterprise	Dec 25, 2025, 1:34 ...		Dec 21, 2025, 2:19 P
Android	HA7WMCB1	1234		radixvmt18@gmail.com	Dec 25, 2025, 1:35 ...		Nov 18, 2025, 12:05
Android	25041UE0R12375	1234			Dec 25, 2025, 1:34 ...		Dec 15, 2025, 1:01 P
Android	40352290CA	1234			Dec 25, 2025, 1:34 ...		
Android	4027093006A2	1234			Dec 25, 2025, 1:34 ...		Dec 14, 2025, 11:27
Android	6015660c3f0a	1234			Dec 25, 2025, 1:34 ...		Apr 10, 2023, 18:52 F
Android	AH7525900735UAA000...	1234			Dec 25, 2025, 1:34 ...		Dec 8, 2025, 6:28 P
Android	cndd2d812b7f77f0	1234			Dec 25, 2025, 1:34 ...		Feb 7, 2022, 3:40 P
Android	K161QWZ9A0036	1234			Dec 25, 2025, 1:34 ...		
Android	HATTJ620	1234		radixvmt18@gmail.com	Dec 25, 2025, 1:34 ...		Dec 10, 2023, 2:55 F
Android	L64PR0249T2203044	1234		radixvmt12@gmail.com	Dec 25, 2025, 1:34 ...		Mar 27, 2025, 9:18 A
Android	HA30E4F7	1234		myia.sahpamminbusiness@gmail.com	Dec 25, 2025, 1:34 ...		Jan 24, 2023, 2:54 F

Figure 4-35: Zeev Kamen's Devices Table. Note from the top of the Devices Table, he is able to view 949 devices

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

User profile

Name: zeevkamen@google-gmail.com/jgs

Contact name: Zeev Kamen

Email address: zeevkamen@gmail.com

Language: English (US)

User type: Admin

Add tag, then press enter

1234

CHANGE USER PERMISSIONS

RESEND CONFIRMATION EMAIL

CANCEL UPDATE

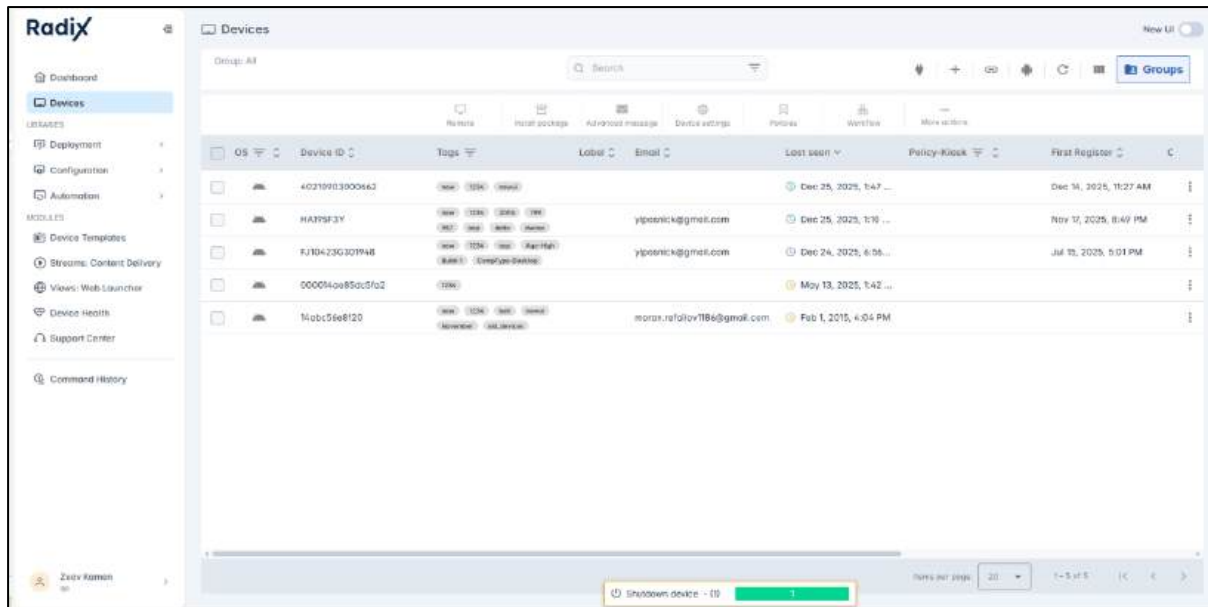


Figure 4-36: Zeev has been assigned the tag "1234", and can only view devices with the tag "1234"

- If the user is tagged with **1234** and **aep**, only devices containing both tags will be visible to the user:

Name

zeevkamen@google-gmail.com@gmail.com

Contact name

Zeev Kamen

Email address

zeevkamen@gmail.com

English (US)

User type

Admin

Add tag, then press enter

1234 aep

CHANGE USER PERMISSIONS

RESEND CONFIRMATION EMAIL

CANCEL

UPDATE

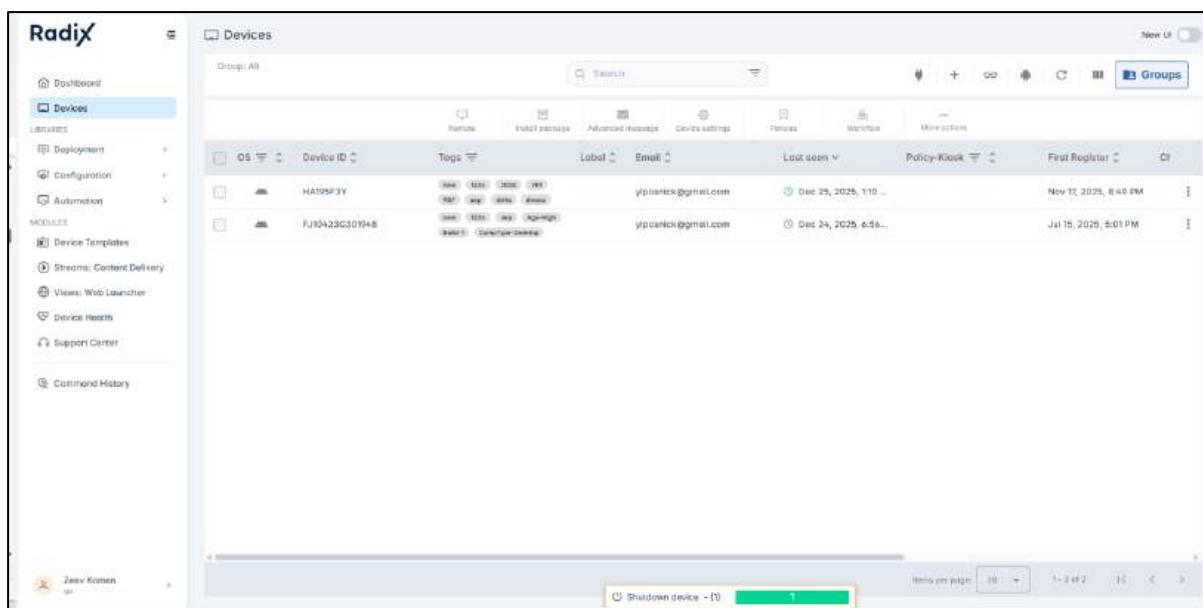


Figure 4-37: Zeev can only view the devices with both tags "1234" and "aep"

4.6.2 Viewing a User's Profile

Clicking on the row of a particular user will display the following User Profile screen:

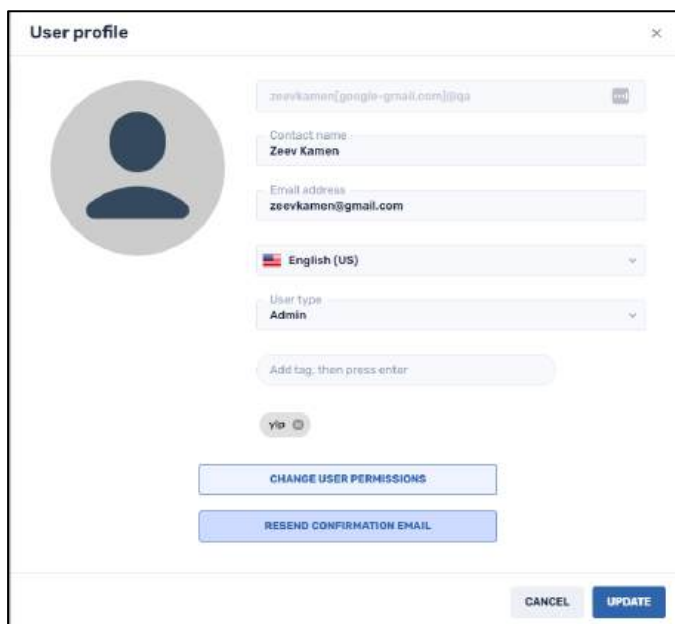
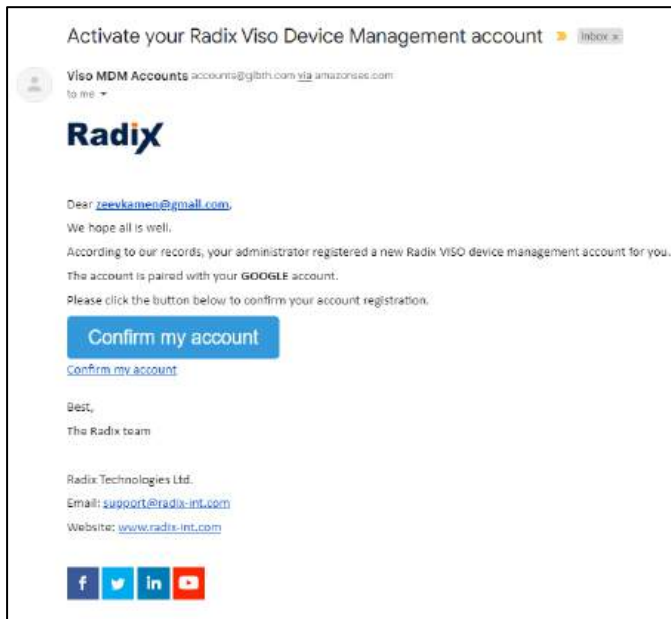


Figure 4-38: User Profile screen

It will display the following information:

- Username in the Radix Device Management system,
- User's contact name,
- User's email address,
- User's interface language,
- User type (Administrator/User/Supporter),
- A field to add tags to the user, to assist in grouping devices,
- An option to change the user's password,

- An option to change the user's permissions,
- A button to resend the confirmation email to the user. Clicking **Resend Confirmation Email** will send a request to the user's email to confirm their email address.



4.6.3 Changing the User's Interface Language

You can use the User Profile window to change the user's interface language.

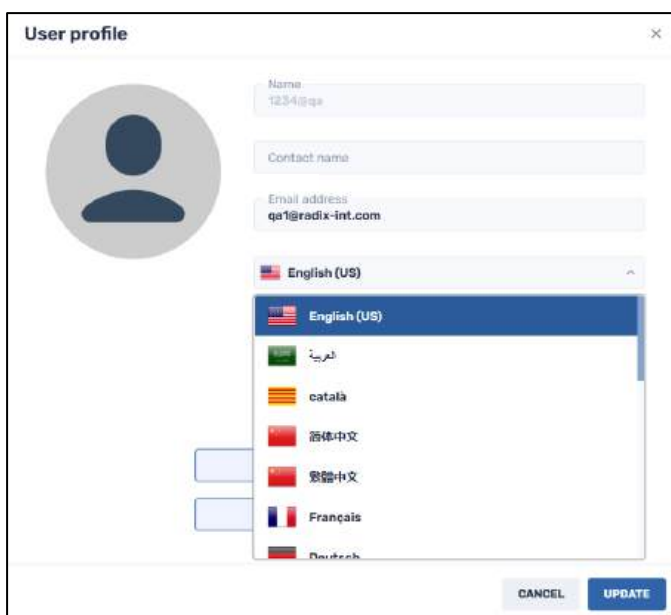


Figure 4-39: Selecting the language of the interface

This is convenient for managing many devices, for users who are comfortable in different languages.

4.6.4 Granting Administrator Privileges to a User

If a person has only User status, their **Account** menu will appear as follows:

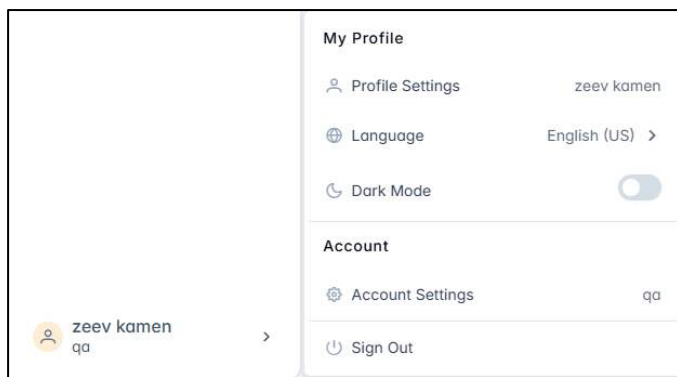


Figure 4-40: User Interface of Person with only "User" status

If the user's status is changed to **Administrator**, their **Account** menu will now include options to view their billing status, the list of users enrolled, and to view audit logs of the other users and their most recent commands.

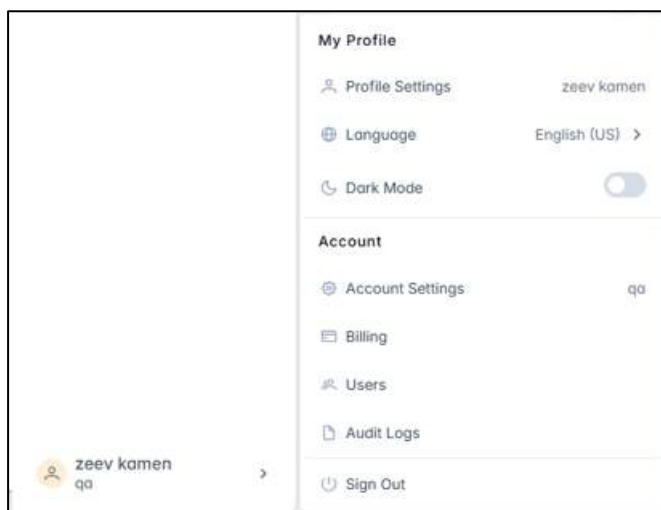


Figure 4-41: User Interface of person with "Admin" status. Note the "Billing", "Users", and "Audit logs" options

4.6.5 Changing User Permissions

If you click on **Change User Permissions**, you will see a full list of permissions that may be granted to an MDM console user:

User permissions [X]

Allow all ☒

Telemetry	☒	Device list manage	☒
Device settings	☒	Group Edit	☒
Remote view	☒	Device tags	☒
Remote control	☒	Fota	☒
Power manage	☒	Billing	☒
Packages install	☒	Account config	☒
Packages manage	☒	Device lock	☒
Device location	☒	Device wipe	☒
Advanced Messaging	☒	Policies/Kiosks	☒
Remote execute	☒	Manage device users	☒
Terminal	☒	Templates	☒
Edit workflow	☒	Template priority	☒

CANCEL **CONFIRM**

Figure 4-42: List of User permissions that can be granted

Note: This list of permissions is the Radix Device Management Platform console user. The settings do not affect the user of the local device in your fleet of devices.

Here is a brief description of each type of permission:

- **Telemetry:** To show/hide device metrics information from the Overview Dashboard. When a user has the Telemetry option turned off, the Dashboard and Insights buttons will be inactive.

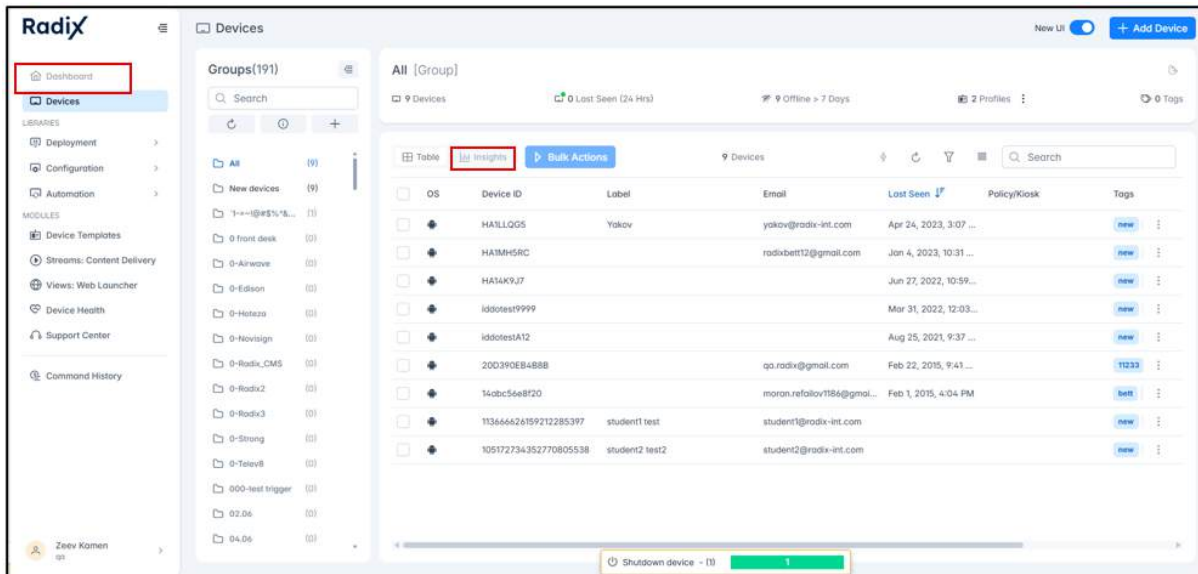


Figure 4-43: With Telemetry option turned off, the user cannot view device metrics from the Overview Dashboard or the Insights tab

- **Device settings:** To show/hide repository items from Device Settings. (See **Section 6.1.8, Device Settings**.) The Device Settings option on the Device Dashboard will be disabled as well. (See **Section 5.8, Device Dashboard**.)
- **Remote view and remote control:** If remote view is enabled, but not remote control, then the user is only allowed to see the screen of the device but will not be able to control the device remotely with their mouse. (See **Section 6.1.22**.)
- **Power manage:** To show/hide the **Shutdown**, **Restart**, and **Wake on LAN** actions. (See **Section 6.1.29, 6.1.25, and 6.1.36**.)
- **Packages install:** To enable/disable installing apps. (See **Section 6.1.13**.)
- **Packages manage:** To allow/disallow the user to clear apps data and start/stop/enable/disable/uninstall software packages. (See **Section 6.1.5, Clear Apps Data; Section 6.1.10, Disable/Enable apps; Section 6.1.34, Uninstall Packages**.)
- **Device location:** To allow/disallow viewing the device location. (See **Section 5.8.3.7, Location**.)
- **Advanced messaging:** To allow/disallow the **Advanced messaging** (**Section 6.1.1**) and **Assets** option.
- **Remote execute:** To enable/disable the **Remote execute** option. (See **Section 6.1.19**.)
- **Terminal:** To enable/disable the **Terminal** option in the Devices Table. (See **Section 6.1.33, Terminal**.)
- **Edit Workflow:** This enables/disables the user's ability to edit workflow items. The Radix MDM user can view and use the existing workflows stored in the repository but may not create or edit workflows. (It will still be possible for the user to edit their own workflows.) See **Section 6.1.37**.
- **Device list manage:** To show/hide the actions listed in the Device Dashboard under the **Manage** tab. (See **Section 5.8.3.10, Manage Menu**.)

- **Group edit:** To enable/disable making any changes to a group, such as creating or deleting a group. (See **Section 5.1.1, Creating a New Group of Devices.**)
- **Device Tags:** This allows/disallows the user from adding or deleting tags from a device. (See **Section 6.1.316.1.32.**)
- **FOTA:** This allows/disallows the user to use the Firmware OTA (=Over-the-Air) update engine command, to install firmware updates. (See **Section 6.1.16.**)
- **Billing:** To enable/disable access to billing information to the user. (See **Section 4.2.**)
- **Account config:** To show/hide the account settings on the Overview Dashboard and shows/hides the panes to access the account settings. (See **Section 4.4.**)
- **Device lock:** To show/hide the device lock and unlock actions. (See **Section 5.8.3.8, Lock Menu.**)
- **Device wipe:** To show/hide the option to wipe a device. (See **Section 5.8.3.8.4, Wipe.**)
- **Policies/Kiosks:** To show/hide the **Policy** and **Kiosk** repository items. (See **Section 6.1.20** and **Section 6.1.14.**)
- **Manage device users:** To enable/disable the ability to create or remove users from the device in the Device Dashboard. (See **Section 5.8.3.10.7, Manage Users.**)
- **Templates:** This will allow/disallow the user from creating, editing, or changing the priority of device templates. (See **Section 8.1, Creating a New Template.**)
- **Template priority:** This will allow/disallow the user from changing the priority level of the different device templates. The **Set Templates Priority** button will not appear in the Templates console. (See **Section 8.6, Setting the Priority of Templates.**)

Note: Any changes to the permissions that you grant to the MDM console users will only take effect the next time that those users log in or refresh their browser.

4.6.6 Deleting a User

Clicking on the three-dot menu in the far-right column will allow you to delete the user:

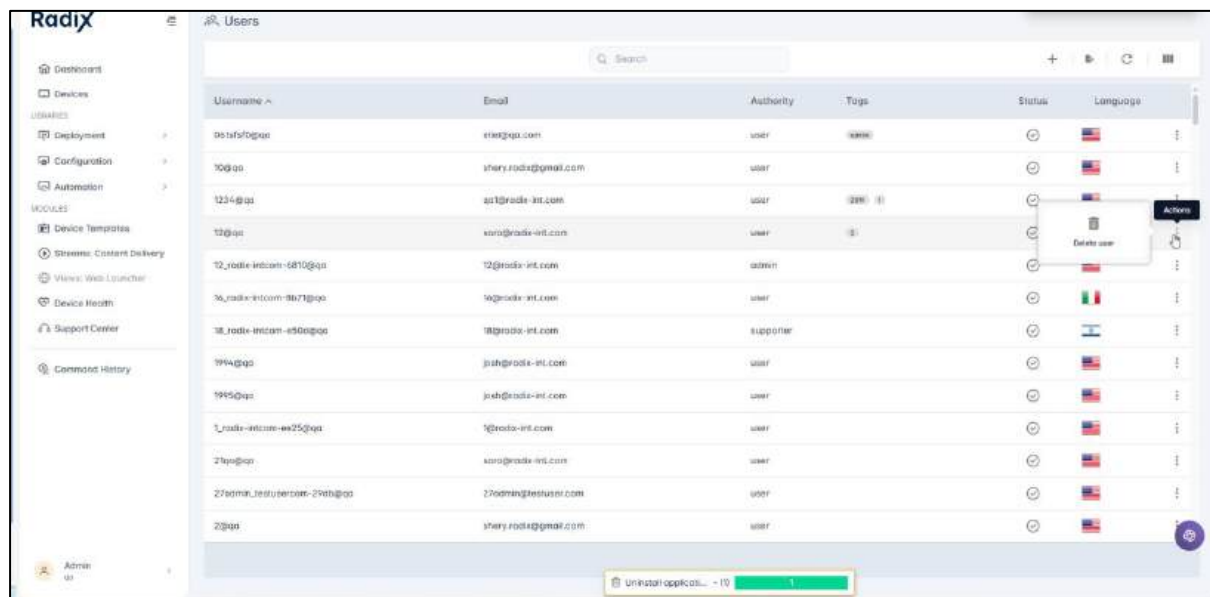
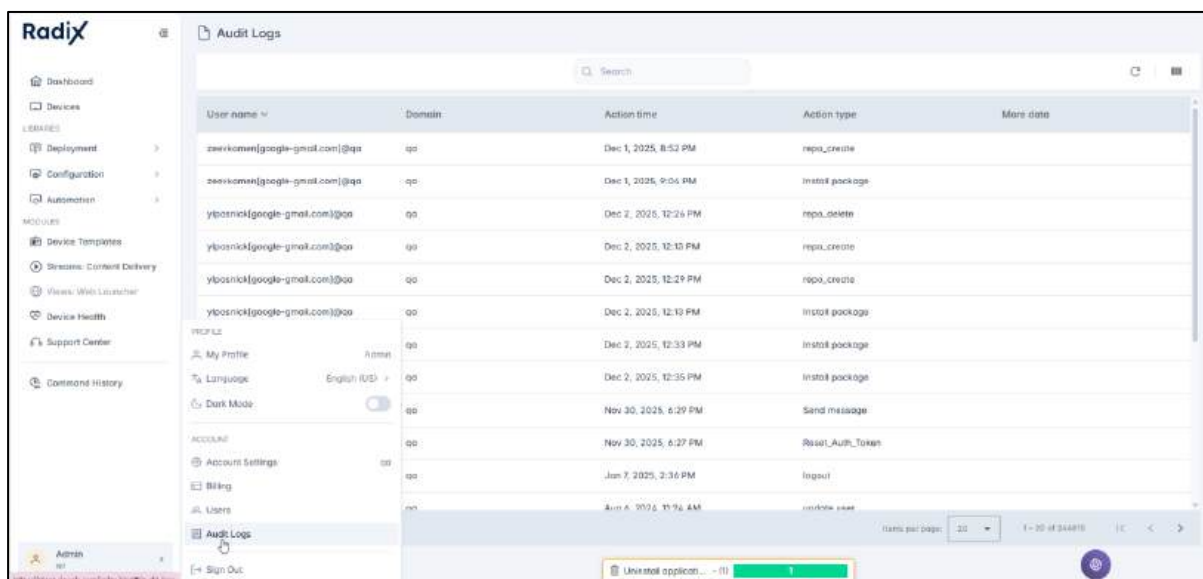


Figure 4-44: Option to delete a user

4.7 Audit Logs

If you have Administrator privileges, you have access to the **Audit Logs** panel. The **Audit Logs** pane allows you to view all of the commands sent by a user. This includes commands that are not shown by default in the Commands History log, such as removing a device, creating/deleting/changing a user account, creating/deleting a repository item, and starting/stopping a remote support session.

To access the Audit Logs pane, click on **Audit Logs** in the User Account Settings menu:



By clicking on the **Columns** icon in the upper right, you can specify which columns of data you wish to display. Options include username, domain name, the time the action was executed, and the type of action.

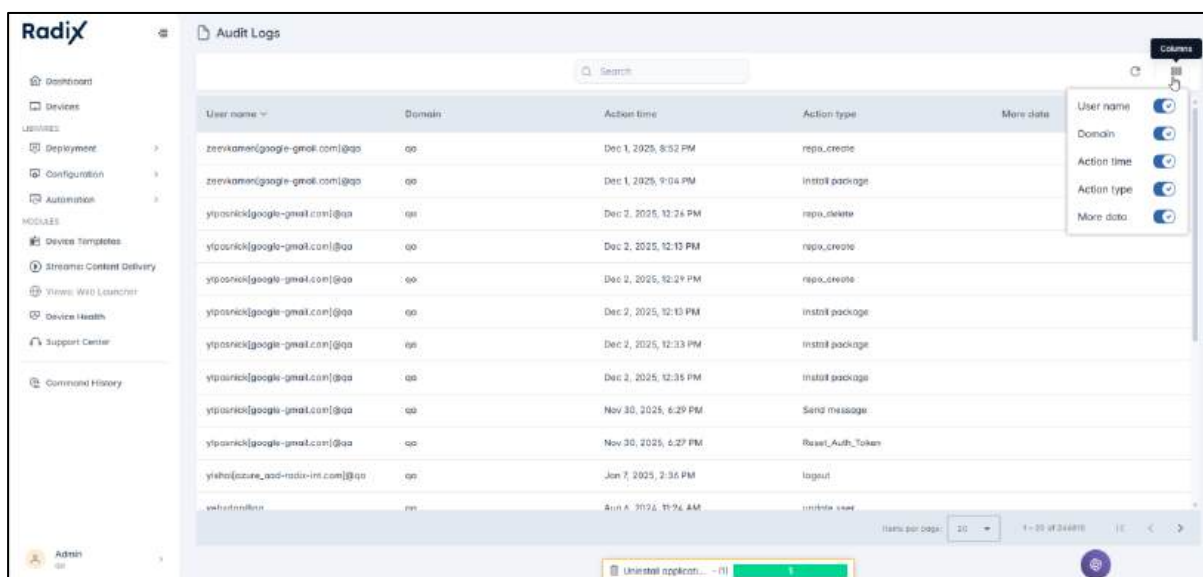


Figure 4-45: Columns icon allows you to select which data is to be displayed

Right-clicking on any entry in the Audit log will copy that entry to the clipboard.

Audit Logs

Search

User name	Domain	Action time	Action type	More data
zeevkamen[google-gmail.com]@qa	qa	Dec 1, 2025, 8:52 PM	repo_create	
zeevkamen[google-gmail.com]@qa	qa	Dec 1, 2025, 9:04 PM	install_package	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:26 PM	repo_delete	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:13 PM	repo_create	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:22 PM	repo_create	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:13 PM	install_package	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:33 PM	install_package	
ylposnick[google-gmail.com]@qa	qa	Dec 2, 2025, 12:35 PM	install_package	
ylposnick[google-gmail.com]@qa	qa	Nov 30, 2025, 6:29 PM	Send message	
ylposnick[google-gmail.com]@qa	qa	Nov 30, 2025, 6:27 PM	Reset_Auth_Token	
yishai@zure-ood-radix-int.com	qa	Jan 7, 2025, 2:36 PM	logout	
valburyn@qa	qa	Jan 6, 2025, 11:24 AM	update user	

4.8 Sign out

Selecting this gets you to the **Sign out** screen.

Radix Users

Search

Type	Username	Email	Authority	Tags	Status	Language
	061n10@qa	061n10@qa.com	user		✓	🇺🇸
	103@qa	103@qa.com	user		✓	🇺🇸
	10admin_testuser.com-0141@qa	10admin_testuser.com	user		✓	🇺🇸
	10admin_testuser.com-0155@qa	10admin_testuser.com	user		✓	🇺🇸
	1234@qa	1234@qa.com	user		✓	🇺🇸
	12@qa	12@qa.com	user		✓	🇺🇸
	12_radix-int.com-0110@qa	12_radix-int.com	admin		✓	🇺🇸
	12admin_testuser.com-0173@qa	12admin_testuser.com	user		✓	🇺🇸
	13admin_testuser.com-0107@qa	13admin_testuser.com	user		✓	🇺🇸
	14admin_testuser.com-0670@qa	14admin_testuser.com	user		✓	🇺🇸
	15admin_testuser.com-0141@qa	15admin_testuser.com	user		✓	🇺🇸
	16_radix-int.com-0173@qa	16_radix-int.com	user		✓	🇮🇹
	16admin_testuser.com-0173@qa	16admin_testuser.com	user		✓	🇺🇸

Sign Out

Are you sure you want to sign out?

NO YES

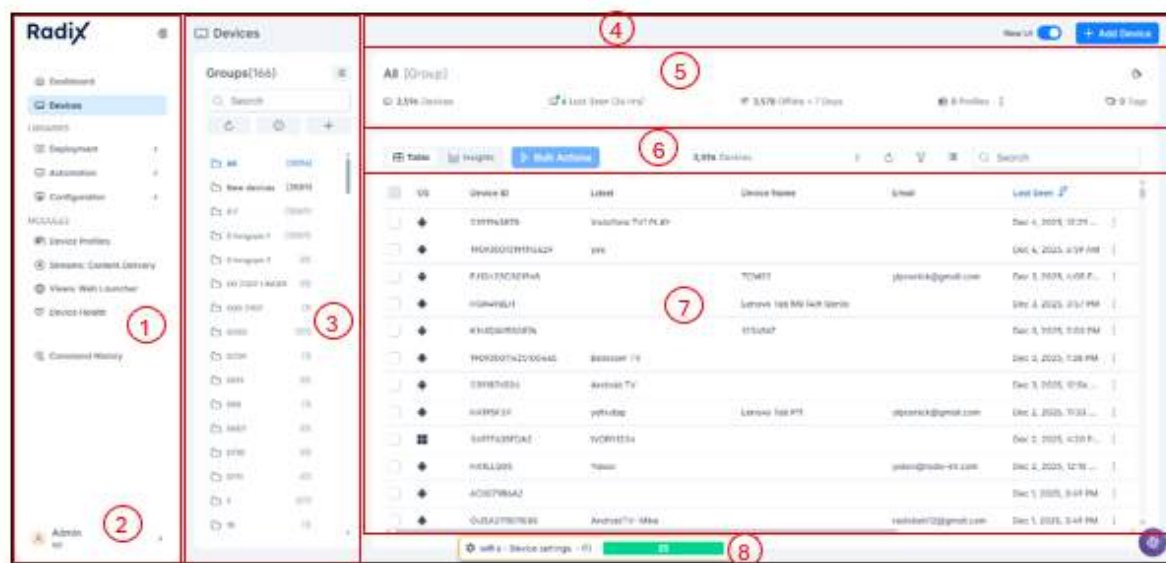
Figure 4-46: Sign out Screen

Chapter 5. Devices Table

The **Devices Table** is considered the “heart” of the Radix Device Management platform. It allows you to see all the devices that are presently in the system, as well as the username, the user’s email, and more. It allows you to assign privileges to a particular device, as well as troubleshoot the device if the user is having problems.

The Radix MDM’s Devices Table gives you options for applying commands to a single device, several devices at once, or even an entire group or fleet of devices.

When you click on Devices in the Navigation Bar menu, the following window opens. You see immediately that it consists of a number of panes:



The following table describes the functions of each pane of the Devices Table:

Item	Description
①	Navigation Sidebar Menu: Explained above in Section 3.1, Overview Dashboard-Navigation Sidebar Menu . This is for actions on devices: modifying device configurations, remote support, and messaging, organized by category. It contains a main menu that is divided into: • Device fleet overview • Device management • Library of command repositories • Configurations • Modules
②	User Profile and Account Management menu: Explained above in Chapter Chapter 4 . The User Profile menu allows you to adjust user permissions and the interface language. The Account Management menu allows you to manage account settings and billing.
③	Dynamic Groups Pane: This pane allows you to create groups of devices and perform commands on entire groups.

④	Top Action Bar: This has a button to revert to the previous UI, as well as a button to enroll new devices in the Devices Table.
⑤	Group Status Bar: This displays stats of a group of enrolled devices and their activity status.
⑥	Bulk actions Bar: This bar has commands to track device group metrics, execute commands on a number of devices simultaneously, filter the display of devices, customize the columns in the console, and search for specific devices.
⑦	Main Devices Table: Displays enrolled devices and allows you to access their Device Dashboard.
⑧	Recent commands status bar: This allows you to view the log of the most recent commands and whether they were executed successfully.

We will discuss the various sections of the Devices Table:

5.1 Dynamic Groups Pane

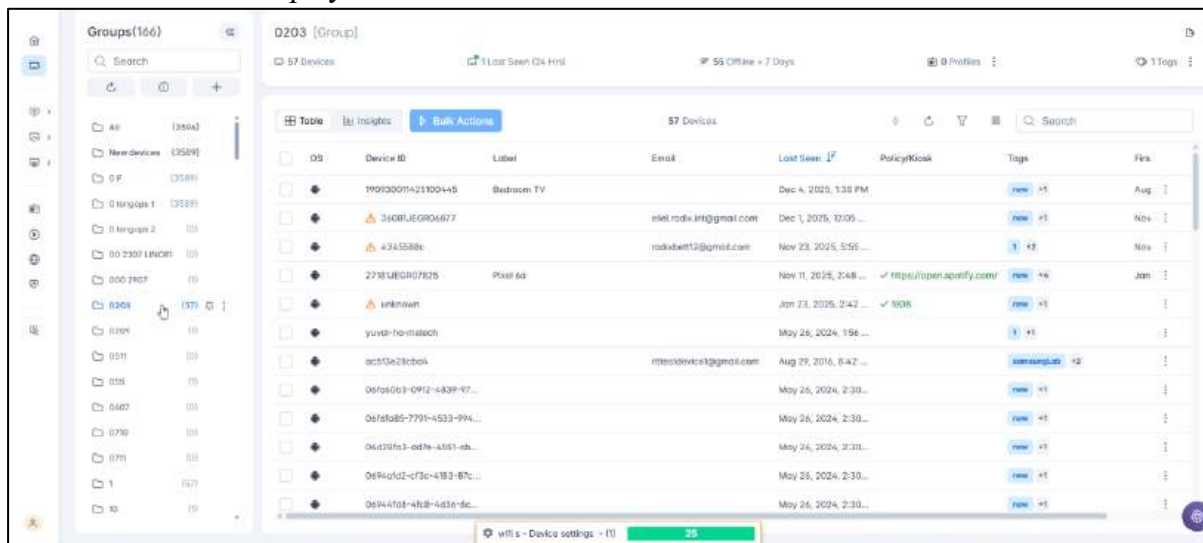
The Dynamic Groups Pane displays all device groups presently enrolled in the system. By creating device groups, you can apply actions to many devices at once. For example, you can send a text message or alert to an entire fleet of devices after placing them together in a group. You can create a group, and filter them by application, by device type, or operating system. You can also apply tags to specific devices in a group and perform actions just on the devices with that tag.



Figure 5-1: List of groups in Groups Pane

When you click on one of the groups, the devices in that group will be displayed in the Devices Table. For example, if we click on the group “0203”, which contains 57 devices, the

Devices Table will display 57 devices:



In order to restore the list of all of the enrolled devices (and not just those associated with the group “0207”), click on the “All” group at the top of the list. Selecting the “All” group will display all of the enrolled devices in the Devices Table.

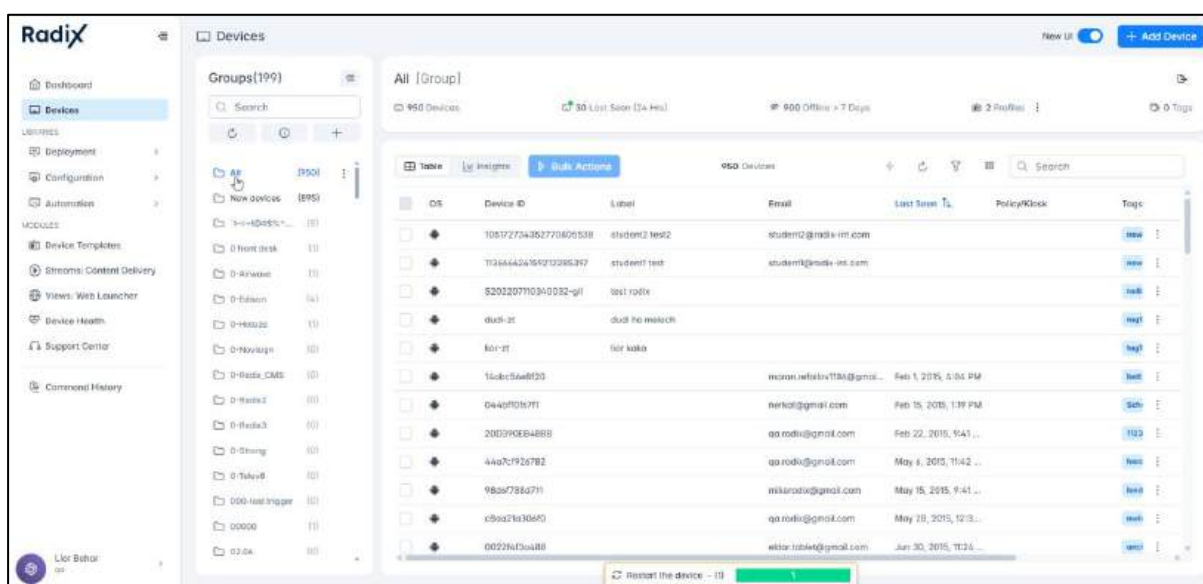


Figure 5-2: Clicking on the "All" group displays all of the enrolled devices

5.1.1 Creating a New Group of Devices

At the top of the Dynamic Groups Pane, you will see four icons:

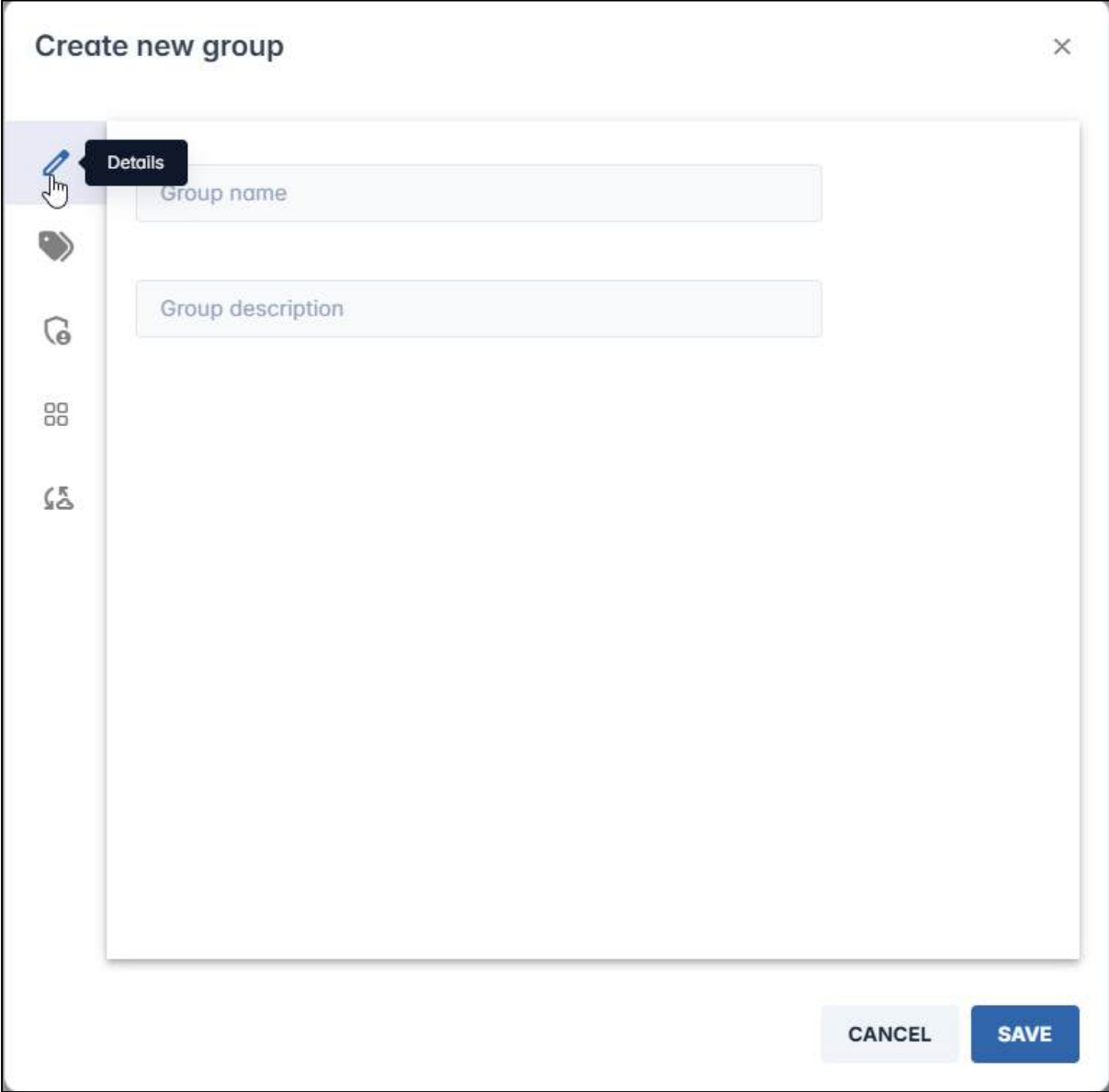
Table 5-1: Groups Window Options

Icon	Description
	Search group by name
	Refresh the list of groups
	Information about the Groups option

	Add a new group
---	-----------------

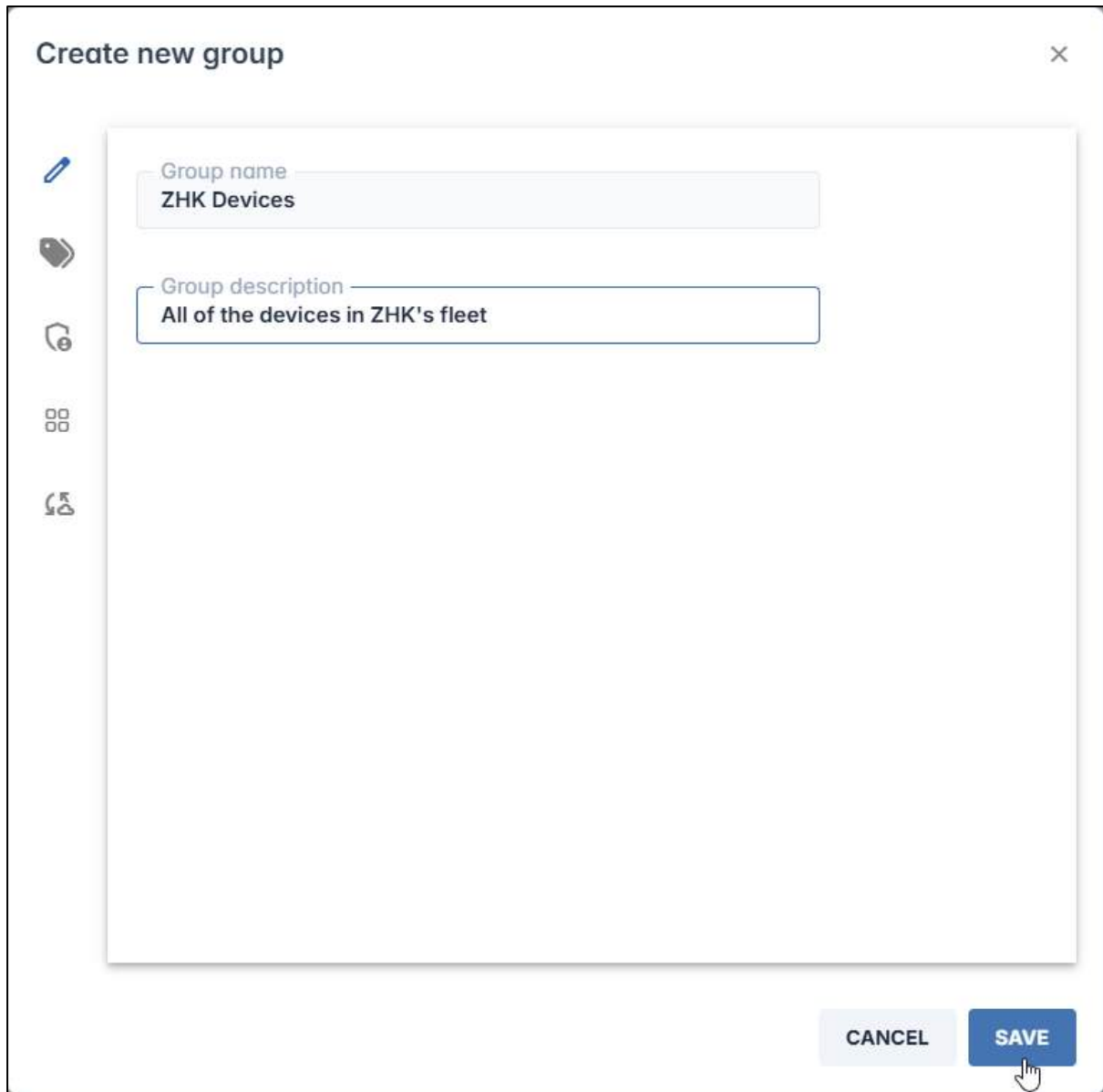
To create a group of devices:

1. Click on the **Add a new group**  icon. The **Create new group** window opens, in the **Edit Details** screen.



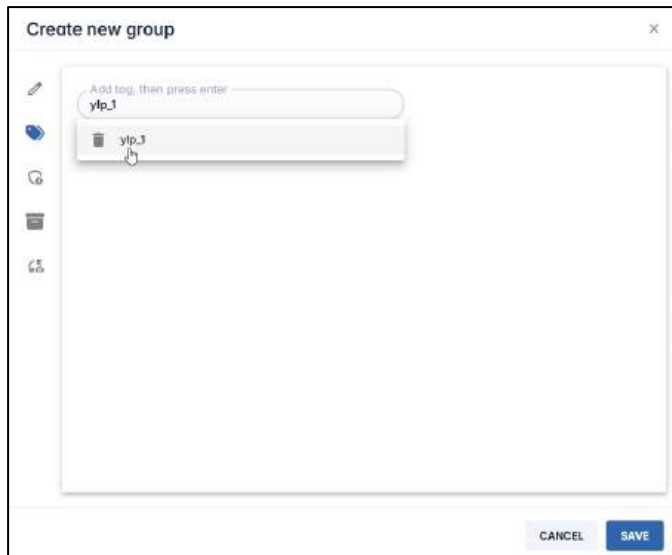
The 'Create new group' dialog box is shown. It has a title bar with 'Create new group' and a close button (X). On the left is a sidebar with five icons: a pencil (selected), a shield, a refresh, a grid, and a link. A 'Details' tooltip is over the pencil icon. The main area contains two text input fields: 'Group name' and 'Group description'. At the bottom right are 'CANCEL' and 'SAVE' buttons.

2. Supply a Group name and Group description.

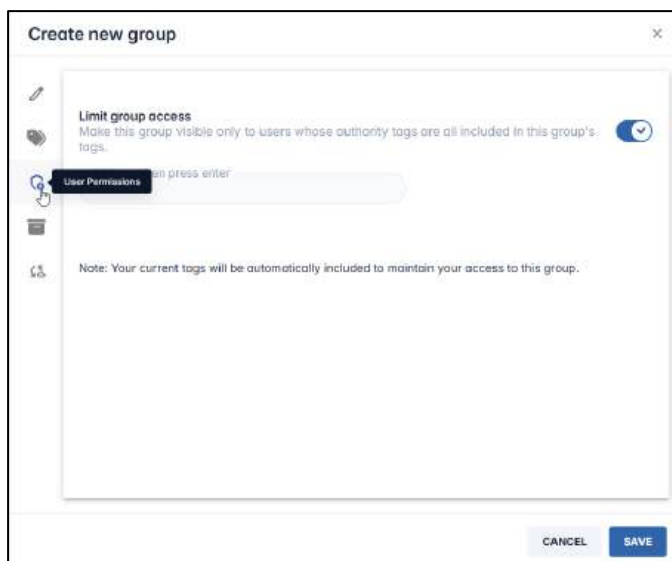


The screenshot shows a 'Create new group' dialog box with a close button (X) in the top right corner. On the left side, there is a vertical toolbar with five icons: a pencil (edit), a shield (security), a headset (support), a grid (groups), and a tag (tags). The main area of the dialog contains two text input fields. The first field is labeled 'Group name' and contains the text 'ZHK Devices'. The second field is labeled 'Group description' and contains the text 'All of the devices in ZHK's fleet'. At the bottom right of the dialog, there are two buttons: a light blue 'CANCEL' button and a dark blue 'SAVE' button. A mouse cursor is pointing at the 'SAVE' button.

3. Click on the **Tags** icon , and add a tag name in the **Add tag** window. The devices in a particular group all share the same tag(s). In the example below, we assign the tag “ylp_1” to the group.



- If you wish to limit who can view and perform changes on the group, click on the **User Permissions** icon  to open the User Permissions pane. By clicking on the **Limit Group Access** button and entering tags in the textbox, only users with the specific tags will be able to view the device group.



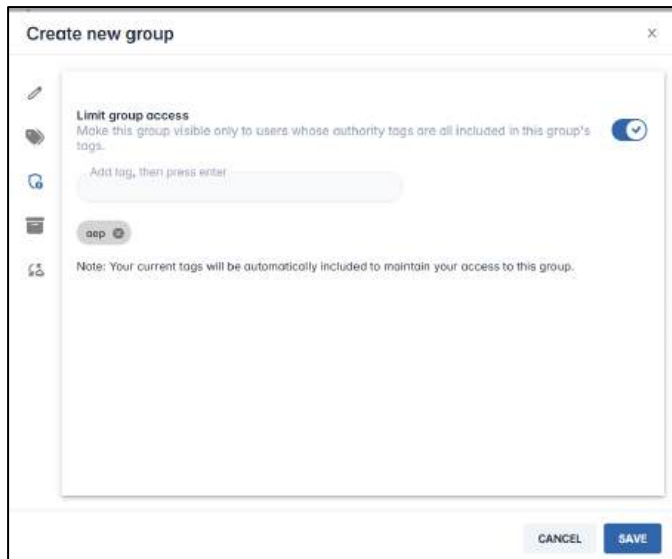
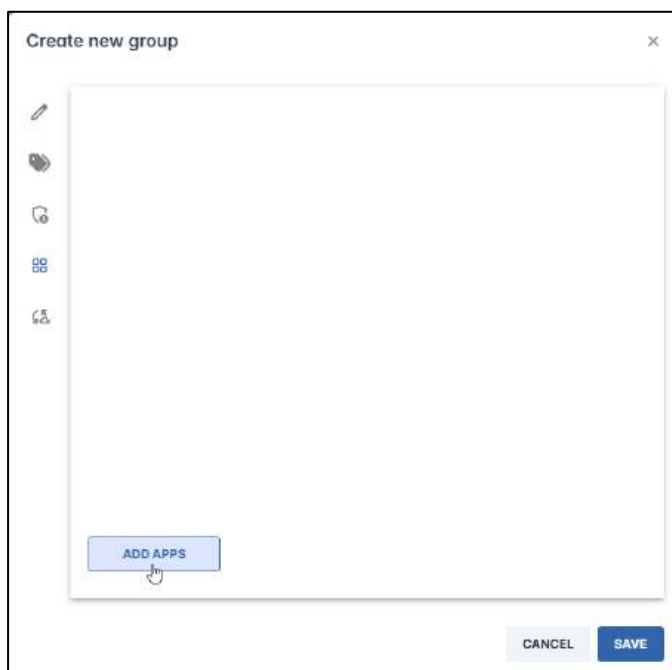
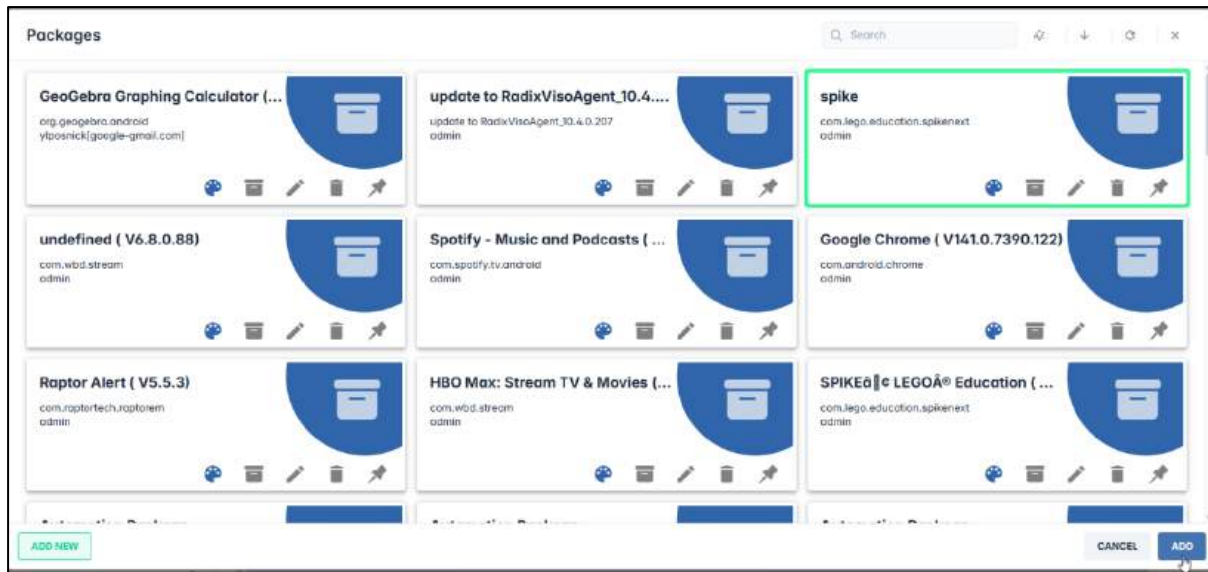


Figure 5-3: Only users with the tag "aep" will be able to view and edit the group

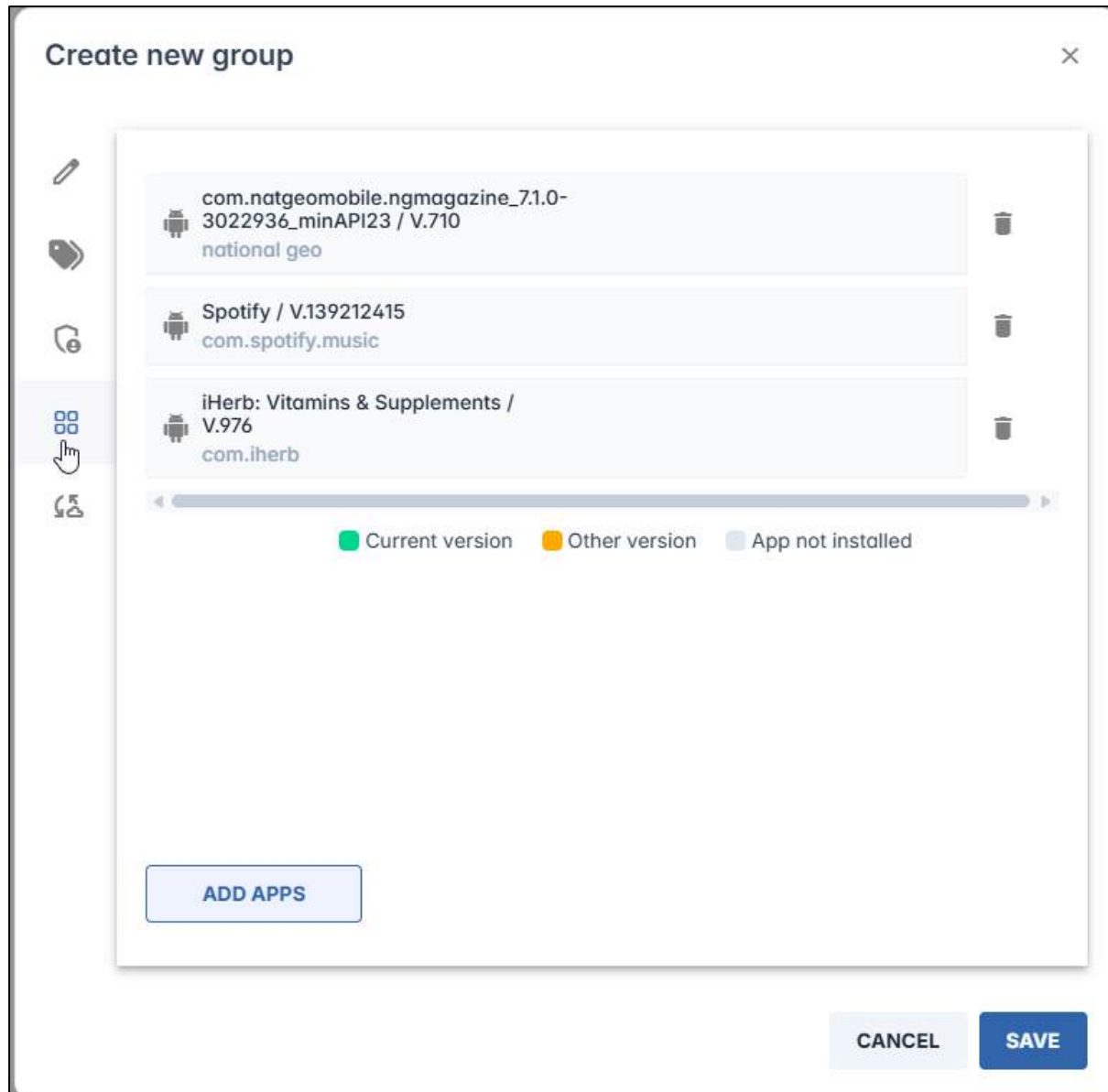
5. If you wish to install software packages to the devices in the group, click on the **Apps** icon , and click on **Add Apps**.



The **Packages** repository opens.



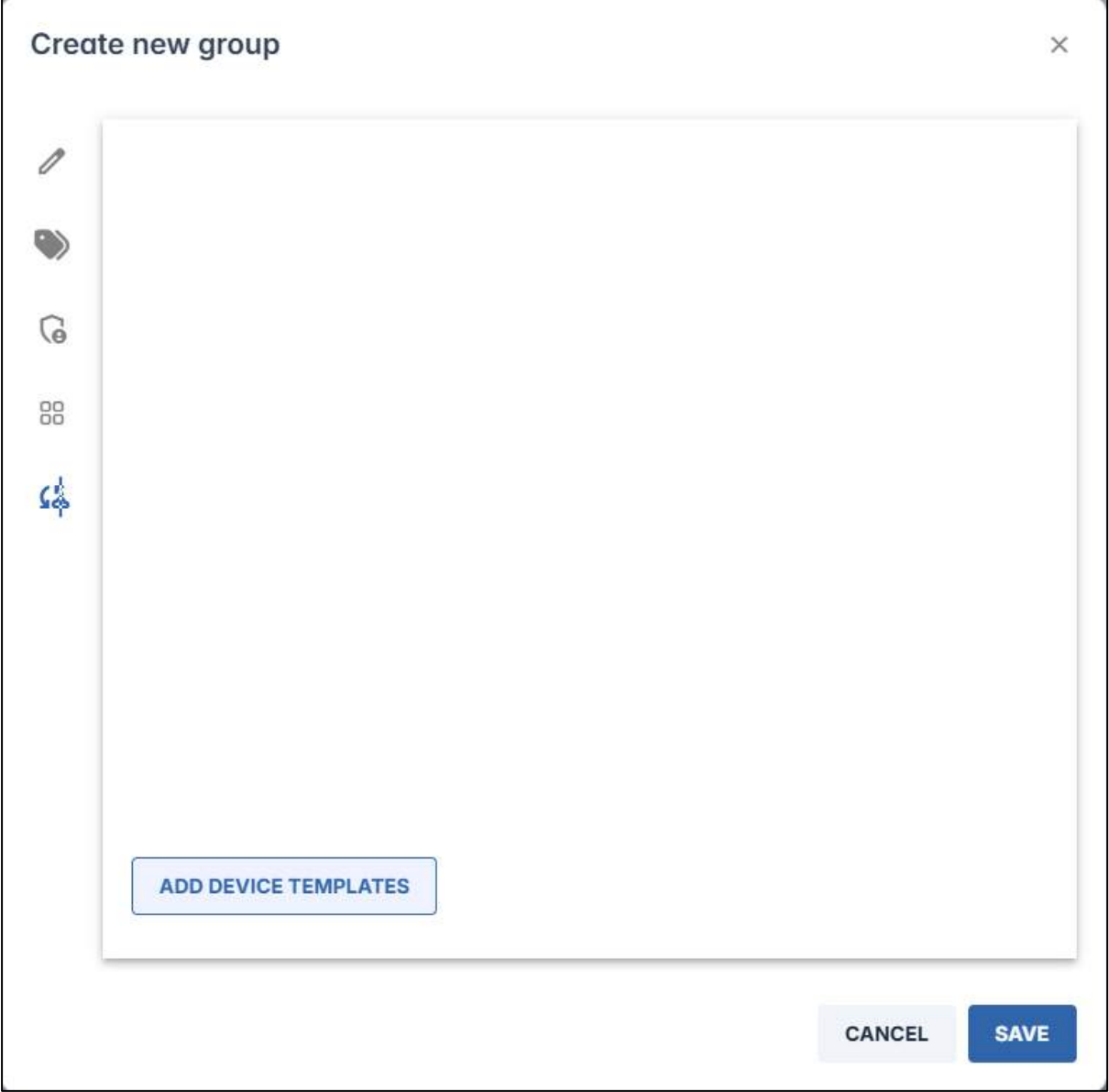
6. Select the software packages that you would like to add to the devices in your group and click **Add**.



You will see the software packages associated with this group, and the distribution of how they are installed on the devices in the group. In the example below, we see that the application **GeoGebra** has been installed on one of the devices in the group **RBP Devices**.

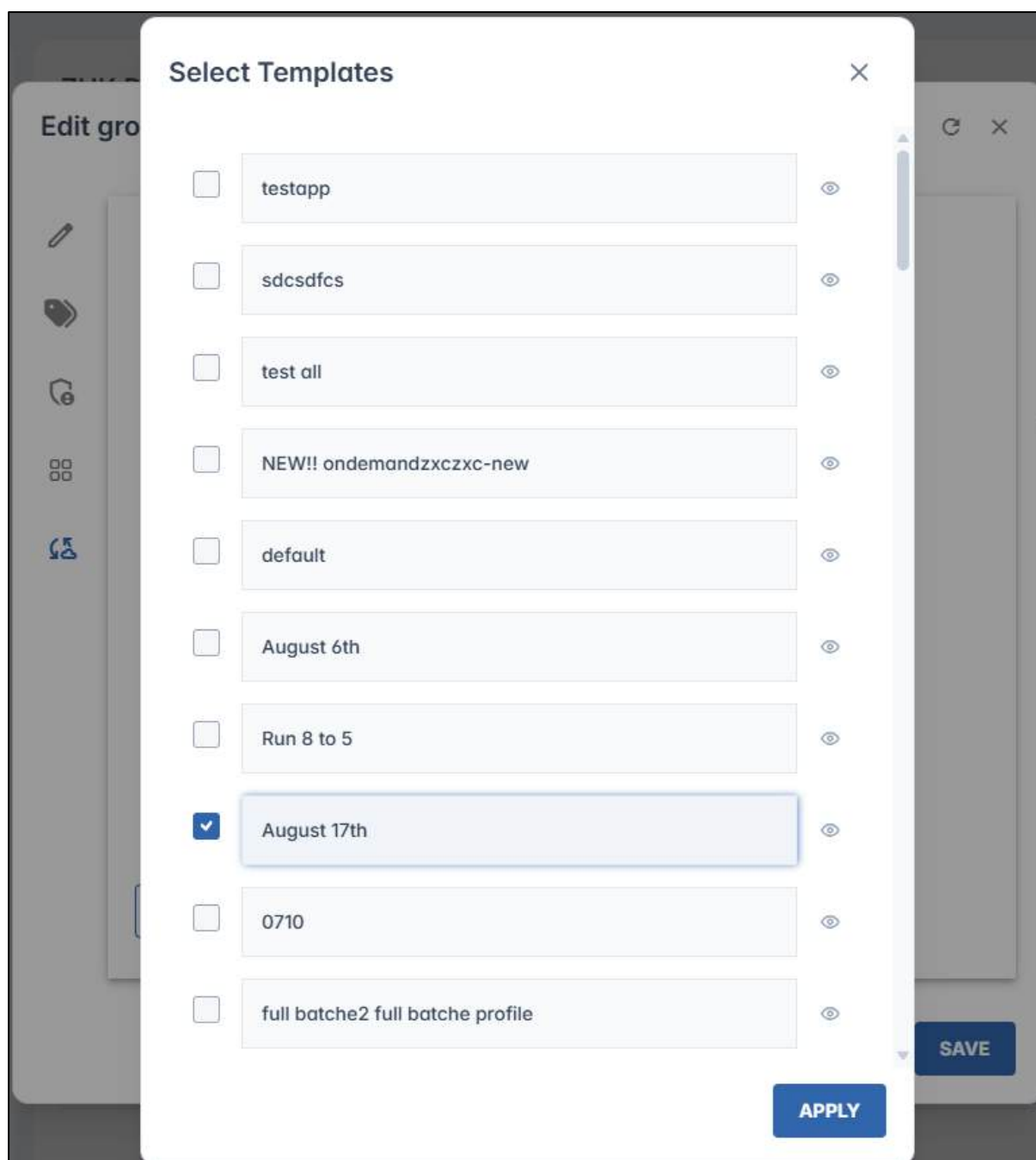


- Click on the **Template** icon  in the sidebar menu. The **Add Device Templates** button appears.



The screenshot shows a 'Create new group' dialog box. It has a title bar with the text 'Create new group' and a close button (X). On the left side, there is a vertical toolbar with five icons: a pencil, a shield, a shield with a plus sign, a grid of four squares, and a plug. The main area of the dialog is a large, empty white rectangle. At the bottom left of this rectangle is a button labeled 'ADD DEVICE TEMPLATES'. At the bottom right of the dialog, outside the main rectangle, are two buttons: 'CANCEL' and 'SAVE'.

8. When you click on the **Add Device Templates** button, you will be given a list of existing templates to add to the group.



9. Select the desired templates to add to the group and click **Apply**.

Edit group 'ZHK Devices'

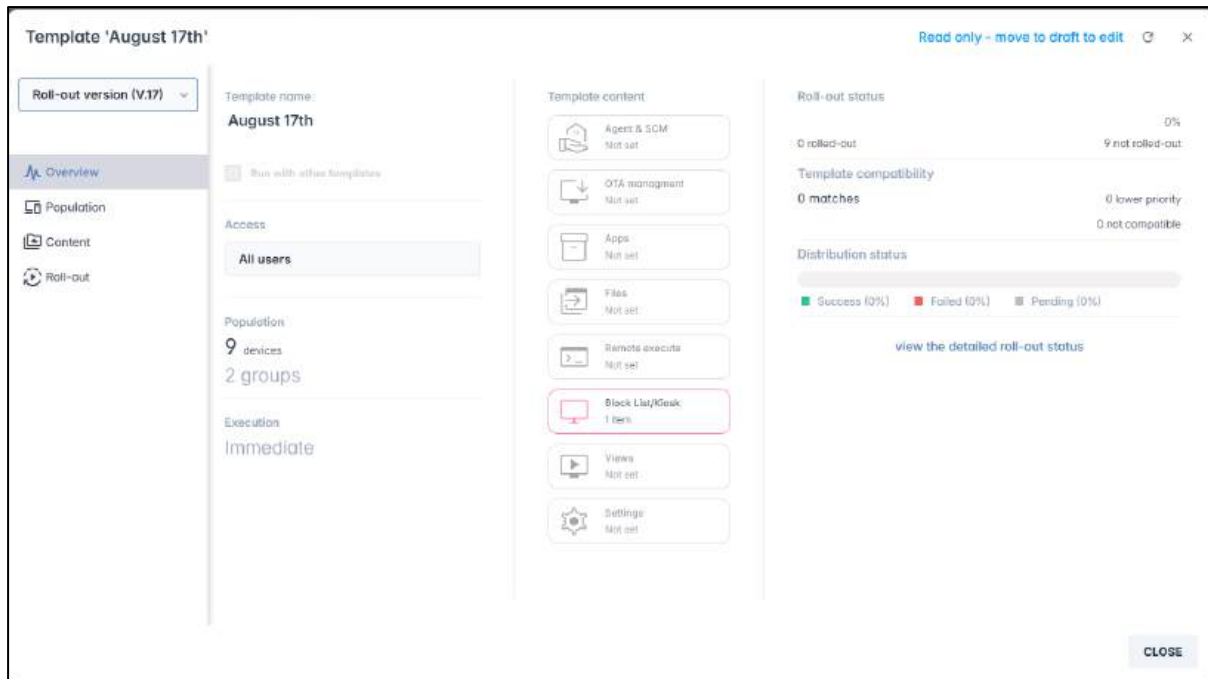
August 17th

ADD DEVICE TEMPLATES

CANCEL SAVE

The template will now appear in the group's list of templates.

10. Click on the template to view its details.



You can see the groups of devices that populate the template, the progress of the OTA updates, installation of software packages, execution of remote execute commands, and files sent to the devices associated with this template:

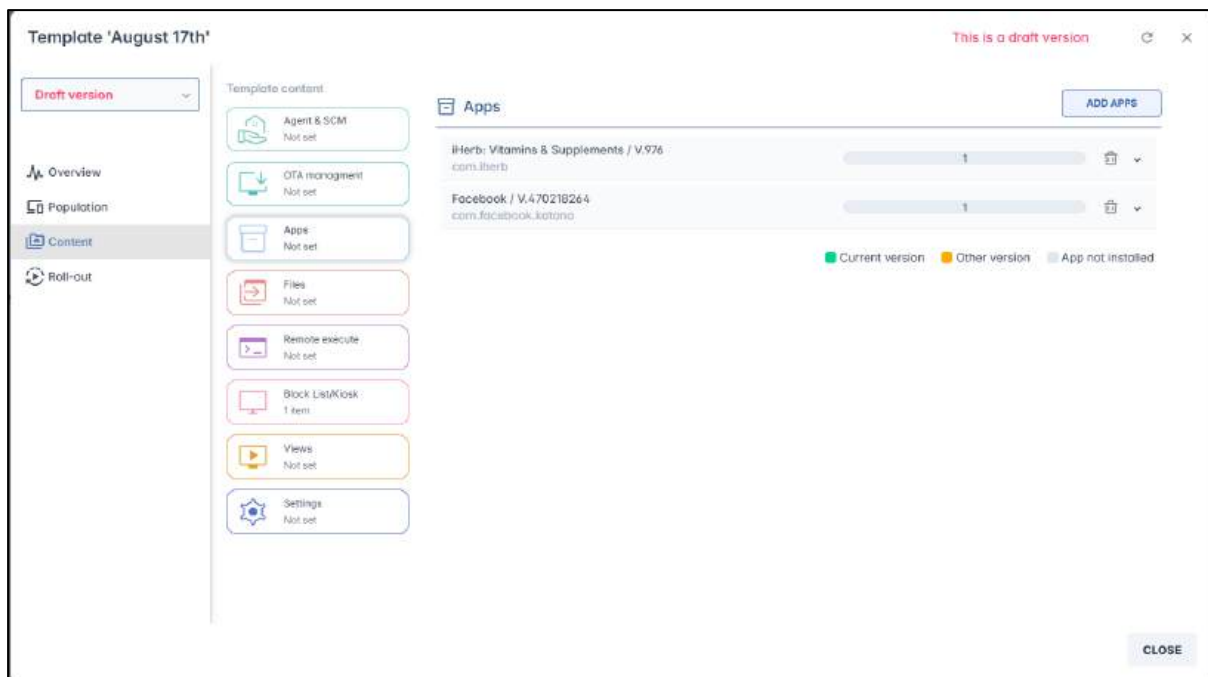
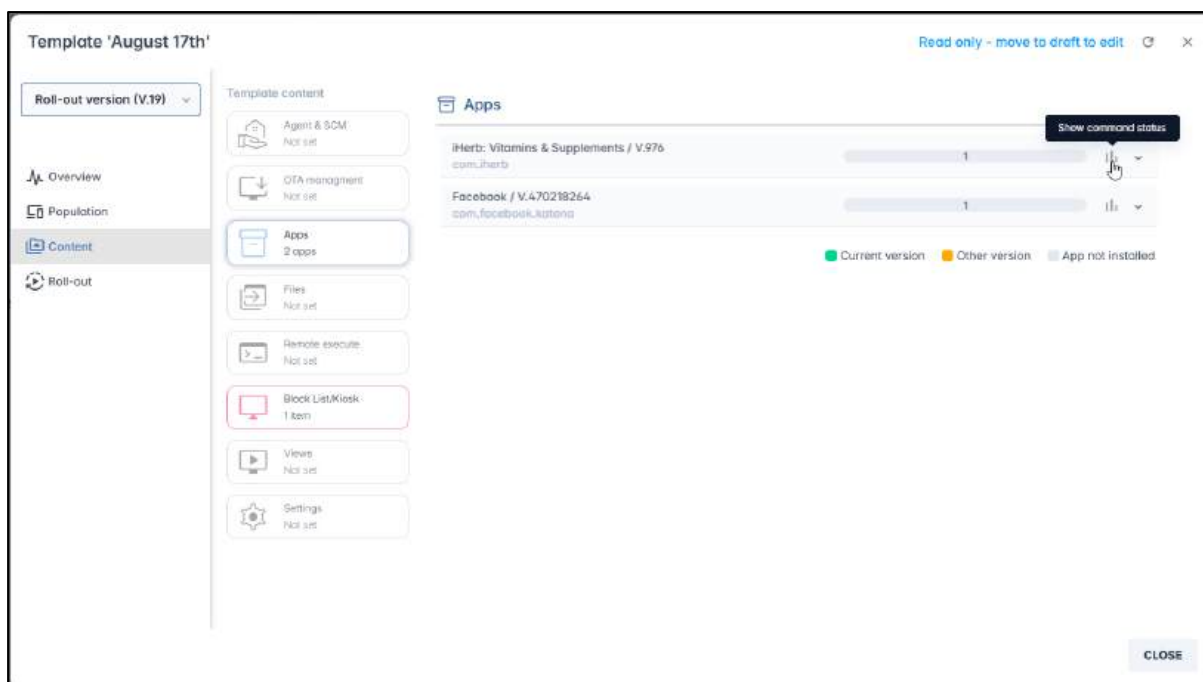


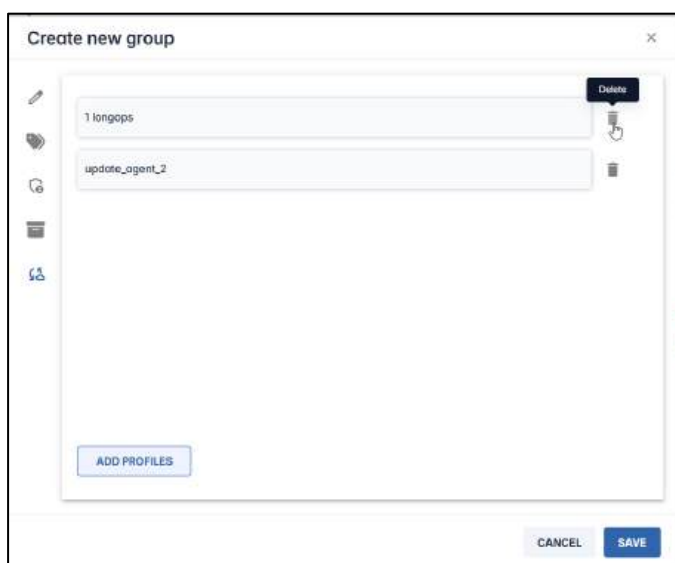
Figure 5-4: Display of software packages installed on devices associated with this template

We will discuss Templates (Device Templates) in greater detail in [Chapter 8, Device Templates Console](#).

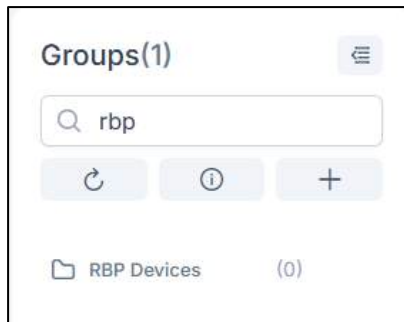
11. Clicking on the **Show Command Status** icon on the far right will display how the installation of software packages is progressing:



12. If you wish to delete a template, click on the **Delete** button next to that template.



13. Click **Save**. The new group will now appear in the list of groups. (In the example below, note that it says that there are no devices in the group “RBP Devices” yet. That is because no devices in our fleet have the identifying tag associated with the group “RBP Devices”. Once we assign a device the tag “ylp_1”, the group RBP devices will immediately have that device in the group.)



You can always edit the details of the group using the **Edit Group** option, as we will see below (**Section 5.1.3**).

5.1.2 Adding Devices to an Existing Group

To add devices to an existing group:

1. In the Devices Table, select devices that you want to add to a group, by clicking on the checkboxes of those devices.

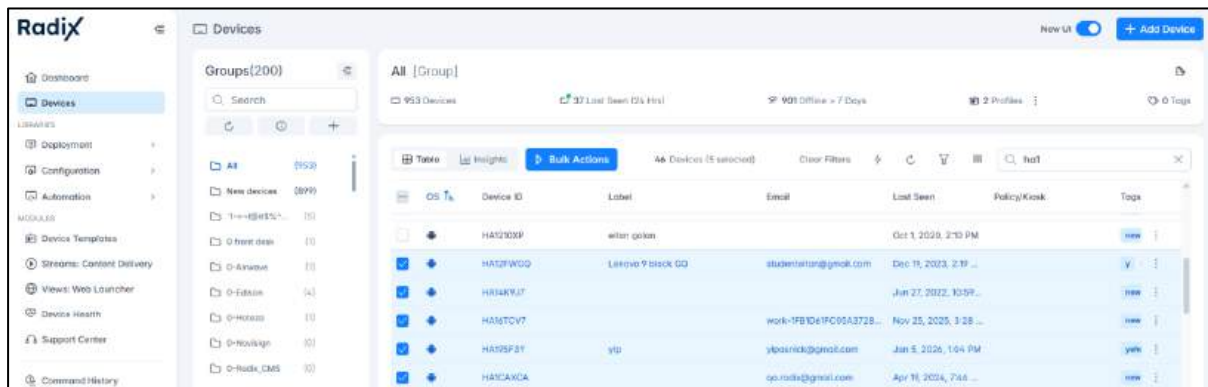


Figure 5-5: Selecting devices to be included in a group

2. Go to **Bulk Actions>Device>Set Device Tags** to open the Tags pane and add tags to the selected devices:

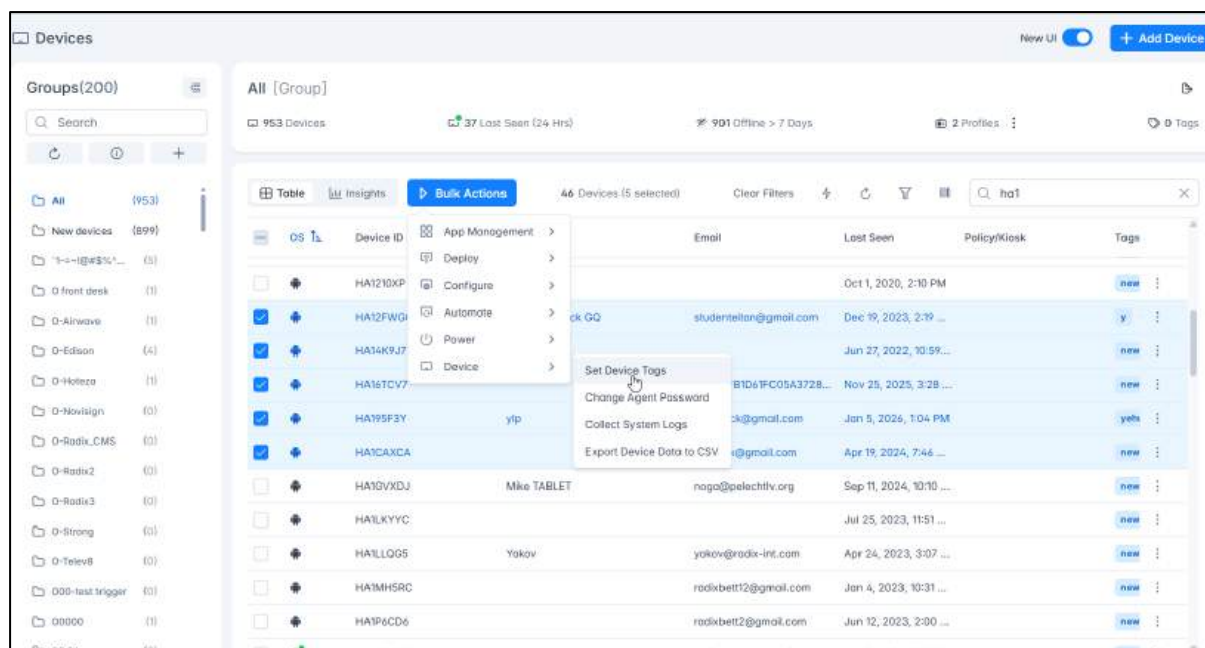


Figure 5-6: Assigning a tag to the selected devices

3. In the **Set Device Tags** pane, type the tag that identifies the group, and press **Confirm**. In our example, we wish to add the tag **ylp_1**. This is the identifying tag for the group “RBP Devices”.

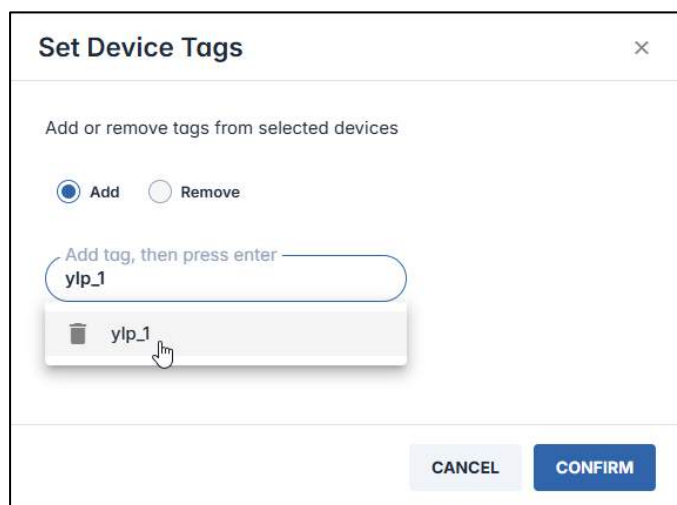
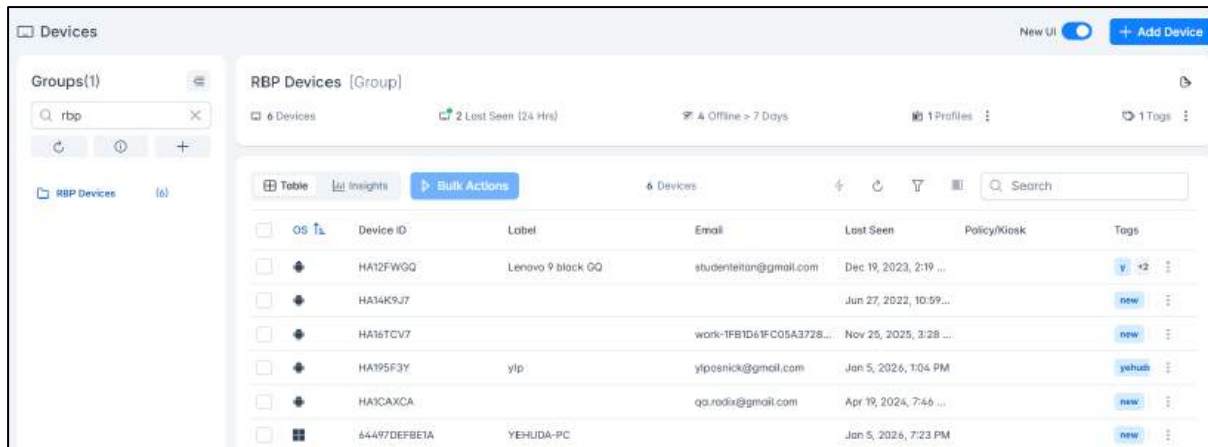


Figure 5-7: Assigning a tag to several devices

4. When you look at the group “RBP devices” in the Groups window, these devices with the **ylp_1** tag will now appear in the group.



The screenshot shows the 'Devices' page in the Radix interface. On the left, there's a sidebar with 'Groups(1)' and a search bar containing 'rbp'. Below it, 'RBP Devices' is listed with a count of 6. The main area displays 'RBP Devices [Group]' with 6 devices. At the top of the main area, there are filters: '6 Devices', '2 Last Seen (24 Hrs)', '4 Offline > 7 Days', and '1 Profiles'. Below these are tabs for 'Table', 'Insights', and 'Bulk Actions'. The 'Table' tab is active, showing a list of devices with columns: Device ID, Label, Email, Last Seen, Policy/Kiosk, and Tags. The data is as follows:

Device ID	Label	Email	Last Seen	Policy/Kiosk	Tags
HA12FWGQ	Lenovo 9 black QQ	studenttan@gmail.com	Dec 19, 2023, 2:19 ...		new
HA14K9J7			Jun 27, 2022, 10:59...		new
HA16TCV7		work-1FB1D61FC05A3728...	Nov 25, 2025, 3:28 ...		new
HA195F3Y	ylp	ylposnick@gmail.com	Jan 5, 2026, 1:04 PM		new
HA1CAKXA		qa.radix@gmail.com	Apr 19, 2024, 7:46 ...		new
6A497DEFBE1A	YEHUDA-PC		Jan 5, 2026, 7:23 PM		new

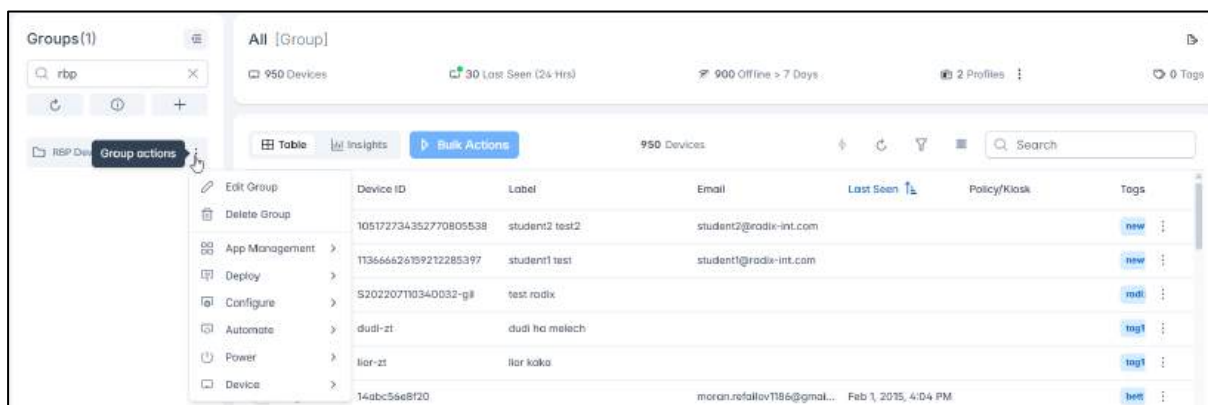
Figure 5-8: Display of devices in the specified group RBP Devices

5.1.3 Group Actions Options

After you have created a group, you may want to make modifications to the software packages applied to the members of the group, or other changes. The **Edit Group** command will allow you to make these modifications.

To manage a group:

1. Click on the **Group Actions** three-dot menu next to the Group name. A drop-down menu of group action commands appears.

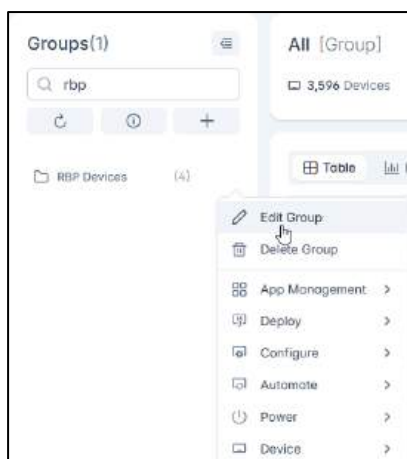


The screenshot shows the 'Groups(1)' sidebar with a search bar containing 'rbp'. Below it, 'RBP Devices' is listed with a count of 6. A dropdown menu is open next to 'RBP Devices', showing the following options: 'Edit Group', 'Delete Group', 'App Management', 'Deploy', 'Configure', 'Automate', 'Power', and 'Device'. The main area displays 'All [Group]' with 950 devices. At the top of the main area, there are filters: '950 Devices', '30 Last Seen (24 Hrs)', '900 Offline > 7 Days', and '2 Profiles'. Below these are tabs for 'Table', 'Insights', and 'Bulk Actions'. The 'Table' tab is active, showing a list of devices with columns: Device ID, Label, Email, Last Seen, Policy/Kiosk, and Tags. The data is as follows:

Device ID	Label	Email	Last Seen	Policy/Kiosk	Tags
10517273435277080538	student2 test2	student2@radix-int.com			new
113666626159212285397	student1 test	student1@radix-int.com			new
S202207110340032-g#	test radix				new
dudi-zt	dudi ha melech				tag1
lior-zt	lior kaka				tag1
14abc56e8f20		moran.refallov1186@gmail...	Feb 1, 2015, 4:04 PM		new

Figure 5-9: Group Actions menu

2. To perform modifications to the group, click on **Edit Group**.



3. An **Edit Group** window opens, with the same functions as the **Add New Group** window.



Figure 5-10: "Edit Group" Window

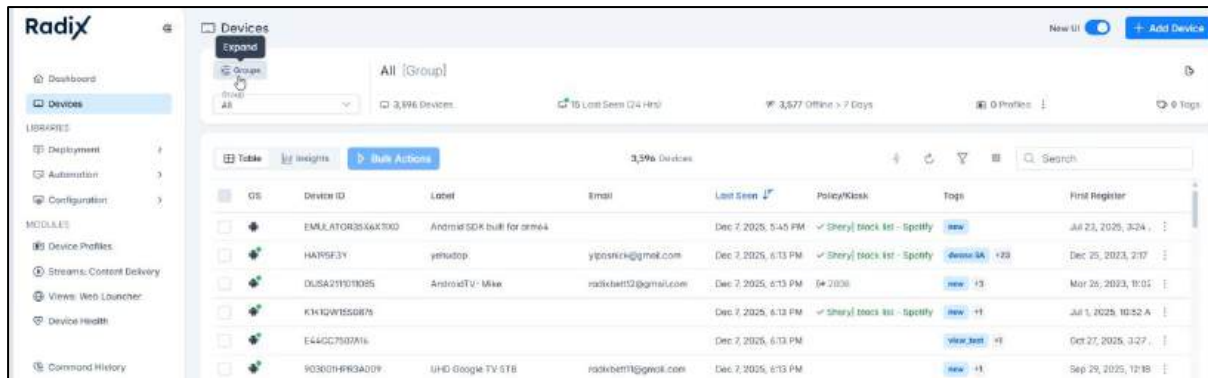
4. Proceed as in **Section 5.1.1**, adding tags, defining user permissions, installing software packages, and assigning a template to the group, if desired.

5.1.4 Deleting a Group

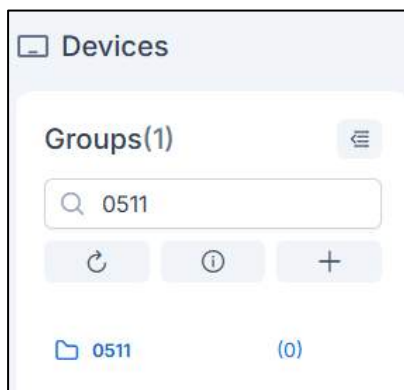
The Groups panel has an option to delete a group.

To delete a group:

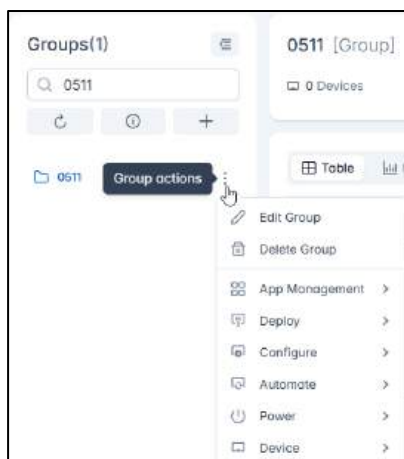
1. In the Radix dashboard, click on the **Devices** icon to open the Devices Table.
2. Click on the **Groups** icon to expand the Groups pane.



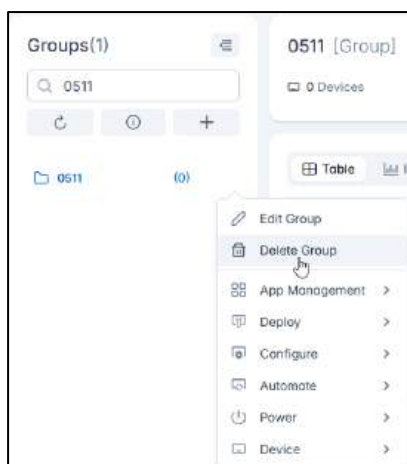
3. In the Search bar, enter the name of the group that you would like to delete.



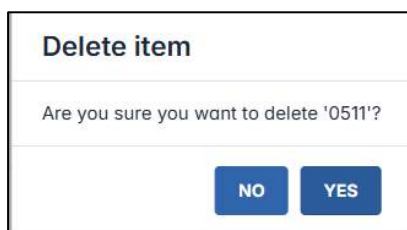
4. Click on the three-dot menu to open the Actions grid.



5. In the drop-down menu, click **Delete Group**.



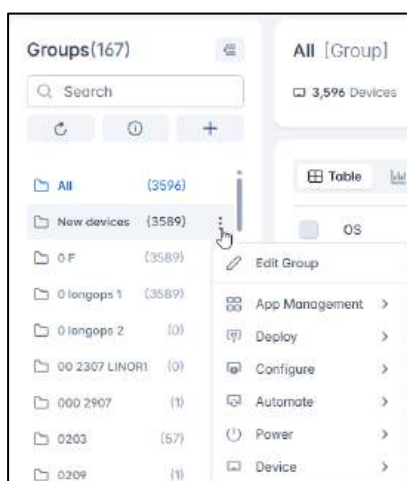
6. You will be prompted if you are certain that you want to delete the group. Click **Yes** to confirm.



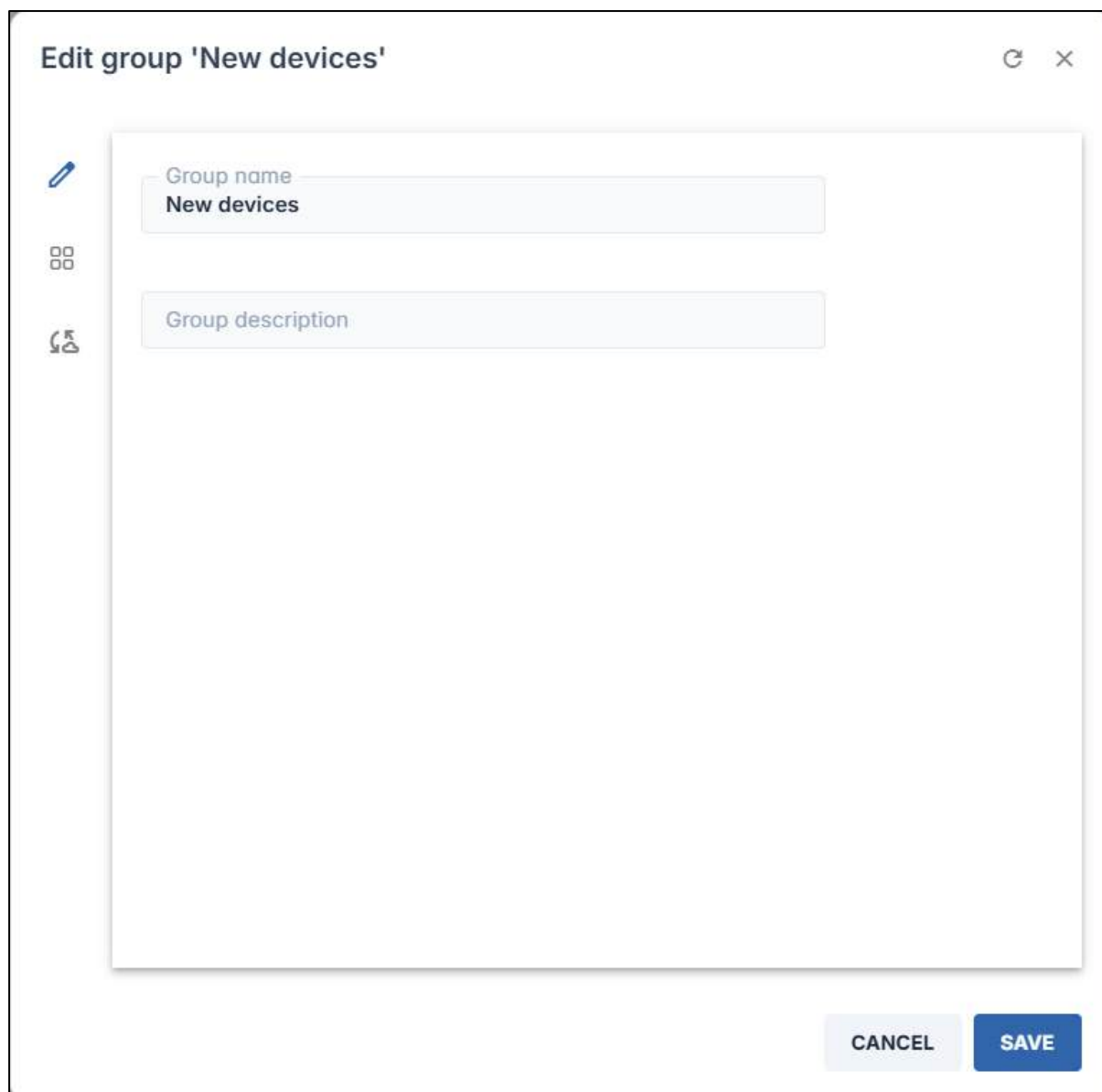
5.1.5 Managing the New Devices Group

For the group **New Devices**, the **Edit Group** command is somewhat different. This will allow you to install mandatory software packages onto any new devices as they are included in the Radix Device Management system.

1. In the **Groups** pane, find the group “**New Devices**”, and click on its three-dot menu.

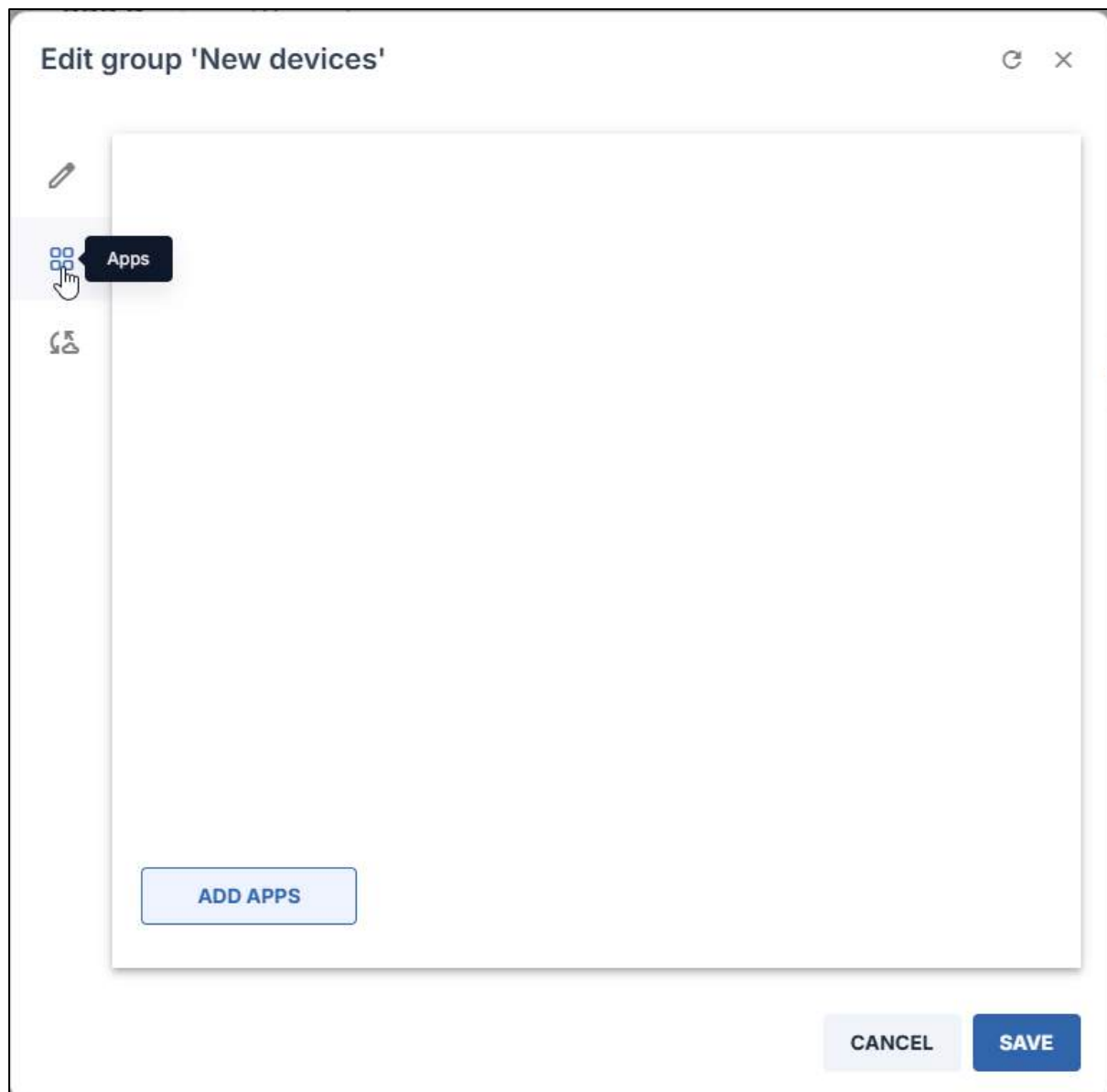


2. Click on the **Edit Group**. The **Edit group ‘New Devices’** window opens.

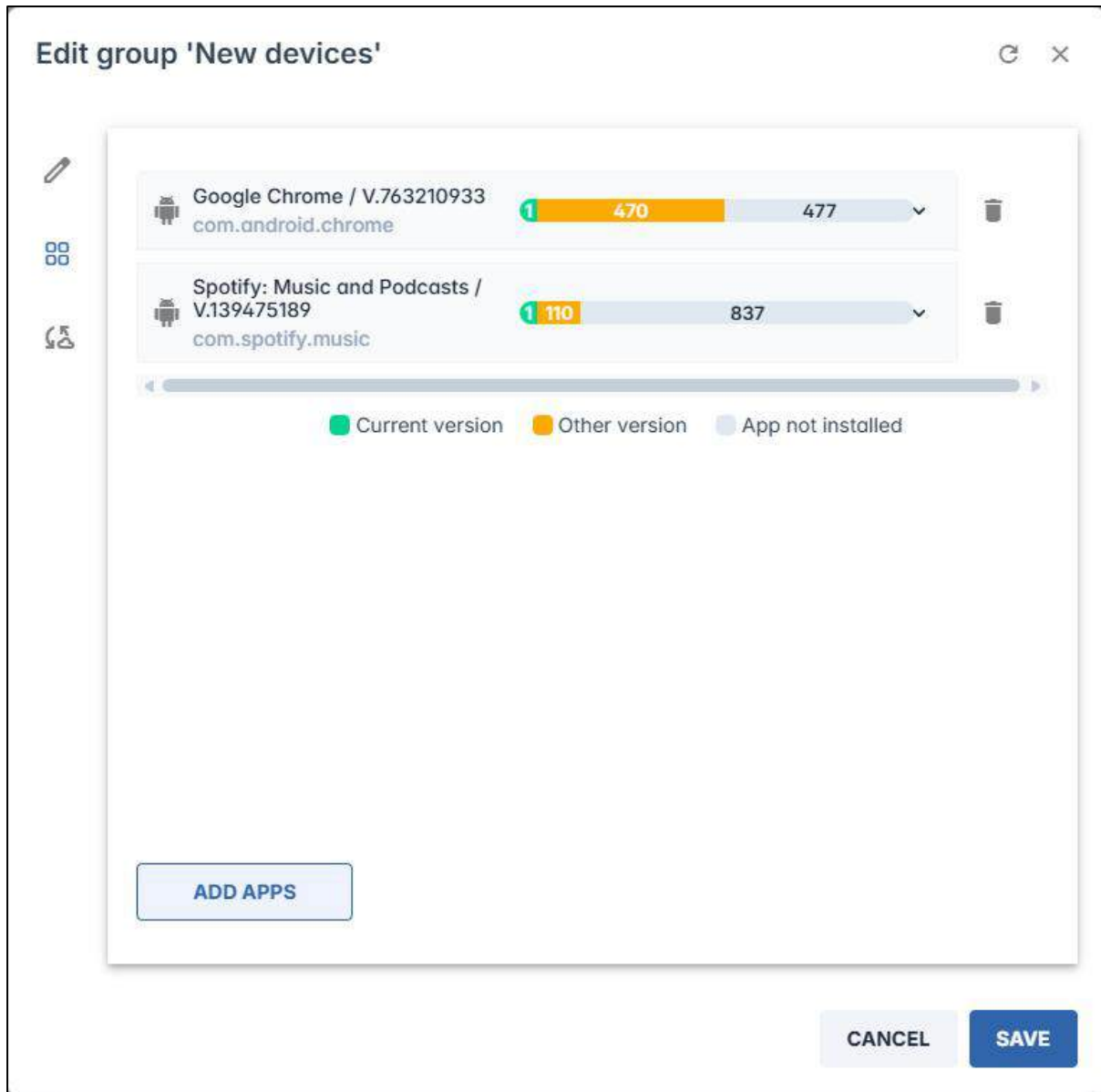


The screenshot shows a modal window titled "Edit group 'New devices'". On the left side of the modal, there is a vertical toolbar with three icons: a pencil (edit), a grid (list view), and a document with a plus sign (add). The main content area contains two text input fields. The first field is labeled "Group name" and contains the text "New devices". The second field is labeled "Group description" and is currently empty. At the bottom right of the modal, there are two buttons: a light blue "CANCEL" button and a dark blue "SAVE" button.

3. When you click on **Apps>Add Apps**, you will be able to add software packages to any new devices enrolled in the Radix Device Management Platform.



4. In the example below, we selected to install Google Chrome and Spotify on all new devices:



We see that from the total number of 948 devices, one has the current version of Spotify, while 110 have another version, and the remaining 837 devices do not have Spotify installed on them yet. (This could be because many of these devices are no longer active.)

5. Click on the row of a particular application. You will see a breakdown of which devices have the current version, a previous version, or do not have the application installed at present.

Edit group 'New devices'

Google Chrome / V.763210933
com.android.chrome

Spotify: Music and Podcasts / V.139475189
com.spotify.music

V.117967992 3 Devices

V.80485999 1 Devices

V.104074605 1 Devices

V.104599397 1 Devices

V.126882575 1 Devices

V.105910845 1 Devices

V.112987095 1 Devices

V.130551968 3 Devices

Current version Other version App not installed

ADD APPS

CANCEL SAVE

- Clicking on the **Show Devices** filter icon next to a particular device in the list will allow you to do a filtered search:

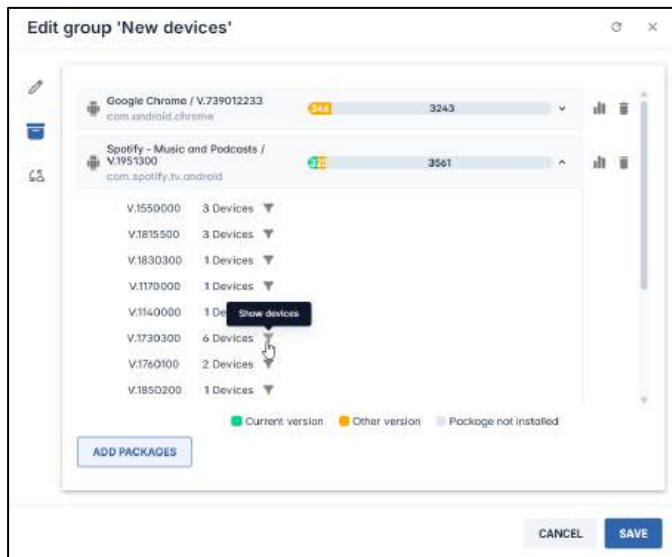


Figure 5-11: Viewing devices with/without the app installed

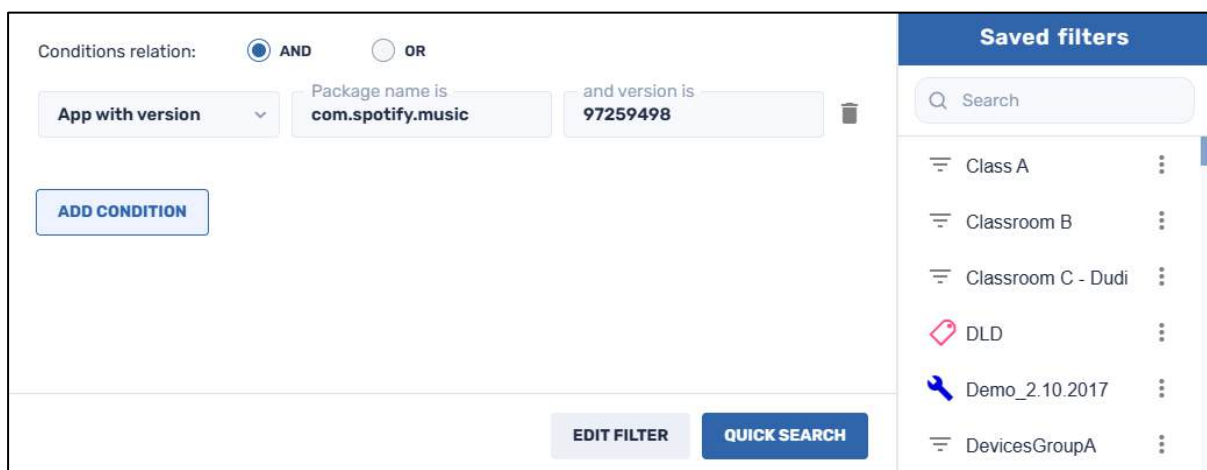
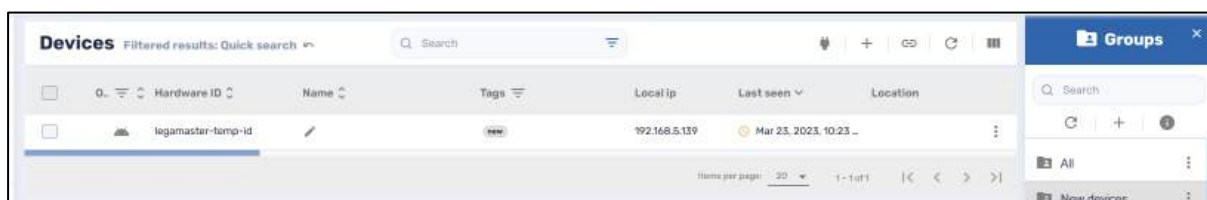
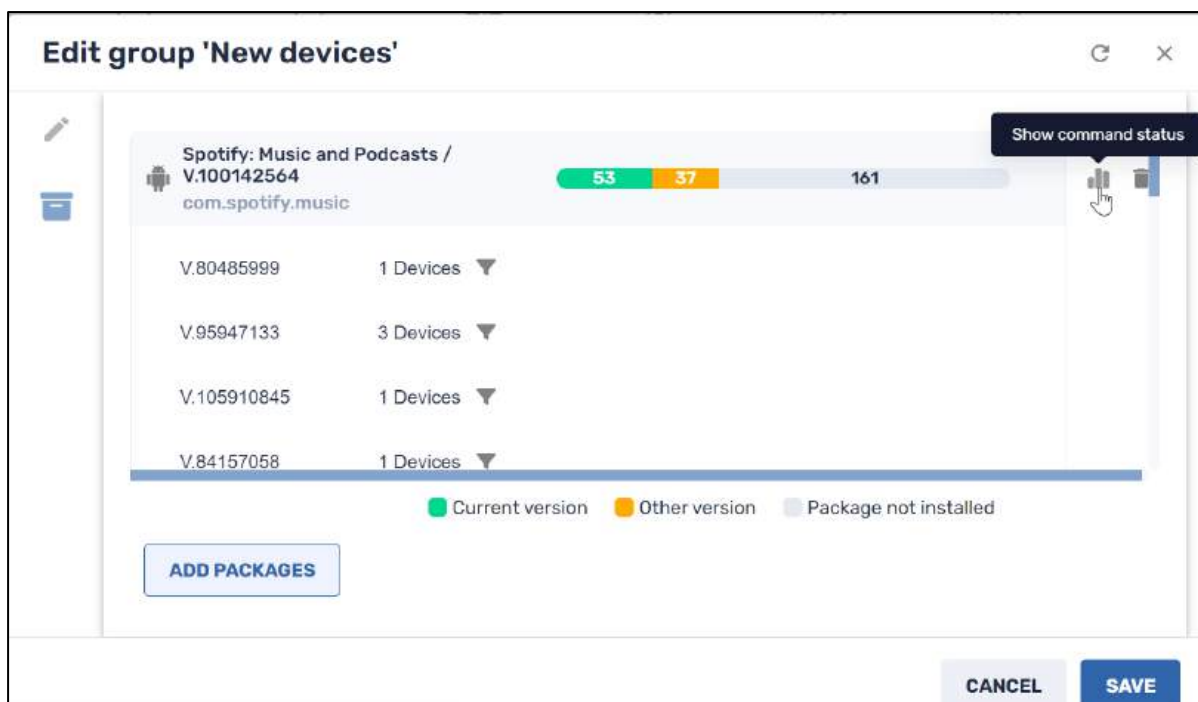


Figure 5-12: Filtering devices by version of app installed

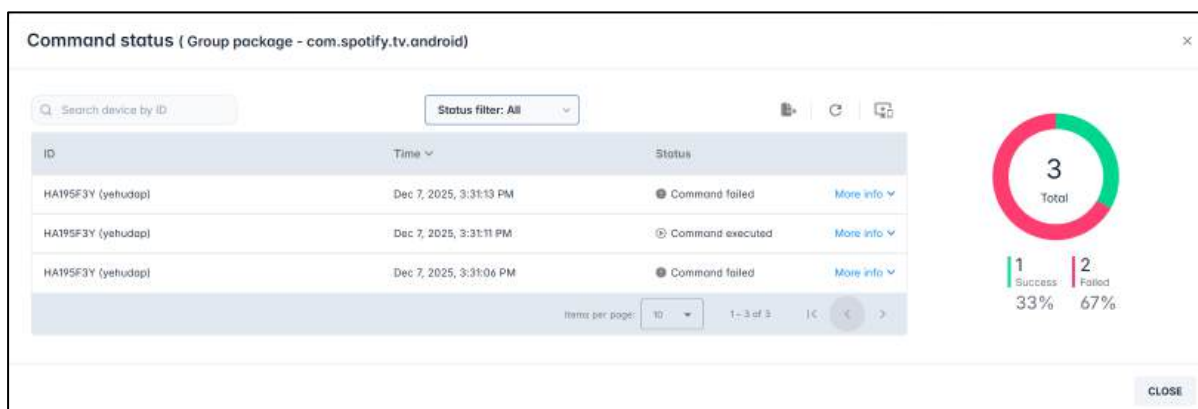
- Click on **Quick Search**. You will see the details of the specific devices that have or do not have the most recent installation of the application:



- Another way to view the breakdown of devices that have the app installed is by clicking on the **Show command status** icon  in the **Edit group** window:



It will provide you with a list of all the devices, whether the app was installed on the device successfully, and any reason the installation failed:



5.1.6 Summary of Remaining Group Commands

Here is a summary of the remaining commands in the drop-down list that appears when you click on the Bulk Actions button:

5.1.6.1 App Management Menu

App Management Menu		
Item	Description	Reference
Install App	Install apps on remote devices	Section 6.1.13, Install App/Install Package
AFW Install/Uninstall	Selects apps and install/uninstall them on remote devices enrolled in Android for Work	Section 6.1.2, Android for Work (AFW) install/uninstall

Uninstall App	Uninstall apps on remote devices	6.1.34, Uninstall Packages
Clear App Data	Clear the user's history on the remote devices	Section 6.1.5, Clear Apps Data
Clear App Cache	Clears the data cached by the specific apps installed on the device	Section 6.1.4, Clear Apps Cache
Enable App	Restores icon of disabled app on a remote device's display	Section 6.1.10, Disable/Enable apps
Disable App	Removes the icon of an app from a remote device's display	Section 6.1.10, Disable/Enable apps

5.1.6.2 Deploy Menu

Deploy Menu		
Item	Description	Reference
Direct Message	Sends a simple text message to remote devices	Section 6.1.9, Direct Message
Messaging	Sends a message with audio/video content to remote devices	Section 6.1.1, Advanced Messaging
Commands & Scripts	Executes scripts on remote devices	Section 6.1.23, Remote Execute
Files	Sends files to remote devices	Section 6.1.28, Send Files
OTA	Performs over-the-air updates on remote devices	Section 6.1.18, OTA.
OTA Update Engine	Performs over-the-air updates on newer remote devices	Section 6.1.19, OTA Update Engine
Firmware Update	Performs an update on remote devices' firmware	Section 6.1.12, Firmware Update
Windows Update	Performs a update of software and/or drivers on remote Windows devices	Section 6.1.38, Windows Update

5.1.6.3 Configure Menu

Configure Menu		
Item	Description	Reference
Device Settings	Modifies settings on remote devices	Section 6.1.8, Device Settings

Kiosk Mode	Allows you to use a device as a display in a kiosk	Section 6.1.14, Kiosk
Block Lists	Allows you to block access on a remote device to certain apps and websites	Section 6.1.21, Policies (Block Lists)
Views	Allows you to create a specialized Kiosk option, where a remote device displays a single URL	Section 6.1.35, Views
Screen Settings	Allows you to adjust the brightness and volume on flat panel devices	Section 6.1.27, Screen Settings
Remove Google Account	Allows removing all Google accounts from a device or retaining one.	Section 6.1.24, Remove Google Accounts from Device
Manage Device Users	Allows you to users on a remote device	Section 6.1.15, Manage users

5.1.6.4 Automate Menu

Automate Menu		
Item	Description	Reference
Workflows	Allows you to combine a series of commands to be executed in sequence	Section 6.1.39, Workflow
Schedules & Triggers	Allows you to execute commands in response to a time schedule or external trigger	Section 6.1.26, Scheduler & Triggers Command

5.1.6.5 Power Menu

Power Menu		
Item	Description	Reference
Restart	Restarts the remote device	Section 6.1.25, Restart
Shut Down	Shuts down the remote device	Section 6.1.29, Shutdown
Wake On LAN	Wakes up a device using Wake-on-LAN	Section 6.1.36, Wake on LAN
Standby	Puts a device in standby mode	Section 6.1.31, Standby
Wake up	Wakes up a device from standby mode	Section 6.1.37, Wake Up

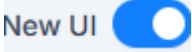
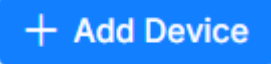
5.1.6.6 Device Menu

Device Menu		
Item	Description	Reference

Set Device Tags	Allows you to add or remove tags from devices	Section 6.1.32, Tags
Change Agent Password	Allows you to change the device's password to make changes on the VISO agent app	Section 6.1.3, Change Agent Password
Metrics	Displays statistics and graphs of app usage on remote devices	Section 5.7.2, Device Usage Insights Display, and Section 6.1.17, Metrics
Smart Recovery	Allows you to run the Smart Recovery program on Windows devices	Section 6.1.30, Smart Recovery
Collect System Logs	Allows you to create a log file of activities performed on a remote device	Section 6.1.6, Collect System Logs
Export Device Data to CSV	Downloads an Excel spreadsheet of device data	Section 6.1.11, Export Device Data to CSV

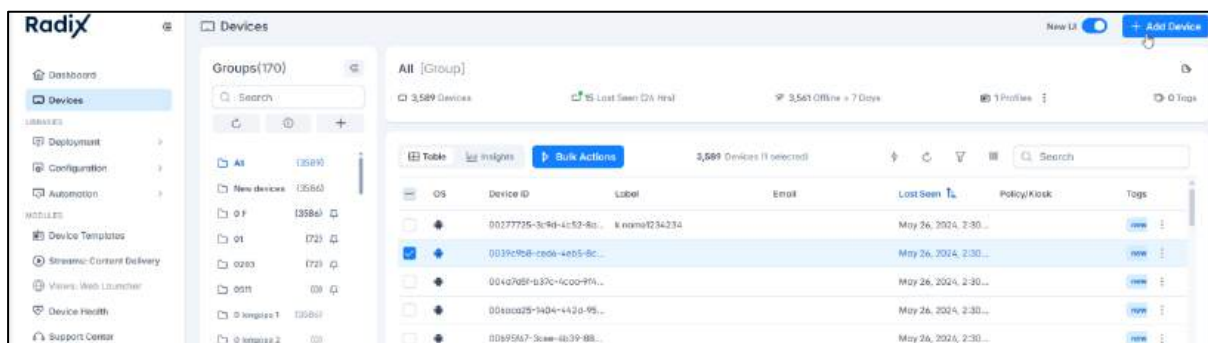
5.2 Top Action Bar

The top action bar of the Devices Table has two commands:

Icon	Description
	Ad-hoc session: This allows you to initiate a session with a device that has the VISO agent app installed, but is not enrolled in your Radix account
	This allows you to toggle between the previous UI and the new UI of the Radix Device Management Platform
	This opens an interface to enroll new devices in the Radix Device Management Platform

5.2.1 Enrolling a New Device

Clicking on the **Add Device** button  will open a dialog box where you can enroll additional devices, according to their operating system: Android, Windows, or ChromeOS.



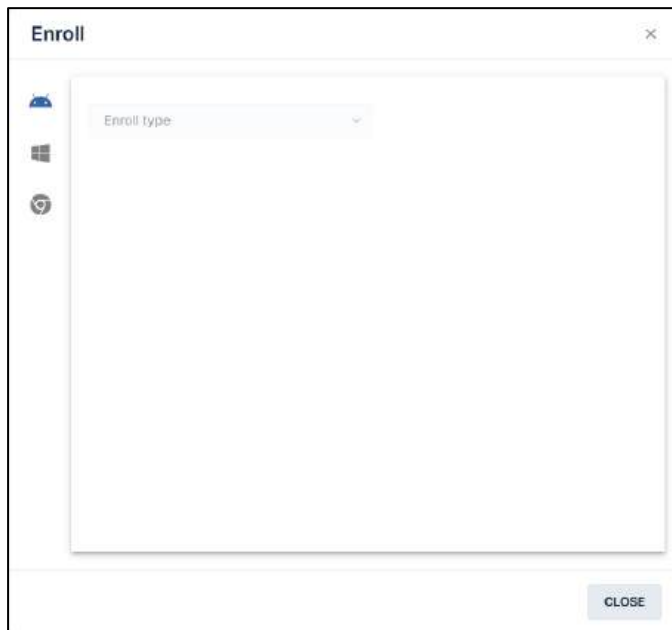


Figure 5-13: Dialog box to enroll Android, Windows, or ChromeOS devices

We will go through the options in turn.

5.2.1.1 Enrolling Android Devices

There are three options that you are offered in the Radix Device Management Platform to enroll an Android device:

- By using a QR code
- Downloading the Android Agent
- Via Google Enterprise Mobility Management

5.2.1.1.1 Enroll using a QR code (AFW)

When you click on this option, you will receive a QR code that you scan with your Android device. That will enroll the Android device.

Note: To enroll your Android device by this method, you must perform a factory reset on the device.

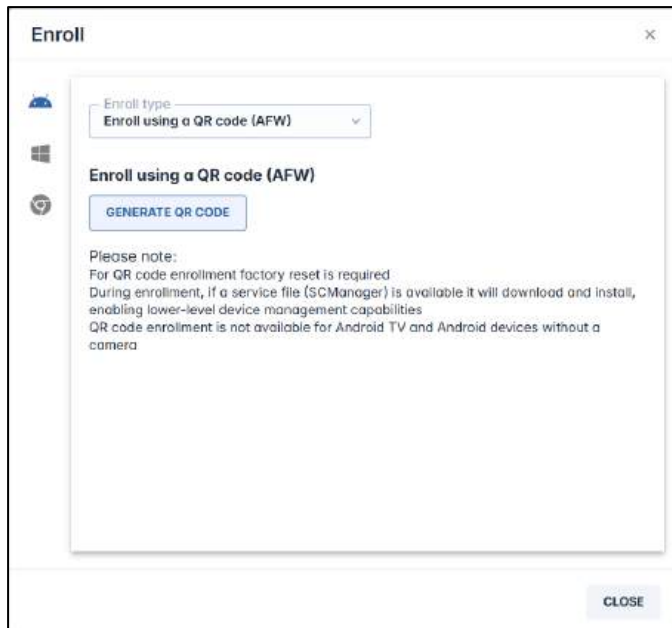
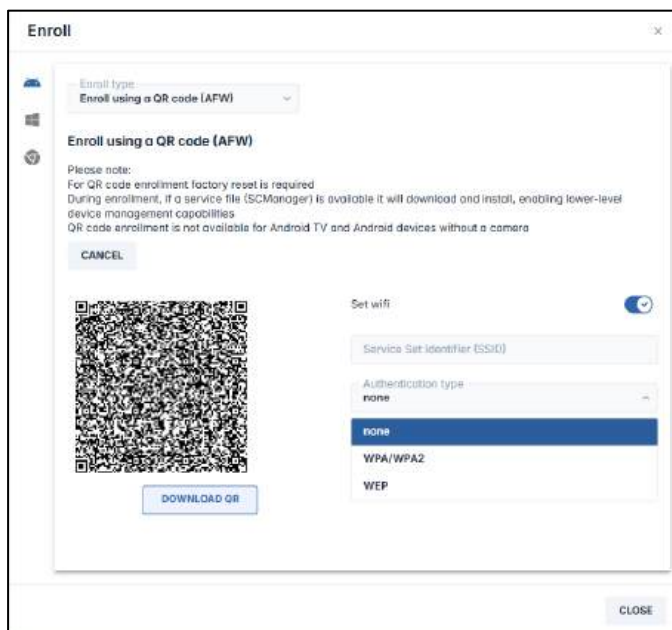


Figure 5-14: Steps for enrolling an Android device via a QR code

1. Select **Enroll using a QR code (AFW)**.
2. Click on **Generate QR Code**. It will create a QR code in the window.



3. Scan the QR code with your Android device or download it to your computer by clicking the **Download QR** button.
4. Click on the **Set Wi-Fi** button, enter the SSID and the authentication type for you Wi-Fi system.

5.2.1.1.2 Download and Install the Android Agent Option

When you click on this option, you receive three methods of downloading the Radix Android Agent:

- [Download the APK file](#) directly to your computer, or

- Go to the Google Play Store and [download the APK](#) from there, or
- Scan the QR code displayed on your computer with the Android device that you want to enroll.

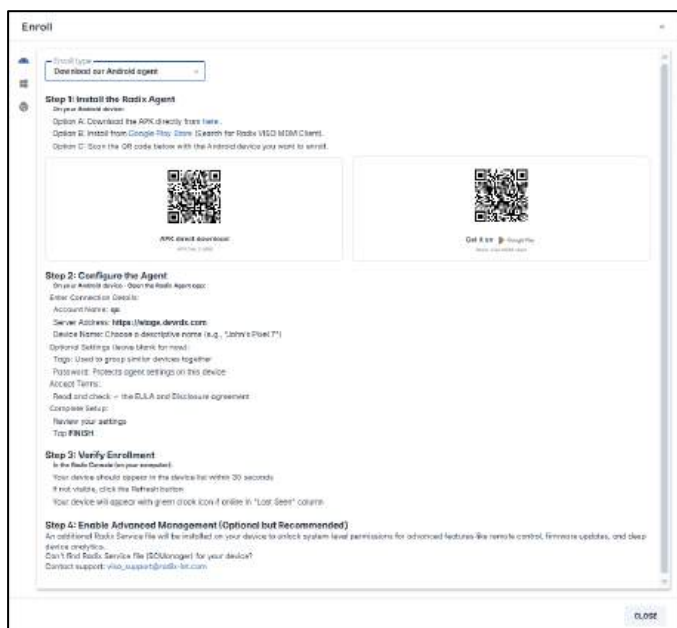


Figure 5-15: Steps for enrolling an Android device via an APK file

After performing the download, perform the steps as displayed in the window to supply the account name, server address, and device name.

You should also install the Service file (SCManager) specific to your Android device.

Note: The SCManager file is not required for Samsung and Sony mobile devices. Instead of an SCManager file, Samsung devices have Samsung Knox. This is hardware built into Samsung devices to provide enhanced device security.

5.2.1.1.3 Google EMM (Android for Work)

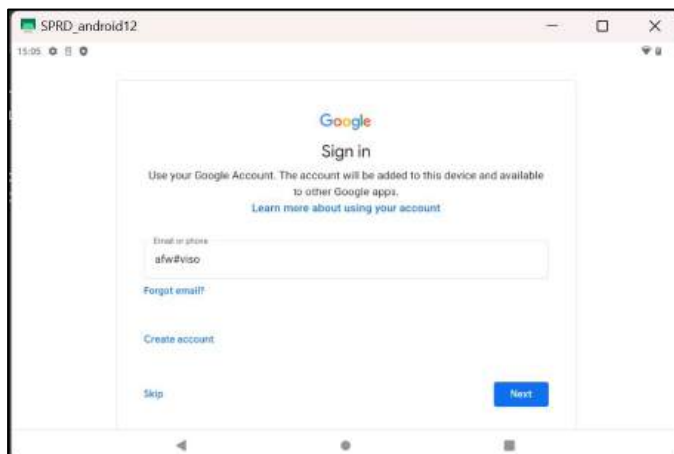
When you click on this option, you will be provided with two links with the following information to enroll an Android device with EMM (=Enterprise Mobility Management) software:



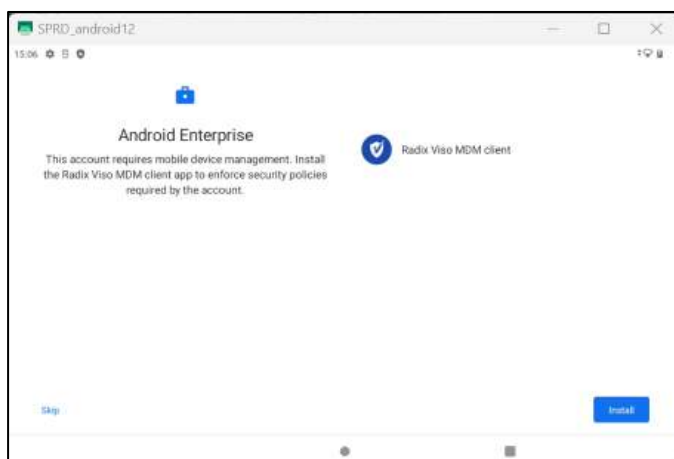
Figure 5-16: Steps to enroll an Android device via the EMM Android for Work software

To enroll a remote device using Android for Work:

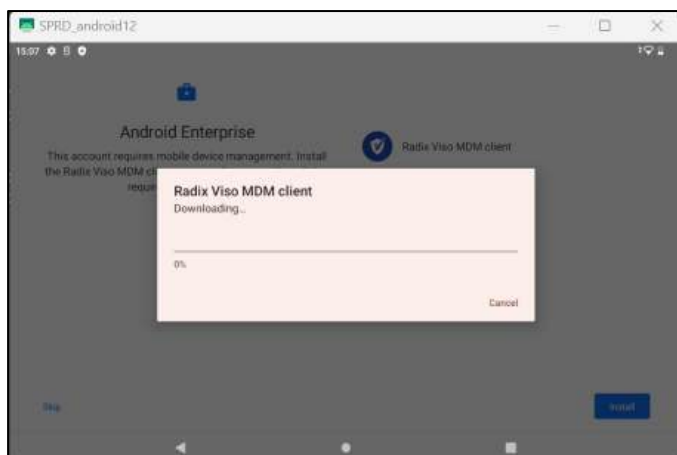
1. After performing a factory reset on a remote device, during registration, where it asks for the Google account, enter **afw#viso**.



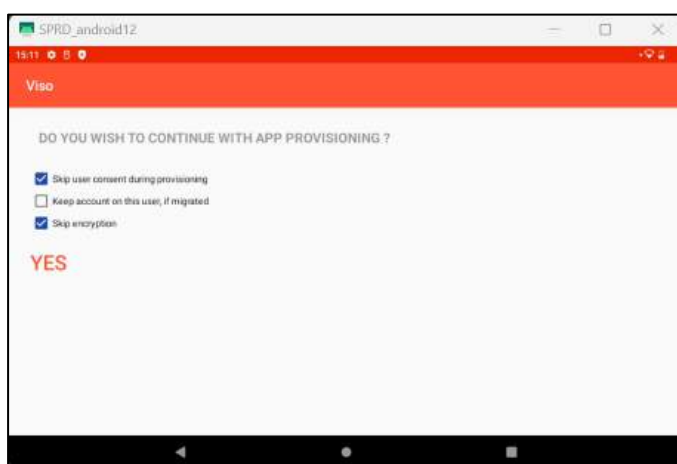
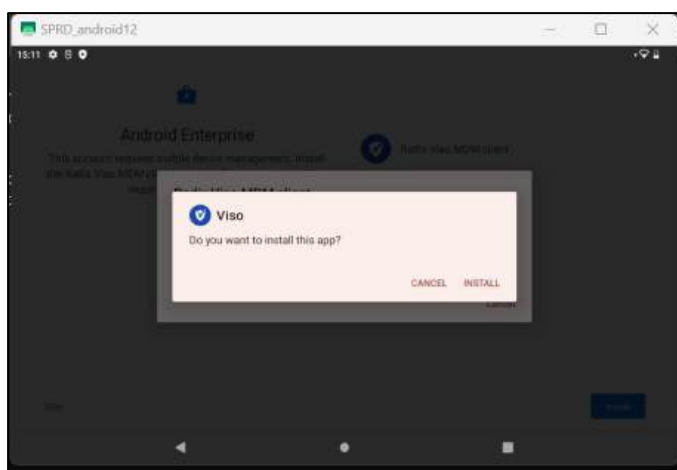
2. Click **Next**. You will receive the following screen:



3. Click **Install**. The device will download the Radix Viso MDM client app:



4. When the download is complete, you will be prompted if you wish to install the VISO app.



5.2.1.2 Enrolling Windows Devices

To enroll a Windows device, you simply have to download and run the executable file provided by the link in the dialog box.

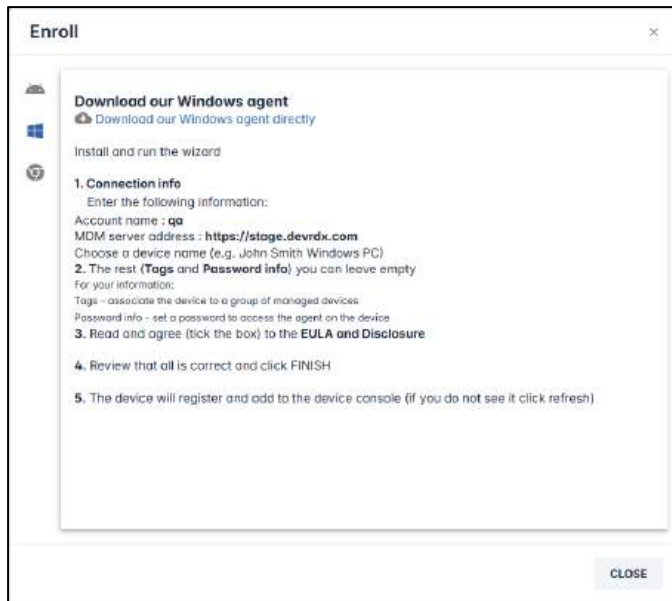


Figure 5-17: Steps to enroll a Windows device

5.2.1.3 Enrolling Chrome Devices

If you select the option to enroll a Chrome device, the following window opens:

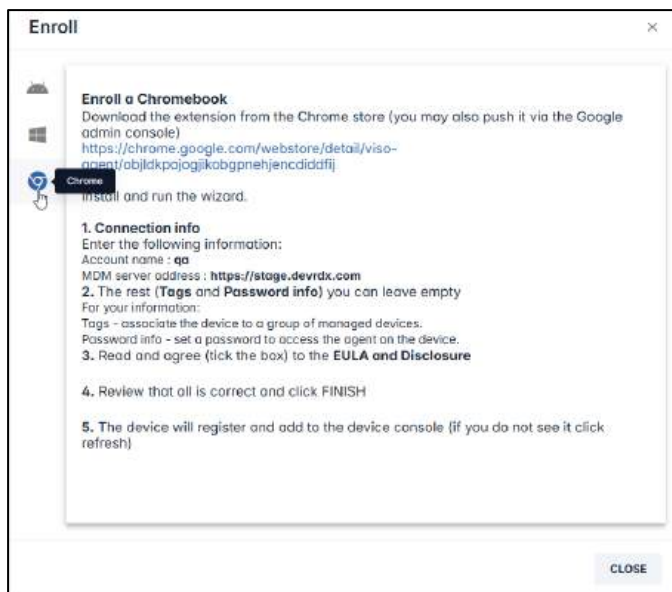
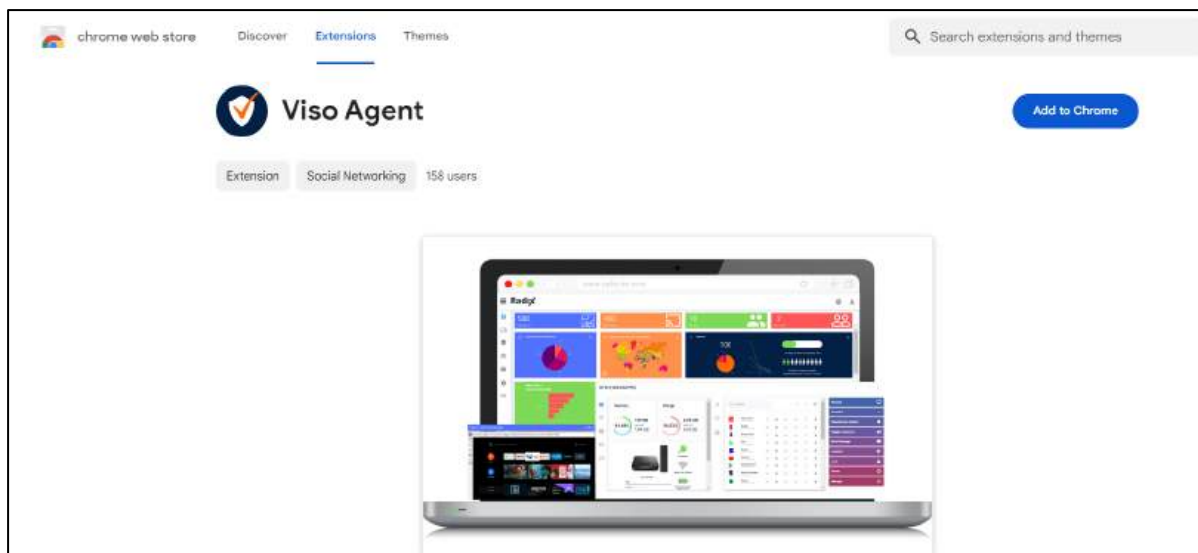
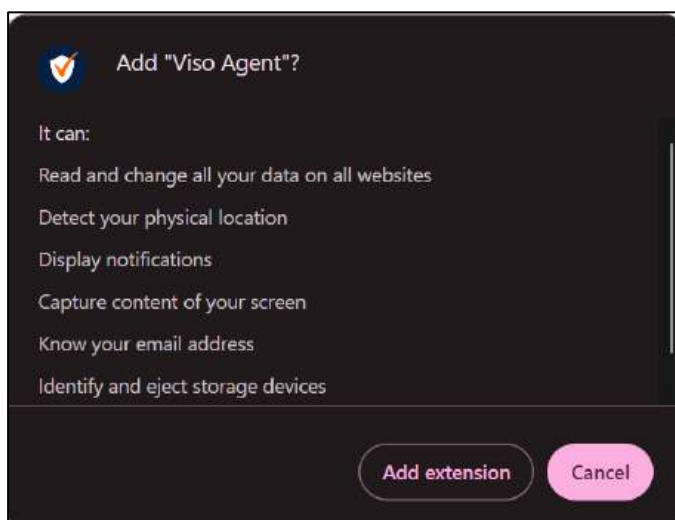


Figure 5-18: Steps to install the Viso Chrome browser extension

1. Click on the link to open a browser tab to add the Viso Agent as a Chrome extension:



2. Click **Add to Chrome**. You will be prompted to add the Viso Agent to your Chrome extensions.



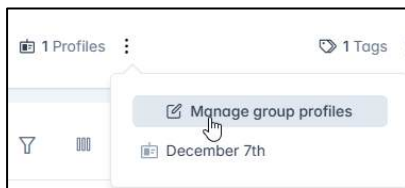
3. Click **Add extension**. You will receive confirmation that the Viso extension has been added to your Chrome browser.
4. In the Viso Agent app, supply the connection information as detailed in the **Enroll a Chromebook** window.

5.3 Group Status Bar



The Group Status bar displays the following information:

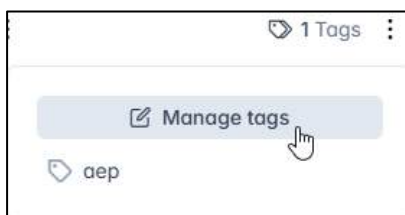
Icon	Description
6 Devices	The total number of devices in the group
2 Last Seen (24 Hrs)	How many have been active in the last 24 hours
3 Offline > 7 Days	How many have been offline for more than 7 days
1 Profiles	How many templates are associated with the devices in the group
1 Tags	How many tags are associated with the group
	Export to CSV



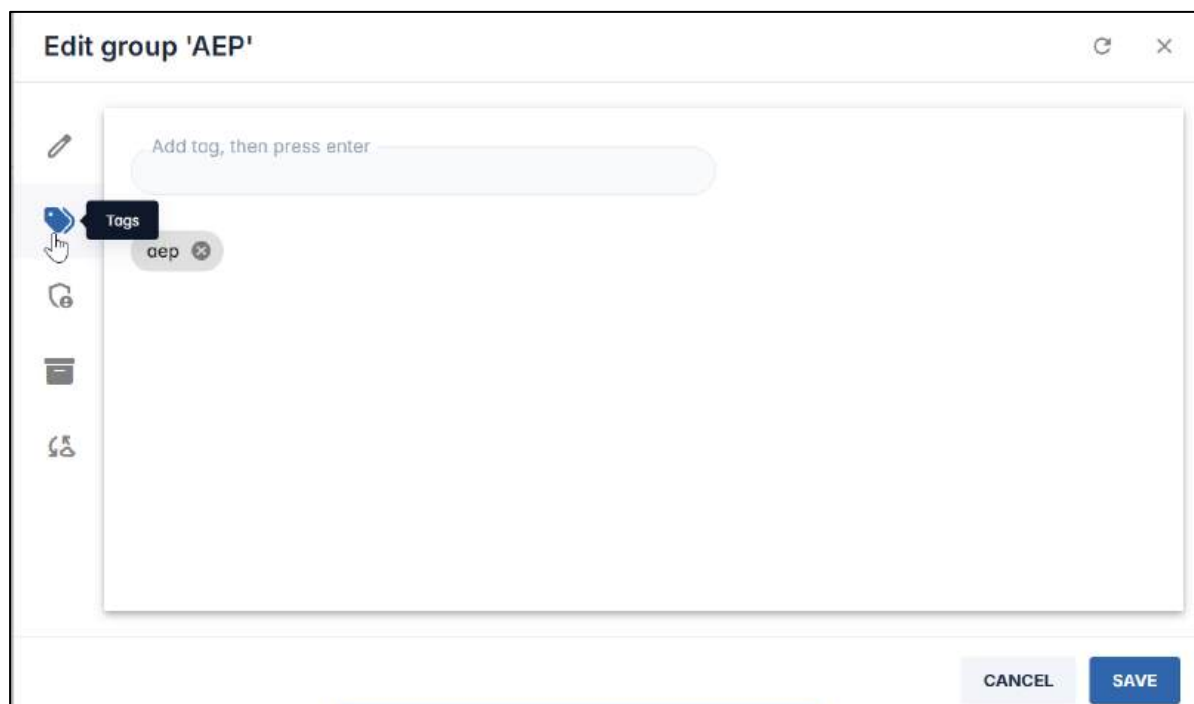
By clicking on the three-dot menu, you can see and modify the details of the template(s) associated with the group:



- How many tags are associated with the group.



By clicking on the **three-dot menu>Manage tags**, you can view and modify the tags associated with the group:



- By clicking on the **Export to CSV** icon , you can download an Excel spreadsheet which displays specific columns of data regarding the devices in the group:



5.4 Bulk Actions Bar

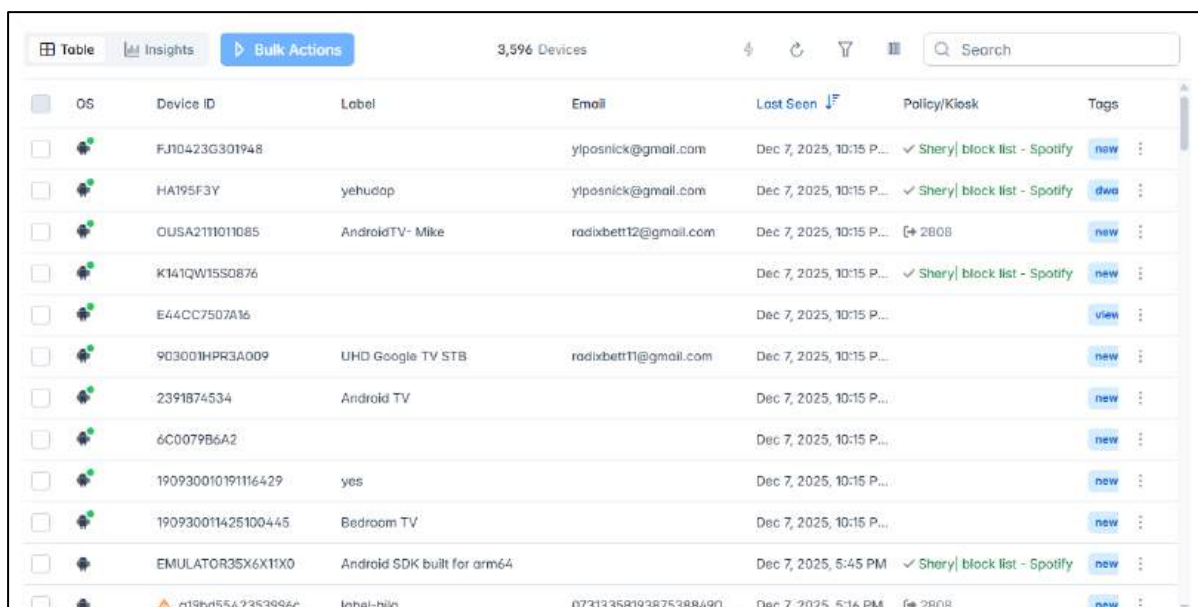
The Bulk Actions bar includes icons that allow you to perform actions on groups of devices, or on selected devices.



Icon	Description
 Table	Clicking on the Table button displays the Devices Table in table form
 Insights	Clicking on the Insights button displays device information such as app usage and firmware versions for all devices, or for a group of devices
 Bulk Actions	Clicking on this button displays a drop-down menu of commands that can be applied in bulk, to a number of devices at once
	Who is online?: This displays the devices that are presently online
	Refresh: Resets the display of devices according to the current filters
	Filter devices: Allows you to apply a filter option to narrow down the devices displayed
	Configure columns: Allows you to select which data columns to display in the Devices Table
 Search	Search: Allows you to search for devices by Device ID, Label, or user name.

5.5 Main Devices Table

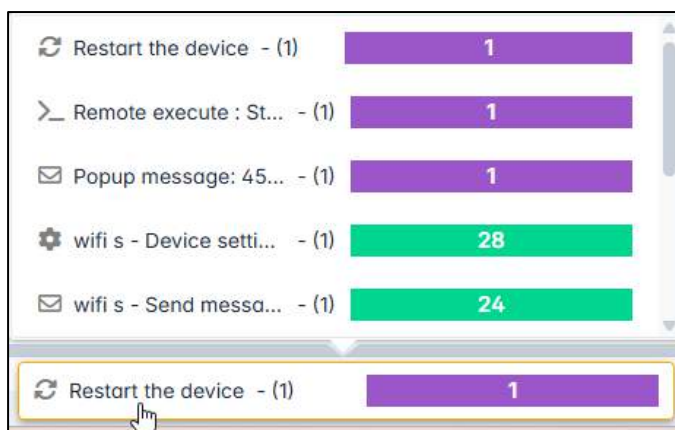
The Main Devices Table displays the enrolled devices. By default, it will display all enrolled devices. If you select a group in the Group Status Bar, it will only display the devices in that group.



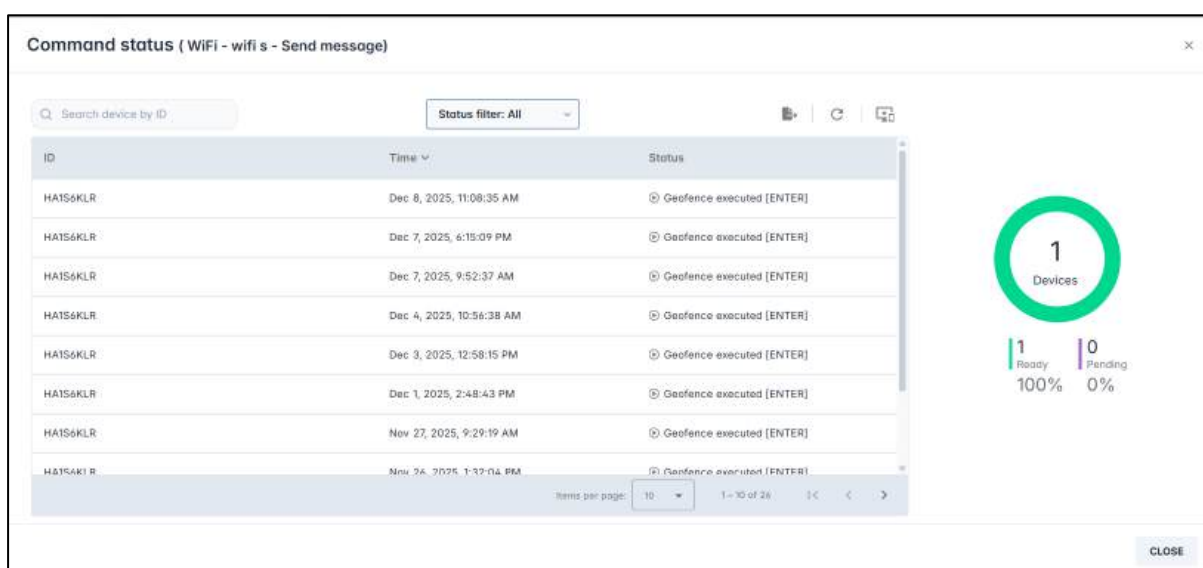
			3,596 Devices					 Search
☐	OS	Device ID	Label	Email	Last Seen	Policy/Kiosk	Tags	
☐		FJ10423G301948		ylposnick@gmail.com	Dec 7, 2025, 10:15 P...	✓ Sheryl block list - Spotify	new	⋮
☐		HA195F3Y	yehudap	ylposnick@gmail.com	Dec 7, 2025, 10:15 P...	✓ Sheryl block list - Spotify	dwa	⋮
☐		OUSA211011085	AndroidTV - Mike	radixbett12@gmail.com	Dec 7, 2025, 10:15 P...	[+ 2808	new	⋮
☐		K141QW15S0876			Dec 7, 2025, 10:15 P...	✓ Sheryl block list - Spotify	new	⋮
☐		E44CC7507A16			Dec 7, 2025, 10:15 P...		view	⋮
☐		903001HPR3A009	UHD Google TV STB	radixbett11@gmail.com	Dec 7, 2025, 10:15 P...		new	⋮
☐		2391874534	Android TV		Dec 7, 2025, 10:15 P...		new	⋮
☐		6C0079B6A2			Dec 7, 2025, 10:15 P...		new	⋮
☐		19093001019116429	yes		Dec 7, 2025, 10:15 P...		new	⋮
☐		190930011425100445	Bedroom TV		Dec 7, 2025, 10:15 P...		new	⋮
☐		EMULATOR35X6X11X0	Android SDK built for arm64		Dec 7, 2025, 5:45 PM	✓ Sheryl block list - Spotify	new	⋮
☐		a19bd5542353996c	label-hilo	07313358193875388490...	Dec 7, 2025, 5:16 PM	[+ 2808	new	⋮

5.6 Recent Commands Status bar

At the bottom of the Devices Table, you will see the Recent Commands status bar. Clicking on it will give the most recent commands sent by the users of the account:



Clicking on an individual command will allow you to see details of the execution of the command:



5.7 Main Devices Table in Detail

5.7.1 Devices Table Tabular Display

The Table icon  displays the information in the Devices Table in table form.

Clicking on the row of a particular device will open that device's Device Dashboard:

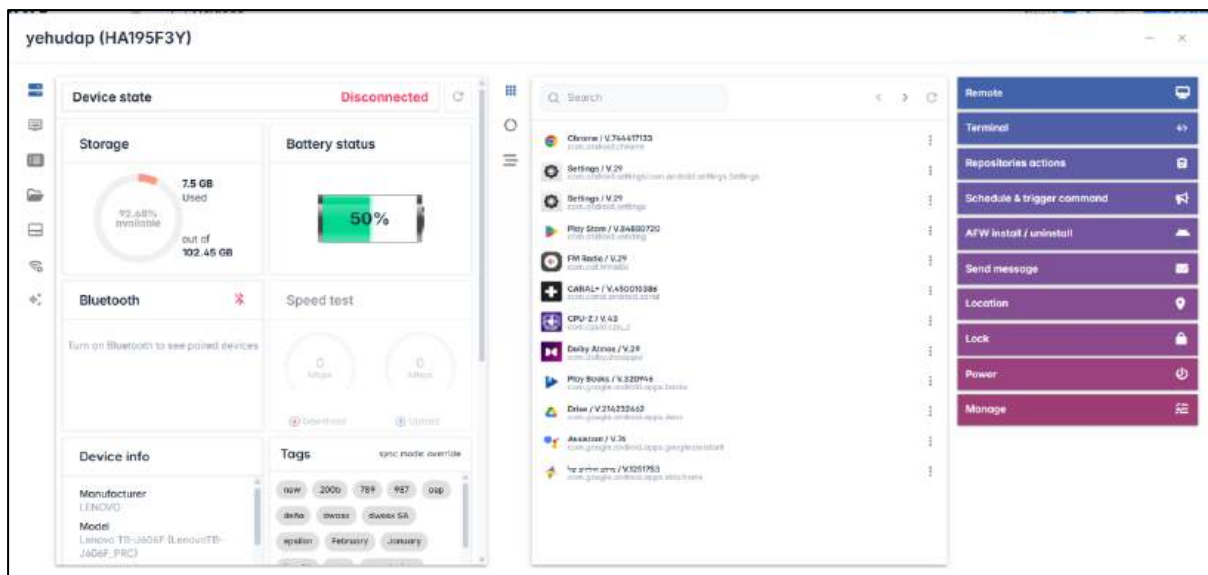


Figure 5-19: Device Dashboard layout for an Android device

- Clicking on the device's three-dot menu ("Device Actions") on the far right will open a drop-down menu of commands:

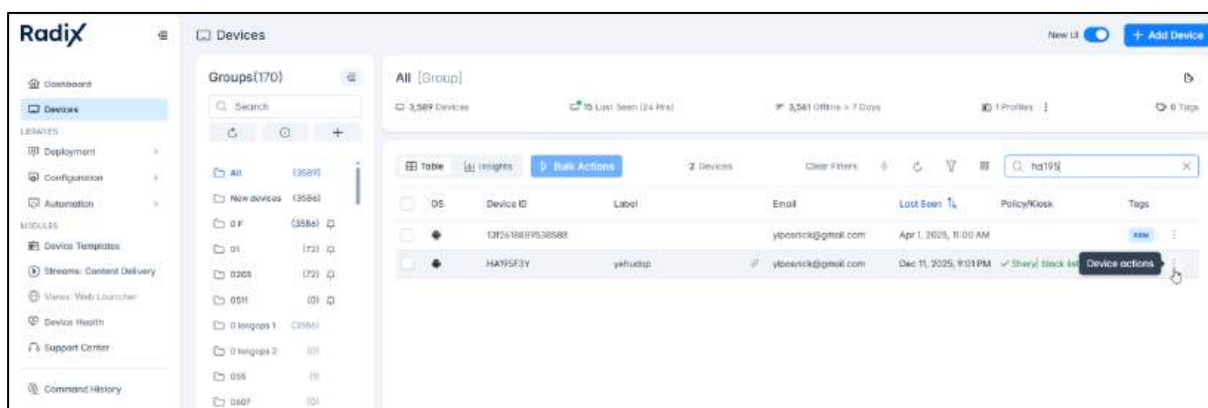


Figure 5-20: Device's Three-Dot ("Kebab") Menu

A drop-down menu of commands will open up with all of the options for working with your device.

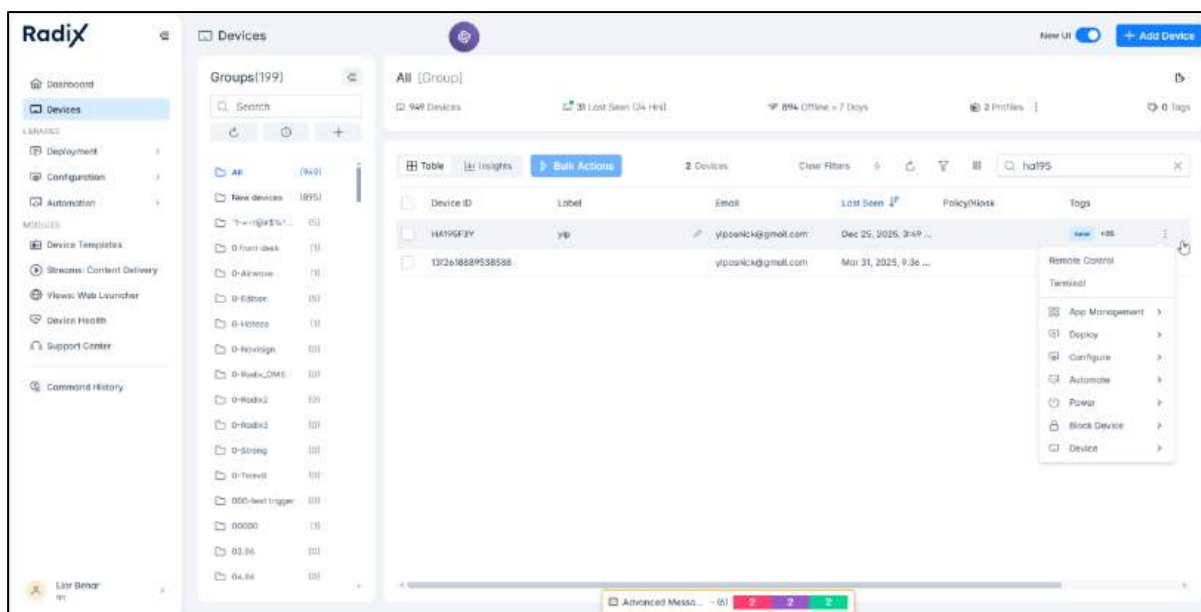
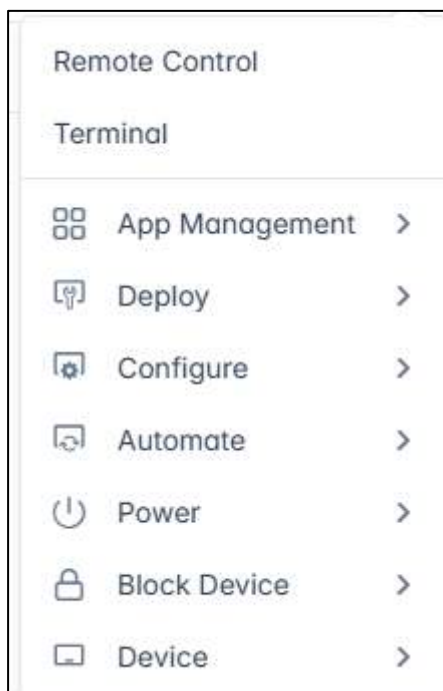


Figure 5-21: Display of Devices Menu Options



Here is a summary of the commands in the drop-down list that appears when you click on a device's three-dots button:

Item	Description	Reference
Remote Control	Allows you to view and operate a remote device	Section 6.1.22, Remote Control
Terminal	Opens a live terminal with an ADB shell connection	Section 6.1.33, Terminal

5.7.1.1 App Management Menu

App Management Menu		
Item	Description	Reference
Install App	Install apps on remote devices	Section 6.1.13, Install App/Install Package
AFW Install/Uninstall	Selects apps and install/uninstall them on remote devices enrolled in Android for Work	Section 6.1.2, Android for Work (AFW) install/uninstall
Uninstall App	Uninstall apps on remote devices	6.1.34, Uninstall Packages
Clear App Data	Clear the user's history on the remote devices	Section 6.1.5, Clear Apps Data
Clear App Cache	Clears the data cached by the specific apps installed on the device	Section 6.1.4, Clear Apps Cache
Enable App	Restores icon of disabled app on a remote device's display	Section 6.1.10, Disable/Enable apps
Disable App	Removes the icon of an app from a remote device's display	Section 6.1.10, Disable/Enable apps

5.7.1.2 Deploy Menu

Deploy Menu		
Item	Description	Reference
Direct Message	Sends a simple text message to remote devices	Section 6.1.9, Direct Message
Messaging	Sends a message with audio/video content to remote devices	Section 6.1.1, Advanced Messaging
Commands & Scripts	Executes scripts on remote devices	Section 6.1.23, Remote Execute
Files	Sends files to remote devices	Section 6.1.28, Send Files
OTA	Performs over-the-air updates on remote devices	Section 6.1.18, OTA
OTA Update Engine	Performs over-the-air updates on newer remote devices	Section 6.1.19, OTA Update Engine
Firmware Update	Performs an update on remote devices' firmware	Section 6.1.12, Firmware Update

5.7.1.3 Configure Menu

Configure Menu		
Item	Description	Reference
Device Settings	Modifies settings on remote devices	Section 6.1.8, Device Settings
Kiosk Mode	Allows you to use a device as a display in a kiosk	Section 6.1.14, Kiosk
Block List	Allows you to block access on a remote device to certain apps and websites	Section 6.1.21, Policies (Block Lists)
Views	Allows you to create a specialized Kiosk option, where a remote device displays a single URL	Section 6.1.35, Views
Screen Settings	Allows you to adjust the brightness and volume on flat panel devices	Section 6.1.27, Screen Settings
Remove Google Account	Allows removing all Google accounts from a device or retaining one.	Section 6.1.24, Remove Google Accounts from Device
Manage Device Users	Allows you to users on a remote device	Section 6.1.15, Manage users

5.7.1.4 Automate Menu

Automate Menu		
Item	Description	Reference
Workflows	Allows you to combine a series of commands to be executed in sequence	Section 6.1.39, Workflow
Schedules & Triggers	Allows you to execute commands in response to a time schedule or external trigger	Section 6.1.26, Scheduler & Triggers Command

5.7.1.5 Power Menu

Power Menu		
Item	Description	Reference
Restart	Restarts the remote device	Section 6.1.25, Restart
Shut Down	Shuts down the remote device	Section 6.1.29, Shutdown
Wake on LAN	Wakes up a device using Wake-on-LAN	Section 6.1.36, Wake on LAN
Standby	Puts a display in standby mode	Section 6.1.31, Standby

Wake Up	Awakens a display that is in standby mode	Section 6.1.37, Wake Up
---------	---	-------------------------

5.7.1.6 Block Device Menu

Block Device Menu		
Item	Description	Reference
Lock Device	Locks a remote device	Section 5.8.3.8.1, Locking a Device
Unlock Device	Undoes the Lock Device command	Section 5.8.3.8.2, Unlock Device
Get Lock Password	Provides the password to unlock a locked device	Section 5.8.3.8.2, Get Device Password
Play Siren	Sounds an alarm on a device	Section 6.1.20, Play Siren

5.7.1.7 Device Menu

Device Menu		
Item	Description	Reference
Set Device Tags	Allows you to add or remove tags from devices	Section 6.1.32, Tags
Change Device Name (Android only)	Allows you to change the device name as it appears in the Devices Table	Section 5.8.3.10.2, Rename/Change Device Name
Change Agent Password	Allows you to change the device's password to make changes on the VISO agent app	Section 6.1.3, Change Agent Password
Metrics	Displays statistics and graphs of app usage on remote devices	Section 5.7.2, Device Usage Insights Display, and Section 6.1.17, Metrics
Remove Device	Removes device from the Devices Table	Section 5.8.3.10.1, Remove Device
Factory Reset (Android only)	Performs a factory reset on an Android device	Section 5.8.3.8.4, Wipe
Smart Recovery (Windows only)	Allows you to run the Smart Recovery program on Windows devices	Section 6.1.30, Smart Recovery
Reset Authentication Token	Resets a device authentication token, to restore device management capabilities	Section 5.8.3.10.5, Reset Authentication Token

Collect System Logs	Allows you to create a log file of activities performed on a remote device	Section 6.1.6, Collect System Logs
Export Device Data to CSV	Downloads an Excel spreadsheet of device data	Section 6.1.11, Export Device Data to CSV

- [Remote Control](#)
- [Terminal](#)
- App Management
 - [Install App](#)
 - [AFW Install/Uninstall](#)
 - [Uninstall App](#)
 - [Clear App Data](#)
 - [Clear App Cache](#)
 - [Enable App](#)
 - [Disable App](#)
- Deploy
 - [Direct Message](#)
 - [Messaging](#)
 - [Commands & Scripts](#)
 - [Files](#)
 - [OTA](#)
 - [OTA Update Engine](#)
 - [Firmware update](#)
- Configure
 - [Device Settings](#)
 - [Kiosk Mode](#)
 - [Block Lists](#)
 - [Views](#)
 - [Screen Settings](#)
 - [Remove Google Accounts](#)
 - [Manage Device Users](#)
- Automate
 - [Workflows](#)
 - [Schedules & Triggers](#)
- Power
 - [Restart](#)
 - [Shut Down](#)
 - [Wake on LAN](#)
 - [Standby](#)
 - [Wake Up](#)
- Block Device
 - [Lock Device](#)
 - [Unlock Device](#)

- [Get Lock Password](#)
- [Play Siren](#)
- Device
 - [Set Device Tags](#)
 - [Change Device Name](#)
 - [Change Agent Password](#)
 - [Metrics](#)
 - [Remove Device](#)
 - [Factory Reset](#)
 - [Smart Recovery](#)
 - [Reset Auth Token](#)
 - [Collect System Logs](#)
 - [Export Device Data to CSV](#)

5.7.2 Device Usage Insights Display

The Insights icon will open a series of bar graphs displaying metrics on device usage.

- If you select the “All” group, it will display app usage statistics for all devices.
- If you select a particular group, it will display app usage statistics for only that group.

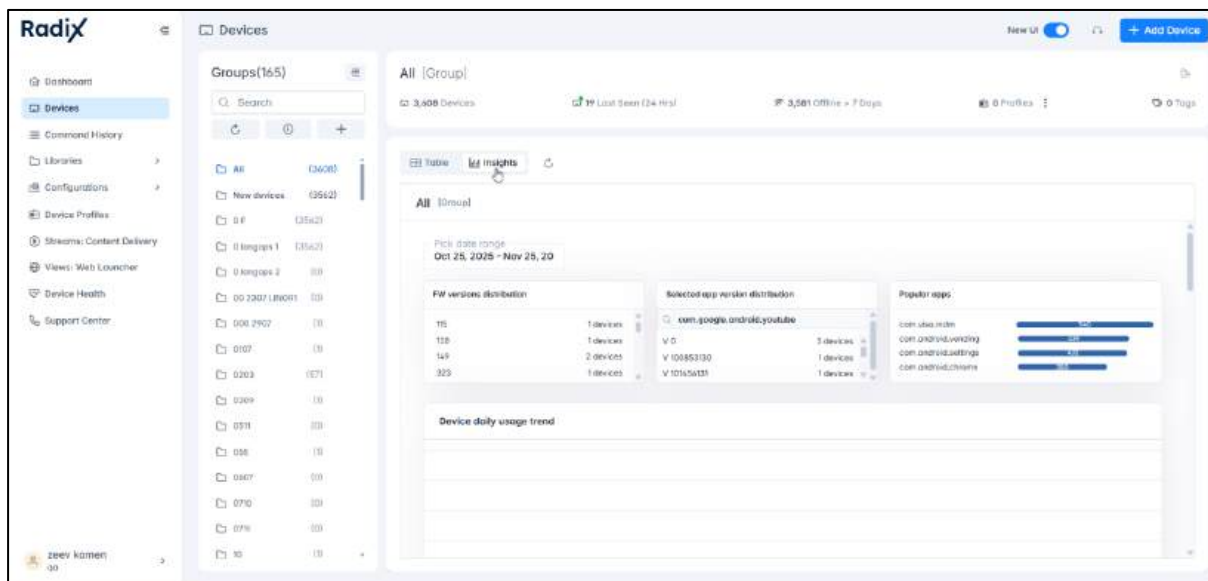


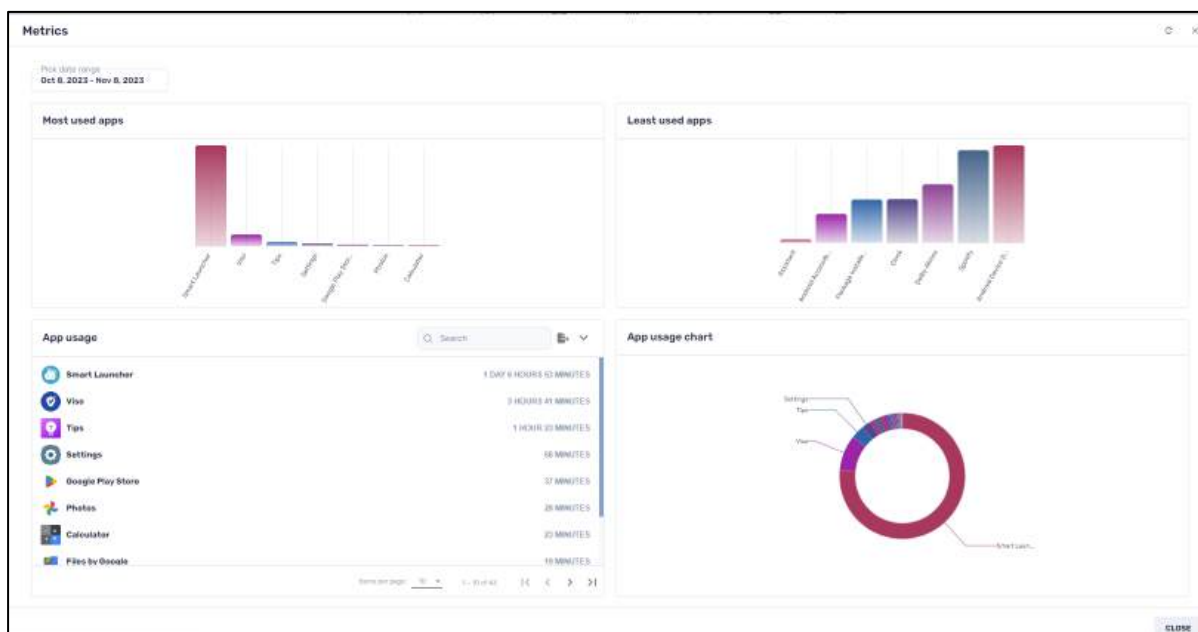
Figure 5-22: App usage insights for all devices

This provides graphical displays of app usage on a device, to see which apps are used the most, and which are used the least. It will also display the status of the device, such as:

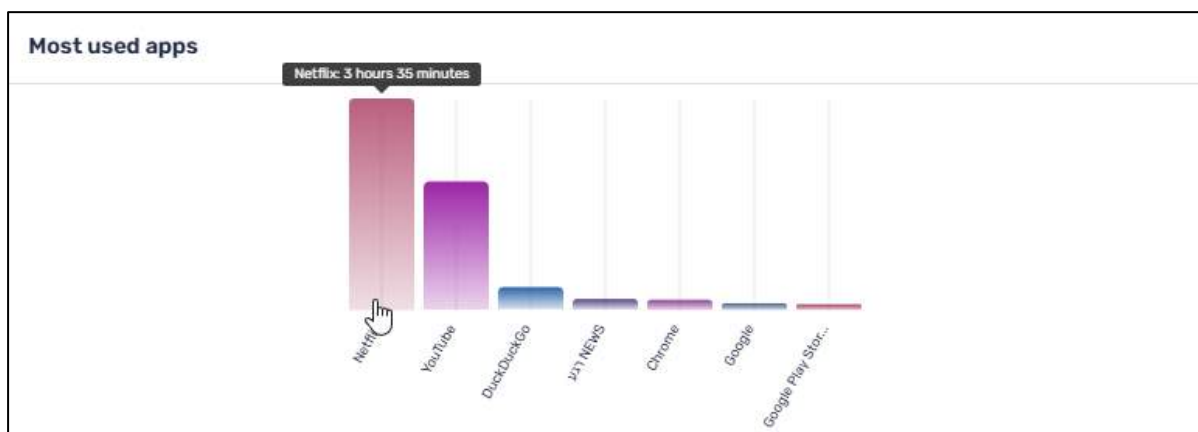
It displays the following parameters:

- CPU temperature
- CPU usage
- RC battery (for devices that use a remote control)
- Storage space
- Memory usage
- Boot time

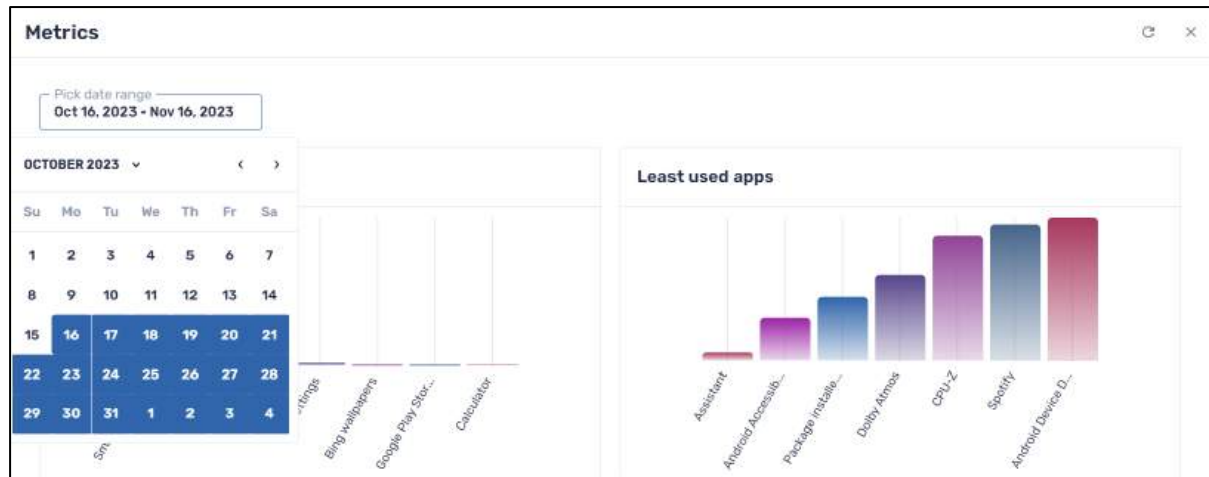
This information can help you make fact-based decisions, to optimize the usage of your device and make it into a true business asset.



Hovering your mouse over one of the bars in the **Most used apps** and **Least user apps** histograms will display the amount of time spent on each app.



There is also an option to select a range of dates, search for an app and view its usage stats, and to graph the results for a specified time period.



When I select a particular group, Insights displays statistics only for the devices in that group. In this example, Insights displays usage statistics only for the six devices in the group AEP.

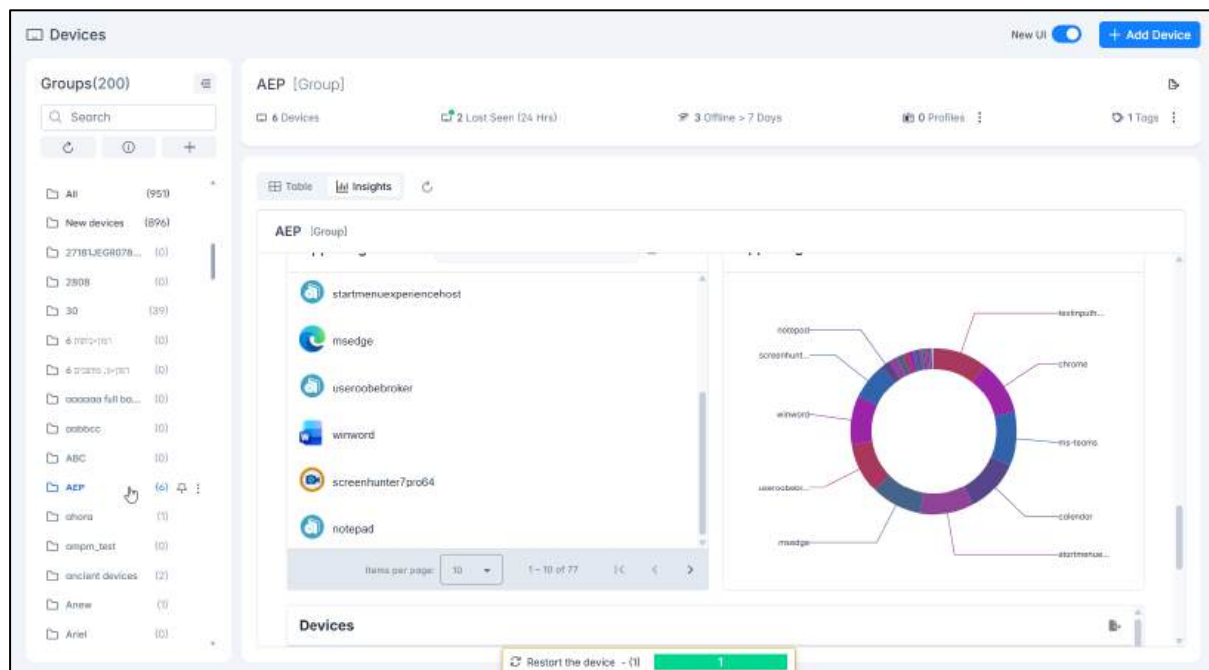
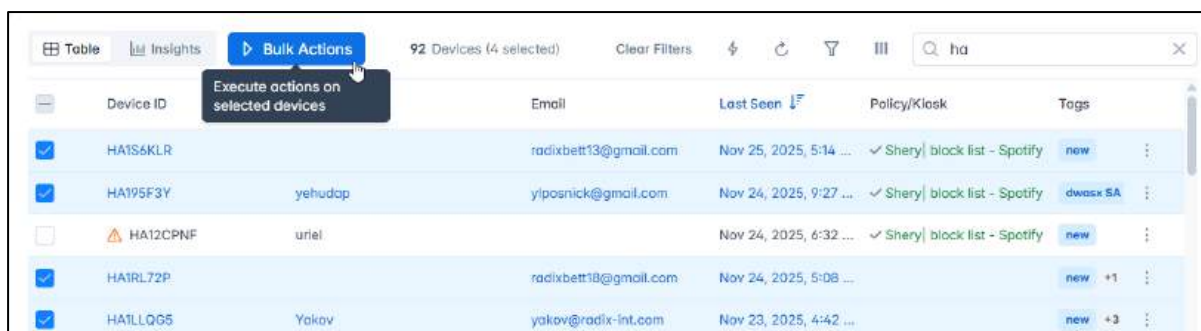


Figure 5-23: Usage statistics for the group AEP

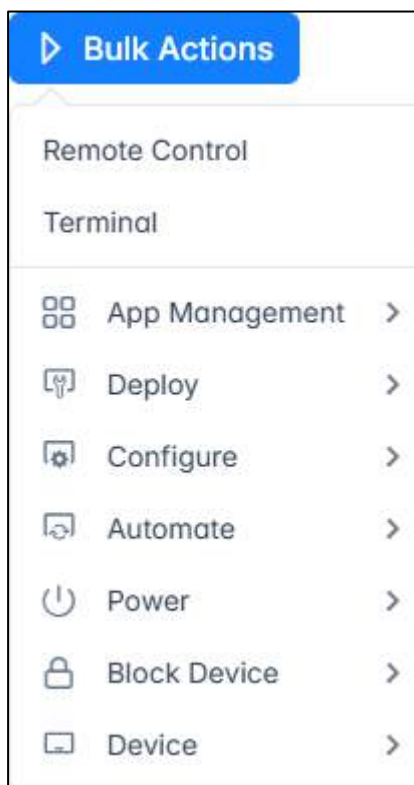
5.7.3 Bulk Actions Options

The Bulk Actions button displays a drop-down menu of commands that you can execute on several devices at once. You first select devices by clicking on their checkbox in the Devices Table listing:

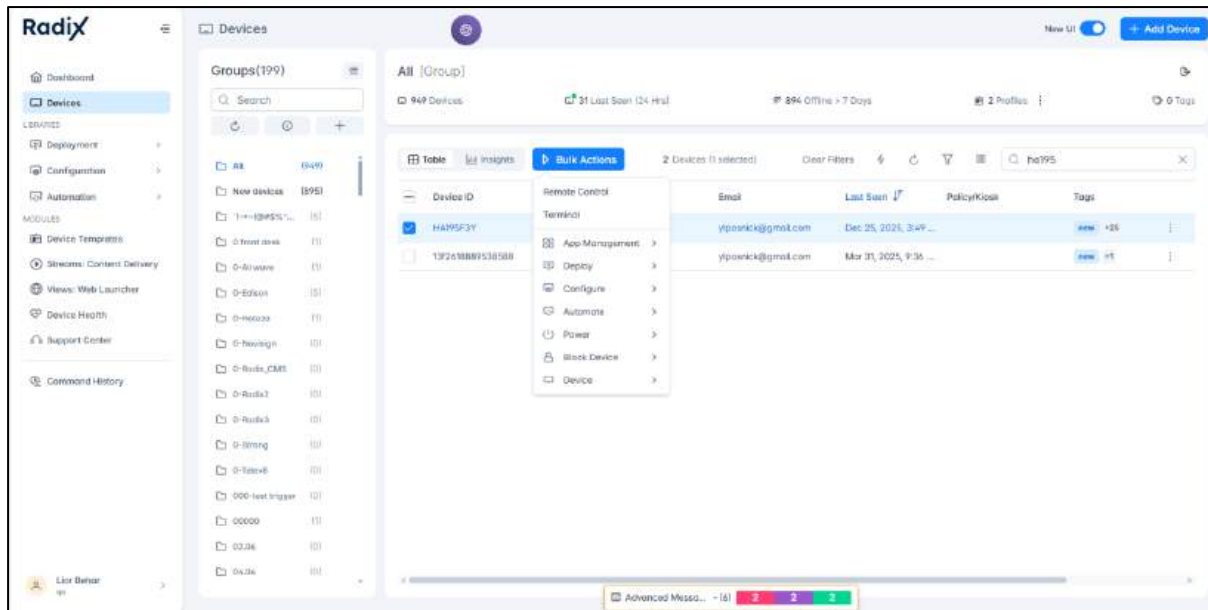


Device ID	Email	Last Seen	Policy/Kiosk	Tags
HA1S6KLR	radixbett13@gmail.com	Nov 25, 2025, 5:14 ...	✓ Sheryl block list - Spotify	new
HA195F3Y	yehudap	Nov 24, 2025, 9:27 ...	✓ Sheryl block list - Spotify	dwask SA
HA12CPNF	uriel	Nov 24, 2025, 6:32 ...	✓ Sheryl block list - Spotify	new
HA1RL72P	radixbett18@gmail.com	Nov 24, 2025, 5:08 ...		new +1
HA1LLQ65	yakov@radix-int.com	Nov 23, 2025, 4:42 ...		new +3

Clicking on **Bulk Actions** presents you with a drop-down list of commands:



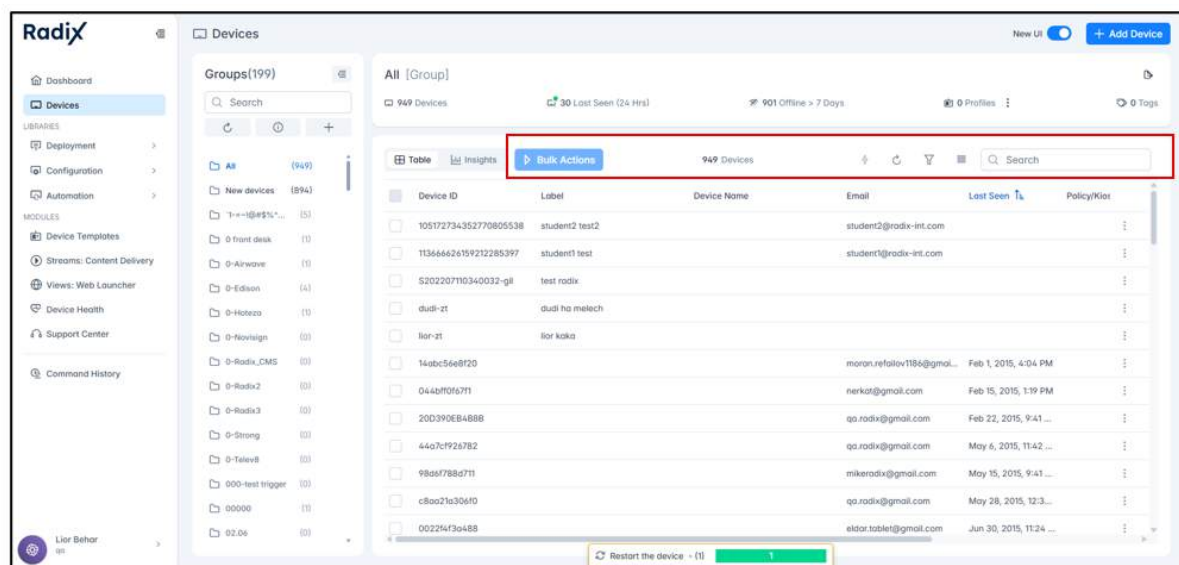
The commands “Remote Control” and “Terminal”, as well as the “Block Device” group of commands, can only be performed on a single device. Therefore, these options appear only if you select a single device in the Devices Table:



The options are identical to those explained in **Section 5.7.1**.

5.7.4 Device Information Viewing Options

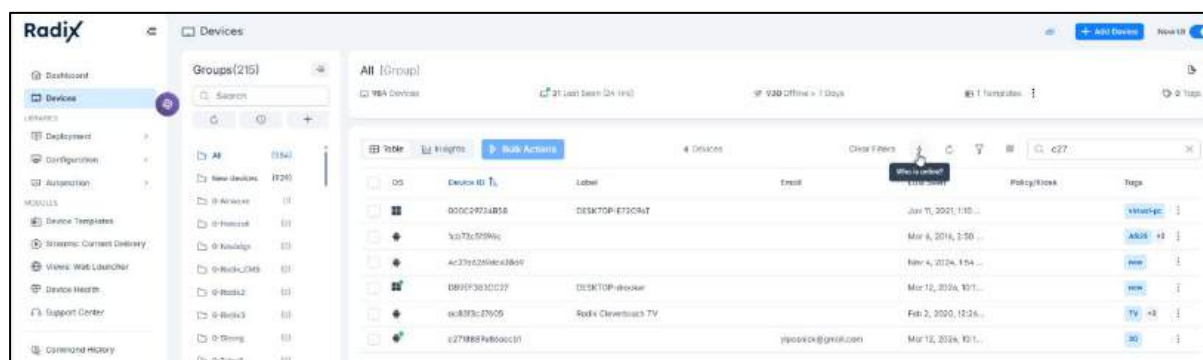
To the right of the **Bulk Actions** button, there is a row of icons that control the Devices Table display:



Icon	Description
	Who is online?: Displays the devices that are presently online
	Refresh: Resets the display of devices according to the current filters
	Filter devices: Allows you to apply a filter option to narrow down the devices displayed
	Configure columns: Allows you to select which data columns to display in the Devices Table
Search	Search: Allows you to search for devices by Device ID, Label, or user name.

5.7.5 Who is Online?

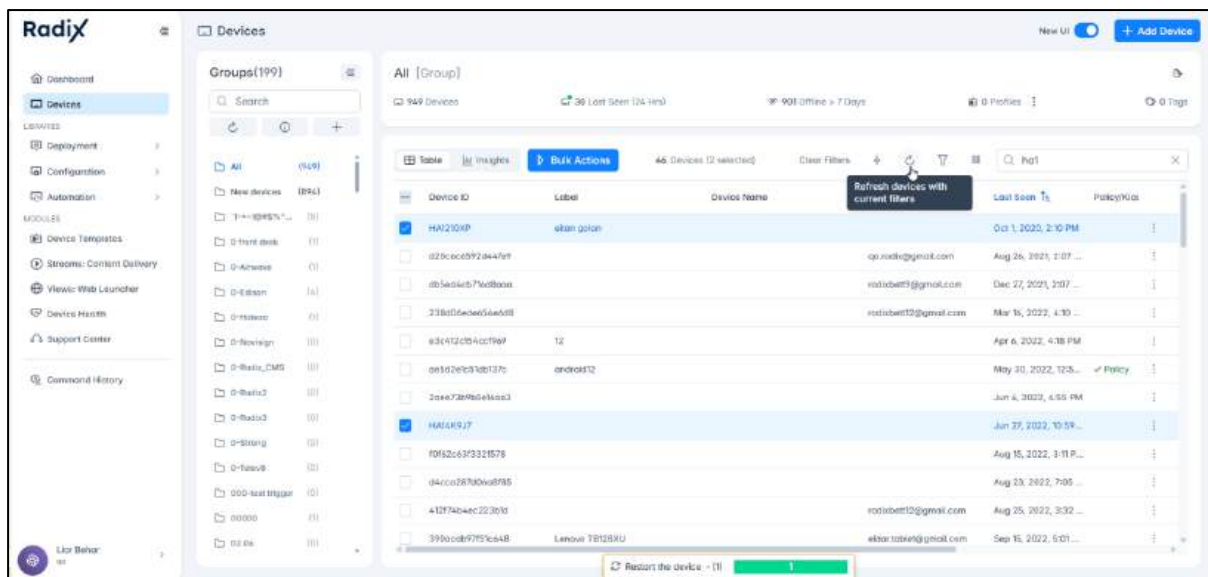
Clicking the “Who is Online” icon will help you identify all the devices and users presently online. If a device is online, a green dot will appear next to the icon of that device’s operating system in the Devices Table. In the example below, we can see that Devices **D89EF383CC27** and **c2718889e86accb1** are both presently online.



You can use this option together with a filter or a search string to narrow down the list.

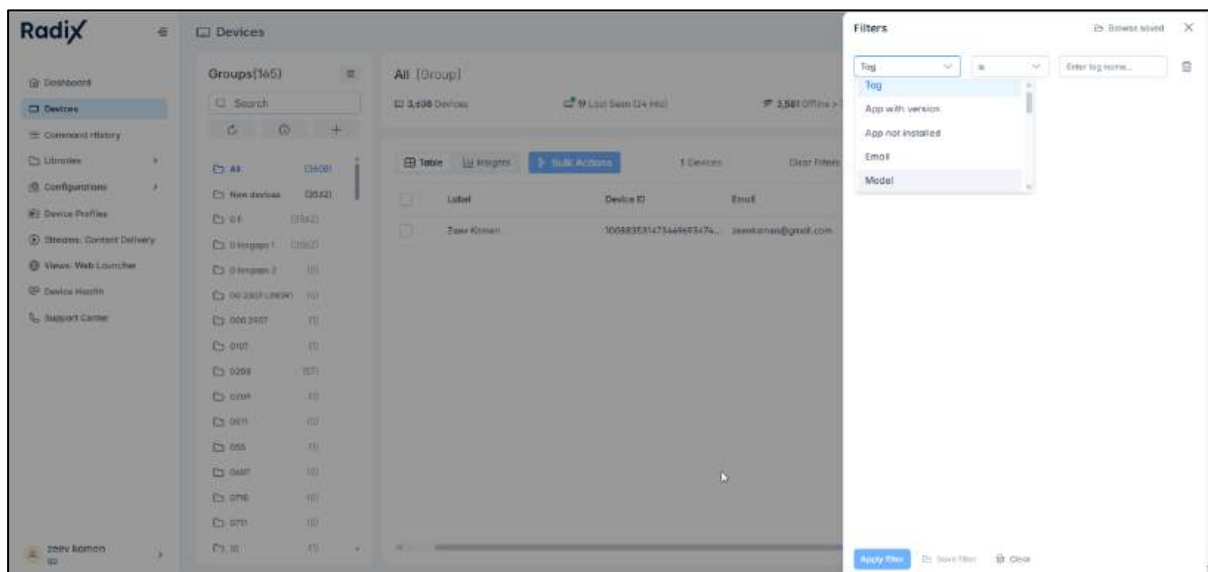
5.7.6 Refresh

Clicking on the **Refresh** icon  will refresh the display of which devices are online at present.



5.7.7 Filter Devices

When you click on the **Filter devices** icon, a window opens which allows you to provide conditions for your search. These conditions will further narrow down the devices or users displayed on the screen (but will not apply to the entire population of devices):



You can use the filtering conditions by requiring that the devices that will appear fulfill all the conditions (“AND”), or only one of the conditions (“OR”)

There are options to add conditions such as:

- **Tag:** Tags are short descriptions that you can apply to certain devices, to make it easier to group them together. You can also use tags to search for specific devices.
- **App with version:** If you wish only to display devices that have a certain version of an app.
- **App not installed:** If you wish only to display devices that do not have a certain app.
- **Email:** where you search by the email of the user of the device.
- **Model:** where you search by the model of the device.

- **Last seen:** If you wish to display only devices that were in use in the past x days.
- **Policy/Kiosk:** If you wish to display devices that have certain applications blocked or unblocked.
- **Available internal storage (in MB)**
- **OS version:** If you wish to display devices with a certain version number of an operating system.
- **Hardware ID**
- **IMEI:** If you wish to sort by International Mobile Equipment Identity number, which is unique for every mobile device.
- **Name:** Will filter by the name assigned to the device. You can assign the device name yourself in the Radix Device Management Platform.
- **Public IP:** Will filter devices by their IP address
- **OS:** Will filter devices by their operating system (Android, Windows, ChromeOS)
- **WLAN Mac Address:** This will filter devices according to their Wi-Fi MAC address
- **Ethernet Mac address:** This will filter devices according to their Ethernet MAC address
- **Firmware version:** Allows you to filter devices by their firmware version ID

If you want to view all the devices again, you can undo the filtered search.

To remove the search filter:

1. Click on the “Clear filter” icon  at the top of the Devices Table.

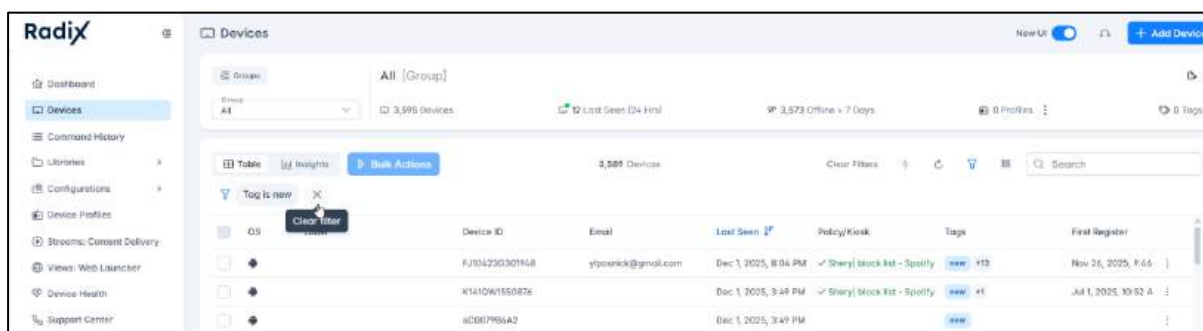
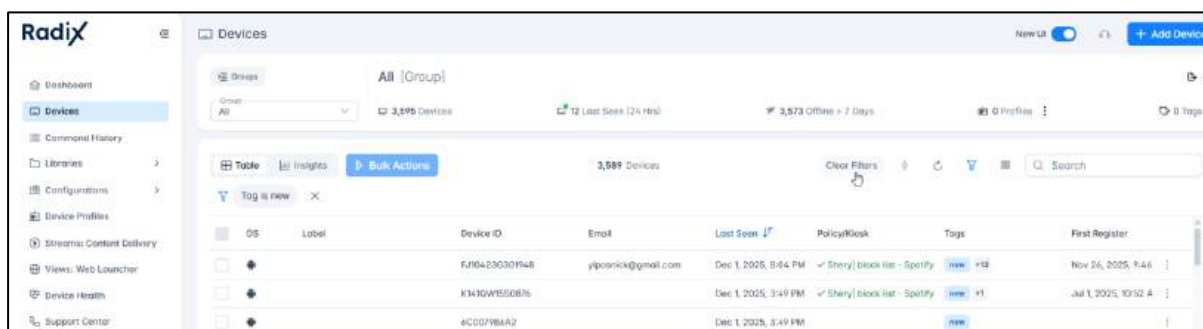


Figure 5-24: Undoing a Search Filter

2. Alternatively, you can click on **Clear Filters**.



3. The Devices Table will now display all devices, and show the group being displayed as **Group: All**.

OS	Label	Device ID	Email	Last Seen	Policy/Kiosk	Tags	First Register
Android		FJ04236303948	yipshkng@gmail.com	Dec 1, 2025, 9:04 PM	✓ Sheryl block list - Spotify	new #12	Nov 26, 2025, 9:46
Android		K14N2W1500876		Dec 1, 2025, 3:49 PM	✓ Sheryl block list - Spotify	new #1	Jul 1, 2025, 19:52 A
Android		6C0079B432		Dec 1, 2025, 3:49 PM		new	
Android TV		2391874534		Dec 1, 2025, 3:49 PM		new #2	Aug 28, 2024, 9:19
Android TV	Mike	0U5423103085	radlebell12@gmail.com	Dec 1, 2025, 3:49 PM		new #3	Mar 26, 2023, 11:05
UHD Google TV	STB	9030014923A009	radlebell11@gmail.com	Dec 1, 2025, 3:49 PM	✓ wikipedia	new #1	Sep 25, 2025, 12:18
Android		E44CC7503A16		Dec 1, 2025, 3:49 PM		view, test #1	Oct 27, 2025, 3:27
Bedroom TV		190V3001425160440		Dec 1, 2025, 3:49 PM		new #1	Aug 26, 2025, 8:46
Android	yes	190V3001019116429		Dec 1, 2025, 3:49 PM		new	
Android		4273888968e0cc01	yipshkng@gmail.com	Dec 1, 2025, 3:49 PM	✓ Sheryl block list - Spotify	new	Dec 1, 2025, 8:05 P
Android		34081UEGR05877	skel.radix@gmail.com	Dec 1, 2025, 12:05 ...		new #1	Nov 6, 2025, 11:07
Vodafone TV	PLAY	2291943878		Dec 1, 2025, 12:05 ...		git #1	Mar 16, 2024, 9:01

5.7.7.1 Creating a New Filter

You can also create and save a new search filter, to narrow down the search results for future searches as well.

To create a new filter:

1. Click on the **Filter Devices** icon . The **Filter Options** window opens.

Filters Browser saved X

Tag Is Enter tag name...

+ Add condition

Apply filter Save filter Clear

Figure 5-25: Filter Options window

2. Supply the conditions of your search, as well as whether the search results must fulfill all of the conditions (AND), or only one of them (OR).

Filters

Tag is new

OR

Tag is stage

OR

Model is Lenovo

+ Add condition

Apply filter Save filter Clear

- Click **Save Filter** on the bottom of the pane to save the search conditions. A **Save Filter** window pops up, prompting you to supply a name for the filter.

Save filter

Filter name

new + stage + lenovo

Set as private

Save

When you apply a filter, the filter condition appears at the top of the Devices Table listing:

All [Group]

3,608 Devices 19 Last Seen (24 Hrs) 3,581 Offline > 7 Days 0 Profiles 0 Tags

Table Insights Bulk Actions 2 Devices Clear Filters Search

OS is ANDROID AND Email starts with "af": OS is ANDROID AND Email starts with "f" X

☐	Label	Device ID	Email	Last Seen	Policy/Kiosk	Tags
☐	mike 123	74042be571b7	familyshoham5@gmail.co...	May 5, 2020, 2:17 PM		lenovo +6
☐		94a1a2a66b7e	fourieruser1@gmail.com	Aug 24, 2016, 10:47...		fourier +1

- Use the **Set as Private** option if you want the search option to only appear to you (as the creator of the filter item) when you are using the Radix Device Management interface.

← Save filter

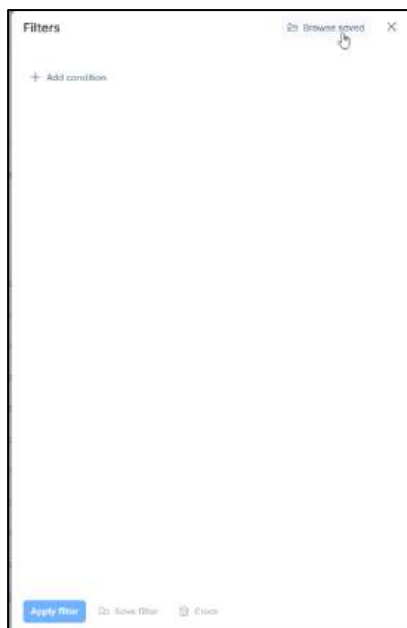
Filter name:

new + stage + lenovo

Set as private ☒

Save as new Update

- You also have options to save a filter as a new item by clicking **Save as new** or to update an existing filter by clicking **Update**.
- If you wish to search for a saved filter option, click on **Browse saved**.



7. Enter the name you assigned the filter in the Search bar. The saved filter option will appear.



Note that there are four options next to the saved filter option:

Icon	Description
	Edit , to edit an existing filter item
	Duplicate , to duplicate a filter item
	Delete , to delete the filter
	Filter actions , which opens a menu of commands that you can execute on the devices that satisfy the filter conditions

5.7.8 Selecting Columns Option

The Radix Device Management Platform interface allows you to display a wide array of columns that display valuable information about your devices. For example, you can choose to display columns that show you the device's operating system, the device's Hardware ID, the device's serial number, the username, the device's IP address, and much more.

In the Radix Device Management Platform screen, there is an option to select which columns should be displayed, by clicking on the **Columns** icon . (The Columns icon is available in the **Command History Log** and **Users Management Menu** as well.)

The screenshot shows the Radix web interface for managing devices. The left sidebar contains navigation links for Dashboard, Devices, Deployment, Configuration, Automation, Device Templates, Streams, Content Delivery, Views, Web Launcher, Device Health, Support Center, and Command History. The main area displays a table of devices under the 'All (Group)' tab. The table has 6 columns: Device ID, Label, Device Name, Email, Last Seen, and Policy/Host. A 'Configure columns' tooltip is visible over the table header. The table lists several devices, including 'HAXI20AP', 'd20cc0592944b9', 'd05ed4cc714d8a0a', '238d0d6d66546d8', 'e3ca12c154c0f56f', 'ae5d2e1c51d137c', '2a9a73b1b1efac03', 'H484c7J', '10f62ca3f3327578', 'd4cc287d0a08f86', '41217d44e223c1d', and '390ac097f51c4d8'. A 'Restart the device' button is visible at the bottom of the table.

Device ID	Label	Device Name	Email	Last Seen	Policy/Host
HAXI20AP	elton garim			Oct 1, 2020, 2:10 PM	
d20cc0592944b9			qs.radix@gmail.com	Aug 26, 2021, 1:07 PM	
d05ed4cc714d8a0a			radixbatt@gmail.com	Dec 27, 2021, 2:07 PM	
238d0d6d66546d8			radixbatt@gmail.com	Mar 16, 2022, 4:10 PM	
e3ca12c154c0f56f	12			Apr 6, 2022, 4:18 PM	
ae5d2e1c51d137c	android12			May 10, 2022, 12:5 PM	Policy
2a9a73b1b1efac03				Jun 6, 2022, 4:55 PM	
H484c7J				Jun 27, 2022, 10:59 PM	
10f62ca3f3327578				Aug 15, 2022, 3:11 PM	
d4cc287d0a08f86				Aug 23, 2022, 7:05 PM	
41217d44e223c1d			radixbatt@gmail.com	Aug 25, 2022, 3:32 PM	
390ac097f51c4d8	Lenovo T130XU		skoradavin@gmail.com	Sep 16, 2022, 5:01 PM	

The 'Select Columns' dialog box is shown, allowing users to configure the columns displayed in the table. It includes a search bar, 'Select All' and 'Reset Columns' buttons, and a list of columns with checkboxes. The selected columns are Device ID, Label, Device Name, Email, and Last Seen.

Select Columns
8 / 41 selected

Search columns...

☐ Select All

- ☐ OS
- ☒ Device ID
- ☒ Label
- ☒ Device Name
- ☒ Email
- ☒ Last Seen
- ☐ Location
- ☐ Ip address
- ☐ Local ip

Figure 5-26: Column Display Options

Note: There are other column options that are presently not selected (Location, IP address, Local IP, etc.). You can add these options in the **Account Settings Menu**, under the **Custom Columns** tab (see **Section 4.4.6**).

5.7.8.1 Columns Sort Options

There are two options to sort the device information on a particular column. There is an option to sort **alphabetically**, or by means of a **filter**.

5.7.8.1.1 Alphabetical Sort

If the column has an alphabetical list icon , clicking on it will allow sorting the information in either alphabetical ascending or descending order.

If there are more columns than can be displayed at once, the Devices Table has a sliding bar which allows you to view other columns.

5.7.8.1.2 Sort by Filter

If the column has a filter icon  next to the column name, clicking on it will allow you to filter the device information by the options in that column. For example, clicking on the filter icon in the Operating System column will allow you to sort devices by their operating system.

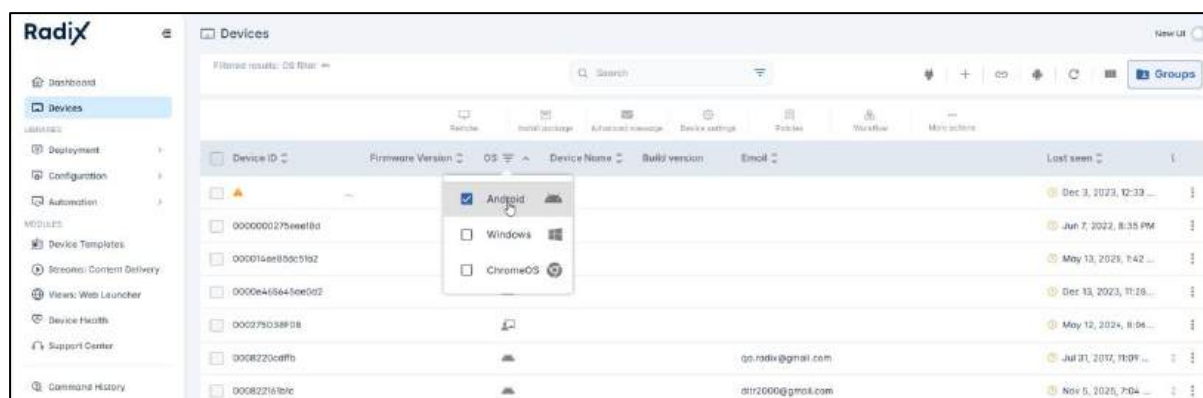
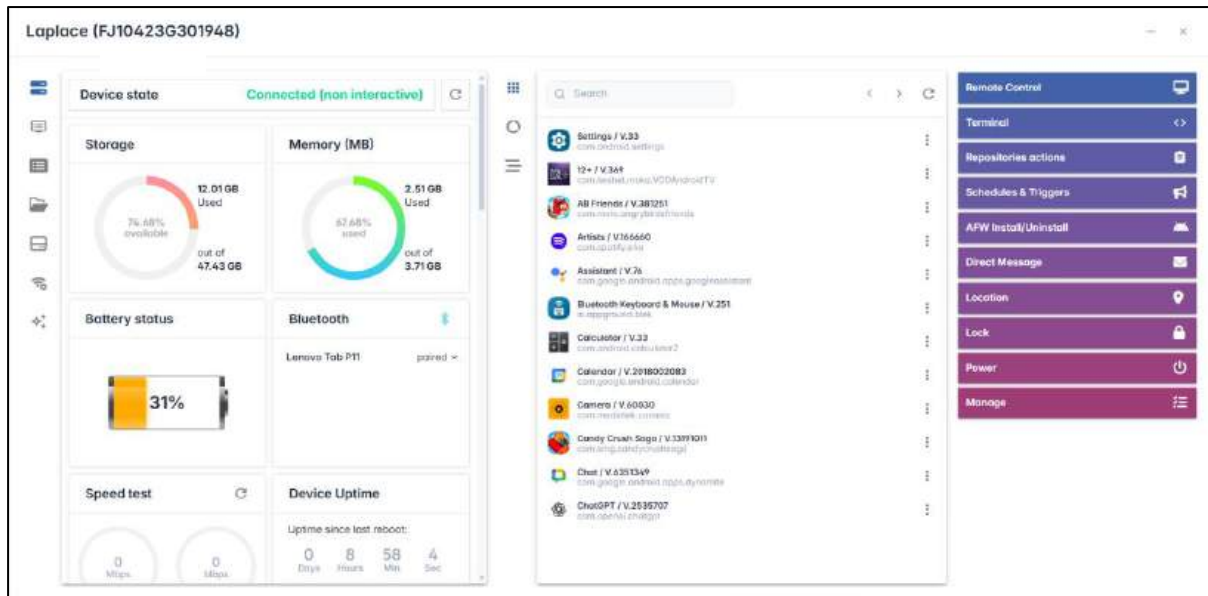


Figure 5-27: Filtering Devices by Operating System

Other columns with the Filter icon include the Agent version, Policy-Kiosk, and Tags columns.

5.8 Device Dashboard

If you would like to manage and view a single device, click on that device in the **Devices Table** list. A window opens which displays the **Device Dashboard** in three panes:



5.8.1 Left Pane Icons-- Device Status Information

This pane gives you information about a device's status and performance, such as CPU (%)/Temperature, Memory/Swap Memory available, Wi-Fi signal strength, storage space, battery level, and more. You can check the internet speed on the device and diagnose any problems. There is even an option to view HDMI resolution and frames per second to diagnose any problems the user is having with the graphics on their device.

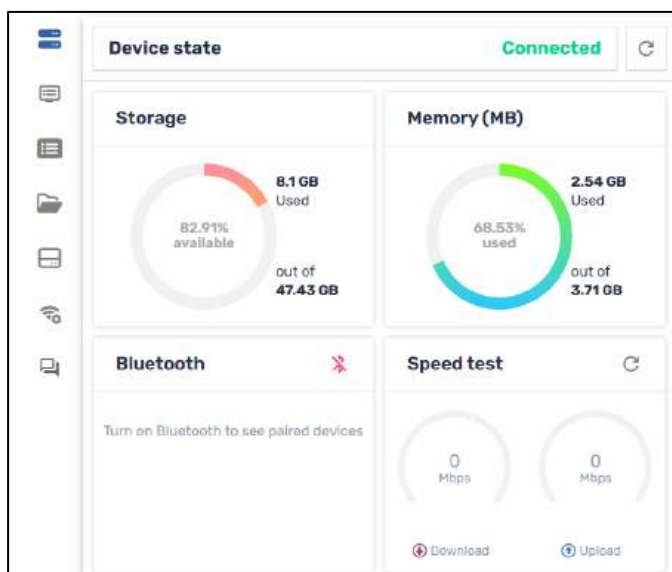


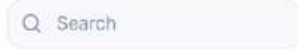
Figure 5-28: Device Status Pane

This table describes the icons on the left of the pane:

Table 5-2: Device Status Icons

Icon	Description
	General Information tab, displaying the device's storage space, memory usage, battery status, etc.
	Device Information tab, giving information about the device's connectivity, model, interface language, etc.
	Device Properties tab, telling you the name of the device and its hardware configuration
	Device's File System tab, displaying the folders and files on the device
	Device Storage Stats tab, displaying how the storage space is distributed on the device
	Device Network System tab, showing whether the device has Internet connectivity, as well as its DHCP information, MAC address, and more. This contains information that is important for IT and support teams.
	Radix AI tab generates a summary of any errors in the functioning of the device's hardware, based on the data received from the device. It also allows you to interact with the system with text messages that can focus on specific functioning issues.

Three of the tabs (Device Properties, Device's File System, and Device Storage Stats) also have the following icons and functions:

Icon	Description
	Search bar to look for package information
	Export to CSV: Option to export the data displayed into a csv file, to work with the data offline
	Expand icon for further information about an app

5.8.2 Center Pane Icons—App Management

The center pane shows all the applications presently installed on a particular device, as well as statistics such as usage time.

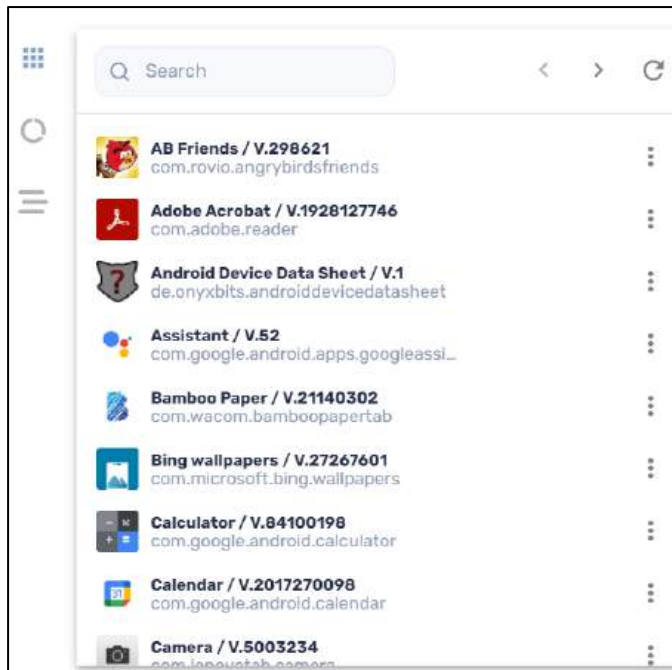


Figure 5-29: App Management Pane

Table 5-3: Apps Management Icons

Icon	Description
	Installed: General list of all apps installed on a device, with menu for each app that allows you start/stop/uninstall/etc. the app remotely
	Usage: Amount of time of usage of each app
	Advanced stats: Allows you to view the app size, app data size, and cache size of an app. Clicking on one of the apps will copy the package name to the clipboard. There are three icons at the top of the Advanced stats

By clicking on the three-dot menu next to an app, you have the options of starting or stopping the app, enabling/disabling the app, or even uninstalling it.

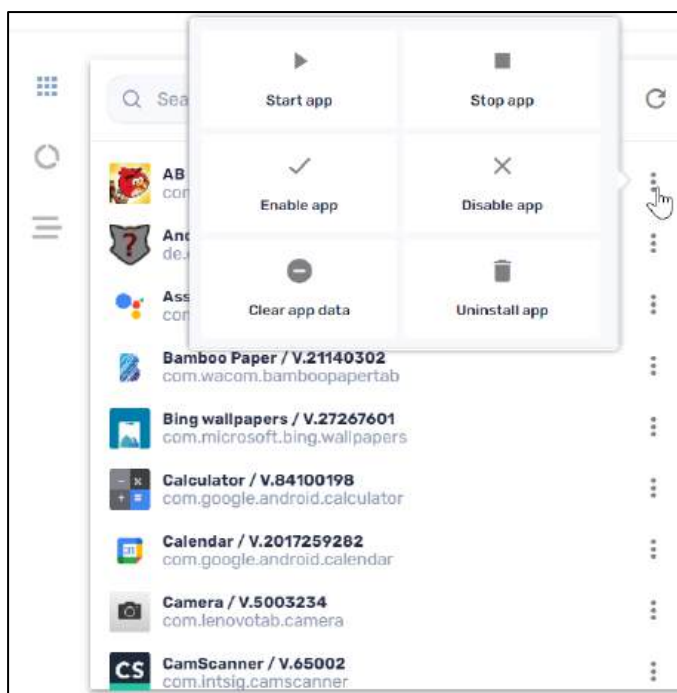


Figure 5-30: Application Management Menu

Take note of the **Clear app data** option. This is a useful feature, where you can assist the user in fixing any issues they may have with an application. It effectively resets and repairs the application by wiping its history. The user can then start the app afresh, without any of the previous baggage that may have caused it to crash.

When you click on the **Advanced Stats** icon , there are three further options:

Icon	Description
	Search bar: To search through the apps by package name
	Export to CSV: To export the app usage statistics to a CSV file
	Expand: To view the usage statistics in an expanded window.

5.8.3 Right Pane Options—Device Actions

The right pane of the Device Dashboard has a list of actions, which allow you to engage with a customer and work on their device remotely.

Table 5-4: Device Actions Icons

Icon	Description
	Remote
	Terminal
	Repositories actions
	Schedule & trigger command
	AFW (= Android for Work) install/uninstall
	Direct Message
	Location
	Lock
	Power
	Manage

We will briefly go through the Device Actions options:

5.8.3.1 Remote

This allows you to interact with the user's device remotely. For details, see **Section 6.1.22, Remote Control**.

5.8.3.2 Live Terminal

This opens a fully featured, live terminal with an ADB (=Android Debug Bridge) shell connection. This allows you to remotely debug an issue with a device, as well as download a log of commands to the device and run exec scripts remotely. For details, see **Section 6.1.33, Terminal**.

5.8.3.3 Repository actions

These are series of commands that can be prepared in advance and stored on the Radix Device Management user interface. You can then apply them to any device in the system. Clicking on the **Repository actions** icon opens a drop-down menu:

Table 5-5: Repository Actions Icons

Icon	Description
	Install Packages: Allows you to create an installation package and install apps remotely, as explained in Section 6.1.13, Install App/Install Package .
	Policies: This allows you to black-list applications that have security issues, or to white-list and allow certain applications that are installed on devices. This is explained in Section 6.1.21, Policies (Block Lists) .
	Kiosk: This creates a whitelist of specific applications that you want to apply to a device. This is good for a store display or hotel room, where you want to only use certain apps. This is explained in Section 6.1.14, Kiosk .

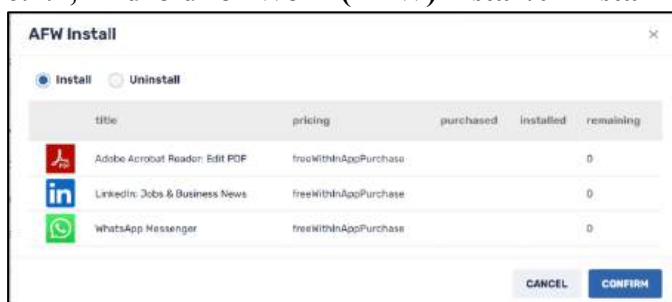
	Views: This is for creating a content management system, a specialized type of Kiosk, consisting of allowed installed apps and/or a web app. This is explained in Section 6.1.35, Views .
	Advanced Messaging: This allows you to interact with users using an engaging message that can contain text, sound, or images. This is explained in Section 6.1.1, Advanced Messaging .
	Device Settings: This allows you to apply different settings to the device. This is explained in Section 6.1.8, Device Settings .
	Remote Execute: This allows you to execute terminal commands on a device remotely. This is explained in Section 6.1.23, Remote Execute .
	Files: This allows you to upload files to a device. This is explained in Section 6.1.28, Send Files .
	OTA: This enables an Android device to receive and install updates to its operating system or apps. This is explained in Section 6.1.18, OTA .
	OTA Update Engine: This provides an alternate method of performing an over-the-air update to an Android device's operating system or apps, for devices running Android 8.0 or newer, and that employ the A/B partition updater. See Section 6.1.19, OTA Update Engine .
	Workflow: This option allows you to batch commands and trigger them, to automate processes. You can also create a Favorites menu, as well as move commands between different workflow stages during setup. This is explained in Section 6.1.39, Workflow .

5.8.3.4 Schedule & trigger command

This allows you to trigger any type of command from within the Device Dashboard. You can also create a **Favorites** menu of commands to be executed. This is treated at length in **Section 6.1.26, Scheduler & Triggers Command**.

5.8.3.5 AFW Install/Uninstall

Clicking on this tile opens the **AFW Install** pane, which allows you to install or uninstall apps on a device that is registered in the Android for Work (AFW) program. See **Section 6.1.2, Android for Work (AFW) install/uninstall**

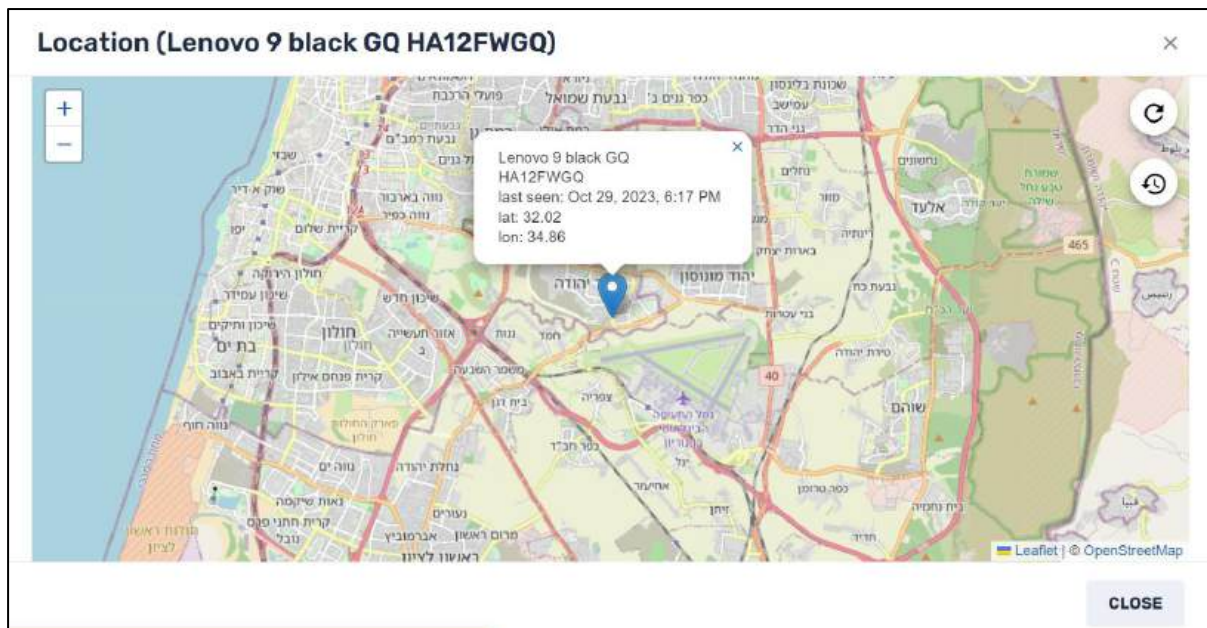


5.8.3.6 Direct Message

This allows you to send a text message to the user on their device. This is treated at length in **Section 6.1.9, Direct Message**.

5.8.3.7 Location

This allows you to see the geographical location of the device, according to Google Information Services.



By clicking on the **Location History** icon , you can see where the device has been over a range of dates. This will help you locate the device if it is lost or stolen.

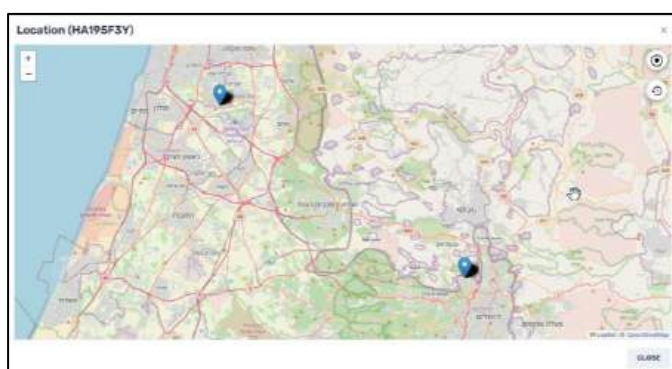
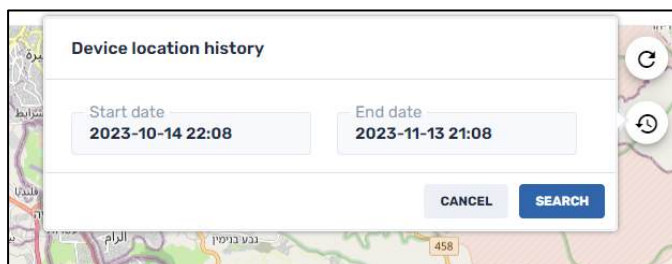


Figure 5-31: Location of a device within the selected time frame

5.8.3.8 Lock Menu

When you click on the Lock option in the right-hand pane of the Device Dashboard, you will see the following options to lock and unlock a lost or stolen device.

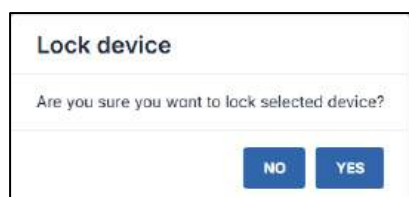
Table 5-6: Lock/Unlock Device Options

Icon	Description
	Lock: This locks the device so that the user cannot change any of the settings.
	Unlock: This unlocks the device, to enable the user to change settings.
	Get Password: This allows you to retrieve the device's password, to allow the remote user to unlock their device, in the event that the user forgot the password.
	Siren: Makes the device sound off an alarm. The Siren command will make the device sound an alert, even if the device has been disconnected from the Radix network.
	Wipe: Restores the device to factory settings.

5.8.3.8.1 Locking a Device

The Lock Device command will lock the remote device. This can be useful as part of a workflow, where you lock down a device if it is lost or stolen.

1. When you click on the Lock tile, this will open the Lock Device dialog box.



2. When you click on **Yes**, the device will be locked. The remote device will only be able to make emergency phone calls:

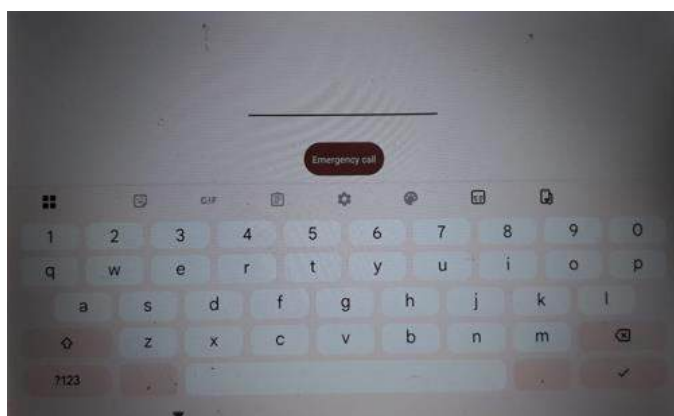


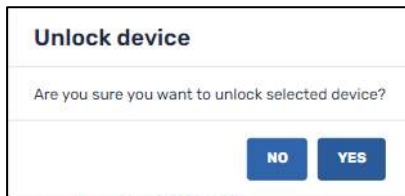
Figure 5-32: Appearance of a locked device

5.8.3.8.2 Unlocking a device—Get Device Password

Once a device is locked, there are two options to unlock the device:

Option 1: From the Radix Device Management Platform:

1. The administrator must click on the Devices icon in the sidebar menu, to open the Devices Table.
2. The administrator should find the locked device in the list of devices in the Devices Table.
3. The administrator should open the device's Device Dashboard, and then click **Lock>Unlock**.
4. The administrator will receive a prompt, asking them to verify that they want to unlock the device:



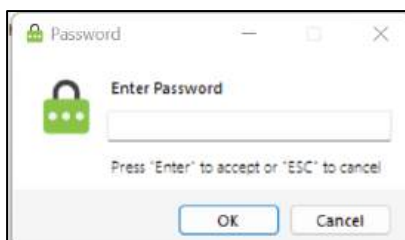
5. Upon clicking **Yes**, the remote device will be unlocked.

Option 2: For the remote device user:

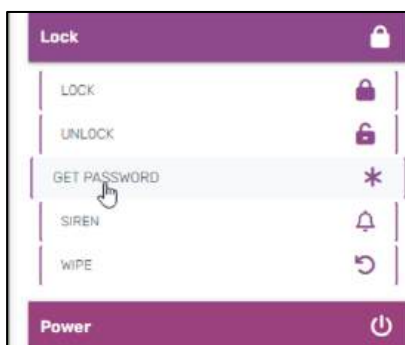
There is also an option for the remote device user to unlock their device. This may be useful if the administrator locked a lost device, and then the remote user finds the device and wants to unlock it themselves.

To unlock a device:

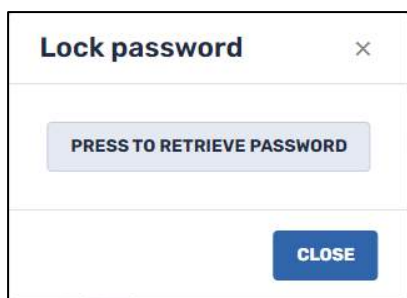
1. On a Windows device, press the key combination **Alt-Ctrl-Shift-F9**. You will receive a prompt requesting the device password:



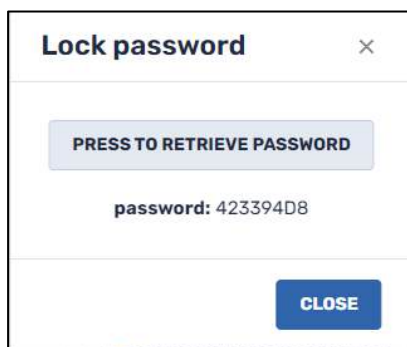
2. Enter the device password and click **OK**. If you do not know the password, ask the Administrator to retrieve it by clicking on the **Get Password** command in the Device Dashboard.



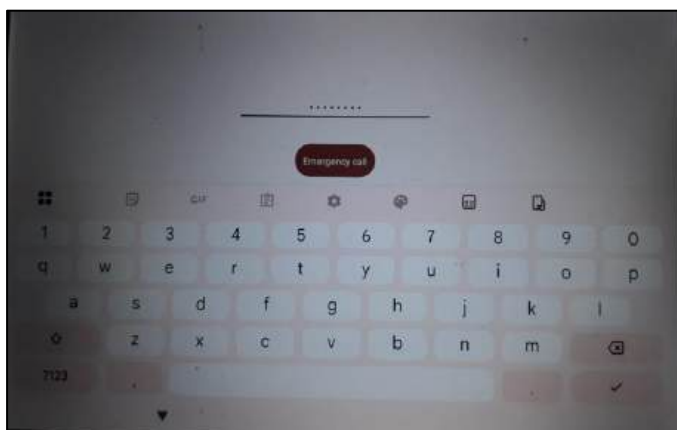
The following window opens, displaying the password to unlock the device:



3. The Administrator clicks **Press to Retrieve Password** to display the device password:



4. **For an Android device**, the remote user should enter this password in the Emergency Call screen and click the checkmark  icon.



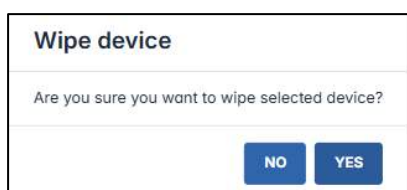
5. When the remote device user enters the password, this should unlock their device.

5.8.3.8.3 Siren

The Siren command will sound a siren on the device. This can be used as part of a workflow, or as a security measure to alert you if a device is stolen or lost. See **Section 6.1.30**.

5.8.3.8.4 Wipe

The Wipe command will restore a device to factory settings. This can also be used as a security measure, to wipe a device clean if it is lost or stolen.



5.8.3.9 Power management options menu

Clicking on the Power icon allows you to restart, shut down, or wake up a device.

Table 5-7: Power Management Options

Icon	Description
	Restart —Allows you to restart a device remotely. See Section 6.1.25, Restart .
	Shutdown —Allows you to shut down a device remotely. See Section 6.1.29, Shutdown .
	Wake-on-LAN —Allows you to wake up or turn on a device by means of a network trigger. See Section 6.1.36, Wake on LAN .

5.8.3.10 Manage Menu

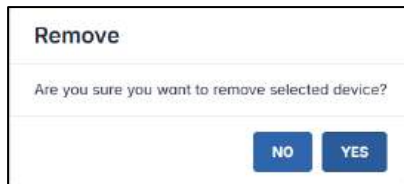
The **Manage** drop-down menu allows you to perform actions on user accounts, such as to change a device name, a password, or to change settings.

Table 5-8: Manage Device Options

Icon	Description
	Remove: Allows you to remove a device from the Radix Device Management system.
	Rename: Allows you to rename your device.
	Tags: Allows you to add or remove tags from a device. Tags make it easier to group similar devices together.
	Change Agent Password: Allows you to change the password on the device remotely.
	Reset Authentication Token: This resets the authentication token for a device. It may be necessary when you see a warning icon next to a device listed.
	Remove Google Accounts: This lets you remove one or all Google accounts from a device.
	Manage Users: This allows you to create or remove a Radix Device Interface user.
	Screen Settings: This allows you to adjust the volume and brightness settings (specifically on a flat panel device).
	Firmware Update: Allows you to update the firmware on the device.

5.8.3.10.1 Remove Device

When you click on **Remove**, this will open the Remove Device dialog box.



Clicking on **Yes** will remove the device from the Radix platform. A message will appear informing the remote user that the device has been removed from the domain.

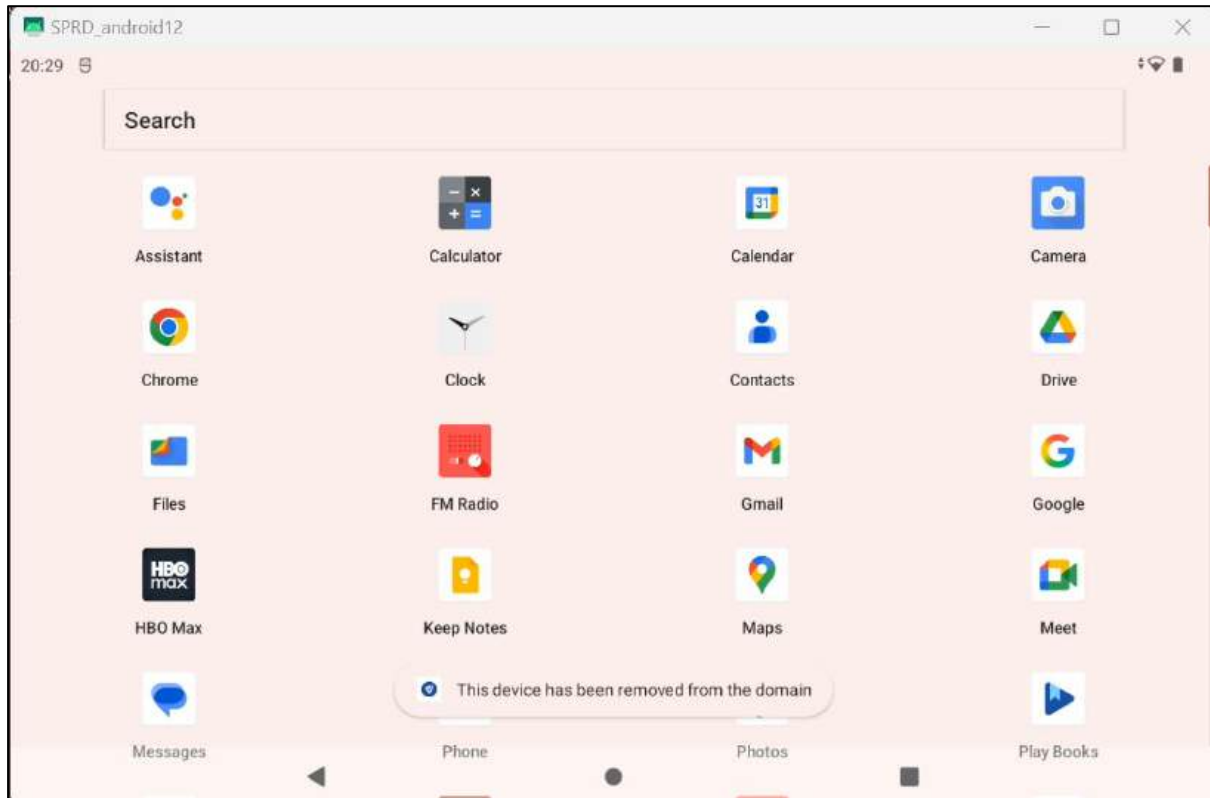
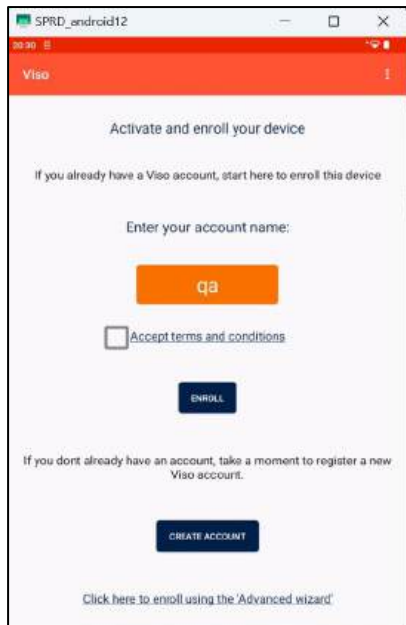


Figure 5-33: Notification that the device has been removed from the Radix Device Management Platform

The Viso app icon will still appear on the remote device. When you click on it, you will be prompted to enroll the device once again.



After you enroll the device, it will appear once again in the Devices Table.

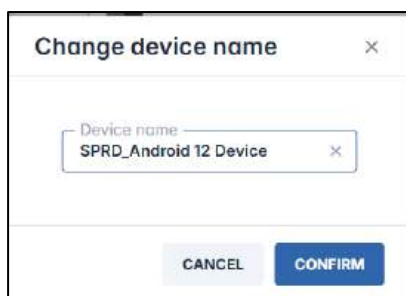
5.8.3.10.2 Rename/Change Device Name

This allows you to change the device name as it appears in the Radix Device Management Platform.

In the example below, the device has no device name.

Device ID	Firmware Version	OS	Device Name	Build version	Email	Last seen
978470d4970c154d	26320				work-A4F7A00218208C96FD522D25B8521D@android-for-work.googleusercontent.com	Dec 22, 2023

When you click on the **Change Device Name** command, the following window opens:



Enter the new device name and click **Confirm** to perform the change.

5.8.3.10.3 Tags

This option allows you to add to or remove tags from a device or user. These tags can help you in grouping users together, or when searching for devices.

Tags

×

Add or remove tags from selected devices

Add tag, then press enter

new

ylp

CANCEL

CONFIRM

- **To add a tag to a device:** Type the name of the tag in the textbox and click **Enter**.
- **To delete a tag from a device:** Click on the  on the tag you would like to delete.

5.8.3.10.4 Change Agent Password

This allows you to change a remote user's password if they wish to make changes to the VISO app installed on their remote device. This command is discussed in **Section 6.1.3**.

5.8.3.10.5 Reset Authentication Token

The Authentication Token is the key for communication between the remote device and Radix server. When you register a device, but you notice that it is not communicating properly with the Radix server, resetting the Authentication Token is the initial step to correct this.

If you see an **Invalid Authentication Token** warning next to a device in the Devices Table, you will have to use the **Reset Authentication Token** command to remove the warning.

Devices Group: All						
Q Search + + + + Groups						
	Hardware ID	Name	Email	Last seen	Location	
	E88F6F0E3DC1511			Dec 25, 2023, 6:05 PM		
	2cdd5f1f0516	My new Android TV	nadav.radix@gmail.com	May 9, 2023, 12:01 PM		
Items per page: 200 1 - 2 of 2 < >						

When you click on the warning icon, you will receive the following popup message:

Invalid authentication token

Why do I receive this message?

You are receiving this message because the server detected that the device authentication token is missing or incorrect. This can be caused after uninstalling and reinstalling the app or factory reset.

Please reset the authentication token in order for the device to sync with the server and regain device management capabilities.

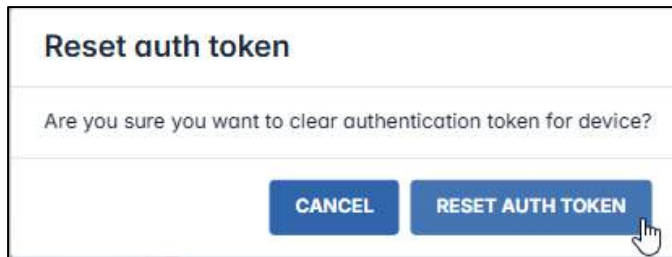
More info

CANCEL

RESET AUTH TOKEN

Clicking on **Reset Authentication Token** should resolve the problem.

Alternatively, you can click on Reset Authentication Token in the device's Dashboard Menu:

A dialog box titled "Reset auth token". Below the title is a question: "Are you sure you want to clear authentication token for device?". At the bottom are two buttons: "CANCEL" and "RESET AUTH TOKEN". A mouse cursor is pointing at the "RESET AUTH TOKEN" button.

Reset auth token

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

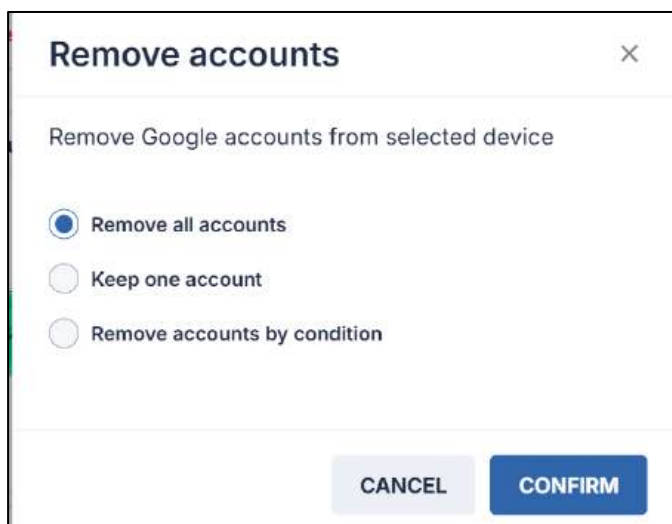
CANCEL RESET AUTH TOKEN

5.8.3.10.6 Remove Google Accounts

This allows the Radix Device Management user to remove all Google accounts from a device, or to retain one. This is useful in instances where you want to transfer the use of a device from one user to another, and you want to switch over the default Google account on the device as well.

To remove Google accounts from a device:

1. Click on the Remove Google Accounts tile. The **Remove Accounts** window appears.

A dialog box titled "Remove accounts" with a close button (X) in the top right corner. Below the title is the text "Remove Google accounts from selected device". There are three radio button options: "Remove all accounts" (which is selected), "Keep one account", and "Remove accounts by condition". At the bottom are two buttons: "CANCEL" and "CONFIRM".

Remove accounts

Remove Google accounts from selected device

☒ Remove all accounts

☐ Keep one account

☐ Remove accounts by condition

CANCEL CONFIRM

2. If you select "Remove all accounts" and click **Confirm**, you will get a confirmation in the lower right corner that the command to remove the Google account(s) has been sent to the device.
3. If you select "Keep one account", you will be prompted to enter a Google account that you would like to retain.

Remove accounts [X]

Remove Google accounts from selected device

☐ Remove all accounts
☒ Keep one account
☐ Remove accounts by condition

Enter an account name you'd like to keep

Email account

CANCEL CONFIRM

- If you select **Remove accounts by condition**, you will be prompted for a condition that the Google account must/must not contain to be removed.

Remove accounts [X]

Remove Google accounts from selected device

☐ Remove all accounts
☐ Keep one account
☒ Remove accounts by condition

☒ Contain ☐ Not contain

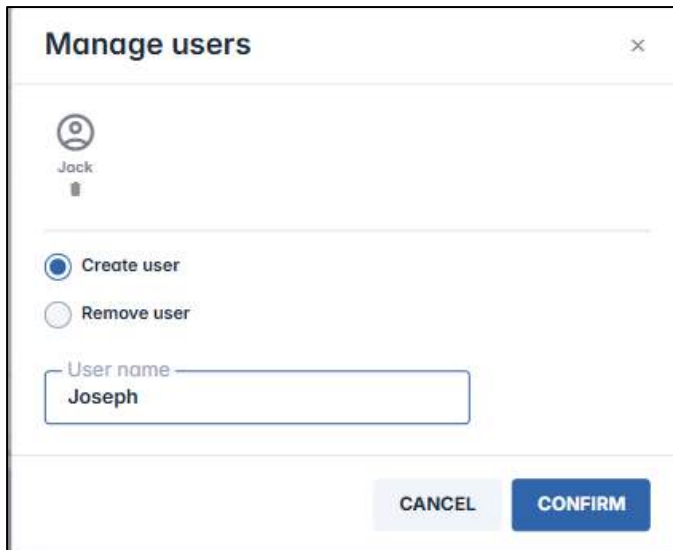
Condition data

CANCEL CONFIRM

- Click **Confirm**. You will get confirmation that all Google accounts have been removed, except for the one(s) that you wished to retain.

5.8.3.10.7 Manage Users

This command allows you to create or remove users on a remote device.



Manage users [X]

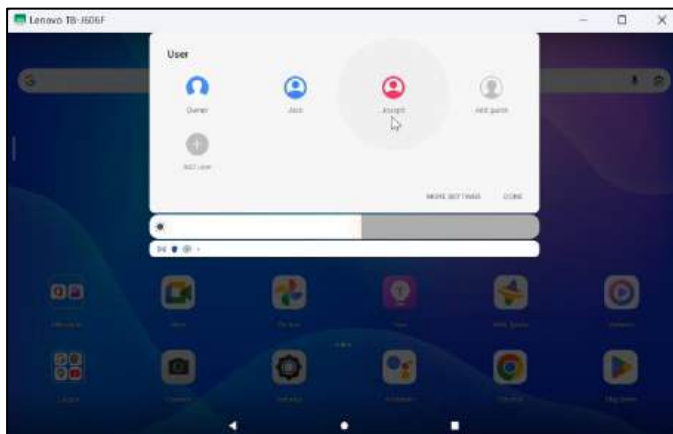
Jack [Trash icon]

☒ Create user
☐ Remove user

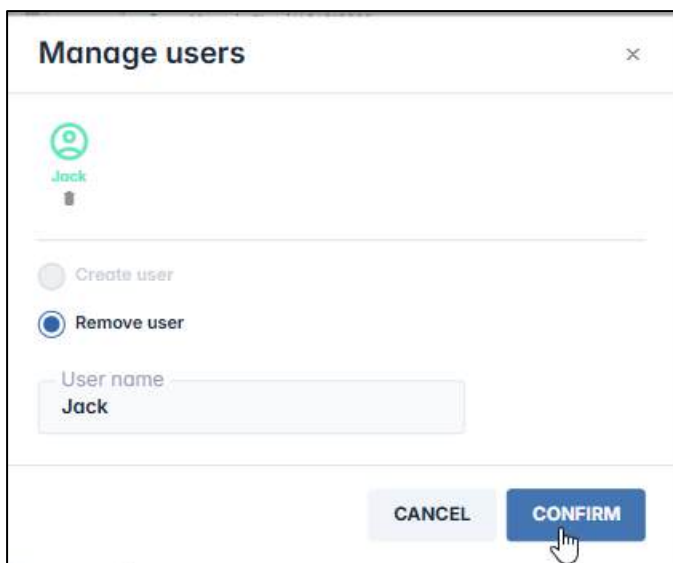
User name:

CANCEL CONFIRM

Upon clicking **Confirm**, the user Joseph will be added to the remote device:



You can also use the command to remove a device user.



Manage users [X]

Jack [Trash icon]

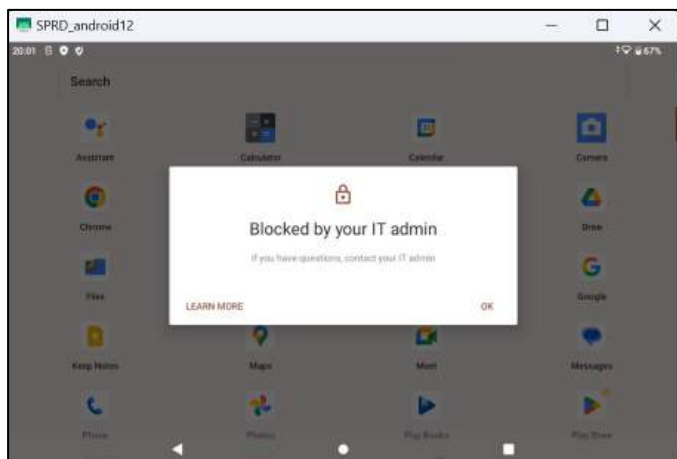
☐ Create user
☒ Remove user

User name:

CANCEL CONFIRM

Upon clicking **Confirm**, Jack's account will be removed from the remote device.

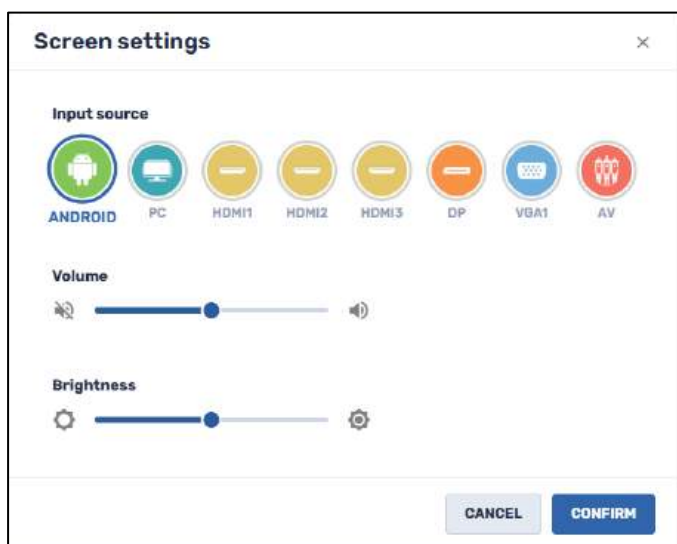
Note: The remote user must have privileges to add or remove users on the remote device. Otherwise, the command will not work.



5.8.3.10.8 Screen Settings

This allows you to adjust the brightness and volume on flat panel devices.

When you click on the **Screen Settings** command tile, the following window opens:



To use the Screen Settings command:

1. Specify the input source for the signal to the flat panel device.
2. Adjust the volume and brightness to the desired levels.
3. Click **Confirm**. You will receive a notification that the command has been sent to the flat panel device.

5.8.3.10.9 Firmware Update

This option allows you to update the device's firmware, for better performance and security.

Firmware update

Are you sure you want to update the firmware on the selected device?

NO
YES

Note: Not all devices allow remote firmware updates via the Radix MDM. If your remote device does not support firmware updates, you will get a “Command failed” message:

Command status (Ad-Hoc - Update firmware)

Status filter: All

ID	Time	Status
HA195F3Y (yehudap)	Sep 29, 2024, 11:54:55 AM	Command failed
Note: Not supported for this device		
HA195F3Y (yehudap)	Sep 29, 2024, 11:54:54 AM	Command sent

1

Devices

0

Success

0%

1

Failed

100%

0

Pending

0%

Items per page: 10

1 - 2 of 2

CLOSE

Figure 5-34 Message when attempting a firmware update on an unsupported device

Chapter 6. List of Commands

Here is a list of all of the options that are displayed in the drop-down list of commands when you click on a device's three-dot menu. The options will differ depending on the device's operating system, since some commands are only relevant for Windows or Chrome devices. All of the command options, for all devices, are discussed in [Appendix A—Alphabetical List of Commands](#).

6.1.1 Advanced Messaging/Messaging

This option sends a text message with an image to a device. For example, the message may be a “Welcome” message, a holiday greeting, or an emergency alert. The message options include an image, an image with sound, a full-screen YouTube video, or interactive clickable HTML forms. The message can be timed and triggered according to time of day and the like.

When you click on the Advanced Messaging icon, a grid of stored advanced messages appears.

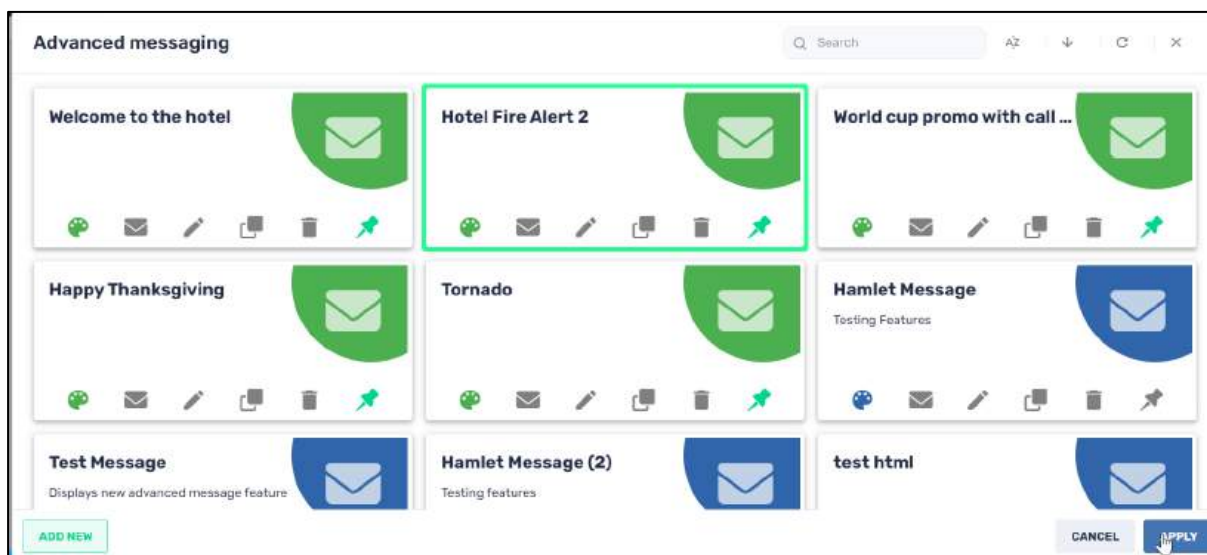
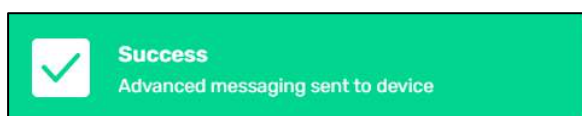


Figure 6-1: Advanced Messaging Grid of Options

To use an existing advanced message:

1. Select one of the messages and click **Apply**.
2. If the message is successfully sent, a “Success” prompt will appear in the lower right corner.



There is also an option to add a new advanced message.

To add a new message:

1. Click on the **Add New** button in the lower left of the Advanced Messaging grid. The “New Advanced Message” screen appears.

New advanced message

Name

Description

☐ Display the message once when device turns on.

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

Set the device volume level (0% - 100%)

0

Switch active source

CANCEL CONFIRM

2. Assign a name and description to the new message.

New advanced message

Name
Horatio message

Description
Message from Hamlet

☐ Display the message once when device turns on.

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

Set the device volume level (0% - 100%)

-1

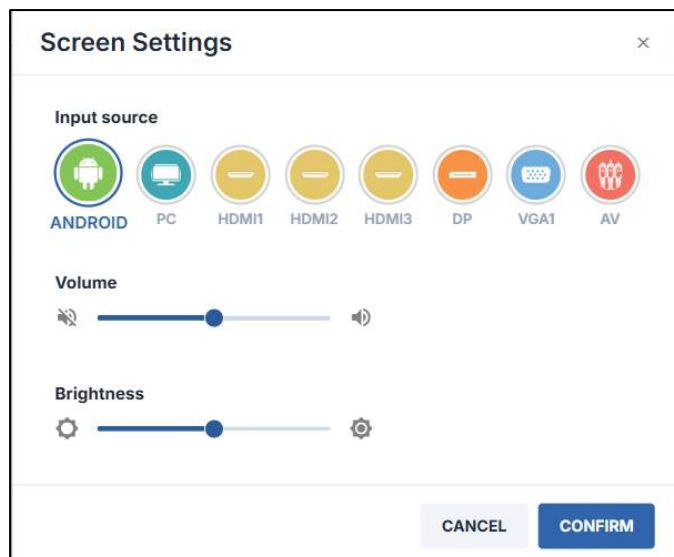
Switch active source

CANCEL CONFIRM

Figure 6-2: New Advanced Message Screen, in Edit mode

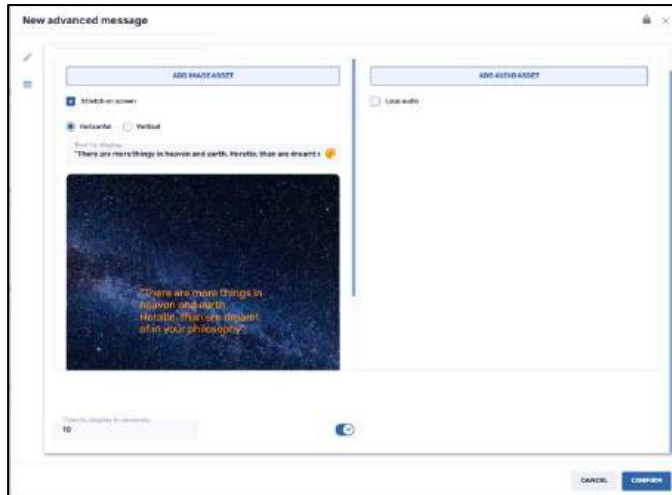
3. Check the checkbox “Display the message once when device turns on”, if you want the device to display the advanced message when the device’s screen goes off and you turn it back on. This can be either:
 - After a screen timeout, when the screen goes black after a period of inactivity, or
 - If you turn off the display with the power button and later turn it back on.
4. Click on the **Set as private** button if you want this new advanced message option to be visible only to you (the creator of the item) when you log in to the Radix Device Management Platform.
5. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
6. Click on the **Set as read-only** button if you want to limit who can edit this advanced message. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
7. Click on the **Set the Device Volume Level** button if you want to specify the volume of the advanced message on the remote devices.
8. Click on **Switch Active Source** if you wish the device to switch the source of the Advanced Message’s video content to Android. If you do not click the Switch Active Source button, then a remote device will only display the Advanced Message if it is presently set to display video content for Android devices. If it is presently set to display HDMI video content, for example, then the Advanced Message will **not** be displayed on the device.

Note: If you want to see the video input source, go to the Device Dashboard, and click on **Manage>Screen Settings**:



9. Click on the **Content** icon  on the left. The **Advanced Message Type** screen opens, allowing you to add media to your advanced message. You have the option of adding:

- **Image or sound files.** You can add an image asset or audio asset to your Advanced Message. You may provide a text message, set the orientation and color of the text, as well as the time it should be displayed.



- **A YouTube URL.** There is also an option to allow the YouTube clip to play in a loop.



- **An embedded URL/HTML text.**

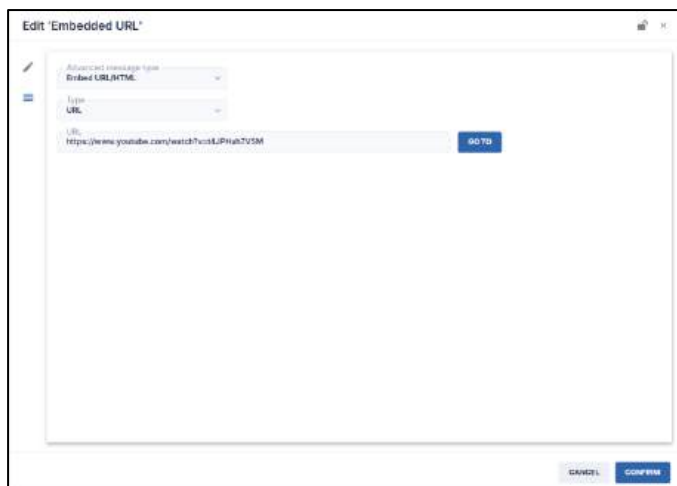


Figure 6-3: Embedded URL option

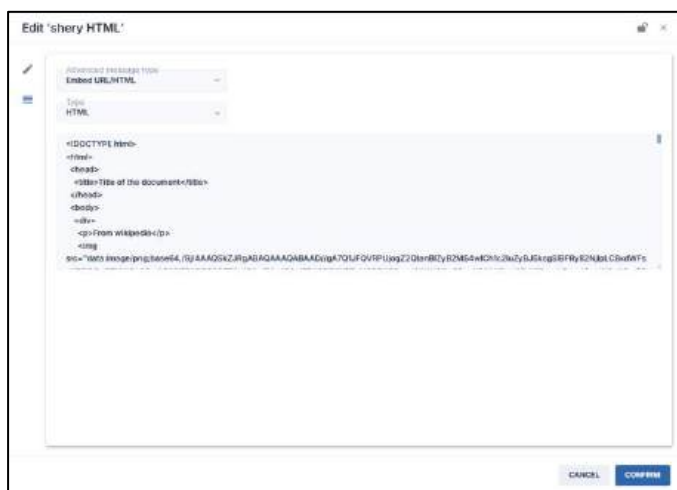
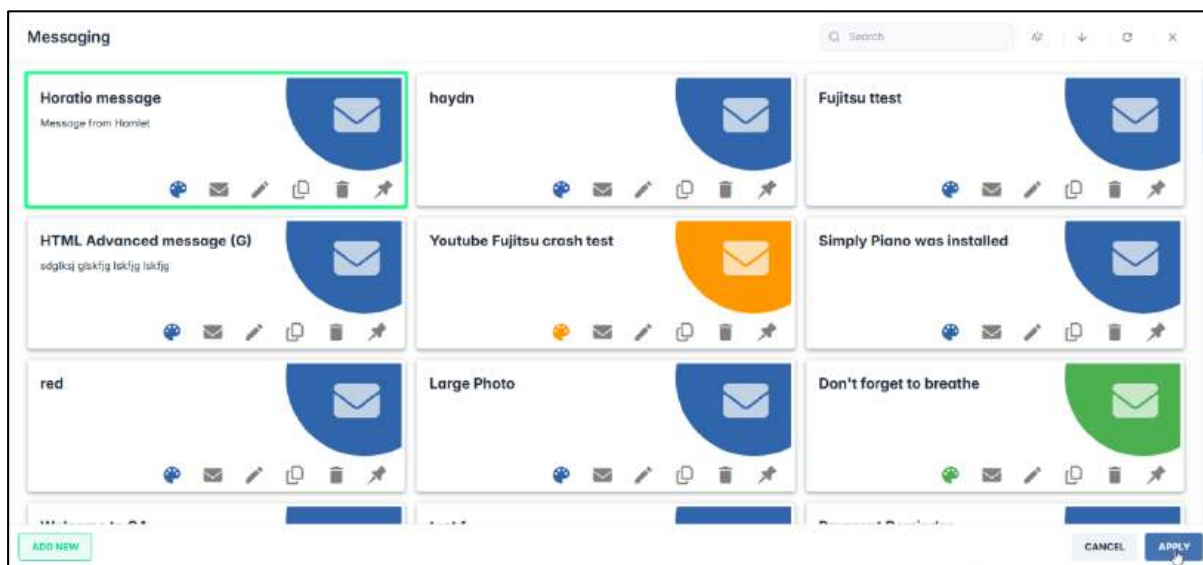


Figure 6-4: Embedded HTML option

10. Click **Confirm** to finalize your message. The Advanced message will appear among the Advanced Messaging options.



11. Select the message and click **Apply**. The message will be displayed on the device.

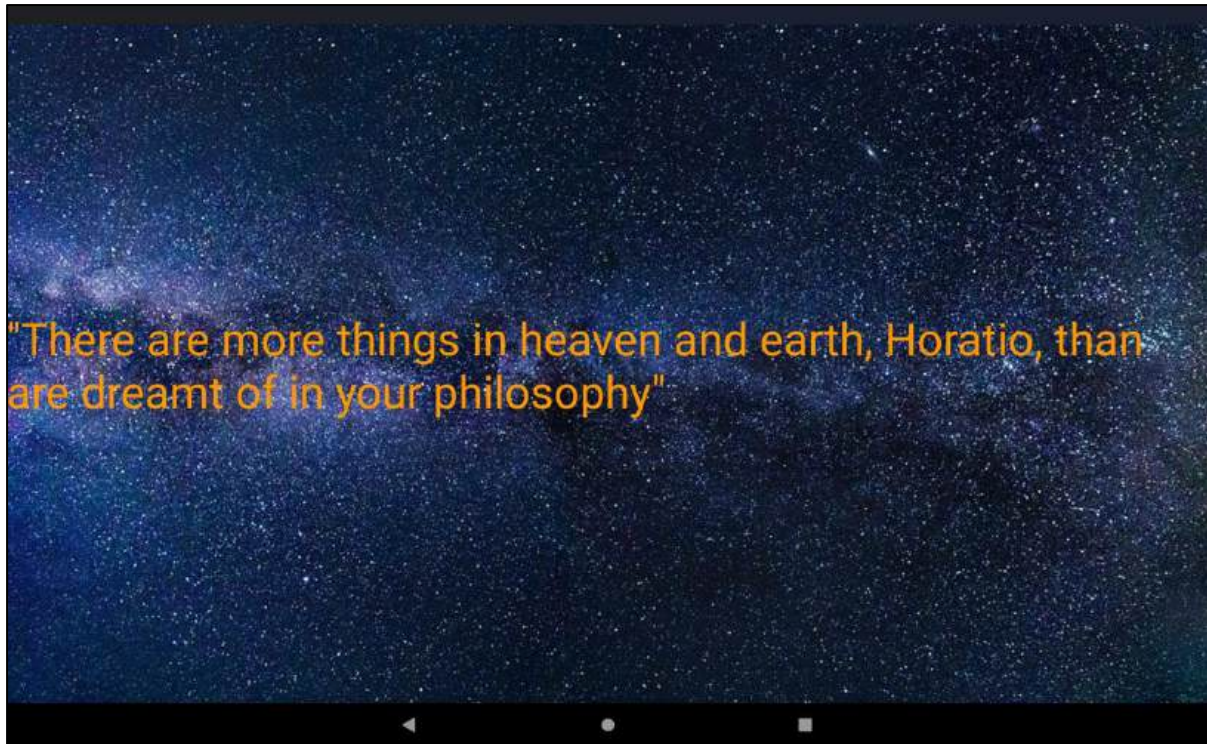


Figure 6-5: Display of an Advanced Message on the remote device

6.1.2 Android for Work (AFW) install/uninstall

Android for Work (also known as “Android Enterprise”) is a feature that allows you to use your personal Android device for work purposes, by setting up a separate device template just for business use. This helps ensure security of work-related apps and data.

Note: In order to install apps on a remote Android device using the AFW install command, you must enroll the device in Android for Work. This is discussed in **Section 5.2.1.1, Enrolling Android Devices**. If a device has been enrolled in AFW properly, you will see the **AFW install/uninstall** option in that device’s Device Dashboard.

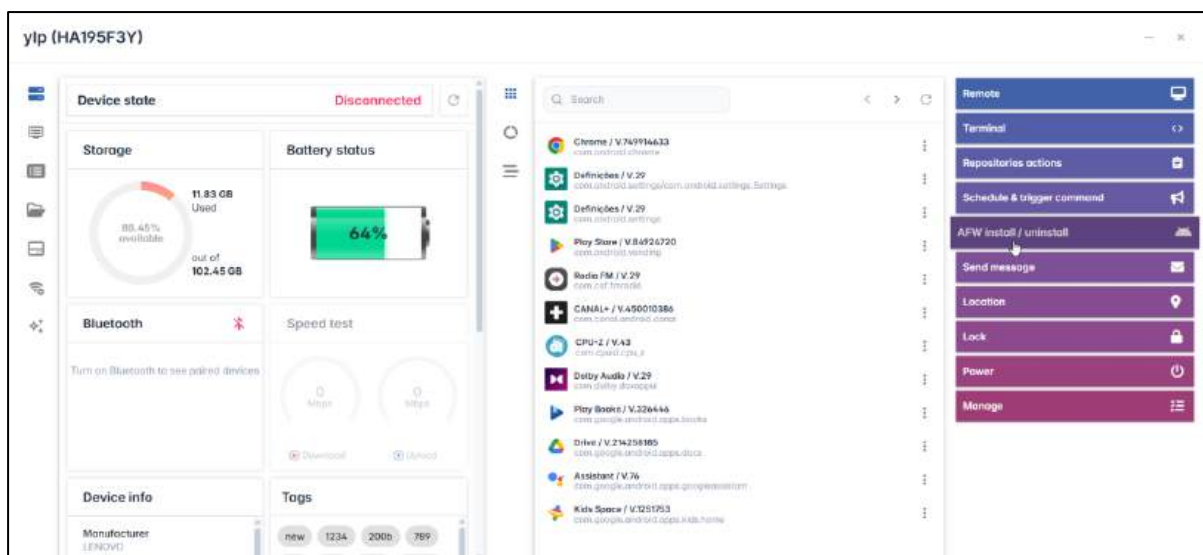


Figure 6-6: The “AFW install/uninstall” command appears in the Device Dashboard

Once you have properly registered in the Android for Work program (as detailed in the chapter on **Account Settings**, in **Section 4.4.3, Android for Work Registration**), you can select apps for specific Android devices using this Radix Device Management Platform feature.

After you have selected apps and policies to be applied to your Android devices enrolled in the Android for Work program as detailed in **Section 7.2.4**, they will appear in the **AFW Install** window:

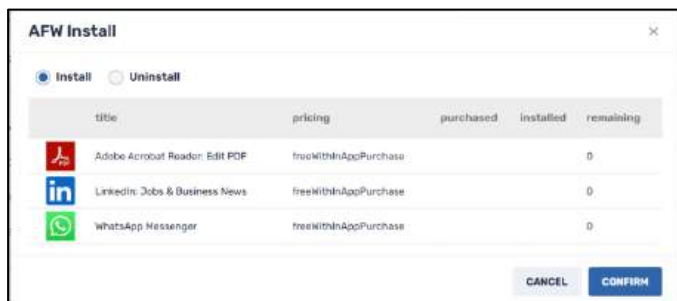
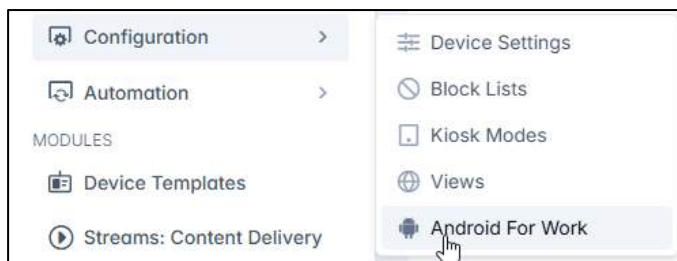
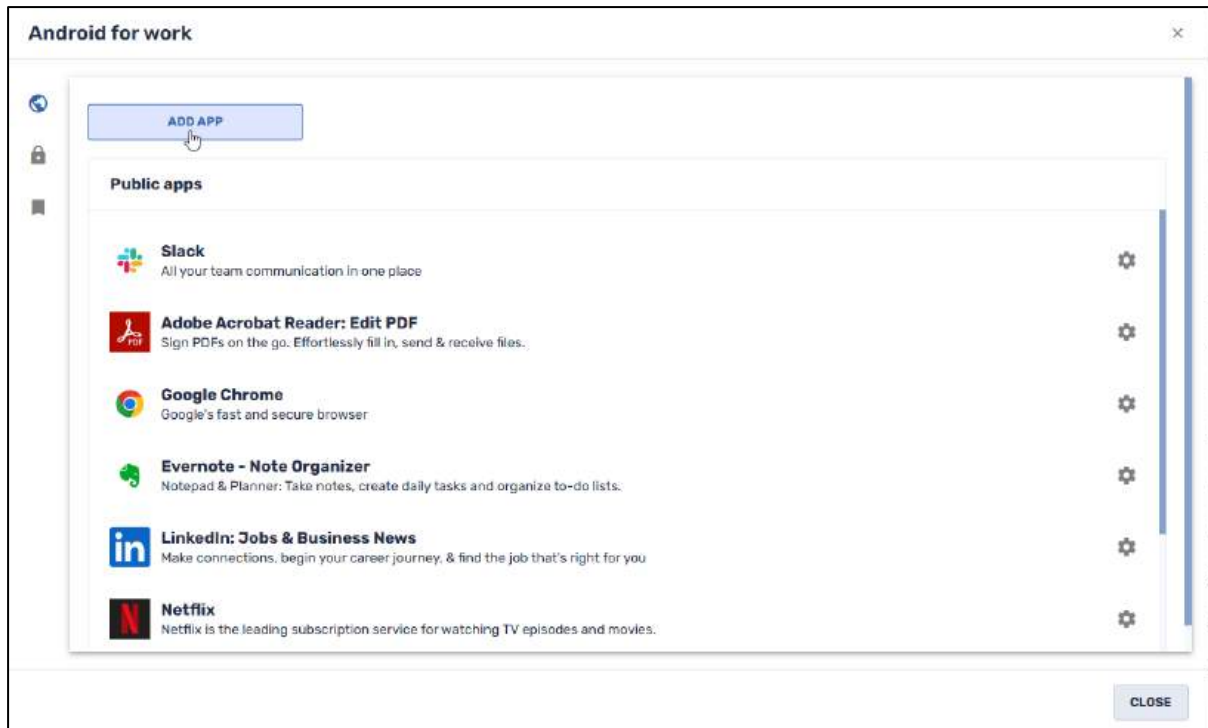


Figure 6-7: Android for Work Install window

As explained in **Section 7.2.4**, click on **Configurations>Android for Work** in the sidebar menu:



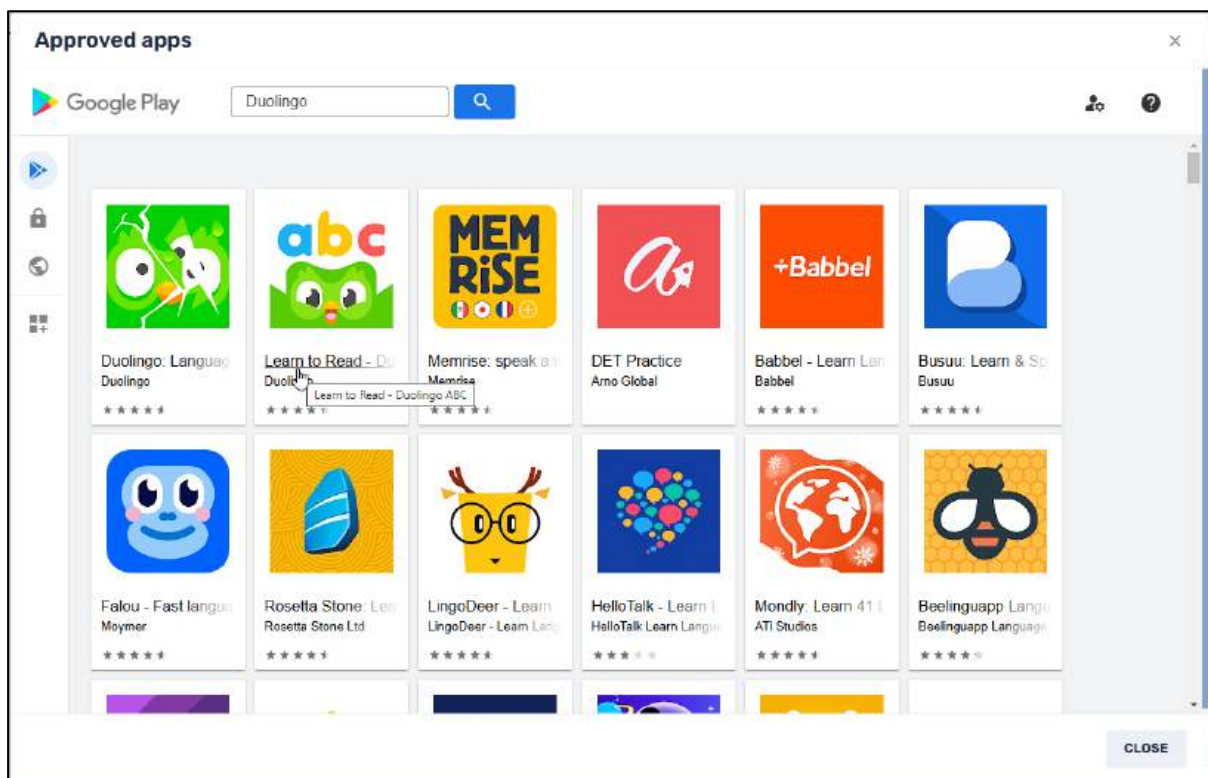
The **Android for Work** app window opens:



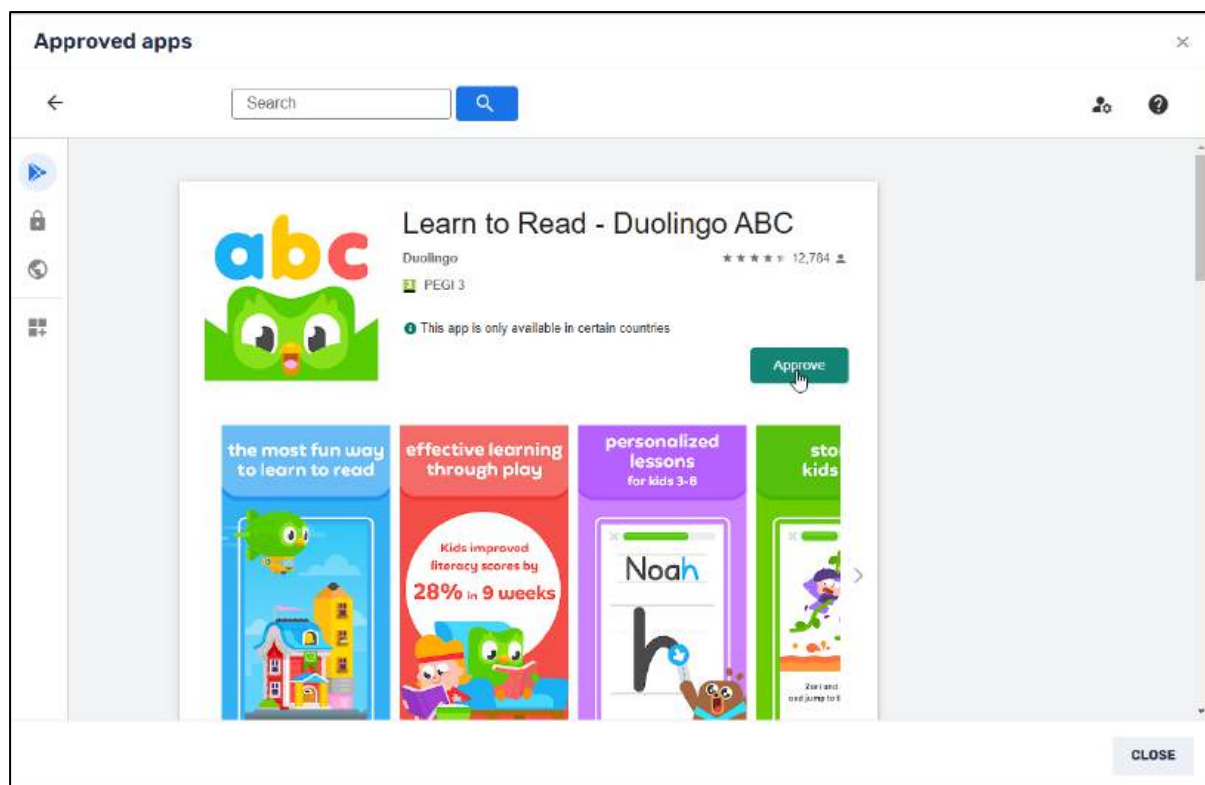
This will give you options to install apps onto devices enrolled in the Android for Work program.

To illustrate, we will select the **Duolingo ABC** app to be installed on our Android device:

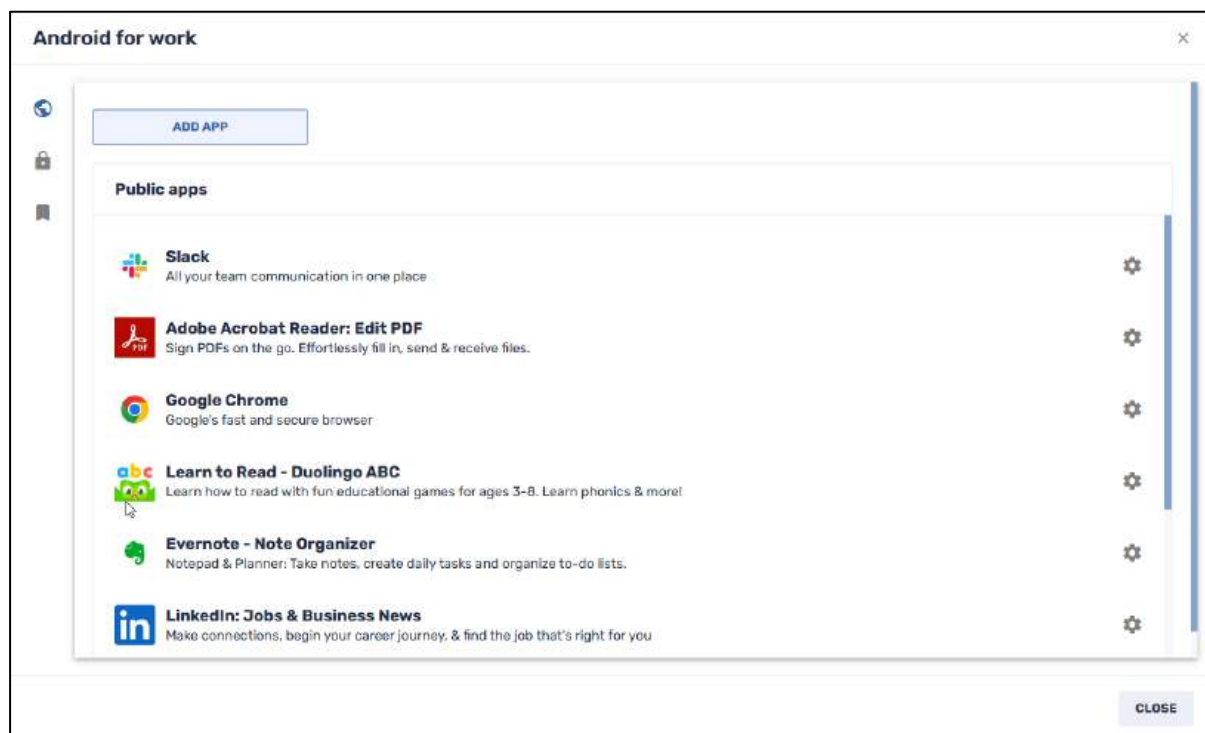
1. Open the **Public apps** window, and click **Add app**.
2. In the **Approved apps** window, search for **Duolingo ABC**.



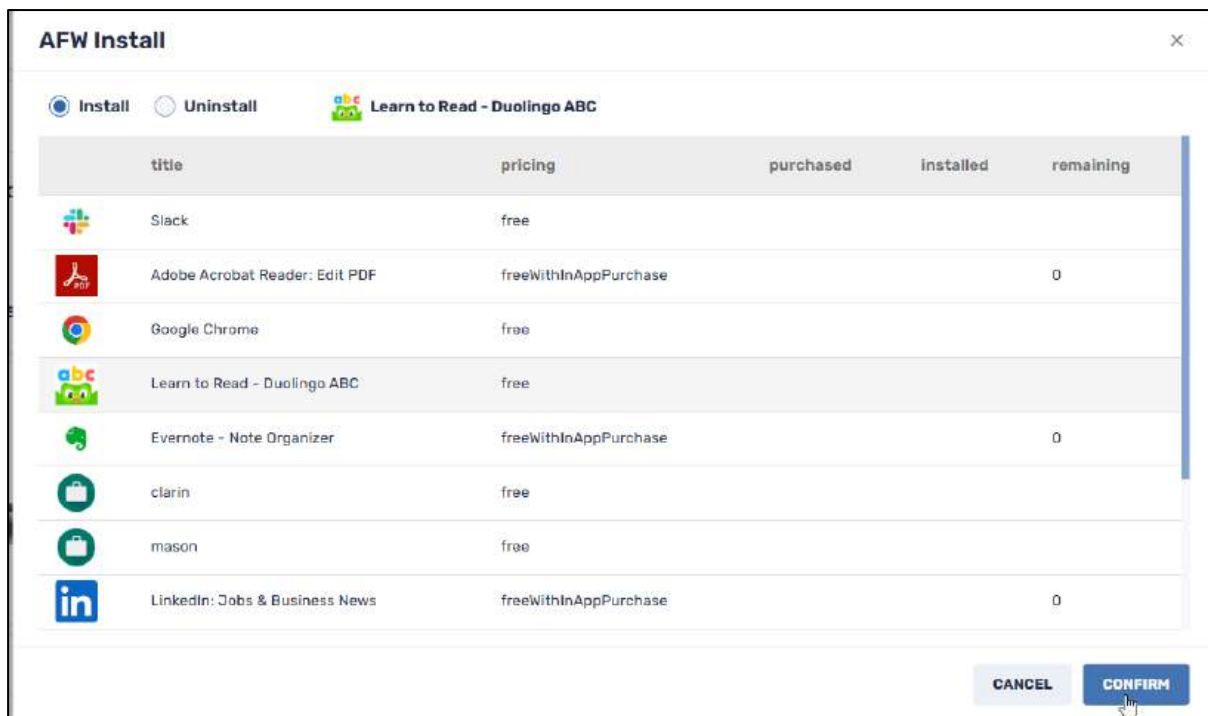
3. Click on the app to select it, and click **Approve**, and then click **Close**.



Duolingo ABC now appears among our options:



4. Go to the **AFW Install/Uninstall** command, select the **Duolingo ABC** app, and click **Confirm**.



Duolingo ABC will now be installed on your Android device.

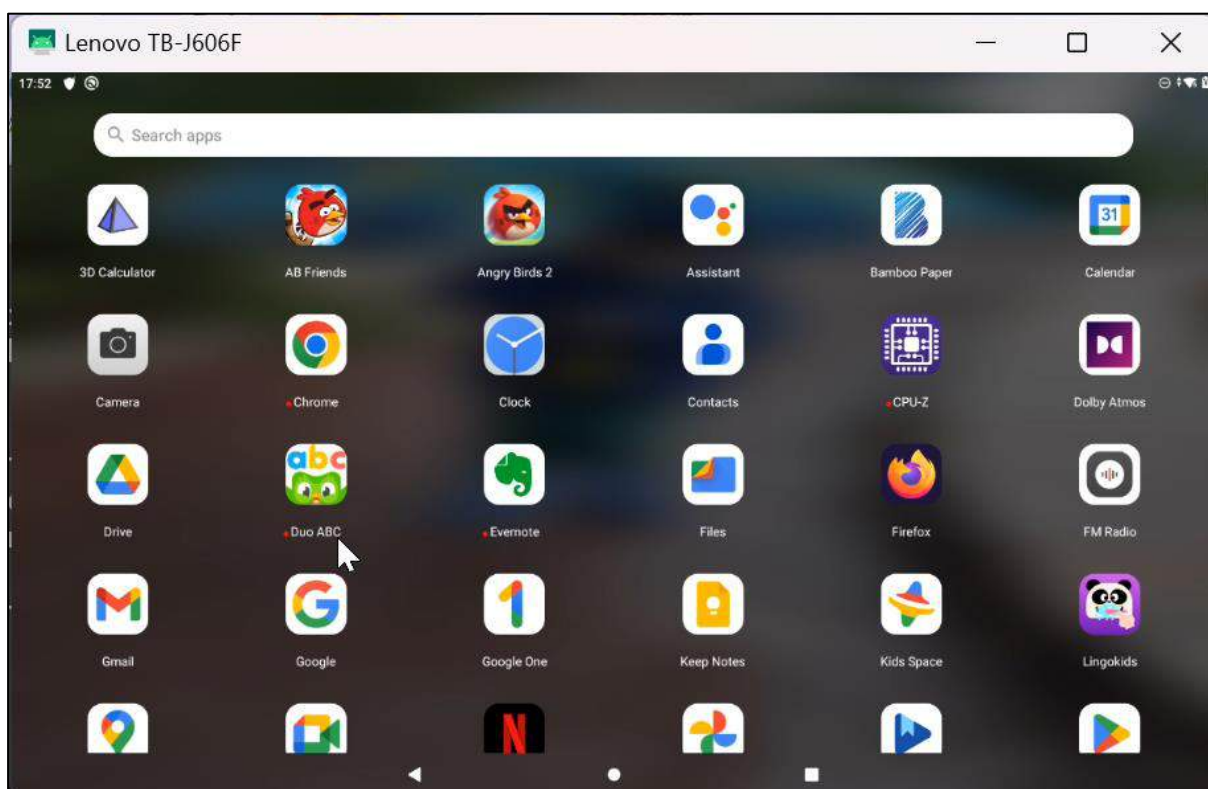
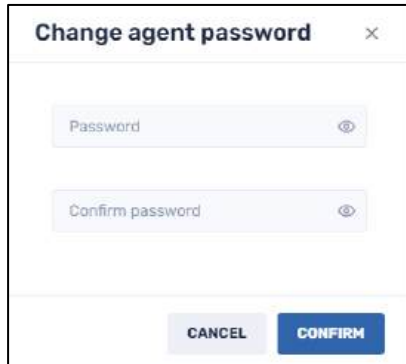


Figure 6-8: The Duolingo ABC app appears on the remote device, after being installed using AFW

Android for Work is described in greater detail in **Section 4.4.3** (about AFW registration) and **Section 7.2.4** (about selecting apps for AFW installation).

6.1.3 Change Agent Password

This allows you to change a user's password on the VISO agent app on their remote device. The remote user will need this password in order to make any changes to the VISO agent app on their device.



A dialog box titled "Change agent password" with a close button (X) in the top right corner. It contains two input fields: "Password" and "Confirm password", each with a toggle icon (an eye) to the right. At the bottom, there are two buttons: "CANCEL" and "CONFIRM".

Figure 6-9: Change Agent Password window

Subsequently, the remote user will have to enter this password when they try to modify the settings on the Viso agent on their remote device:

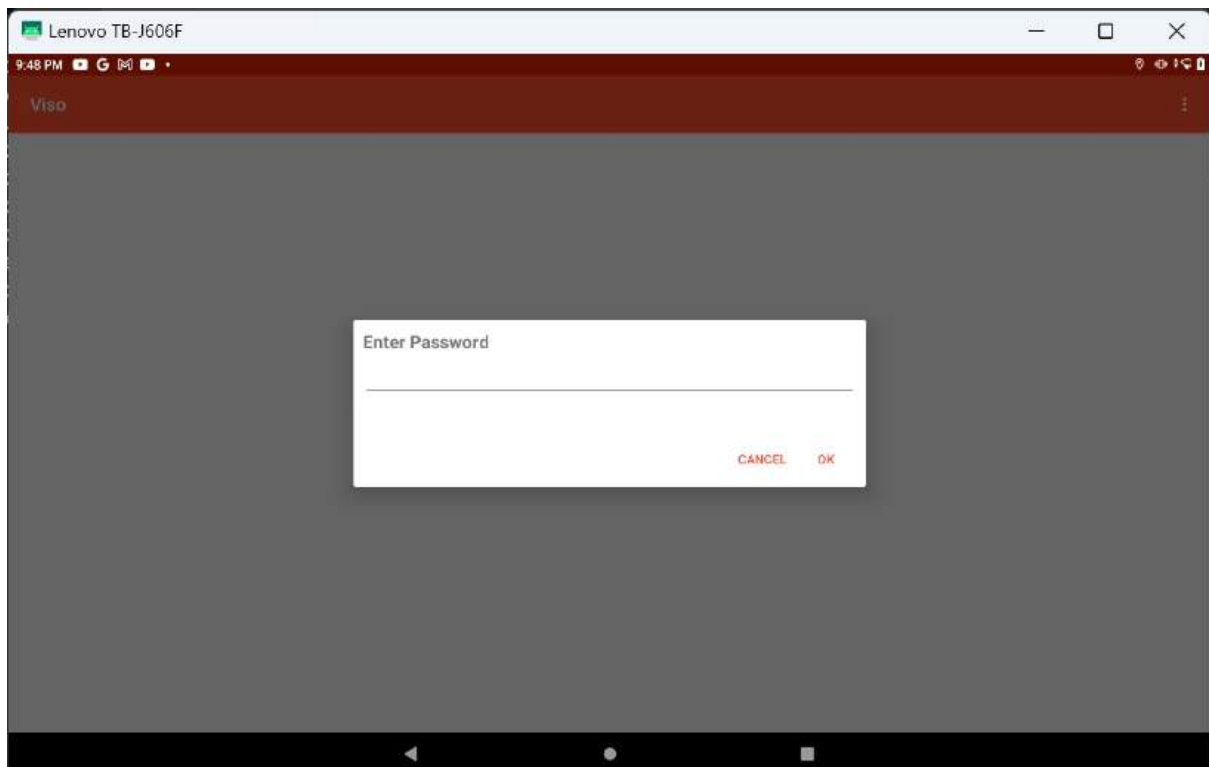
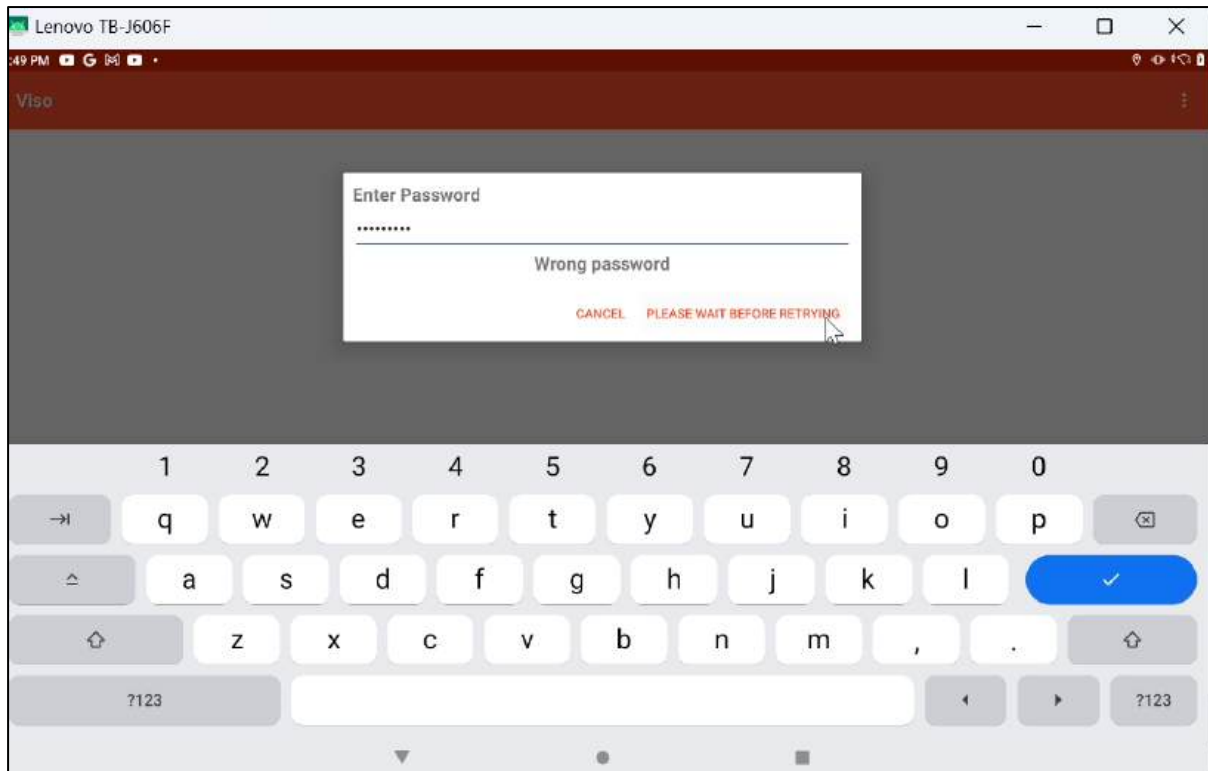
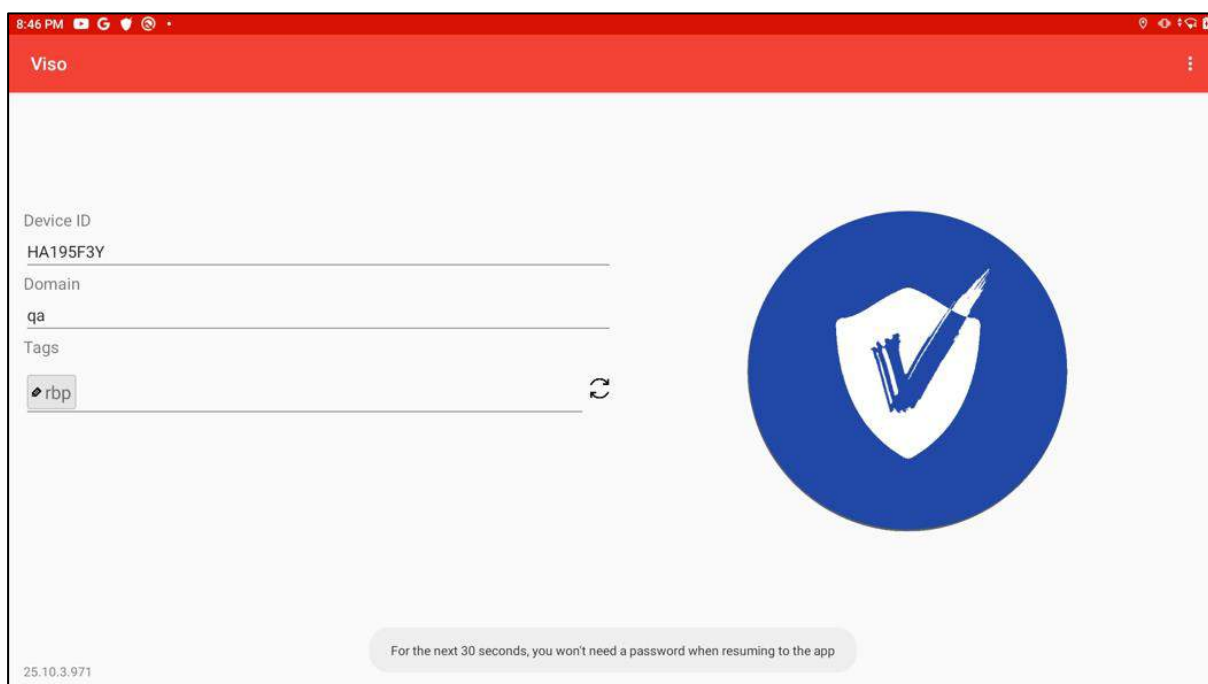


Figure 6-10: Remote device user being prompted to enter the Viso Agent password

If they enter the wrong password, they will receive the following prompt:



Once the remote user enters the password correctly, they will be able to resume use of the Viso Agent app for 30 seconds without having to enter the password again:

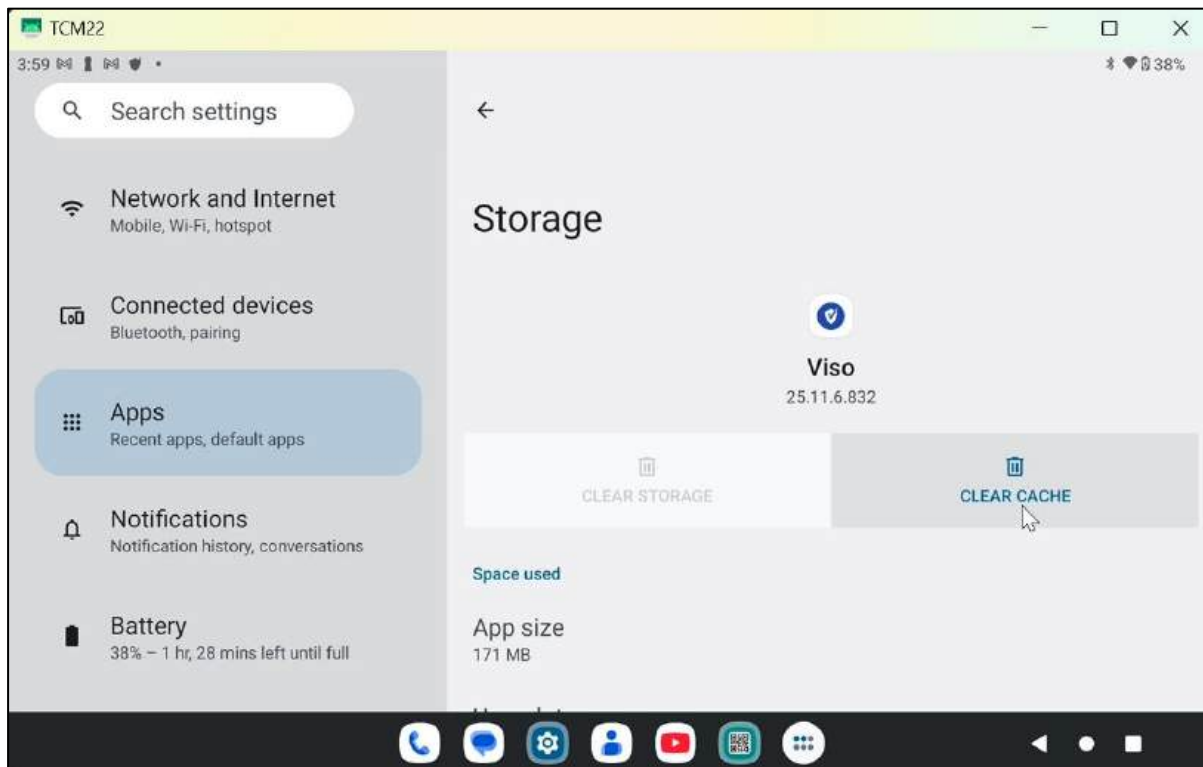


6.1.4 Clear Apps Cache

Clearing the cache for an individual app frees up some storage space on a remote device and improve performance on an app that is malfunctioning or even crashing. The **Clear apps**

cache command will clear the data cached by the specific apps installed on the device. This is a preliminary step to try, when encountering performance issues.

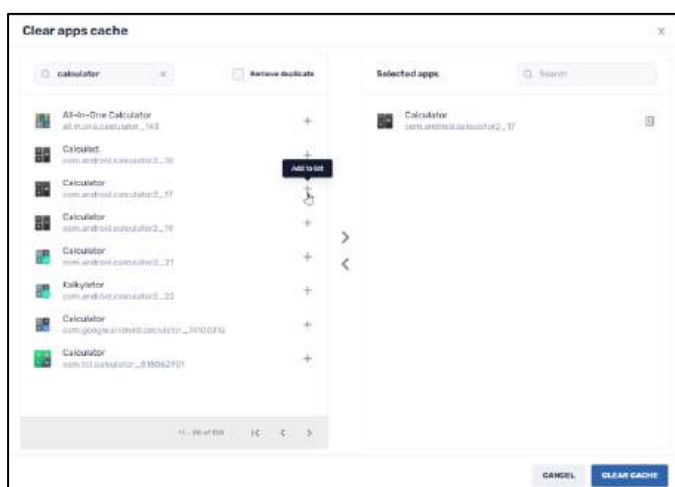
The remote users can clear the apps cache on their Android devices by going to **Settings>Apps & notifications>Selecting the problematic app>Storage>Clear cache**.



However, using the Radix Device Management Platform command can allow clearing the cache for many apps, on many devices simultaneously.

Note: If the selected apps on the device are still not working properly, you can continue with the **Clear Apps Data** command in the [next section](#), which removes all app data on the device.

When you click on the **Clear apps cache** tile, the **Clear apps cache** panel opens.



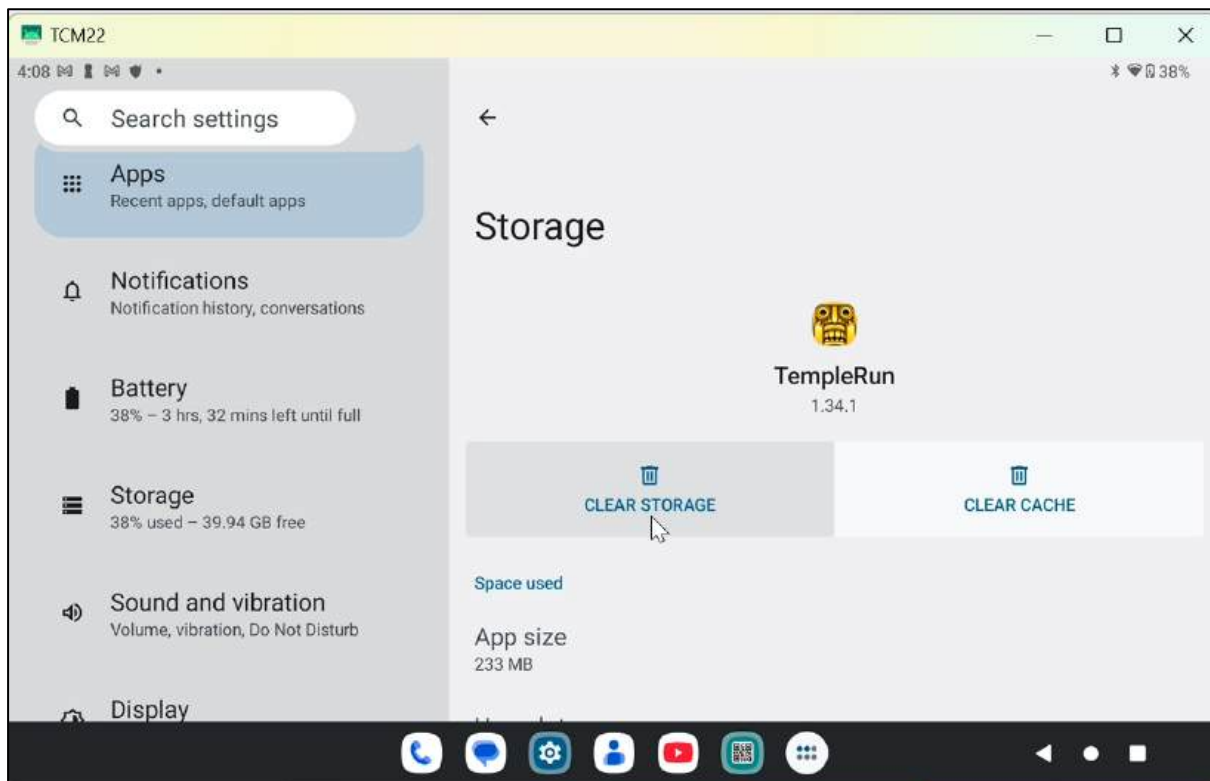
1. Select a particular app by clicking on the **Add** icon **+**. The app will now appear in the right-hand column of Selected apps.

- After you have selected the desired apps, click **Clear cache**. This clears the cached data on the device.

6.1.5 Clear Apps Data

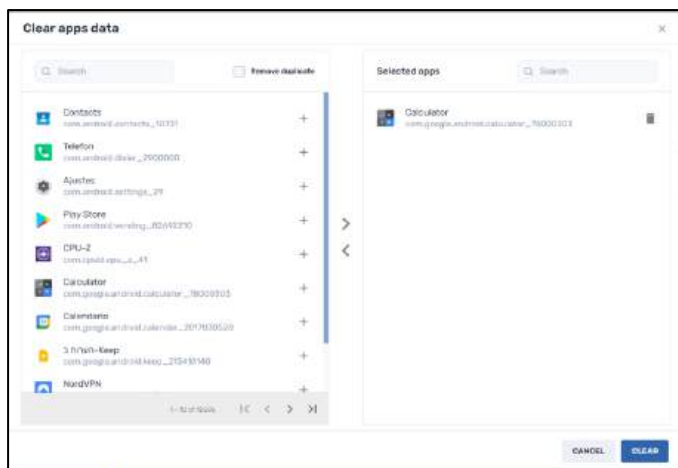
This is useful in situations where an app is crashing or displaying other issues. **Clear apps data** will clear the user's history on the device and require them to log in again. This typically will solve most performance issues.

As with the Clear Apps Cache command, you can perform this command on an individual remote device from **Settings>Apps & notifications>Selecting the problematic app>Storage>Clear storage**.



The Radix Device Management Platform command will allow you to do this on many devices simultaneously.

When you click on the **Clear apps data** tile, the **Clear apps data** panel opens.



1. Select a particular app by clicking on the **Add** icon **+**. The app will now appear in the right-hand column of Selected apps.
2. After you have selected the desired apps, click **Clear**. This clears any data on the device.
For example, if you select the **Calculator** app, it will remotely clear the calculator display on the device, and close the app.

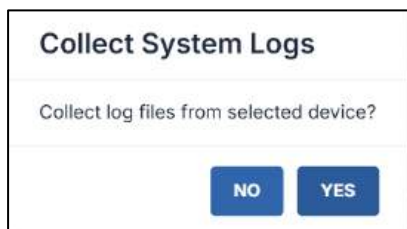
6.1.6 Collect System Logs

This allows you to create a log file of activities performed on a remote device.

This option is available from:

- The Bulk Actions button, or
- The device's three-dot menu.

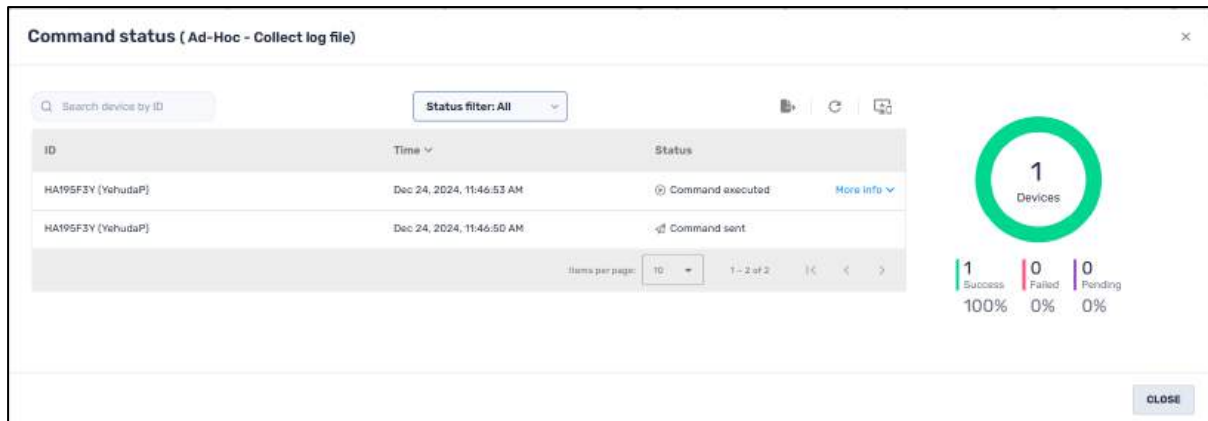
1. When you click on **Collect system logs**, the **Collect System Logs** dialog box opens, asking if you want to collect activity logs from the selected device.



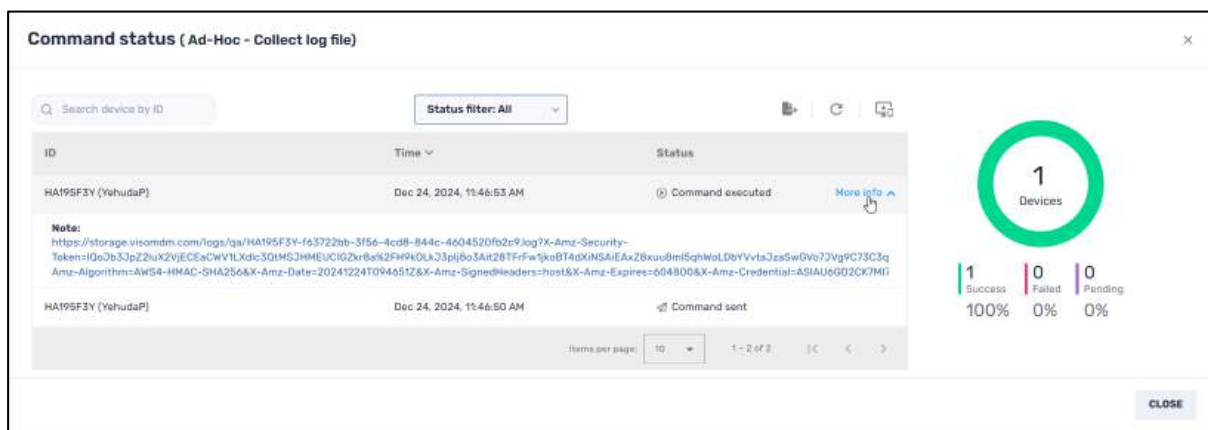
2. If you click **Yes**, a confirmation that the command was sent will appear in the lower right corner, and a notification will appear in the lower left corner, indicating if the log file was created successfully. If you performed the command on a number of devices, the number of devices will appear in parentheses.



3. Click on the notification, to open the **Command Status** window.



4. When you click on **More info**, you will receive a clickable link of the log file.



5. Click on the link to download the log file to your computer. Alternatively, you can right-click on the link to copy it to the clipboard, and then paste it into a browser tab. This will also download the log file. The log file will be in *.txt format.

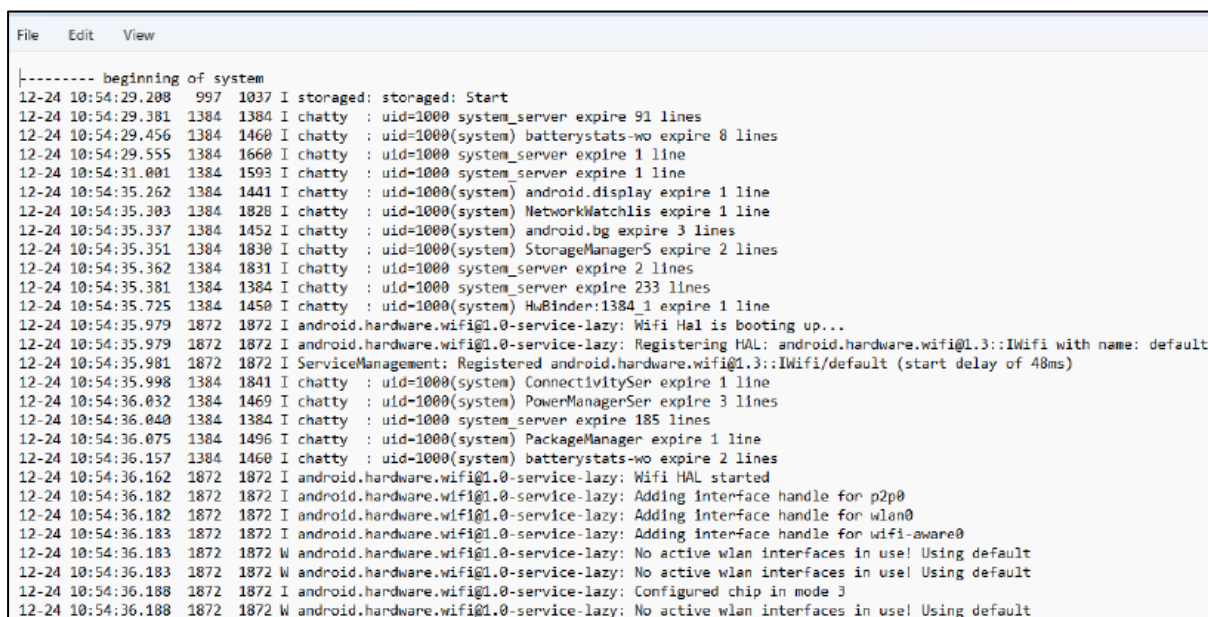


Figure 6-11: Typical log file

If you want to collect logs from several devices, you can check the checkboxes for the devices in the Devices Table, and then click on **Bulk Actions>Device>Collect System Logs**. In the example below, logs will be collected from three devices.

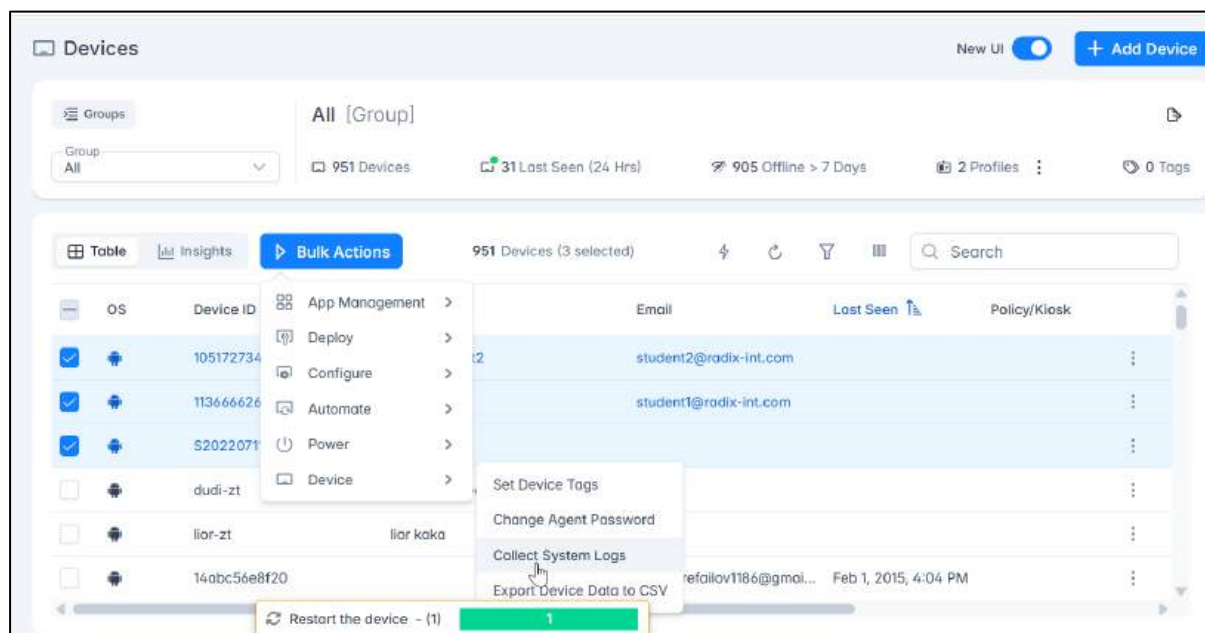


Figure 6-12: Collecting logs from several devices

6.1.7 Commands & Scripts

See **Section 6.1.23, Remote Execute/Commands & Scripts**.

6.1.8 Device Settings

This option allows the Radix Device Management user to remotely adjust a device's settings. This could include selecting a type of keyboard, enabling or disabling a screen saver, or performing a reset on the device.

When you click on the Device Settings icon, the **Device Settings options** window opens:

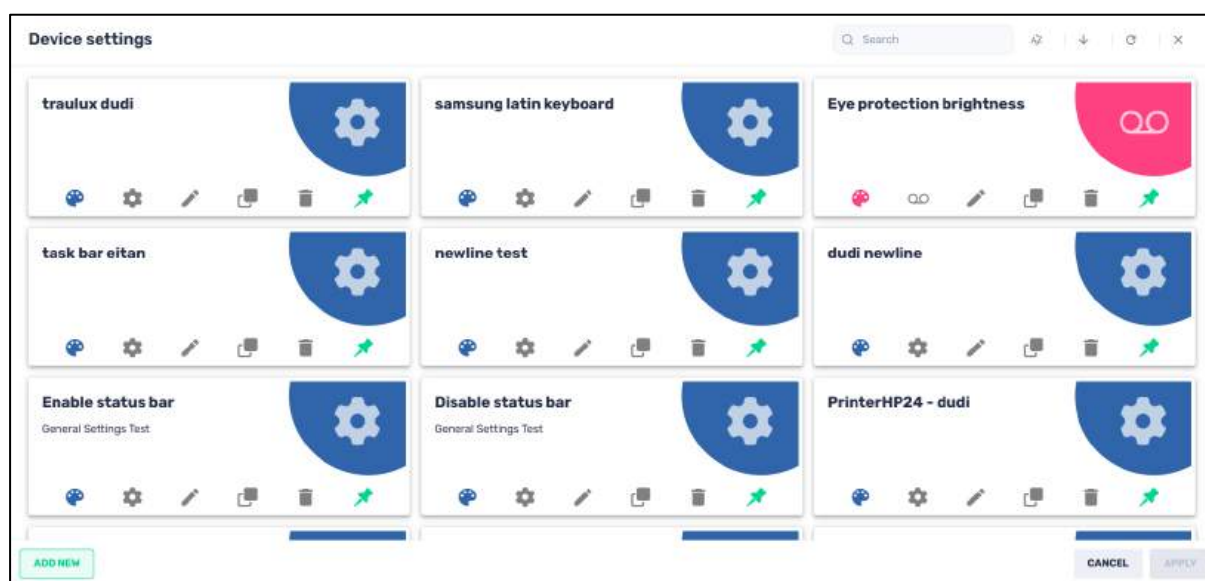


Figure 6-13: Device Settings options

You can add more options as well, with the **Add New** button. To add a new device setting, you will have to provide the connectivity details of the remote device.

To add a new device setting tile:

1. Click on **Add New** in the Device Settings screen.

The “New Setting” screen opens, in **Edit Details** mode.

Figure 6-14: New Device Settings screen

The icons on the left-hand side of the screen have the following functions:

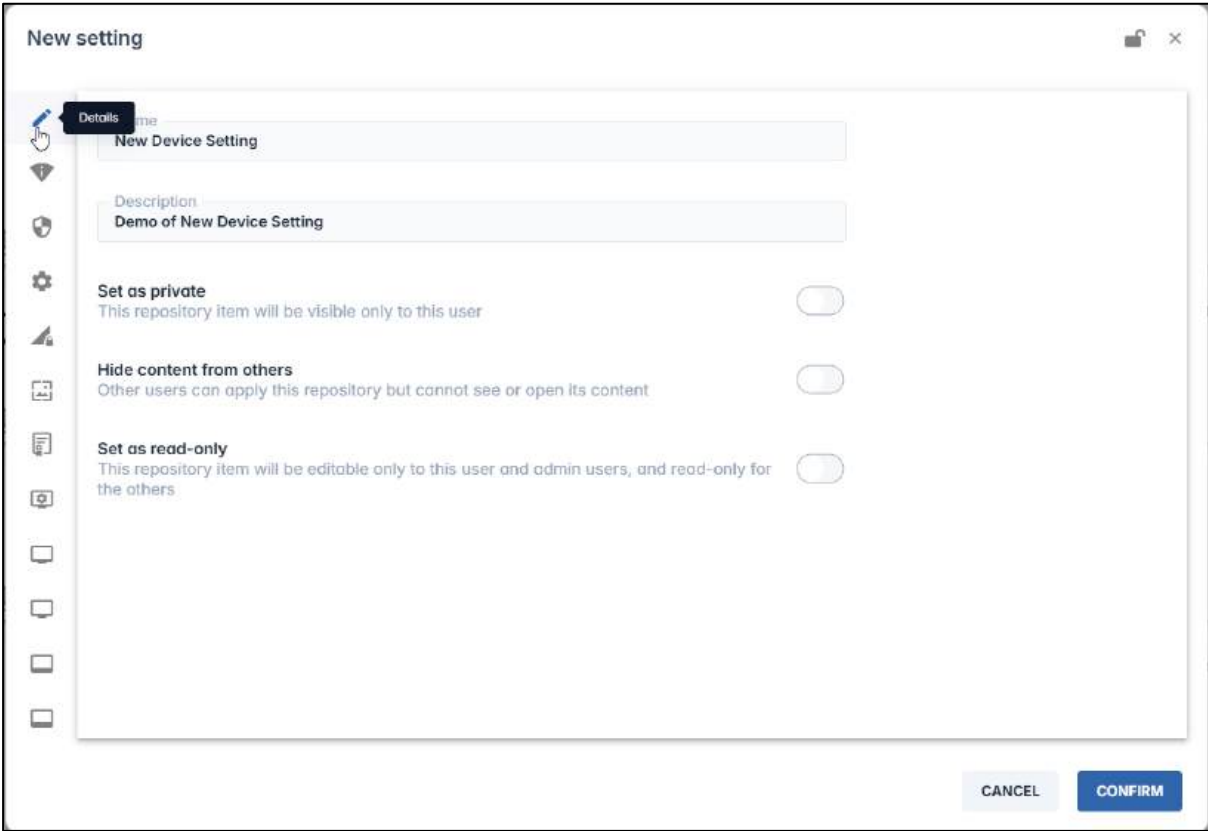
Table 6-1: Device Settings Options

Icon	Description
	Edit Details
	Wi-Fi
	Security
	General
	Set APN
	Wallpaper
	Install Certificate

	Panel Settings (for specialized use)
	Smartboard Settings (for specialized use)
	App Permissions (for specialized use)
	App Configurations (for specialized use)

6.1.8.1 Edit Details

This allows you to provide a name and description of the Device Setting, as it will appear in the grid of settings.



There are two additional options to limit who can view and edit this device setting:

- **Set as private option:** Click on the **Set as private** button if you want this new device setting option to be visible only to you (the creator of the item) when you log in to the Radix Device Management Platform.
- **Hide content from others:** Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
- **Set as read-only option:** Click on this if you want to restrict who will be able to modify the details of this device setting. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .

6.1.8.2 Wi-Fi

This opens a pane to set the device's Wi-Fi connectivity details.

The screenshot shows a 'New setting' dialog box with a sidebar on the left containing various device management icons. The 'Wi-Fi' icon is selected and highlighted with a dark blue background. The main content area is titled 'Set device wifi' and features a toggle switch in the top right corner that is turned on. Below the title, there are several configuration fields: 'Select type' with a dropdown menu showing 'Manual'; 'Service Set Identifier (SSID)' with a text input field and a help icon; 'Authentication type' with a dropdown menu showing 'WPA2'; 'Password' with a text input field, a help icon, and an eye icon for toggling visibility; 'Encryption type' with a dropdown menu showing 'AES'; 'Hidden' with a toggle switch; 'Auto Join' with a toggle switch; and 'Forget wifi' with a toggle switch. At the bottom right of the dialog, there are two buttons: 'CANCEL' and 'CONFIRM'.

You can also choose an option to “forget” the Wi-Fi connection:

Edit 'Forget WiFi - Mintz'

Set device wifi ☐

Forget wifi ☒

Service Set Identifier (SSID)
Robo\$\$\$\$

CANCEL CONFIRM

6.1.8.3 Security

This allows you to adjust login settings for the device, such as password length, password history, number of login attempts allowed, and the like.

New setting

Maximum number of login attempts that are allowed before the device wipes itself

Set the maximum time for user activity until the device will lock, this limits the length that the user can set

set the password expiration timeout

Set the length of the password history

Set the minimum allowed password length

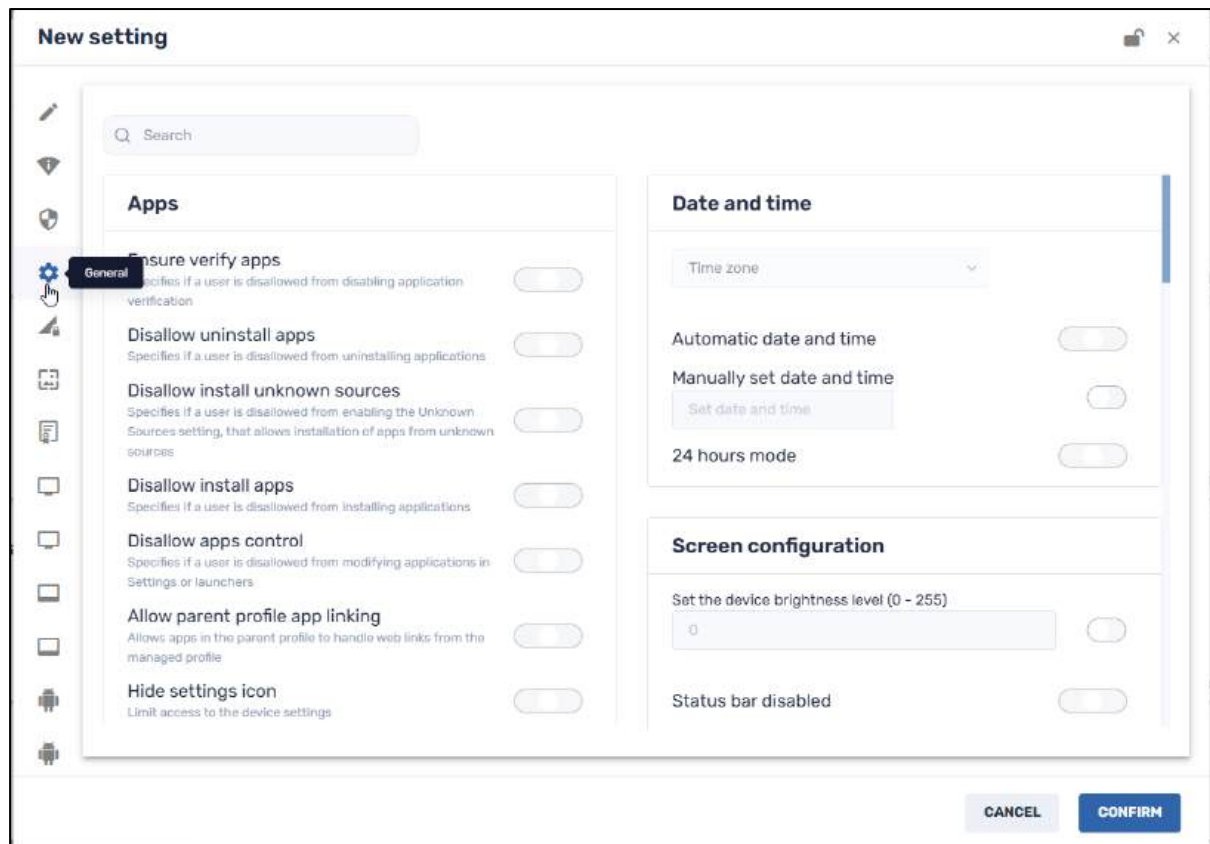
Set the minimum number of letters required in the password

Set the minimum number of lower case letters required in the password

CANCEL CONFIRM

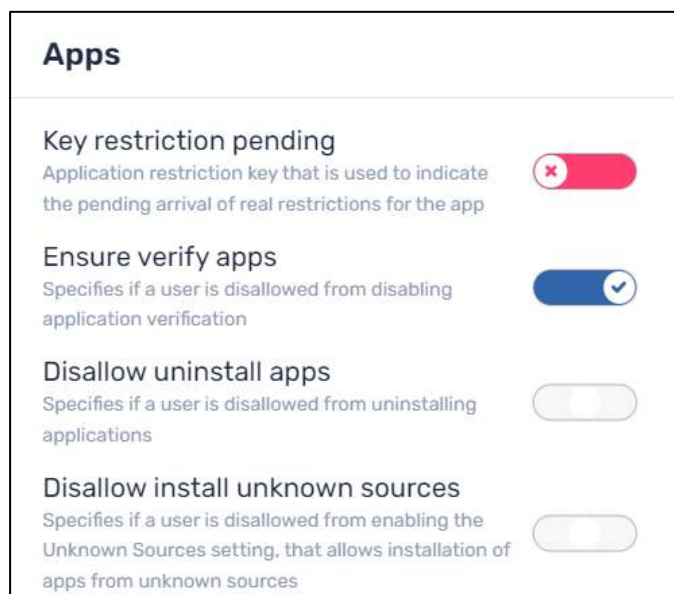
6.1.8.4 General Settings

This is an interactive table where you can modify the device's settings regarding apps, users, connectivity, date & time, audio settings, and more.



Note that the buttons in the General Settings window have three modes:

- **Enable** (Blue)
- **Neutral** (Gray, meaning that this settings item is ignored, and the device remains on its current setting)
- **Disable** (Red):



6.1.8.5 Set APN

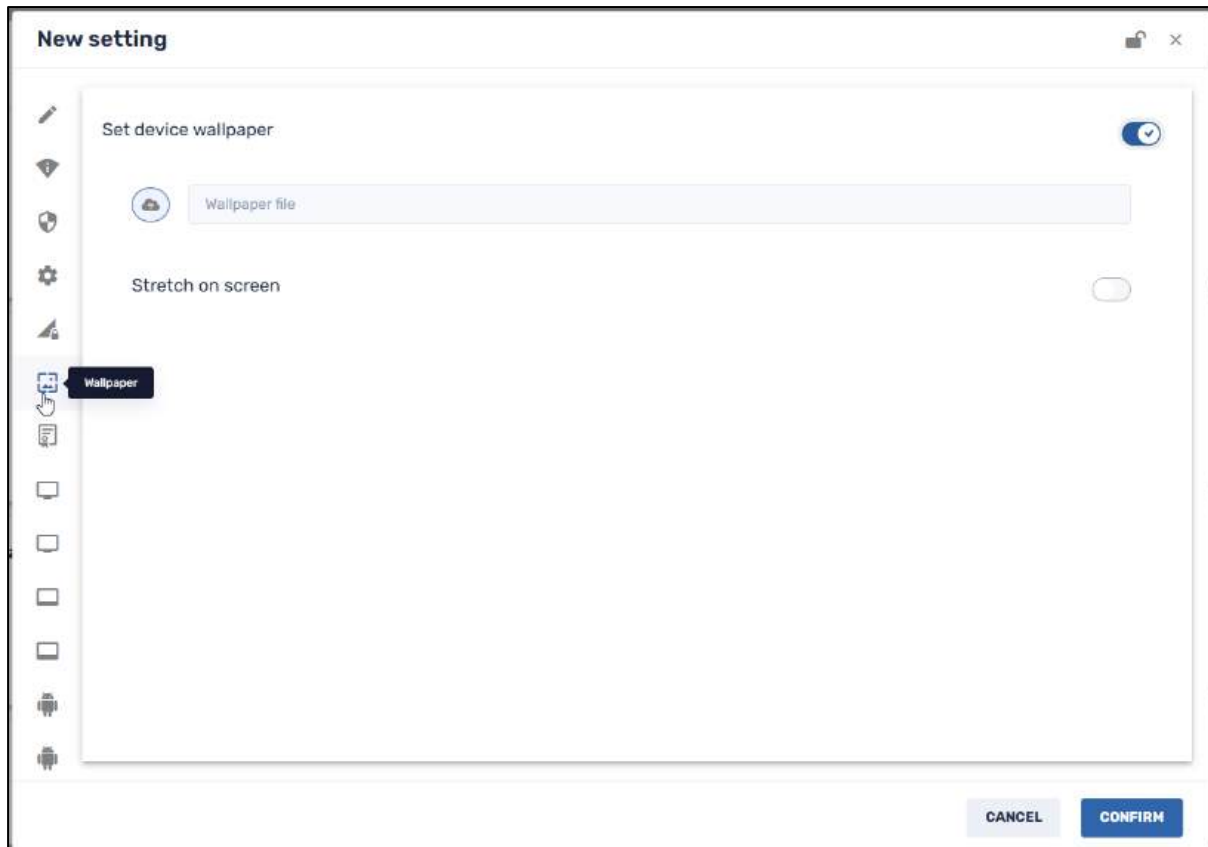
This screen allows you to set up the details of an Access Point Name (=APN), such as an MNC (= Mobile Network Code), an MCC (= Mobile Country Code), and MMSC (=Multimedia Messaging Service Center).



The screenshot shows a 'New setting' dialog box with a title bar containing a lock icon and a close button. On the left is a vertical sidebar with various system icons. The main area is titled 'Set Apn' and includes a toggle switch in the top right corner. Below the title are five text input fields labeled 'Name', 'Apn', 'MCC', 'MNC', and 'MMSC'. A 'Type' label is positioned below the 'MMSC' field. At the bottom right of the dialog are two buttons: 'CANCEL' and 'CONFIRM'. A tooltip labeled 'APN' is visible over the 'MCC' input field.

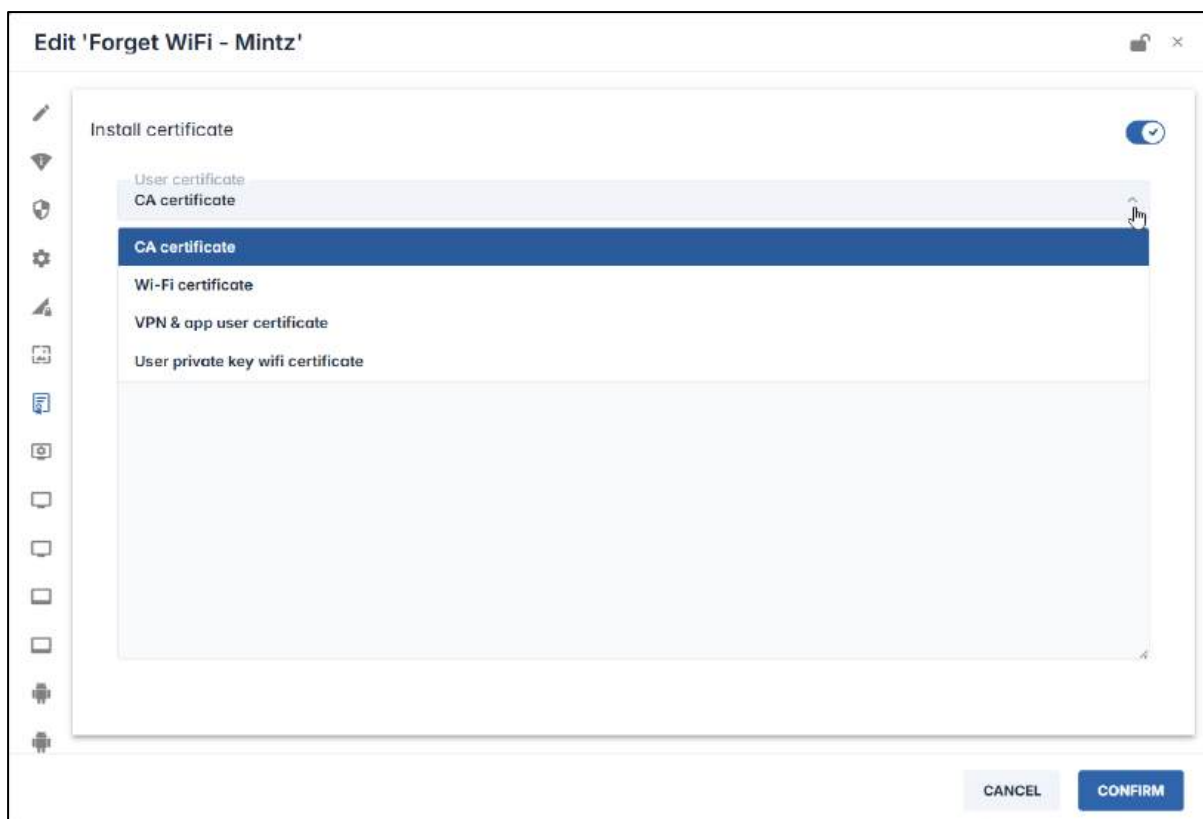
6.1.8.6 Wallpaper

This allows you to change the wallpaper on the device. You select an image from your computer and click **Confirm**.



6.1.8.7 *Install Certificate*

Certificates are used for web filtering, VPN authentication, and many other uses. These device settings options on the Radix Device Management interface allow you to install VPN and app certificates.



The options are as follows:

- CA (=Certificate Authority) certificate
- Wi-Fi certificate
- VPN and app user certificate
- User private key Wi-Fi certificate

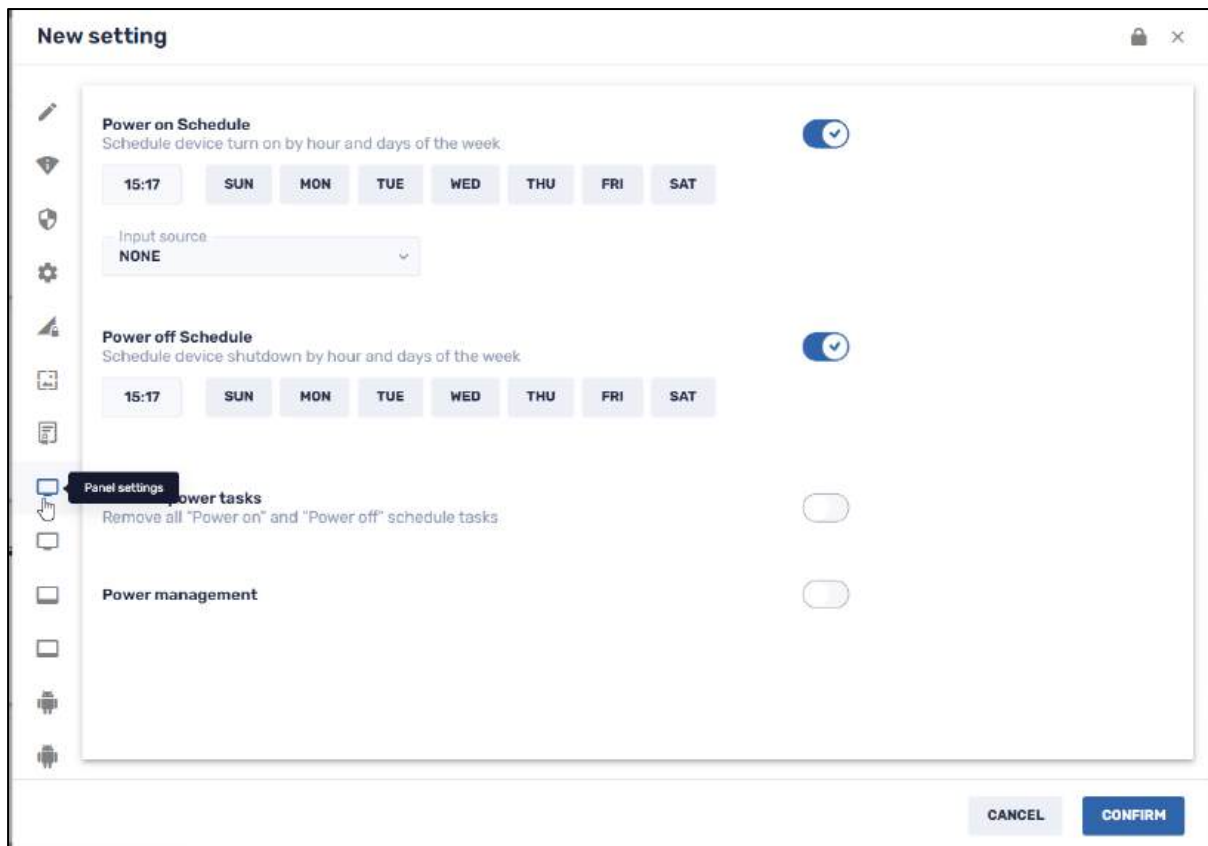
To install a certificate:

1. First obtain a VPN or app certificate.
2. Copy the entire text of the certificate.
3. Paste it into the **Certificate body** field and click **Confirm**.



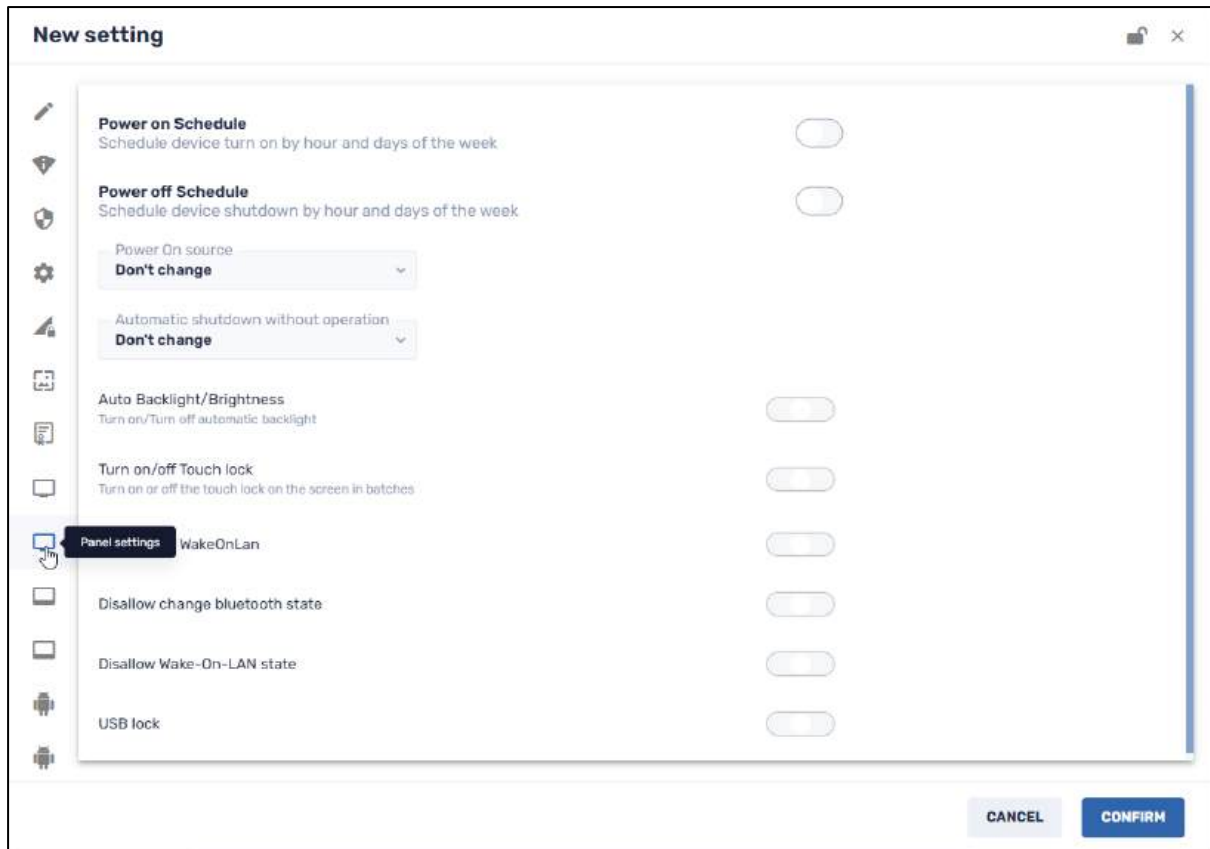
6.1.8.8 Panel Settings---First Panel (For Specialized Use)

The first Panel Settings panel has options to power up or power down your flat panel device, and other power management options.



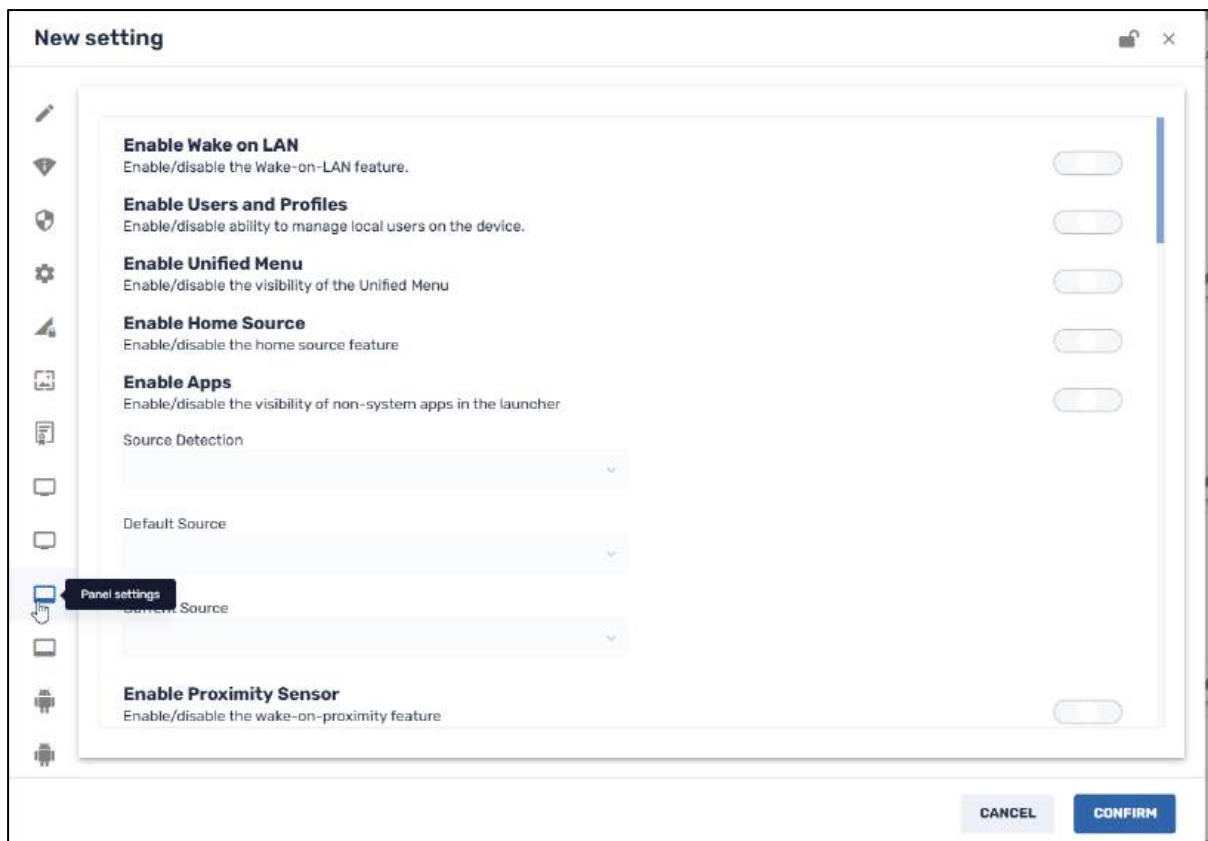
6.1.8.9 Panel Settings—Second Panel (For Specialized Use)

The second Panel Settings panel has additional device settings options for other flat panel devices, such as being able to lock the touch lock on the device, allowing or disallowing the Wake-On-LAN option, and more.



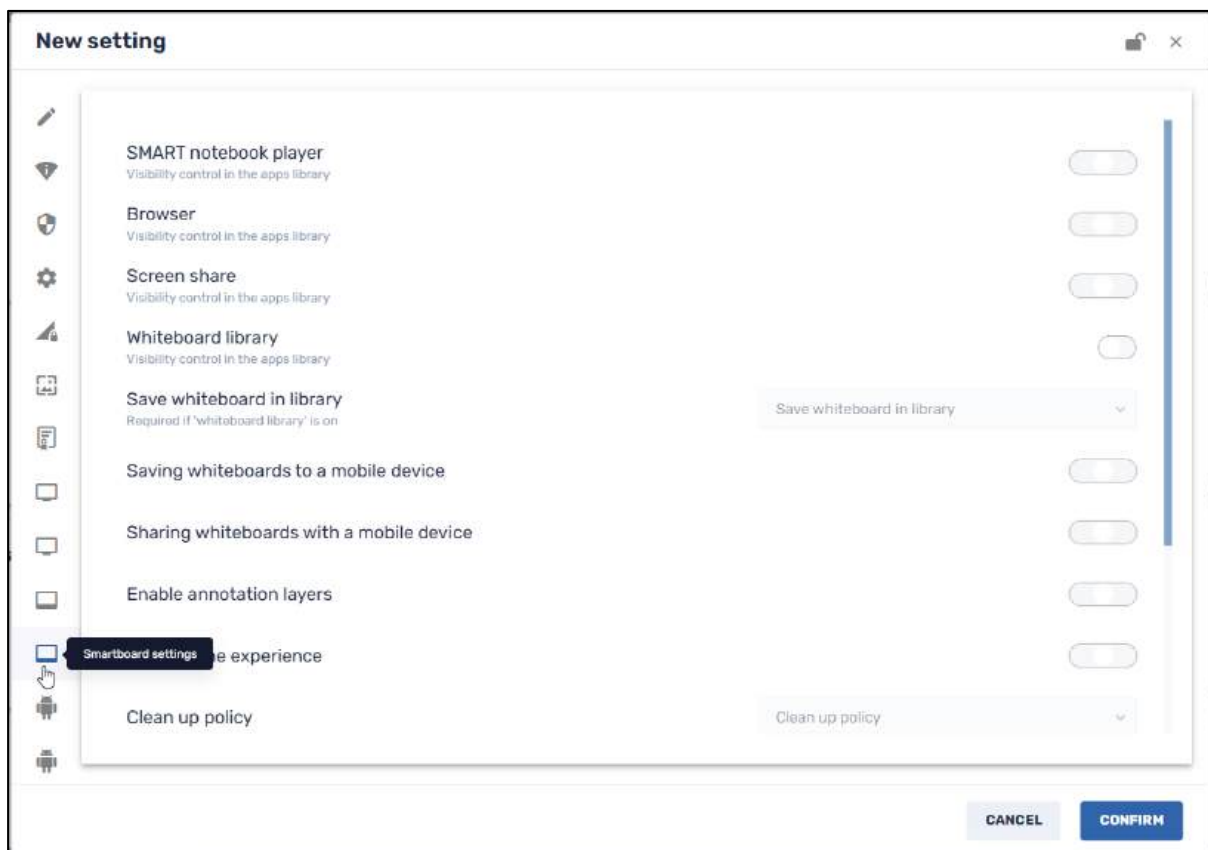
6.1.8.10 Panel Settings—Third Panel (For Specialized Use)

This has more specialized settings for smart panel devices, for options such as Wake-on-LAN, panel speaker settings, network settings, and more.



6.1.8.11 Smartboard Settings

These are specialized device settings for smartboard panels.



6.1.8.12 App Permissions/Configurations/Applications settings

These menu options are for assigning permissions and configurations for applications on Android devices.

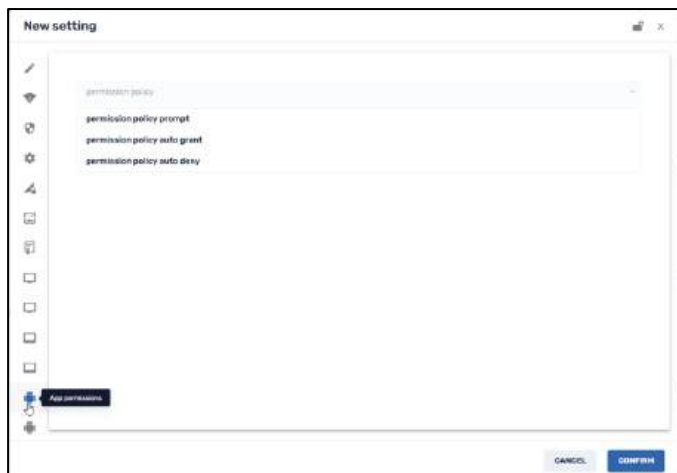


Figure 6-15: App Permissions Settings

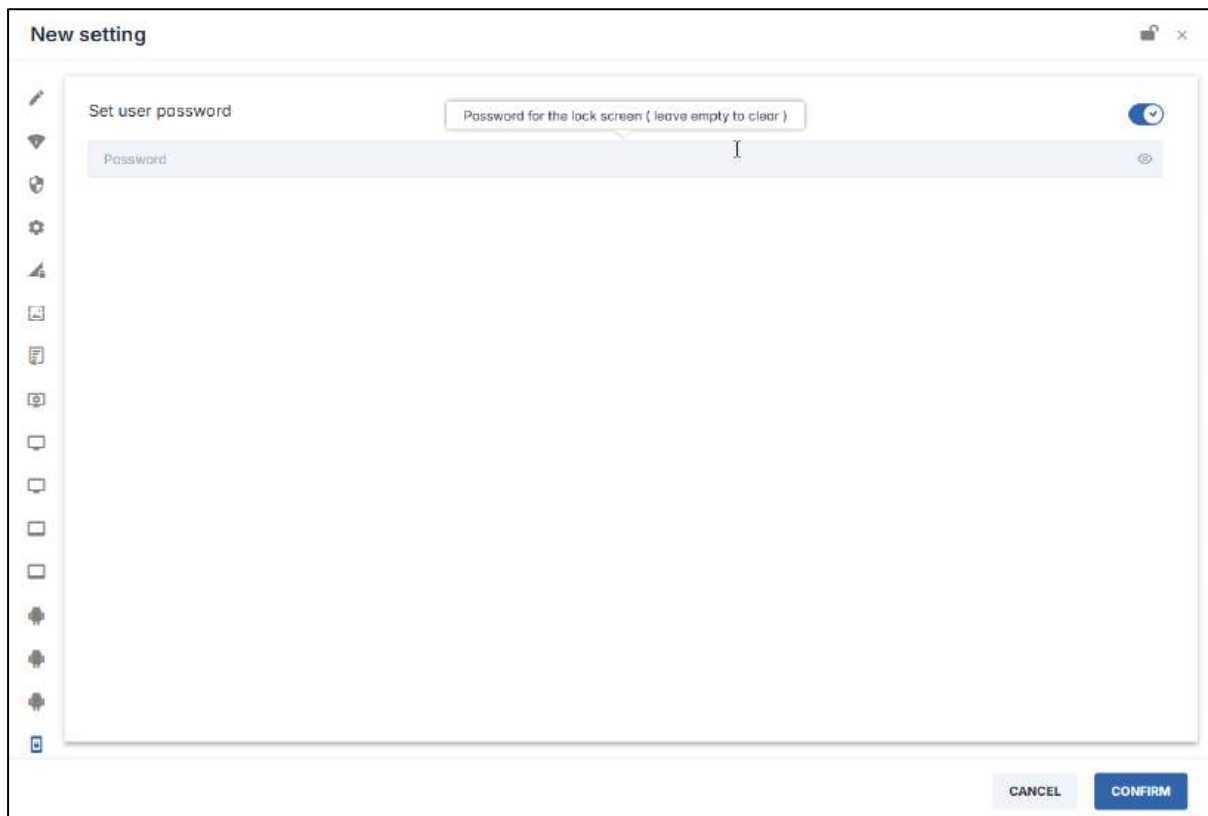


Figure 6-16: App Configuration Settings



Figure 6-17: Available application settings

6.1.8.13 Lock Screen Password



When you apply this setting, the remote user will be prompted to enter the saved password to free up their display.

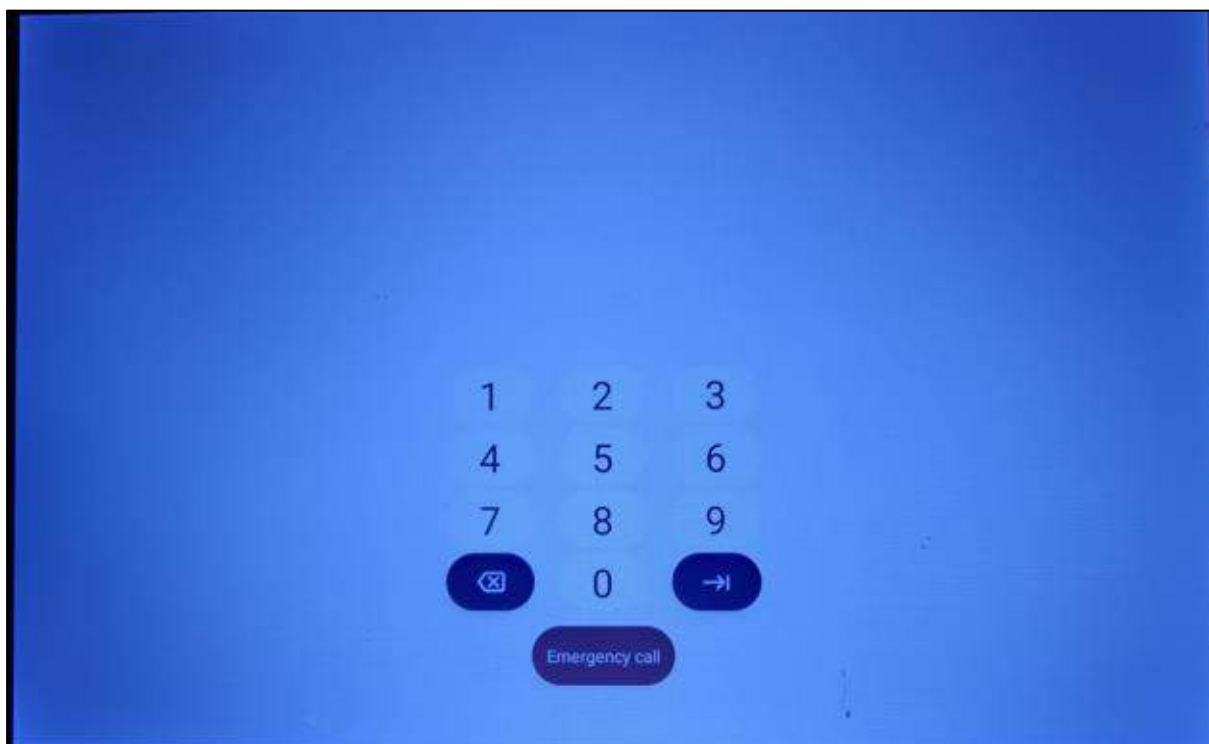


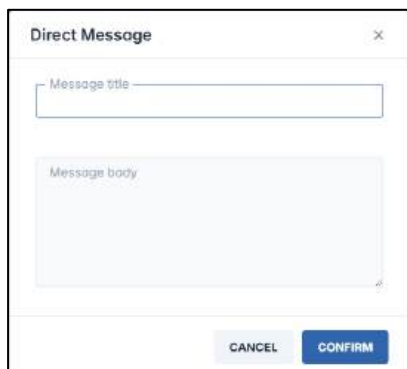
Figure 6-18: Prompt for password to release a locked device

6.1.9 Direct Message

This command allows you to send a plain text message, with a message title and body, to a device.

To send a message:

1. Click on the **Direct Message** command. The Direct Message window opens.
2. Supply a message title and body and click **Confirm**. The message is sent immediately to the device.



A screenshot of the 'Direct Message' dialog box. It has a title bar with a close button. Inside, there is a text input field for 'Message title' and a larger text area for 'Message body'. At the bottom, there are two buttons: 'CANCEL' and 'CONFIRM'.

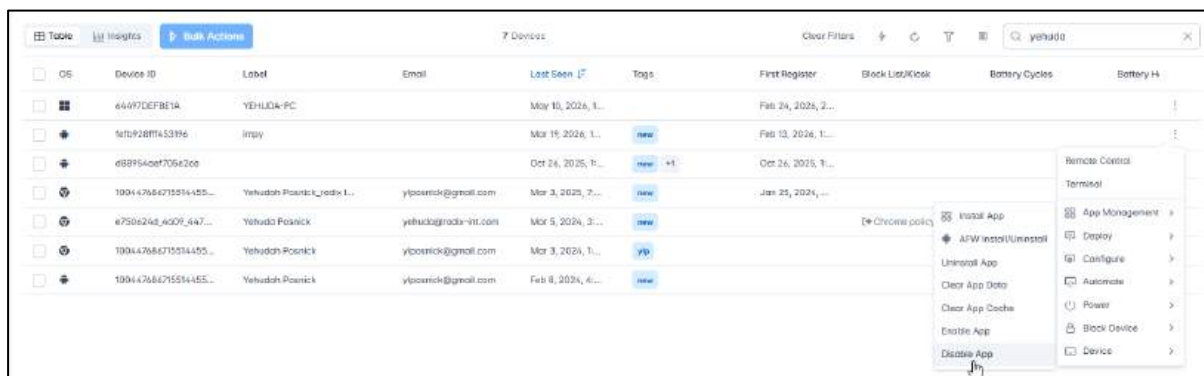
6.1.10 Disable/Enable apps

The command “Disable apps” allows you to remove the icon of an app from a device. It will not uninstall the app on the device. But the remote user will not be able to execute the app.

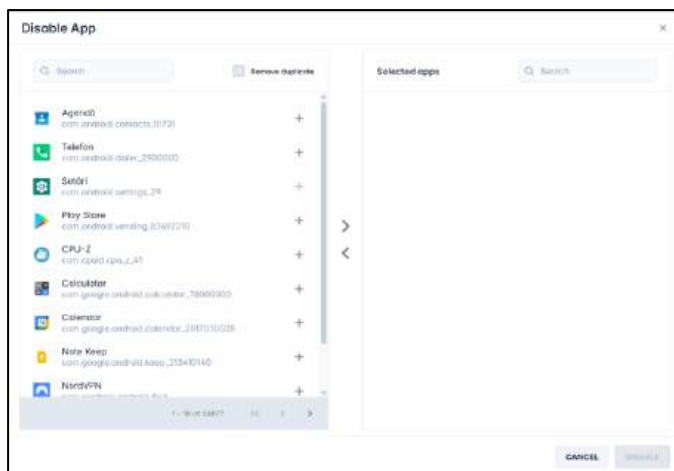
The command “Enable apps” restores the icon of the app to the device display. The remote user will be able to use the app once again.

This option is available from:

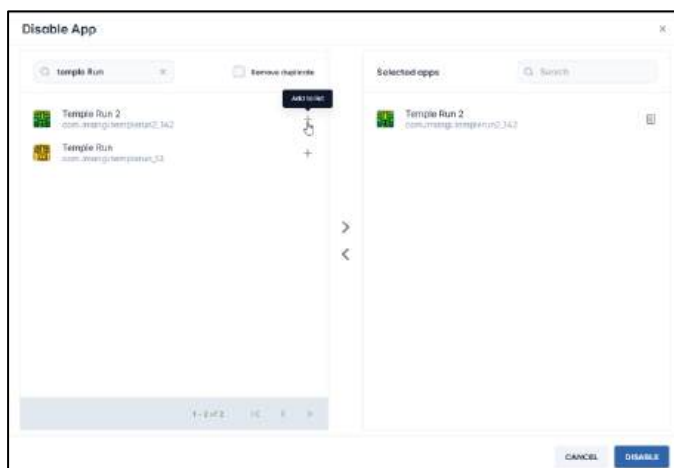
- **Bulk Actions>App Management>Disable App**, or
- The device’s **three-dot menu>App Management>Disable App**.



1. When you click on the **Disable App** option, the **Disable App** screen opens.



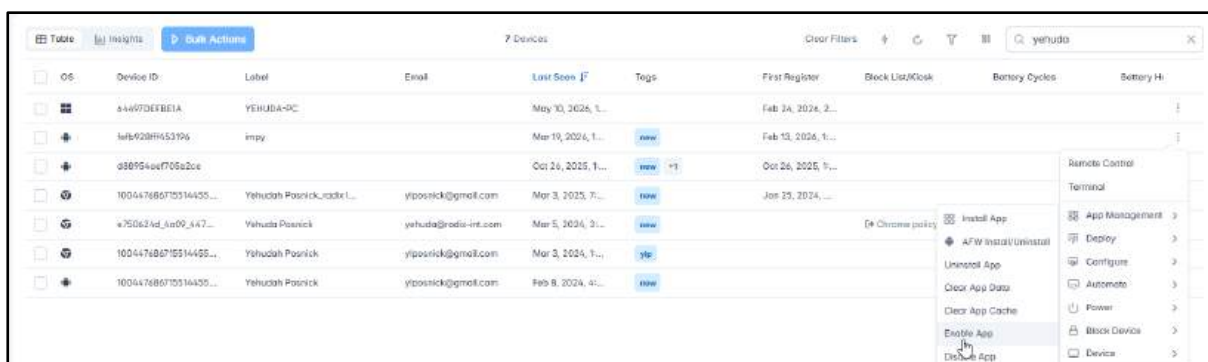
2. Select the apps that you wish to disable by clicking on the **Add to List** icon **+**. The app will now appear in the **Selected apps** column.



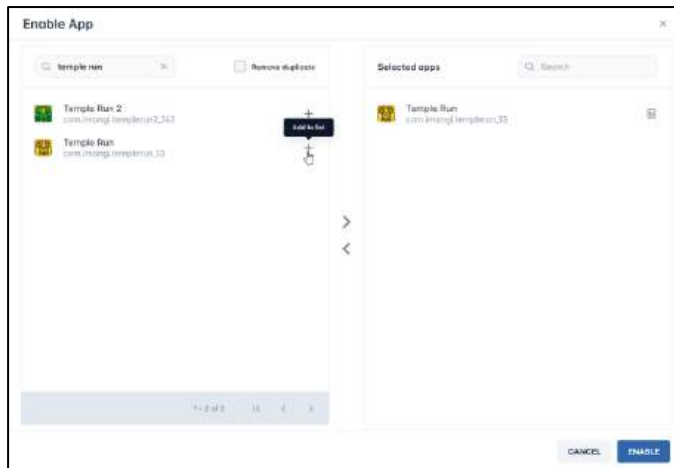
3. Click **Disable**. The apps that you selected will now be disabled on the device.

To reverse the process and enable an app:

1. Click on the device's **three-dot menu>App Management>Enable App**.



2. Select the apps that you want to enable, by clicking on the **Add to List** icon.



3. Click **Enable**. The app will now be enabled on the device, and the app icon will appear once again on the device.

6.1.11 Export Device Data to CSV

When you click on the Export Device Data to CSV command, you will receive the following pane:



Figure 6-19: Export to CSV selection options

1. You can choose to display all columns available, or only the columns currently shown in the **Devices** table.
2. Select which columns to display and click **Confirm**. An Excel spreadsheet will download to your computer, displaying the data in the following format:

ID	Device ID	Label	Device Name	Email	Last Seen	Location	IP address	Local IP
1	ANDROID	google-play-market			26/09/2018 12:04	147.236.121.74		
2	ANDROID	whitel_23_488_1225	virtual		24/09/2017 7:03	79.181.116.145		10.0.2.15
3	ANDROID	whitel-service06	ACISP on sunfsh		04/02/2014 17:27	82.166.75.33		
4	ANDROID	whitel-service04	ACISP on sunfsh		04/02/2014 17:29	82.166.75.33		
5	ANDROID	whitel-service03	ACISP on sunfsh		04/02/2014 17:24	82.166.75.33		
6	ANDROID	whitel-service02	ACISP on sunfsh		04/02/2014 17:23	82.166.75.33		
7	ANDROID	unknown			25/01/2018 12:42	213.8.100.110		102.168.108.32
8	ANDROID	mt123s	googleplay	qaz.radix@gmail.com	05/07/2019 12:33	31.160.21.51		
9	ANDROID	07			12/05/2024 15:07	213.8.100.110		
10	ANDROID	testdevice06	0910		01/09/2019 15:31	79.180.113.3		
11	ANDROID	testdevice04	0910		01/09/2019 15:29	79.180.113.3		
12	ANDROID	testdevice03	0910		01/09/2019 15:28	79.180.113.3		
13	ANDROID	testdevice02	0910		01/09/2019 15:25	79.180.113.3		
14	ANDROID	testdevice01	0910		01/09/2019 15:22	79.180.113.3		
15	ANDROID	test02			30/06/2025 17:58	82.166.75.33		
16	ANDROID	test01			30/06/2025 17:58	82.166.75.33		
17	ANDROID	#8C9000050145600836	smartward the board		01/09/2019 15:10	213.8.100.110		102.168.108.32
18	ANDROID	#8C9000050145600836			28/11/2025 0:09	213.8.100.110		102.168.108.32
19	ANDROID	#8C9010000000000000	connecting.com		01/09/2019 15:17	213.8.100.110		102.168.108.32

6.1.12 Firmware Update

This option allows you to update the device’s firmware, for better performance and security.

Firmware update

Are you sure you want to update the firmware on the selected device?

NO
YES

Note: Not all devices allow remote firmware updates via the Radix MDM. If your remote device does not support firmware updates, you will get a “Command failed” message:

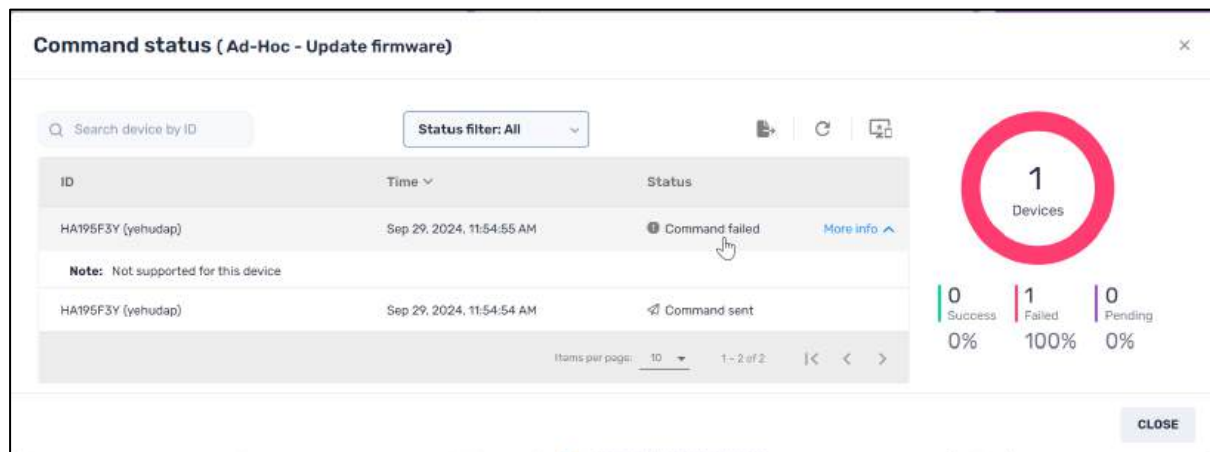


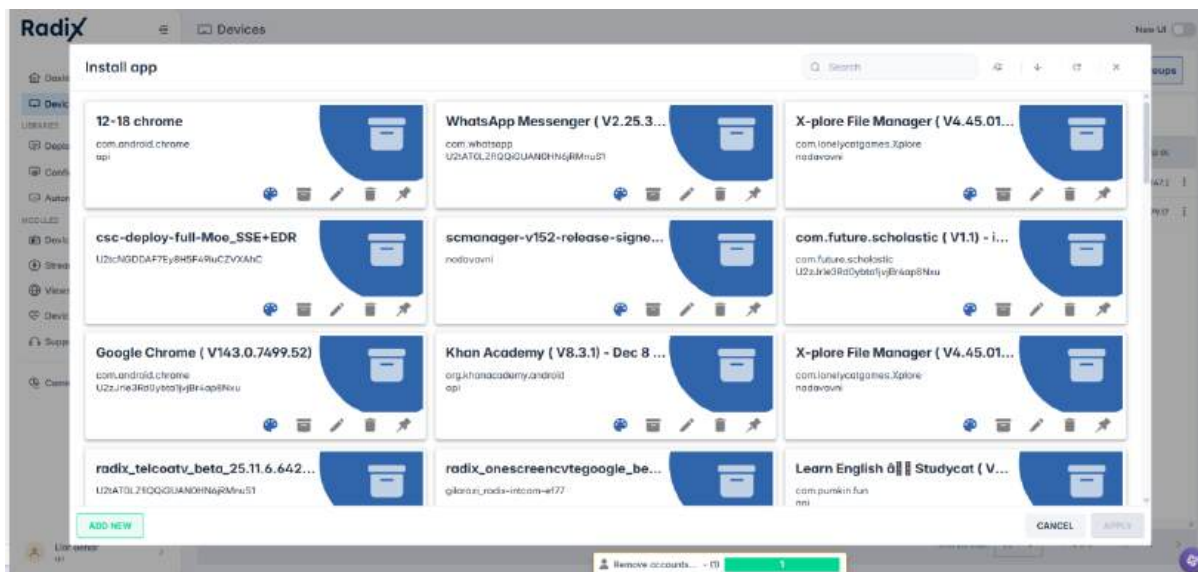
Figure 6-20: Message when attempting a firmware update on an unsupported device

6.1.13 Install App/Install Package

This option allows you to remotely install software packages on a particular device. When you click on a device’s **three-dot menu>App Management>Install App**, a grid of software packages appears. These are software packages that have already been stored in the Radix system.

6.1.13.1 Installing a package in the Radix Device Management interface:

In the screenshot below, the user will install the GeoGebra app on the remote device:



To install a package on a device remotely:

1. Click on a selected software package.
2. Click the **Apply** button. A message will be sent to the device, and a (green) notification will appear in the lower left of the Devices Table, indicating that the app was installed successfully on the device. (The Devices Table will also alert you if the installation failed (a red notification), or in Pending status (a purple notification).)

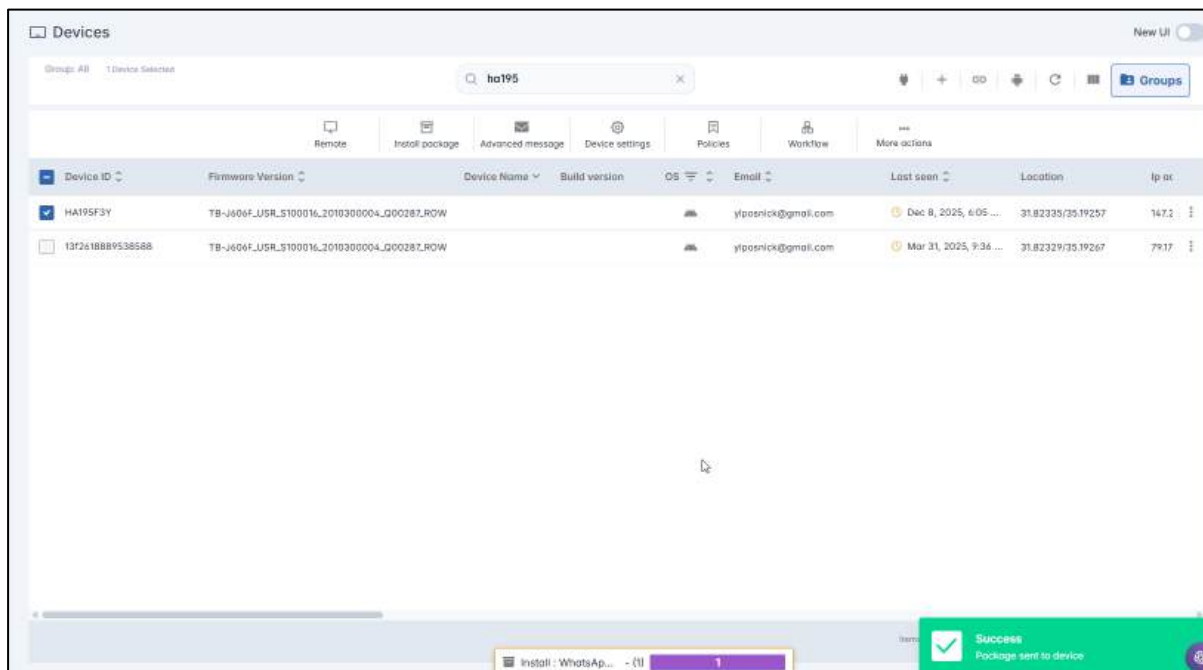


Figure 6-21: Notification that the app was installed successfully

3. Clicking on the notification in the bottom center of the screen will open the **Command status** screen:

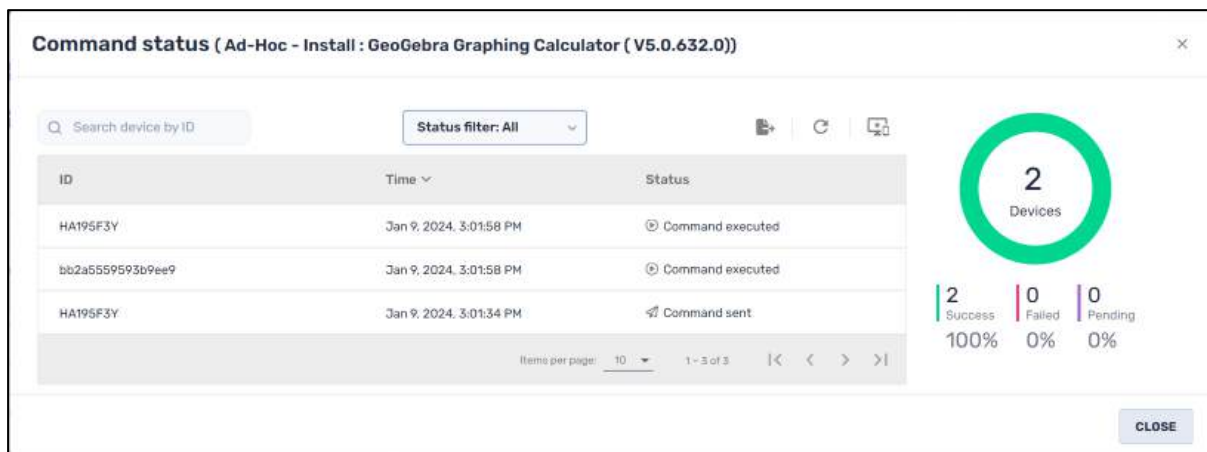


Figure 6-22: Display of status of command sent to a device

The **Command status** screen has several options to display or store results of commands sent to devices:

Table 6-2: Command Status Screen Display Options

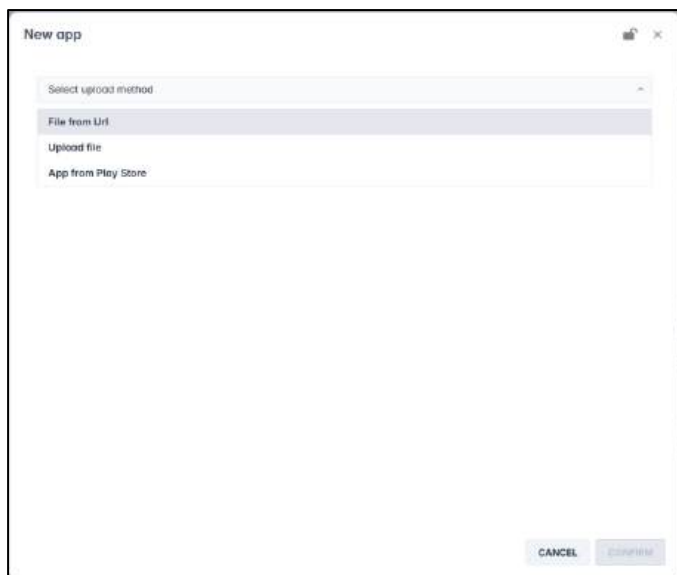
Icon	Description
Status filter: All	Allows you to filter results by commands sent, executed, pending, etc.
	Export to CSV: Allows you to export the table of results to an Excel CSV file
	Refresh: Refreshes the results displayed in the table
	List by Time: Allows you to display the list of commands by the date and time that they were issued
	List by Device: Allows you to display which devices have had the selected app installed

6.1.13.2 Adding a new package to install

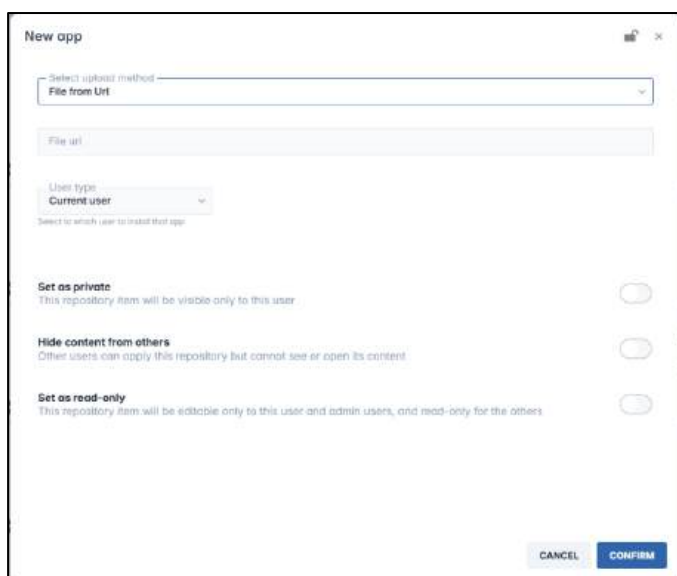
You can also add new software packages and install them on devices. (The user of the device may have to complete the installation.)

To add a new software package to install:

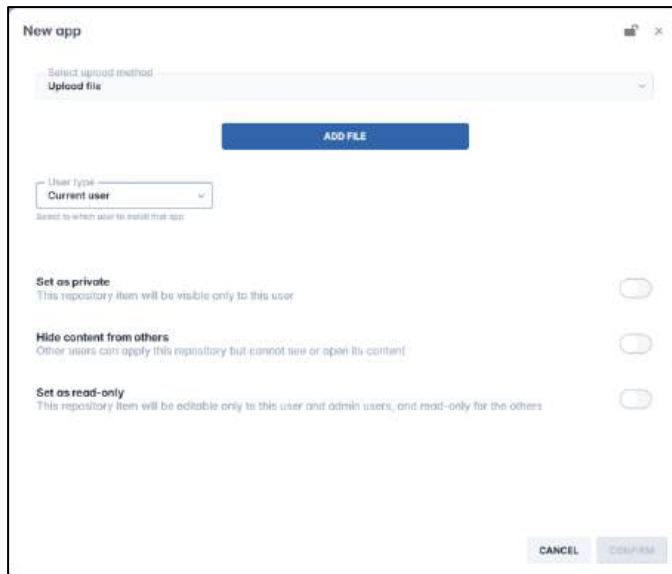
1. Click the **Add New** button on the lower left of the **Install Package** screen. The **New Package** screen appears.



2. You have the option of uploading a new software package from a URL, a file from your computer, or from the Google play store.
 - If you select **File from URL**, you will be prompted for the file's URL.

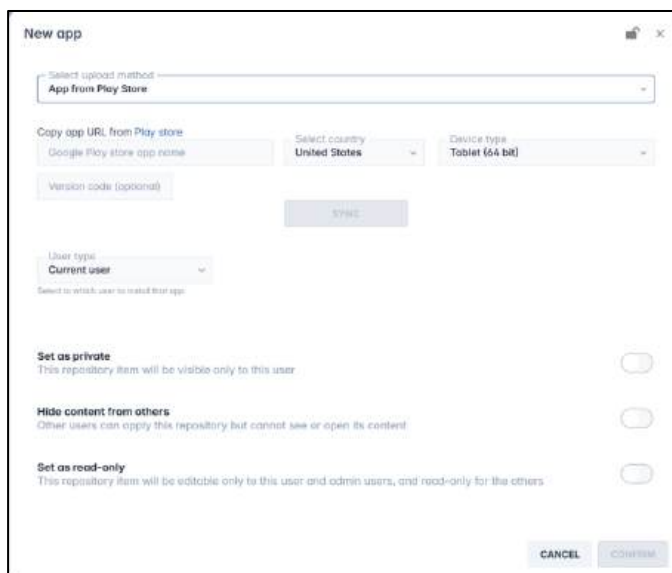


- If you select **Upload file**, you can select a file from your computer.



The 'New app' dialog box shows the 'Upload file' method selected. It includes an 'ADD FILE' button, a 'User type' dropdown set to 'Current user', and three toggle options: 'Set as private', 'Hide content from others', and 'Set as read-only'. All three toggles are currently turned off. At the bottom are 'CANCEL' and 'CONFIRM' buttons.

- If you select to upload a software package from the Google play store, you will be prompted for the app URL from the Play store.



The 'New app' dialog box shows the 'App from Play Store' method selected. It includes a 'Copy app URL from Play store' section with a text input field, a 'Select country' dropdown set to 'United States', and a 'Device type' dropdown set to 'Tablet (64 bit)'. There is also a 'Version code (optional)' input field and a 'SKIP' button. Below these are the same 'User type' dropdown and three toggle options as the previous screenshot. At the bottom are 'CANCEL' and 'CONFIRM' buttons.

- **Set as private option:** Click on the **Set as private** button if you want this new software package option to be visible only to you (the creator of the item) when you log in to the Radix Device Management Platform.
- **Hide content from others:** Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this software package, without allowing them to edit its details.
- **Set as read-only:** Click on the **Set as read-only** button if you want to restrict who will be able to modify the details of this software package. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .

6.1.13.3 Installing a Software Package on a Group of Devices

The **Install Packages** option can be applied to a group as well. This is a convenient way to install software on an entire fleet of devices at once. You can also track the success of the installation.

To install a software package on a group of devices:

1. In the Devices Table, click on the **Groups** icon  to open the Groups pane.
2. Find the group to which you wish to install the software packages, and click on its **three-dot menu>App Management>Install App**.

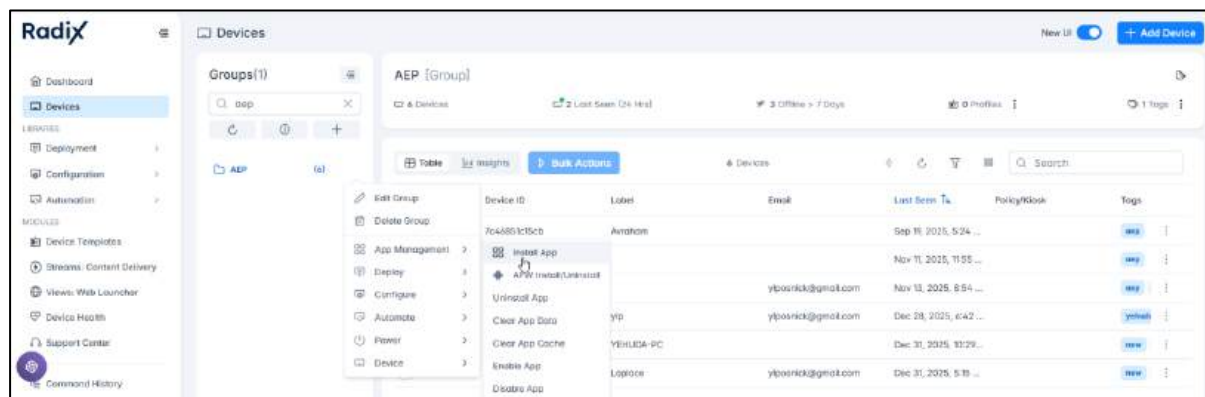
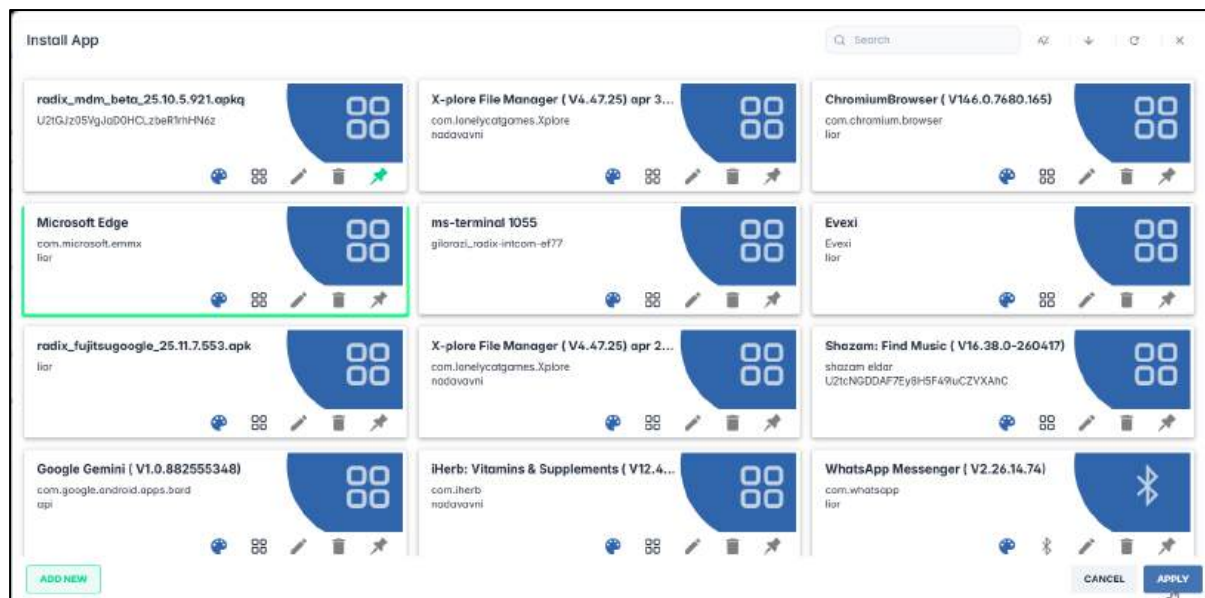


Figure 6-23: Groups three-dot menu, for executing commands to entire groups of devices

The **Install App** repository window opens.

3. Select the desired software package and click **Apply**. The software package will be installed on the entire group of devices.



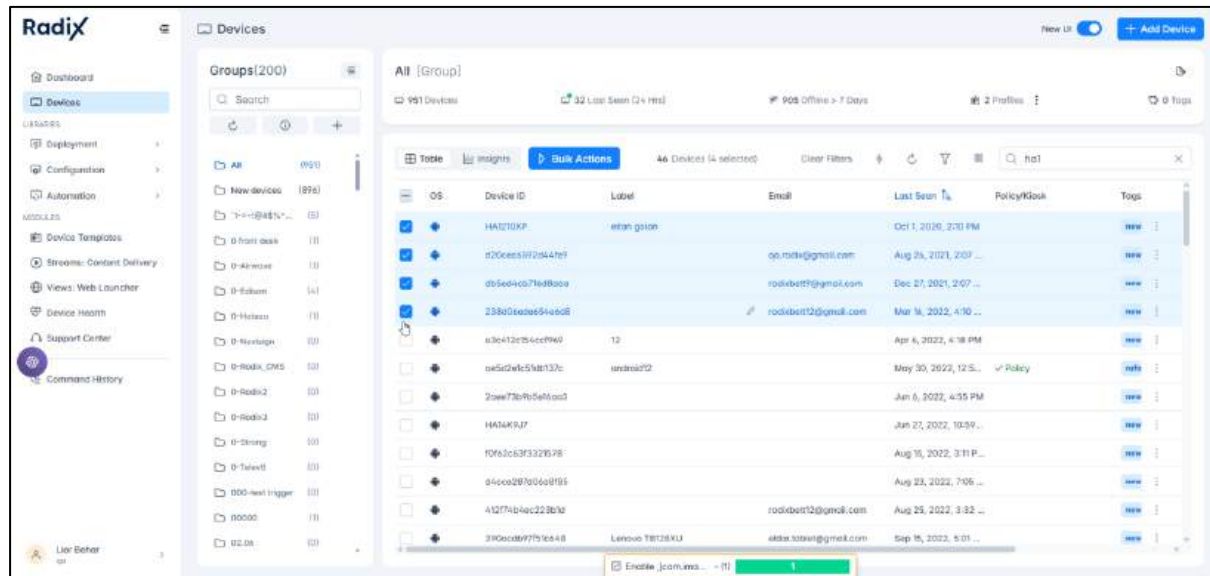
4. You can later check the success of the installation by opening the Commands Status window (**Section 10.3**).

6.1.13.4 Installing a Software Package on Selected Devices

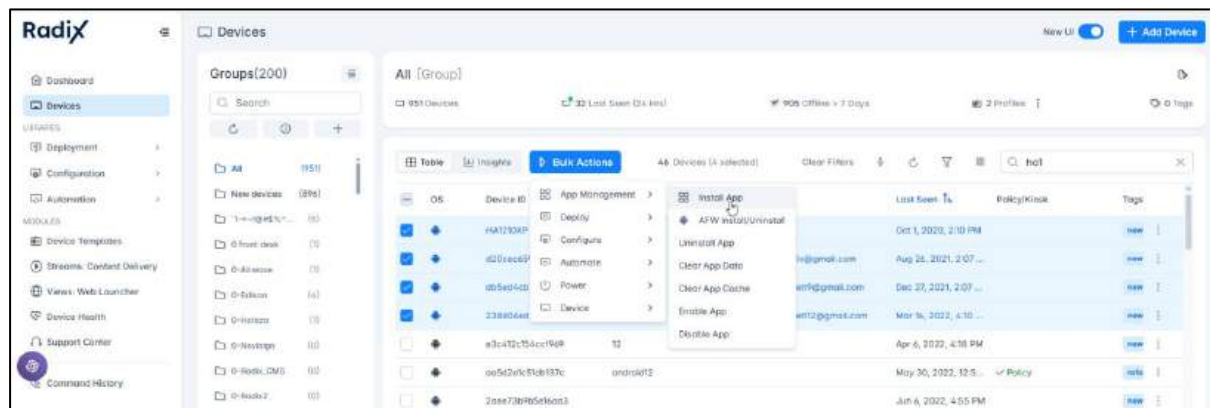
There is also an option to select particular devices manually and install a software package on them.

To select devices manually:

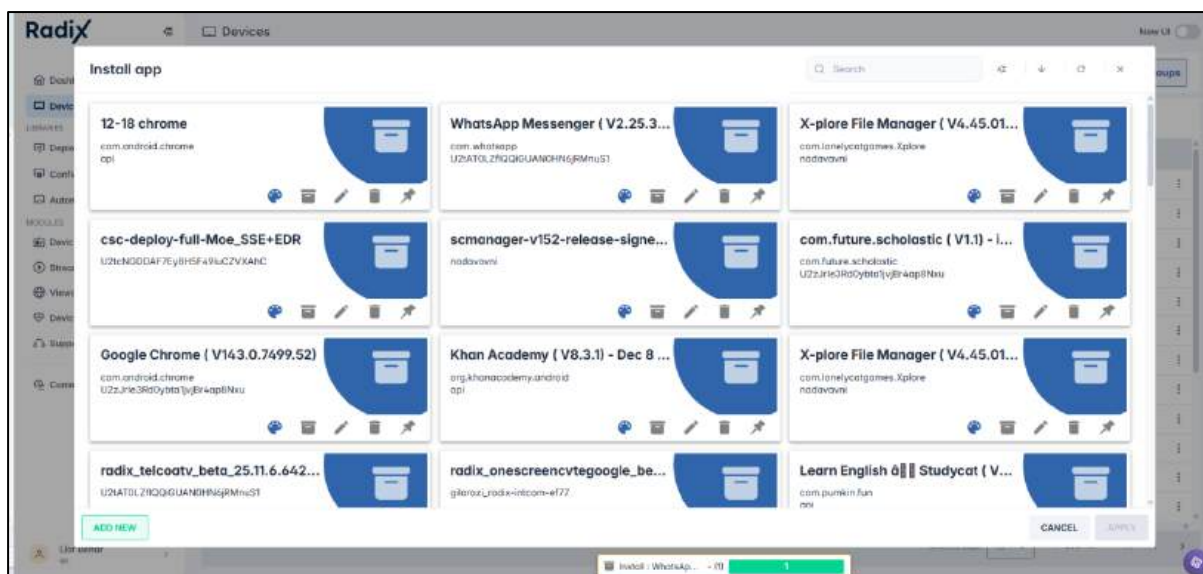
1. Click on the **Devices** icon, to open the Devices Table.
2. Select particular devices by clicking their checkbox in the far-left column.



3. Click on **Bulk Actions>App Management>Install App**:



The **Install App** window opens.



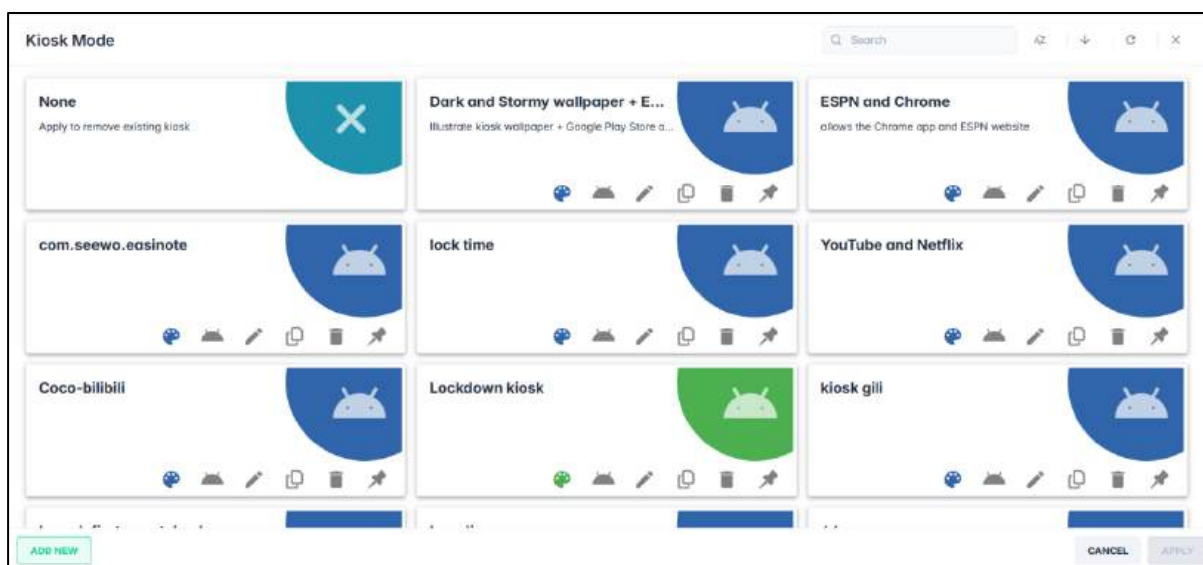
4. Proceed as above to select and install packages.

6.1.14 Kiosk

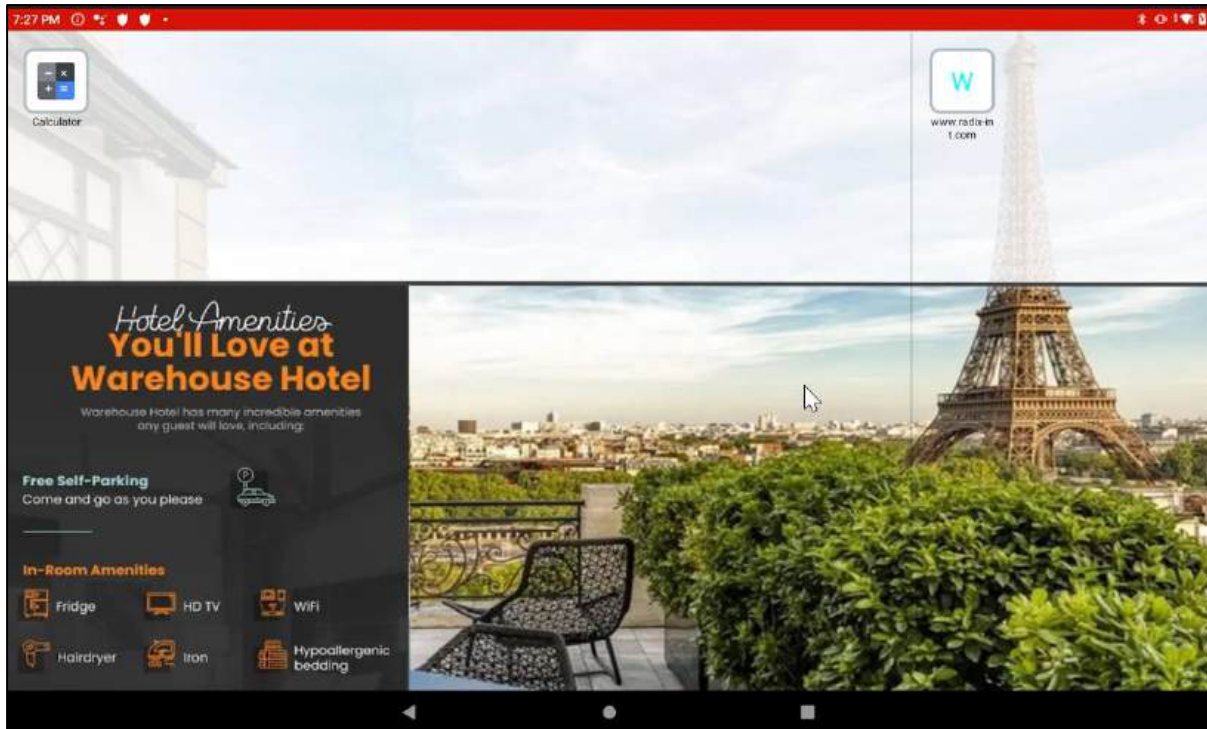
This option allows you to use a device as a display in a kiosk, as in a storefront or hotel.

6.1.14.1 Applying a Kiosk Option

1. When you click on a device's **three-dot menu>Configure>Kiosk mode**, the Kiosk options that are relevant to that device's operating system will appear.



2. Click on one of the kiosk options to select it, and then click **Apply**. In our example, we selected the **Hotel Kiosk** display.
The kiosk option that you selected will be displayed on the device automatically.



You can also add a new Kiosk option and customize it according to your preferences.

6.1.14.2 Creating a New Kiosk Option

To create a new Kiosk option:

1. Click on **Add New**. The **New Android Kiosk** screen opens in the **Edit Details** option.

The New Android Kiosk window has the following icons:

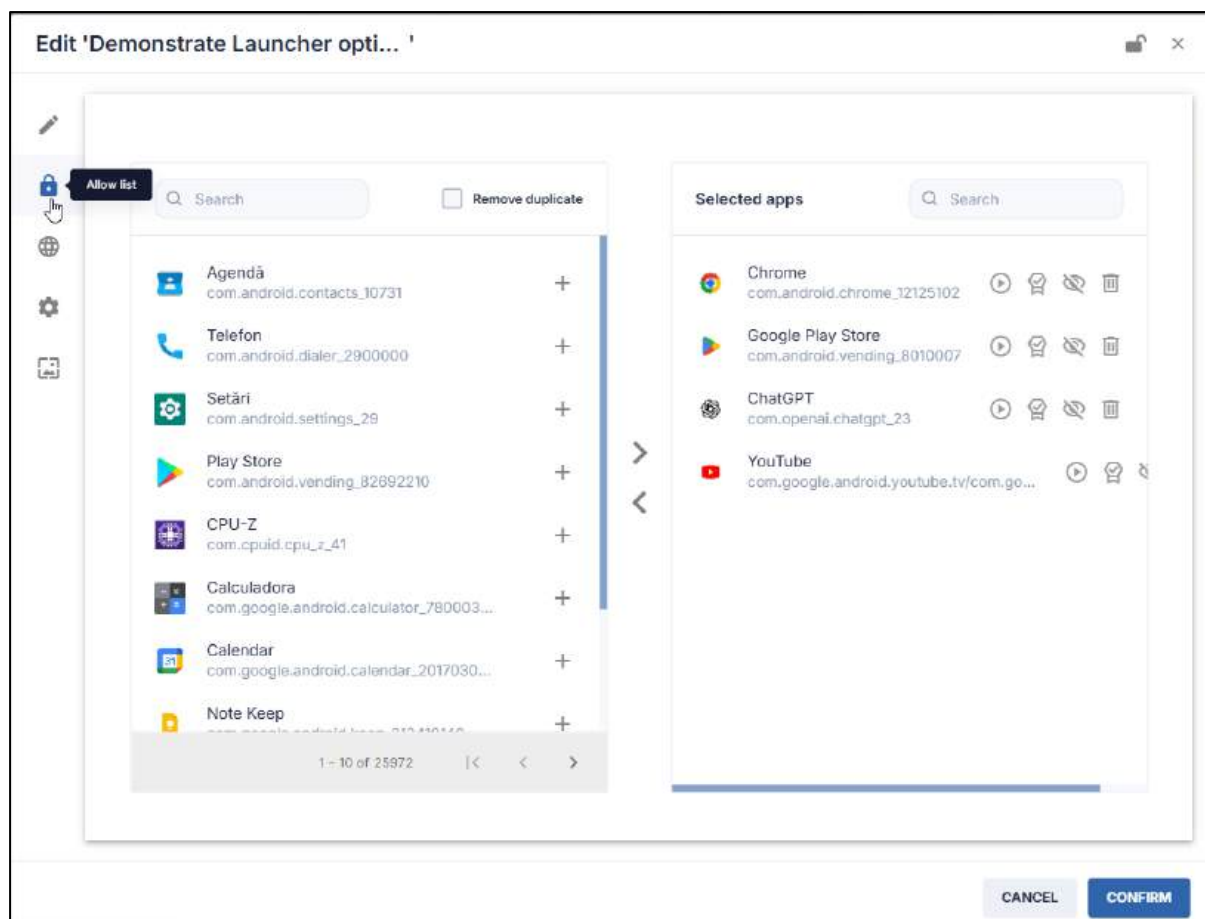
Table 6-3: Kiosk Editing Options

Icon	Description
	Edit Details
	Allow List: List of allowed apps
	Web: List of allowed websites
	General: General Display Settings
	Wallpaper: Set a wallpaper on the remote device

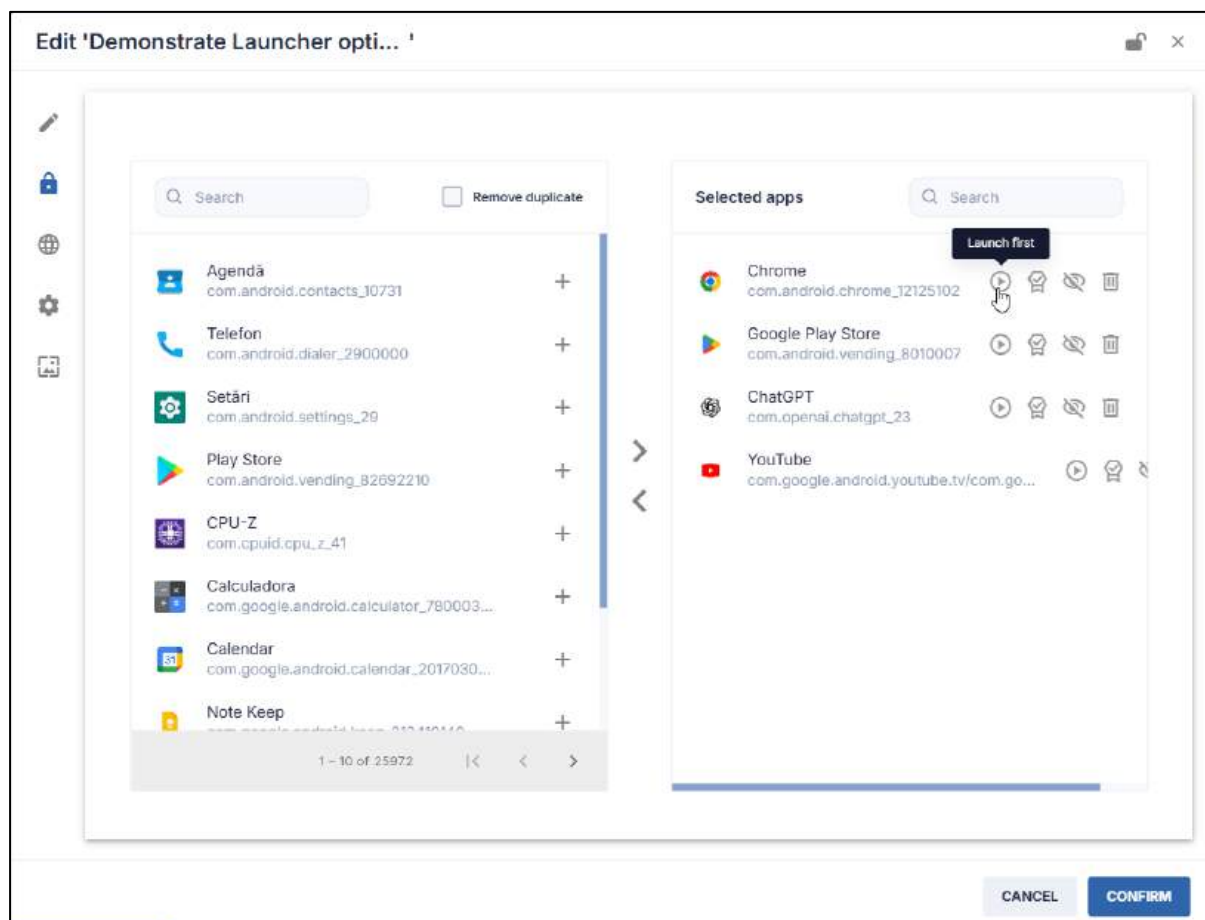
2. Assign the Kiosk command a name and a description.
3. Click on the **Set as private** button if you would like the Kiosk option to only be visible to you (as the creator of the item) when using the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Kiosk. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .

6.1.14.2.1 Kiosk—App Allow/Block List

1. Click on the **Allow List** icon. You can select which device apps will be included in the Kiosk option by clicking on the **Add to List** icon . The apps that you selected will now appear on the right-hand side in the **Selected apps** column.



- Once you have added an app to the **Selected apps** list, you have a number of options to run the app as soon as the remote device boots up:



The options are as follows:

Icon	Description
	Launch first
	Launcher app
	Hide icon
	Remove

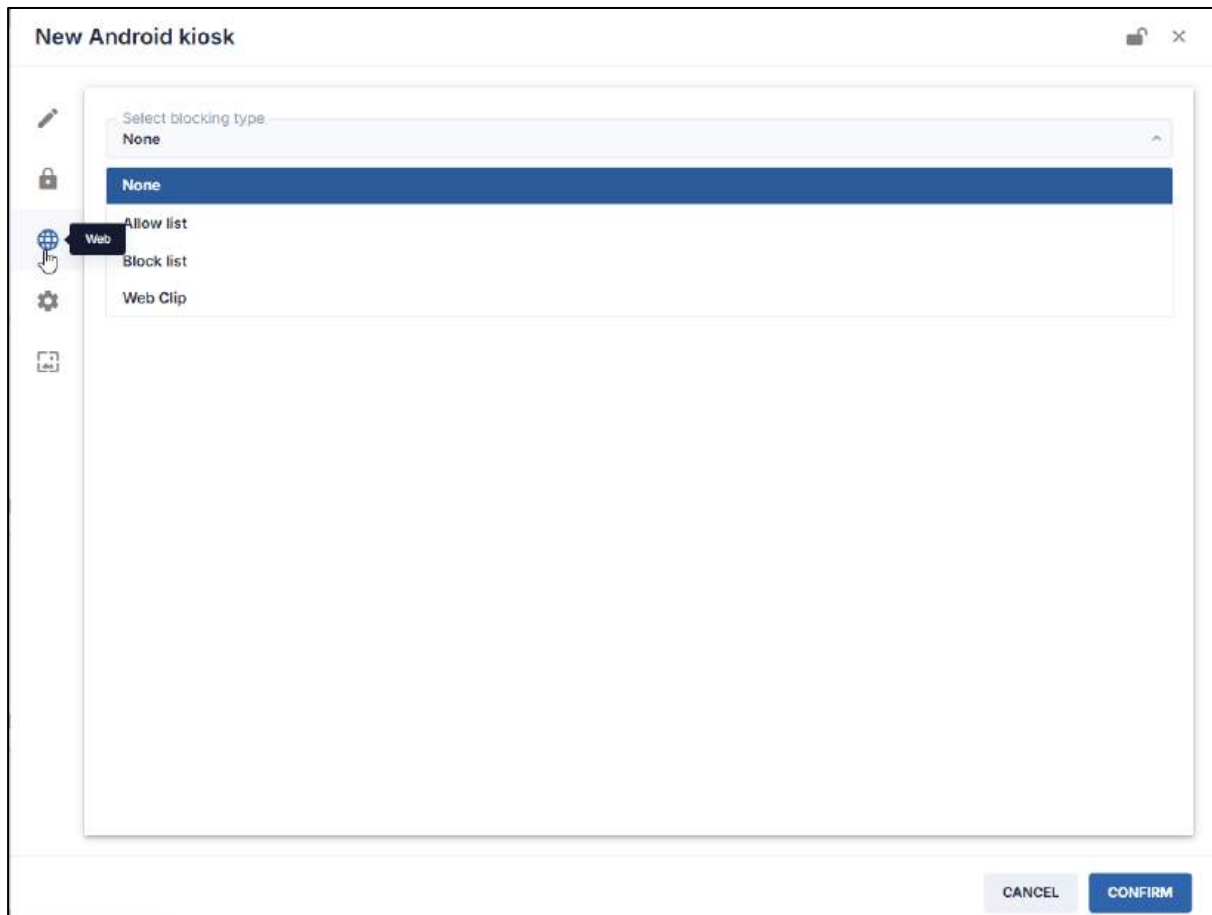
- Launch first:** Selecting this will launch the app upon every restart/boot/startup. Once you close that app, it will be displayed on the Home page with all the other apps.
- Launcher app:** Selecting this will prioritize this app as a “launcher app”: This launches the selected app as soon as the Kiosk command is sent to the remote device. Assigning an app to **Launcher app** status will effectively lock the device into running **only** that app. The Home, Back, and Recent Apps buttons on the remote device will essentially be inoperative. The device will automatically revert to the app selected to be the Launcher app.

Note: Only one of the selected apps in a specific Kiosk can be assigned **Launch first** or **Launcher app** status.

- **Hide icon:** This will hide the icon of this app on the device. The remote user will not be able to operate this app, until the Radix Device Management Platform user reactivates the icon.
- **Remove:** This will remove the app from the **Selected apps** list.

6.1.14.2.2 Kiosk—Website Allow List/Block List

1. Click on the **Web** icon to select whether you want to display
 - an **Allow list** of URLs that you want on the Kiosk device,
 - a **Block list** of URLs that you do not want on the Kiosk device,
 - a **Web clip** from a specific URL.



- The **Allow list** window offers the following options:

For the browser, you either select Google Chrome, or the Radix Secure Browser on the remote device.

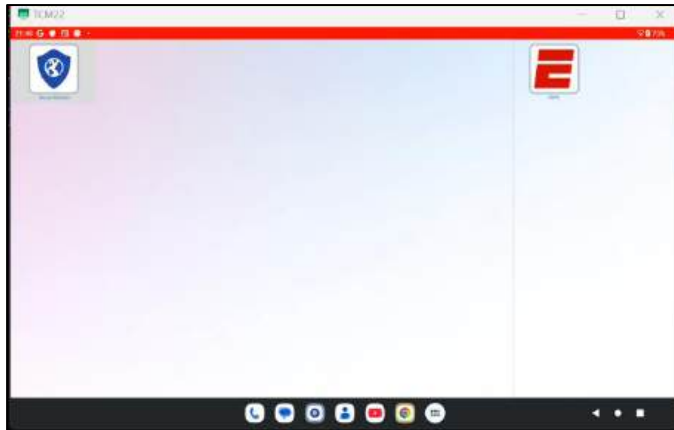


Figure 6-24: Icon for the Radix Secure Browser app on the left

To add a URL to the Allow list:

- Enter the URL, as well as a distinctive name for the website.
- If you wish, you can upload a Web favicon from your computer to employ as the icon on the Kiosk device to distinguish this website. If you choose not to upload a favicon file, the Device Management platform will use the default favicon for that website.
- Click on the **Add URL to List** icon.

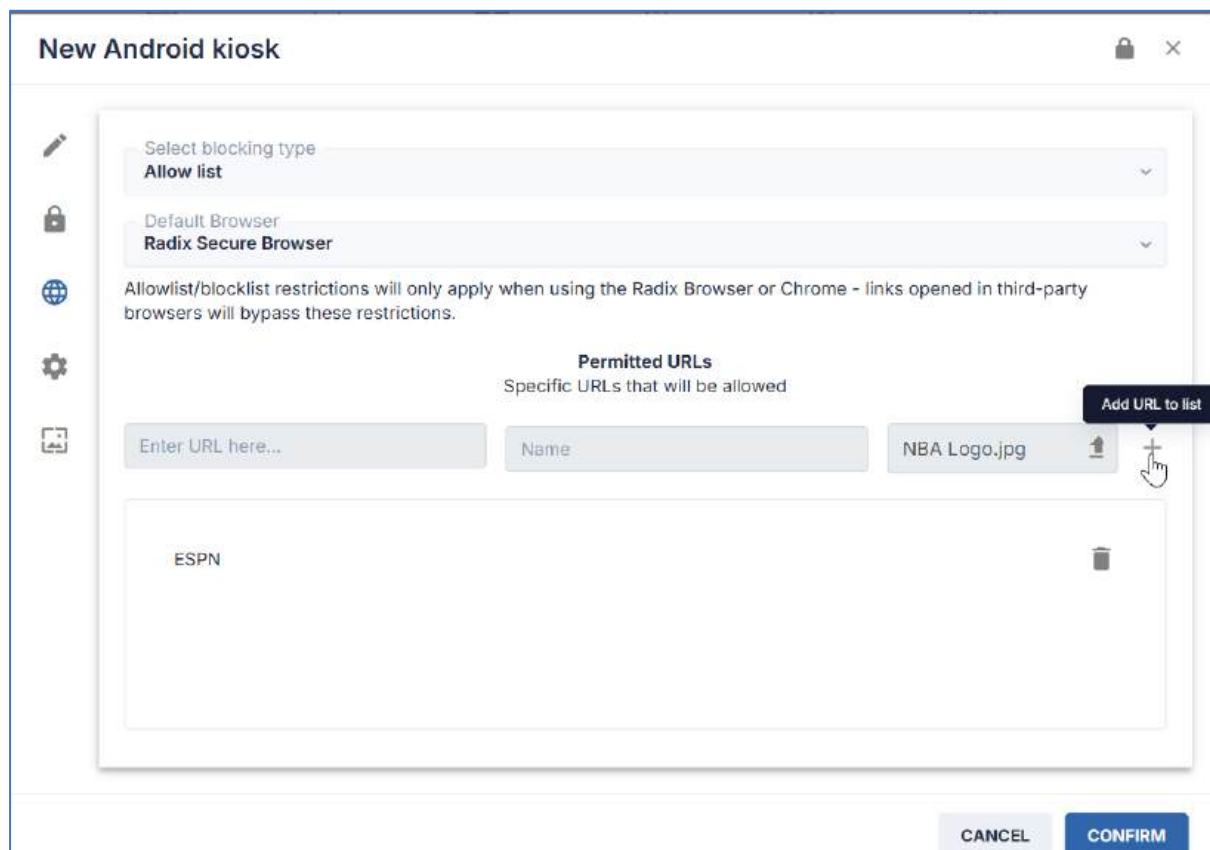
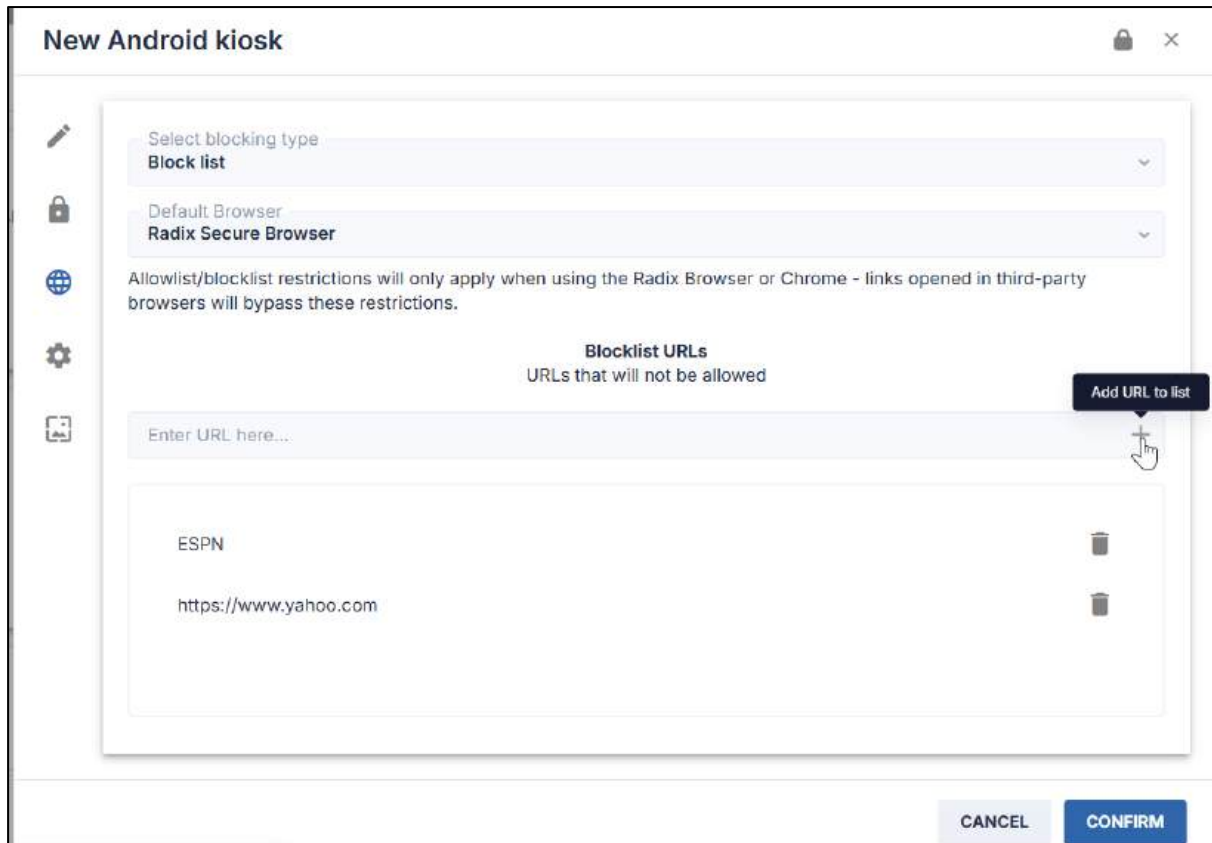


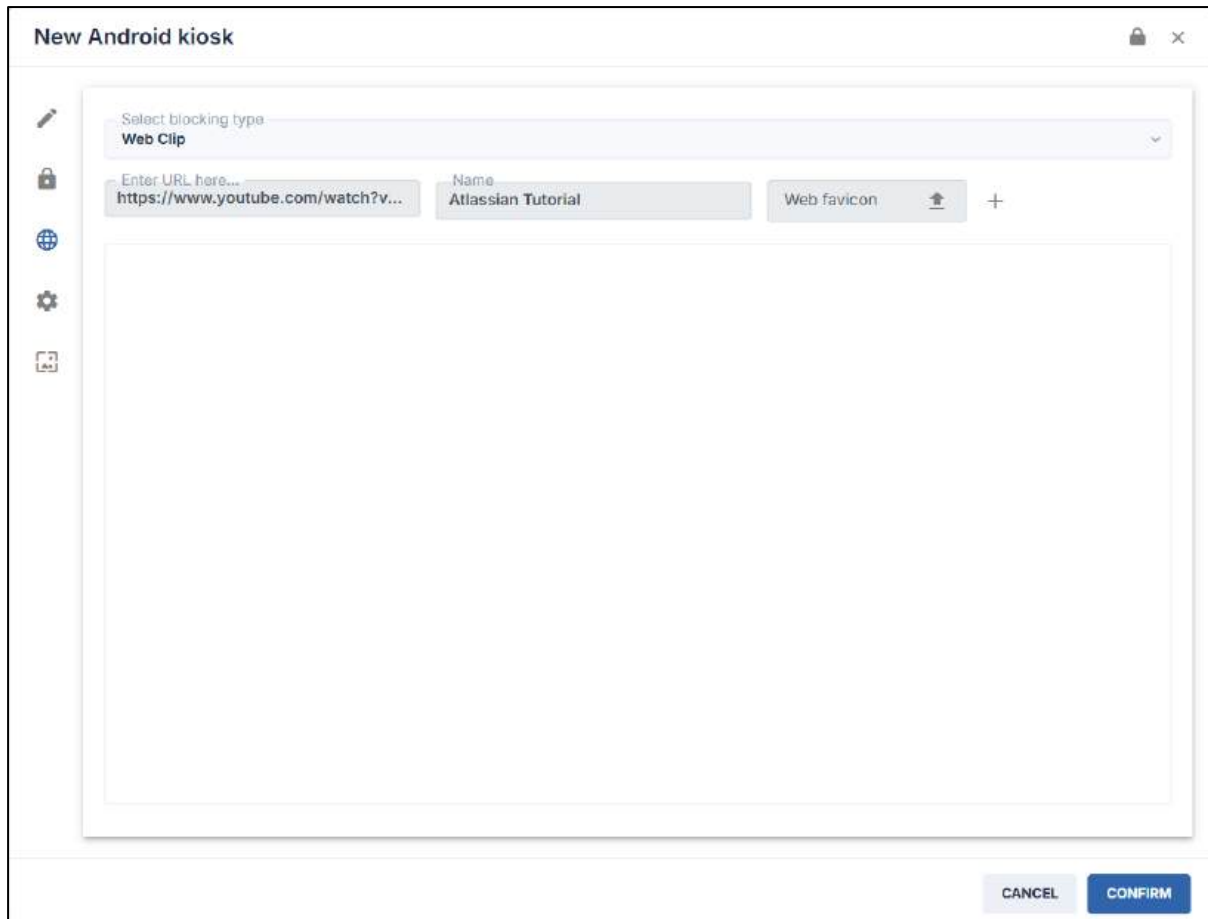
Figure 6-25: When selected, this kiosk mode will only allow access to the YouTube and ESPN websites

- The **Block list** pane offers the following options:

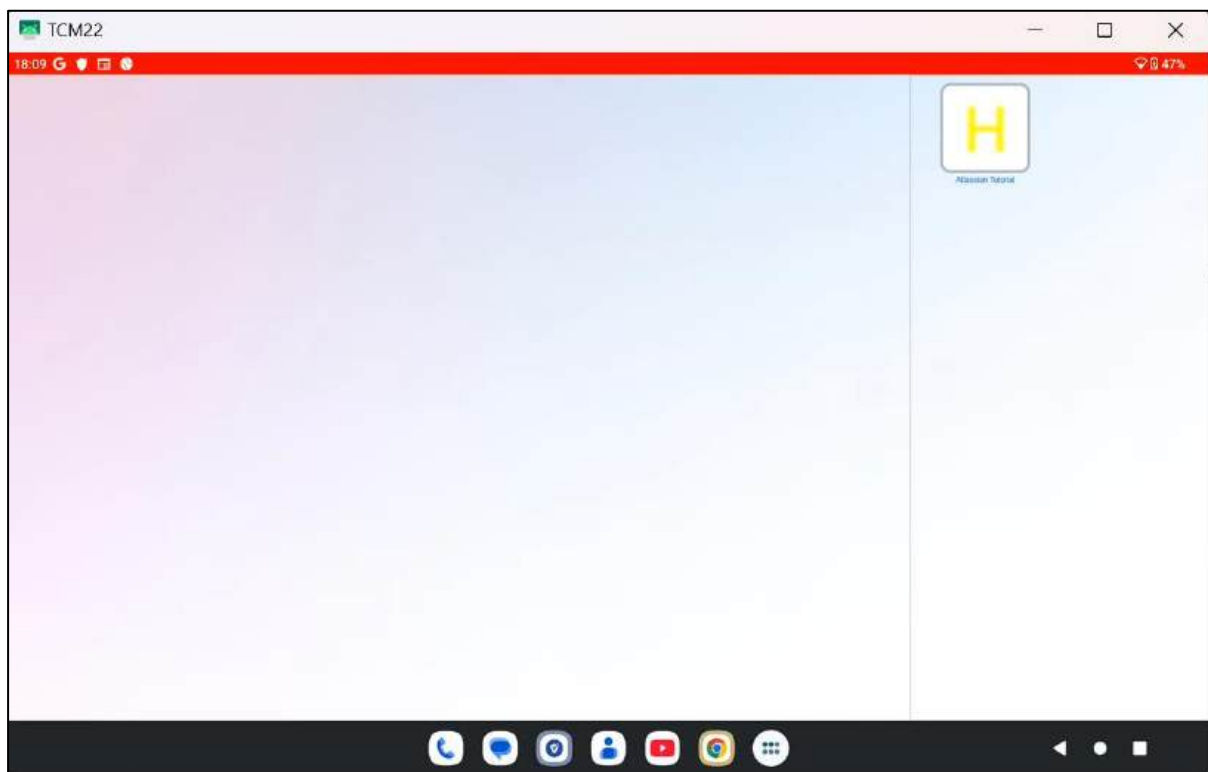


To block access to a website on the kiosk device

- a. Enter the website's URL in the text box.
- b. Click on the **Add URL to list** icon to add it to the Block list.
- The **Web Clip** option allows you to insert a video clip from a website to be displayed on the remote devices when in Kiosk mode:



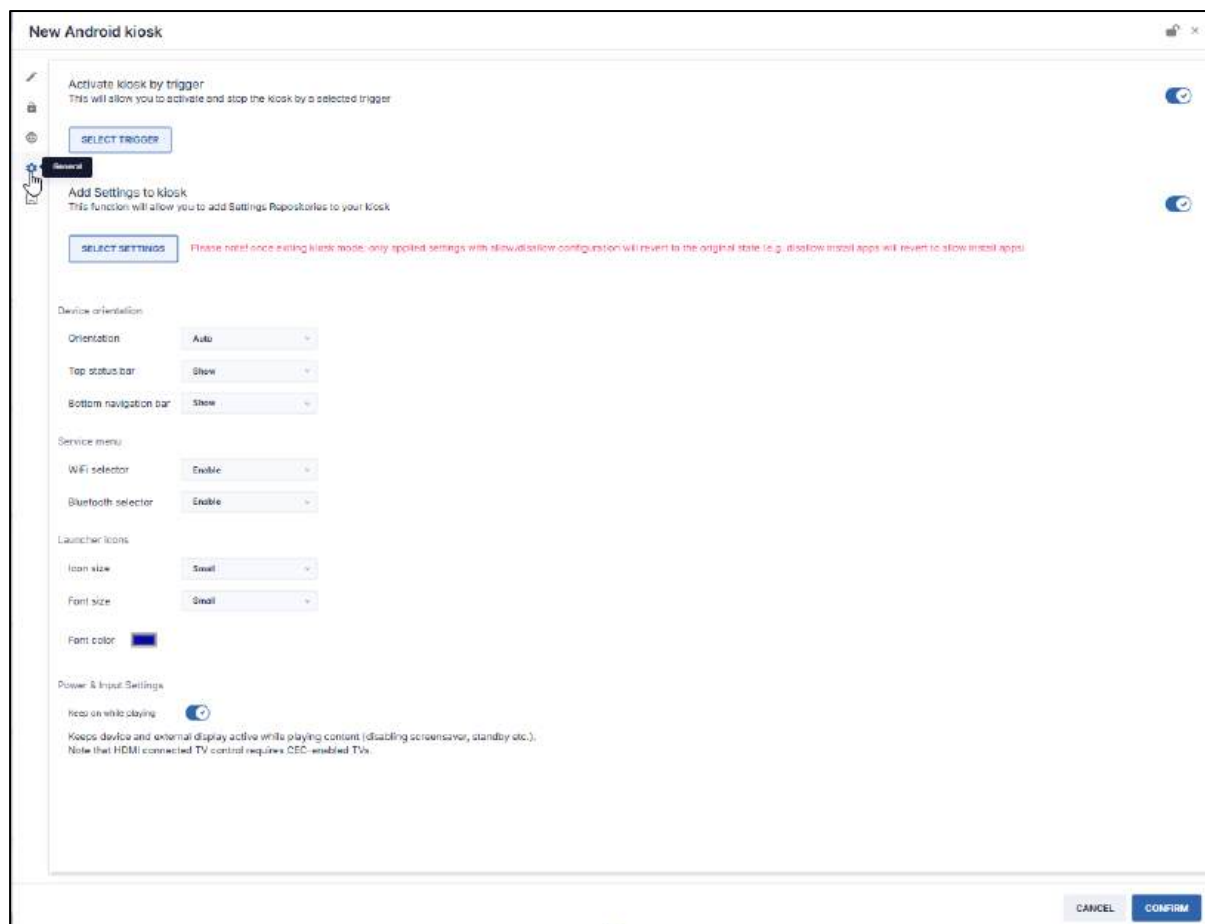
When we run the Web Clip option on a device, it displays the following.



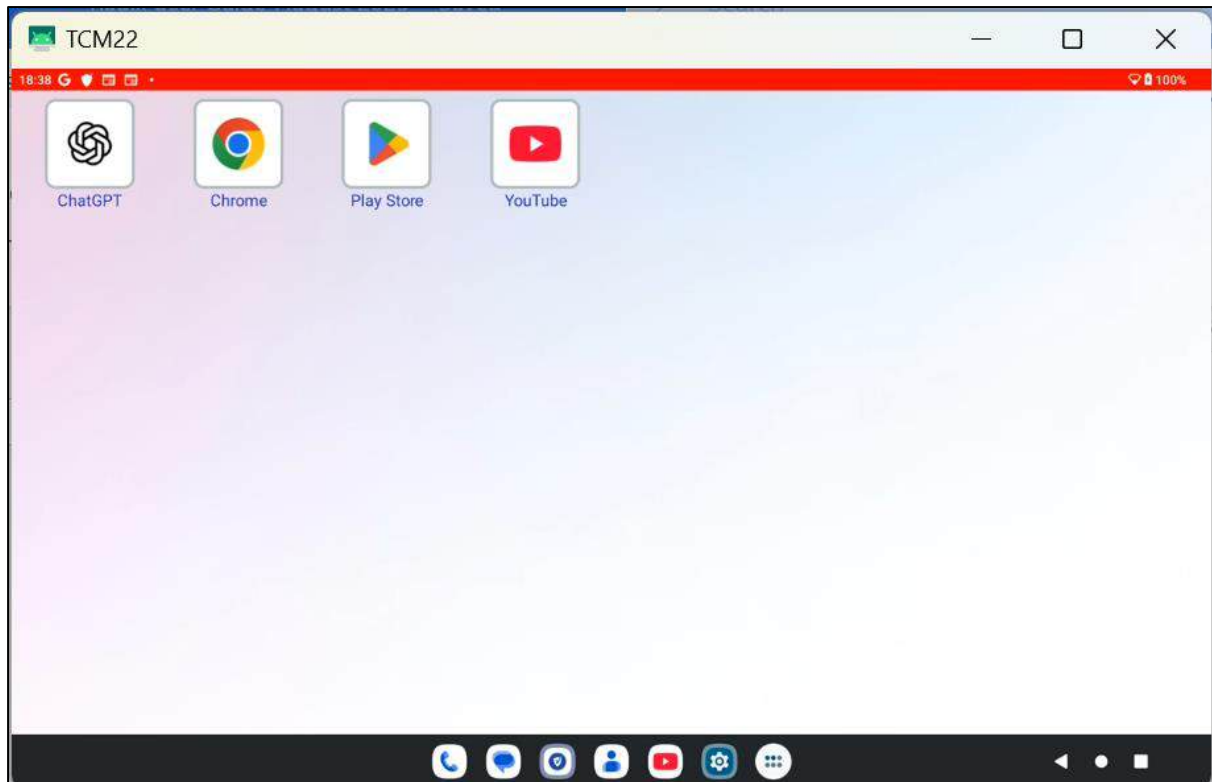
Tapping on the “Atlassian Tutorial” icon will run the YouTube clip.

6.1.14.2.3 Kiosk—General Display Settings

1. Click on the **General** icon. This window contains options to trigger the display of the kiosk, as well as the appearance of icons and text on the kiosk screen.



With these Settings, the Kiosk we have selected appears as follows:



- Click the **Activate kiosk by trigger button** if you wish to activate the kiosk by means of a predetermined trigger. The Trigger options are treated in **Section 6.1.26, Scheduler & Triggers Command**.
- Click the **Add Settings to kiosk** button if you wish to apply specific device settings to the devices running the kiosk. Device settings options are treated in **Section 6.1.8, Device Settings**.

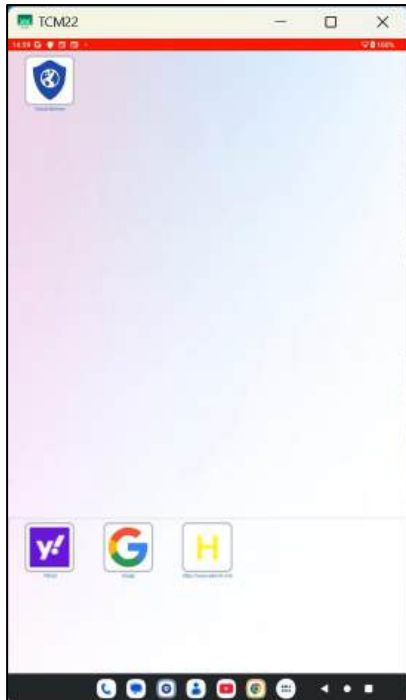
Here is a brief explanation of the remaining settings options:

6.1.14.2.3.1 Device orientation

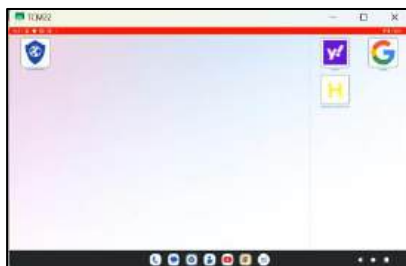
6.1.14.2.3.1.1 Orientation

This allows you to select the orientation of the remote device's display. The options are:

- **Auto:** This allows the orientation of the device's display of the View to adjust automatically, according to whether it is positioned in portrait or landscape mode.
- **Portrait:** This displays the View in portrait form.



- **Landscape:** This displays the View in landscape form.



6.1.14.2.3.1.2 Top status bar

The red status bar appears at the top of the Kiosk display. The options here are **Show/Hide**, to show the status bar at the top of the display, or to hide it.



Figure 6-26: Tablet displaying the top status bar (left) and without the status bar

6.1.14.2.3.1.3 Bottom navigation bar

The navigation bar appears at the bottom of the display, with Back, Home, and Stop buttons. Similarly, the options here are either **Show/Hide**.

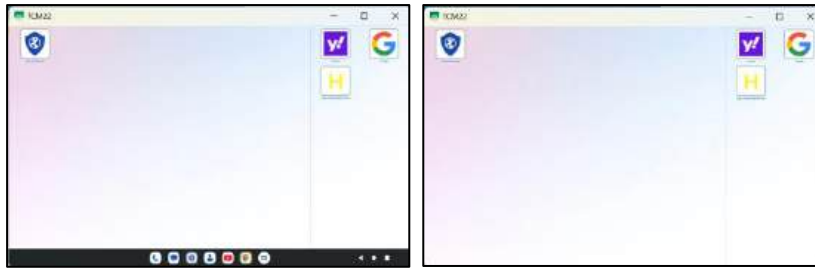


Figure 6-27: Tablet displaying the bottom navigation bar (left) and without the navigation bar

6.1.14.2.3.2 Service menu

When a remote device is displaying a Kiosk, you typically won't be able to access the icons for the apps on the device. However, you can temporarily pause the display of the Kiosk by accessing the Service Menu. From the Service Menu, you can select another Wi-Fi or Bluetooth network, or run apps installed on the remote device.

You can access the Service menu in one of two ways:

1. By pressing on the device's Volume Up-Volume Down buttons three times in quick succession, or
2. By tapping on the display 5 times in quick succession.

The following menu appears:

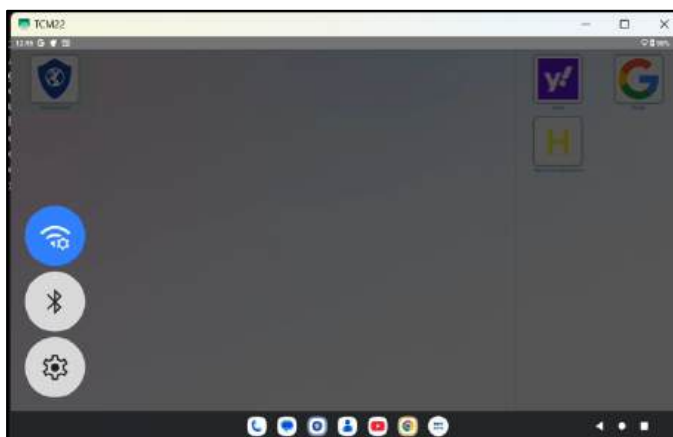


Figure 6-28: Settings icons while running a View

The Service Menu displays three icons:

Icon	Description
	Select a Wi-Fi network
	Select a Bluetooth device
	Kiosk settings

If you choose to disable the display of the Wi-Fi and Bluetooth buttons, then when you access the Service Menu, you will only see the Kiosk Settings icon.



Figure 6-29: Disabling the display of the Wi-Fi selector and Bluetooth selector

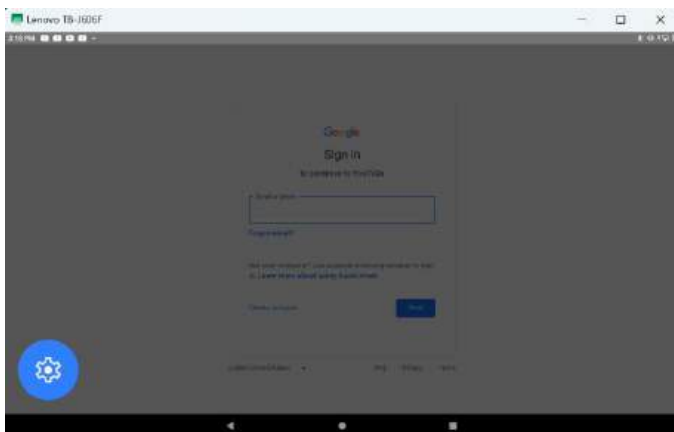
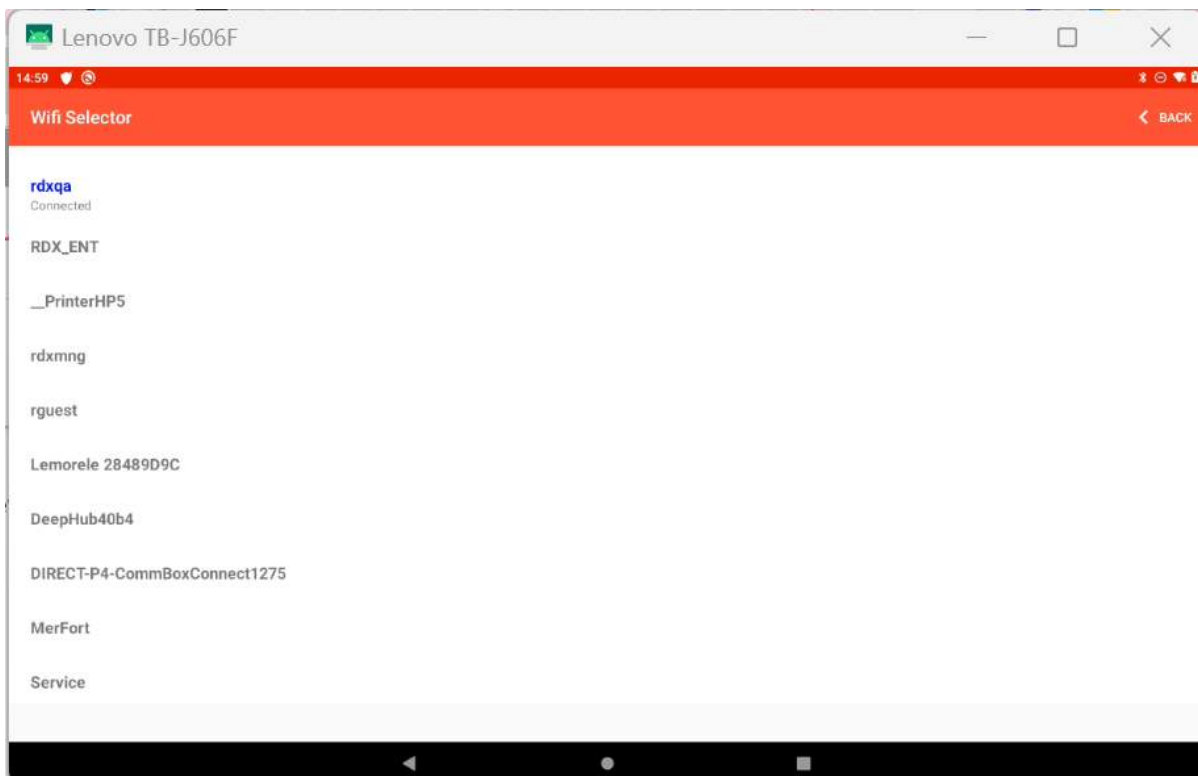


Figure 6-30: Service menu displaying only the Settings icon

We will briefly describe the functionality of the buttons.

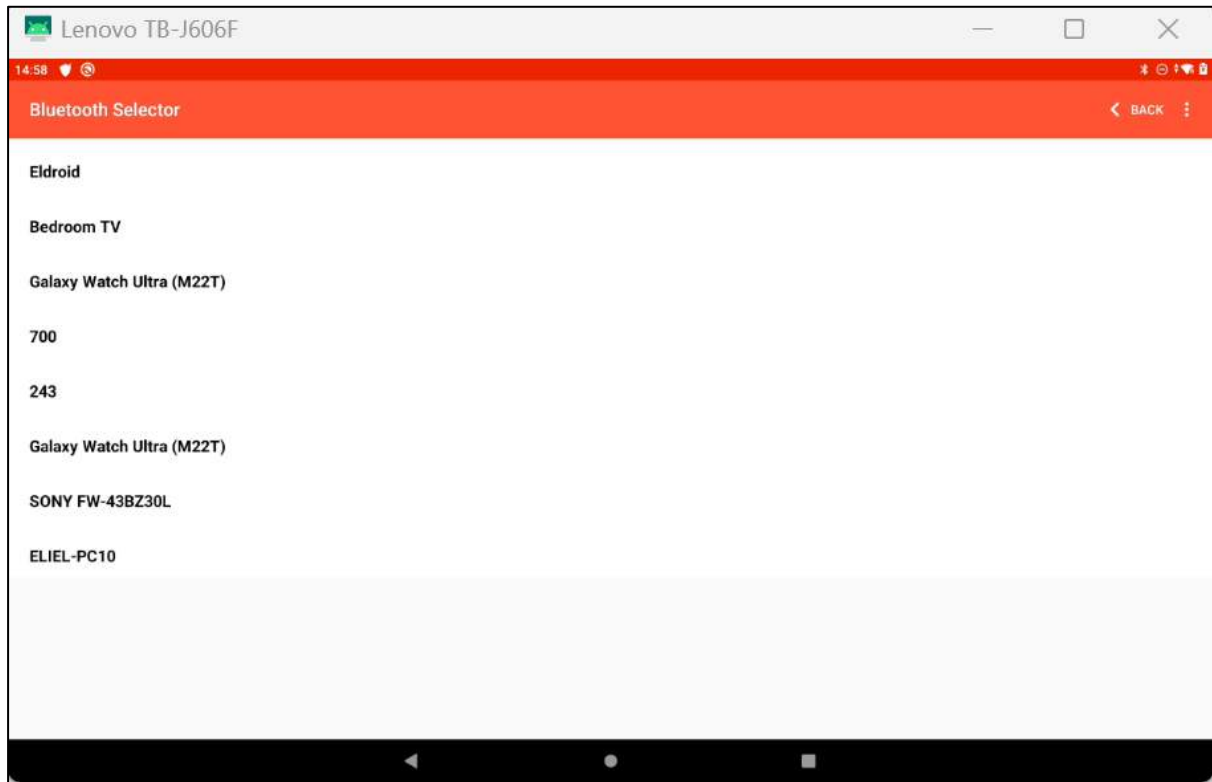
6.1.14.2.3.2.1 Wi-Fi Selector

The options in the Views Console are **Enable/Disable**. This will display or hide the Wi-Fi selector icon. Clicking on the Wi-Fi selector displays the following screen, showing all of the available Wi-Fi networks in the area:



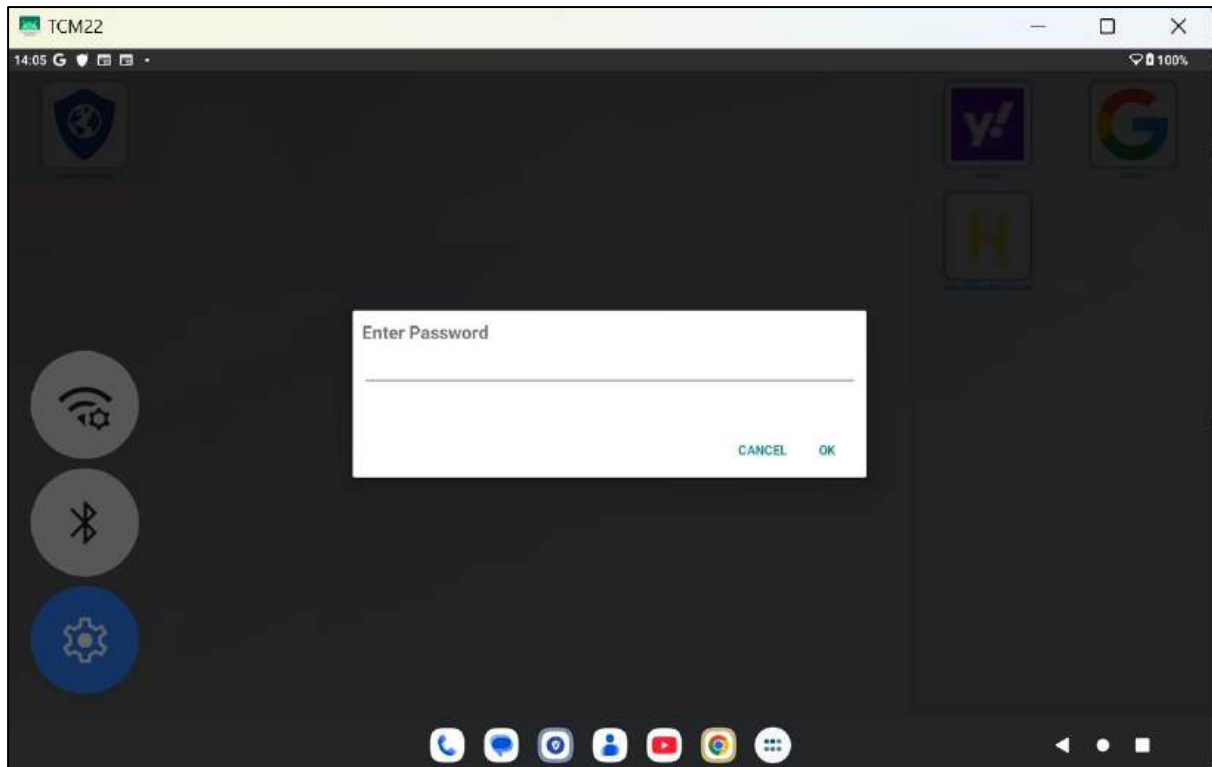
6.1.14.2.3.2.2 Bluetooth Selector

The options in the Settings window are **Enable/Disable**, to show or hide the Bluetooth selector icon. Tapping the Bluetooth Selector icon will open a list of Bluetooth devices in your area:

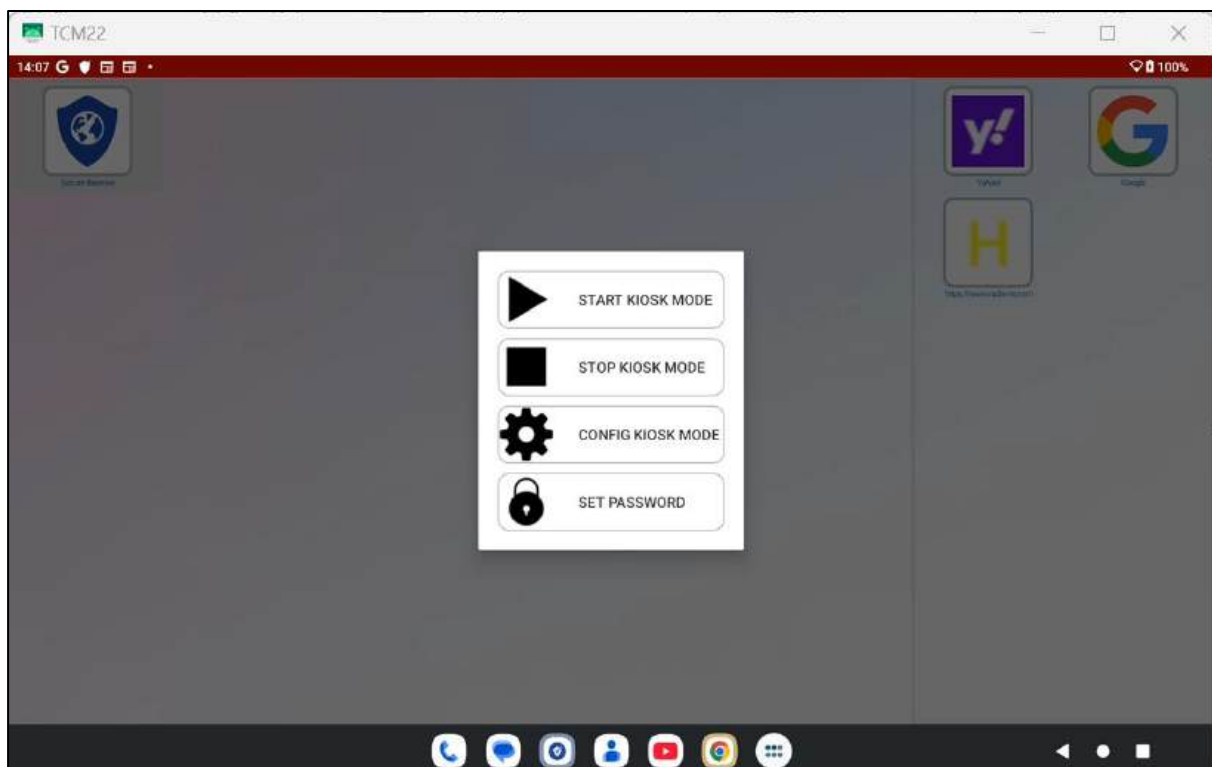


6.1.14.2.3.2.3 Kiosk Settings

If you click on the **Settings** icon, it prompts you for a password to modify the device settings:



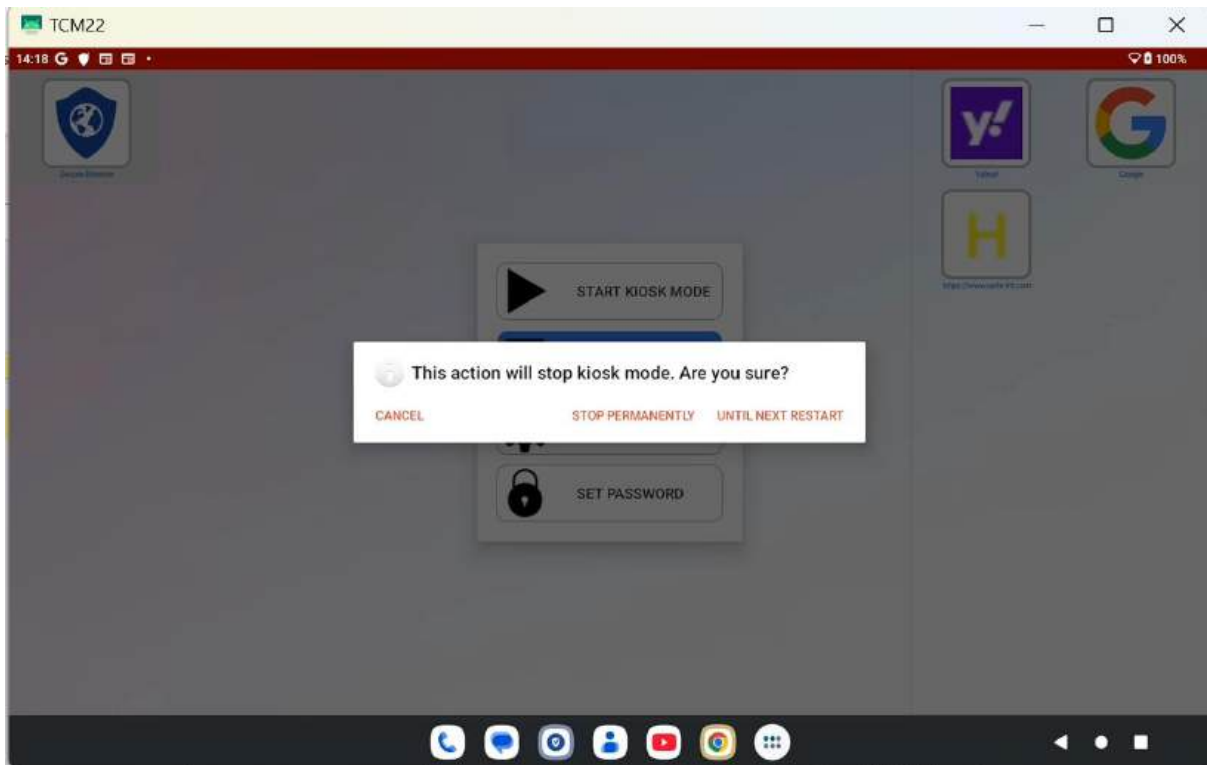
After you enter the password, the **Kiosk Settings** menu appears:



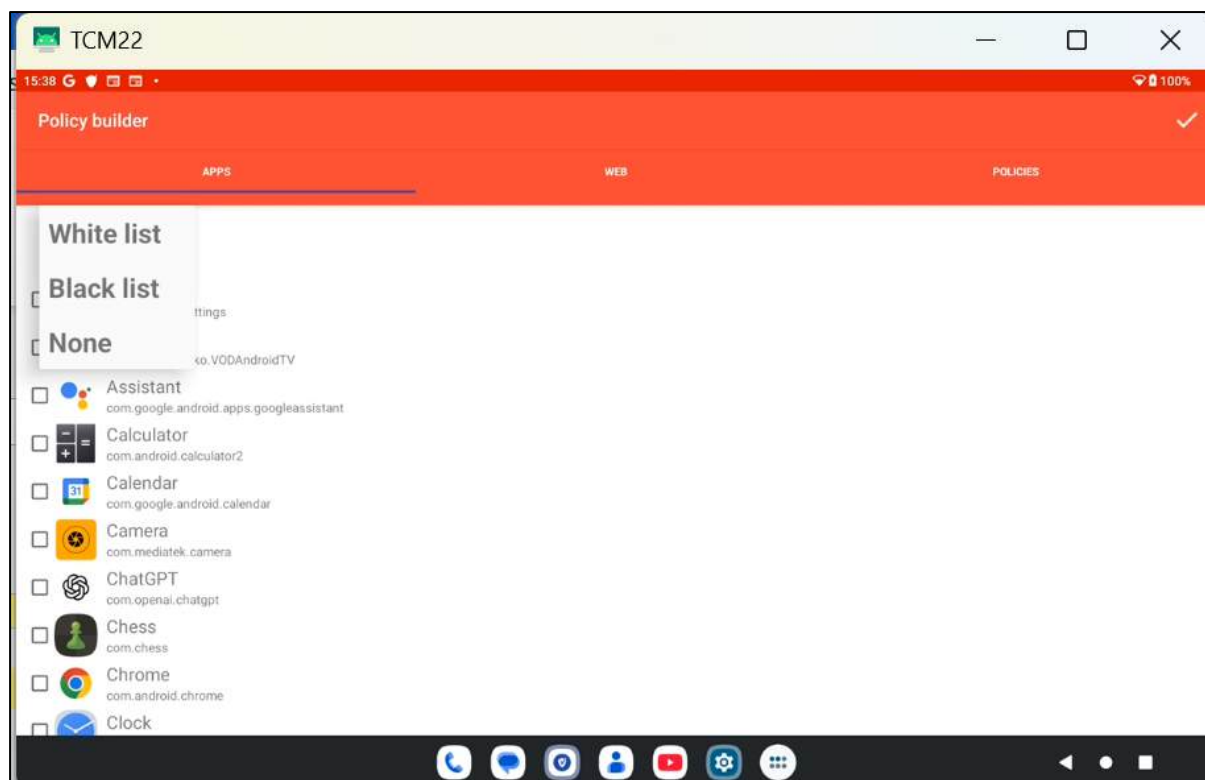
The options are as follows:

- **Start Kiosk Mode:** To resume the Kiosk that you have paused

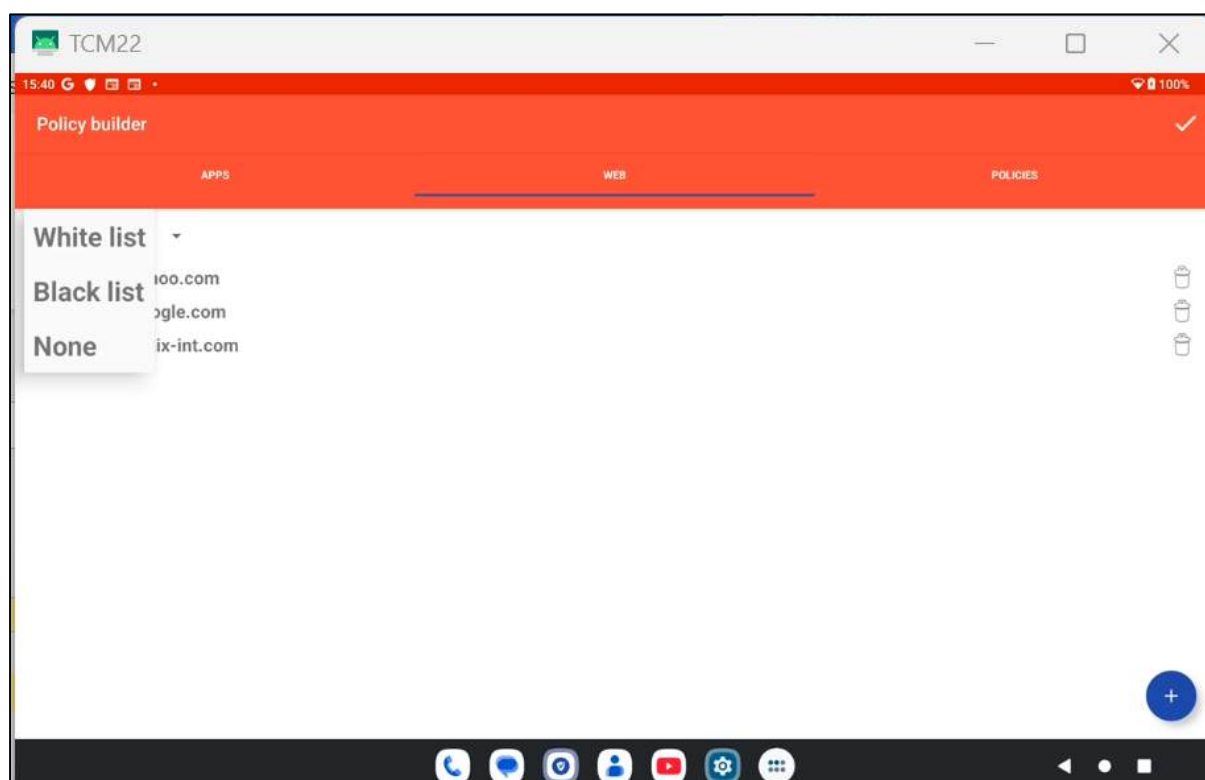
- **Stop Kiosk Mode:** You will be prompted if you wish to stop Kiosk mode permanently, or until the next restart of the device:



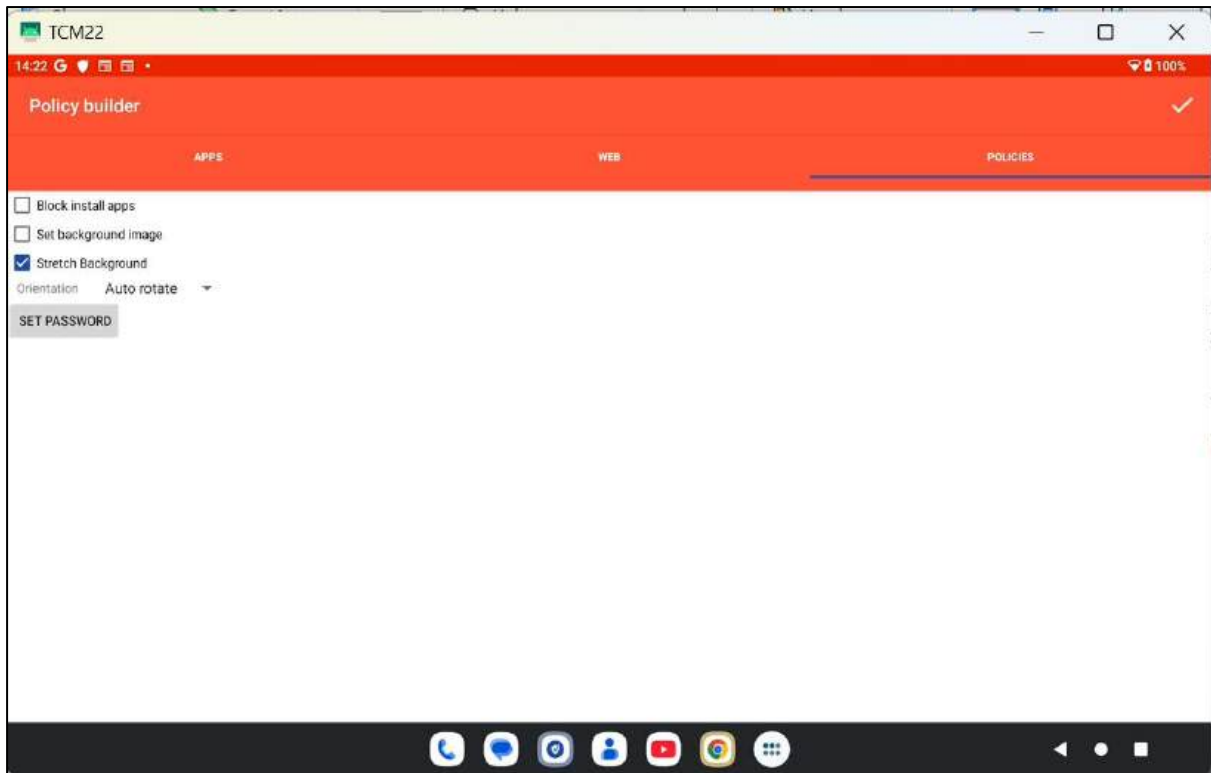
- **Configure Kiosk mode:** This displays a menu where you can select which apps, websites, and background image parameters you would like to display in the kiosk mode:
 - **Apps Policy:** Here, you can either select a whitelist of apps to allow, or a blacklist of apps to disallow, when the kiosk is running.



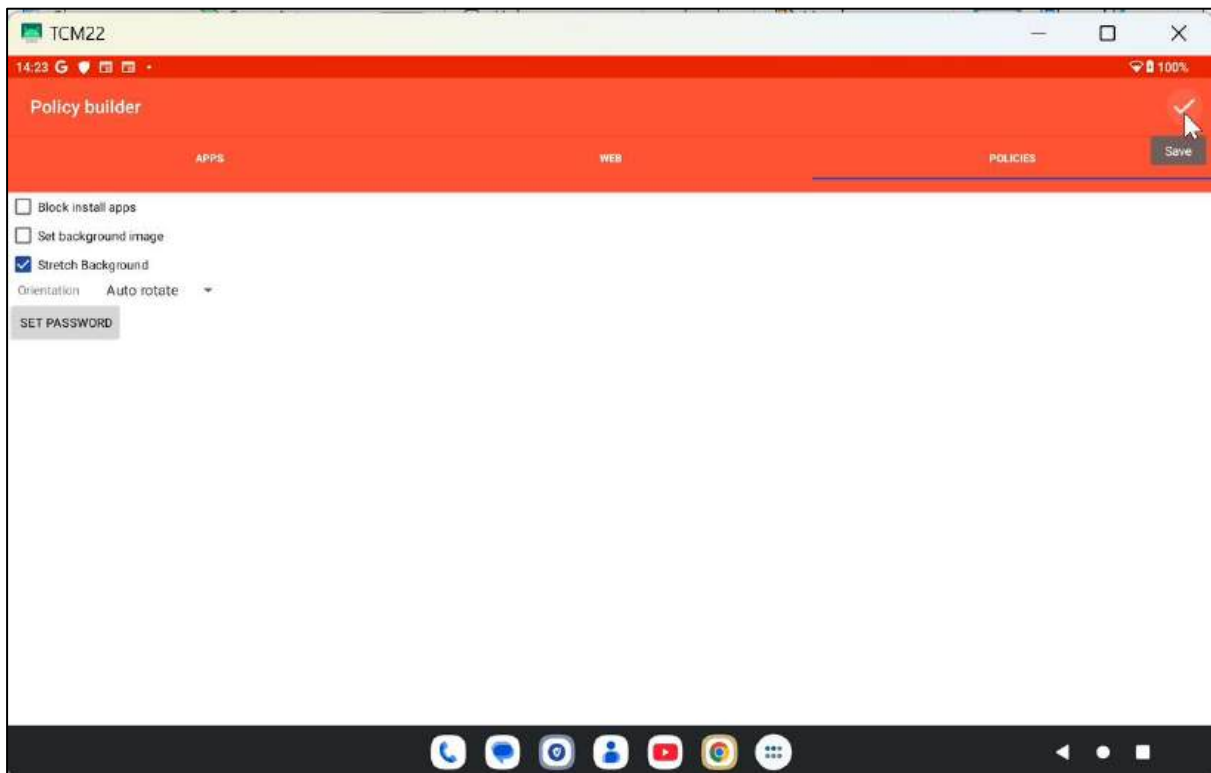
- **Web policy:** This allows you to create a whitelist of allowed URLs, or blacklist of blocked URLs.



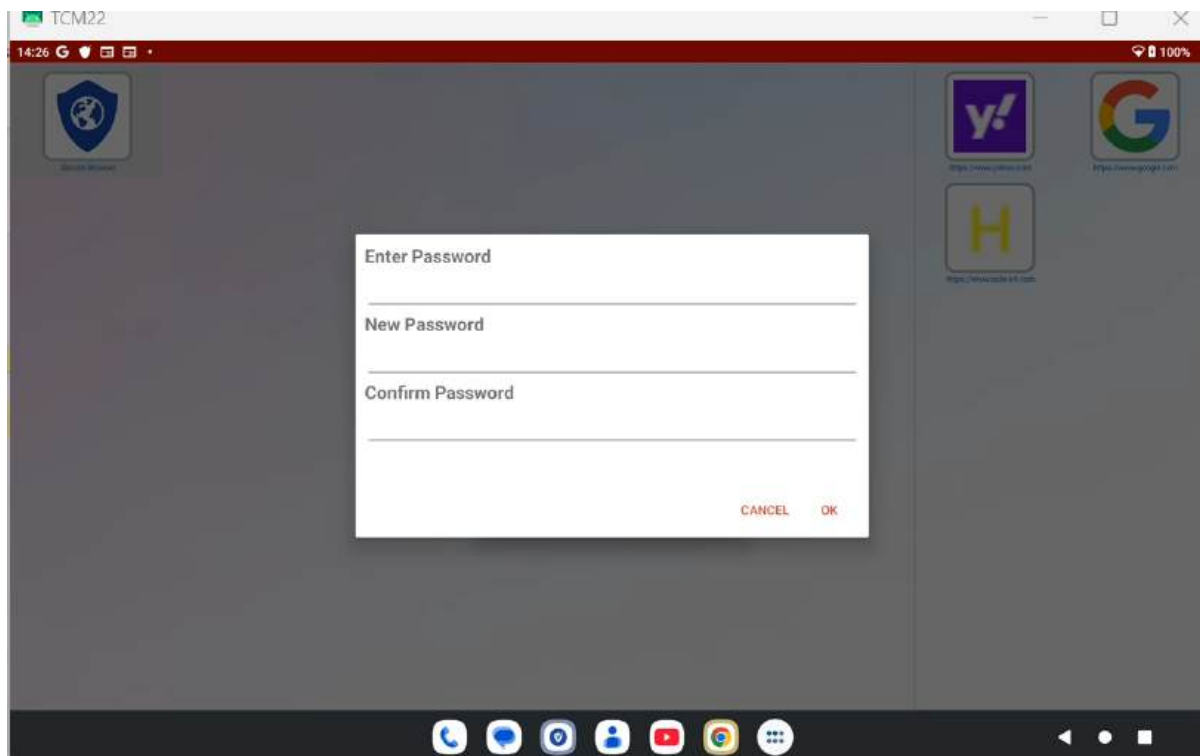
- **Policies:** This allows you to choose the background image and align it, as well as set the password to enter the Kiosk Settings window.



When you have made your selection, click **Save** in the upper right corner:



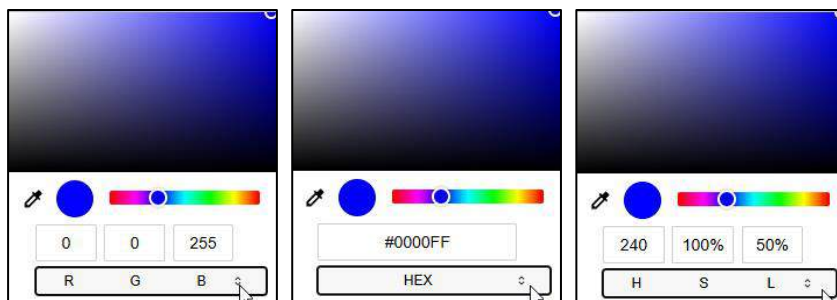
- **Set Password:** This allows you to set a password that you must supply if you wish to modify the kiosk settings in the future.



6.1.14.2.4 Launcher Icons Options

In the Launcher Icons options, you can select:

- **Icon size** (Small, Medium, Large)
- **Font size** (Small, Medium, Large)
- **Font color**, where you can select the font color under the icons in the Kiosk either by RGB, Hex color code, or HSL (hue, saturation, and lightness).



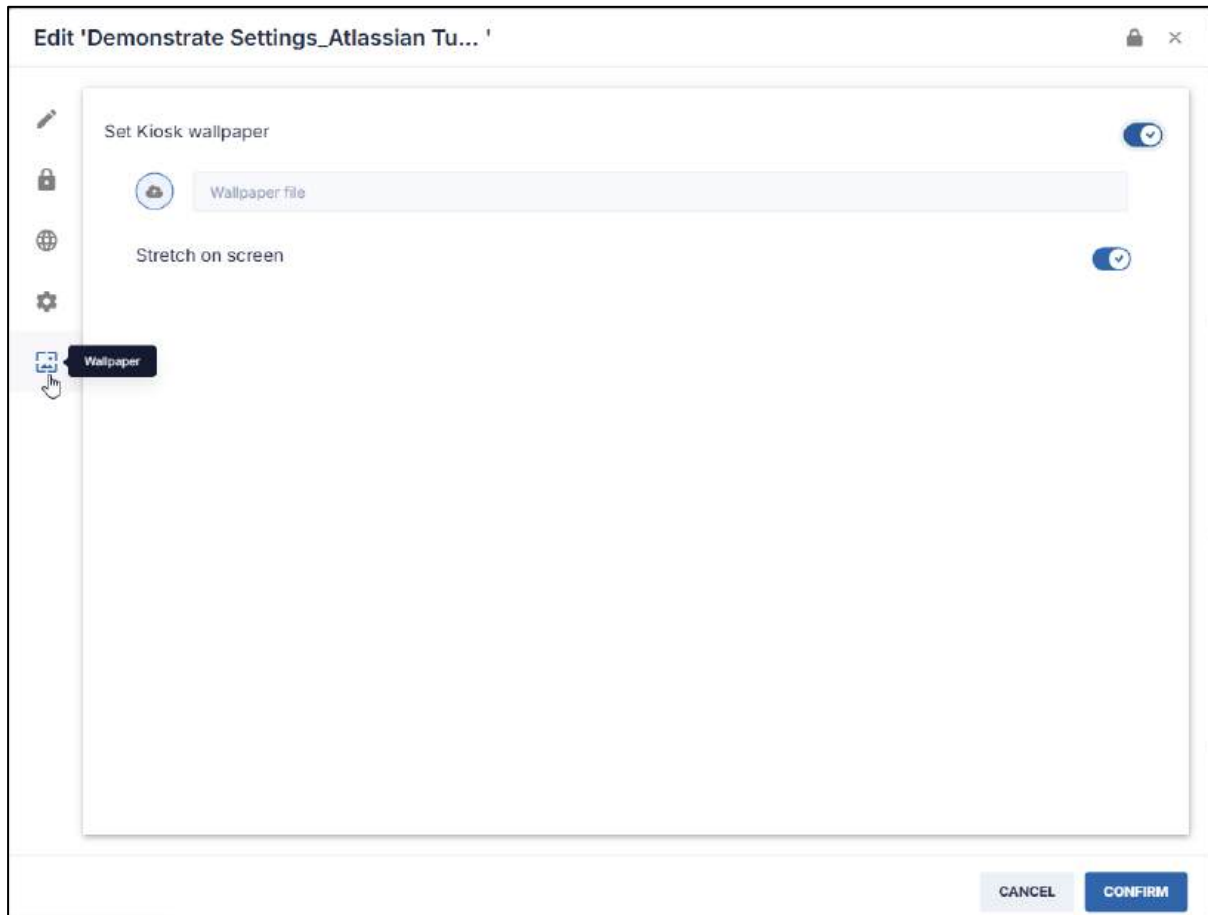
6.1.14.2.5 Power & Input Settings

When you click on the “Keep on while playing” button in the General Settings pane, the remote device will continue to display the Kiosk. It will not enter into a screensaver mode or go blank.



6.1.14.2.6 Kiosk—Wallpaper Selector

1. Back in Kiosk option in the Radix Device Management Platform interface, click on the **Wallpaper** icon  to select an image to serve as the kiosk's wallpaper.



If you do not select a wallpaper, there is a default wallpaper option that will be loaded instead:

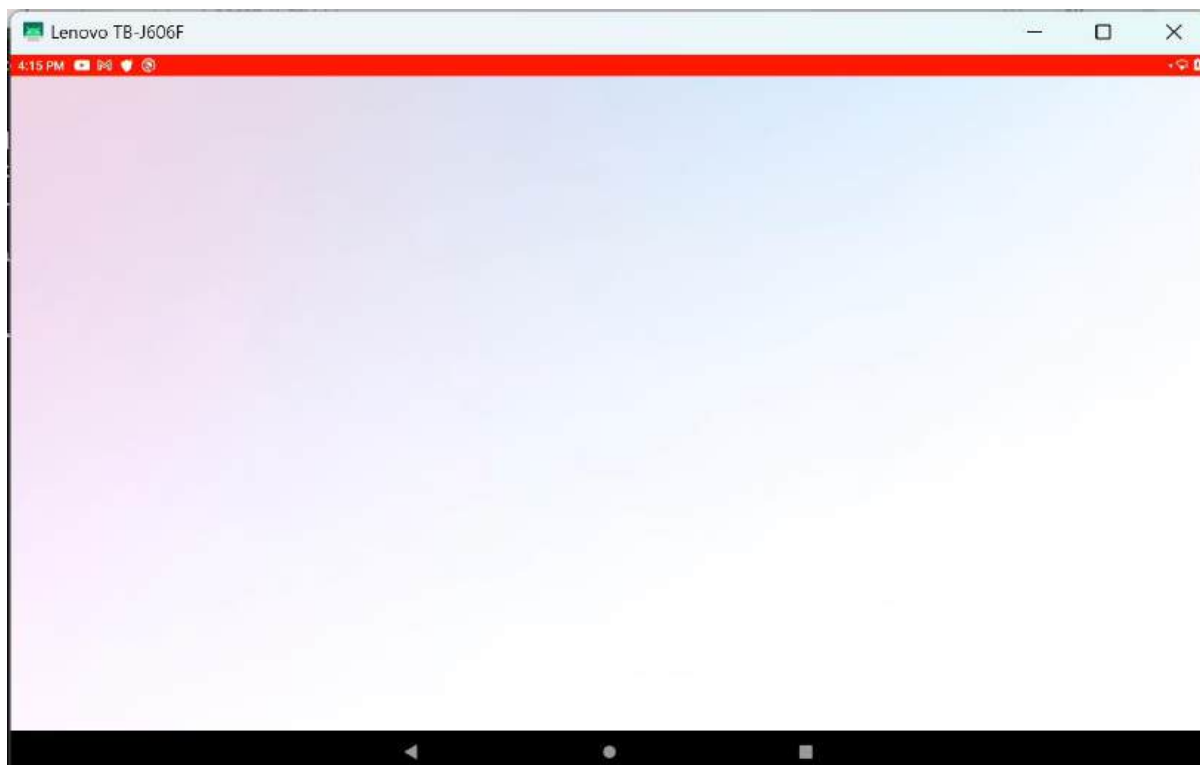


Figure 6-31: Default Kiosk Wallpaper on remote device (no apps have been selected)

2. Click **Confirm**. The kiosk option that you created will be saved in the Kiosk window.
3. To use a kiosk option, select it from the Kiosk window, and click **Apply**.

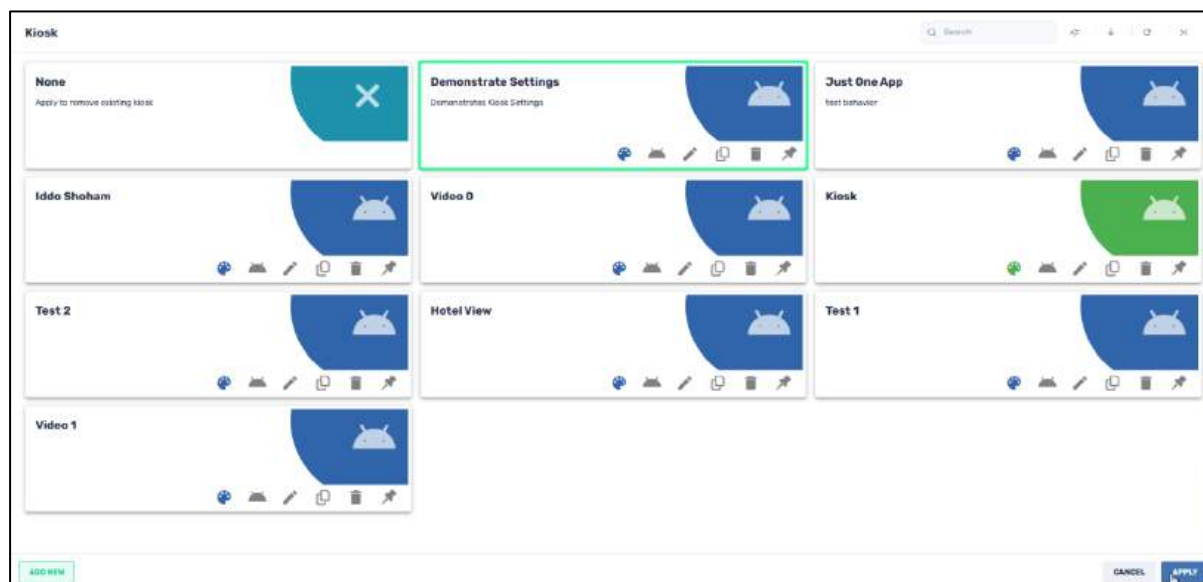
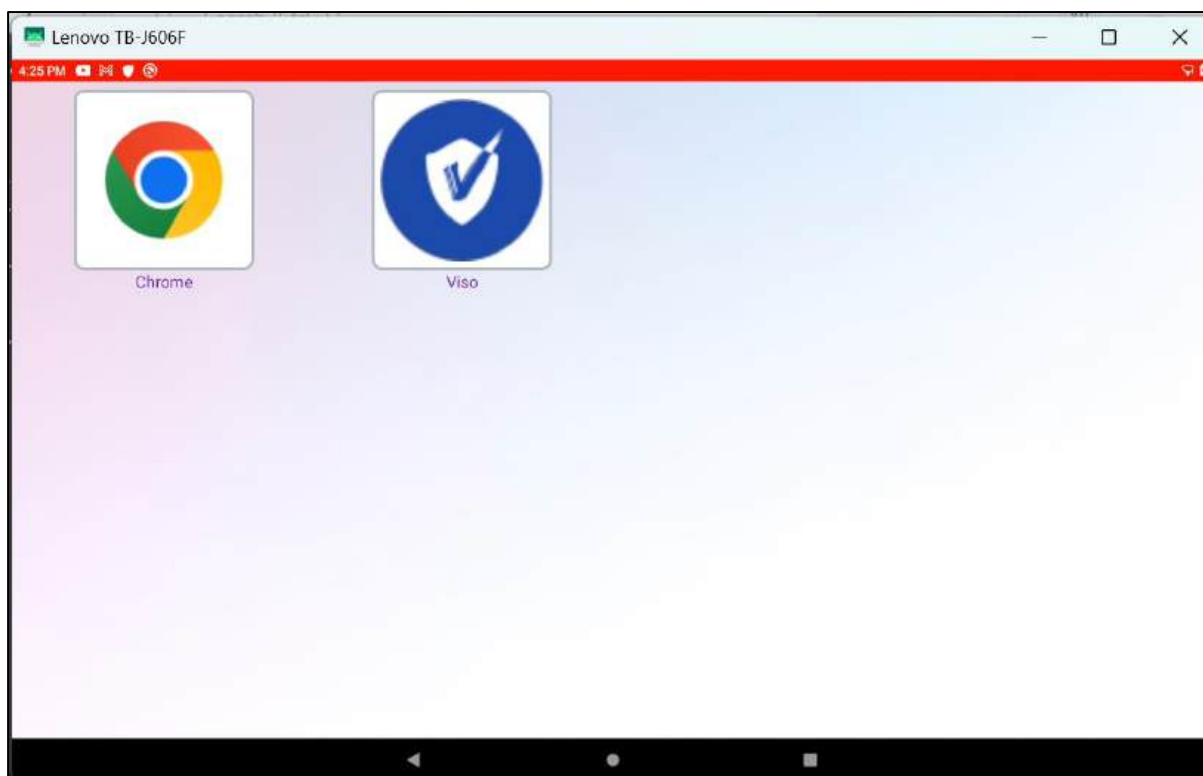


Figure 6-32: This will apply the selected kiosk option on a remote device

Here is the selected kiosk option, illustrating our display choices for the apps we selected: large icons, large font, and purple font color.



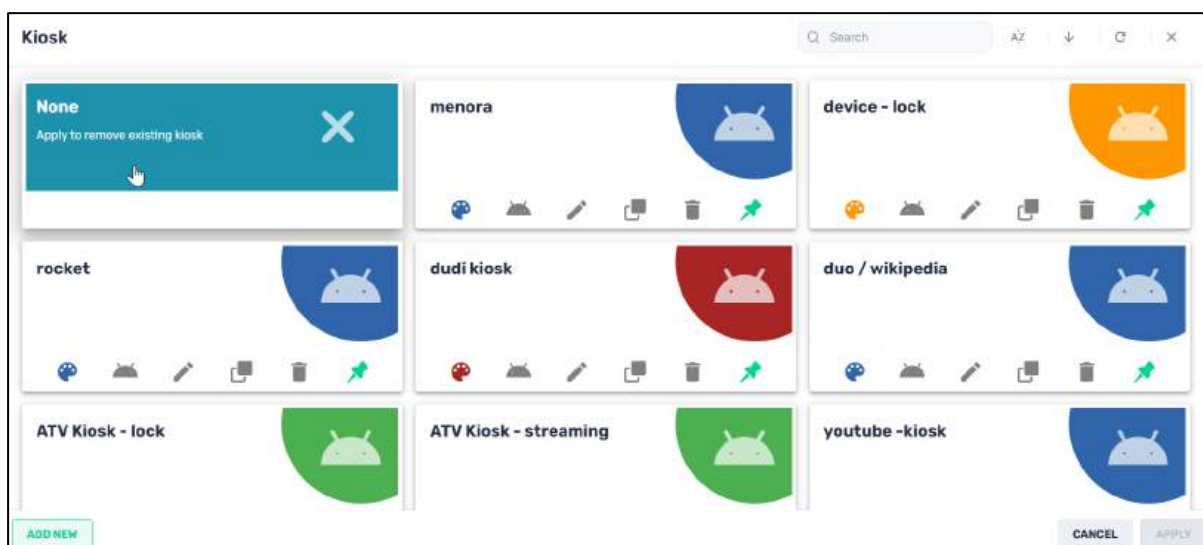
6.1.14.3 Stopping a Kiosk Option

The remote device will be limited only to the selected apps and websites associated with that kiosk item, for the duration of while it is in Kiosk mode. If you want to use the device for other apps, you will have to remove the Kiosk mode that you have applied to the device.

If you wish to stop a kiosk option on a remote device, so that it can go back to normal functioning, you can stop the kiosk mode either from the Radix Device Management Platform, or from the side of the user of the remote device.

6.1.14.3.1 Method One: Stopping the Kiosk from the Radix Device Management Platform side
To remove a Kiosk mode in the Radix Device Management Platform:

1. Select the Kiosk command tile. The Kiosk window opens.



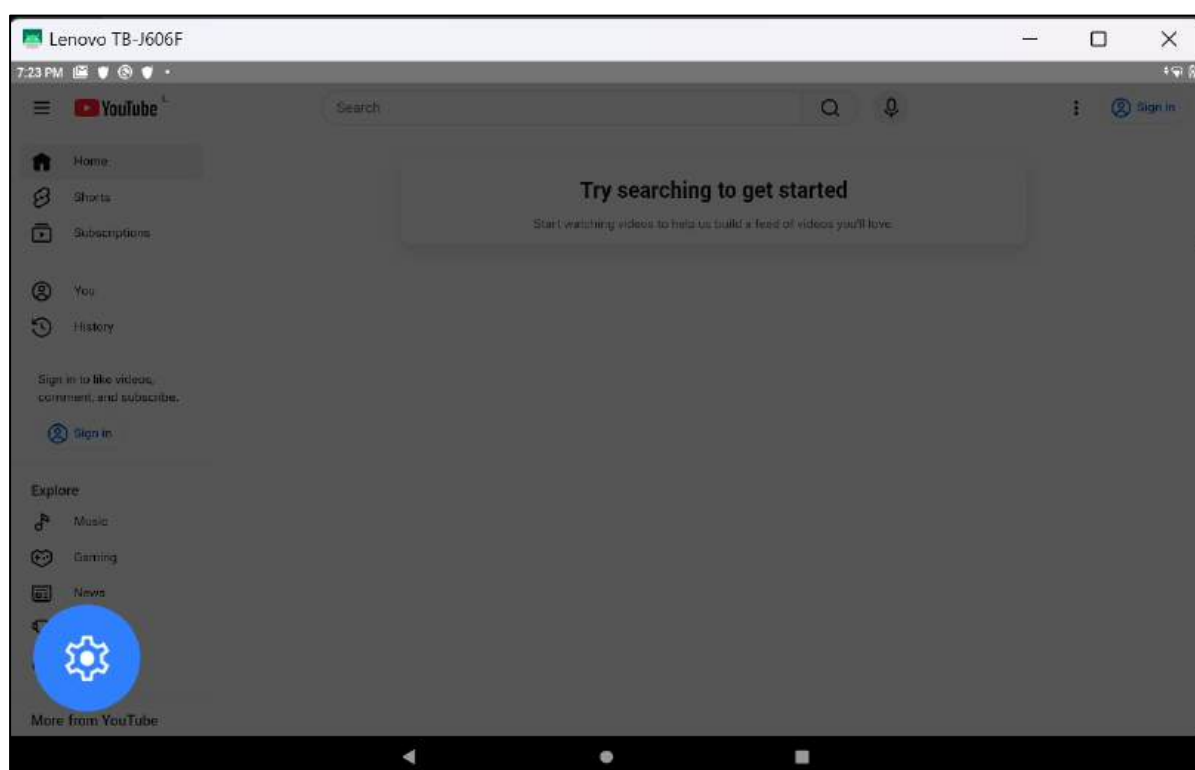
2. Select the **None** option and click **Apply**. The device will now revert to full functionality again.

6.1.14.3.2 Method Two: Stopping a Kiosk Option from the Remote Device (Viso Agent) side

When in Kiosk mode, a remote device is limited to a fixed set of applications and websites. In the event that it is not possible to remove the Kiosk mode from the Radix Device Management Platform, there is also an option for a remote user to cancel Kiosk mode on their remote device.

To remove the Kiosk option from a remote device:

1. On an **Android** device, tap on the screen 5 times, or click the Volume Up and Volume Down buttons three times in quick succession.
2. For a **Windows** or **ChromeOS** device, perform 5 mouse clicks on the computer display. The following screen will be displayed, with a Settings icon:

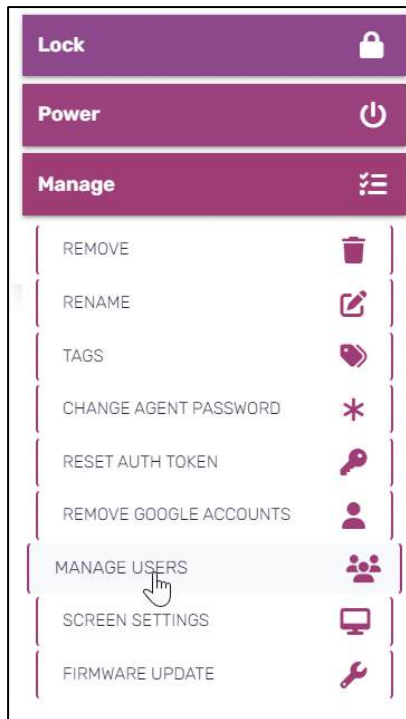


6.1.15 Manage users

This allows you to create or remove users on a particular device.

The **Manage users** feature can be accessed by:

- The device's three-dot menu
- The Bulk Actions drop-down menu,
- The Device Dashboard, under **Manage**.



1. When you click on the **Manage users** icon, the **Manage users** dialog box appears.
2. Supply the username, select **Create user** or **Remove user**, and click **Confirm**.

The screenshot shows a 'Manage users' dialog box with a close button (X) in the top right corner. Inside the dialog, there are three radio button options: 'Create user' (selected), 'Remove user', and 'Change user password'. Below these options is a text input field labeled 'User name'. Underneath the 'User name' field is a checked checkbox labeled 'Set user password'. Below this checkbox are two text input fields: 'Password' and 'Confirm password', each with an eye icon for toggling visibility. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'CONFIRM'.

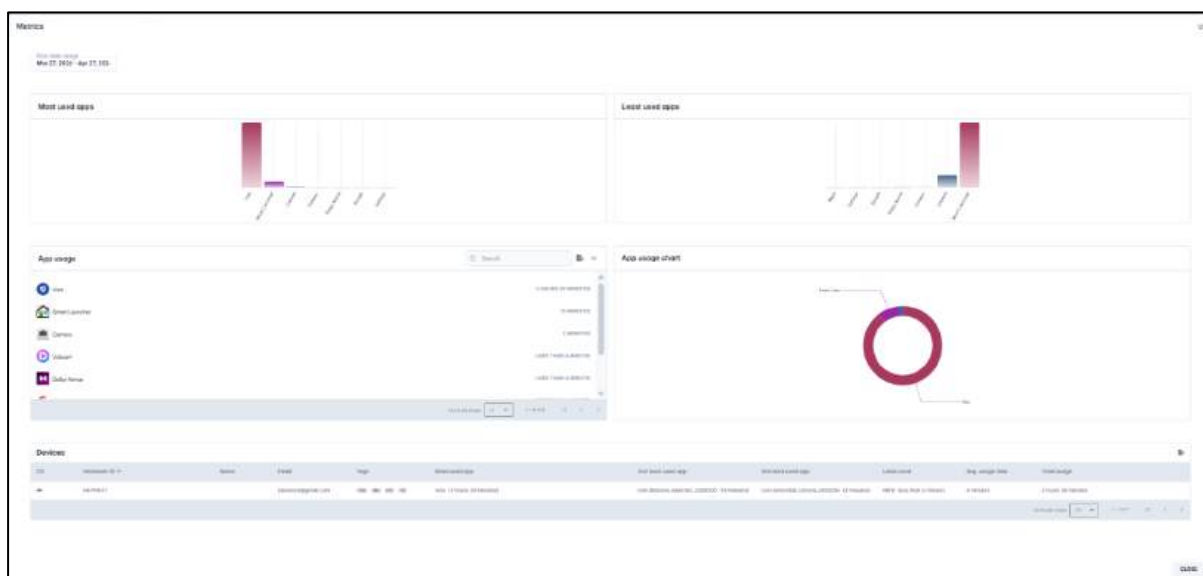
Note: You must have Administrator privileges to use this command to create and remove users on the remote device.

6.1.16 Messaging

See **Section 6.1.1, Advanced Messaging/Messaging**.

6.1.17 Metrics

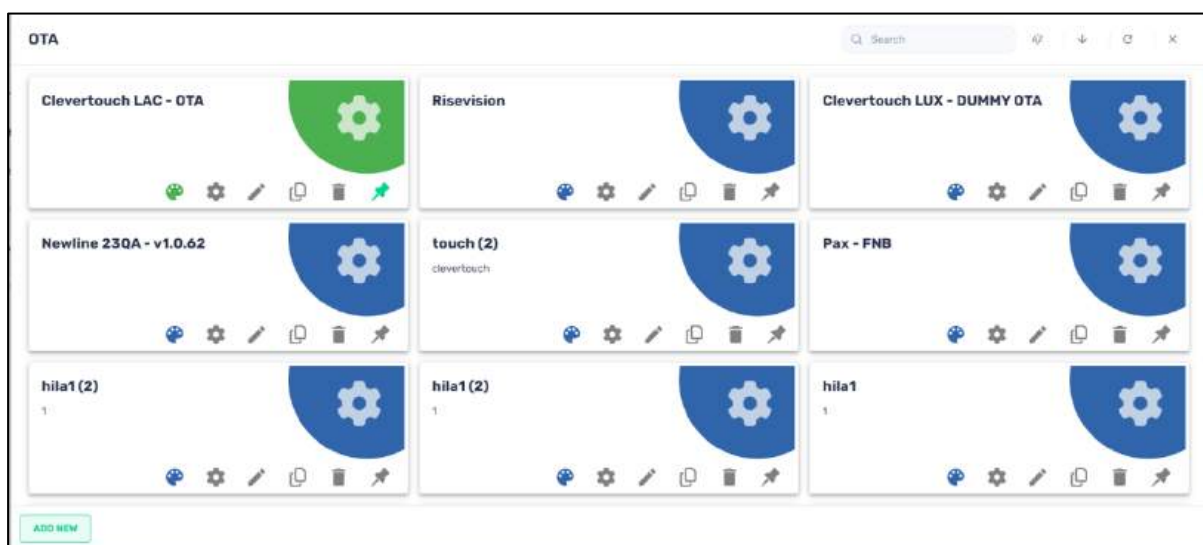
This provides information about the frequency of app usage on a particular device. You can also employ this command on an individual device, several devices, or a group of devices.



6.1.18 OTA

This enables an Android device to receive and install updates to its operating system or apps, or to dispatch an image of an operating system to a device. This option is primarily for older Android devices, running an operating system older than Android 8.0, or that don't employ virtual A/B slot partitions.

When you click on **OTA**, a grid of stored OTA updates appears.



You can choose to edit an existing OTA setting or add a new one.

To edit an existing OTA setting:

1. Select the tile of the desired OTA setting and click on the tile's **Edit** icon. The “Edit” window opens.
2. Supply the name, description, URL etc., and click **Confirm**.

Edit 'newline - wot 2023 V3.0.2'

Name

newline - wot 2023 V3.0.2

Description

File url

http://dudi.devrdx.com:8000/OTA_T982_C4HHT_V3.0.2_20230703.zip

File hash

31dad176f5e2d017ad5743fabc779415

Version

V3.0.2

Set as private

This repository item will be visible only to this user

Hide content from others

Other users can apply this repository but cannot see or open its content

Set as read-only

This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL

CONFIRM

To create a new OTA setting:

1. Click on **Add New** in the OTA panel of options. The **New OTA** window opens.

New OTA

Name

Description

File url

File hash

Version

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

2. Supply the necessary information in the fields. You will have to know the URL of the update file for this method.
3. Click on the **Set as private** button if you would like the OTA setting to only be visible to you (as the creator of the item) when using the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the OTA setting. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
6. Click **Confirm** to save the OTA setting.
7. To send an OTA option to a device, select the relevant tile, and click **Apply**.

6.1.19 OTA Update Engine

This option provides an alternate method of performing an over-the-air update to an Android device’s operating system or apps. The OTA Update Engine option is for devices running Android 8.0 or newer, and that employ the A/B partition updater.

When you click on **OTA Update Engine**, a grid of stored OTA updates appears:



To create a new OTA Update Engine setting:

1. Click on **Add New** in the lower left corner. The following window opens:

The screenshot shows the 'New OTA Update engine' form. It contains the following fields and controls:

- Name**: A text input field.
- Description**: A text input field.
- Select upload method**: A dropdown menu with 'Upload file' selected.
- ADD FILE**: A blue button.
- Version**: A text input field.
- CANCEL** and **CONFIRM**: Buttons at the bottom right.

There are two upload methods:

New OTA Update engine

Name

Description

Select upload method

Upload file

File from URL

Version

Model

All models

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

2. To upload an OTA update file from your computer, click on **Add File**, and attach the file.
3. To upload an OTA update file from an URL, select **File from URL** from the dropdown list. The following window opens:

New OTA Update engine

Description

Select upload method

File from URL

Payload url

Payload size

Version

Model

All models

Offset

Headers

header

header

header

header

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

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

4. Supply the signed payload URL, the payload size of the file, and the other parameters, and click **Confirm**. The OTA Update Engine option will be saved to the repository.

When you employ the OTA update selection, the Radix Device Management Platform will stream the update file, verify it, and write it to the device's operating system.

6.1.20 Play Siren

This option sounds an alarm on the device. This may be handy in an emergency situation, or if the device has been stolen. You can instruct the device to sound off the alarm if it is taken outside of a specified geographical area.



6.1.21 Policies (Block Lists)

If certain applications on your device violate your rights, have security issues, or are not play-protected, you can essentially blacklist and block these applications.

You can access this command by clicking on a **device's three-dot menu>Configure>Block Lists**.

Alternatively, you can select a device and access this command by clicking on **Bulk Actions>Configure>Block Lists**.

When you click on **Block Lists**, a grid of stored policies (block lists) appears.

6.1.21.1 Applying a Software Policy

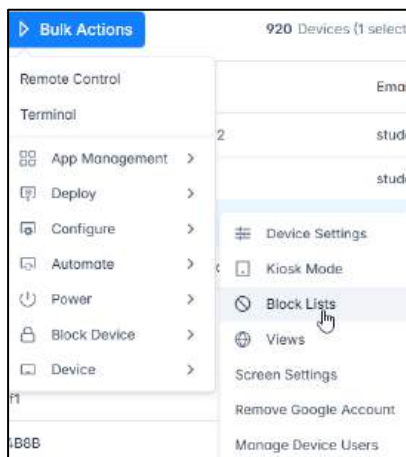
You can select an existing software policy, or add and apply a new one:

To add a new policy:

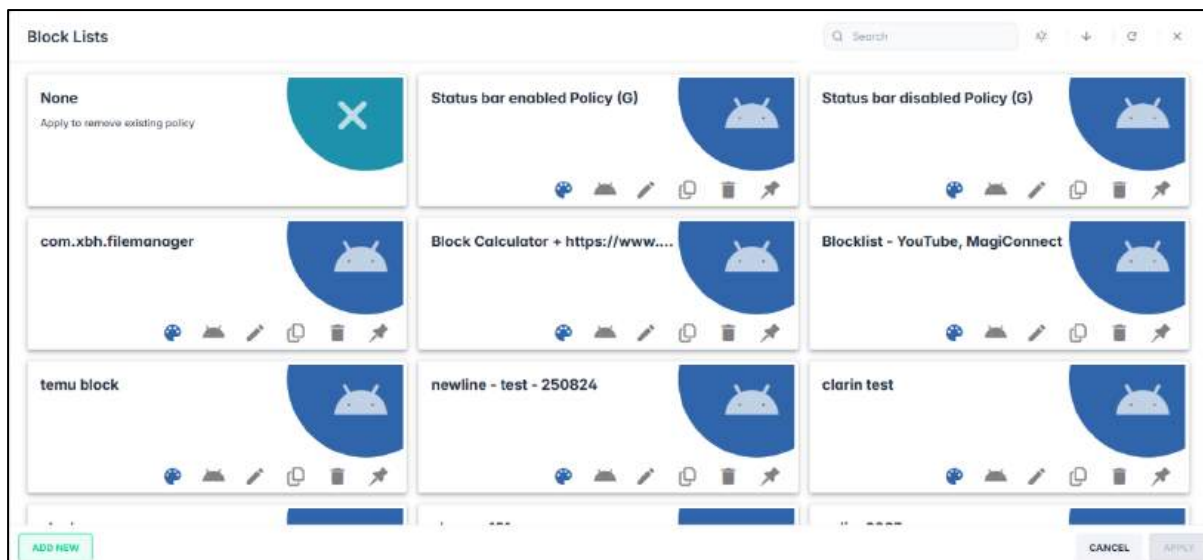
Method One: From the Bulk Actions Button:

If you have selected a particular device (or devices) in the Devices Table, the Bulk Actions button will display a drop-down menu of options.

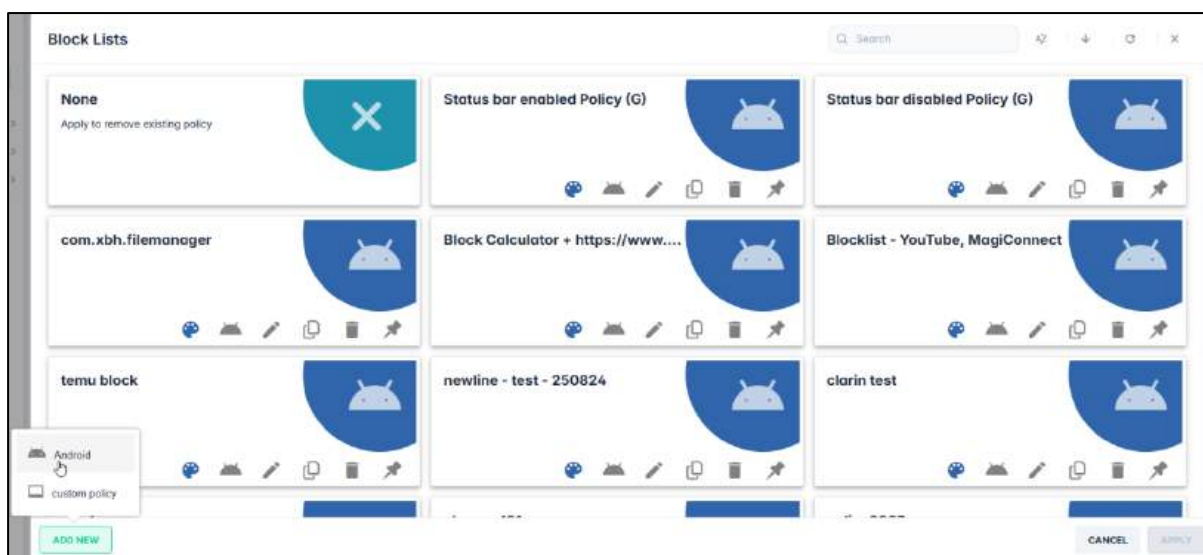
1. Click on the checkbox of the Android device for which you would like to create a new policy.
2. Click on **Bulk Actions>Configure>Block Lists**.



The **Block Lists** repository opens.



2. Click on the **Add New** button in the lower left. Since you selected an Android device in the Devices Table, you can select whether to create a policy item for an Android device or a custom policy:



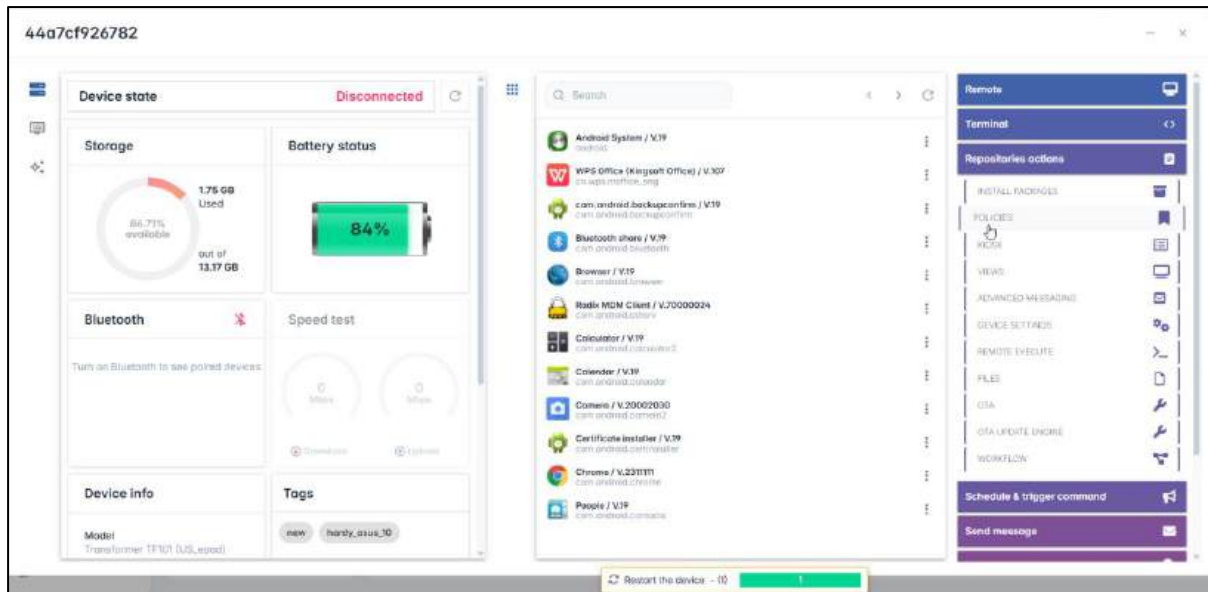
Method Two: From the Device's Dashboard

1. Click on the row of the device to which you would like to apply a block list of apps and websites.



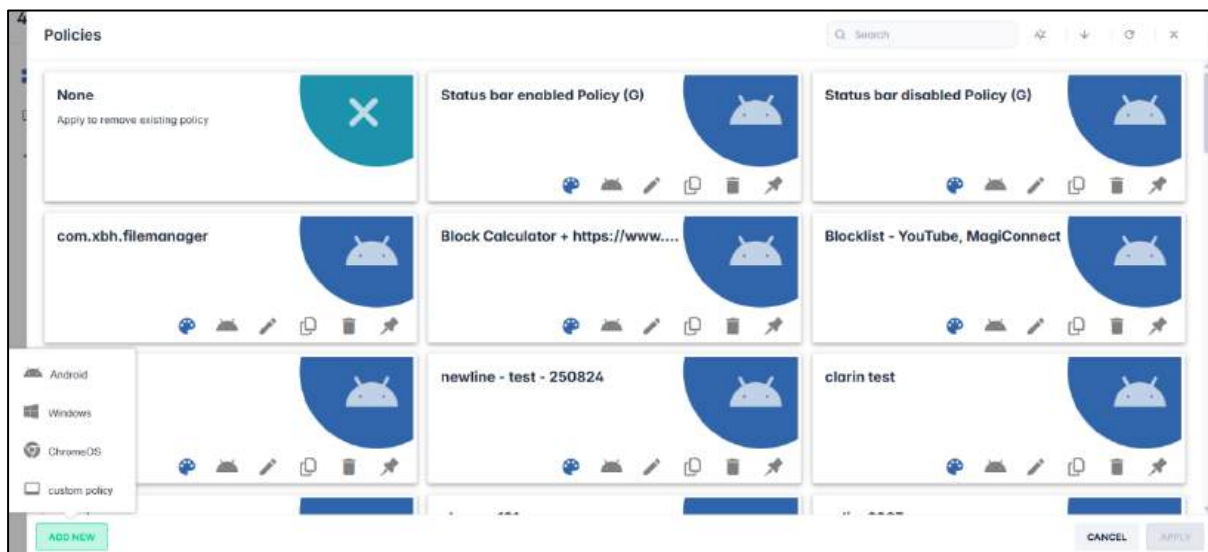
The device's dashboard opens.

2. Go to **Repository actions>Policies**.



The Policies repository window opens.

3. Click on **Add New** button in the lower left. If you would like to install policies on a group of devices that employ different operating systems, you will be prompted as to which operating system you wish to apply a software policy.



Once you select the operating system, the **New Policy** screen opens. The parameters that you must provide will differ, depending on the operating system that you select.

6.1.21.1.1 Adding a New Android Policy

When you click on the Android icon to create a new Android policy, the following screen appears:

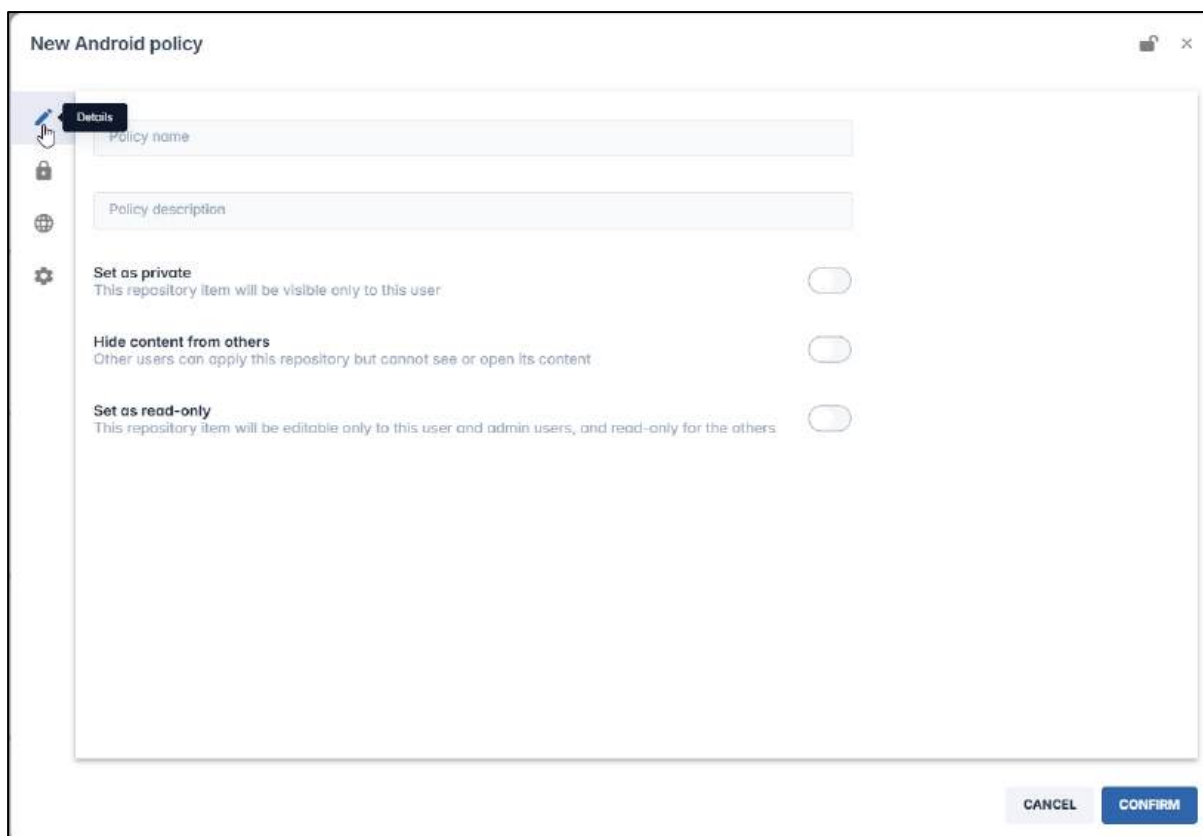


Figure 6-33: Android Policy Edit Screen

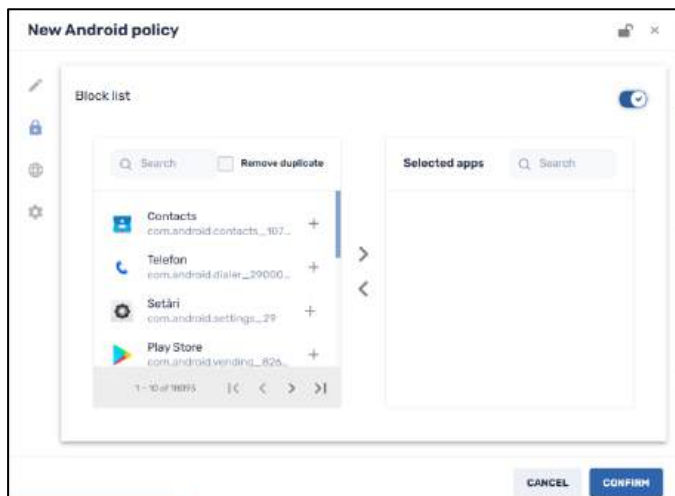
The following is a brief explanation of the icons on the left of the Android Policy screen:

Table 6-4: Android Policies icons

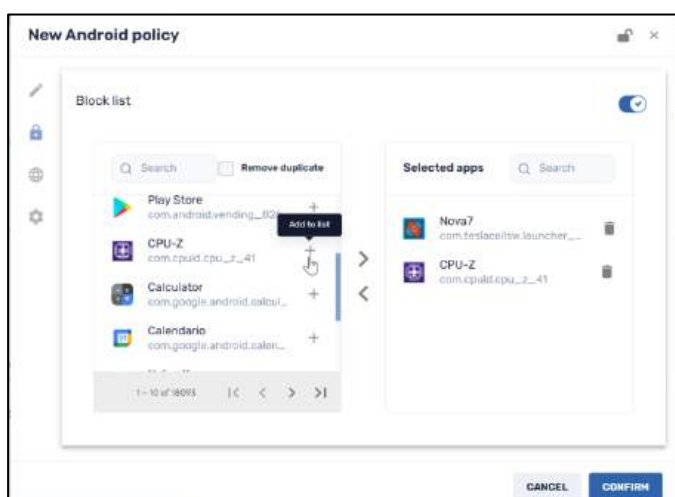
Icon	Description
	Edit Details
	Block List
	Web Content Filter
	General

1. In the **Edit Details** window, enter a policy name and description.
2. Click on the **Set as private** button if you would like the Android policy option to only be visible to you (the creator of the item) when using the Radix Device Management Platform.
3. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Android policy. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .

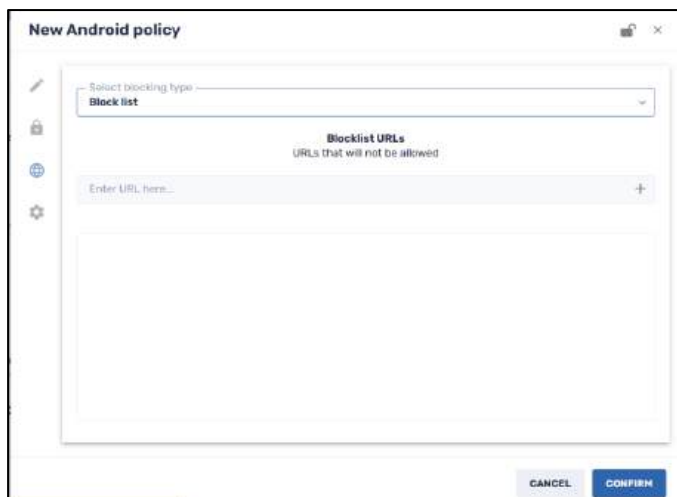
- Click on the **Block List** icon . The **Block List** window opens.



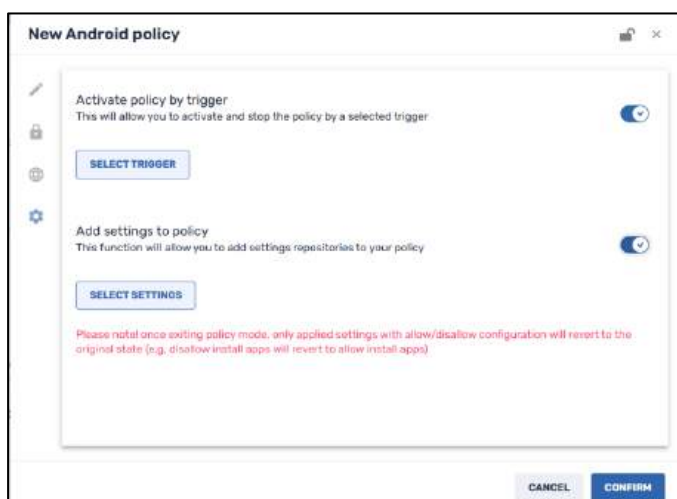
- Select the apps that you wish to block from the device by clicking on the **Add to list** icon. The selected apps will now appear in the right-hand column of Selected apps.



- Click on the **Web Content Filter** icon  and select the type of list you are applying to this policy: a list of apps to be allowed, or a list of apps to be blocked.
- Supply the URLs of the apps to be blocked, or to be allowed.



9. Click on the **General** icon . The General window opens. This window allows for setting a trigger to activate or stop a device policy.



10. Supply the trigger and settings and click **Confirm**. The new policy will appear in the **Policies** window.
11. Apply the policy to a device by selecting the policy and clicking **Apply**.

6.1.21.1.2 Adding a New Windows Policy

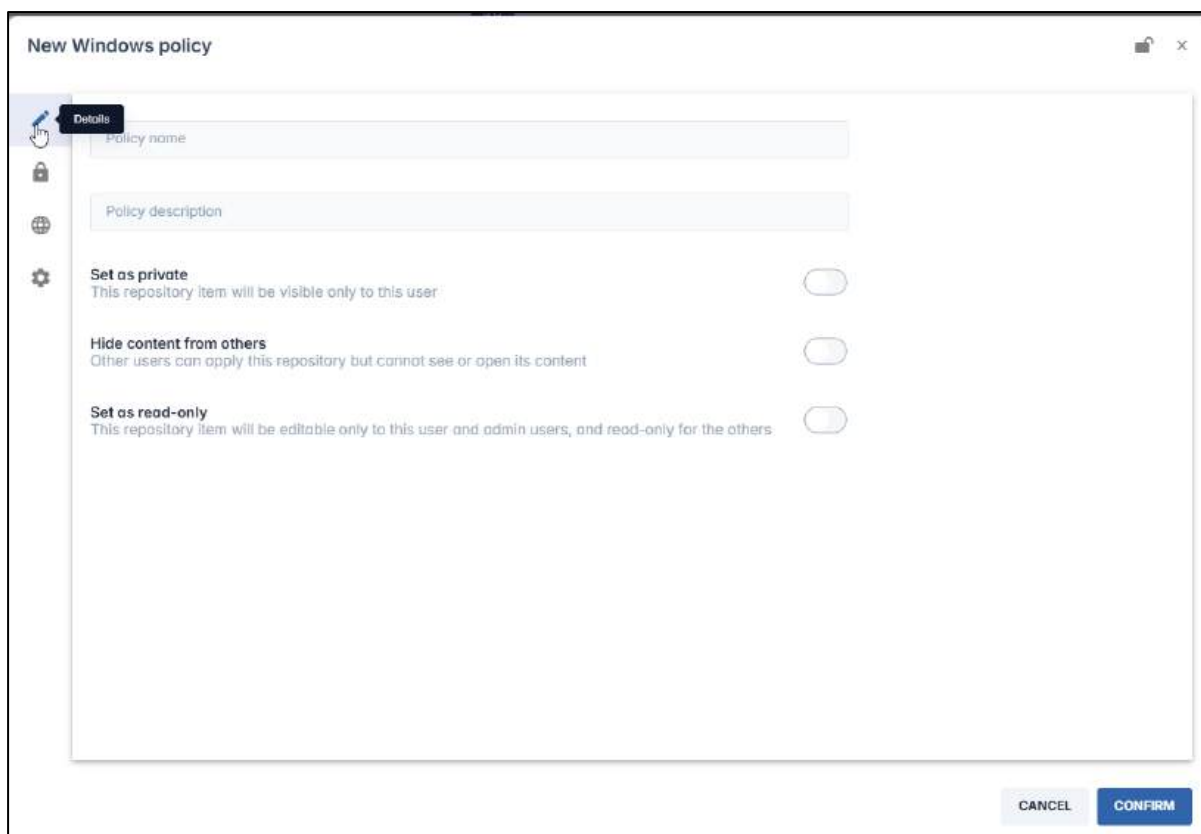
When you select the option to add a new Windows policy, the following window appears.

The following is a brief explanation of the icons on the left of the Windows Policy screen:

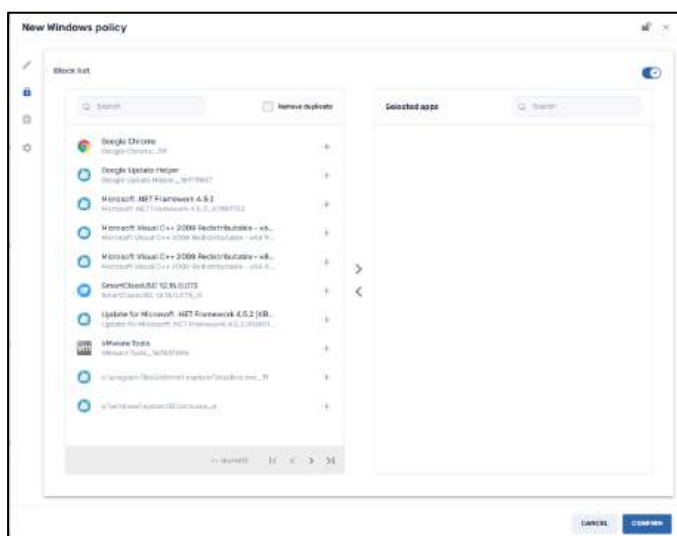
Table 6-5: Windows Policies icons

Icon	Description
	Edit Details
	Block List
	Web Content Filter
	General Tab

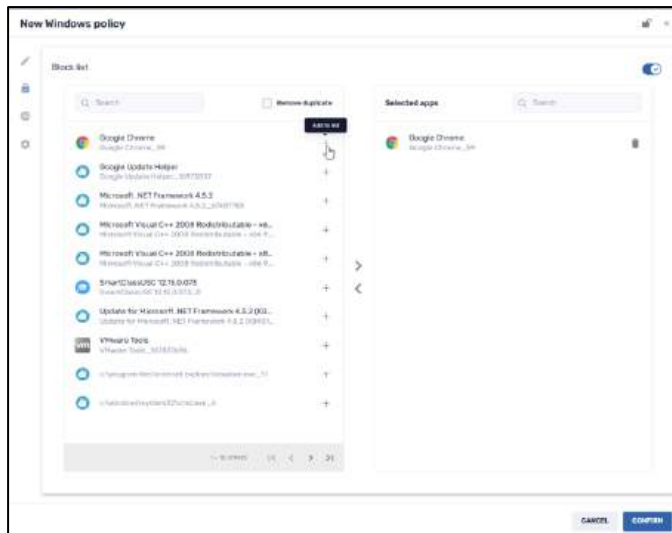
1. In the **Edit Details** window, enter a policy name and description.
2. Click on the **Set as private** button if you would like the Windows policy option to only be visible to you (the creator of the item) when using the Radix Device Management Platform.
3. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Windows policy. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .



5. Click on the **Block List** icon. The **Block List** window opens.



6. Select the apps that you wish to block from the device by clicking on the **Add to list** icon. The selected apps will now appear in the right-hand column of Selected apps.



- Click on the **Web Content Filter** icon  and select the type of list you are applying to this policy: a list of apps to be allowed, or a list of apps to be blocked.



- Supply the URLs of the apps to be blocked, or to be allowed.



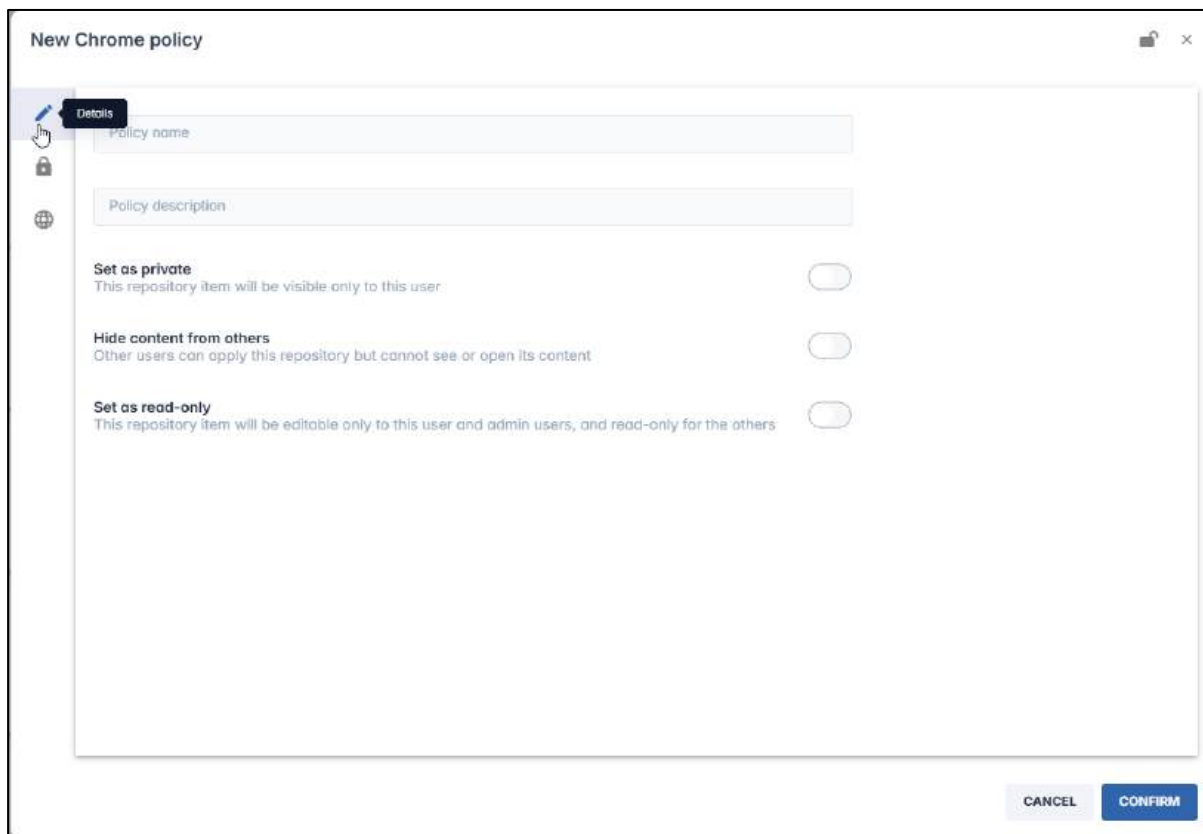
9. Click on the **General** icon . The General window opens. This window allows you to determine whether a Windows device can accept USB devices. It also allows you to set a trigger to activate or stop a device policy.



10. Supply the trigger and settings and click **Confirm**. The new policy will appear in the **Policies** window.
11. Apply the policy to a device by selecting the policy and clicking **Apply**.

6.1.21.1.3 Adding a New ChromeOS Policy

When you select the option to add a new ChromeOS policy, the following window appears.

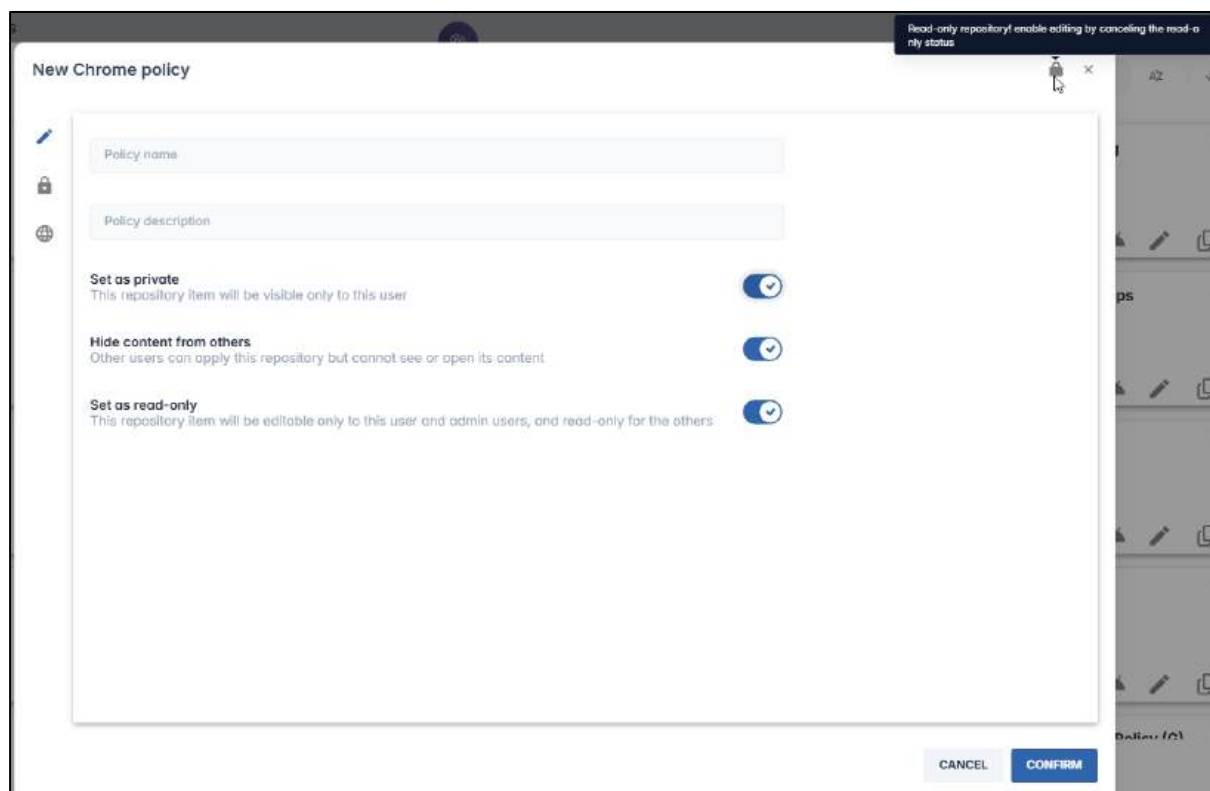


The following is a brief explanation of the icons on the left of the ChromeOS Policy screen:

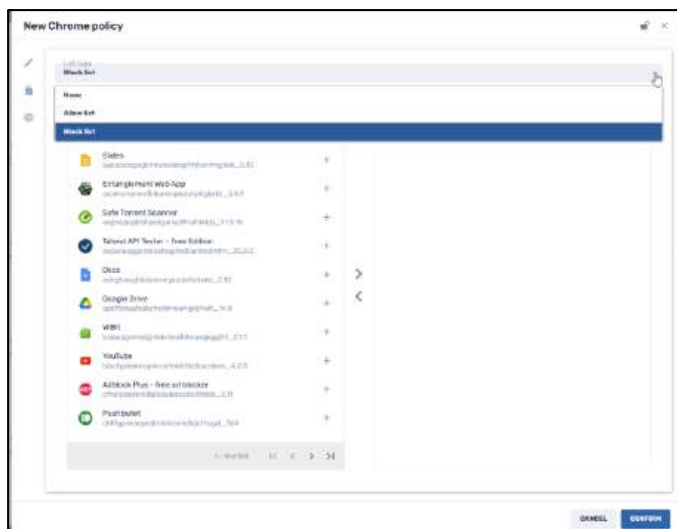
Table 6-6: ChromeOS Policies icons

Icon	Description
	Edit Details
	Block List
	Web Content Filter

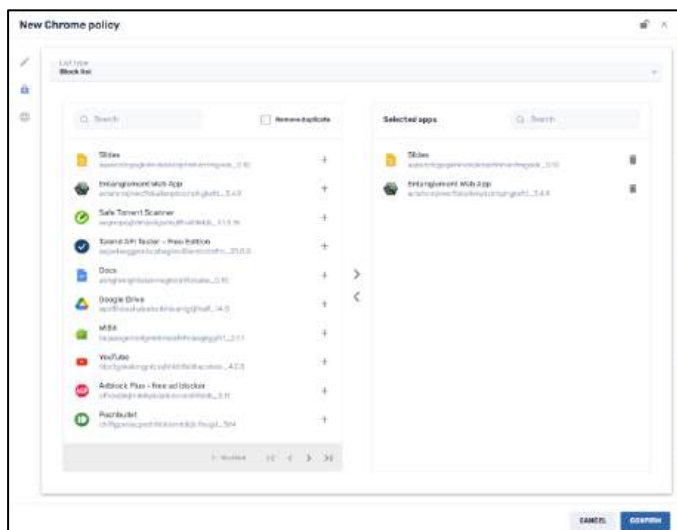
1. In the **Edit Details** window, enter a policy name and description.
2. Click on the **Set as private** button if you would like the ChromeOS policy option to only be visible to you (the creator of the item) when using the Radix Device Management Platform.
3. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the ChromeOS policy. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .



5. Click on the **Block List** icon. The **Block List** window opens.



6. Select the apps that you wish to block from the device by clicking on the **Add to list** icon. The selected apps will now appear in the right-hand column of Selected apps.



7. Click on the **Web Content Filter** icon  and select the type of list you are applying to this policy: a list of websites to be allowed, or a list of websites to be blocked.



8. Supply the URLs of the apps to be blocked, or to be allowed.



9. Click **Confirm**. The new policy will appear in the **Policies** window.
10. Apply the policy to a device by selecting the policy and clicking **Apply**.

6.1.21.1.4 Adding a New Custom Policy

The Custom Policy option is for managers of specific devices to create a unique device policy.

When you select the option to add a new Custom policy, the following window appears.

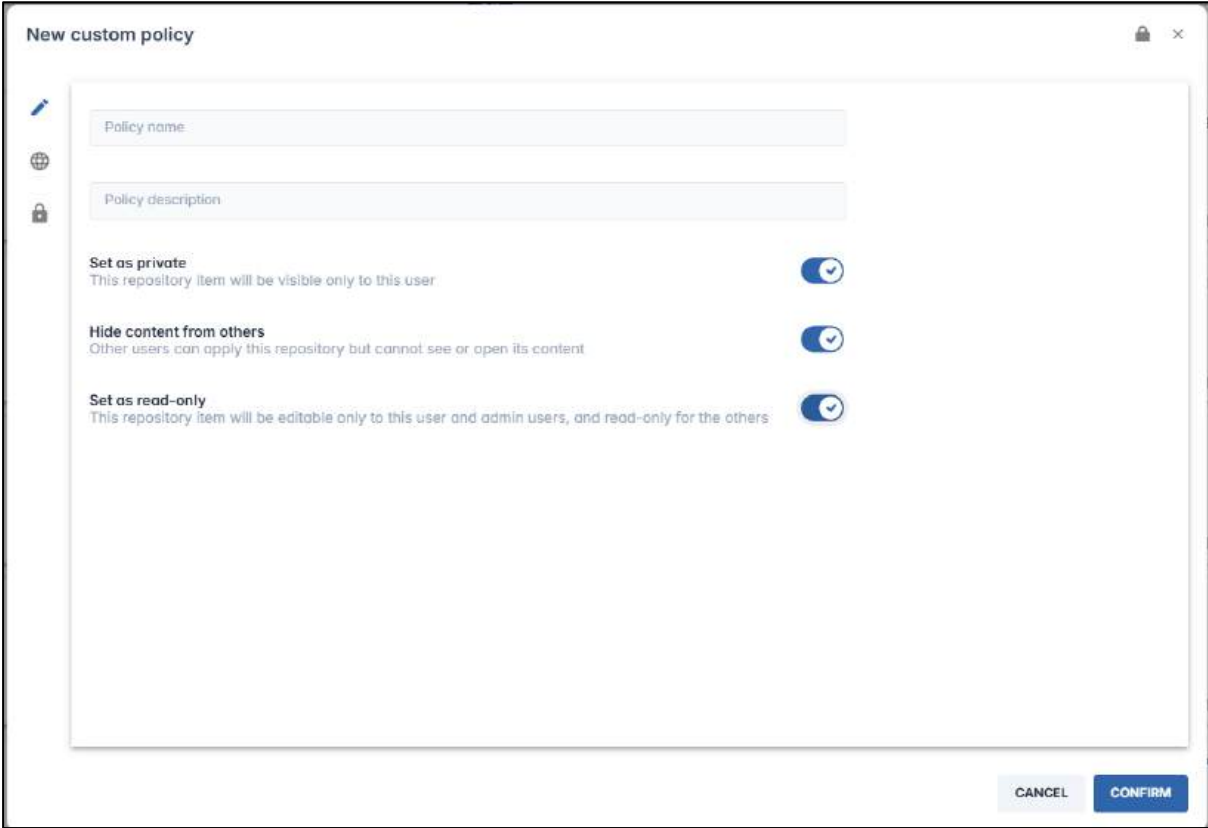


The following is a brief explanation of the icons on the left of the Custom Policy screen:

Table 6-7: Custom Policies icons

Icon	Description
	Edit Details
	Block List
	Settings Lockdown

1. In the **Edit Details** window, enter a policy name and description.
2. Click on the **Set as private** button if you would like the custom policy option to only be visible to you (the creator of the item) when using the Radix Device Management Platform.
3. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Custom policy. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .



5. Click on the **Web Content Filter** icon  and select the type of list you are applying to this policy: a list of websites to be allowed, or a list of websites to be blocked.



6. Supply the URLs of the apps to be blocked, or to be allowed.

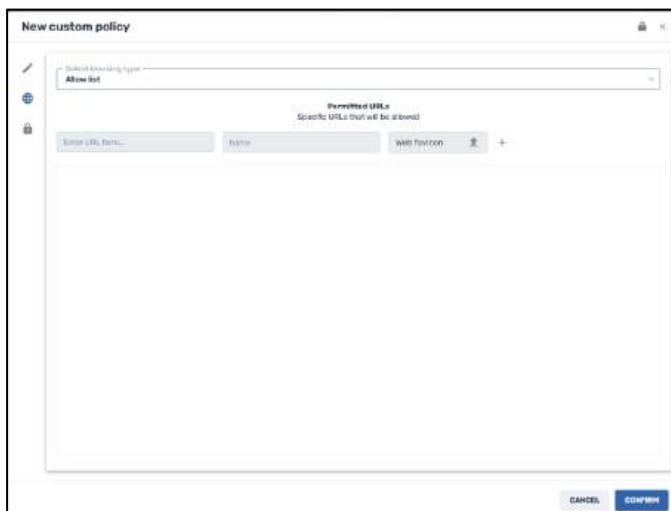
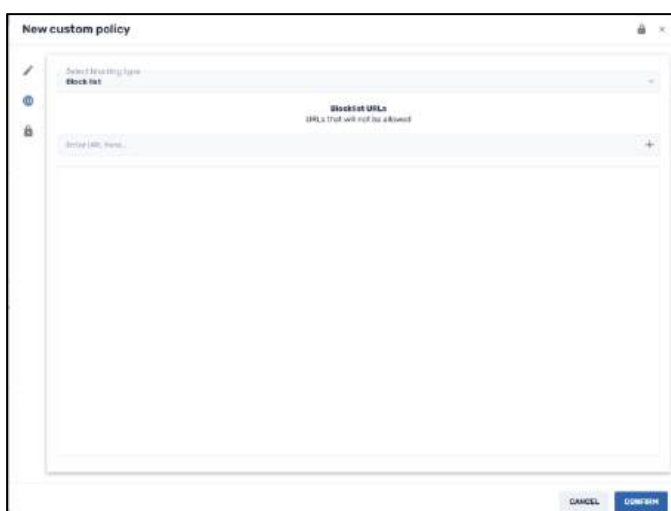


Figure 6-34: Creating a list of allowed URLs

7. If you wish to create a list of blocked URLs, select the **Block List** icon. The **Block List** window opens.



- Enter a URL that you would like to block and click on the **Add URL to list** icon.



Note: You must supply the URL in the form **https://** for it to be valid.

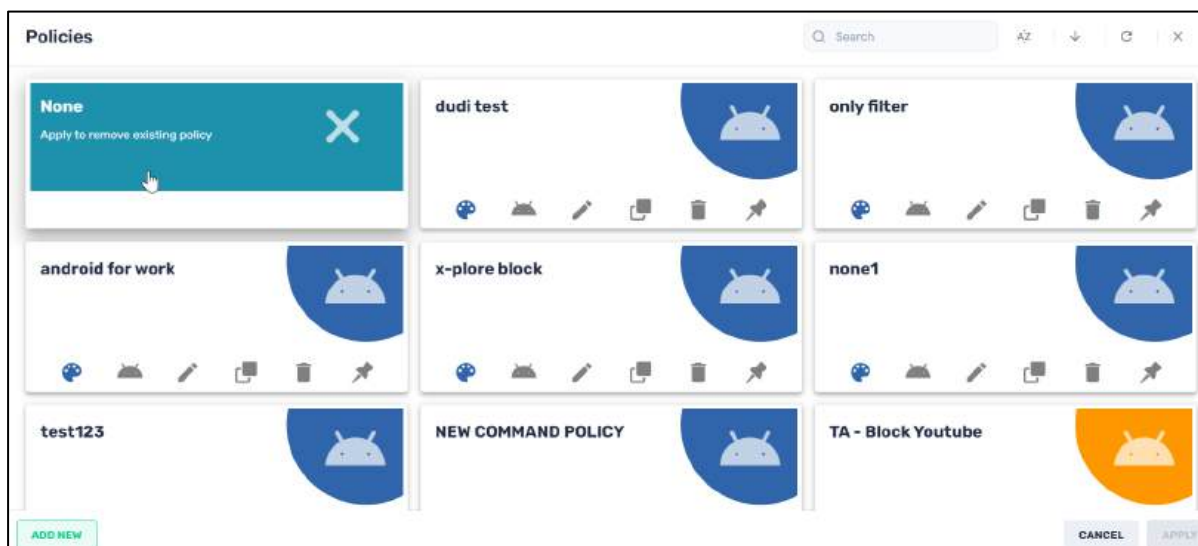
- Click **Confirm**. The new policy will appear in the **Policies** window.
- Apply the policy to a device by selecting the policy and clicking **Apply**.

6.1.21.2 Removing a Software Policy from a Device

If you wish to remove the software policy that you applied to a device, there is an option in the Policies screen to erase any policies.

To remove a policy from a device:

- Open the **Policies** window.



- In the Policies window, select the **None** option, and click **Apply**.
You will see a popup informing you if the software policy was removed successfully.

6.1.22 Remote Control

The Radix Device Management interface includes a remote-control option which allows you to interact with and essentially operate the user's device. It is especially useful in situations such as:

- Customer support,
- Debugging a device,
- In “attended mode”, where you can provide a live demo to a user of how to access a feature on their device,
- In ‘unattended mode’, where there is no user near the remote device, which is being used in an unmanned display.

Note: The Remote Control command can only be performed on one device at any time.

6.1.22.1 User permission for Remote Control

If the device's Account Settings require users' permission for remote control (see **Section 4.4.1, Remote Control Option**), when you click on the **Remote** or **Remote Control** icon, a message will appear on the user's device, prompting them to allow a remote-control session:

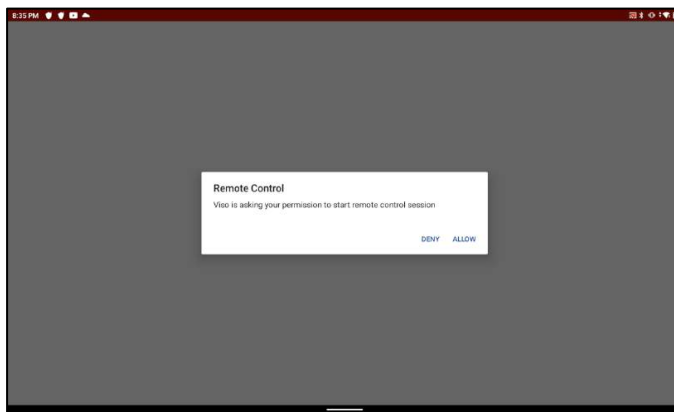


Figure 6-35: Prompt on the user's device, to allow remote control of a device

After the user allows remote access, the device's display will appear in the Radix Device Management interface:

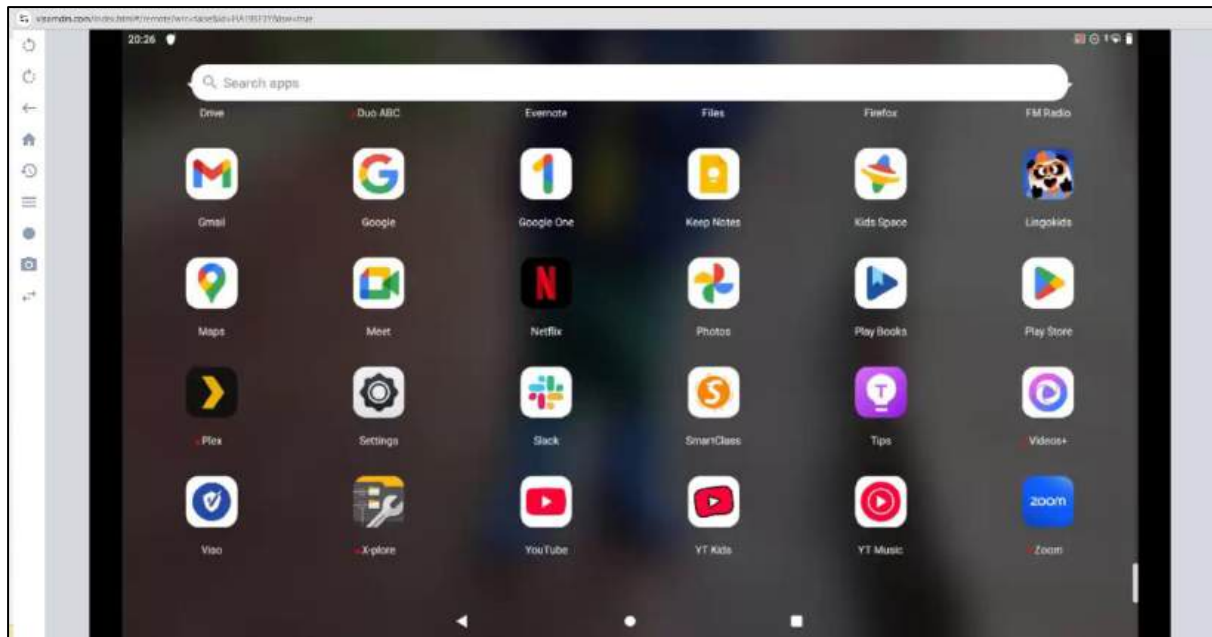


Figure 6-36: Radix Device Management Remote Display of Tablet Computer

In this example, the Radix Device Management User has full access to all the functions and apps in the user's tablet computer.

There is a set of icons on the left of the display, enabling the Radix Device Management user to perform the following actions:

Table 6-8: Remote Access Commands

Icon	Description
	Rotate left —Rotates the device display 90° counterclockwise
	Rotate right —Rotates the device display 90° clockwise
	Back —Goes back to the previous screen
	Home —Goes to the device's home screen
	App switch —Allows you to switch to one of your recently-used apps
	Menu —Goes to the user menu on an app that is presently in use
	Record Video —Allows you to record a video of a number of mouse clicks on the remote device
	Save Recorded Video —Downloads the recorded video in the form of a web media file (with the extension *.webm)
	Capture Screen —Allows you to take a screen capture of the remote device's entire display. The screen capture is downloaded as a *.png file
	D-pad —Emulates a directional pad as on a gaming console, to move in different directions

Clicking on the  icon opens a directional pad, which emulates a game controller:

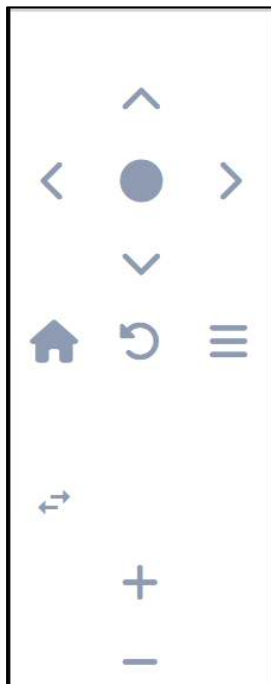


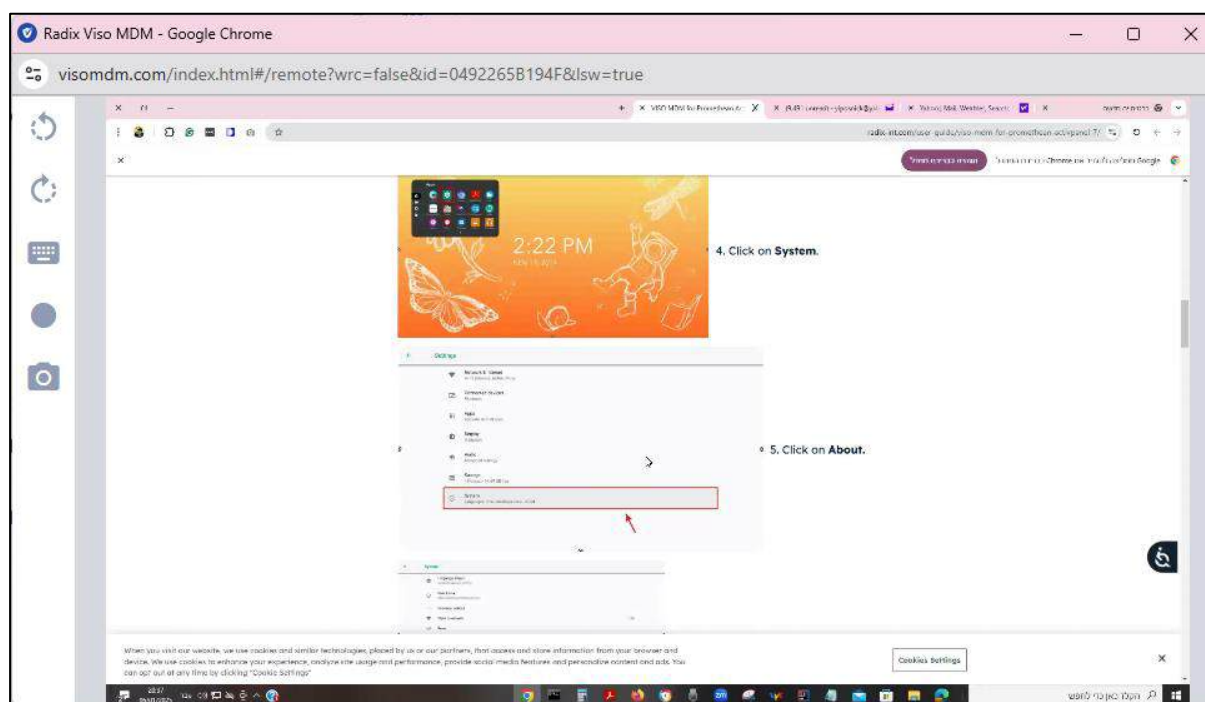
Figure 6-37: Directional Pad Icons

Here is a brief description of the directional pad commands:

Table 6-9: Directional Pad Options

Icon	Description
	Moves the cursor up/down/right/left. Clicking on the center button “selects” the item where the cursor is positioned.
	Home: Goes to Home screen
	Back: Goes back to the previous screen
	Menu: Goes to the user menu on an app that is presently in use
	Toggle: Allows you to toggle back and forth between the D-pad menu and the Remote menu
	Volume control: Raises and lowers the volume on the device

If you perform the Remote Control command on a Windows device, the screen will appear as follows:

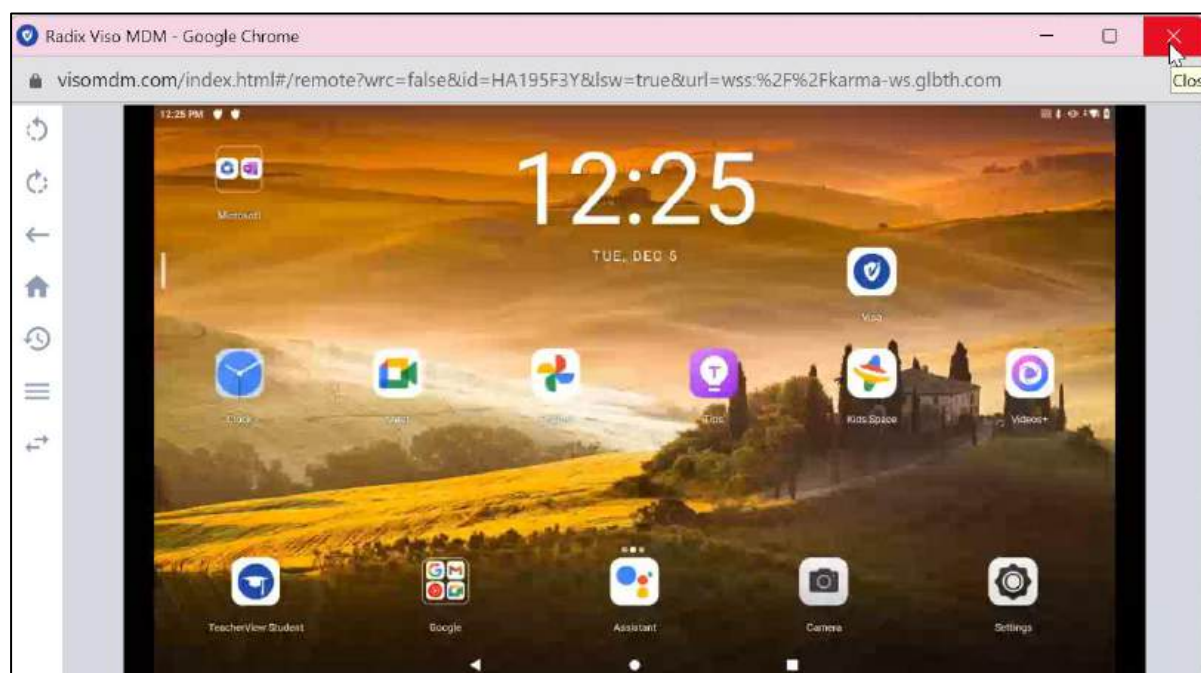


The options in the sidebar menu are as follows:

Icon	Description
	Rotate left —Rotates the device display 90° counterclockwise
	Rotate right —Rotates the device display 90° clockwise
	Ctrl-Alt-Del —This is the equivalent of pressing Ctrl-Alt-Del on the Windows device, and it opens the Task Manager screen. You can either lock the computer, sign out, change the computer password, or open the task manager to kill certain processes
	Record Video —Allows you to record a video of a number of mouse clicks on the remote device
	Save Recorded Video ---Downloads the recorded video in the form of a web media file (with the extension *.webm)
	Capture Screen —Allows you to take a screen capture of the remote device's entire display. The screen capture is downloaded as a *.png file

6.1.22.2 Ending a Remote-Control Session

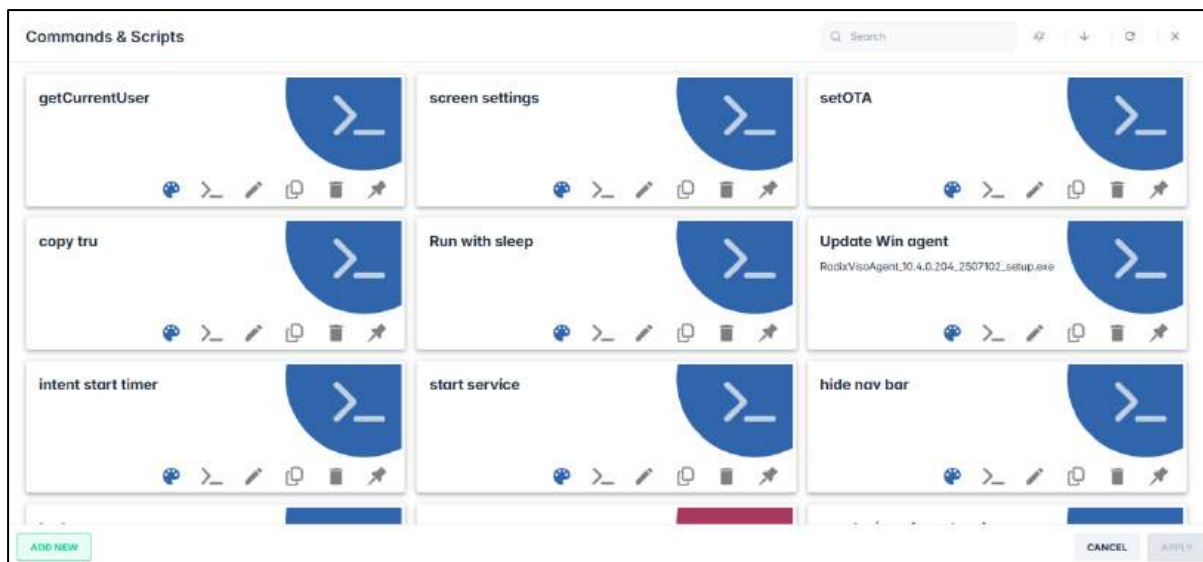
To stop Remote Control mode, simply close the Remote Control window.



6.1.23 Remote Execute/Commands & Scripts

This option allows the Radix Device Management user to execute a particular command line command or script on a device, or even on a group of devices at once.

When you click on a device's **three-dot menu>Deploy>Commands & Scripts**, the **Commands & Scripts** window appears.



You can select one of the existing options or create a new script to be executed remotely.

To create a new command to be executed remotely:

1. Click on **Add New** in the **Commands & Scripts** repository window. The **New Remote Execution** window appears.

Figure 6-38: Remote execute command interface

Supply the command line arguments, or a script, and click **Confirm**. The new command will appear in the Remote Execute window. The table in [Appendix E: Remote Execute Command Reference](#) has some useful command line commands, as well as instructions for filling in the other keyevent command options.

2. Click on the **Set as private** button if you would like the Remote Execute option to only be visible to you (as the creator of the item) when using the Radix Device Management Platform.
3. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Remote Execute command. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
5. Select the command and click **Apply**. The command will be sent to the selected device.

6.1.23.1 Examples of a Remote Execute Command

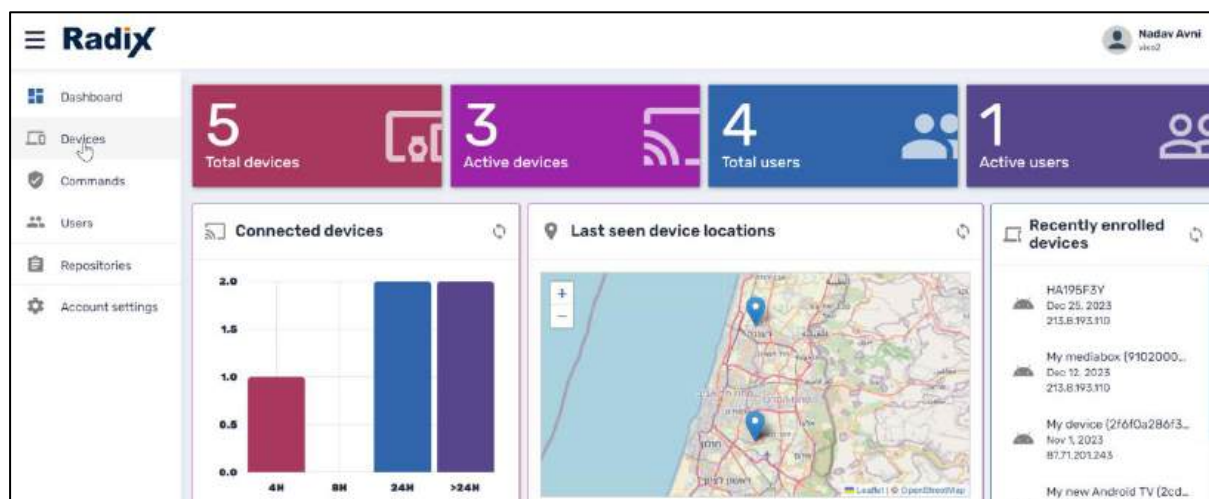
Let us perform some simple examples of a command that we send to a device remotely.

6.1.23.1.1 Example No. 1: Top Command

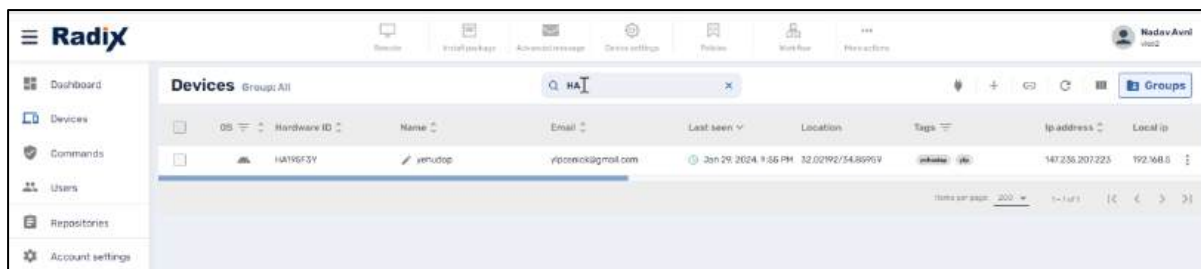
We will illustrate the remote execute command with the Android command “top”. The “top” command will get a list of processes running on the remote device and display the result.

To use the Remote Execute command “top”:

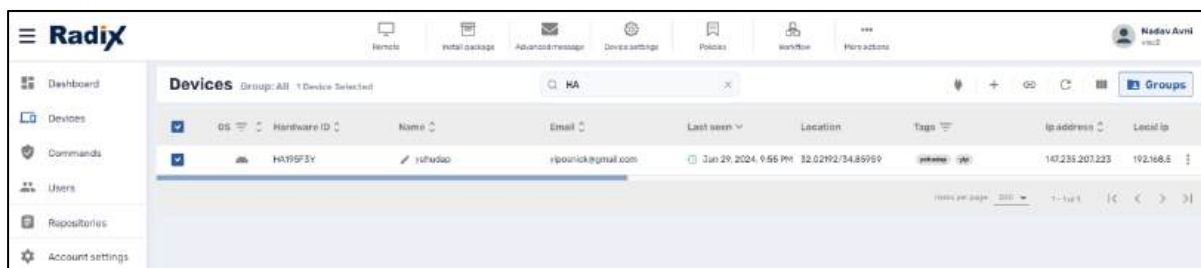
1. From the Overview Dashboard, click on the **Devices Table** icon, to see a list of all the available devices.



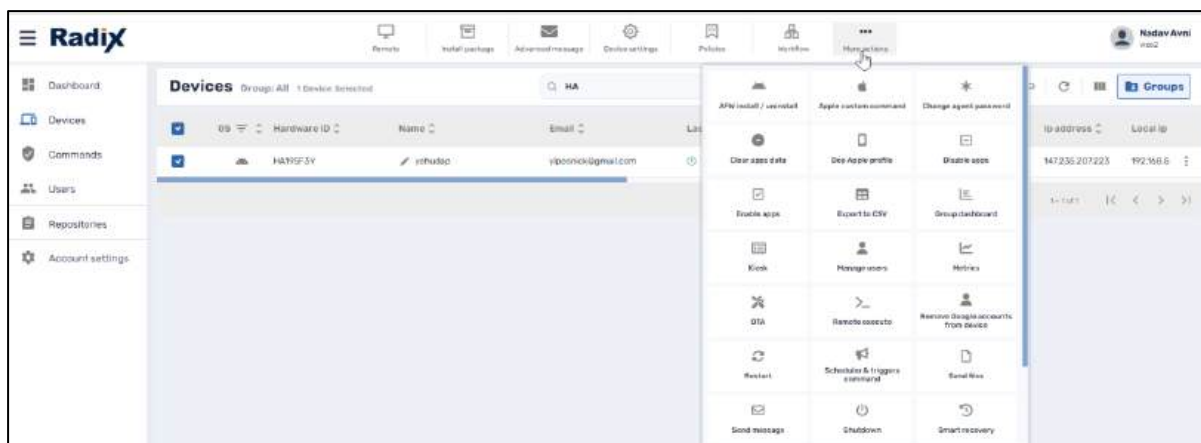
2. Find the device to which you would like to execute the command. Use the Search Bar at the top, to narrow down the selection.



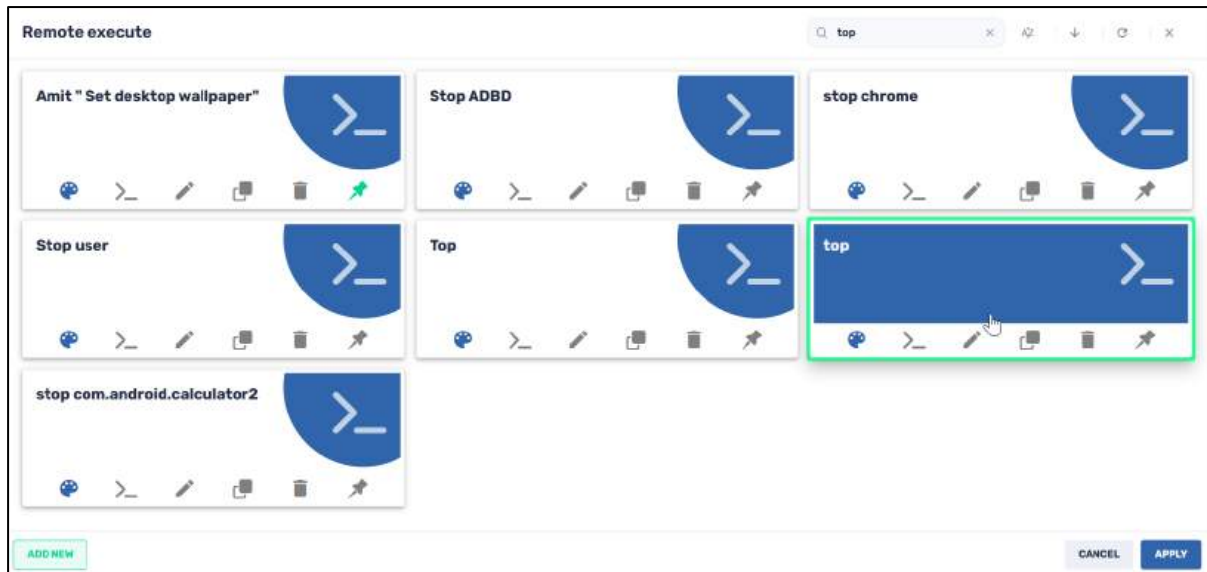
3. In the list of devices, click on the device's checkbox at the beginning of the line where the device is listed. The Bulk Actions Ribbon at the top of the screen will become active.



4. Click on the **More Actions** icon in the ribbon at the top of the Devices Table page. A drop-down list of possible commands opens.



5. Select **Remote Execute**. The **Remote Execute Commands** window opens.
6. In the Search bar at the top of the window, enter "top," to find the "top" command (the second entry in the table above).



This is what the “top” command looks like “under the hood” when we click on the Edit icon  on the **Remote Execute** tile:

Edit 'top'

Name
top

Description

Command
top

Arguments
-n 1

☒ Command line ☐ Script

☒ Wait for exit

☒ Collect output

☒ Run with high privileges

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

Figure 6-39: Remote Execute command "top", showing the command and its arguments

(The argument `-n 1` displays 1 line in the list of apps currently running.)

- Click on the tile for the “**top**” command and click **Apply**.



You will get an alert in the lower left-hand corner, indicating that the command has been executed.

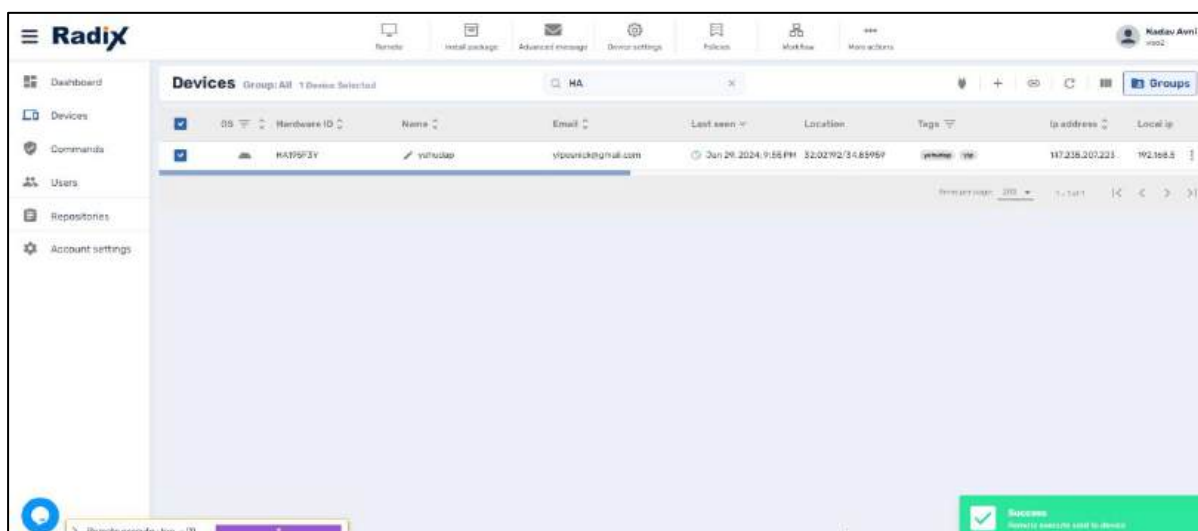


Figure 6-40: Alert that the Remote Execute command has been performed successfully

When you click on the **Remote Execute** command in the lower left-hand corner, the Command Status window opens, showing you the result when the command “top” is executed:

ID	Time	Status
HA1	Dec 17, 2023, 4:10:36 PM	Command executed
Result code:0 Command result: <pre>[s [999C [999B [6n [u [H [J [725l [H [J [s [999C [999B [6n [uTasks: 1 total, 1 running, 0 sleeping, 0 stopped, 0 zombie Mem: 5.5G total, 5.1G used, 442M free, 4.8M buffers Swap: 3.0G total, 555M used, 2.4G free, 2.7G cached 800%cpu 0%user 0%nice 0%sys 800%idle 0%iow 0%irq 0%irq 0%host 7m PID USER PR NI VIRT RES SHR S[%CPU] %MEM TIME+ ARGS [0m 1m25668 system 20 0 35M 3.6M 2.9M R 4.0 0.0 0:00.03 top -n 1 [m [725h [0m [1000:1H [K [725h [725h [0m [1000:1H [K</pre>		
HA1	Dec 17, 2023, 4:10:35 PM	Command sent

Figure 6-41: Command Status window, displaying the results of the “top” command

6.1.23.1.2 Example No. 2: Set System Settings

Another useful example is adjusting a device’s system settings using a remote execute command. The syntax is as follows:

Syntax: **set_system <key> <value>**

Here, we use the argument `screen_off_timeout`, which sets how long a device’s display will remain lit, until it goes to sleep.

Edit 'set system'

Name
set system

Description

Command
!internal

Arguments
set_system screen_off_timeout 7100000

☒ Command line ☐ Script

☒ Wait for exit

☒ Collect output

☒ Run with high privileges

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

☐

Hide content from others
Other users can apply this repository but cannot see or open its content

☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

☐

CANCEL CONFIRM

You can fill out the fields with the following parameters:

- **Command:** `!internal` (the “!internal” command helps ensure that the user has sufficient permissions to execute the command)
- **Arguments:** `set_system screen_off_timeout 7100000`

In this example, the command will set how long the screen on the Android device will remain lit. The argument for the amount of time it will stay lit is set for 7,100,000 milliseconds (= 118 minutes and 20 seconds).

6.1.23.1.3 Example No. 3: Set Global Settings

In this example, this command will turn on automatic date and time settings on the remote Android device.

Syntax: **set_global <key> <value>**

Here, we use the argument `set_global auto_time 1`, to allow the Android device to set its date and time settings automatically.

The screenshot shows a dialog box titled "Edit 'internal set_global auto_time 1'". It contains the following fields and options:

- Name:** `internal set_global auto_time 1`
- Description:** `Allows Android device to set date and time automatically`
- Command:** `!internal`
- Arguments:** `set_global auto_time 1`
- Execution Type:** ☒ Command line, ☐ Script
- Options:**
 - ☒ Wait for exit
 - ☒ Collect output
 - ☒ Run with high privileges
- Permissions:**
 - Set as private:** ☐ (This repository item will be visible only to this user)
 - Hide content from others:** ☐ (Other users can apply this repository but cannot see or open its content)
 - Set as read-only:** ☐ (This repository item will be editable only to this user and admin users, and read-only for the others)
- Buttons:** CANCEL, CONFIRM

You can fill out the fields with the following parameters:

Command: `!internal` (as above, the “!internal” command helps ensure that the user has sufficient permissions to execute the command)

Arguments: `set_global auto_time 1`

6.1.23.1.4 Example No. 4: Set Secure Settings

In this example, we use the “secure settings” option to disallow installing apps from any unknown sources.

Syntax: **set_secured** <key> <value>

Dialog box titled "Edit 'Disallow install app from unknown sources'".

- Name:** Disallow install app from unknown sources
- Description:** (empty)
- Command:** !internal
- Arguments:** set_secured INSTALL_NON_MARKET_APPS 0
- Options:**
 - ☒ Command line ☐ Script
 - ☒ Wait for exit
 - ☒ Collect output
 - ☒ Run with high privileges
 - ☐ Set as private (This repository item will be visible only to this user)
 - ☐ Hide content from others (Other users can apply this repository but cannot see or open its content)
 - ☐ Set as read-only (This repository item will be editable only to this user and admin users, and read-only for the others)
- Buttons:** CANCEL, CONFIRM

You can fill out the fields with the following parameters:

Command: !internal (as above)

Arguments: set_secured INSTALL_NON_MARKET_APPS 0

In this example, we employ the argument “INSTALL_NON_MARKET_APPS” and set the parameter to “0”, to disallow installing apps from suspicious sites.

6.1.24 Remove Google Accounts from Device

This allows the Radix Device Management user to remove all Google accounts from a device, or to retain one. This is useful in instances where you want to transfer the use of a device from one user to another, and you want to switch over the default Google account on the device as well.

To remove Google accounts from a device:

1. Click on a device’s **three-dot menu>Configure>Remove Google Account**. The **Remove Accounts** window appears.

2. If you select “Remove all accounts” and click **Confirm**, you will get a confirmation in the lower right corner that the command to remove the Google account(s) has been sent to the device.
3. If you select “Keep one account”, you will be prompted to enter a Google account that you would like to retain.

4. If you select “Remove accounts by condition”, you will be prompted for a condition that the Google account must/must not contain to be removed.

5. Click **Confirm**. You will get confirmation that all Google accounts have been removed, except for the one(s) that you wished to retain.

6.1.25 Restart

This allows the Radix Device Management user to restart a device remotely.

To use the Restart command:

1. Click on the device's **three dot menu>Power>Restart** command tile. The **Restart** window opens:

A dialog box titled "Restart" with a question "Are you sure you want to restart selected device?" and two buttons: "NO" and "YES".

Restart

Are you sure you want to restart selected device?

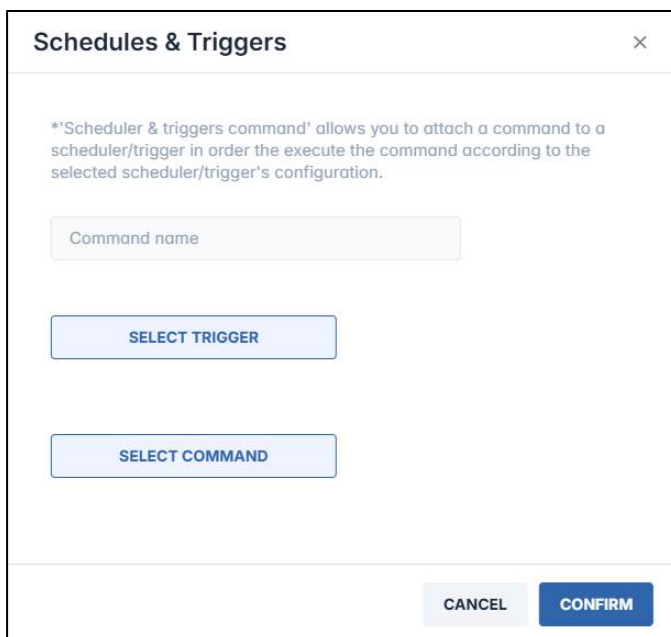
NO **YES**

2. Click on **Yes**. The device will restart remotely.

6.1.26 Scheduler & Triggers Command

This allows you to create a trigger for a device (by timing, geofencing, Wi-Fi, or upon Startup) from within the Device Dashboard and lets you program the device's reaction to the trigger, by selecting a particular command to be executed.

When you click on a device's **three-dot menu> Automate>Schedules & Triggers**, the **Schedules & Triggers** window opens:

A window titled "Schedules & Triggers" with a close button (X). It contains a description: "*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." Below this is a text input field for "Command name". There are two buttons: "SELECT TRIGGER" and "SELECT COMMAND". At the bottom are "CANCEL" and "CONFIRM" buttons.

Schedules & Triggers X

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.

Command name

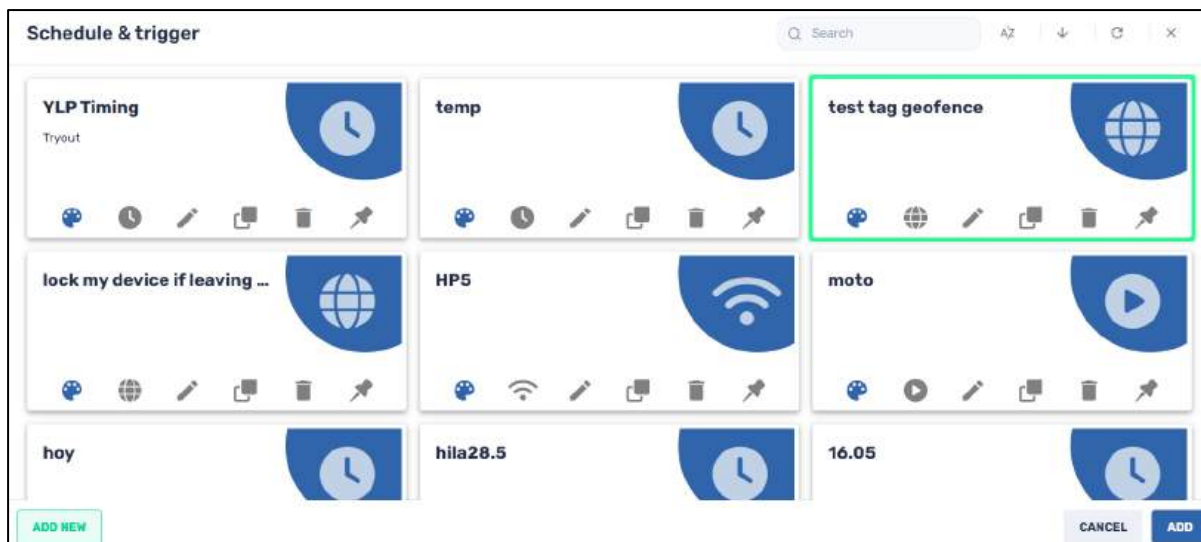
SELECT TRIGGER

SELECT COMMAND

CANCEL **CONFIRM**

To use the Schedules & triggers command:

1. Assign a name to the command.
2. Click **Select Trigger**. The **Schedule & Trigger** window opens, with saved options.



If you wish to create a new **Schedule & trigger** command.

1. Click on **Add New**. The **New scheduler and trigger** window opens.

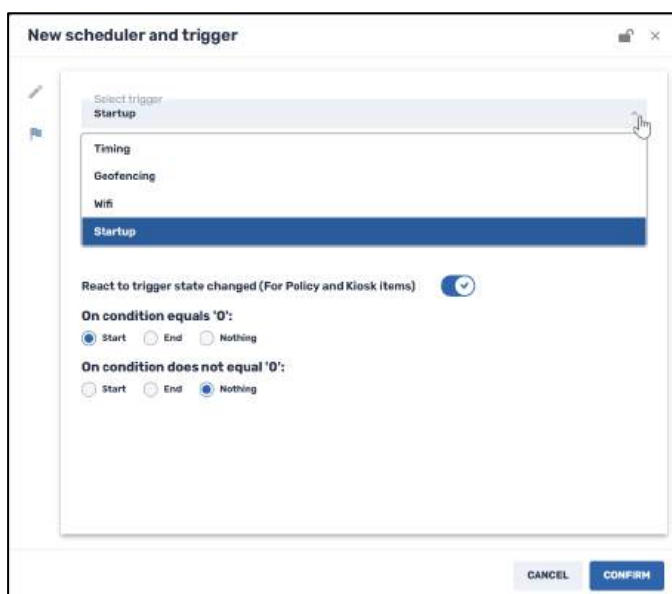
The screenshot shows the 'New scheduler and trigger' form. It has a sidebar with a pencil icon and a flag icon. The main form area contains the following fields and options:

- Name**: A text input field.
- Description**: A text input field.
- Set as private**: A toggle switch. Below it, the text reads: 'This repository item will be visible only to this user'.
- Hide content from others**: A toggle switch. Below it, the text reads: 'Other users can apply this repository but cannot see or open its content'.
- Set as read-only**: A toggle switch. Below it, the text reads: 'This repository item will be editable only to this user and admin users, and read-only for the others'.

At the bottom right, there are two buttons: 'CANCEL' and 'CONFIRM'.

2. Assign a name and description to the scheduled command and its trigger.

3. Click on the **Set as private** button if you want this new Schedule & Trigger option to be visible only to you (as the creator of the item) when you log in to the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you want to restrict who will be able to modify the details of this Schedule & Trigger option. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
6. Click on the **Add trigger** icon . You have four options to select as a trigger:



- **Timing:** To execute a command at a particular date and time. The timing can be a one-time trigger, a trigger limited to a range of dates, or a perpetual trigger with no definite end date.

The screenshot shows a 'New scheduler and trigger' dialog box. The 'Select trigger' dropdown is set to 'Timing'. The 'Timing type' dropdown is set to 'Once'. The 'Start date' field is empty, and the 'Execution time' field is set to '15:40'. The 'Time to live' section has a toggle switch turned on, and the 'Time to live (seconds)' field is set to '1'. The 'Apply only if idle' section has a toggle switch turned on, and the text below it says 'Apply trigger to the device only if it is idle during the time slot'. The 'Condition command line (run if exit code = 0, Optional)' field is empty. At the bottom, there are 'CANCEL' and 'CONFIRM' buttons.

Figure 6-42: Timing option with a one-time trigger

The screenshot shows a 'New scheduler and trigger' dialog box. The 'Select trigger' dropdown is set to 'Timing'. The 'Timing type' dropdown is set to 'From/To date'. The 'Start date' field is set to 'Apr 14, 2024', the 'Execution time' field is set to '15:40', and the 'End date' field is empty. The 'Range type' dropdown is set to 'Interval'. The 'Time to live' section has a toggle switch turned on, and the 'Time to live (seconds)' field is set to '1'. The 'Apply only if idle' section has a toggle switch turned off. The 'Condition command line (run if exit code = 0, Optional)' field is empty. At the bottom, there are 'CANCEL' and 'CONFIRM' buttons.

Figure 6-43: Timing option with a trigger on defined dates

Figure 6-44: Trigger option with no end date

There are two other parameters that you can adjust in the Trigger option:

- **Time to live:** This is the time in seconds that you allow for the command to be executed if the remote device is not accessible at the specified time
- **Apply only if idle:** When you click on this option, you specify that you want the trigger to operate only if the remote device is idle. This is preferable in instances where you do not want the remote user to be disturbed in the middle of using a device.
- **Condition command line:** Here you can supply a line of code that will run the trigger if the code runs properly and provides an exit code equal to 0.
- **Geofencing:** To execute a command within a certain geographic perimeter. You can draw the perimeter on a map and specify that the command should be executed if the device leaves that perimeter. This feature can be useful if a device is lost or stolen. For example, you can use this feature to track a lost device and lock it down using the **Lock Device** command or even wipe all personal data with the **Wipe Device** command (see **Section 5.8.3.8, Lock Menu**).

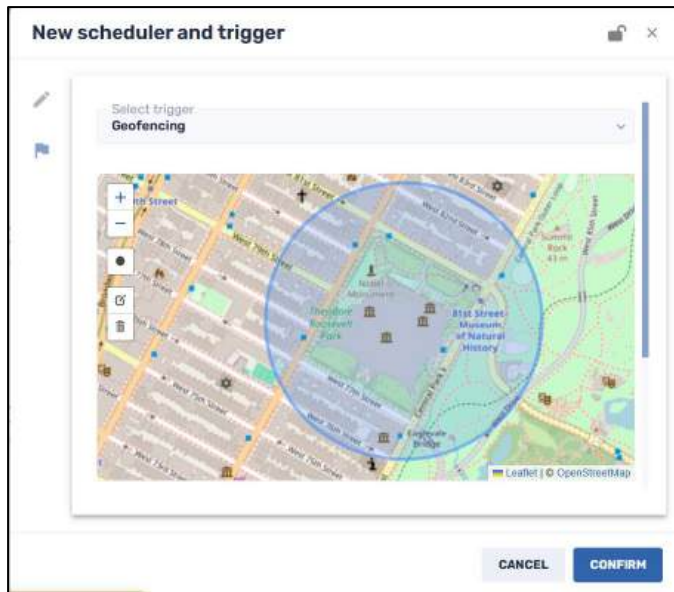
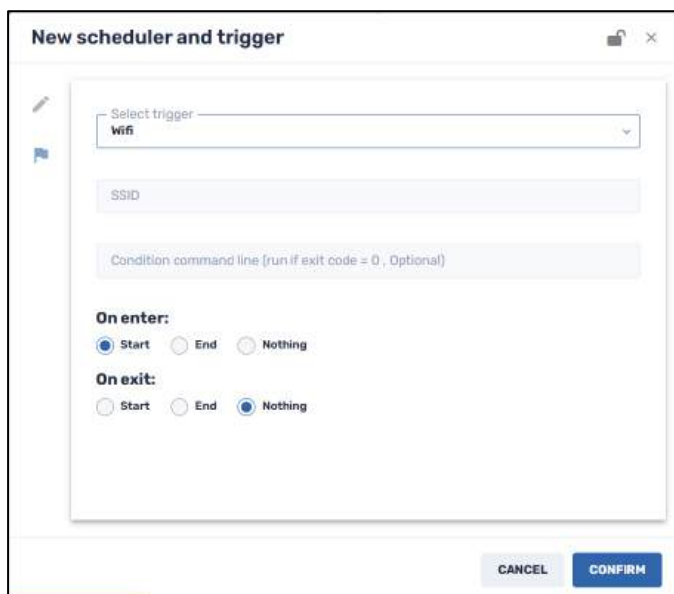


Figure 6-45: Geofencing Option, delimiting a geographical area

- **Wi-Fi:** To execute a command upon receiving a Wi-Fi trigger.



- **Startup:** To execute a command on the device every time it starts up, or upon the first registration of the device only.

New scheduler and trigger

Select trigger
Startup

When to execute
Every startup

Condition command line (run if exit code = 0, Optional)

React to trigger state changed (For Policy and Kiosk items) ☒

On condition equals '0':
☒ Start ☐ End ☐ Nothing

On condition does not equal '0':
☐ Start ☐ End ☒ Nothing

CANCEL CONFIRM

New scheduler and trigger

Select trigger
Startup

When to execute
On first registration only

Condition command line (run if exit code = 0, Optional)

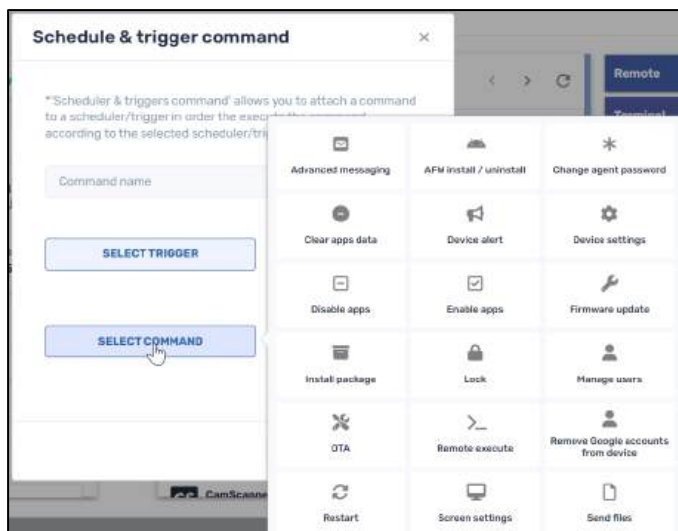
React to trigger state changed (For Policy and Kiosk items) ☒

On condition equals '0':
☒ Start ☐ End ☐ Nothing

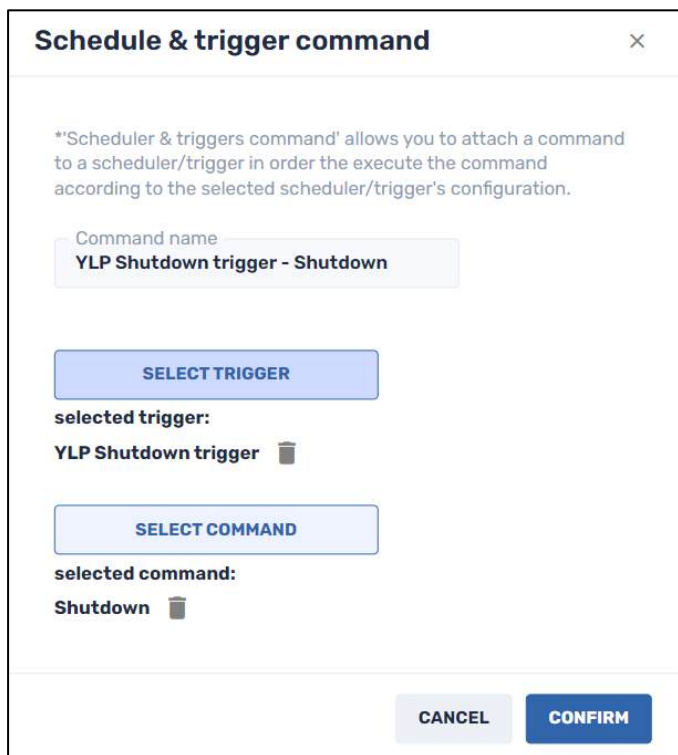
On condition does not equal '0':
☐ Start ☐ End ☒ Nothing

CANCEL CONFIRM

- After you have selected a trigger, you then click on the **Select Command** button to specify a command to be executed.



8. After you select the command, you link it together with the desired trigger. The result should appear something like this:



9. Click **Confirm**. The command will be sent to the device and will be executed when the trigger condition is met. In our example, the device will shut down when the shutdown trigger condition is met.

6.1.27 Screen Settings

This allows you to adjust the brightness and volume on flat panel devices.

When you click on a device's **three-dot menu>Configure>Screen Settings**, the following window opens:



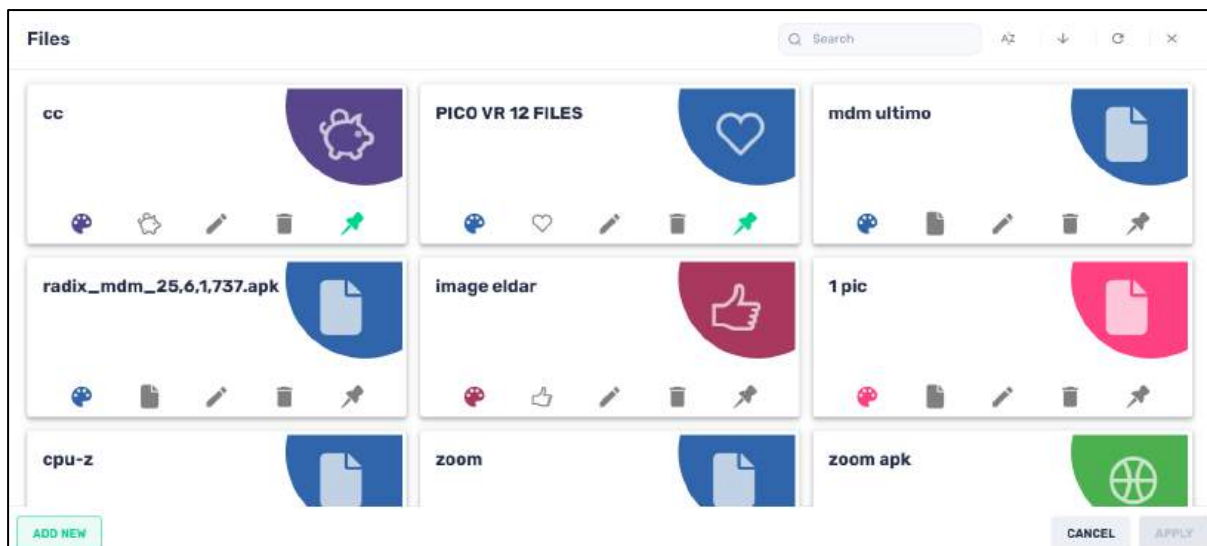
To use the Screen Settings command:

1. Specify the input source for the signal to the flat panel device.
2. Adjust the volume and brightness to the desired levels.
3. Click **Confirm**. You will receive a notification that the command has been sent to the flat panel device.

6.1.28 Send Files

This allows you to send specific files to a remote device. You can either supply a URL from which to retrieve the file or upload a file from your computer.

When you click on a device's **three-dot menu>Deploy>Files**, the Files window opens.



To add a file to the repository from the Internet:

1. Click on **Add New** in the lower left corner. The **New File** window opens.

New file

Select upload method

Upload file

File from Url

Upload file

Destination

ADD FILES

Set as private

This repository item will be visible only to this user

Hide content from others

Other users can apply this repository but cannot see or open its content

Set as read-only

This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL

CONFIRM

- From the **Select upload method** drop-down list, choose **File from URL**, and supply the URL, as well as a name for the file in the repository, and a file destination (= where you would like the file to be stored on the target device).

Edit '1 airplane'

File url
orage-prod.visomdm.com/qa/cace90588f8826bafaf1f1526d1576f0eb73e68015460adb721

Name
1 airplane

Destination
/sdcard/downloads ⓘ

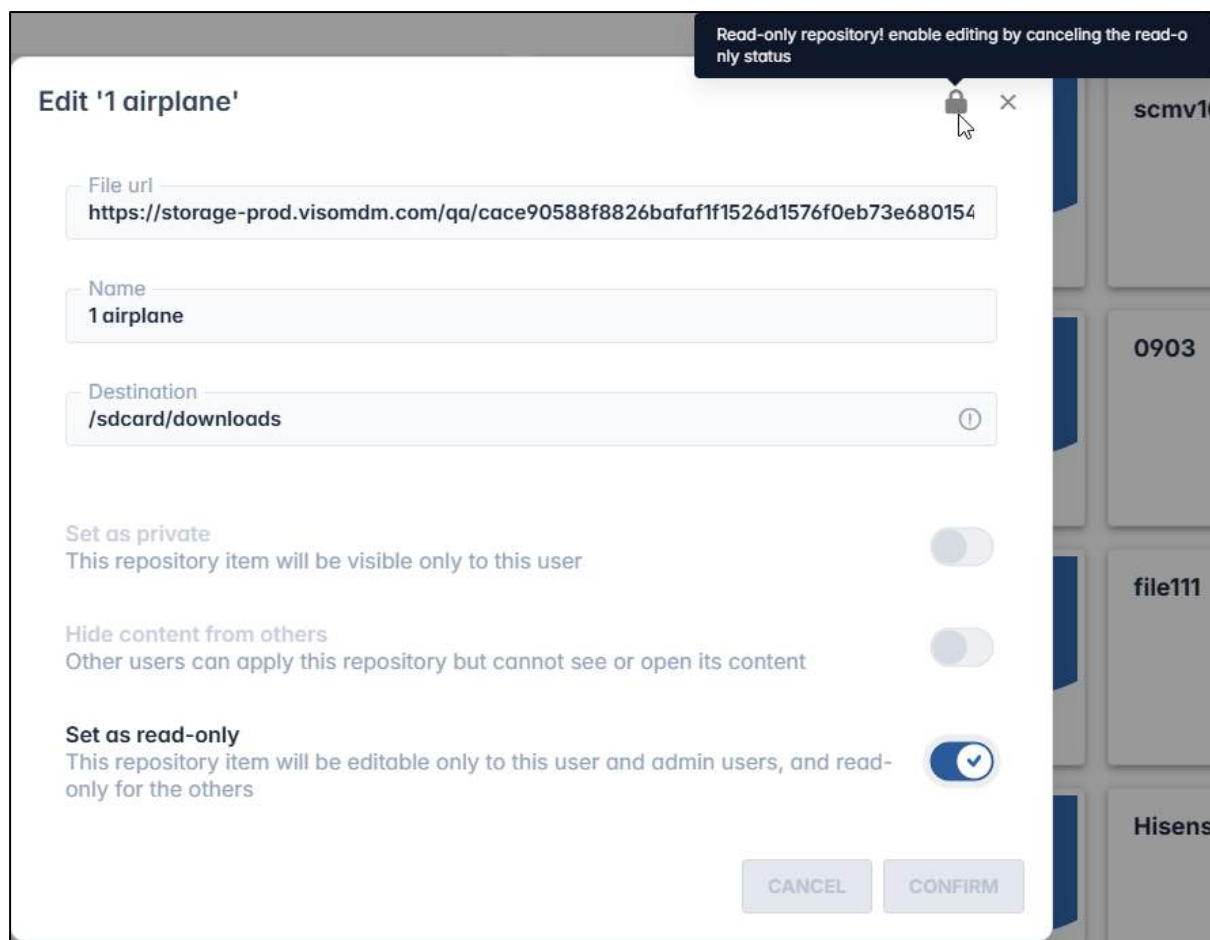
Set as private
This repository item will be visible only to this user ☐

Hide content from others
Other users can apply this repository but cannot see or open its content ☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others ☐

CANCEL **CONFIRM**

3. Click on the **Set as private** button if you would like the file option to only be visible to you (as the creator of the item) when using the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the file uploaded. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .



6. Click **Confirm**. The new **File** option will appear in the Files window, allowing you to send it to the selected devices.

To add a file from your computer to the repository:

1. Click on **Add New** in the lower left corner. The **New File** window opens.
2. Choose **Upload file** to upload a file from your computer to the Files repository on the Radix Device Management interface.

New file

Select upload method
Upload file

Name

Destination

ADD FILES

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL **CONFIRM**

3. Supply a name for the file for how it will appear in the Files repository, and supply a destination as a path, such as `/mnt/sdcard/Documents`.
4. Click **Add Files** to search for a file from your computer to upload. You can add several files to the repository.

New file

Select upload method

Upload file

Name

background file

Destination

/sdcard/Download/test/

ADD FILES

Set as private

This repository item will be visible only to this user

Hide content from others

Other users can apply this repository but cannot see or open its content

Set as read-only

This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL

CONFIRM

- When you have finalized your selection of files, click on **Upload All**.

New file

Select upload method

Upload file

Name

background file

Destination

/sdcard/Download/test/

IMG_20260310_151740_063.jpg

IMG_20260310_151704_155.jpg

20260322_185224.jpg

ADD FILES

Upload all

Set as private

This repository item will be visible only to this user

Hide content from others

Other users can apply this repository but cannot see or open its content

Set as read-only

This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL

CONFIRM

- Click on the **Set as private** button if you would like the file option to only be visible to you (as the creator of the item) when using the Radix Device Management Platform.
- Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
- Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of these files. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
- Click **Confirm**. The files will be added to the Files repository item under the name that you selected.

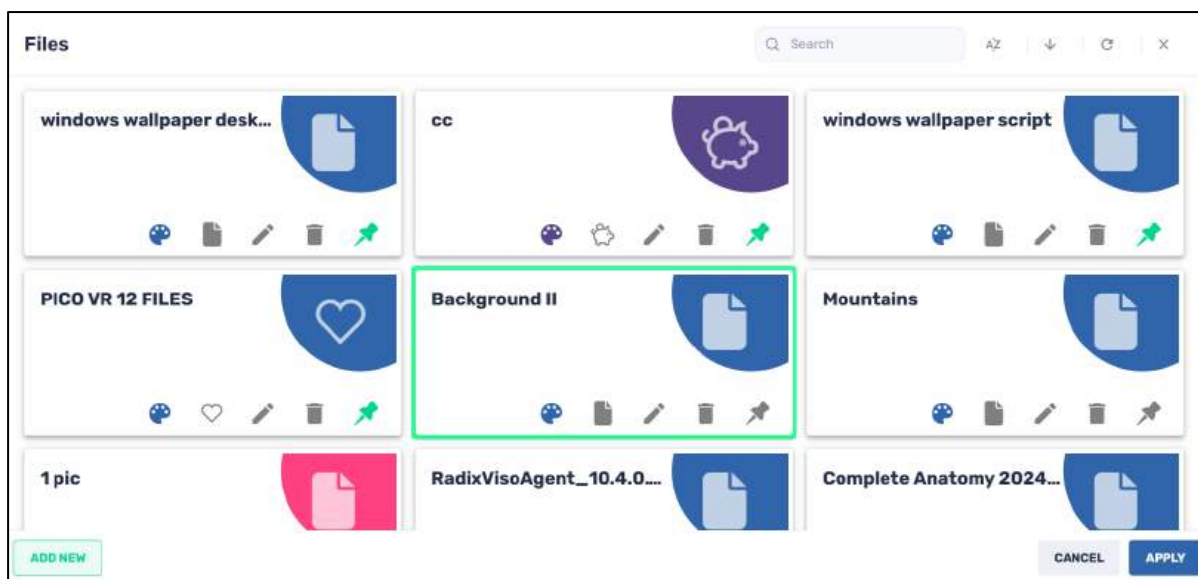


Figure 6-46: The Files repository item "Background II" has been added

6.1.29 Shutdown

This command shuts the device down remotely.

To shut down a device remotely:

1. Click on the **Shutdown** command. The Shutdown window opens.
2. Click on **Yes** when prompted whether you wish to shut down the device.

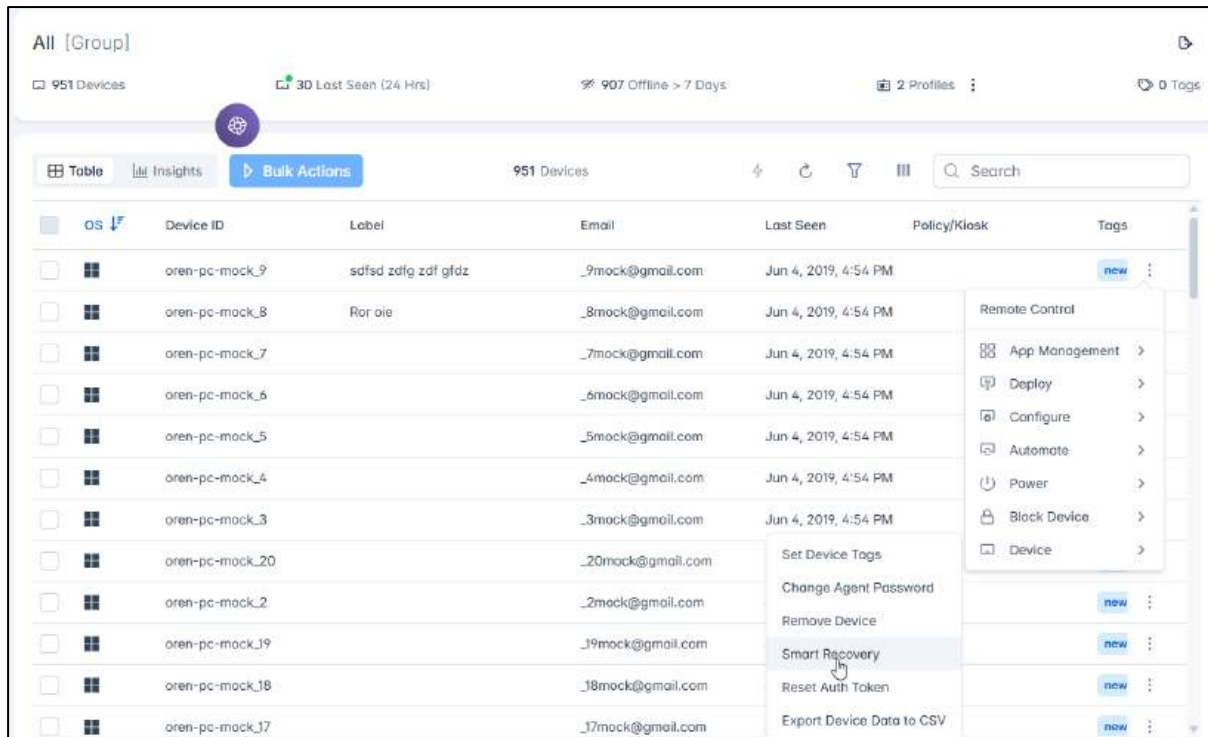


6.1.30 Smart Recovery

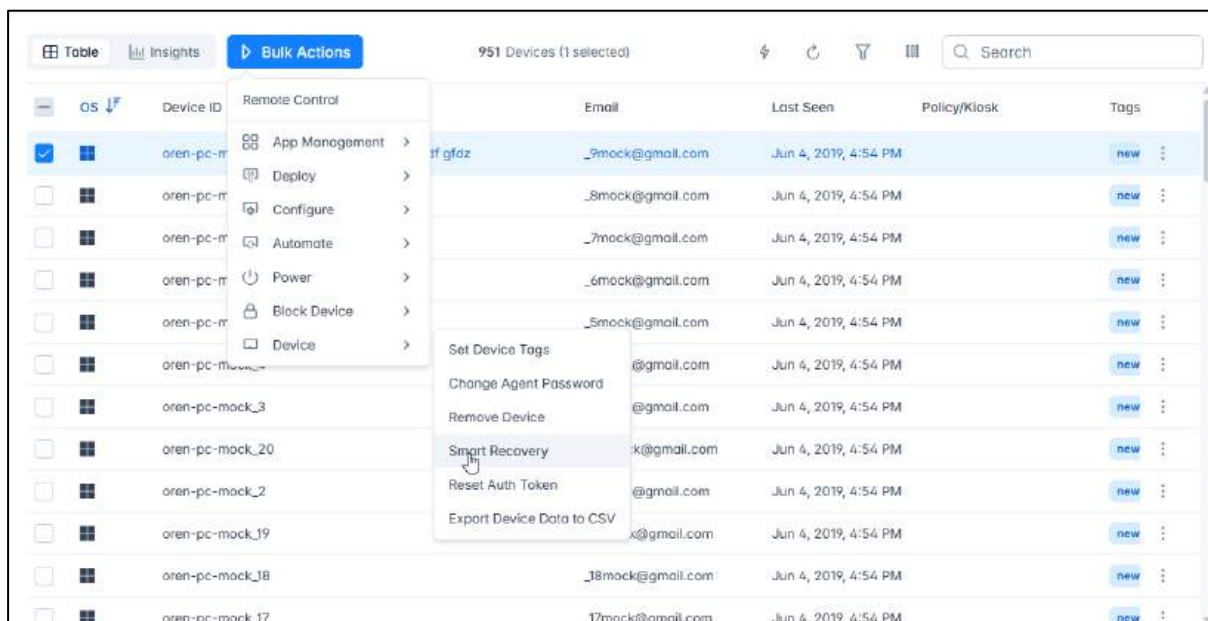
This opens the repository of Smart Recovery options. Smart Recovery is a Windows application that allows you to perform a system restore so as to repair a Windows device that has crashed. Once you have installed Smart Recovery on a remote Windows device, you can execute Smart Recovery commands via the Radix Device Management Platform interface.

Smart Recovery options include restoring a device's system configuration and settings to the latest system snapshot, or factory settings. You can access this command by:

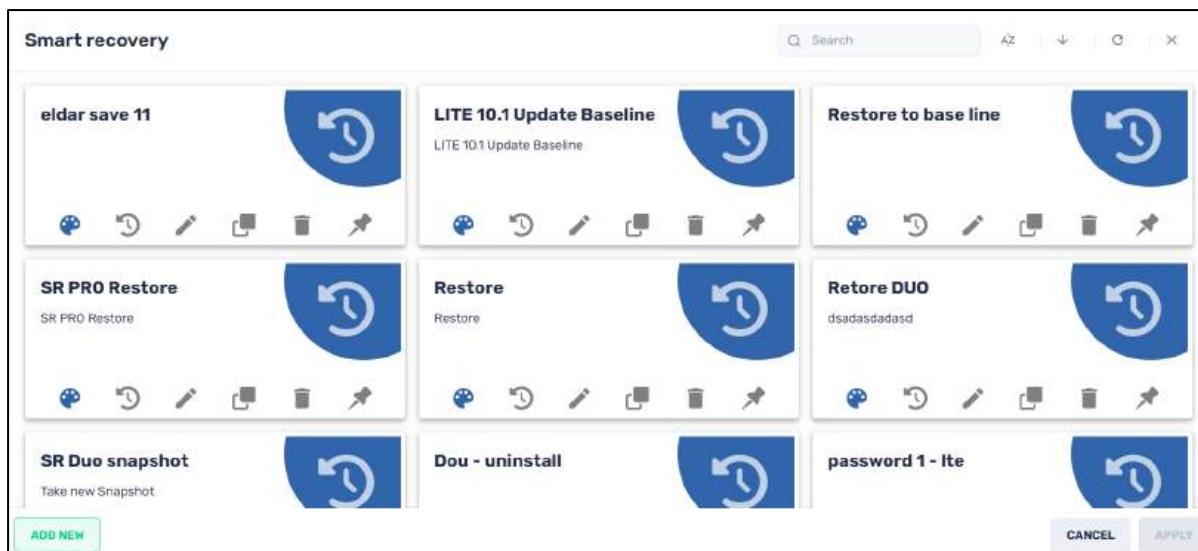
- Clicking on a Windows device's three-dot menu>**Device>Smart Recovery**.



- Checking a Windows device's checkbox and clicking on **Bulk Actions>Device>Smart Recovery**.



When you click on the **Smart Recovery** option, the **Smart Recovery** window opens.



If you wish to create a new Smart Recovery option:

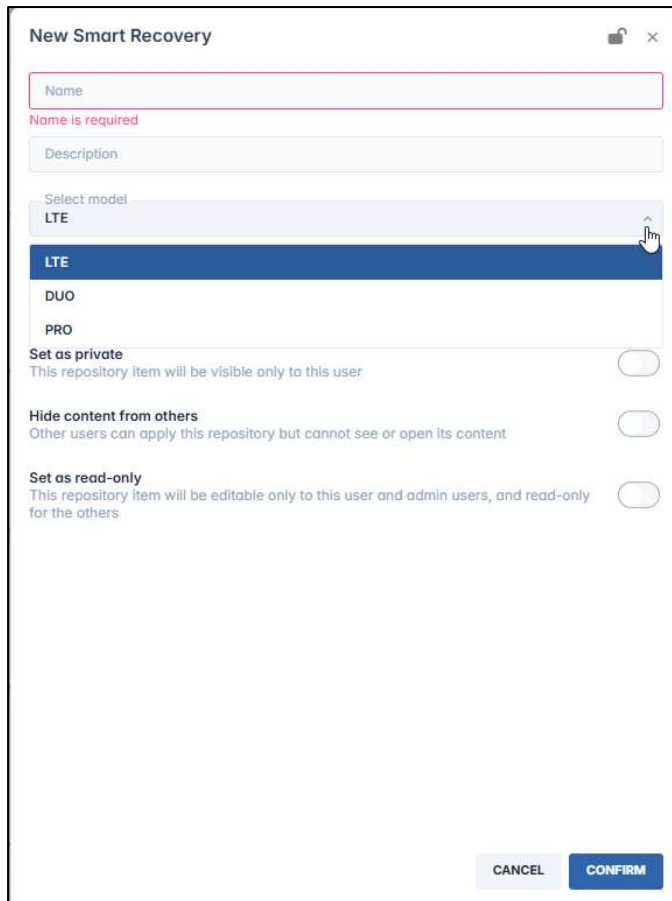
1. Click **Add New**. The **New Smart Recovery** window opens.

The screenshot shows the 'New Smart Recovery' form. It has a title bar with a lock icon and a close button. The form contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Select model:** A dropdown menu with 'LTE' selected.
- Action:** A dropdown menu.
- Set as private:** A toggle switch with the text 'This repository item will be visible only to this user'.
- Hide content from others:** A toggle switch with the text 'Other users can apply this repository but cannot see or open its content'.
- Set as read-only:** A toggle switch with the text 'This repository item will be editable only to this user and admin users, and read-only for the others'.

 At the bottom right, there are 'CANCEL' and 'CONFIRM' buttons.

2. Select a name and description of the recovery activity.
3. Select the version of the Smart Recovery application that you wish to use. There are three options:



New Smart Recovery

Name

Name is required

Description

Select model

LTE

LTE

DUO

PRO

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

Hide content from others
Other users can apply this repository but cannot see or open its content ☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others ☐

CANCEL **CONFIRM**

Figure 6-47: Smart Recovery options to be applied to a remote device

- **Smart Recovery LTE (or LITE):** This version allows you to restore a Windows device to a previous baseline state. You can choose between:
 - An **Automatic Restore Mode**, where the computer undergoes a system restore every time it boots, or
 - A **Manual Restore Mode**, where the computer is restored to the most recently saved baseline state.

The Smart Recovery LTE interface appears as follows on a Windows device.

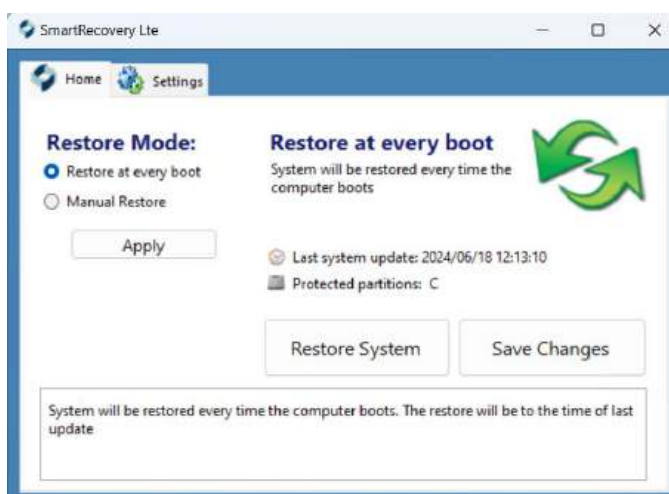


Figure 6-48: Smart Recovery LTE Main Screen

Note: Smart Recovery LITE allows only **one** baseline point.

- **Smart Recovery DUO:** In addition to the Smart Recovery LITE options, this version allows you to choose to restore a Windows device to one of **two** (= hence the name “DUO”) states:
 - A **fixed baseline state** (referred to as the “root” baseline point), or
 - A **dynamic restore point** that you can adjust if you wish.
- The Smart Recovery Duo interface appears as follows:

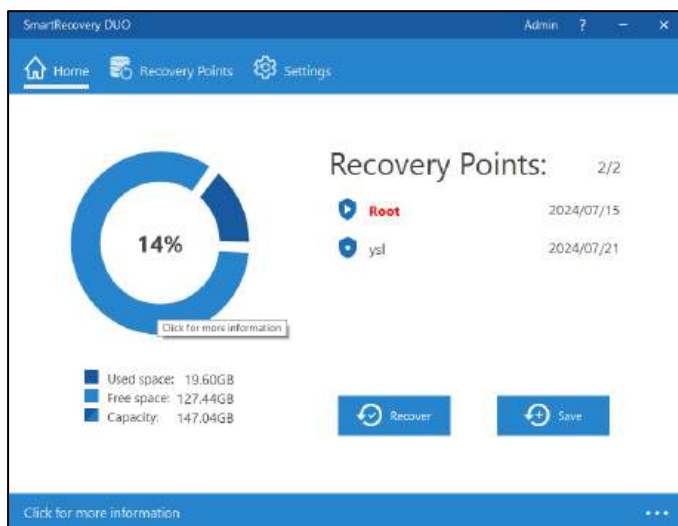


Figure 6-49: Smart Recovery DUO Main Screen

- **Smart Recovery PRO:** This version of Smart Recovery allows you to restore your computer to
 - A **fixed baseline state**,
 - Any of 4 additional **dynamic restore points** that you have saved as a snapshot of the system, or
 - The **current snapshot**.
- The Smart Recovery Pro application appears as follows:

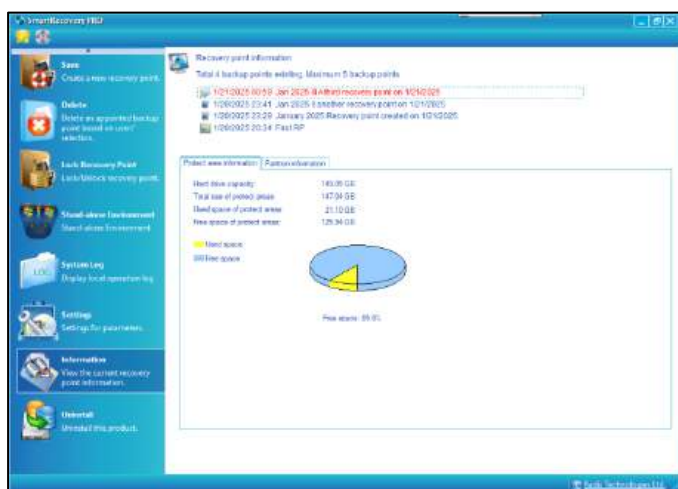


Figure 6-50: Smart Recovery PRO Main Screen

[Appendix D](#) has a table that summarizes the three Smart Recovery options.

4. Choose a restore action from the drop-down menu. The options include:
 - **Change restore mode:** You can select between restoring the system at every reboot, or a manual restore. (Automatically restoring the system to a baseline configuration each time the device is booted may be desirable if you wish to undo any installations or downloads that clients have performed on their devices.)
 - **Restore system:** This allows you to restore the system to the baseline settings, or a previous snapshot.
 - **Save changes:** This allows you to save the system configuration as it is currently, as a dynamic recovery point.
 - **Change client Smart Recovery password:** This lets you create a new password for the user when they wish to configure their use of the Smart Recovery app.
 - **Register:** This option lets you register a client using the Smart Recovery app, using a registration name and serial number.
 - **Installation mode,** to install Smart Recovery on the remote device,
 - **Uninstall client smart recovery:** This lets you uninstall Smart Recovery on remote devices. You can keep the current system and then uninstall or restore the device to its baseline settings.

5. For the options **Restore System**, **Save Changes**, and **Uninstall client Smart Recovery**, you will see the option **Don't restart, run command on the next system boot** checkbox. Check this checkbox if you want to apply the System Restore only when the remote user reboots their device. If you do not check this checkbox, it will restart the user's device and perform a system restore immediately upon receiving the Smart Recovery command.

New Smart Recovery

Name

Name is required

Description

Select model

Action

Select option

☒ Don't restart, run command on the next system boot

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

Hide content from others
Other users can apply this repository but cannot see or open its content ☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others ☐

Figure 6-51: Illustration of "Don't restart" checkbox

- For the **Save changes** option in the **Duo** and **Pro** versions of Smart Recovery, you will see the **Save on Windows** checkbox. Check this option if you want to save the changes to a device when Windows boots up on that device.

New Smart Recovery

Name Name is required

Description
admin

Select model
DUO

Action
Save changes

Save the current system as daynamic recovery point

Snapshot name

Snapshot description

☒ Save on Windows

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

Hide content from others
Other users can apply this repository but cannot see or open its content ☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others ☐

CANCEL CONFIRM

Figure 6-52: Illustration of Save on Windows checkbox on Smart Recovery DUO

7. **For Smart Recovery Pro:** Click on the **Lock Snapshot** checkbox to lock the snapshot taken of the Windows device.

New Smart Recovery

Name Name is required

Description
admin

Select model
PRO

Action
Save changes

Save the current system as daynamic recovery point

Snapshot name

Snapshot description

☒ Save on Windows

☒ Lock snapshot

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

Hide content from others
Other users can apply this repository but cannot see or open its content ☐

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others ☐

CANCEL CONFIRM

Figure 6-53: Illustration of Save on Windows checkbox on Smart Recovery Pro

8. Click on the **Set as private** button if you want this Smart Recovery option to be visible only to you (as the creator of the item) when you log in to the Radix Device Management Platform.
9. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
10. Click on the **Set as read-only** button if you want to restrict who will be able to modify the details of this Smart Recovery option. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
11. Click **Confirm**. The Smart Recovery method will be saved.
12. To implement a Smart Recovery method, select it from the list, and click **Apply**.

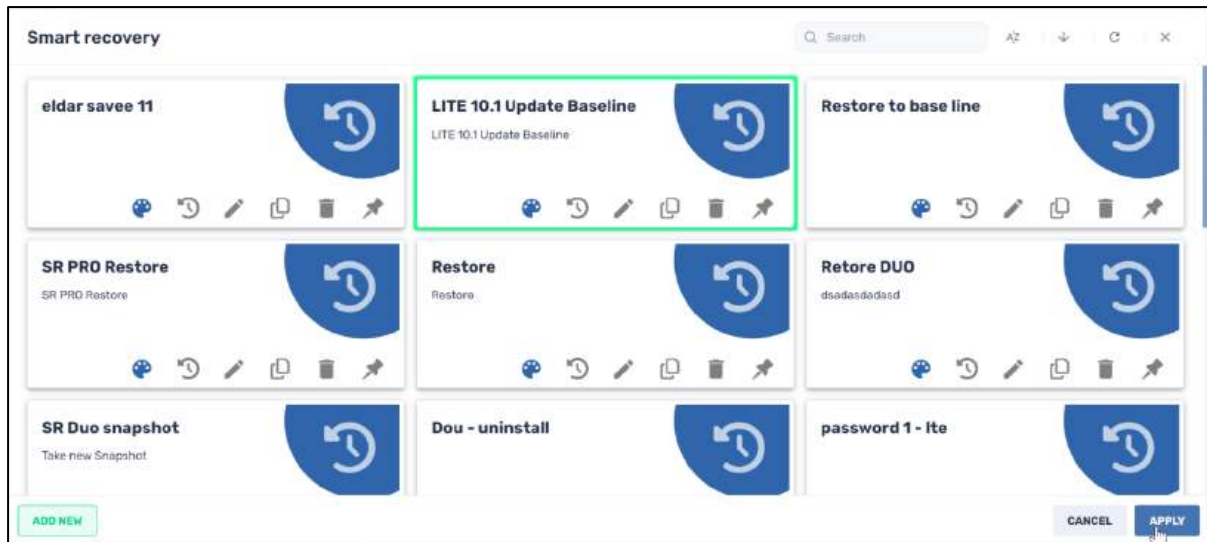
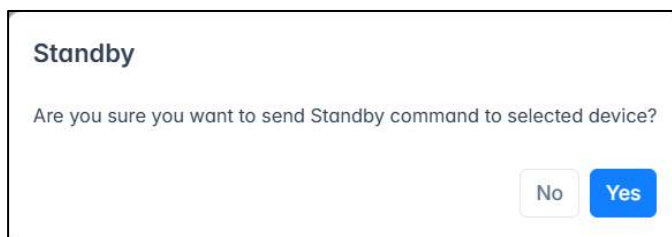


Figure 6-54: The Smart Recovery option "LITE 10.1 Update Baseline" has been selected

6.1.31 Standby

This option will put a remote device in standby mode (otherwise called “Hibernate” or “Sleep Mode”).

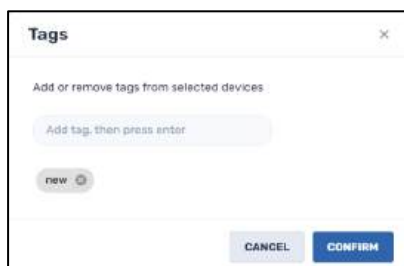


Click **Yes** to put the remote device in Standby mode.

The **Wake Up** command (Section 6.1.37) will power up the display on the remote device after it has been in Standby mode.

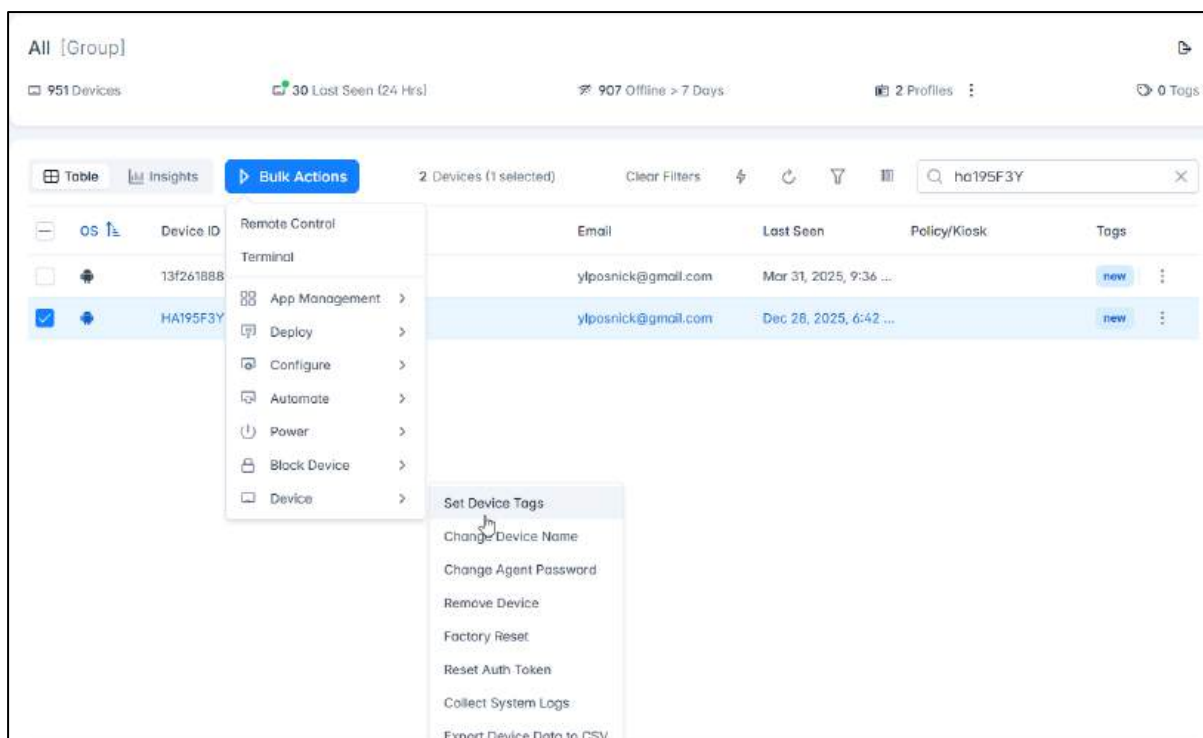
6.1.32 Tags

This option allows you to add to or remove tags from a device or user. These tags can help you in grouping users together, or when searching for devices.

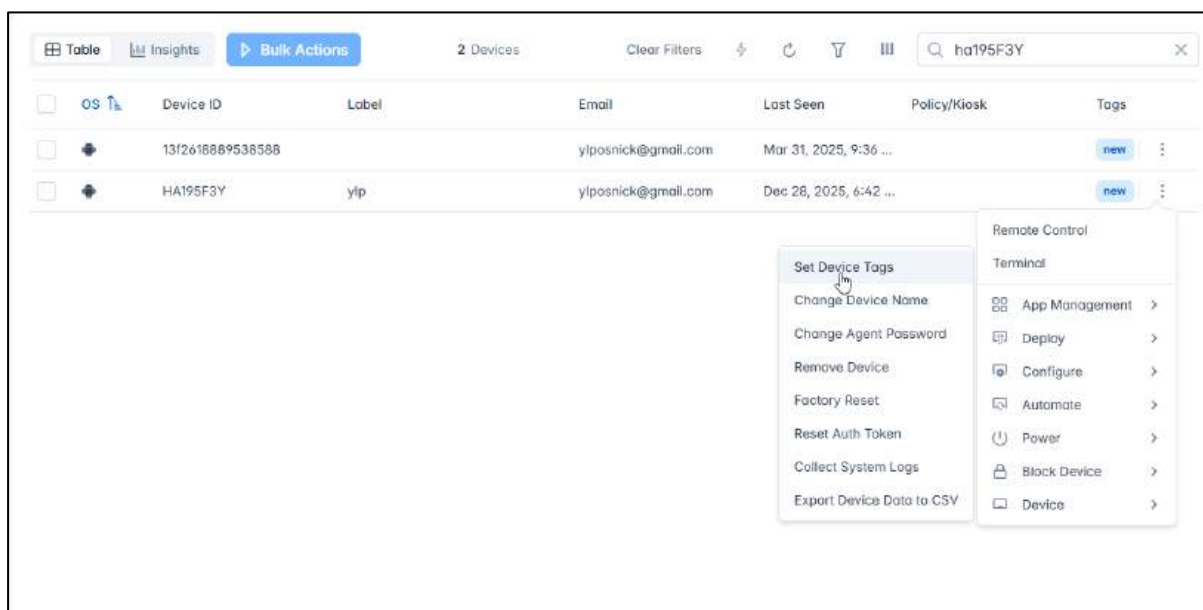


To add a tag:

1. In the Devices Table, select a device, or several devices, by checking their checkbox in the far-left column.
2. Click on **Bulk Actions>Device>Set Device Tags**.



If you wish to work with a single device, click on its **three-dot menu>Device>Set Device Tags**.



- Enter the name of the tag that you want to apply to these devices, click **Enter**, and press **Confirm**. You can add several tags this way. In our example, we add the tag “January” to these three devices that we have checked above:

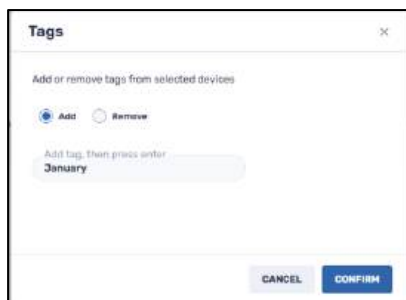
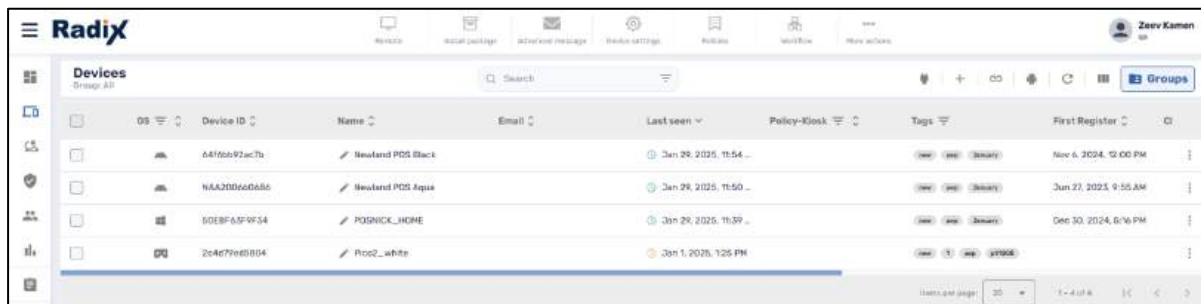
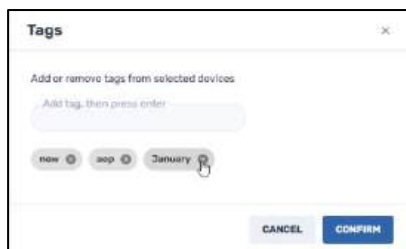


Figure 6-55: The tag "January" will be added to those three devices



- If you wish to delete a tag from a device, select that device, click on the **Tags** command, and click on the  on the tag you would like to delete.



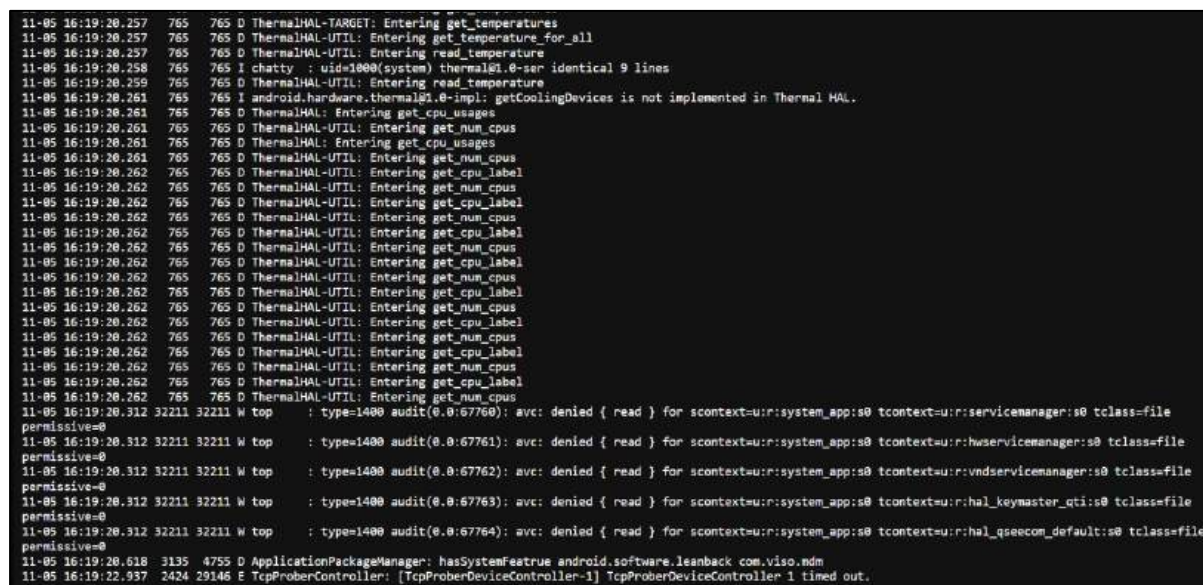
6.1.33 Terminal

This opens a fully featured, live terminal with an ADB (=Android Debug Bridge) shell connection. This allows you to remotely debug an issue with a device, as well as download a log of commands to the device and run exec scripts remotely.



There are also two icons in the upper right:

Icon	Description
	Get log —Allows you to download a log of command-line commands to be able to work on the device while offline
	Enable run as system —Allows you to change permissions. When you enable this feature, the icon will turn green. Another click will disable this feature, and the icon will turn gray again.

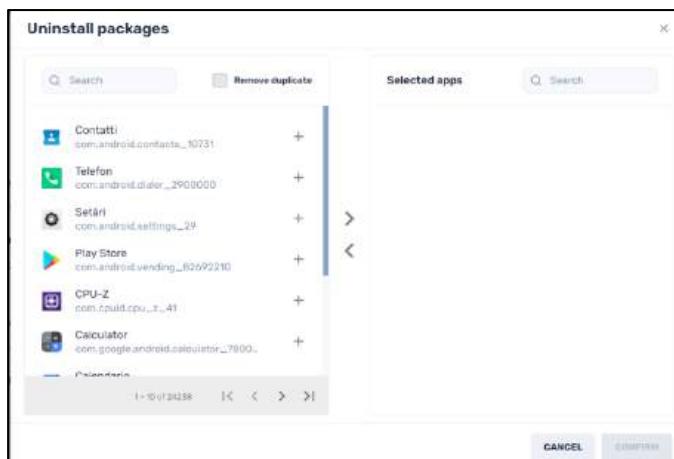


Note: The **Terminal** command can be used only on a single device at a time.

6.1.34 Uninstall Packages

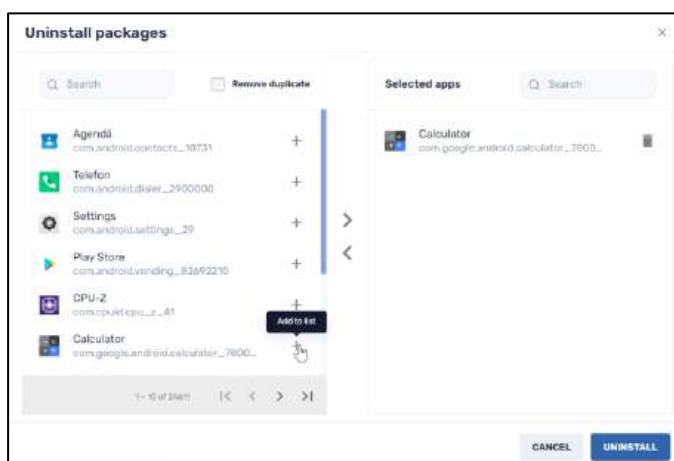
This command lets you uninstall software packages or apps on a device.

When you click on the **Uninstall packages** tile, the **Uninstall packages** window opens:



To uninstall a software package:

1. Click on the **Add to list** icon next to the software package you wish to uninstall. The package will now appear in the **Selected apps** column.



2. Click **Uninstall** to remove the software packages from the device.

6.1.35 Views

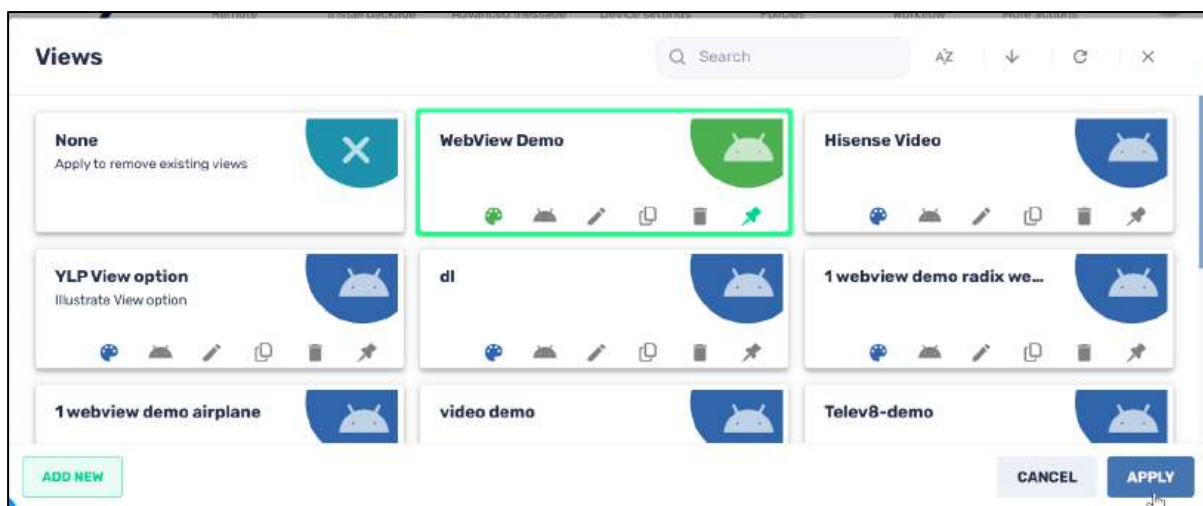
The **Views** repository option allows you to create a specialized Kiosk option where you choose allowed apps and access to a single URL on the remote device.

To access the Views command, go to:

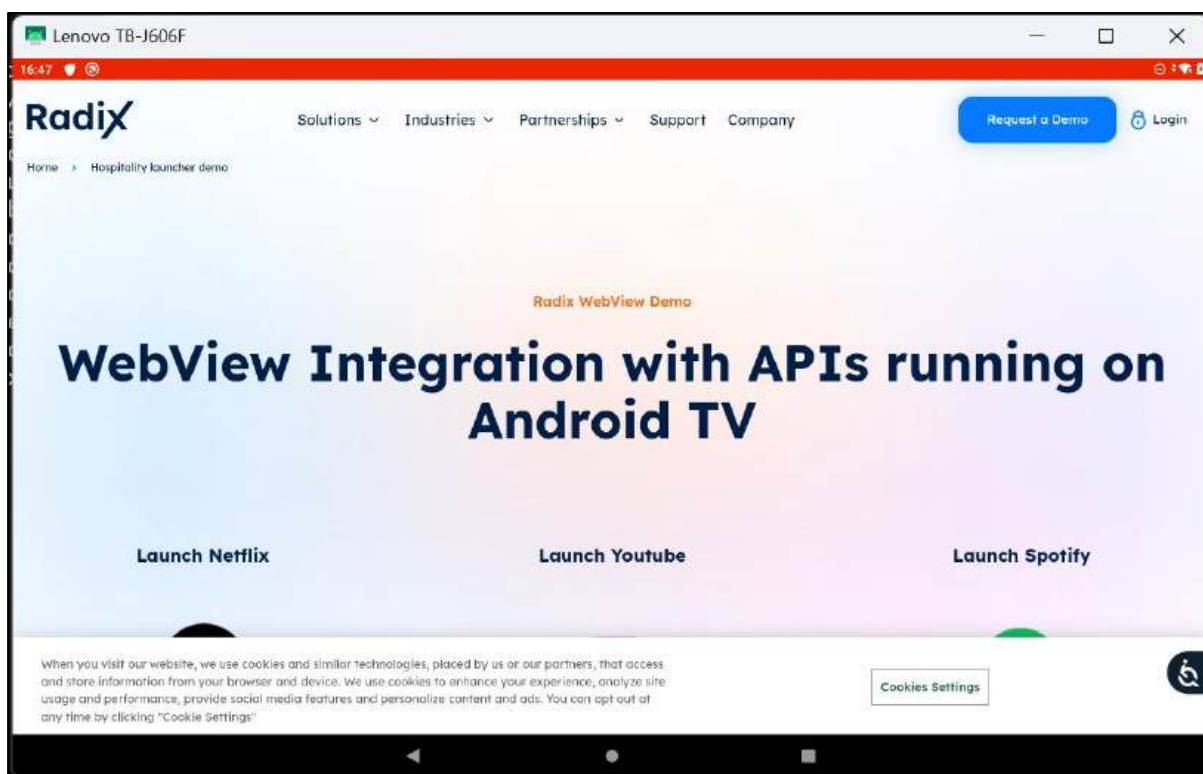
- The **Bulk Actions** button>**Configure**>**Views**
- The device's **three-dot Menu**>**Configure**>**Views**
- The **Device Dashboard**>**Repository Actions**>**Views**

6.1.35.1 Applying a View Option

1. When you click on **Bulk Actions**>**Configure**>**Views**, the **Views** options will appear.



- Click on one of the **Views** options to select it, and then click **Apply**. In our example, we selected the **WebView Demo** option.
The View option that you selected will be displayed on the device automatically.



6.1.35.2 Creating a New View Option

You can also add a new View option and customize it according to your preferences.

To add a new **View** option:

- Click on the **Add New** button at the lower left corner of the “**Views**” screen.
The “New View” screen opens.

New View

View name

View description

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

2. Assign a name and description to the new **View** option.

New View

View name
TMX View Option

View description
Illustrate View Option

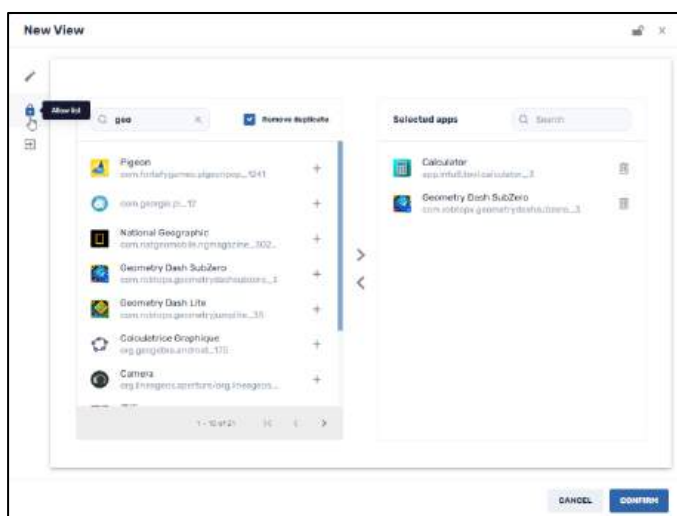
Set as private
This repository item will be visible only to this user

Hide content from others
Other users can apply this repository but cannot see or open its content

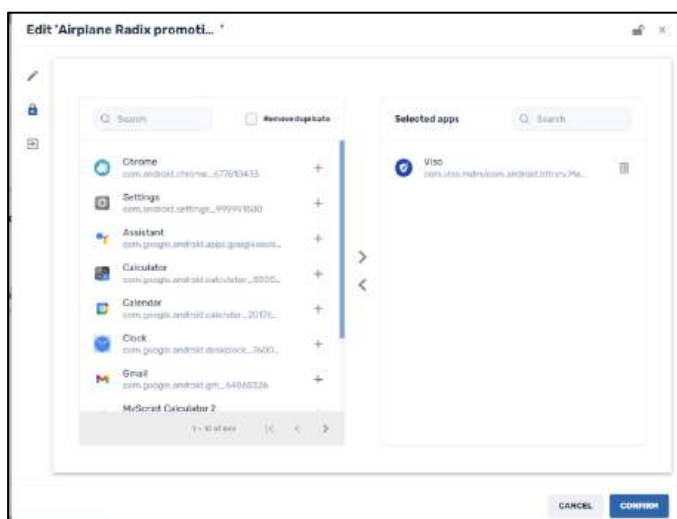
Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

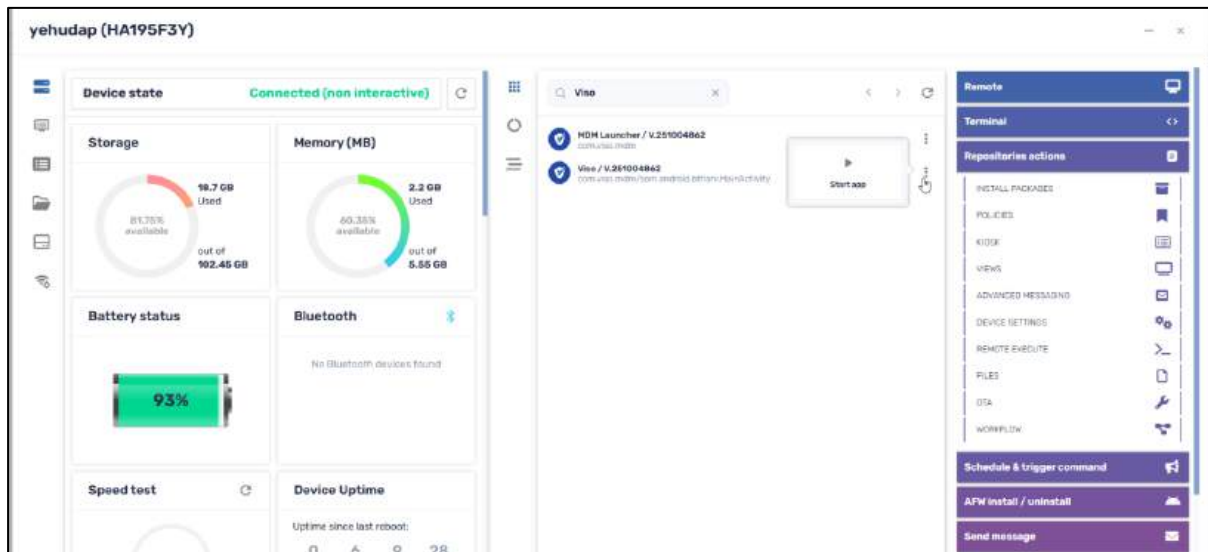
3. Click on the **Set as private** button if you want this new View option to be visible only to you (the creator of the item) when you log in to the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you want to limit who can edit this View option. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
6. Click on the **Allow list** icon and select the apps that you would like to allow on the remote device.



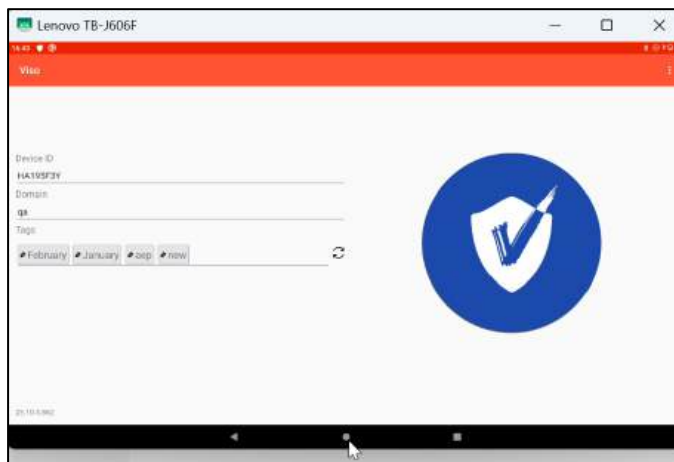
Note: These apps will not be accessible on the remote device. However, the administrator running the Radix MDM will be able to start the whitelisted apps from the Device Dashboard. For example, if the we add the Viso Agent app to the whitelist for our device, we the View will appear as follows:



When we apply the View, we can activate the Viso Agent app from the device's Device Dashboard:



- Clicking **Start app** will pause the video from the View's URL, and present the Viso Agent app.
- Tapping the **Home** button on the remote device will stop the app and restart the View's video URL.



7. Click on the **Web app** icon and provide a Web app URL in the textbox.



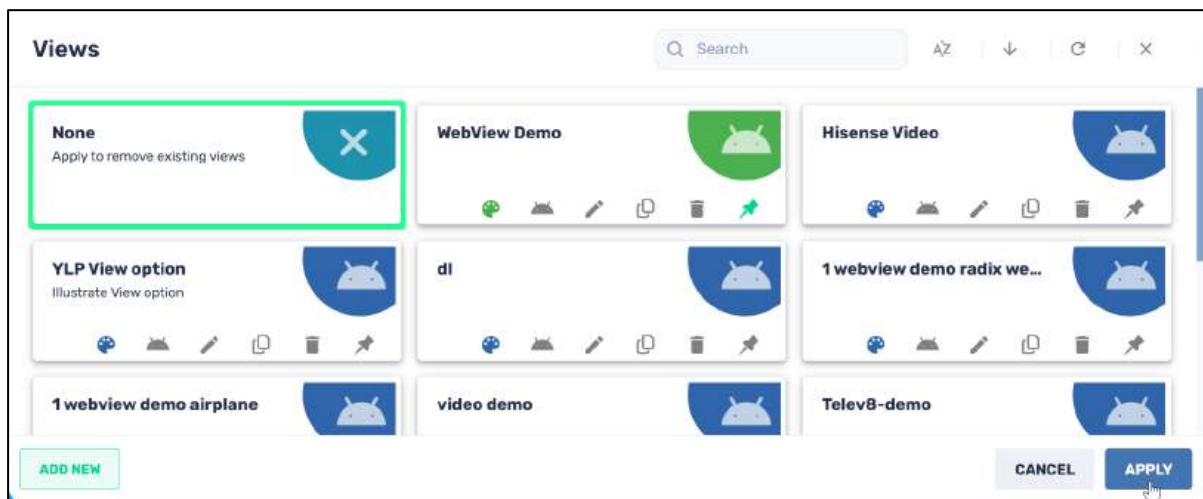
8. Click **Confirm**. The new **View** option will now appear in the Views Repository.

6.1.35.3 Removing a View Option from a Remote Device

The remote device will be limited only to the selected apps and a website associated with that View item for the duration of the time that you have applied that View option. If you want to use the device for other apps, you will have to remove the View mode that you have applied to the device. This can only be done from the Radix Device Management Platform.

To remove a View mode:

1. Select the **Views** command tile. The Views window opens.



2. Select the **None** option and click **Apply**. The device will now revert to full functionality again.

6.1.36 Wake on LAN

This option allows a device (or group of devices) to be turned on or “awakened” by means of a network message or a time trigger. However, this option is only available if:

- The remote device that you are trying to wake up has an Ethernet connection, and
- The remote device was turned off manually (not by means of the Radix interface’s Shutdown command).

When you click on the Wake on LAN tile, the **Wake on LAN** window opens:

Figure 6-56: Wake-on-LAN window

You have the following options:

- **By using a filter:** With this option, you can turn on a group of devices based on a predetermined search filter.

- **By Group Name:** Here, you supply the name of the group in the “Select group” field, either by typing in the name, or selecting it from a drop-down list. This will turn on

the group of devices, by sending the Wake-on-LAN signal to the entire group, if all the devices in the group have an Ethernet connection and were turned off manually.

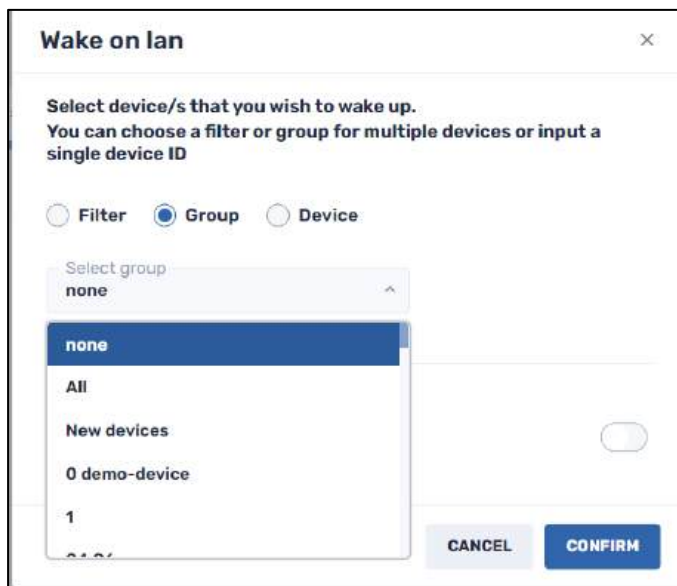


Figure 6-57: Wake-on-LAN option to turn on a group of devices

- **By Device ID:** Here, you can opt to wake up a single device by supplying its Device ID. You can find the Device ID in the list of devices, in the Devices Table:

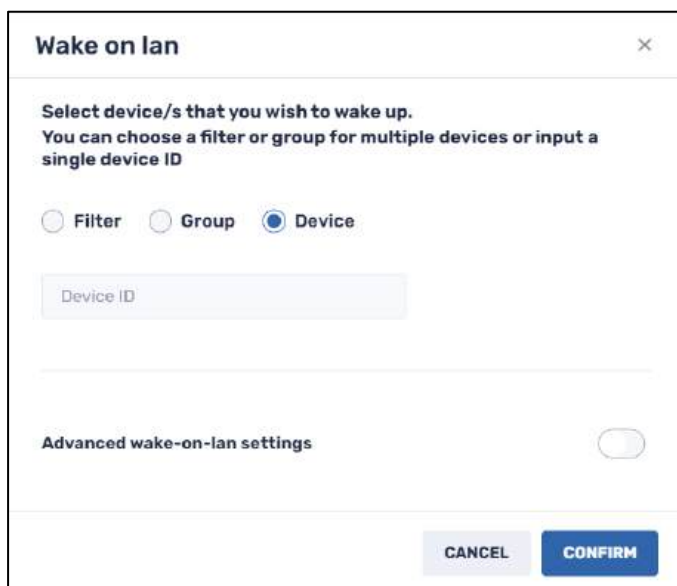


Figure 6-58: Wake-on-LAN option to turn on a single device

6.1.36.1 Advanced Wake-on-LAN

There is also an “Advanced Wake-On-LAN” setting option if your network has stricter rules and requires the Broadcast Address and Port to execute a command over LAN. This is useful if there is a specific Broadcast Address and IP port for your network of devices.

Figure 6-59: Advanced Wake-on-LAN fields

6.1.37 Wake Up

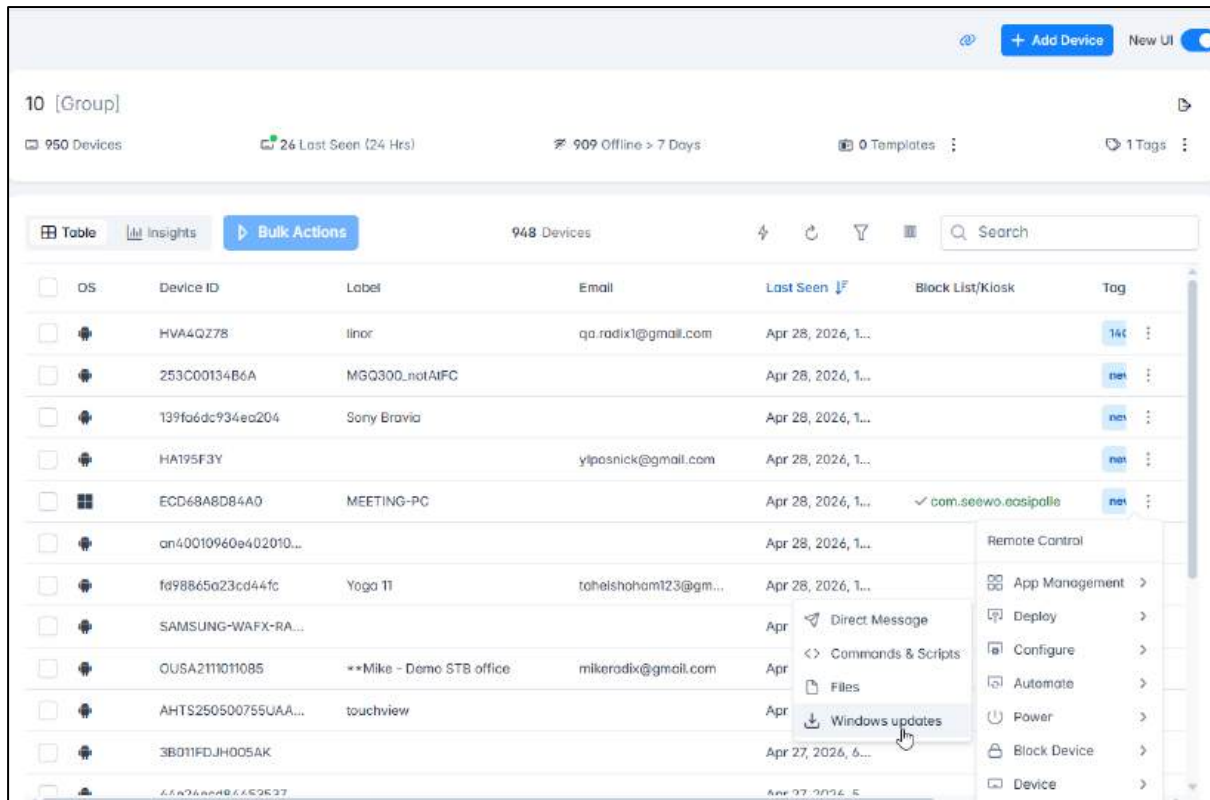
After a device has been put in Standby mode, the **Wake Up** command will turn the device's display back on.

Click **Yes** to wake up a device in Standby mode.

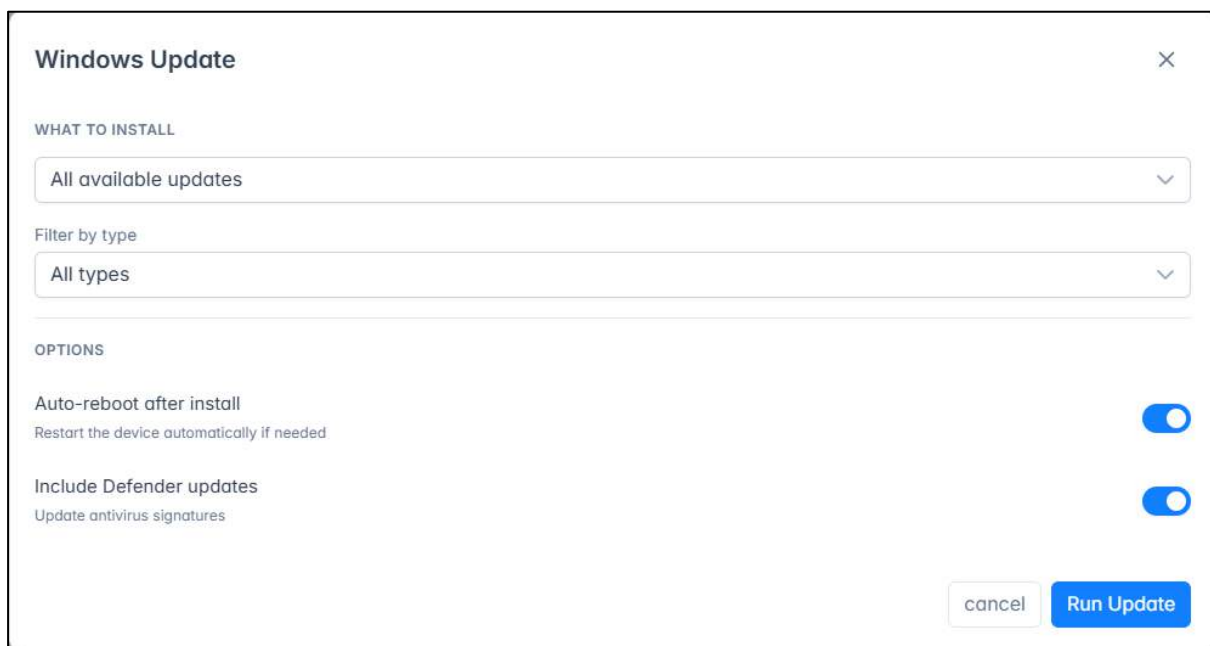
6.1.38 Windows Update

This feature allows you to install updates on Windows devices in your fleet. You can select whether to perform specific updates by their Knowledge Base number. Also, you can specify whether to update software packages, drivers, or both.

1. Click on a Windows device's three-dot menu>**Deploy>Windows Updates**:

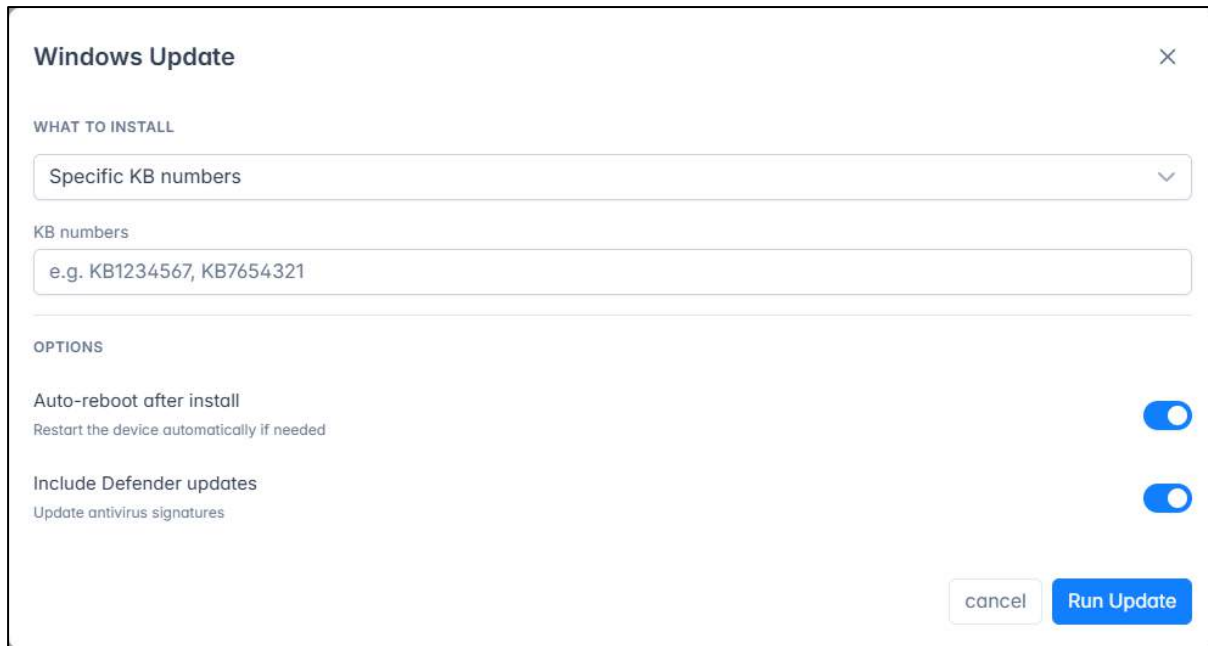


The Windows Update pane opens:



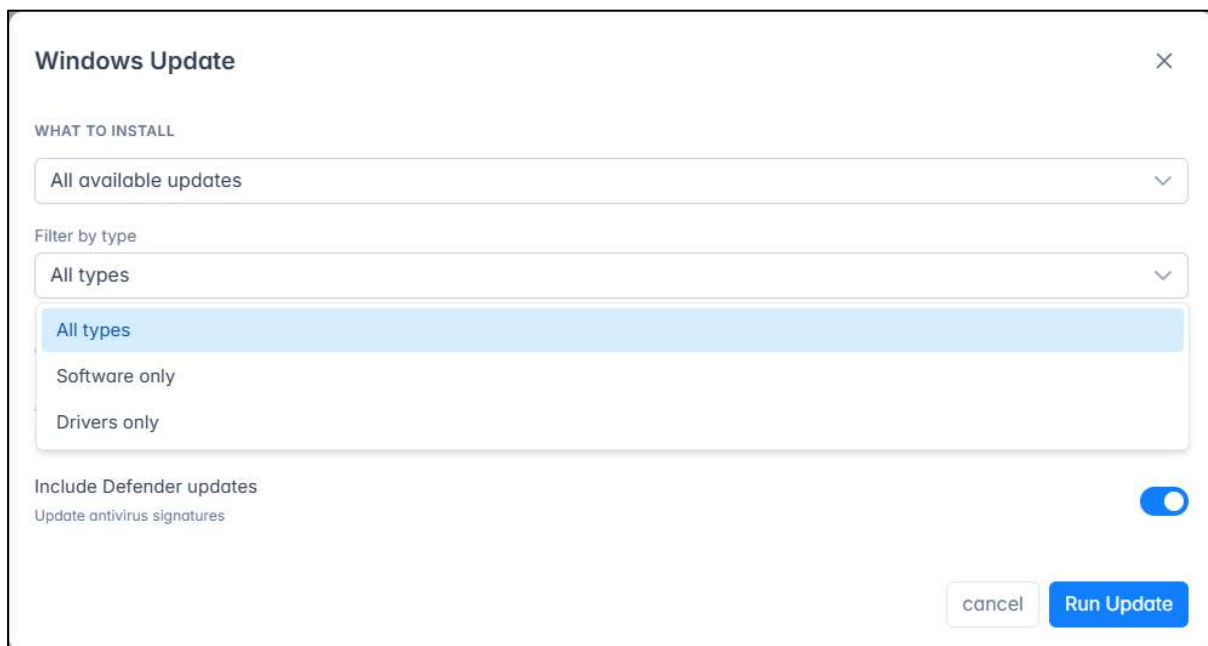
The options are as follows:

- **Which updates to install:** You can choose either to install all available updates, or specific updates by their Knowledge Base number:



The screenshot shows a 'Windows Update' dialog box. Under the 'WHAT TO INSTALL' section, the 'Specific KB numbers' option is selected in a dropdown menu. Below this, there is a text input field containing 'e.g. KB1234567, KB7654321'. In the 'OPTIONS' section, both 'Auto-reboot after install' and 'Include Defender updates' are toggled on. At the bottom right, there are 'cancel' and 'Run Update' buttons.

- **What type of update to install:** You can select whether to install software updates, driver updates, or both:



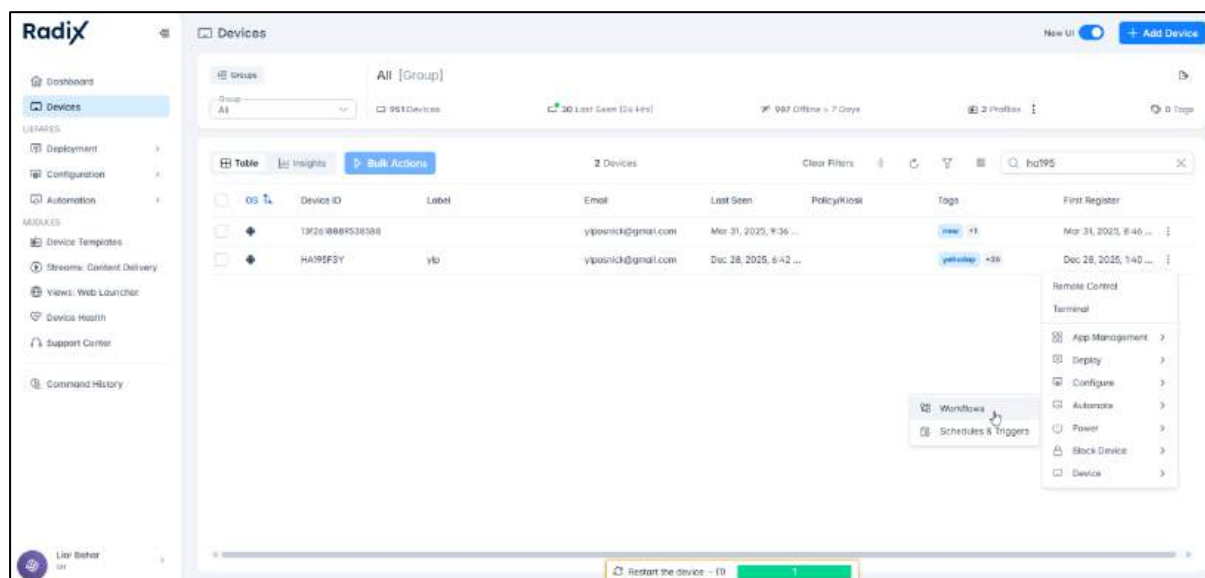
The screenshot shows a 'Windows Update' dialog box. Under the 'WHAT TO INSTALL' section, the 'All available updates' option is selected in a dropdown menu. Below this, there is a 'Filter by type' section with a dropdown menu showing 'All types' selected. A list of options is visible: 'All types', 'Software only', and 'Drivers only'. In the 'OPTIONS' section, 'Include Defender updates' is toggled on. At the bottom right, there are 'cancel' and 'Run Update' buttons.

- **Auto-reboot after install:** By clicking on this button, you can have the remote device automatically reboot after installing the update.
- **Include Defender updates:** By clicking on this button, you can update Windows Defender as well.

6.1.39 Workflow

This feature allows sending a series of commands to a device. The **Workflow** command allows you to arrange a series of commands in a particular order, save the arrangement, and deploy the workflow to a device or fleet of devices. There are also options to create a Favorites menu or move commands around within workflows.

Click on a device's three-dot menu>**Automate**>**Workflow**:



The Workflow repository opens:



You select an existing workflow and apply it or add a new workflow tile to the list.

To add a new Workflow:

1. Click on the **Add New** button in the lower left corner of the Workflow window.
The **New Workflow—Edit Details** screen opens.

New workflow

Workflow name
Workflow Illustration

Workflow description
Illustrates use of workflow

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

Hide content from others
Other users can apply this repository but cannot see or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

2. Provide a name and description for the workflow.
3. Click on the **Set as private** button if you would like the Workflow option to only be visible to you (the creator of the item) when using the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the Workflow. Anyone with **Administrator** privileges can edit it, while someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position .
6. To add commands to the workflow, click on the Commands icon .
7. Click on **Add Command**.
The **Commands Grid** opens.

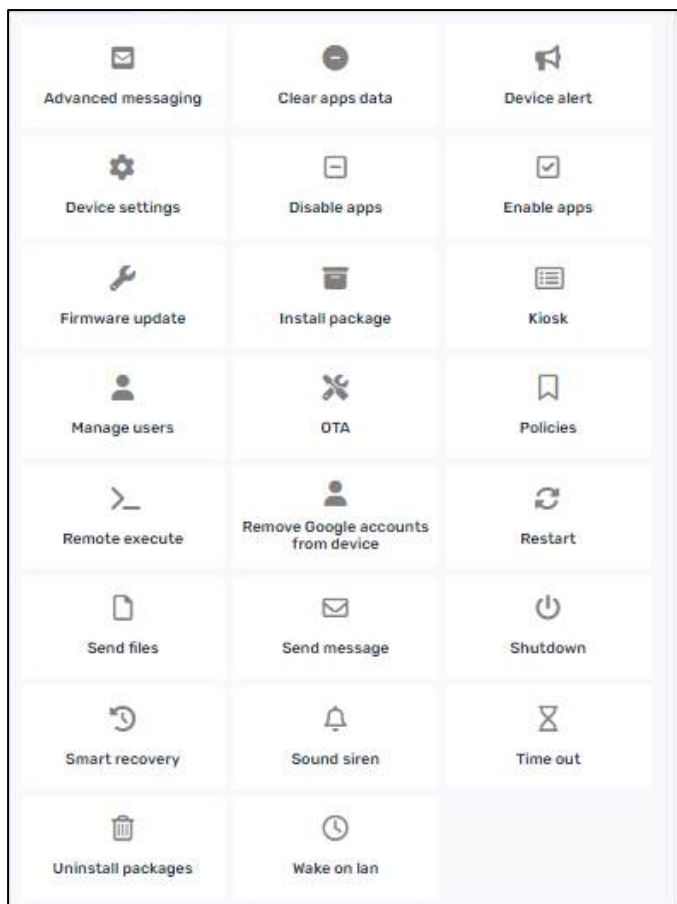
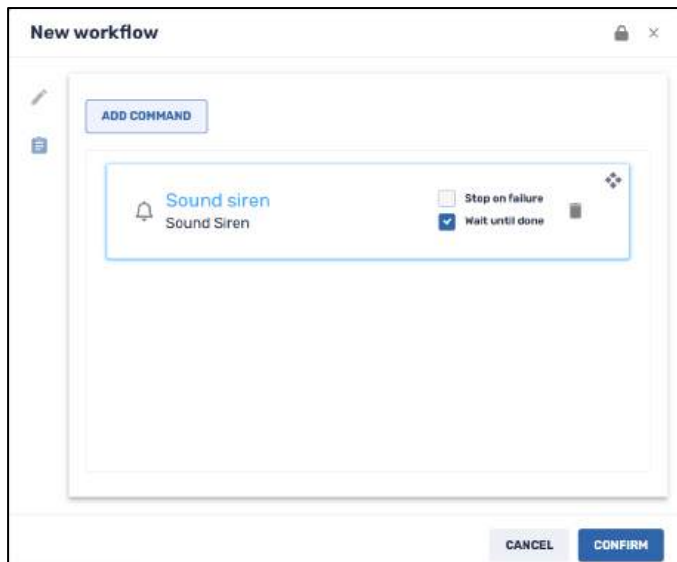
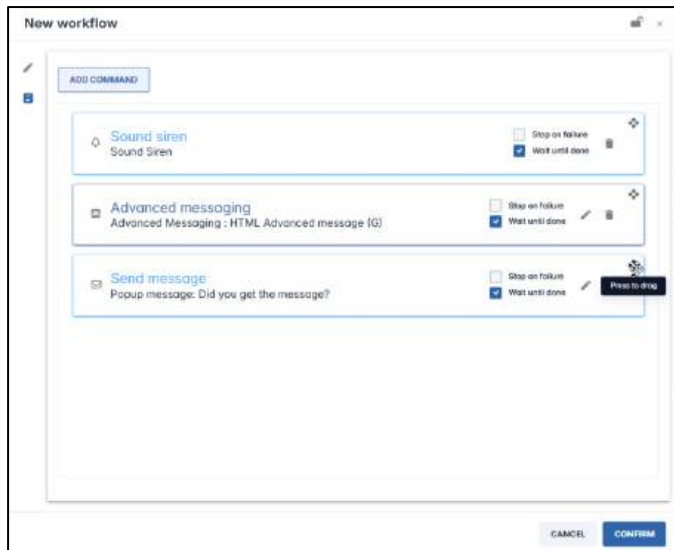


Figure 6-60: Workflow Commands Grid

8. Select a command from the grid. It will appear in the **New Workflow** window.



9. Select all the commands for the desired workflow in the same manner, using **Add Command**.
10. If you wish to rearrange the order, click on the **Press to drag** icon, and move the commands in the preferred order.



11. Click **Confirm** to save the Workflow.
12. To implement the Workflow, select it in the Workflow window, and click **Apply**.

6.2 Warning Icons

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

On occasion, you will see that a device has a warning icon  next to its Device ID. This indicates that the device has lost its authentication token and cannot register with the server. It could be due to the device being uninstalled and reinstalled, a factory reset, or data being wiped from the device.

You should reset the device's authentication token, to enroll your device on the server again.

Software ID	Serial number	Name	Local ip	Last seen	Location	Sim	Email	Ip address	Agent version	Email
195F3V	H	Etan	192.168.5.42	Nov 5, 2023, 10:27 AM			radi	213.8.193.110	250902681	
12FWDQ	H4	Lemovo 9 black GG	192.168.5.37	Oct 26, 2023, 6:07 PM	32.02246/34.85181		stut	213.8.193.110	103802748	86691904000975
H412		etan golan	192.168.1.157	Oct 1, 2023, 2:40 PM	31.89716/34.78091			84.229.89.78	105200489	

Figure 6-61: Warning icon next to device in Devices Table

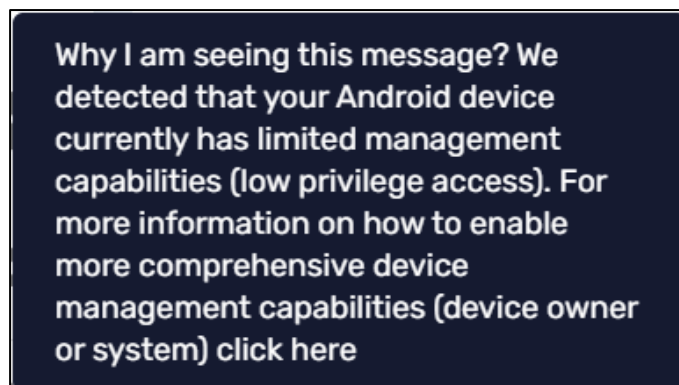


Figure 6-62: Text of Warning Message

If you click on the warning icon, a window opens, giving you options to enable comprehensive management capabilities on the device and reset the device's authentication token. After taking the necessary steps, you will be prompted to confirm the reset. After confirming, the warning icon should disappear.

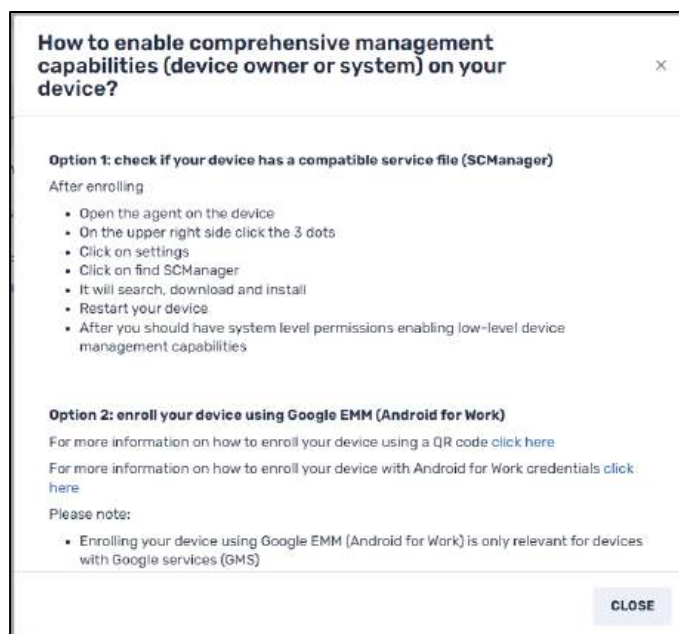
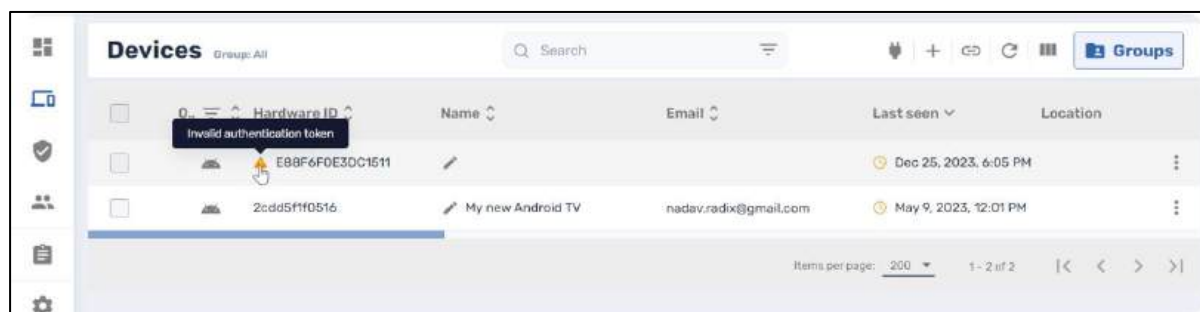


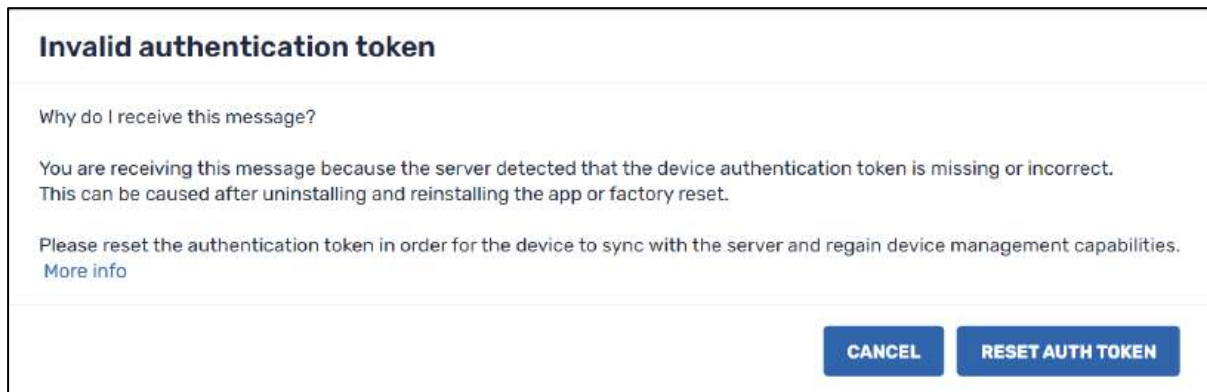
Figure 6-63: Instructions to re-enroll a device

6.2.1 Invalid Authentication Token Warning

Another warning icon that you may encounter in the Devices Table is an Invalid Authentication Token warning.



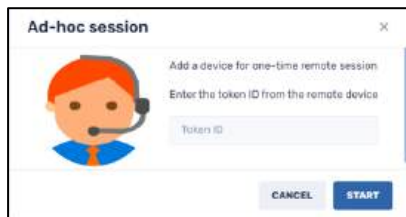
When you click on the warning icon, you will receive the following popup message:



Clicking on **Reset Authentication Token** should resolve the problem.

6.2.2 Ad-Hoc Session

This icon opens a dialog box where you can enter a token ID for a one-time remote session with a device. This can be useful if you want to service a device that has the Viso app installed but is not among the fleet of devices that you control. Opening an Ad-Hoc session lets another Radix Device Management Platform administrator access the device.



Meanwhile, the user of the remote device must supply the token ID.

To supply a token ID and start an ad-hoc session:

1. The user of the remote device opens the Viso app on their device.
2. The user taps on the three-dot menu in the upper right-hand corner. A drop-down menu appears, with the option “Start Ad-hoc session”.

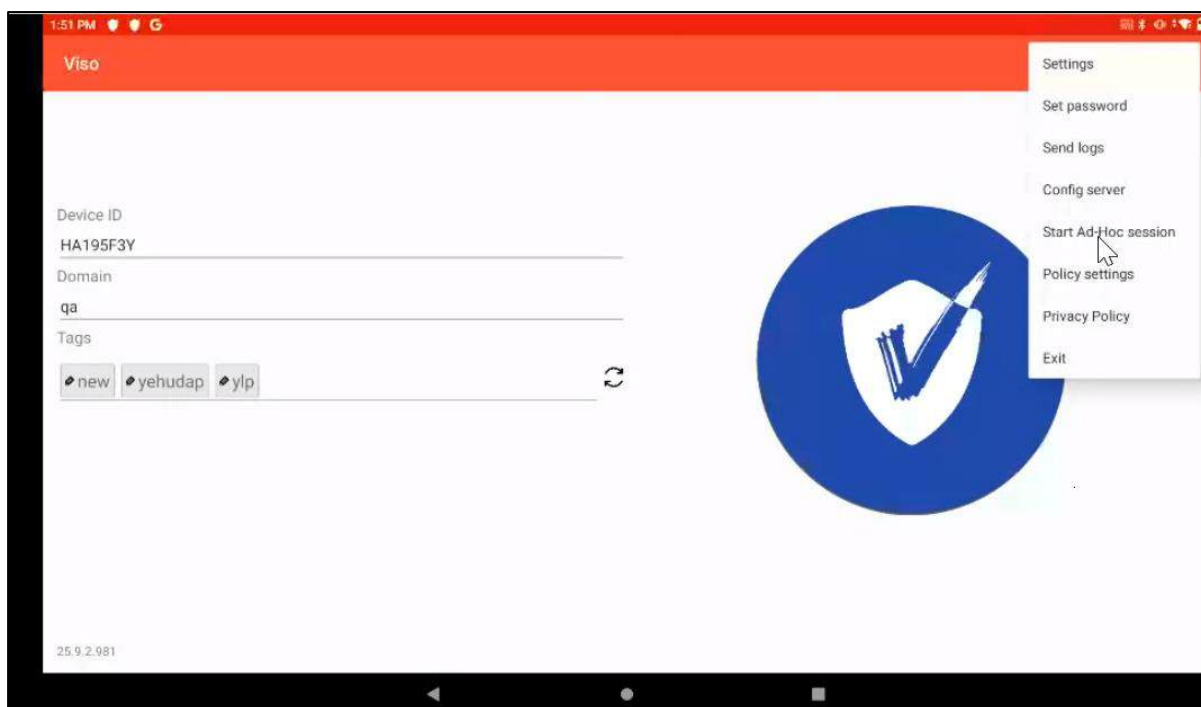


Figure 6-64: Start Ad-Hoc session option on the remote device

- When the remote user taps on **Start Ad-hoc session**, a window will open on their device, supplying the token ID.

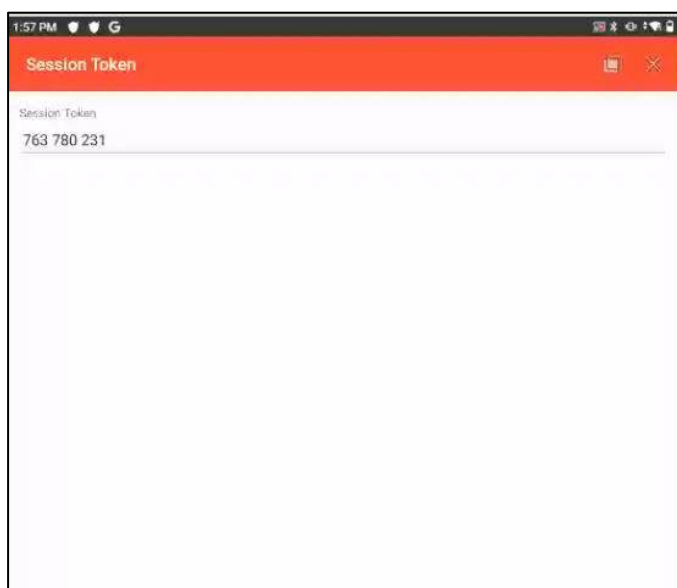


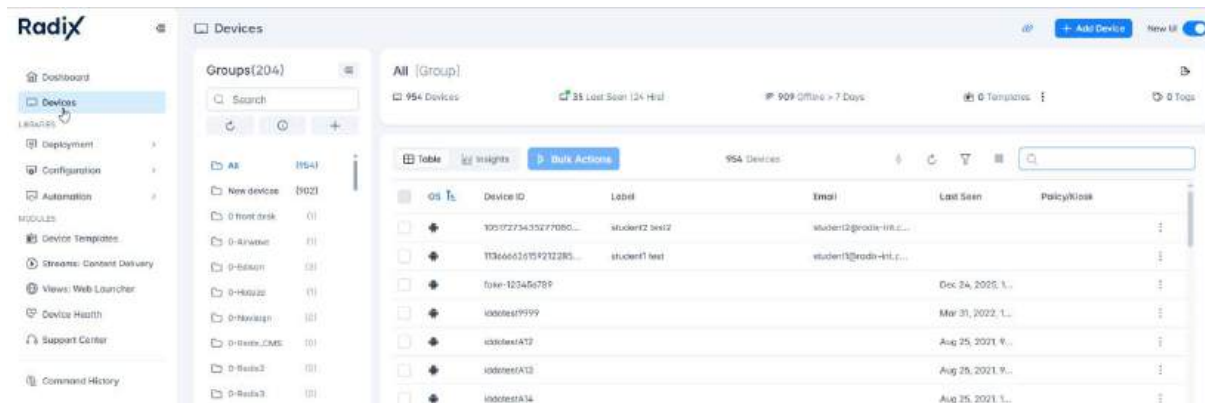
Figure 6-65: Session Token window, as it appears on the remote device

- After supplying the Session Token ID to the administrator in the Radix Device Management interface, the device will now appear in the interface's list of devices.

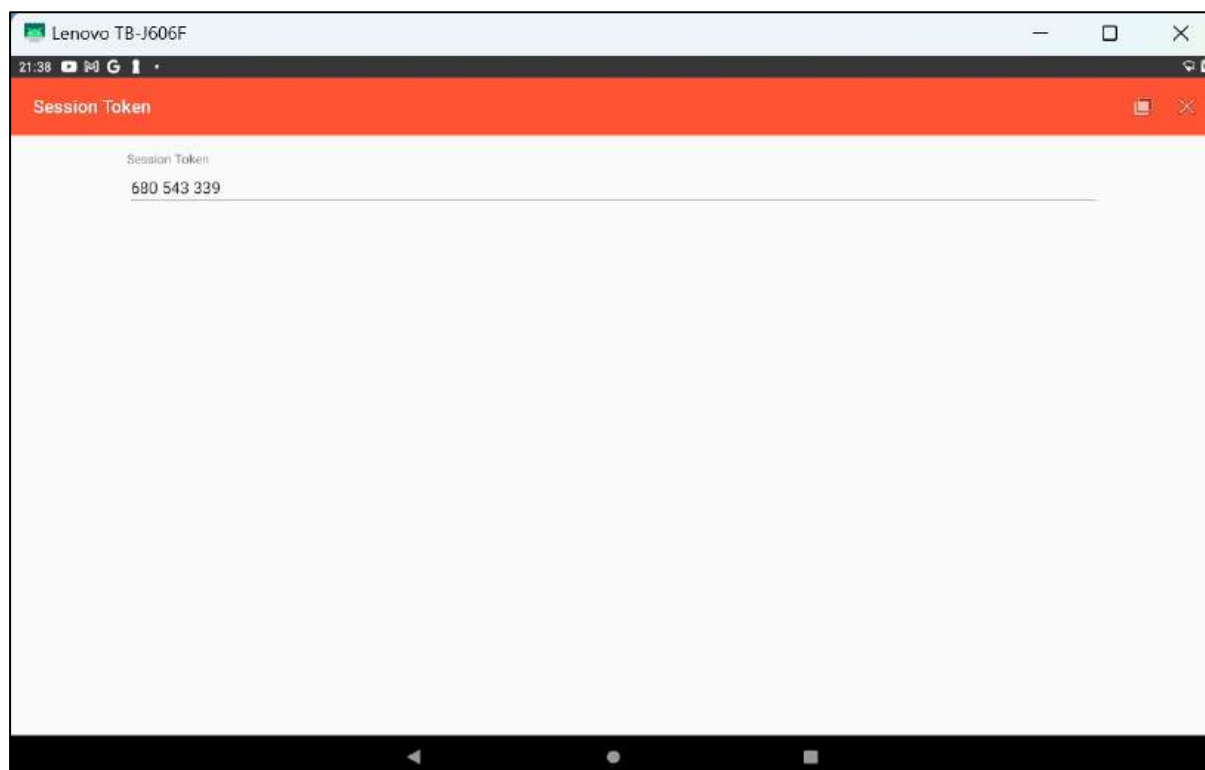
6.2.2.1 Example of an Ad Hoc Session

Here is an example of an Ad Hoc session.

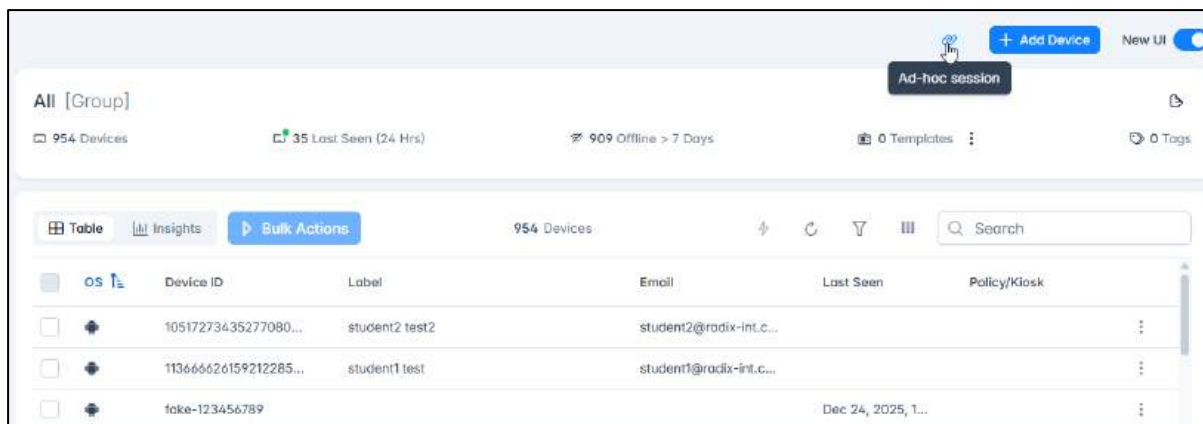
- A Radix Device Management Platform administrator opens their list of devices by clicking on the **Devices** icon in the Overview Dashboard.



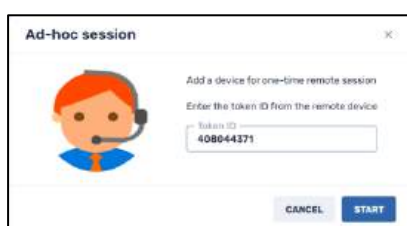
- Let us say the administrator wants to add the device HA195F3Y (a Lenovo tablet computer), so that the administrator can service it. The user of the device opens the Viso app on their remote device, as above, and generates the Session Token.



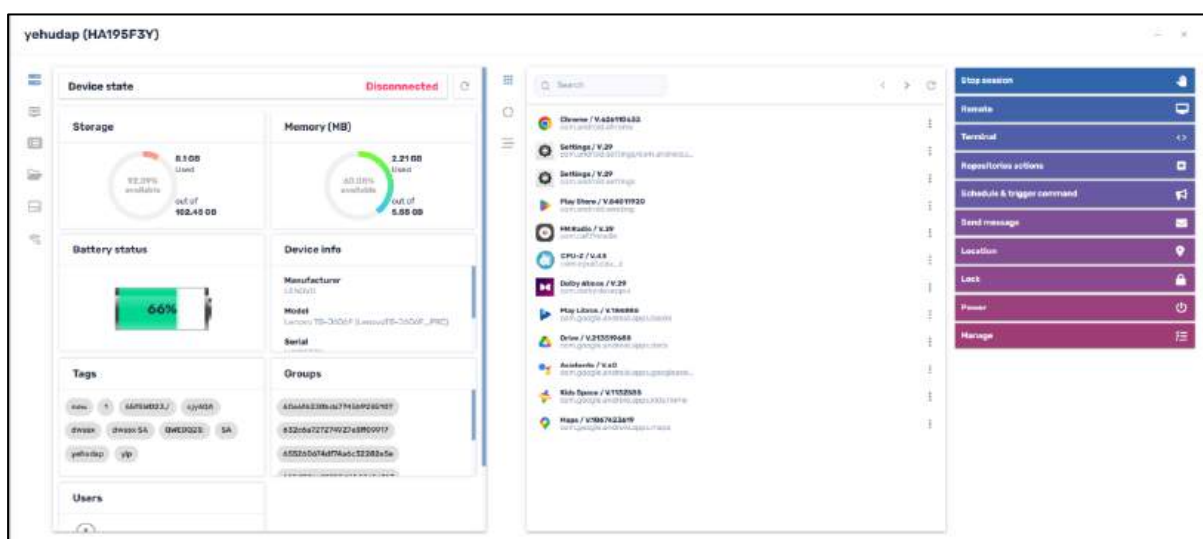
- The Radix Device Management Platform Administrator opens an Ad-Hoc session on their device by clicking on the Ad-Hoc Session icon.



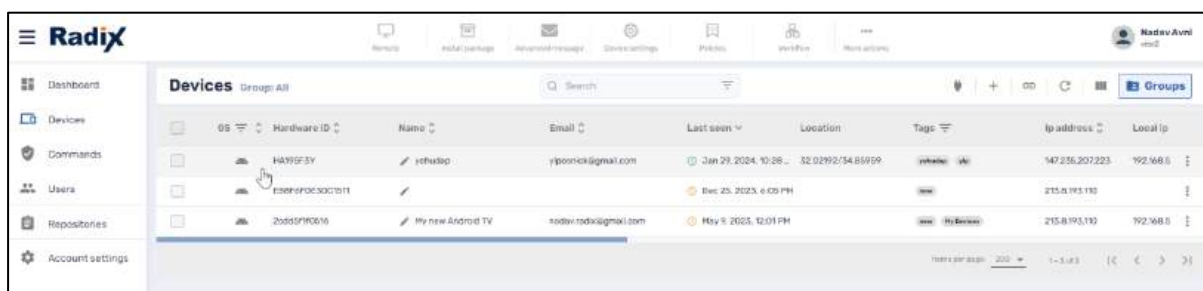
- The Radix Device Management Platform administrator enters the Token ID in the Ad-hoc Session window and clicks **Start**.



- The Device Dashboard for the newly added device HA195F3Y opens, allowing the Radix Device Management Platform to access it.

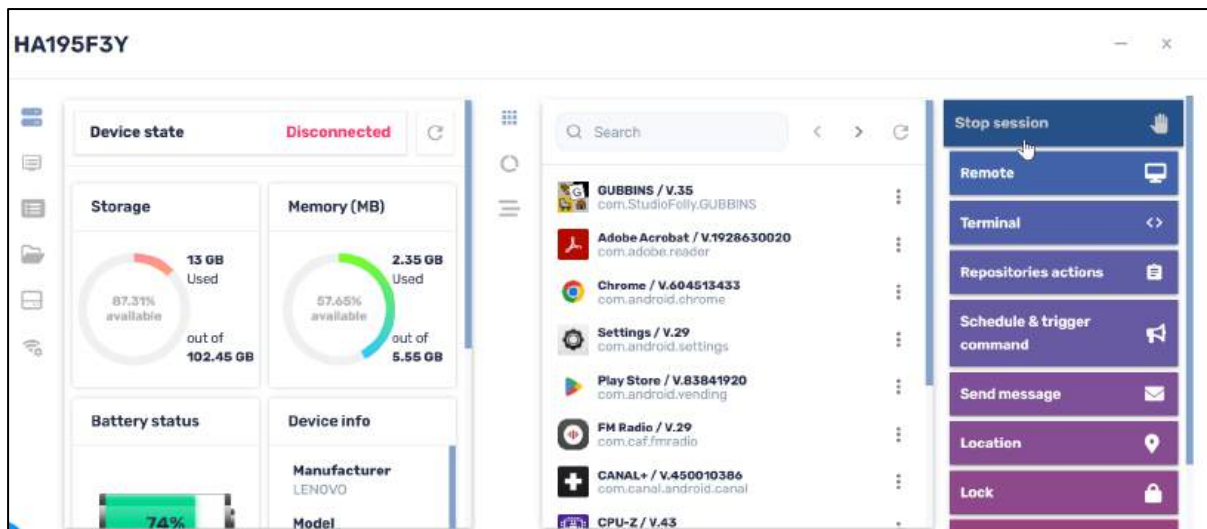


Also, the device will appear in the Radix Device Management Platform Administrator's list of devices:

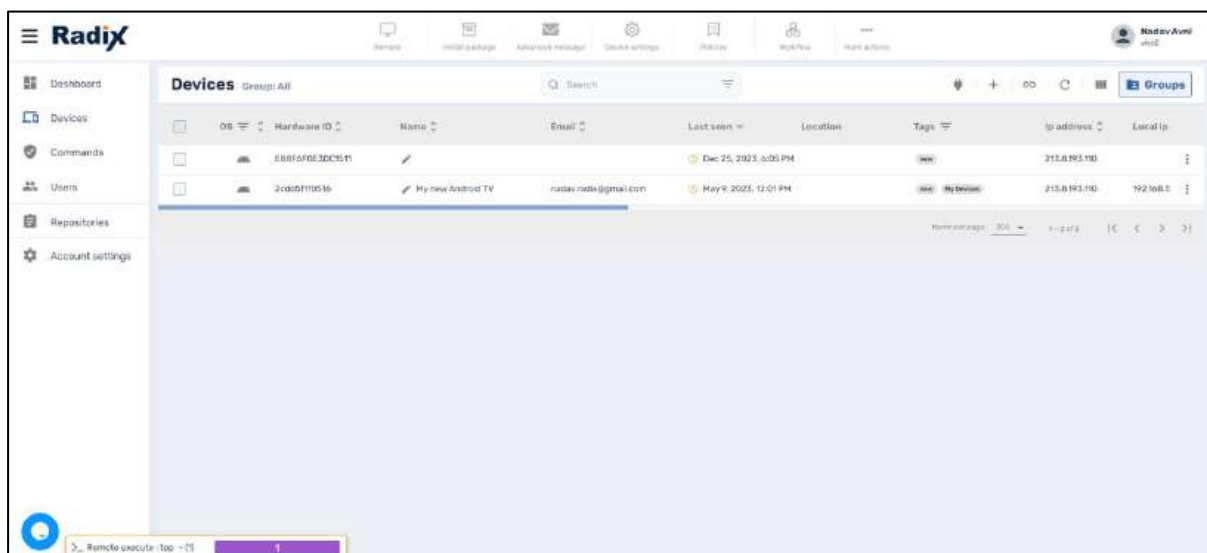


6.2.2.2 Ending an Ad-hoc Session

The Administrator can click on **Stop Session** in the device's Device Dashboard to end the Ad Hoc session.



The device will no longer appear in the administrator's list of devices:



Chapter 7. Libraries Menu

The sidebar menu has the Libraries category. It consists of three types of repositories of commands. After creating these repository items, you can then assign them to devices in your fleet.



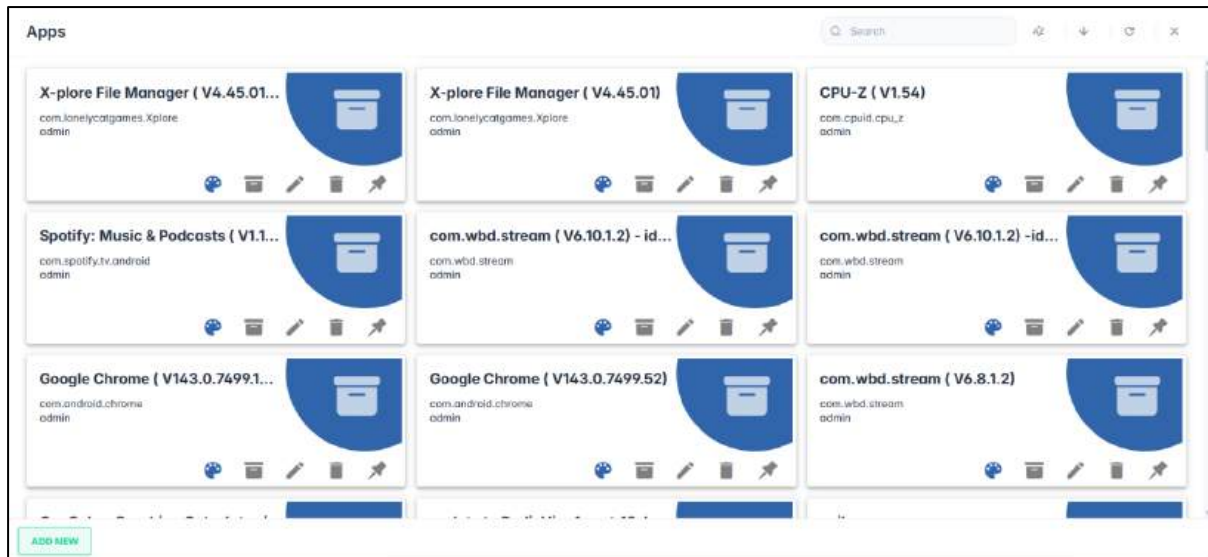
- **Deployment Repository:** This contains the commands:
 - [Apps](#)
 - [Messaging](#),
 - [Commands & Scripts](#),
 - [OTA](#),
 - [OTA Update Engine](#),
 - [Files](#),
 - [Smart Recovery](#).
- **Configuration Repository:** This contains the commands
 - [Device Settings](#),
 - [Block Lists](#),
 - [Kiosk Modes](#),
 - [Views](#),
 - [Android for Work](#)
- **Automation Repository:** This contains the commands:
 - [Workflows](#),
 - [Schedules & Triggers](#)

You can create these repository items here in the Libraries console. However, you can only employ these items by executing a command either from the Commands Ribbon, the device dashboard, or the device's three-dot menu. You must select a device or group of devices and execute these commands on them.

7.1 Deployment Options

7.1.1 Apps

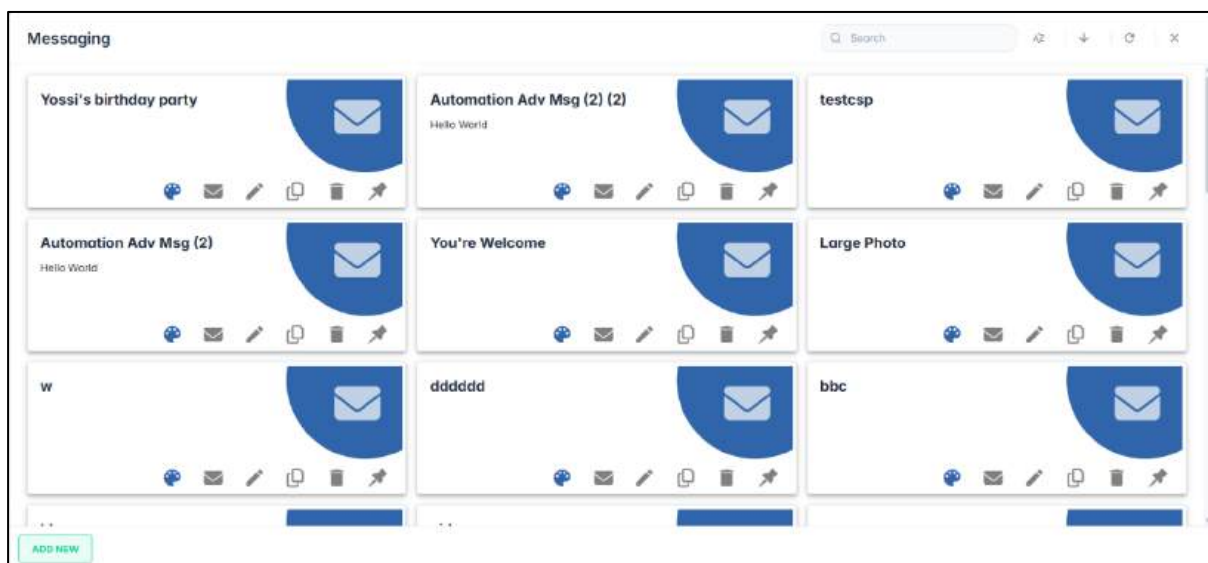
This option allows you to remotely install software packages on a particular device. When you click on **Apps**, a grid of software packages appears. These are software packages that have already been stored in the Radix system. See **Section 6.1.13, Install App/Install Package**.



7.1.2 Messaging

This option sends a text message with an image to a device. For example, the message may be a “Welcome” message, a holiday greeting, or an emergency alert. The message options include an image, an image with sound, a full-screen YouTube video, or interactive clickable HTML forms. The message can be timed and triggered according to time of day and the like. See **Section 6.1.1, Advanced Messaging**.

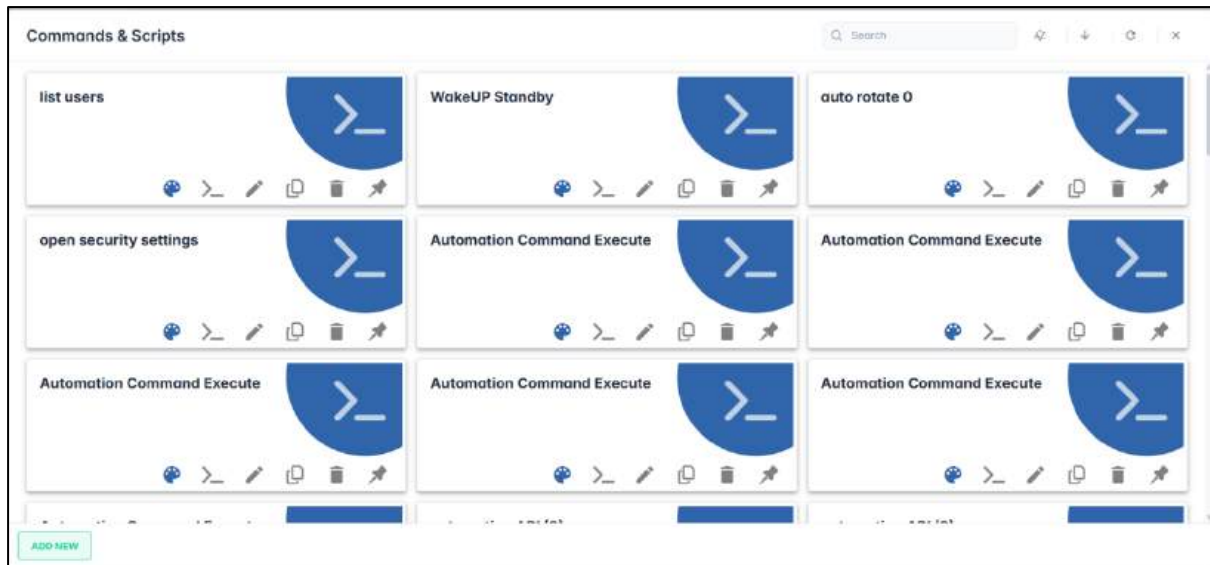
When you click on Messaging, the Messaging window opens:



7.1.3 Commands and Scripts

This option allows the Radix Device Management user to execute a particular command line command or script on a device, or even on a group of devices at once. See **Section 6.1.23, Remote Execute**.

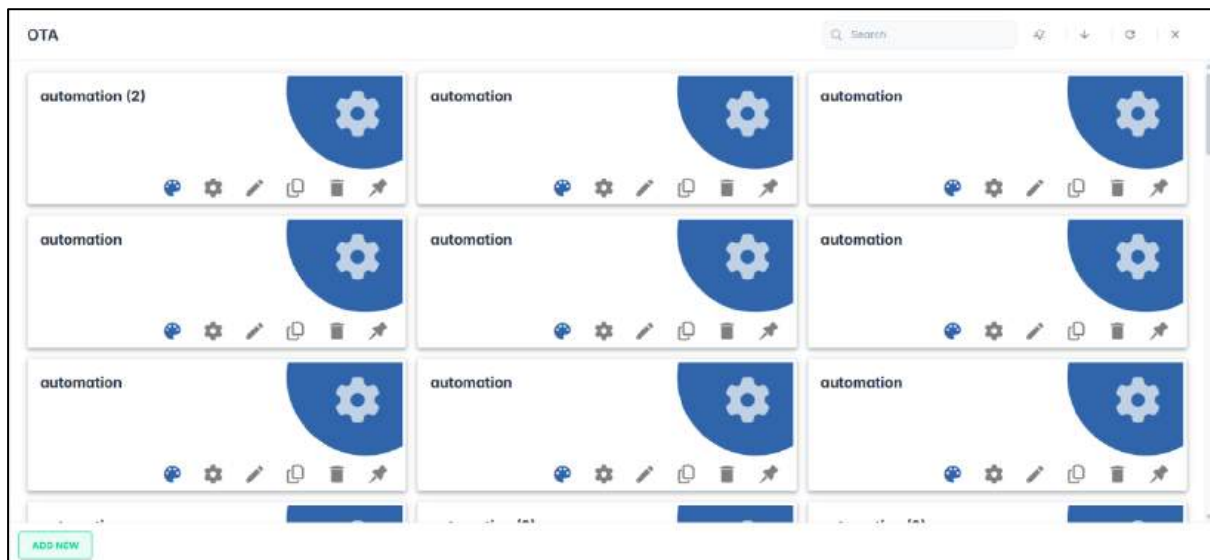
When you click on Commands & Scripts, the following window opens:



7.1.4 OTA

This enables an Android device to receive and install updates to its operating system or apps, or to dispatch an image of an operating system to a device. The OTA option is primarily for older Android devices, running an operating system older than Android 8.0, or that don't employ virtual A/B slot partitions. See **Section 6.1.18, OTA**.

When you click on OTA, the following window opens:

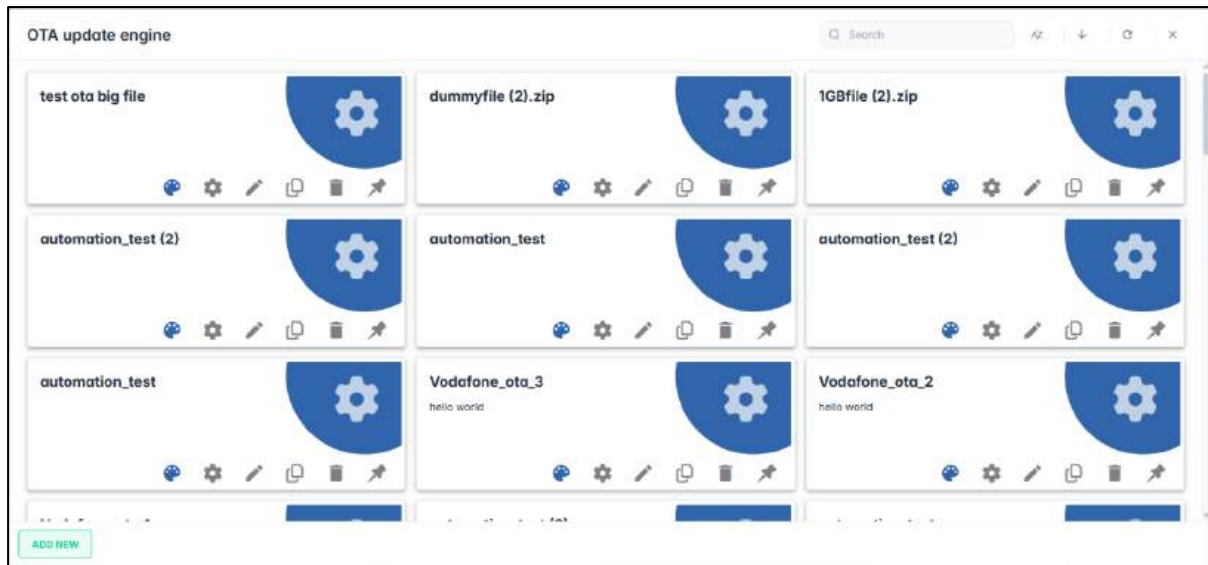


For newer devices, you should use the **OTA Update Engine** command (**Section 6.1.19, OTA Update Engine**).

7.1.5 OTA Update Engine

This option provides a method of performing an over-the-air update to an Android device's operating system or apps, or to dispatch an image of an operating system to a device. The OTA Update Engine option is for devices running Android 8.0 or newer, and that employ the A/B partition updater. See **Section 6.1.19, OTA Update Engine**.

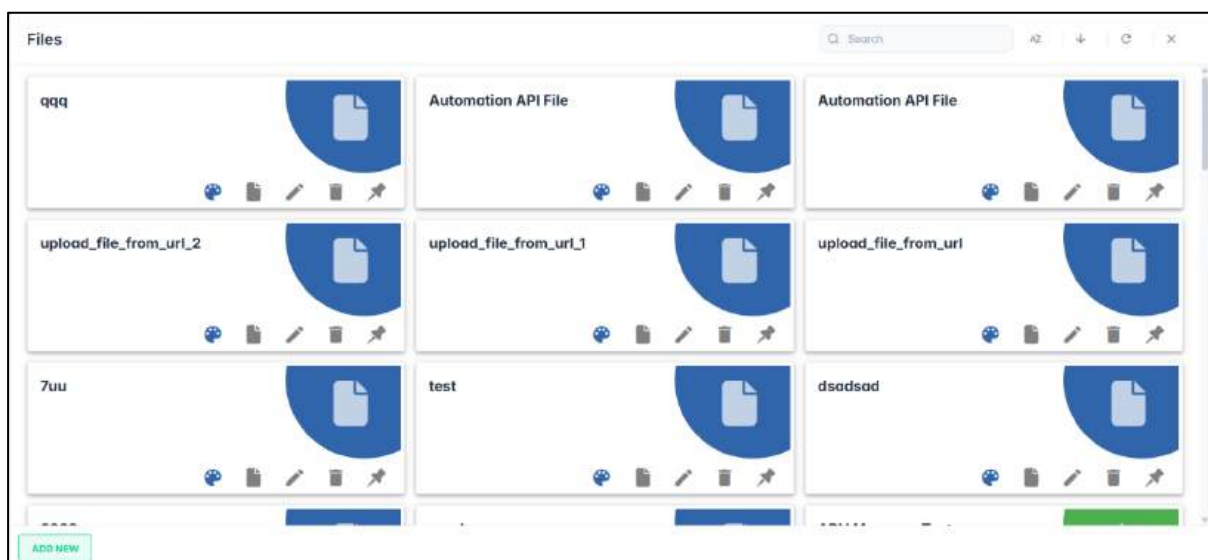
When you click on OTA Update Engine, the following window opens:



7.1.6 Files

This allows you to send specific files to a remote device. You can either supply a URL from which to retrieve the file or upload a file from your computer. See **Section 6.1.28, Send Files**.

When you click on Files, the following window opens:



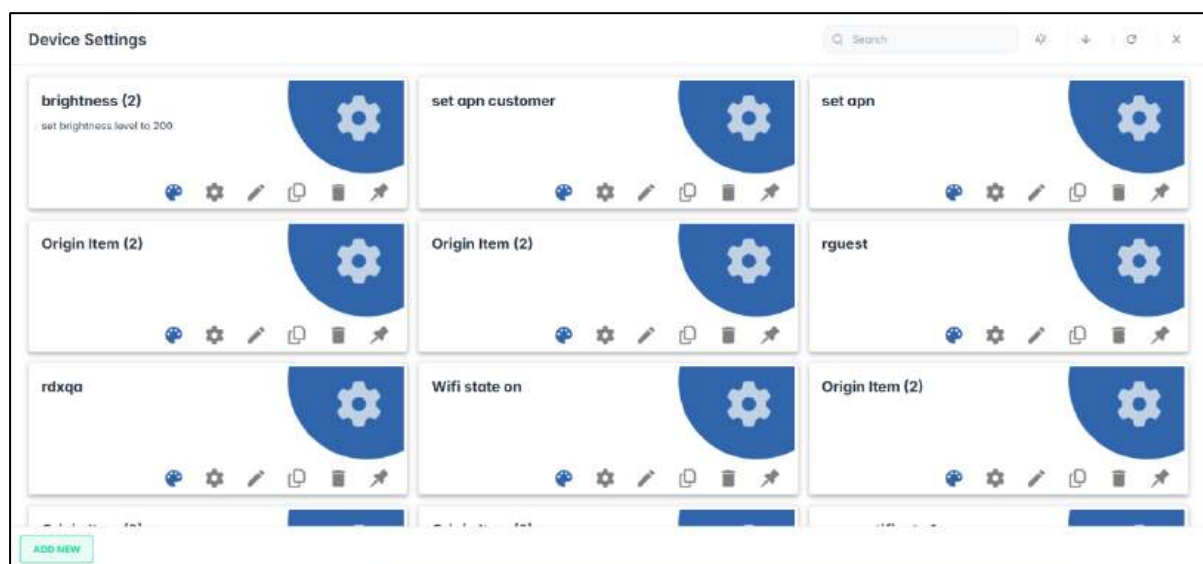
7.1.7 Smart Recovery

Smart Recovery is a Windows application that allows you to implement settings to repair a Windows device that has crashed. Once you have installed Smart Recovery (LITE, DUO, or PRO) on a remote Windows device, you can execute Smart Recovery commands via the Radix Device Management Platform interface and roll back the Windows computer to a prior state.

7.2 Configurations Options

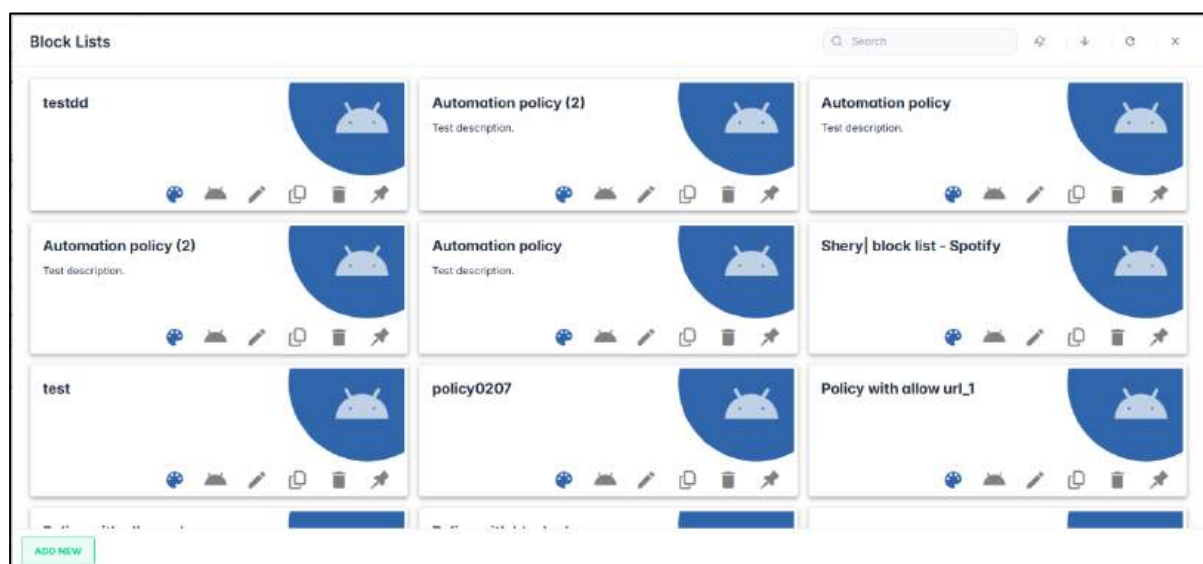
7.2.1 Device Settings

This option allows the Radix Device Management user to remotely adjust a device's settings. This could include selecting a type of keyboard, enabling or disabling a screen saver, or performing a reset on the device. See **Section 6.1.8, Device Settings**.



7.2.2 Block Lists

If certain applications on your device violate your rights, have security issues, or are not play-protected, you can essentially blacklist and block these applications. This can be done using the **Block Lists** option in the drop-down menu. See **Section 6.1.21, Policies (Block Lists)**.



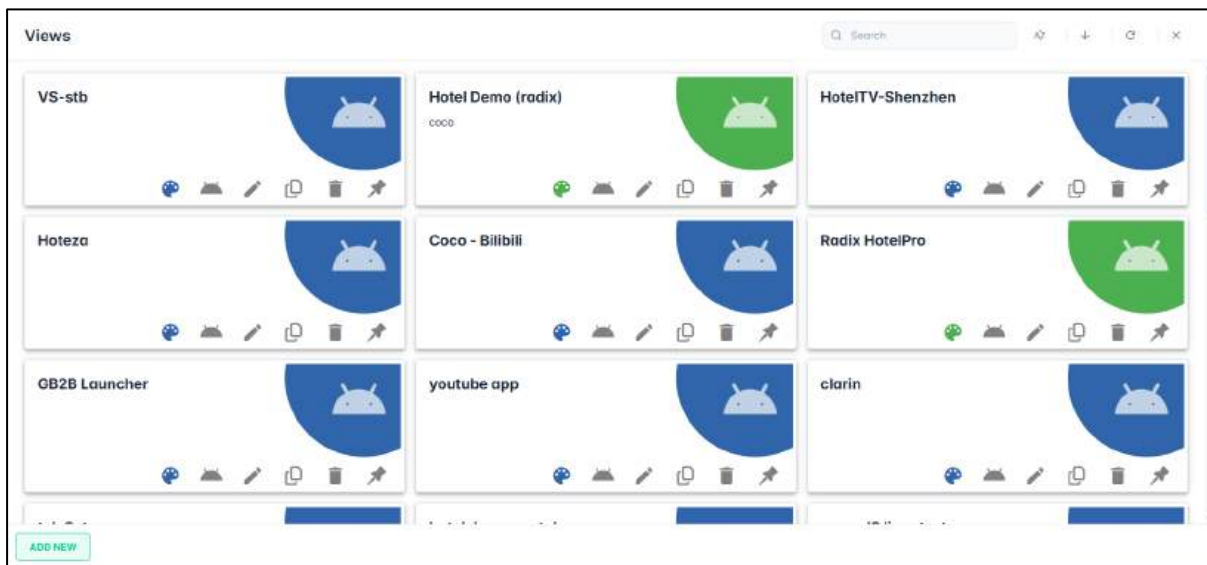
7.2.3 Kiosk Modes

This option allows you to use a device as a display in a kiosk, as in a storefront or hotel. See **Section 6.1.14, Kiosk**.

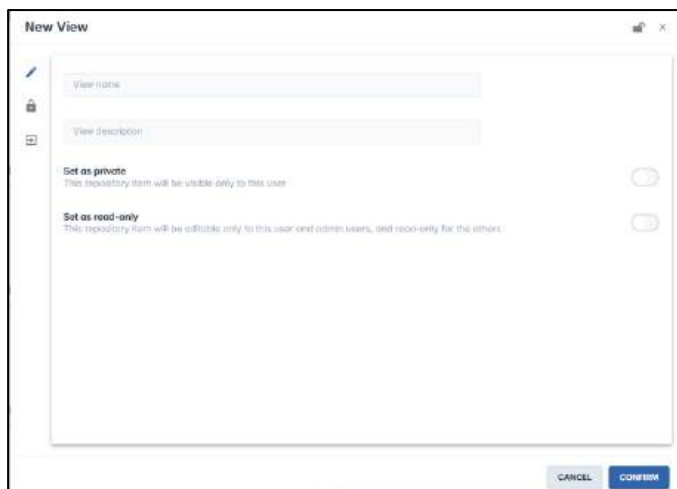


7.2.4 Views

As mentioned in **Section 6.1.35**, the **Views** repository option allows you to create a specialized Kiosk option where you choose allowed apps and access to a single URL on the remote device.



When you click on **Add New** in the lower left corner, the **New View** window opens up:



Proceed as in **Section 6.1.35** to create a new View item.

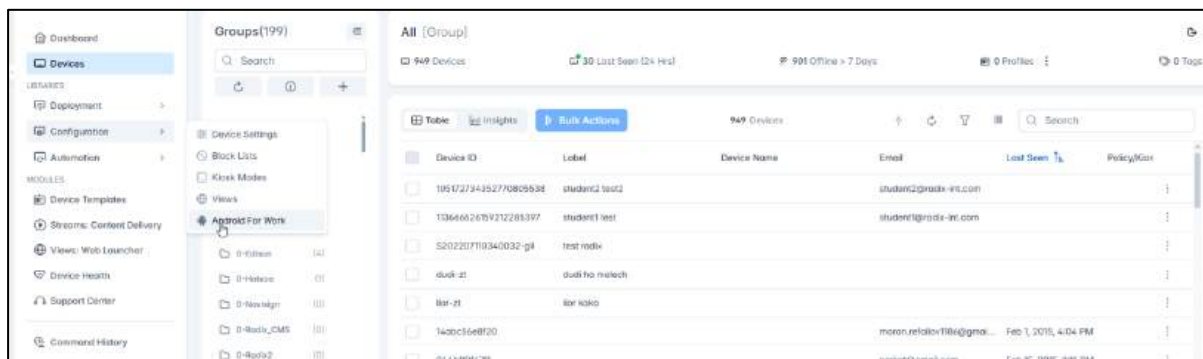
7.2.5 Android for Work

We mentioned previously in **Section 6.1.2**, that you can install Android apps on remote devices by means of the Radix Device Management Platform by means of the **AFW install** command. However, you must first create a list of the approved apps and software policies that you would like to apply to your Android devices in the AFW program. You can perform this by clicking on the **Android for Work** option in the Configuration drop-down list.

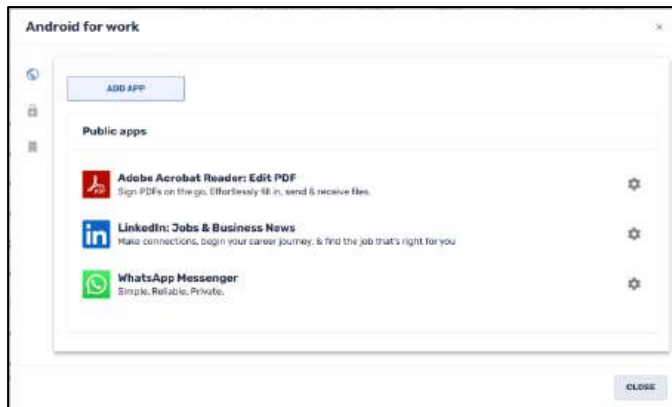
Note: You must first register in Android for Work using the Radix EMM account, using the Account Settings pane. See **Section 4.4.3, Android for Work Registration**.

To approve apps to be installed via the Android for Work feature:

1. Click on **Configuration>Android for Work** in the Devices Table's sidebar menu.



The **Android for Work** window opens.



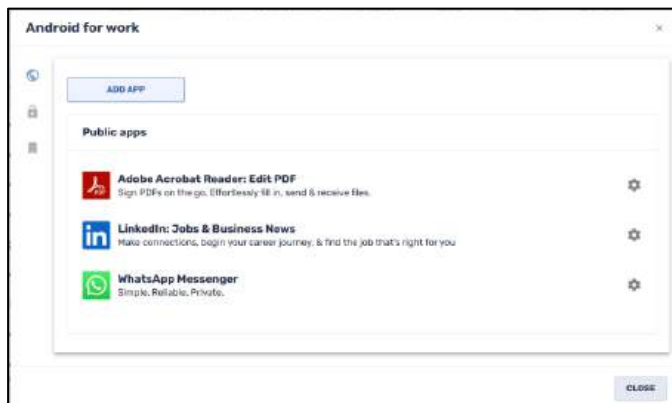
Note the following icons on the left side of the window:

Icon	Description
	Public apps: Allows you to add apps that are available to all devices in the Radix Device Management Platform
	Private apps: Allows you to add apps that are available to only specific devices in the Radix Device Management Platform
	Policy: Allows you to select a software policy for a device, blocking or allowing specific apps.

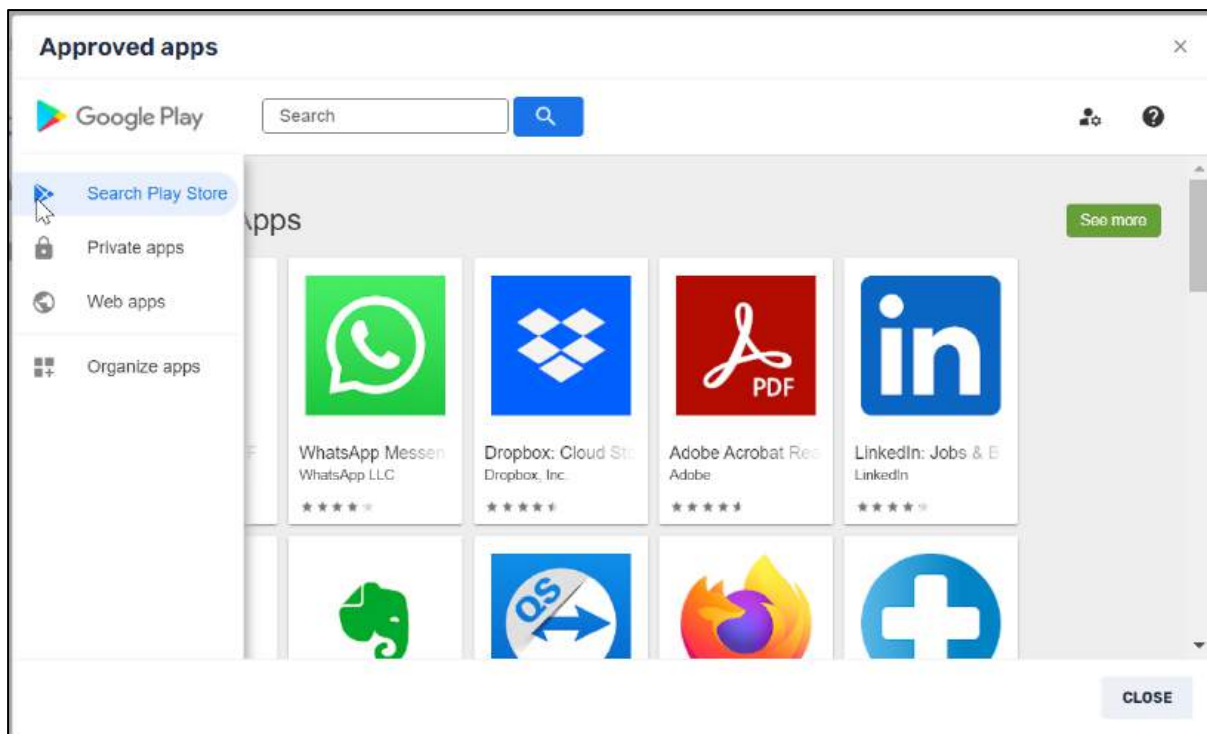
We will go through the functions of these icons in turn:

7.2.5.1 Public Apps

When you click on the Public Apps icon, the **Public Apps** window opens.

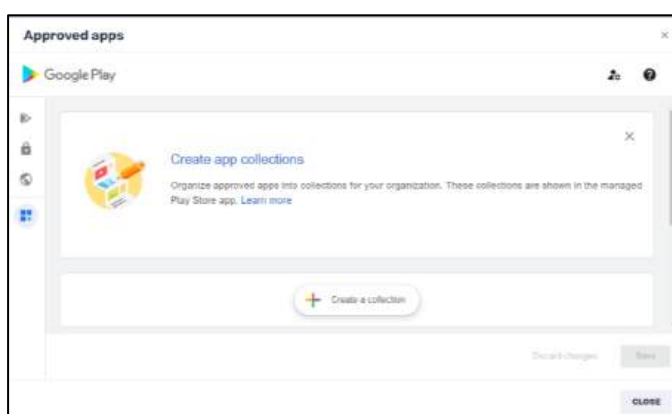


1. Click on the **Add App** button. A list of featured approved apps appears.



You have options of selecting apps from either:

- **Google Play Store**,
 - **Private apps** specifically for your organization that have been uploaded already, or
 - **Web Apps**, which are applications from elsewhere on the Web, other than the Google Play Store.
2. There is an additional option to organize your collection of apps, by clicking on the **Organize apps**  icon:



7.2.5.2 Private Apps

This option allows you to select from apps that have been approved for your organization to be installed on your fleet of devices.



7.2.5.3 Install Policy

This allows you to install a software policy on a device.



The process is identical to what is outlined in **Section 6.1.20, Play Siren**

This option sounds an alarm on the device. This may be handy in an emergency situation, or if the device has been stolen. You can instruct the device to sound off the alarm if it is taken outside of a specified geographical area.



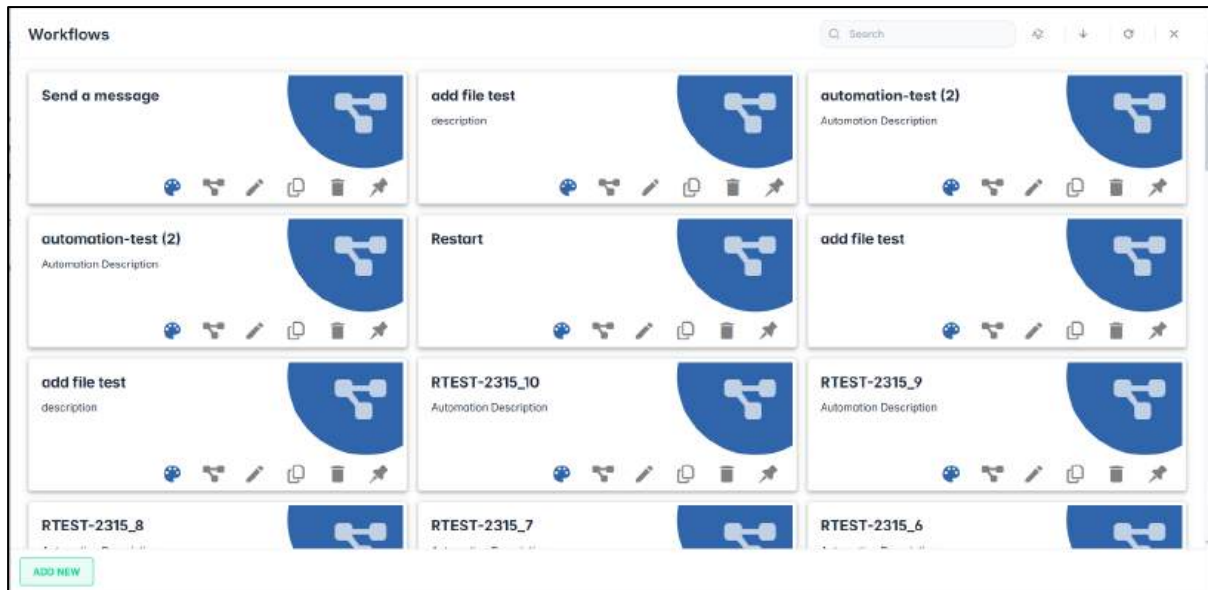
Policies.

After you have finished approving apps and a software policy to be employed in Android for Work, proceed from **Section 6.1.2** to actually install the approved apps using the **Android for Work Install** command.

7.3 Automation Options

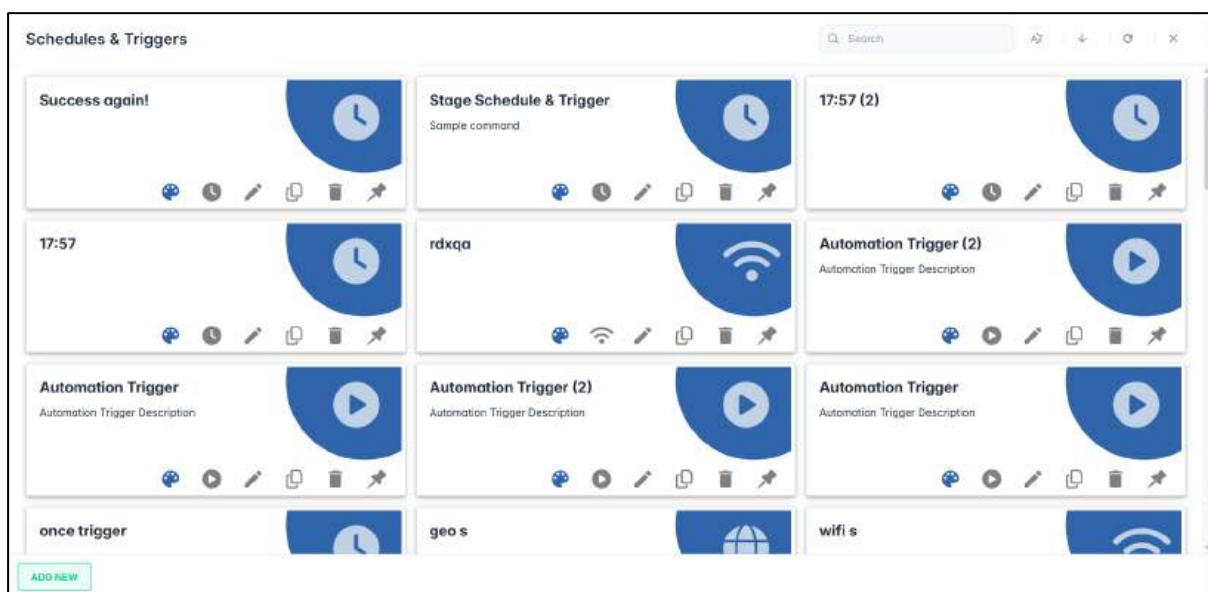
7.3.1 Workflows

This feature allows sending a series of commands to a device. The **Workflow** command allows you to arrange a series of commands in a particular order, save the arrangement, and deploy the workflow to a device or fleet of devices. There are also options to create a Favorites menu or move commands around within workflows. See **Section 6.1.39, Workflow**.



7.3.2 Schedules & Triggers

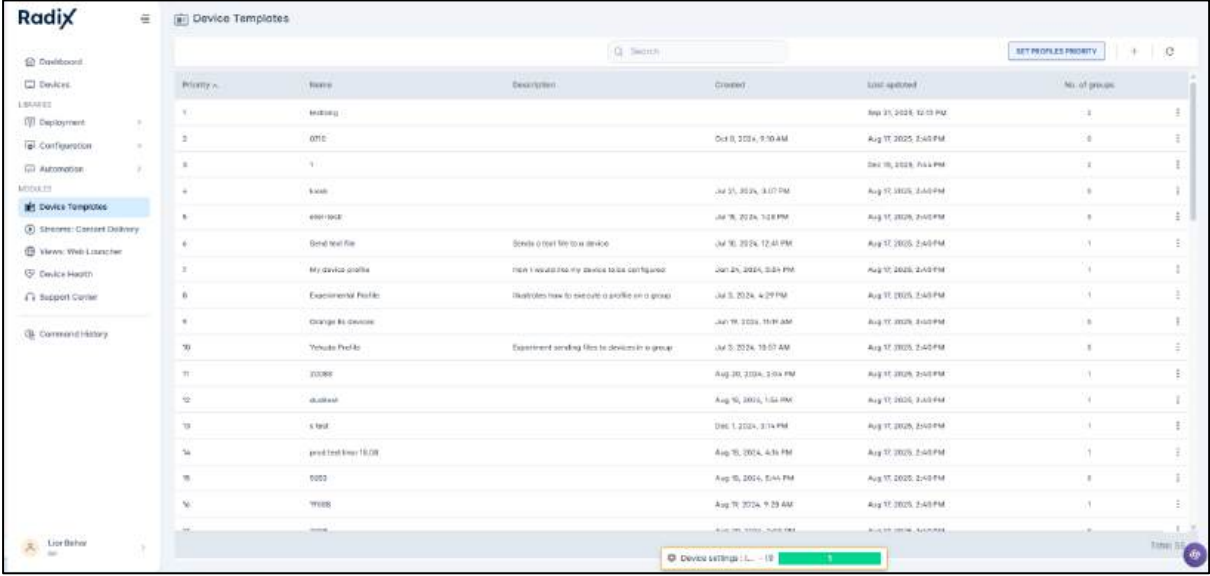
This allows you to create a trigger for a device (by timing, geofencing, Wi-Fi, or upon Startup) from within the Device Dashboard and lets you program the device's reaction to the trigger, by selecting a particular command to be executed. **See Section 6.1.26, Scheduler & Triggers Command.**



Chapter 8. Device Templates Console

The Device Templates Console allows you to create a template of several groups of devices. Once you have created a template, you can then select software packages and OTA updates to apply to groups of devices. You can also send files over to the devices in the template. Also, if you add additional groups to the template later, the specified software packages, OTA updates, and files will be automatically installed on these groups as well.

When you click on the Device Templates Console icon , you will see a list of existing templates in the Radix Device Management Platform.



Priority	Name	Description	Created	Last updated	No. of groups
1	testimg			Aug 31, 2025, 12:13 PM	2
2	OTC		Oct 8, 2024, 9:10 AM	Aug 17, 2025, 2:45 PM	0
3	1			Dec 10, 2025, 10:4 PM	2
4	1		Jul 31, 2024, 3:07 PM	Aug 17, 2025, 2:45 PM	0
5	testimg		Jul 16, 2024, 7:28 PM	Aug 17, 2025, 2:45 PM	0
6	Send test file	Sends a test file to a device	Jul 16, 2024, 12:41 PM	Aug 17, 2025, 2:45 PM	1
7	My device profile	My 1 device has my device to be configured	Jun 21, 2024, 5:34 PM	Aug 17, 2025, 2:45 PM	1
8	Experimental Profile	Illustrates how to create a profile on a group	Jul 3, 2024, 4:29 PM	Aug 17, 2025, 2:45 PM	1
9	Change file device		Jul 19, 2024, 11:39 AM	Aug 17, 2025, 2:45 PM	0
10	Yohuko Profile	Experiment sending files to devices in a group	Jul 3, 2024, 10:57 AM	Aug 17, 2025, 2:45 PM	0
11	20200		Aug 20, 2024, 2:04 PM	Aug 17, 2025, 2:45 PM	1
12	akulwal		Aug 16, 2024, 1:54 PM	Aug 17, 2025, 2:45 PM	1
13	s test		Dec 1, 2024, 3:14 PM	Aug 17, 2025, 2:45 PM	1
14	prod test line 18,08		Aug 16, 2024, 4:36 PM	Aug 17, 2025, 2:45 PM	1
15	0003		Aug 16, 2024, 5:44 PM	Aug 17, 2025, 2:45 PM	0
16	W1005		Aug 16, 2024, 9:29 AM	Aug 17, 2025, 2:45 PM	1
17	1000		Aug 16, 2024, 9:45 AM	Aug 17, 2025, 2:45 PM	0

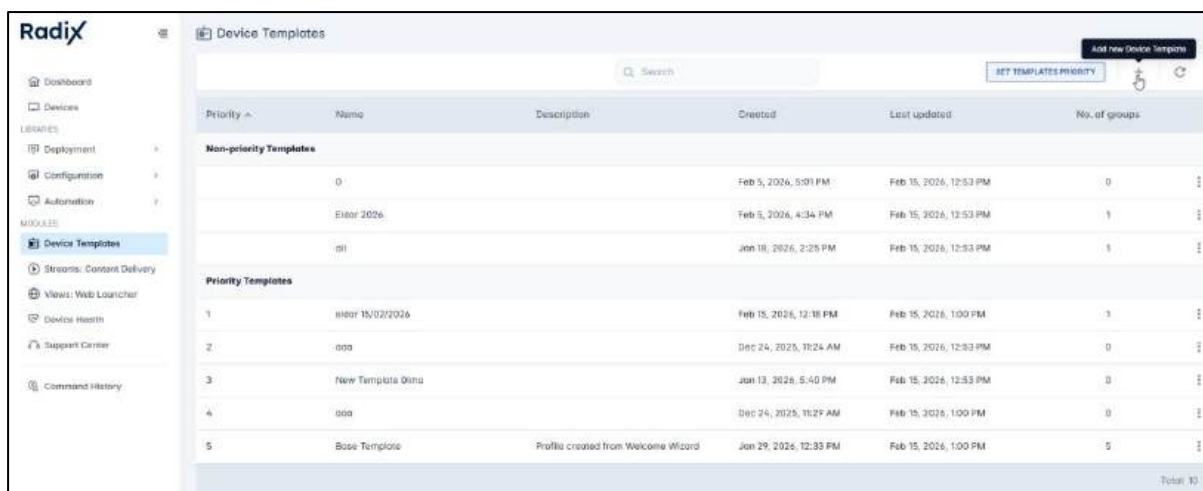
Figure 8-1: Device Templates Console, displaying all existing templates

8.1 Creating a New Template

If you have Administrator privileges, you can create a new user template.

To create a new template:

1. Click on the **Add New Device Template** icon  at the top of the Device Templates Console.

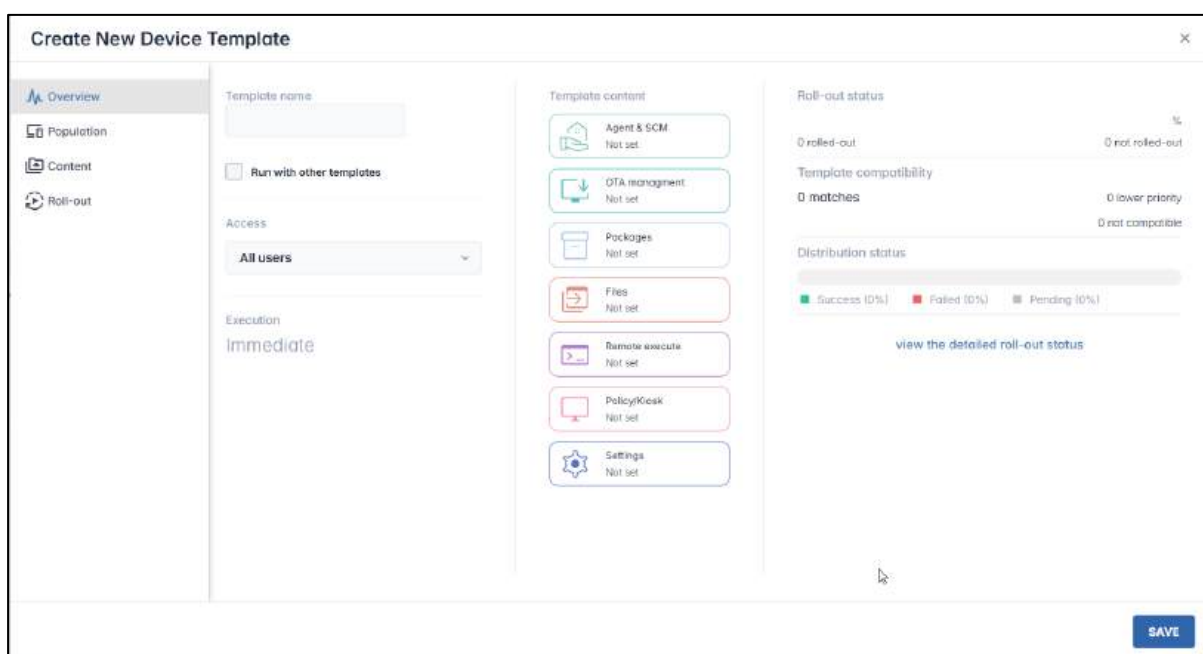


The screenshot shows the 'Device Templates' console with a sidebar on the left containing navigation links like Dashboard, Devices, Deployment, Configuration, Automation, and Device Templates. The main area displays a table of templates categorized into 'Non-priority Templates' and 'Priority Templates'.

Priority	Name	Description	Created	Last updated	No. of groups
Non-priority Templates					
	0		Feb 5, 2026, 5:01 PM	Feb 15, 2026, 12:53 PM	0
	Editor 2026		Feb 5, 2026, 4:34 PM	Feb 15, 2026, 12:53 PM	1
	all		Jan 18, 2026, 2:25 PM	Feb 15, 2026, 12:53 PM	1
Priority Templates					
1	Editor 15/02/2026		Feb 15, 2026, 12:18 PM	Feb 15, 2026, 1:00 PM	1
2	000		Dec 24, 2025, 10:24 AM	Feb 15, 2026, 12:53 PM	0
3	New Template Demo		Jan 13, 2026, 5:40 PM	Feb 15, 2026, 12:53 PM	0
4	000		Dec 24, 2025, 11:27 AM	Feb 15, 2026, 1:00 PM	0
5	Base Template	Profile created from Welcome Wizard	Jan 29, 2026, 12:33 PM	Feb 15, 2026, 1:00 PM	5
					Total: 10

Figure 8-2: Icon for Adding a New Device Template

The **Create New Device Template** window opens.



The 'Create New Device Template' window is divided into several sections:

- Overview:** Includes tabs for Population, Content, and Roll-out.
- Template name:** A text input field.
- Run with other templates:** A checkbox.
- Access:** A dropdown menu currently set to 'All users'.
- Execution:** A dropdown menu currently set to 'Immediate'.
- Template content:** A list of components with 'Not set' status:
 - Agent & SCM
 - OTA management
 - Packages
 - Files
 - Remote execute
 - Policy/Kiosk
 - Settings
- Roll-out status:**
 - 0 rolled-out (0% not rolled-out)
 - Template compatibility: 0 matches (0 lower priority, 0 not compatible)
 - Distribution status: Success (0%), Failed (0%), Pending (0%)
 - Link: view the detailed roll-out status
- SAVE:** A button at the bottom right.

- Supply a name for the template in the **Template Name** textbox.

- If you click the **Run with other templates** checkbox, this template will appear as a “non-priority template”. You will notice in the main Device Template Console that there are two categories of device templates:

Priority	Name	Description	Created	Last updated	No. of groups
Non-priority Templates					
	ondemand-new		Feb 27, 2025, 11:56 AM	Dec 24, 2025, 3:05 PM	1
Priority Templates					
1	Run 8 to 5		Jan 22, 2026, 11:33 AM	Jan 22, 2026, 11:59 AM	1
2	Jan 21st		Jan 21, 2026, 7:28 PM	Jan 22, 2026, 1:45 PM	0
3	0710		Oct 8, 2024, 9:10 AM	Jan 22, 2026, 11:34 AM	1
4	testpush		Dec 18, 2025, 10:32 AM	Jan 22, 2026, 11:34 AM	1
5	testlong			Jan 22, 2026, 11:34 AM	2
6	1			Jan 22, 2026, 11:34 AM	2
7	etel-profile_3		Dec 24, 2025, 3:05 PM	Jan 22, 2026, 11:34 AM	1
8	etel-profile_2		Dec 24, 2025, 3:04 PM	Jan 22, 2026, 11:34 AM	1
9	etel-profile_1		Dec 24, 2025, 3:03 PM	Jan 22, 2026, 11:34 AM	1

- Priority Templates** are applied to their associated group of devices according to their listed priority. If you assign two templates to a group, the template with the higher priority executes first. If you change the priority level later, then the higher priority template executes.
- Non-priority templates** are not limited by their priority number. Thus, they are always applied to their respective groups. Thus, when we check “Run with other templates”, our new template appears in this section of the Device Template Console:

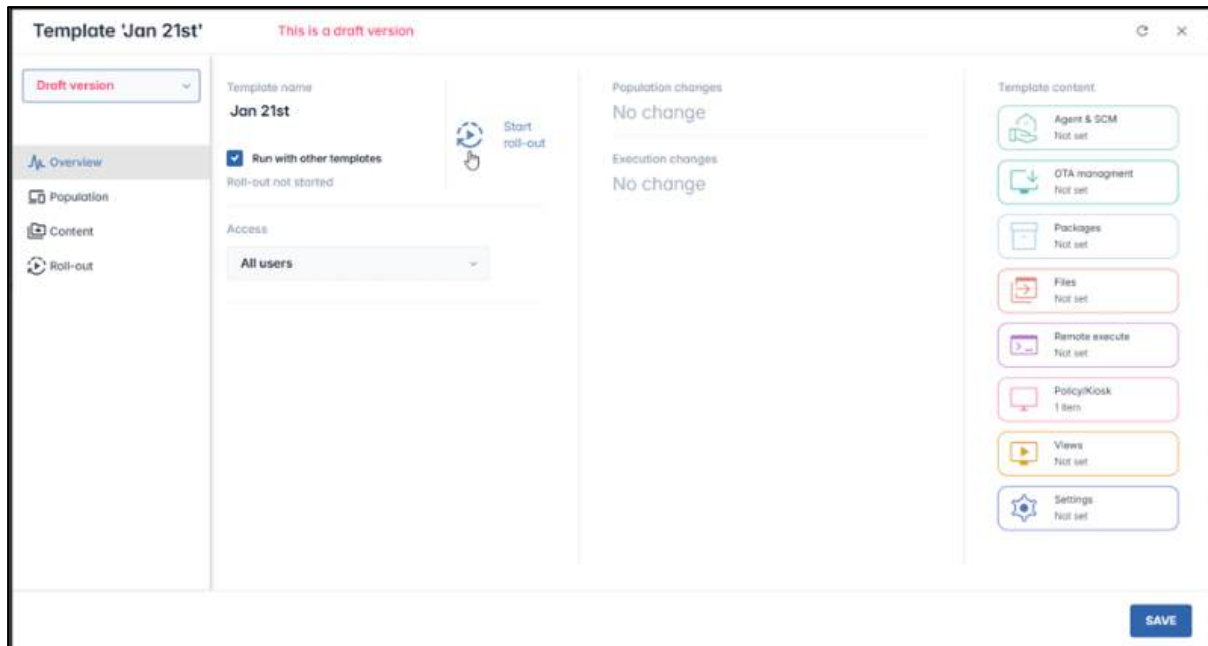


Figure 8-3: Template "Jan 21st" appears among the "non-priority templates"

The following table explains the icons on the left-hand side:

Table 8-1: Device Templates Console Icons

Icon	Description
 Overview	Overview: Allows you to provide a name for the template and specify which users can access the template
 Population	Population: Allows you to populate the template with groups, as well as apply filters
 Content	Content: This option has submenus that allow you to add the following content: • Agent & SCM: Apply a software installation package from the Radix Android Agent, or the SCManager for Android devices • OTA Management: Manage Over-the-Air (= OTA) updates • Packages: Install software packages • Files: Send files to devices in the template • Remote Execute: Apply a script to be executed remotely • Policy/Kiosk: Apply a software policy or a kiosk to the devices associated with the template • Views: This is for creating a content management system, a specialized type of Kiosk, consisting of allowed installed apps and/or a web app. • Settings: To modify device settings to the devices in the template
 Roll-out	Roll-out: Allows you to specify a time for applying the execution of the device template.

Here is a brief description of each of the icons in the sidebar menu:

8.1.1 Overview Panel

The first screen that you see is the **Overview** panel. Once you have finished creating the template, the Overview panel will display all the template's parameters at a glance. For example, the Overview panel of the following template displays:

- The template name,
- The groups and filters associated with the template,
- The content of the template, and
- When the template will be rolled out.

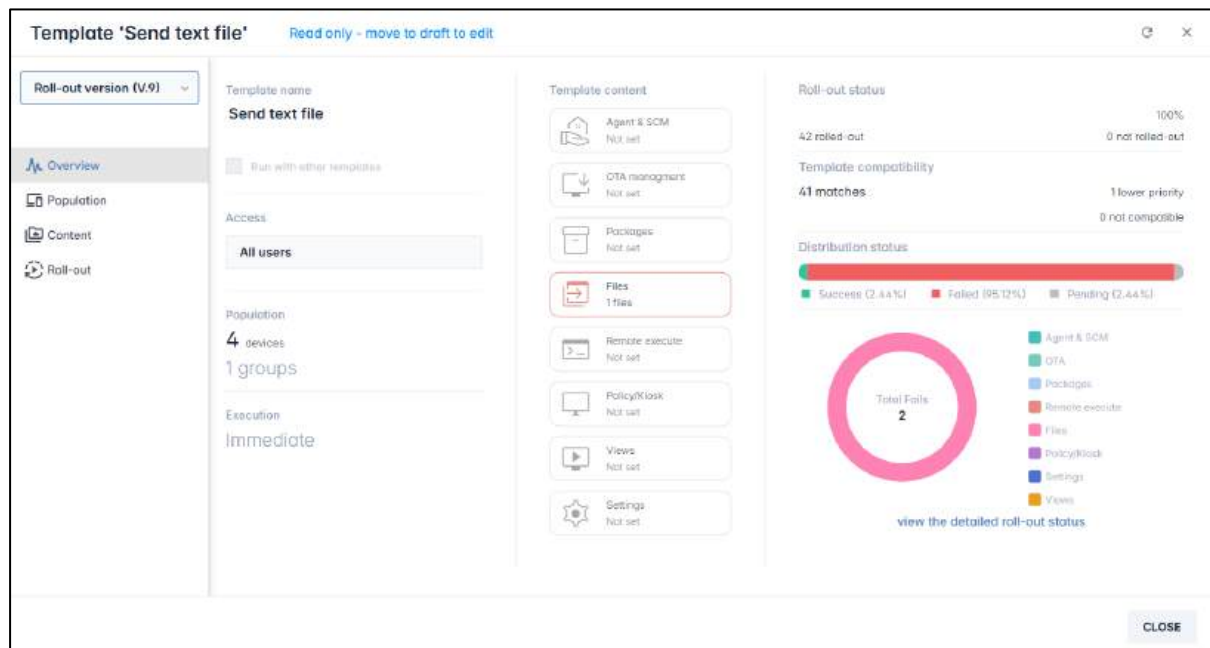
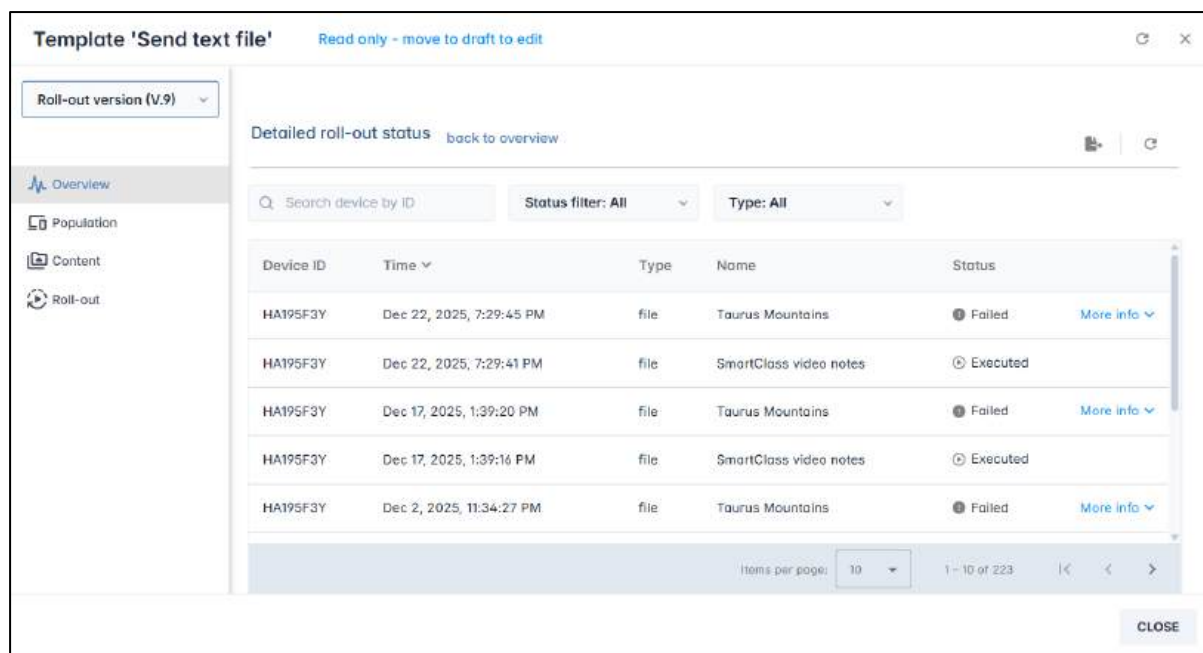
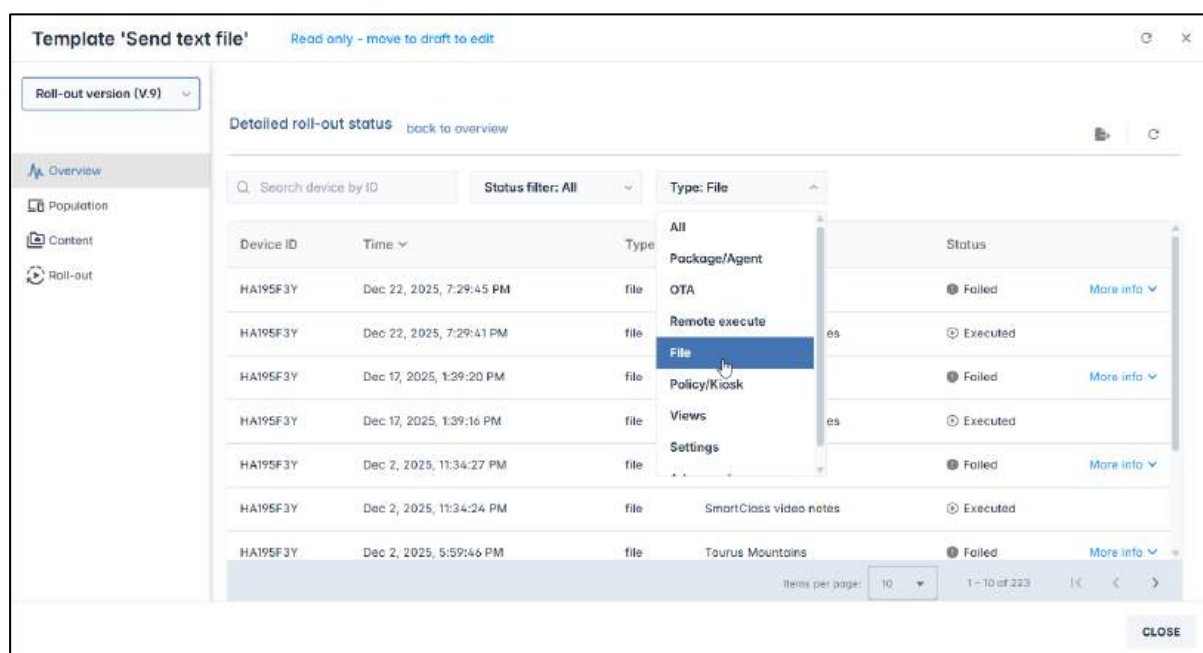


Figure 8-4: Overview Panel of an existing device template

1. If you click on **View the detailed roll-out status** in the Overview Panel, you will see details about the execution of this template:



This display also has options to filter results by whether the template was executed successfully or not, as well as which content item was executed:



- Clicking on **Back to Overview** will send you back to the Overview panel.

8.1.2 Population Panel

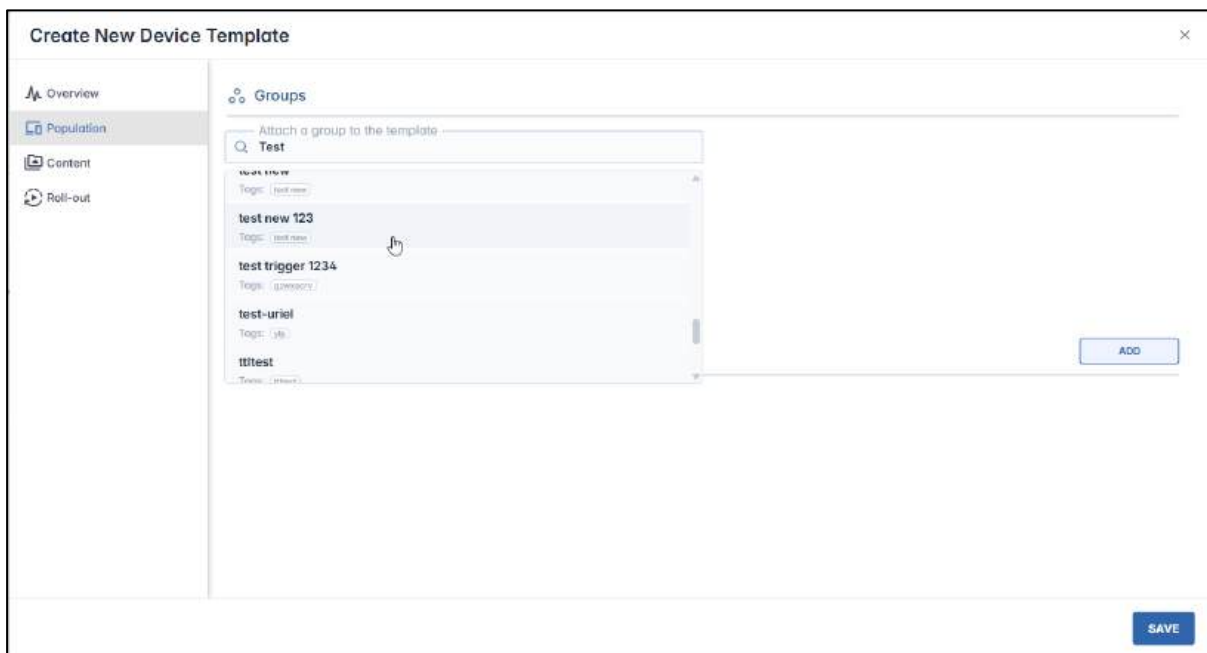
The Population panel allows you to associate groups of devices with the template. You can also narrow down the list of devices associated with the template by adding filters.

To populate the template with a group of devices:

- Click on the **Population** tab. The following screen opens:



2. In the Groups search bar, enter the name of a group of devices that you would like to associate with the template.



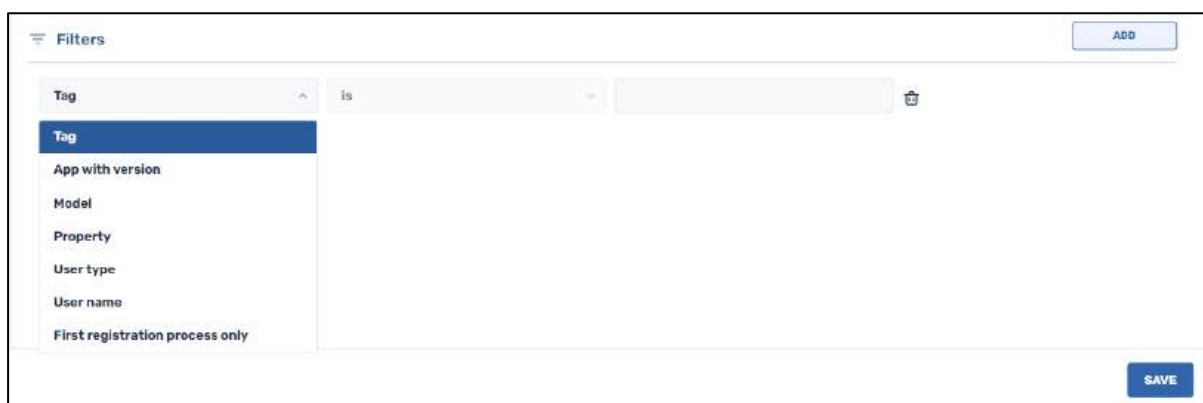
Note: The search is **not** case sensitive. Thus, the search string “Test” will also yield groups containing the string “test”.

3. When you have added a group, you will notice two icons next to the listing of the group:



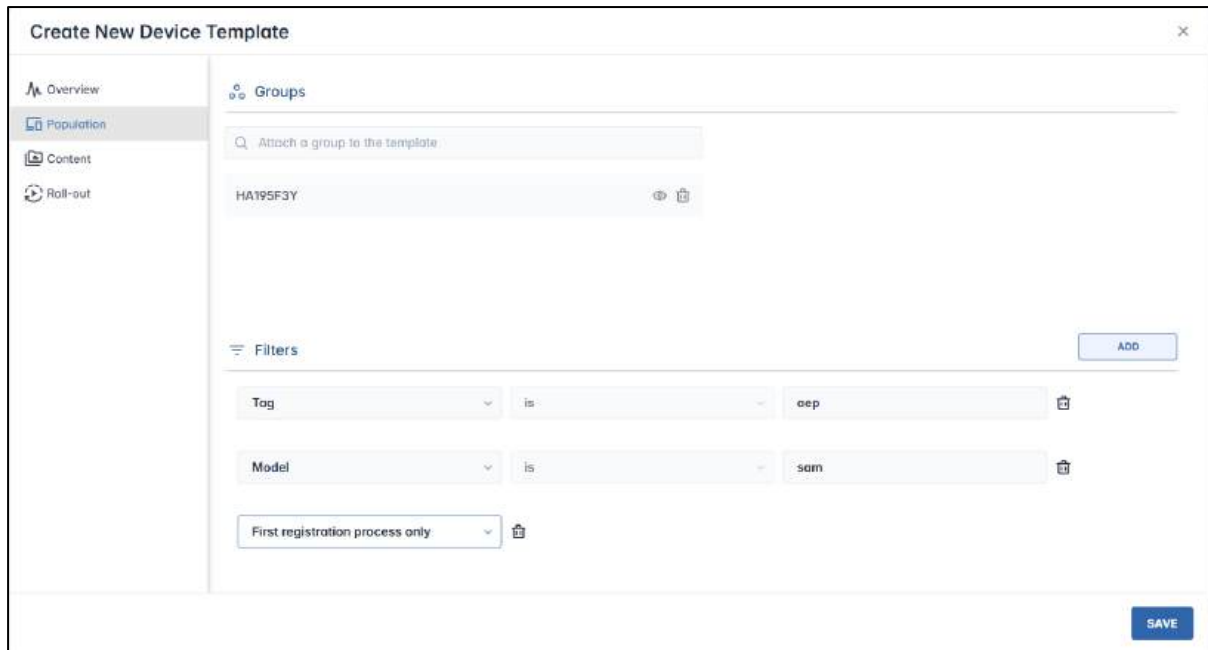


- **View details:** This will display the number of tags associated with this group.
 - **Remove:** This will remove the group from the device template.
4. If you wish to filter the devices to which the template will be applied, click on the **Add** button to further refine which devices will be included in the template.



The filter options include:

- **Tag:** To filter devices by the tags that they have been assigned.
 - **App with version:** To filter devices by which version they have of a specific application. You then provide the name of the application and the version number.
 - **Model:** This allows you to select a specific model of a device to apply the template.
 - **Property:** This allows you to apply a template to devices with a specific property.
 - **User type:** This allows you to filter out the devices by user type. The options include **owner**, **user**, or **guest**.
 - **User name:** This allows you to filter out the devices in the group by user name.
 - **First registration process only:** This applies the template to devices only at the time of their first registration in the Radix Device Management Platform.
5. You can combine and save several search conditions, to refine the selection of devices in the template.



8.1.3 Content Panel

When you click on the Content tab, you will have eight submenus to specify what content to apply to the devices in the template you have created:

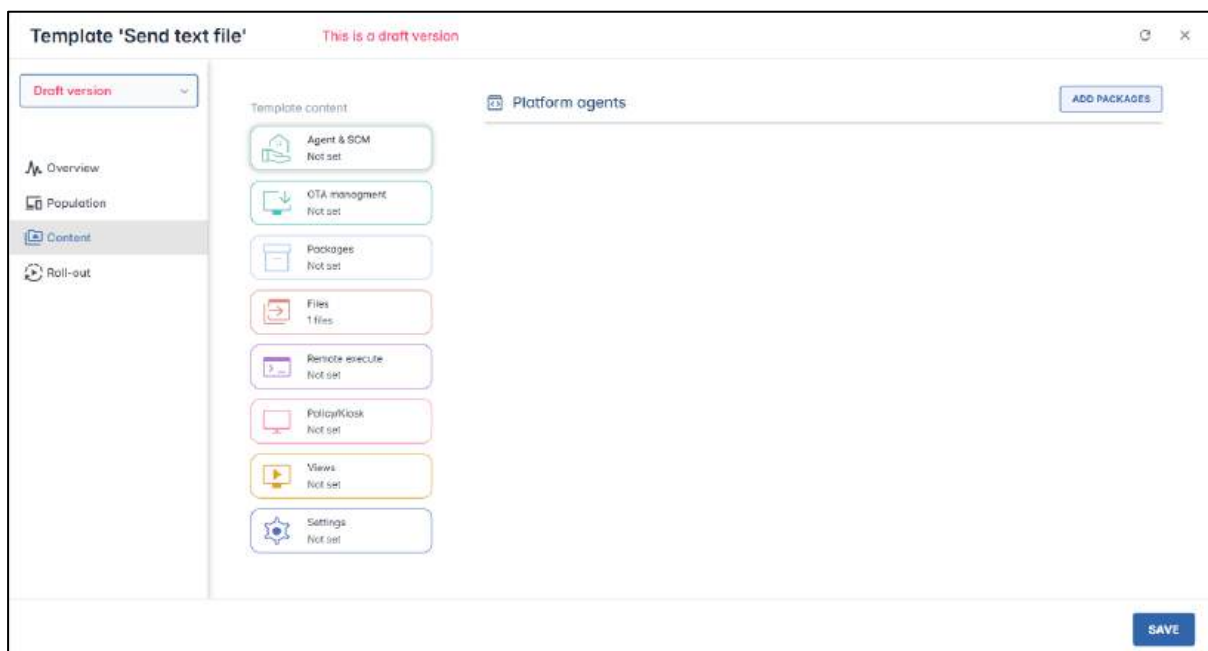


Figure 8-5: Device Template Content window, displaying the types of content that can be added

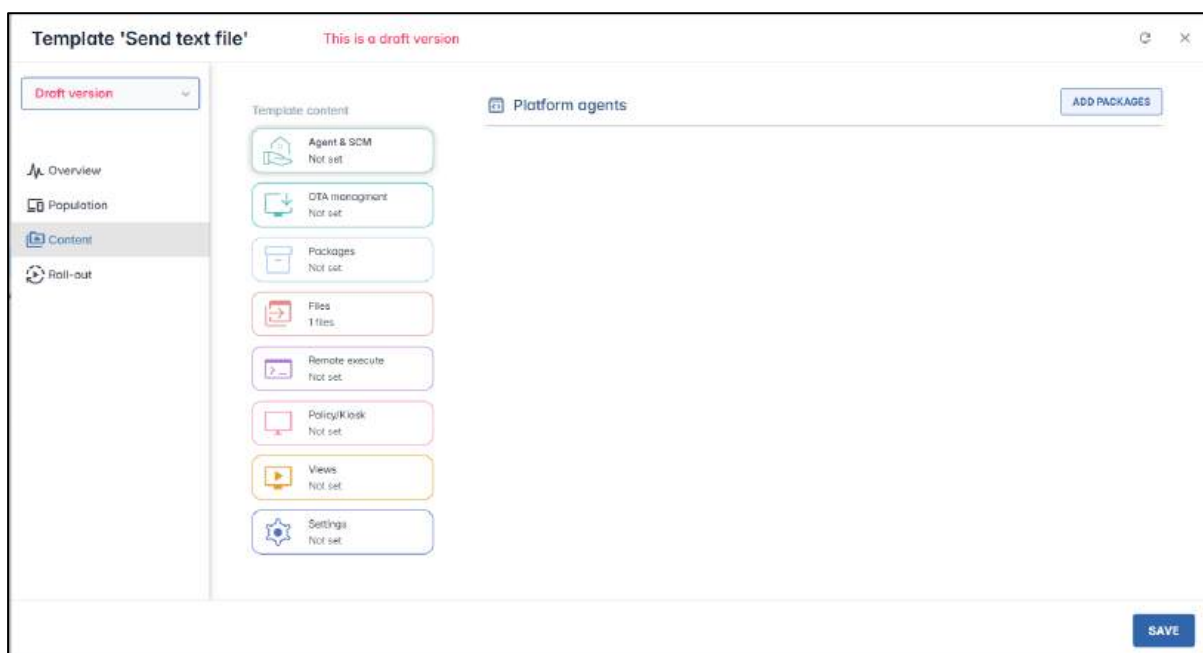
- **Agent & SCManager:** These include Radix installation files and SCManager files to be applied to Android devices.
- **OTA updates** to deploy Over-the-Air updates to the devices in a template
- **Software packages** to be installed
- **Files** to be sent to the devices in the template
- **Remote Execute** scripts to be executed
- **Policy/Kiosk** items to be assigned to the devices in a template

- **Views**, a specialized type of kiosk setting, consisting of selected apps and a single website
- **Settings**, to modify device settings to the devices in the template

We will examine these content options in turn.

8.1.3.1 Agent & SCManager

This allows you to attach software packages from the Radix agent and the SCManager to Android devices to which you apply the template.



1. When you click on **Add Packages**, you will receive a repository of Radix installation files and SCManager packages to install on Android devices:

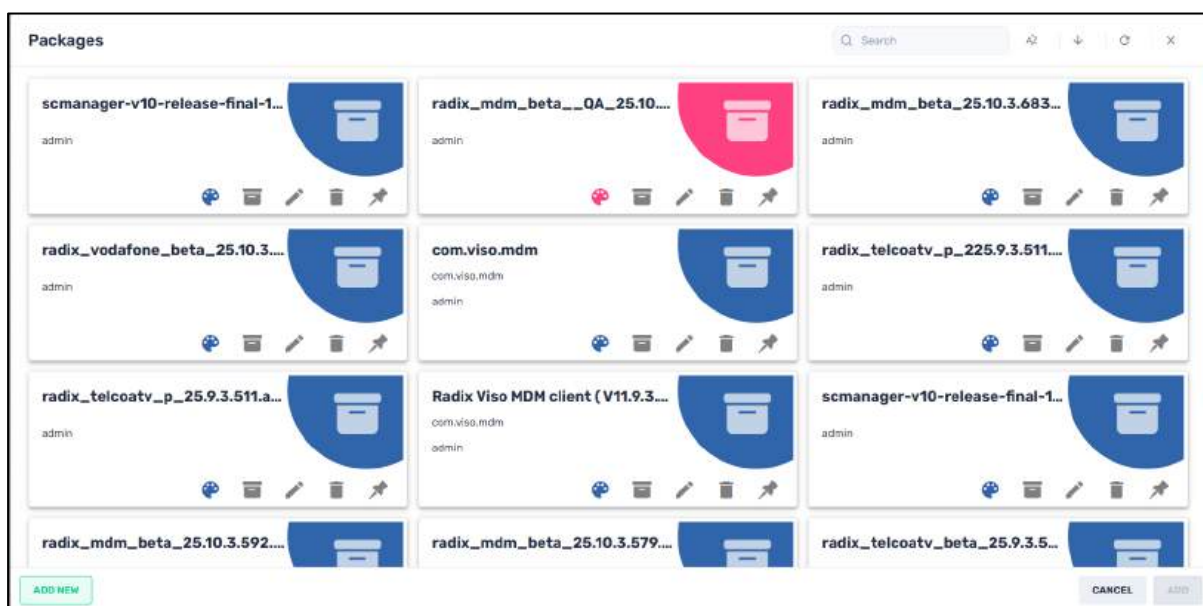


Figure 8-6: Repository of Radix installation files and SCManager packages

- You can click on several packages in order to select them. Clicking **Add** in the lower right will add them to the new template.

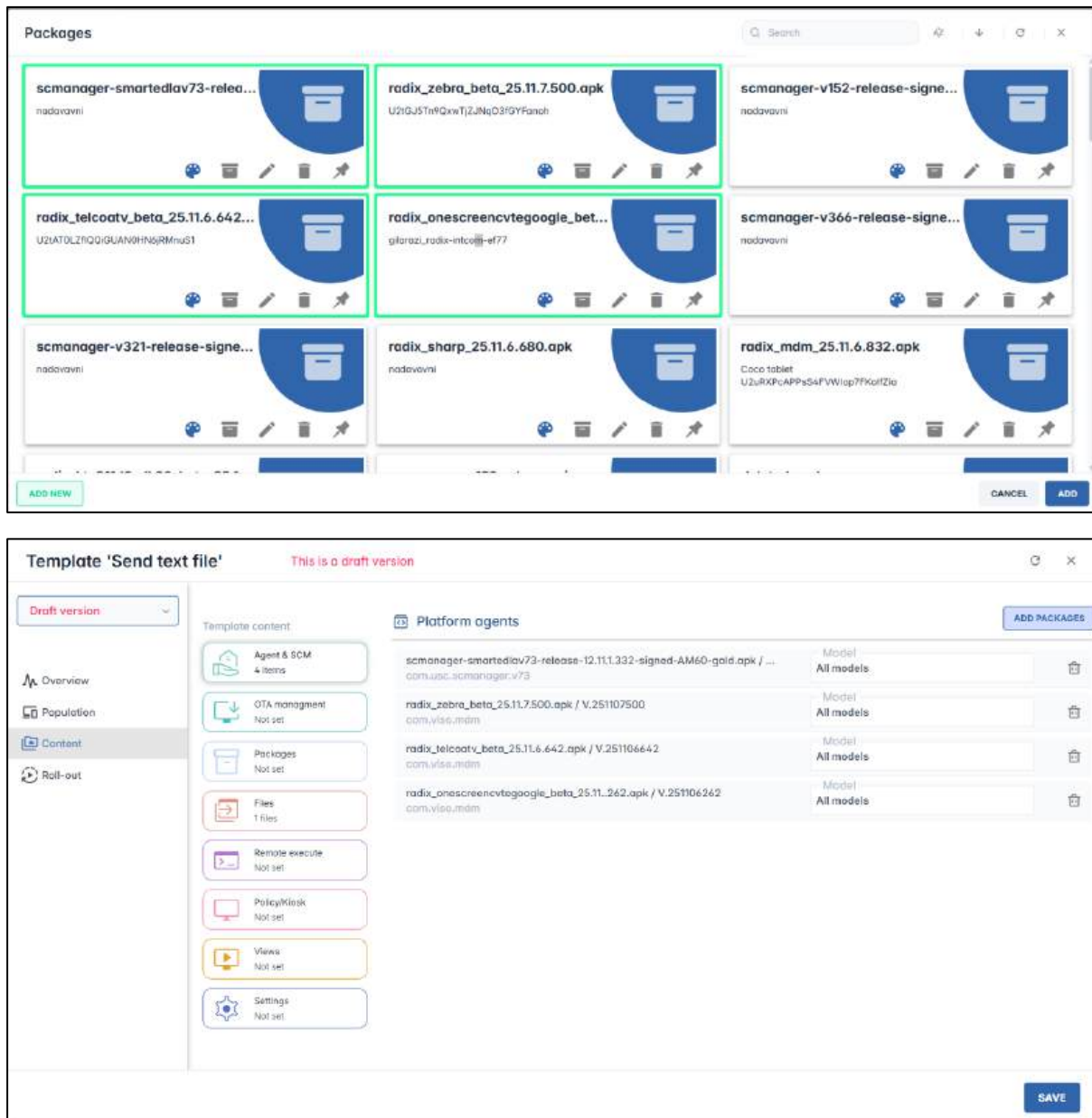
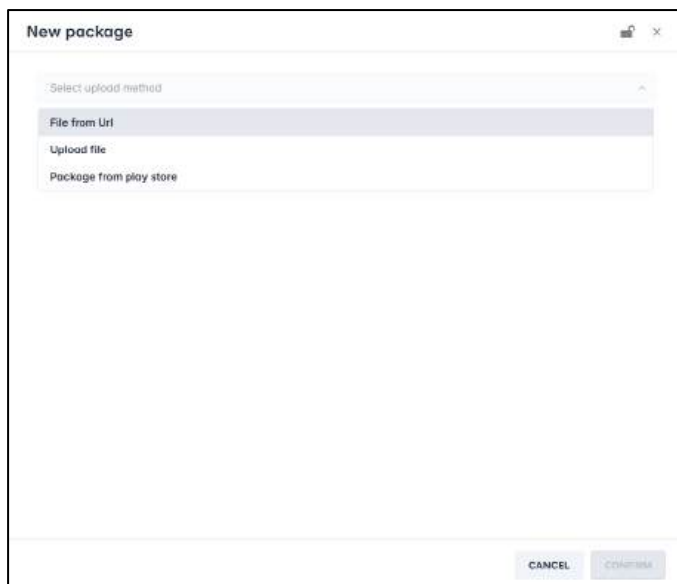


Figure 8-7: Four Radix packages were selected and added to the template

- If you wish to add a new installation package that doesn't appear in the repository, click on **Add New** in the lower left corner. The following window opens:



4. You can proceed with adding a new Radix package as explained above in **Section 6.1.13, Install App/Install Package**.

8.1.3.2 OTA Management

This option allows you to deploy Over-the-Air updates to the devices in a template. When you click on the **OTA management** tab, the following window opens:

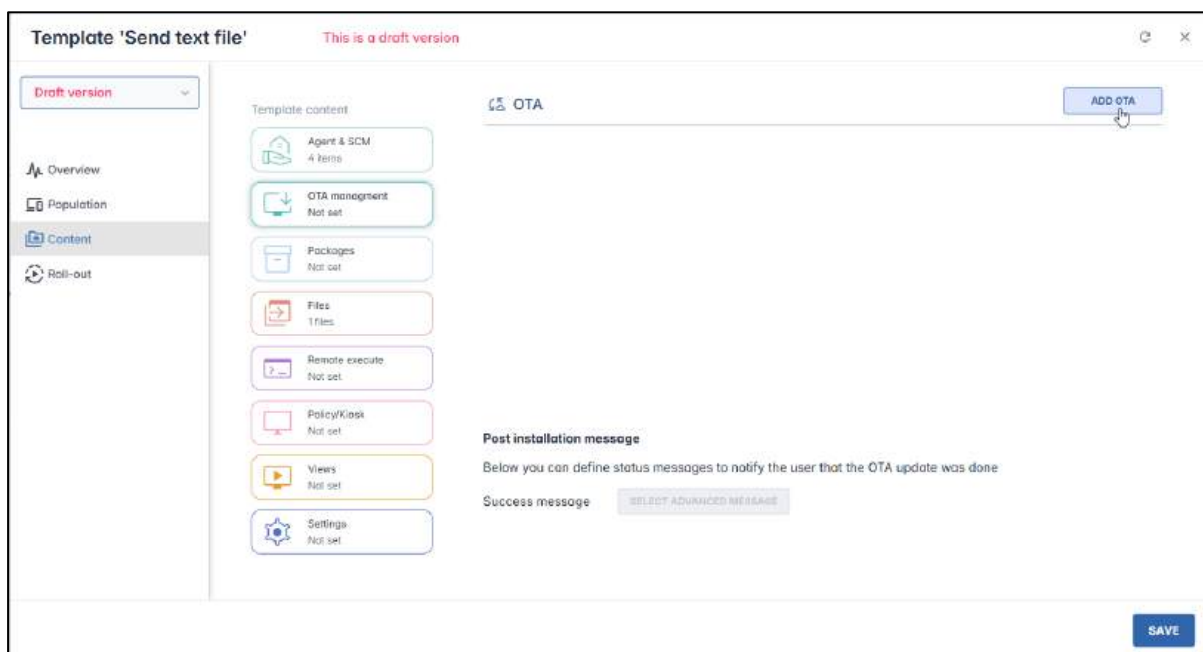


Figure 8-8: Option to apply an OTA update to specific device models

8.1.3.2.1 Adding an Existing OTA Update Package

To add an OTA update to devices in the template:

1. Click on **Add OTA** in the upper right-hand corner. The **OTA Update Engine** window opens.



Figure 8-9: OTA window, displaying all OTA update packages

2. Click on one or several existing OTA update packages to select them to be added to the device template.
3. The **Add** button in the lower right corner becomes active.

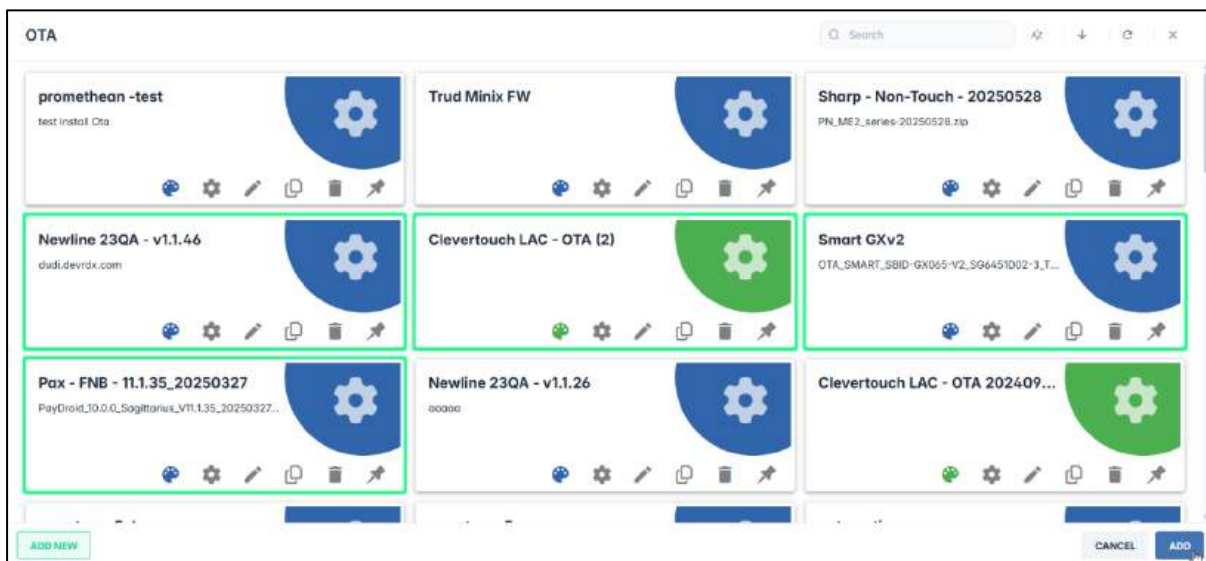


Figure 8-10: Four OTA update packages have been selected

4. Click on **Add**. The OTA update packages will appear in the template.

Template 'Send text file' This is a draft version

Draft version

- Overview
- Population
- Content**
- Roll-out

Template content

- Agent & SCM
4 items
- OTA management
4 OTAs
- Packages
Not set
- Files
1 file
- Networks
Not set
- Policy/Usage
Not set
- Views
Not set
- Settings
Not set

OTA

OTA	Model	Action
Smart GKv2 / V.20250420163914 OTA_Smart_GKv2-V2_504451002-3_T982_B1_H_5_release_smart_Android81...	All models	
Newline Z3GA - v11.46 / V11.46 dual_devices.com	All models	
Pax - FNB - T11.35.20250327 / V.20250327 PeyDroid_10.0.0_Supervisor_V11.35_20250327.OTA.zip	All models	
Clevertouch LAC - OTA (2) / V.20240406020631	All models	

Post installation message

Below you can define status messages to notify the user that the OTA update was done

Success message: SELECT ADVANCED MESSAGE

SAVE

- Click on **Select Advanced Message** to add an Advanced Message to notify the remote user that the OTA update was performed successfully.,

Template 'Send text file' This is a draft version

Draft version

- Overview
- Population
- Content**
- Roll-out

Template content

- Agent & SCM
4 items
- OTA management
4 OTAs
- Packages
Not set
- Files
1 file
- Networks
Not set
- Policy/Usage
Not set
- Views
Not set
- Settings
Not set

OTA

OTA	Model	Action
Smart GKv2 / V.20250420163914 OTA_Smart_GKv2-V2_504451002-3_T982_B1_H_5_release_smart_Android81...	All models	
Newline Z3GA - v11.46 / V11.46 dual_devices.com	All models	
Pax - FNB - T11.35.20250327 / V.20250327 PeyDroid_10.0.0_Supervisor_V11.35_20250327.OTA.zip	All models	
Clevertouch LAC - OTA (2) / V.20240406020631	All models	

Post installation message

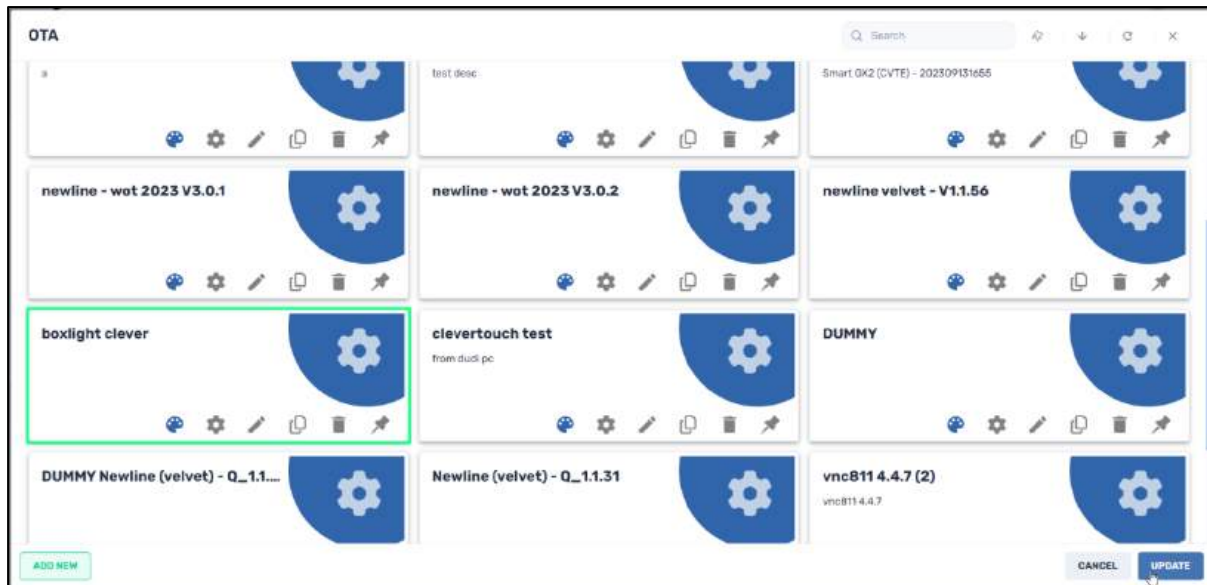
Below you can define status messages to notify the user that the OTA update was done

Success message: SELECT ADVANCED MESSAGE

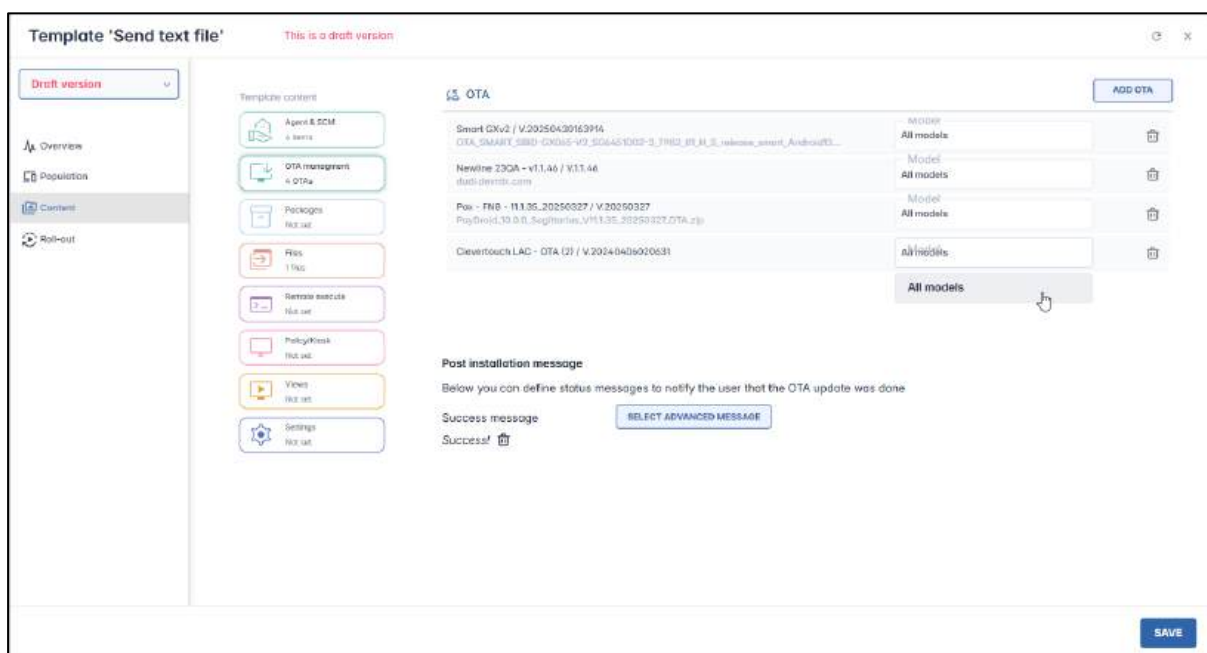
Success!

SAVE

- By repeating the process of adding OTA updates, you can later append several OTA updates to a single device template. The button will appear as **“Update”** instead of **“Add”**, if you are modifying an existing template.



- Note that there is a **Model** parameter, which allows you to specify that an OTA update is for a **specific model** of a device, or **all** models:



- Click **Save** to save the addition of the OTA updates to the template.

8.1.3.2.2 Creating a New OTA Update

The Device Template Console also allows you to create a **new** OTA firmware or software update.

To create a new OTA update engine:

- Click on **Add New** in the lower left-hand corner of the OTA window. The **New OTA Update Engine** window opens.

New OTA Update engine

Name

Description

Select upload method
Upload file

ADD FILE

Version

Model
All models

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

Hide content from others
Other users can apply this repository but cannot use or open its content

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

CANCEL CONFIRM

2. Supply the necessary parameters for an OTA update. You can either upload a file from your computer or download a file by supplying its URL. These are the fields that you must complete when creating an OTA update from a URL:

New OTA Update engine

Name

Description

Select upload method
File from Url

Payload url

Payload size

Version

Offset

Headers

header

header

CANCEL CONFIRM

3. Click on the **Set as private** button if you wish to make the OTA update visible only to you (as the creator of the item) when using the Radix Device Management Platform.
4. Click on the **Hide content from others** button if you wish to allow other Radix Device Management Platform users to use this item, without allowing them to edit its details.
5. Click on the **Set as read-only** button if you would like to limit who will be able to edit this OTA update. Anyone with **Administrator** privileges can edit it, while

someone with only **User** privileges can only access it and use it but cannot edit it. When you click on **Set as read-only**, you will see the lock icon at the top of the screen turn to a “locked” position.

Figure 8-11: Lock icon indicates that the OTA update has been set to read-only

6. Click **Confirm**.

The newly added OTA update will now appear in the list of Template Groups above.

7. If you wish to remove the OTA update from the template, click on the **Remove** icon to have it removed.

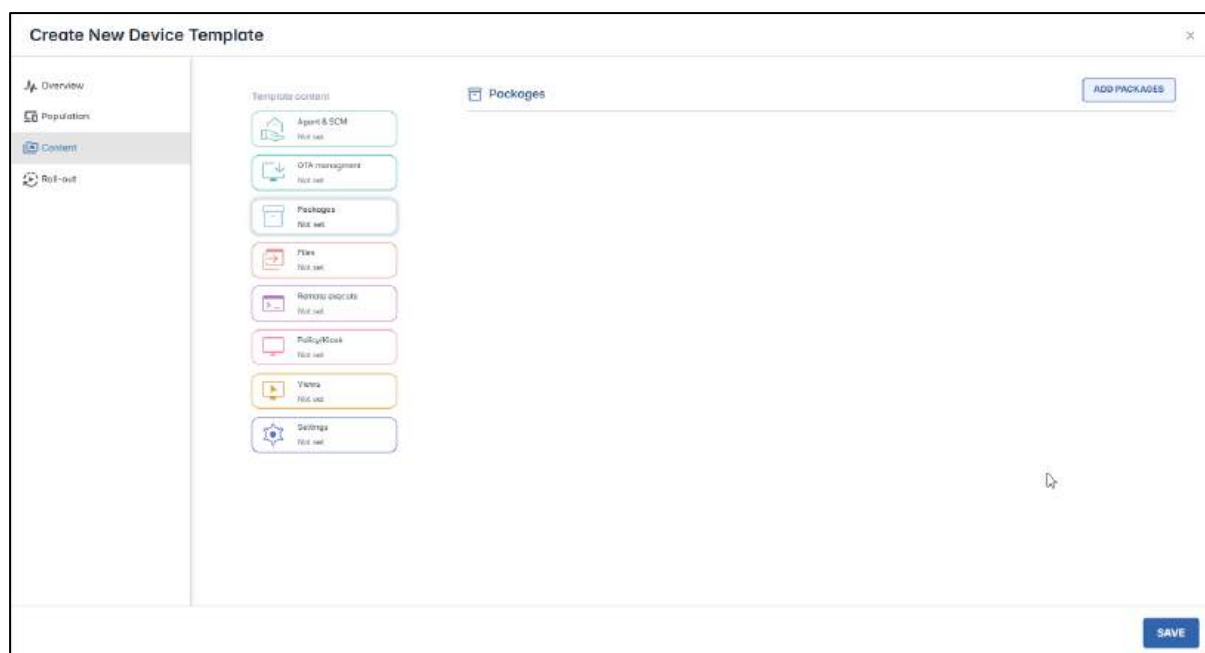
- Click **Save** to save the OTA update option for your template.

8.1.3.3 Packages

This provides you with a list of software packages that you can apply to the devices in the template. If a group is assigned to this template in the future, the software packages will also apply to that group.

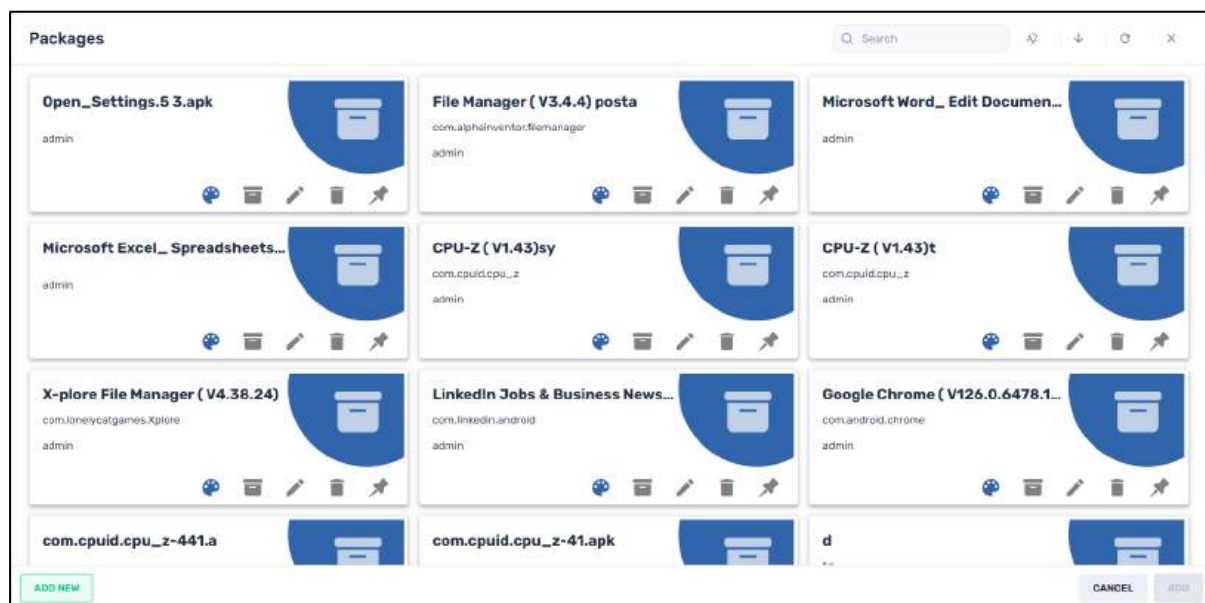
8.1.3.3.1 Adding an existing software package

When you click on the Packages tab, the following window opens:



To add a software package to the template of devices:

- Click on **Add Packages**. The **Packages** repository opens.



- Select one or several software packages to be added to the template by clicking on the tiles. The **Add** button in the lower right corner becomes active.

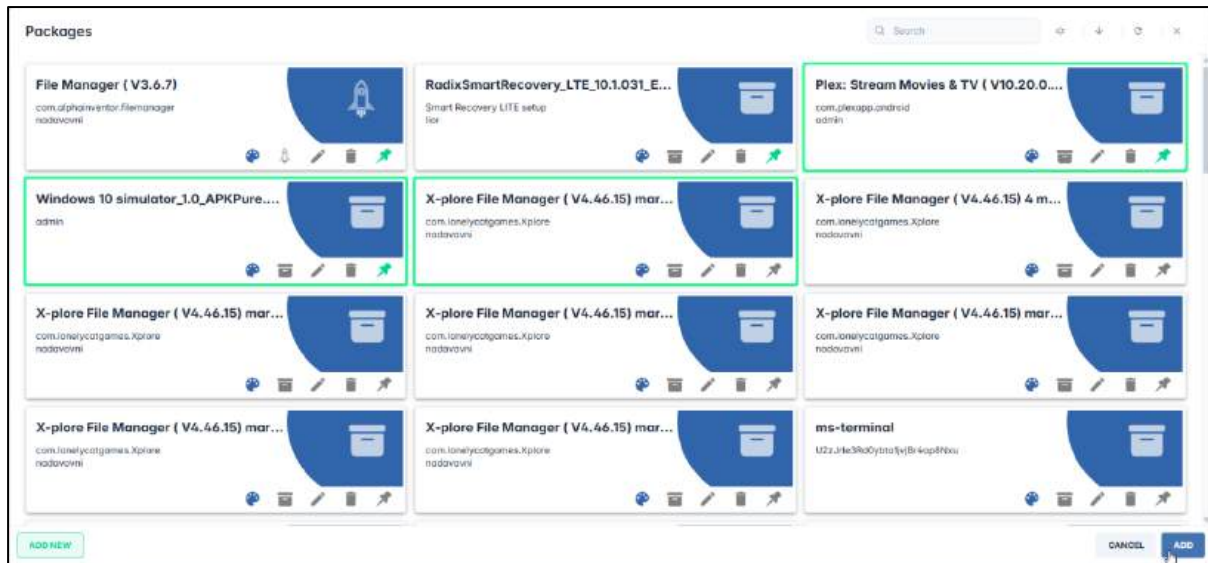
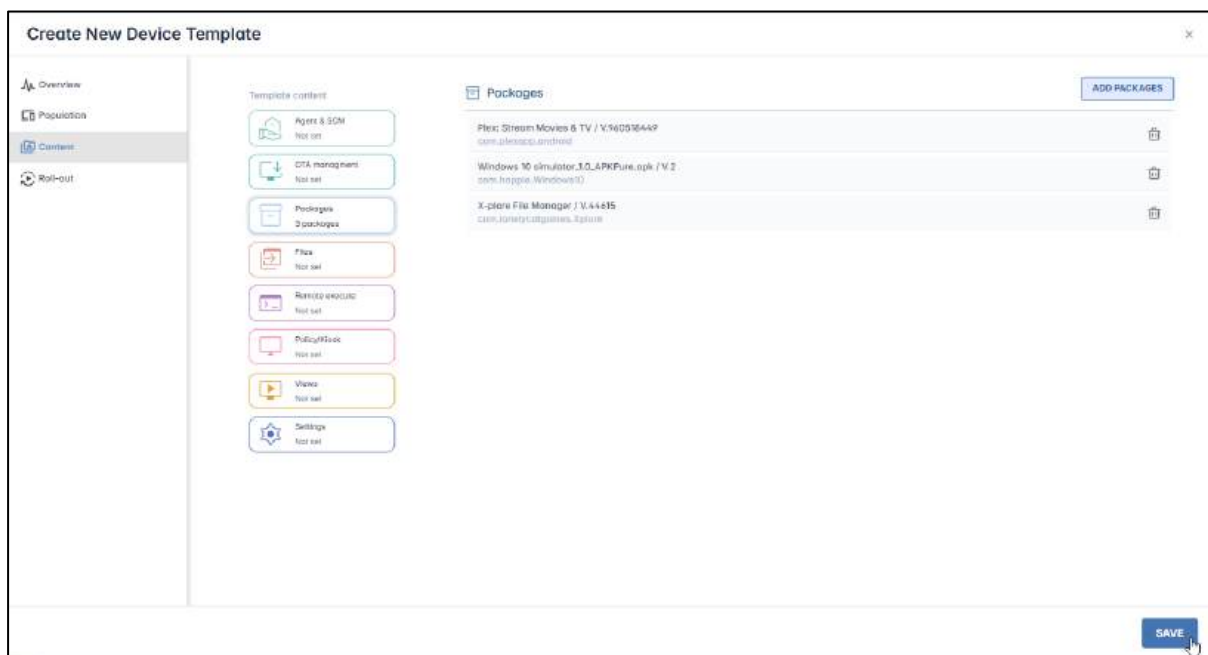


Figure 8-12: Selecting the Windows 10 simulator, X-plore, and Plex software packages to be applied to devices in the template

3. Click **Add**. The software package(s) you selected will now appear in the template.



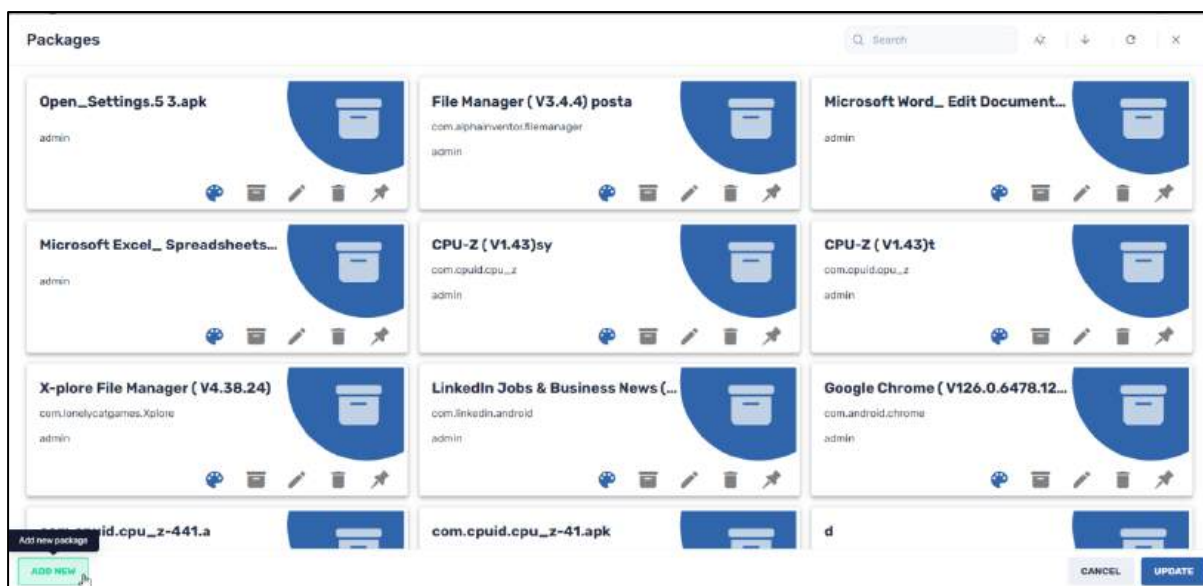
4. Click **Save** to store your selection in the device template.

8.1.3.3.2 Adding a new software package

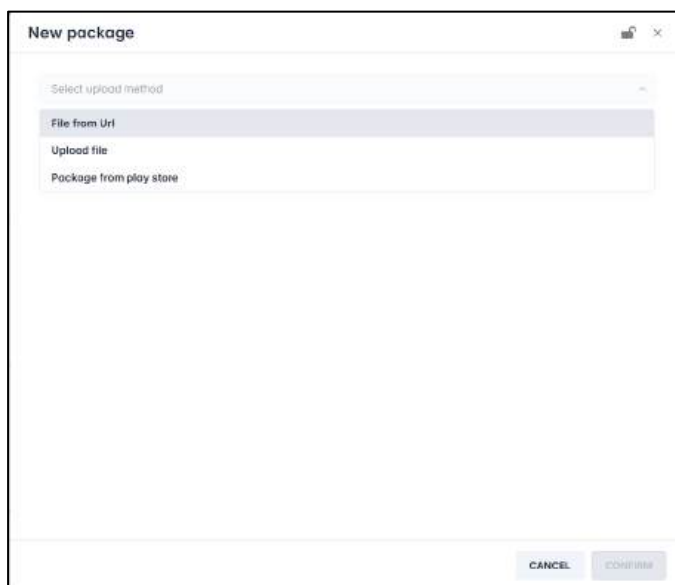
There is also an option to add a software package that does not appear yet in the Packages repository.

To add a new software package to the repository:

1. In the Packages screen, click **Add New**.



The **New Package** window opens.



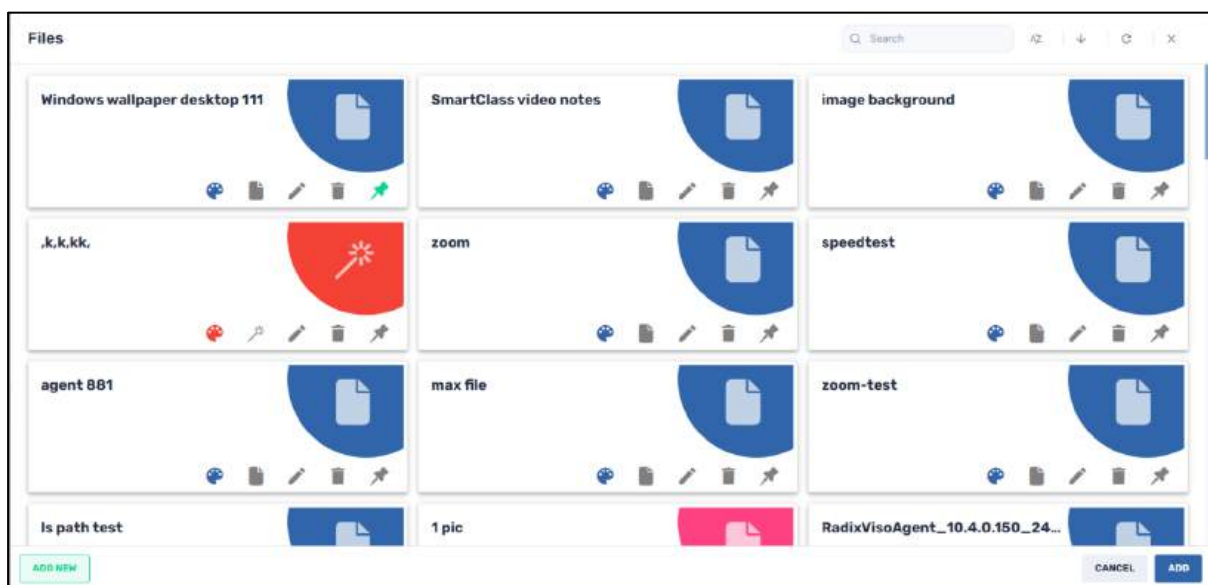
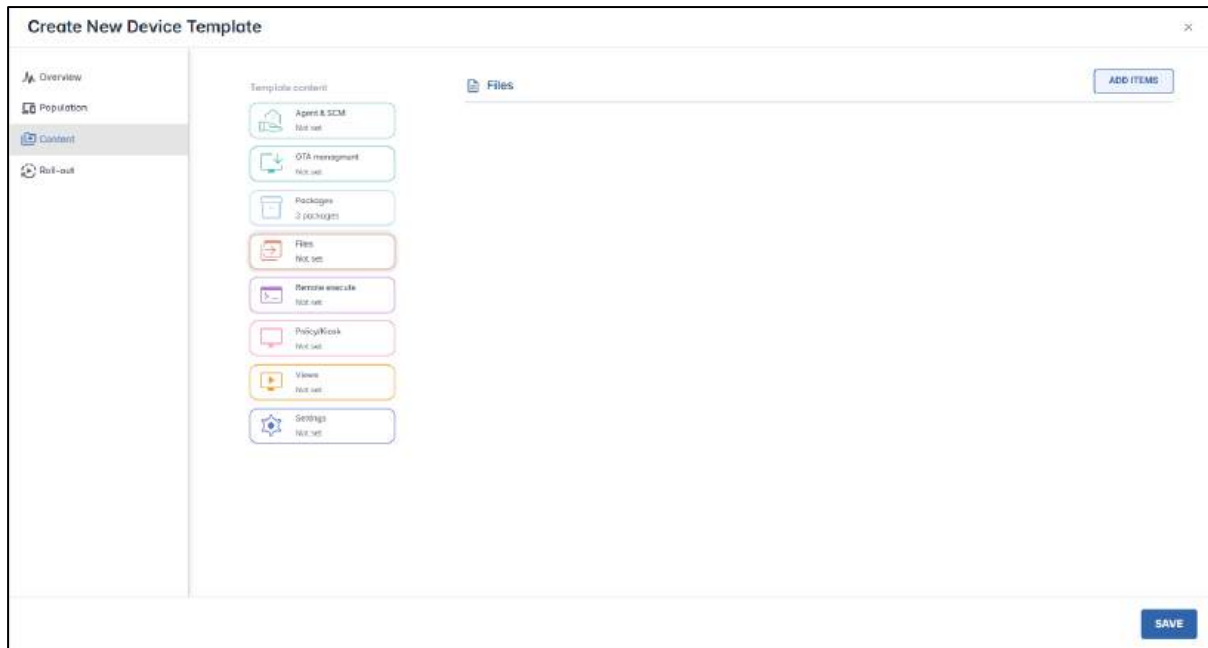
2. Select one of the upload methods for the software package you would like to add to the template: downloading a software package from a URL, uploading a file from your computer, or getting an installation package from the Google Play Store.
3. Proceed as in **Section 6.1.13, Install App/Install Package**, regarding adding a new software package.
4. Upon selecting a software package to apply to the devices, click **Save**.

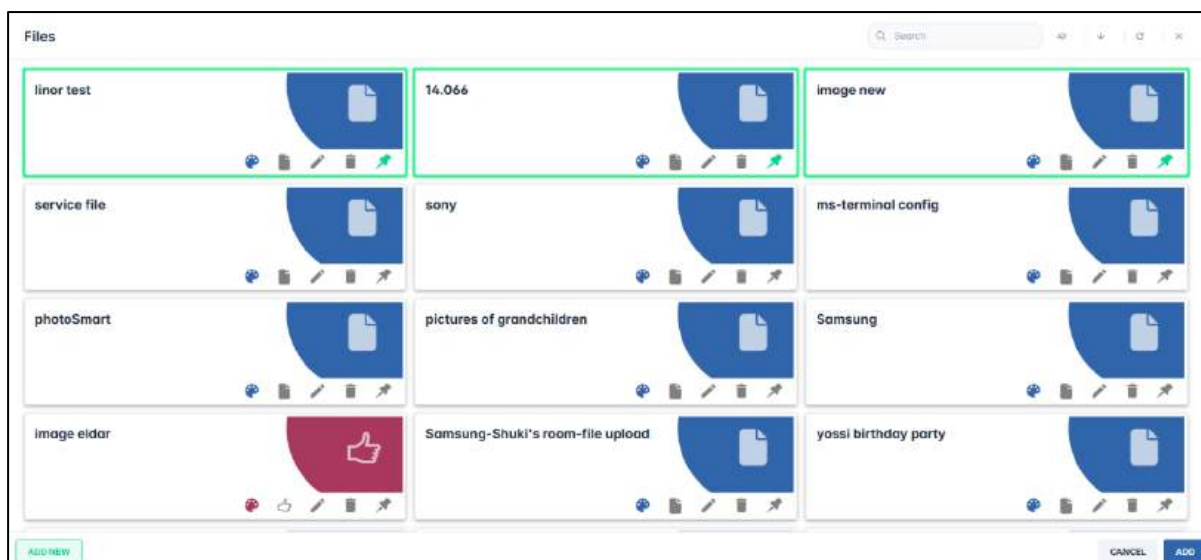
8.1.3.4 Files

This allows you to select files to be sent to the devices in the template.

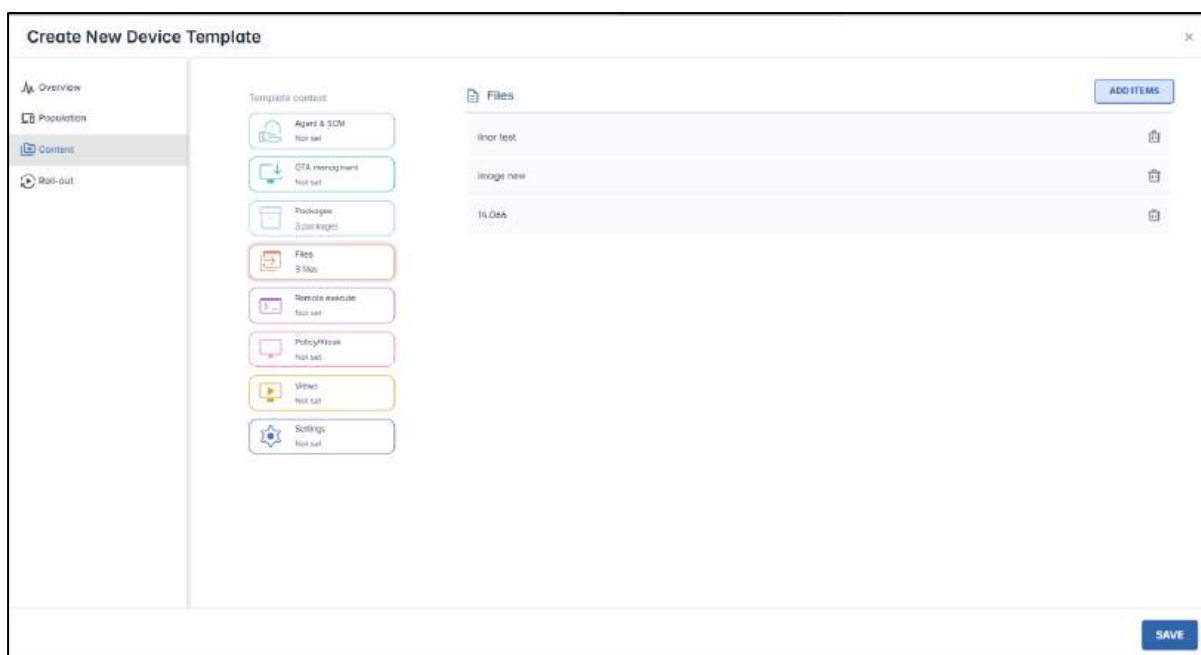
To add files to the devices in a template:

1. Click on the **Files** tab to open the Files window.





3. Click **Add** or **Update** when you have finished your selection. The selected file(s) will be added to the device template. All the devices in the template will have the files copied over.



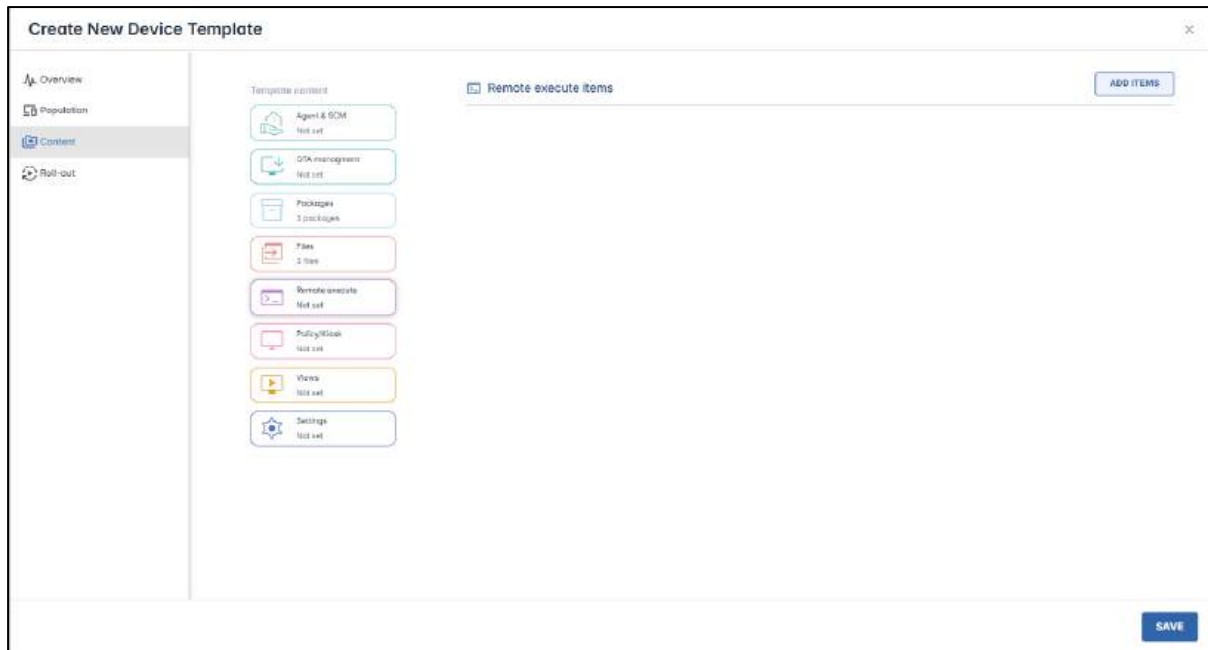
4. Click **Save** to save the selection of files that you wish to add to the devices in the template.

8.1.3.5 Remote Execute

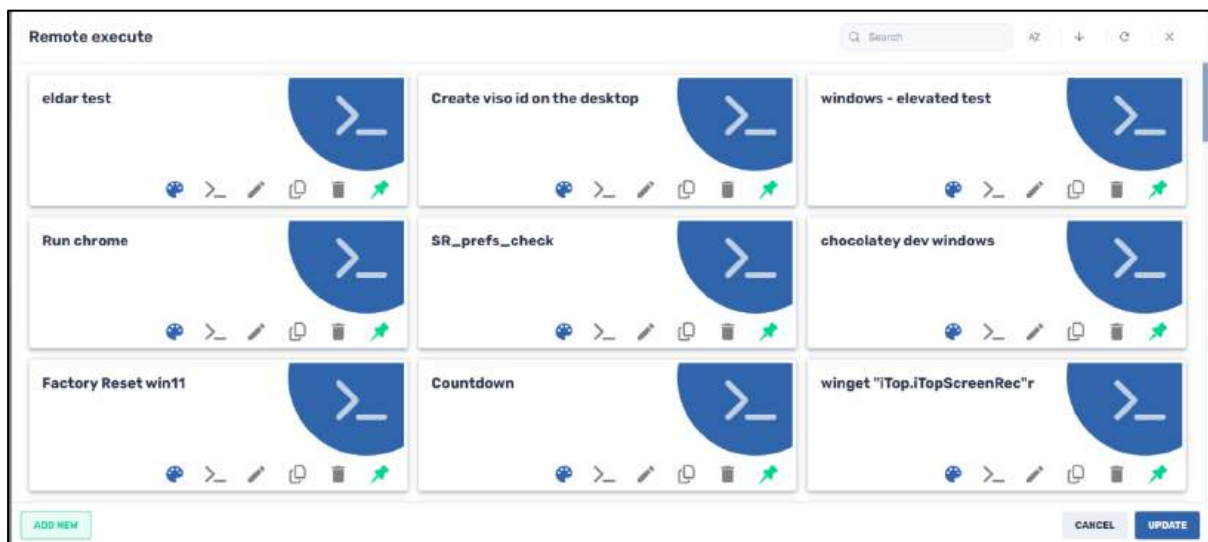
There is also the option to apply a Remote Execute command line script to a template to be executed on the remote devices.

To apply a Remote Execute command:

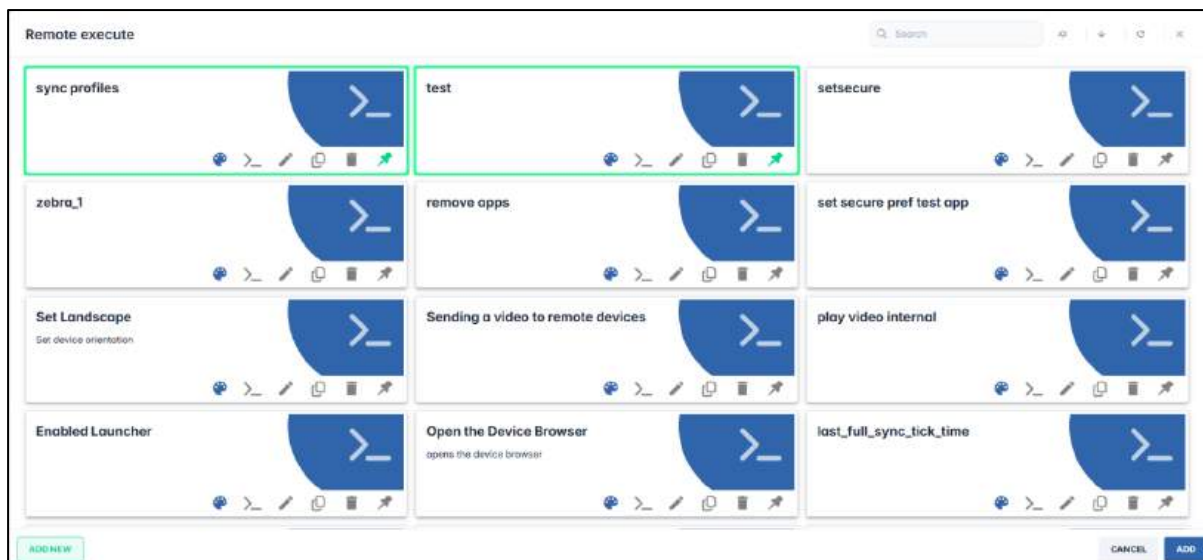
1. Click on the **Remote Execute** button and click on **Add Items**.



The **Remote Execute** repository window opens.



- Click on one or more of the listed remote execute scripts to attach them to the template and click **Add**.



If you wish to create a new remote execute script, refer to **Section 6.1.23, Remote Execute**.

New remote execution

Name

Name is required

Description

Command

Arguments

☒ Command line
 ☐ Script

☒ Wait for exit

☒ Collect output

☒ Run with high privileges

Set as private

This repository item will be visible only to this user

Hide content from others

Other users can apply this repository but cannot see or open its content

Set as read-only

This repository item will be editable only to this user and admin users, and read-only for the others

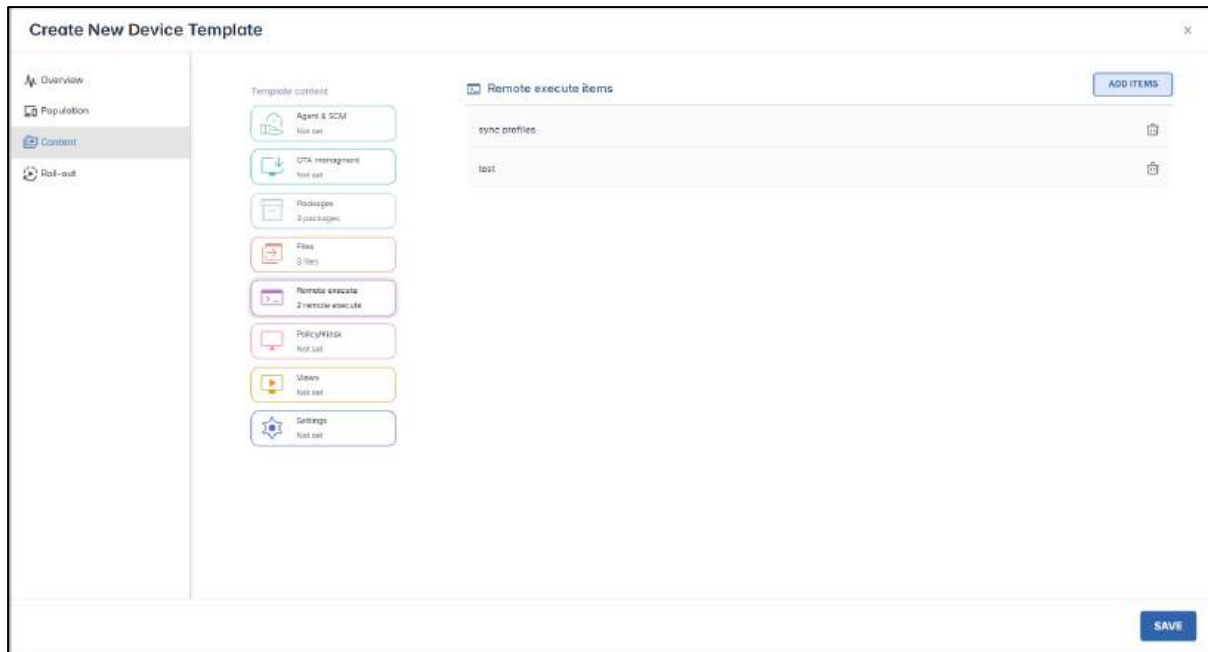
CANCEL

CONFIRM

- After adding the Remote Execute script, the selection will appear in the **Template** window.

All rights reserved by Radix Technologies Ltd.
 © Radix Device Management User Manual
 www.radix-int.com | Telephone: 03-9606350

Page 331



4. Click **Save** to save your selection.

8.1.3.6 Policy/Kiosk

Under the Policy/Kiosk tab, you will be able to add a software policy of allowed or blocked applications or have devices in the device template to function in Kiosk mode, where they are limited to a fixed number of options.

- Regarding policies, refer to **Section 6.1.21, Policies (Block Lists)**.
- Regarding using a device in a kiosk display, refer to **Section 6.1.14, Kiosk**.

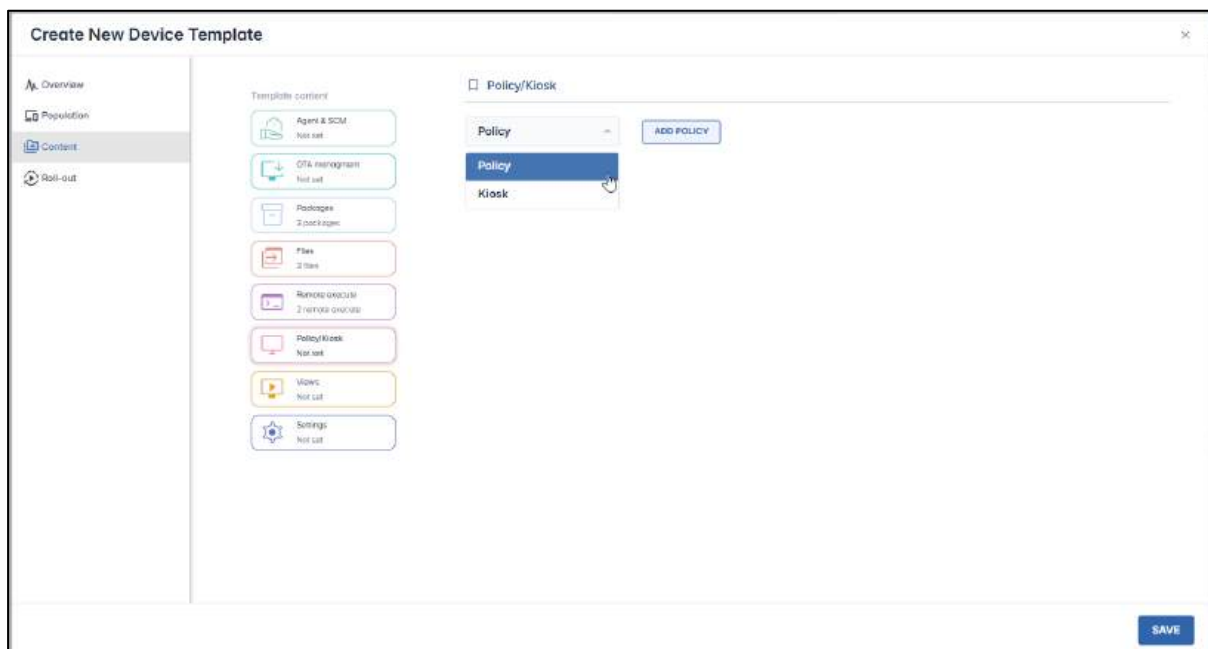


Figure 8-13: The user has selected the Policy option

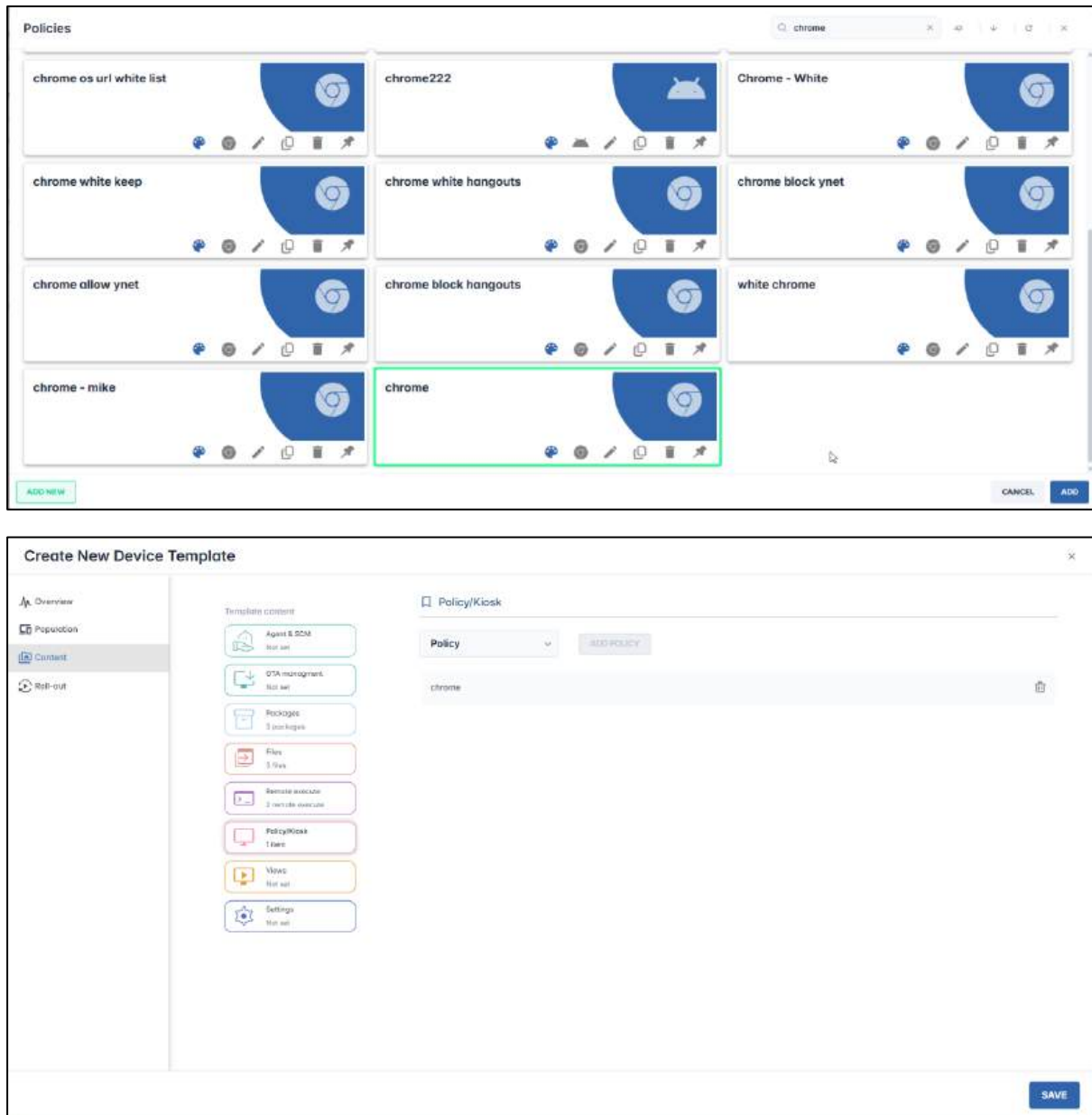
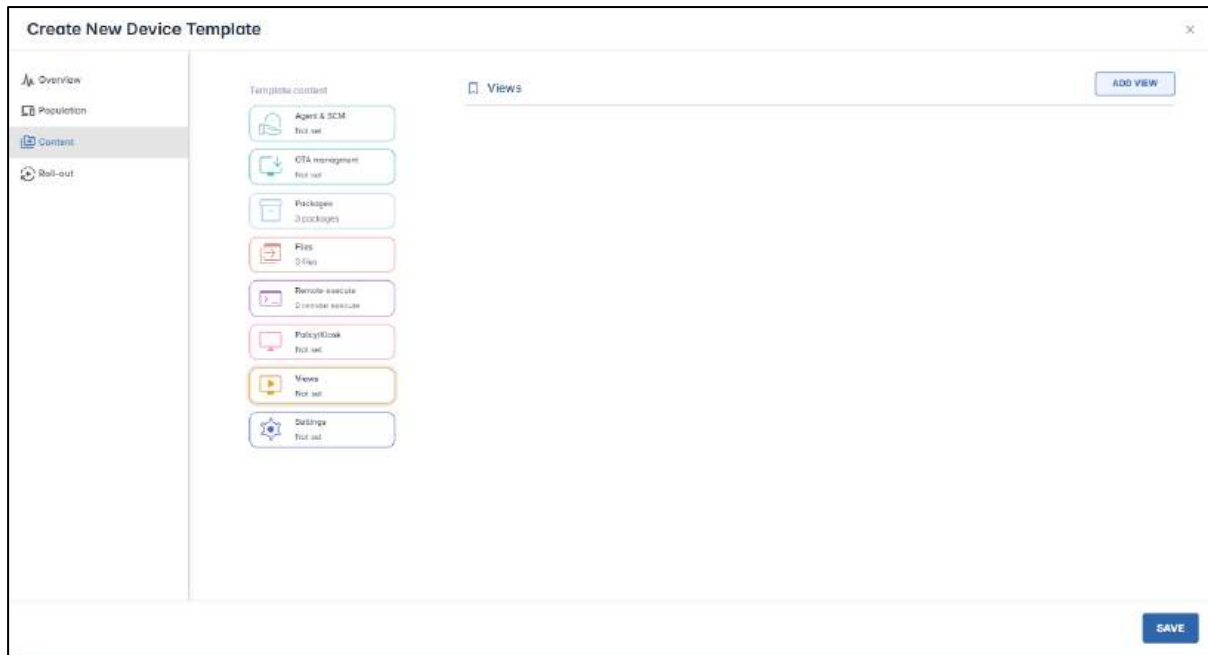


Figure 8-14: The user has selected the Chrome browser to be on the list of blocked apps

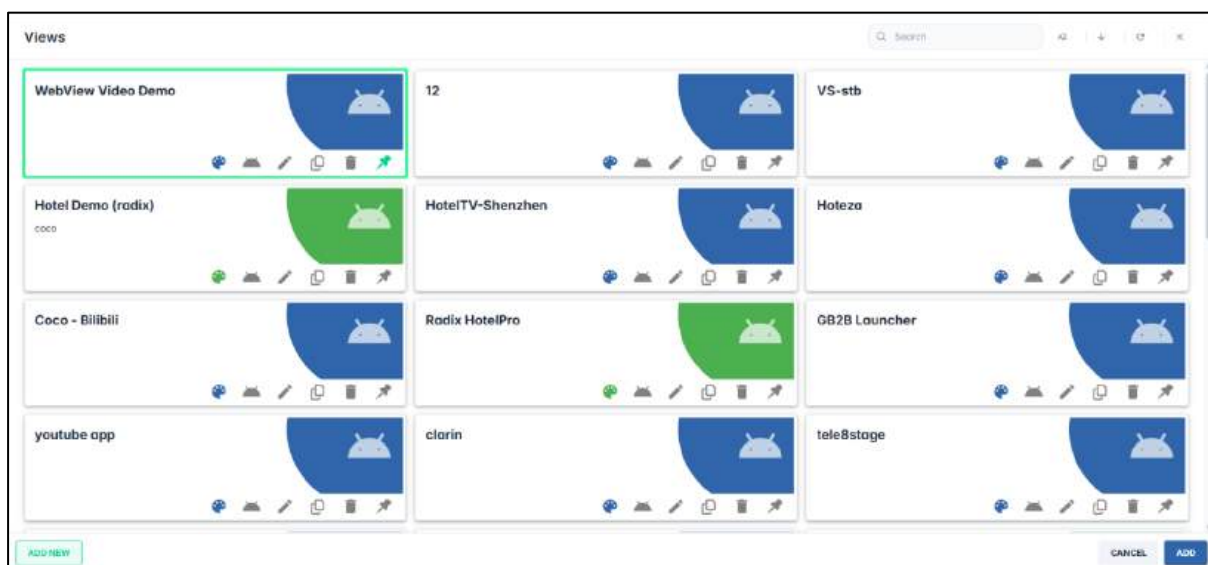
8.1.3.7 Views

The **View** option is a specialized type of Policy/Kiosk option. It allows you to select a list of permitted apps on a remote device, and to be able to view a single website.

Note: If you have already selected an item under the **Policy/Kiosk** tab, the **View** option will be disabled. Similarly, once you have selected a View option, the Policy/Kiosk option will be disabled.



When you click on the **Add View** button, the following window opens:



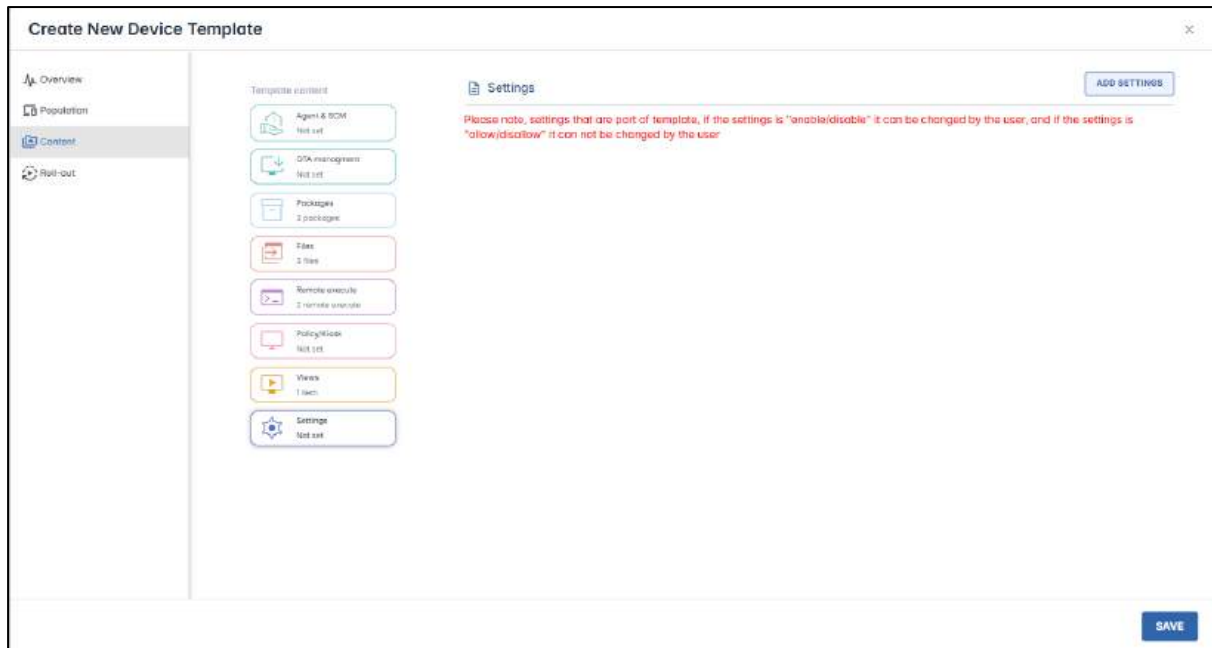
You can select a view option from the repository, or click on **Add New** in the lower left, to create a new View option. Creating a new View option is treated in **Section 6.1.35**.

8.1.3.8 Settings

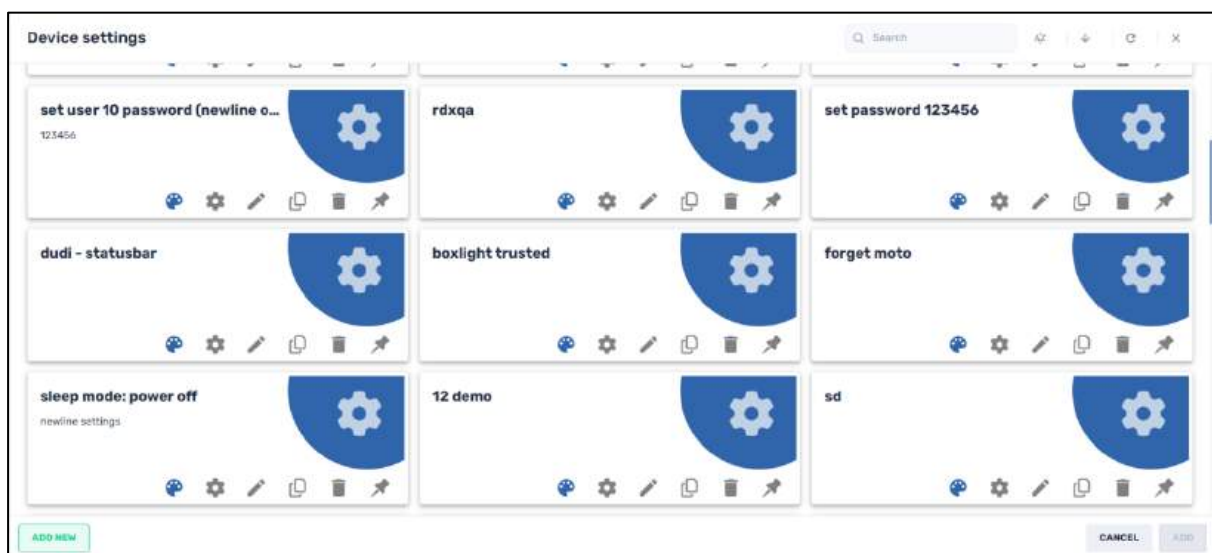
This allows you to modify device settings to the devices in the template.

To adjust device settings to the devices in a template:

1. Click on the **Settings** tab to open the Settings window.



2. Click on **Add Settings**. The Device Settings window opens.

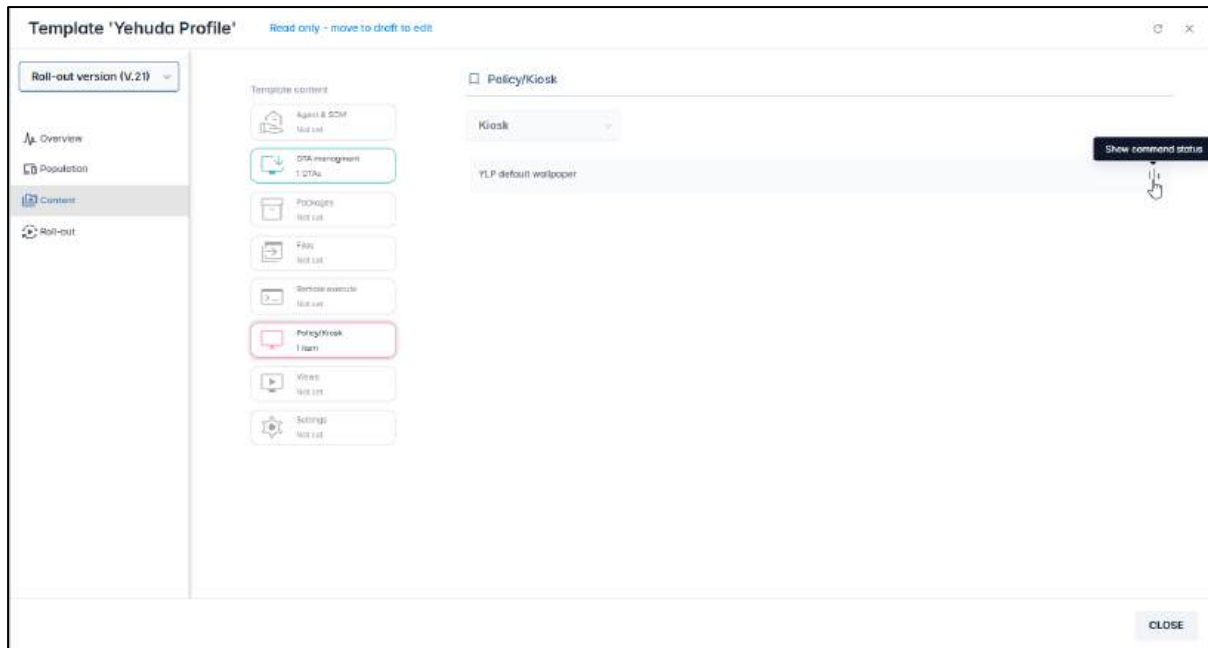


3. Proceed as in **Section 6.1.8, Device Settings** to apply device settings that already appear in the Device Setting repository, or to create a new device setting.

8.1.4 Command Status View and Delete Options

Note that there are two icons next to each of the eight content options.

- **Show Command Status:** When in **Read only mode**, you will see a “Show Command Status” icon. Clicking on the content item displays when the OTA update will be applied to the devices in the template, and when the various commands in the software package will be executed.



The **Show Command Status** pane shows the ID of the command, when it was to be executed, which commands were executed successfully, which are pending, which failed to execute, etc.

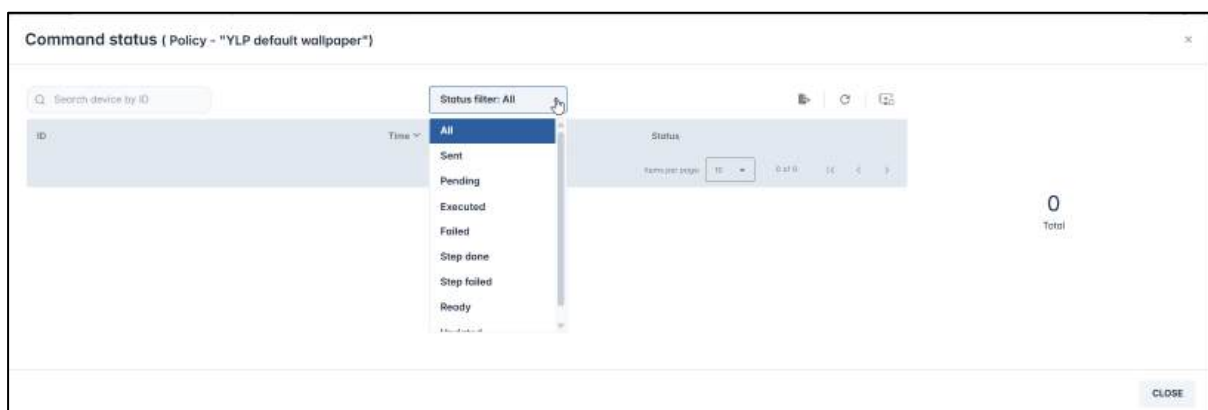


Figure 8-15: Command status of an OTA update applied to a device template

- Removing a Content Item from a Template:** When in **Draft Version** mode, you will see a **Remove** icon near a Content item. If you wish to delete a content item from a device template, go to **Draft Version**, and click on the **Remove** icon next to that item:

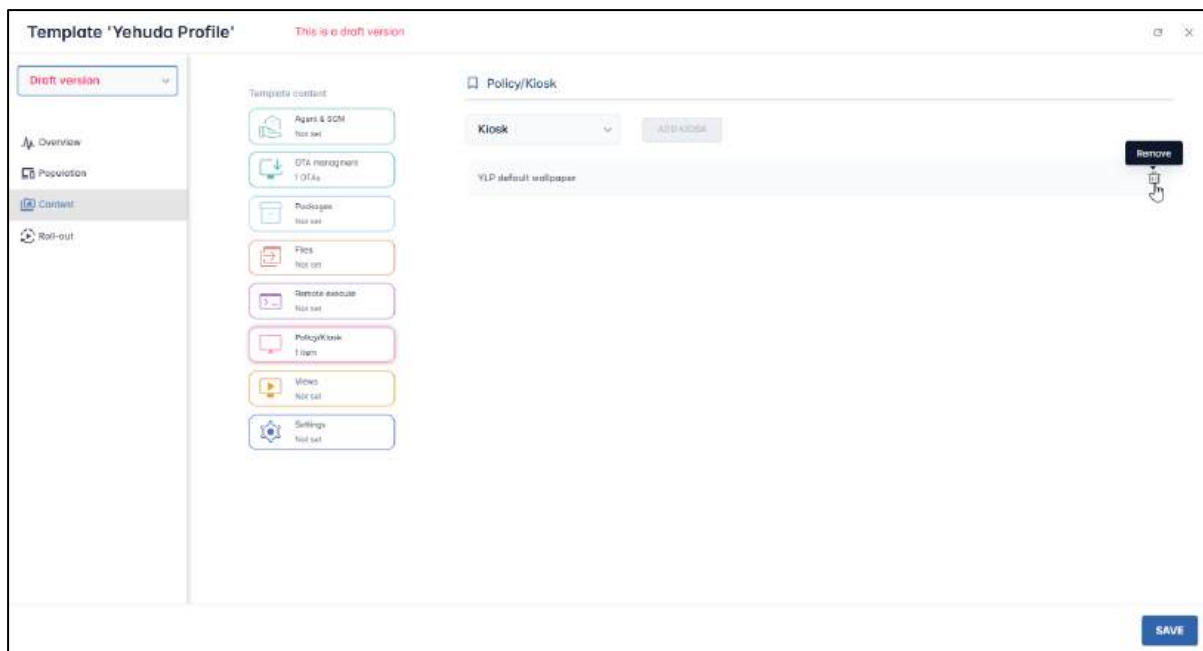


Figure 8-16: Radix packages that you can apply to remote devices

8.1.5 Roll-out Panel

The Roll-out window allows you to specify when to execute the details of a template.

The Roll-out window is divided into three sections:

- Roll-out configuration
- Execution configuration
- Post installation message

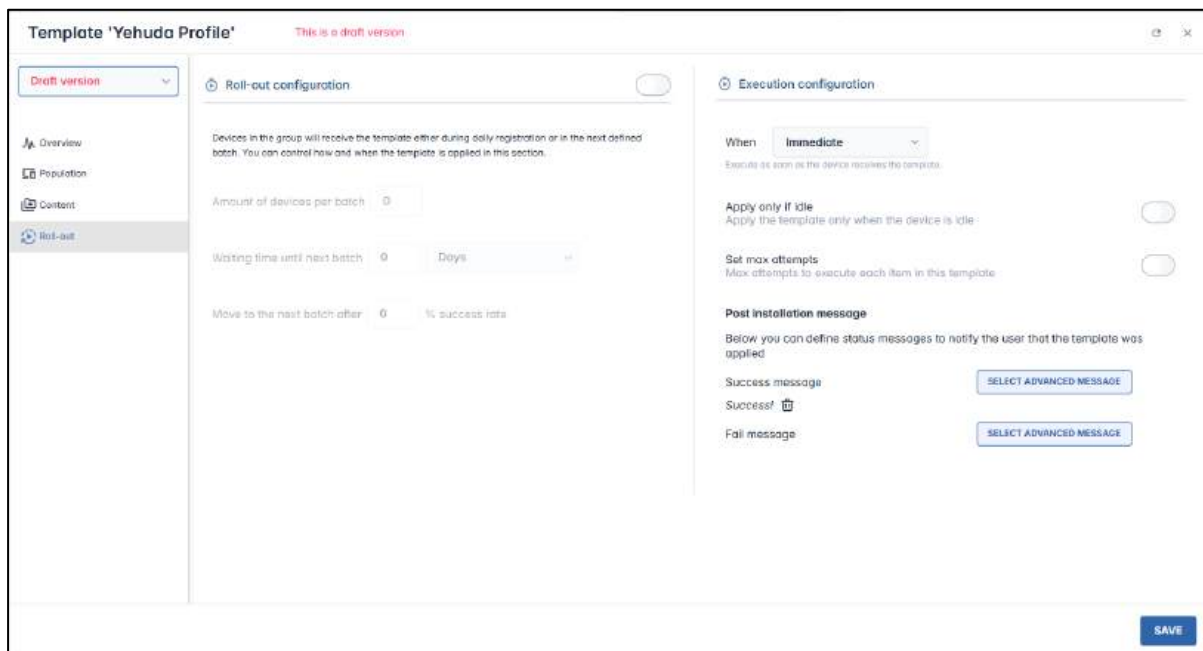


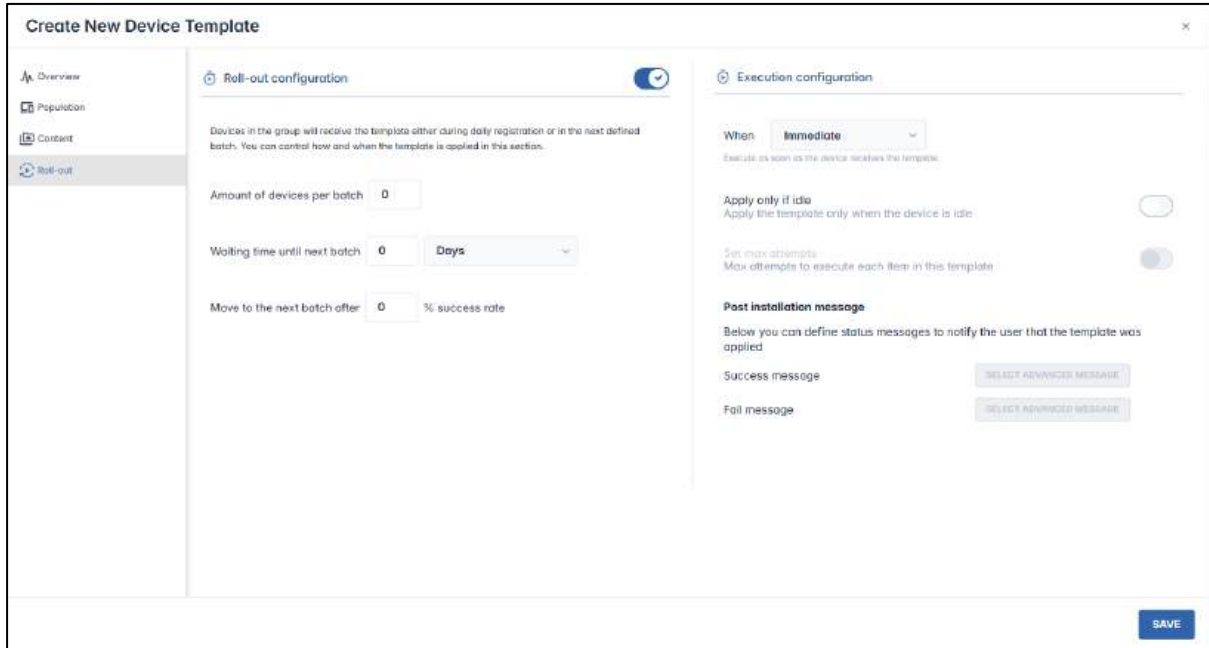
Figure 8-17: Layout of Roll-out Window

8.1.5.1 Roll-out configuration

The **Roll-out configuration** pane lets you allocate batches of devices to which to assign the template.

To use the roll-out configuration options:

1. Click on the **Roll-out** tab and click on the button at the top of the Roll-out configuration pane.



The screenshot shows the 'Create New Device Template' dialog box. On the left is a sidebar with tabs: Overview, Population, Content, and Roll-out (selected). The main area is divided into two panes. The 'Roll-out configuration' pane (active) contains a toggle switch at the top, a description, and three input fields: 'Amount of devices per batch' (0), 'Waiting time until next batch' (0 Days), and 'Move to the next batch after' (0 % success rate). The 'Execution configuration' pane contains a 'When' dropdown (Immediate), a toggle for 'Apply only if idle', a toggle for 'Set max attempts', and a 'Post installation message' section with 'Success message' and 'Fail message' buttons. A 'SAVE' button is at the bottom right.

The batch options are now active.

2. You can assign the following parameters:
 - a. The number of devices per batch
 - b. The waiting time between batches, in units of hours or days
 - c. The success rate of proper execution of the template, before proceeding to the next batch of installations.

The screenshot shows the 'Create New Device Template' interface. On the left is a sidebar with navigation links: Overview, Population, Content, and Roll-out (which is selected). The main area is divided into two tabs: 'Roll-out configuration' (active) and 'Execution configuration'. The 'Roll-out configuration' tab contains a description of how devices receive the template, input fields for 'Amount of devices per batch' (0), 'Waiting time until next batch' (0), and 'Move to the next batch after' (0). A dropdown menu is open for the 'Waiting time' and 'Move to the next batch' fields, showing options for 'Days', 'Hours', and 'Days' (highlighted). The 'Execution configuration' tab is visible in the background, showing options for 'When' (Immediate), 'Apply only if idle', 'Set max attempts', and 'Post installation message'.

8.1.5.2 Execution configuration

In this pane, you set the time when you want the device template to be executed on the specified devices. There are three options:

- **Immediate:** The template will be implemented as soon as the device gets the template.

This is a duplicate of the screenshot above, showing the 'Create New Device Template' interface with the 'Roll-out configuration' and 'Execution configuration' tabs.

- **Time frame:** You can assign a start time and end time between which the template should be executed.

Note: If the content of the Template contains a View, the View will continue to be displayed by the remote devices even after the “end time” of the time frame. The time frame discussed here refers to the time interval over which the Template will **start** to

be executed—but not when it will **stop**. In order to disengage a group from a template, you must delete the group in the Population tab.

- **On demand:** The template will only be executed when you initiate it manually.

Figure 8-18: Sample template that will be rolled out "on demand"

Note: This option is available when the **only** content assigned to the template is an OTA update. If there is any other type of content in the template (software packages, remote execute scripts, files, views, software policies), this option will be grayed out.

There are two other roll-out options:

- **Apply only if idle:** The device template will be applied specifically when the device is not in use. This is desirable if you don't want to disturb users of the remote devices while they are using their device.
- **Set max attempts:** You can set a maximum number of attempts to execute the device template, before determining that the implementation was unsuccessful. You can assign the number of attempts as any number from 1-50, with the default being three attempts.

The screenshot displays the 'Create New Device Template' interface. On the left, a sidebar contains links for Overview, Population, Content, and Roll-out (which is selected). The main area is divided into two panels: 'Roll-out configuration' and 'Execution configuration'. The 'Roll-out configuration' panel includes fields for 'Amount of devices per batch' (set to 0), 'Waiting time until next batch' (0 Days), and 'Move to the next batch after' (0 % success rate). The 'Execution configuration' panel includes a 'When' dropdown set to 'Time frame', a 'Define end time' checkbox (checked), 'Start date' (Mar 5, 2026) and 'End date' (Mar 17, 2026), 'In days' (S, M, T, W, T, F, S), 'Start time' (21:32) and 'End time' (21:32), and two toggle switches: 'Apply only if idle' (checked) and 'Set max attempts' (checked). A 'SAVE' button is located at the bottom right.

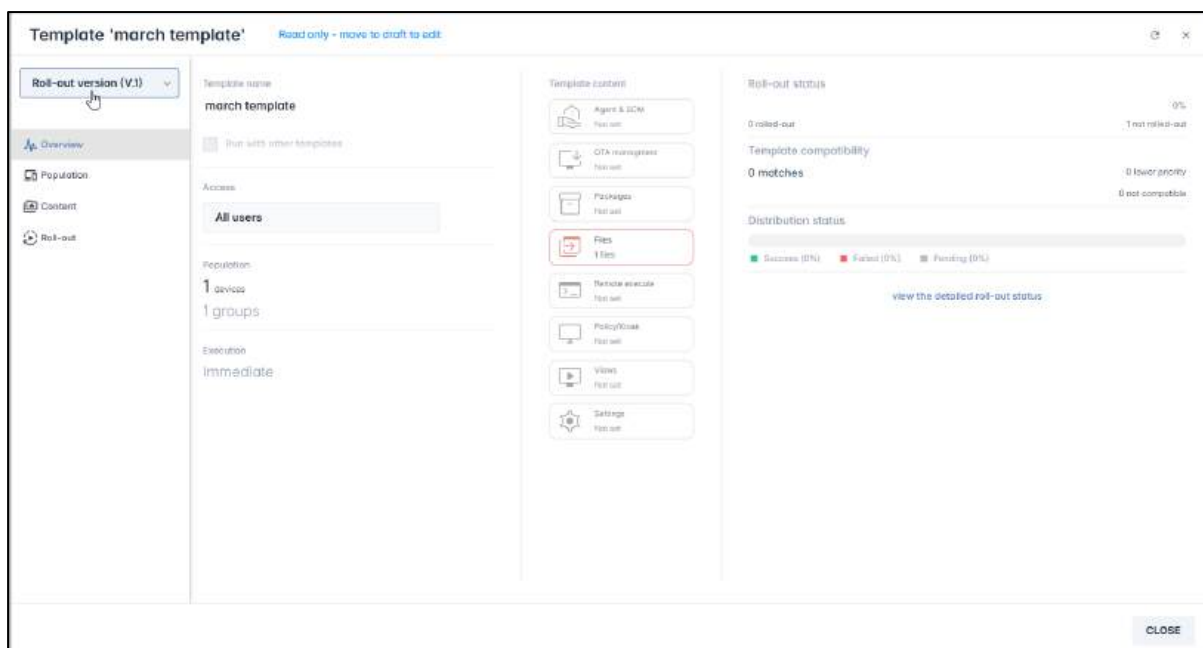
Figure 8-19: Illustration of the Roll-out options

8.1.5.3 Post-Installation Message

This option allows you to send the remote user notifications that the template was either executed successfully or failed to execute. You can select the messages from the **Advanced message** repository.

If the content of the template includes an OTA update, and you attached an Advanced Message if it is executed properly (see **Section 8.1.3.2.1, Adding an Existing OTA Update Package**), the template will display **both** Advanced Messages if it is executed successfully.

Upon clicking **Start roll-out** in the Overview tab, the **Roll-out version** selection will give a summary of the template:



You will get a prompt in the lower right corner that the template was created correctly, and the new template will appear in the Device Templates Console.

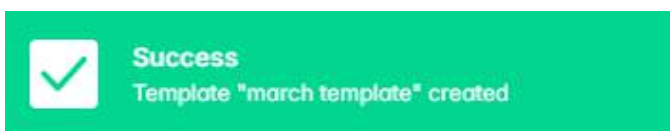


Figure 8-20: Popup Notification that the template was created

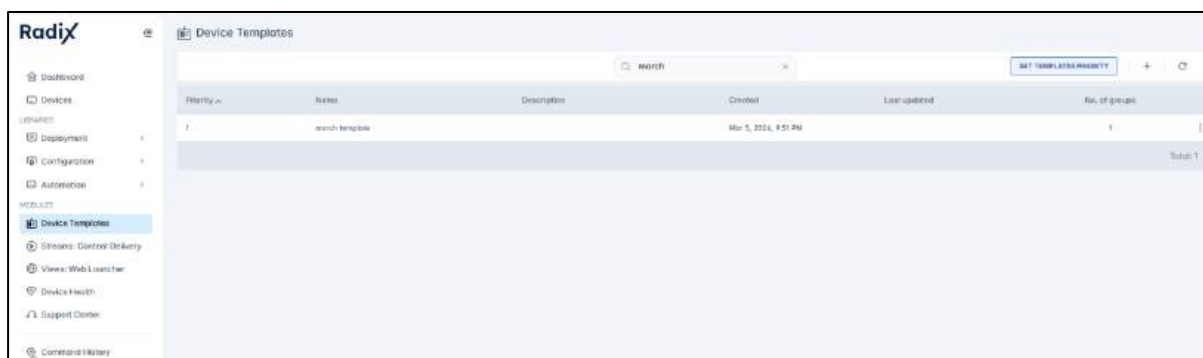


Figure 8-21: The Device Templates Console, with the new template (“march template”) at the top of the list

After you have created the template, you can modify it at any time by clicking on it in the Device Templates list.

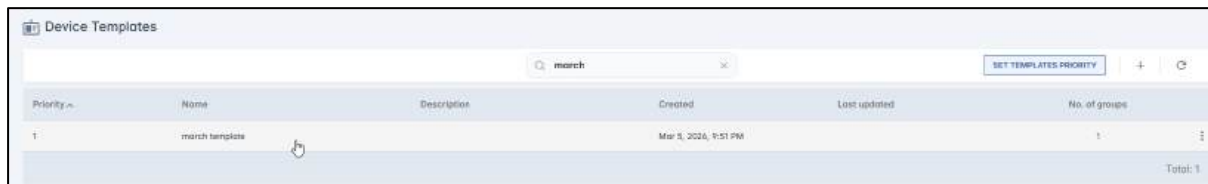
8.2 Starting a Device Template

Once you have entered all of the details of a device template (to which group(s) of devices you would like to apply the template, the contents of the template, and the manner in which the template will be executed), you are now ready to start rolling out the template.

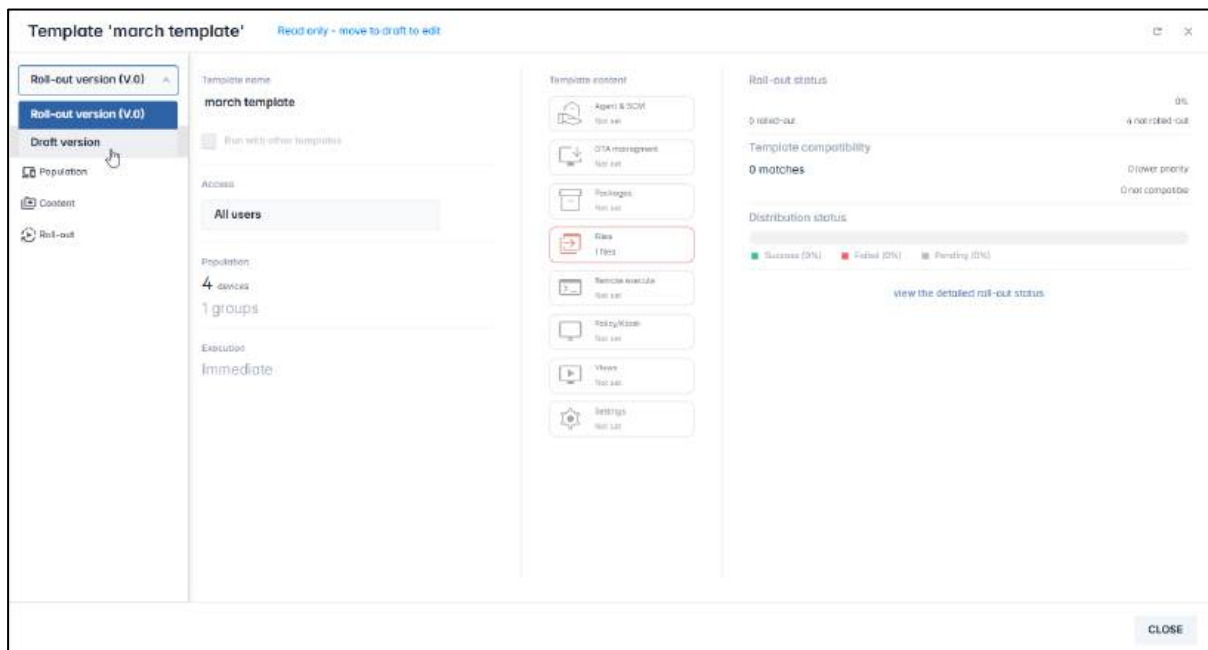
To roll out a template:

1. Click on the **Templates** icon in the sidebar menu, to open the Templates Console.

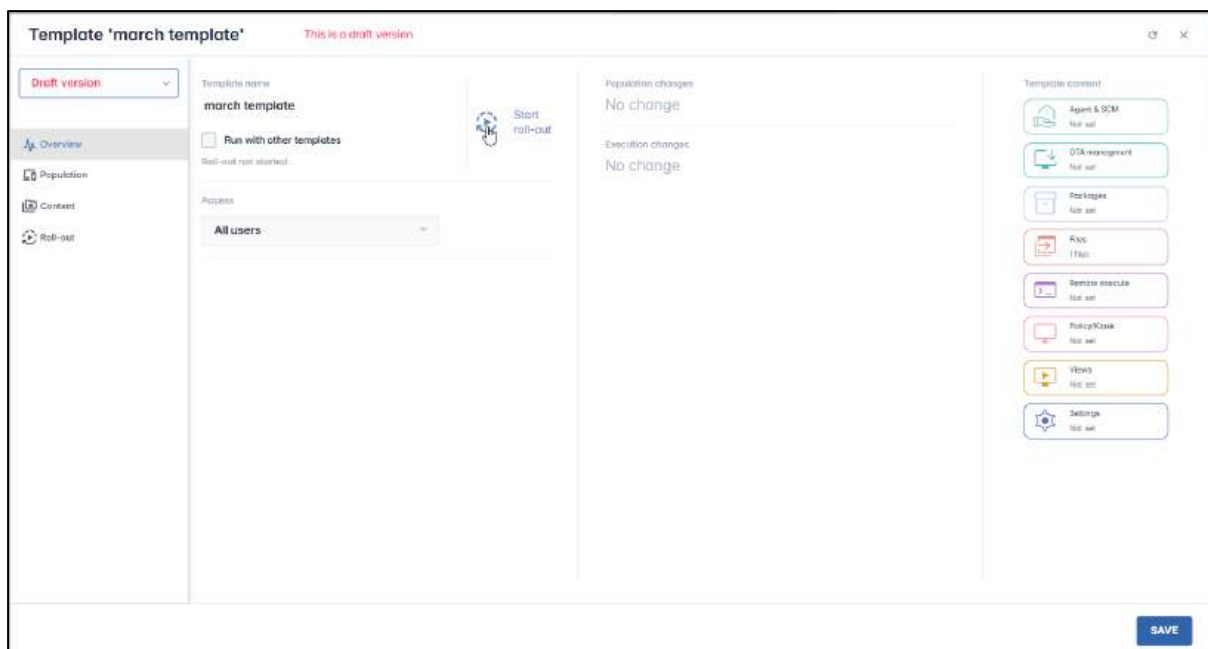
- Click on the row of the template you would like to apply.



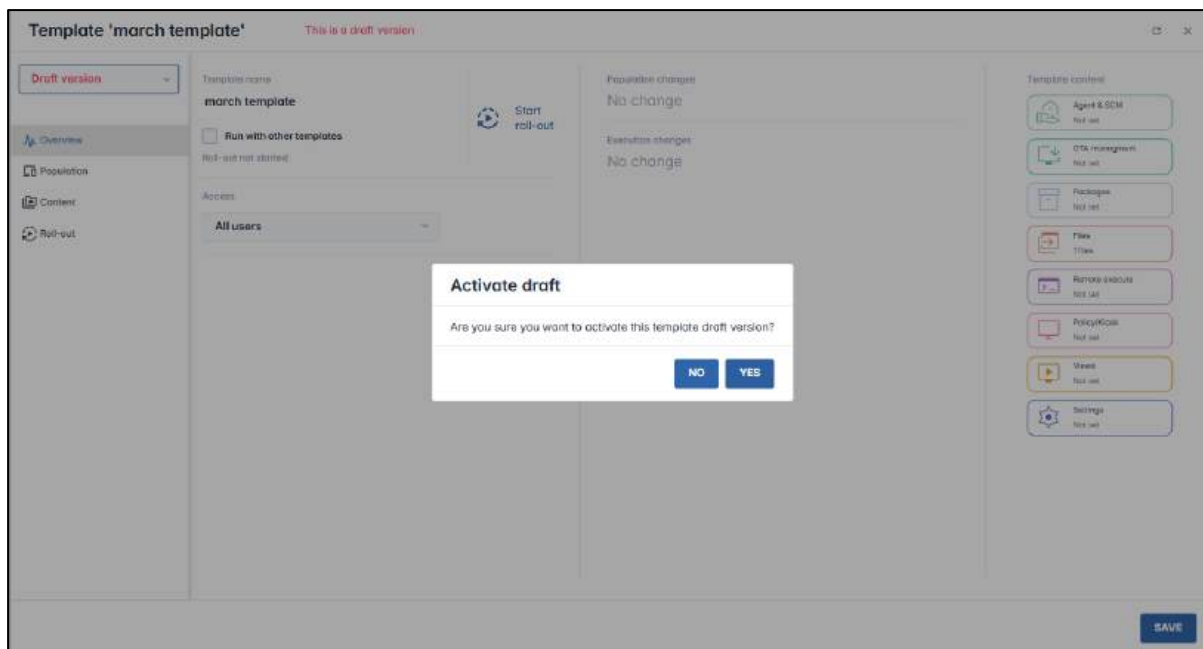
- In the dropdown menu in the upper left corner, select **Draft version**.



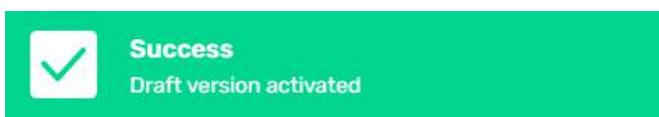
- In the Draft version window, click on **Start roll-out**.



- You will be prompted as to whether to activate the template. Click **Yes**.



A popup notification will appear, informing you that the template has been activated.



The template will be executed on the remote devices in the group. If you have assigned an Advanced Message to indicate that the template was executed successfully, it will display on the remote devices.



- After you tap on the **Back** icon on the remote device, it will display the content of your template. In our example, our selected content was a view of a video:



8.3 Stopping a Template

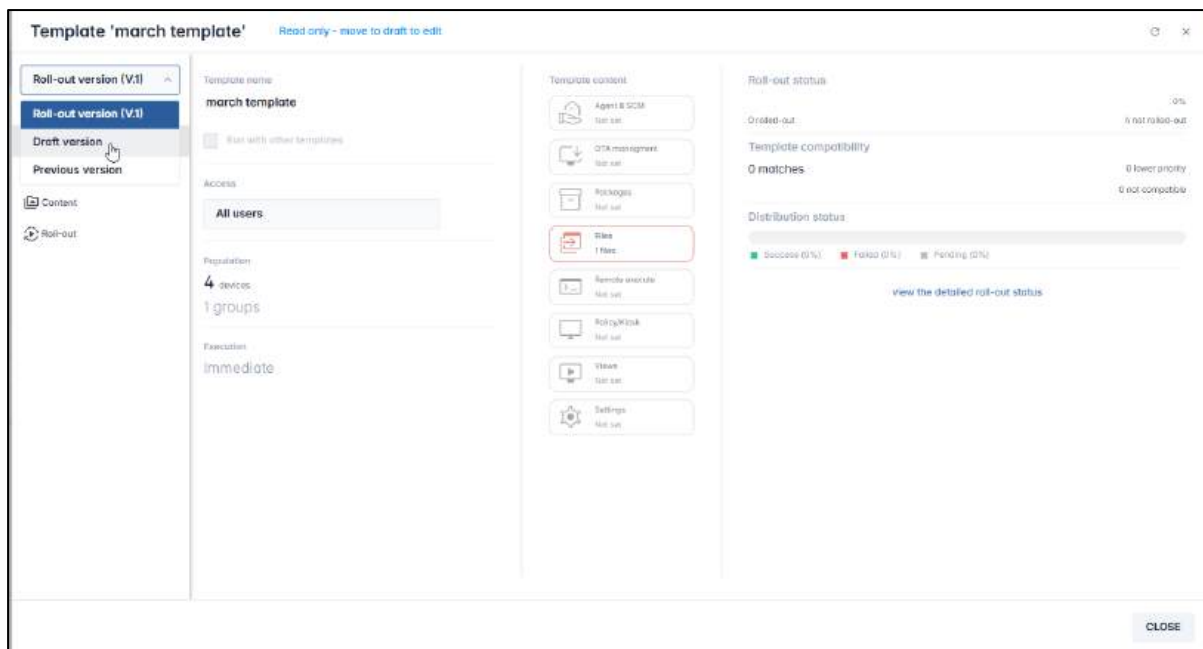
If you wish to stop a template from being executed, you must first remove the group of devices from the template in the Population tab. This will allow the devices in the group to go back to their regular functionality.

To stop a template:

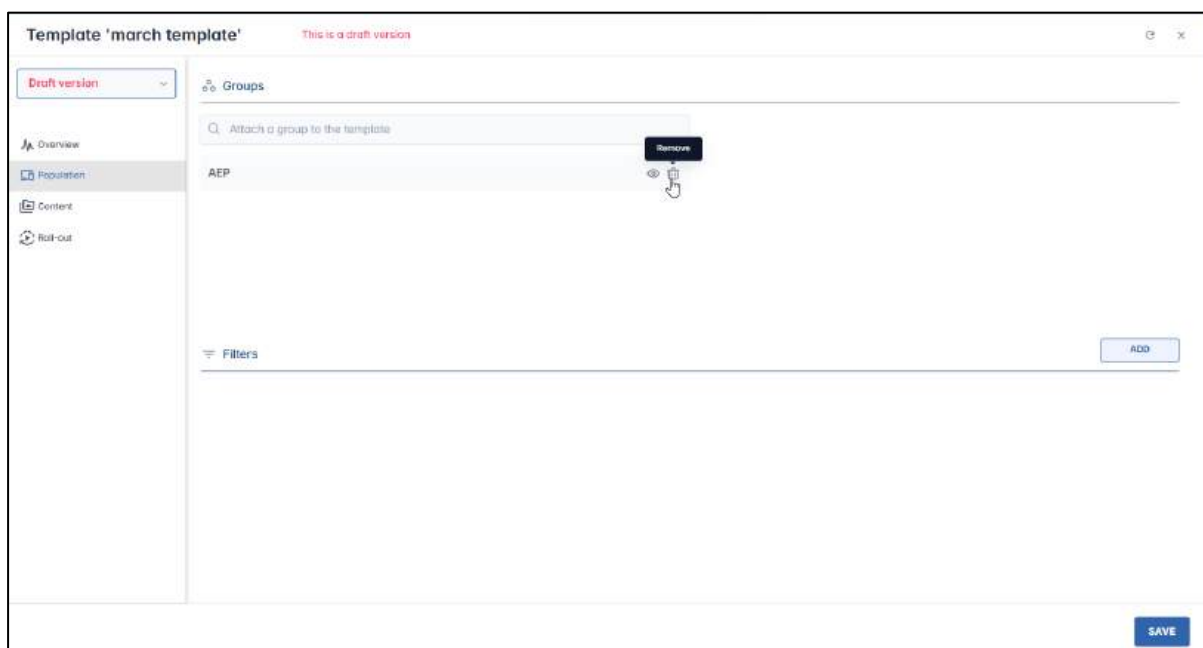
1. Click on the template that you want to stop.

Priority	Name	Description	Created	Last updated	No. of groups
37	6653		Aug 18, 2024, 5:44 PM	Jan 25, 2026, 9:25 PM	0
38	19058		Aug 19, 2024, 9:38 AM	Jan 25, 2026, 9:25 PM	1
39	update agent and clear all		Aug 13, 2025, 5:07 PM	Jan 25, 2026, 9:25 PM	1
40	2018		Aug 20, 2024, 2:09 PM	Jan 25, 2026, 9:25 PM	0
41	XG Base		Oct 11, 2025, 6:11 AM	Jan 25, 2026, 9:25 PM	1
42	formatting		Sep 6, 2024, 12:52 PM	Jan 25, 2026, 9:25 PM	1
42	test media		Dec 17, 2025, 1:19 PM	Jan 25, 2026, 9:25 PM	1
44	test		Dec 24, 2025, 4:51 PM	Jan 25, 2026, 9:25 PM	0
45	search template		Mar 5, 2026, 9:51 PM	Mar 6, 2026, 11:20 AM	1
46	My Device Template		Jan 25, 2026, 9:04 PM	Mar 6, 2026, 11:20 AM	0
47	A brand new template		Jan 24, 2026, 9:40 PM	Mar 6, 2026, 11:20 AM	0
48	Sept 22		Sep 22, 2024, 9:16 PM	Mar 6, 2026, 11:20 AM	0
49	test report		Nov 7, 2024, 10:44 AM	Mar 6, 2026, 11:20 AM	0
50	October 27th		Oct 27, 2024, 4:20 PM	Mar 6, 2026, 11:20 AM	0
51	test test		Nov 17, 2024, 1:03 PM	Mar 6, 2026, 11:20 AM	1
52	test test		Jan 24, 2025, 12:30 PM	Mar 6, 2026, 11:20 AM	0
53	test test		Jan 24, 2025, 12:30 PM	Mar 6, 2026, 11:20 AM	1

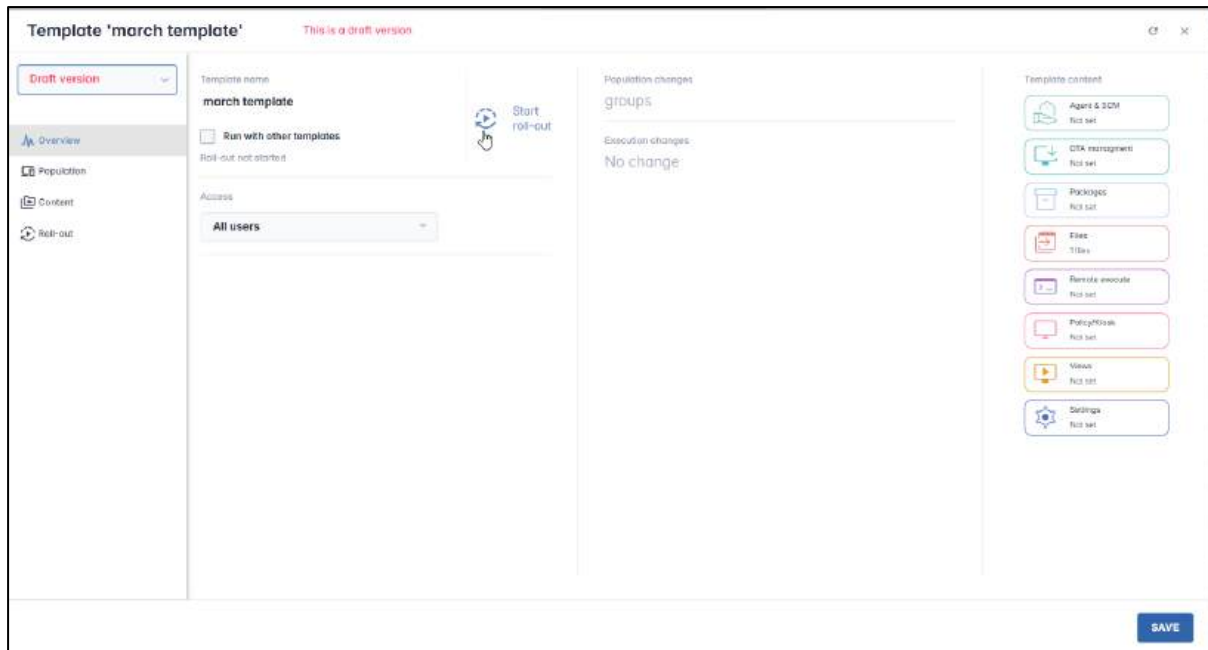
2. Go to **Draft Version** to allow you to make changes to the template.



3. Go to the **Population** tab and remove the group of devices from the template.



4. Go to the **Overview** tab and click **Start roll-out**. It will now run the template again, but with no groups associated with the template.



5. Click **Yes** in the notification popup to activate the revised template:



This will disassociate the group from the template, and the devices in the group will go back to normal functionality.

8.4 Editing a Template

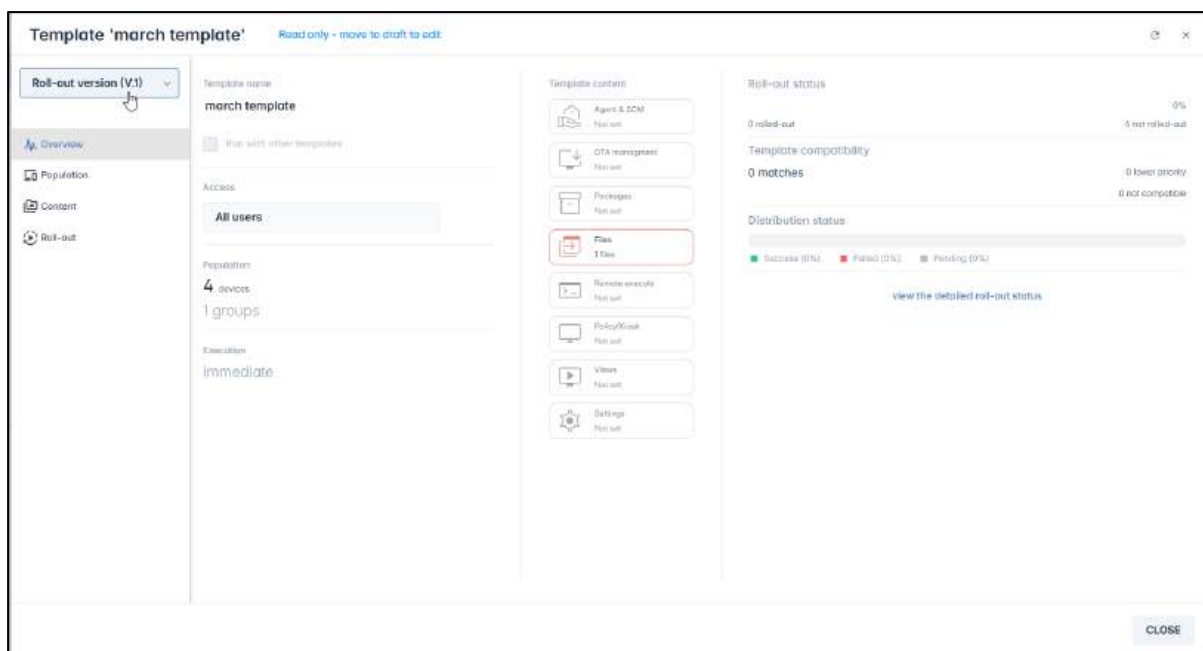
After creating a template, you can later make modifications by entering **Draft Version** mode.

To modify a template:

1. From the Overview Dashboard, click on the **Device Template** icon to open the Device Template Console.
2. Find the template that you would like to modify. You can use the Search bar at the top of the list. (**Note:** The search is **not** case sensitive.)

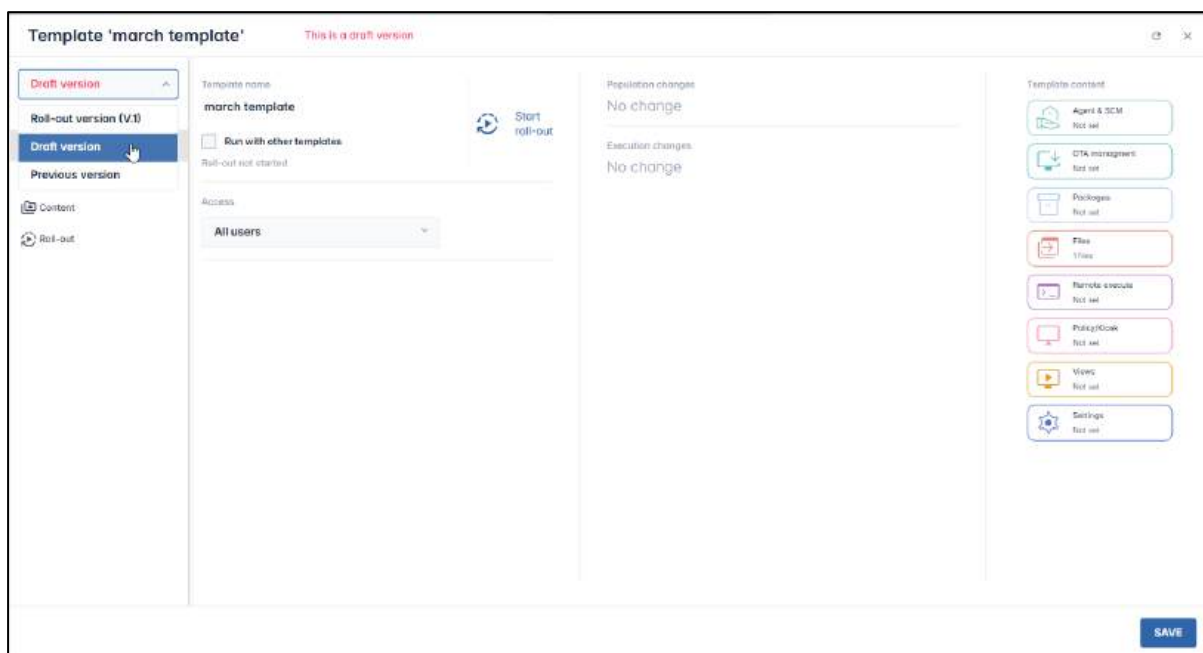


3. Click on the template that you would like to modify. The template's Overview screen will open in **Read only** mode, displaying the "Roll-out version" of the template.



The content items that are contained in the template will be in color, while the items that are not included will be grayed out.

4. In the upper left corner, there is a drop-down list. Select **Draft version** to be able to edit the template.



5. When in **Draft version**, you can make changes to all the parameters of the template. Any changes will be recorded in the draft version of the template. When you click **Save**, you will receive a notification, reminding you that your changes are only in the Draft version. You must click on “Start roll-out” to actually save the changes to the template.

Edit template

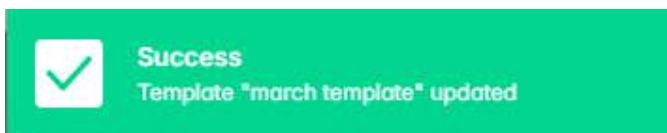
Your changes will be saved as a draft version only and the rollout process will not be started.

You can continue to edit the draft version at any time in the header section.

The rollout process can be initiated by clicking on the "start roll-out" button in the profile dashboard in the drafts section.

CLOSE

A popup will appear in the lower right corner, informing you that the changes have been saved to the draft of the template:



- When you have made the desired changes, click on **Start roll-out** in the template's Overview screen.

Template 'march template'

This is a draft version

Draft version

Overview

Population

Content

Roll-out

Template name

march template

☐ Run with other templates

Roll-out not started

Created by: lin

Last updated: Mar 8, 2026, 11:20

Access

All users

Start roll-out

Preparation changes

No change

Execution changes

No change

Template content

Agent & SCM

Not set

OTA management

Not set

Packages

Not set

File

1 file

Resource associate

Not set

Policy/Role

1 item

Views

Not set

Settings

Not set

SAVE

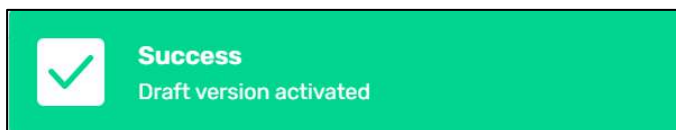
You will be prompted if you are sure that you want to activate the template:

Activate draft

Are you sure you want to activate this template draft version?

NO YES

- Click **Yes** to activate the new, updated template. A pop-up notification will appear in the lower right corner, indicating that the template has been activated.



8.5 Viewing a Previous Version of a Template

If you make changes to a template and execute it, you can still view the results of the previous versions that you executed. This is possible using the **Previous version** option.

To view a previous version of a template:

- From the Overview Dashboard, click on the **Device Templates** icon, to open the **Device Templates** Console.
- Find the template for which you would like to view its previous versions. You can use the Search bar at the top of the list. (Note: The search is **not** case sensitive.)

The screenshot shows the "Device Templates" console with a search bar containing "august". Below the search bar is a table with the following columns: Priority, Name, Description, Created, Last updated, and No. of groups. There are three rows of templates listed.

Priority	Name	Description	Created	Last updated	No. of groups
1	August 6th		Sep 9, 2024, 4:44 PM	Jan 29, 2024, 9:25 PM	0
2	August 17th		Aug 17, 2025, 2:26 PM	Jan 29, 2024, 10:00 PM	1
3	August 11th		Aug 11, 2025, 9:24 PM	Mar 1, 2024, 4:46 PM	0

Total: 3

- Click on the template version that you would like to view. The template's Overview screen will open in **Read only** mode, displaying the "Roll-out version" of the current version of the template.

The screenshot shows the "Template 'August 17th'" Overview screen. The left sidebar has a "Roll-out" section with options: "Roll-out version (V15)", "Draft version", and "Previous version". The main content area shows the "Roll-out status" with a "100% Success" bar and a "1 matches" count. The right sidebar shows the "Template content" with various components like "Agent & SDK", "OTA management", "Packages", "Policies", "Remote access", "Policy/Task", "Views", and "Settings".

- In the upper left corner, click on the drop-down list, and select **Previous version**. You will be presented with a list of all previous versions of the template.

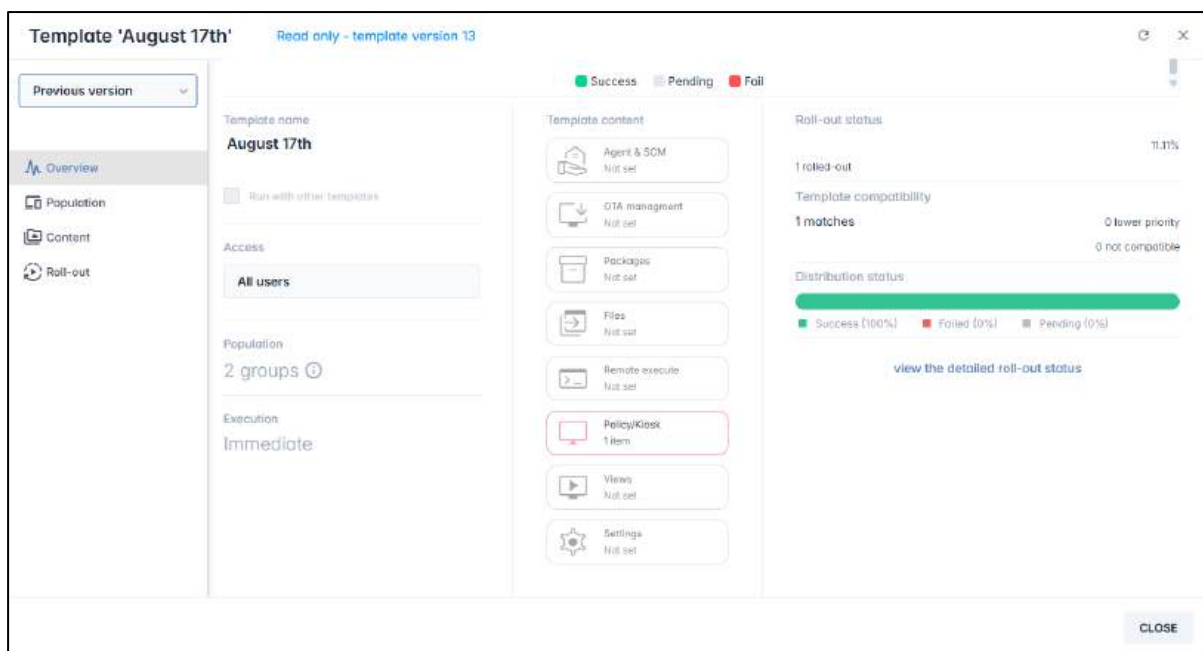


Figure 8-22: Previous versions of a template

- Clicking on the **View Template** icon will allow you to see the Overview screen of the previous version of the template.



The version number of the template will be displayed at the top of the screen:

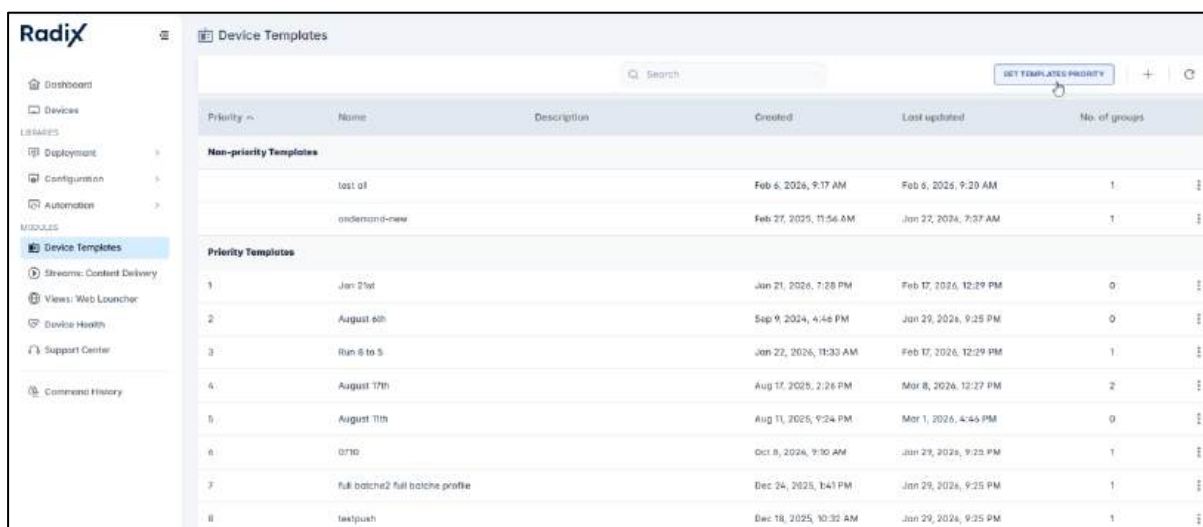


8.6 Setting the Priority of Templates

When you open the Templates Console, the device templates appear in a particular order. You can also choose to rearrange the priority of the templates so that certain ones will be executed first. The template with the lowest number is of the highest priority. Therefore, the devices that meet the filtering conditions of Template No. 1 will be installed with the software and updates associated with that template. The other templates will not be executed on these devices, until you disassociate the device group that is assigned to Template No. 1 from that template, and then assign it to another template.

To prioritize a particular template:

1. Click on the **Device Templates** icon to open the **Device Templates** Console.
2. Click the **Set Templates Priority** button at the top of the list.



3. Note that when you place your mouse over one of the templates, the mouse pointer becomes a hand icon, allowing you to rearrange the priorities of the templates.

Device Templates					
Priority	Name	Description	Created	Last updated	No. of groups
Non-priority Templates					
	test all		Feb 6, 2026, 9:17 AM	Feb 6, 2026, 9:20 AM	1
	ondemand-new		Feb 27, 2025, 11:56 AM	Jan 27, 2026, 7:37 AM	1
Priority Templates					
1	Jan 21st		Jan 21, 2026, 7:28 PM	Feb 17, 2026, 12:29 PM	0
2	August 6th		Sep 9, 2024, 4:46 PM	Jan 29, 2026, 9:25 PM	0
3	Run 8 to 5		Jan 22, 2026, 11:33 AM	Feb 17, 2026, 12:29 PM	1
4	August 17th		Aug 17, 2025, 2:26 PM	Mar 8, 2026, 12:27 PM	2
5	August 11th		Aug 11, 2025, 9:24 PM	Mar 1, 2026, 4:46 PM	0
6	0710		Oct 8, 2024, 9:10 AM	Jan 29, 2026, 9:25 PM	1
7	full batche2 full batche profile		Dec 24, 2025, 1:41 PM	Jan 29, 2026, 9:25 PM	1
8	testpush		Dec 18, 2025, 10:32 AM	Jan 29, 2026, 9:25 PM	1

Rearrange the priorities of the templates by dragging the rows.

SAVE CHANGES CANCEL

- When you have completed prioritizing the list of templates, click **Save Changes** to save the new listing.

Device Templates					
Priority	Name	Description	Created	Last updated	No. of groups
Non-priority Templates					
	test all		Feb 6, 2026, 9:17 AM	Feb 6, 2026, 9:20 AM	1
	ondemand-new		Feb 27, 2025, 11:56 AM	Jan 27, 2026, 7:37 AM	1
Priority Templates					
1	Jan 21st		Jan 21, 2026, 7:28 PM	Feb 17, 2026, 12:29 PM	0
2	August 6th		Sep 9, 2024, 4:46 PM	Jan 29, 2026, 9:25 PM	0
3	Run 8 to 5		Jan 22, 2026, 11:33 AM	Feb 17, 2026, 12:29 PM	1
4	August 17th		Aug 17, 2025, 2:26 PM	Mar 8, 2026, 12:27 PM	2
5	August 11th		Aug 11, 2025, 9:24 PM	Mar 1, 2026, 4:46 PM	0
6	0710		Oct 8, 2024, 9:10 AM	Jan 29, 2026, 9:25 PM	1
7	full batche2 full batche profile		Dec 24, 2025, 1:41 PM	Jan 29, 2026, 9:25 PM	1
8	testpush		Dec 18, 2025, 10:32 AM	Jan 29, 2026, 9:25 PM	1

Rearrange the priorities of the templates by dragging the rows.

SAVE CHANGES CANCEL

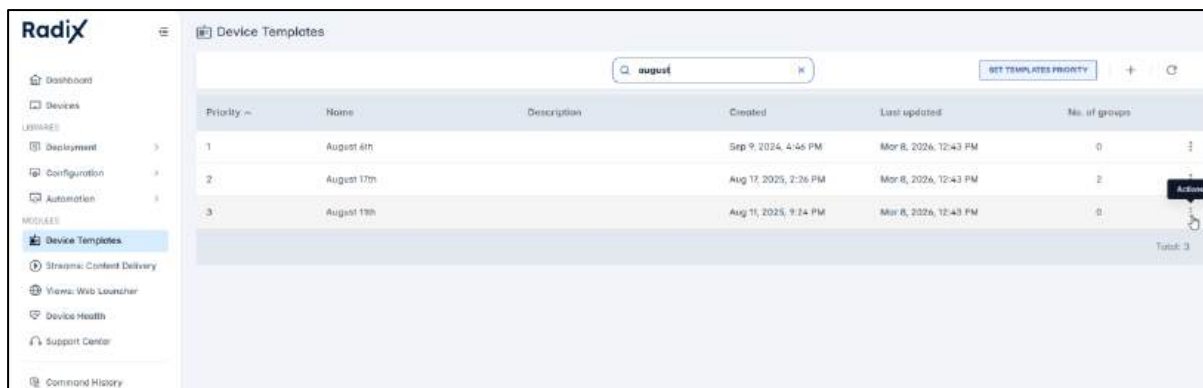
Daily shut down ... - (2) 11

8.7 Deleting a Template

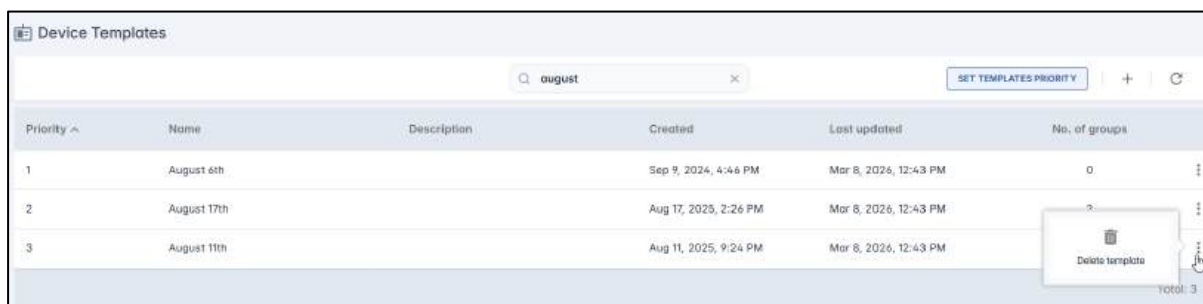
You can also delete a template that you created.

To delete a template:

- Click on the **Device Templates** icon to open the Device Templates Console.
- Find the template which you wish to delete from the list of templates.
- Click on the template's three-dot menu (Actions) in the far-right column.



The **Delete Template** tab opens.



- Click on **Delete Template** to remove the selected template. You will be prompted before deleting the template.

Delete template

Are you sure you want to delete selected template?

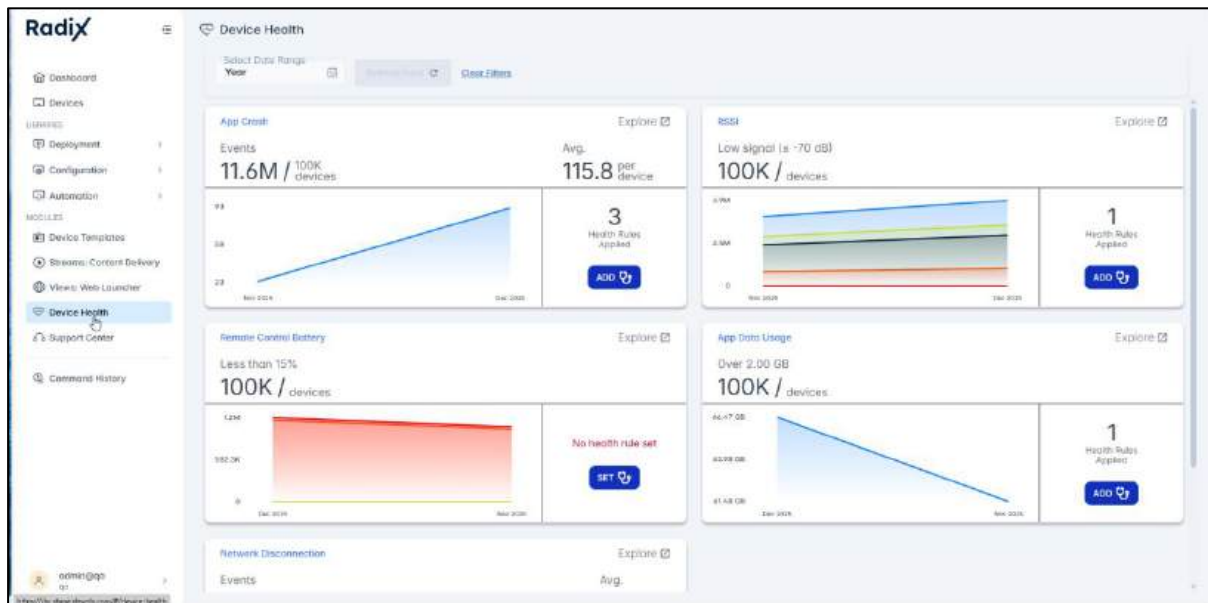
NO
YES

- Check **Yes** to delete the template. You will receive confirmation that the template has been deleted:



Chapter 9. Device Health Console

When you click on the **Device Health** icon in the Device Management platform sidebar menu, the following window opens:



There are two panes in the Fleet Health console: Device Health, and Incidents.

9.1 Device Health Pane

At the top of the Device Health pane, you have an option for selecting the range of dates over which to survey the health of the devices in your fleet. Options range from viewing data over the last 7 days to over the last year. You can also select a custom range of dates, to zero in on a particular time period.

Select Date Range

Quarter

Last 7 Days

Last 30 Days

Current Month

Last Month

Quarter

Half Year

Year

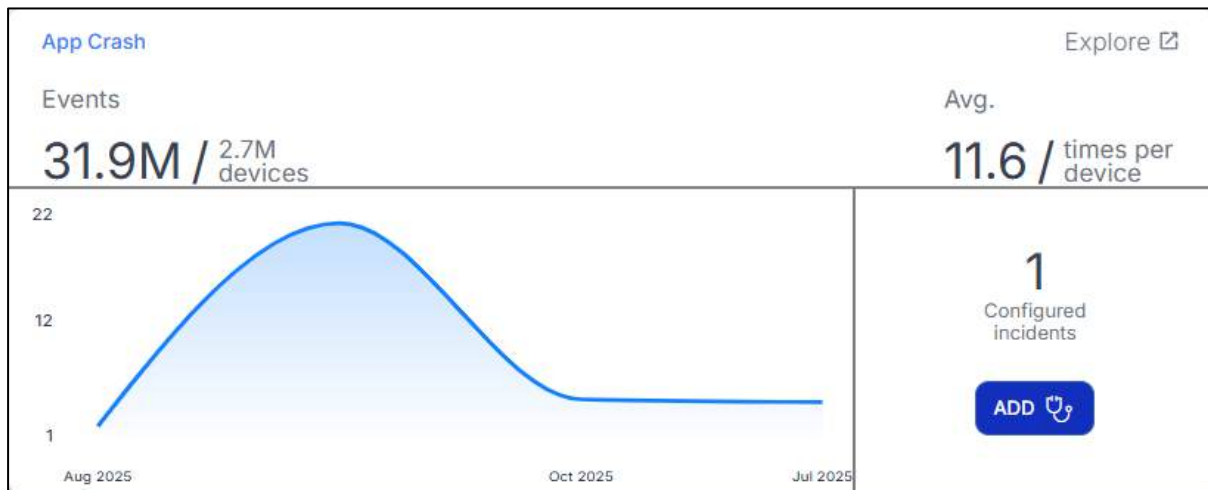
Custom

9.1.1 Device Health Graphs

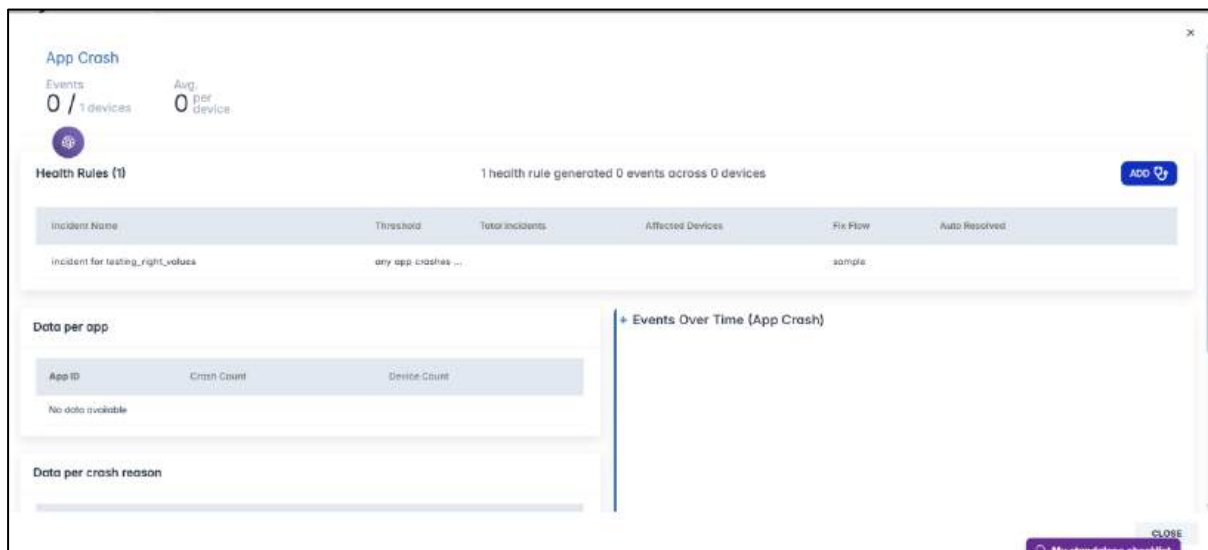
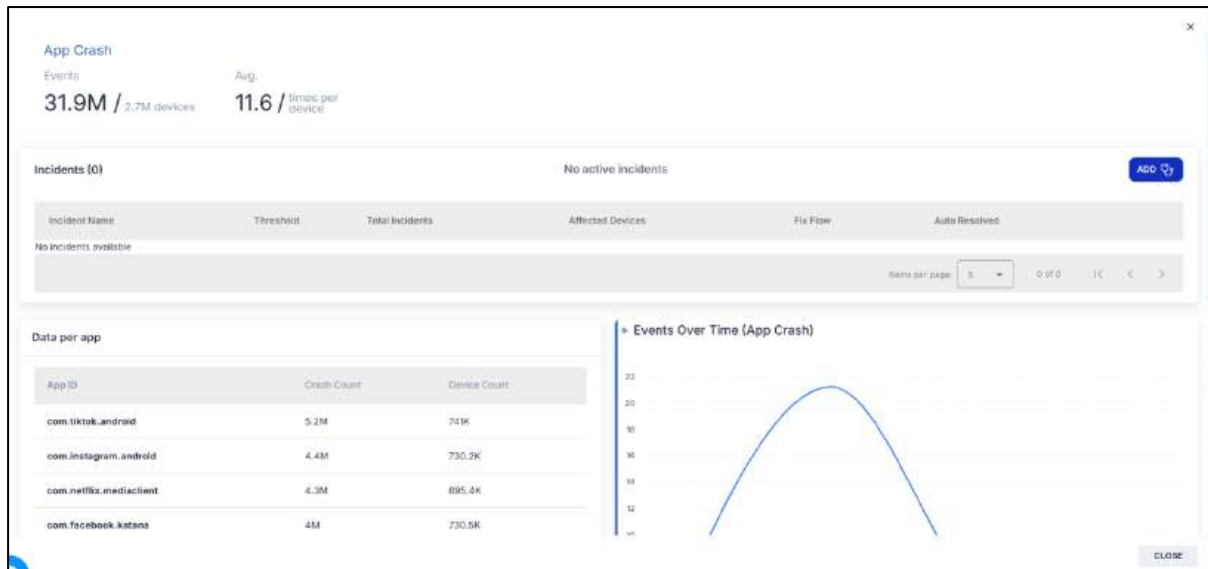
The Device Health Pane displays graphs of device health incidents over the date range you have specified. There are four health parameters:

9.1.1.1 App Crash

This displays the number of app crashes over the specified time period. It displays the number of devices which experienced an app crash, out of the total number of devices in the fleet, as well as an average of how many apps crashed on each device.



When you click **Explore**, the following window opens:



When you click **Add** , the **App Crash Rule** window opens which allows you to assign threshold values:

App Crash Rule

Rule | Population | Summary

Threshold & Remediation
Define when the rule triggers and what happens

Event Type:

Threshold: | Limit:
number of crashes | time from the first to the last crash

Require User Approval: ☐

Message:

Remediation:

In the Rule tab, you can define:

- the event that you wish to track,

- the threshold value of the number of crashes,
- the time from the first to last crash, in the form of HH:MM, and
- a message you would like to display to the user in the event of excessive app crashes,
- the device's reaction, by initiating a workflow.

App Crash Rule

Rule

Threshold & Remediation

Define when the rule triggers and what happens

Event Type
com.google.android.youtube.tv

Threshold
number of crashes

HH:mm
time from the first to the last crash

Require User Approval

Message
The YouTube app is experiencing technical difficulties.

Remediation
SELECT WORKFLOW

View summary **Save**

In the **Event Type** textbox, you select the app that you wish to track. In the example below, we chose the YouTube app:

In the **Threshold** textbox, you enter the number of app crashes which will trigger a warning response.

In the **Time for the first to the last crash** box, enter the time duration from the first to the last app crash, in the form HH:MM.

App Crash Rule

Rule

Threshold & Remediation

Define when the rule triggers and what happens

Event Type
com.google.android.youtube.tv

Threshold
number of crashes

HH:mm
time from the first to the last crash

Require User Approval

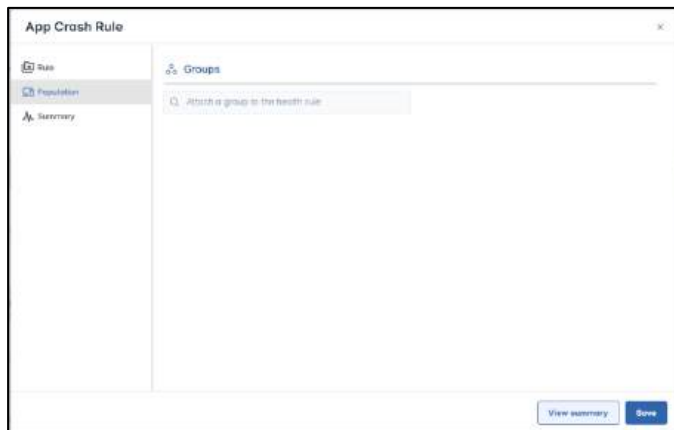
Message
The YouTube app is experiencing technical difficulties.

Remediation
SELECT WORKFLOW

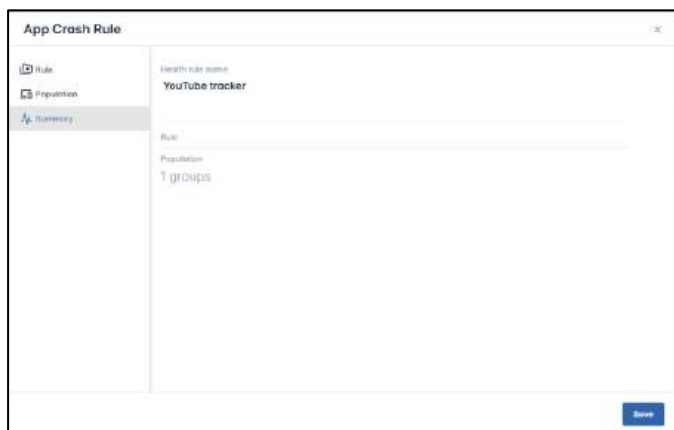
View summary **Save**

Click on the **Select Workflow** button to choose a workflow to resolve the issue.

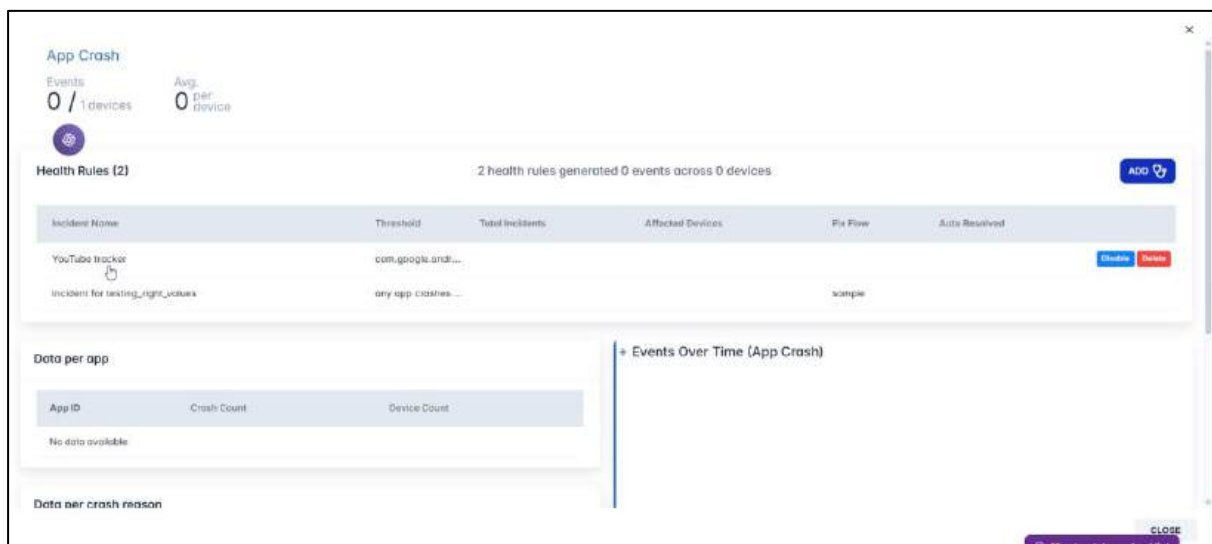
In the **Population** tab, you can specify the group of devices for which you wish to set a threshold.



When you click on the Summary tab, you can assign a name to the health rule:



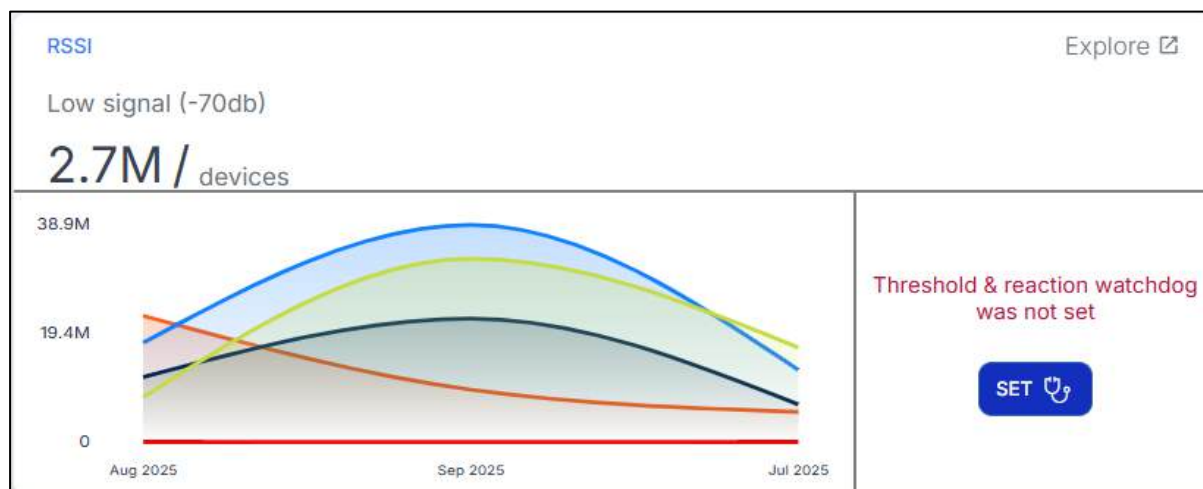
When you click **Save**, the incident will be saved in the list of incidents to be reported:



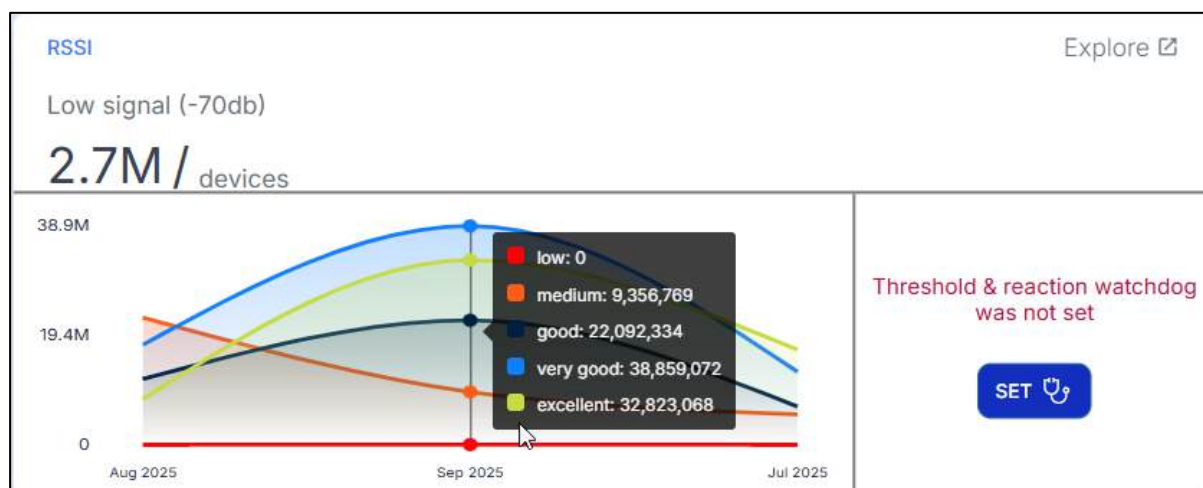
9.1.1.2 RSSI

This measures the Received Signal Strength Indicator (= RSSI) percentage.

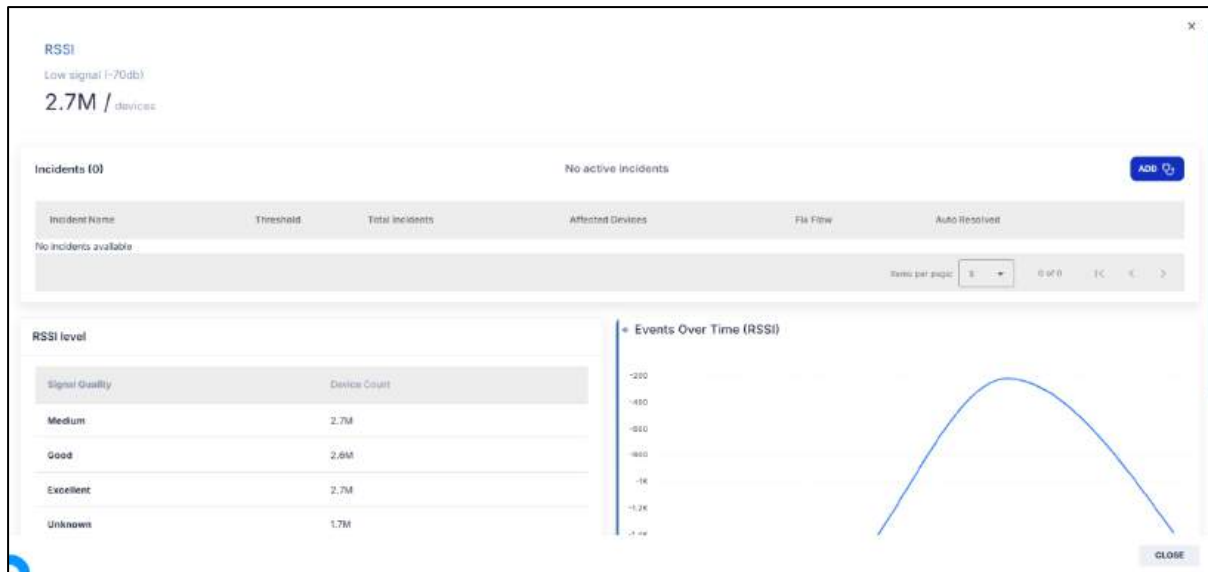
This sets a threshold for the Received Signal Strength Indicator (=RSSI) of the Wi-Fi signal received by a remote device in decibel-milliwatts. In the example below, an alert is created if the Wi-Fi signal drops below 70 dBm five times a day or more.



As you drag the mouse pointer over the graph, you will get a detailed breakdown of the RSSI values:



When you click **Explore**, the following window opens:



When you click **Add**, a window opens which allows you to assign the RSSI threshold. When you click on the **Rule** icon in the sidebar menu, you can assign the threshold values:

RSSI Rule

Rule

Threshold & Remediation

Define when the rule triggers and what happens

Threshold: HH:mm

DB (less than) 0--100

Duration since the RSSI got lower than

Require User Approval

Message

Message body

Remediation

SELECT WORKFLOW

View summary **Save**

When you click on the **Summary** icon in the sidebar menu, you can assign a name to the RSSI rule:

The screenshot shows the 'RSSI Rule' configuration window with the 'Summary' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The main content area displays the following fields:

- Health rule name:** A text input field.
- Rule:** A text input field.
- Population:** A text input field showing '0 groups'.

A 'Save' button is located at the bottom right of the window.

In the **Population** tab, you can specify the group of devices for which you wish to set a threshold.

The screenshot shows the 'RSSI Rule' configuration window with the 'Population' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The main content area displays the following fields:

- Groups:** A section with a search bar labeled 'Attach a group to the health rule' and a search icon. Below the search bar, a group named 'aep' is listed with the description 'just for HA195F3Y' and tags 'Tags: -aep'.

At the bottom right, there are two buttons: 'View summary' and 'Save'.

In the **Rule** tab, you can define:

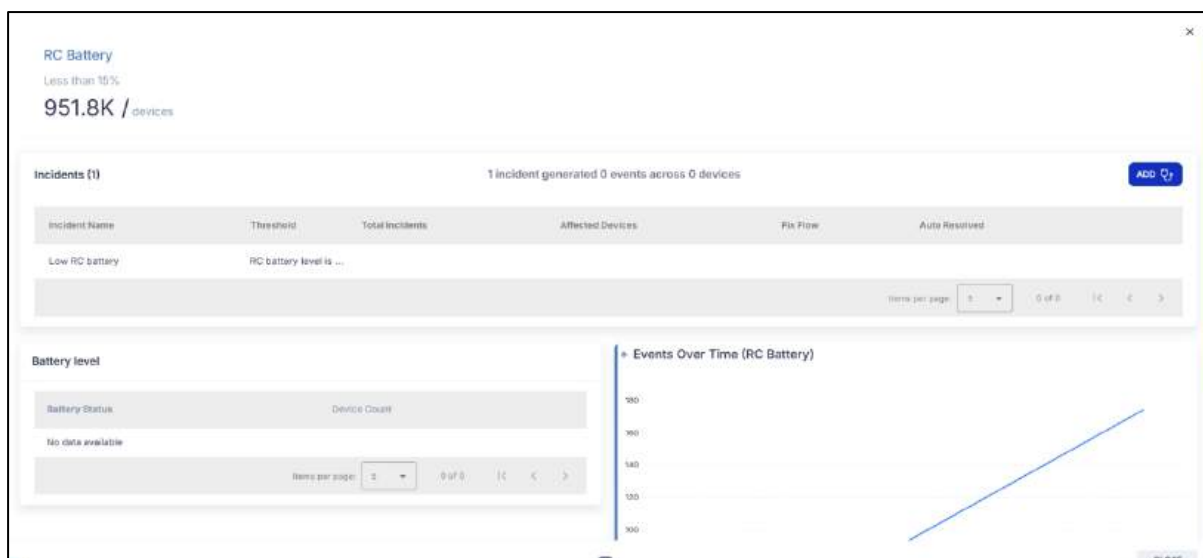
- the threshold value of the RSSI value,

- the duration of time from that the RSSI level went below the threshold, in the form of HH:MM, and
- the device's reaction, by supplying a text message to be displayed to the user, as well as a workflow of commands.

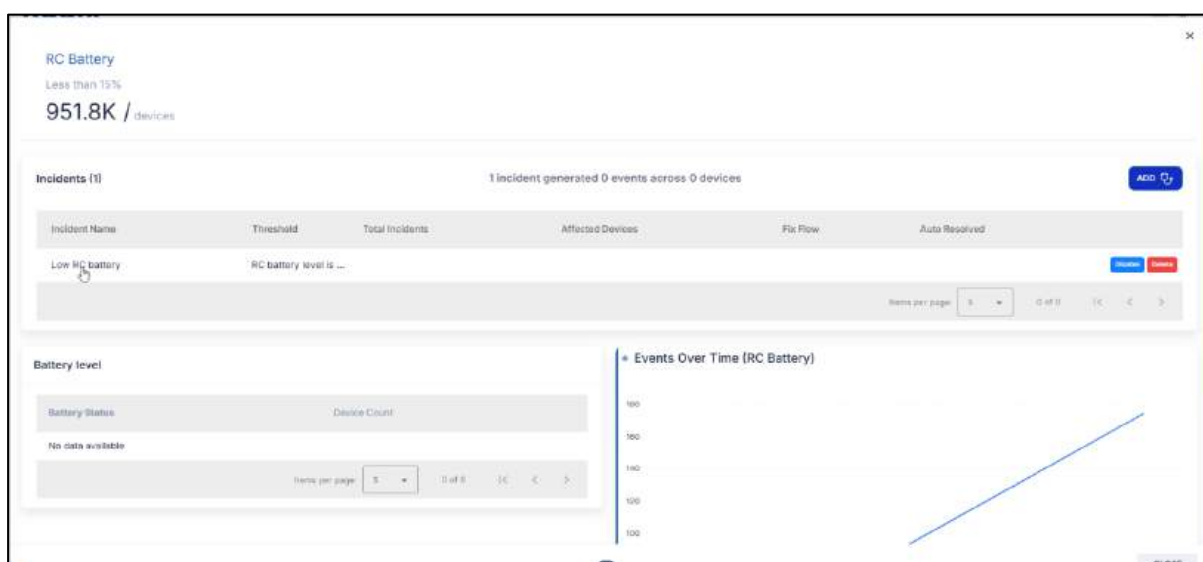
9.1.1.3 Remote Control battery

This monitors the lowest battery percentage on the remote devices. You supply a battery threshold level in the **Threshold** window. In the below example, a message will be sent to the Radix Device Management Platform if the battery level on a device drops below 15%.

When you click on **Explore**, the following window opens:



When you click on the row of the Low RC battery incident, the following interface opens:



The screenshot shows the 'Remote Control Battery Rule' configuration window with the 'Threshold & Remediation' tab selected. The left sidebar contains three tabs: 'Rule' (active), 'Population', and 'Summary'. The main content area is titled 'Threshold & Remediation' and includes the instruction 'Define when the rule triggers and what happens'. It features an 'Event Type' dropdown menu, a 'Threshold' input field, and a 'HH:mm' time input field. Below these are checkboxes for 'Require User Approval' and a 'Message' section with a 'Message body' text area. A 'Remediation' section contains a blue 'SELECT WORKFLOW' button. At the bottom right, there are 'View summary' and 'Save' buttons.

The **Summary** tab displays the name of the incident, the Watchdog level for the RC battery level, and the number of groups which have been associated with this threshold level.

The screenshot shows the 'Remote Control Battery Rule' configuration window with the 'Summary' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary' (active). The main content area displays the 'Health rule name' as 'Low battery levels'. Below this, it shows the 'Rule' and 'Population' sections, with the population count listed as '1 groups'. A blue 'Save' button is located at the bottom right.

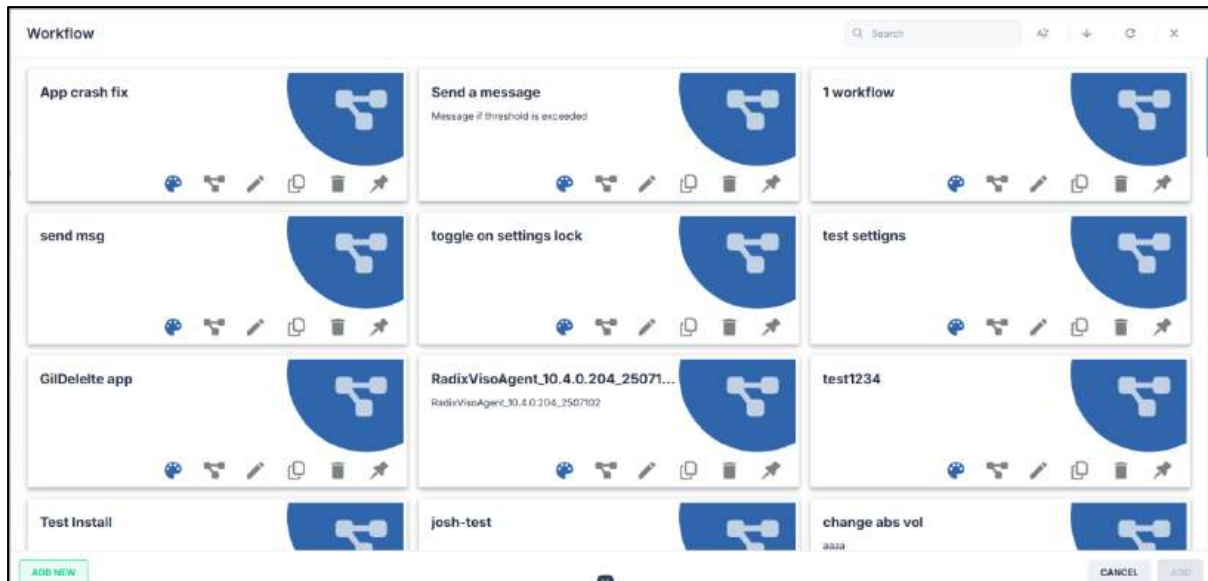
The **Population** tab will display the groups included in the RC battery incident:

The screenshot shows the 'Remote Control Battery Rule' dialog box with the 'Groups' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The 'Groups' tab on the right has a search bar with the placeholder text 'Attach a group to the health rule'. Below the search bar, a group named 'aep' is listed with an eye icon and a trash icon. At the bottom right, there are two buttons: 'View summary' and 'Save'.

When you click on the **Rule** tab, you open a pane which allows you to set the battery threshold level, the duration of time that the battery level must drop below this level for the incident to be reported, and a message that will be displayed to the remote user when their device's battery level drops below the threshold.

The screenshot shows the 'Remote Control Battery Rule' dialog box with the 'Rule' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The 'Rule' tab on the right is titled 'Threshold & Remediation' and contains the following fields: 'Event Type' (a dropdown menu), 'Threshold' (a text box with the value '85'), 'Period' (a text box with the value '03:02'), 'Require User Approval' (a checkbox), 'Message' (a text box with the value 'RC battery is running low.'), and 'Remediation' (a button labeled 'SELECT WORKFLOW'). At the bottom right, there are two buttons: 'View summary' and 'Save'.

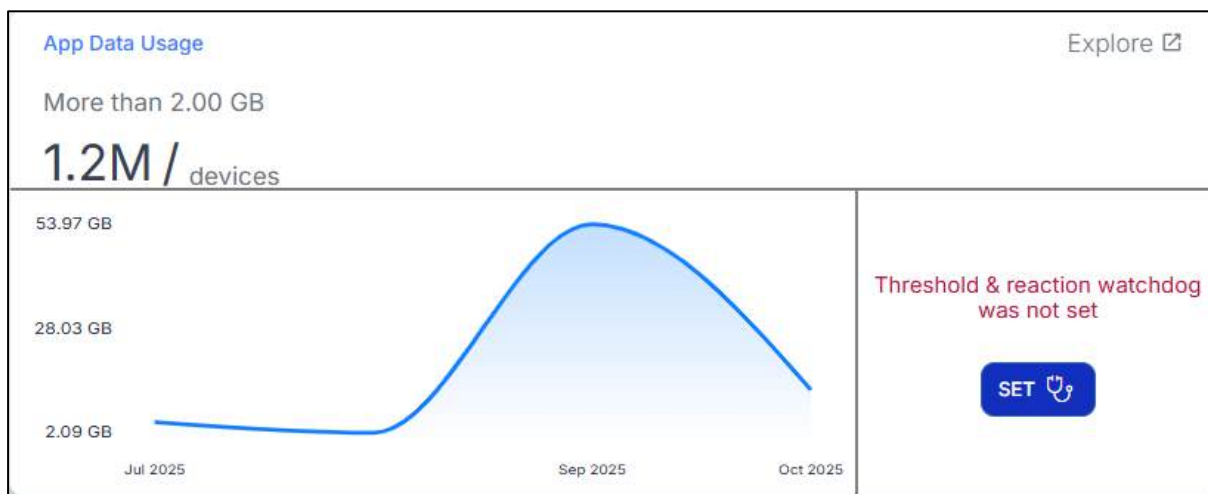
If you click on **Select Workflow**, you can create a workflow of commands to be executed when the RC Battery drops below threshold:



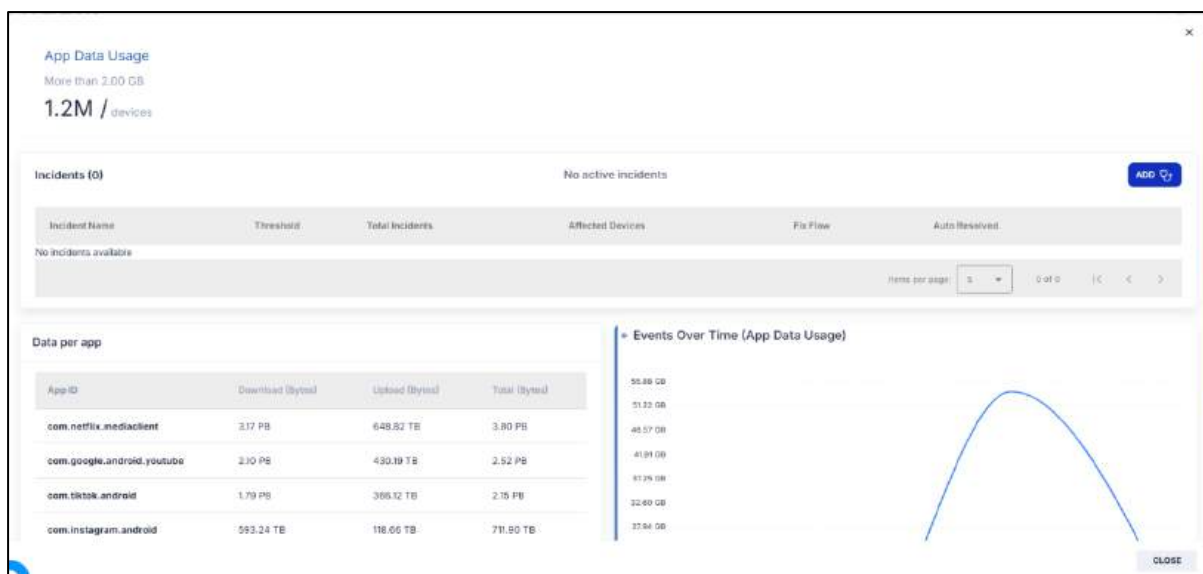
9.1.1.4 App Data Usage

This tracks application data usage per device.

This setting will send a message to the Device Management Platform if the data usage on a device exceeds a threshold amount. In the example below, the threshold was set at 1024 MB per day.



When you click **Explore**, the following window opens:



When you click **Add**, a window opens which allows you to assign a threshold:

App Data Usage incident

Overview

Incident name

Watchdog

Population

0 groups

SAVE

In the **Summary** pane, you assign a name to the incident:

The screenshot shows the 'App Data Usage Rule' dialog box with the 'Summary' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The 'Summary' tab is highlighted. The main area displays the 'Health rule name' as 'App Data Usage Threshold'. Below this, there are two empty text input fields labeled 'Rule' and 'Population'. The 'Population' field shows '0 groups'. A 'Save' button is located at the bottom right.

In the **Population** tab, you can specify the group of devices for which you wish to set a threshold.

The screenshot shows the 'App Data Usage Rule' dialog box with the 'Population' tab selected. The left sidebar contains three tabs: 'Rule', 'Population', and 'Summary'. The 'Population' tab is highlighted. The main area displays the 'Groups' section with a search bar labeled 'Attach a group to the health rule'. Below the search bar, there is a list of groups: 'All' (All account devices), 'New devices' (Tags: new), 'O F' (Tags: new), 'O longops 1' (Tag: new), and 'O longops 2'. A 'View summary' button and a 'Save' button are located at the bottom right.

In the **Rule** tab, you can define:

- the event that you wish to track,
- the amount of data usage by that app in MB,

- the duration of time from that the app data usage level went above the threshold, in the form of HH:MM, and
- the device's reaction, by initiating a workflow.

App Data Usage Rule

Rule

Population

Summary

Threshold & Remediation

Define when the rule triggers and what happens

Event Type

Threshold

HH:mm

amount of data usage in MB (aggregated)

Require User Approval

Message

Message body

Remediation

SELECT WORKFLOW

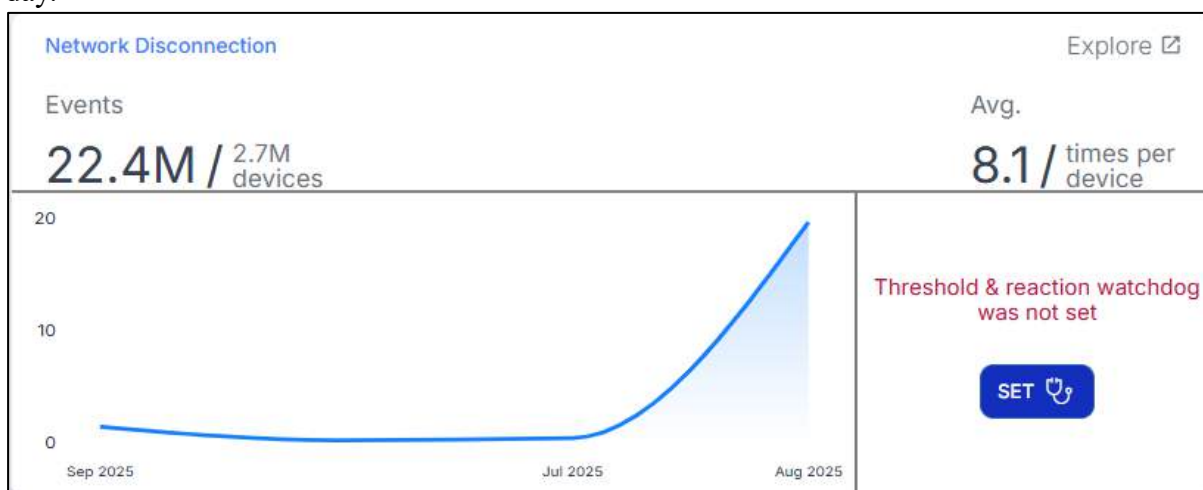
View summary

Save

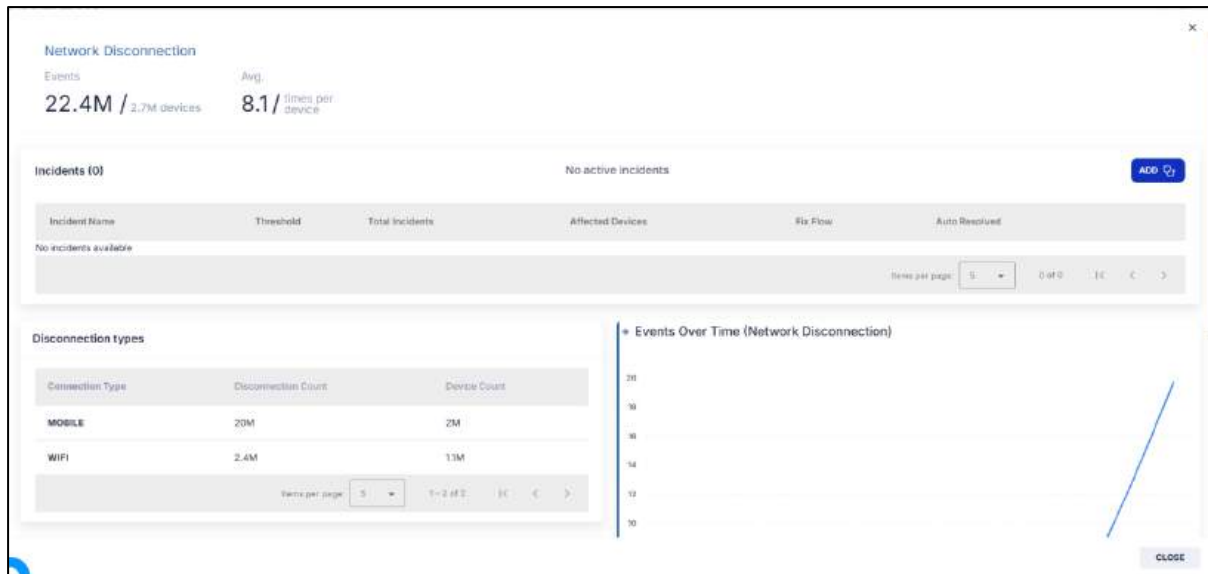
9.1.1.5 Network Disconnection

This counts the number of network disconnections per device.

This sends a notification if the remote device disconnects from its Wi-Fi network more than the threshold value. In the example below, the system will send the Device Management platform a message if a remote device disconnects from the network more than 10 times per day.



When you click **Explore**, the following window opens:



When you click **Add**, a window opens which allows you to assign a threshold:

Network Disconnection Rule

Rule | **Population** | **Summary**

Health rule name:

Rule:

Population:

0 groups

Save

In the **Summary** pane, you assign a name to the incident:

Network Disconnection Rule

Rule

Population

Summary

Health rule name

Network Disconnection Incident Example

Rule

Population

0 groups

Save

In the **Population** tab, you can specify the group of devices for which you wish to set a threshold.

Network Disconnection Rule

Rule

Population

Summary

Groups

Attach a group to the health rule

View summary Save

In the **Rule** tab, you can define:

- the event that you wish to track,
- the amount of data usage by that app in MB,

- the duration of time from that the app data usage level went above the threshold, in the form of HH:MM, and
- the device's reaction, by initiating a workflow.

Network Disconnection Rule

Rule

Population

Summary

Threshold & Remediation

Define when the rule triggers and what happens

Event Type

Threshold

HH:mm

number of disconnections

time from the first to the last disconnection

Require User Approval

Message

Message body

Remediation

SELECT WORKFLOW

View summary

Save

Network Disconnection incident

Overview

Population

Watchdog

Threshold & Reaction

Define the threshold and reaction for that issue

Sub-event

☐
☐ lan
 ☐ wifi
 ☐ mobile

HH:mm

time from the first to the last disconnection

Reaction

SELECT WORKFLOW

VIEW OVERVIEW

SAVE

Network Disconnection incident

Overview

Population

Watchdog

Threshold & Reaction

Define the threshold and reaction for that issue

Sub-event

wifi

Threshold

100

number of disconnections

Period

03:03

time from the first to the last disconnection

Reaction

SELECT WORKFLOW

Send a message

VIEW OVERVIEW

SAVE

Chapter 10. Command History Log

The **Command History Log** allows you to look at the status of all or some of the commands executed on a particular device. Also, you can view the execution of a particular command on a group of devices.

Type	Description	Command	Group	Owner	Creation time	Total
WiFi	rdxga - Send message	Send message		api@qga	Oct 10, 2025, 2:54:24 PM	1
WiFi	rdxga - Send message	Send message		api@qga	Oct 10, 2025, 2:54:06 PM	1
WiFi	Exit Office Wi-Fi - Shutdown	Shutdown		lor@qga	May 14, 2025, 5:49:38 PM	1
WiFi	Exit Office Wi-Fi - Send message	Send message		lor@qga	May 14, 2025, 5:38:03 PM	1
WiFi	Exit Office Wi-Fi - Send message	Send message		lor@qga	May 14, 2025, 5:35:42 PM	1
WiFi	Exit Office Wi-Fi - Send message	Send message		lor@qga	May 14, 2025, 5:30:45 PM	1
WiFi	Exit Office Wi-Fi - Send message	Send message		yehuda@qga	May 14, 2025, 4:38:36 PM	1
WiFi	Exit Office Wi-Fi - Send message	Send message		yehuda@qga	May 14, 2025, 4:37:10 PM	1
WiFi	Exit Office Wi-Fi - Shutdown	Shutdown		yehuda@qga	May 14, 2025, 4:28:31 PM	1
WiFi	Exit Office Wi-Fi - Shutdown	Shutdown		yehuda@qga	May 14, 2025, 4:22:57 PM	1
WiFi	WiFi auto jax - printer24 - Advanced messaging	Advanced messaging		elie@azure_cad-radix-int.com@qga	Feb 25, 2025, 11:59:56 AM	1

Figure 10-1: You can access the Command History Log via the Commands icon in the Overview Dashboard

10.1 Types of Commands in the Command History Log

In the **Type** column in the Command History Log, you will see several types of commands. The Wi-Fi, Startup, and Schedule commands are all arranged by means of the **Scheduler and Trigger** option (see **Section 6.1.26**), while an Ad-Hoc command is sent via the other Radix Device Management Platform command options.

Icon	Description
 Ad-Hoc	Commands that are sent to a device on a one-time basis.
 WiFi	Commands that are executed when the device enters or exits a specific Wi-Fi network.
 Startup	Commands that are scheduled to be executed when the device starts up.
 Schedule	Commands that are executed according to a defined schedule. The schedule is set by means of the Timing option in the Scheduler and Trigger command.

10.2 Command Search Options

You can search for commands either by:

- The description of the command, as displayed in the Description column,
- The Device ID,
- The type of command, (from the list of command options), or
- The trigger name.

Note: If you search by Device ID, you must supply the entire Device ID. Also, the search is case-sensitive. Therefore, when looking for device “HA195F3Y”, be certain to use capital letters.

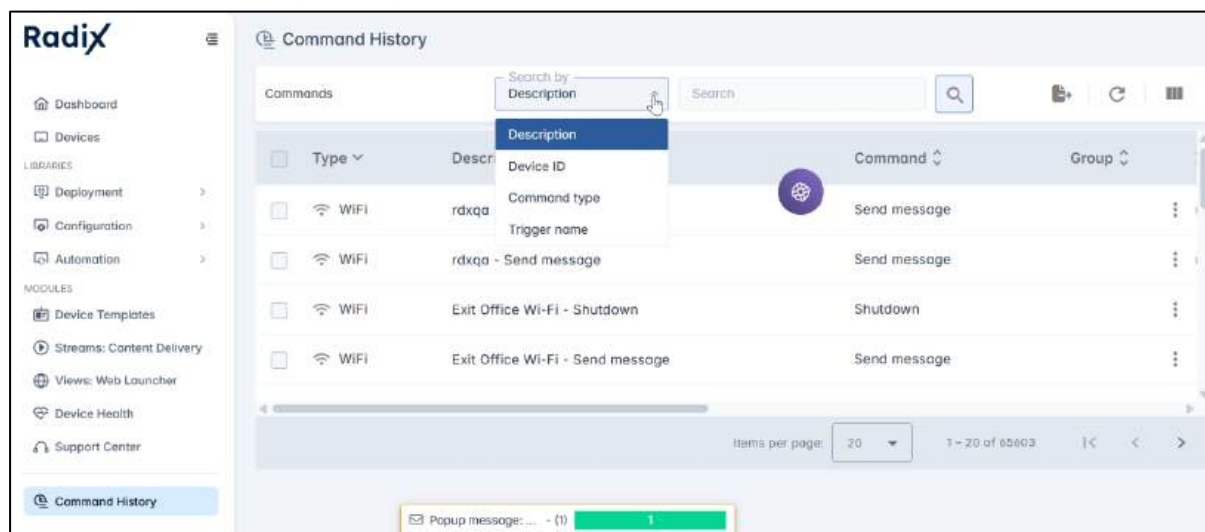


Figure 10-2: Various search criteria for commands

10.3 Viewing the Status of a Particular Command

You can select a particular command by checking the command’s checkbox in the far-left column. By clicking on the selected row, you can then view the command status: whether it was executed successfully, unsuccessfully, or is still pending.

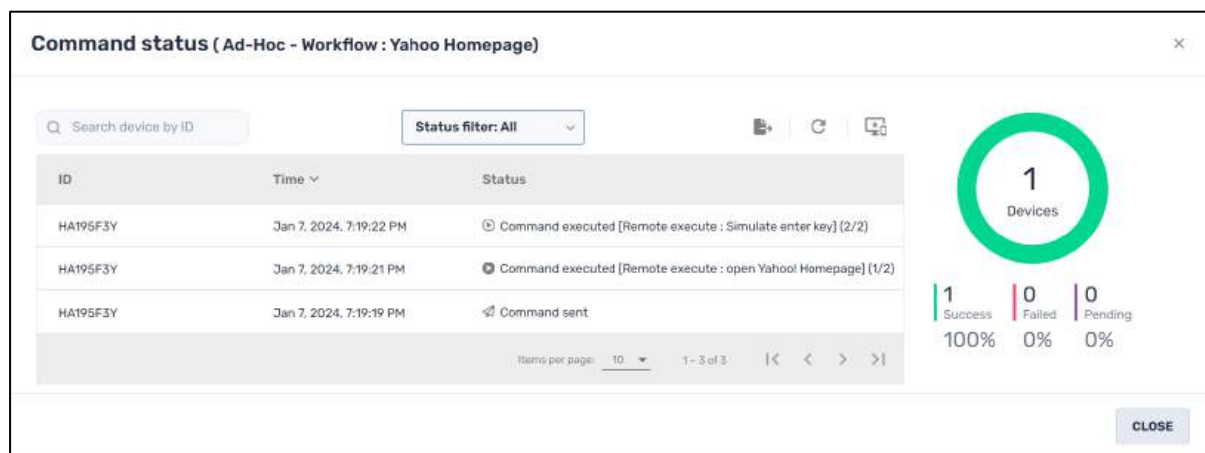


Figure 10-3: Command status of a "Successful" command

If you send a command to an entire fleet of devices, the Command Status Pane will display all the devices which have received the command. If you wish to filter the results, you can filter the results with the Status filter:

- **All:** Displays the status of all commands sent to the device: when they were sent, when they were executed, etc.
- **Sent:** Displays only commands that were sent to the device.
- **Pending:** Displays commands that were sent to a device that was offline and are waiting to be executed.

- **Executed:** Displays only the commands that were executed successfully.
- **Failed:** Displays commands that failed to execute.
- **Step done:** In an instance where a sequence of commands was to be performed in a workflow, displays the steps that were executed successfully.
- **Step failed:** In an instance where a sequence of commands was to be performed in a workflow, displays the steps that failed to execute.
- **Ready:** Lists commands that are ready to be executed—for example, commands that are activated by a trigger.
- **Updated:** Provides an updated list of commands to be executed.

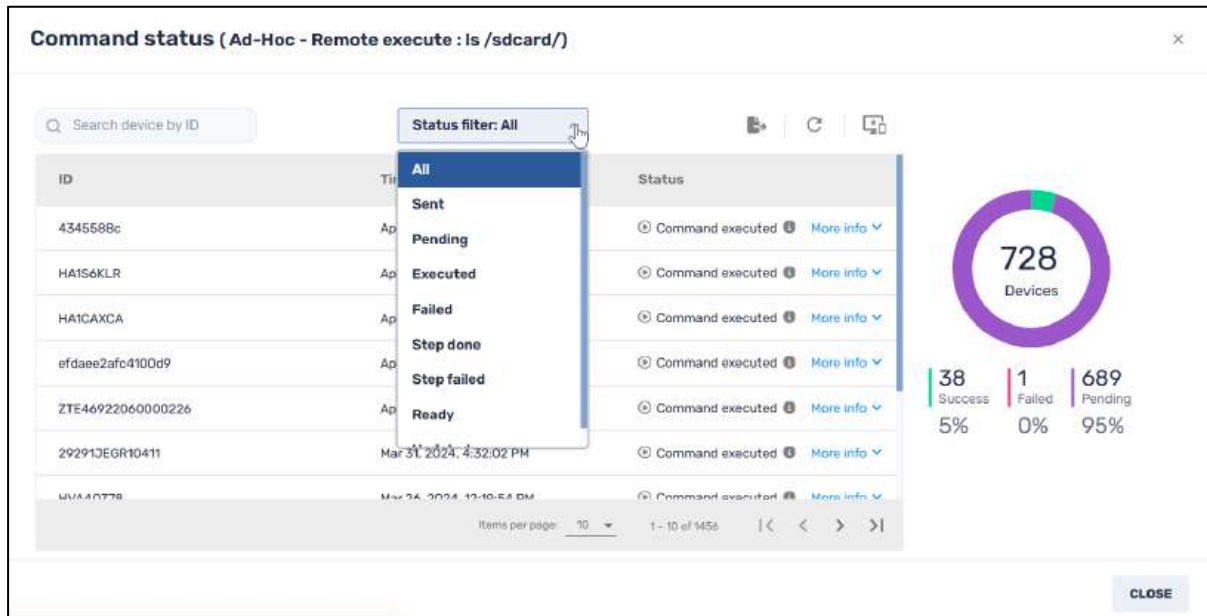


Figure 10-4: Command status window--Status Filter

The **Command Status Window** also allows you to view commands either by the device to which they were sent, or by the time of the command. This is especially useful when sending a series of commands to a fleet of devices.

There are three icons to the right of the Status filter bar:

Icon	Description
	Export to CSV: To export the search results in a CSV Excel file
	Refresh: To refresh the list of commands
	List by device/ List by Time: To display the commands by device, or by the time when they were sent.

You can toggle the display between listing the commands by the device to which they were sent, or by the time when the command was sent:

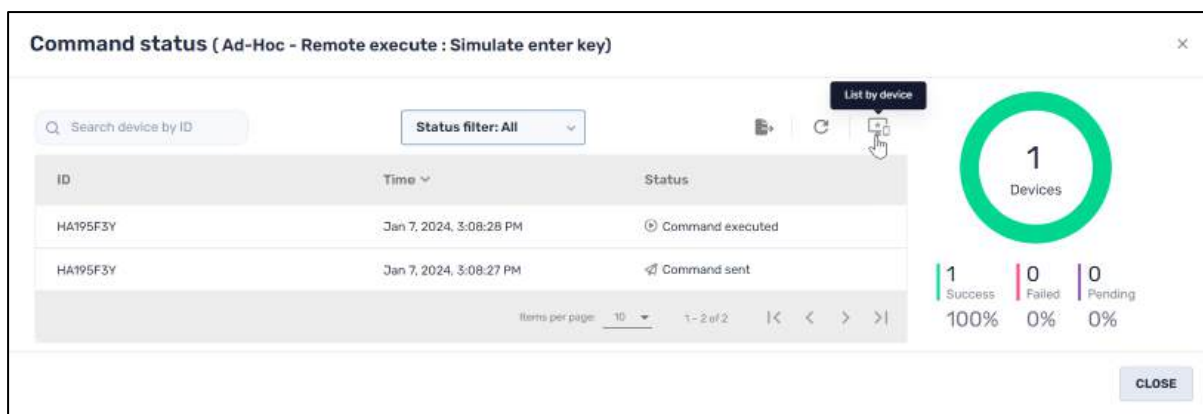


Figure 10-5: Commands listed by device

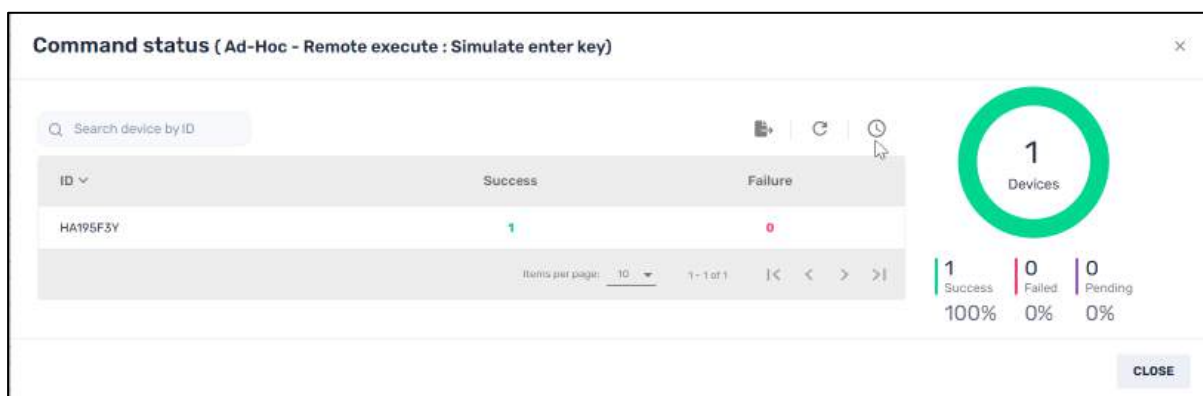


Figure 10-6: Commands listed by time sent

10.4 Executing Commands from the Command History Log

By clicking on the command's three-dot menu in the far-right column of the Command History Log you will see options to start, stop, edit, resend, or delete this command.

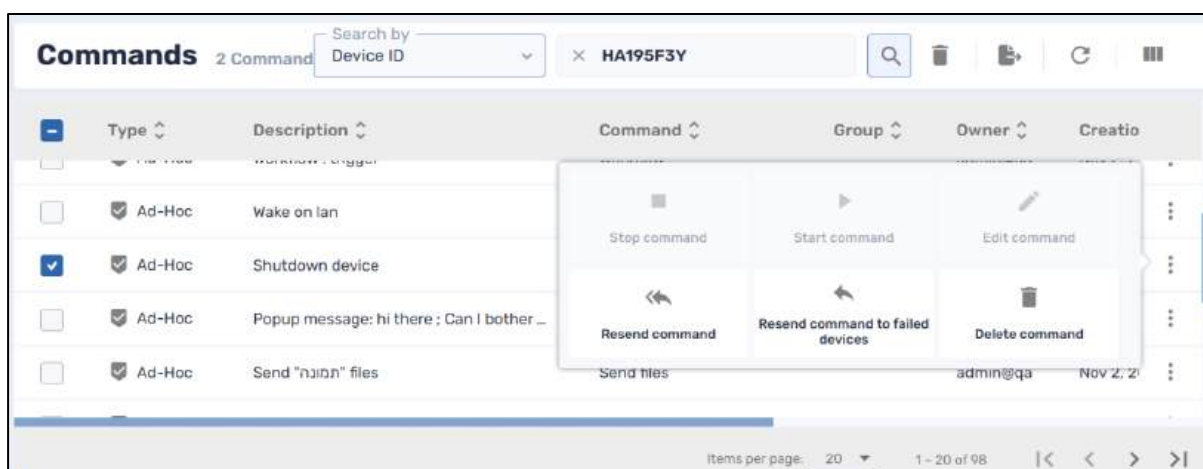


Figure 10-7: Options to start, stop, resend, or delete command

10.5 Use of the Persist Command for Groups

If you are performing commands on a group of devices, you will also have the **Persist** command. **Persistence** means that all the commands that are applied to the devices in a group will be applied to any devices that will be added to the group in the future.

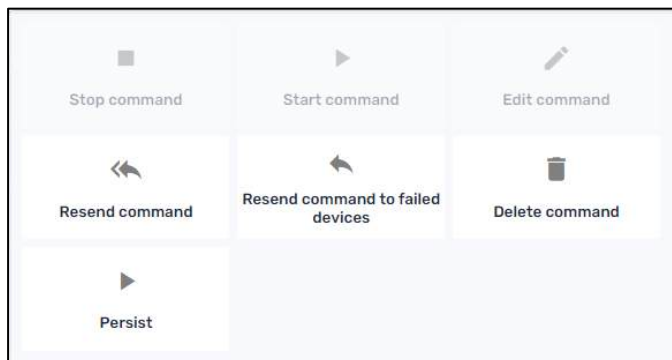
To employ persistence in a group:

1. Find the desired group in the Commands list and click on the group's three-dot menu.

☐	Ad-Hoc	Device settings : Screen configuration S...	Device settings	admin@gs	Nov 2, 2023, 2:43:10 PM	1	0	1	0	Nov 2, 2023, 3:46:4	⋮	
☒	Ad-Hoc	Popup message: Hi	Send message	New devices	admin@gs	Nov 6, 2023, 10:06:52 AM	260	34	0	226	Nov 8, 2023, 4:16:4	⋮
☐	Ad-Hoc	Send "audio" files	Send files	admin@gs	Nov 2, 2023, 1:29:04 PM	1	0	1	0	Nov 2, 2023, 1:29:0	⋮	
☐	Ad-Hoc	Device settings : wallpaper 17.05	Device settings	admin@gs	Nov 6, 2023, 11:09:31 AM	1	1	0	0	Nov 6, 2023, 11:09:	⋮	
☐	Ad-Hoc	Workflow : Elder_test	Workflow	admin@gs	Nov 2, 2023, 2:57:10 PM	1	0	0	1	Nov 2, 2023, 3:46:4	⋮	

The Commands options grid opens.

2. Select **Persist**.



You will be prompted if you want to employ persistence.

Persist

Are you sure you want to make command persistent?

NO YES

3. Click **Yes**. The command's icon will now change in color from blue to green, indicating that it will be applied with persistence. Any new devices that are added to the group will have the group's software apps installed on them automatically.

☐	Ad-Hoc	Device settings: Screen configuration S...	Device settings	admin@gs	Nov 2, 2023, 2:43:10 PM	1	0	1	0	Nov 2, 2023, 3:46:4	⋮	
☒	Ad-Hoc	Popup message: Hi	Send message	New devices	admin@gs	Nov 6, 2023, 10:06:52 AM	260	34	0	226	Nov 8, 2023, 4:16:4	⋮

4. If for some reason you wish to disable persistence, select a group with persistence, and select **Stop persistence** from its three-dot menu.

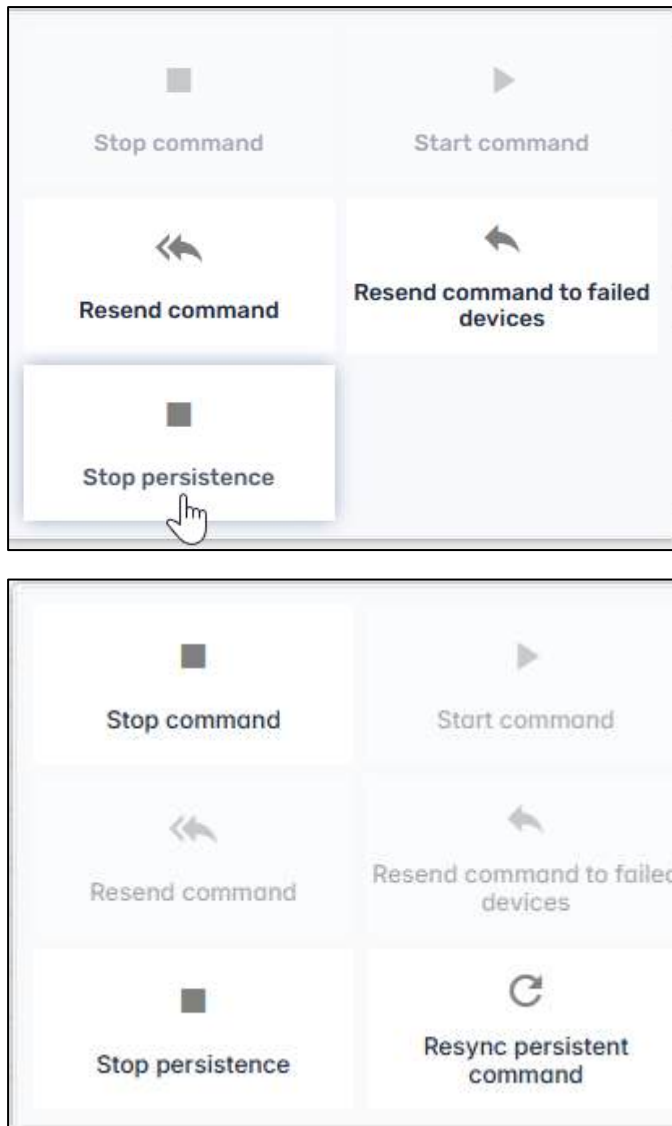


Figure 10-8: Stop Persistence option

5. You will be prompted if you wish to stop persistence. Click **Yes**.

Stop persistence

Are you sure you want to stop command persistence?

NO
YES

The color of the command's icon in the Command History Log will now revert from green to blue. This indicates that the command no longer has persistence.

Chapter 11. Further Resources

We have surveyed the main functions of the Radix Device Management MDM interface, giving brief examples of most of the commands and options. However, functionality may differ, depending on the user's device, OS version, and permissions.

Throughout the Radix MDM interface, you have the option of completing a Customer Request Form by clicking on the dialog bubble in the lower left of the screen. Enter your name, email, and a brief statement of your request, and we will provide a response via email.

The screenshot shows the Radix MDM interface with a Customer Request Form overlay. The form has a blue header with the text "Please fill out the form below and we will get back to you as soon as possible." Below the header are three input fields: "* Name", "* Email", and "* Message". A blue "Submit" button with a right-pointing arrow is at the bottom of the form. In the background, a table of device information is visible, including columns for "Name" and "ID". At the bottom of the screen, there is a blue circular button with a white 'X' and a status bar showing "Popup message: Hi - (266)" and two colored boxes with the numbers "226" and "40".

Figure 11-1: Customer Request Form

Besides the option to fill out a Customer Request Form, you can also register [here](#) for the Radix weekly webinar. The webinar is held every Monday and Wednesday at 3:00 AM EST/10:00 AM CET, and 10:00 AM EST/4:00 PM CET. You can also attend a live demo of the Radix MDM interface.

The [Radix website](#) also features a Virtual Assistant, so that you can engage in a live chat to step you through the product's capabilities.

Chapter 12. Appendices

Appendix A—Alphabetical List of Commands

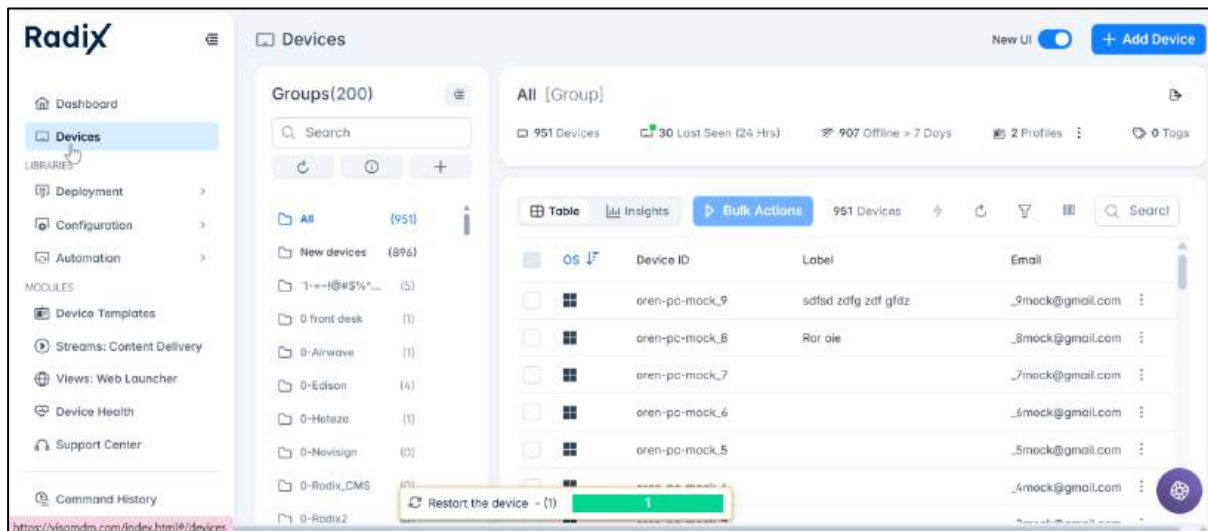
12.1 Methods of Accessing Commands

When using the Radix Device Management Platform, you will notice several ways of accessing a grid of commands that can be sent to either a single device, or to a group of devices. The “Commands Grid” contains many command options, arranged alphabetically. But the actual commands that are available will differ, depending on how you access the Commands Grid, or on the operating system of the device you are accessing.

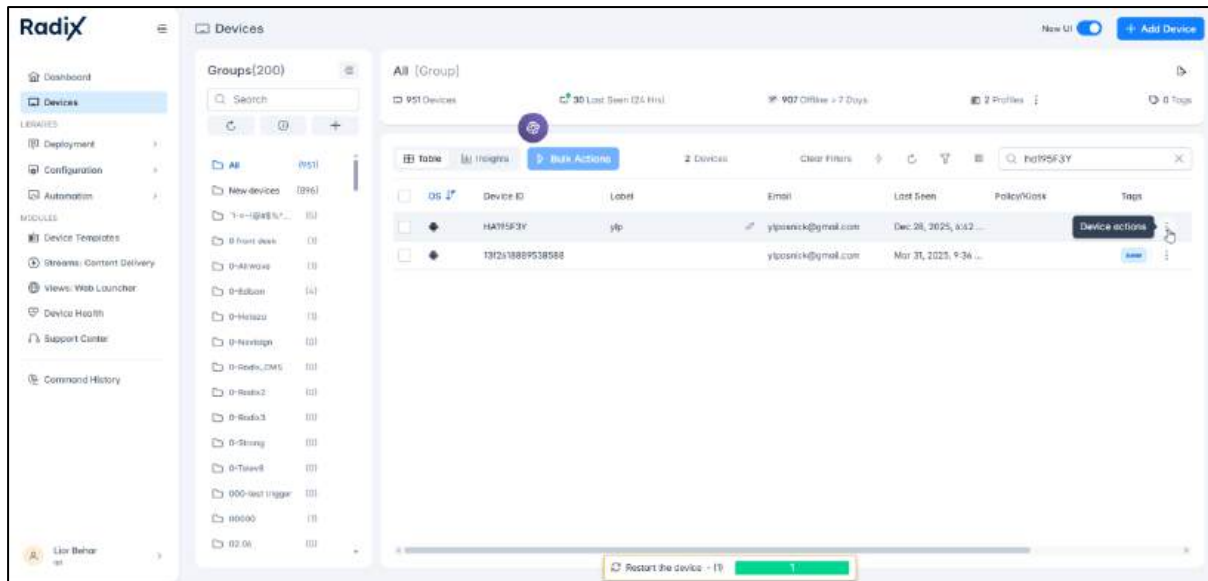
To access the Commands Grid from the Radix Device Management Dashboard:

Method 1: Via the device’s three-dot menu:

1. Click on the **Devices** icon  on the left side of the Dashboard.



2. Click on the three-dot menu on the far right-hand column of any of the devices listed.



A drop-down menu opens.

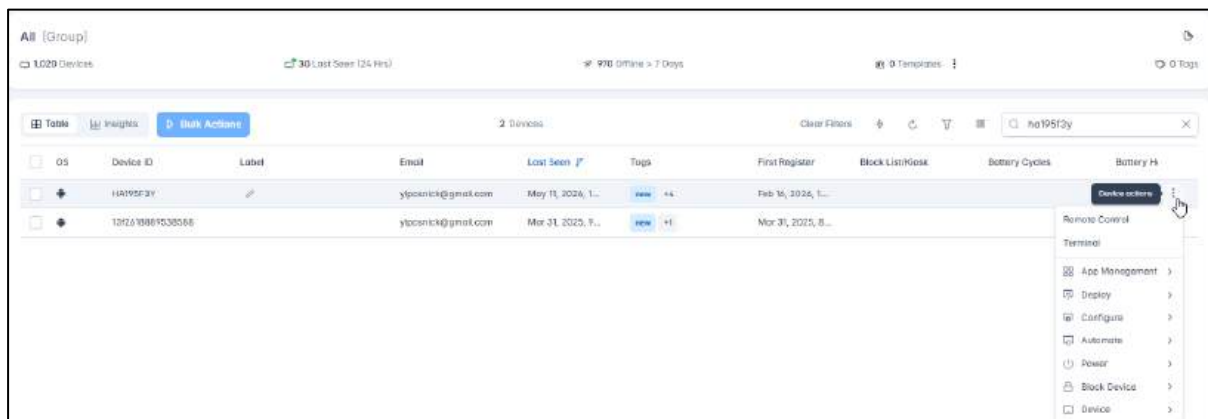
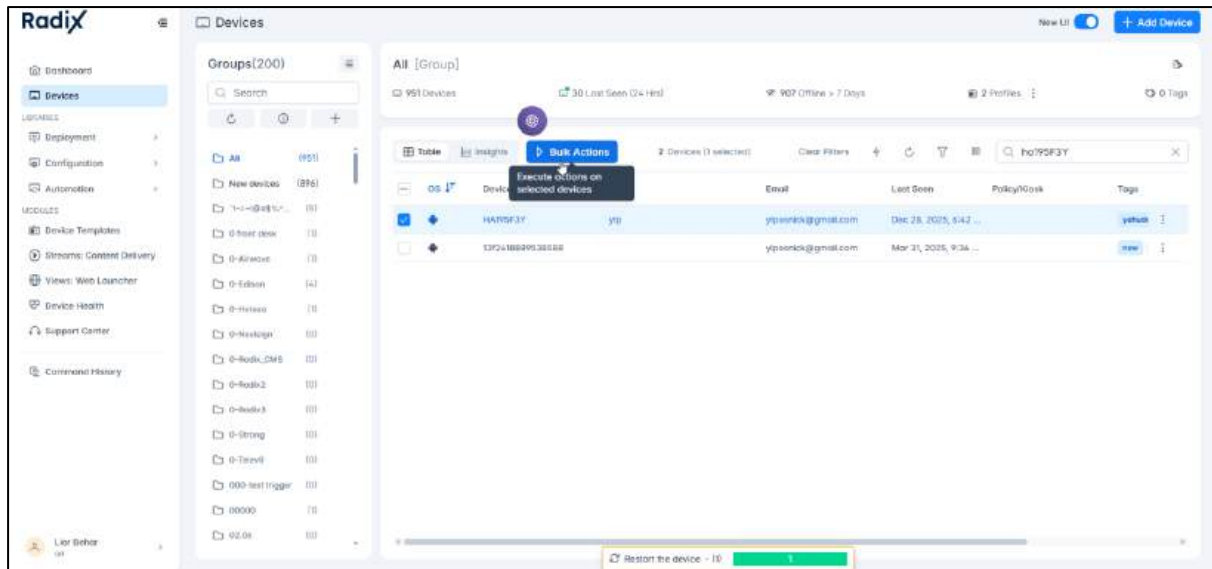


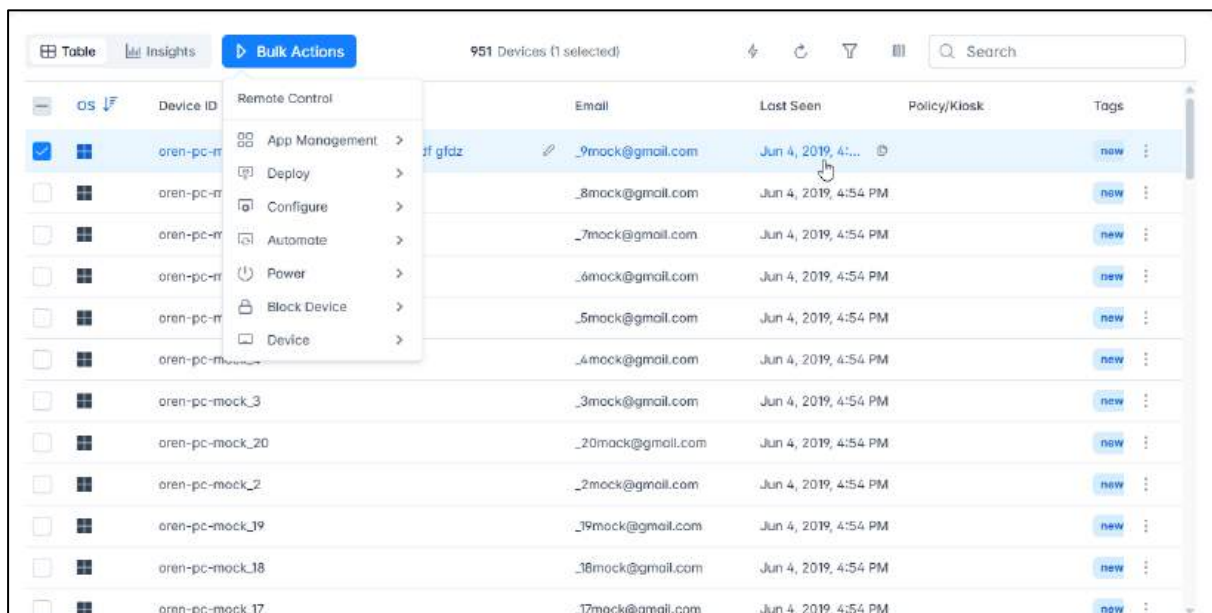
Figure 12-1: Commands menu as accessed from the device's three-dot menu

Method 2: From the Bulk Actions button:

1. Click on the **Devices** icon  on the left side of the Dashboard.
2. In the list of devices, select a particular device (or devices) by checking its checkbox in the far-left column. The **Bulk Actions** button becomes active.



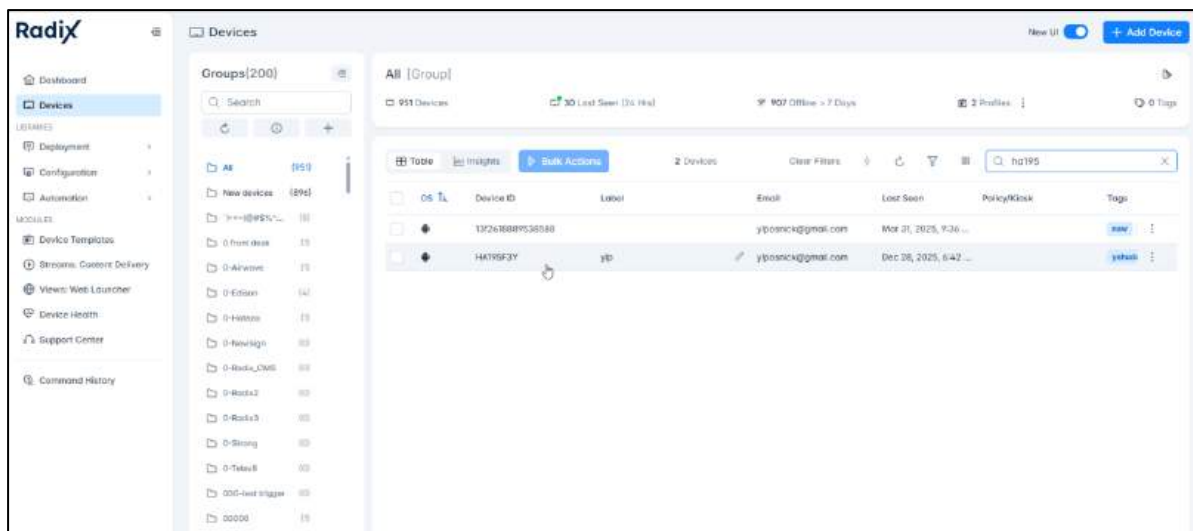
3. By clicking on the **Bulk Actions** button, you can access many other commands in the drop-down menu:



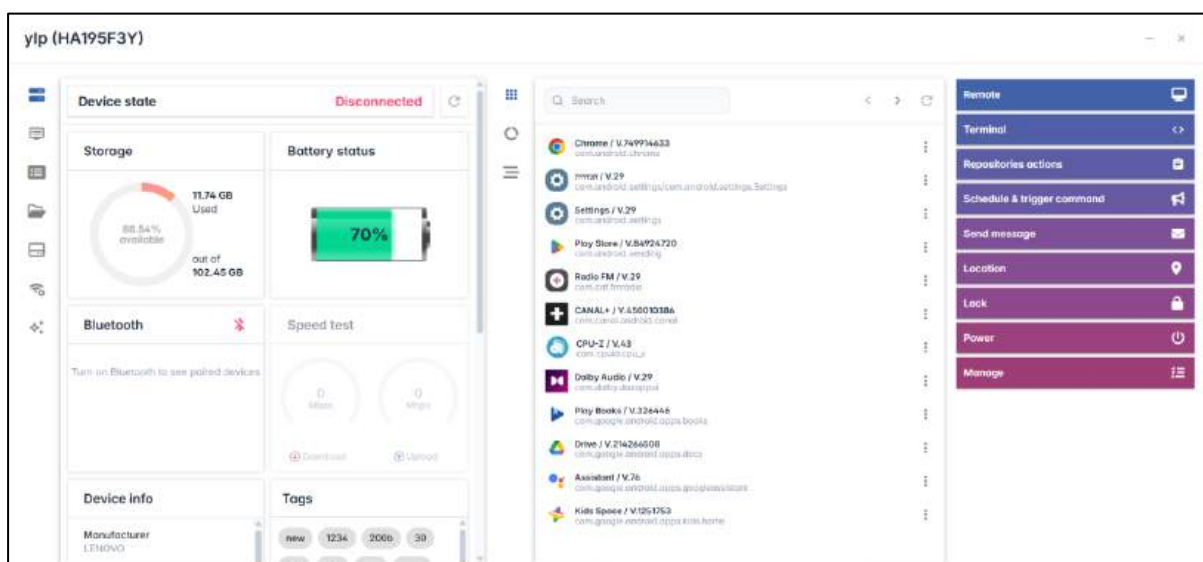
Method 3: From the Device Dashboard:

The Device Dashboard will allow you to access a sizeable number of the available commands.

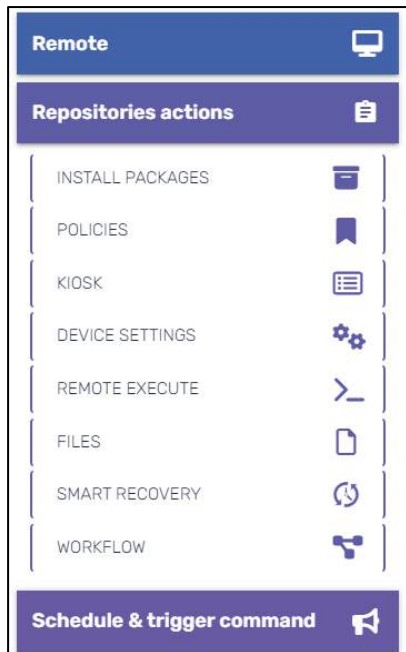
1. Click on the **Devices** icon  on the left side of the Dashboard.
2. Click on the row of any of the devices listed.



3. The **Device Dashboard** pops up.



4. The right-hand pane will allow you access to many of the available commands, especially under the **Repositories actions** tab.



Here is a brief reference for accessing all the commands:

12.1.1 Advanced messaging

- **Function:** This allows you to interact with users using an engaging message that can contain text, sound, or images.
- **Access:** The Advanced Messaging feature can be accessed by:
 - The **device's three-dot menu**>**Deploy**>**Messaging**,
 - The **Bulk Actions button**>**Deploy**>**Messaging**,
 - The Device Dashboard, under **Repositories actions**>**Advanced messaging**.
- **Further Details:** This is discussed in detail in **Section 6.1.1, Advanced Messaging**.

12.1.2 AFW Install/Uninstall

- **Function:** This allows you to install or uninstall the Android for Work option on your device.
- **Access:** The AFW Install/Uninstall feature can be accessed by:
 - The **device's three-dot menu**>**App Management**>**AFW Install/Uninstall**,
 - The **Bulk Actions button**>**App Management**>**AFW Install/Uninstall**,
 - The Device Dashboard> **AFW Install/Uninstall**
- **Further details:** This is discussed in detail in **Section 6.1.2, Android for Work (AFW) install/uninstall**.

12.1.3 Block Lists (Policies)

This is treated under Policies (**Section 12.1.21, Policies**).

12.1.4 Change Agent Password

- **Function:** This allows you to change a user's password in the VISO agent app on the remote device.
- **Access:** The Change Agent Password feature can be accessed by:
 - The **device's three-dot menu**>**Device**>**Change Agent Password**,
 - The **Bulk Actions button**>**Device**>**Change Agent Password**,

- The Device Dashboard, under the **Manage** tab>**Change Agent Password**.
- **Further details:** This is discussed in detail in **Section 6.1.3, Change Agent Password**.

12.1.5 Clear apps cache

- **Function:** This is useful in situations where a specific app is malfunctioning or not performing as fast as you would expect. Clearing the app's cached data will free up some space in memory and improve performance.
- **Access:** The **Clear apps cache** command can be accessed from:
 - The **device's three-dot menu**>**Apps Management**>**Clear Apps Cache**,
 - The **Bulk Actions button**>**Apps Management**>**Clear Apps Cache**,
- **Further details:** This is discussed in detail in **Section 6.1.4, Clear Apps Cache**.

12.1.6 Clear apps data

- **Function:** This is useful in situations where an app is crashing or displaying other issues. It clears the user's history on the device and requires them to log in again. This typically will solve most performance issues.
- **Access:** The **Clear Apps Data** command can be accessed from:
 - The **device's three-dot menu**>**Apps Management**>**Clear Apps Data**,
 - The **Bulk Actions button**>**Apps Management**>**Clear Apps Data**.
- **Further details:** This is discussed in detail in **Section 6.1.5, Clear Apps Data**.

12.1.7 Collect system logs

- **Function:** This allows you to create a log file of activities performed on a remote device.
- **Access:** The **Collect logs** command can be accessed from:
 - The **device's three-dot menu**>**Device**>**Collect System Logs**,
 - The **Bulk Actions button**>**Device**>**Collect System Logs**.
- **Further details:** This is discussed in detail in **Section 6.1.6, Collect System Logs**.

12.1.8 Device Alert

This sends a text message alert to an email address, or several email addresses. This option is one of the commands that you can insert in the **Workflow** command. To have an alert sent to a mail address, you enter a valid email address in the textbox and click **Enter**. You may choose to send device alerts to several mail addresses.

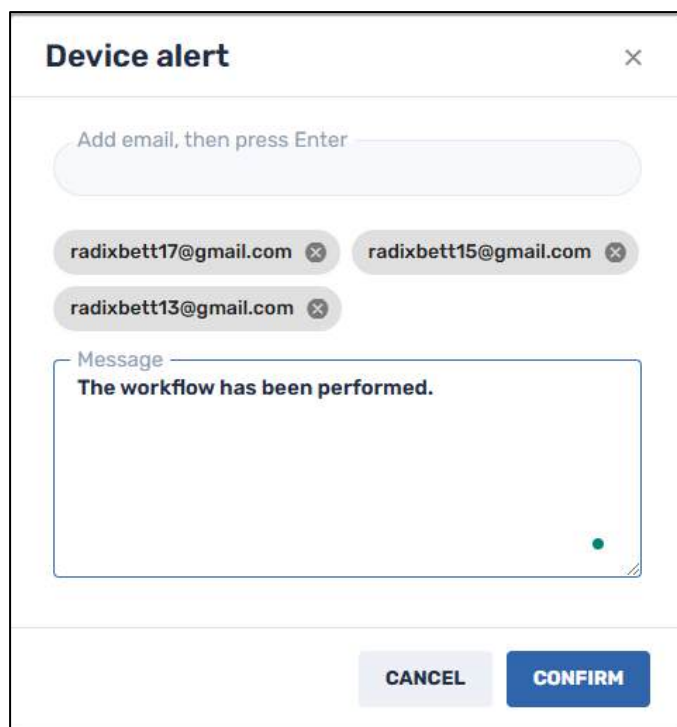


Figure 12-2: Window to send device alert

In the example below of a Workflow, a device will be assigned a Kiosk setting. Upon completion of that task, a text message will be sent to the email address(es) specified in the Device Alert command.

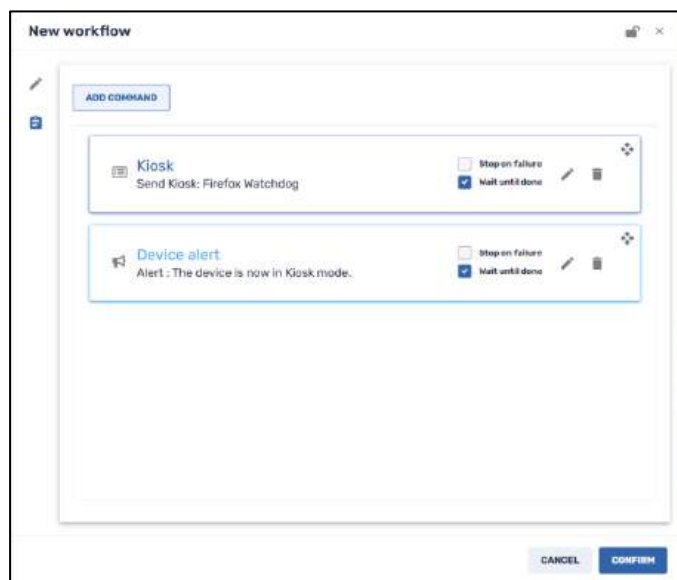


Figure 12-3: Workflow that illustrates use of Device Alert command

12.1.9 Device Settings

- **Function:** This option allows the Radix MDM user to remotely adjust a device's settings.
- **Access:** You can access the Device Settings window by
 - The device's three-dot menu>**Configure>Device Settings**,
 - The **Bulk Commands** button>**Configure>Device Settings**,

- The Device Dashboard, from **Repositories actions> Device Settings**.
- **Further details:** This is discussed in detail in **Section 6.1.8, Device Settings**.

12.1.10 Direct Message

- **Function:** This command allows you to send a simple text message, with a message title and body, to a device.
- **Access:** The **Direct Message** feature can be accessed by:
 - The Device Dashboard, from the **Direct Message** tab.
 - The device's three-dot menu>**Deploy>Direct Message**.
 - The **Bulk Actions button>Deploy>Direct Message**.
- **Further details:** The Direct Message command is discussed in **Section 6.1.9, Direct Message**.

12.1.11 Disable/Enable Apps

- **Function:** “Disable apps” allows you to remove the icon of an app from a device so that the user cannot run it. “Enable apps” restores the icon of the app on the device, so that the user can run it again.
- **Access:** You can access the Disable/Enable Apps command by
 - The device's three-dot menu>**App Management>Disable Apps**,
 - The **Bulk Actions button>App Management>Disable Apps**.
- **Further details:** This is discussed in detail in **Section 6.1.10, Disable/Enable apps**.

12.1.12 Export Device Data to CSV

- **Function:** This allows you to export the table of results to an Excel CSV file.
- **Access:** You can access the Export to CSV command by
 - In the device's three-dot menu>**Device>Export Device Data to CSV**,
 - The **Bulk Actions Button>Device>Export Device Data to CSV**,
 - In the Group Status Bar, from the **Export** icon:



Figure 12-4: Location of Export icon on Group Status Bar

You can choose to display all columns available, or only the columns currently shown in the **Devices** table.



Figure 12-5: Export to CSV selection options

12.1.13 Firmware update

- **Function:** This allows you to update the device's firmware remotely.
- **Access:** You can access the Firmware Update command from
 - The device's three-dot menu>**Deploy>Firmware update**,
 - The Bulk Actions button>**Deploy>Firmware update**,
 - The Device Dashboard, under **Manage>Firmware Update**.
- **Further details:** This is discussed in detail in **Section 6.1.12, Firmware Update**.

12.1.14 Edit Group

- **Function:** If you have created a group, but want to perform modifications, use the **Edit Group** command.
- **Access:** You can access the **Edit Group** command from a Group's **three-dot menu in the Devices Table>Edit Group**:

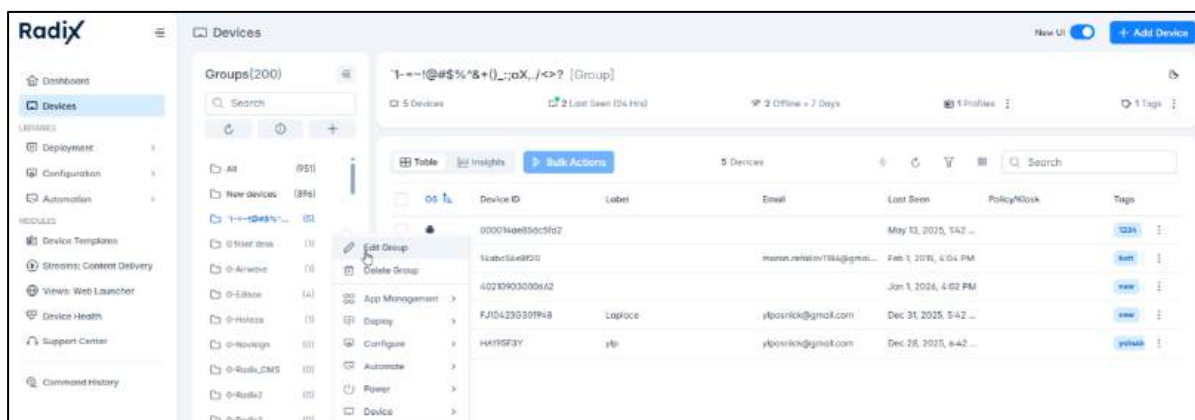


Figure 12-6: Three-dot menu for the Group "Eldary"

- **Further details:** The **Edit Group** option is discussed in **Section 5.1.3**.

12.1.15 Install App/Install Packages

- **Function:** This allows you to install software packages to a device or fleet of devices.
- **Access:** The **Install Packages** feature can be accessed by:
 - The device's three-dot menu>**App Management>Install App**.
 - The **Bulk Actions button>App Management>Install App**,
 - The Device Dashboard, from **Repositories>Install Packages**.

- **Further details:** The Install Packages command is treated in **Section 6.1.13, Install App/Install Package**.

12.1.16 Kiosk

- **Function:** This option allows you to use a device as a display in a kiosk, as in a storefront or hotel.
- **Access:** The **Kiosk** feature can be accessed by:
 - The device's three-dot menu>**Configure>Kiosk Mode**,
 - The **Bulk Actions button>Configure>Kiosk Mode**,
 - The Device Dashboard, from **Repositories>Kiosk**.
- **Further details:** The Kiosk command is treated in **Section 6.1.14, Kiosk**.

12.1.17 Manage Users

- **Function:** This allows you to create or remove users on a particular device.
- **Access:** The **Manage users** feature can be accessed by:
 - The device's **three-dot menu>Configure>Manage Device Users**,
 - The **Bulk Actions button>Configure>Manage Device Users**,
 - The Device Dashboard>**Manage>Manage Users**.
- **Further details:** The Manage users command is discussed in **Section 6.1.15, Manage users**.

12.1.18 Metrics

- **Function:** This provides information about the frequency of app usage on a particular device.
- **Access:** The **Metrics** feature can be accessed by:
 - The device's **three-dot menu>Device>Metrics**,
 - The **Bulk Actions button>Device>Metrics**,
- **Further details:** The Metrics command is discussed in **Section 6.1.17, Metrics**.

12.1.19 OTA (= Over-the-Air)

- **Function:** This enables an Android device to receive and install updates to its operating system or apps, or to dispatch an image of an operating system to a device.
- **Access:** The feature can be accessed by:
 - The device's three-dot menu>**Deploy>Firmware>OTA**,
 - The Bulk Actions button>**Deploy>Firmware>OTA**,
 - The Device Dashboard, from **Repository actions>OTA**.
- **Further details:** The OTA command is discussed in **Section 6.1.18, OTA..**

12.1.20 OTA Update Engine

- **Function:** This option provides an alternate method of performing an over-the-air update to an Android device's operating system or apps. The OTA Update Engine option is for devices running Android 8.0 or newer, and that employ the A/B partition updater.
- **Access:** The feature can be accessed by:
 - The device's three-dot menu>**Deploy>Firmware>OTA Update Engine**,
 - The Bulk Actions button>**Deploy>Firmware>OTA Update Engine**,
 - The Device Dashboard, from **Repository actions>OTA Update Engine**.

- **Further details:** The OTA Update Engine command is discussed in **Section 6.1.19, OTA Update Engine**.

12.1.21 Policies/Block Lists

- **Function:** The Block Lists/Policies option is for blacklisting and blocking apps that have security issues, and you would prefer that they not run on certain devices.
- **Access:** The Block Lists/Policies feature can be accessed by:
 - The device's three-dot menu>**Configure>Block Lists**,
 - The Bulk Actions button>**Configure>Block Lists**,
 - The Device Dashboard, under **Repositories actions>Policies**.
- **Further details:** Creating and applying policies to devices is dealt with in **Section 6.1.21, Policies (Block Lists)**.

12.1.22 Remote Control

- **Function:** The Remote Control option allows you to access a device's controls remotely.
- **Access:** The Remote Control feature can be accessed by:
 - The device's three-dot menu>**Remote Control**,
 - The **Bulk Actions button>Remote Control**,
 - The Device Dashboard, from the **Remote** tab in the right-hand menu.
- **Further details:** This command is discussed in **Section 6.1.22, Remote Control**.

12.1.23 Commands & Scripts/Remote Execute

- **Function:** This option is to execute a particular command prompt command or script on a device.
- The **Remote execute** feature can be accessed by:
 - The device's three-dot menu>**Deploy>Commands & Scripts**,
 - The **Bulk Actions button>Deploy>Commands & Scripts**,
 - The Device Dashboard, from **Repositories Actions>Remote Execute**.
- **Further details:** The **Commands & Scripts/Remote Execute** command is treated in **Section 6.1.23, Remote Execute**.

12.1.24 Remove Google Accounts from a Device

- **Function:** This allows you to remove all Google accounts from a device, or to retain one.
- **Access:** The **Remove Google Accounts** feature can be accessed by:
 - The device's three-dot menu>**Configure>Remove Google Account**,
 - The **Bulk Actions button>Configure>Remove Google Account**,
 - The Device Dashboard, from **Manage>Remove Google Account**.
- **Further details:** The Remove Google Accounts command is treated in **Section 6.1.24, Remove Google Accounts from Device**.

12.1.25 Restart

- **Function:** This allows the Radix Device Management user to restart a device remotely.
- **Access:** The **Restart** feature can be accessed by:
 - The device's three-dot menu>**Power>Restart**,

- The **Bulk Actions button>Power>Restart**,
- The Device Dashboard, from **Power>Restart**.
- **Further details:** The Restart command is treated in **Section 6.1.25, Restart**.

12.1.26 Scheduler & trigger command

- **Function:** This allows you to create a schedule for executing a command, as well as trigger the command (either by timing, geofencing, Wi-Fi, or upon every startup of the device).
- **Access:** The **Scheduler & trigger command** feature can be accessed by:
 - The device's three-dot menu>**Automate>Schedules & Triggers**,
 - The **Bulk Actions>Automate>Schedules & Triggers**,
 - The Device Dashboard, from the **Schedules & trigger command** tab.
- **Further details:** The Scheduler & Trigger Command is treated in **Section 6.1.26, Scheduler & Triggers Command**.

12.1.27 Screen settings

- **Function:** This allows you to adjust the brightness and volume on flat panel devices.
- **Access:** The **Screen settings** feature can be accessed by:
 - The device's three-dot menu>**Configure>Screen Settings**,
 - The **Bulk Actions>Configure>Screen Settings**,
 - The Device Dashboard, under the **Manage tab>Screen Settings**.
- **Further details:** The **Screen settings** command is treated in **Section 6.1.27, Screen Settings**.

12.1.28 Send Files/Files

- **Function:** This allows you to send specific files to a device.
- **Access:** The **Send Files** feature can be accessed by:
 - The device's three-dot menu>**Deploy>Files**,
 - The **Bulk Actions button>Deploy>Files**,
 - The Device Dashboard, from **Repositories actions>Files**.
- **Further details:** The Send Files command is treated in **Section 6.1.28, Send Files**.

12.1.29 Shutdown

- **Function:** This command shuts the device down remotely.
- **Access:** The **Shutdown** feature can be accessed by:
 - The device's three-dot menu>**Power>Shut down**,
 - The **Bulk Actions button>Power>Shut down**,
 - The Device Dashboard, from the **Power** tab, under **Shutdown**.
- **Further details:** The Shutdown command is treated in **Section 6.1.29, Shutdown**.

12.1.30 Smart Recovery (Windows Devices Only)

- **Function:** This allows you to implement settings to repair a Windows device that has crashed, such as restoring a device's system configuration and settings to the latest system snapshot, or factory settings.
- **Access:** You can access this command from:
 - The device's three-dot menu>**Device>Smart Recovery**,
 - The **Bulk Actions button>Device>Smart Recovery**,

- The **Device Dashboard>Repositories Actions>Smart Recovery**.
- **Further details:** This command is discussed in **Section 6.1.30, Smart Recovery**.

12.1.31 Siren/Sound Siren

- **Function:** This option sounds an alarm on the device.
- **Access:** The **Sound Siren** feature can be accessed by:
 - The device's three-dot menu>**Block Device>Play Siren**,
 - The **Bulk Actions button>Block Device>Play Siren**,
 - The device's Device Dashboard, under **Lock>Siren**.
- **Further details:** The Sound Siren command is treated in **Section 5.8.3.8.3, Siren**.

12.1.32 Standby

- **Function:** This command put a remote device in standby mode (otherwise called “Hibernate” or “Sleep Mode”).
- **Access:** The **Standby** feature can be accessed by:
 - The device's three-dot menu>**Power>Standby**,
 - The **Bulk Actions button>Power>Standby**,
 - A group's three-dot menu>**Power>Standby**.
- **Further details:** The Standby command is treated in **Section 6.1.31, Standby**.

12.1.33 Tags

- **Function:** This command allows you to add to or remove tags from a device or user. Tags can help you create a group of users or devices to which you apply actions simultaneously.
- **Access:** The **Tags** feature can be accessed by:
 - The device's three-dot menu>**Device>Set Device Tags**,
 - The **Bulk Actions button>Device>Set Device Tags**,
 - The Device Dashboard, from the **Manage** tab, under **Tags**.
- **Further details:** The Tags command is treated in **Section 6.1.32, Tags**.

12.1.34 Timeout

- **Function:** You can use this as part of the Workflow command (see **Section 6.1.39, Workflow**). When you create a workflow of several commands, the Timeout option puts a time delay between the commands.
- **Access:** To access the Timeout command, go to **Automate>Workflow>Add New Workflow>Add Command>Time out**.

12.1.35 Uninstall Packages

- **Function:** This command lets you uninstall software packages or apps on a device.
- **Access:** The **Uninstall packages** feature can be accessed by:
 - The device's three-dot menu>**App Management>Uninstall App**.
 - The **Bulk Actions button>App Management>Uninstall App**.
- **Further details:** For more information about the Uninstall Packages command, see **Section 6.1.34, Uninstall Packages**.

12.1.36 Views

- **Function:** This command allows you to create a specialized Kiosk option for a remote device, where you select allowed apps and access to single URL on the remote device.
- **Access:** The **Views** option can be accessed by:
 - The device's three-dot menu>**Views**,
 - The **Bulk Actions button**>**Views**,
 - The Device Dashboard, from the **Repositories Actions** tab, under **Views**.
- **Further details:** This command is dealt with at length in **Section 6.1.35, Views**.

12.1.37 Wake on LAN

- **Function:** This option allows a device (or group of devices) to be turned on or “awakened” by means of a network message or a time trigger.
- **Access:** The **Wake on LAN** feature can be accessed by:
 - The device's three-dot menu>**Power**>**Wake on LAN**,
 - The **Bulk Actions button**>**Power**>**Wake on LAN**,
 - The Device Dashboard, from the **Power** tab, under **Wake on LAN**.
- **Further details:** This command is dealt with at length in **Section 6.1.36, Wake on LAN**.

12.1.38 Wake Up

- **Function:** After a device has been put in Standby mode, the **Wake Up** command will turn the device's display back on.
- **Access:** The **Wake Up** feature can be accessed by:
 - The device's three-dot menu>**Power**>**Wake Up**,
 - The **Bulk Actions button**>**Power**>**Wake Up**,
 - A group's **three-dot menu**>**Power**>**Wake Up**.
- **Further details:** The Wake Up command is treated at length in **Section 6.1.37, Wake Up**.

12.1.39 Windows Update

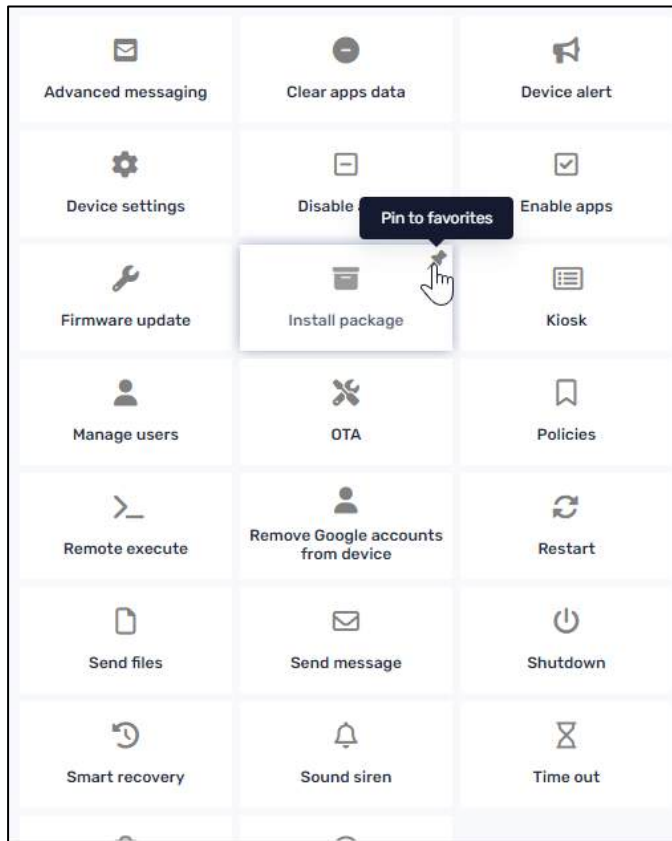
- **Function:** This allows you to update software and drivers on remote Windows devices.
- **Access:** The **Windows Update** feature can be accessed by:
 - The device's three-dot menu>**Deploy**>**Windows Updates**,
 - The **Bulk Actions button**>**Deploy**>**Windows Updates**,
- **Further details:** The Windows Update command is treated at length in **Section 6.1.38, Windows Update**.

12.1.40 Workflow

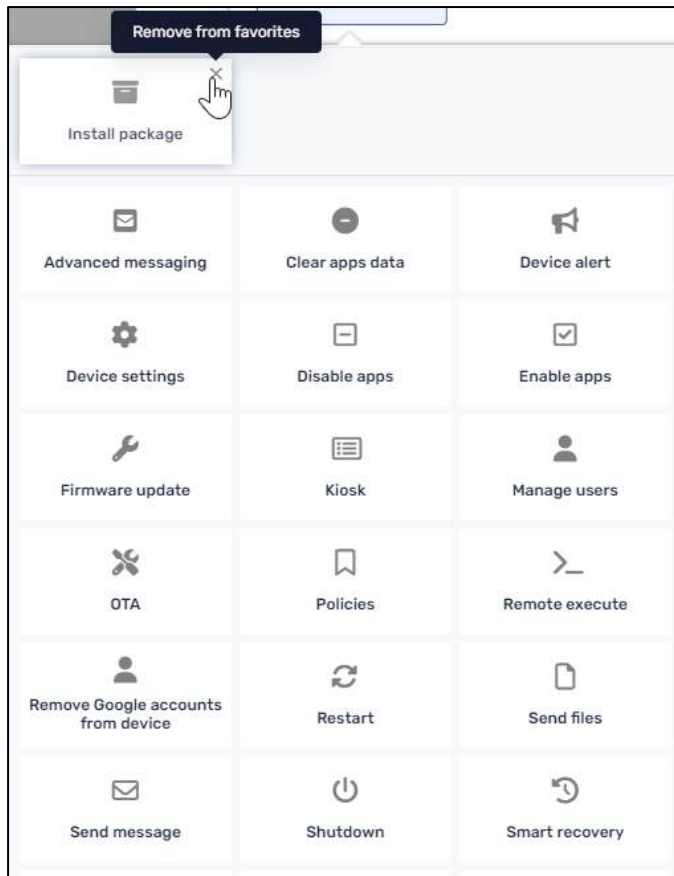
- **Function:** The Workflow command allows you to send a series of commands to be executed, one after the other, to a single device or group of devices.
- **Access:** The **Workflow** feature can be accessed by:
 - The device's three-dot menu>**Automate**>**Workflows**,
 - The **Bulk Actions button**>**Automate**>**Workflows**,
 - The Device Dashboard, from the **Repositories actions** tab, under **Workflow**.
- **Further details:** The Workflow option is treated at length in **Section 6.1.39, Workflow**.

12.2 Pinning and Unpinning Commands

In the Schedule and Trigger command, you will see an alphabetical grid of commands. By clicking on the pin icon in the upper right of one of the tiles, you can pin that tile to the top rows of “favorite” commands.



You can later remove that command from the Favorites row by clicking on **Remove from favorites**. The command tile will revert to its place in the alphabetical list of commands.



Appendix B: General Devices Table Tile options

12.3 Repository Tile Command Editing Options

The Radix Device Management Repository items will have tiles with editable settings. You can adjust the color of the tile, change the icon displayed, pin it to the top of the screen for easier access, and more.

Depending on the command, the tile will have either five or six options:

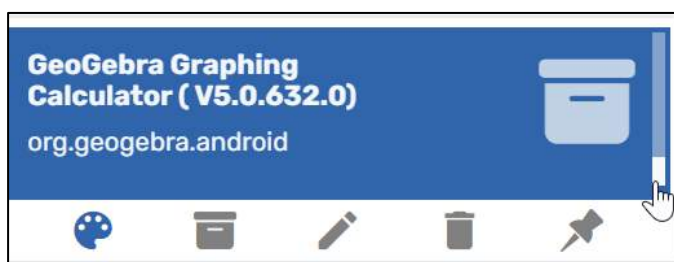


Figure 12-7: Sample Install Package Tile, with five editing options.

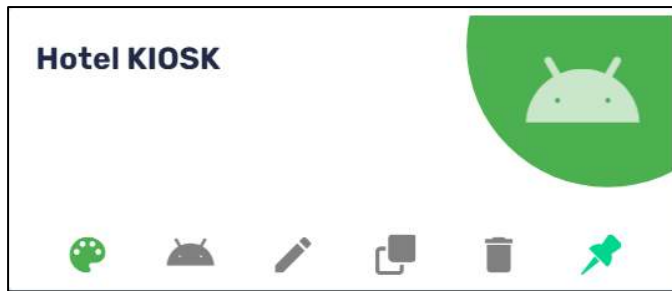


Figure 12-8: Sample Kiosk Tile, with six editing options

Table 12-1: Tile Editing Options

Icon	Description
	Pick Color
	Pick Icon
	Edit
	Clone
	Delete
	Pin to Top

12.3.1 Pick Color

The **Pick Color** palette icon  allows you to set a color for the package to be installed, to distinguish this particular package from the others.



12.3.2 Pick Icon

Clicking on **Pick Icon**  allows you to set an icon for a particular command tile, instead of the default “Control Panel” icon.



12.3.3 Edit Icon

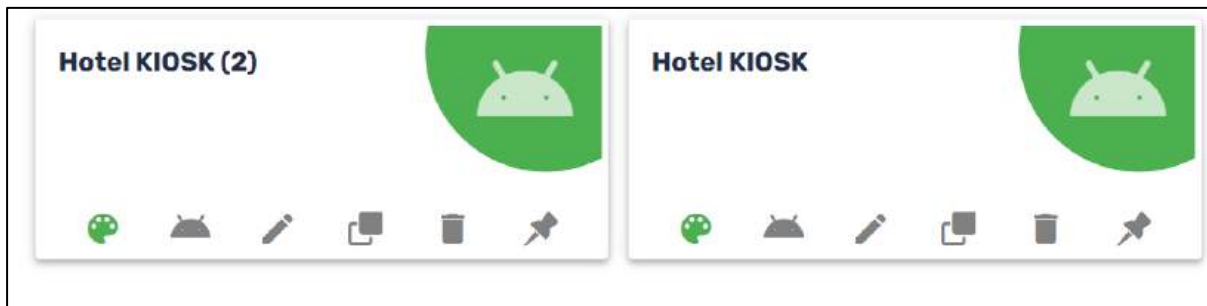
Clicking on the Edit icon  will allow you to edit the data in the particular command.

12.3.4 Clone

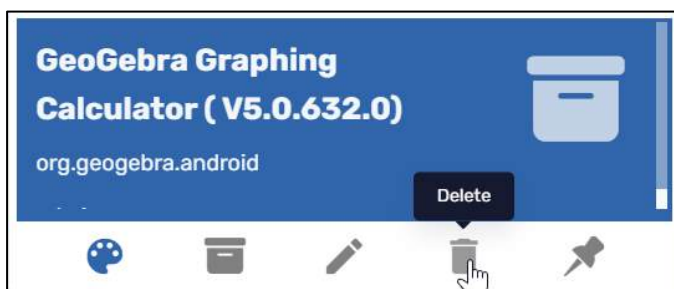
This allows you to create a duplicate of a particular tile.



The clone will receive the same name as the original setting, with the addition of the suffix (2):



12.3.5 Delete



This allows you to delete the **Install package** tile. You will receive a prompt to verify if you are sure about deleting the tile:



12.3.6 Pin to Top

This option allows you to pin the command to the top of the **Install Package** screen, for easier access. This is handy if you want to install an app on many devices.



Appendix C: List of All Commands

This is a table of all the Radix Device Management Platform commands, as well as the operating system for which they are relevant.

Table 12-2: List of Commands--All Operating Systems

Icon	Description	Device Operating System		
		Android	Chrome	Windows
	Advanced Messaging	Android		
	AFW Install/Uninstall	Android		
	Change agent password	Android		Windows
	Clear apps cache	Android		
	Clear apps data	Android		
	Collect logs	Android		
	Device Settings	Android		Windows
	Direct message	Android	Chrome	Windows
	Disable apps	Android		
	Enable apps	Android		
	Export to CSV	Radix Device Management Interface Feature		
	Firmware update	Android		
	Edit Group	For managing groups of devices/users		
	Install Packages	Android		Windows
	Kiosk	Android	Chrome	Windows
	Manage Users	Android		
	OTA	Android		
	Policies	Android	Chrome	Windows
	Remote Control	Android		Windows

	Remote Execute	Android		Windows
	Remove Google accounts from device	Android		
	Restart	Android		Windows
	Scheduler & triggers command	Android		Windows
	Screen settings	Android		
	Send files	Android		Windows
	Shutdown	Android		Windows
	Smart Recovery			Windows
	Sound Siren	Android		
	Standby	Android		
	Tags	Android	Chrome	Windows
	Timeout	Feature in Workflow Command		
	Uninstall packages	Android		Windows
	Views	Android	Chrome	
	Wake on LAN	Android		Windows
	Wake up	Android		
	Windows Update			Windows
	Workflow	Android		Windows

Appendix D: Smart Recovery Version Comparison

	LITE	DUO	PRO
Change Restore Mode	Restore at every boot Manual restore	Restore at every boot Manual restore	Restore at every boot Manual restore
Restore System	The baseline	The baseline The latest snapshot Another snapshot (you must provide the name of the snapshot)	The baseline The latest snapshot Another snapshot (you must provide the name of the snapshot) The current snapshot
Save Changes	Save the current system as a dynamic recovery point	Save the current system as a dynamic recovery point: Snapshot name Snapshot description	Save the current system as a dynamic recovery point: Snapshot name Snapshot description
Change Client Smart Recovery Password	Enter a new password Confirm password	Enter a new password Confirm password	Enter a new password Confirm password
Register	Registration name Registration serial number	Registration name Registration serial number	Registration name Registration serial number
Uninstall client Smart Recovery Password	Keep the current state and then uninstall Restore to the baseline and then uninstall	Keep the current state and then uninstall Restore to the baseline and then uninstall Restore to the latest snapshot and then uninstall	Keep the current state and then uninstall Restore to the baseline and then uninstall Restore to the latest snapshot and then uninstall

Appendix E: Remote Execute Command Reference

Here is a list of all Android keyevent commands, for use in the Remote Execute command. For example, enter “input” as the command, and “keyevent XX” as the argument, where “XX” is the number of the keycode.

0 → "KEYCODE_UNKNOWN"	21 → "KEYCODE_DPAD_LEFT"	42 → "KEYCODE_N"	63 → "KEYCODE_SYM"
1 → "KEYCODE_MENU"	22 → "KEYCODE_DPAD_RIGHT"	43 → "KEYCODE_O"	64 → "KEYCODE_EXPLORER"
2 → "KEYCODE_SOFT_RIGHT"	23 → "KEYCODE_DPAD_CENTER"	44 → "KEYCODE_P"	65 → "KEYCODE_ENVELOPE"
3 → "KEYCODE_HOME"	24 → "KEYCODE_VOLUME_UP"	45 → "KEYCODE_Q"	66 → "KEYCODE_ENTER"
4 → "KEYCODE_BACK"	25 → "KEYCODE_VOLUME_DOWN"	46 → "KEYCODE_R"	67 → "KEYCODE_DEL"
5 → "KEYCODE_CALL"	26 → "KEYCODE_POWER"	47 → "KEYCODE_S"	68 → "KEYCODE_GRAVE"
6 → "KEYCODE_ENDCALL"	27 → "KEYCODE_CAMERA"	48 → "KEYCODE_T"	69 → "KEYCODE_MINUS"
7 → "KEYCODE_0"	28 → "KEYCODE_CLEAR"	49 → "KEYCODE_U"	70 → "KEYCODE_EQUALS"
8 → "KEYCODE_1"	29 → "KEYCODE_A"	50 → "KEYCODE_V"	71 → "KEYCODE_LEFT_BRACKET"
9 → "KEYCODE_2"	30 → "KEYCODE_B"	51 → "KEYCODE_W"	72 → "KEYCODE_RIGHT_BRACKET"
10 → "KEYCODE_3"	31 → "KEYCODE_C"	52 → "KEYCODE_X"	73 → "KEYCODE_BACKSLASH"
11 → "KEYCODE_4"	32 → "KEYCODE_D"	53 → "KEYCODE_Y"	74 → "KEYCODE_SEMICOLON"
12 → "KEYCODE_5"	33 → "KEYCODE_E"	54 → "KEYCODE_Z"	75 → "KEYCODE_APOSTROPHE"
13 → "KEYCODE_6"	34 → "KEYCODE_F"	55 → "KEYCODE_COMMA"	76 → "KEYCODE_SLASH"
14 → "KEYCODE_7"	35 → "KEYCODE_G"	56 → "KEYCODE_PERIOD"	77 → "KEYCODE_AT"
15 → "KEYCODE_8"	36 → "KEYCODE_H"	57 → "KEYCODE_ALT_LEFT"	78 → "KEYCODE_NUM"
16 → "KEYCODE_9"	37 → "KEYCODE_I"	58 → "KEYCODE_ALT_RIGHT"	79 → "KEYCODE_HEADSETHOOK"
17 → "KEYCODE_STAR"	38 → "KEYCODE_J"	59 → "KEYCODE_SHIFT_LEFT"	80 → "KEYCODE_FOCUS"
18 → "KEYCODE_POUND"	39 → "KEYCODE_K"	60 → "KEYCODE_SHIFT_RIGHT"	81 → "KEYCODE_PLUS"
19 → "KEYCODE_DPAD_UP"	40 → "KEYCODE_L"	61 → "KEYCODE_TAB"	82 → "KEYCODE_MENU"
20 → "KEYCODE_DPAD_DOWN"	41 → "KEYCODE_M"	62 → "KEYCODE_SPACE"	83 → "KEYCODE_NOTIFICATION"
84 → "KEYCODE_SEARCH"		85 → "TAG_LAST_KEYCODE"	

Table 12-3: Useful Remote Execute Commands

Function	CMD	Arguments	Wait for Exit	Collect Output	Run with High Privileges
Disable Google Play store	pm	disable com.android.vending			X
Get a list of currently running apps and display result	top	-n 1	X	X	X
Open a website using a default browser	am	start -a android.intent.action.VIEW -d https://www.radix-int.com			
Run using the Monkey command	monkey	-p org.chromium.webview_shell -c android.intent.category.LAUNCHER 1			X
Clear app data	am	clear com.android.browser			X
To type a string: 1234	input	text 1234			X
To type a string: 12 34	input	text 12%s34			X
To simulate the home button	input	keyevent 3			X
To simulate the menu button	input	keyevent 82			X
To simulate a tap in screen coordinates 300 x 550	input	tap 300 500			X
To simulate a swipe from coordinates 300 x 550 to coordinates 900 X 600 with speed of 250ms	input	swipe 300 500 900 600 250			X
To simulate a long press with a duration of 1000ms in coordinates 300 x 550	input	swipe 300 500 300 500 1000			X