Radix Device Management User Guide

Radix Device Management Platform

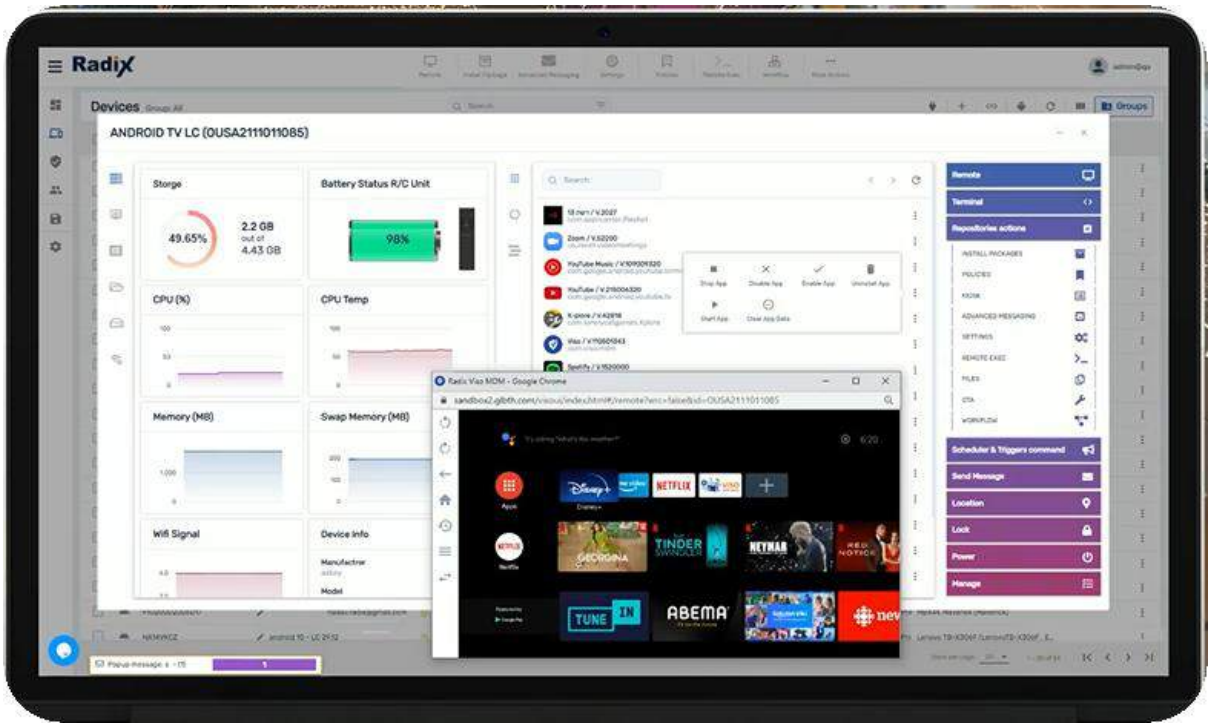


Table of Contents

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, Apple OS, iOS, 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. Login Screen

To start using Radix Device Management, go to the login page at https://visomdm.com/v2/index.html#/login. You will see the login screen on the left side, along with a brief description of the advantages of the Radix Device Management on the right.

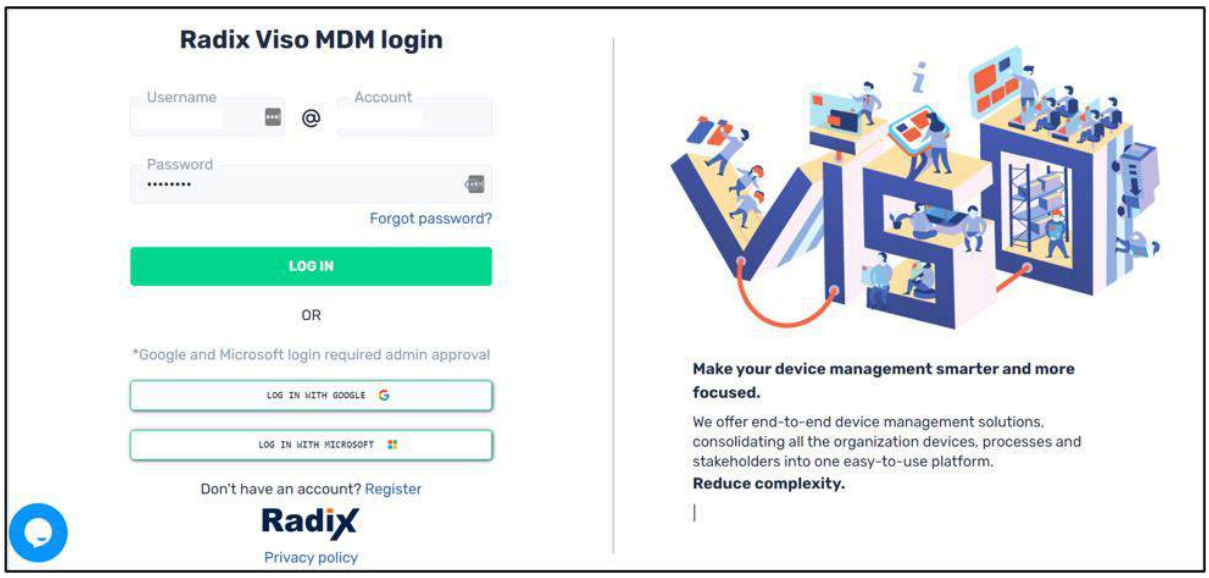


Figure 2-1: Radix Device Management Login Screen

When creating a Radix account, you will be assigned a Radix username, account name, and password.

Once you have created an account, either as an administrator, user, or just "supporter" (where you can only request customer support), you can log in using a Google or Microsoft account as well. 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.

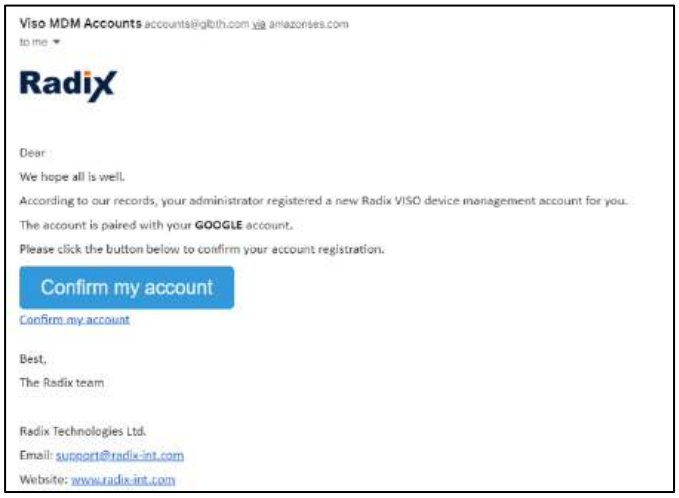


Figure 2-2: Google Confirmation E-mail

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.

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.

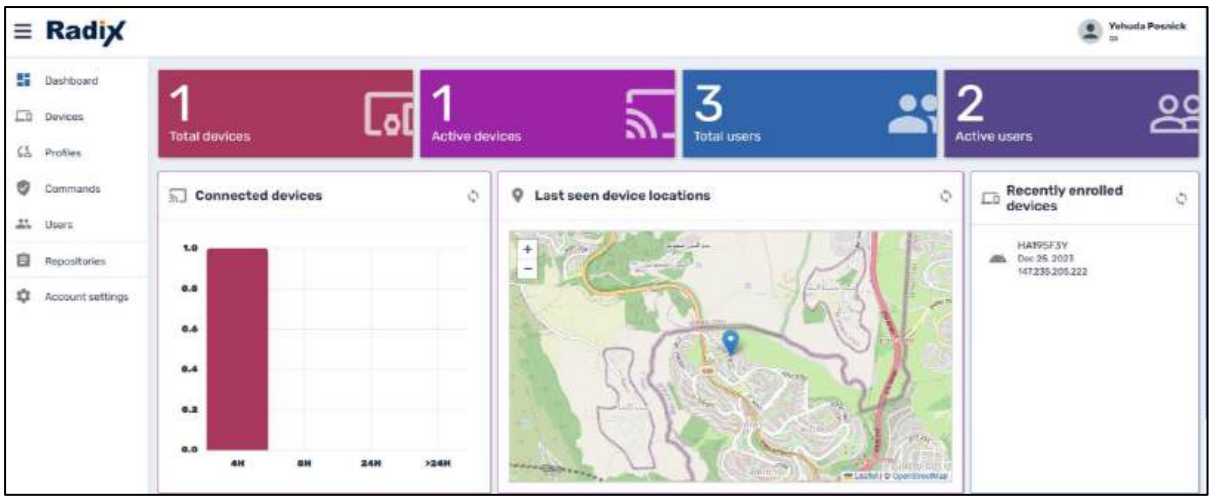


Figure 3-1: Overview Dashboard—Top Pane

You can collapse the options on the left side of the screen by clicking on the hamburger menu on the upper left:

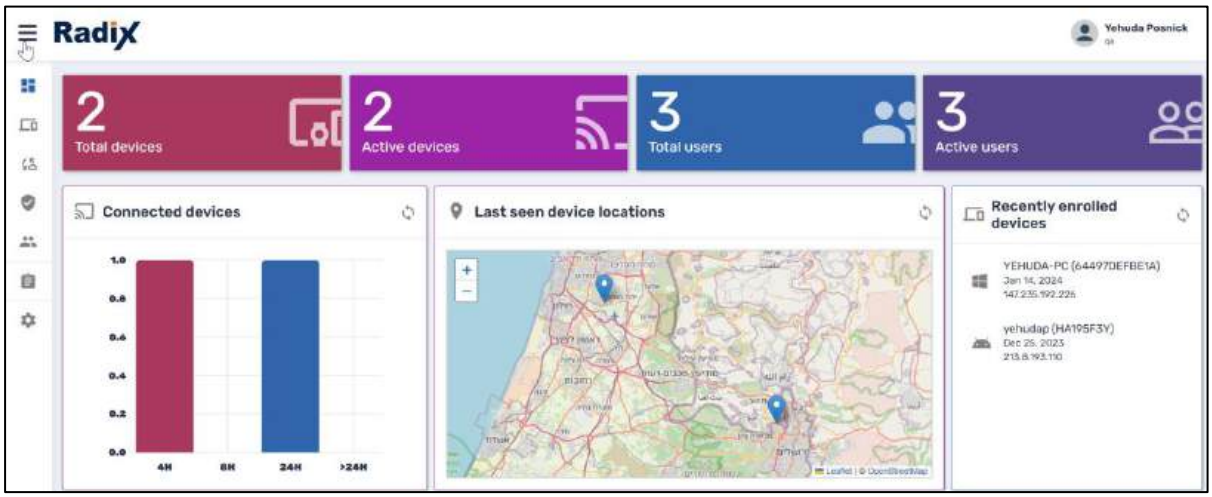


Figure 3-2: Overview Dashboard—Top Pane with Hamburger Menu collapsed

3.1 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

3.2 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.

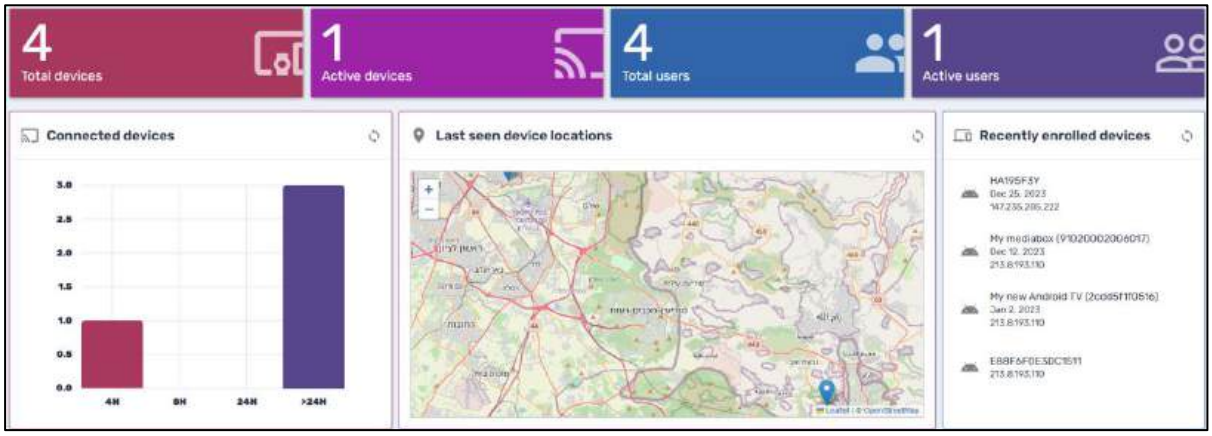


Figure 3-4: Overview Dashboard--Middle Panes

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 Manager, as well as the date and IP address of the login.

3.3 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.

3.3.1 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.

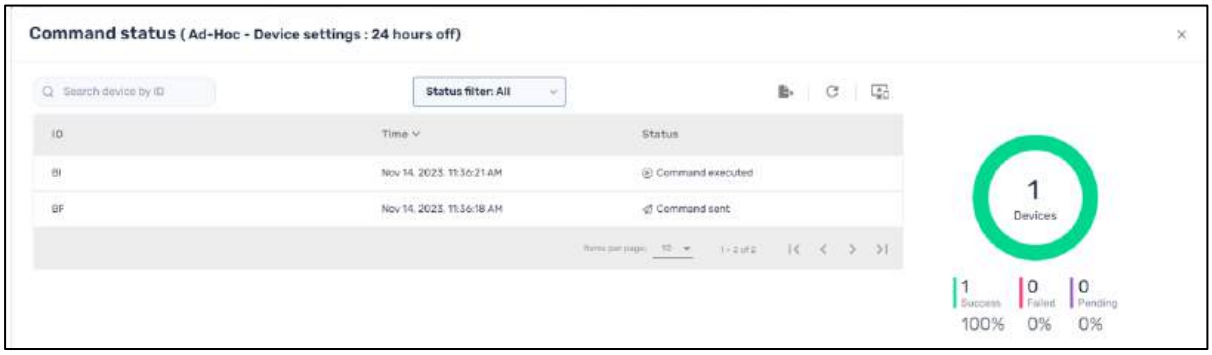


Figure 3-6: Command Status window, showing that the command was successfully executed

We will see the Command Status window when we discuss the Commands Console (**Chapter 5**).

3.4 User Profile Menu

When you click on the **User** icon in the upper-right 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:

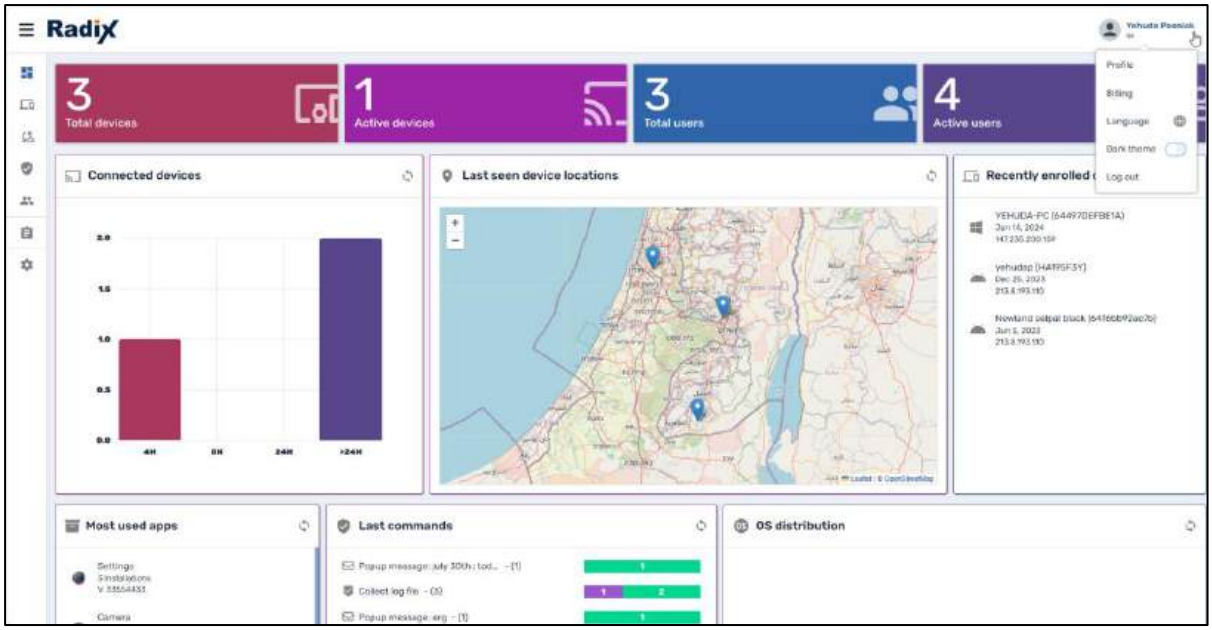


Figure 3-7: User Profile Menu, in upper right

- **Profile**, with user account options,
- **Billing**, displaying information about payments and credit balance,
- **Language**, for adjusting the interface language,
- **Dark Theme**, to toggle between a white or dark background,
- **Log out**, to exit the system.

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

Figure 3-8: User Profile menu for non-Admin users

We will go through the options in detail:

3.4.1 User Profile Option

The **User 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.

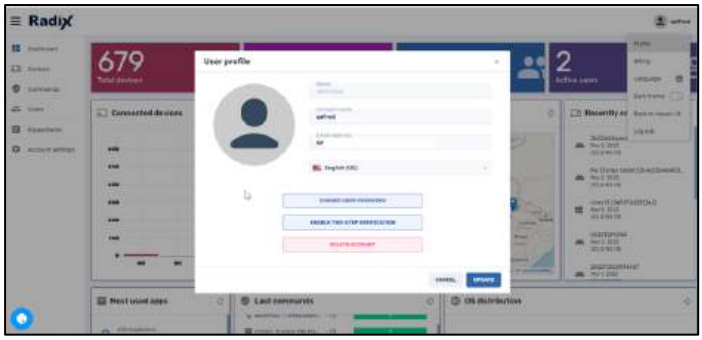


Figure 3-9: User Profile Screen, with options to change password, enable two-step verification, or delete an account

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.

Figure 3-10: Two-step verification options

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

To delete an account:

1. Click on **Delete Account**.

2. When prompted if you are sure that you want to delete the account, click **Yes**.

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:

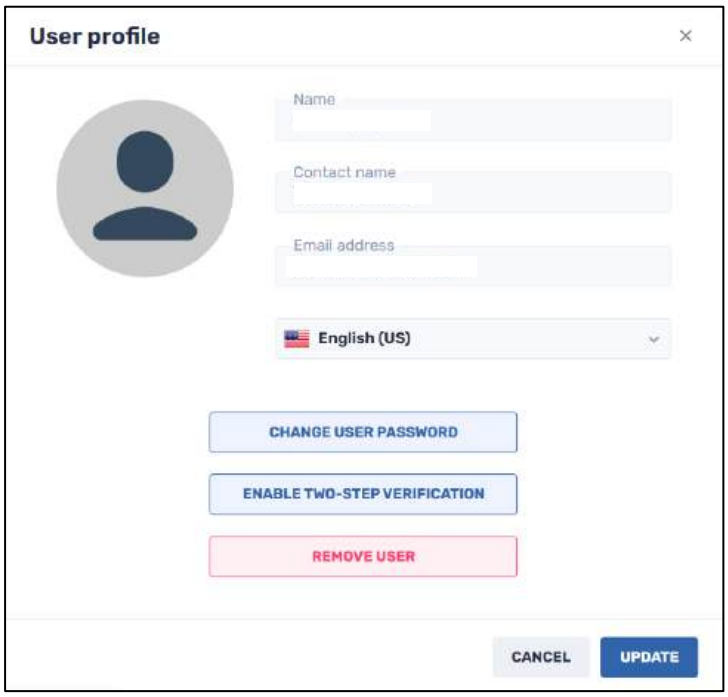


Figure 3-11: User Profile dialog box for regular client user

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.

3.4.2 Billing Option

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.

3.4.2.1 Billing Data--Background

When you create an account on the Radix Device Manager, 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 Manager account, it initiates a "countdown" to the number of credits, decreasing by one credit a day per device.

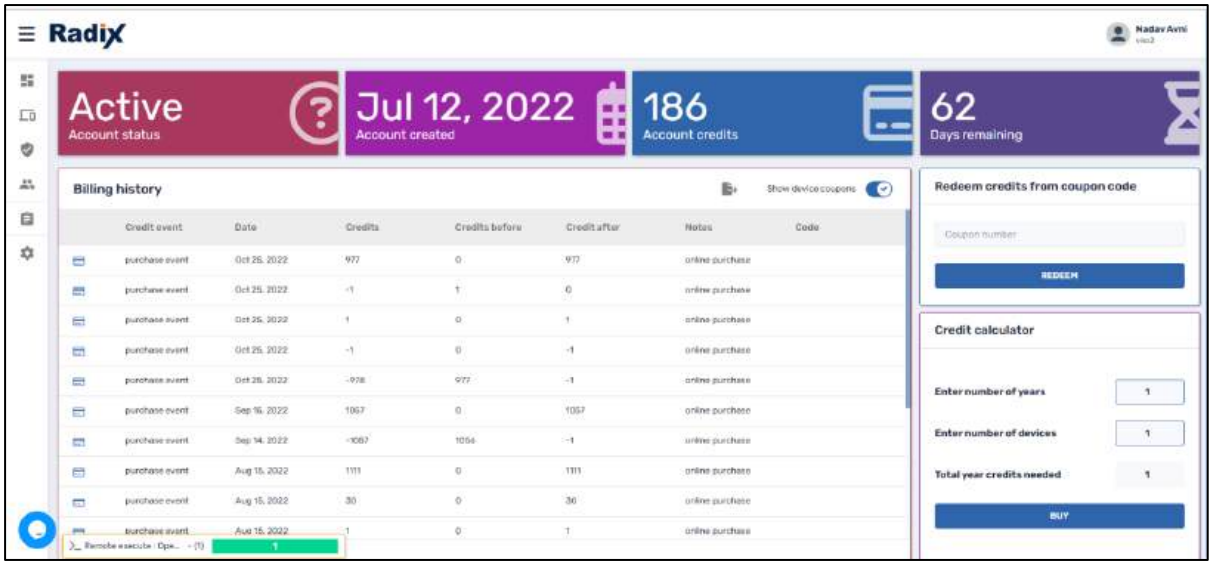


Figure 3-12: Billing History Display

3.4.2.2 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.

Figure 3-13: 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 

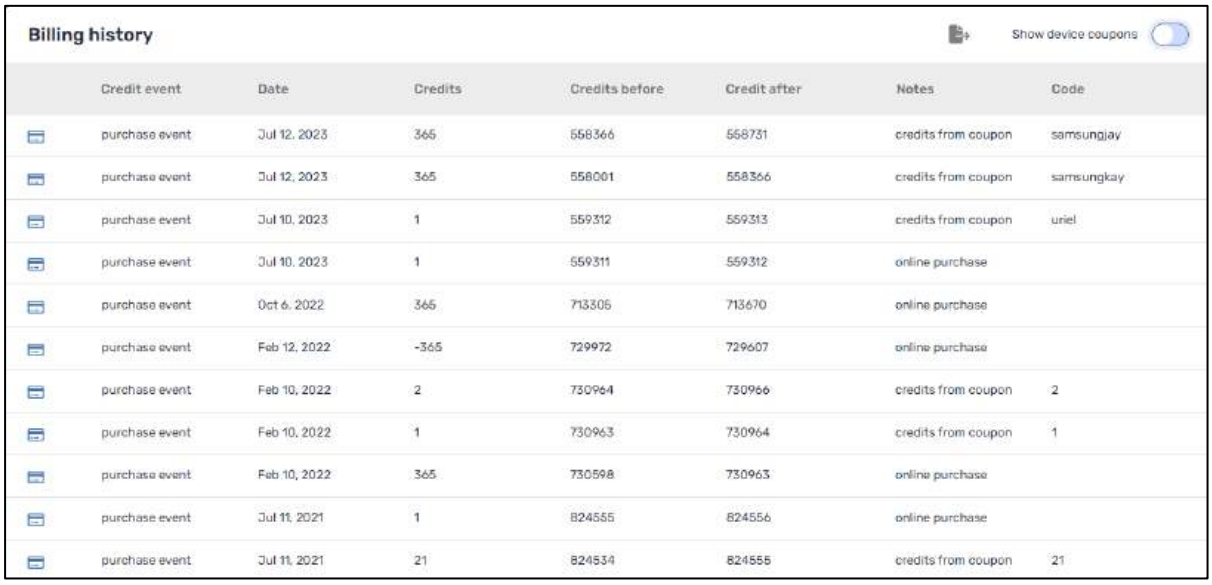
, you can toggle between viewing all transactions, including credits from device coupons, or only credits from online purchases.

Billing history

Show device coupons

	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	6438428ab059ed5f
	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	BFFS0CNND60002

Figure 3-14: Billing History spreadsheet, including device coupons



Billing history

Show 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	713305	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 3-15: 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.

Figure 3-16: 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.

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

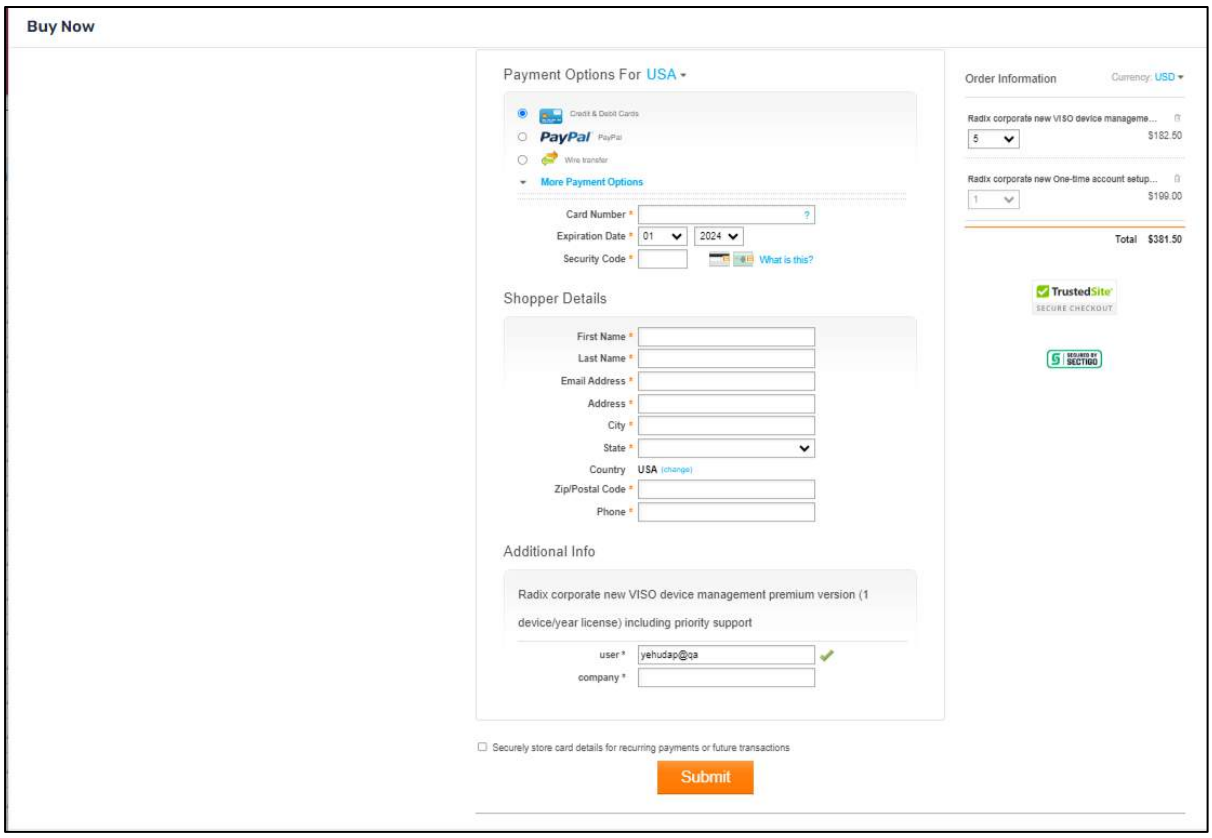


Figure 3-17:"Buy Now" screen, allowing you to purchase additional credits

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 Manager 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.

3.4.3 Language Options

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

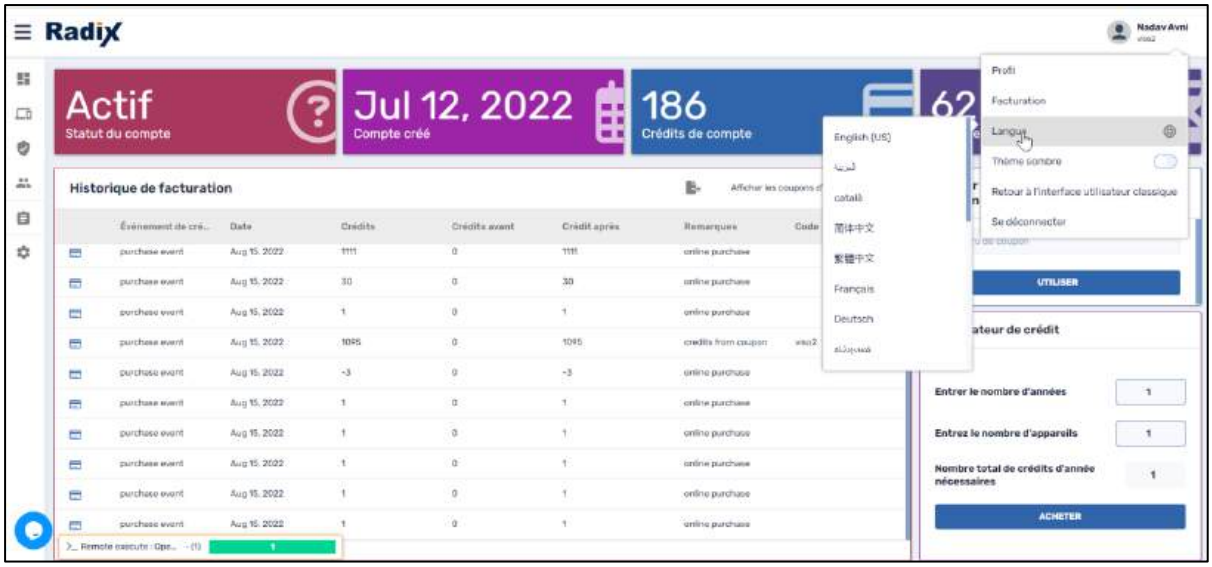


Figure 3-18: The Language option, with French selected as the interface language

This option is available for users without Administrator privileges. We will see in **Section 7.3** that a user with Administrator privileges can change the interface language for all users.

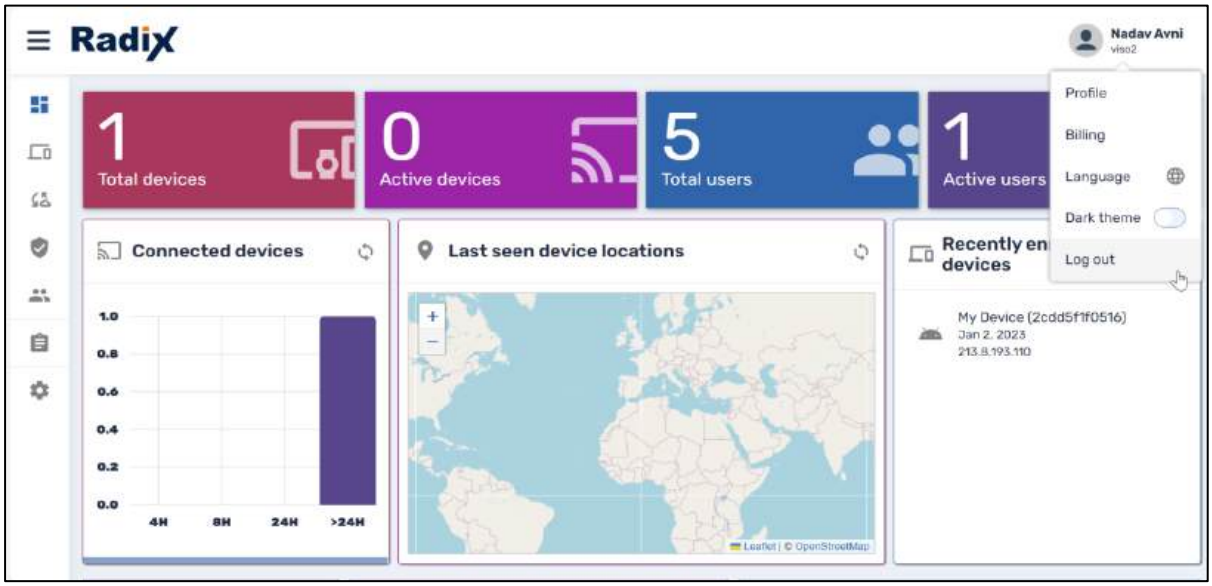
3.4.4 Display Theme Options

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

When you first log in to the Radix Device Manager, 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 themes:

1. Click on the **Profile** icon in the upper left corner.
   A drop-down list will appear, allowing you to select Profile information, view billing information, select the display language, select a dark or light display, or log out of the interface.



2. Click on **Dark Theme** to change the display to dark mode.

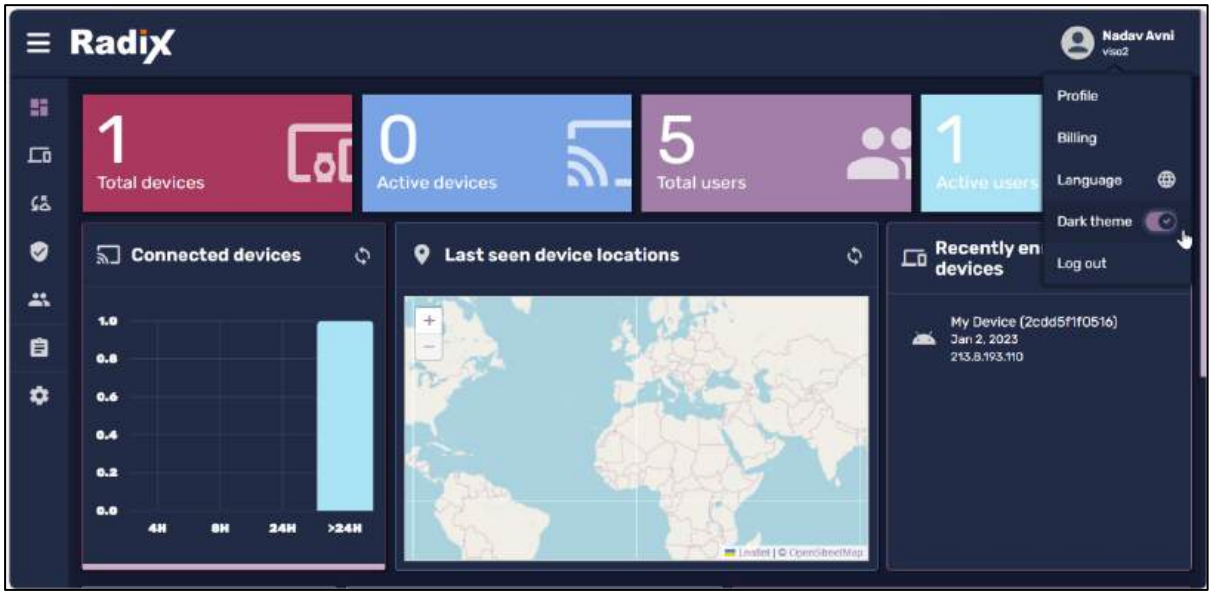


Figure 3-19: Dark Theme Overview Dashboard

3.4.5 Logout

Selecting this gets you to the Logout screen.

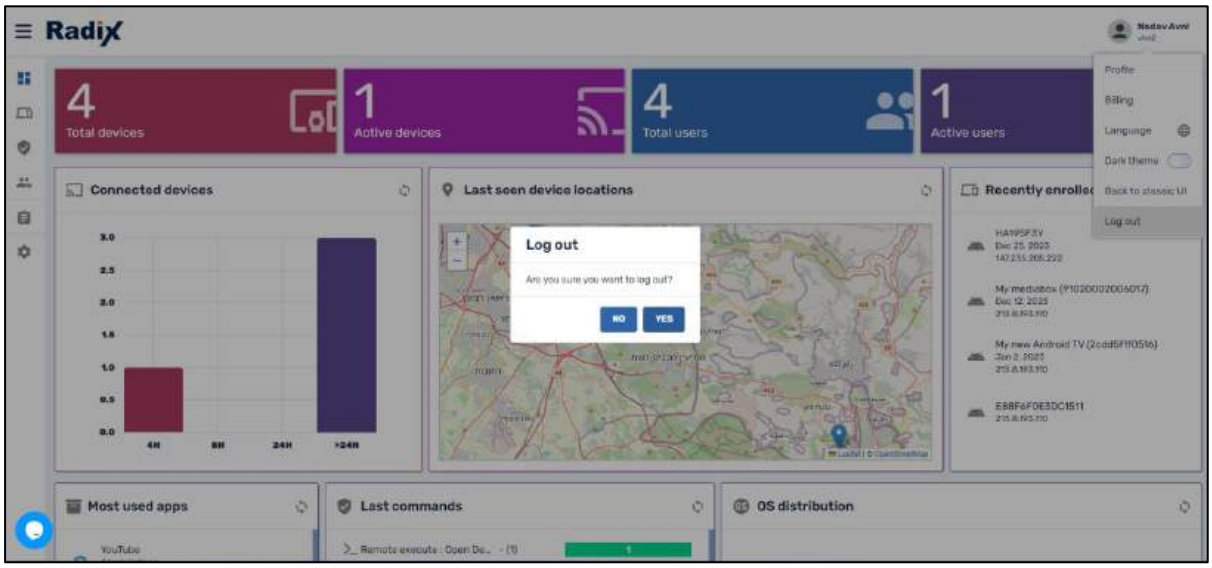


Figure 3-20: Logout Screen

Chapter 4. Devices Console

The **Devices Console** 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 gives you options for applying commands to a single device, several devices at once, or even an entire group or fleet of devices. The commands that you use the most appear at the very top, and you have an option to expand the menu.

To view the Devices console, click on the **Devices** icon in the Overview Dashboard.

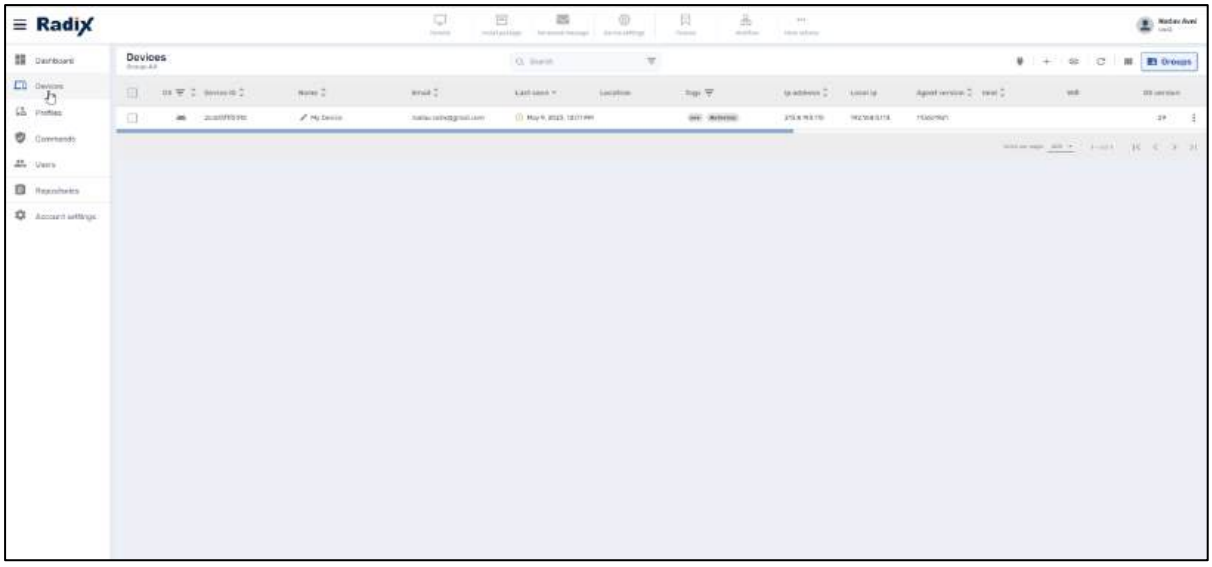


Figure 4-1: Devices Console

To work with a specific device, click on that device's three-dot menu ("kebab menu") on the far right.

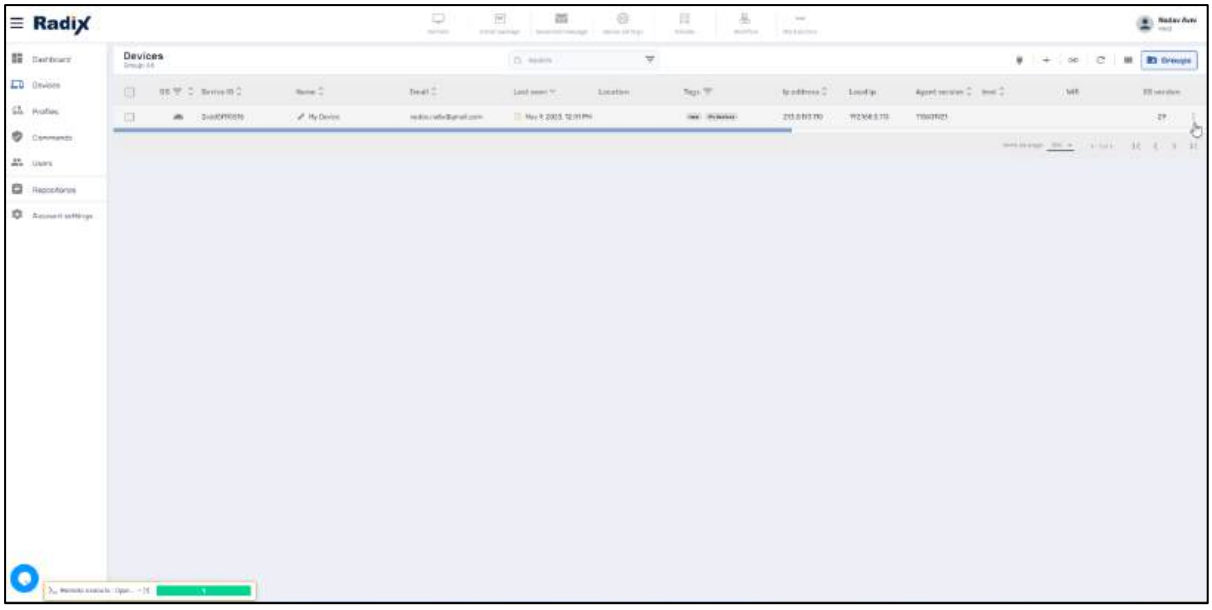


Figure 4-2: Device's Three-Dot ("Kebab") Menu

A grid of commands will open up with all of the options for working with your device.

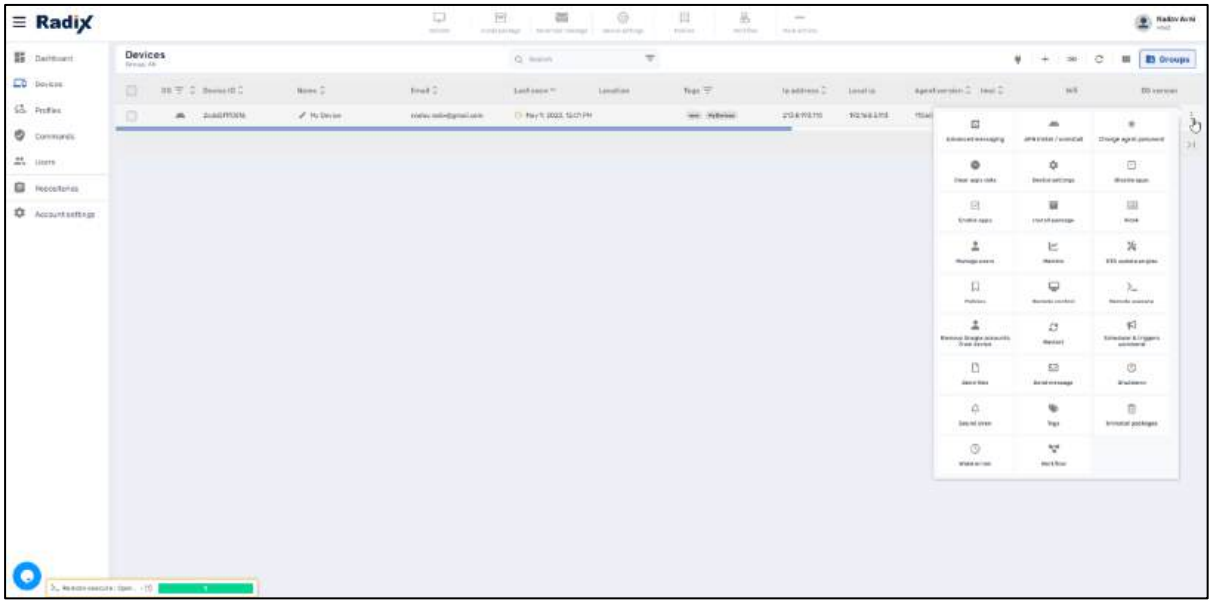


Figure 4-3: Display of Devices Menu Options

The commands will be displayed depending on your device's operating system. (For example, there are 27 available commands for Android devices, and only 5 available commands for ChromeOS devices.)

All the Command options, for all devices, are covered in **Appendix A—Alphabetical List of Commands**.

4.1 Using the Devices Console Ribbon

When you open the Devices Console, you will notice menu options at the top of the page that are inactive. When you check the checkbox for a particular device in the device list, these

menu options at the top of the Devices Console become active. This menu contains the commands that you will employ the most. Depending on your operating system, the remaining commands can be accessed by the “More actions” icon.

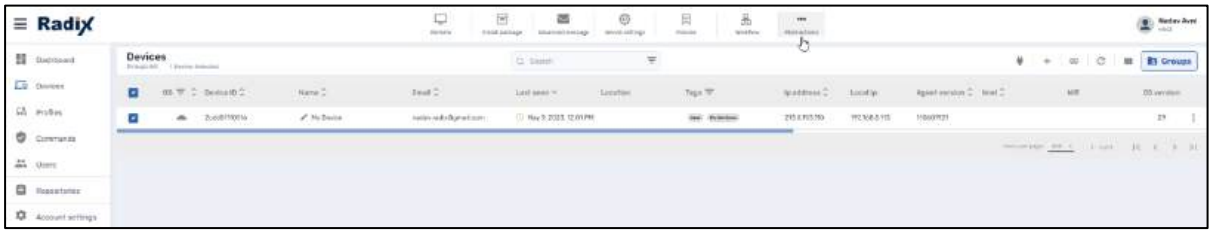


Figure 4-4: Devices Console Ribbon of Commands

Table 4-1: Devices Console Commands

Icon	Description
Remote	Allows the Radix Device Management interface user to access and operate a device remotely
Install package	Allows the Radix Device Management interface user to install a software package on a device
Advanced message	Allows the Radix Device Management user to select a message containing audio/visual content, and send it to a device
Device settings	Allows the Radix Device Management user to modify settings on a device
Policies	Sends a policy for a feature to the device
Workflow	Sends a workflow (= a series of commands to be executed) to the device
More actions	Opens a grid of additional actions that can be performed on a device

We will briefly go through the options in the Devices Console Ribbon:

4.1.1 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.

4.1.1.1 User permission for Remote Control

If the device’s Account Settings require users’ permission for remote control (see **Section 10.1, 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:

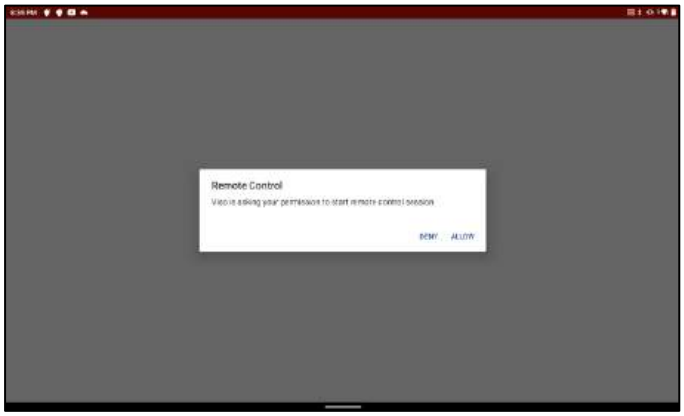


Figure 4-5: Prompt on the user’s device, to allow remote control of a device

After the user allows remote access, the device’s display will appear in the Radix Device Management interface:

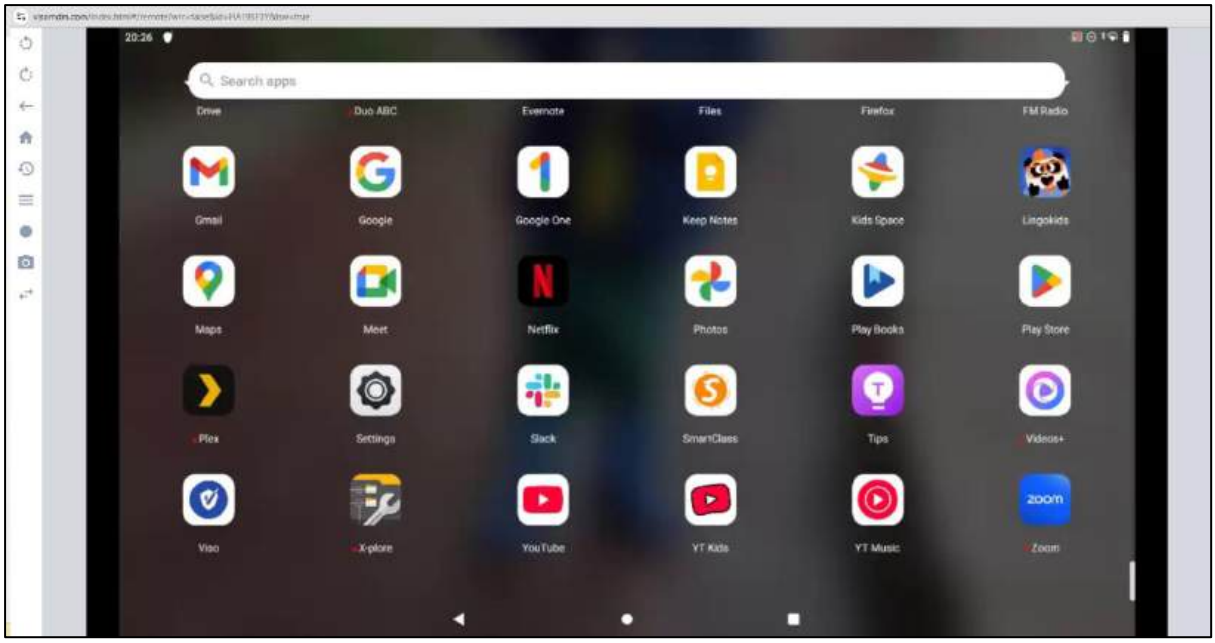


Figure 4-6: Radix Device Management Remote Display of Tablet Computer

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 4-2: 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:

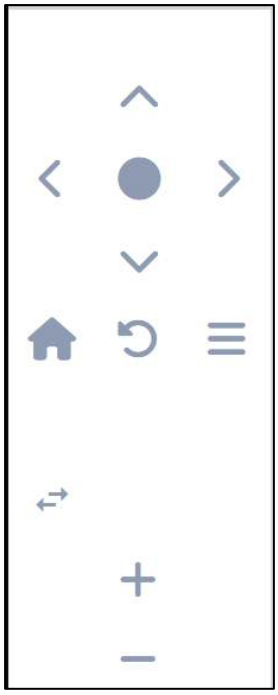


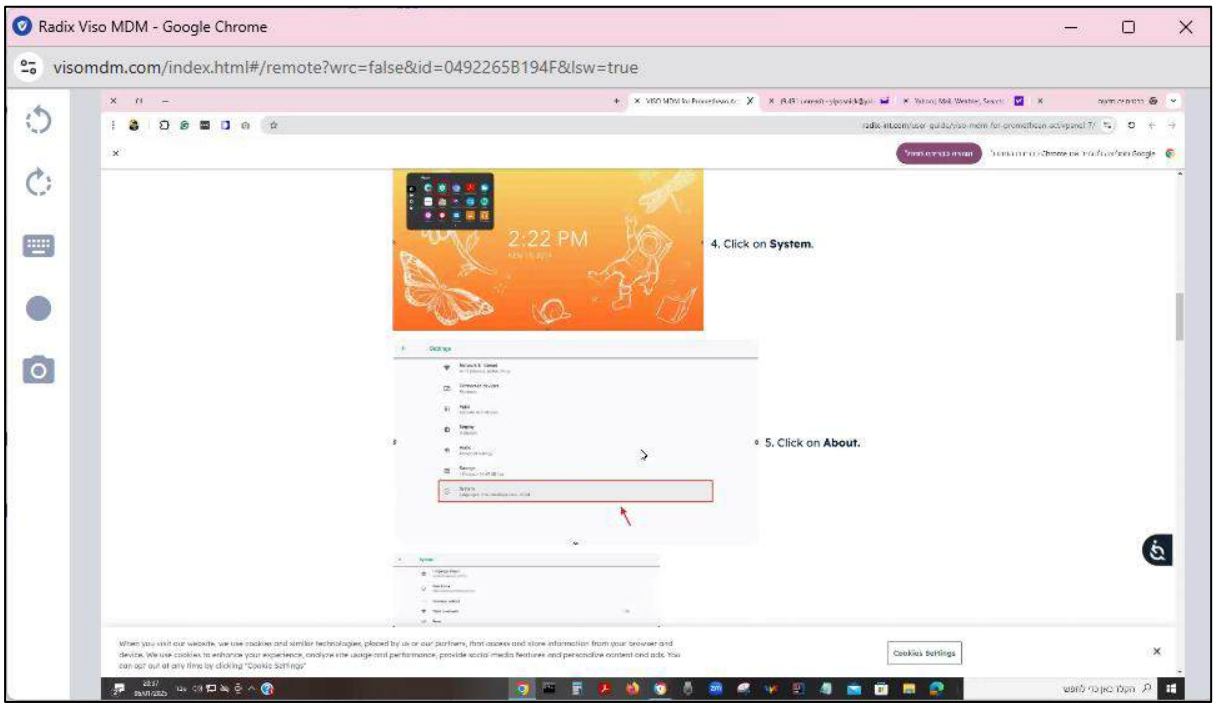
Figure 4-7: Directional Pad Icons

Here is a brief description of the directional pad commands:

Table 4-3: 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:

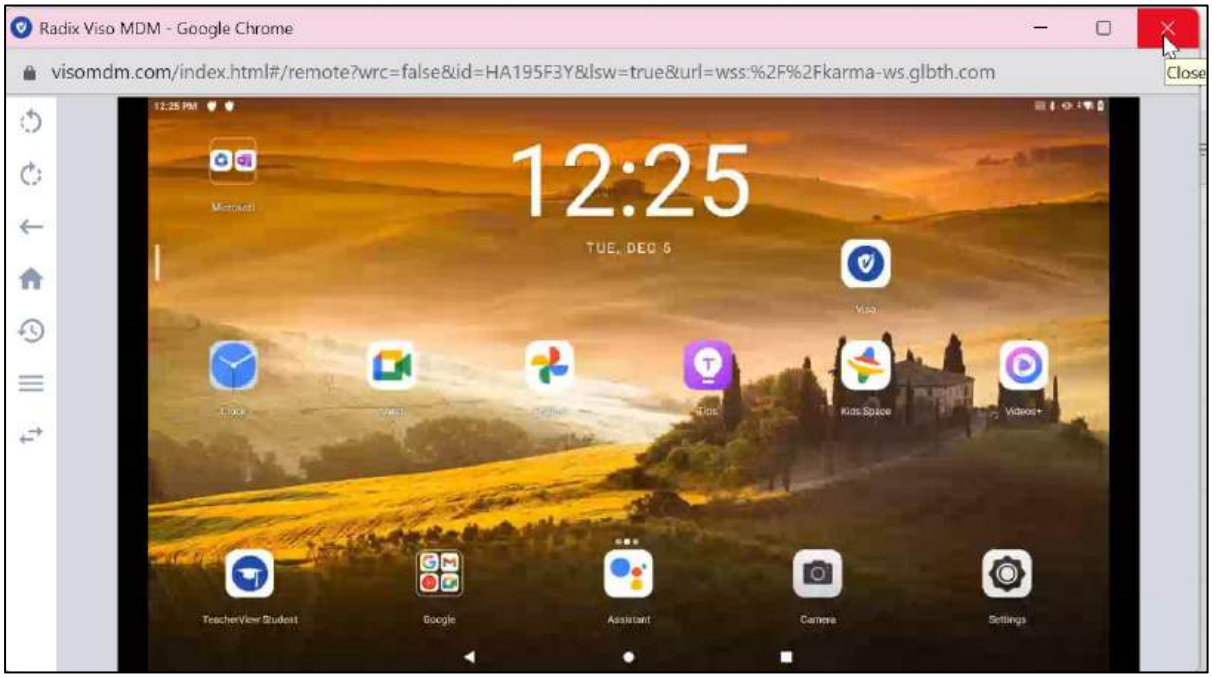


The options in the sidebar menu are as follows:

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

4.1.1.2 Ending a Remote-Control Session

To stop Remote Control mode, simply close the Remote Control window.

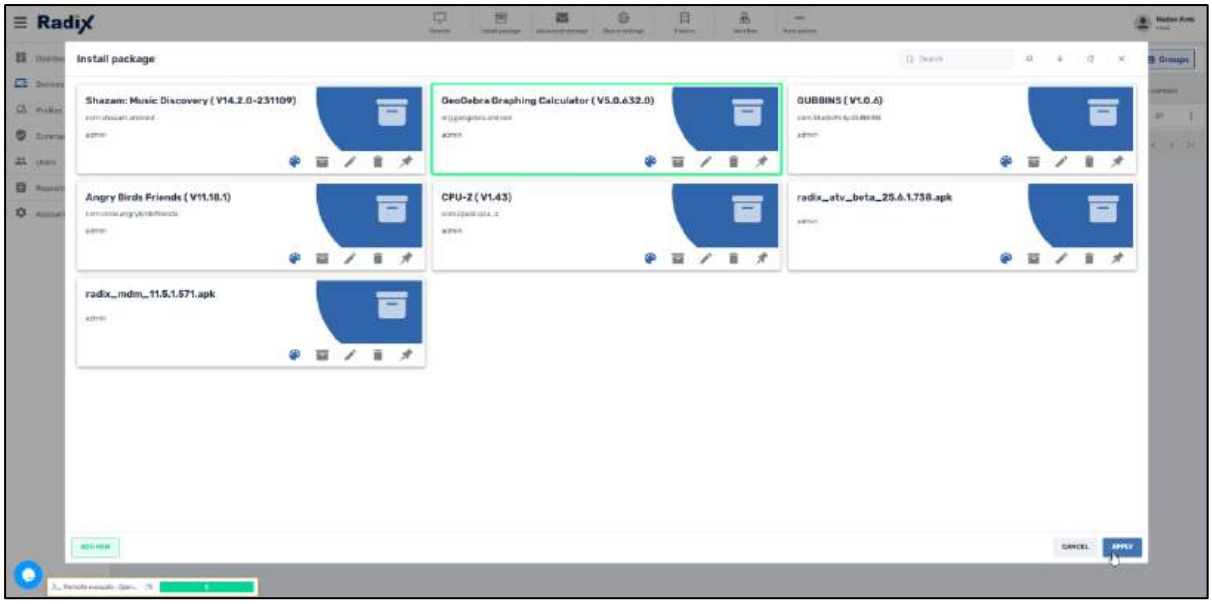


4.1.2 Install Package

This option allows you to remotely install software packages on a particular device. When you click on **Install Packages**, a grid of software packages appears. These are software packages that have already been stored in the Radix system.

4.1.2.1 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 Console, indicating that the app was installed successfully on the device. (The Devices Console will also alert you if the installation failed (a red notification), or in Pending status (a purple notification).)

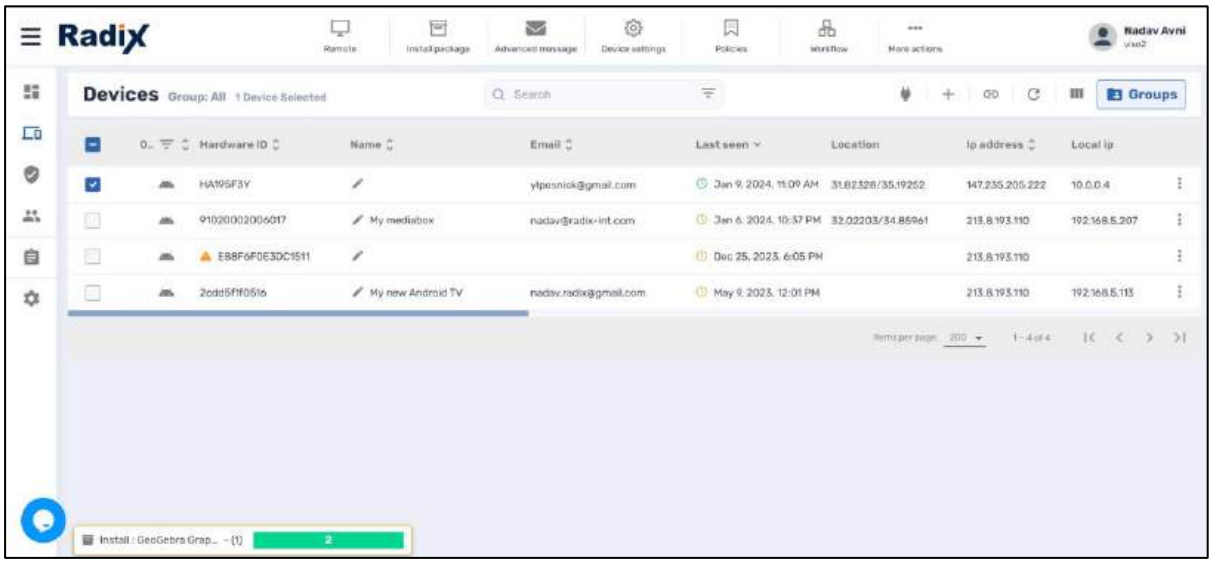


Figure 4-8: Notification that the app was installed successfully

3. Clicking on the notification in the lower left corner of the screen will open the **Command status** screen:

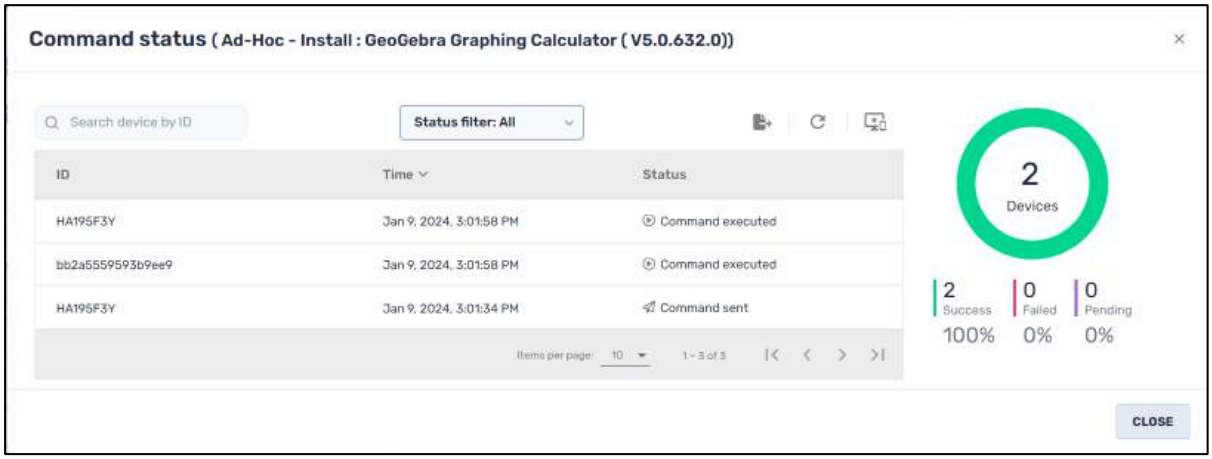


Figure 4-9: Display of status of command sent to a device

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

Table 4-4: Command Status Screen Display Options

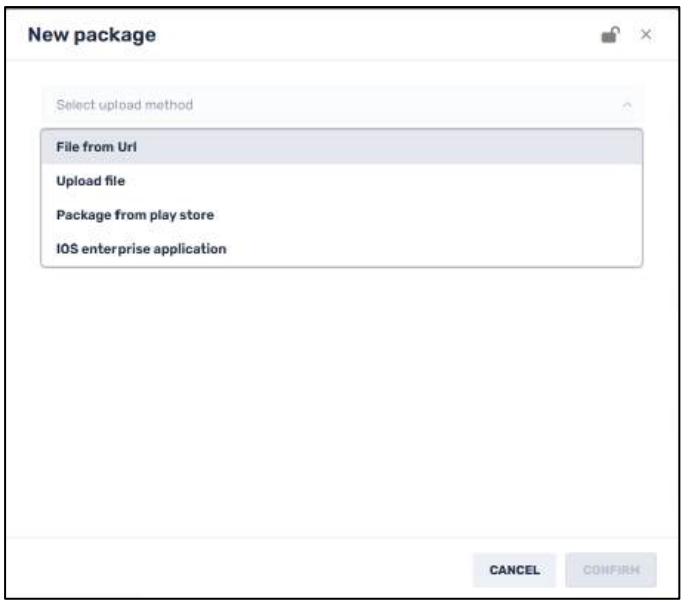
Icon	Description
Status filter: All	Allows you to filter results by commands sent, executed, pending, etc.
	Export to CSV: Allows you to export the table of results to an Excel CSV file
	Refresh: Refreshes the results displayed in the table
	List by Time: Allows you to display the list of commands by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

4.1.2.2 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.)

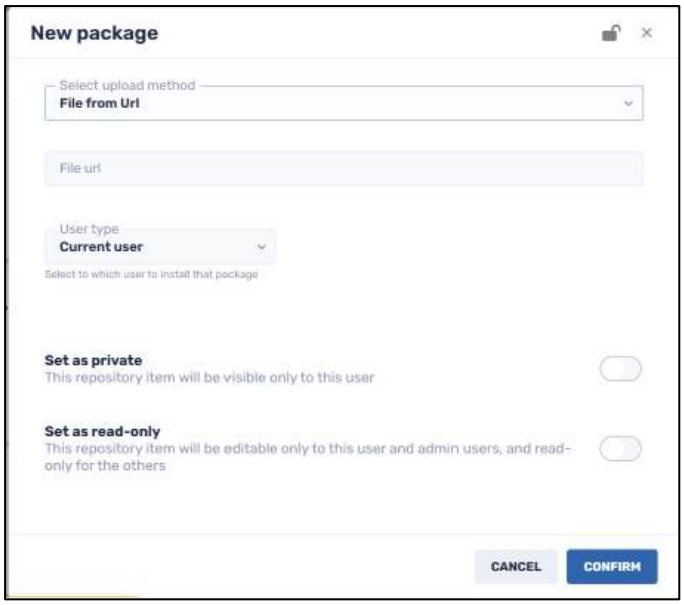
To add a new software package to install:

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

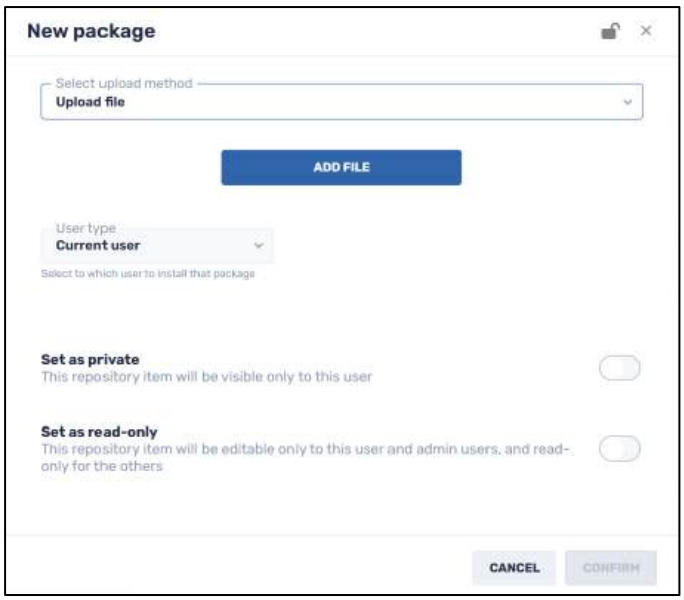


2. You have the option of uploading a new software package from a URL, a file from your computer, from the Google play store, or an iOS enterprise application.

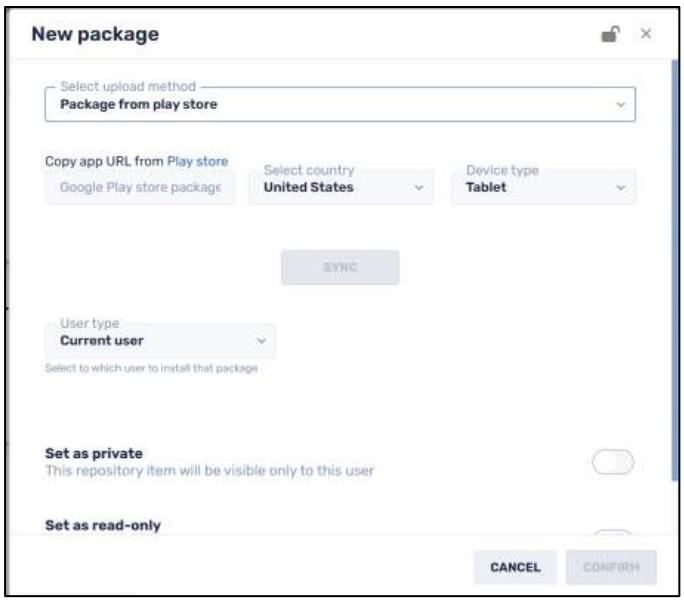
- If you select **File from URL**, you will be prompted for the file's URL.



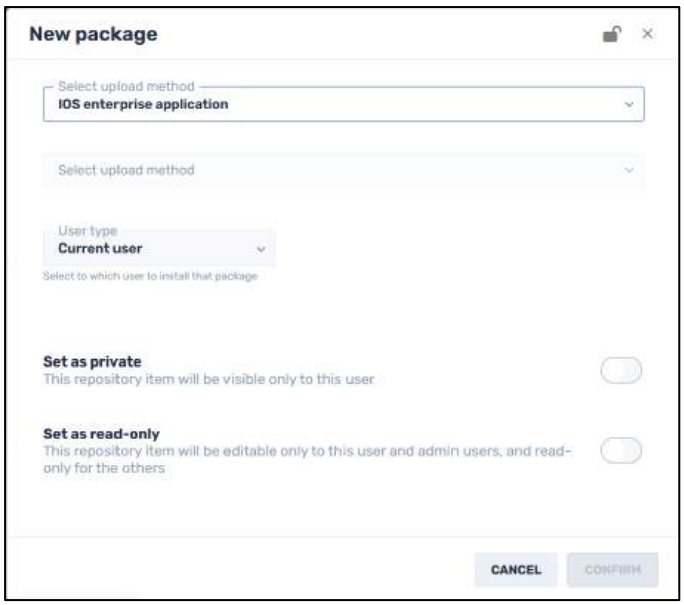
- If you select **Upload file**, you can select a file from your computer.



- 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.



- If you choose **iOS enterprise application**, you will be prompted whether to upload the package by its URL, or from your computer.



- **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 Manager.
- **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 .

4.1.2.3 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 Console, click on the Groups icon Groups. The Groups window opens.
2. Find the group to which you wish to install the software packages, and click on its three-dot menu:

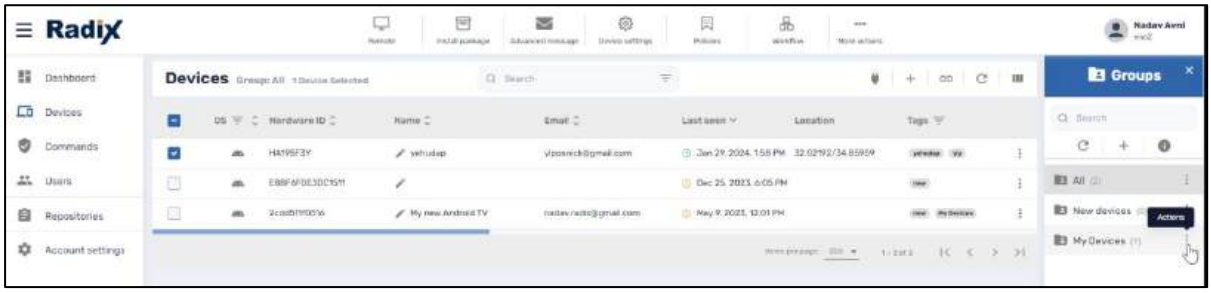


Figure 4-10: Groups three-dot menu, for executing commands to entire groups of devices

The Commands panel opens.

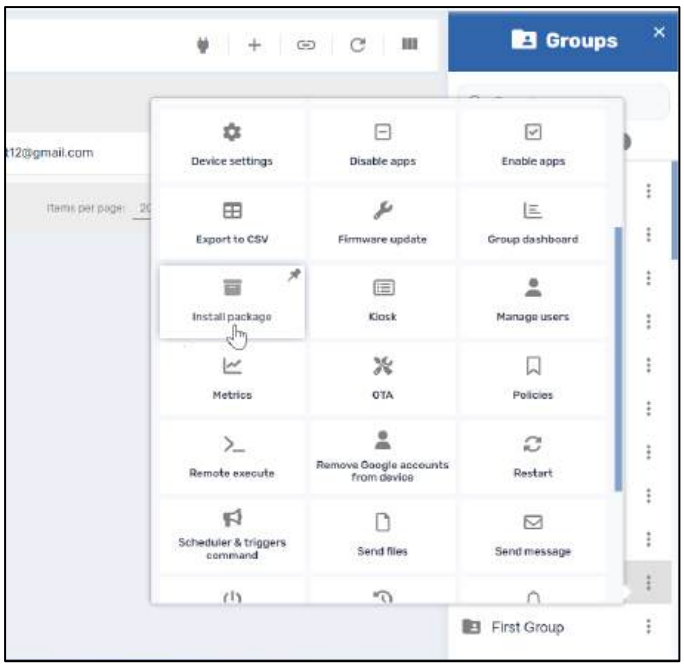


Figure 4-11: Groups Command panel, showing the Install Package command tile

3. Select the **Install Package** icon. The Install Package window opens.
4. Select the desired software package and click **Apply**. The software package will be installed on the entire group of devices.

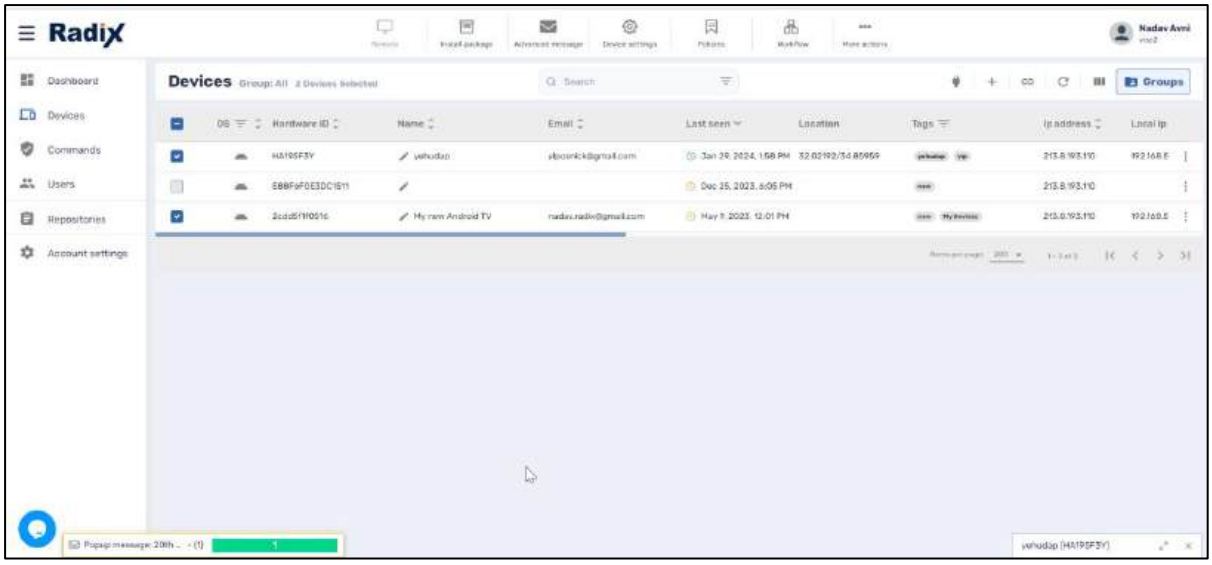
5. You can later check the success of the installation by opening the Commands Status window (**Section 6.3**).

4.1.2.4 Installing a Software Package on Selected Devices

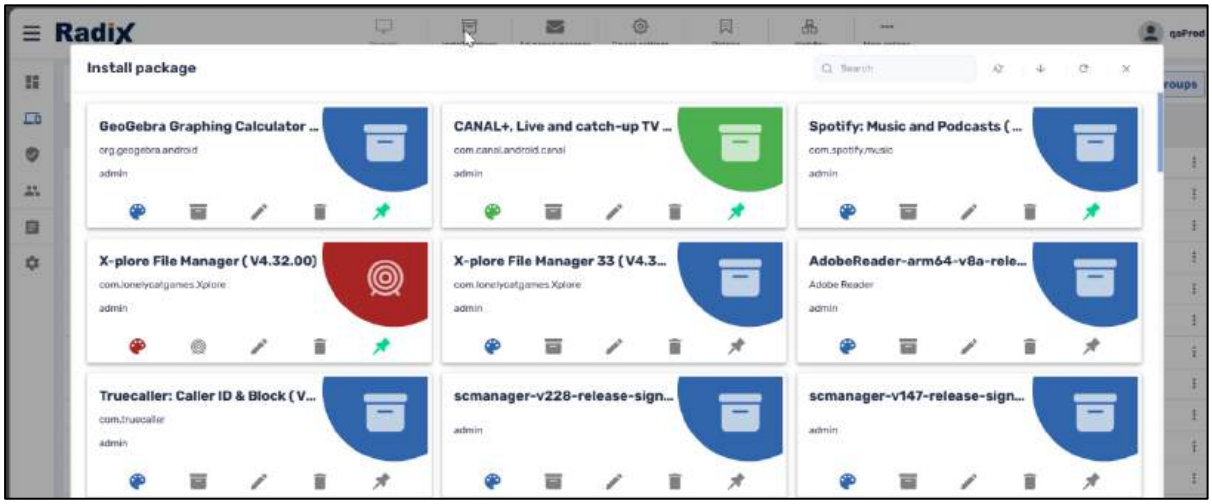
There is also an option to select particular devices manually and install a software package on them.

To select devices manually:

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



3. Click on the **Install Package** icon in the Devices Console Ribbon. The Install Package window opens.



4. Proceed as above to select and install packages.

4.1.3 Advanced 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.

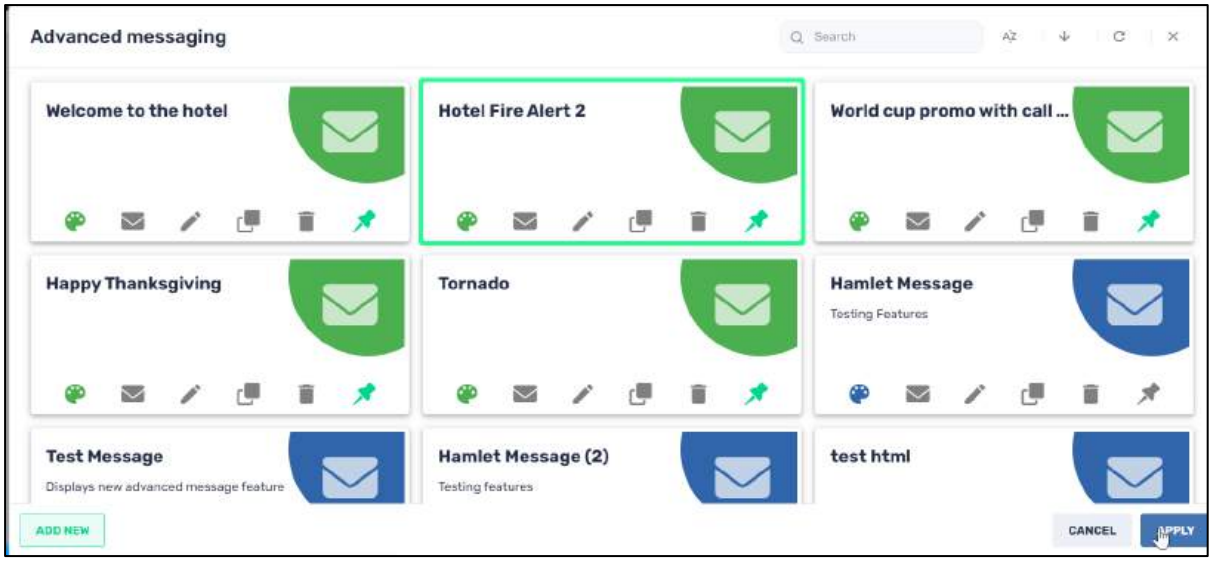
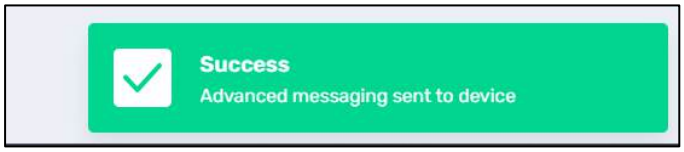


Figure 4-12: Advanced Messaging Grid of Options

To use an existing advanced message:

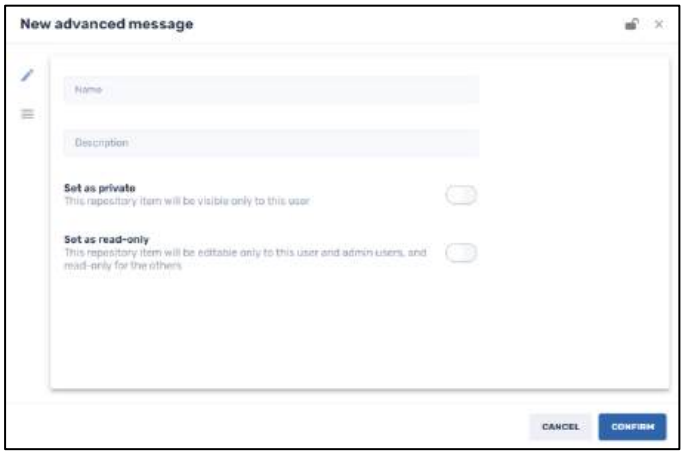
1. Select one of the messages and click **Apply**.
2. If the message is successfully sent, a "Success" prompt will appear in the lower right corner.



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.



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

4. 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 .

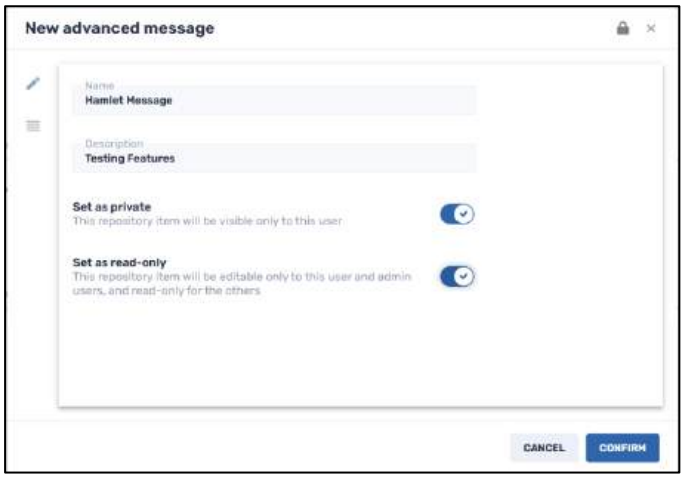
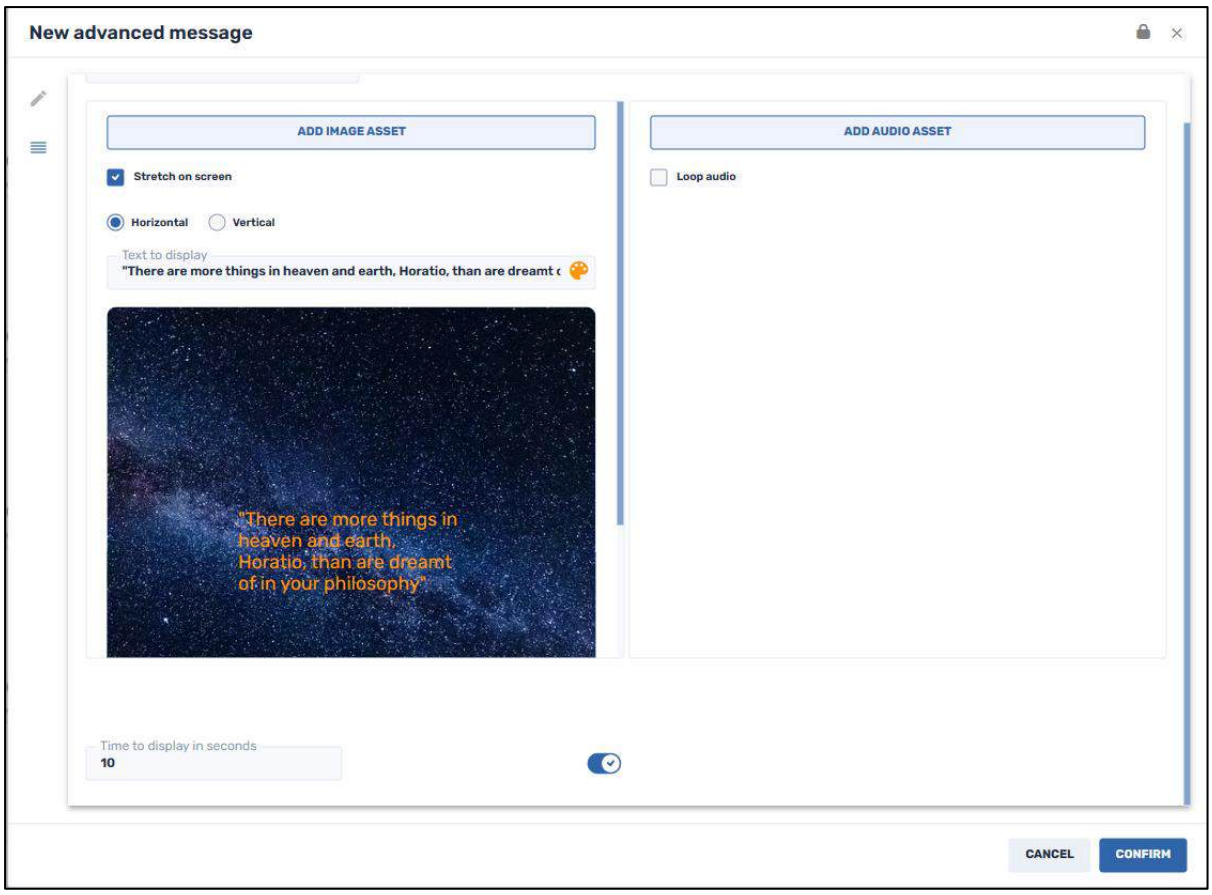
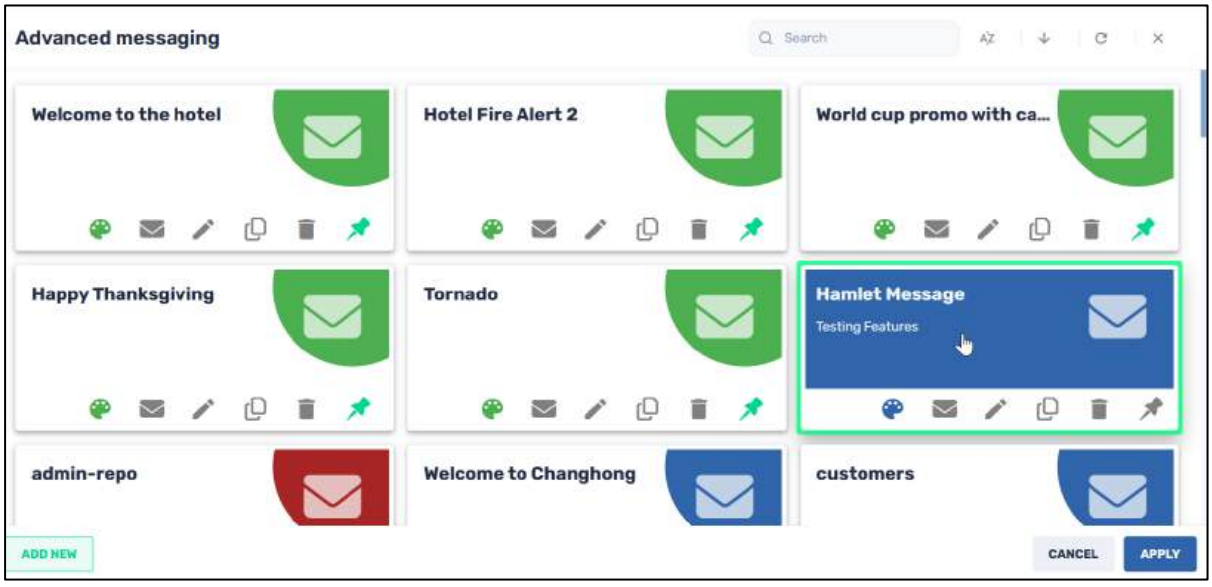


Figure 4-13: New Advanced Message Screen, in Edit mode

5. 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**,
   - **An embedded URL/HTML text**.



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



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

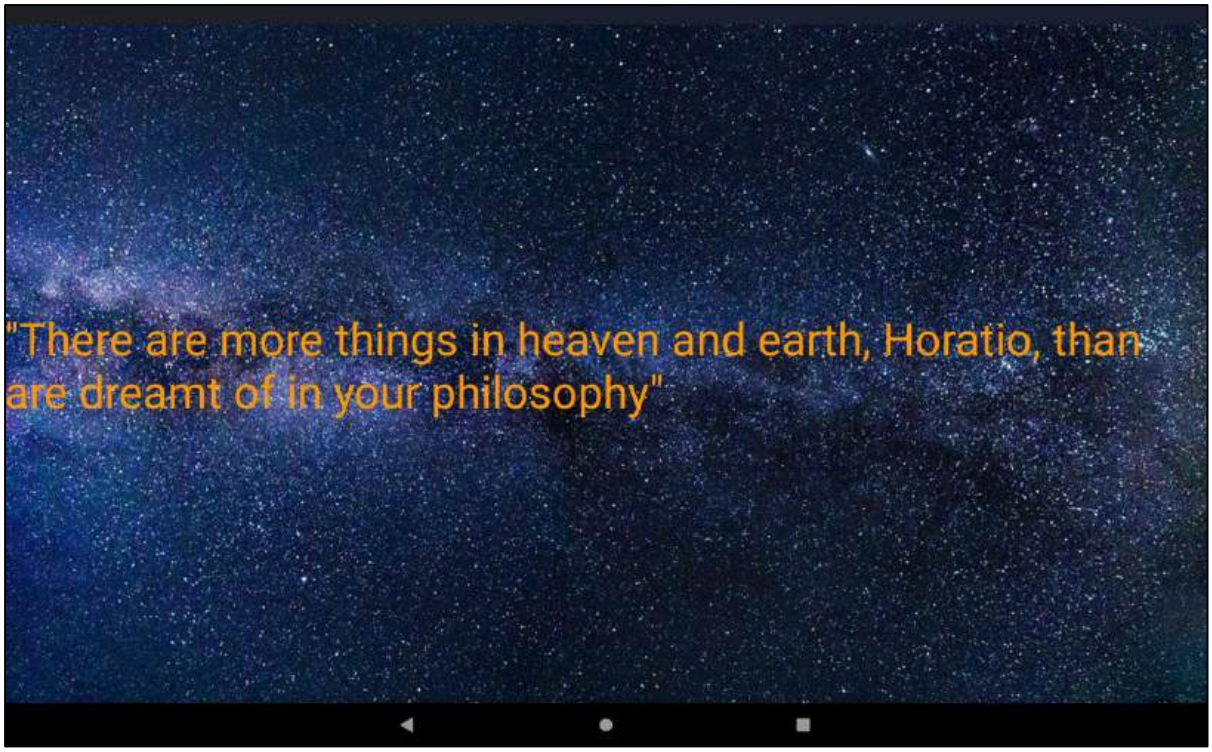


Figure 4-14: Display of an Advanced Message on the remote device

4.1.4 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:

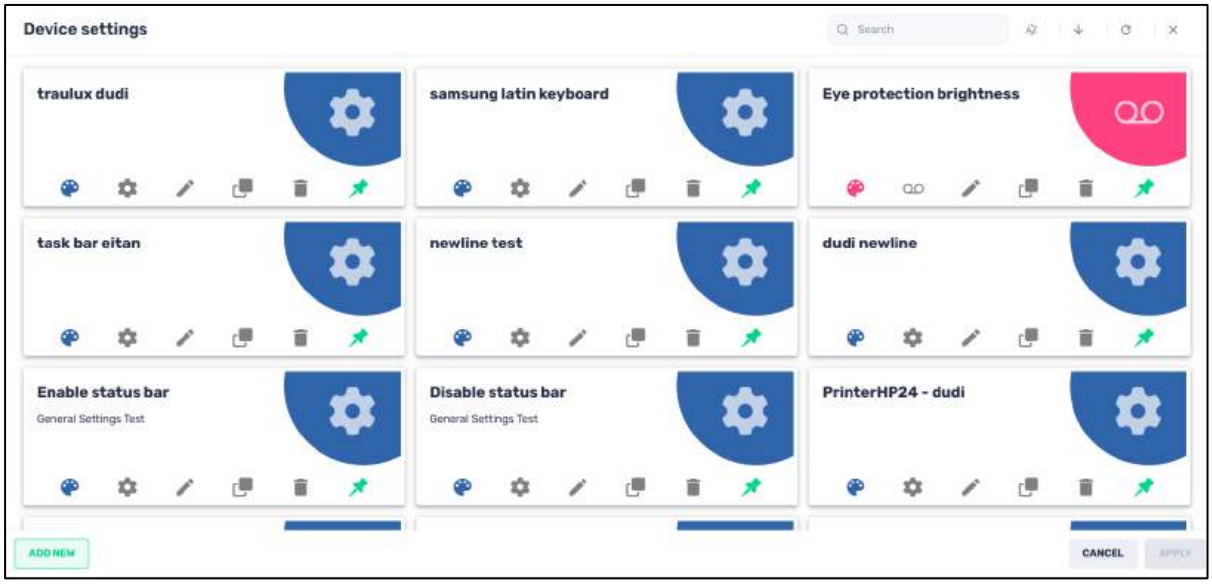


Figure 4-15: Device Settings options

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.

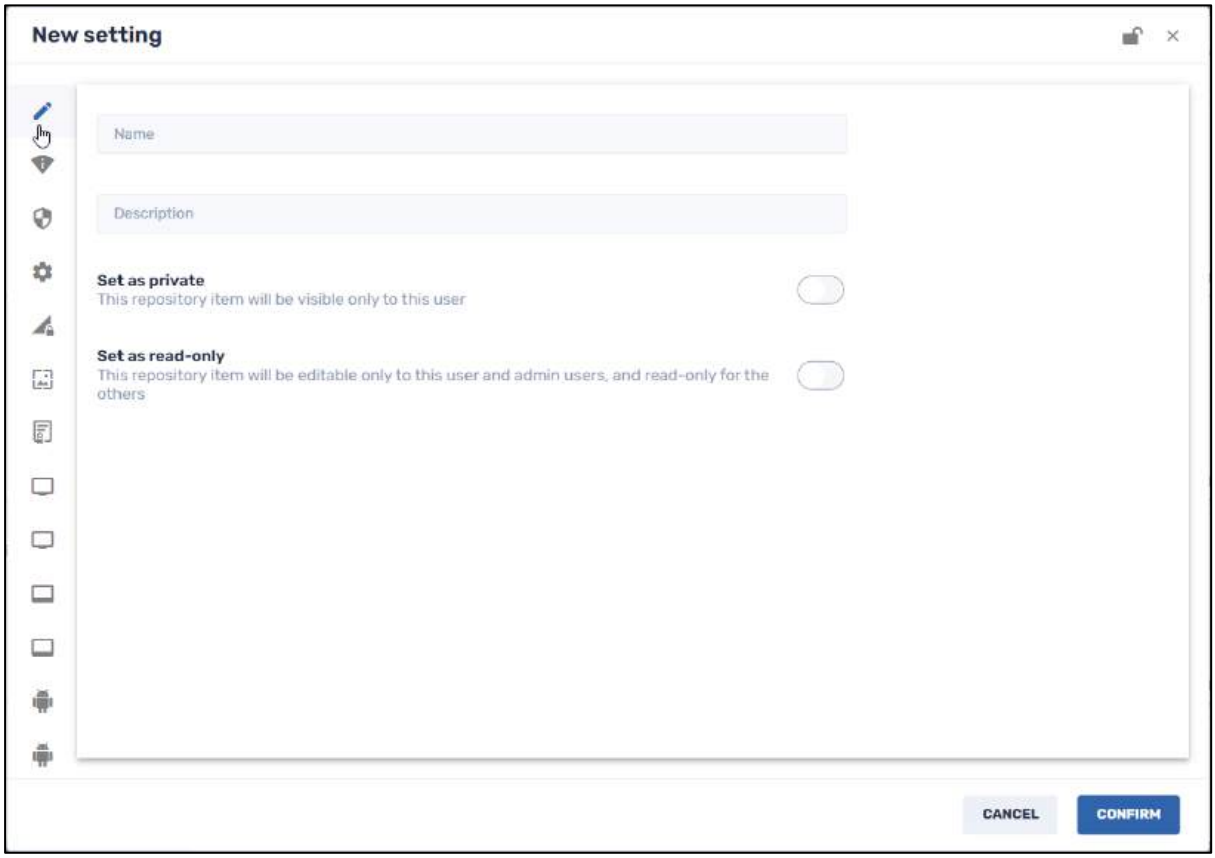


Figure 4-16: New Device Settings screen

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

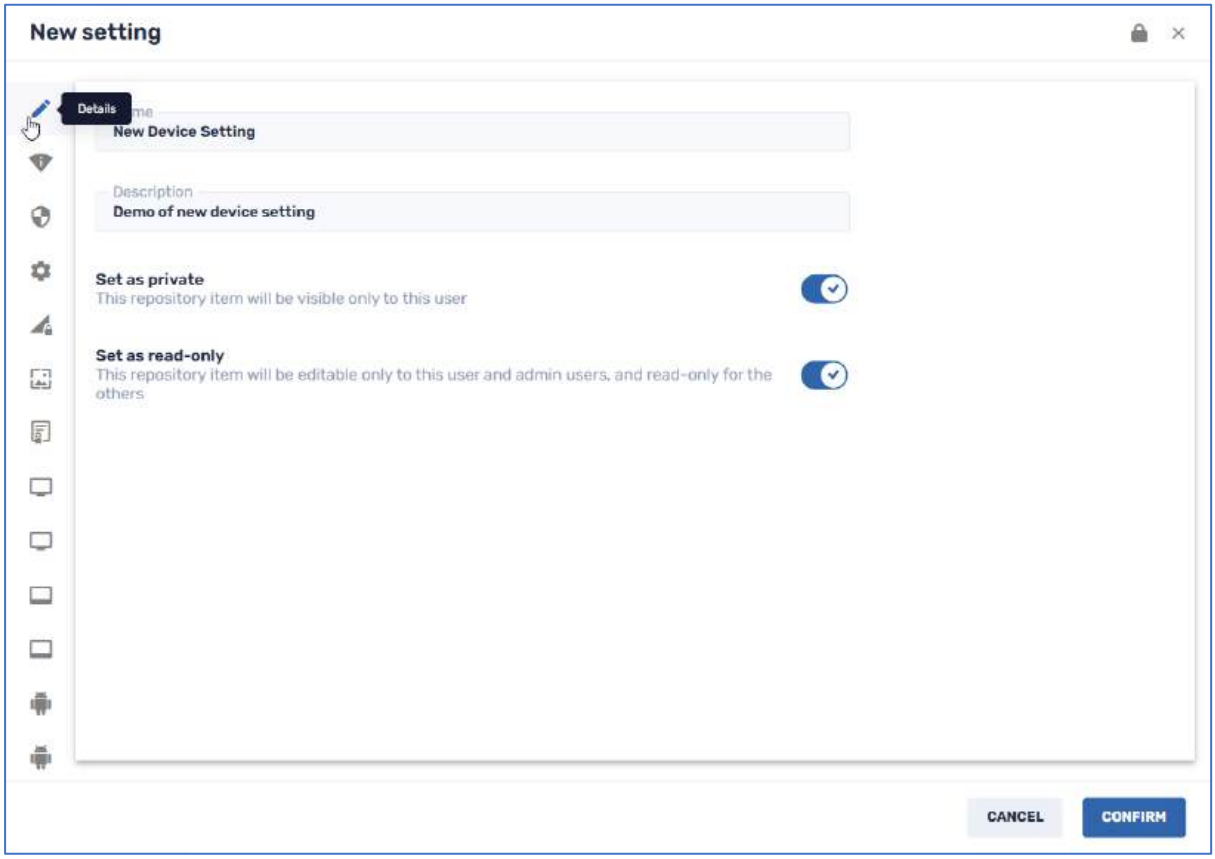
Table 4-5: Device Settings Options

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)

4.1.4.1 Edit Details

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

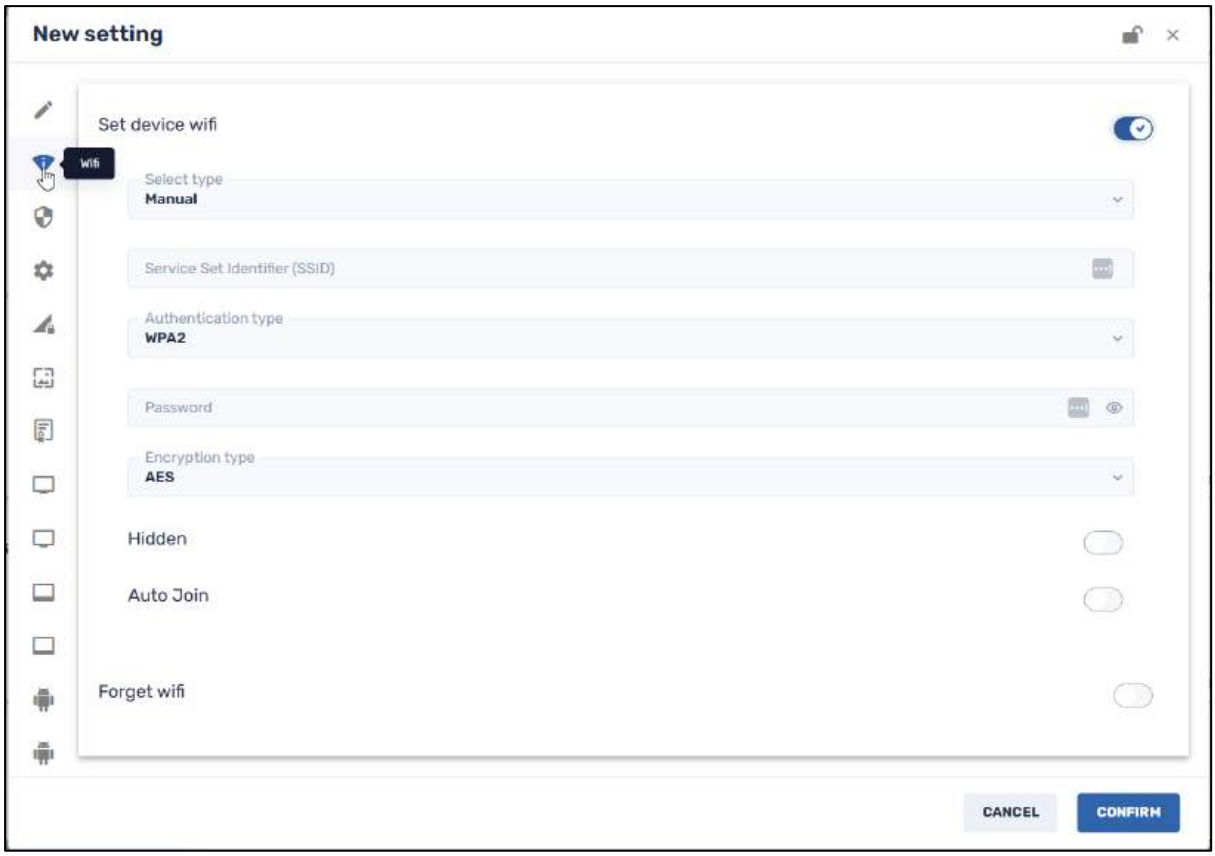


There are two additional options to limit who can view and edit this device setting:

- **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 Manager.
- **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 .

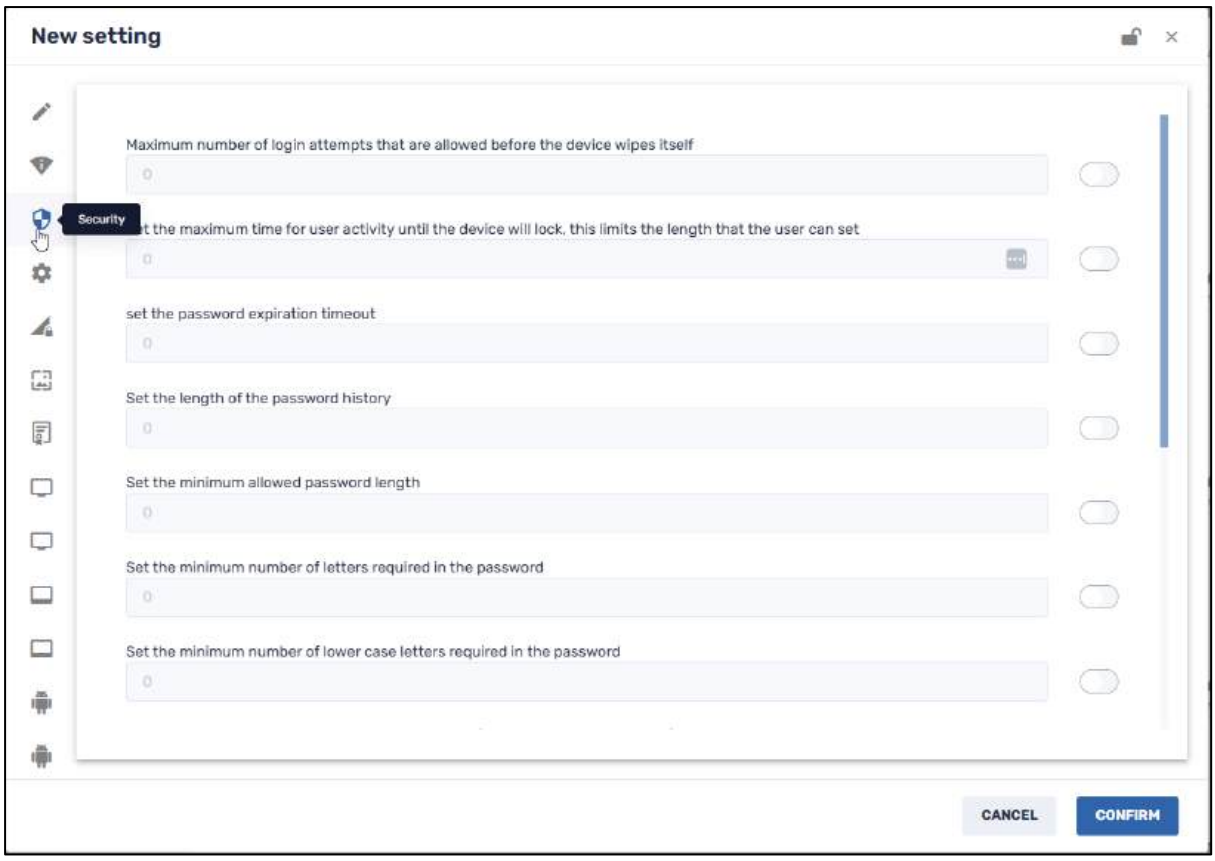
4.1.4.2 Wi-Fi

This opens a pane to set the device's Wi-Fi connectivity details. You can also choose an option to "forget" the Wi-Fi connection:



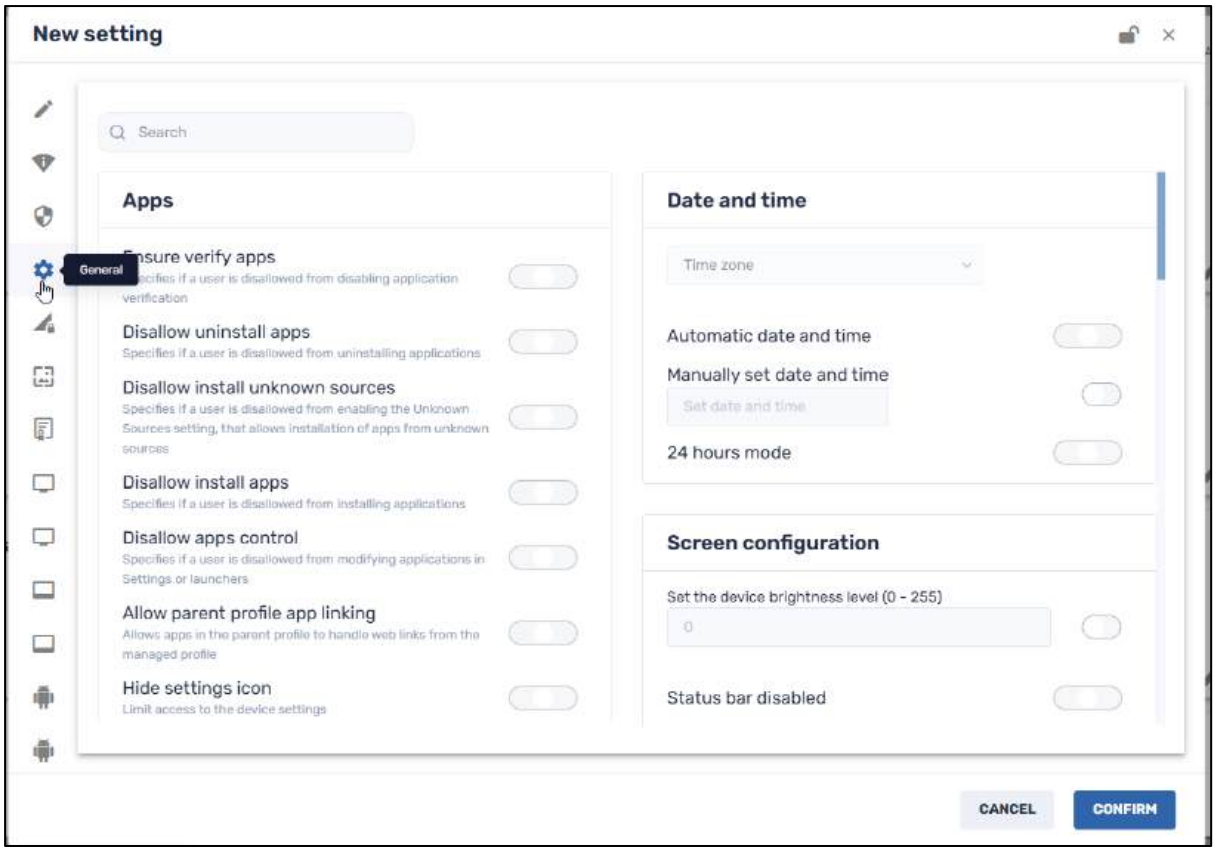
4.1.4.3 Security

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



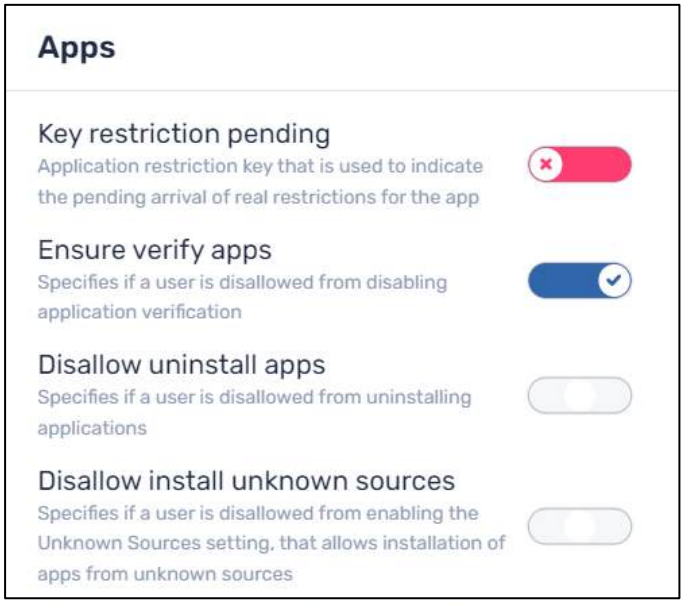
4.1.4.4 General Settings

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):

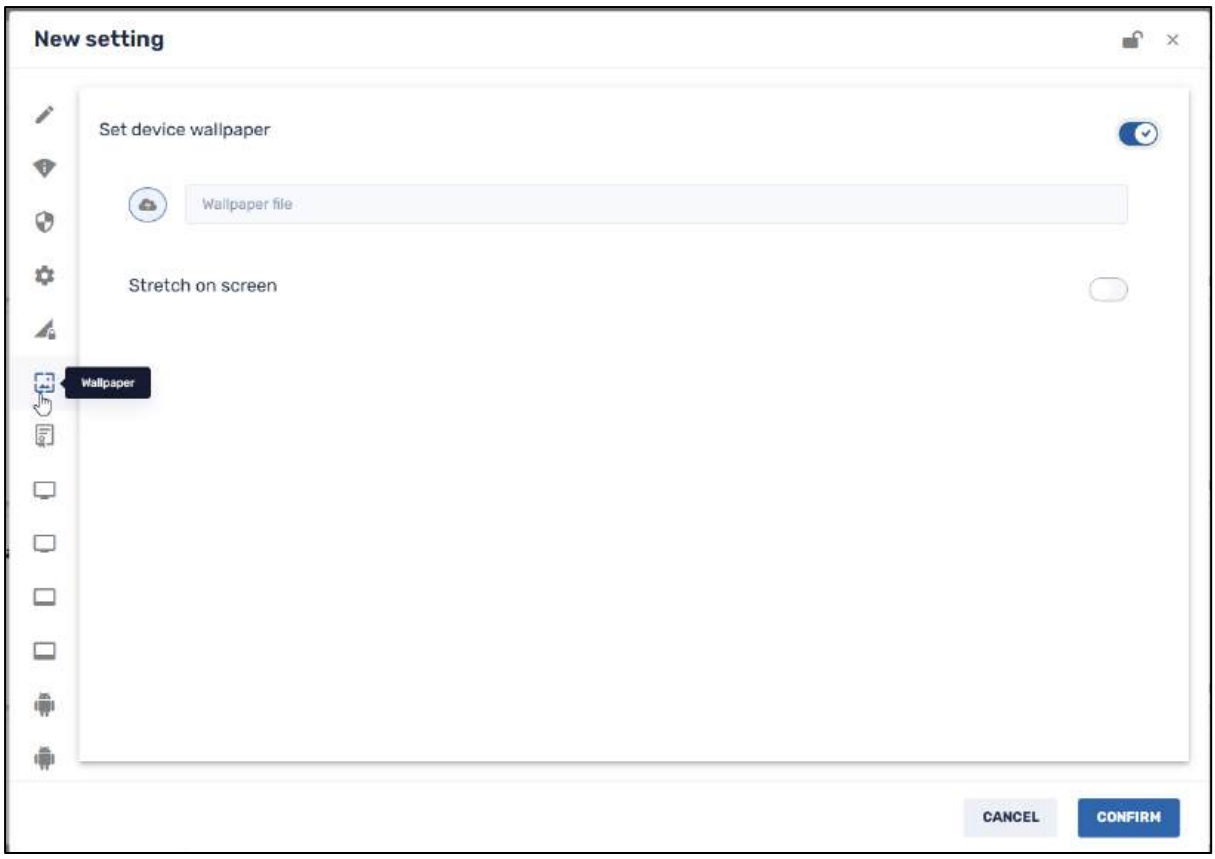


4.1.4.5 Set APN

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).

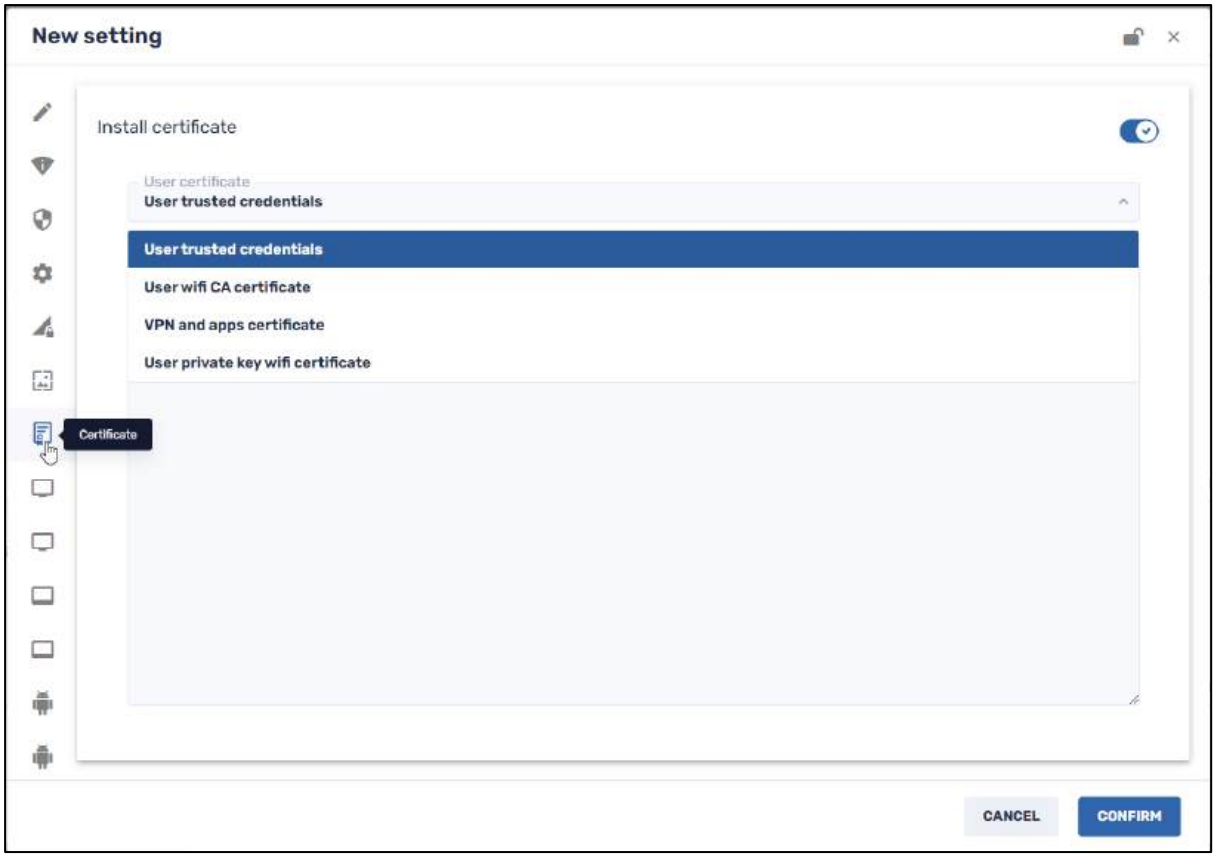
4.1.4.6 Wallpaper

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



4.1.4.7 *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:

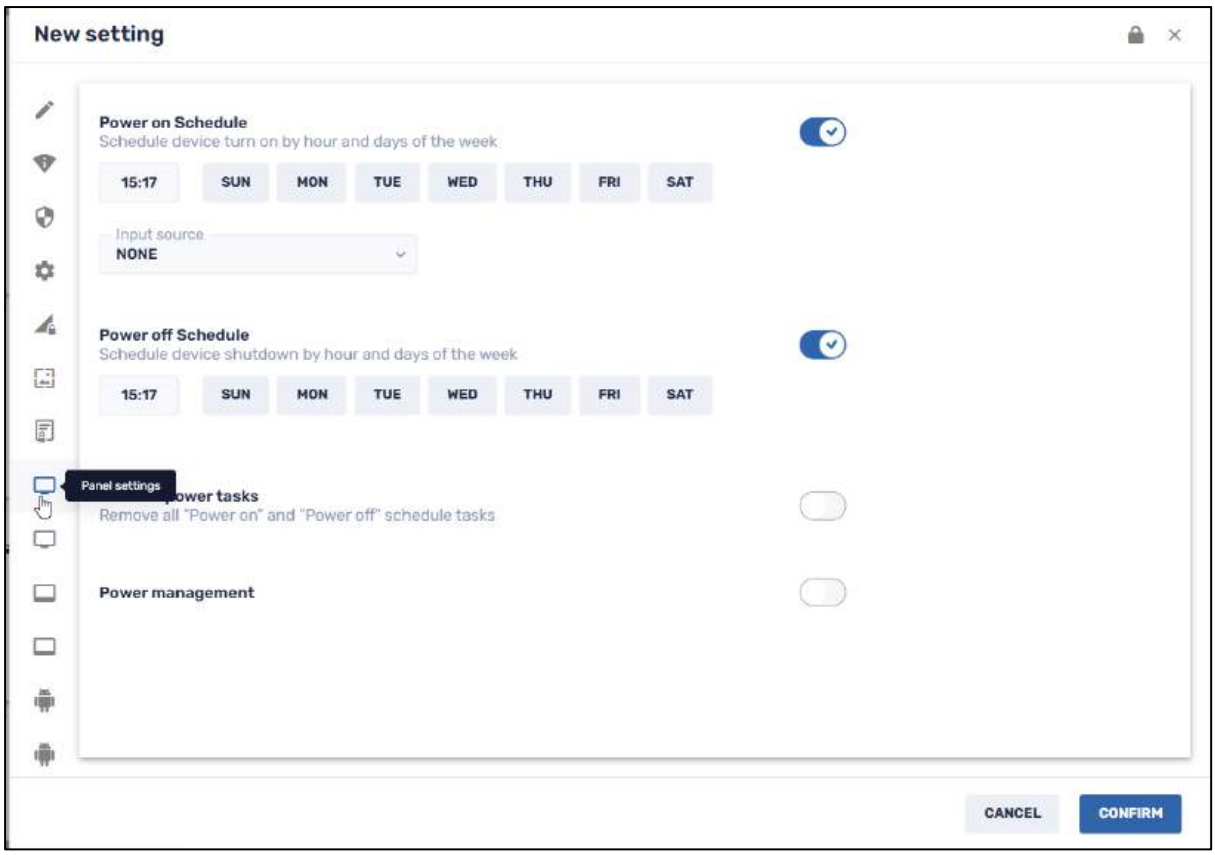
- User-trusted credentials
- User Wi-Fi CA (=Certificate Authority) certificate
- VPN and apps certificate
- User private key Wi-Fi certificate

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**.

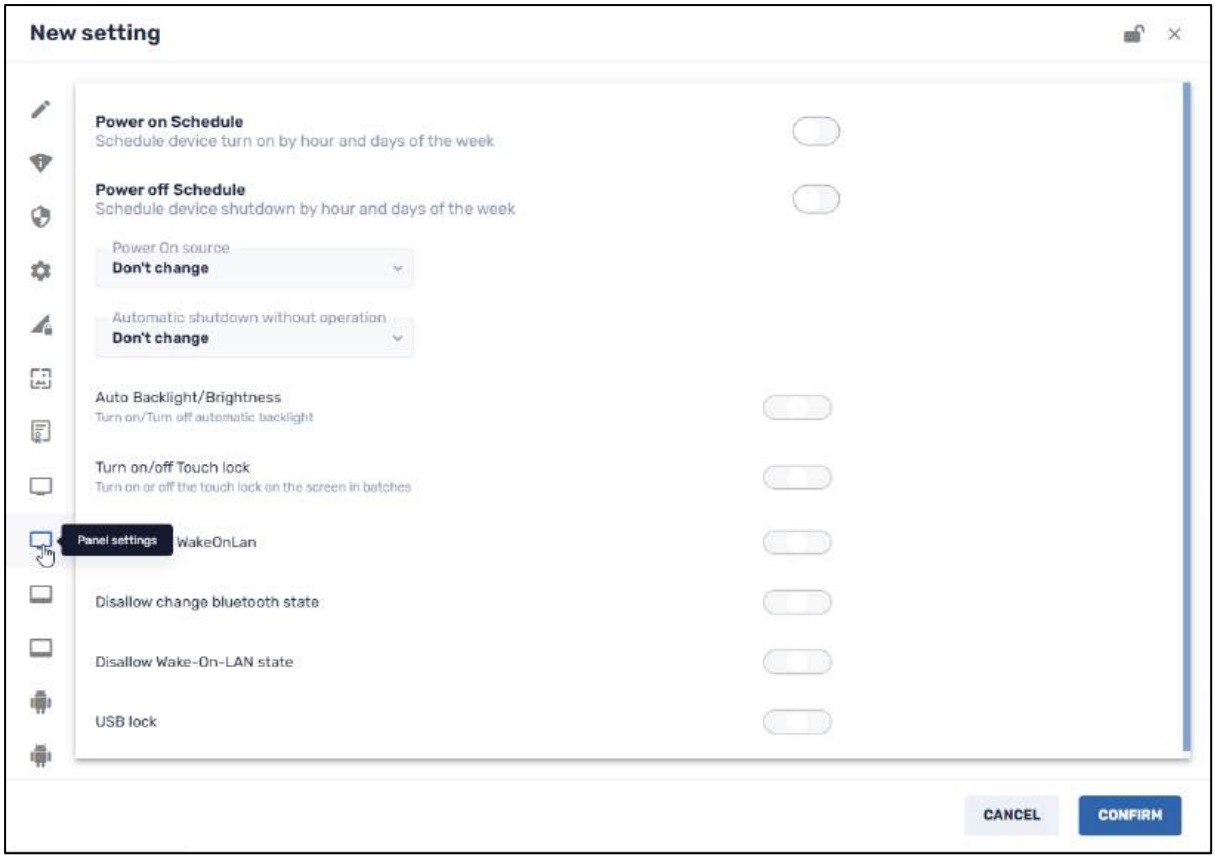
4.1.4.8 Panel Settings---First Panel (For Specialized Use)

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



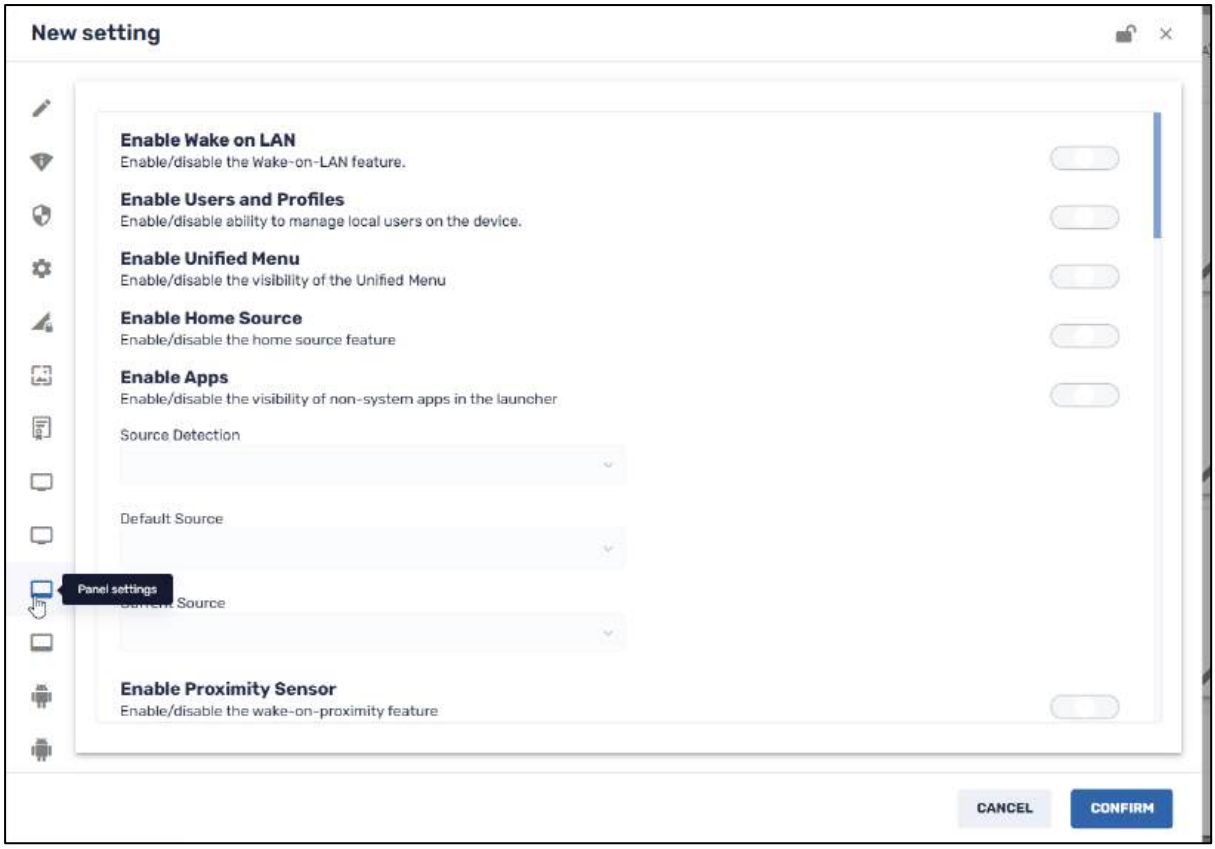
4.1.4.9 Panel Settings—Second Panel (For Specialized Use)

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.



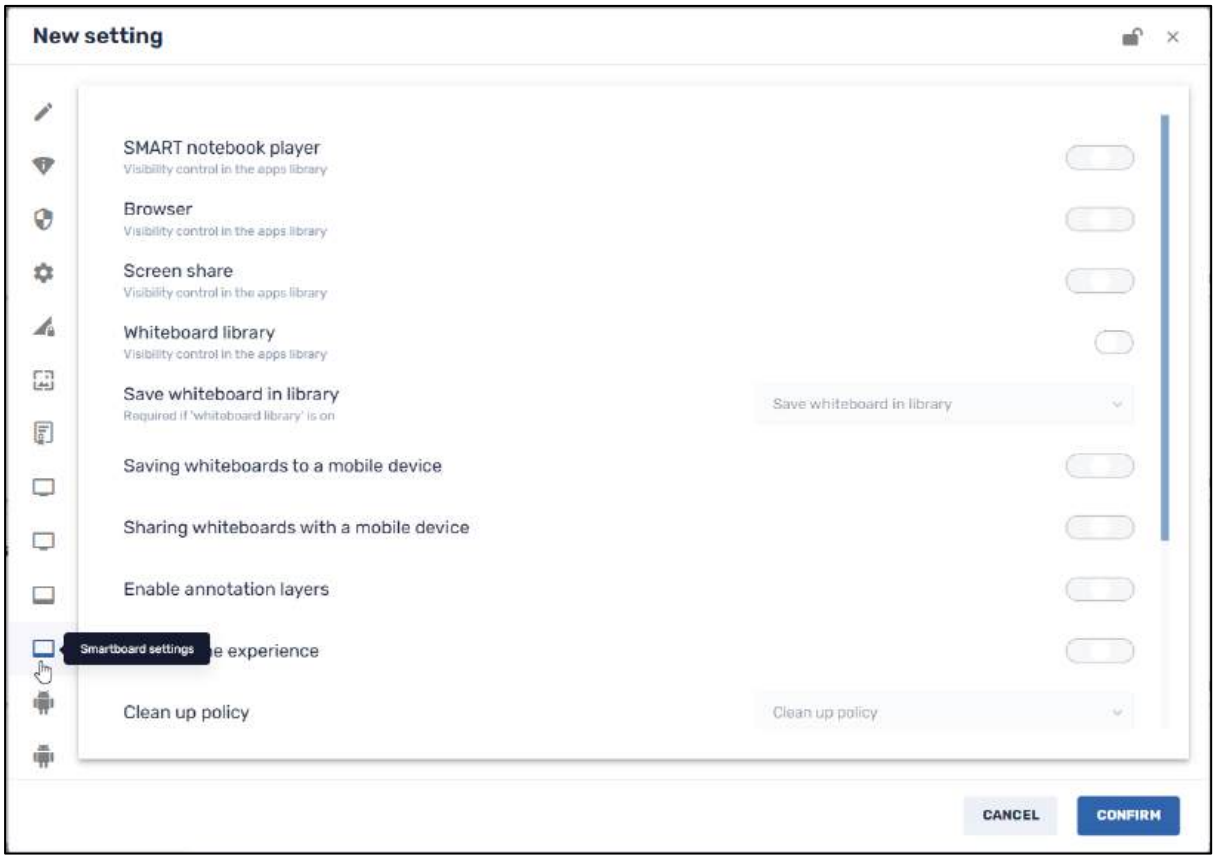
4.1.4.10 Panel Settings—Third Panel (For Specialized Use)

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



4.1.4.11 *Smartboard Settings*

These are specialized device settings for smartboard panels.



4.1.4.12 App Permissions/Configurations

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

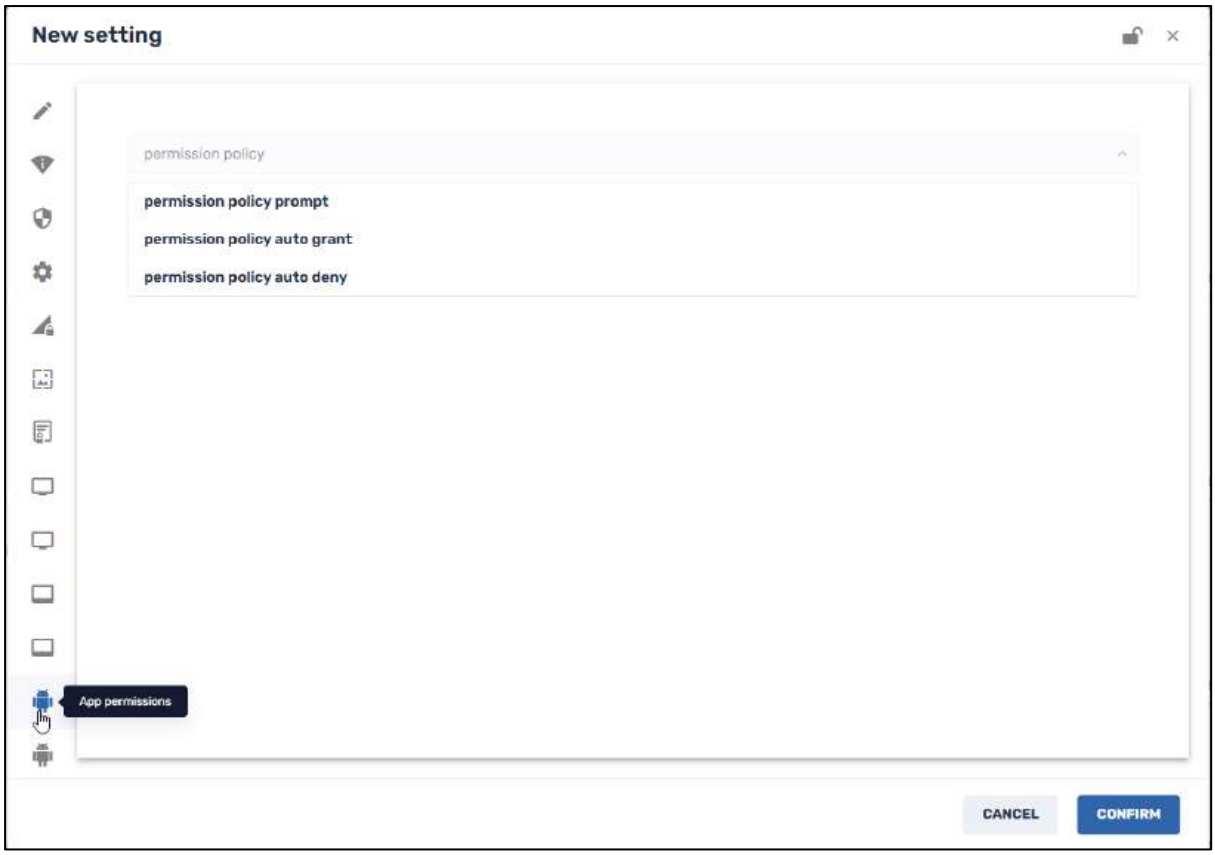


Figure 4-17: App Permissions Settings

Figure 4-18: App Configuration Settings

4.1.5 Policies

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 **Policies** option in the Devices Control Ribbon.

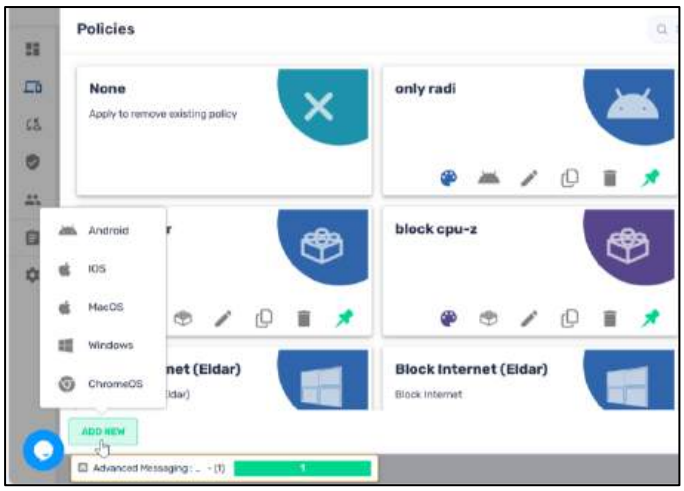
When you click on **Policies**, a grid of stored policies appears.

4.1.5.1 Applying a Software Policy

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

To add a new policy:

1. Click on the **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.

4.1.5.1.1 Adding a New Android Policy

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

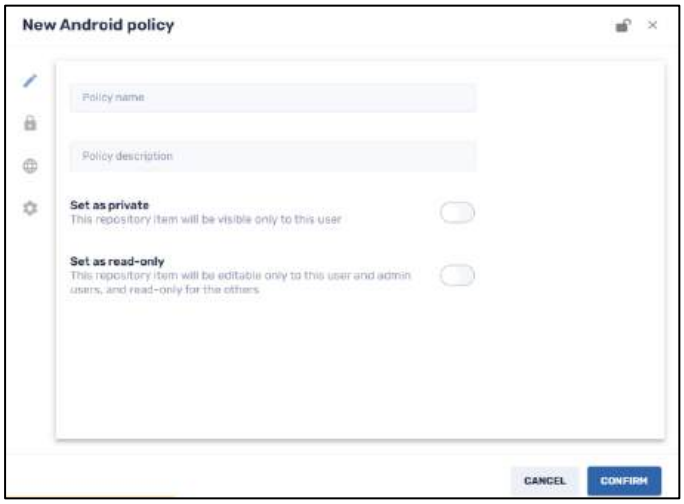


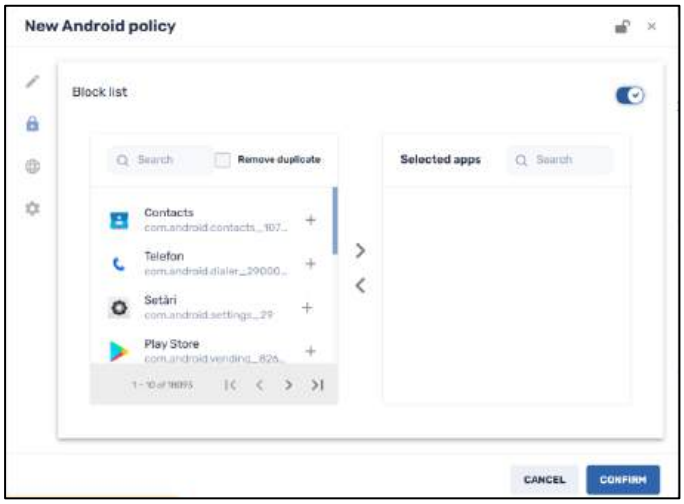
Figure 4-19: Android Policy Edit Screen

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

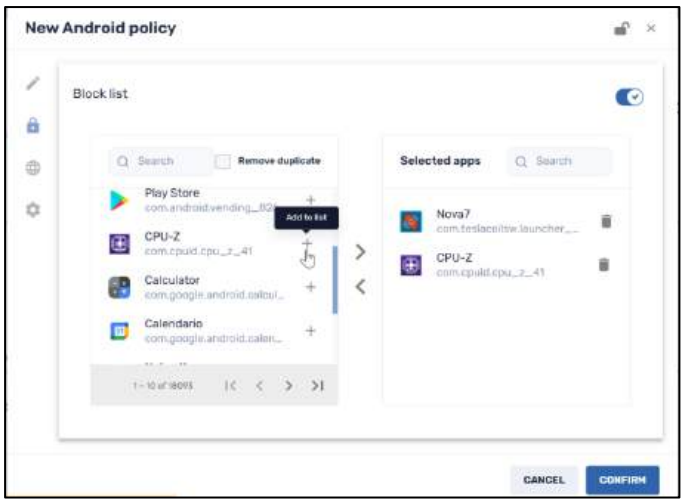
Table 4-6: Android Policies icons

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 Manager.
3. 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 .
4. Click on the **Block List** icon . The **Block List** window opens.

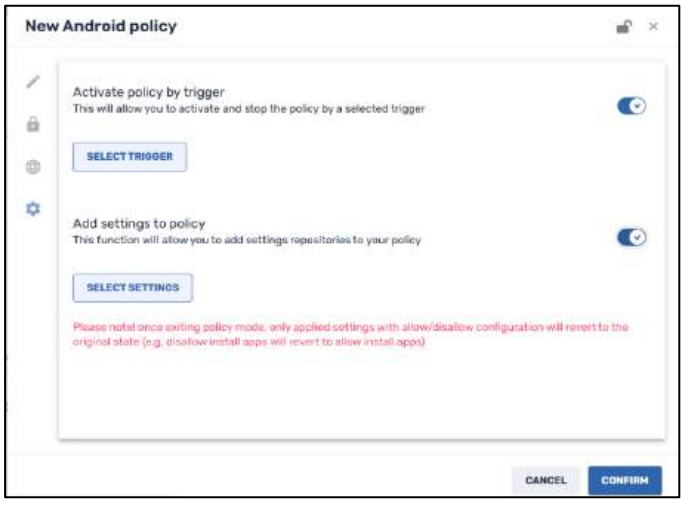


5. Select the apps that you wish to block from the device by clicking on the **Add to list** icon. The selected apps will now appear in the right-hand column of Selected apps.



6. 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.
7. Supply the URLs of the apps to be blocked, or to be allowed.

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



9. Supply the trigger and settings and 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**.

4.1.5.1.2 Adding a New iOS Policy

When you select the option to add an iOS policy, the following window appears.

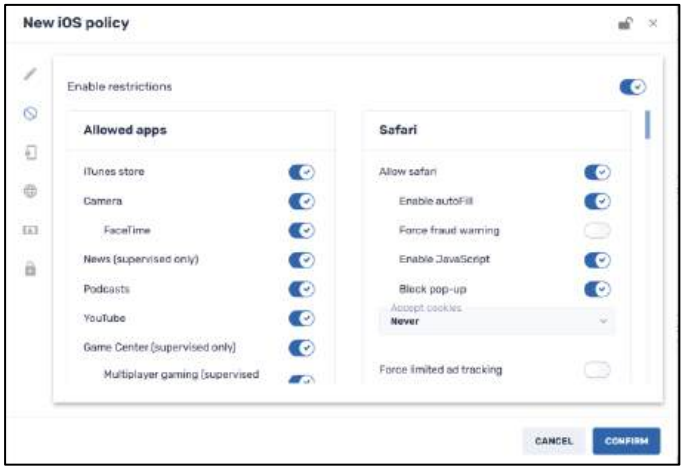
The following is a brief explanation of the icons on the left of the iOS Policy screen:

Table 4-7: iOS Policies icons

Icon	Description
	Edit Details
	Enable restrictions
	Passcode
	Content Filter
	Single app
	Block List

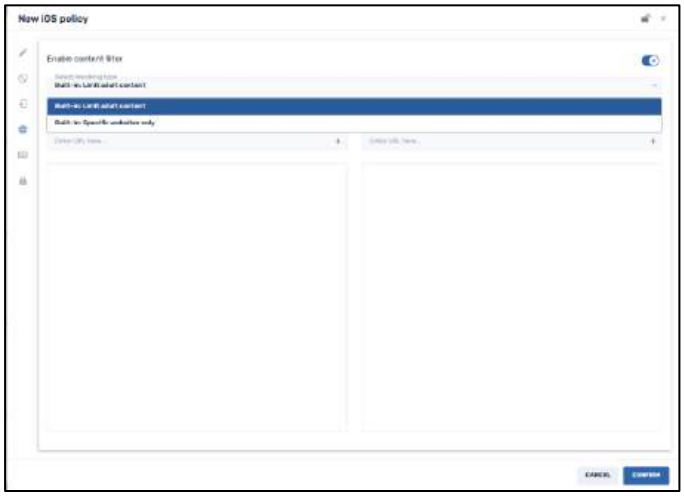
2. In the **Edit Details** window, enter a policy name and description.
3. Click on the **Set as private** button if you would like the iOS policy option to only be visible to you (the creator of the item) when using the Radix Device Manager.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the iOS 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 **Enable restrictions** icon. You will have options to allow and disallow apps and control the settings on the Safari browser, Siri, iCloud, and more.

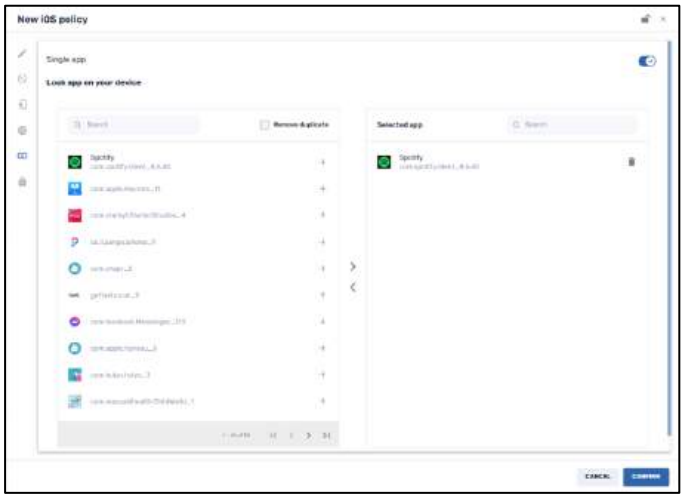


6. Click on the **Enable Passcode** icon. You will be able to set the parameters for the passcode on the iOS device.

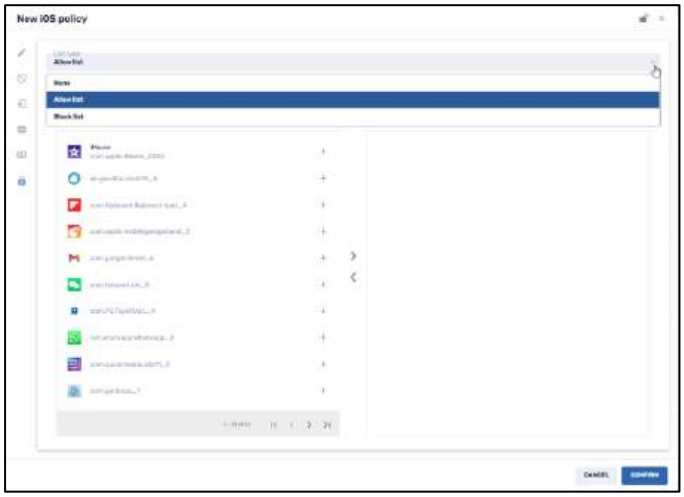
7. Click on the **Enable Content Filter** icon. A window opens that lets you filter out inappropriate websites or limit the browsing on the iOS device to specific websites.



8. Click on the **Single app** icon. You will be presented with the apps installed on the iOS device. By clicking on the **Add to list** + icon, you can select which app to be locked onto the device, so that it will only be able to run that specific app.



9. 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.
10. Click on the **Block List** icon, to choose whether you would like to make a list of allowed apps, or apps to be blocked on the iOS device.



11. Supply the URLs of the apps to be blocked, or to be allowed.
12. Click **Confirm**. The new policy will appear in the **Policies** window.
13. Apply the policy to a device by selecting the policy and clicking **Apply**.

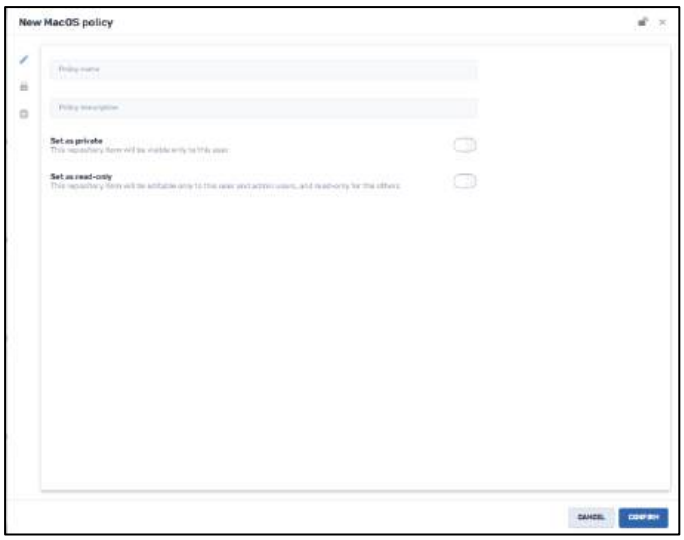
4.1.5.1.3 Adding a New MacOS Policy

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

Table 4-8: MacOS Policies icons

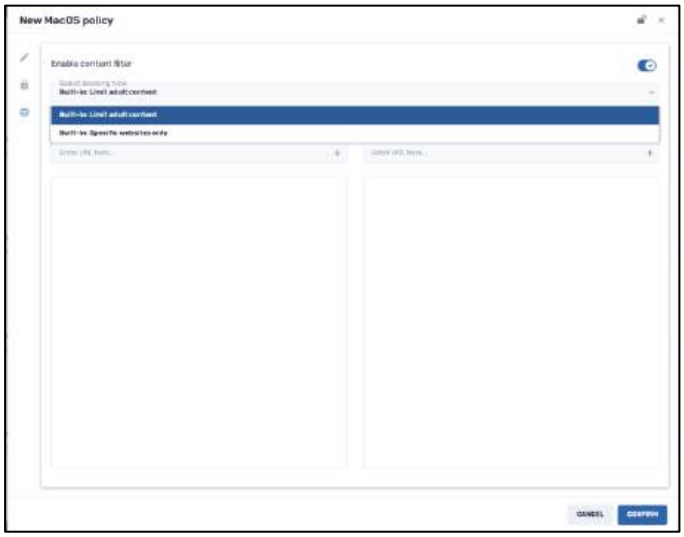
Icon	Description
	Edit Details
	Passcode
	Content filter

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 MacOS policy option to only be visible to you (the creator of the item) when using the Radix Device Manager.
3. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the MacOS 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 .



4. Click on the **Enable Passcode** icon. You will be able to set the parameters for the passcode on the iOS device.

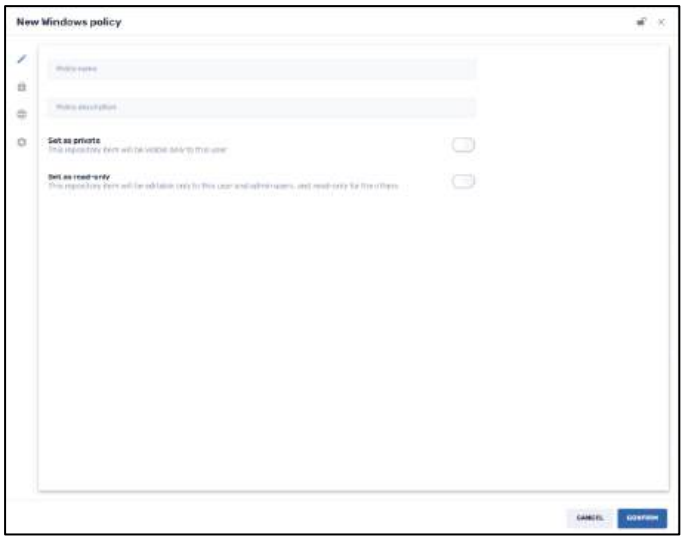
5. Click on the **Enable Content Filter** icon. A window opens that lets you filter out inappropriate websites or limit the browsing on the iOS device to specific websites.



6. Click **Confirm**. The new policy will appear in the **Policies** window.
7. Apply the policy to a device by selecting the policy and clicking **Apply**.

4.1.5.1.4 Adding a New Windows Policy

When you select the option to add a new Windows policy, the following window appears.

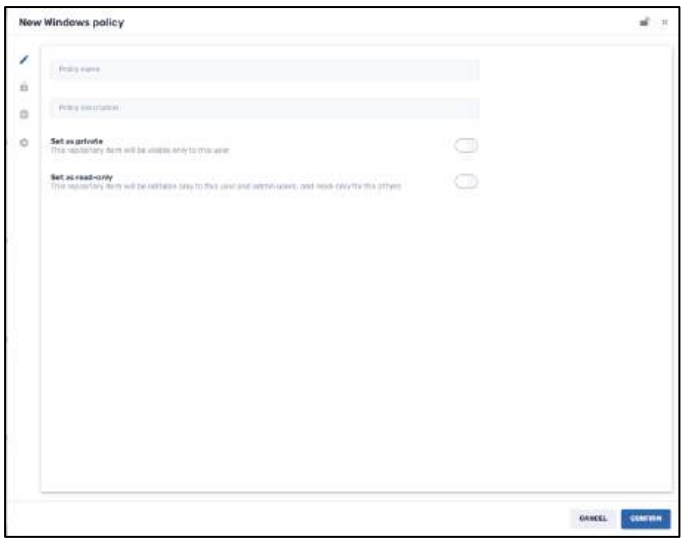


The following is a brief explanation of the icons on the left of the Windows Policy screen:

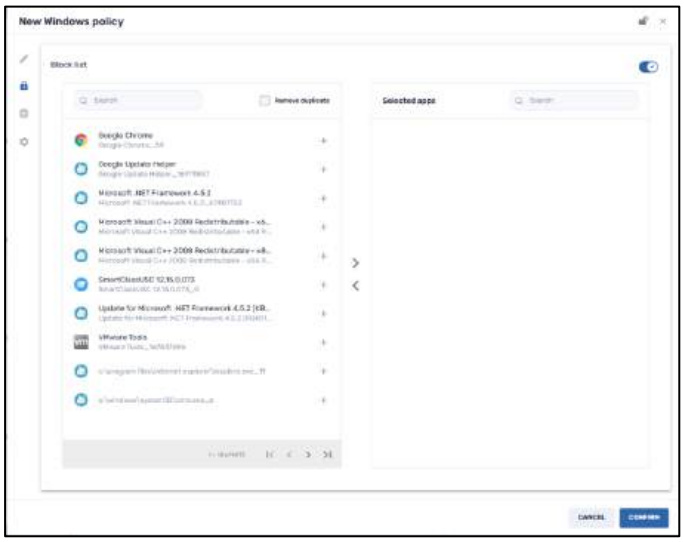
Table 4-9: Windows Policies icons

Icon	Description
	Edit Details
	Block List
	Web Content Filter
	General Tab

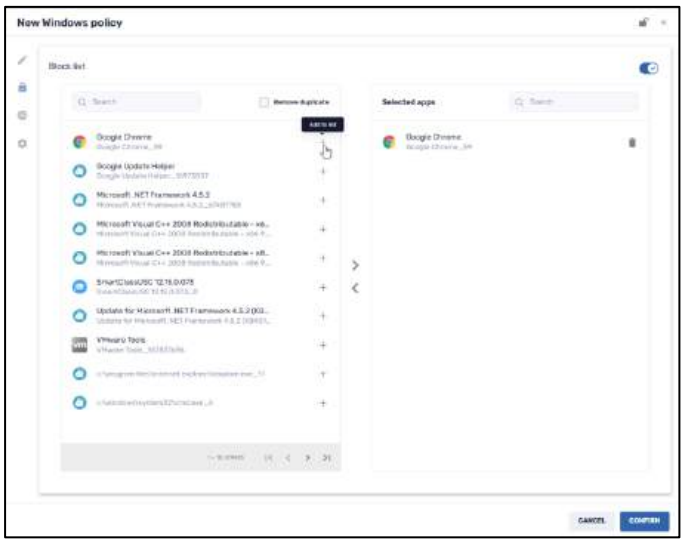
1. In the **Edit Details** window, enter a policy name and description.
2. Click on the **Set as private** button if you would like the Windows policy option to only be visible to you (the creator of the item) when using the Radix Device Manager.
3. Click on the **Set as read-only** button if you would 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  .



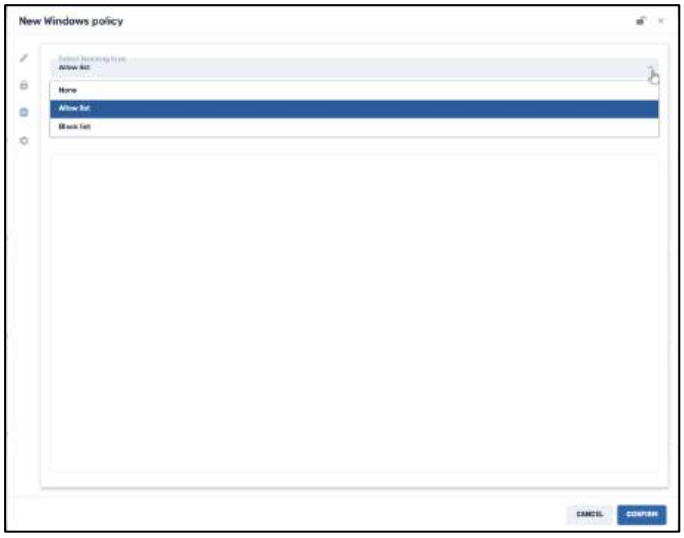
4. Click on the **Block List** icon. The **Block List** window opens.



5. 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.



6. 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.



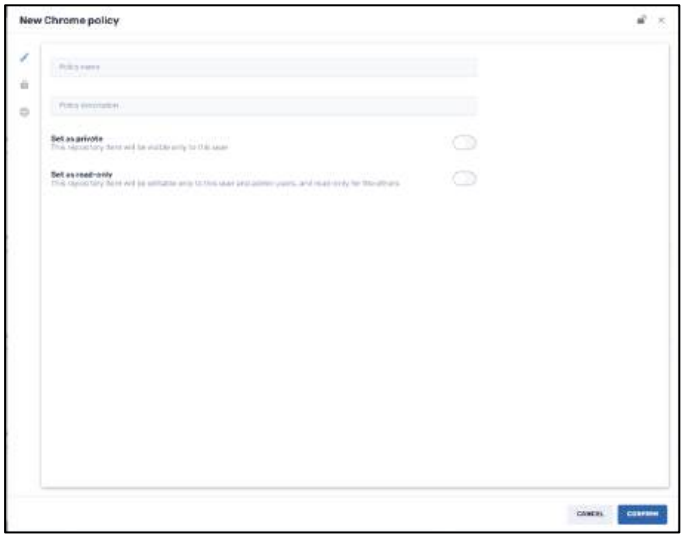
7. Supply the URLs of the apps to be blocked, or to be allowed.

8. 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.

9. Supply the trigger and settings and 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**.

4.1.5.1.5 Adding a New ChromeOS Policy

When you select the option to add a new ChromeOS policy, the following window appears.



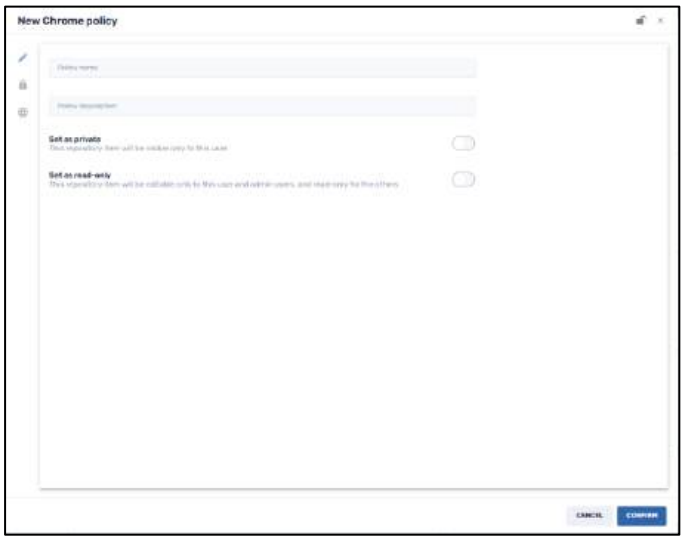
The following is a brief explanation of the icons on the left of the ChromeOS Policy screen:

Table 4-10: ChromeOS Policies icons

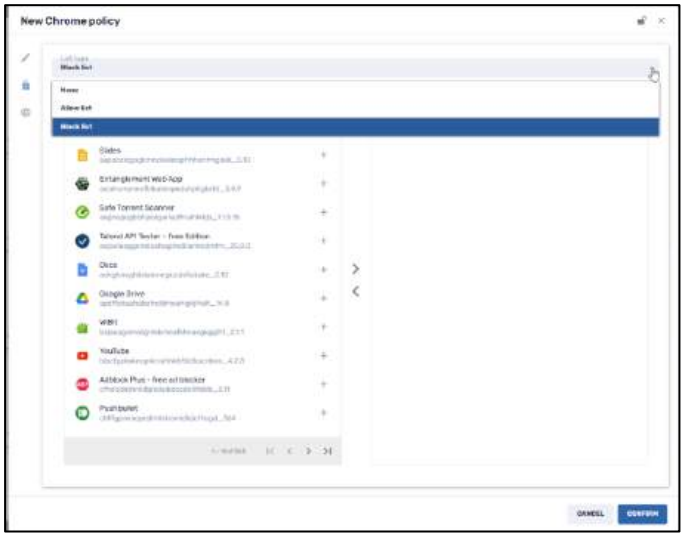
Icon	Description
	Edit Details
	Block List
	Web Content Filter

1. In the **Edit Details** window, enter a policy name and description.

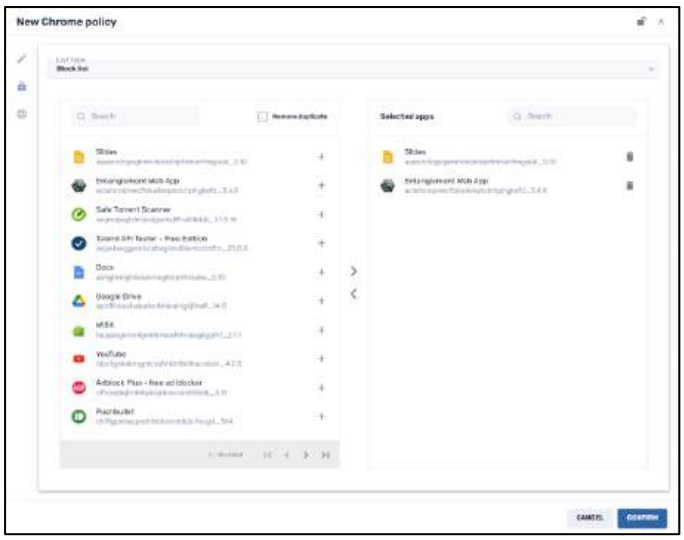
2. Click on the **Set as private** button if you would like the ChromeOS policy option to only be visible to you (the creator of the item) when using the Radix Device Manager.
3. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the ChromeOS policy. 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 .



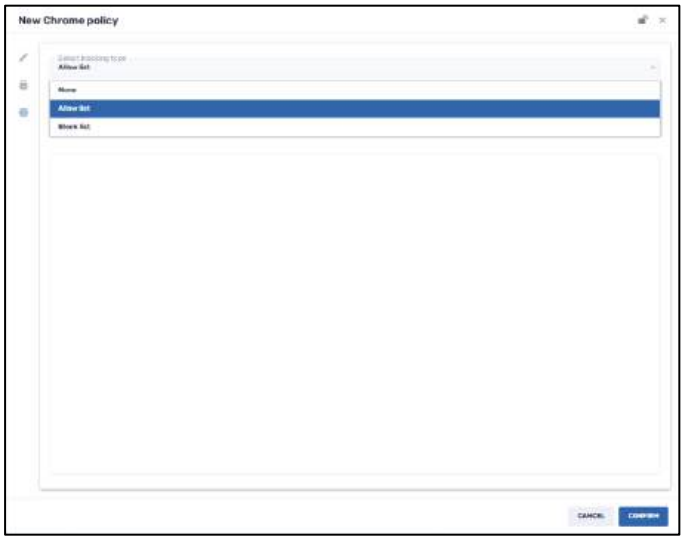
4. Click on the **Block List** icon. The **Block List** window opens.



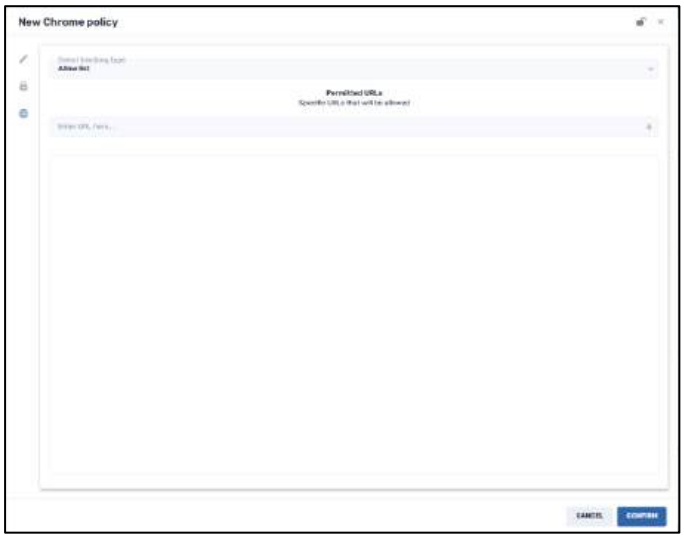
5. Select the apps that you wish to block from the device by clicking on the **Add to list** icon. The selected apps will now appear in the right-hand column of Selected apps.



6. 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.



7. Supply the URLs of the apps to be blocked, or to be allowed.



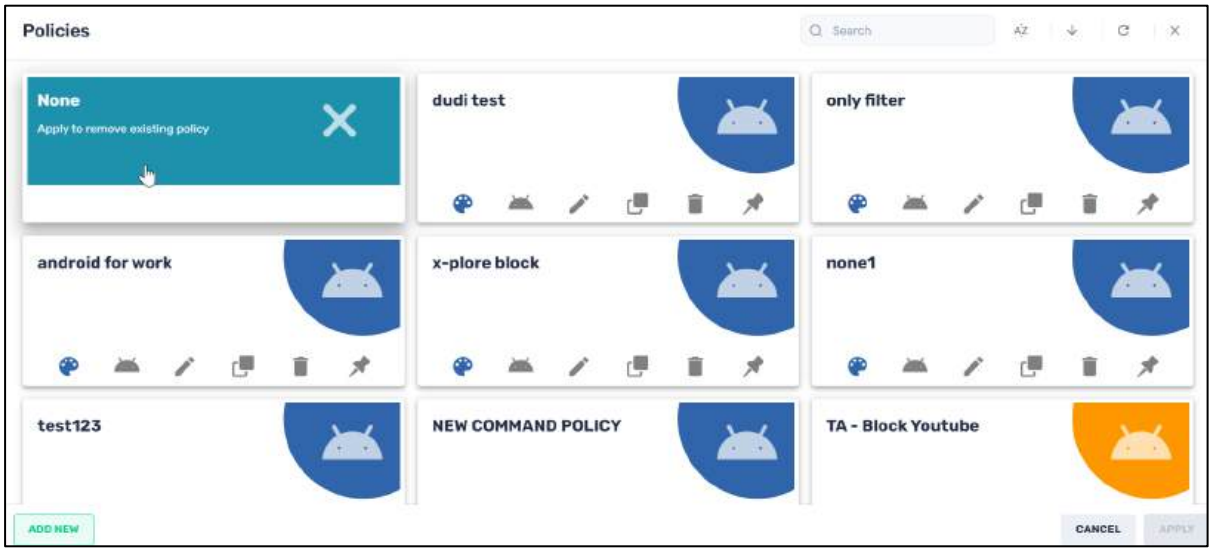
8. Supply the trigger and settings and click **Confirm**. The new policy will appear in the **Policies** window.
9. Apply the policy to a device by selecting the policy and clicking **Apply**.

4.1.5.2 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:

1. Open the **Policies** window.



2. 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.

4.1.6 Workflow

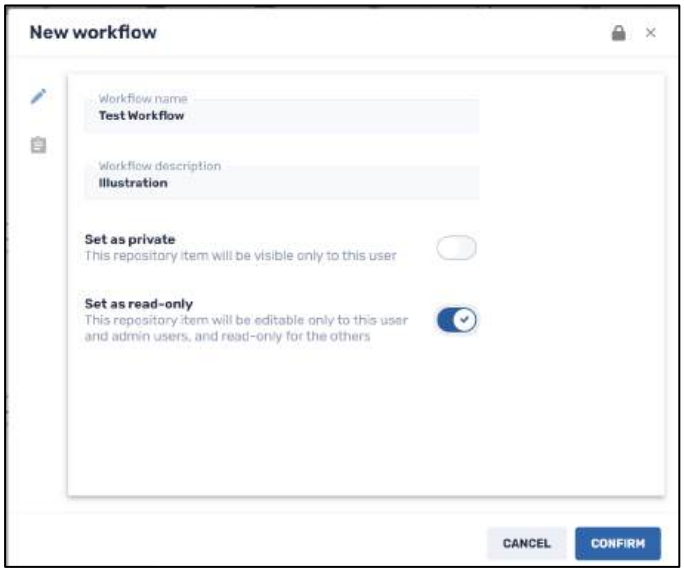
This feature allows sending a series of commands to a device. The **Workflow** command allows you to arrange a series of commands in a particular order, save the arrangement, and deploy the workflow to a device or fleet of devices. There are also options to create a Favorites menu or move commands around within workflows.

When you click on the Workflow icon, the Workflow window 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.



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 Manager.
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 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 .
5. To add commands to the workflow, click on the Commands icon .
6. Click on **Add Command**.

The **Commands Grid** opens.

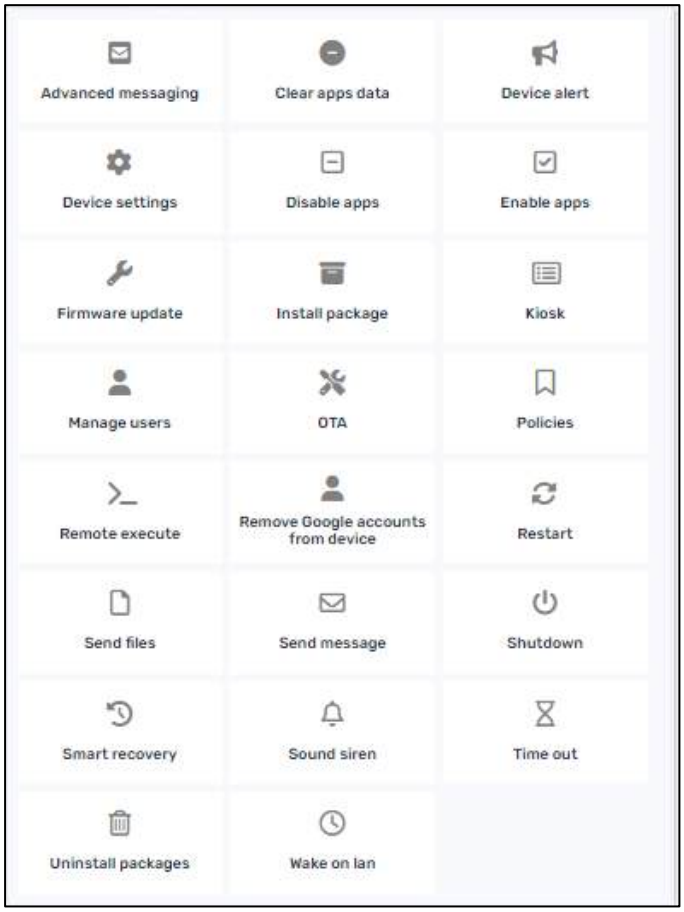
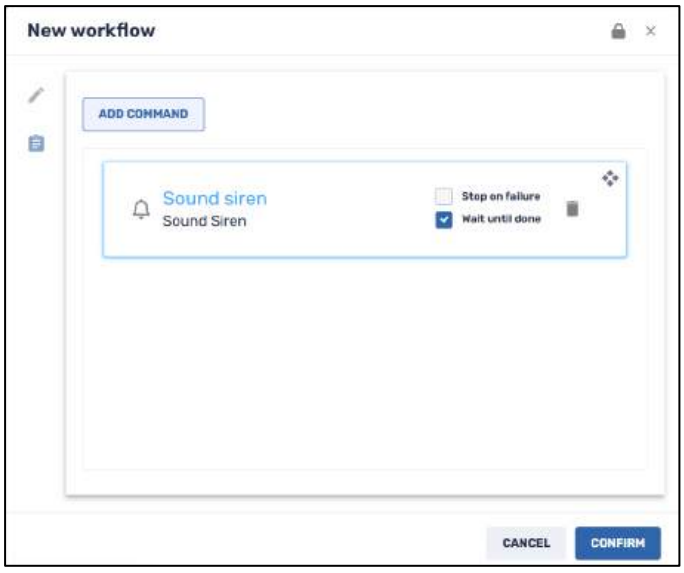
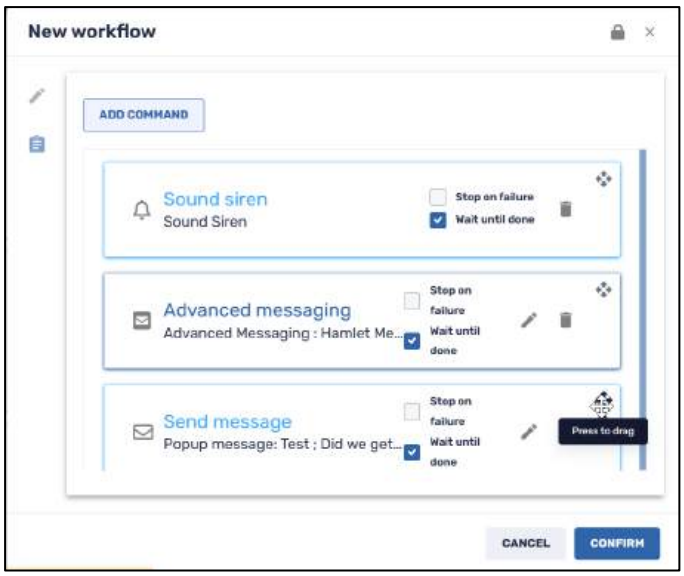


Figure 4-20: Workflow Commands Grid

7. Select a command from the grid. It will appear in the **New Workflow** window.



8. Select all the commands for the desired workflow in the same manner, using **Add Command**.
9. If you wish to rearrange the order, click on the **Press to drag** icon, and move the commands in the preferred order.



10. Click **Confirm** to save the Workflow.
11. To implement the Workflow, select it in the Workflow window, and click **Apply**.

4.2 More actions—Additional Commands

Clicking on the "**More Actions**" button will give you access to all the other options in the Command Grid. The commands that will be displayed will depend on the operating system of the user's device, since there are commands that apply only to Android or Windows devices, for example. A full list of commands appears in Appendix A.

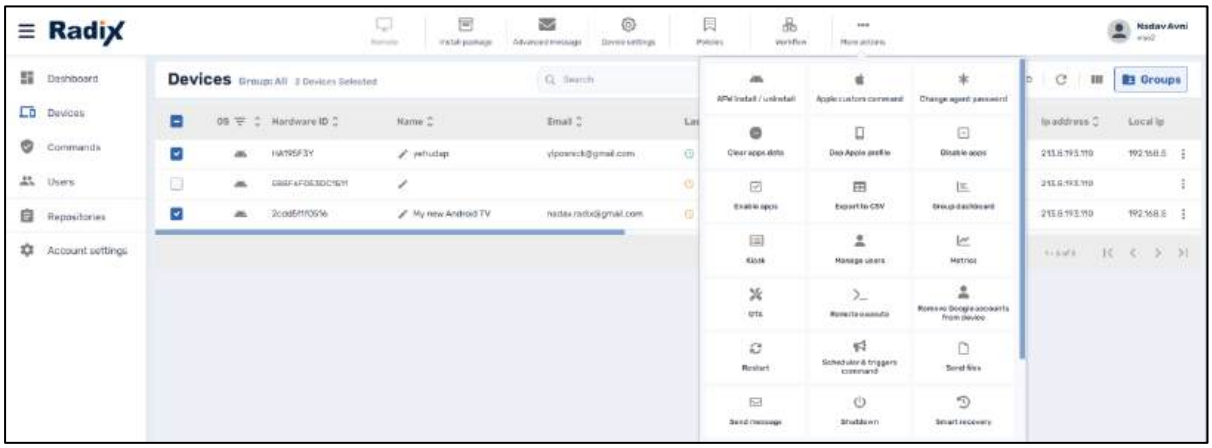


Figure 4-21: Accessing the Commands from the More Actions button

4.2.1 Android Commands

4.2.1.1 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 profile just for business use. This helps ensure security of work-related apps and data.

If you have properly enrolled in the Android for Work program (as detailed in the chapter on Account Settings, in **Section 10.5, Android for Work**), you can select apps for specific Android devices using this Radix Device Manager 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 4.3.5**, they will appear in the **AFW Install** window:

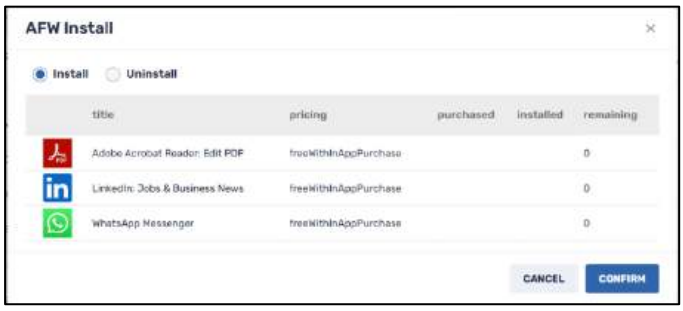
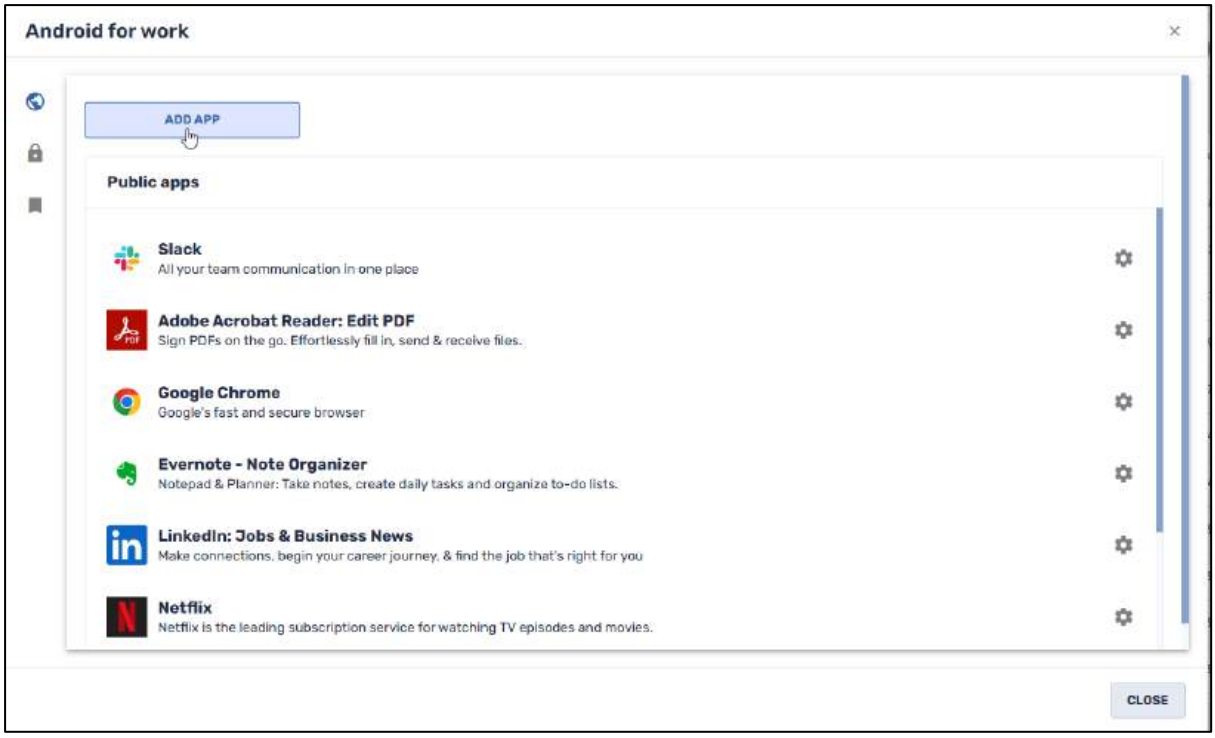


Figure 4-22: Android for Work Install window

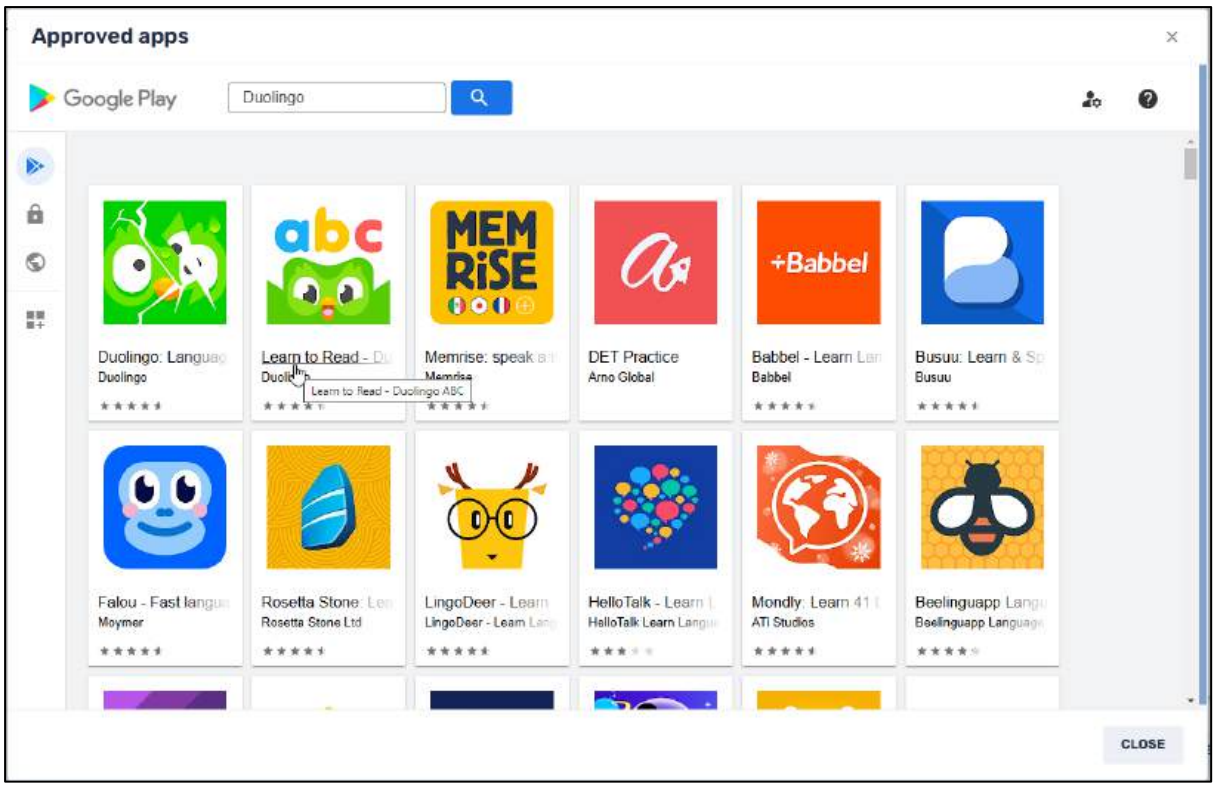
As explained in **Section 4.3.5**, click on the **Android for Work** icon in the Devices Console, to open the Android for Work window:



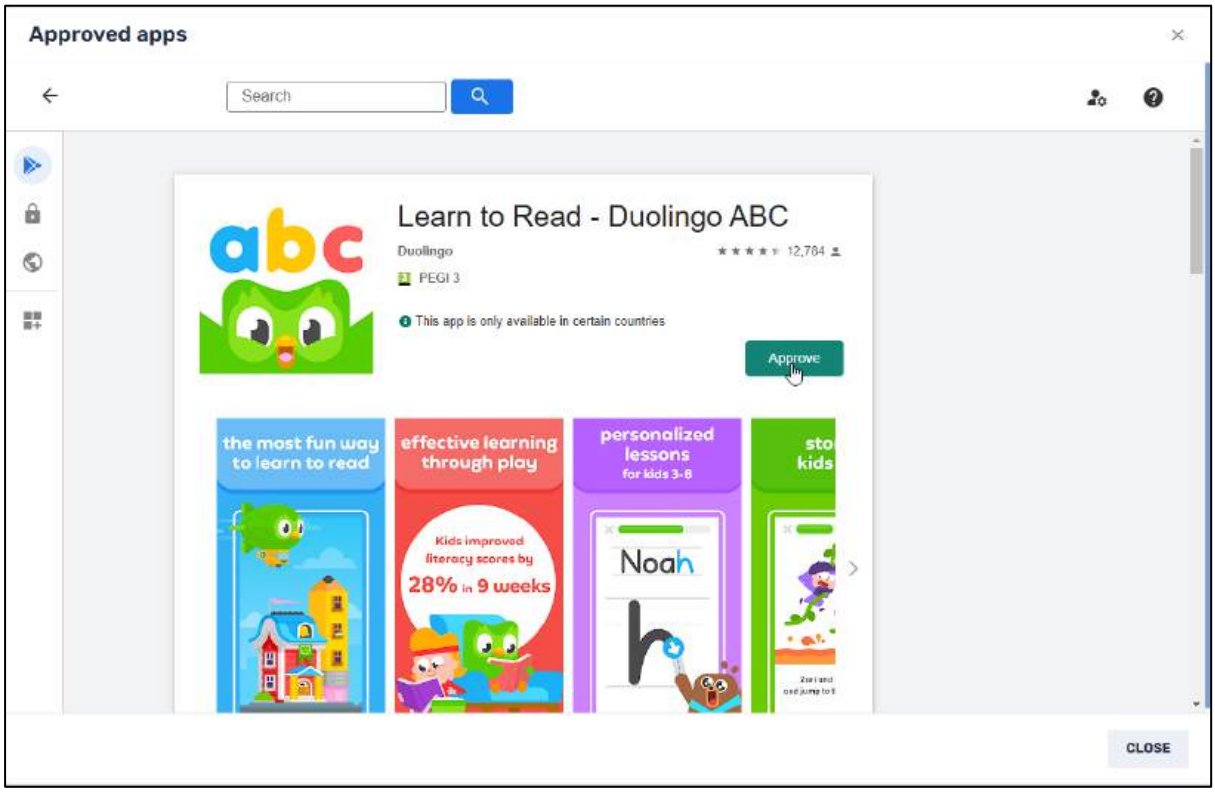
This will give you options to install apps onto devices enrolled in the Android for Work program.

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

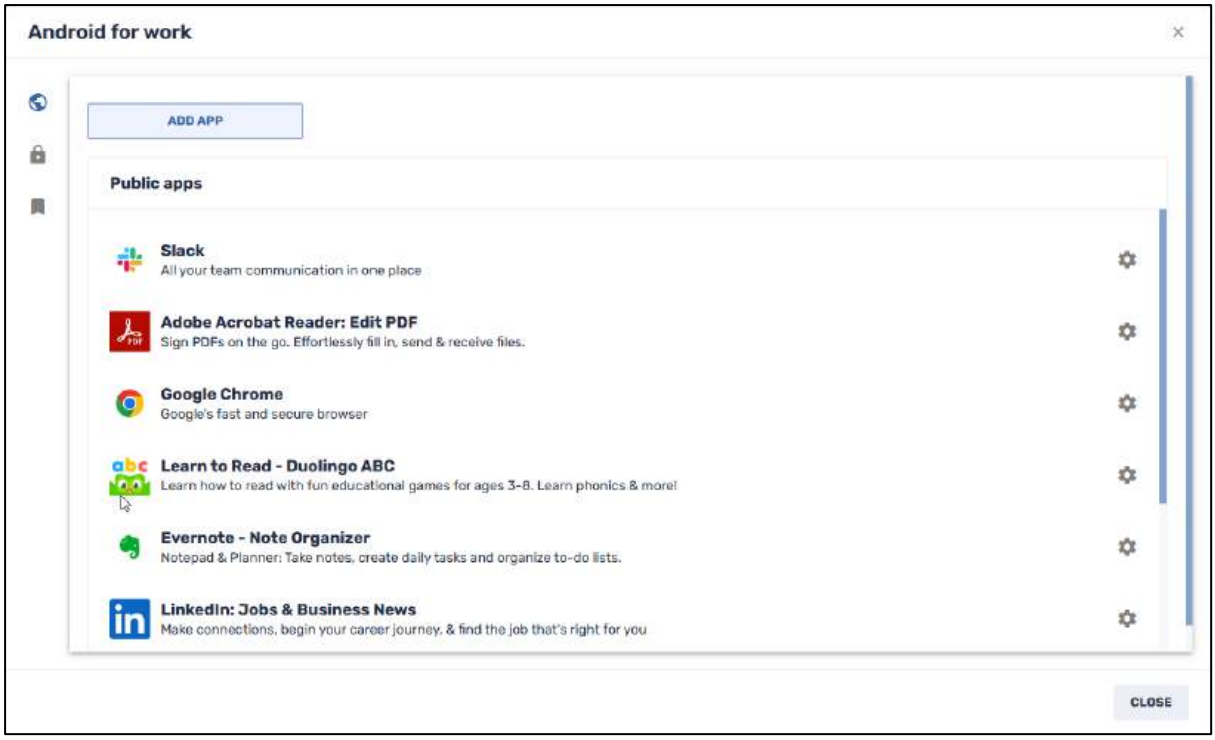
1. Open the **Public apps** window, and click **Add app**.
2. In the **Approved apps** window, search for **Duolingo ABC**.



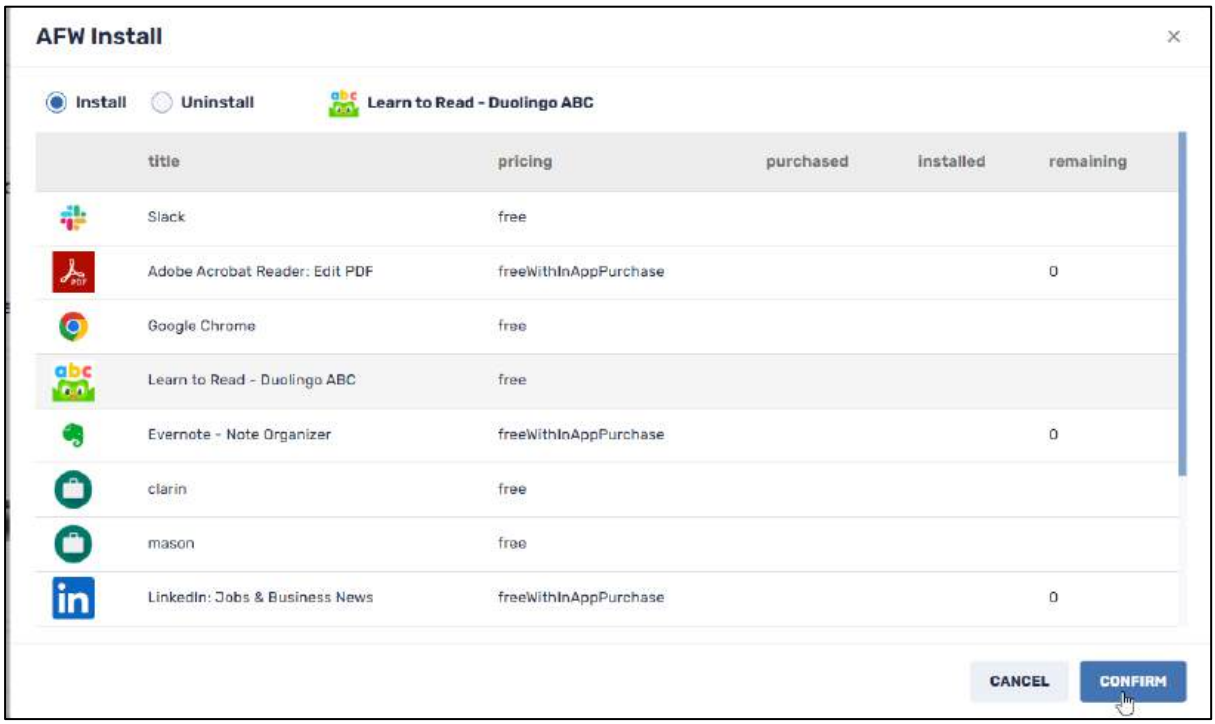
3. Click on the app to select it, and click **Approve**, and then click **Close**.



Duolingo ABC now appears among our options:



4. Select the **Duolingo ABC** app in **AFW Install** and click **Confirm**.



Duolingo ABC will now be installed on your Android device.

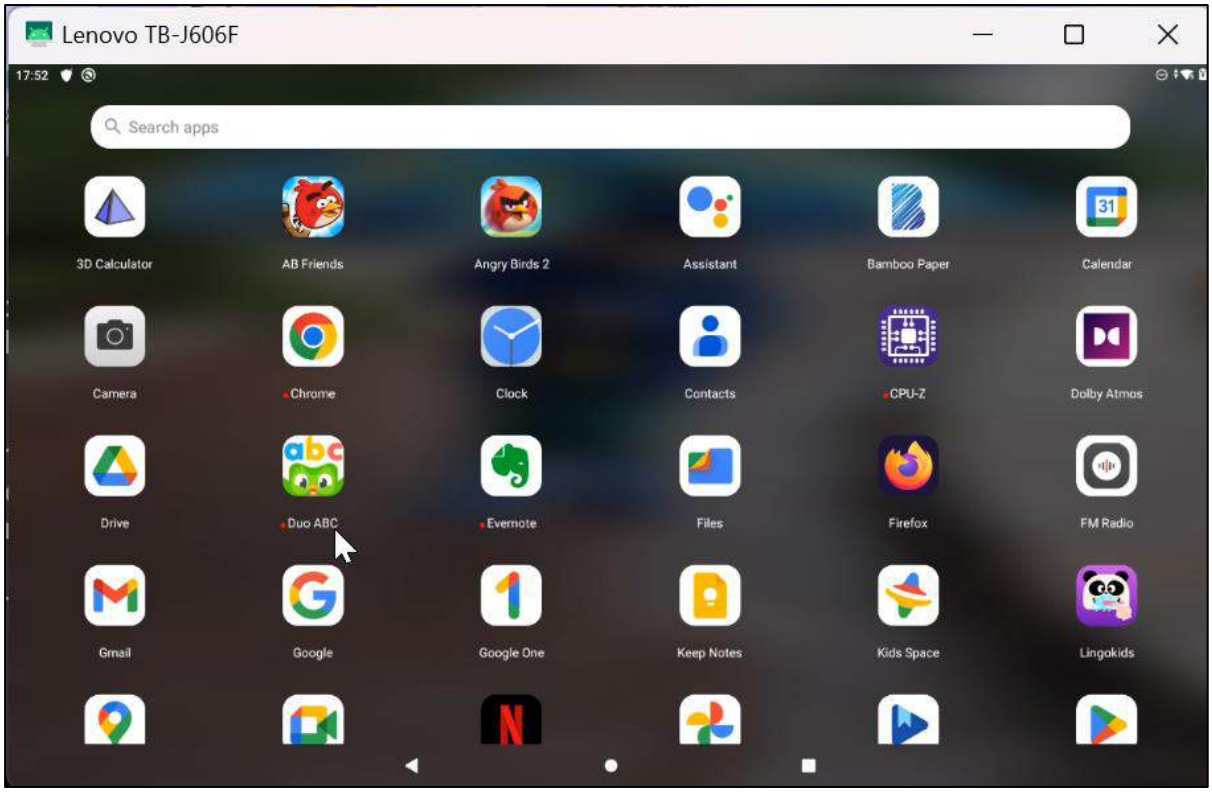


Figure 4-23: The Duolingo ABC app appears on the remote device, after being installed using AFW

Android for Work is described in greater detail in **Section 4.3.5** and **Section 10.5**.

4.2.1.2 Change Agent Password

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

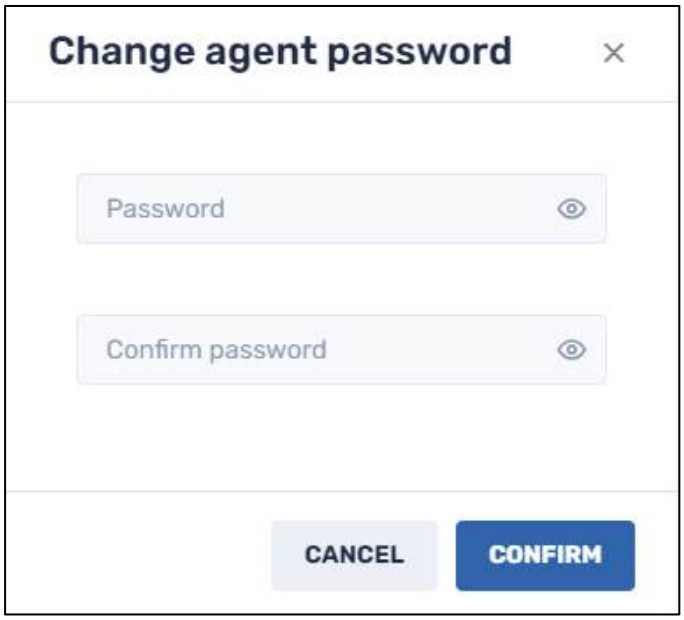


Figure 4-24: Change Agent Password window

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:

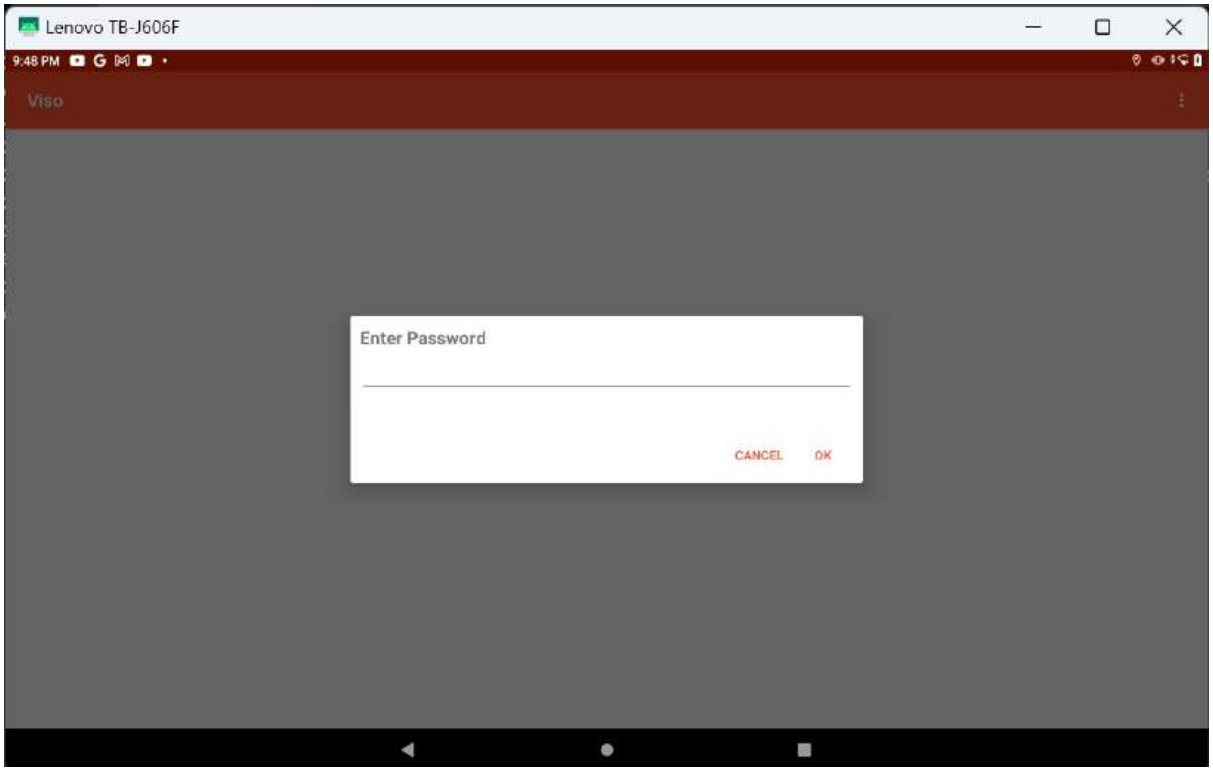
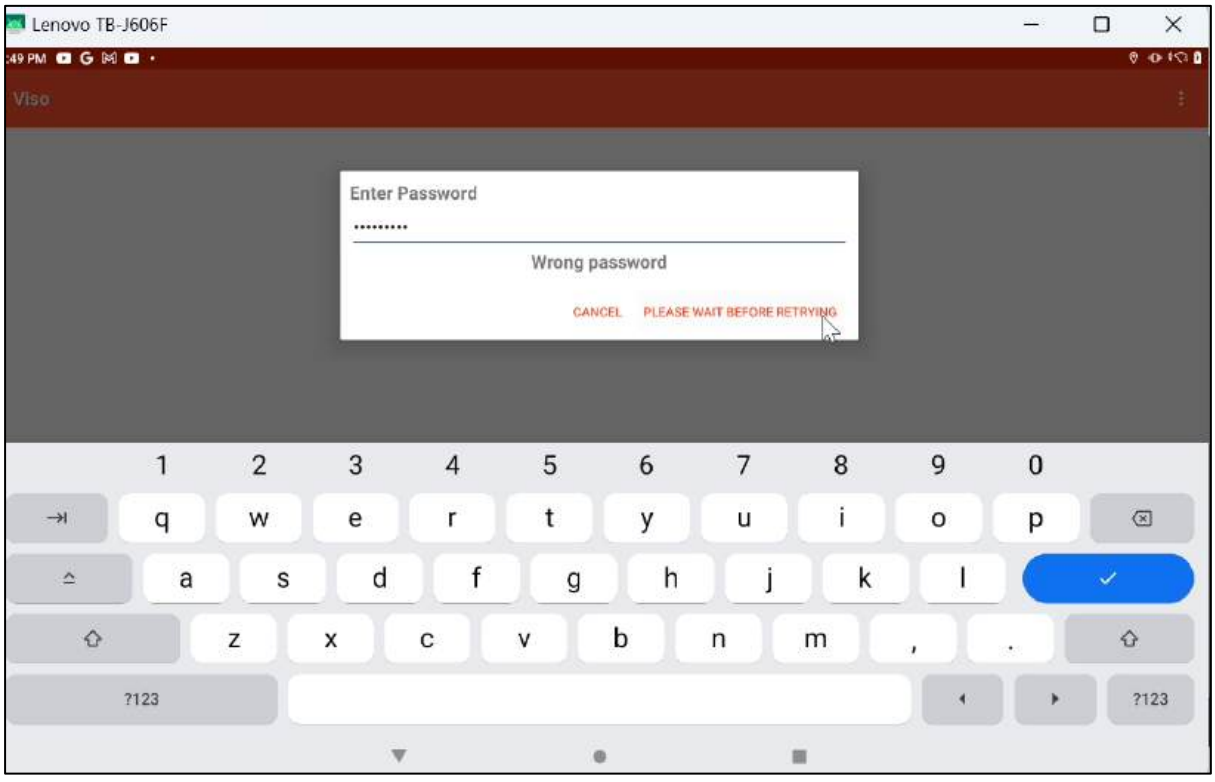
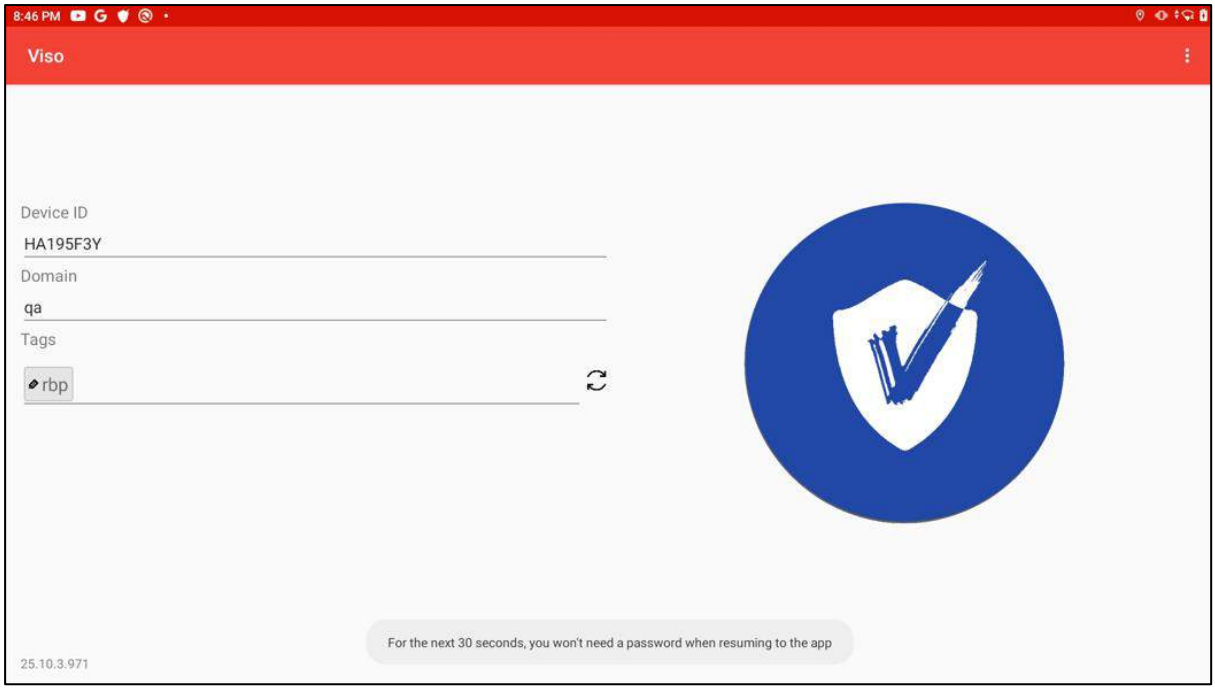


Figure 4-25: Remote device user being prompted to enter the Viso Agent password

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:



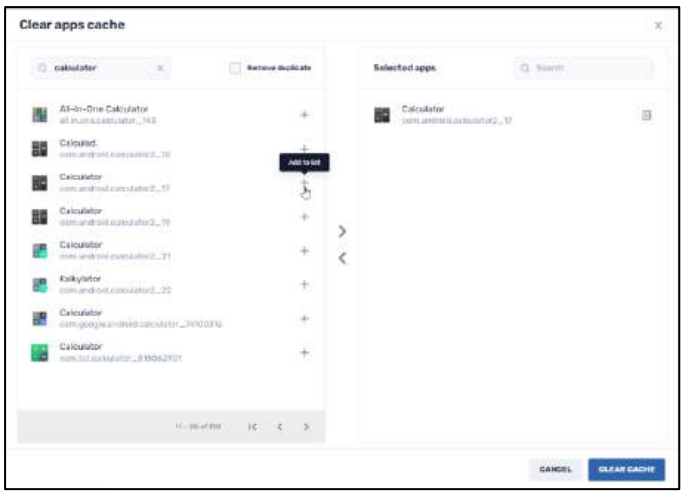
4.2.1.3 *Clear Apps Cache*

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**. But doing it via the Radix Device Manager 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.

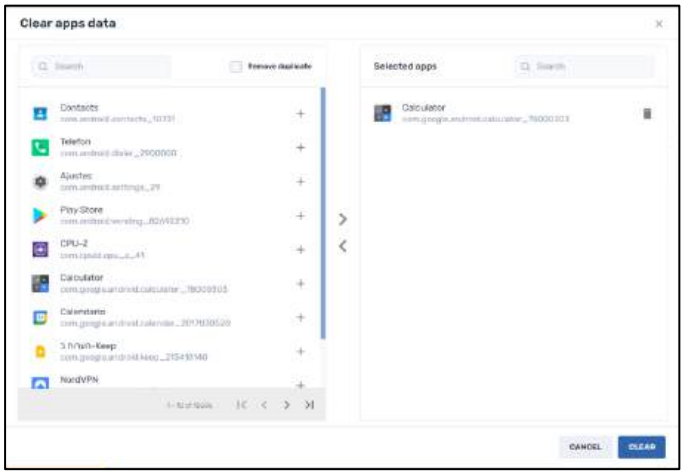


1. Select a particular app by clicking on the **Add** icon + . The app will now appear in the right-hand column of Selected apps.
2. After you have selected the desired apps, click **Clear cache**. This clears the cached data on the device.

4.2.1.4 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.

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

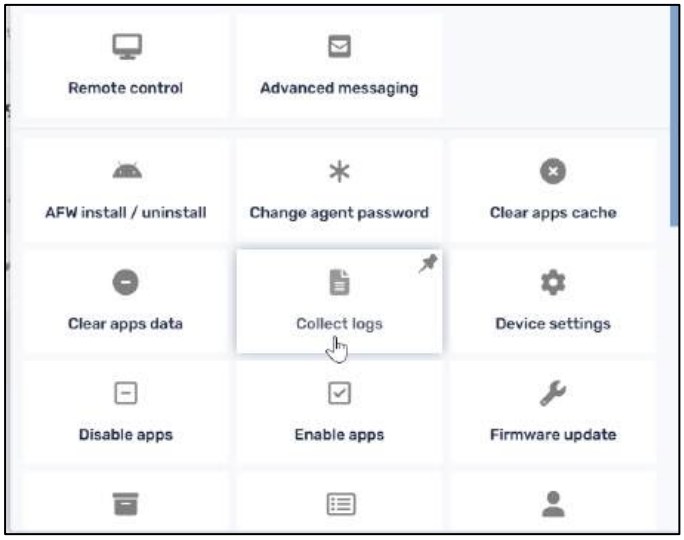


3. Select a particular app by clicking on the **Add** icon + . The app will now appear in the right-hand column of Selected apps.
4. After you have selected the desired apps, click **Clear**. This clears any data on the device.
   For example, if you select the **Calculator** app, it will remotely clear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

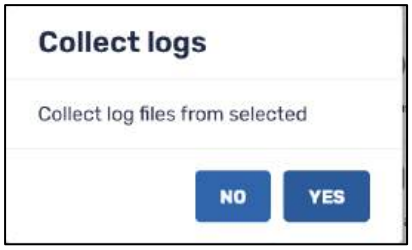
4.2.1.5 Collect Logs

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

This option is available from the Devices Console Ribbon, or from the device's three-dot menu.

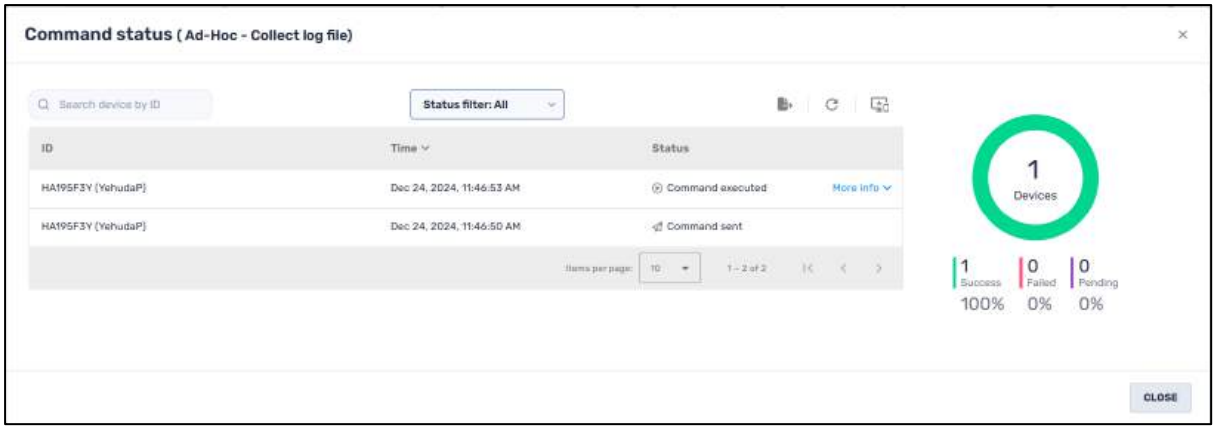


1. When you click on **Collect logs**, the Collect logs dialog box opens, asking if you want to collect activity logs from the selected device.

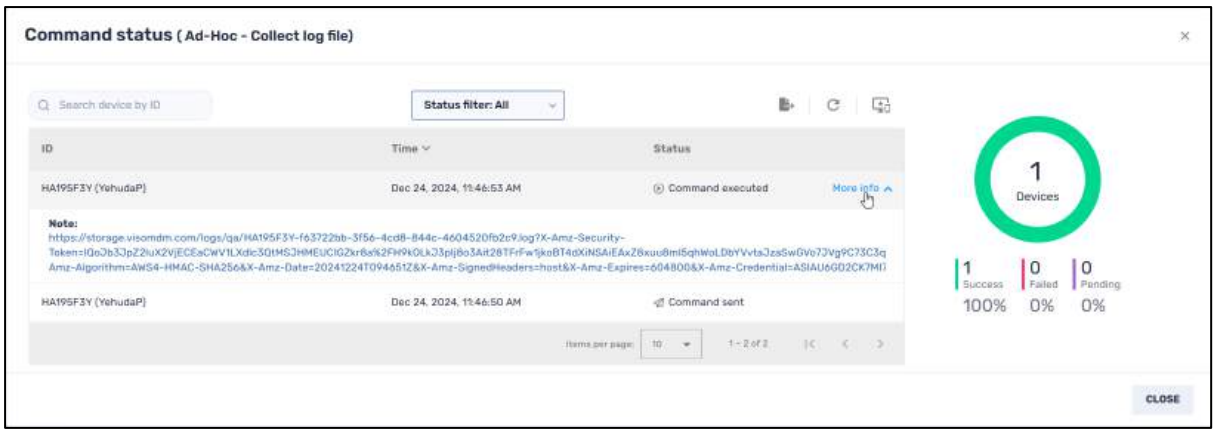


2. If you click **Yes**, a confirmation that the command was sent will appear in the lower right corner, and a notification will appear in the lower left corner, indicating if the log file was created successfully. If you performed the command on a number of devices, the number of devices will appear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

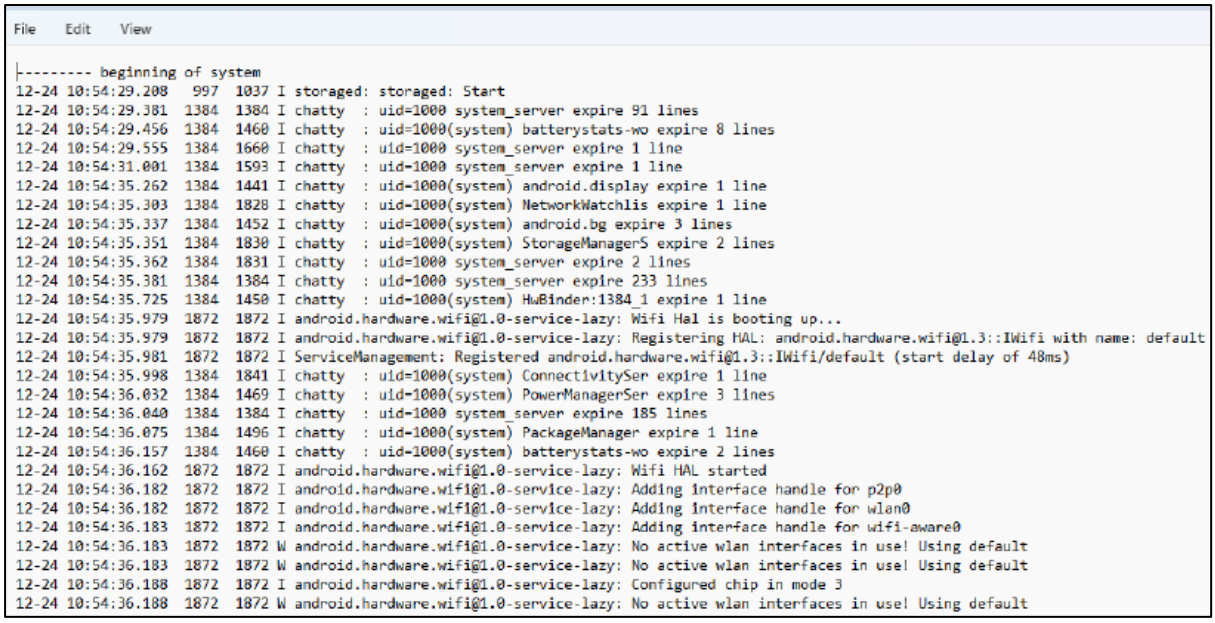


Figure 4-26: Typical log file

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

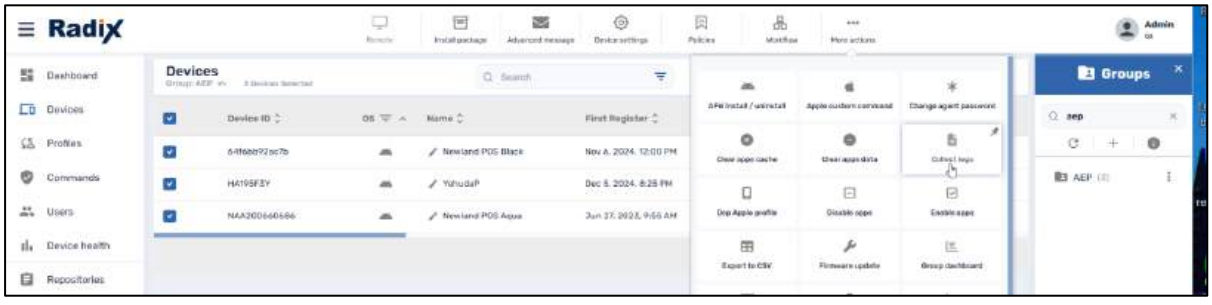
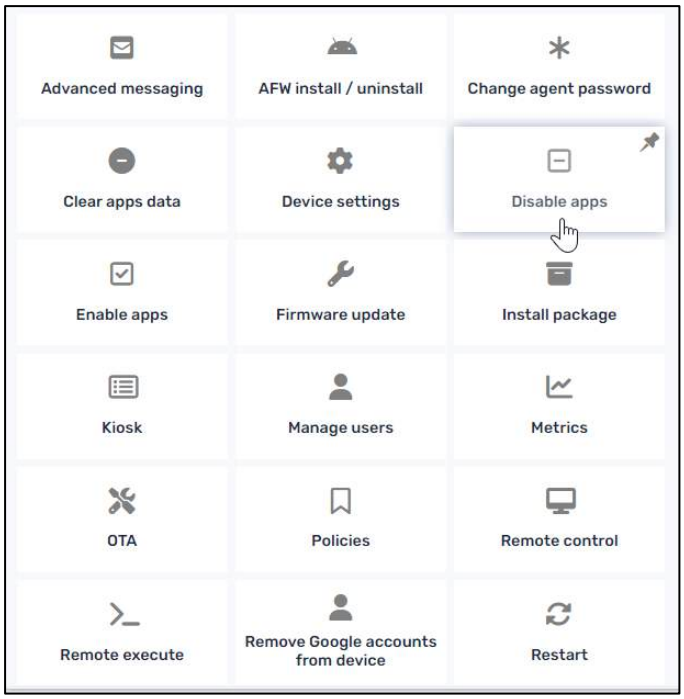


Figure 4-27: Collecting logs from several devices

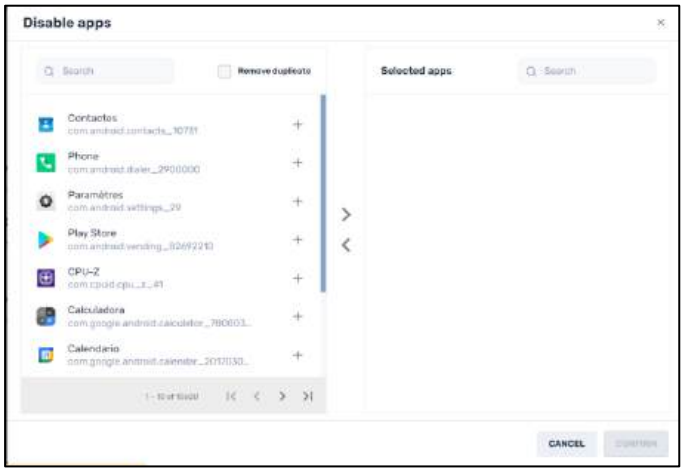
4.2.1.6 Disable/Enable apps

This allows you to remove an app from a device or reinstall it.

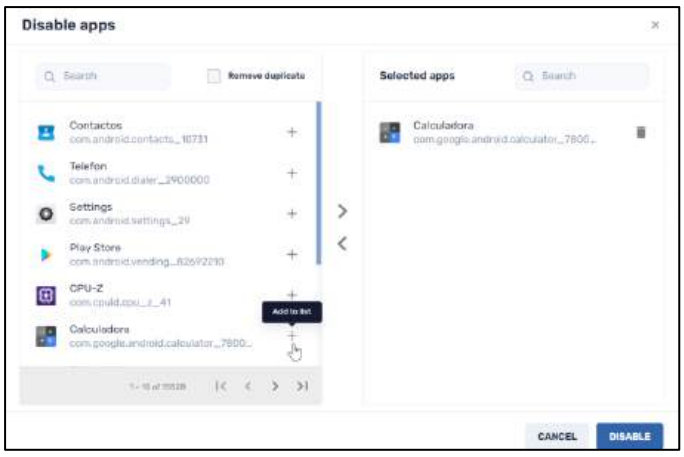
This option is available from the Devices Console Ribbon, or from the device's three-dot menu.



1. When you click on the **Disable Apps** tile, the **Disable Apps** screen opens.



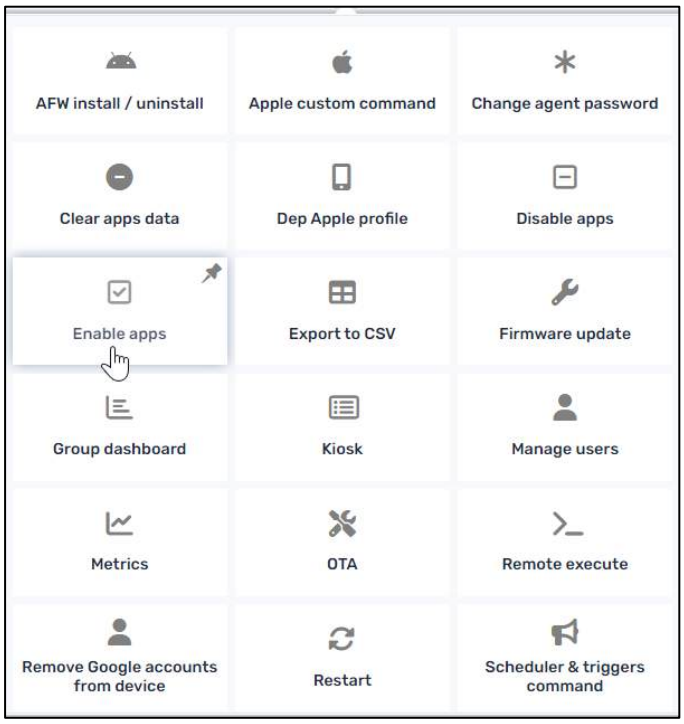
2. Select the apps that you wish to disable by clicking on the **Add to List** icon +. The app will now appear in the **Selected apps** column.



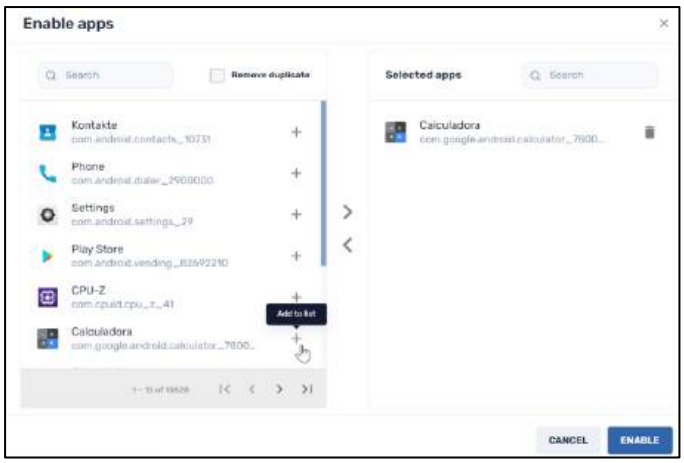
3. Click **Disable**. The apps that you selected will now be disabled on the device.

To reverse the process and enable an app:

1. Click on the **Enable apps** tile.



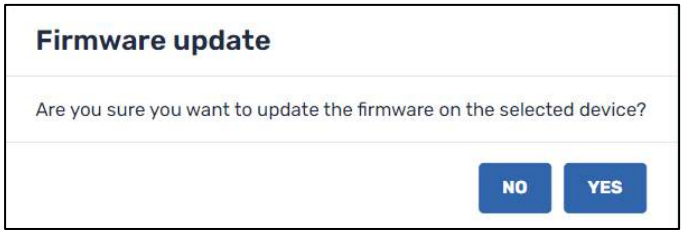
2. Select the apps that you want to enable, by clicking on the **Add to List** icon.



3. Click **Enable**. The app will now be enabled on the device.

4.2.1.7 *Firmware Update*

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



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:

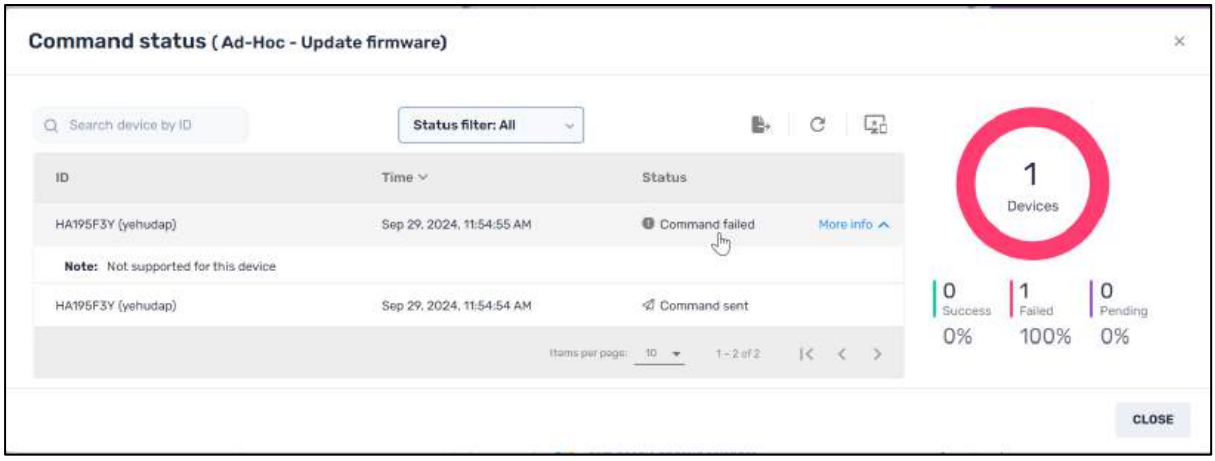


Figure 4-28: Message when attempting a firmware update on an unsupported device

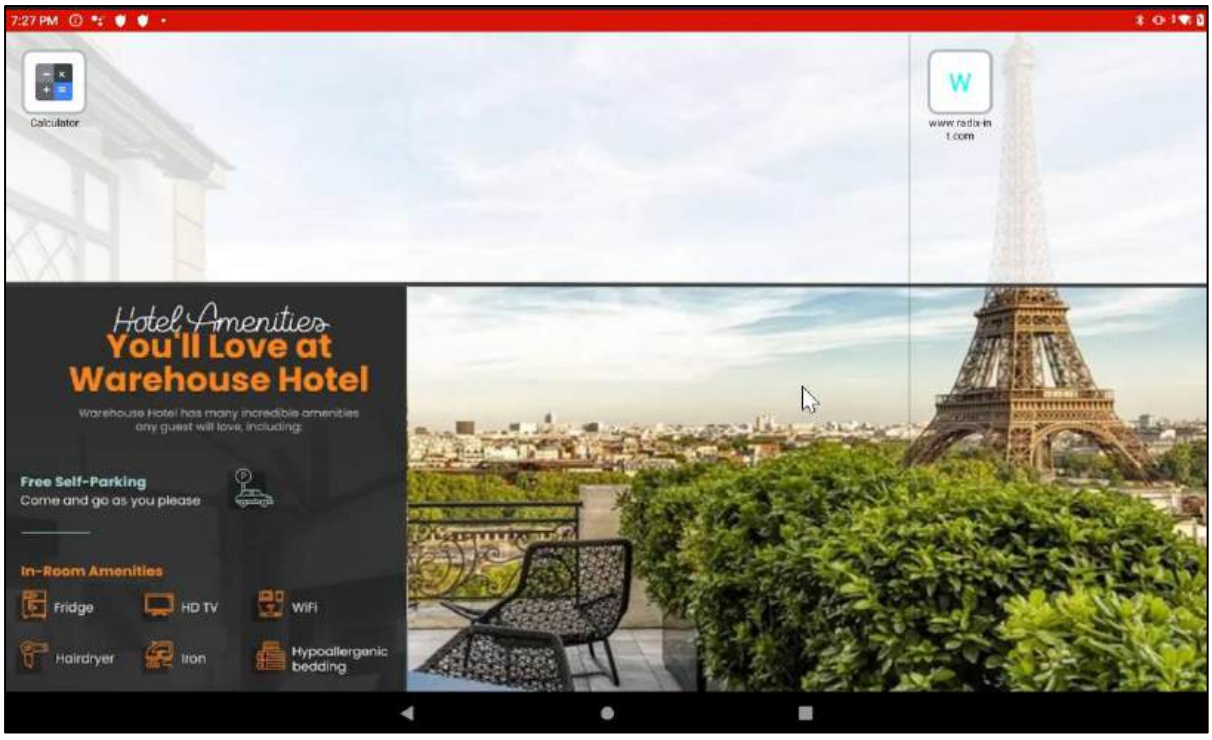
4.2.1.8 *Kiosk*

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

4.2.1.8.1 Applying a Kiosk Option

1. When you click on the **Kiosk** command tile for a selected device, 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.

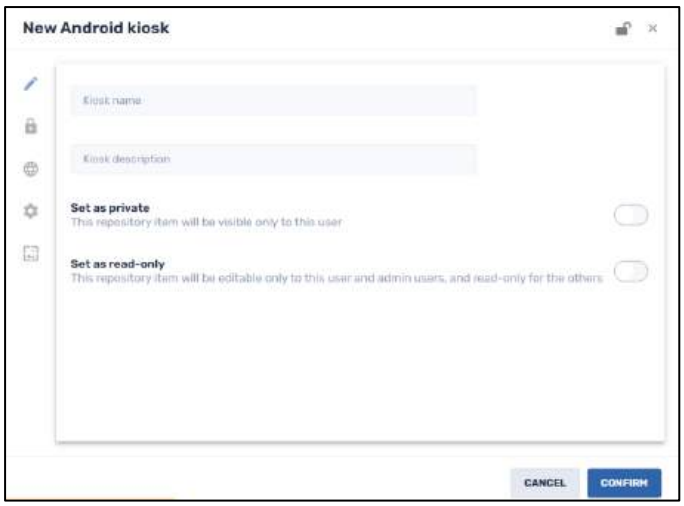


You can also add a new Kiosk option and customize it according to your preferences.

4.2.1.8.2 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.

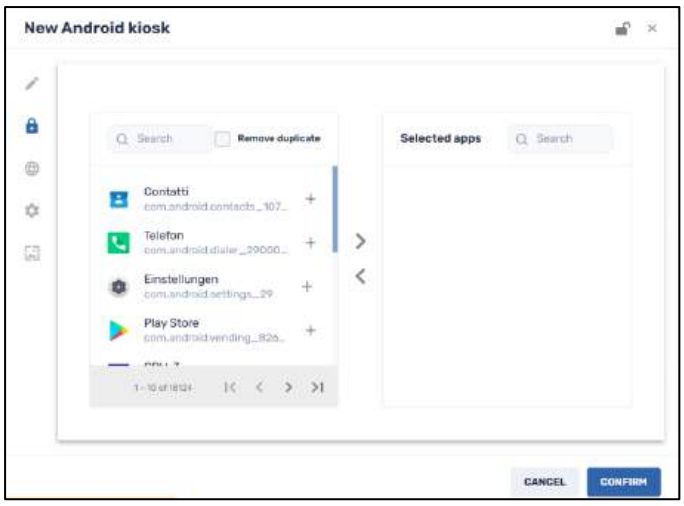


The New Android Kiosk window has the following icons:

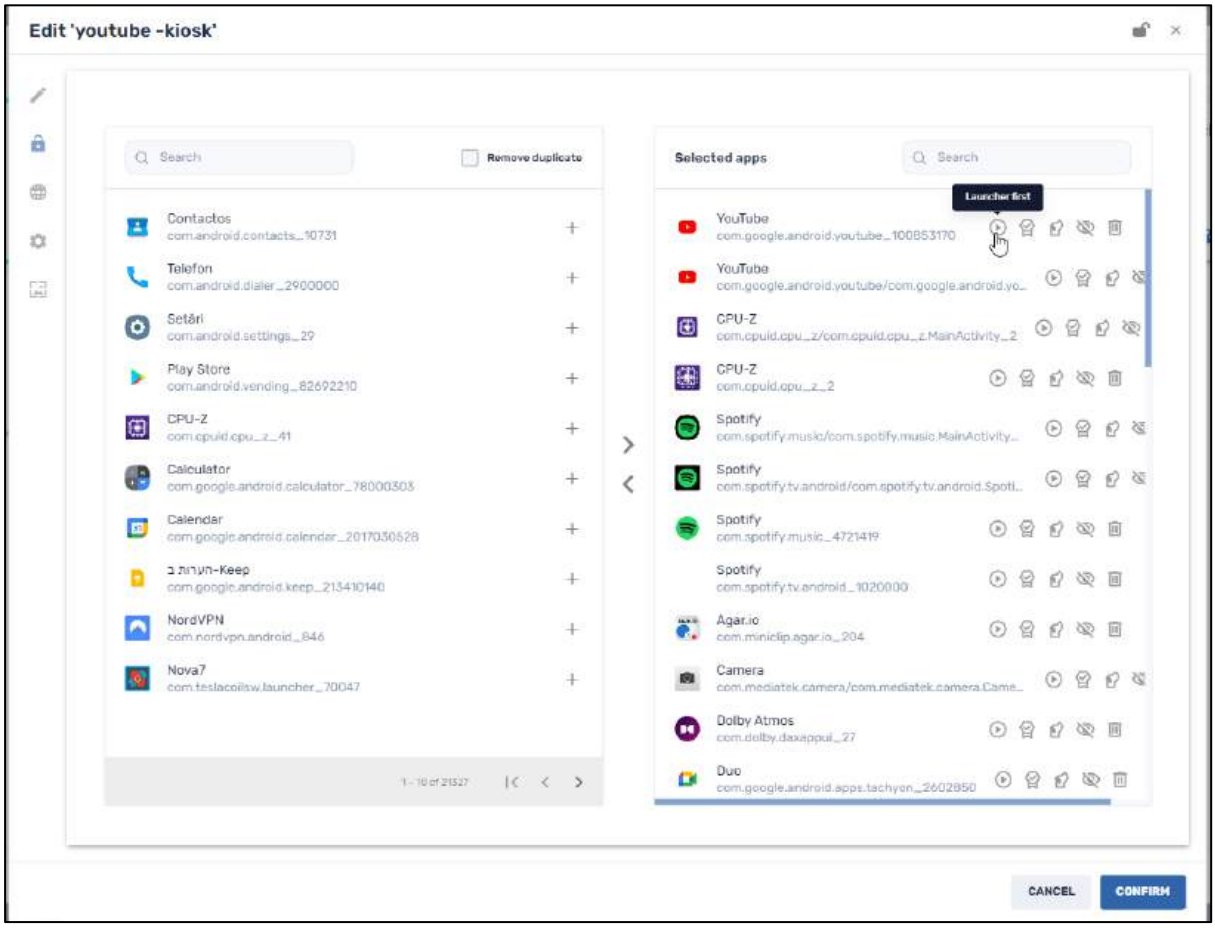
Table 4-11: Kiosk Editing Options

Icon	Description
	Edit Details
	Allow List
	Web
	General
	Wallpaper

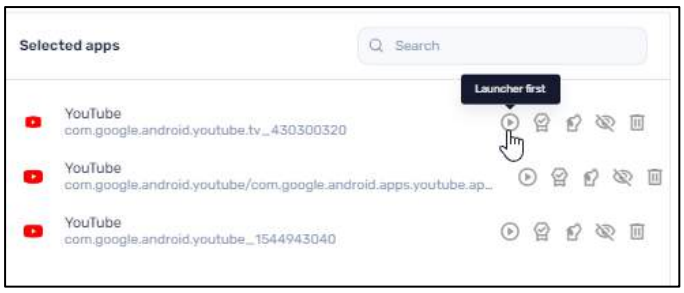
2. Assign the Kiosk command a name and a description.
3. Click on the **Set as private** button if you would like the Kiosk option to only be visible to you (as the creator of the item) when using the Radix Device Manager.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the 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 .
5. 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.



6. 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:

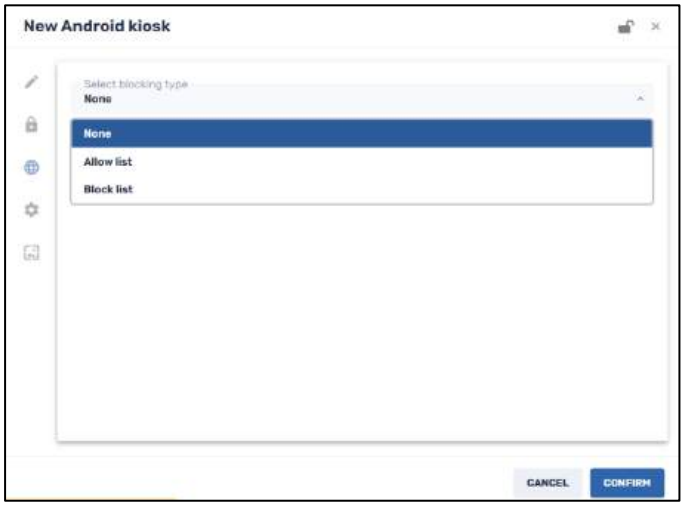


- **Launch first**: Selecting this will launch the app upon every restart/boot/startup. Once you close that app, it will be displayed on the Home page with all the other apps.
- **Launcher app**: Selecting this will prioritize this app as a "launcher app": This launches the selected app as soon as the 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 back to the app selected to be the Launcher app.

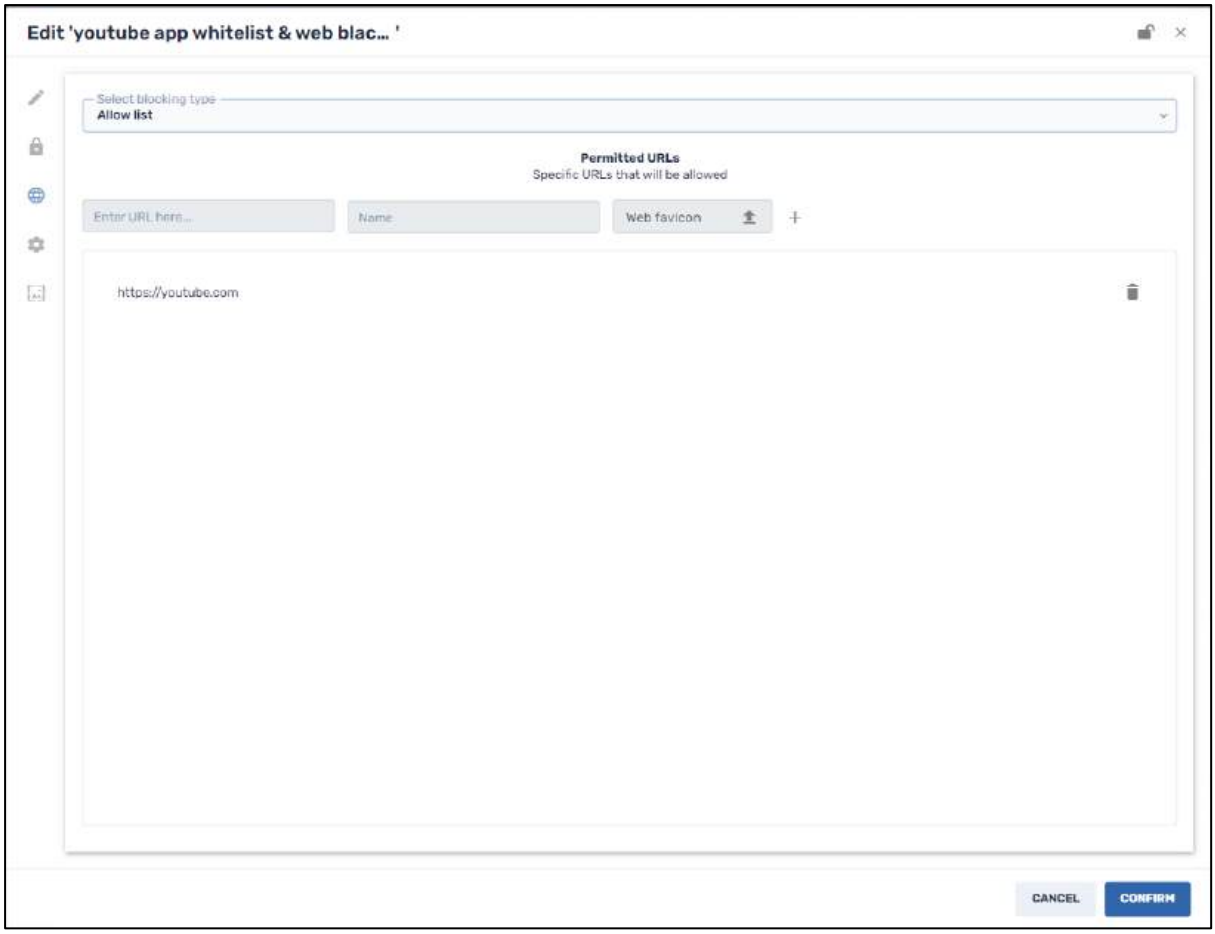
Note: Only one of the selected apps in a specific Kiosk can be assigned **Launch first** or **Launcher app** status.

- **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 Manager user reactivates the icon.
- **Remove**: This will remove the app from the **Selected apps** list.

7. Click on the **Web** icon, to select whether you want an **Allow list** of URLs that you want on the Kiosk device, or a **Block list** of URLs that you do not want on the Kiosk device.



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



To add a URL to the Allow list:

a. Enter the URL, as well as a distinctive name for the website
b. 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 Manager will use the default favicon for that website.
c. Click on the **Add to Allow List** icon.

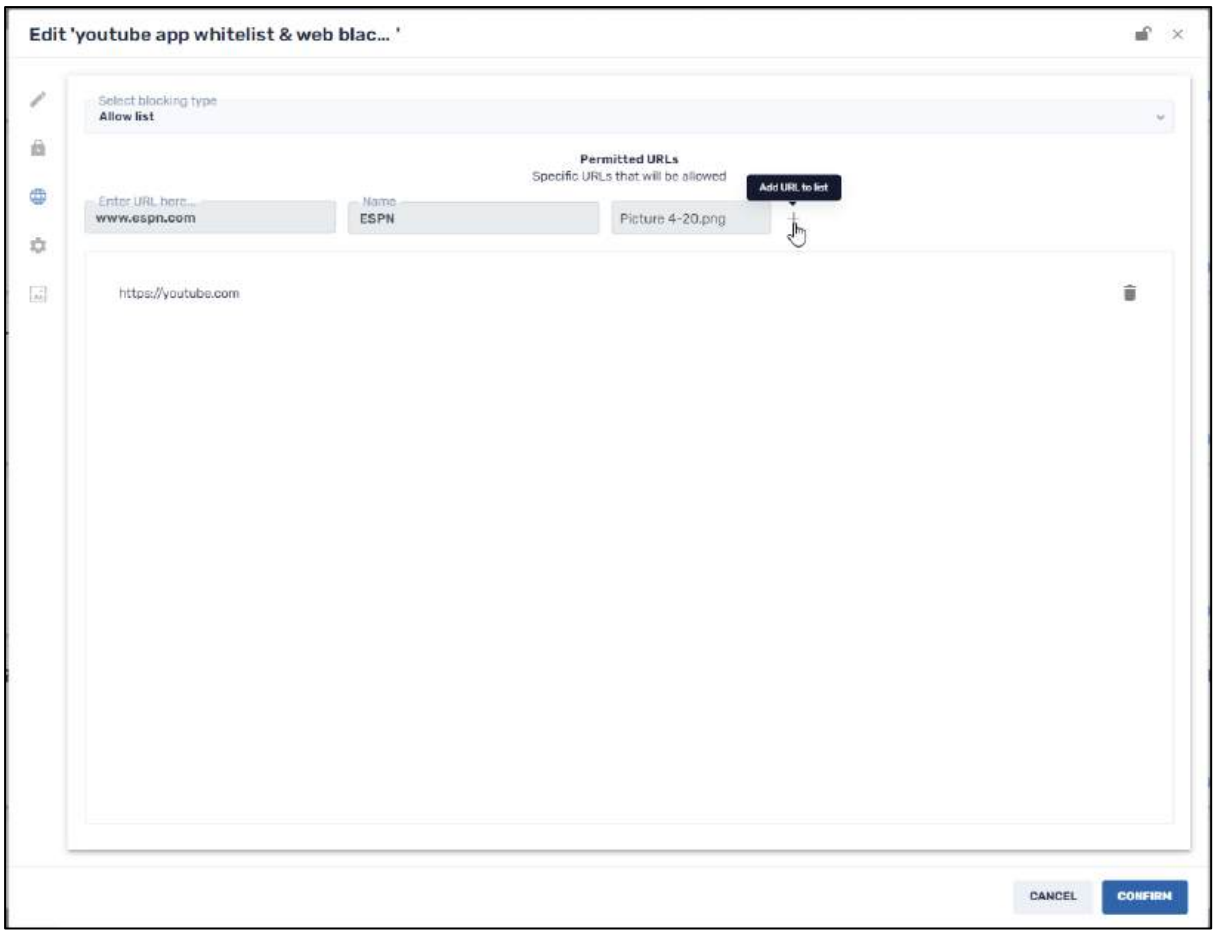
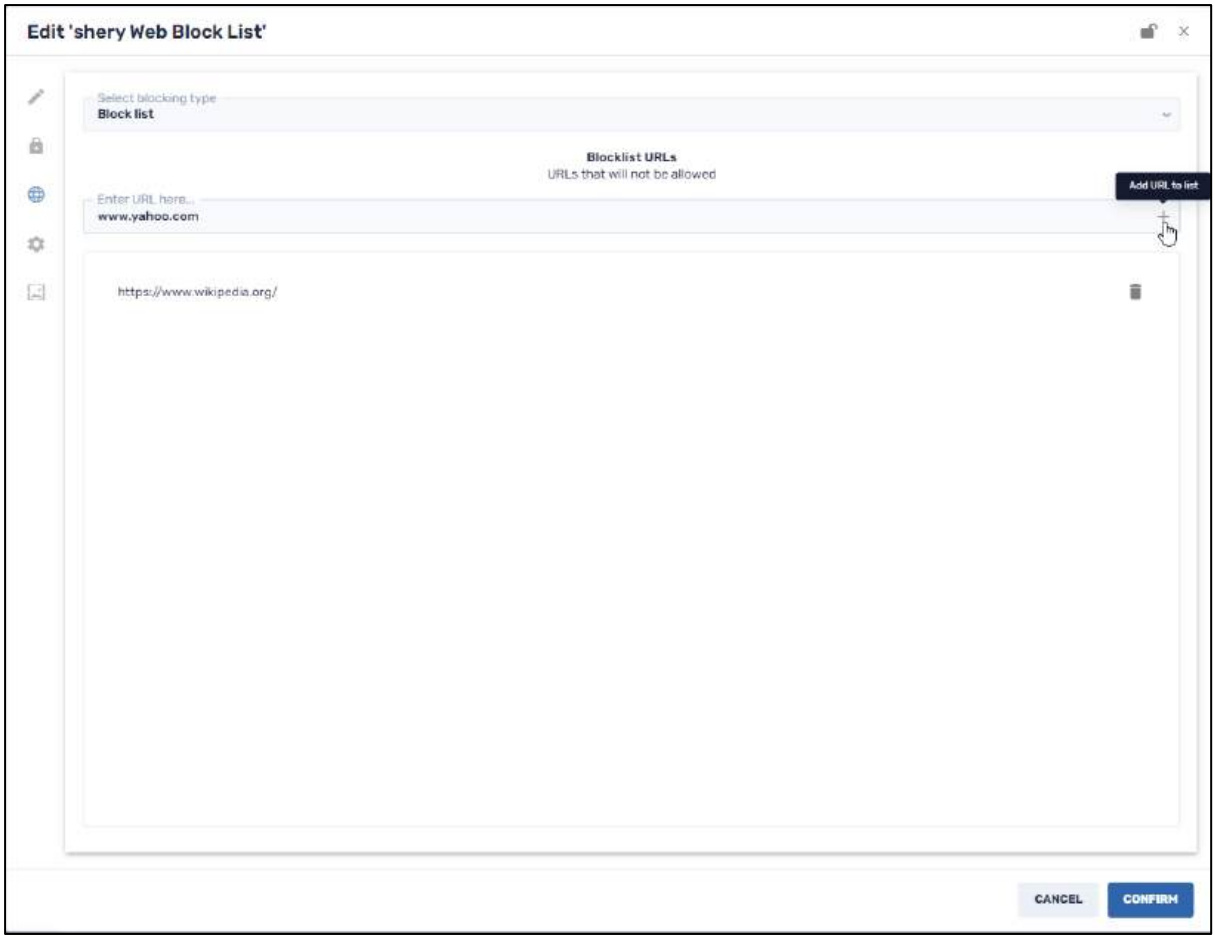


Figure 4-29: When selected, this kiosk mode will only allow access to the YouTube and ESPN websites

The Block list window 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.

8. Click on the **General** icon. This contains options to choose:
    - A method of triggering the Kiosk, as treated in **Section 4.2.1.15, Scheduler & Triggers Command**,
    - Adding settings to the Kiosk, as treated in **Section 4.1.4, Device Settings**, and
    - Determining the orientation of the Kiosk's wallpaper, as well as options to adjust the icon size and font size in the Kiosk display.

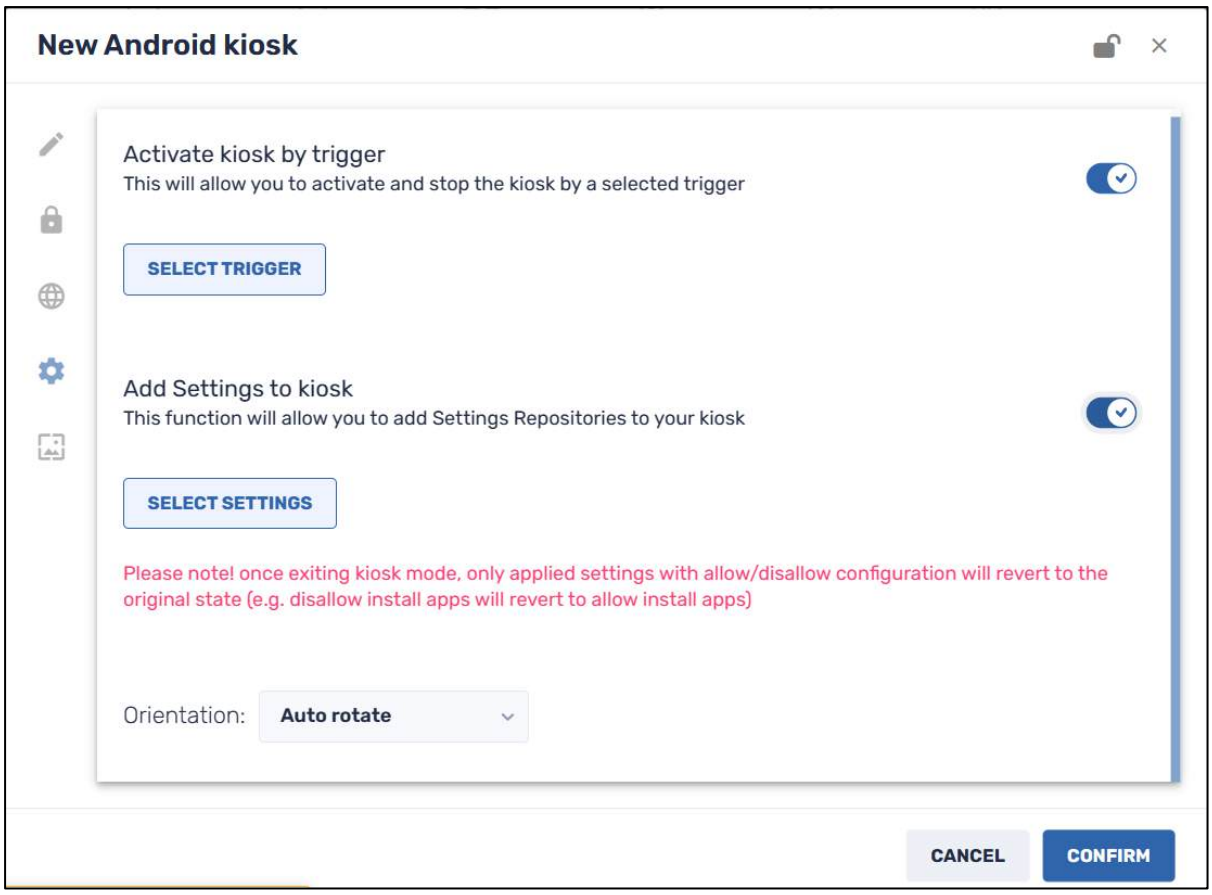


Figure 4-30: Kiosk Mode Trigger and Settings options

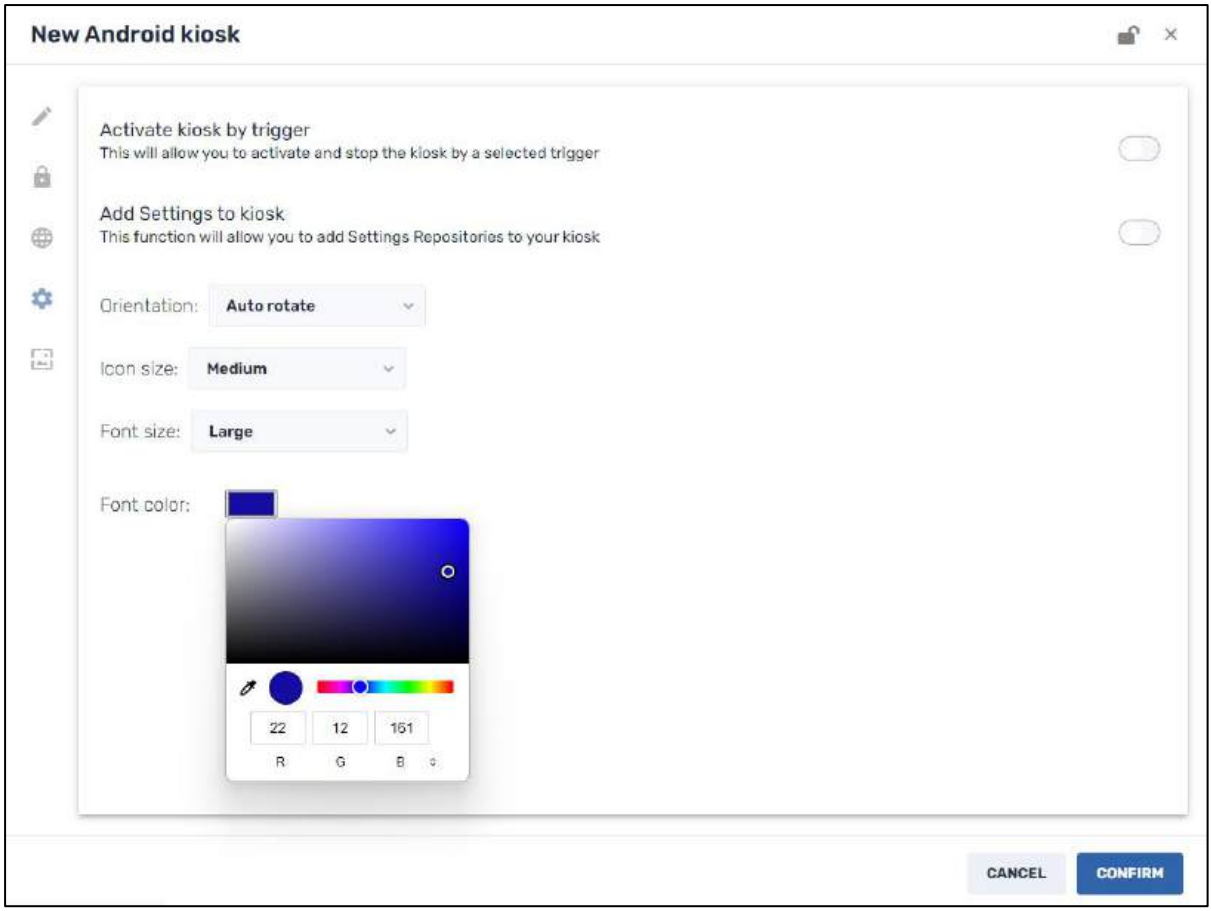
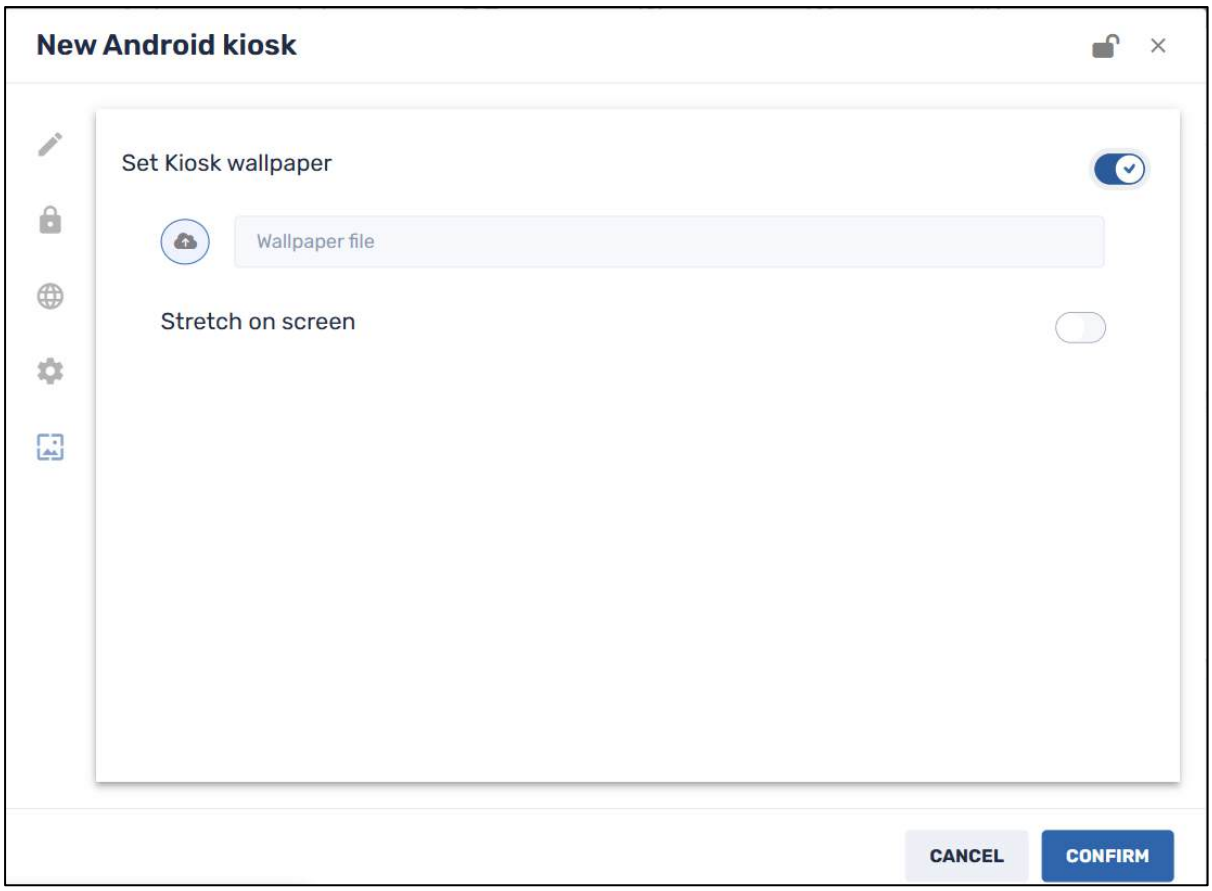


Figure 4-31: Options to adjust icon size and font color in the Kiosk display

9. 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:

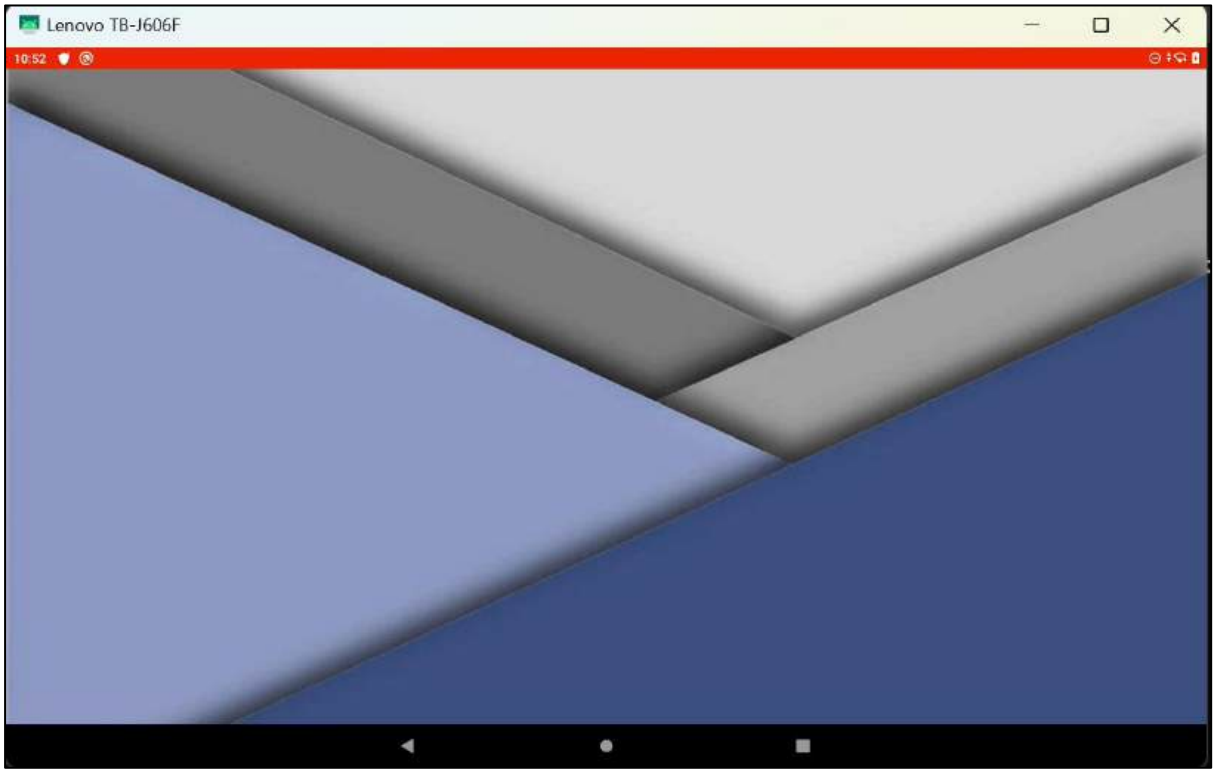


Figure 4-32: Default Kiosk Wallpaper on remote device

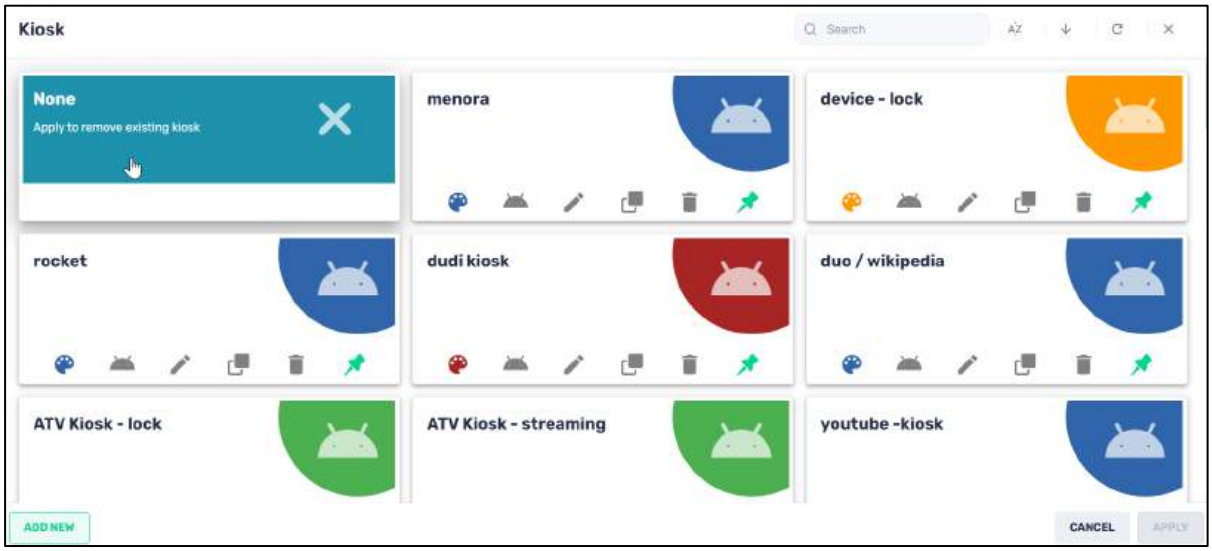
10. Click **Confirm**. The kiosk option that you created will be saved in the Kiosk window.
11. To use a kiosk option, select it from the Kiosk window, and click **Apply**.

4.2.1.8.3 Removing a Kiosk Option from the Radix Device Manager side

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.

To remove a Kiosk mode:

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



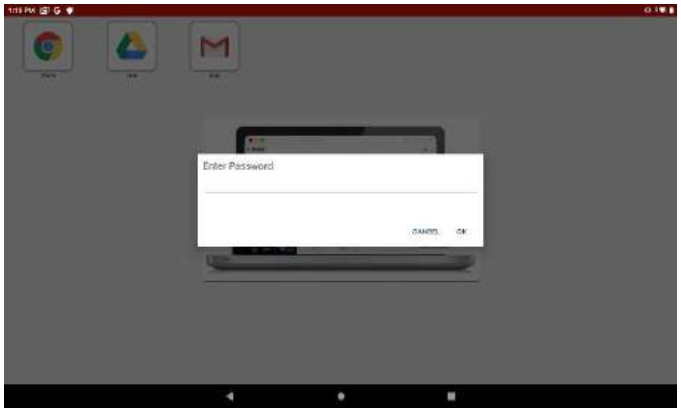
2. Select the **None** option and click **Apply**. The device will now revert to full functionality again.

4.2.1.8.4 Removing 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 Manager, 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. For a Windows or ChromeOS device, perform 5 mouse clicks on the computer display. You will be prompted for a password.



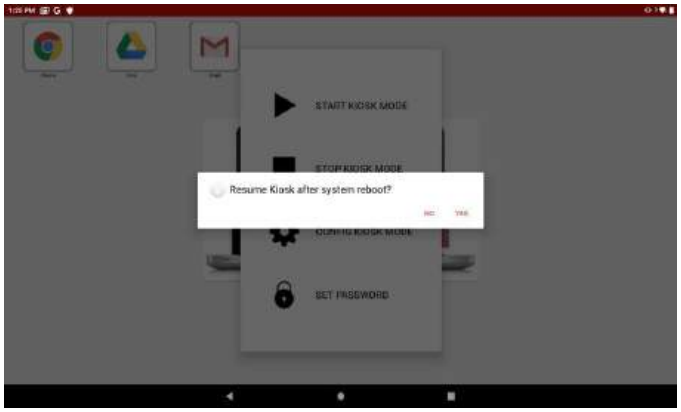
2. Enter a password (or leave it blank, if the kiosk is not password-protected), and click **OK**. The Kiosk menu opens:

4.2.1.8.4.1 Start Kiosk Mode

If you tap **Start Kiosk Mode**, the device will resume the latest Kiosk setting.

4.2.1.8.4.2 Stop Kiosk Mode

If you tap **Stop Kiosk Mode**. the device will go back to its normal functionality. You will receive the following screen:

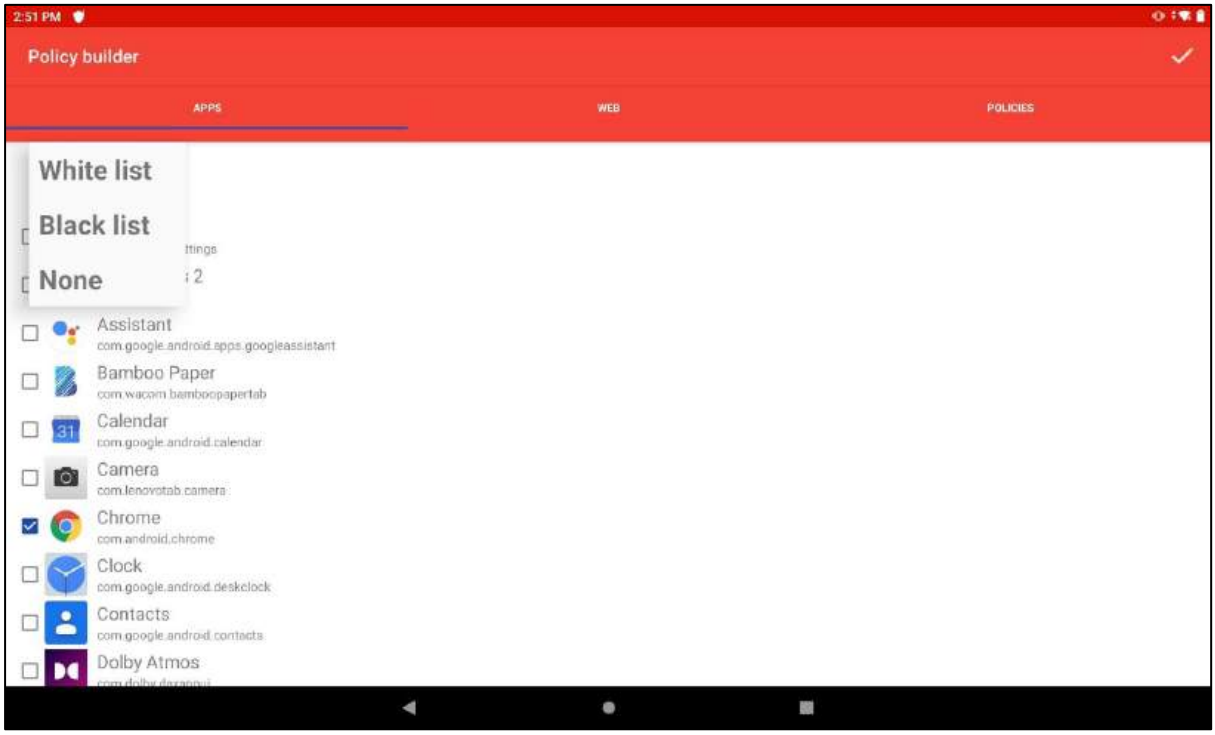


- Select **Yes** if you want the device to revert to Kiosk mode after you reboot it.
- Select **No** if you want to remove the Kiosk mode from the device entirely.

4.2.1.8.4.3 Config Kiosk Mode

Tap **Config Kiosk Mode** to modify the kiosk settings. You can change the list of allowed apps and URLs and apply a software policy to the device.

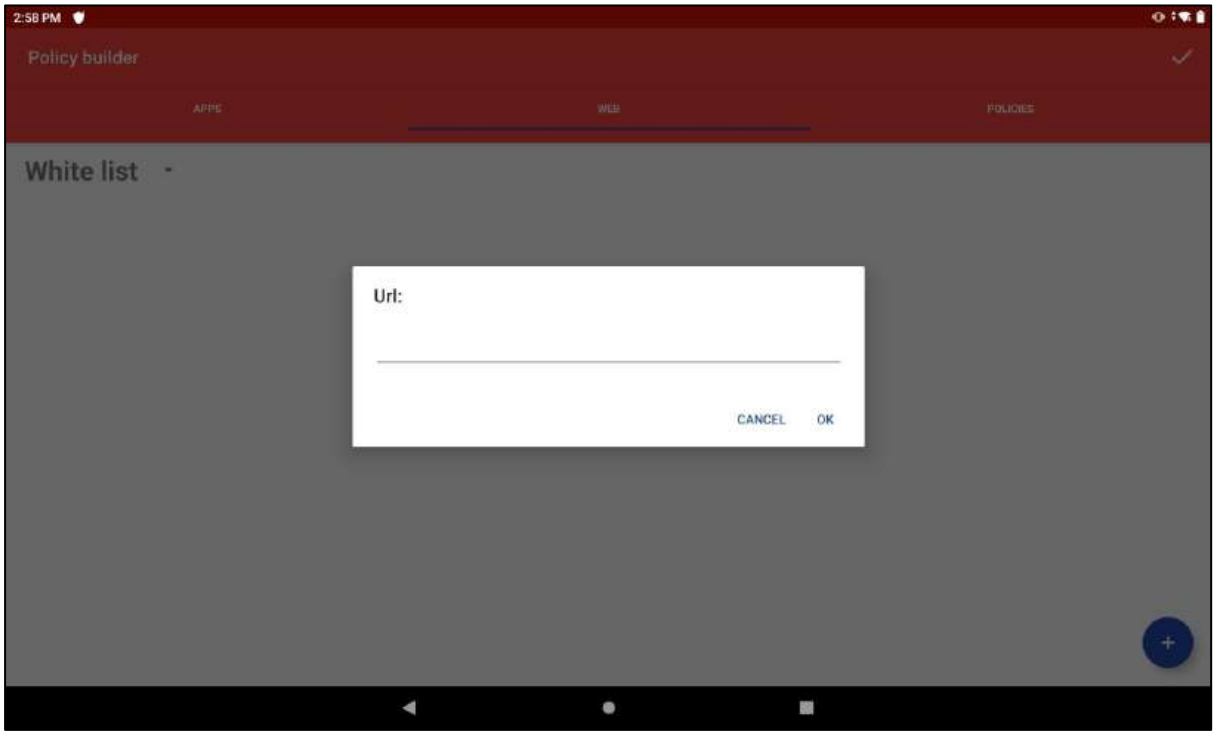
- **Apps whitelist/blacklist**: This allows you to select from apps already installed on the device, whether they should be allowed or blocked.



- **Web Whitelist/Blacklist**: You can select URLs to allow or block on the Kiosk device, by adding them to a whitelist or blacklist.

To add a URL:

1. Select whether you want the URL to be on an allow list (whitelist) or a block list (blacklist).
2. Click the blue **Add** icon in the lower right corner. The following window opens, prompting you for an URL:

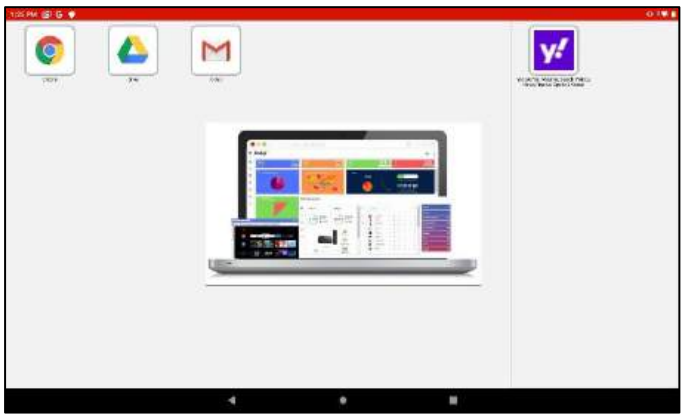


3. Enter the URL and tap OK. In the example below, we added Yahoo! to the allowed URLs.

The URL will be added to the whitelist of allowed URLs.

4. To delete the newly added URL, tap the **Delete** icon on the right.

5. The tablet's Kiosk display now shows the added URL:



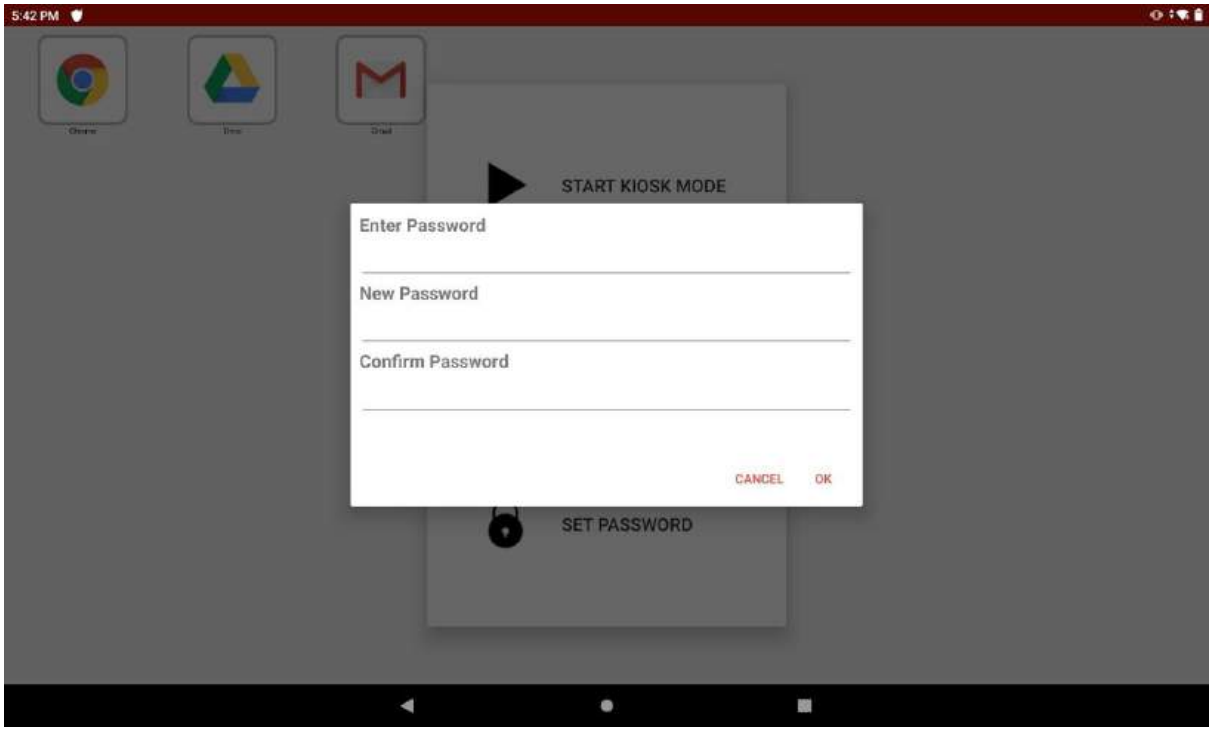
- **Policies**: This allows you the user to block or unblock the ability to install apps on the remote device, set the background image and its orientation, and set a policy password.

To save changes to the list of apps, URLs, and policies, tap the checkmark in the upper right.

You will see a confirmation in the lower left corner that the Kiosk policy has been saved.

4.2.1.8.4.4 Set Password

This allows you to set a new password to the Kiosk mode.

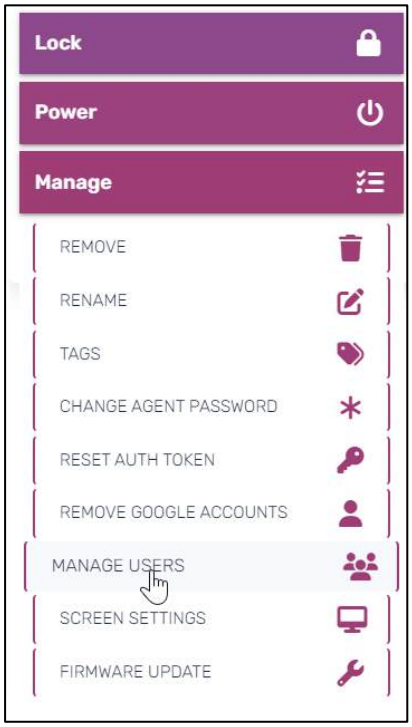


4.2.1.9 Manage users

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

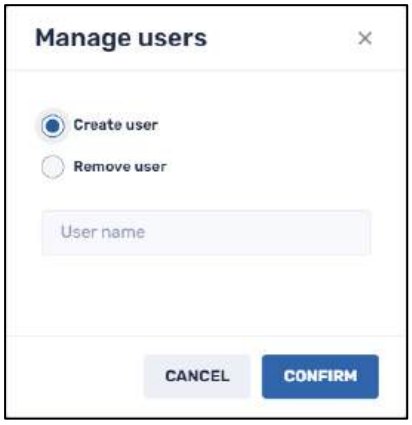
The **Manage users** feature can be accessed by:

- The device's three-dot menu
- The Devices Console Ribbon
- 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**.

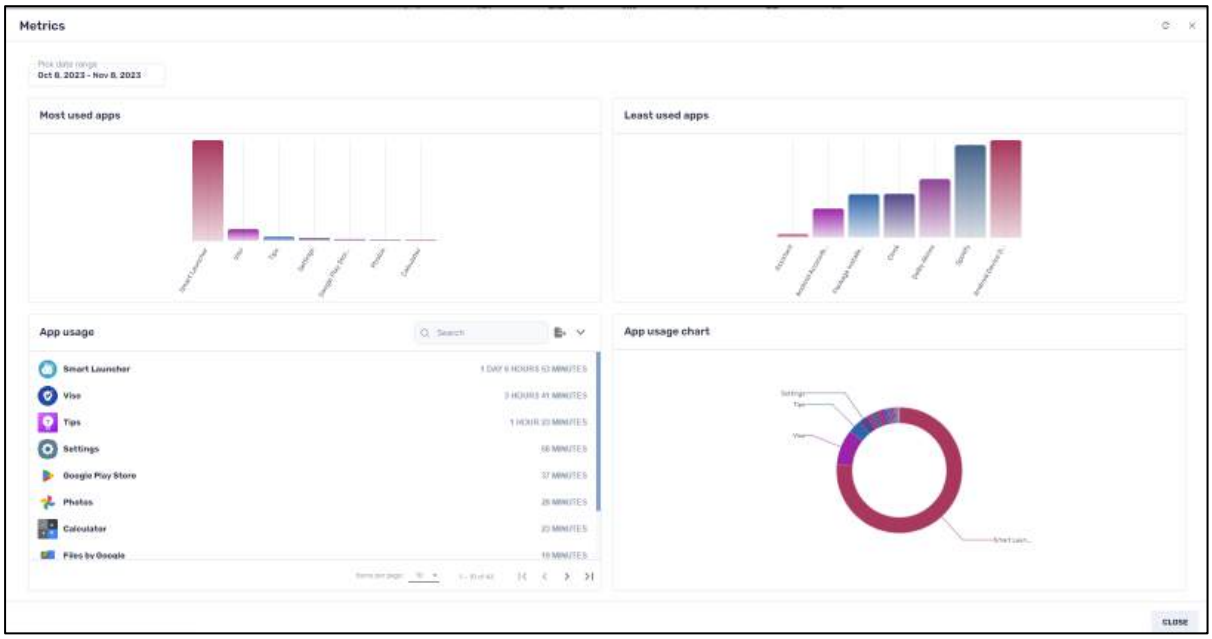


Note: You must have Administrator privileges to create and remove users from using this feature.

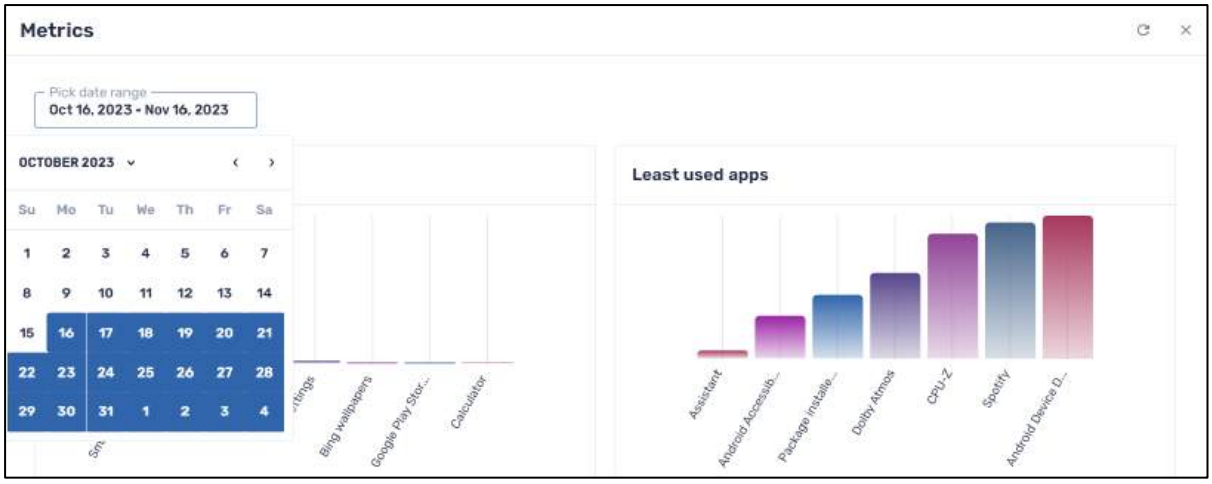
4.2.1.10 Metrics

This provides graphical displays of app usage on a device, to see which apps are used the most, and which are used the least. This information can help you make fact-based decisions, to optimize the usage of your device and make it into a true business asset.

When you click on the **Metrics** tile, you will see graphs that tell you about app usage.



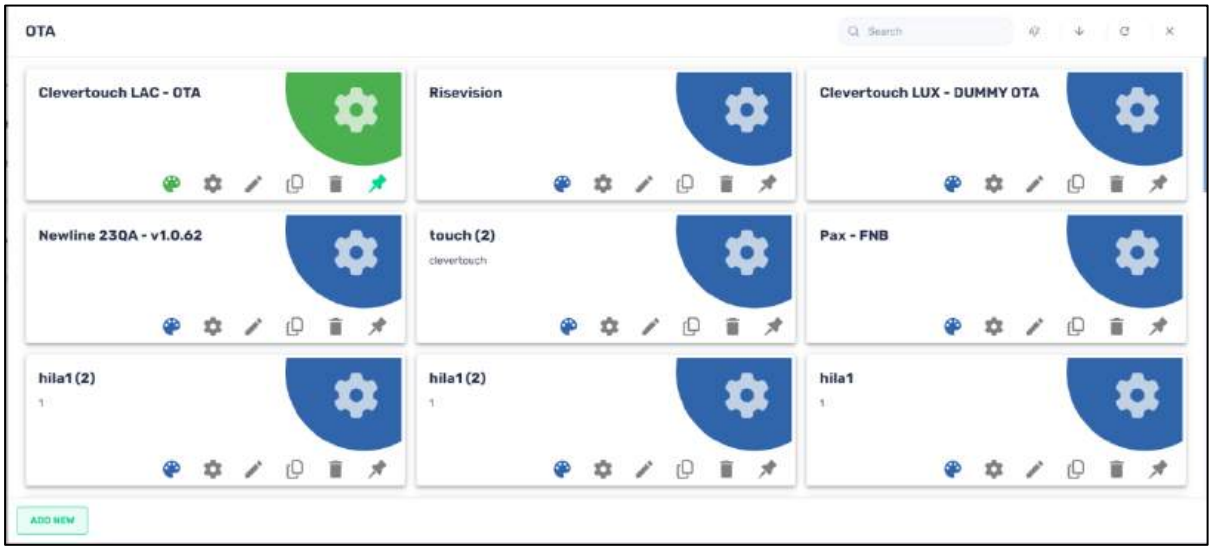
There is also an option to select a range of dates, search for an app and view its usage stats, and to graph the results for a specified time period.



4.2.1.11 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.

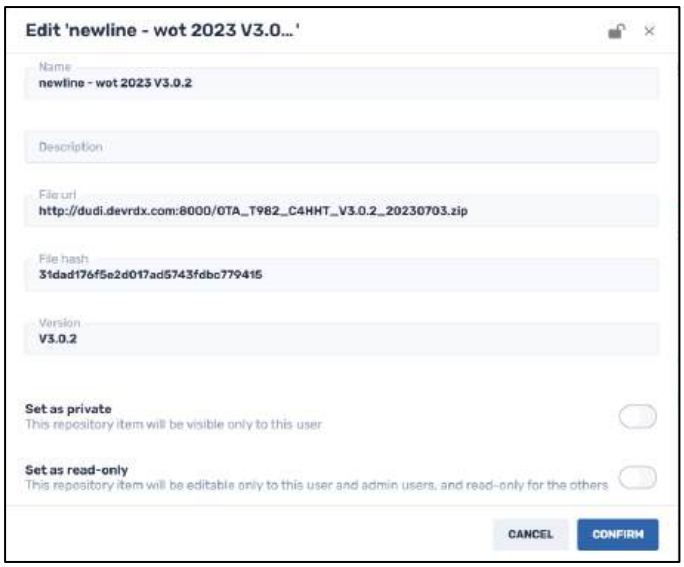
When you click on **OTA**, a grid of stored OTA updates appears.



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

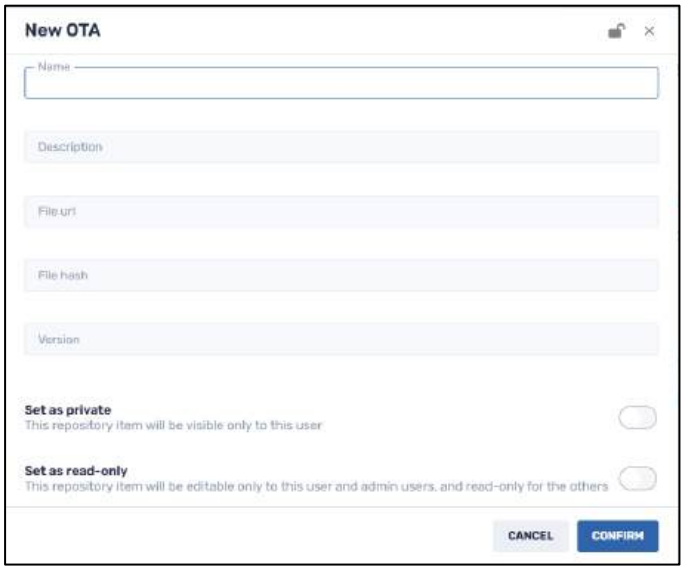
To edit an existing OTA setting:

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**.



To create a new OTA setting:

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

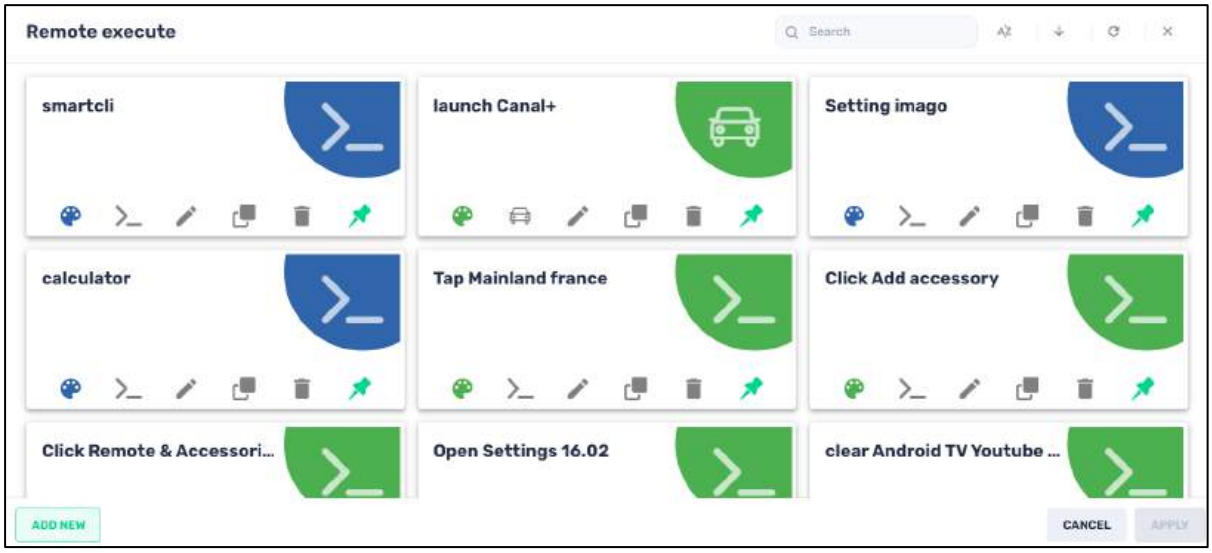


2. Supply the necessary information in the fields.
3. Click on the **Set as private** button if you would like the OTA setting to only be visible to you (as the creator of the item) when using the Radix Device Manager.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the 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 .
5. Click **Confirm** to save the OTA setting.
6. To send an OTA option to a device, select the relevant tile, and click **Apply**.

4.2.1.12 Remote Execute

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 the **Remote Execute** tile, the Remote Execute 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 **Remote execute** window. The **New Remote Execution** window appears.

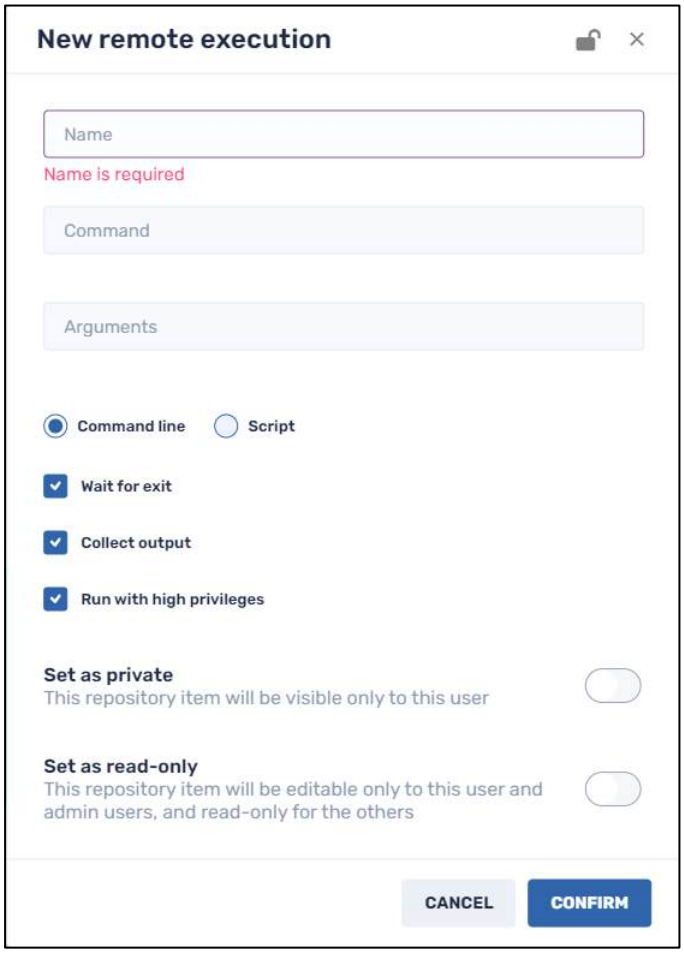


Figure 4-33: Remote execute command interface

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 Manager.
3. 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 .
4. Select the command and click **Apply**. The command will be sent to the selected device.

4.2.1.12.1 Examples of a Remote Execute Command

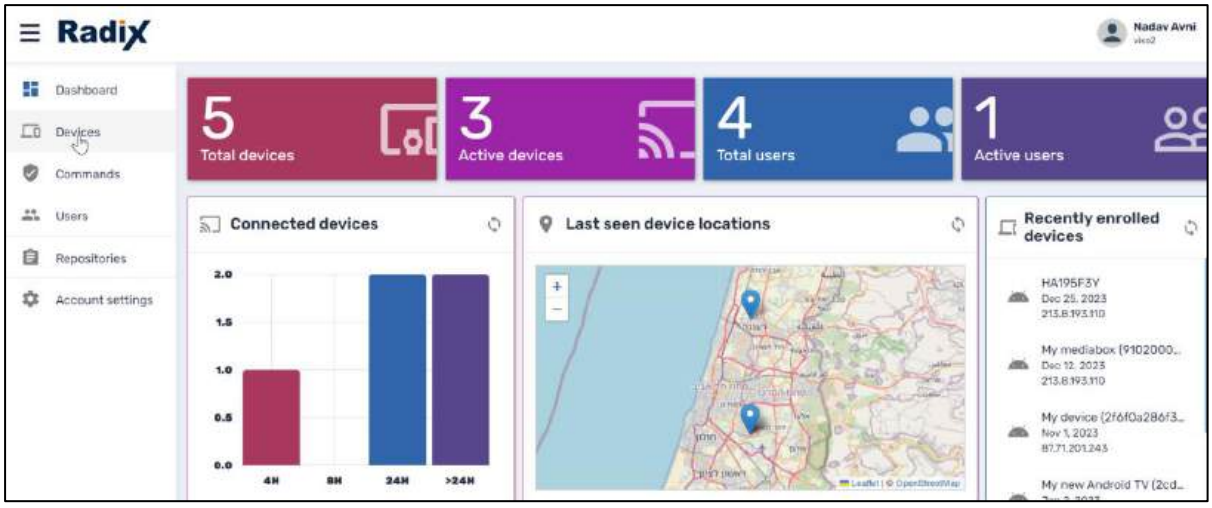
Let us perform some simple examples of a command that we send to a device remotely.

4.2.1.12.1.1Example No. 1: Top Command

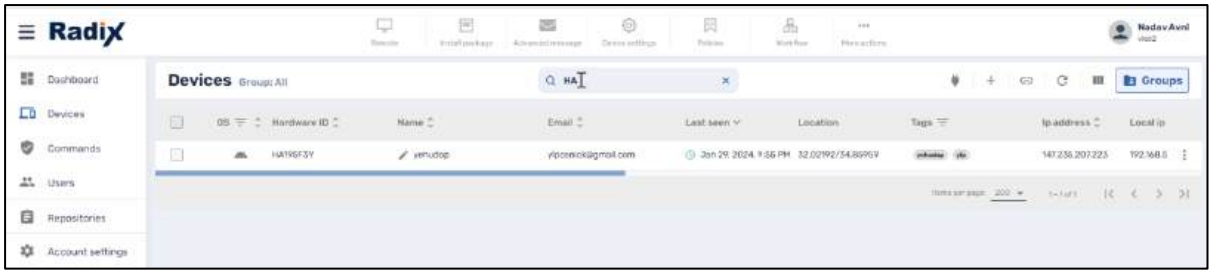
We will illustrate the remote execute command with the Android command "top". The "top" command will get a list of processes running on the remote device and display the result.

To use the Remote Execute command "top":

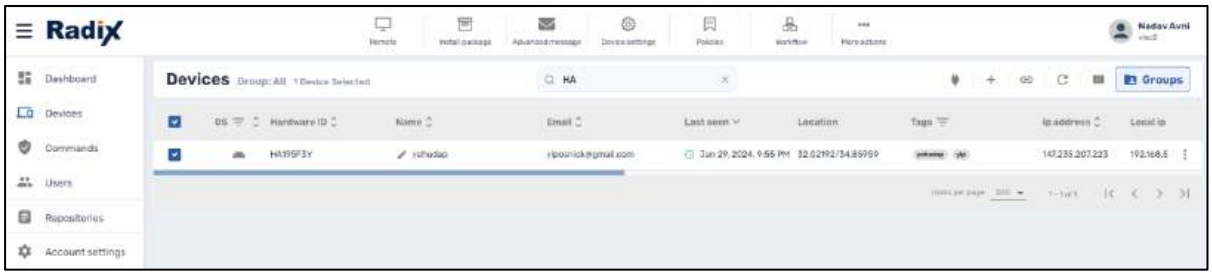
1. From the Overview Dashboard, click on the **Devices Console** icon, to see a list of all the available devices.



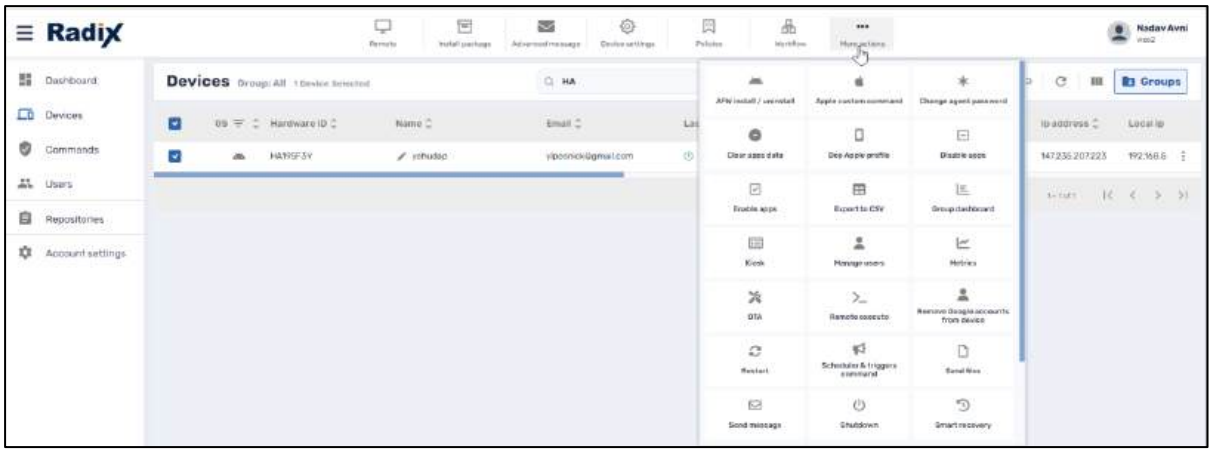
2. Find the device to which you would like to execute the command. Use the Search Bar at the top, to narrow down the selection.



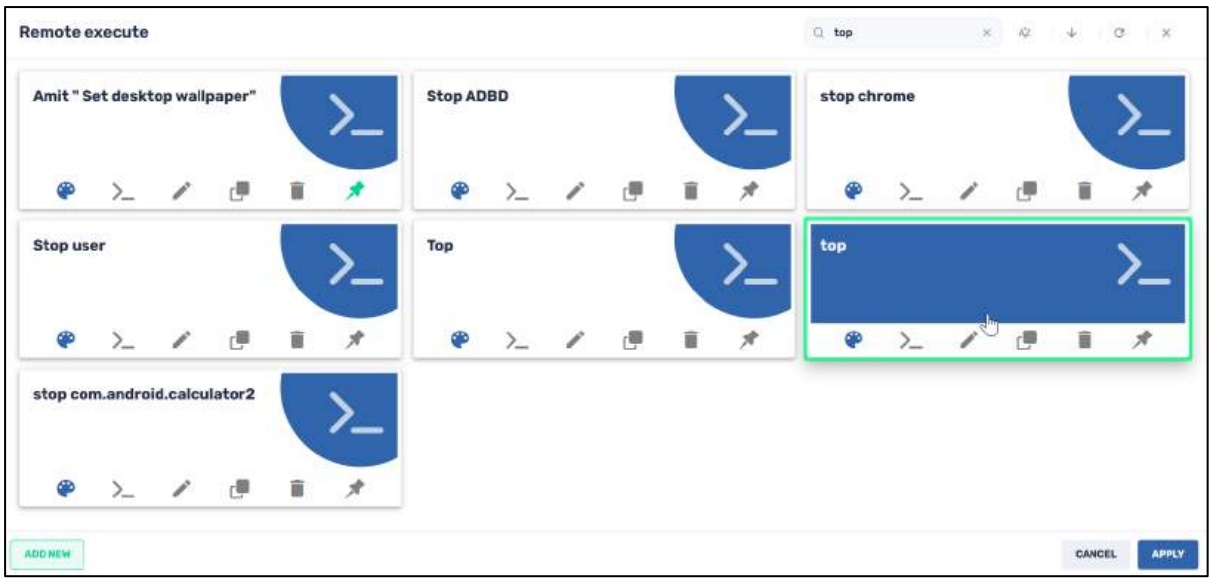
3. In the list of devices, click on the device's checkbox at the beginning of the line where the device is listed. The Devices Console Ribbon at the top of the screen will become active.



4. Click on the **More Actions** icon in the ribbon at the top of the Devices Console 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:

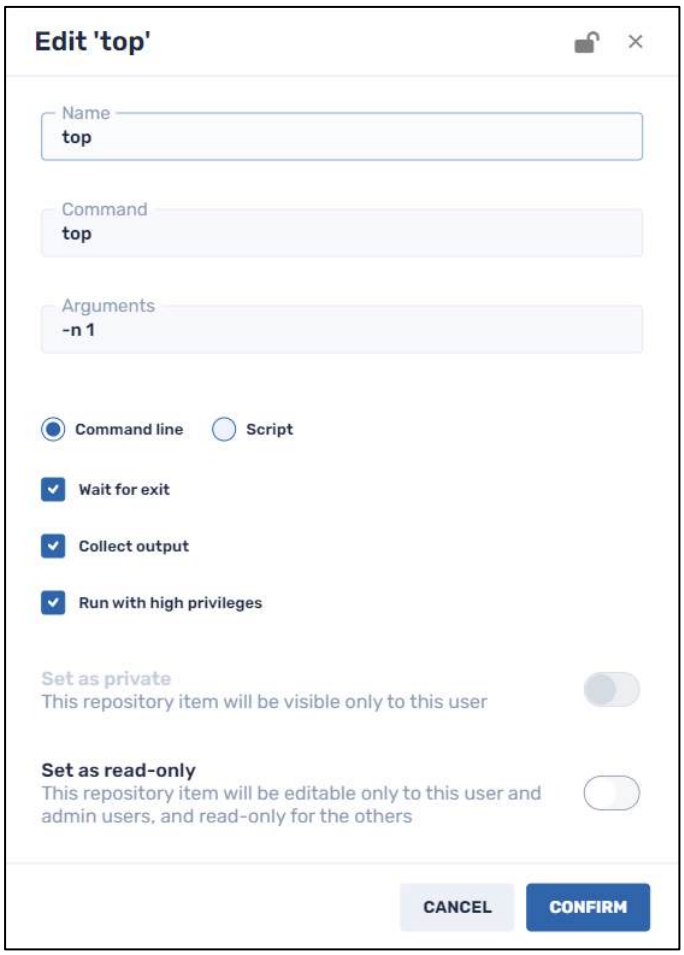


Figure 4-34: Remote Execute command "top", showing the command and its arguments

(The argument `-n 1` displays 1 line in the list of apps currently running.)

7. 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.

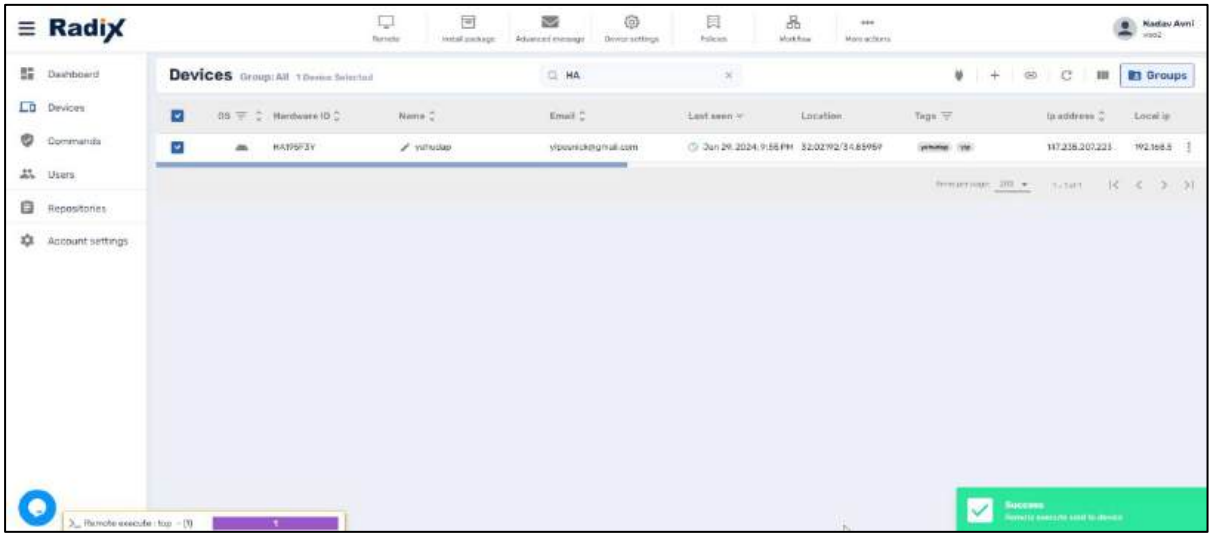


Figure 4-35: Alert that the Remote Execute command has been performed successfully

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:

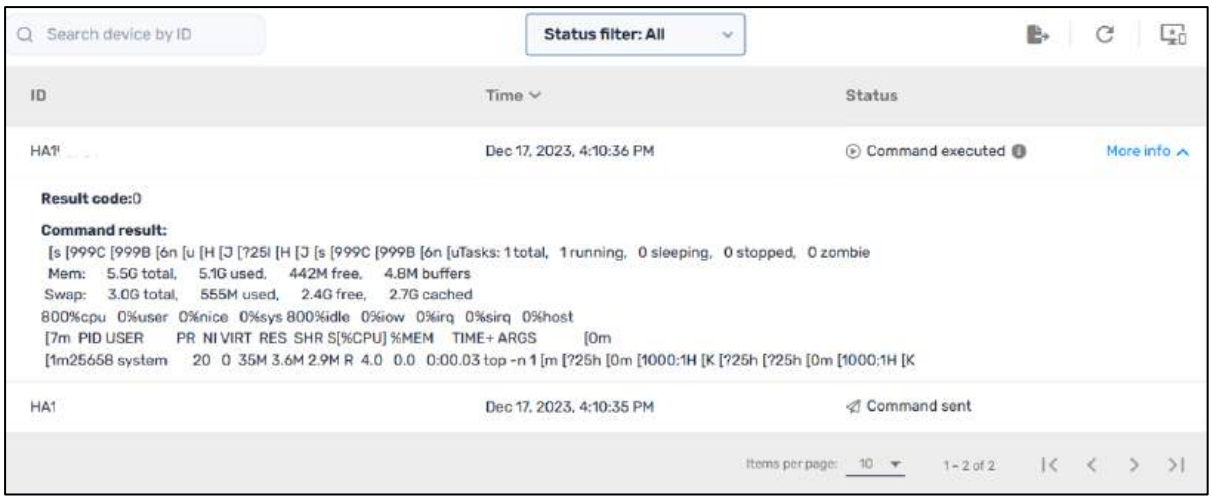


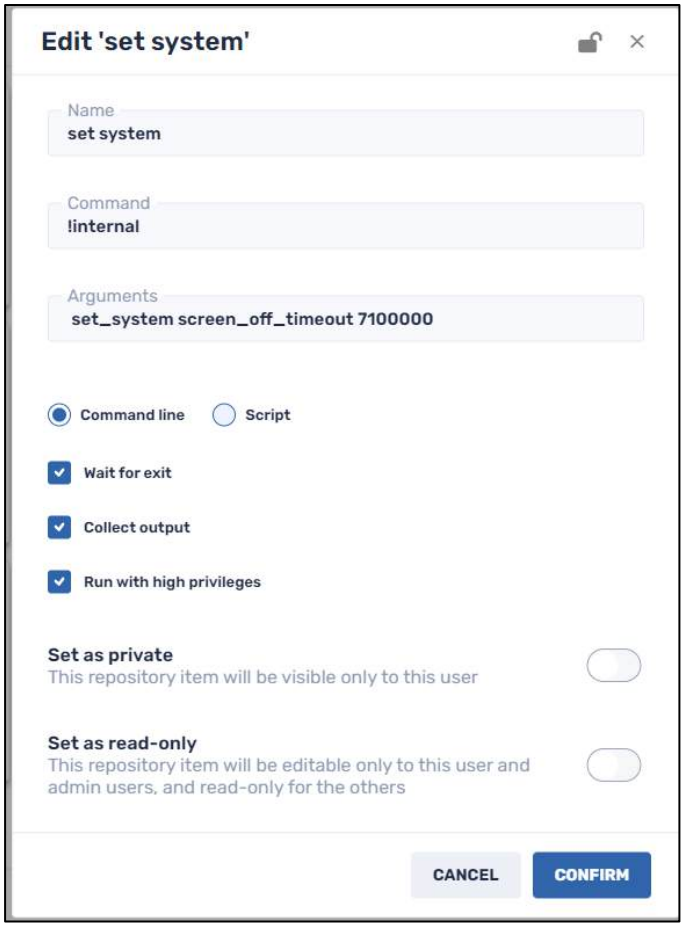
Figure 4-36: Command Status window, displaying the results of the "top" command

4.2.1.12.1.2 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.



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`

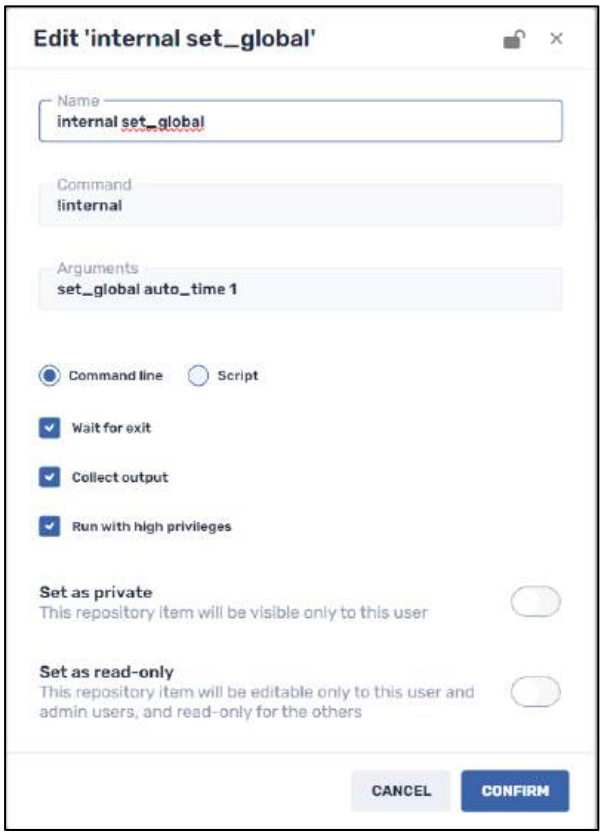
In this example, the command will set how long the screen on the Android device will remain lit. The argument for the amount to time it will stay lit is set for 7,100,000 milliseconds (= 118 minutes and 20 seconds).

4.2.1.12.1.3 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.



You can fill out the fields with the following parameters:

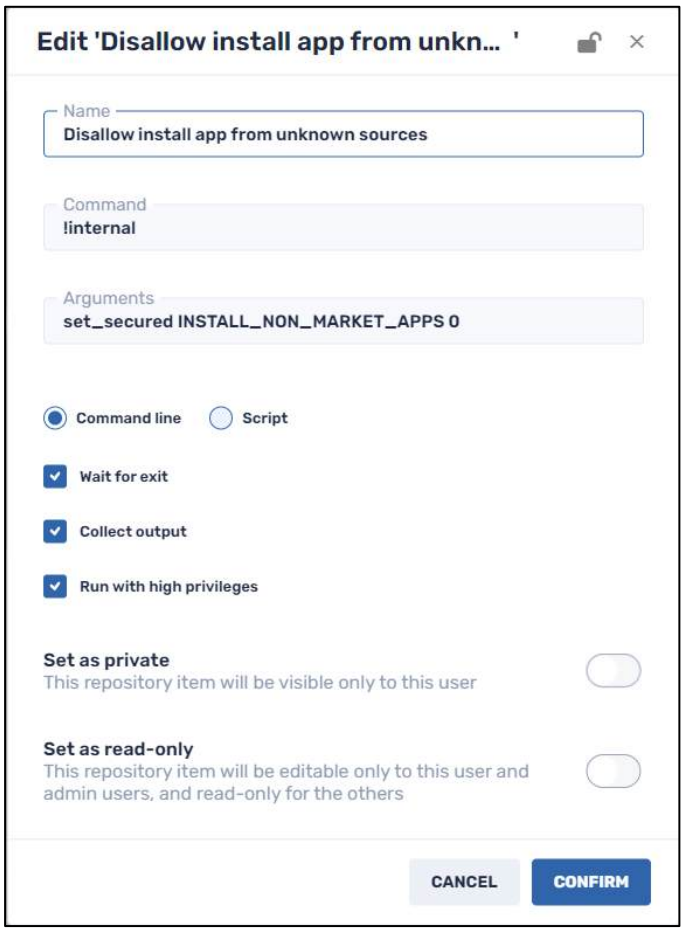
Command: `!internal` (as above, the "!internal" command helps ensure that the user has sufficient permissions to execute the command)

Arguments: `set_global auto_time 1`

4.2.1.12.1.4 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>`**



You can fill out the fields with the following parameters:

Command: `!internal` (as above)

Arguments: `set_secured INSTALL_NON_MARKET_APPS 0`

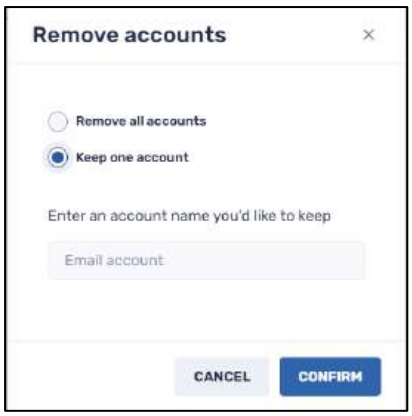
In this example, we employ the argument "`INSTALL_NON_MARKET_APPS`" and set the parameter to "0", to disallow installing apps from suspicious sites.

4.2.1.13 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 the Remove Google Accounts tile. The **Remove Accounts** window appears.



2. If you select "Remove all accounts" and click **Confirm**, you will get confirmation 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. Click **Confirm**. You will get confirmation that all Google accounts have been removed, except for the one that you wished to retain.

4.2.1.14 Restart

This allows the Radix Device Management user to restart a device remotely.

To use the Restart command:

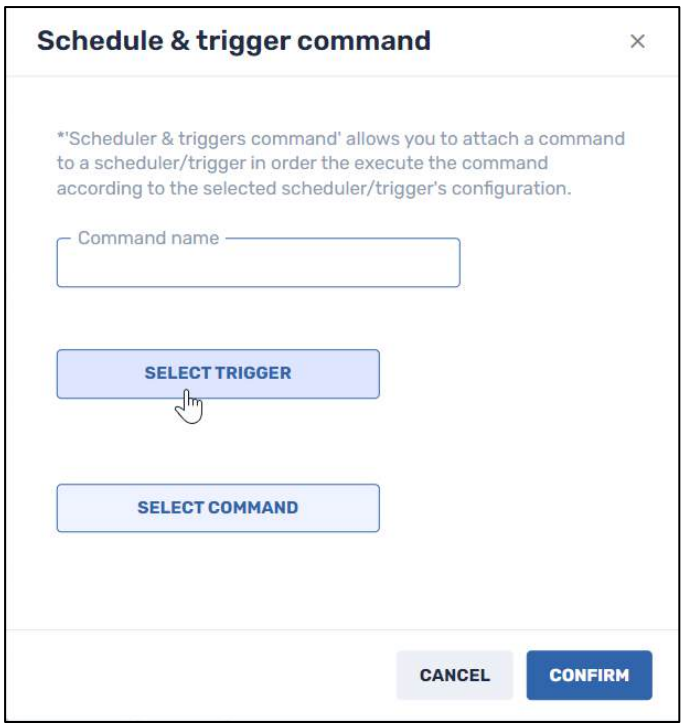
1. Click on the **Restart** command tile. The Restart window opens:

2. Click on **Yes**. The device will restart remotely.

4.2.1.15 Scheduler & Triggers Command

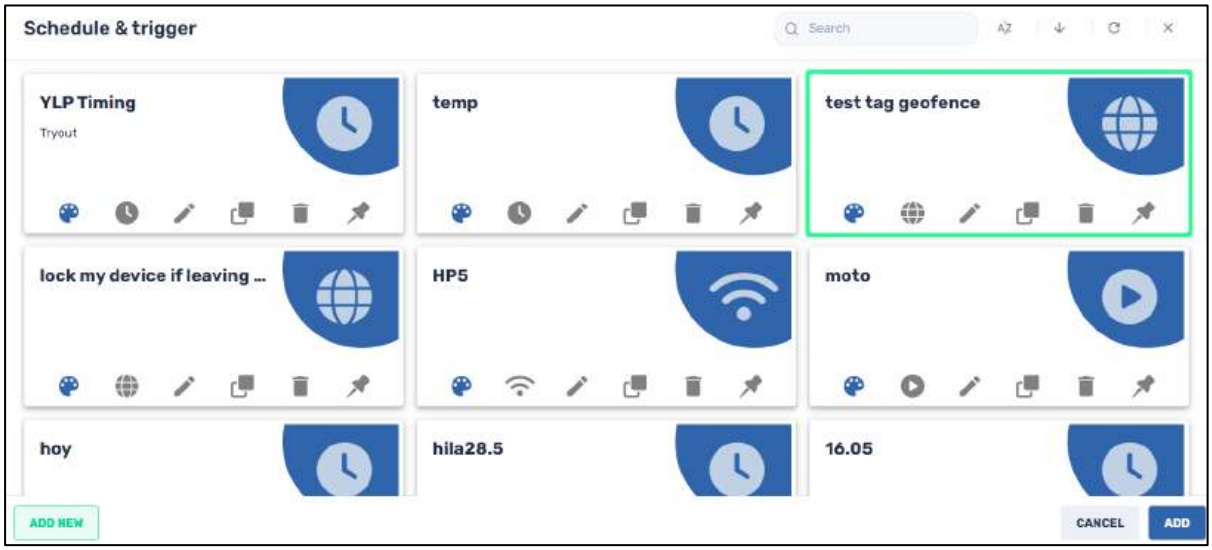
This allows you to create a trigger for a device (by timing, geofencing, Wi-Fi, or upon Startup) from within the Device Dashboard, and lets you program the device's reaction to the trigger, by selecting a particular command to be executed.

When you click on the **Schedule & Trigger command** tile, the **Schedule & Trigger Command** window opens:



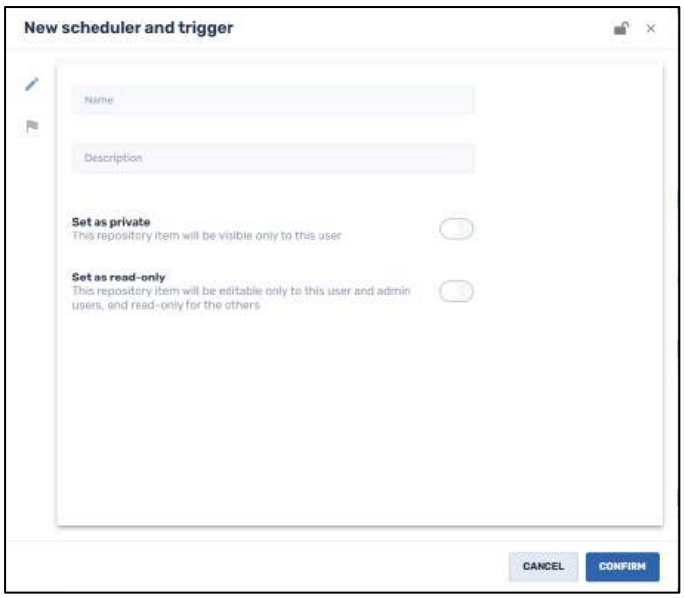
To use the Schedule & trigger command:

1. Assign a name to the command.
2. Click **Select Trigger**. The **Schedule & Trigger** window opens, with saved options.

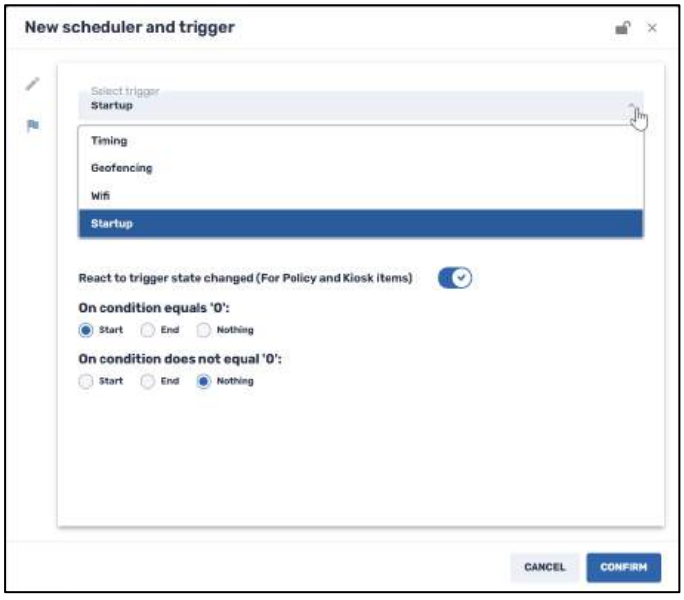


If you wish to create a new **Schedule & trigger** command.

1. Click on **Add New**. The **New scheduler and trigge**r window opens.



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 Manager.
4. 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 .
5. 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.

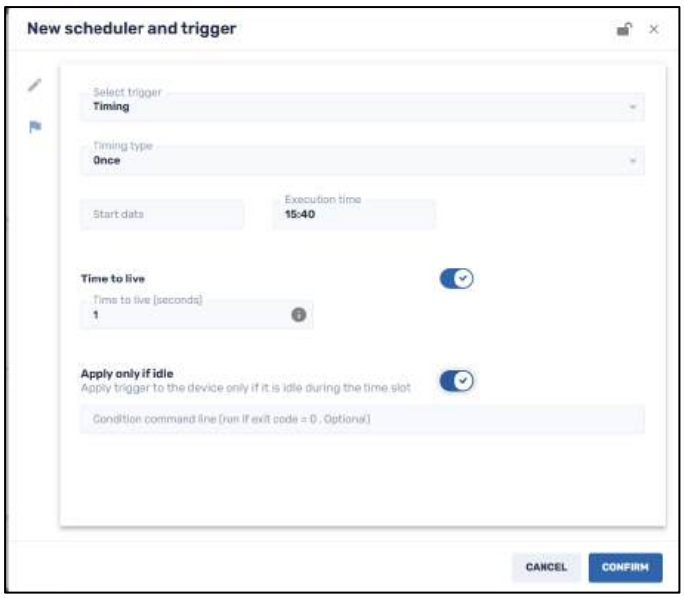


Figure 4-37: Timing option with a one-time trigger

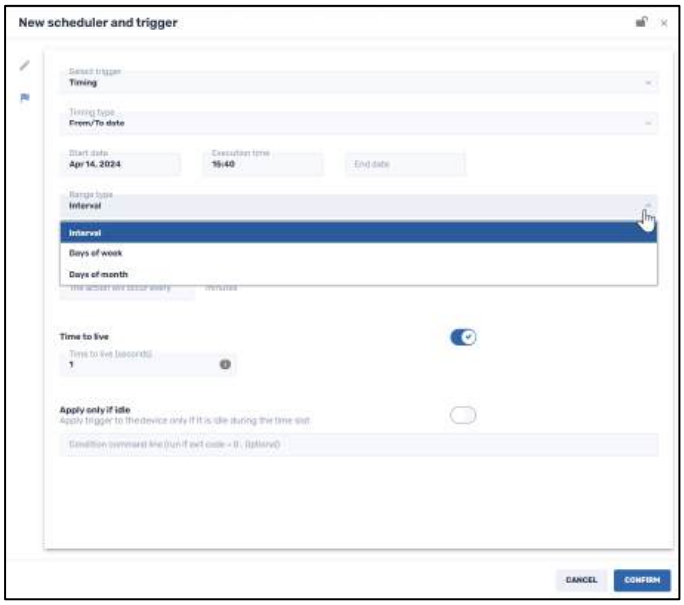


Figure 4-38: Timing option with a trigger on defined dates

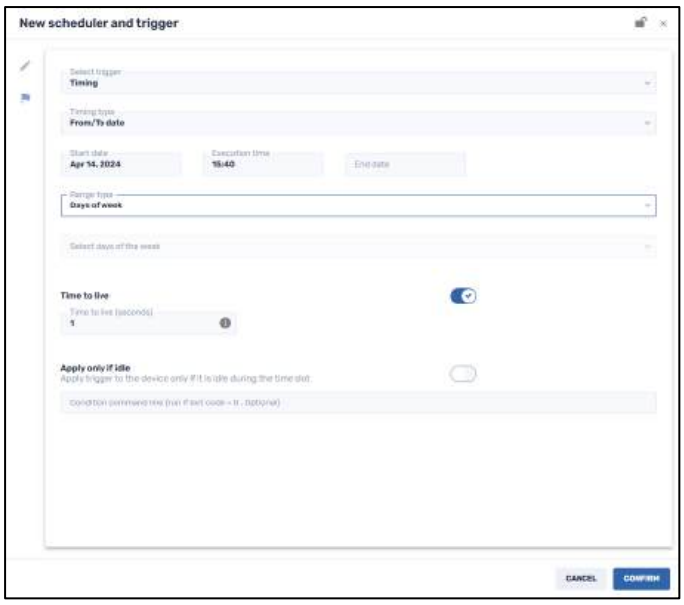


Figure 4-39: Trigger option with no end date

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 (**Section 4.4.3.8**).

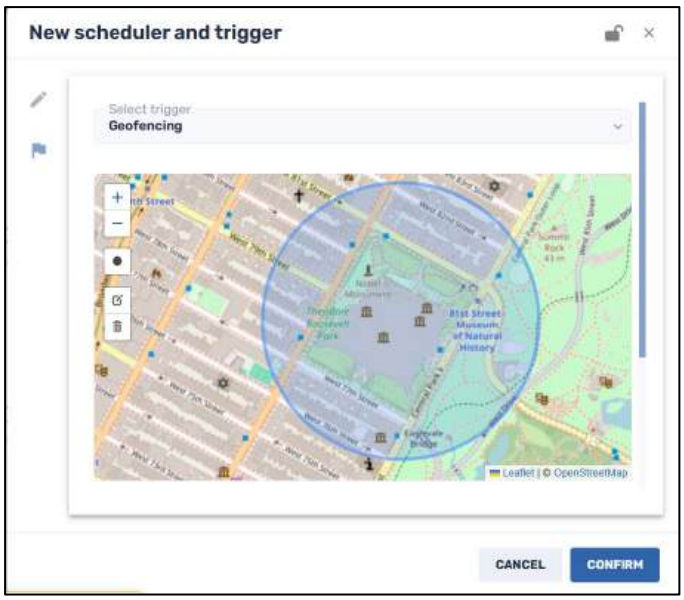
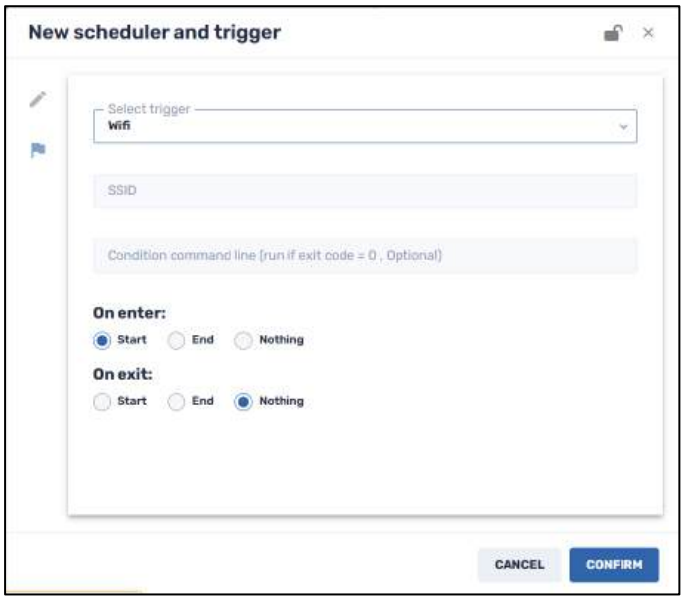
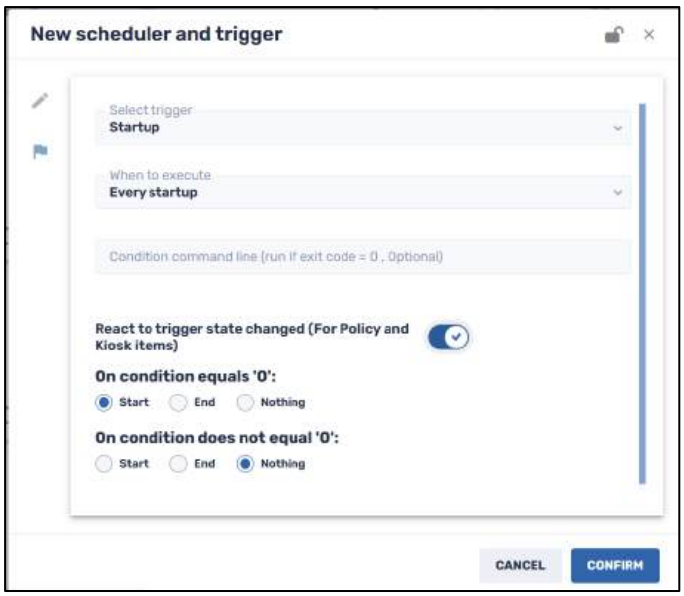


Figure 4-40: Geofencing Option, delimiting a geographical area

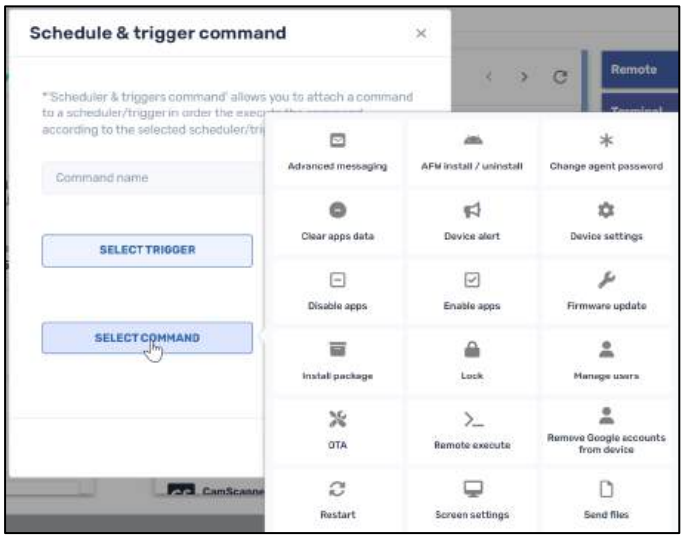
- **Wi-Fi**: To execute a command upon receiving a Wi-Fi trigger.



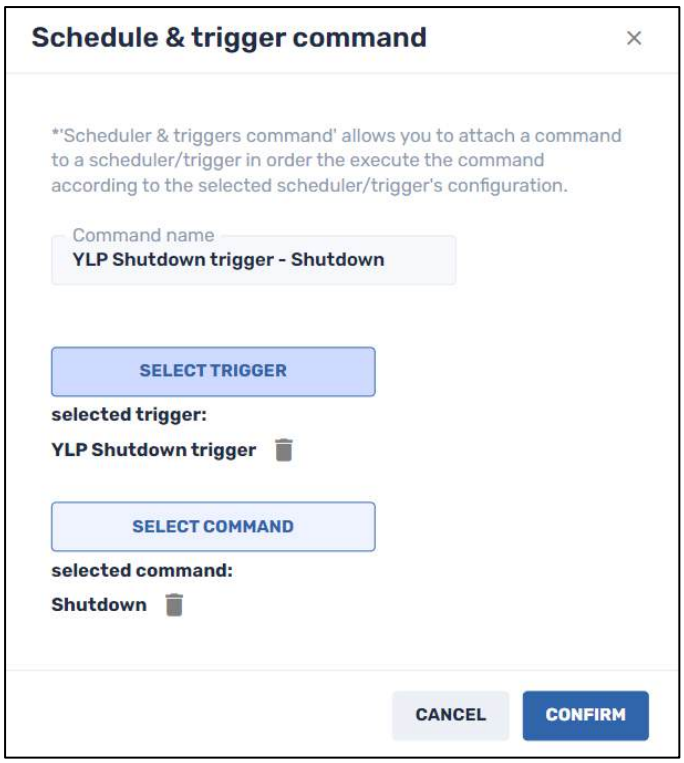
- **Startup**: To execute a command on the device every time it starts up.



6. After you have selected a trigger, you then click on the **Select Command** button to specify a command to be executed.



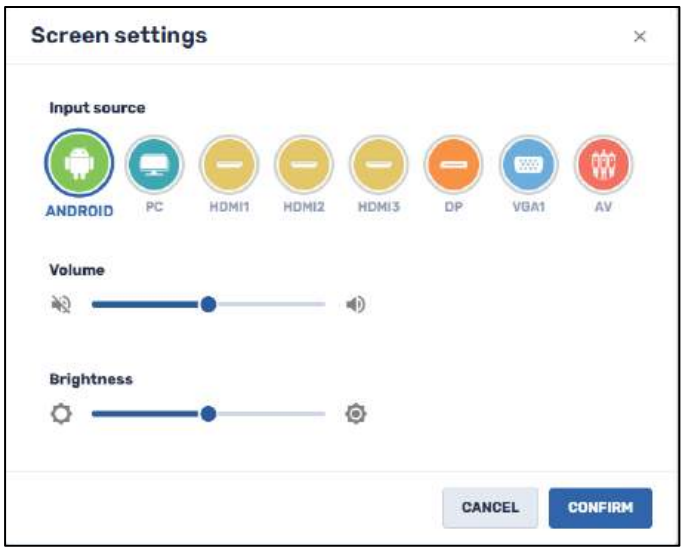
7. After you select the command, you link it together with the desired trigger. The result should appear something like this:



4.2.1.16 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:



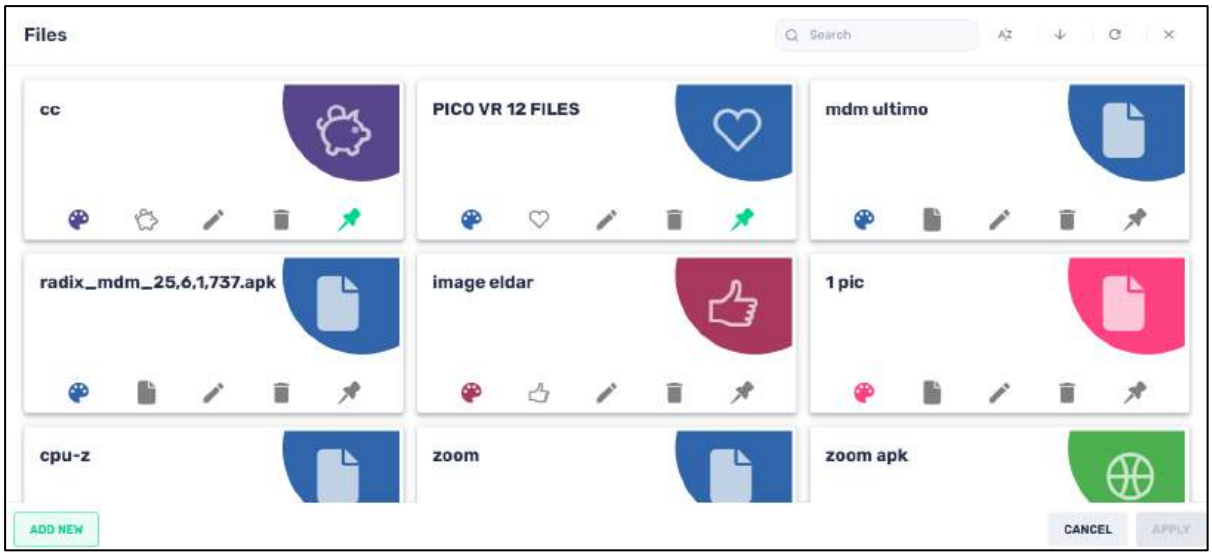
To use the Screen Settings command:

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.

4.2.1.17 Send Files

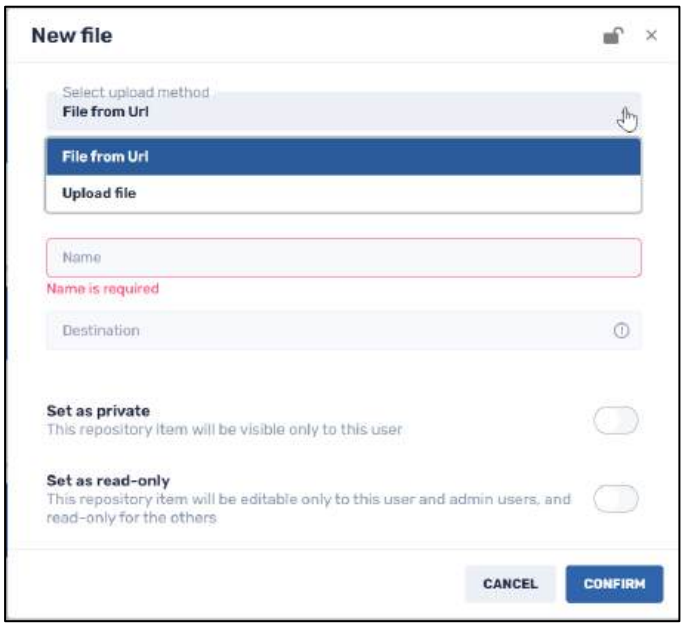
This allows you to send specific files to a remote device. You can either supply a URL from which to retrieve the file or upload a file from your computer.

When you click on the **Send files** tile, the Files window opens.

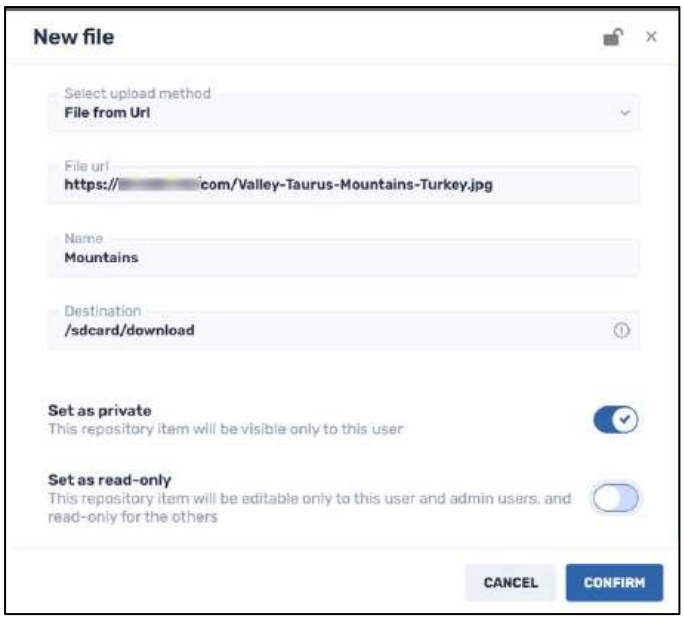


To add a file to the repository from the Internet:

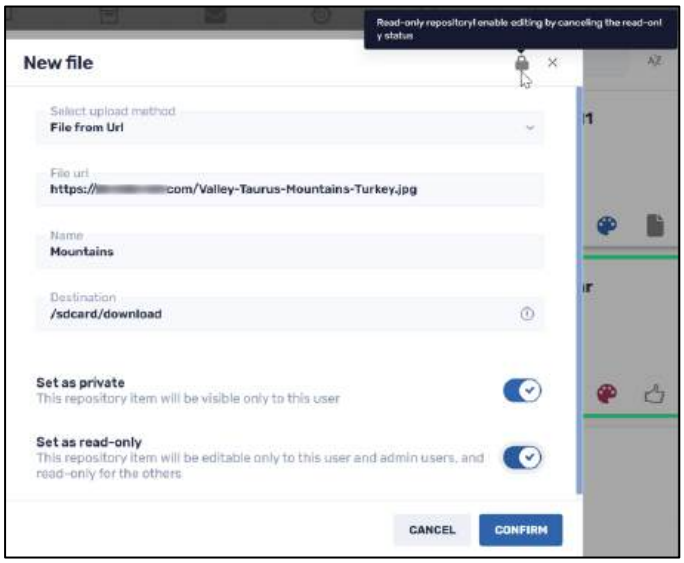
1. Click on **Add New** in the lower left corner. The **New File** window opens.



2. 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).



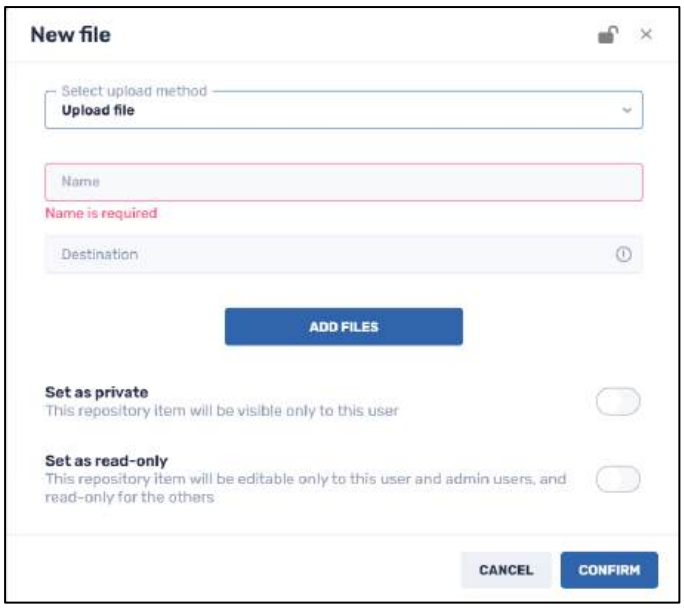
3. Click on the **Set as private** button if you would like the file option to only be visible to you (as the creator of the item) when using the Radix Device Manager.
4. Click on the **Set as read-only** button if you would like to limit who will be able to edit the details of the file uploaded. Anyone 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 .



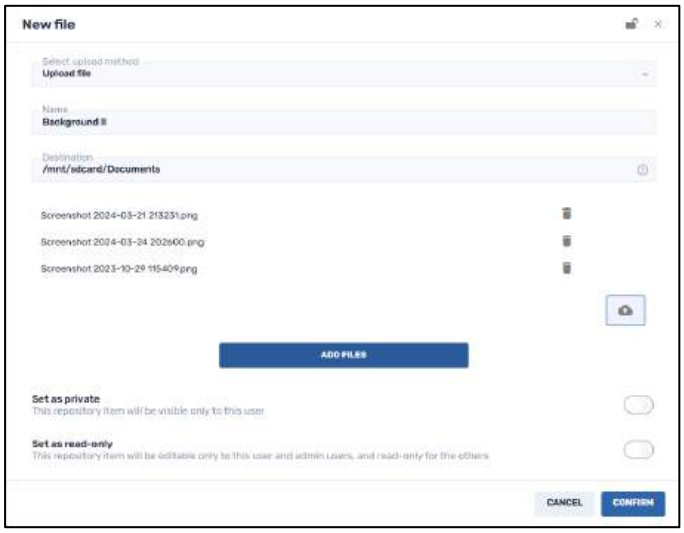
5. Click **Confirm**. The new **File** option will appear in the Files window, allowing you to send it to the selected devices.

To add a file from your computer to the repository:

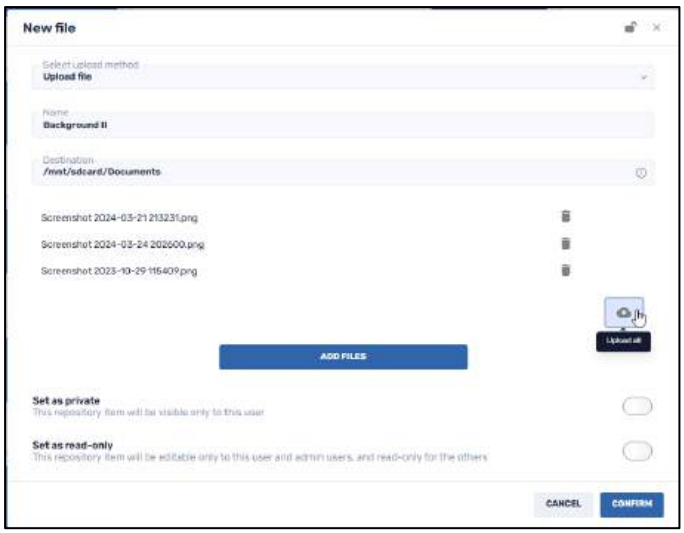
1. Click on **Add New** in the lower left corner. The **New File** window opens.
2. Choose **Upload file** to upload a file from your computer to the Files repository on the Radix Device Management interface.



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.



5. When you have finalized your selection of files, click on **Upload All**.



6. 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 Manager.
7. 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 .
8. Click **Confirm**. The files will be added to the Files repository item under the name that you selected.

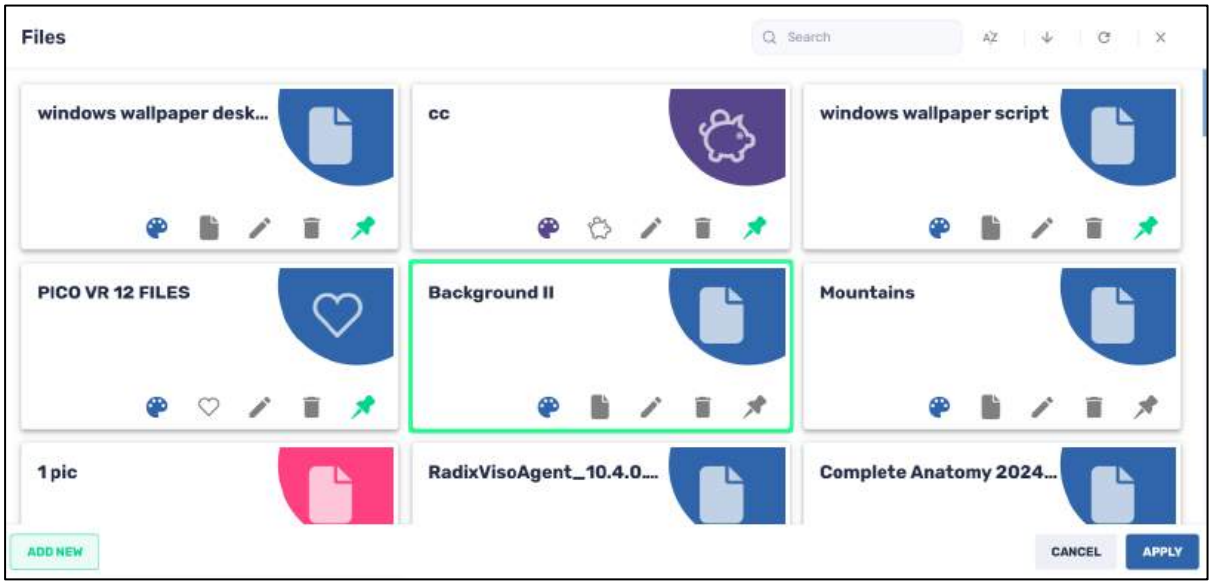


Figure 4-41: The Files repository item "Background II" has been added

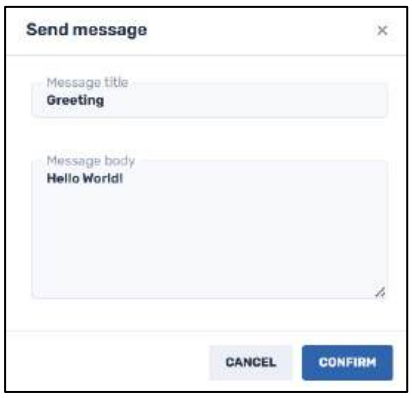
4.2.1.18 Send Message

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 **Send Message** command. The Send Message window opens.

2. Supply a message title and body and click **Confirm**. The message is sent immediately to the device.



4.2.1.19 Shutdown

This command shuts the device down remotely.

To shut down a device remotely:

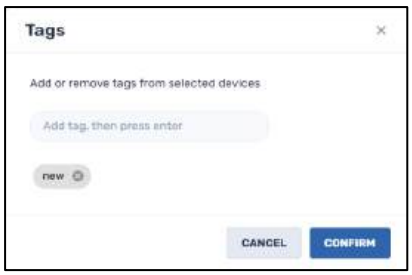
1. Click on the **Shutdown** command. The Shutdown window opens.
2. Click on **Yes** when prompted whether you wish to shut down the device.

4.2.1.20 Sound 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.

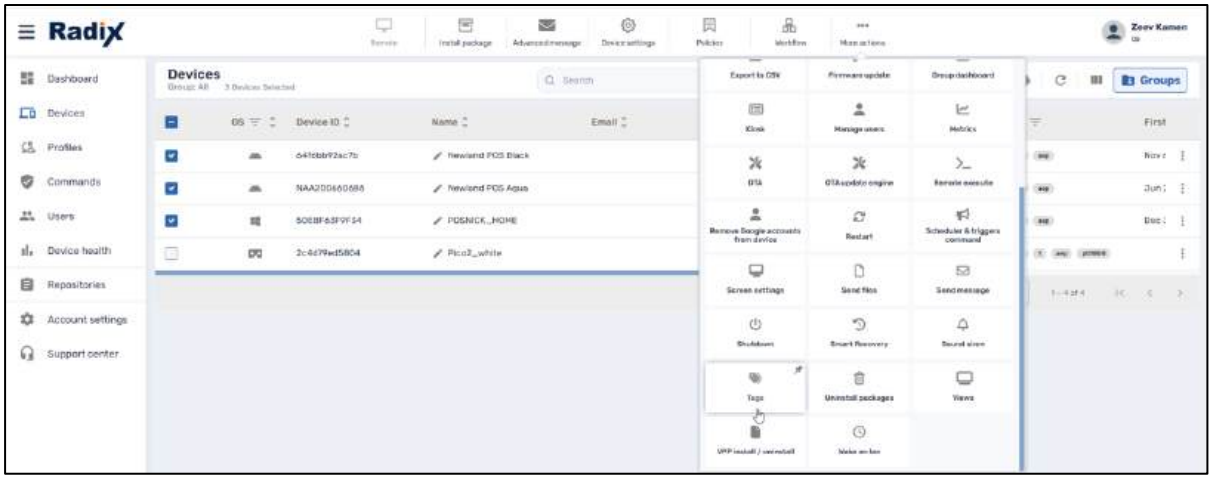
4.2.1.21 Tags

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 Device Console, select a device, or several devices, by checking their checkbox in the far-left column.
2. Click on **More Actions** in the Devices Console Ribbon and select the **Tags** tile.



3. 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:

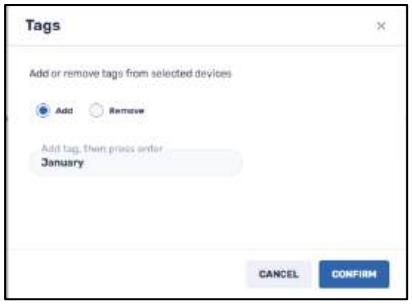
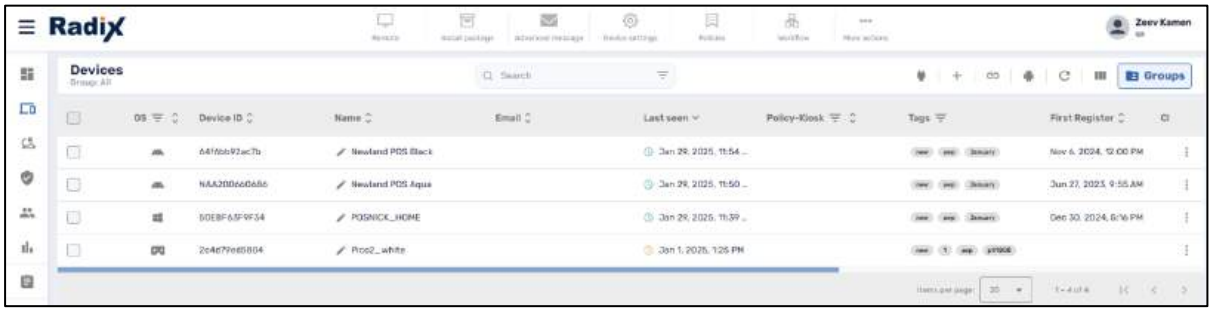
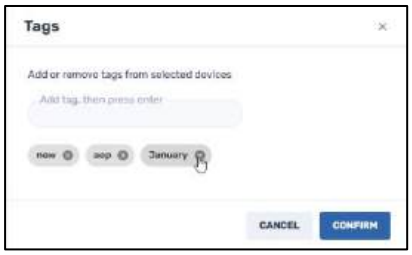


Figure 4-42: The tag "January" will be added to those three devices



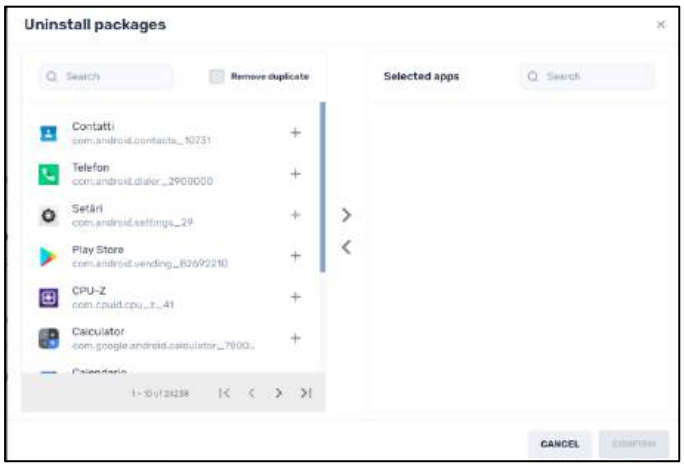
4. If you wish to delete a tag from a device, select that device, click on the **Tags** command, and click on the  on the tag you would like to delete.



4.2.1.22 Uninstall Packages

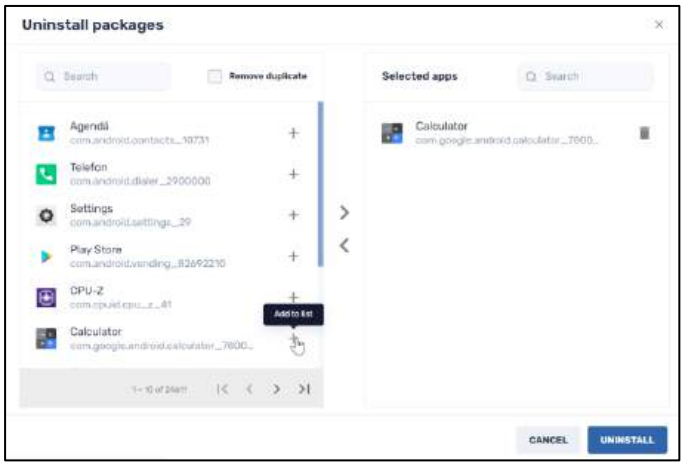
This command lets you uninstall software packages or apps on a device.

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.



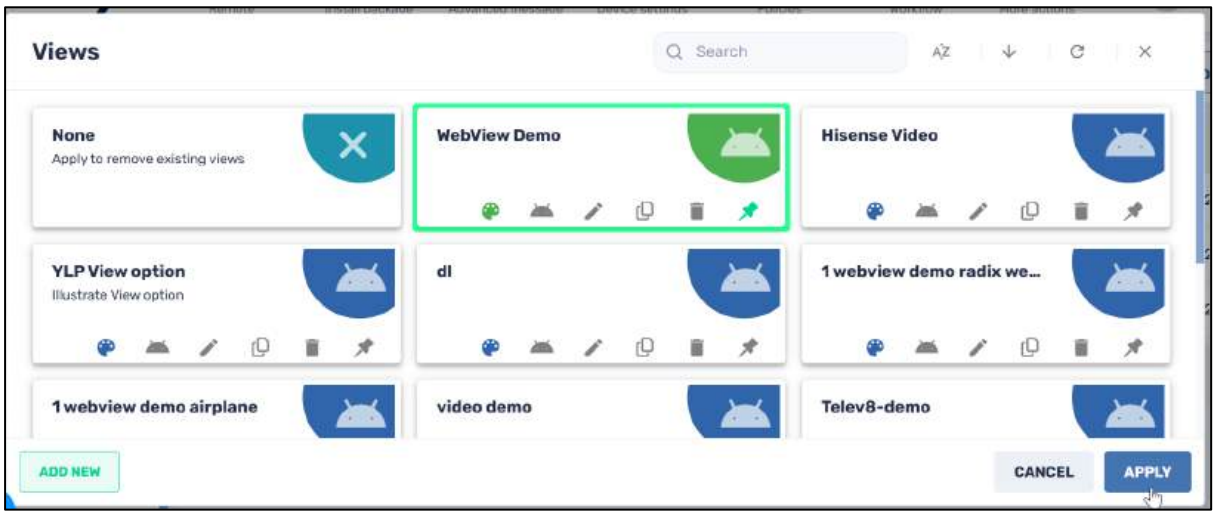
2. Click **Uninstall** to remove the software packages from the device.

4.2.1.23 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.

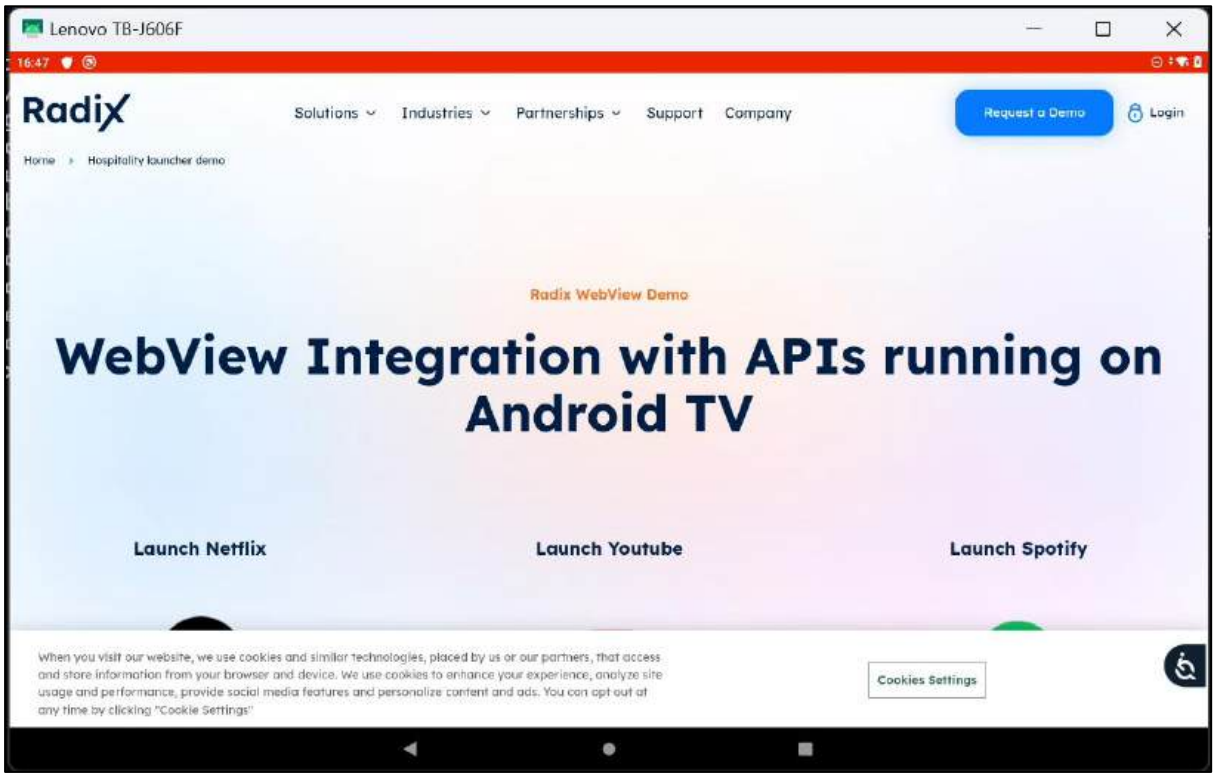
4.2.1.23.1 Applying a View Option

4. When you click on the **Views** tile, the **Views** options will appear.



5. 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.

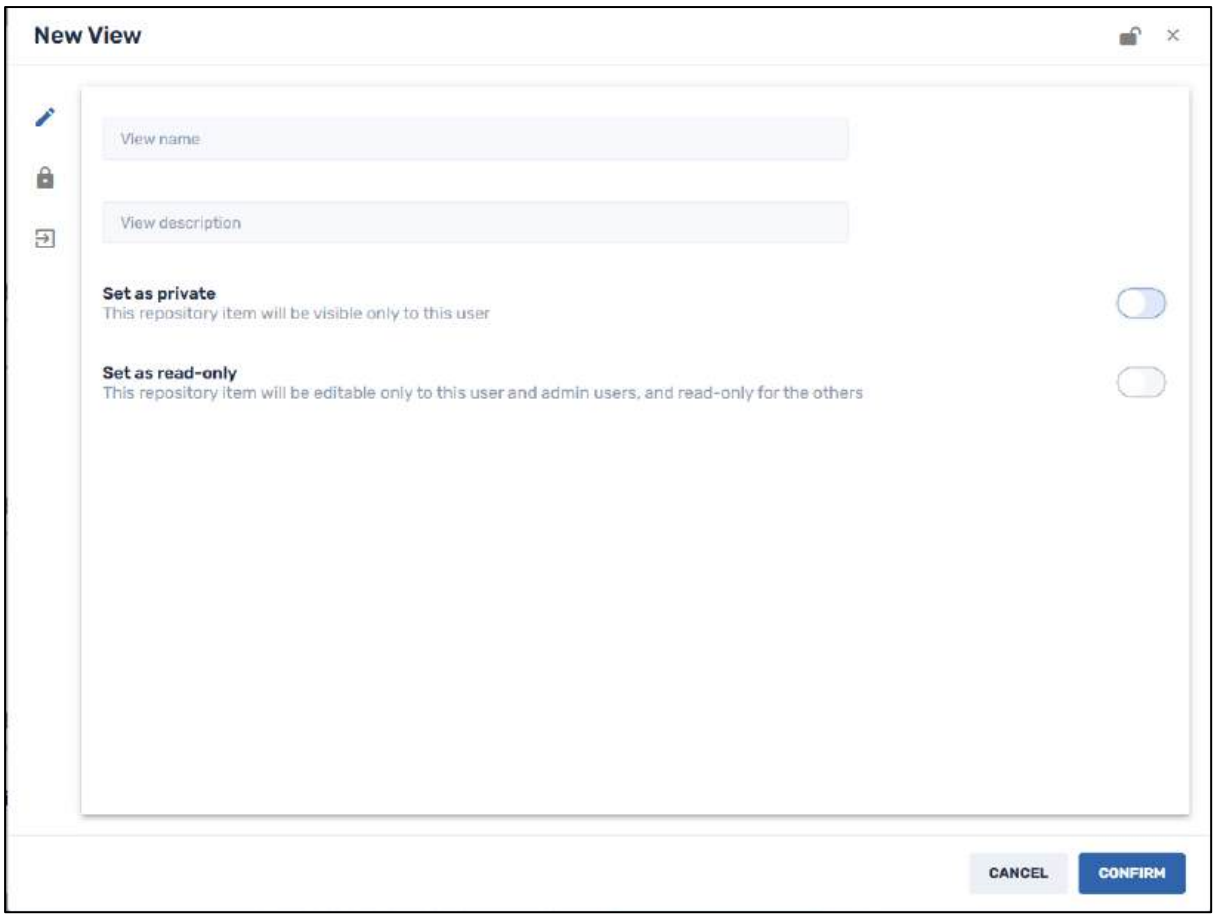


4.2.1.23.2 Creating a New View Option

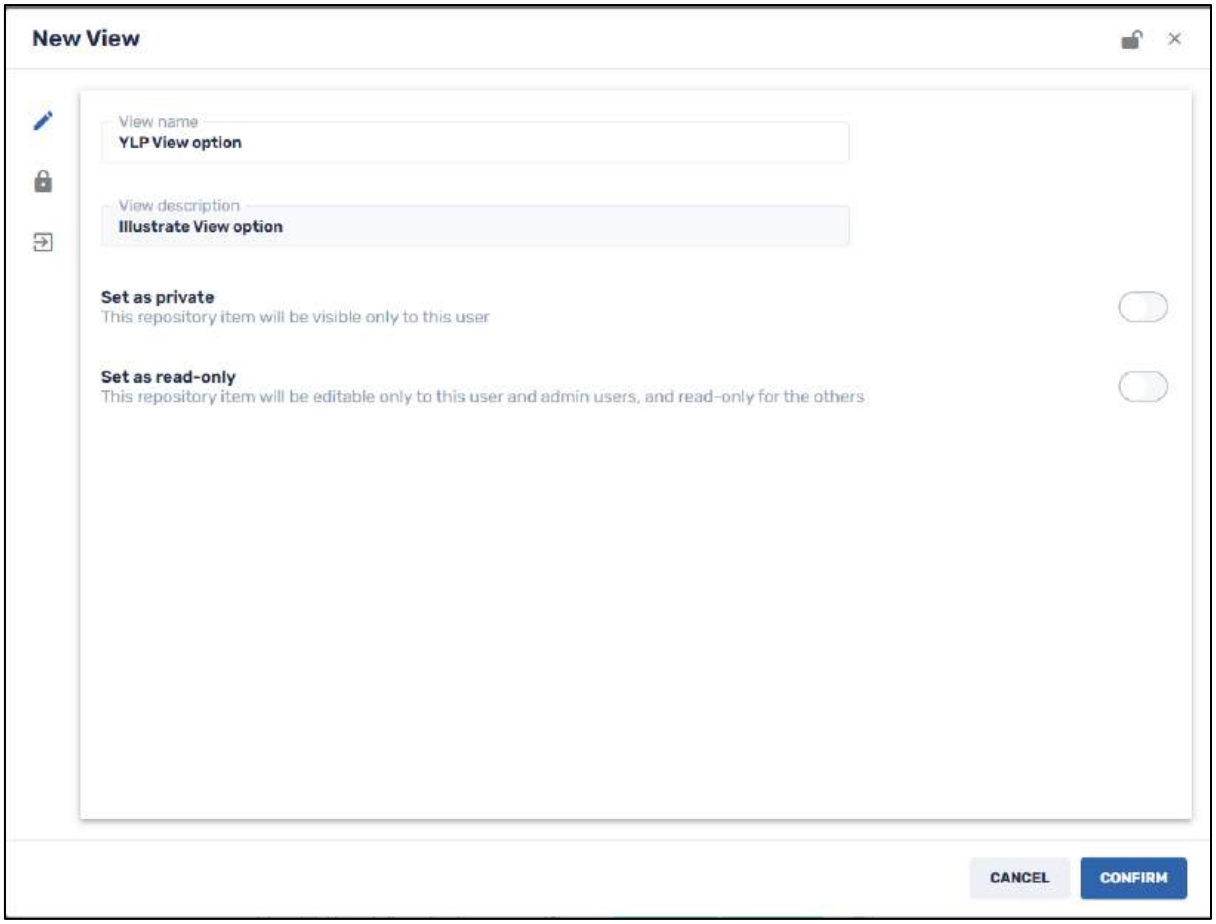
You can also add a new View option and customize it according to your preferences.

To add a new **View** option:

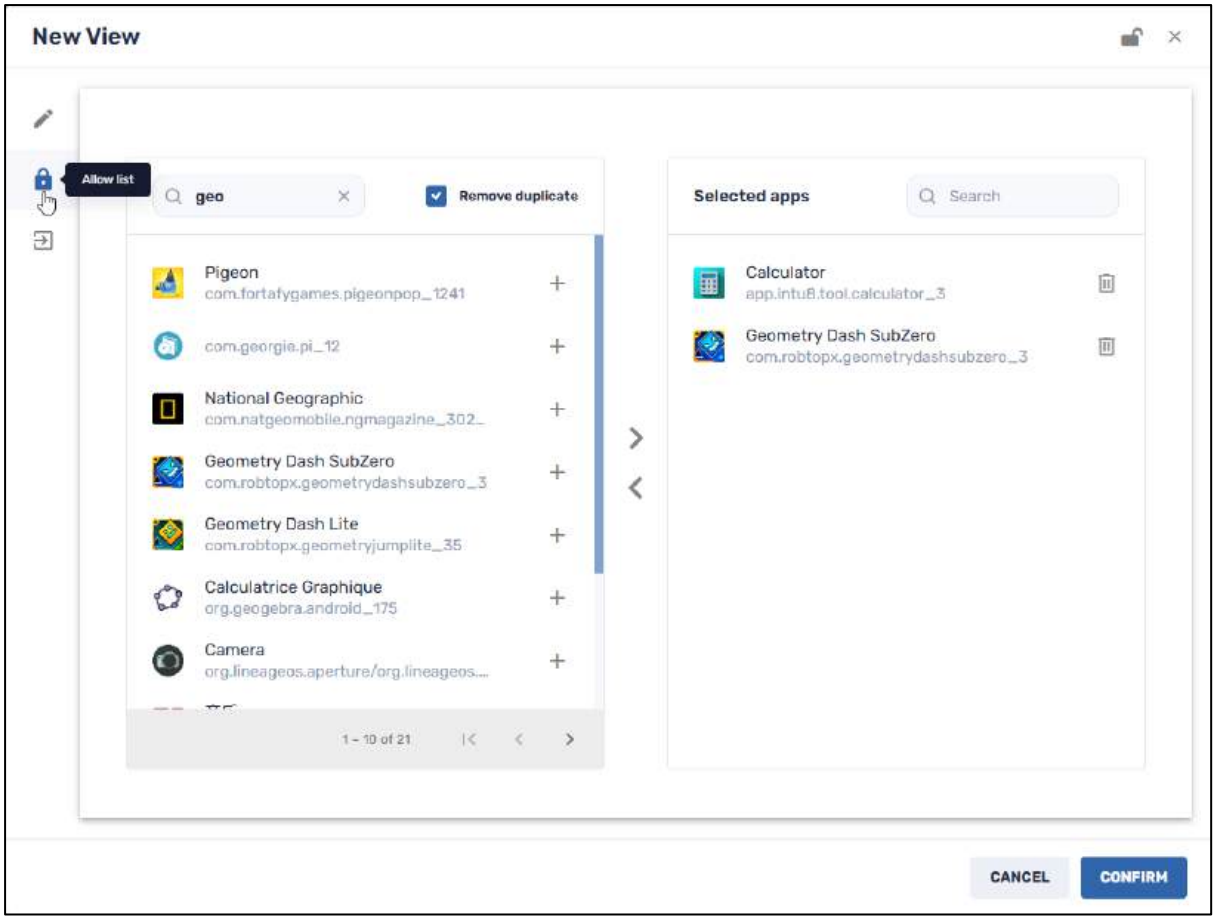
1. Click on the **Add New** button at the lower left corner of the "**Views**" screen. The "New View" screen opens.



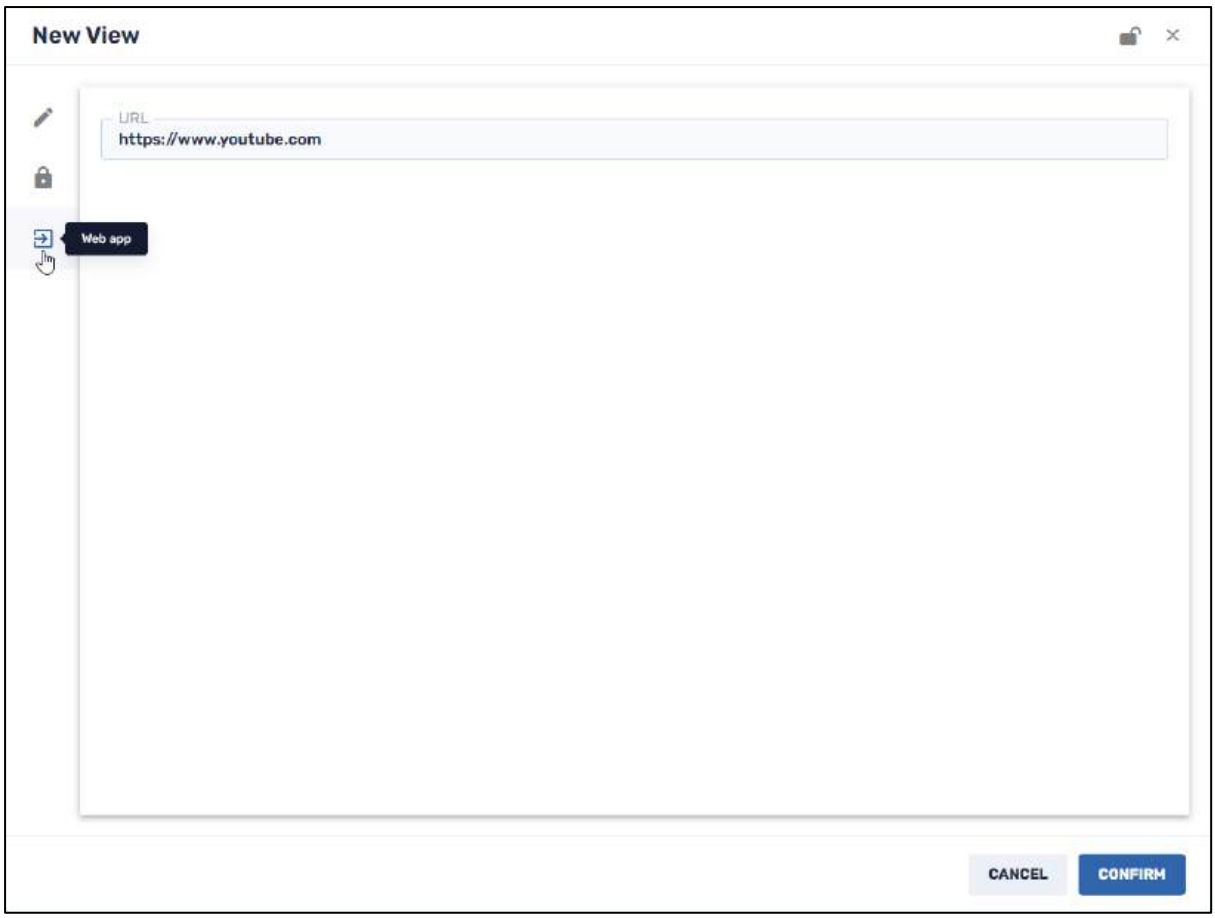
2. Assign a name and description to the new **View** option.



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 Manager.
4. 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 .
5. Click on the **Allow list** icon and select the apps that you would like to allow on the remote device.



6. Click on the **Web app** icon and provide a Web app URL in the textbox.



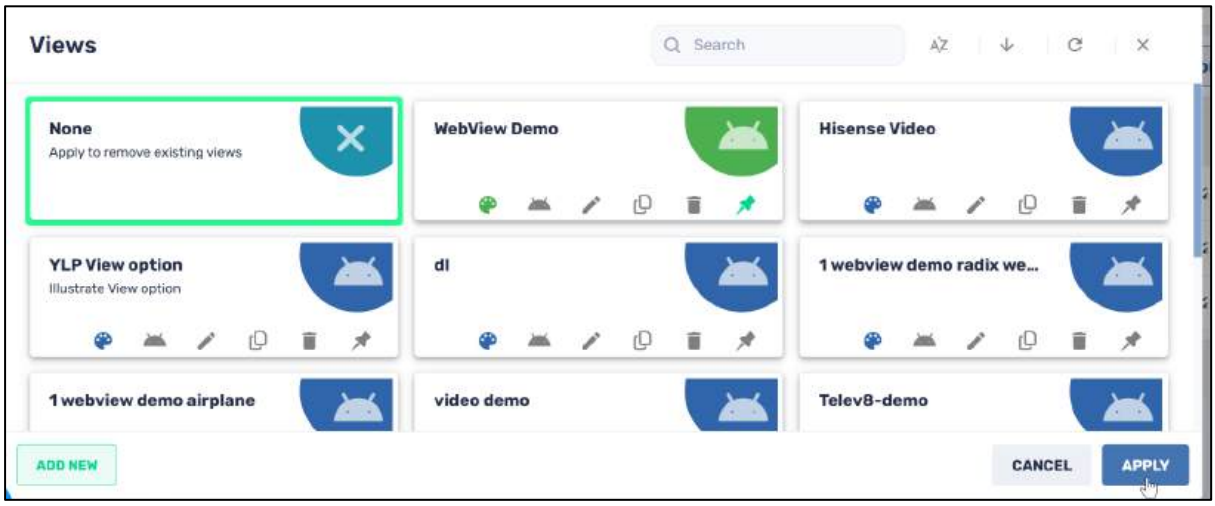
7. Click **Confirm**. The new **View** option will now appear in the Views Repository.

4.2.1.23.3 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 Manager.

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.

4.2.1.24 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:

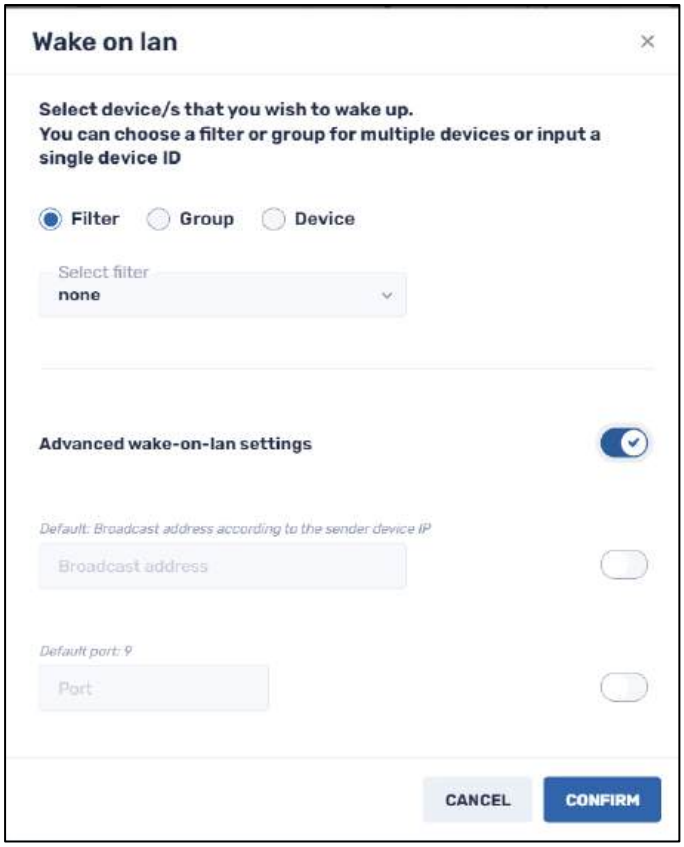


Figure 4-43: Wake-on-LAN window

You have the following options:

- **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 Device Console:

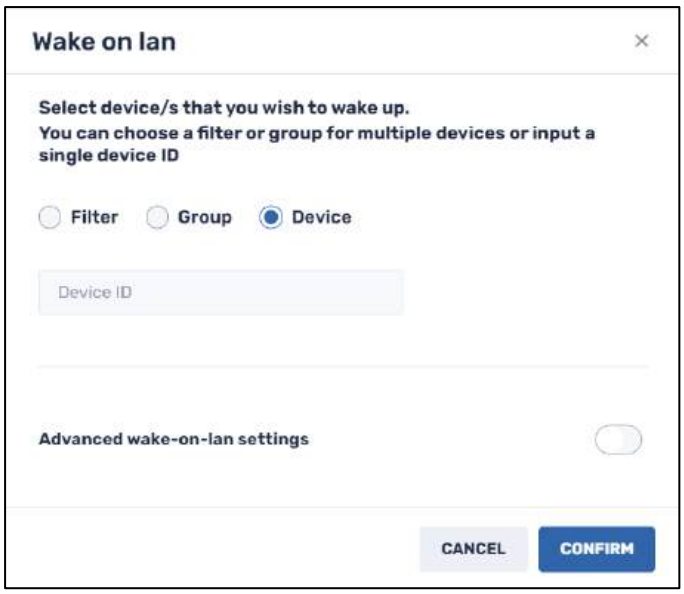


Figure 4-44:Wake-on-LAN option to turn on a single device

- **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.

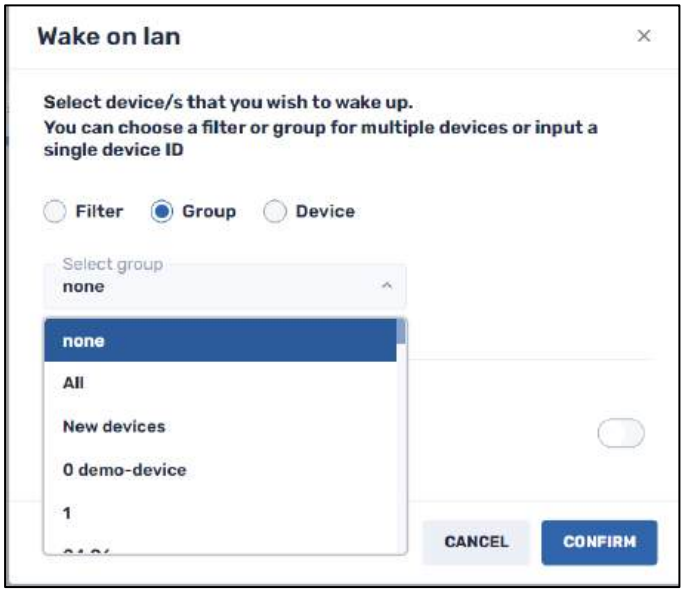
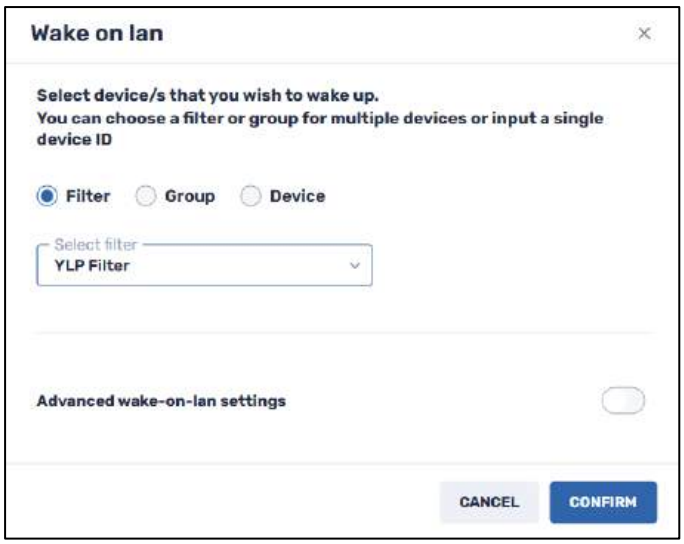


Figure 4-45: Wake-on-LAN option to turn on a group of devices

- **By using a filter**: With this option, you can turn on a group of devices based on a predetermined search filter. You can use existing filter options, or create a new filter, as mentioned in **Section 4.3.1.2**.



4.2.1.25 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.

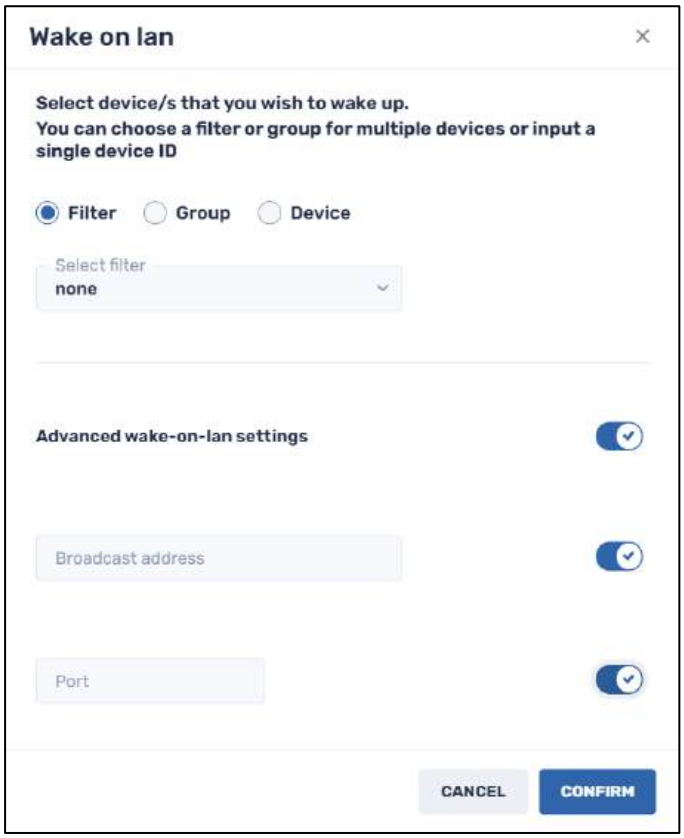


Figure 4-46: Advanced Wake-on-LAN fields

4.2.2 iOS/Apple Commands

4.2.2.1 Apple Custom Command

This option allows you to execute a plist (=property list) file on a MacOS device.

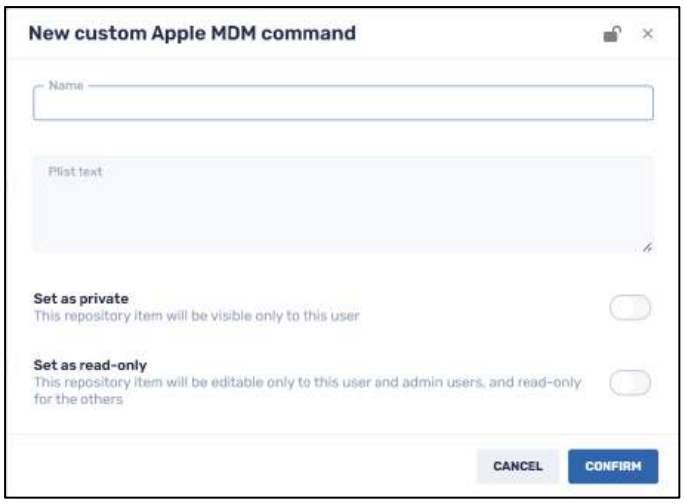
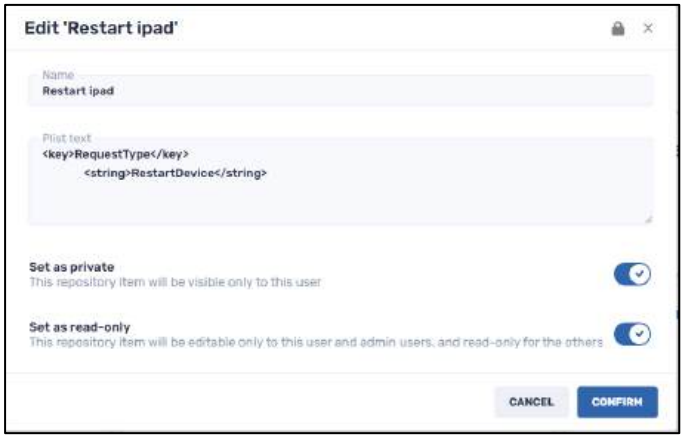


Figure 4-47: Apple Custom Command window

Here is an example of an Apple custom command:



To use the Apple Custom Command option:

1. Supply a name for the custom command.
2. Enter the text of the command in the Plist text box.
3. Click on the **Set as private** button if you want this new Apple custom command option to be visible only to you (as the creator of the item) when you log in to the Radix Device Manager.
4. Click on the **Set as read-only** button if you want to restrict who will be able to modify the details of this Apple custom 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 .

4.2.2.2 DEP Apple profile

This allows you to set up a Device Enrollment Program (=DEP) for an Apple device.

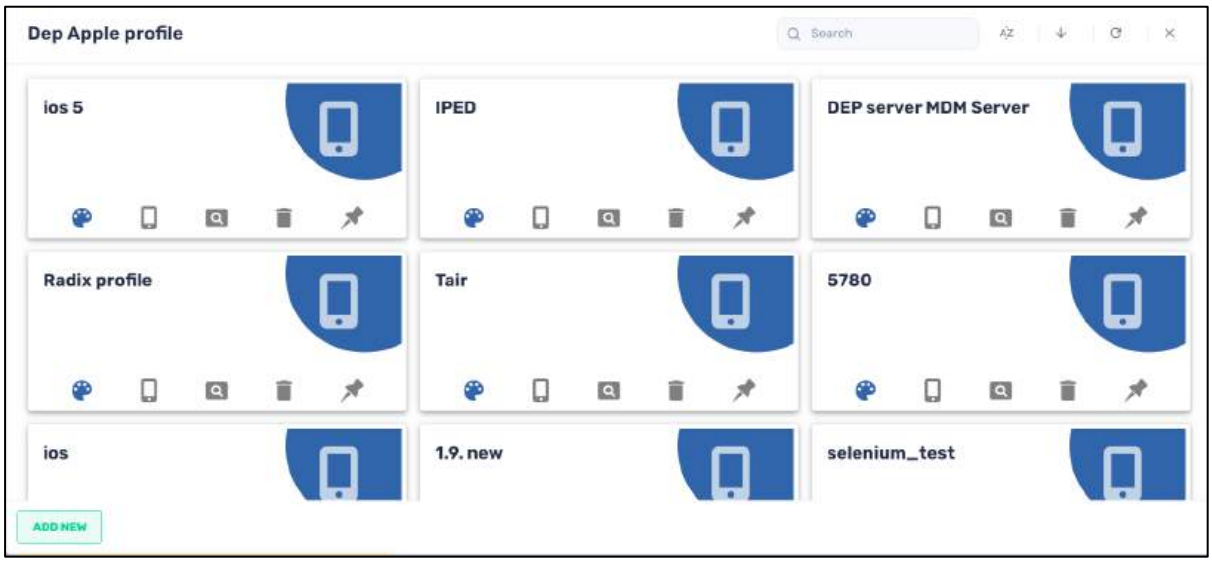
To apply an existing DEP profile:

1. Click on **More Actions** in the Devices Console Ribbon.
2. Select **DEP Apple profile**.

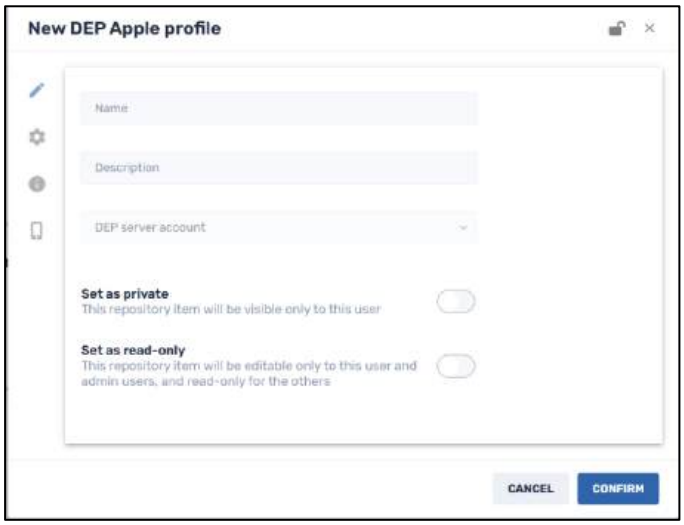
3. Select one of the profiles that appear and click **Apply**.

To create a new DEP Apple profile:

1. Go to the Repositories Console and click on **Dep Apple Profile**, or
2. Click **More Actions** in the Device Control Ribbon and click on **Dep Apple Profile**. The Dep Apple Profile Window opens.



3. Click on **Add New**. The **New DEP Apple Profile** window appears.

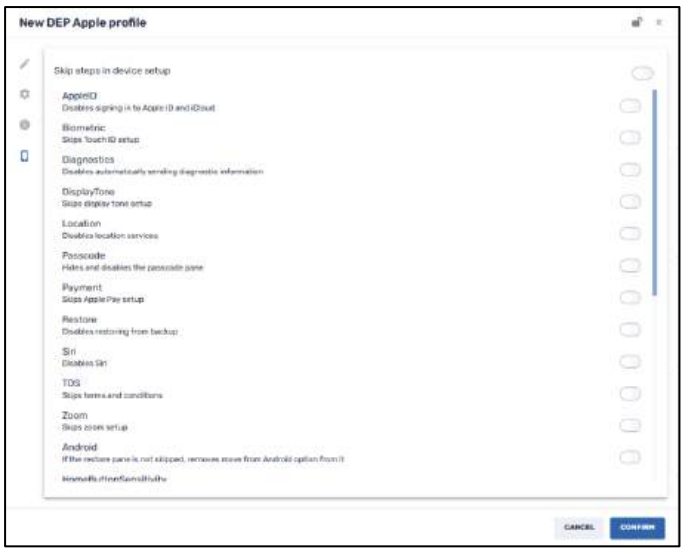


4. In the **Edit Details** pane (accessed from clicking on the **Edit** icon), add Name, Description, and DEP Server Account details.
5. Click on the **Set as private** button if you want this new DEP Apple profile option to be visible only to you (as the creator of the item) when you log in to the Radix Device Manager.
6. Click on the **Set as read-only** button if you want to restrict who will be able to modify the details of this DEP Apple profile. 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 **General** icon and provide the Apple device details.

8. Click on the **Support info** icon and provide the requested information, such as a support phone number and email.

9. Click on the **Setup Assistant** icon and select the Apple services that you would like to enable on your device.

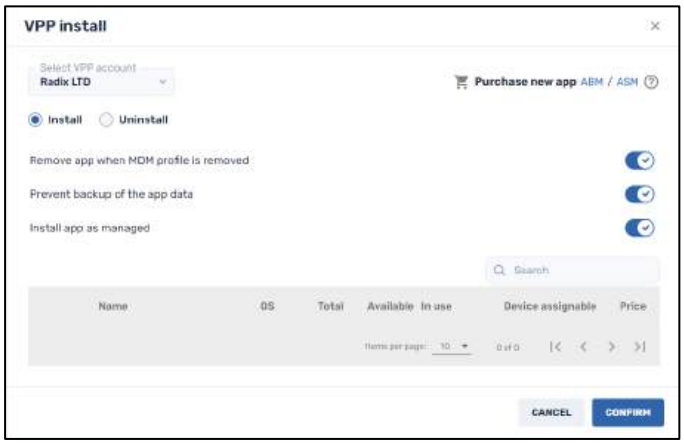


10. Click **Confirm**. The new DEP Apple profile will be saved.

4.2.2.3 VPP Install/Uninstall

This allows you to install or uninstall an Apple app via the Apple Volume Purchase Program (=VPP).

The **VPP Install/Uninstall packages** feature can be accessed by the Devices Console Ribbon, under **More actions**.



4.2.3 Windows Commands

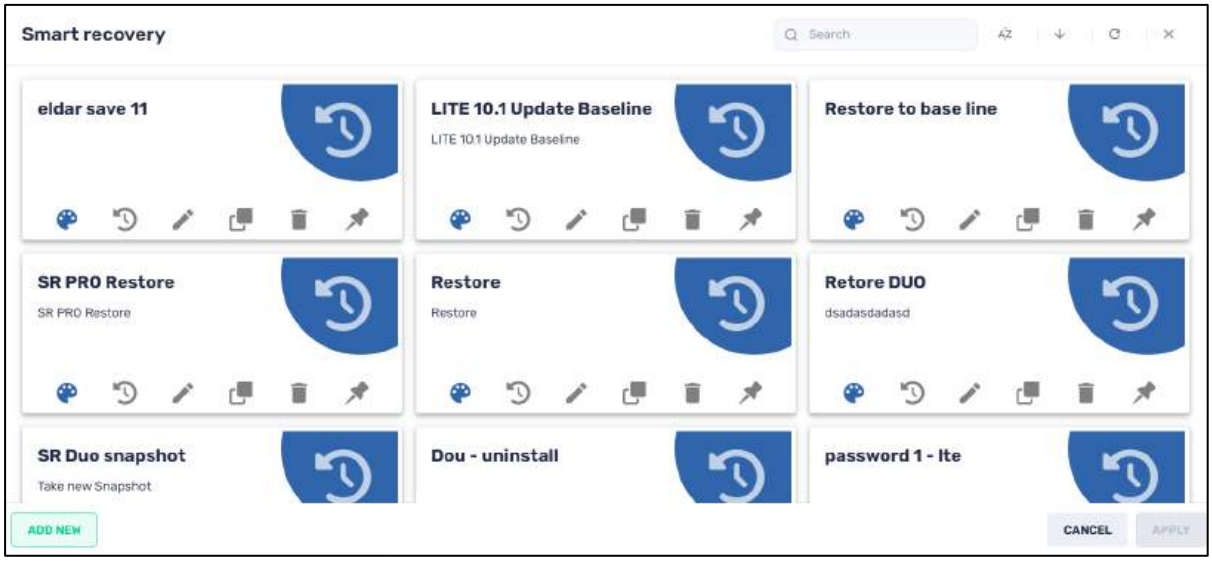
4.2.3.1 Export Blue Screen Data

If you are managing a Windows device, this option sends information about a system crash in Windows. The data comes in the form of an Excel spreadsheet, listing the Device ID, details of the blue screen error, and when the blue screen appeared.

4.2.3.2 Smart Recovery

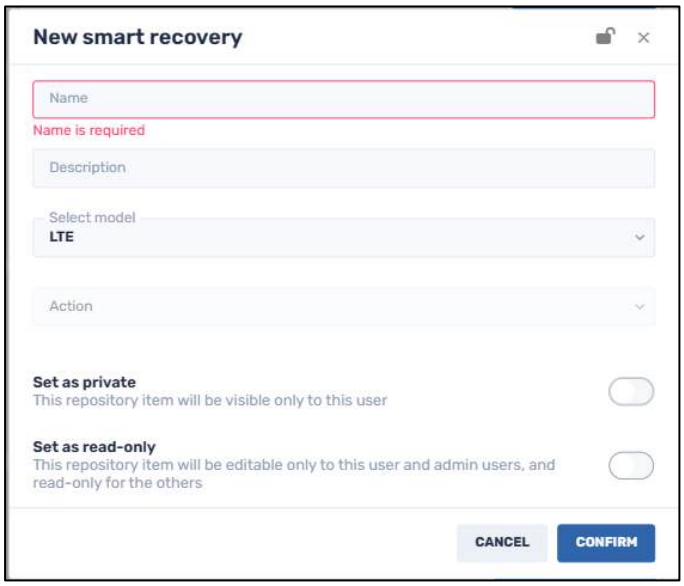
Smart Recovery is an application that allows you to implement settings to repair a Windows device that has crashed. Options include restoring a device's system configuration and settings to the latest system snapshot, or factory settings. You can access this command from the Devices Console Ribbon, under **More actions**.

When you click on the **Smart Recovery** option in the device's three-dot menu, 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.



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:

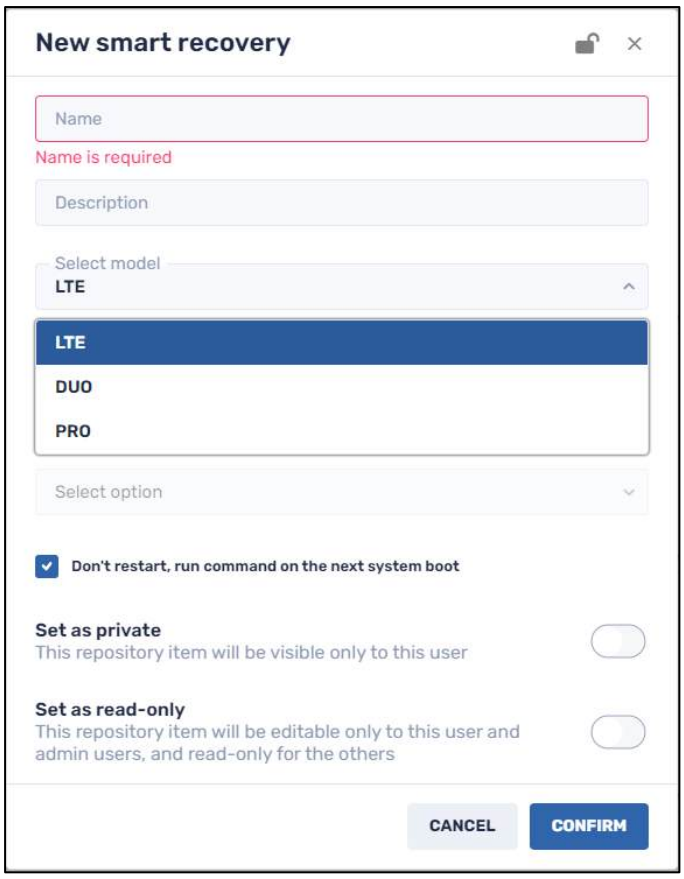


Figure 4-48: Smart Recovery options to be applied to a remote device

- **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.

  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.
- **Smart Recovery PRO**: This version of Smart Recovery allows you to restore your computer to
  - A **fixed baseline state**,
  - A **dynamic restore point** that you have saved as a snapshot of the system, or
  - The **current snapshot**.

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.

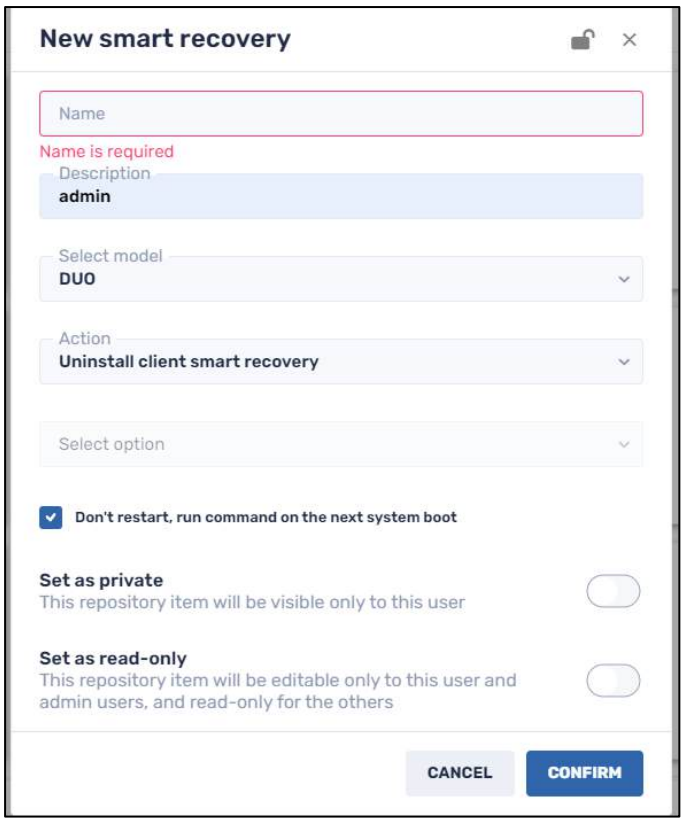


Figure 4-49: Illustration of "Don't restart" checkbox

6. 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.
7. **For Smart Recovery Pro**: Click on the **Lock Snapshot** checkbox to lock the snapshot taken of the Windows device.

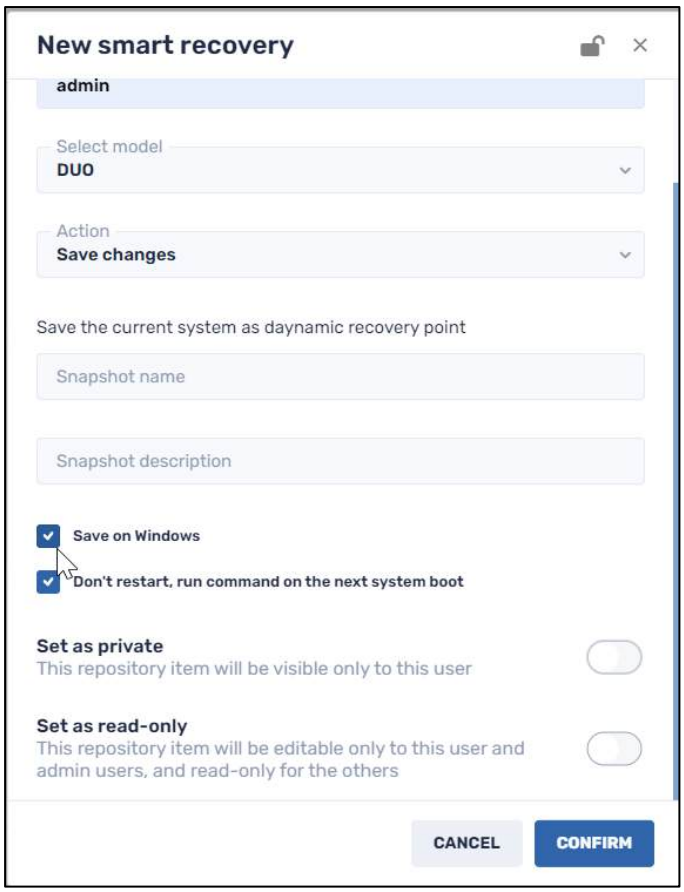


Figure 4-50: Illustration of Save on Windows checkbox on Smart Recovery DUO

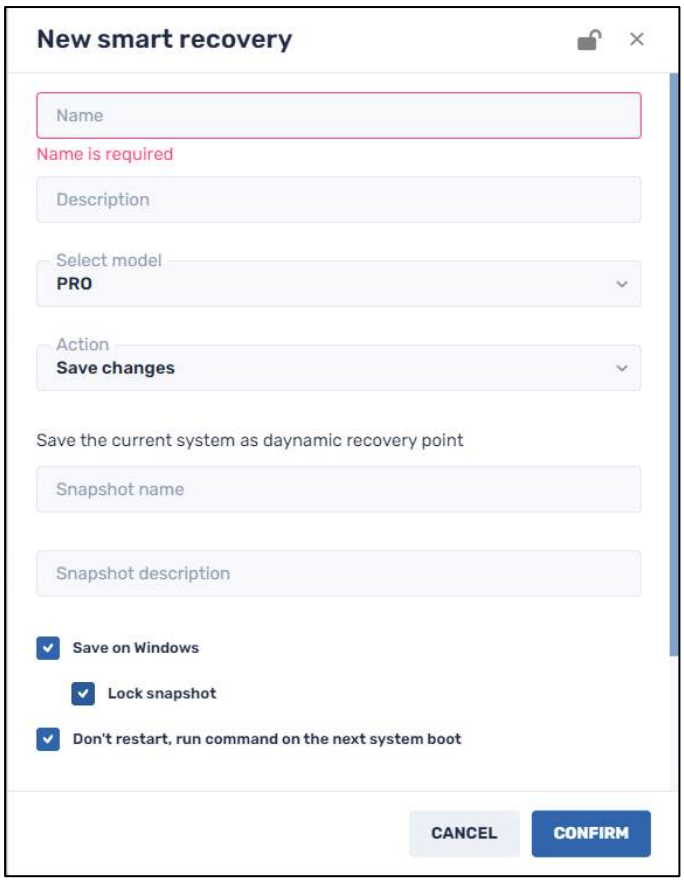


Figure 4-51: Illustration of Save on Windows checkbox on Smart Recovery Pro

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 Manager.
9. 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 .
10. Click **Confirm**. The Smart Recovery method will be saved.
11. To implement a Smart Recovery method, select it from the list, and click **Apply**.

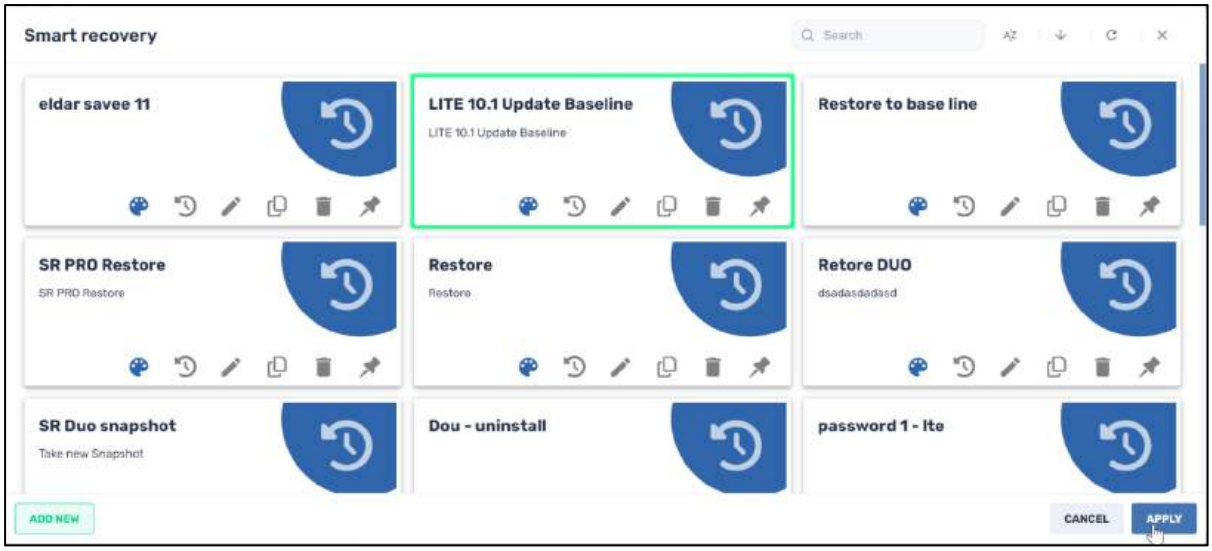


Figure 4-52: The Smart Recovery option "LITE 10.1 Update Baseline" has been selected

4.2.4 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.

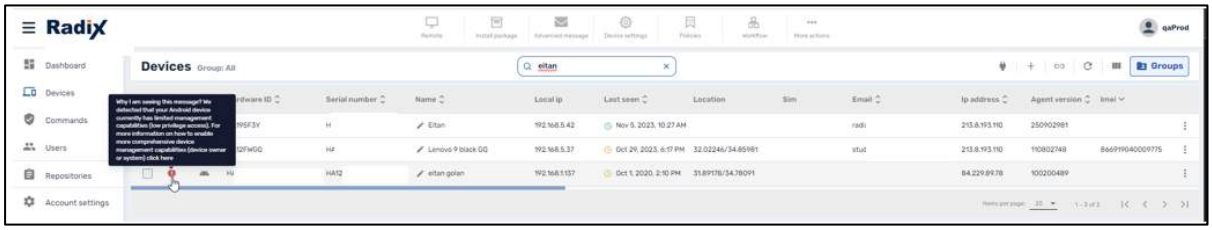


Figure 4-53: Warning icon next to device in Device Console

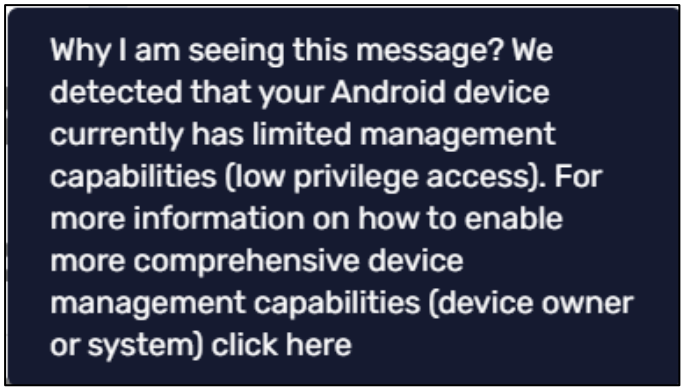


Figure 4-54: Text of Warning Message

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.

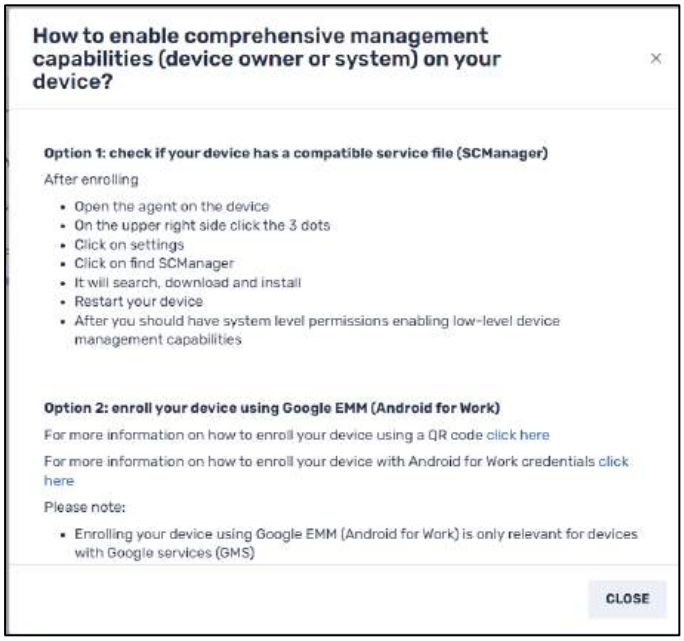
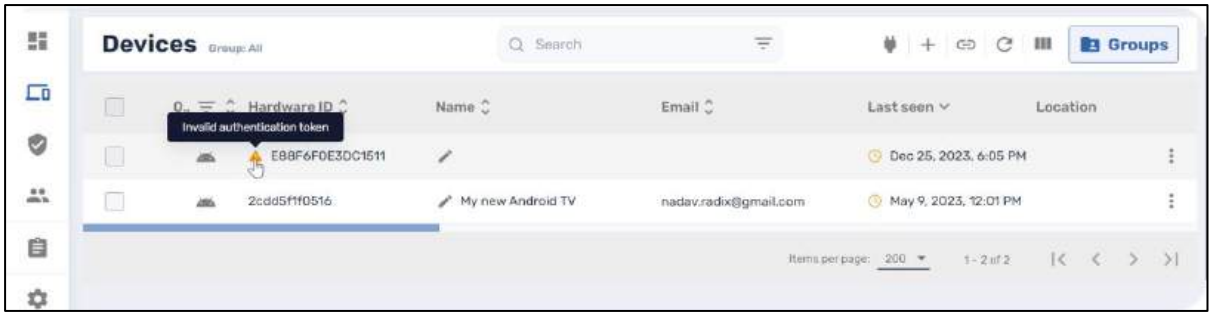


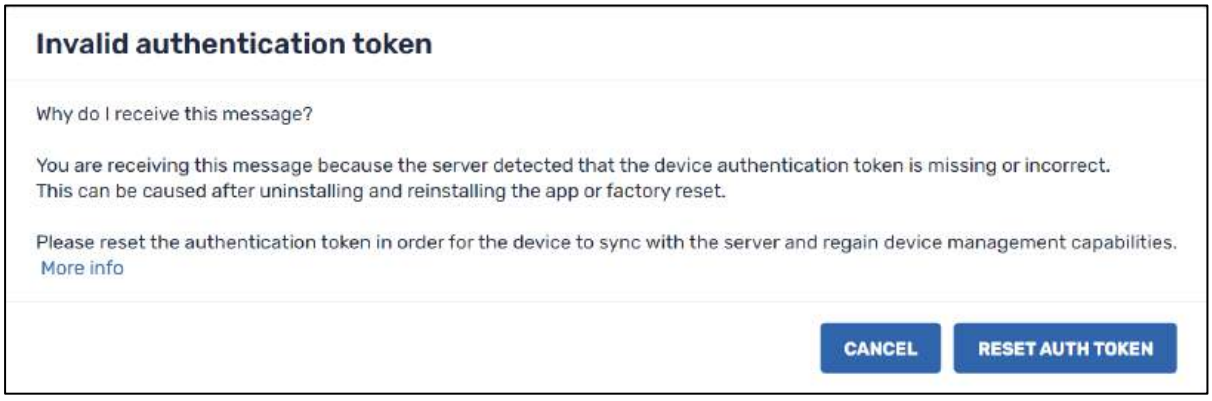
Figure 4-55: Instructions to re-enroll a device

4.2.4.1 Invalid Authentication Token Warning

Another warning icon that you may encounter in the Device Console 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.

4.3 Search Bar Ribbon

At the top of the Devices panel, underneath the Devices Console Ribbon, you will see a search bar, with additional commands:

Figure 4-56: Search Bar Ribbon Commands

Table 4-12: Explanation of Search Bar Icons

Icon	Description
	Search Bar: The Filter icon allows you to add conditions to the search.
	**Who is online?**: Allows you to see which devices are currently online.
	**Enroll**: Allows you to enroll additional devices, according to operating system: Android, Windows, MacOS/iOS, Chrome.
	**Ad-hoc:** Allows you to add a device for a one-time, ad-hoc remote session using the Radix Device Management system.
	**Android for Work:** This allows you to add apps to an Android device, once you have installed Android for Work (as detailed in **Section 10.5, Android for Work**)
	**Refresh:** Refreshes the devices displayed after any changes.
	**Columns**: Allows you to select which data columns to display.
	**Groups option**: Allows you to group users, or search for existing groups.

We will go through these options briefly:

4.3.1 Search Bar

In the Search Bar, you can search for a particular device, according to the Hardware ID, the Device Name, email address, assigned tags, or practically any of the criteria presently displayed.

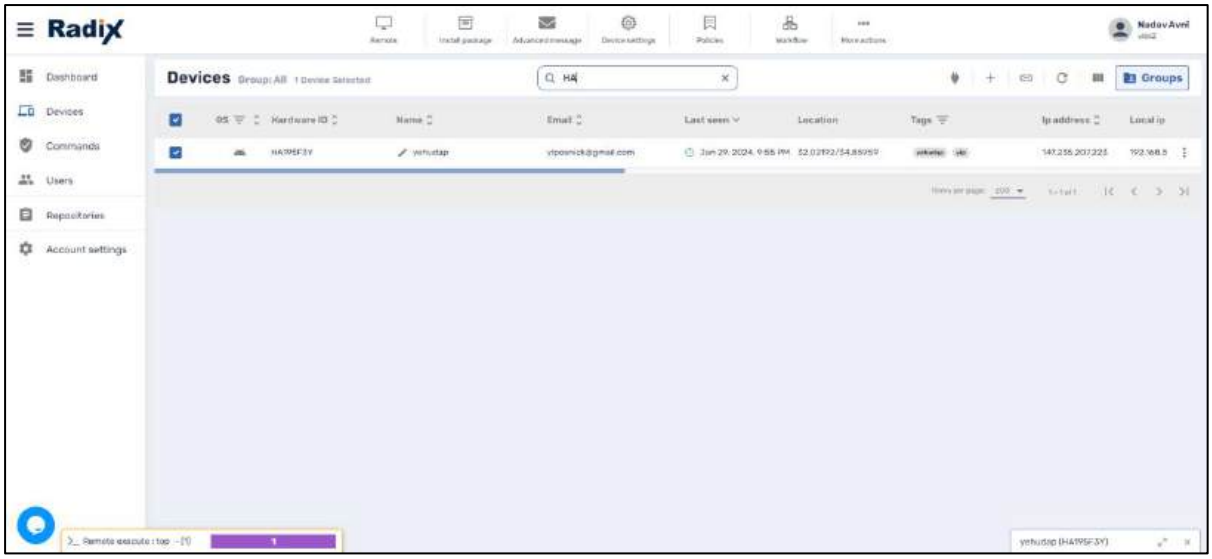


Figure 4-57: Searching for Device by Hardware ID

Note: The Search bar in the Devices Console is **not** case-sensitive. Therefore, you will get the same search results whether you type “HA1” or “ha1”.

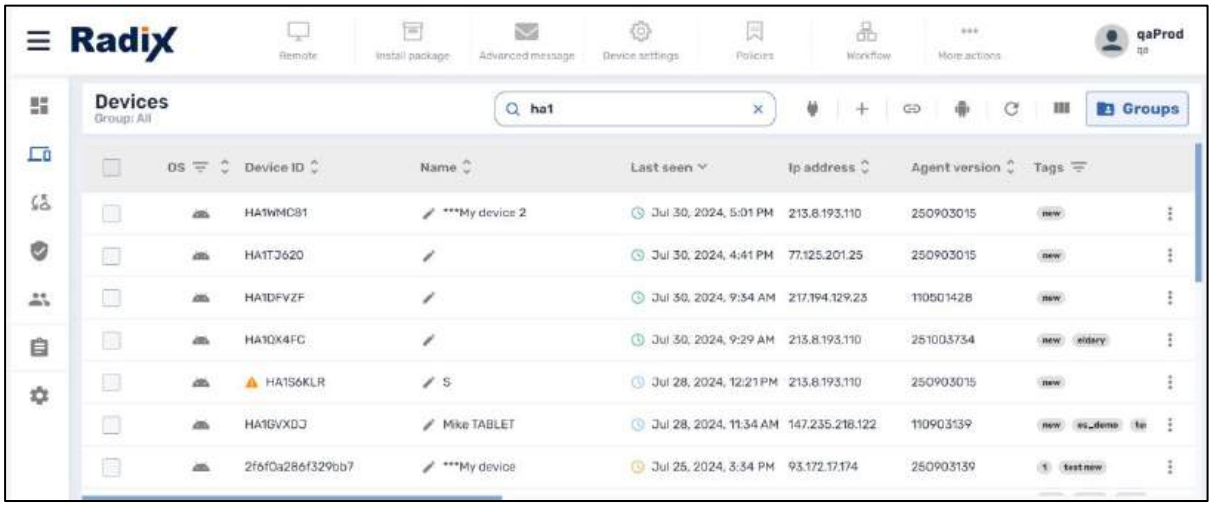


Figure 4-58: Searching for devices with the string "HA1" in the Device ID. "ha1" will yield the same results

4.3.1.1 Filtering the Search Results

When you click on the Filter icon, a window opens which allows you to provide conditions for your search.

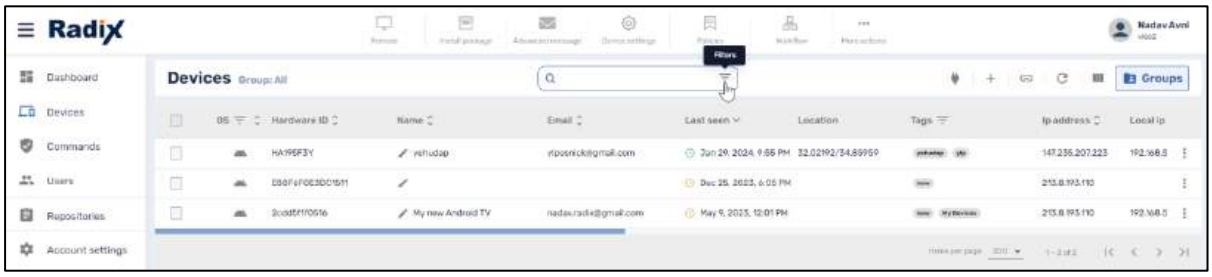


Figure 4-59: Filter option

These conditions will further narrow down the devices or users displayed on the screen (but will not apply to the entire population of devices):

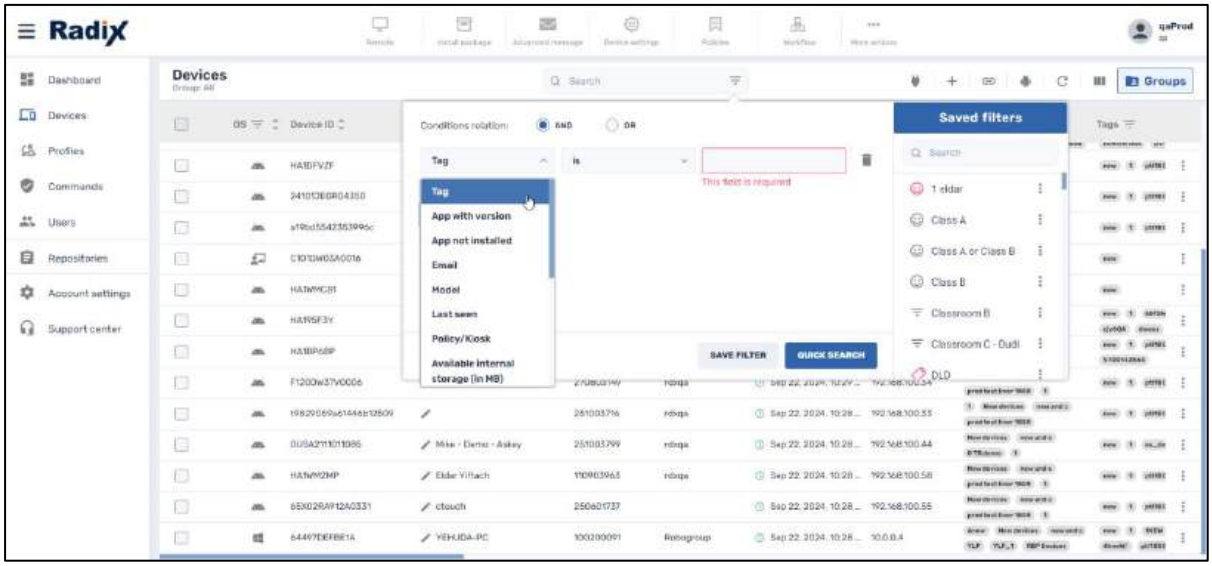


Figure 4-60: Filter pop-up window

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 Manager.
- **Public IP**: Will filter devices by their IP address
- **OS**: Will filter devices by their operating system (Android, Windows, ChromeOS, iOS, MacOS)
- **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 "Undo" icon (("Show all devices") next to **Filtered results: Quick Search** at the top of the search results.

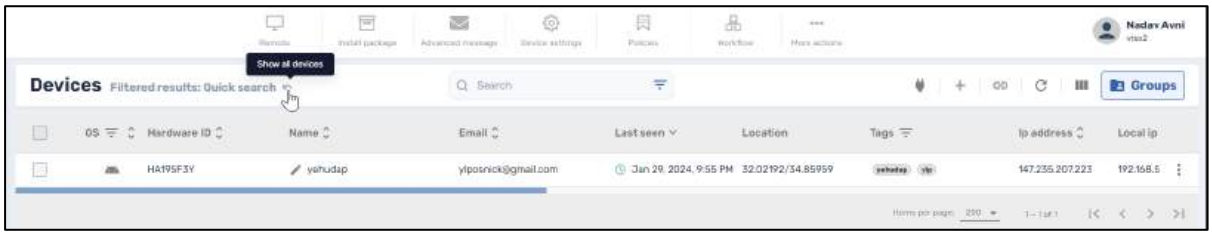
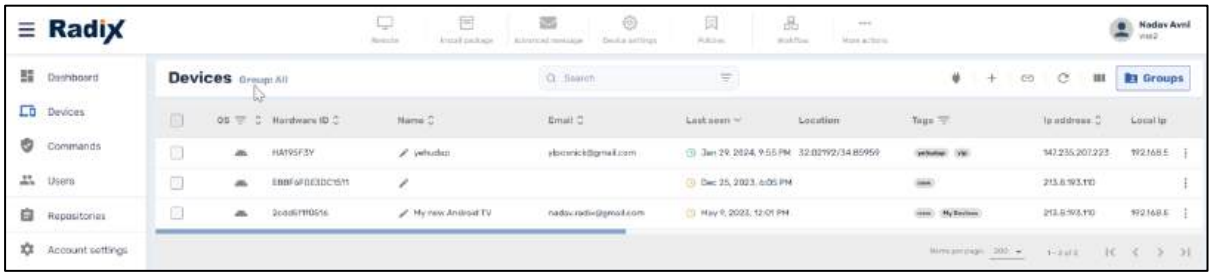


Figure 4-61: Undoing a Search Filter

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



4.3.1.2 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.

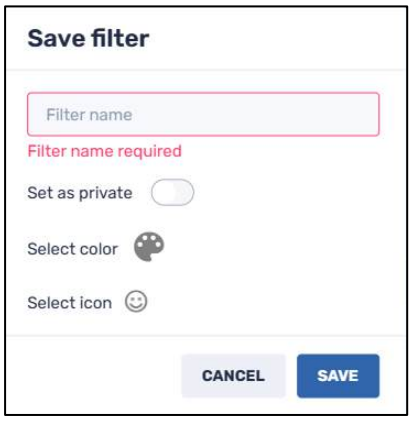
To create a new filter:

1. Click on the **Filter** icon in the Search bar. The **Filter Options** window opens.

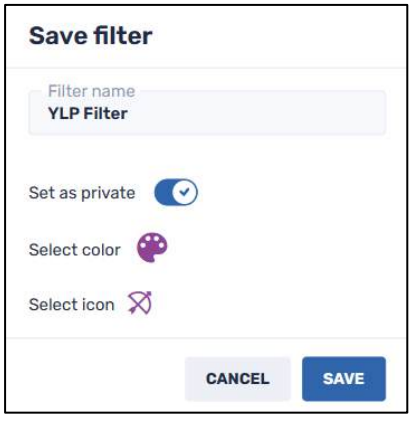
Figure 4-62: Filter Options window

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

3. Click **Save Filter** to save the search conditions. A **Save Filter** window pops up, prompting you to supply a name for the filter.
4. 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.



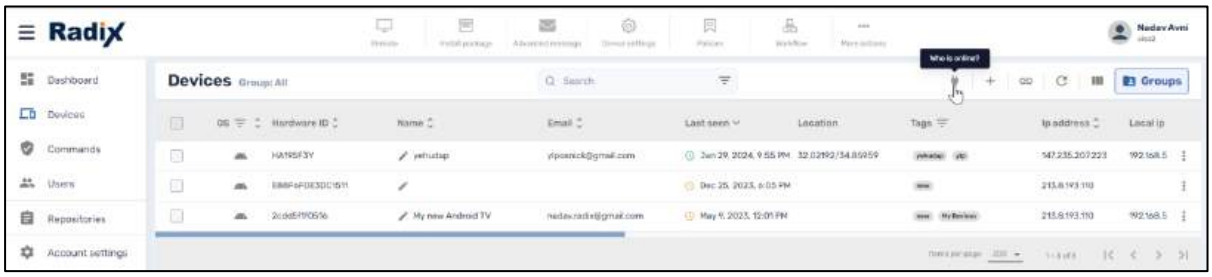
5. Supply a name, color, and icon for your new filter, and click **Save**.



6. Enter the filter name in the Search bar under Saved Filters. The new filter will appear in the search.

4.3.2 Who is Online?

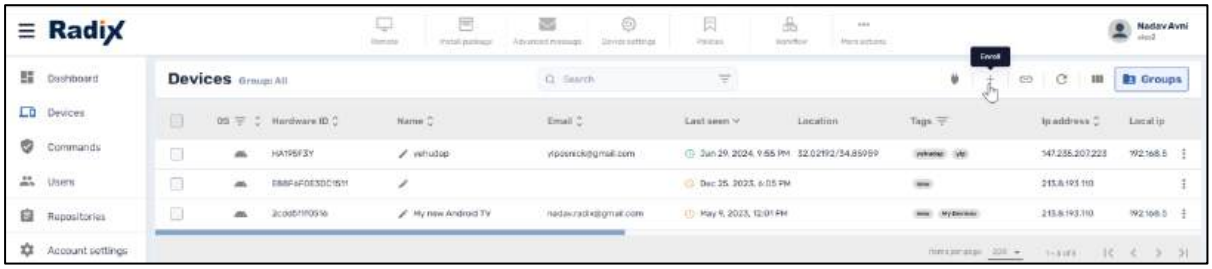
Clicking the “Who is Online” icon will list all the devices and users presently online.



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

4.3.3 Enroll

Clicking on the **Enroll** icon + will open a dialog box where you can enroll additional devices, according to their operating system: Android, Windows, Apple, or ChromeOS.



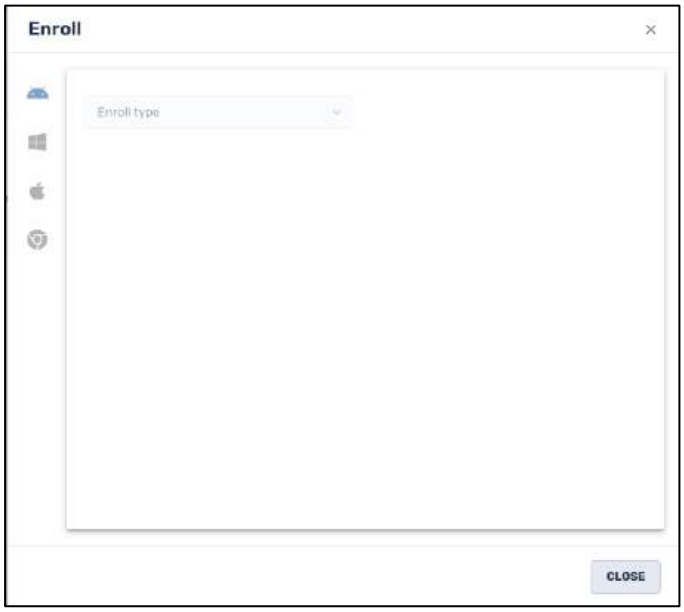


Figure 4-63: Dialog box to enroll Android, Windows, Apple, or ChromeOS devices

We will go through the options in turn.

4.3.3.1 Enrolling Android Devices

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

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

4.3.3.1.1 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.

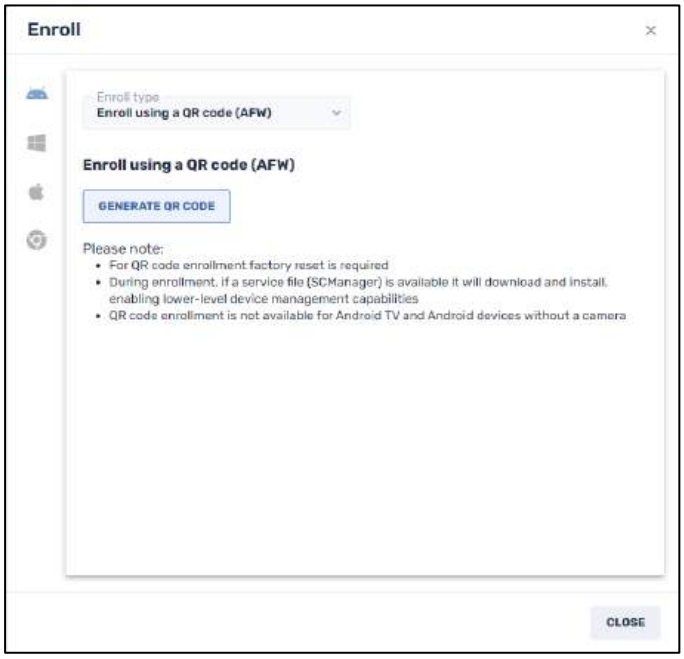


Figure 4-64: Steps for enrolling an Android device via a QR code

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.

4.3.3.1.2 Download Android Agent Option

When you click on this option, you receive two methods of downloading the Viso Android Agent:

- Download the APK file directly to your computer, or
- Go to the Google Play Store and download the APK from there.

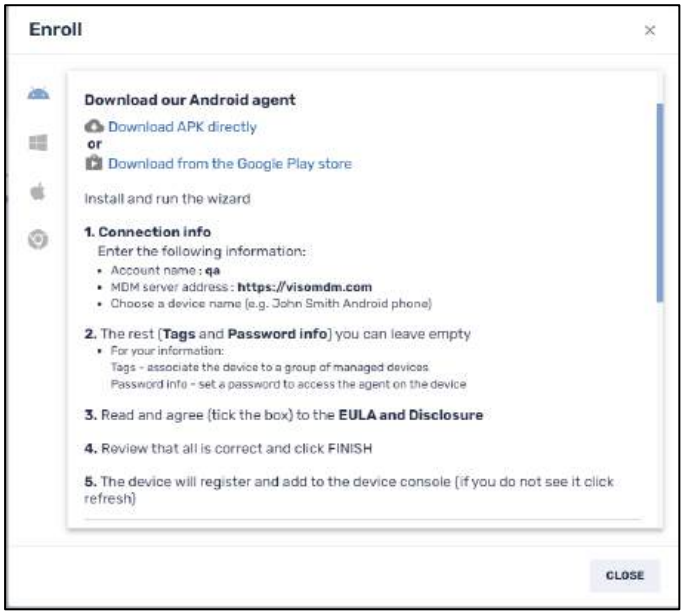


Figure 4-65: Steps for enrolling an Android device via an APK file

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.

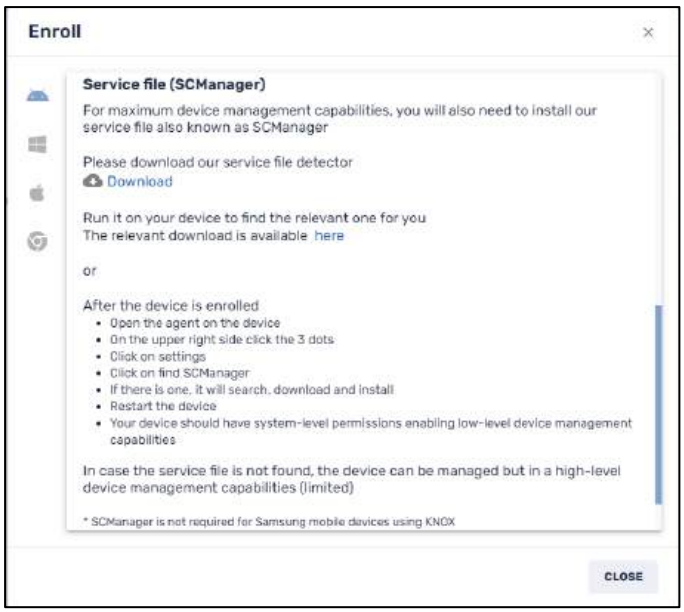


Figure 4-66: Steps to install the SCManager

4.3.3.1.3 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:

- Step-by-step written instructions to enroll an Android device in the Android for Work option.
- A video that illustrates the steps.

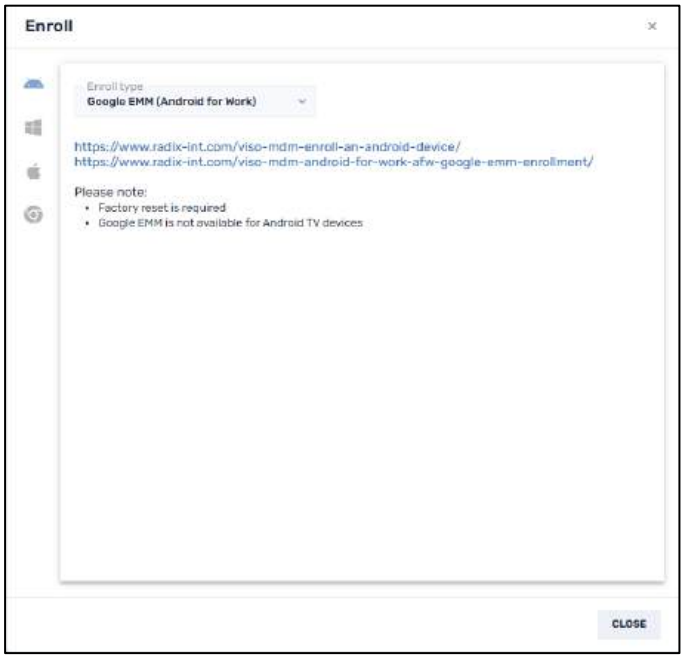


Figure 4-67: Steps to enroll an Android device via the EMM Android for Work software

4.3.3.2 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.

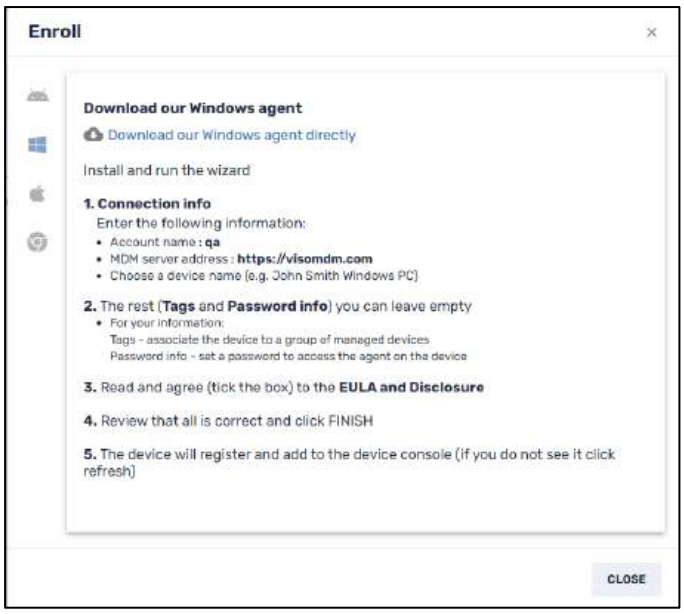
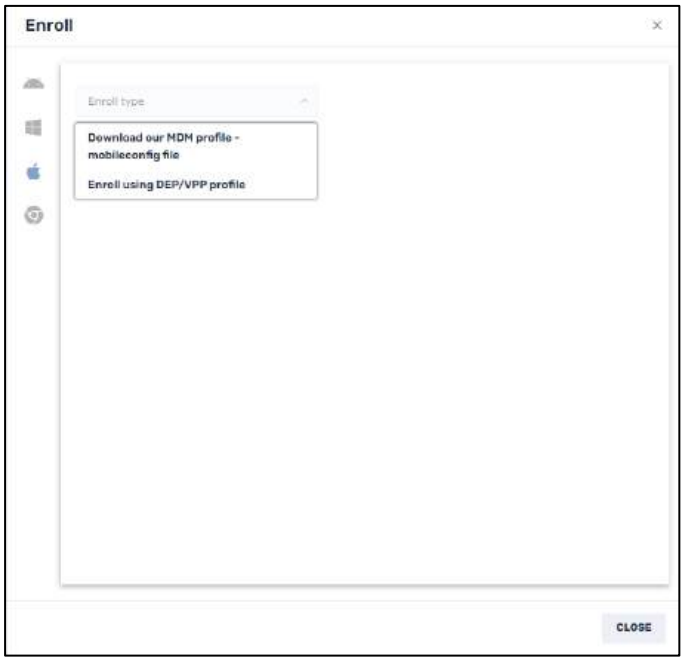


Figure 4-68: Steps to enroll a Windows device

4.3.3.3 Enrolling Apple Devices

There are two options that you are offered in the Radix Device Manager to enroll an Apple device:



4.3.3.3.1 Downloading the MDM Profile File

This option will download a configuration file for your Apple device. Download the file and follow the on-screen directions to send it to your Apple device and install it.

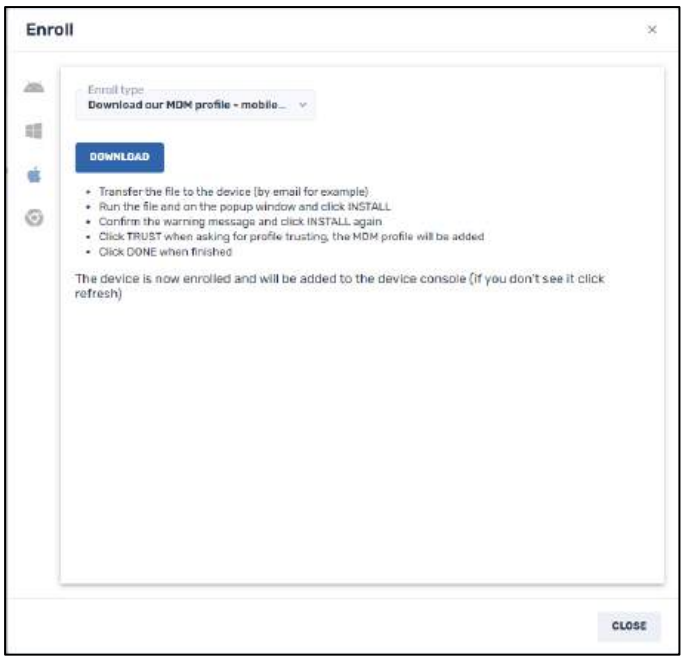


Figure 4-69: Steps to enroll an Apple device using a mobileconfig file

4.3.3.3.2 Enrolling using the DEP/VPP Profile

This option will provide you with access to a link where you can download the necessary documentation to pair an Apple device with the Radix Device Manager.

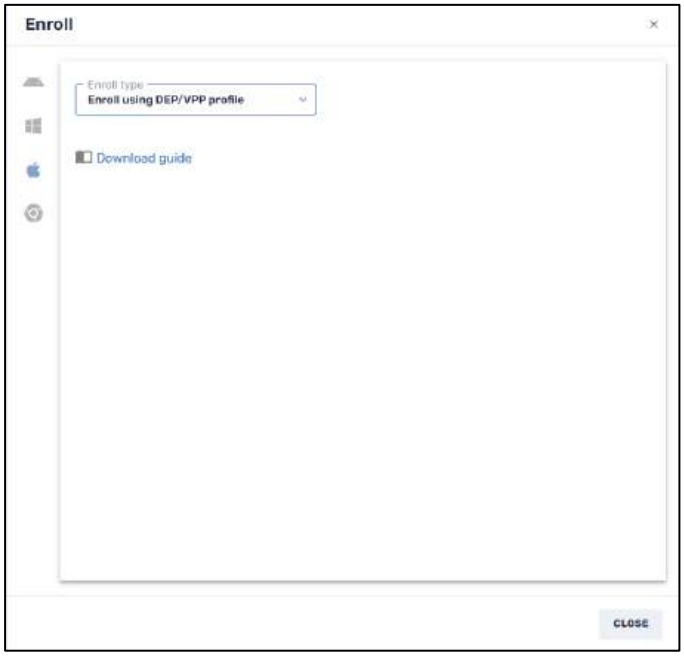


Figure 4-70: Enrolling an Apple device via a DEP/VPP profile

4.3.3.4 Enrolling Chrome Devices

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

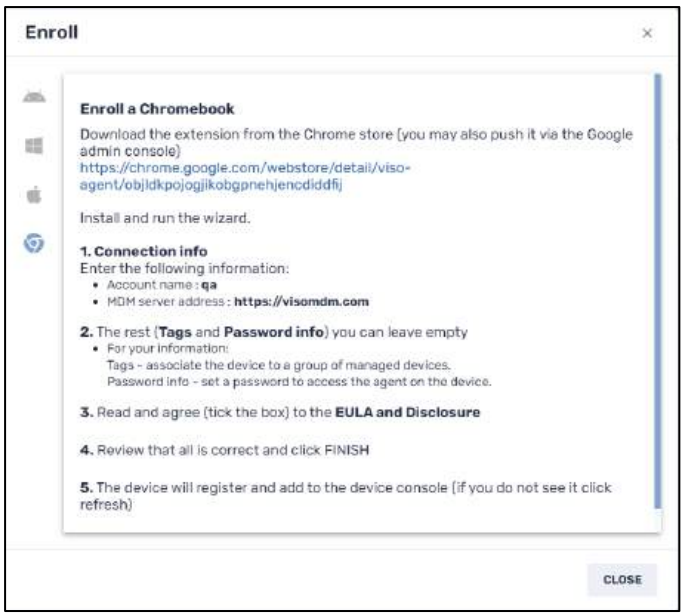
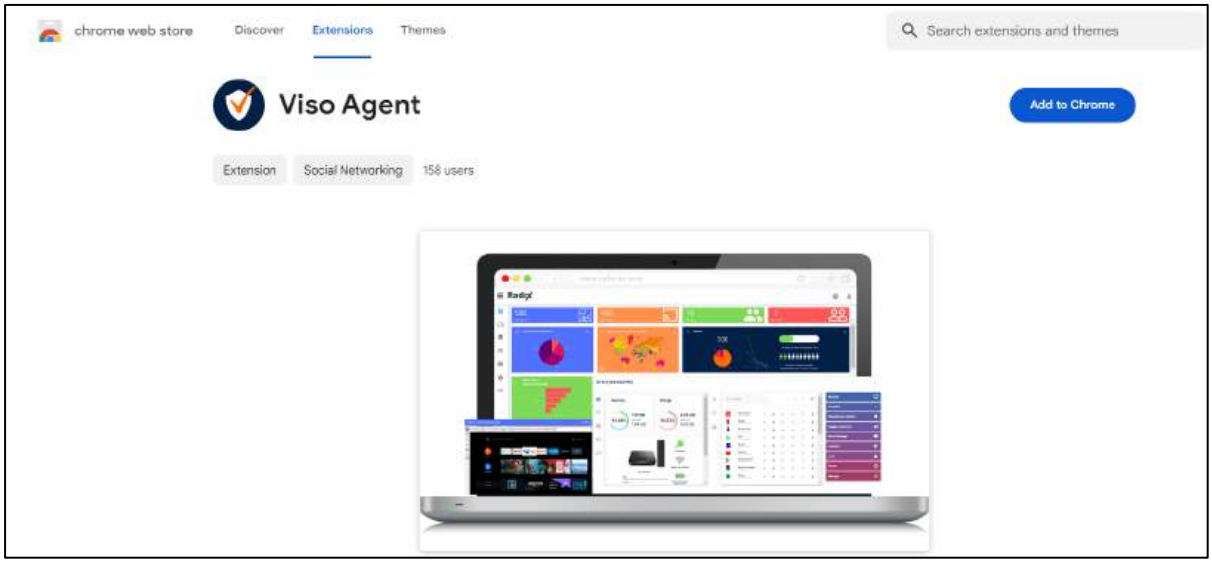
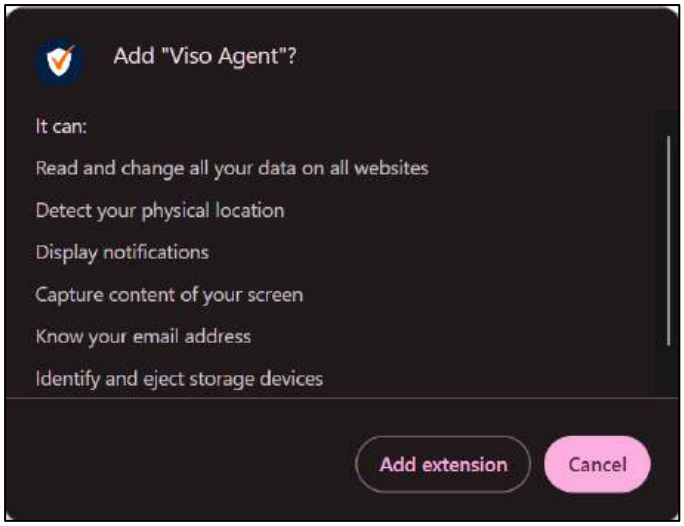


Figure 4-71: Steps to install the Viso Chrome browser extension

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



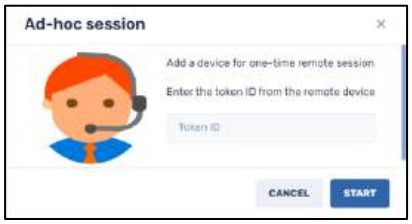
2. Click **Add to Chrome**. You will be prompted to add the Viso Agent to your Chrome extensions.



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

4.3.4 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 Manager 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”.

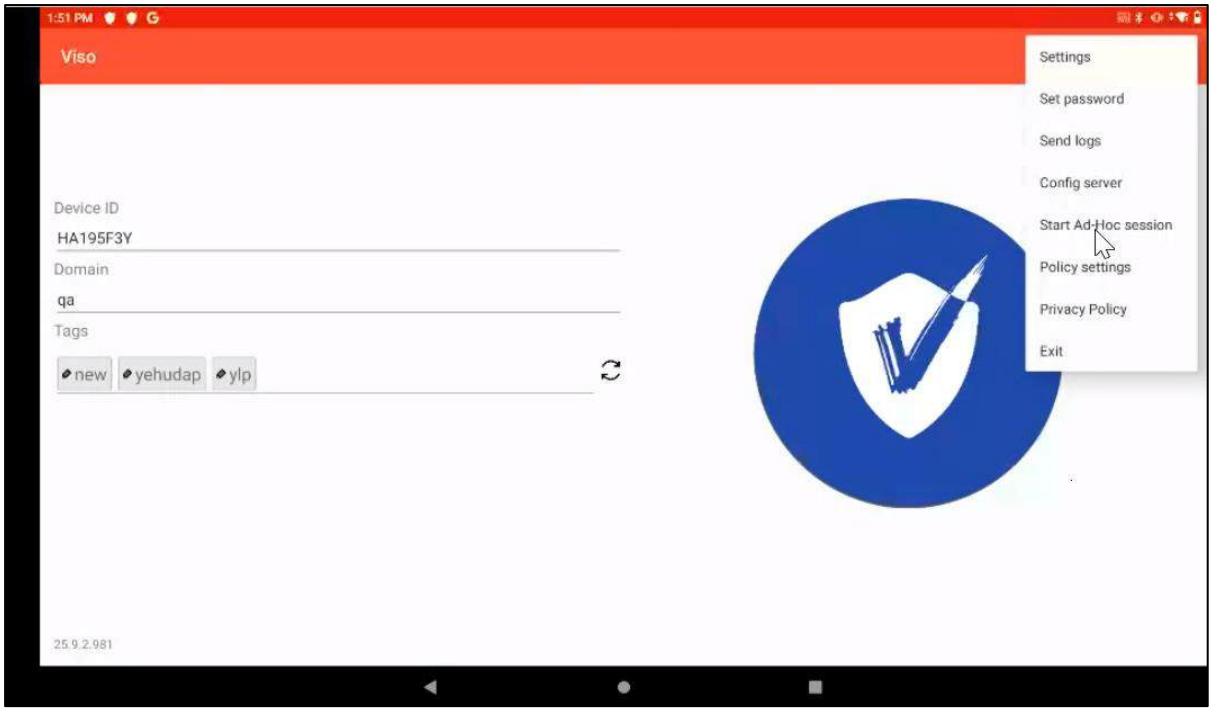


Figure 4-72: Start Ad-Hoc session option on the remote device

3. When the remote user taps on **Start Ad-hoc session**, a window will open on their device, supplying the token ID.

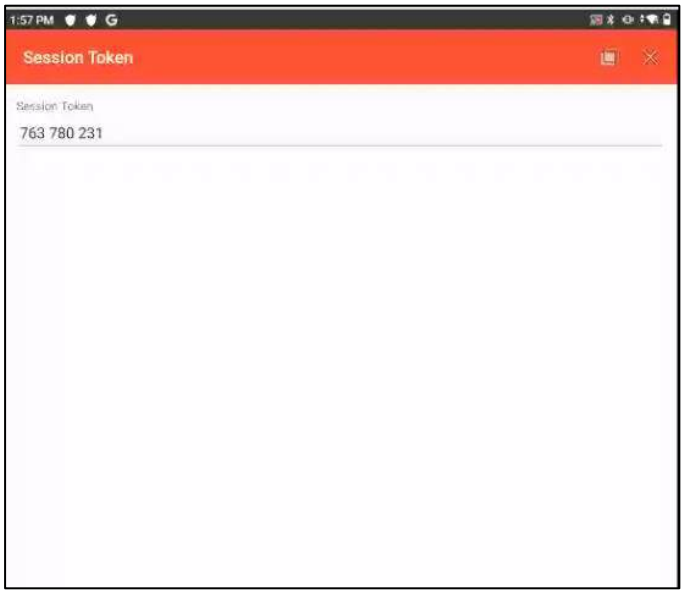


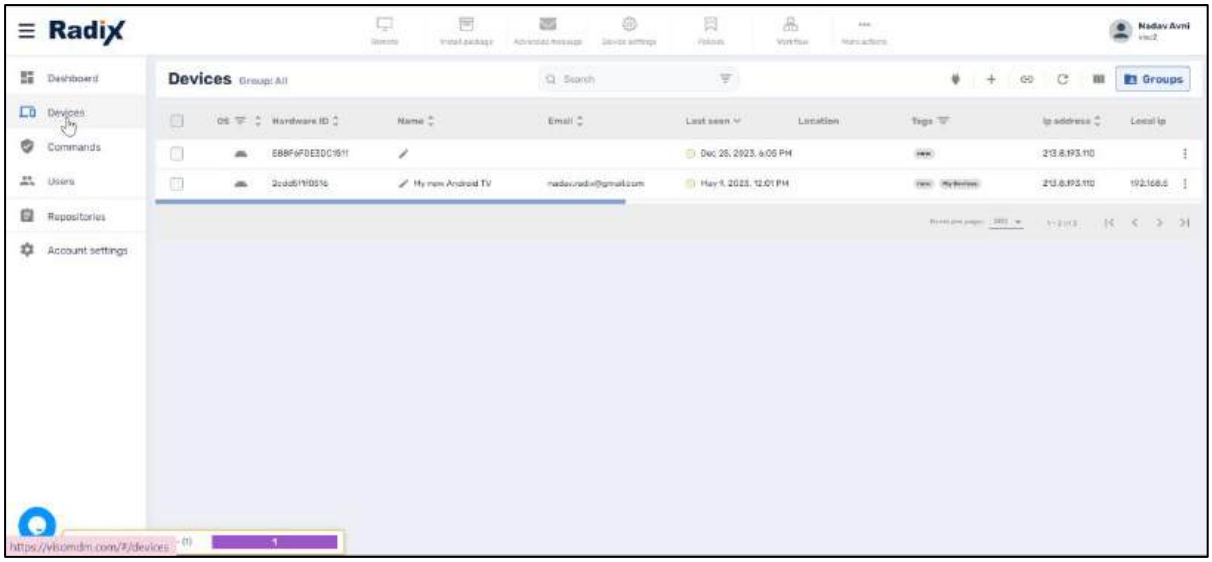
Figure 4-73: Session Token window, as it appears on the remote device

4. 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.

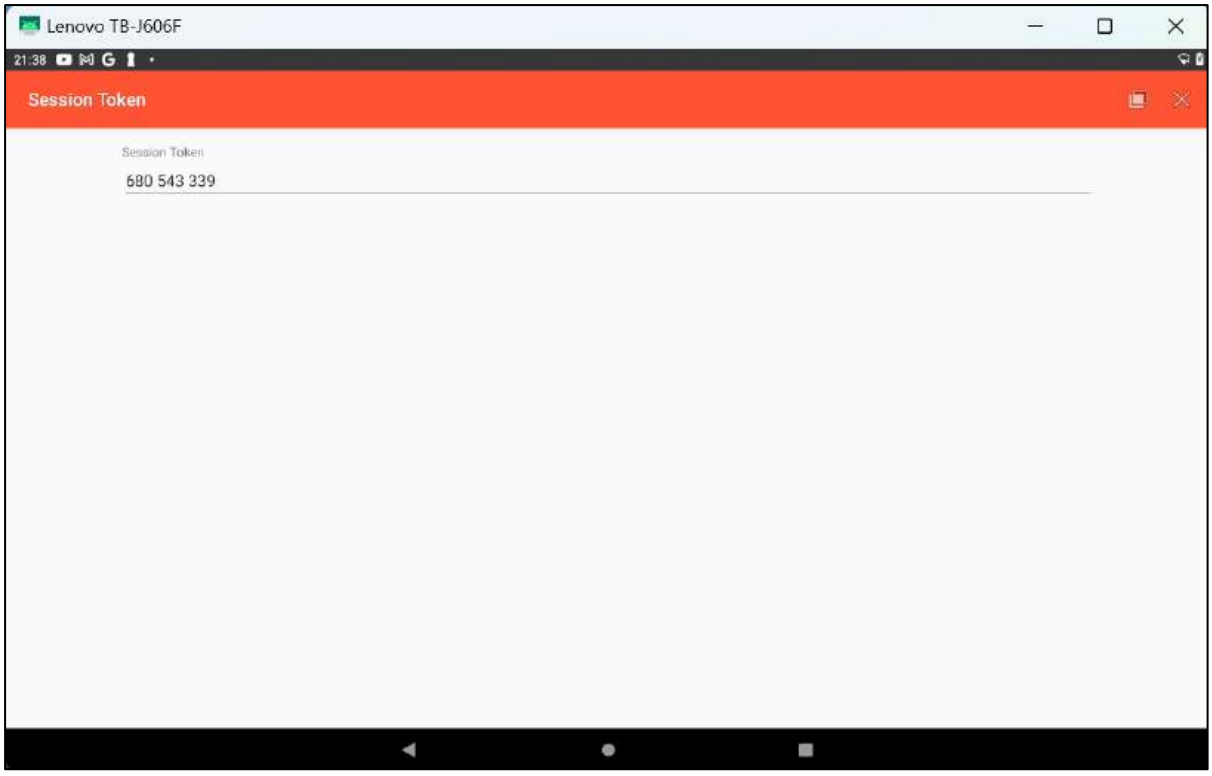
4.3.4.1 Example of an Ad Hoc Session

Here is an example of an Ad Hoc session.

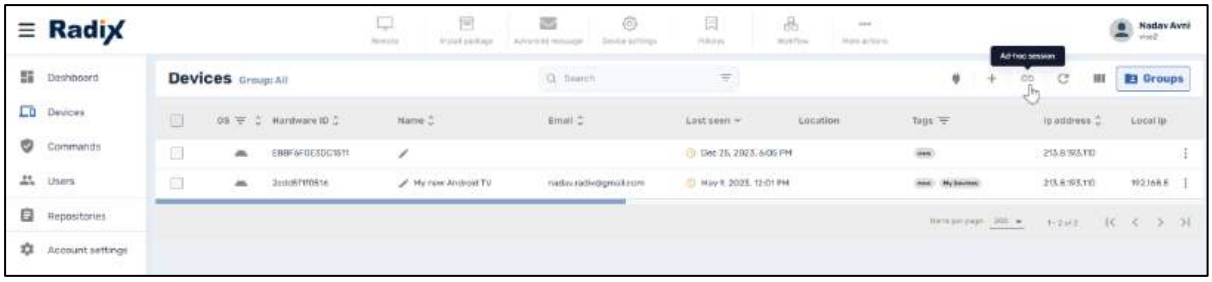
1. A Radix Device Manager administrator opens their list of devices by clicking on the **Devices** icon in the Overview Dashboard.



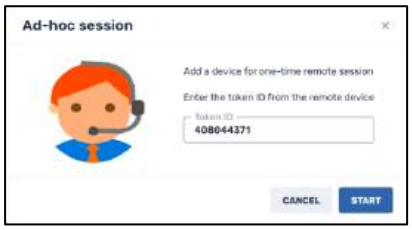
2. Let us say the administrator wants to add the device HA195F3Y (a Lenovo tablet computer), so that the administrator can service it. The user of the device opens the Viso app on their remote device, as above, and generates the Session Token.



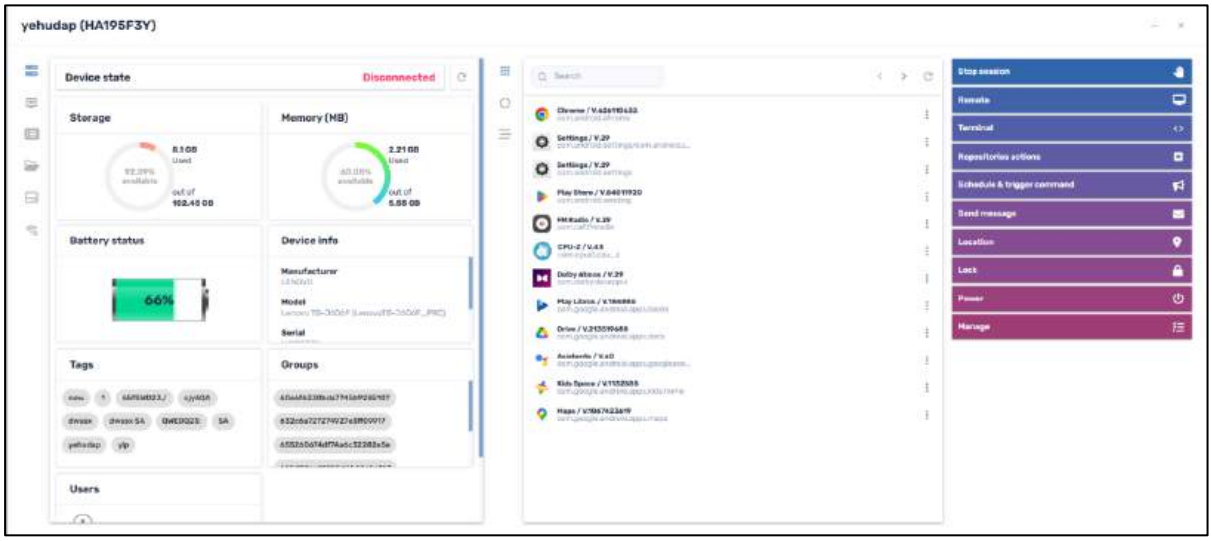
3. The Radix Device Manager Administrator opens an Ad-Hoc session on their device by clicking on the Ad-Hoc Session icon.



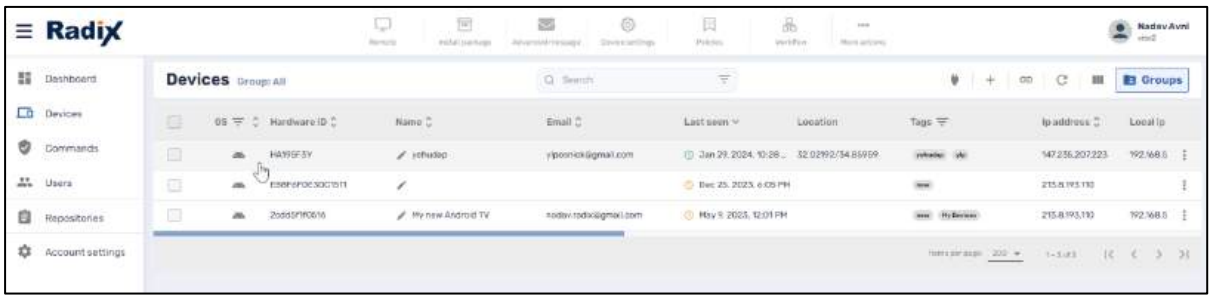
4. The Radix Device Manager administrator enters the Token ID in the Ad-hoc Session window and clicks **Start**.



5. The Device Dashboard for the newly added device HA195F3Y opens, allowing the Radix Device Manager to access it.

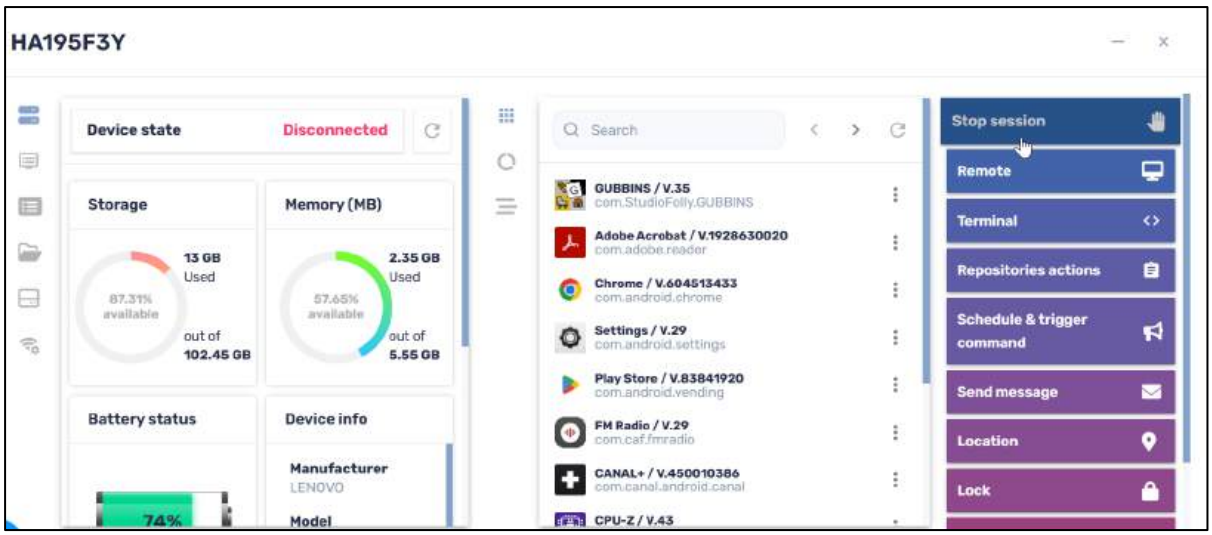


Also, the device will appear in the Radix Device Manager Administrator's list of devices:

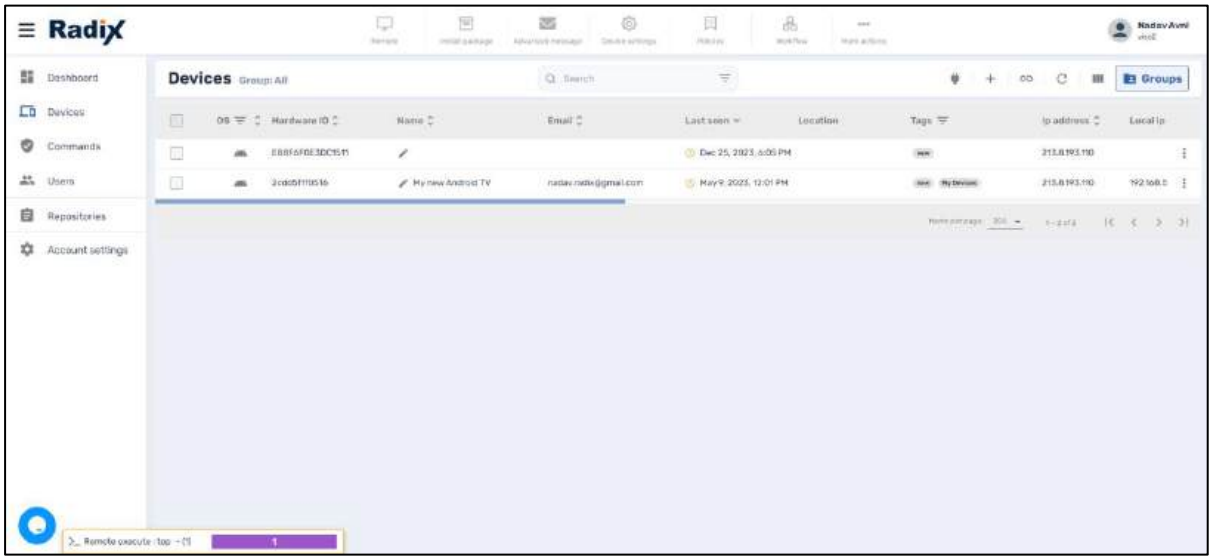


4.3.4.2 Ending an Ad-hoc Session

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:

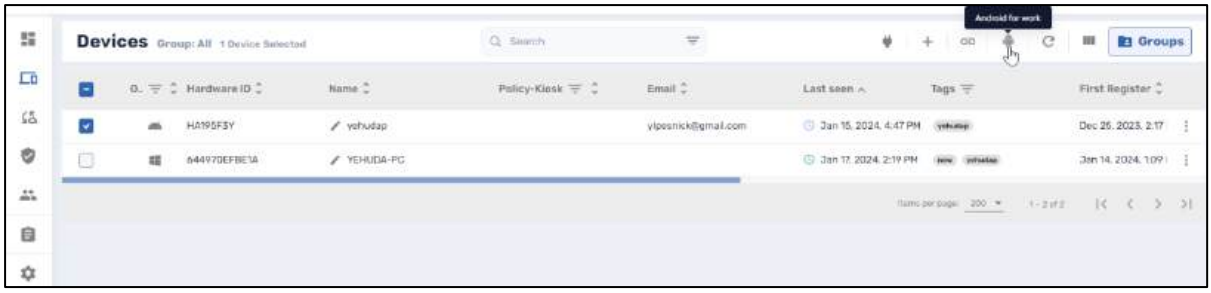


4.3.5 Android for Work

We mentioned previously in **Section 4.2.1.1, Android for Work (AFW) install/uninstall**, that you can install Android apps on remote devices by means of the Radix Device Manager 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** icon in the Devices Console.

To approve apps to be installed via the Android for Work feature:

1. Click on the **Android for Work** icon in the Device Console.



The **Android for Work** window opens.

Note the following icons on the left side of the window:

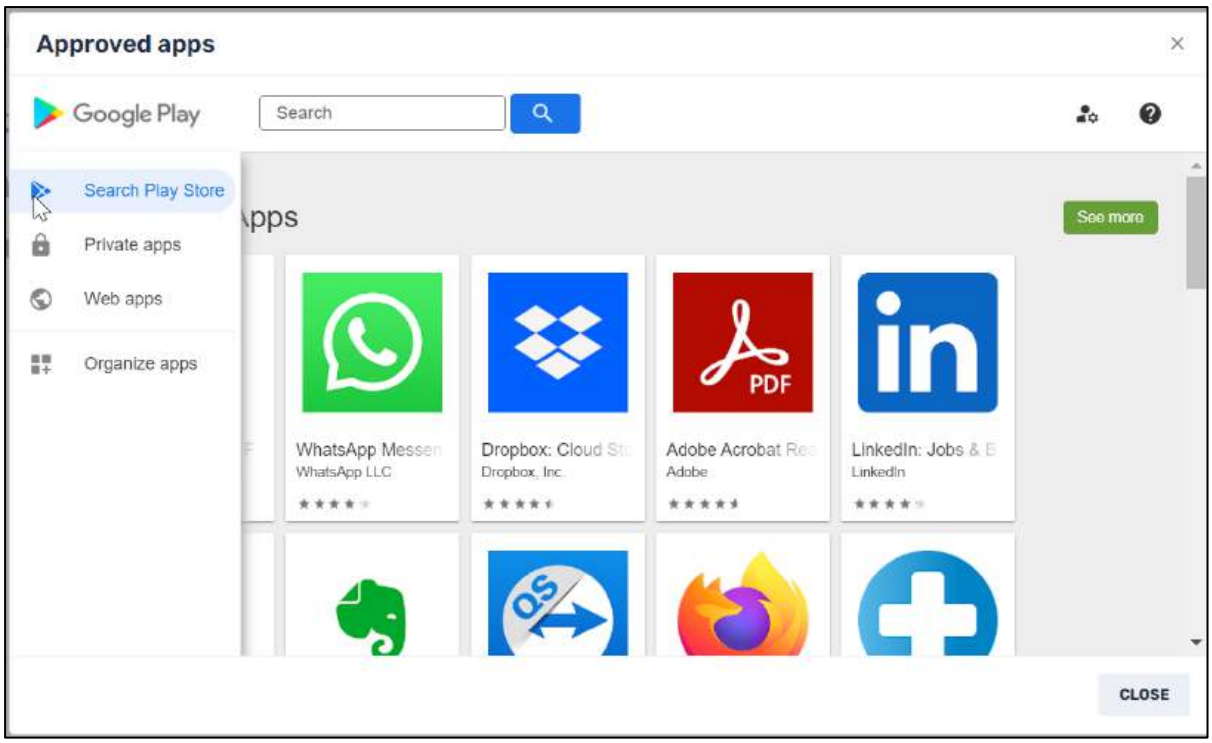
Icon	Description
	Public apps: Allows you to add apps that are available to all devices in the Radix Device Manager
	Private apps: Allows you to add apps that are available to only specific devices in the Radix Device Manager
	Policy: Allows you to select a software policy for a device, blocking or allowing specific apps.

We will go through the functions of these icons in turn:

4.3.5.1 Public Apps

When you click on the Public Apps icon, the **Public Apps** window opens.

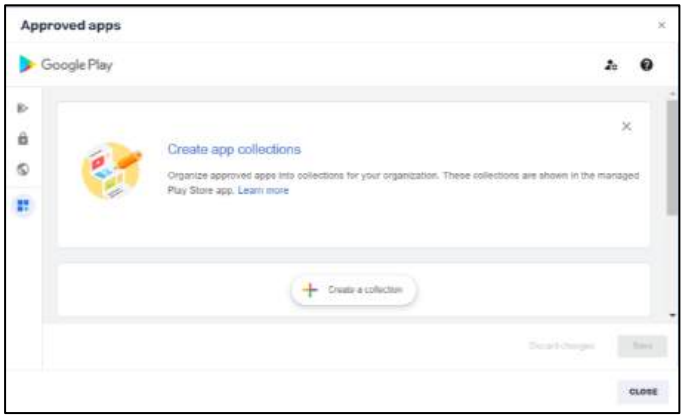
1. Click on the **Add App** button. A list of featured approved apps appears.



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:



4.3.5.2 *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.

4.3.5.3 *Install Policy*

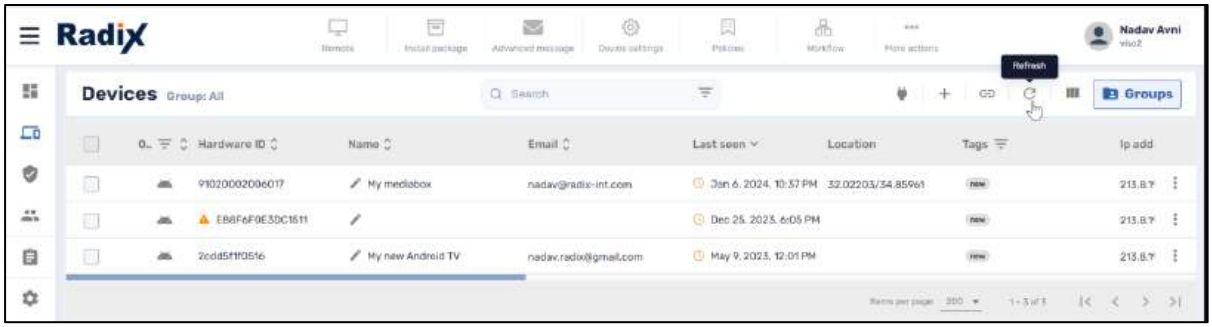
This allows you to install a software policy on a device.

The process is identical to what is outlined in **Section 4.1.5, Policies**.

After you have finished approving apps and a software policy to be employed in Android for Work, proceed from **Section 4.2.1.1** to actually install the approved apps using the **Android for Work Install** command.

4.3.6 Refresh

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



4.3.7 Selecting Columns Option

The Radix Device Manager 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 Manager 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 **Commands Console** and **Users Console** as well.)

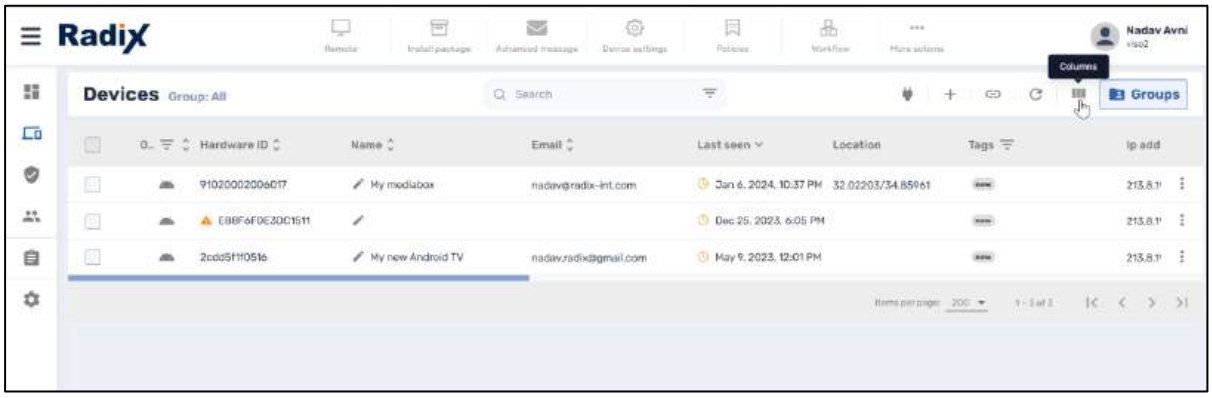


Figure 4-74: Columns icon

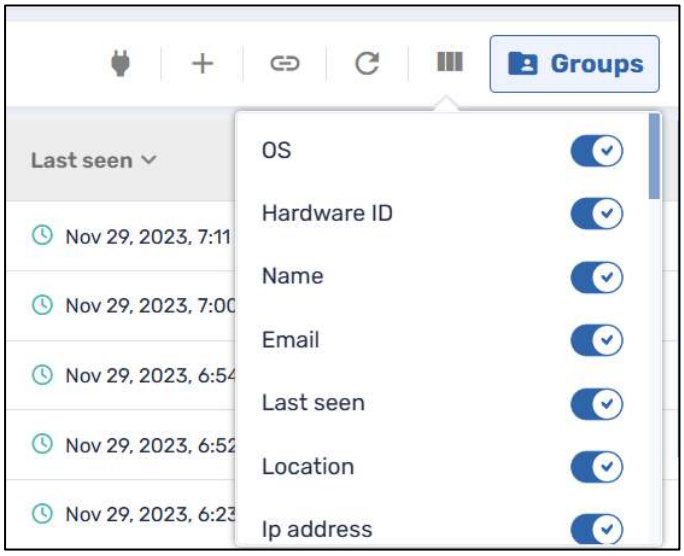


Figure 4-75: Column Display Options

4.3.7.1 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**.

4.3.7.1.1 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 Console has a sliding bar which allows you to view other columns.

4.3.7.1.2 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.

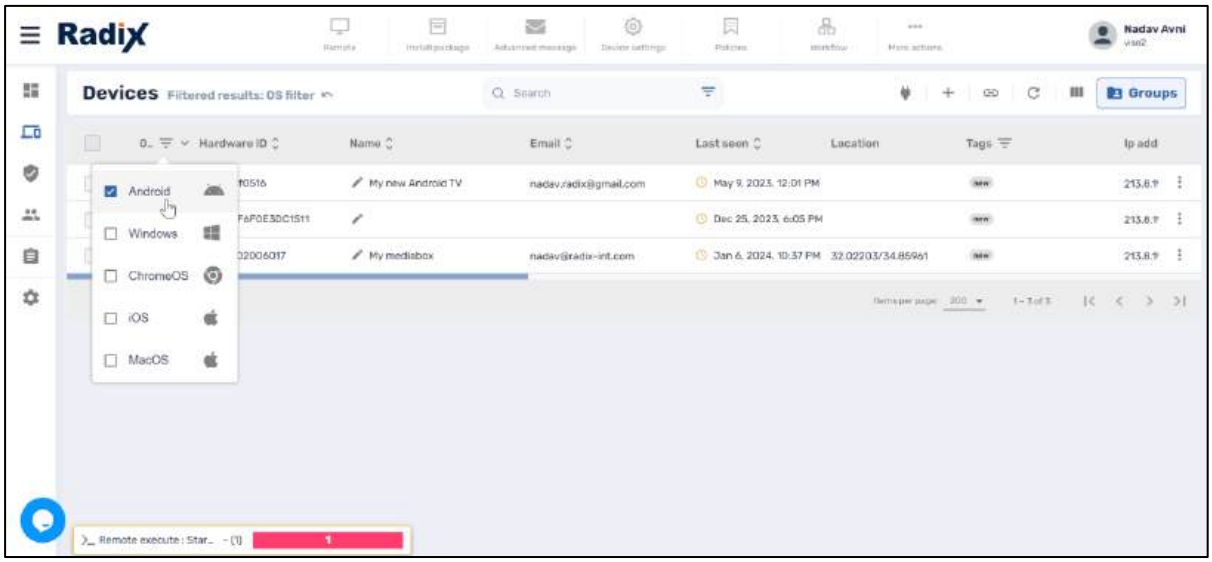


Figure 4-76: Filtering Devices by Operating System

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

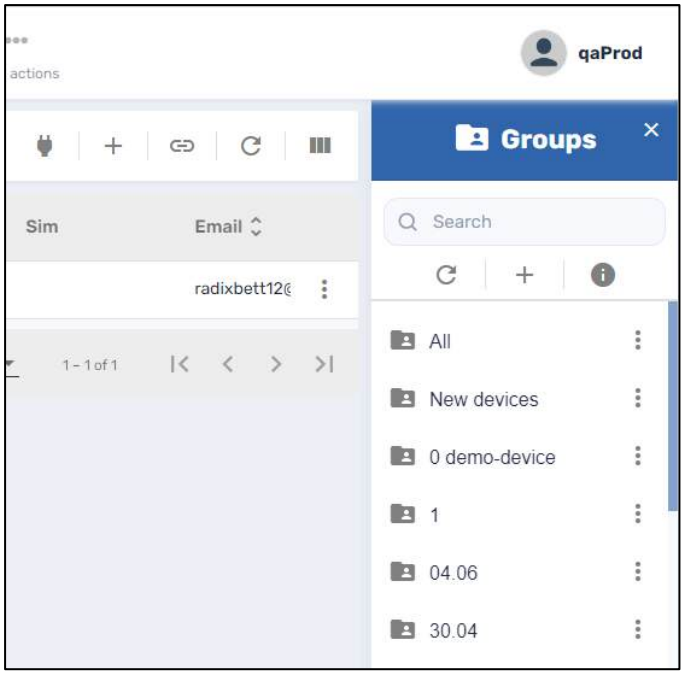
4.3.8 Grouping Devices

You can also group devices together in a folder, using the **Groups** icon. This lets you 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.

4.3.8.1 Creating a New Group of Devices

To create a group of devices:

1. Click on the **Groups** icon in the Search Bar. The Groups window opens.



Note the "All" group at the top of the list. Selecting this group will allow you to perform actions on all the devices listed.

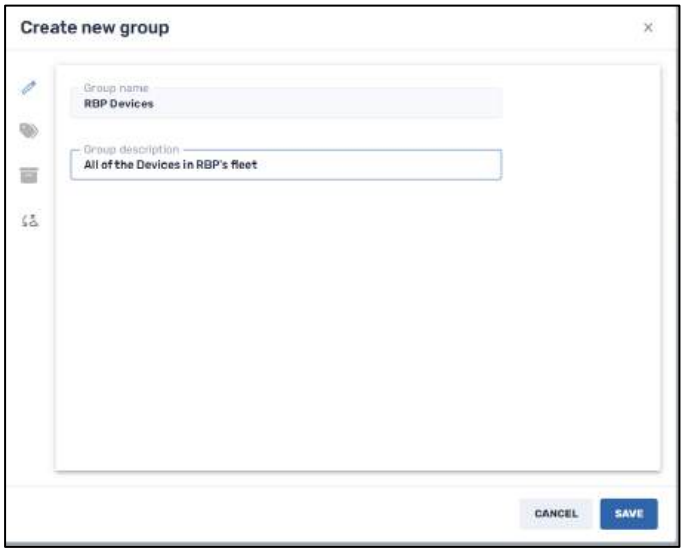
The Groups window has the following options:

Table 4-13: Groups Window Options

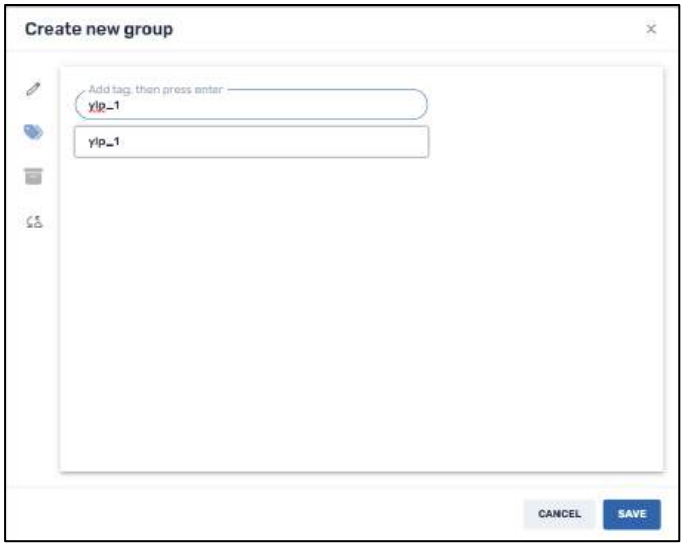
Icon	Description
Search	Search group by name
	Refresh the list of groups
	Add a new group
	Information about the Groups option

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

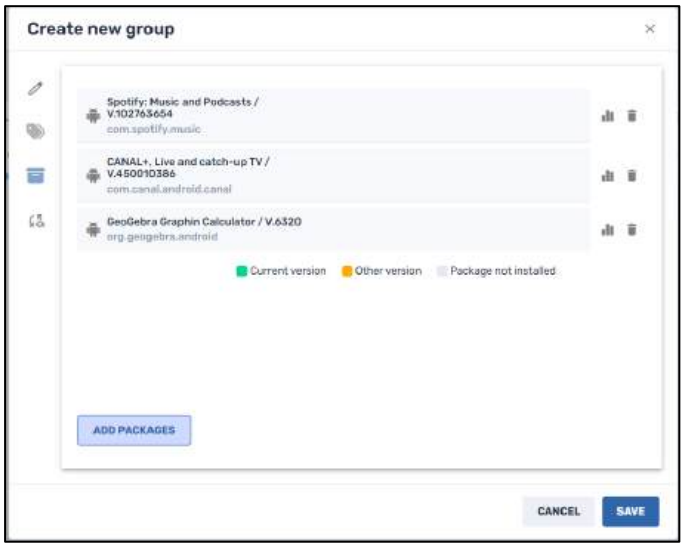
3. Supply a Group name and Group description.



4. 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).



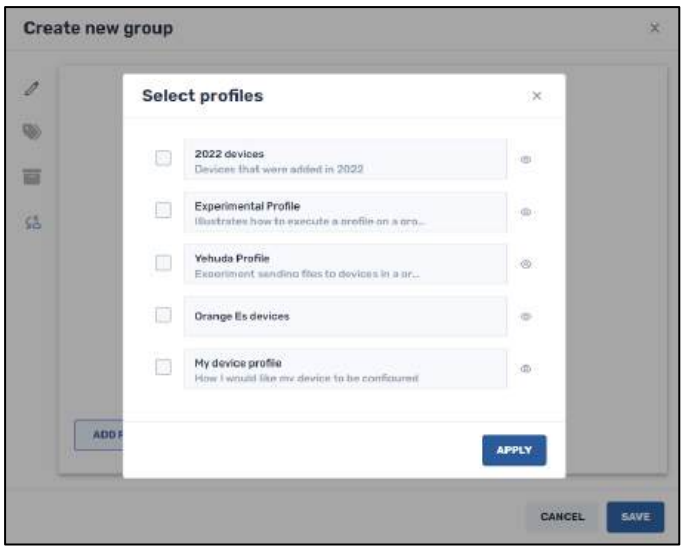
5. If you wish to install software packages to the devices in the group, click on the **Packages** icon , and click on **Add Packages**.
   The **Packages** window opens.
6. Select the software packages that you would like to add to the devices in your group and click **Add**.



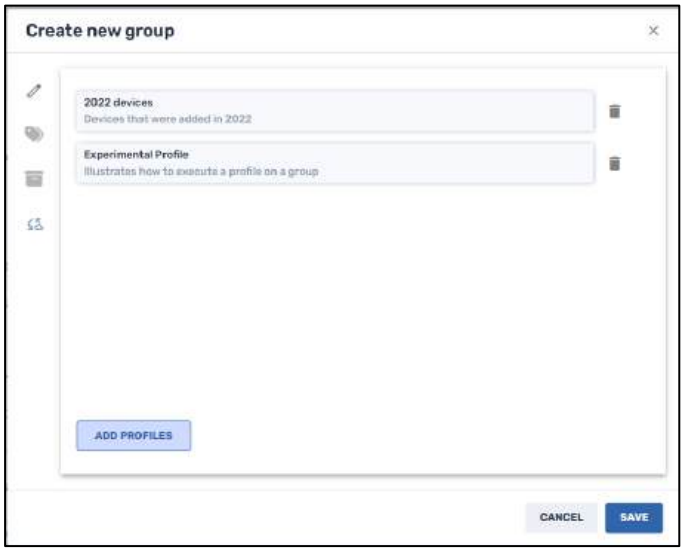
7. Click on the **Profile** icon . The **Add Profiles** window opens.

(The Profiles feature is treated in greater detail in **Section Chapter 5, Profiles Console**.)

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

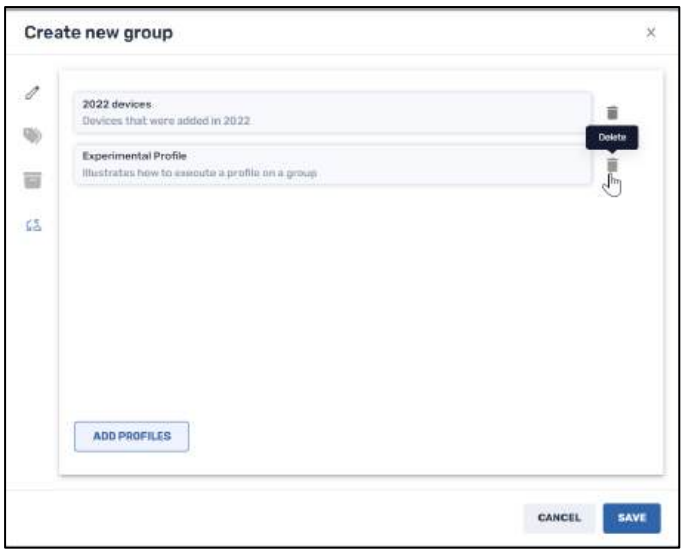


9. Select the desired profiles to add to the group and click **Apply**.

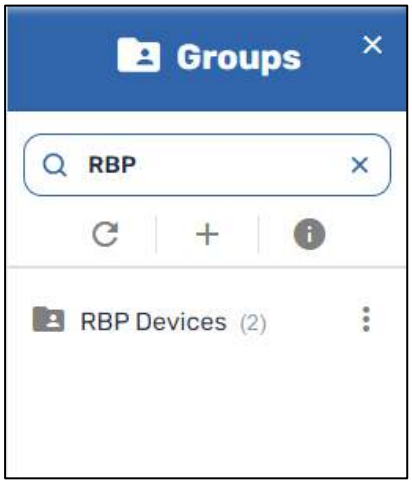


The profile will now appear in the group's list of profiles.

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



11. Click **Save**. The new group will now appear in the list of groups.



You can always edit the details of the group using the **Group Management** command, as we will see below (**Section 4.3.8.3, Group Management Options**).

4.3.8.2 Adding Devices to an Existing Group

To add devices to an existing group:

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

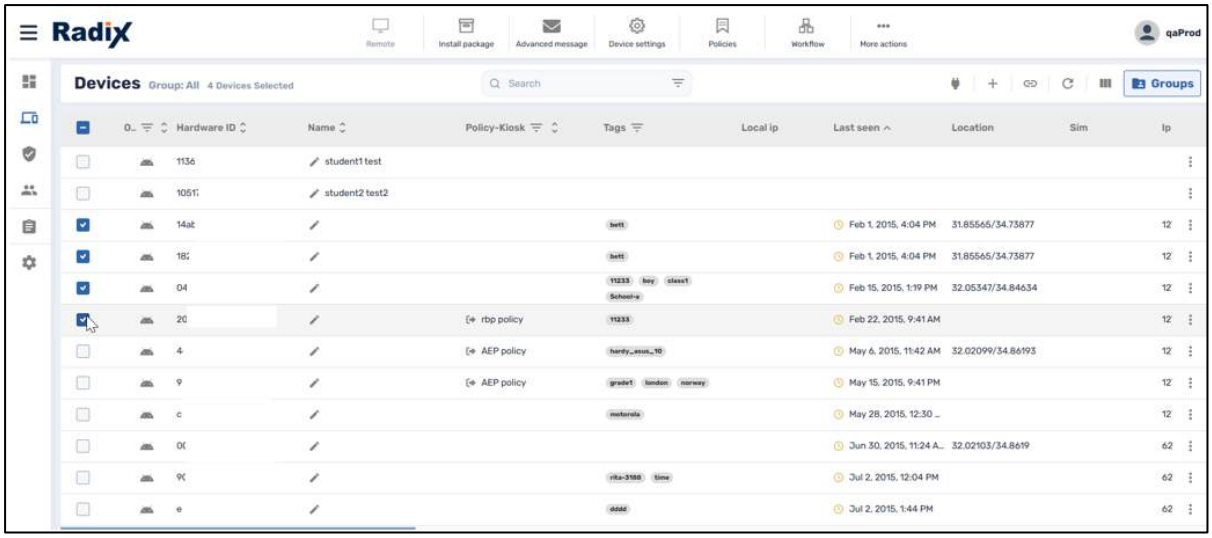


Figure 4-77: Selecting devices to be included in a group

2. Open the Tags option, either from the **More actions** icon in the Devices Console Ribbon, or from the devices' three-dot menu.

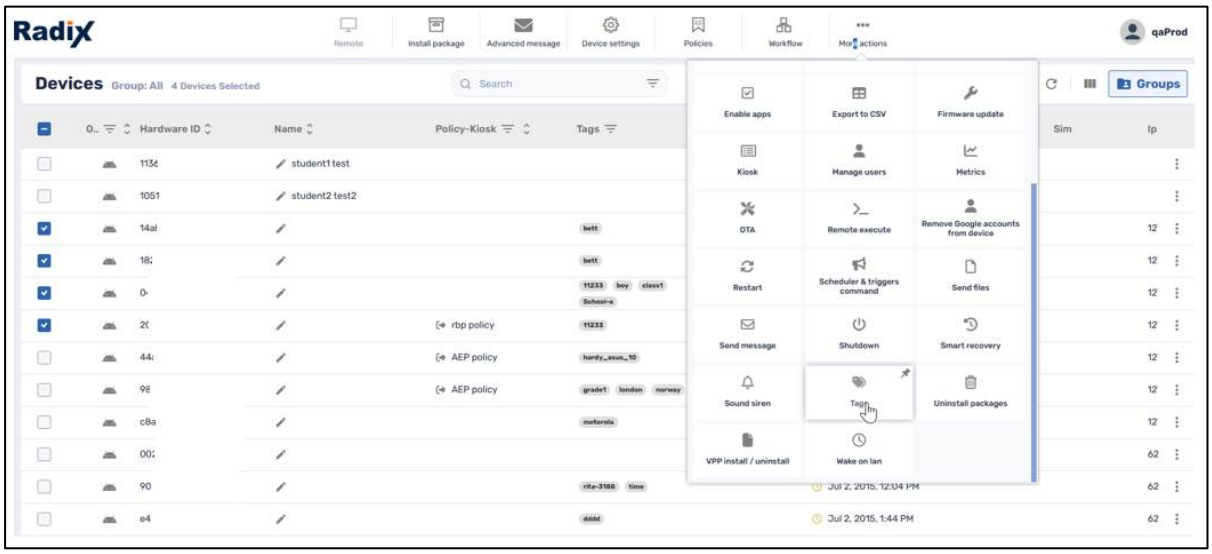


Figure 4-78: Assigning a tag to the selected devices

3. Add the tag that distinguishes the new group to these selected devices and click **Confirm.** (In our example, the tag is **old_devices**.)

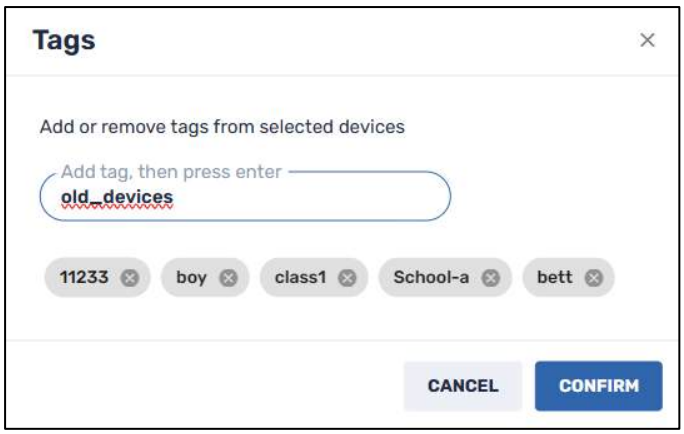


Figure 4-79: Assigning a tag to several devices

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

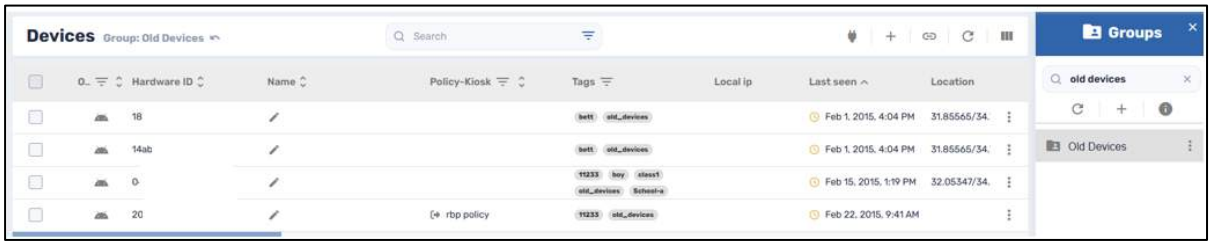


Figure 4-80: Display of devices in the specified group Old Devices

4.3.8.3 Group Management 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 Group Management command will allow you to make these modifications.

To manage a group:

1. Click on the **Actions** three-dot menu next to the Group name. The **Commands** window opens.

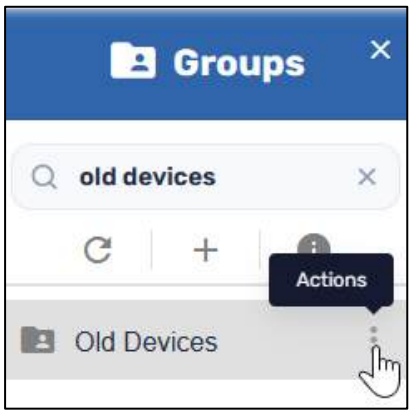


Figure 4-81: Actions menu button

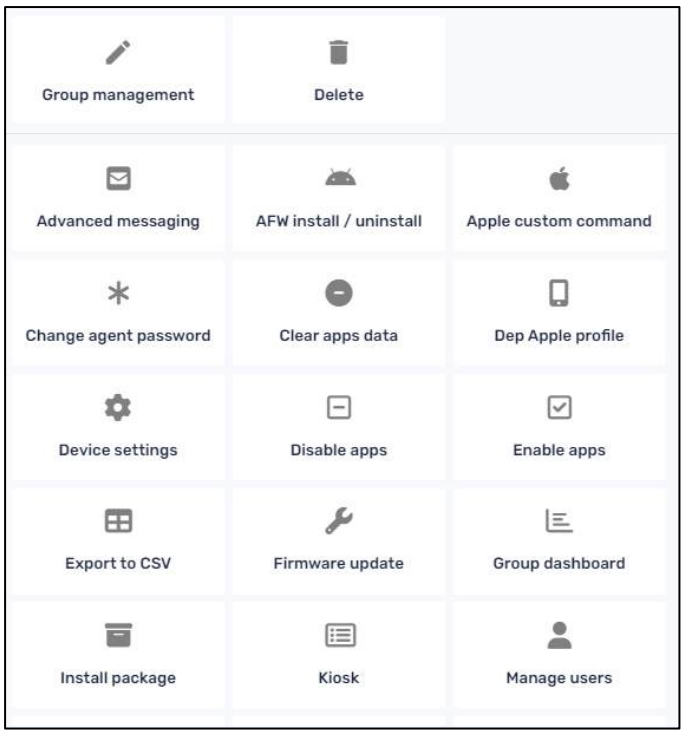


Figure 4-82: Actions menu

2. **To perform modifications to the group**, click on the **Group management** tile. An **Edit Group** window opens, with the same functions as the **Add New Group** window.

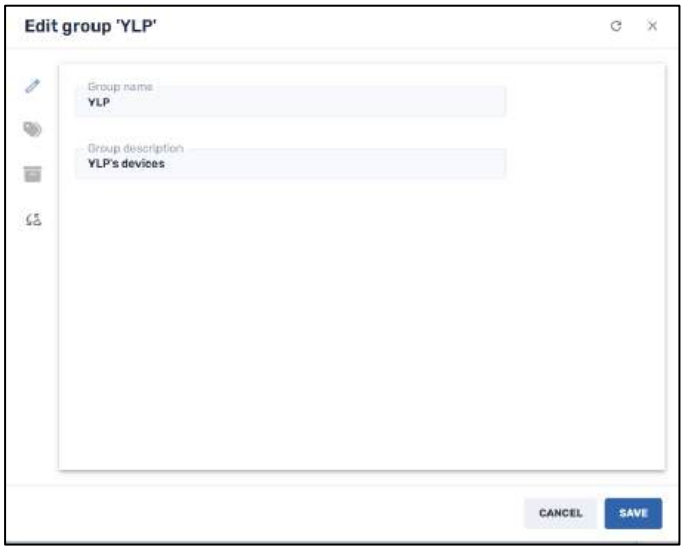
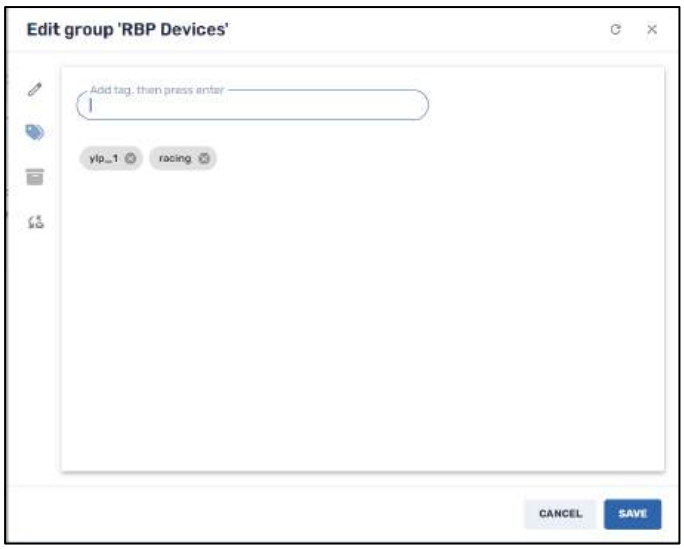
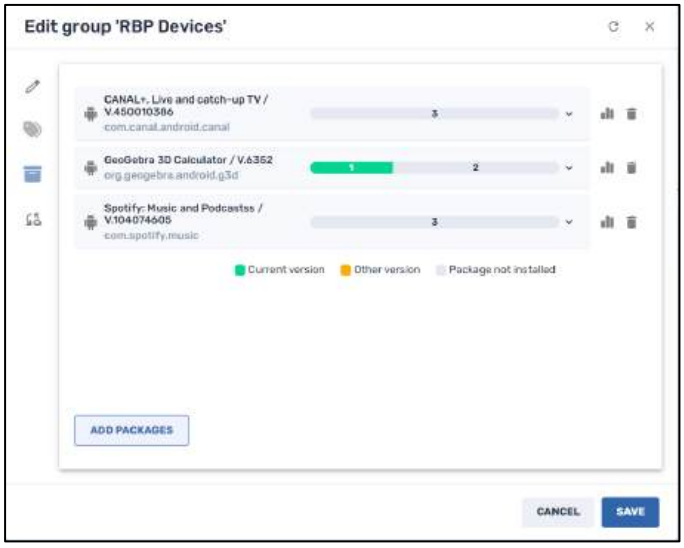


Figure 4-83: "Edit Group" Window

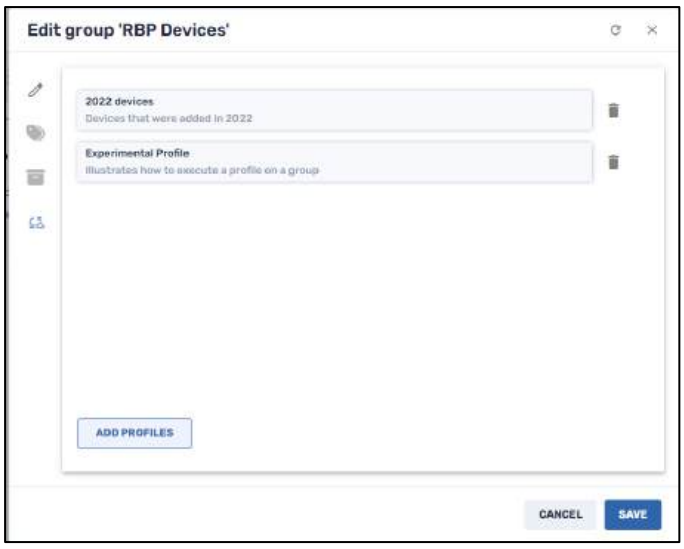
3. Click on the **Tags** icon to add tags to a group. Any devices with that tag will now be included in this group.



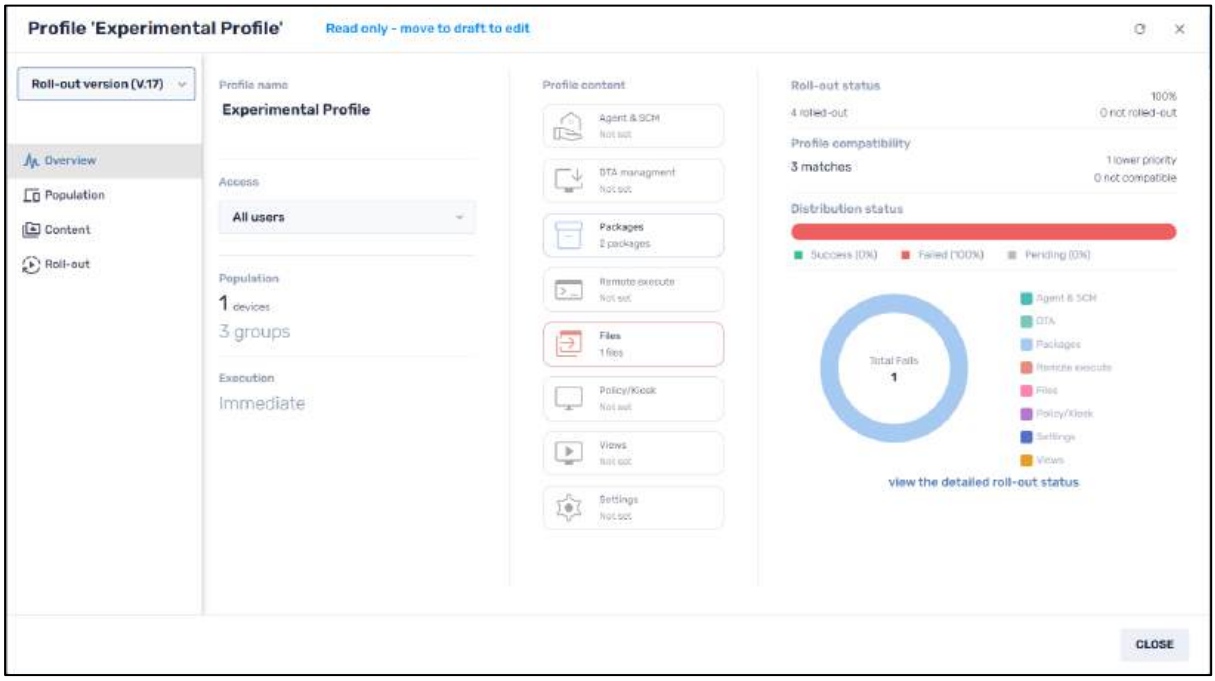
4. Click on the **Packages** icon . You will see the software packages associated with this group, and the distribution of how they are installed on the devices in the group. In the example below, we see that the application **Geogebra** has been installed on one of the devices in the group **RBP Devices**.



5. Click on the **Profiles** icon . You will see the profiles associated with this group.



6. Click on one of the profiles to view its details.



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

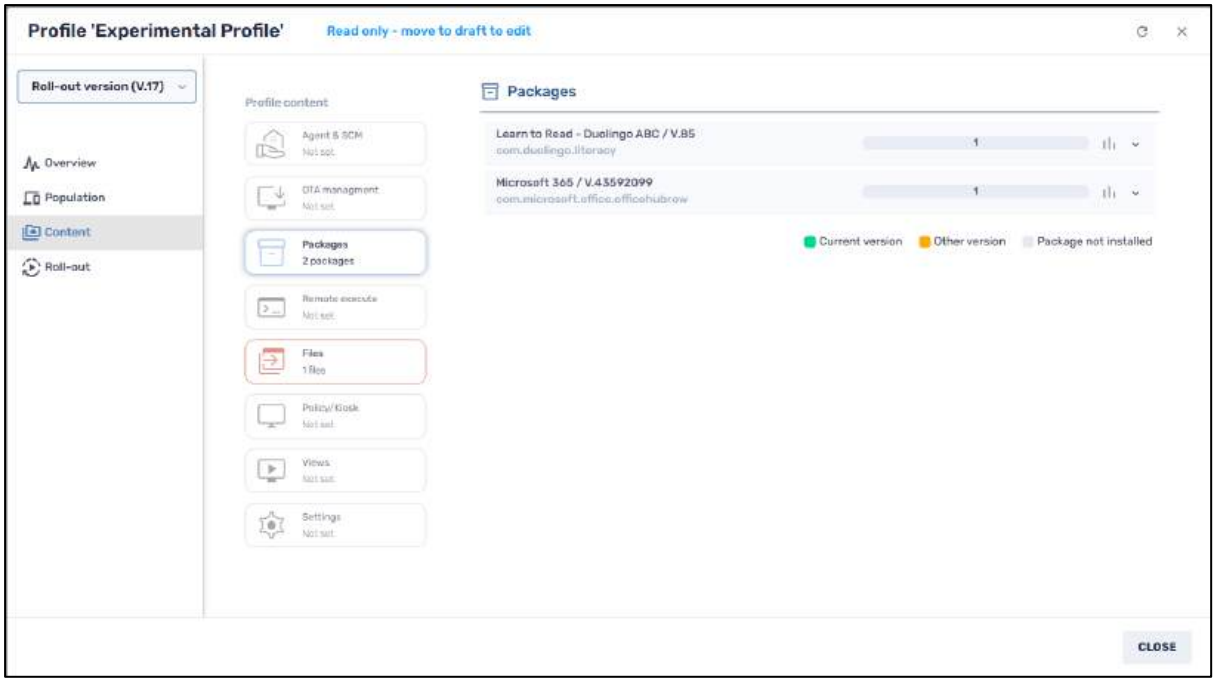
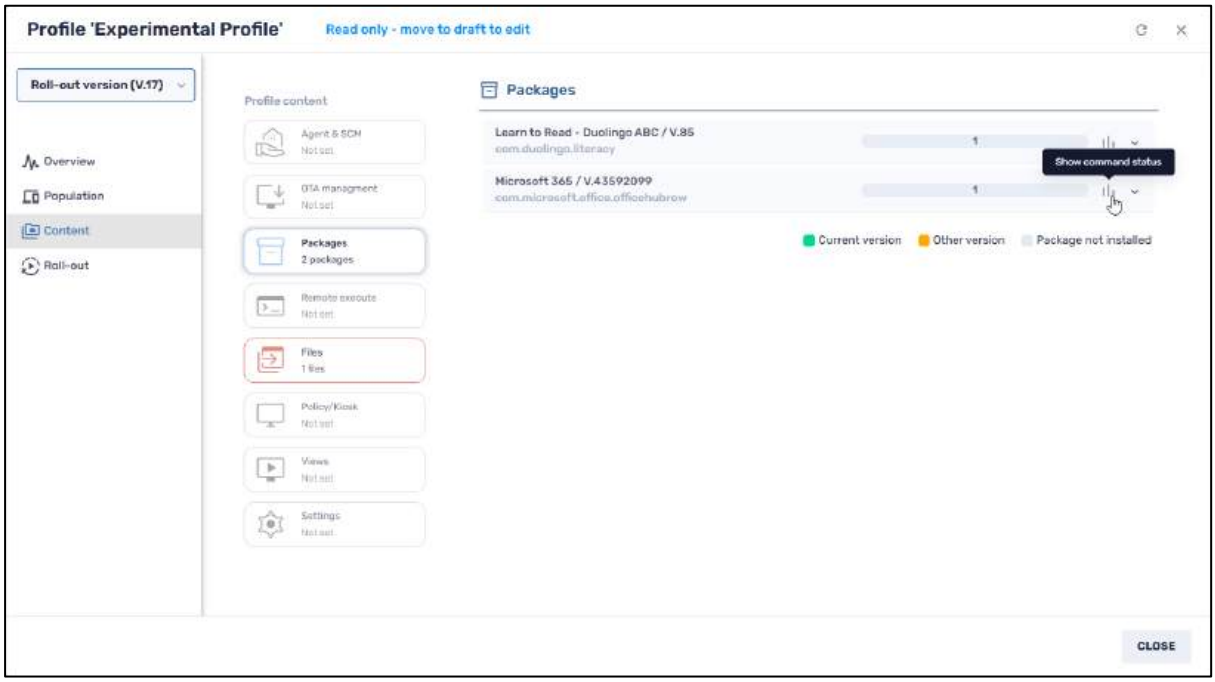


Figure 4-84: Display of software packages installed on devices associated with this profile

We will discuss Device Profiles in greater detail in **Chapter 5, Profiles Console**.

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

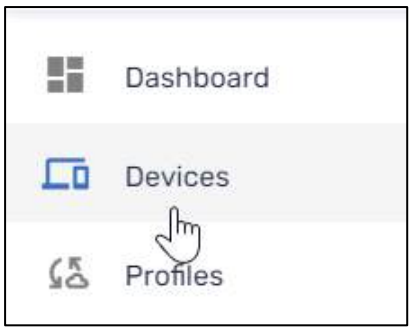


4.3.8.4 Deleting a Group

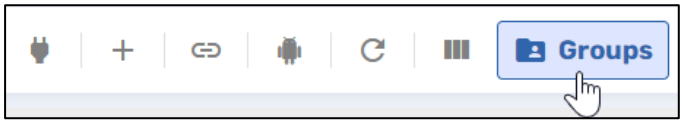
The Groups panel has an option to delete a group.

To delete a group:

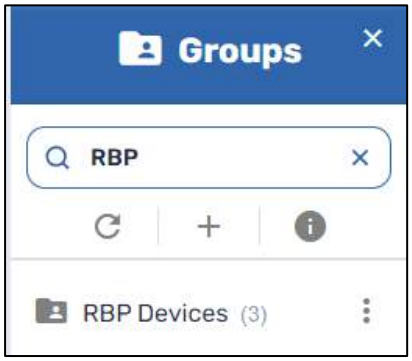
1. In the Radix dashboard, click on the **Devices** icon to open the Devices console.



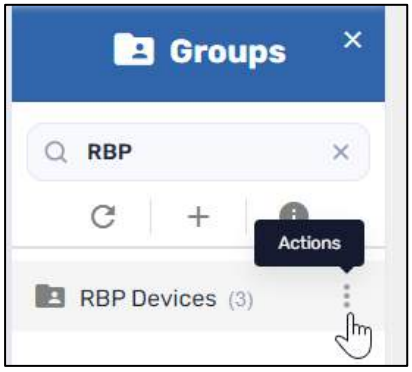
2. Click on the **Groups** icon on the far right of the Devices console to view the list of groups to open the Groups window.



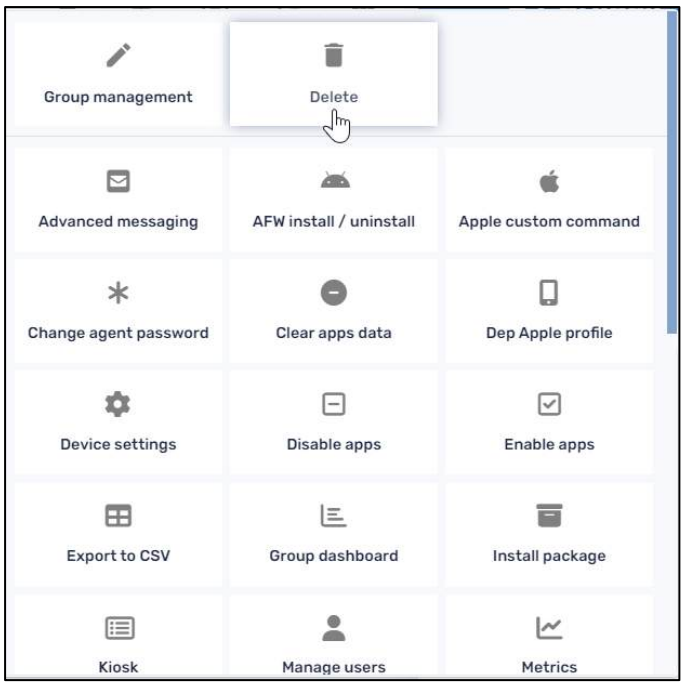
3. In the Groups window, enter the name of the group that you would like to delete in the Search bar.



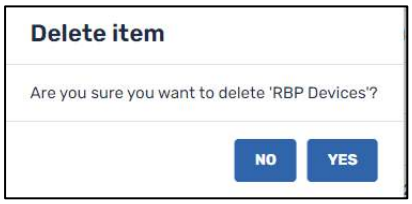
4. Click on the three-dot menu to open the Actions grid.



5. In the grid of options, click on the **Delete** tile.



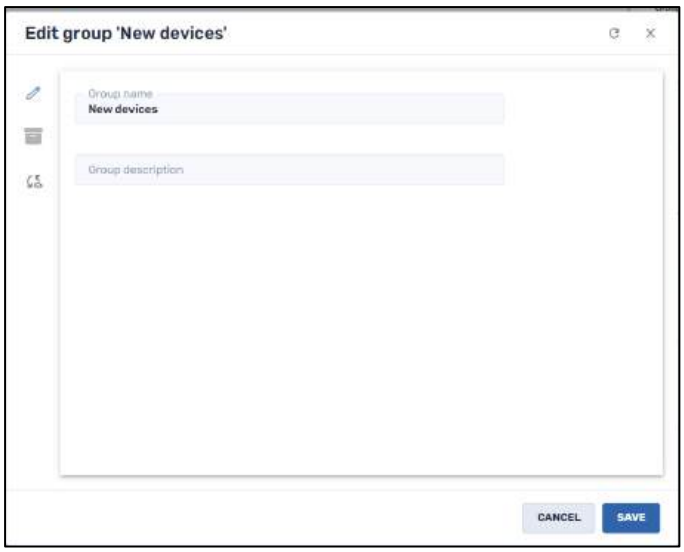
6. You will be prompted if you are certain that you want to delete the group. Click **Yes** to confirm.



4.3.8.5 Managing the New Devices Group

For the group **New Devices**, the Group Management 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. Click on the **Groups** icon in the Devices Console and find the **New Devices** group.
2. Click on the **New Devices** three-dot menu. The **Commands** grid opens.
3. Click on the **Group Management** tile. The **Edit group 'New Devices'** window opens.



4. When you click on the **Packages** icon, you will notice that there are certain mandatory software applications that already appear.

In this display, from the total number of devices available (= 250 devices), we see that 32 devices have the current version of Spotify, 37 devices have a previous version, and 161 devices do not have Spotify installed presently. (This could be because many of these 161 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.

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

Figure 4-85: Viewing devices with/without the app installed

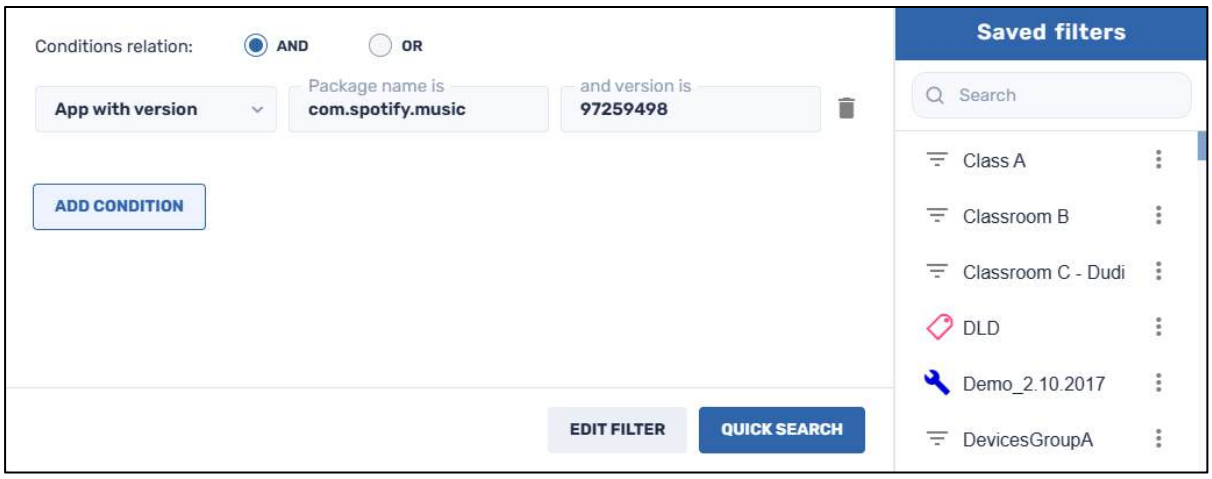
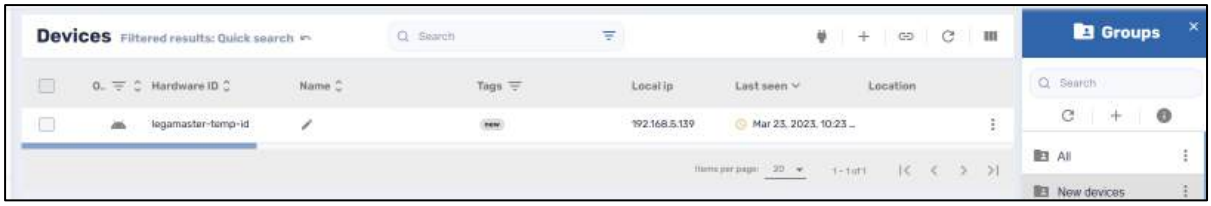
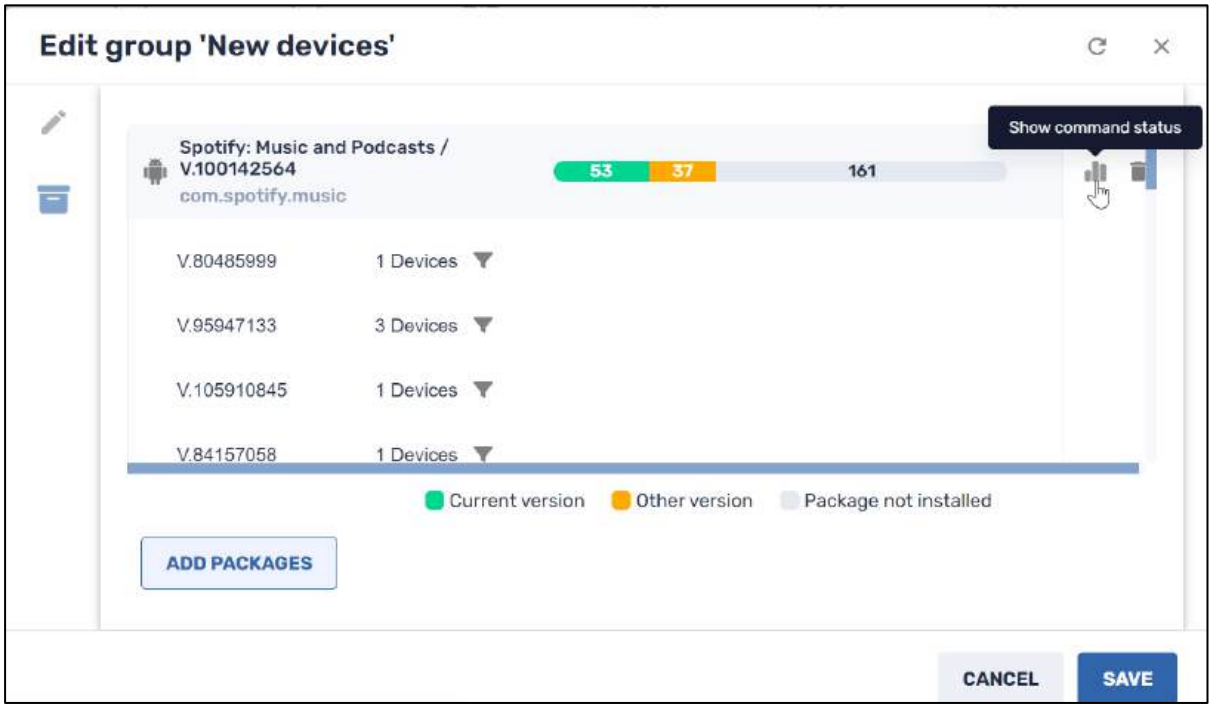


Figure 4-86: Filtering devices by version of app installed

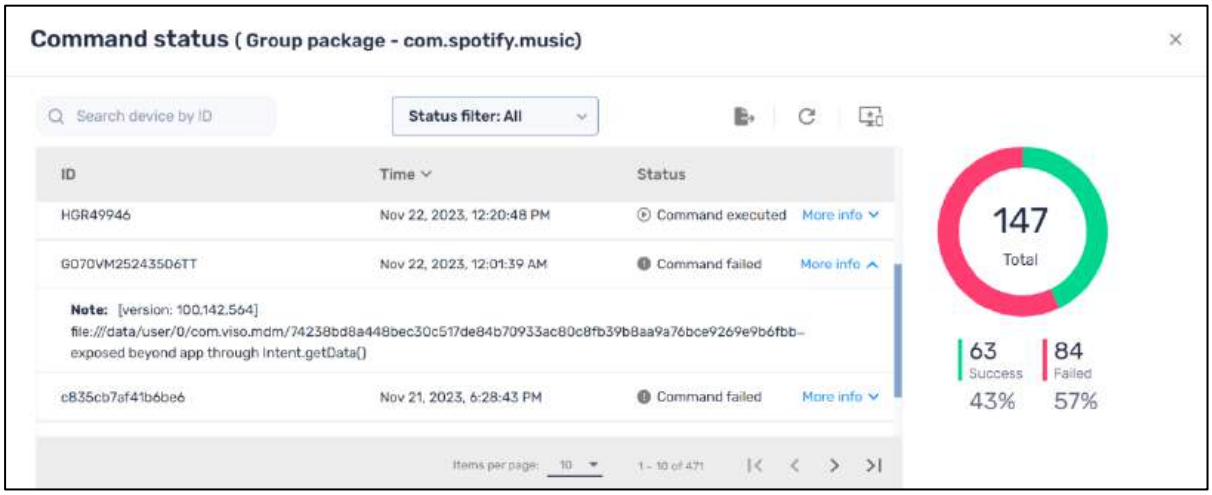
7. Click on **Quick Search**. You will see the details of the specific devices that have or do not have the most recent installation of the application:



8. 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:

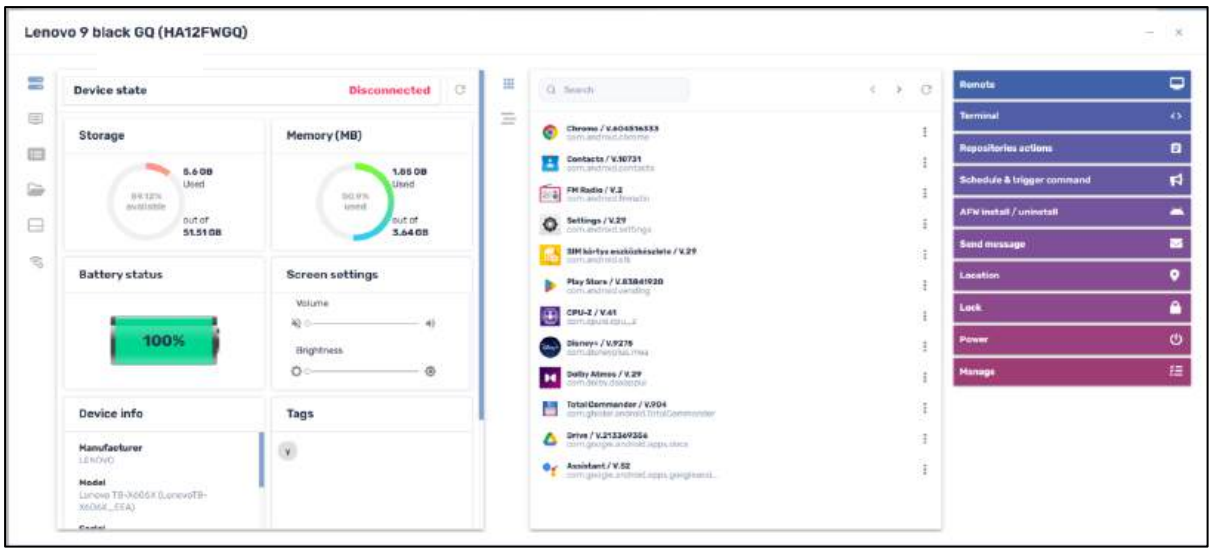


It will provide you with a list of all the devices, whether the app was installed on the device successfully, and any reason the installation failed:



4.4 Device Dashboard

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



4.4.1 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.

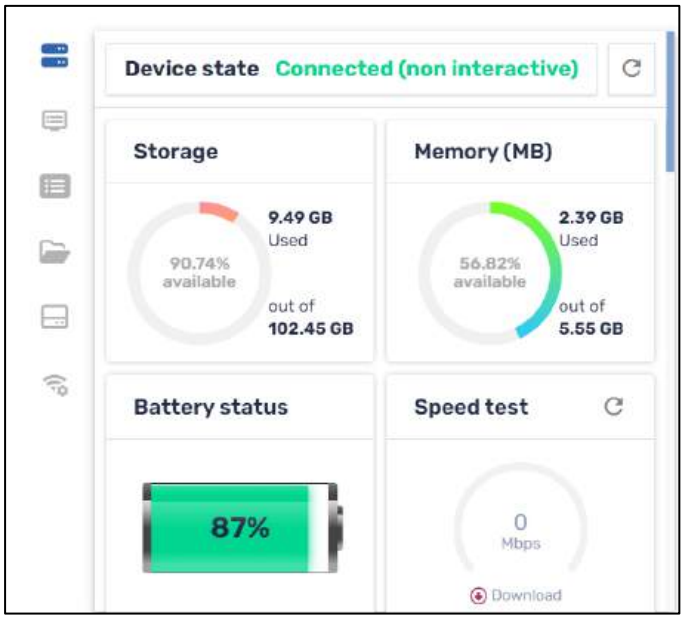


Figure 4-87: Device Status Pane

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

Table 4-14: 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.

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

4.4.2 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.

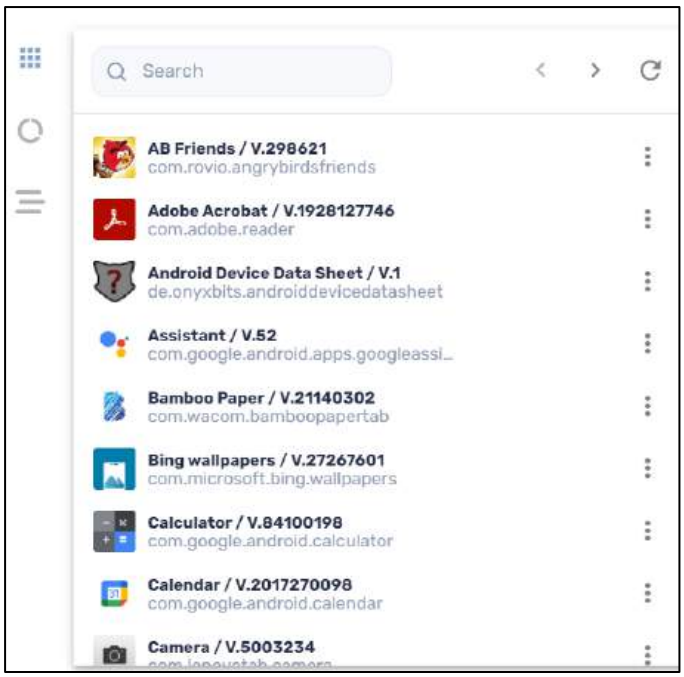


Figure 4-88: App Management Pane

Table 4-15: 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.

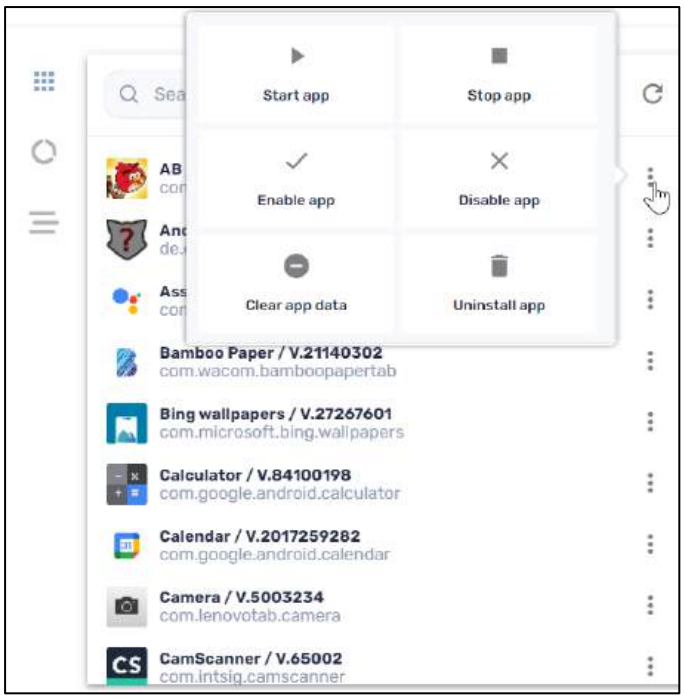


Figure 4-89: Application Management Menu

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	**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.

4.4.3 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 4-16: Device Actions Icons

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

We will briefly go through the Device Actions options:

4.4.3.1 Remote

As explained in **Section 4.1.1**, this allows you to interact with the user's device remotely.

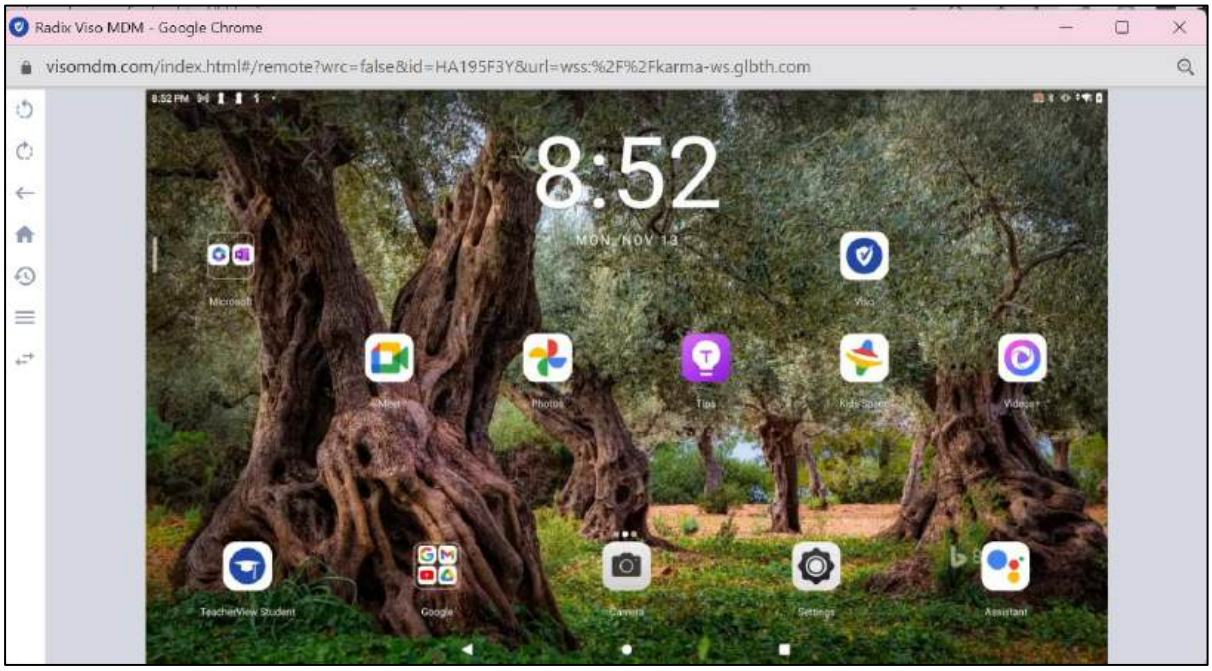


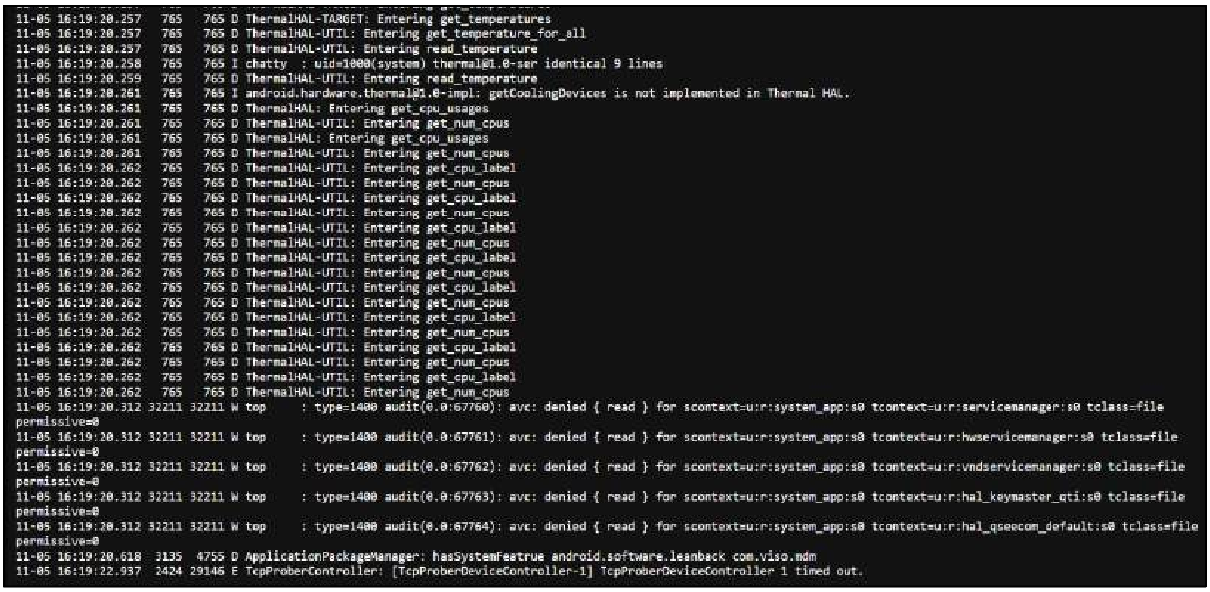
Figure 4-90: Viewing a User's Device Remotely

4.4.3.2 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.

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 **Remote** and **Terminal** commands can be used only on a single device at a time.

The following actions in the right pane of the Device Dashboard can be performed on several devices at once:

4.4.3.3 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 4-17: Repository Actions Icons

Icon	Description
	**Install Packages**: Allows you to create an installation package and install apps remotely, as explained in **Section 4.1.2**.
	**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 4.1.5, Policies**.
	**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 4.2.1.8, 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.
	**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 4.1.3**.
	**Device Settings**: This allows you to apply different settings to the device. This is explained in **Section 4.1.4**.
	**Remote Execute:** This allows you to execute terminal commands on a device remotely. This is explained in **Section 4.2.1.12**.
	**Files**—This allows you to upload files to a device. This is explained in **Section 4.2.1.16**.
	**OTA**— This enables an Android device to receive and install updates to its operating system or apps. This is explained in **Section 4.2.1.11**.
	**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 4.1.6**.

4.4.3.4 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 4.2.1.15, Scheduler & Triggers Command**.

4.4.3.5 AFW Install/Uninstall

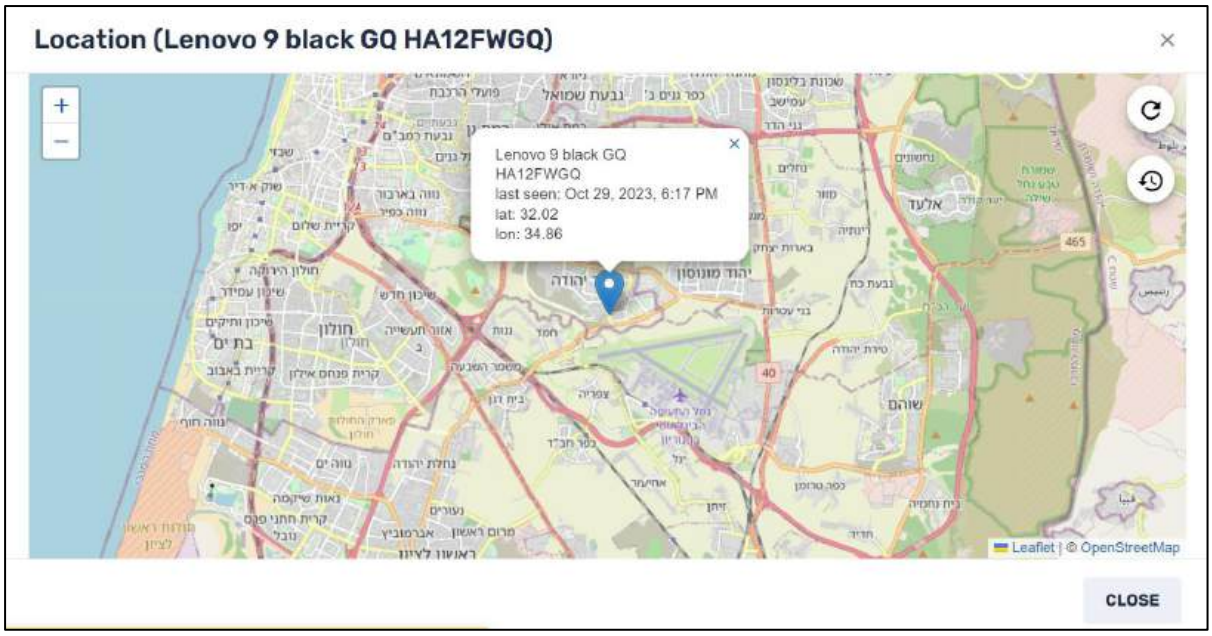
Clicking on this tile opens the window that we saw above in **Section 4.2.1.1**, which allows you to install or uninstall a device in the Android for Work (AFW) program.

4.4.3.6 Send Message

This allows you to send a text message to the user on their device. This is treated at length in **Section 4.2.1.18, Send Message**.

4.4.3.7 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.

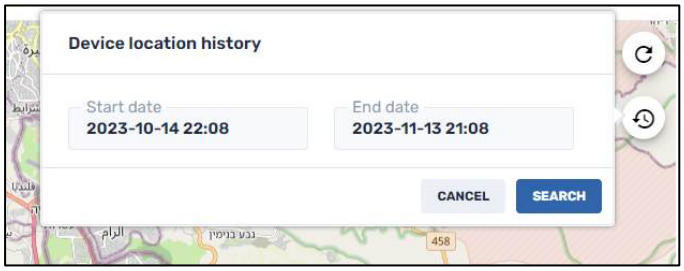


Figure 4-91: Location of a device within the selected time frame

4.4.3.8 Lock

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 4-18: Lock/Unlock Device Options

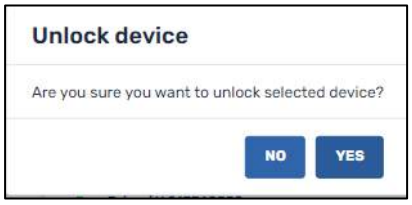
Icon	Description
	**Lock**: This locks the device so that the user cannot change any of the settings.
	**Unlock**: This unlocks the device, to enable the user to change settings.
	**Get Password**: This allows you to retrieve the device's password, to allow the remote user to unlock their device, in 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.

4.4.3.8.1 Unlocking a device

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

Option 1: From the Radix Device Manager:

1. The administrator must click on the Devices icon in the sidebar menu, to open the Device Console.
2. The administrator should find the locked device in the list of devices in the Device Console.
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.

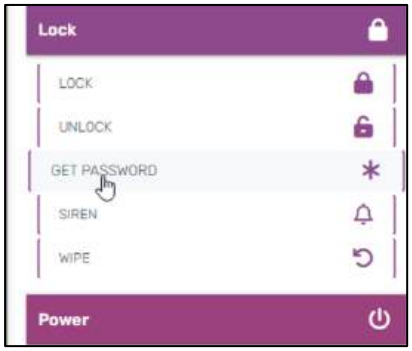
Option 2: For the remote device user:

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 locked device:

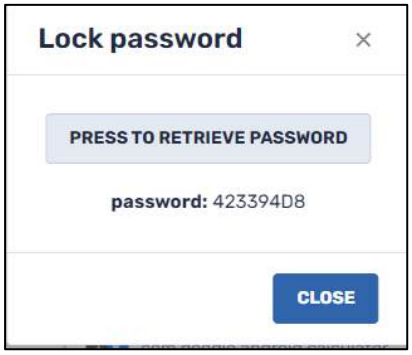
1. Press the key combination **Alt-Ctrl-Shift-F9**. You will receive a prompt requesting the device password:

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

4.4.3.9 Power management

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

Table 4-19: Power Management Options

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

4.4.3.10 Manage

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

Table 4-20: 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.

Chapter 5. Profiles Console

The Profiles Console allows you to create a profile of several groups of devices. Once you have created a profile, 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 profile. Also, if you add additional groups to the profile later, the specified software packages, OTA updates, and files will be automatically installed on these groups as well.

When you click on the Profiles Console icon , you will see a list of existing profiles in the Radix Device Manager.

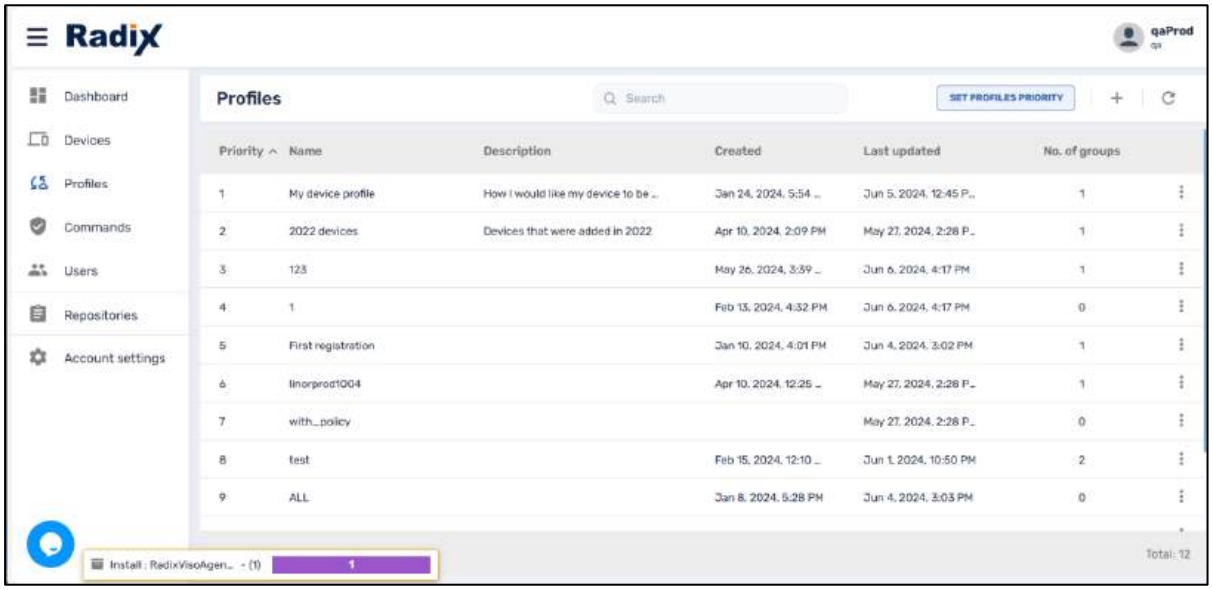


Figure 5-1: Profiles Console, displaying all existing profiles

5.1 Creating a New Profile

If you have Administrator privileges, you can create a new user profile.

To create a new profile:

1. Click on the **Add New Profile** icon at the top of the Profiles Console.

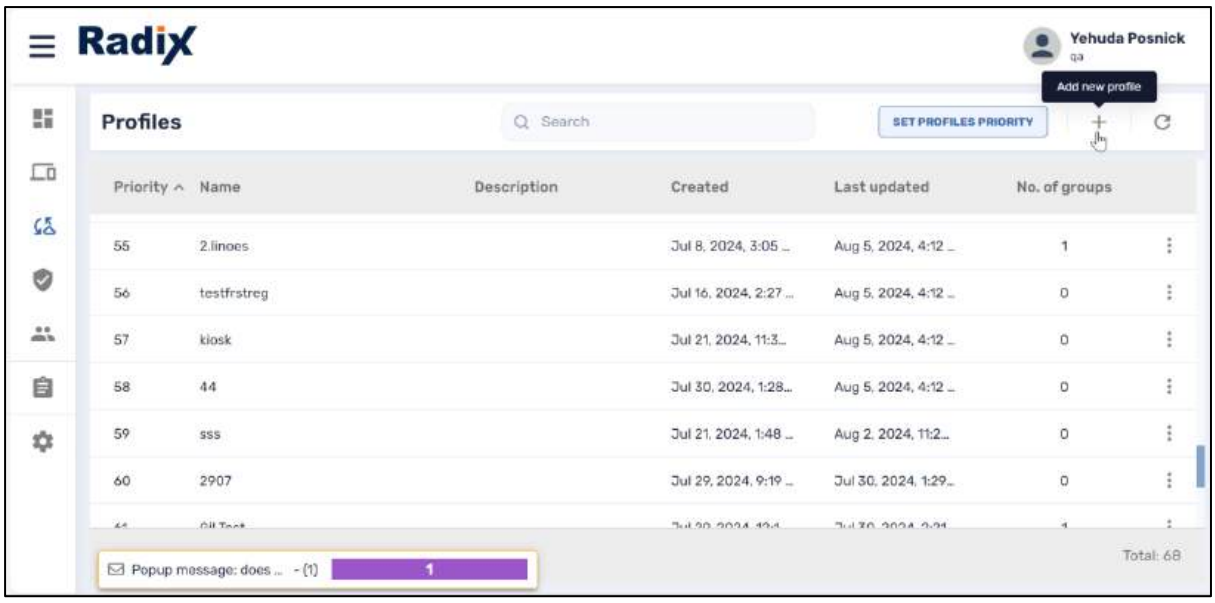
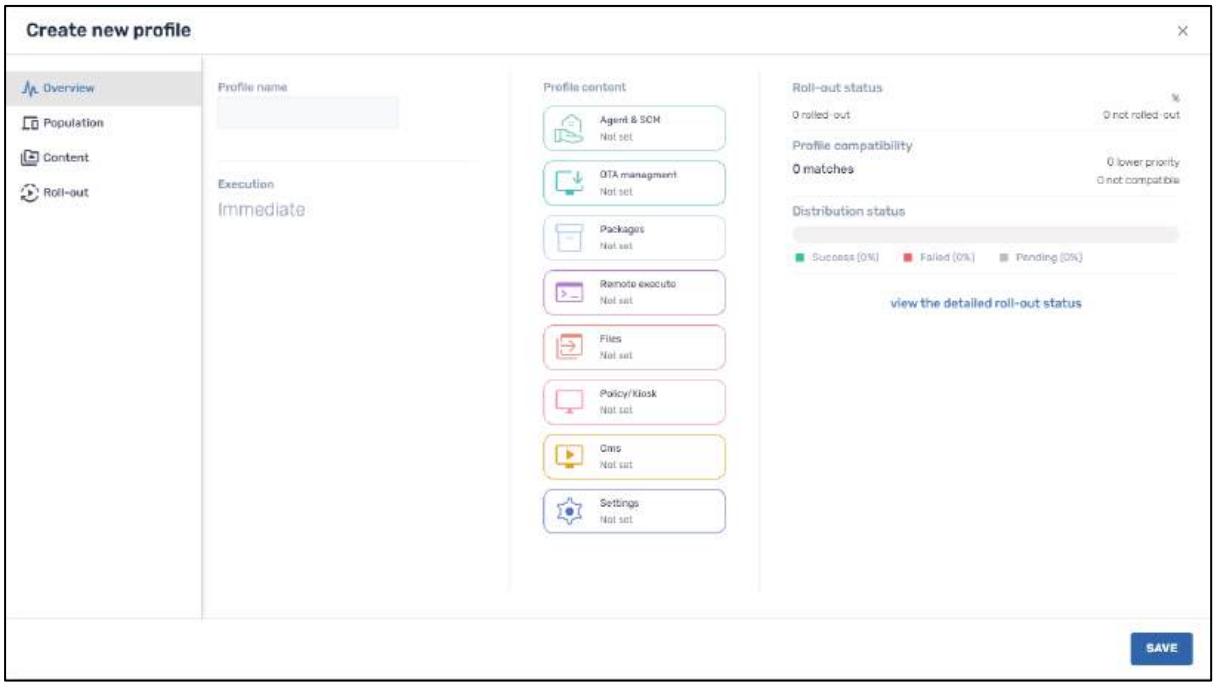
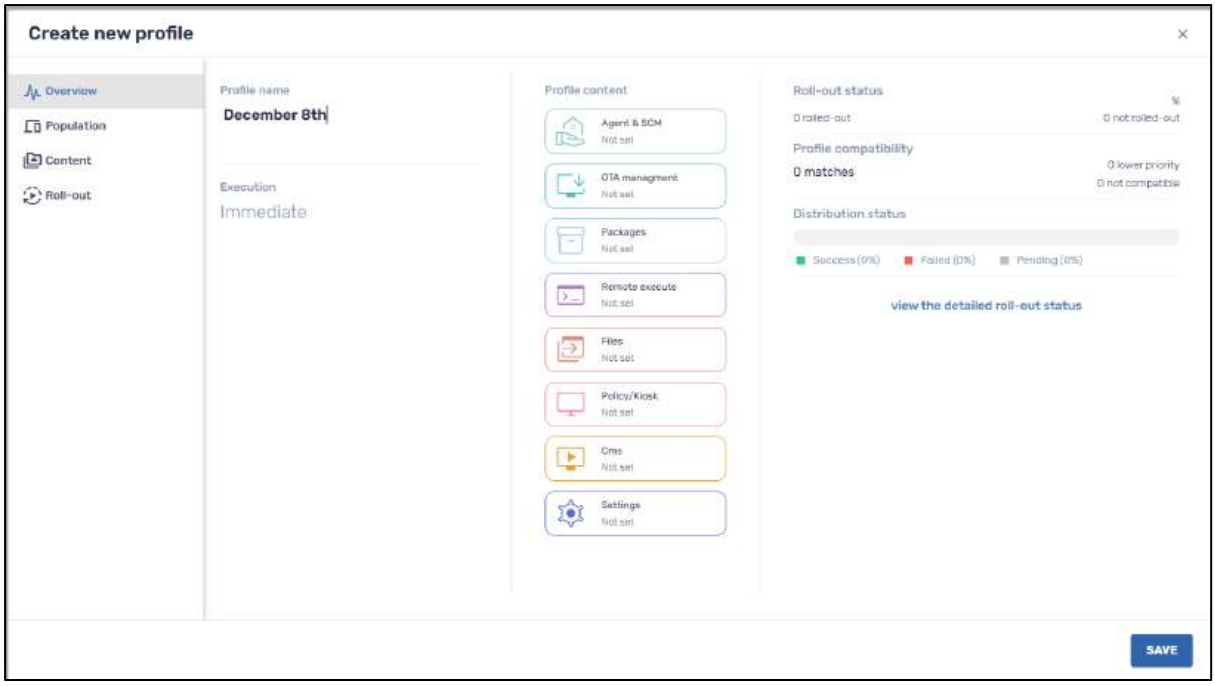


Figure 5-2: Icon for Adding a New Profile

The **Create New Profile** window opens.



2. Supply a name for the profile in the Profile name textbox.



The following table explains the icons on the left-hand side:

Table 5-1:Profiles Console Icons

Icon	Description
Overview	**Overview**: Allows you to provide a name and description of the profile
Population	**Population**: Allows you to populate the profile 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 SC Manager for Android devices • **OTA Management**: Manage Over-the-Air (= OTA) updates • **Packages**: Install software packages • **Remote Execute**: Apply a script to be executed remotely • **Files**: Send files to devices in the profile • **Policy/Kiosk**: Apply a software policy or a kiosk to the devices associated with the profile • **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 profile
Roll-out	**Roll-out**: Allows you to specify a time for applying the execution of the device profile.

Here is a brief description of each of the icons in the sidebar menu:

5.1.1 Overview Panel

The first screen that you see is the **Overview** panel. Once you have finished creating the profile, the Overview panel will display all the profile's parameters at a glance. For example, the Overview panel of the following profile displays:

- The profile name,
- The groups and filters associated with the profile,
- The content of the profile, and
- When the profile will be executed.

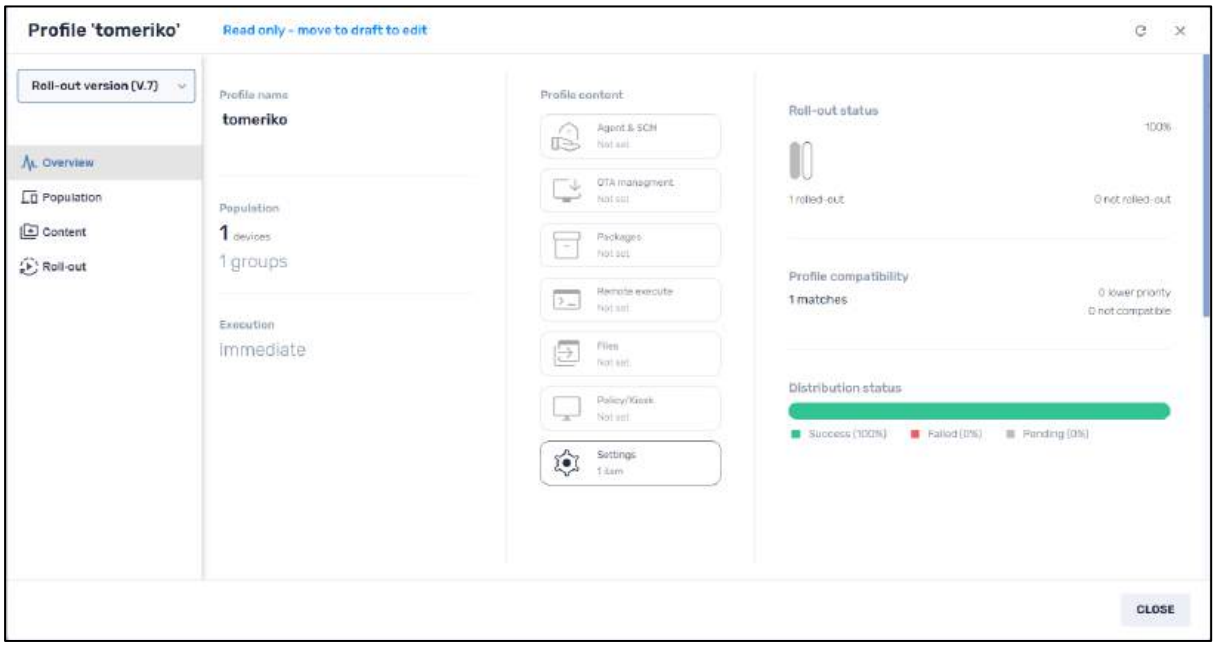
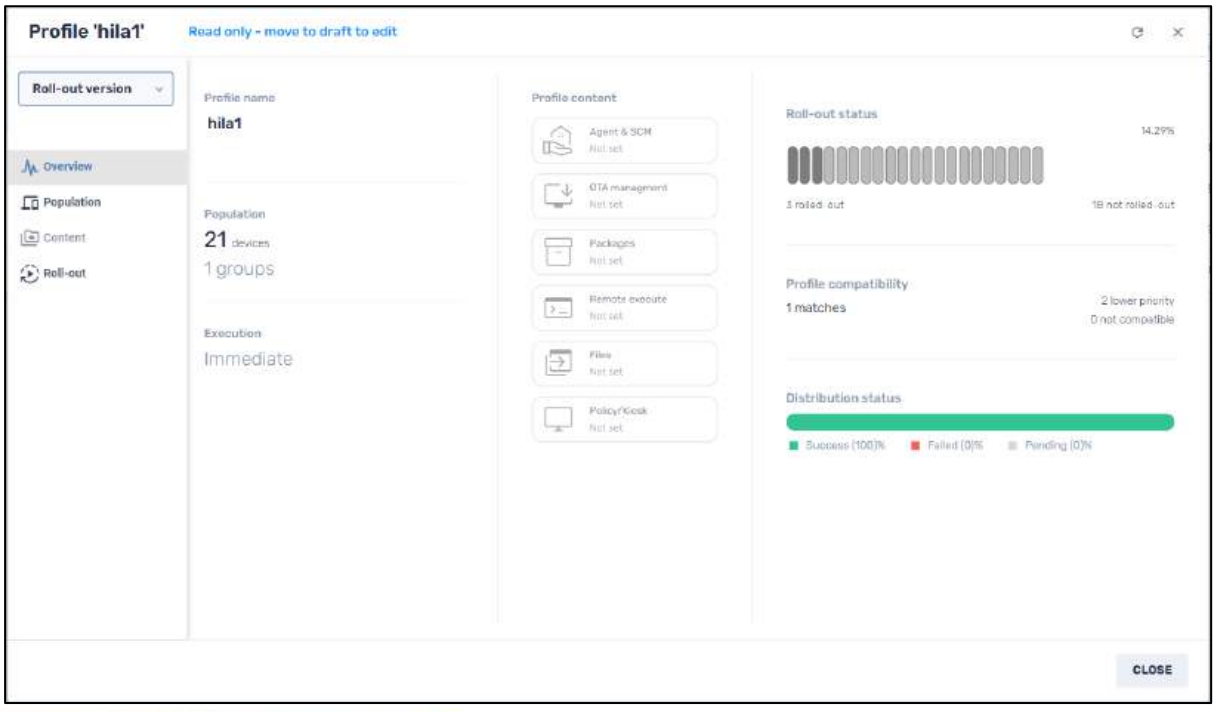


Figure 5-3: Overview Panel of an existing device profile



5.1.2 Population Panel

The Population panel allows you to associate groups of devices with the profile. You can also narrow down the list of devices associated with the profile by adding filters.

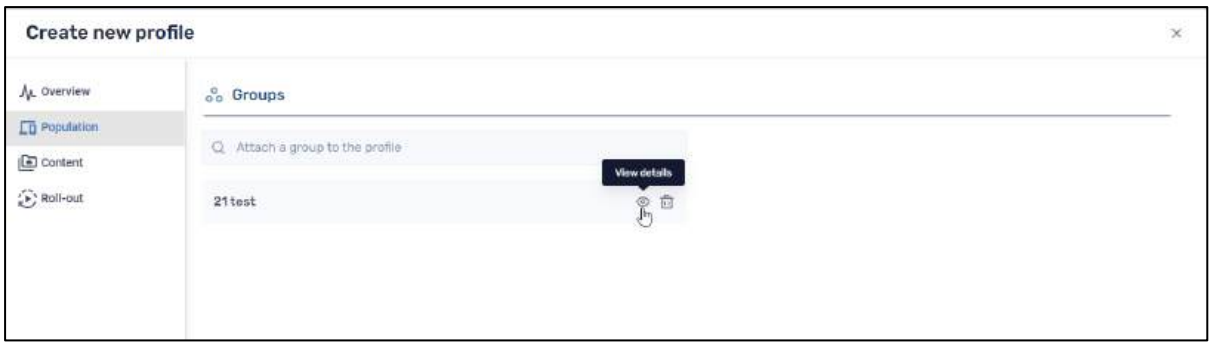
To populate the profile with a group of devices:

1. 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 profile.

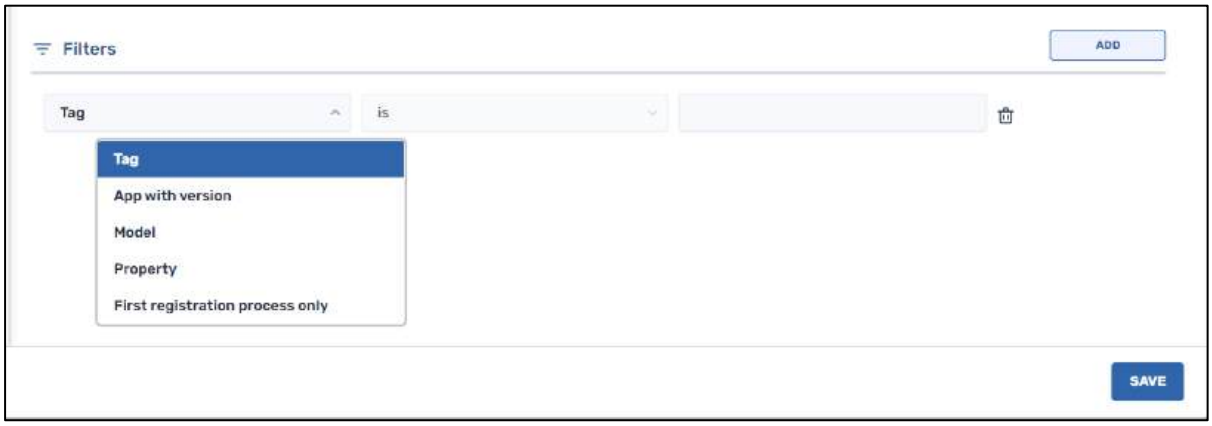
Note: The search is **not** case sensitive. Thus, the search string “Test” will also yield groups containing the string “test”.

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 profile.

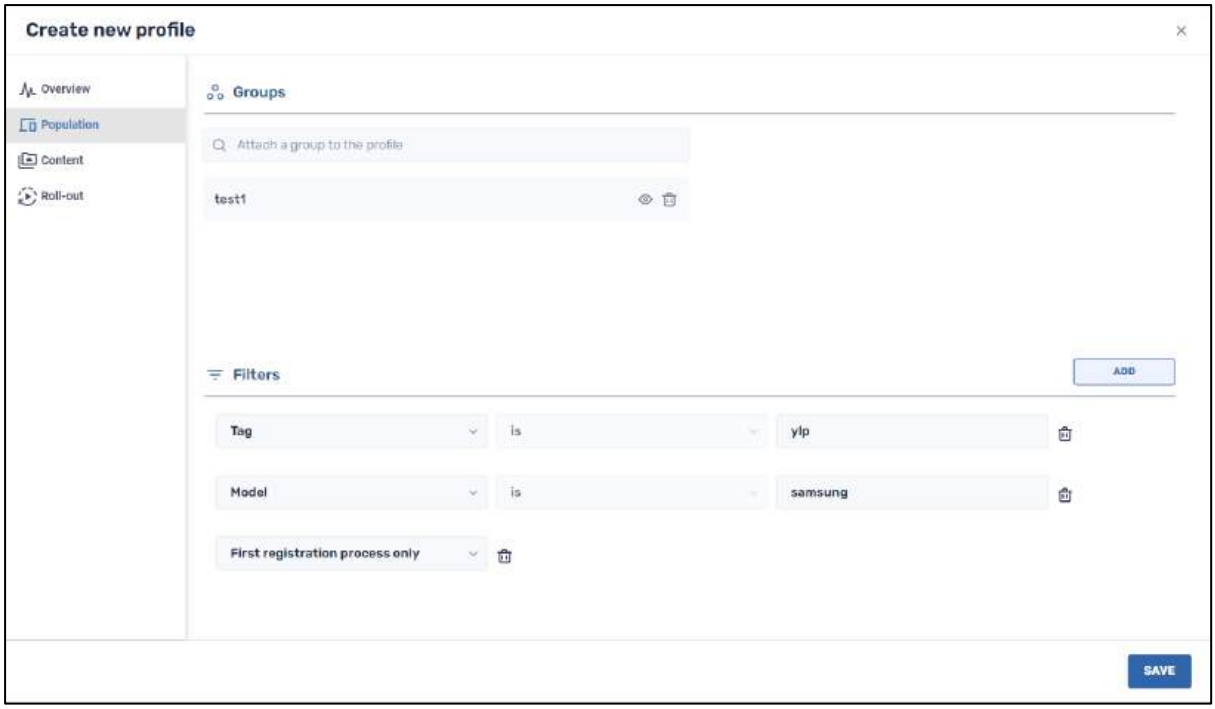
4. If you wish to filter the devices to which the profile will be applied, click on the **Add** button to further refine which devices will be included in the profile.



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 profile.
- **Property**: This allows you to apply a profile to devices with a specific property.
- **First registration process only**: This applies the profile to devices only at the time of their first registration in the Radix Device Manager.

5. You can combine and save several search conditions, to refine the selection of devices in the profile.



5.1.3 Content Screen

When you click on the Content tab, you will have six submenus to specify what content to apply to the devices in the profile you have created:

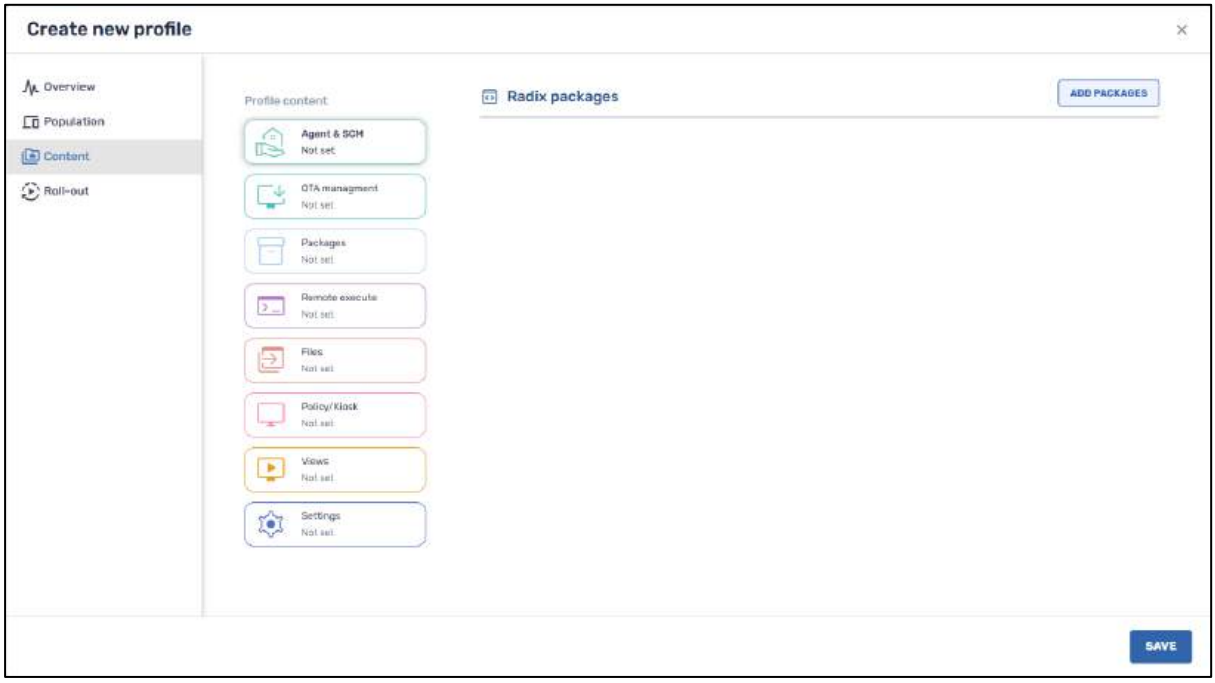


Figure 5-4: Profile Content window, displaying the types of content that can be added

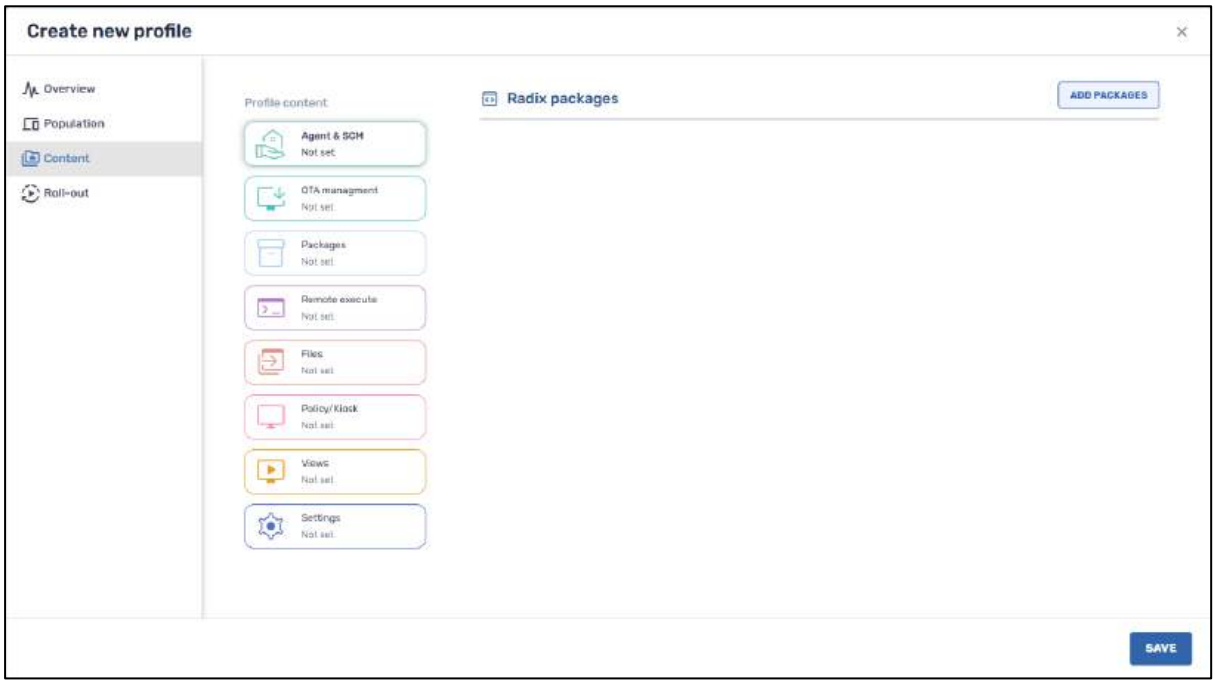
- **Agent & SC Manager**: These include Radix installation files and SC Manager files to be applied to Android devices.
- **OTA updates** to deploy Over-the-Air updates to the devices in a profile
- **Software packages** to be installed

- **Remote Execute** scripts to be executed
- **Files** to be sent to the devices in the profile
- **Policy/Kiosk** items to be assigned to the devices in a profile
- **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 profile

We will examine these content options in turn.

5.1.3.1 Agent & SC Manager

This allows you to attach software packages from the Radix agent and the SC Manager to Android devices to which you apply the profile.



1. When you click on **Add Packages**, you will receive a repository of Radix installation files and SC Manager packages to install on Android devices:

Figure 5-5: Repository of Radix installation files and SC Manager packages

2. You can click on several packages in order to select them. Clicking **Add** in the lower right will add them to the new profile.

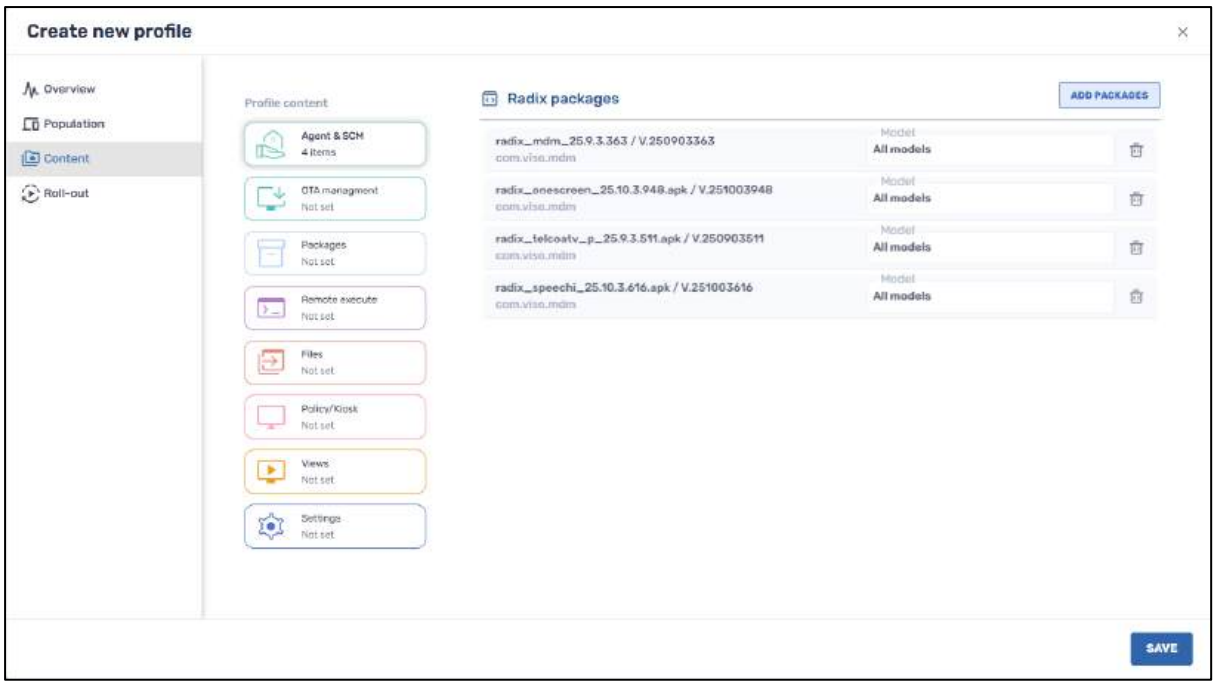
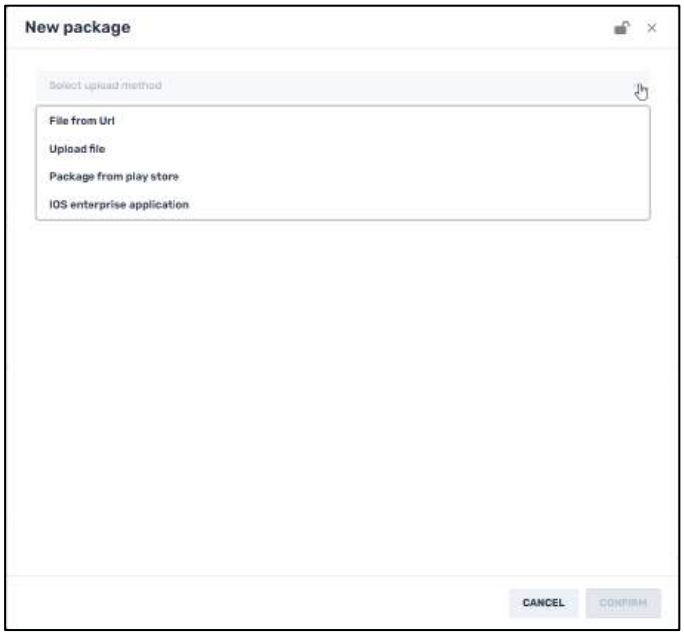


Figure 5-6: Four Radix packages were selected and added to the profile

3. 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 4.1.2.2, Adding a new package to install**.

5.1.3.2 OTA Management

This option allows you to deploy Over-the-Air updates to the devices in a profile. When you click on the **OTA management** tab, the following window opens:

Figure 5-7: Option to apply an OTA update to specific device models

5.1.3.2.1 Adding an Existing OTA Update Package

To add an OTA update to devices in the profile:

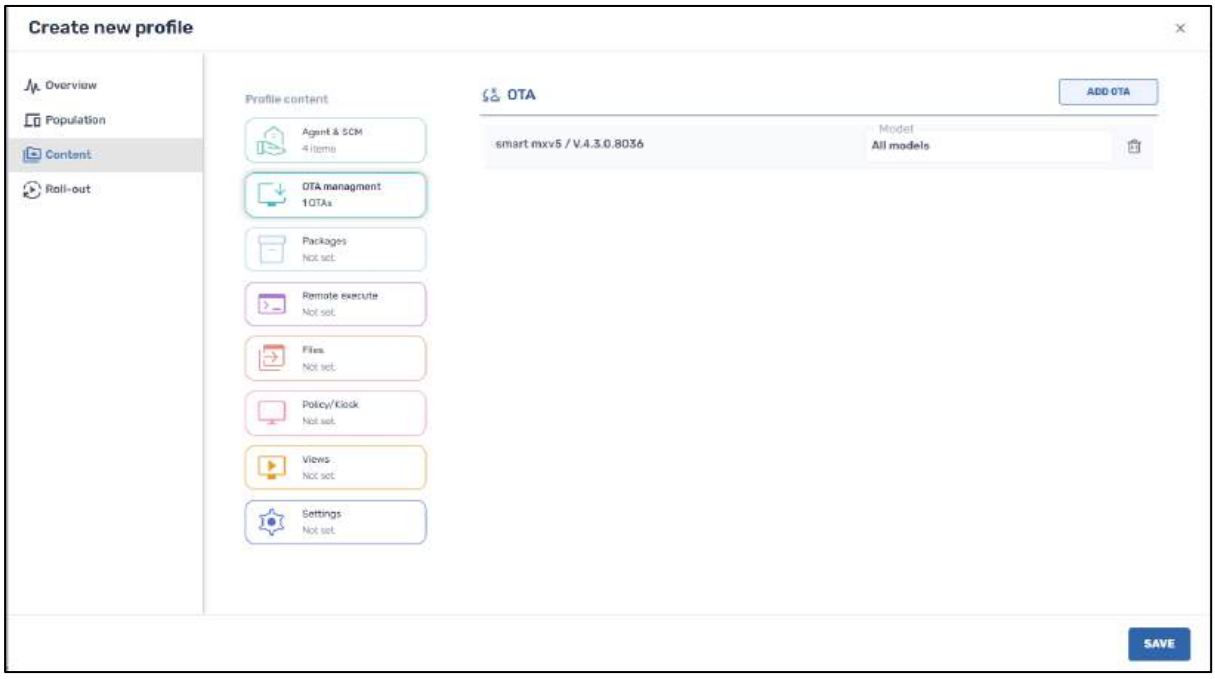
1. Click on **Add OTA** in the upper right-hand corner. The **OTA Update Engine** window opens.

Figure 5-8: OTA window, displaying all OTA update packages

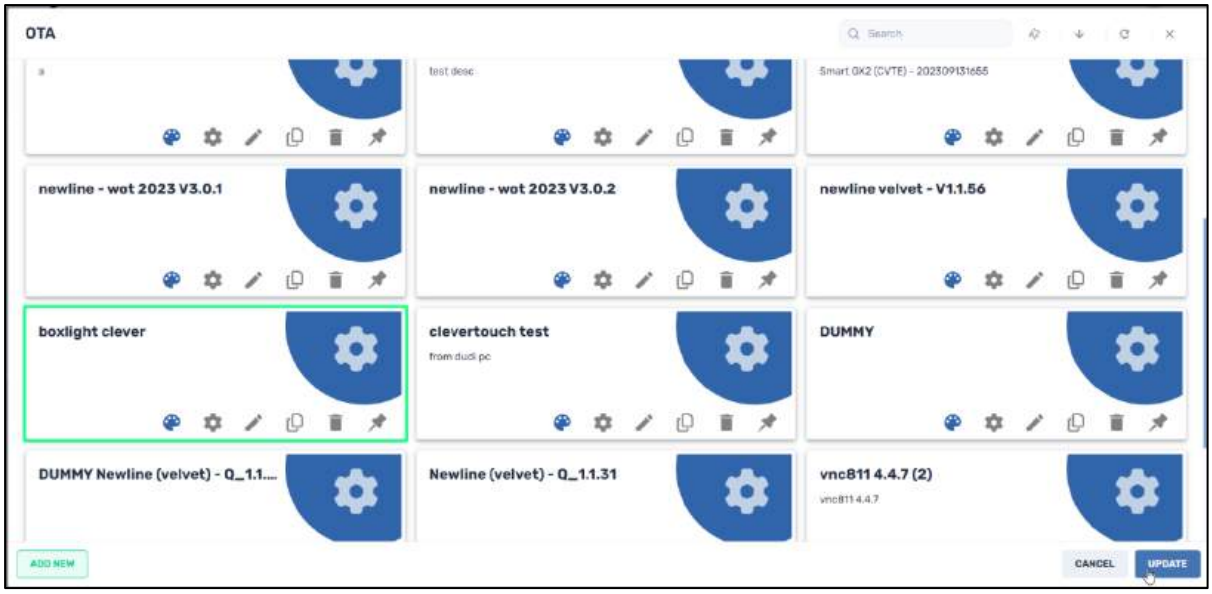
2. Click on one or several existing OTA update packages to select them to be added to the device profile.
3. The **Add** button in the lower right corner becomes active.

Figure 5-9: Four OTA update packages have been selected

4. Click on **Add**. The OTA update packages will appear in the profile.



5. By repeating the process of adding OTA updates, you can later append several OTA updates to a single device profile. The button will appear as "**Update**" instead of "**Add**", if you are modifying an existing profile.



6. 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:

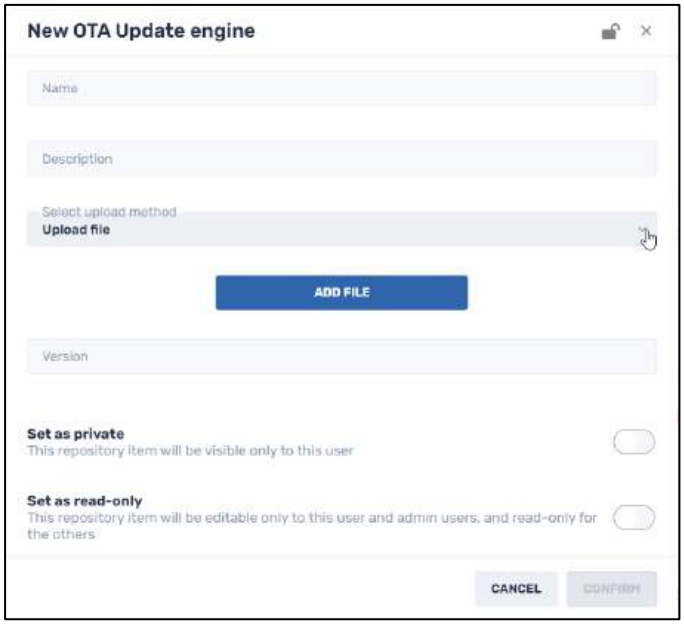
7. Click **Save** to save the addition of the OTA updates to the profile.

5.1.3.2.2 Creating a New OTA Update

The Profile Console also allows you to create a **new** OTA firmware or software update.

To create a new OTA update engine:

1. Click on **Add New** in the lower left-hand corner of the OTA window. The **New OTA Update Engine** window opens.



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.
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 Manager.
4. 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.

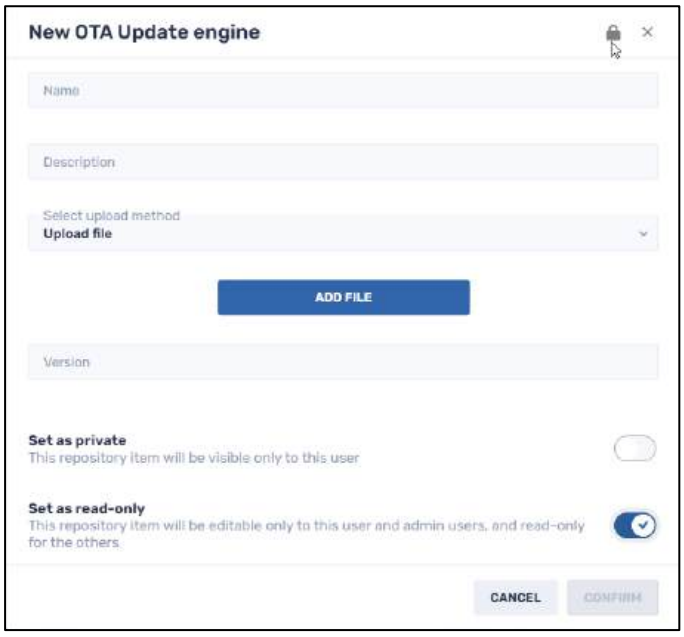


Figure 5-10: Lock icon indicates that the OTA update has been set to read-only

5. Click **Confirm**.

The newly added OTA update will now appear in the list of Profile Groups above.

6. If you wish to remove the group from the profile, click on the **Remove** icon to have it removed.

7. Click **Save** to save the OTA update option for your profile.

5.1.3.3 Packages

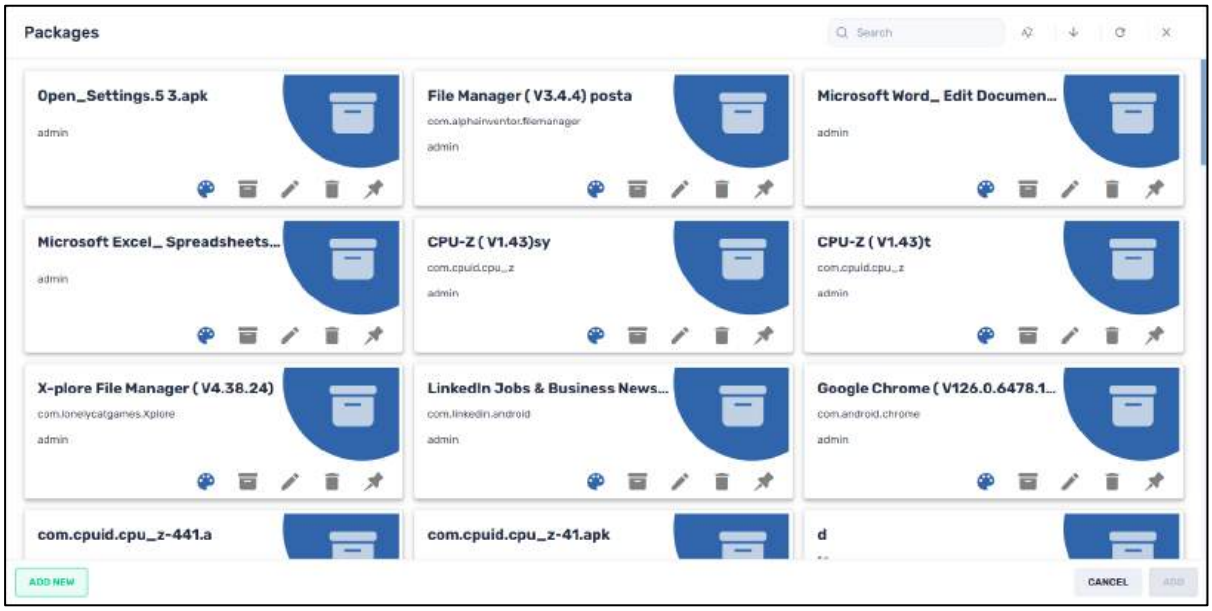
This provides you with a list of software packages that you can apply to the devices in the profile. If a group is assigned to this profile in the future, the software packages will also apply to that group.

5.1.3.3.1 Adding an existing software package

When you click on the Packages tab, the following window opens:

To add a software package to the profile of devices:

1. Click on **Add Packages**. The **Packages** repository opens.



2. Select one or several software packages to be added to the profile by clicking on the tiles. The **Add** button in the lower right corner becomes active.

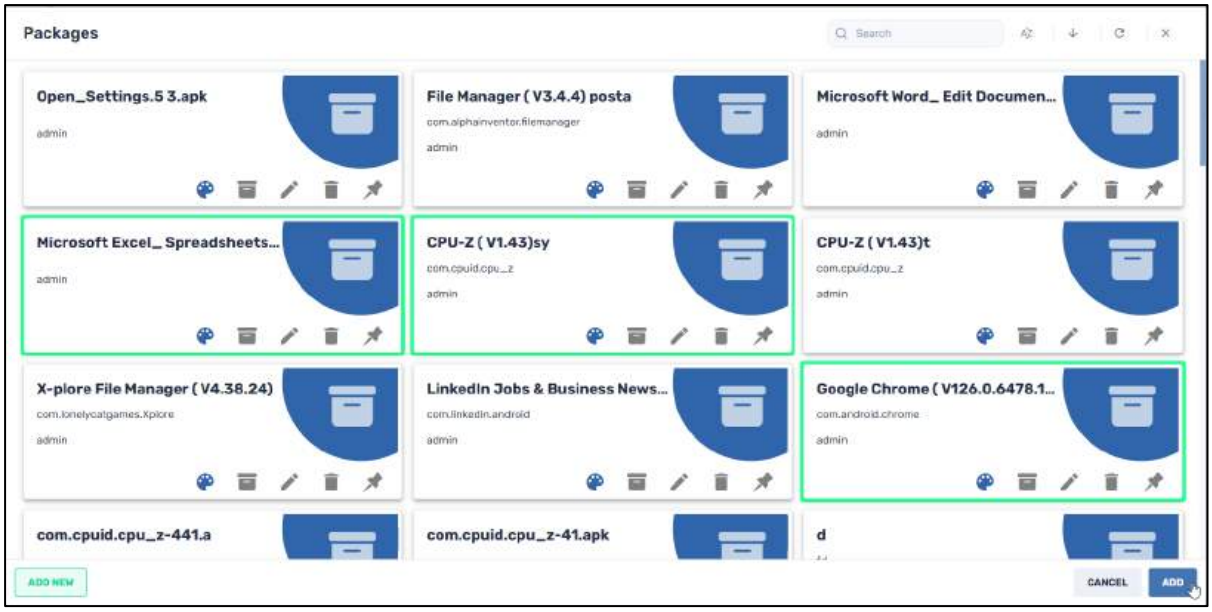
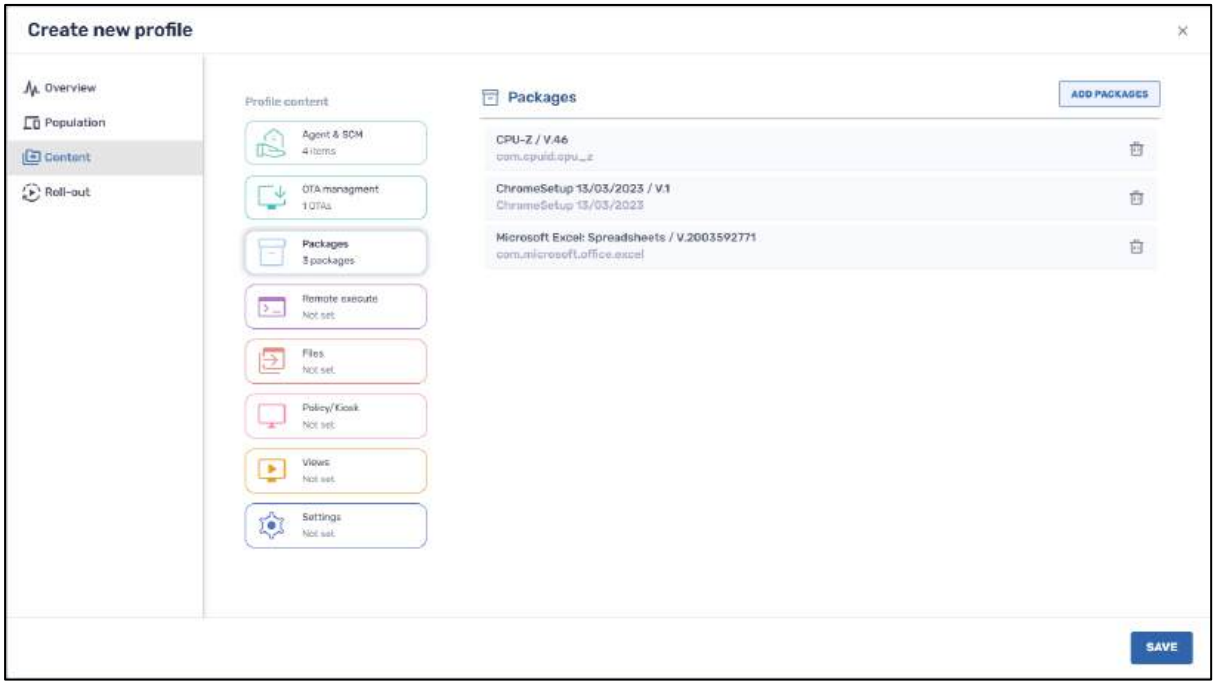


Figure 5-11: Selecting the Windows 10 simulator, X-plore, and Plex software packages to be applied to devices in the profile

3. Click **Add**. The software package(s) you selected will now appear in the profile.



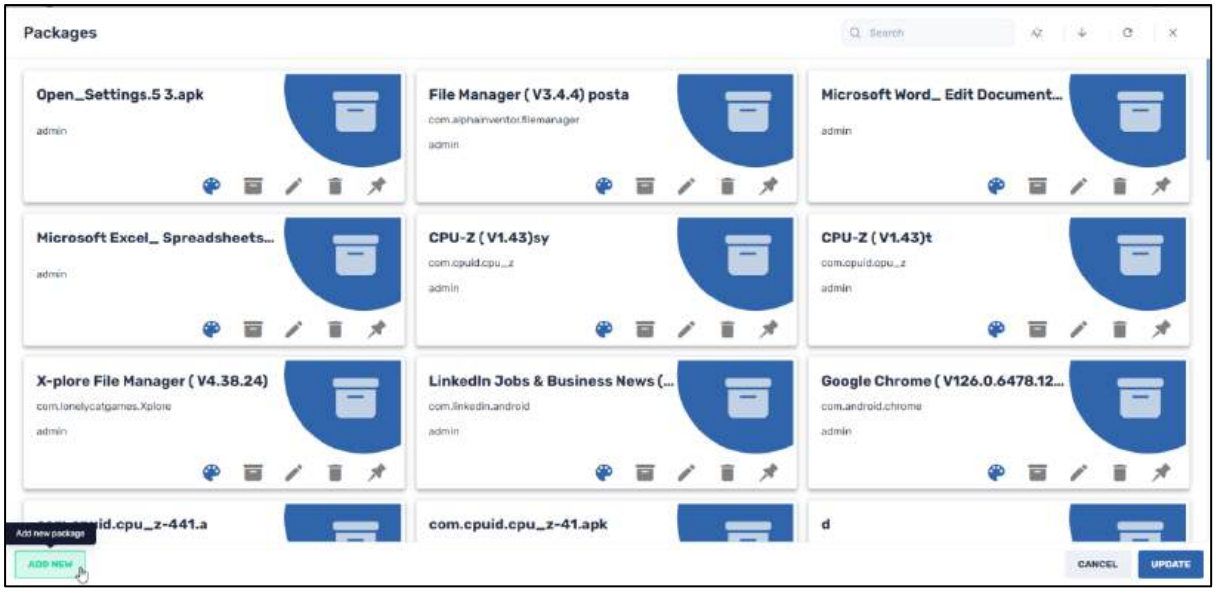
4. Click **Save** to store your selection in the device profile.

5.1.3.3.2 Adding a new software package

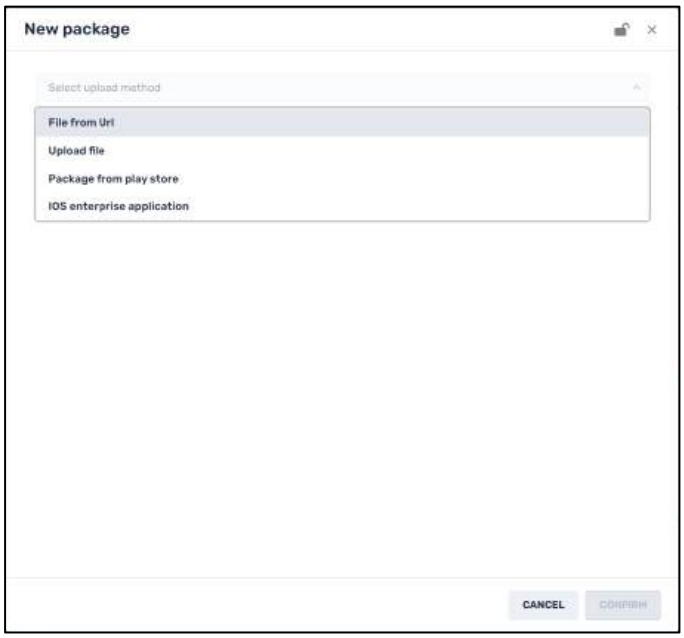
There is also an option to add a software package that does not appear yet in the Packages repository.

To add a new software package to the repository:

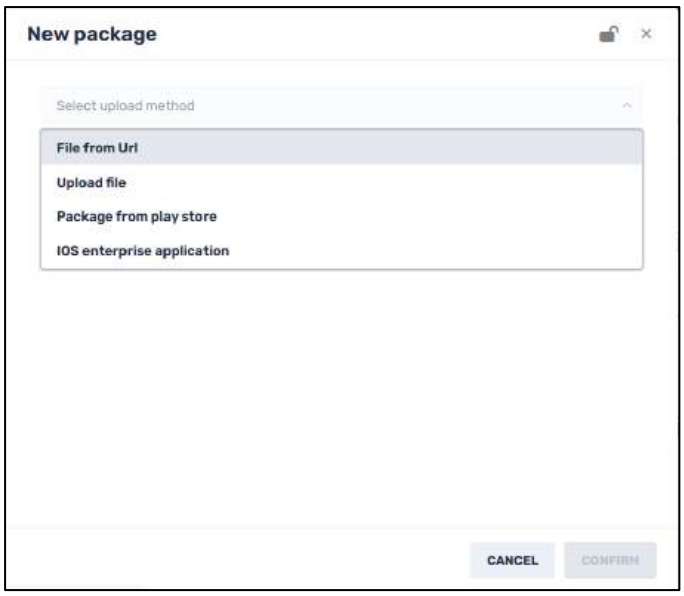
1. In the Packages screen, click **Add New**.



The **New Package** window opens.



2. Select one of the upload methods for the software package you would like to add to the profile: From a URL, uploaded from your computer, a package from the Google Play Store, or an iOS Enterprise Application.



3. Proceed as in **Section 4.1.2.2**, regarding adding a new software package.
4. Upon selecting a software package to apply to the devices, click **Save**.

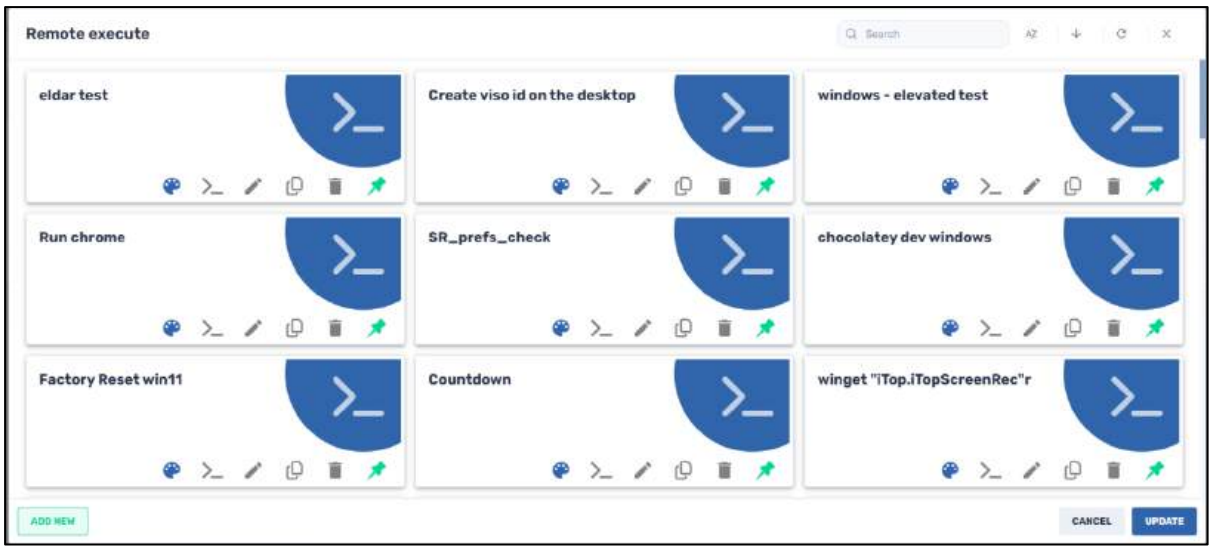
5.1.3.4 Remote Execute

There is also the option to apply a Remote Execute command line script to a profile.

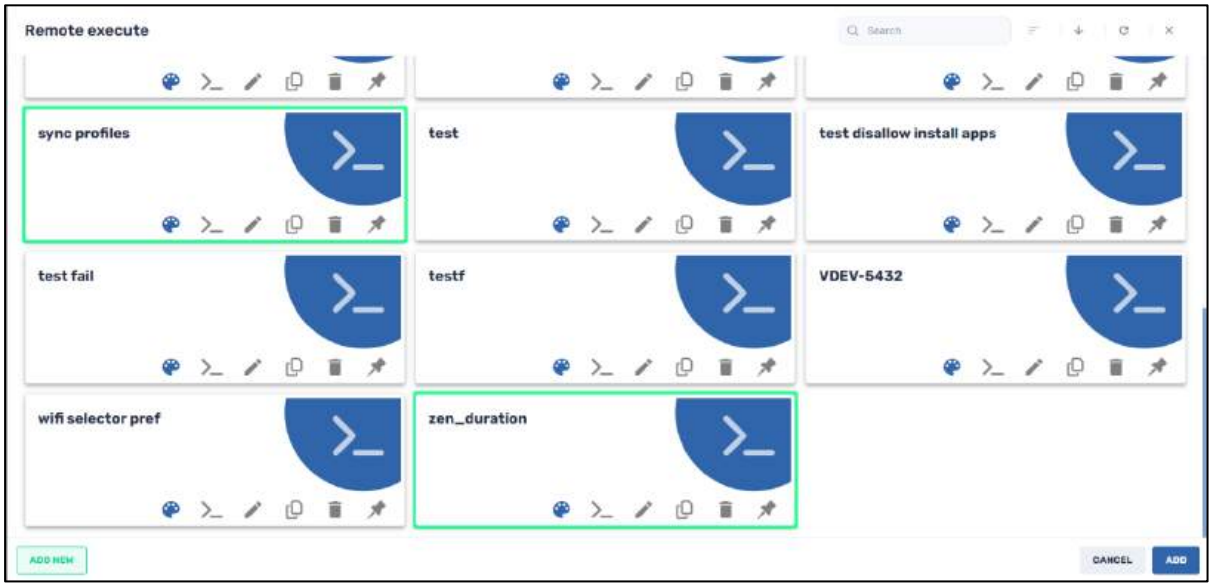
To apply a Remote Execute command:

1. Click on the **Remote Execute** button and click on **Add Items**.

The **Remote Execute** repository window opens.

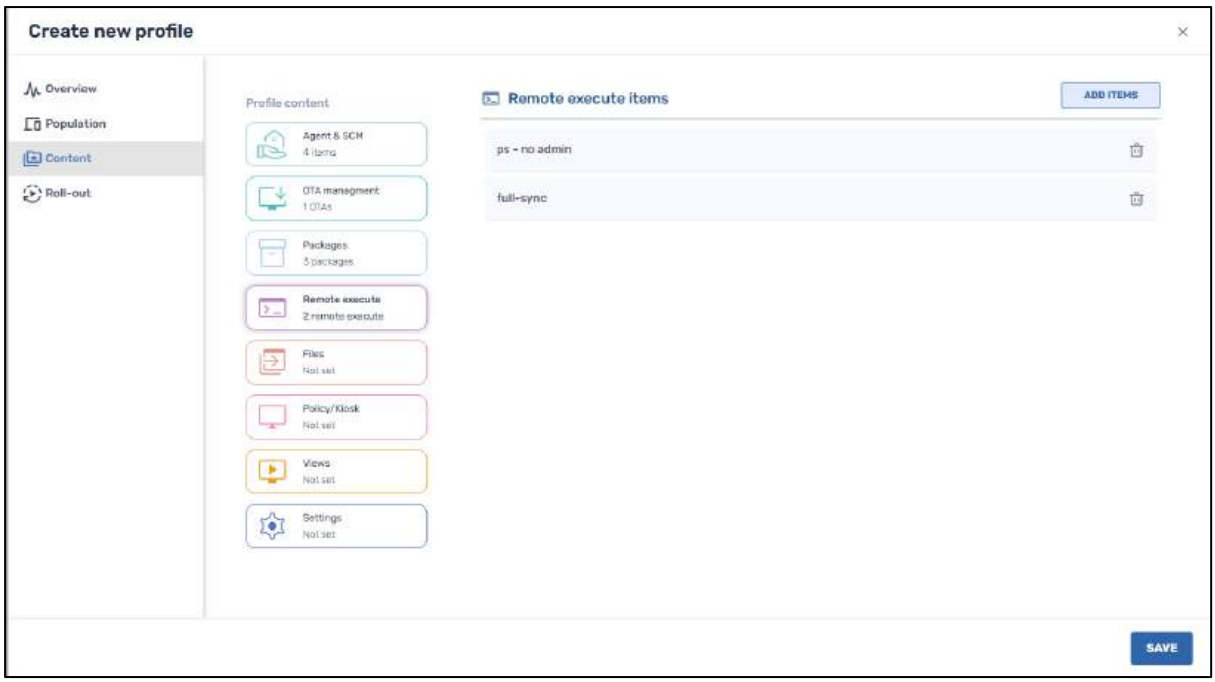


2. Click on one or more of the listed remote execute scripts to attach them to the profile and click **Add**.



If you wish to create a new remote execute script, refer to **Section 4.2.1.12, Remote Execute**.

3. After adding the Remote Execute script, the selection will appear in the **Profile** window.



4. Click **Save** to save your selection.

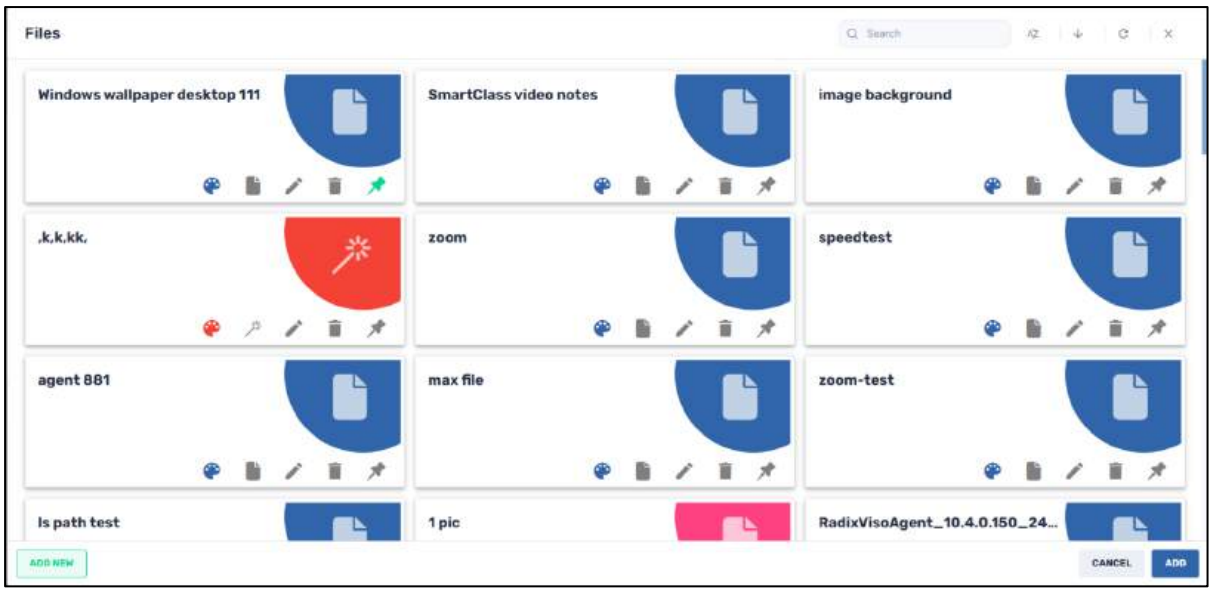
5.1.3.5 Files

This allows you to send files to the devices in the profile.

To add files to the devices in a profile:

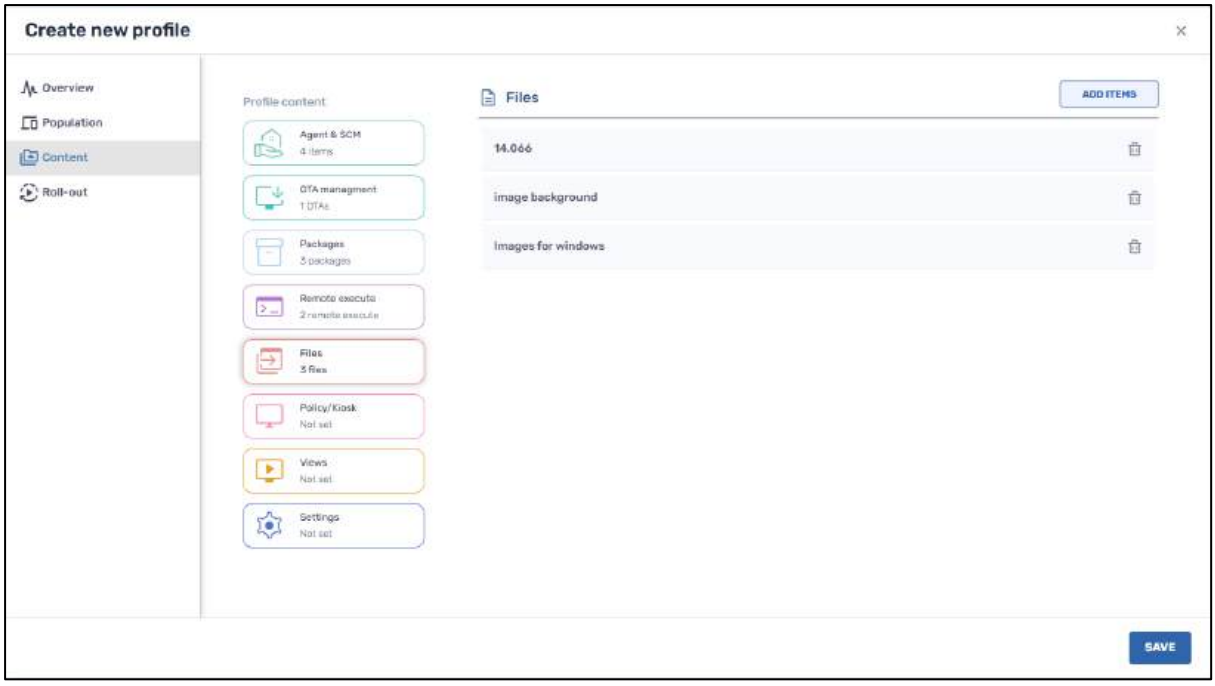
1. Click on the **Files** tab to open the Files window.

2. Click **Add Items**. The Files repository will appear.



By clicking on the tiles, you can select one or several of the files. In the example below, we have selected three files from the Files repository to be uploaded to the profile.

3. Click **Add** or **Update** when you have finished your selection. The selected file(s) will be added to the device profile. All the devices in the profile 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 profile.

5.1.3.6 *Policy/Kiosk*

Under the Policy/Kiosk tab, you will be able to add a software policy or kiosk to the device profile.

- Regarding policies, refer to **Section 4.1.5, Policies**.
- Regarding using a device in a kiosk display, refer to **Section 4.2.1.8, Kiosk.**

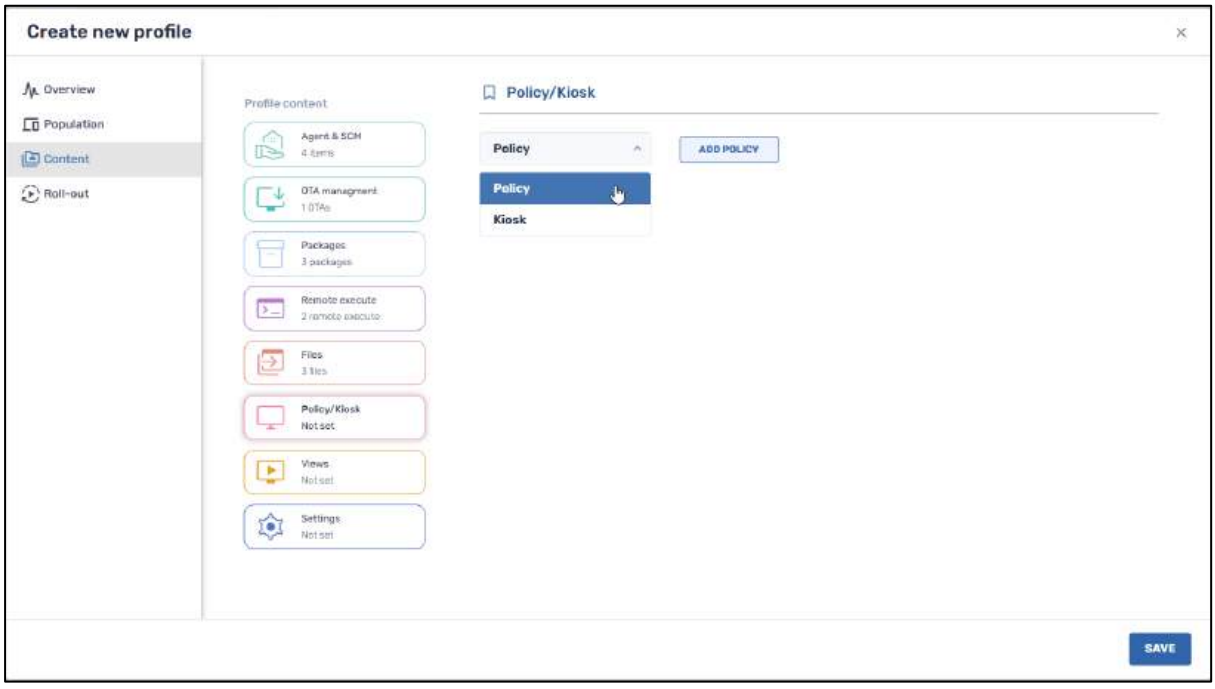


Figure 5-12: The user has selected the Policy option

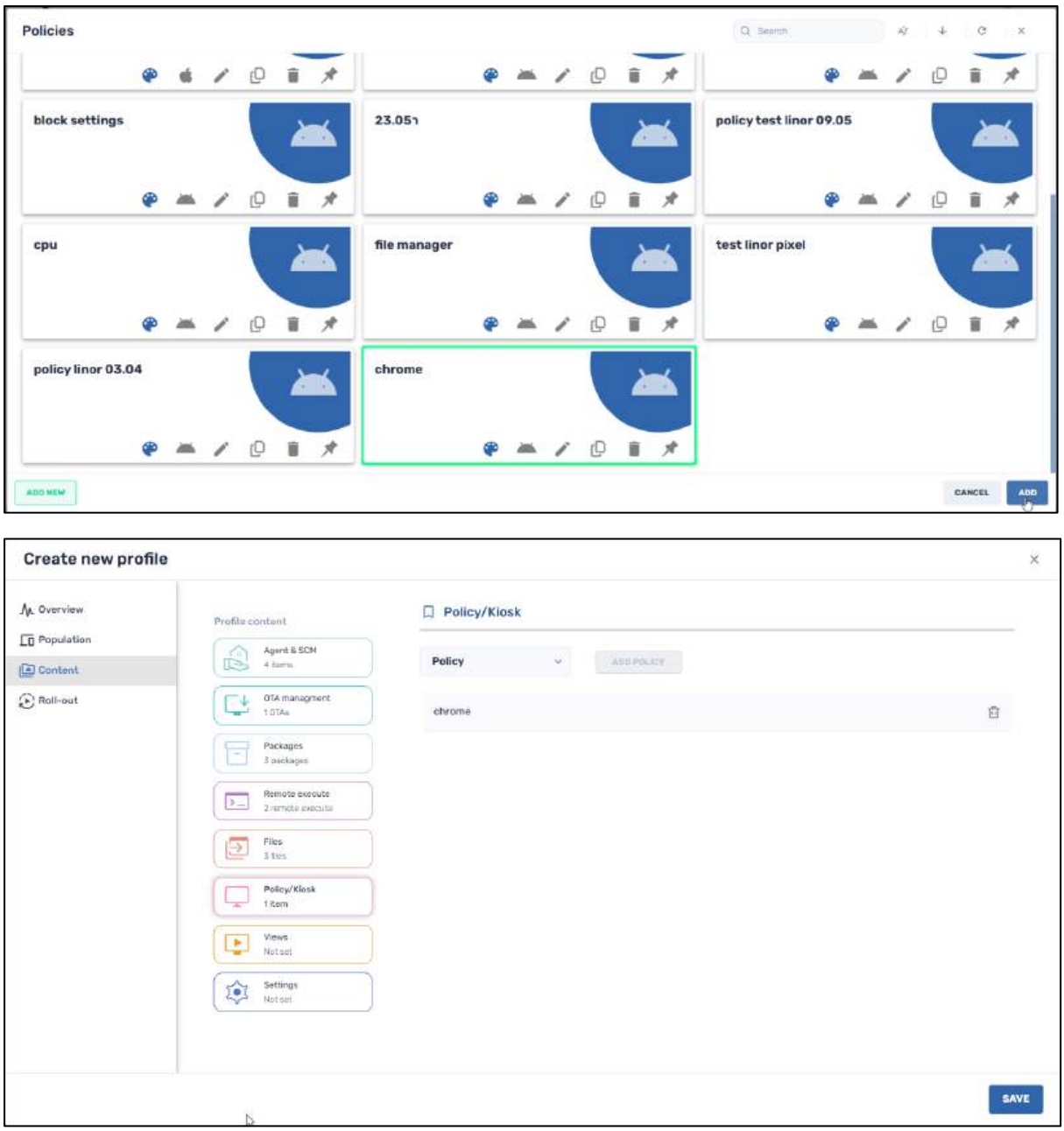


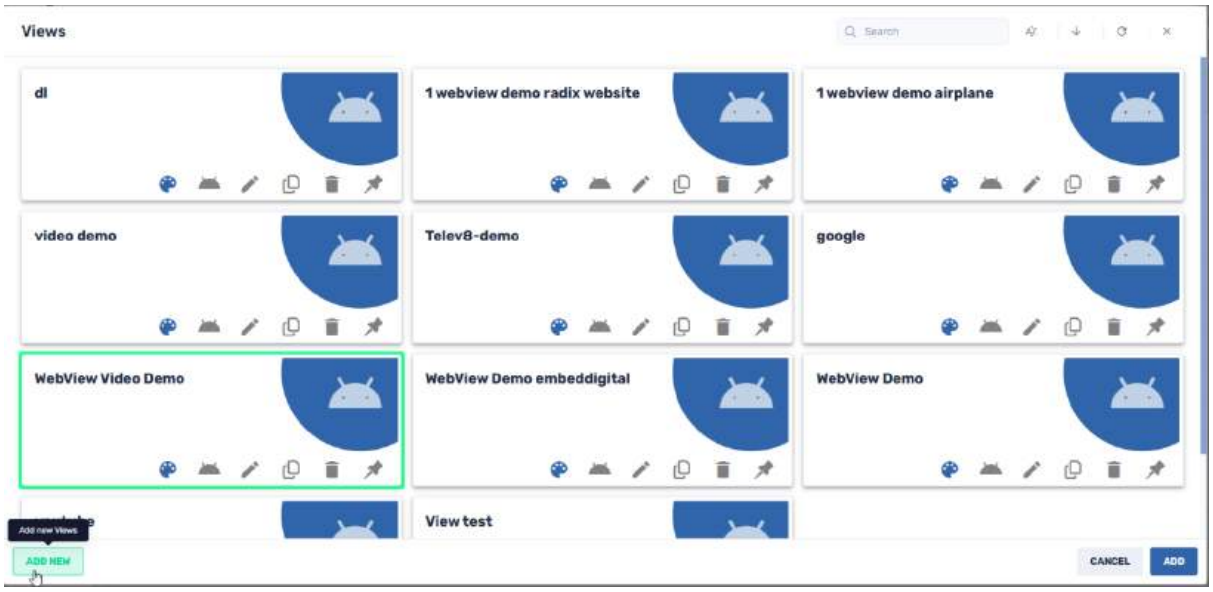
Figure 5-13: The user has selected the Chrome browser to be on the list of blocked apps

5.1.3.7 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:



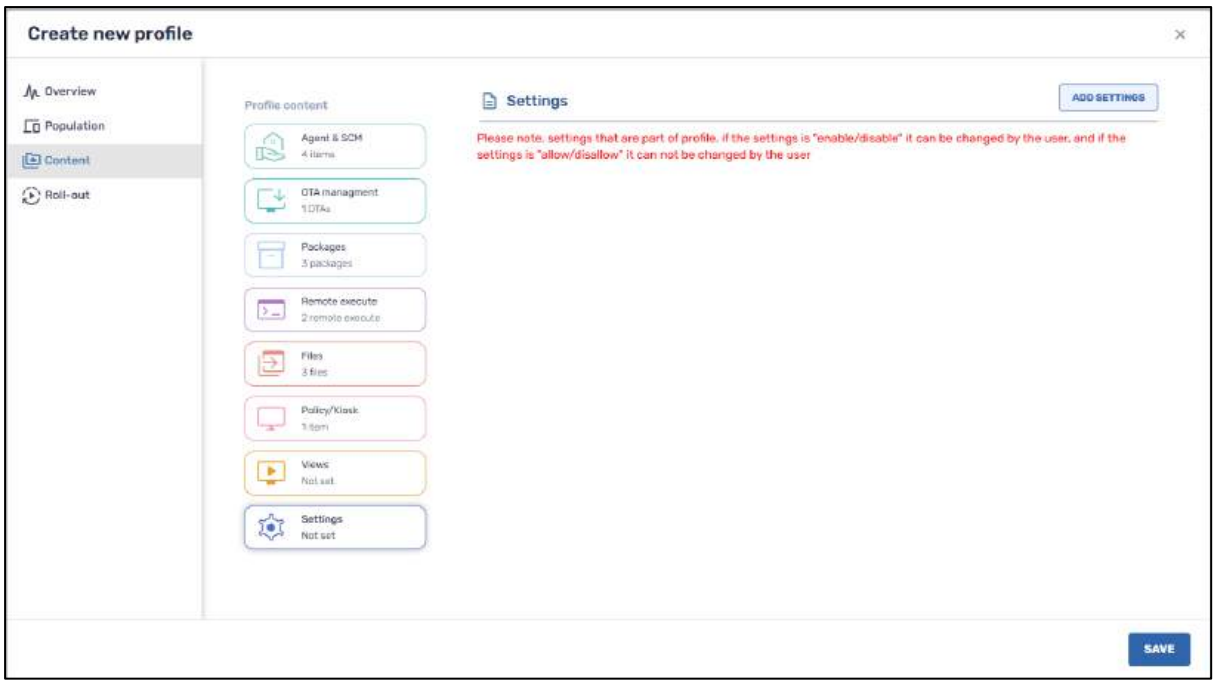
You can select a view option from the repository, or click on **Add New** in the lower left, to create a new View option. Creating a new View option is treated in **Section 4.2.1.23**.

5.1.3.8 Settings

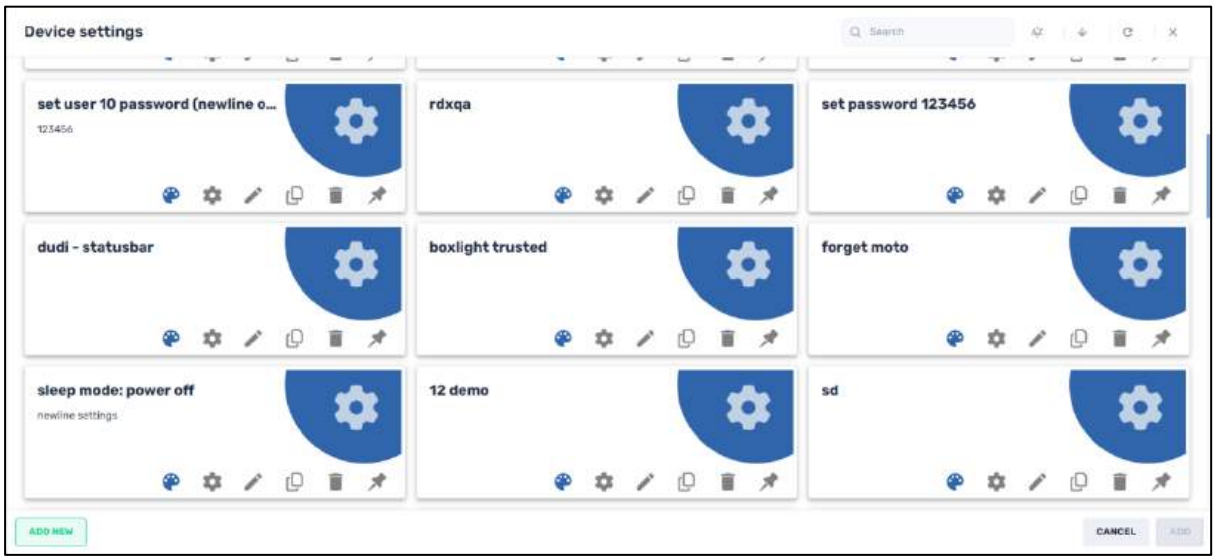
This allows you to modify device settings to the devices in the profile.

To adjust device settings to the devices in a profile:

1. Click on the **Settings** tab to open the Settings window.



2. Click on **Add Settings**. The Device Settings window opens.

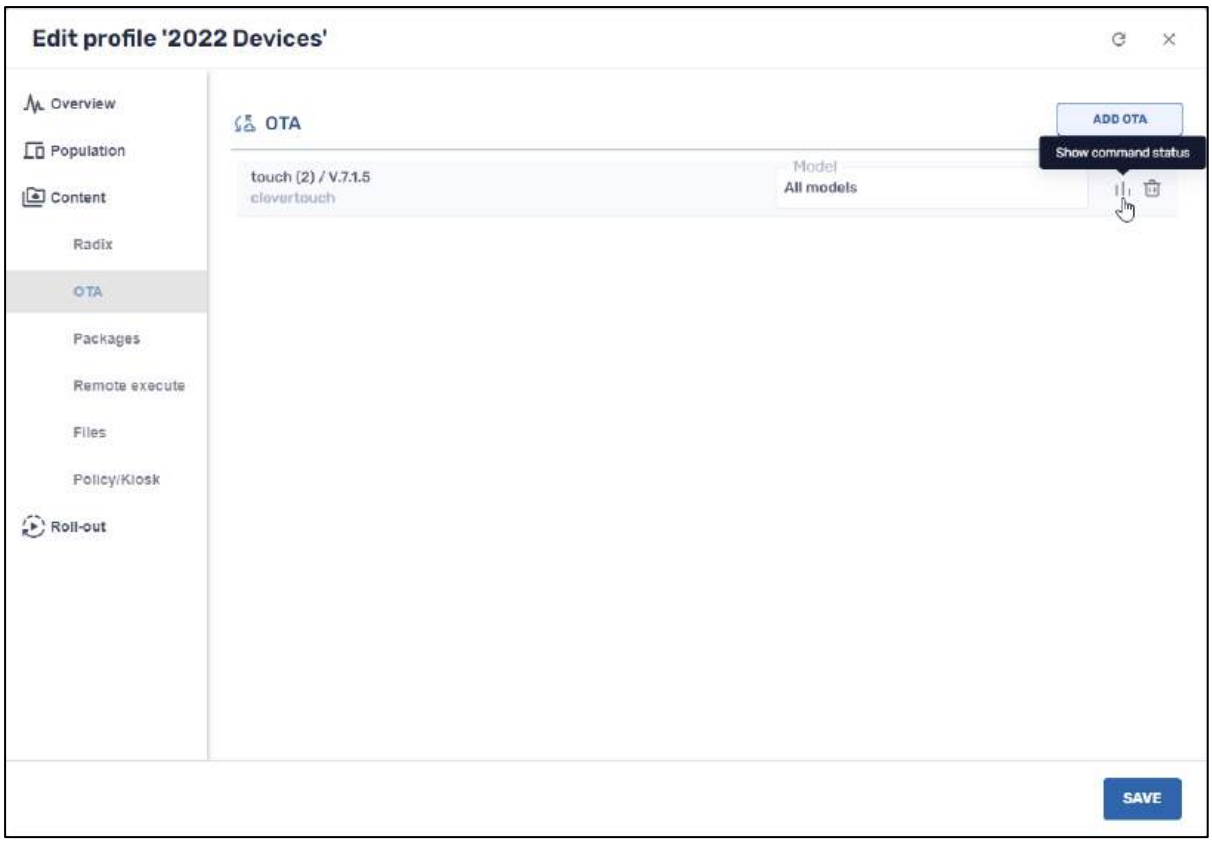


3. Proceed as in **Section 4.1.4, Device Settings**, to apply device settings that already appear in the Device Setting repository, or to create a new device setting.

5.1.4 Command Status View Option

Note that there are two icons next to each of the six content options:

- **Show Command Status**: This displays when the OTA update will be applied to the devices in the profile, 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.



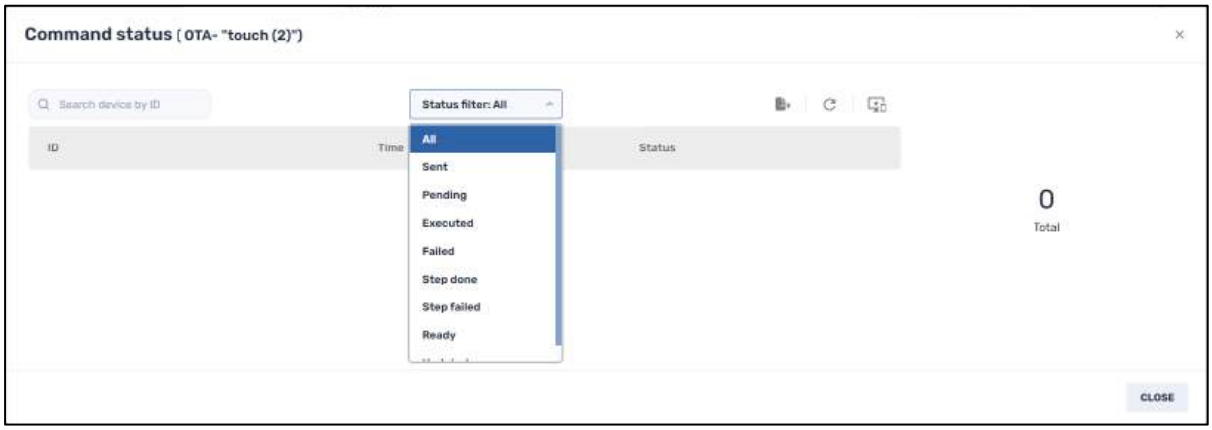


Figure 5-14: Command status of an OTA update applied to a device profile

5.1.4.1 Removing a Content Item from a Profile

If you wish to delete a content item from a device profile, click on the **Remove** icon next to that item:

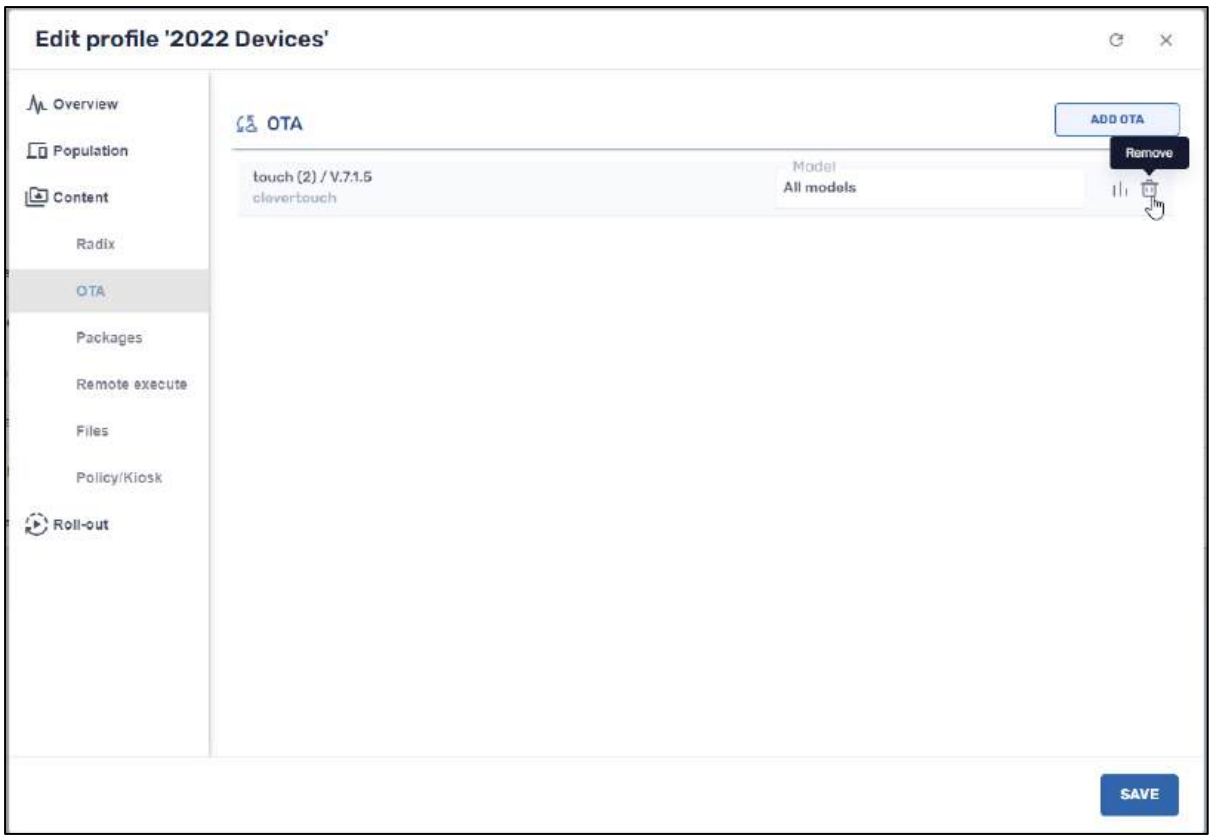
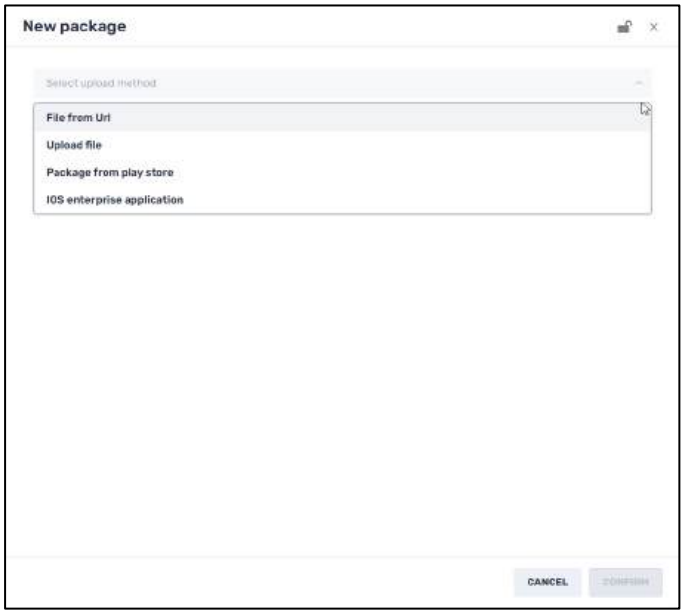
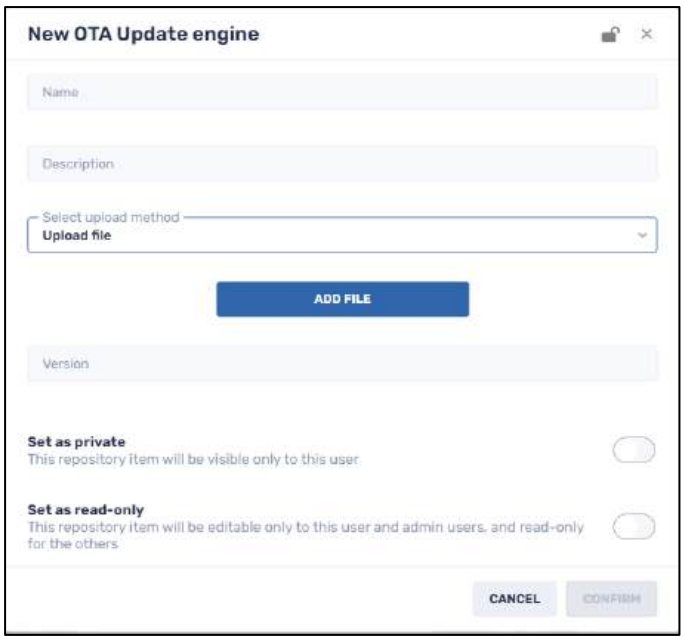


Figure 5-15: Radix packages that you can apply to remote devices

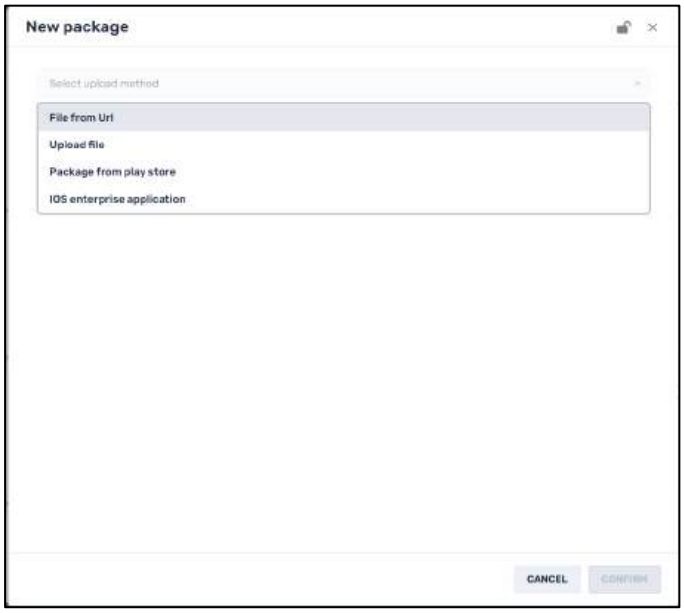
If you wish to add a Radix software package, click on **Add New**. You will have the options of downloading a software package from an URL, uploading a file from your computer, getting an installation package from the Google Play Store, or an iOS enterprise application.



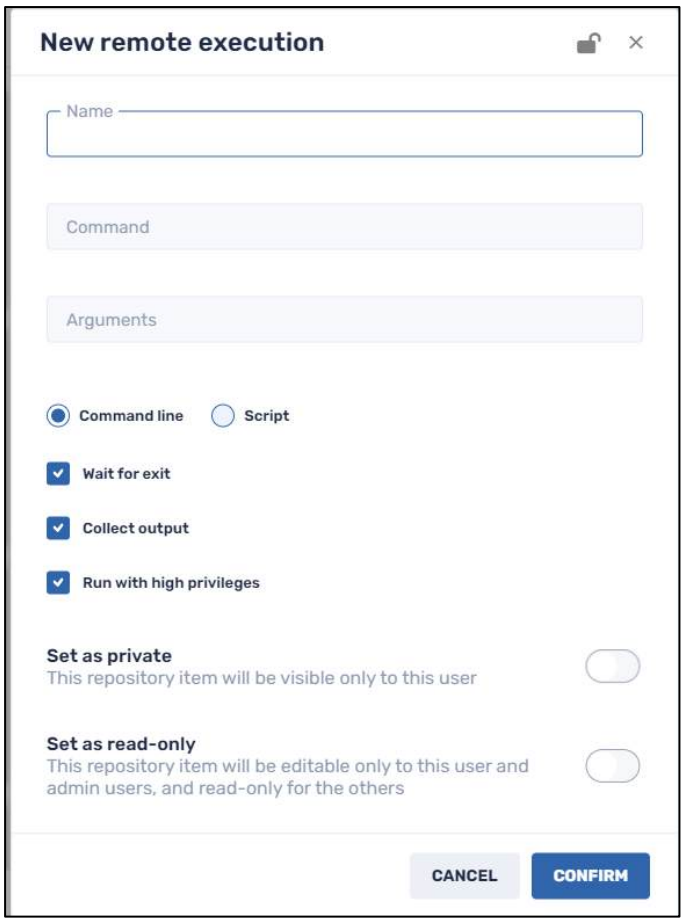
- **OTA update engine management**: This allows you to upload an Over-the-Air update file for the remote devices.



- **Packages**: This will allow you to add software packages to the devices in the profile.



- **Remote execute**: This allow you to add command line commands and scripts to be executed on the remote devices.



- **Files**: This option allows you to select files to be sent to the devices in the profile
- **Policy/Kiosk:** To either create a software policy of allowed or blocked applications, or to limit a device to a fixed number of options, to function in Kiosk mode

5.1.5 Roll-out

The Roll-out window allows you to specify when to execute the details of a profile.

The Roll-out window is divided into two sections:

- Roll-out configuration
- Execution configuration

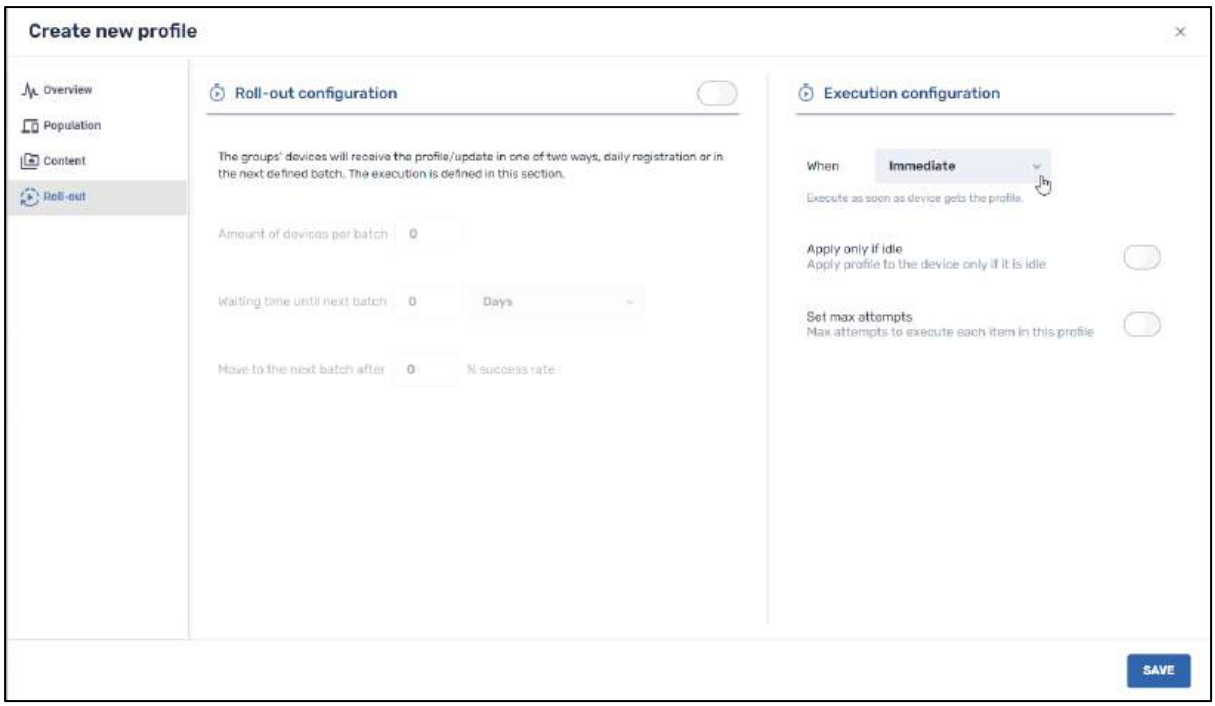


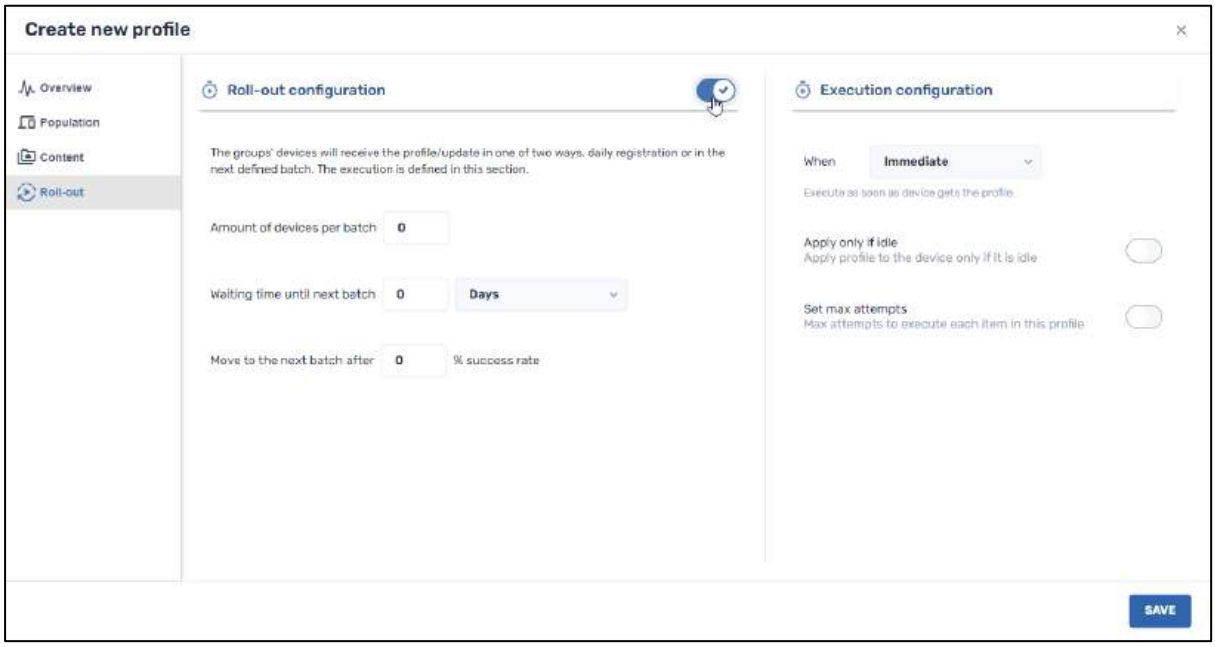
Figure 5-16: Layout of Roll-out Window

5.1.5.1 Roll-out configuration

The **Roll-out configuration** pane lets you allocate batches of devices to which to assign the profile.

To use the roll-out configuration options:

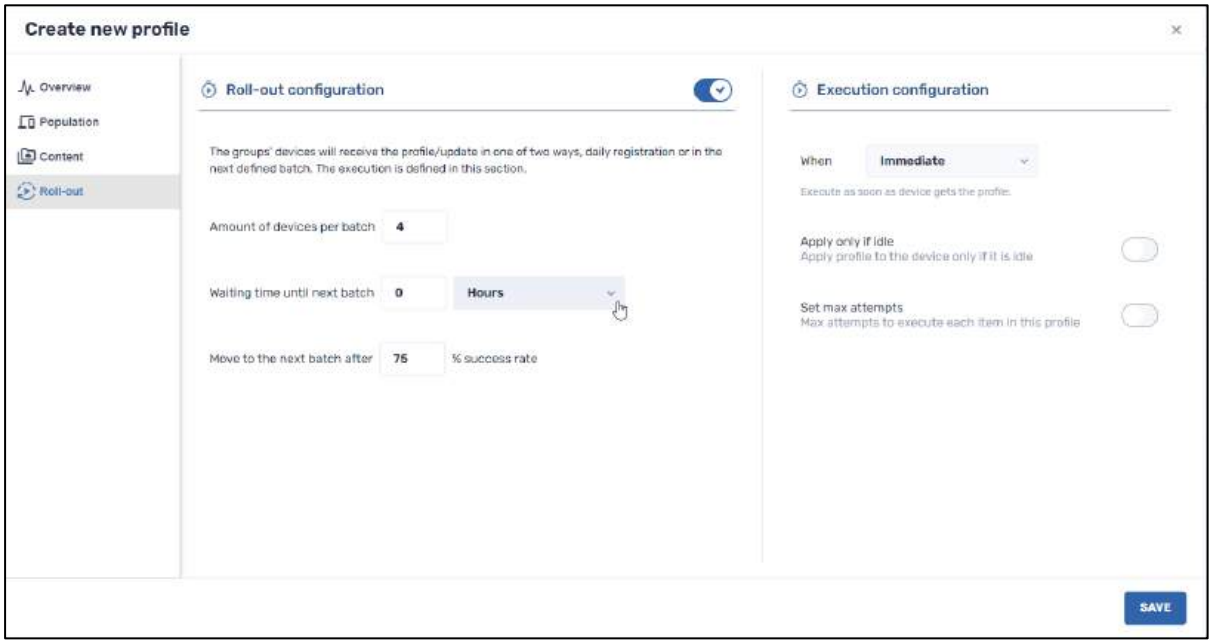
1. Click on the **Roll-out** tab and click on the button at the top of the Roll-out configuration pane.



The batch options are now active.

2. You can assign the following parameters:

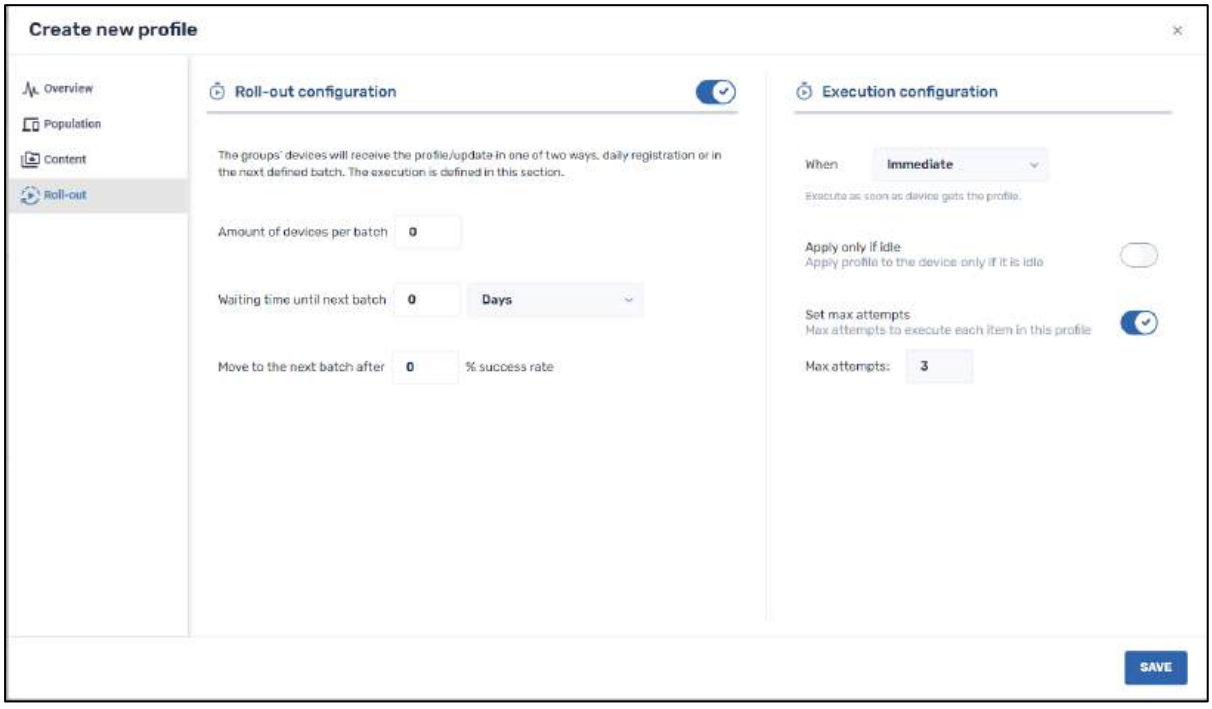
a. The number of devices per batch
b. The waiting time between batches, in units of hours or days
c. The success rate of proper execution of the profile, before proceeding to the next batch of installations.



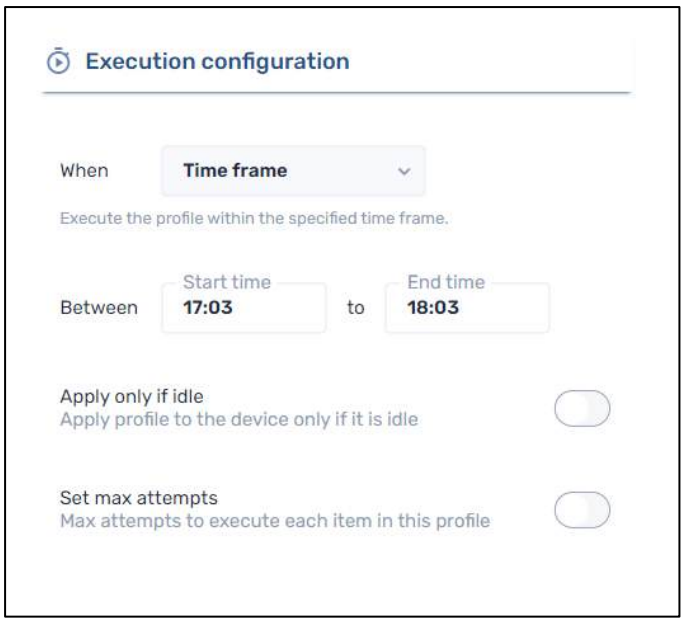
5.1.5.2 *Execution configuration*

In this pane, you set the time when you want the device profile to be executed on the specified devices. There are three options:

- **Immediate**: The profile will be implemented as soon as the device gets the profile.



- **Time frame**: You can assign a start time and end time between which the profile should be executed.



- **On demand**: The profile will only be executed when you initiate it manually.

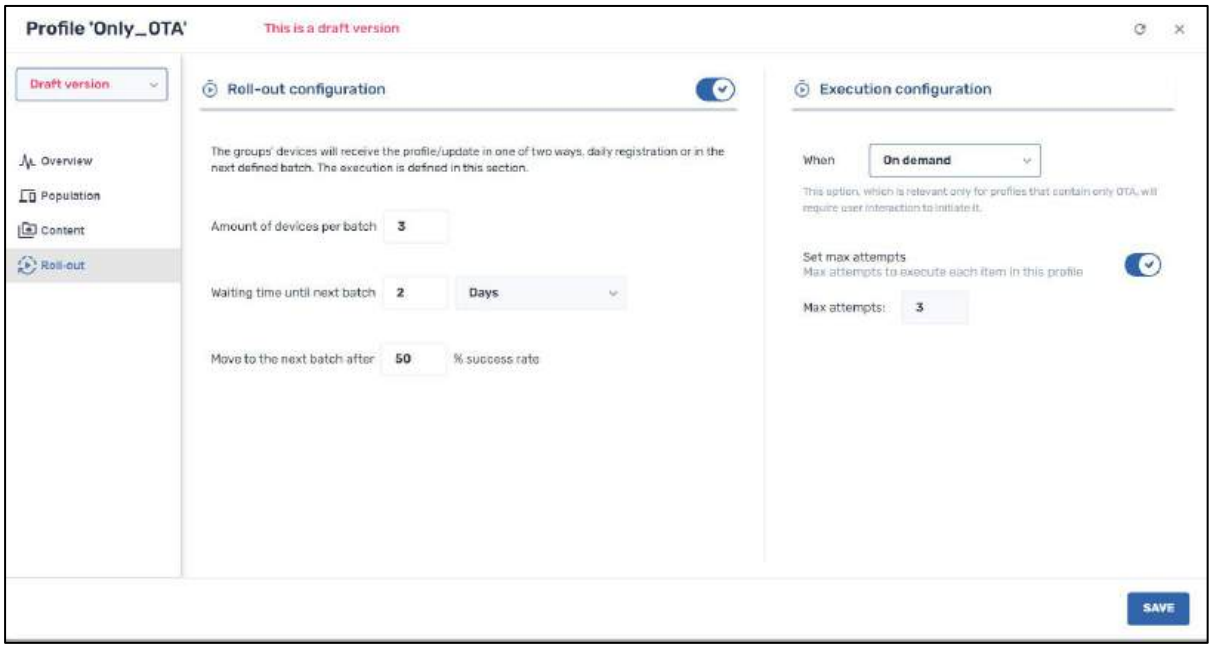


Figure 5-17: Sample profile that will be rolled out "on demand"

Note: This option is available when the **only** content assigned to the profile is an OTA update. If there is any other type of content in the profile (software packages, remote execute scripts, files, software policies), this option will be grayed out.

There are two other roll-out options:

- **Apply only if idle**: The device profile 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 profile, 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.

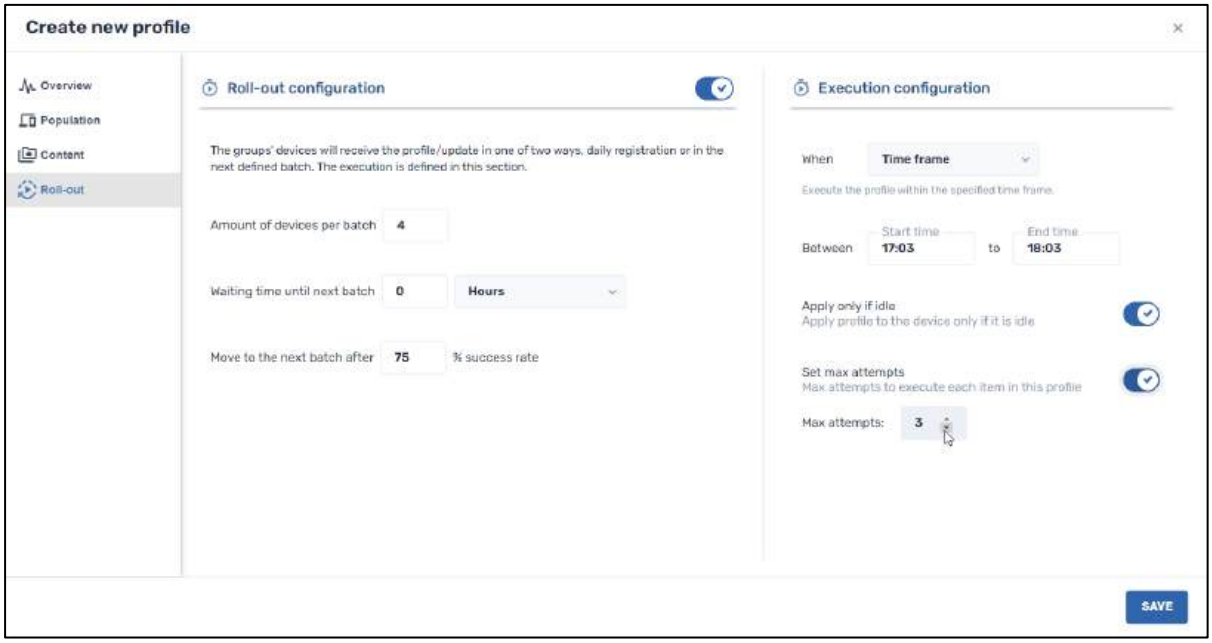
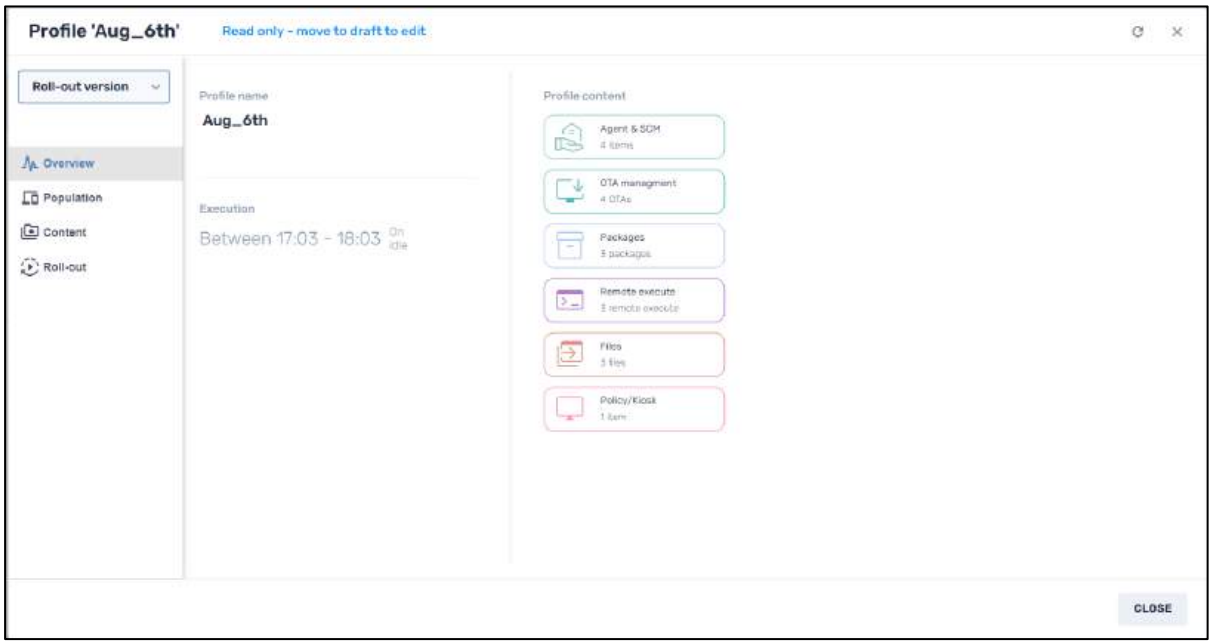


Figure 5-18: Illustration of the Roll-out options

Upon clicking **Save** in the lower right corner, the Overview window will give a summary of the profile:



You will get a prompt in the lower right corner that the profile was created correctly, and the new profile will appear in the Profiles Console.

Figure 5-19: Popup Notification that the profile was created

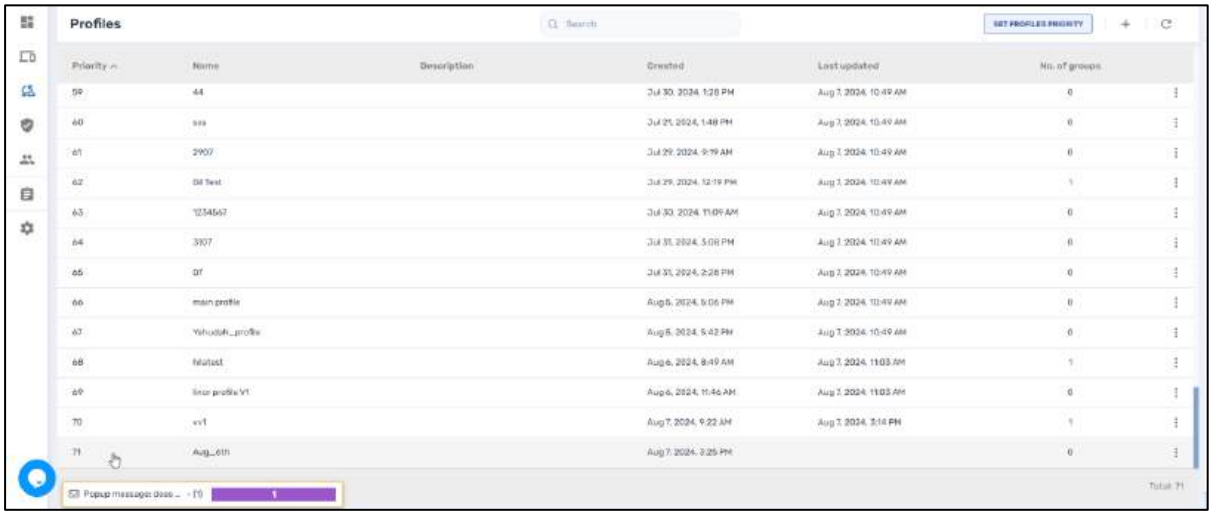


Figure 5-20: The Profiles Console, with the new profile ("Aug_6th") listed at the bottom

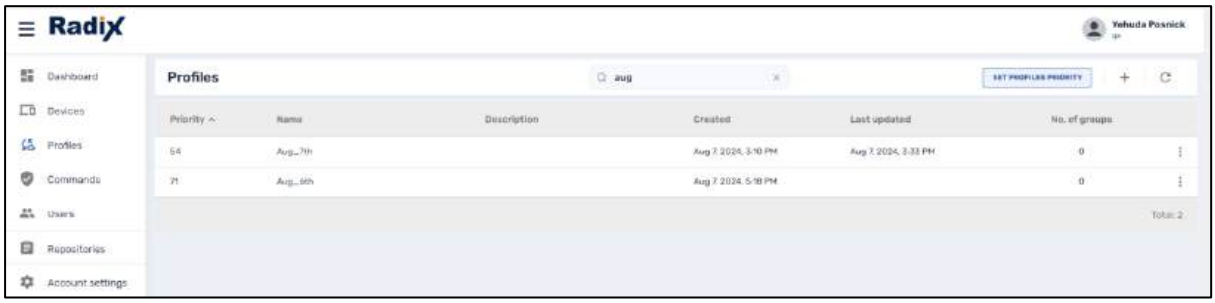
After you have created the profile, you can modify it at any time by clicking on it in the Profiles list.

5.2 Editing a Profile

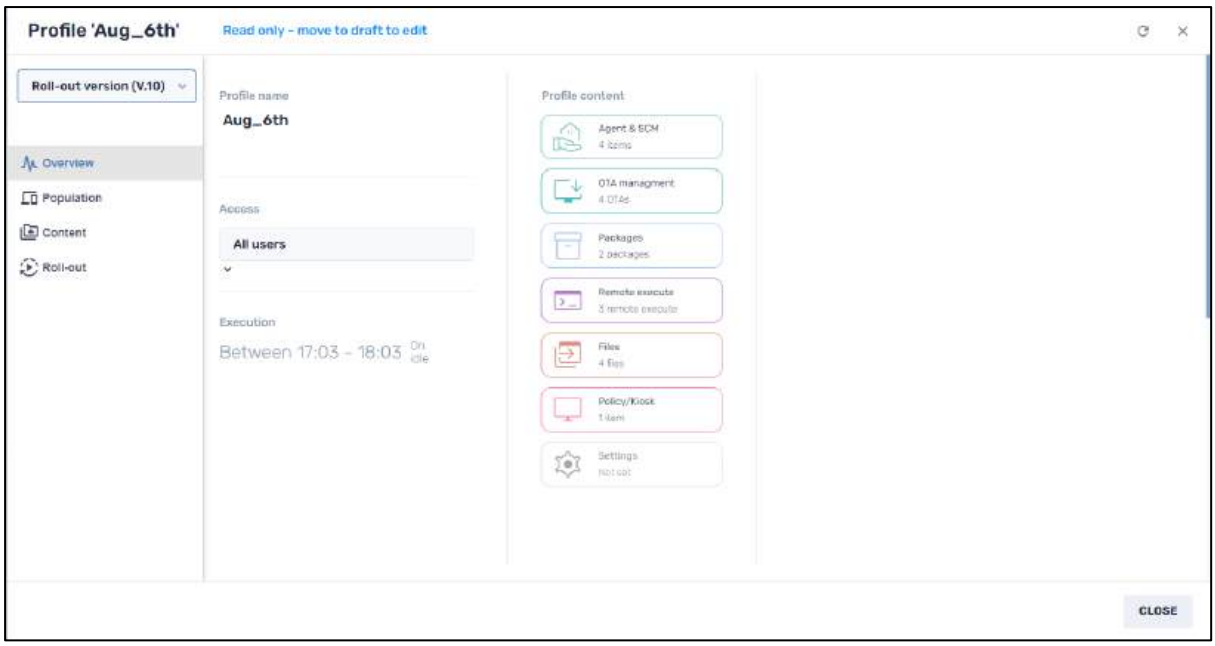
After creating a profile, you can later make modifications using the **Draft Version** option.

To modify a profile:

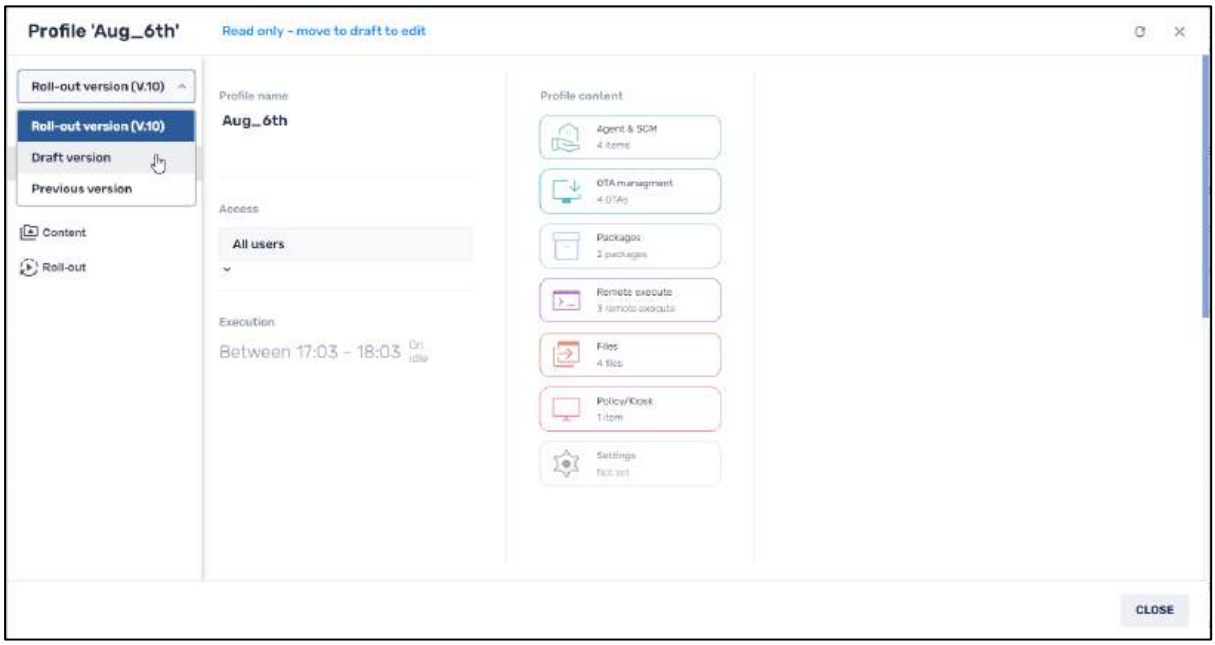
1. From the Overview Dashboard, click on the Profiles icon, to open the Profiles Console.
2. Find the profile that you would like to modify. You can use the Search bar at the top of the list. (Note: The search is **not** case sensitive.)



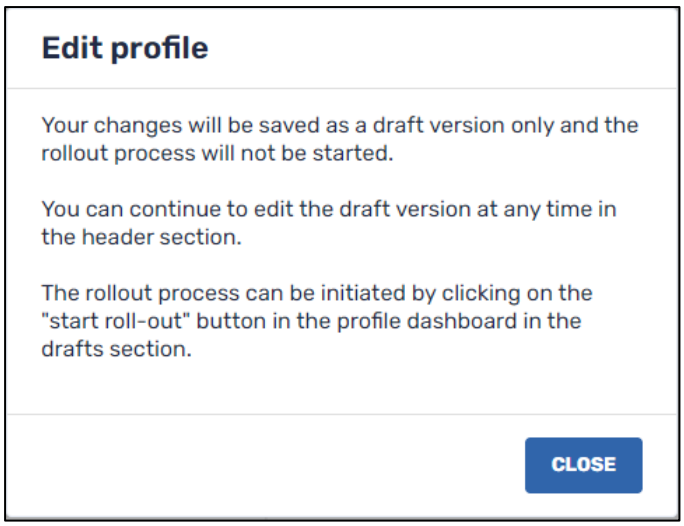
3. Click on the profile that you would like to modify. The profile's Overview screen will open in **Read only** mode, displaying the "Roll-out version" of the profile.



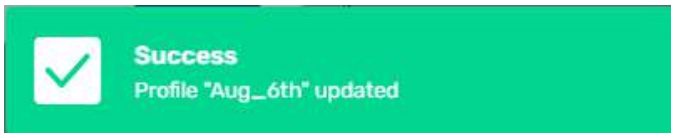
4. In the upper left corner, there is a drop-down list. Select **Draft version** to be able to edit the profile.



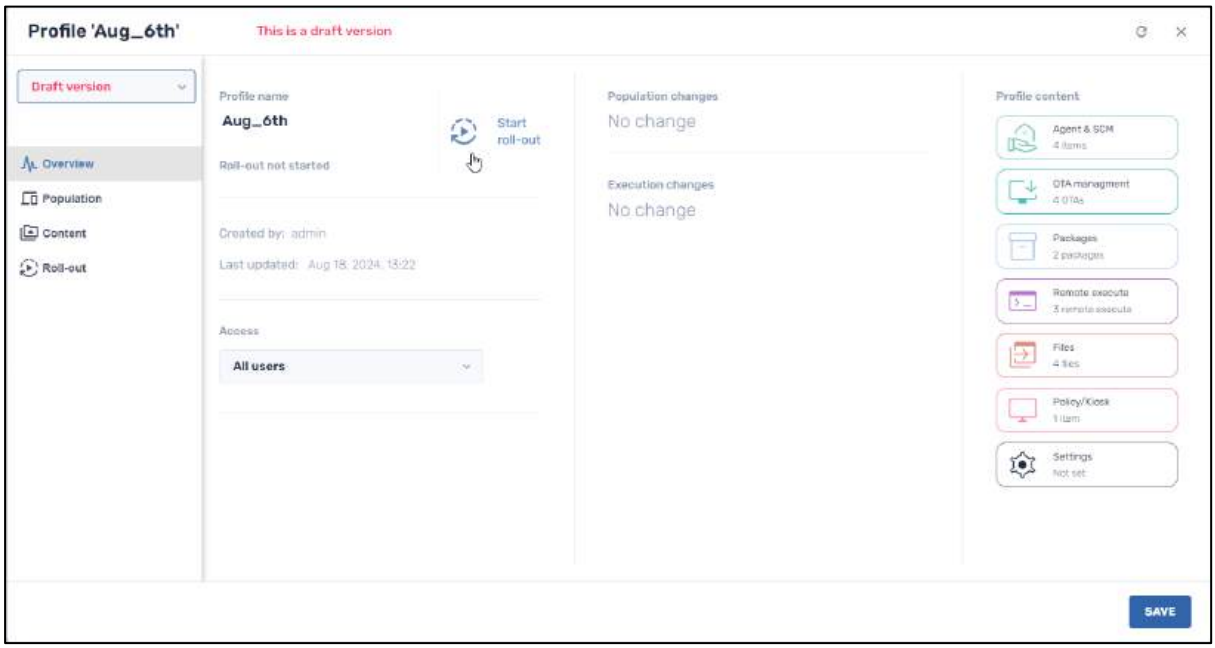
5. When in Draft version, you can make changes to all the parameters of the profile. Any changes will be recorded in the draft version of the profile. You will receive a notification, reminding you to save the changes before rolling out the profile.



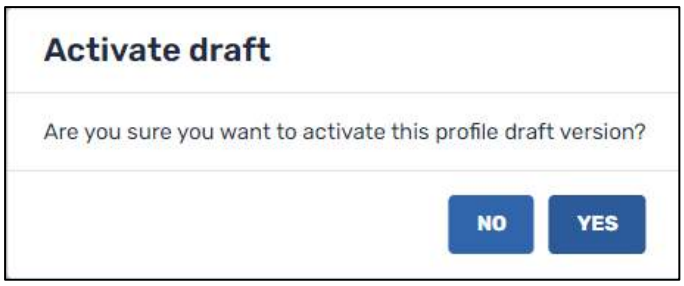
6. If you click **Save** to save all the changes to the profile, a popup notification will appear in the lower right, telling you that the changes were saved successfully.



7. When you have made the desired changes, click on **Start roll-out** in the profile's Overview screen.



You will be prompted if you are sure that you want to activate the profile:



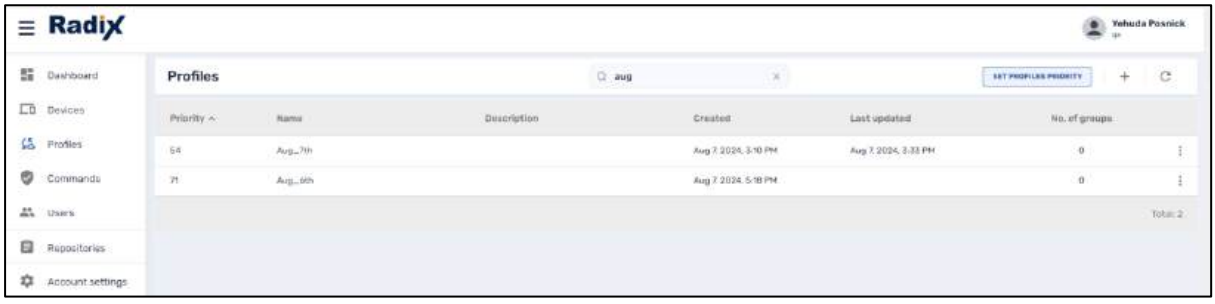
8. Click **Yes** to activate the new, updated profile. A pop-up notification will appear in the lower right corner, indicating that the profile has been activated.

5.3 Reverting to a Previous Version of Profile

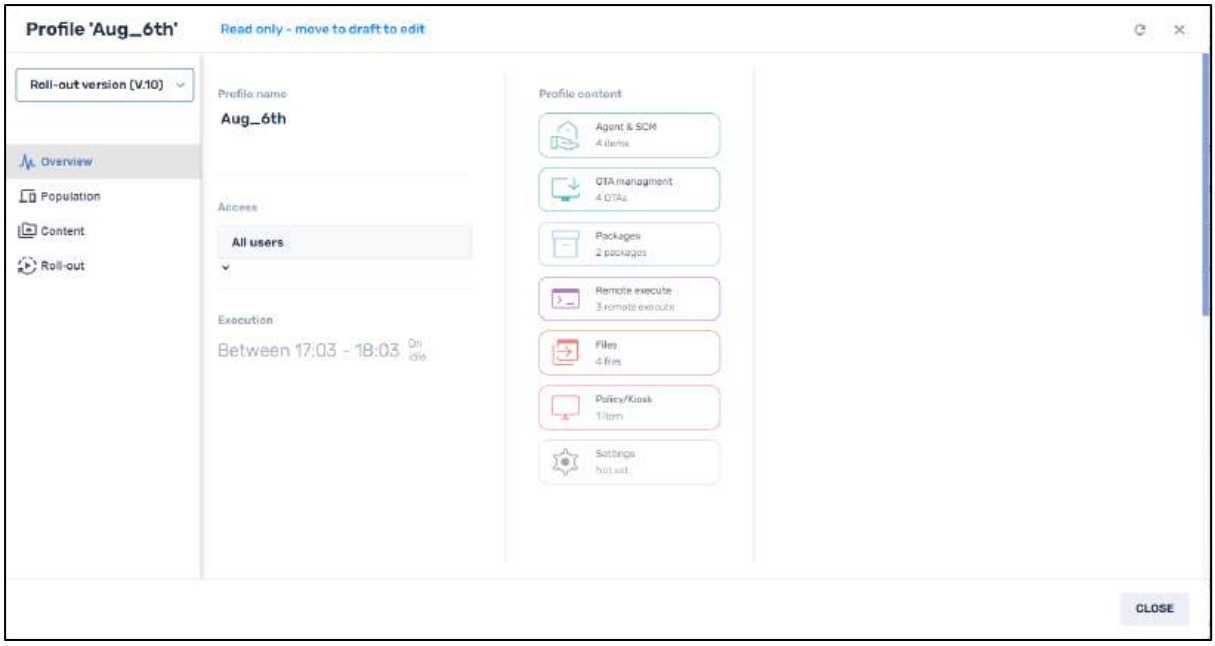
If, after making changes to a profile, you can go back to a previously saved version. This is possible using the **Previous version** option.

To revert to a previous version of a profile:

1. From the Overview Dashboard, click on the **Profiles** icon, to open the Profiles Console.
2. Find the profile which you would like to switch back to a previous version. You can use the Search bar at the top of the list. (Note: The search is **not** case sensitive.)



3. Click on the profile that you would like to modify. The profile's Overview screen will open in **Read only** mode, displaying the "Roll-out version" of the profile.



4. 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 profile.

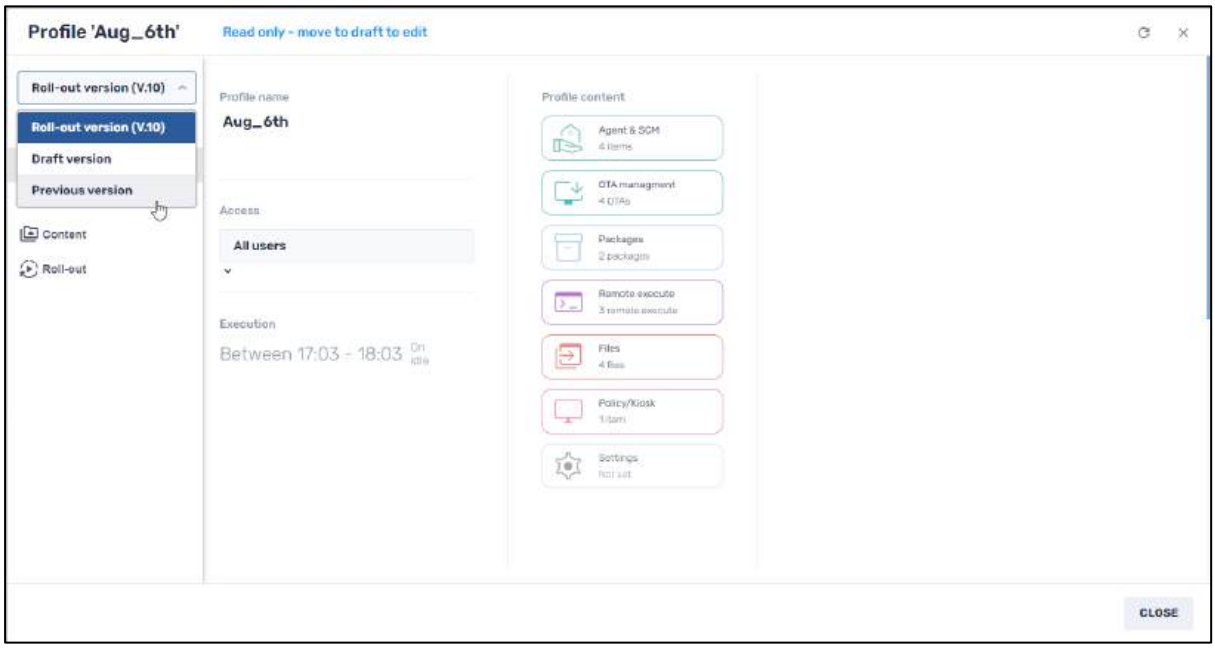
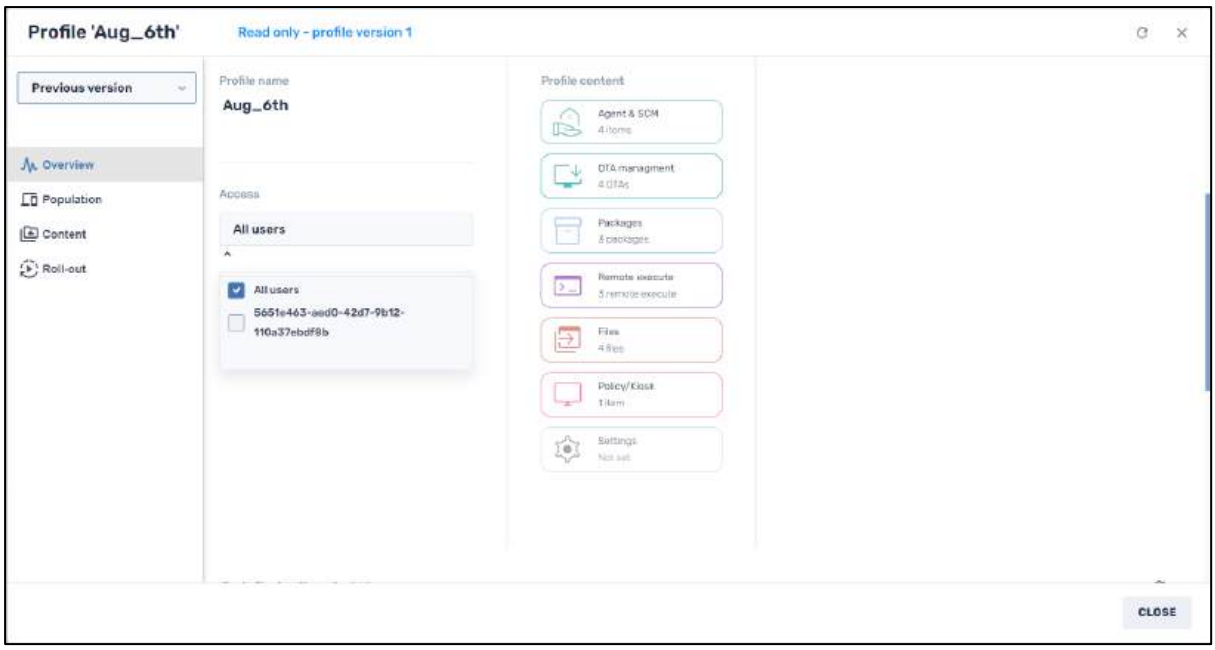


Figure 5-21: Previous versions of a profile

5. Clicking on the **View Profile** icon will allow you to see the Overview screen of the previous version of the profile.

The version number of the profile will be displayed at the top of the screen:

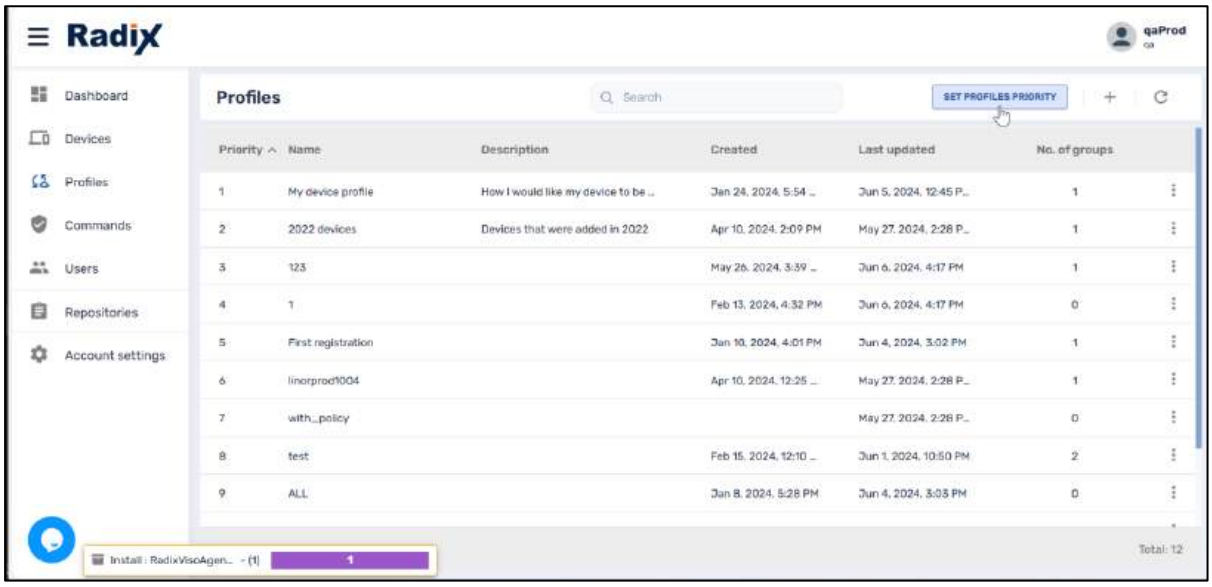


5.4 Setting the Priority of Profiles

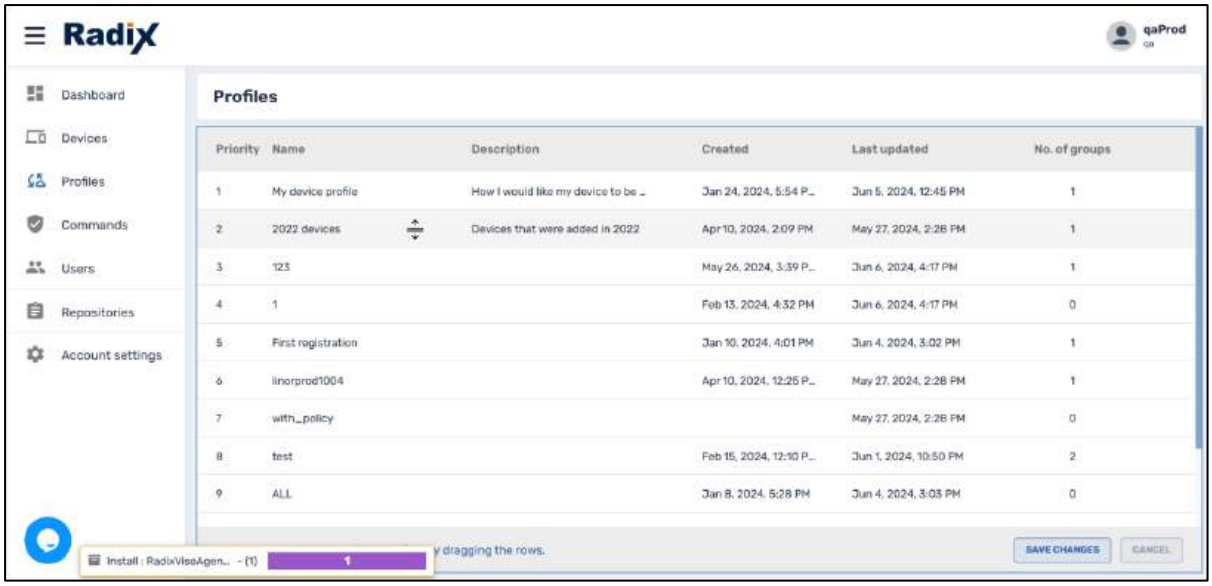
When you open the Profiles Console, the device profiles appear in a particular order. You can also choose to rearrange the priority of the profiles so that certain ones will be executed first. The profile with the lowest number is of the highest priority. Therefore, the devices that meet the filtering conditions of Profile No. 1 will be installed with the software and updates associated with that profile. The other profiles will not be executed on these devices.

To prioritize a particular profile:

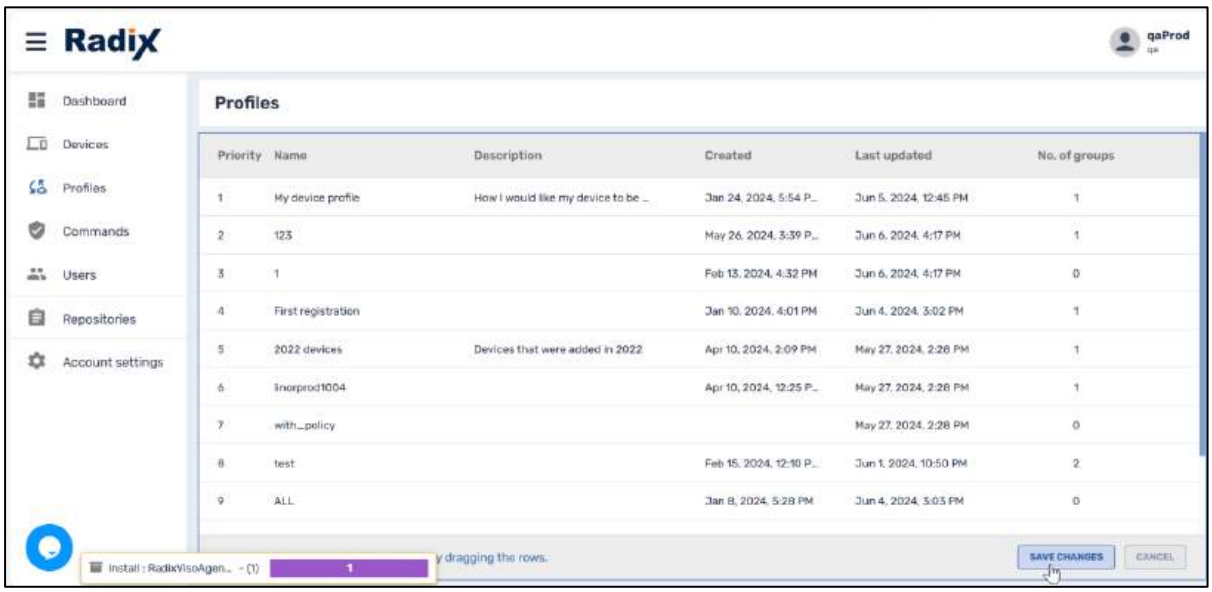
1. Click on the **Profiles** icon to open the Profiles Console.
2. Click the **Set Profiles Priority** button at the top of the list.



3. Note that when you place your mouse over one of the profiles, the mouse pointer becomes a double-headed arrow, allowing you to rearrange the priorities of the profiles.



4. When you have completed prioritizing the list of profiles, click **Save Changes** to save the new listing.

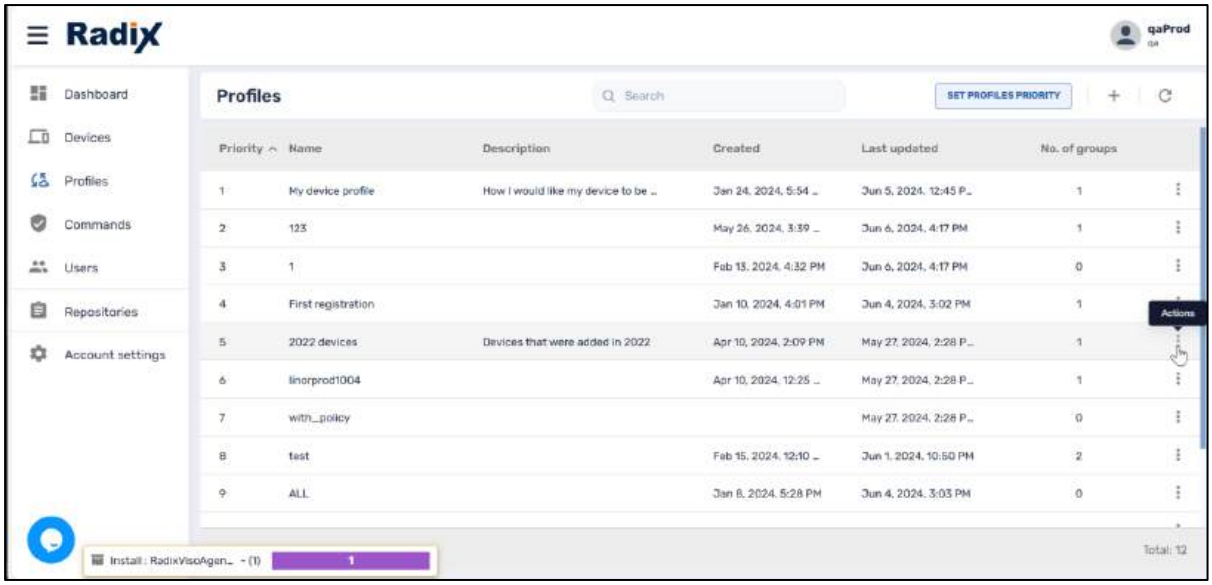


5.5 Deleting a Profile

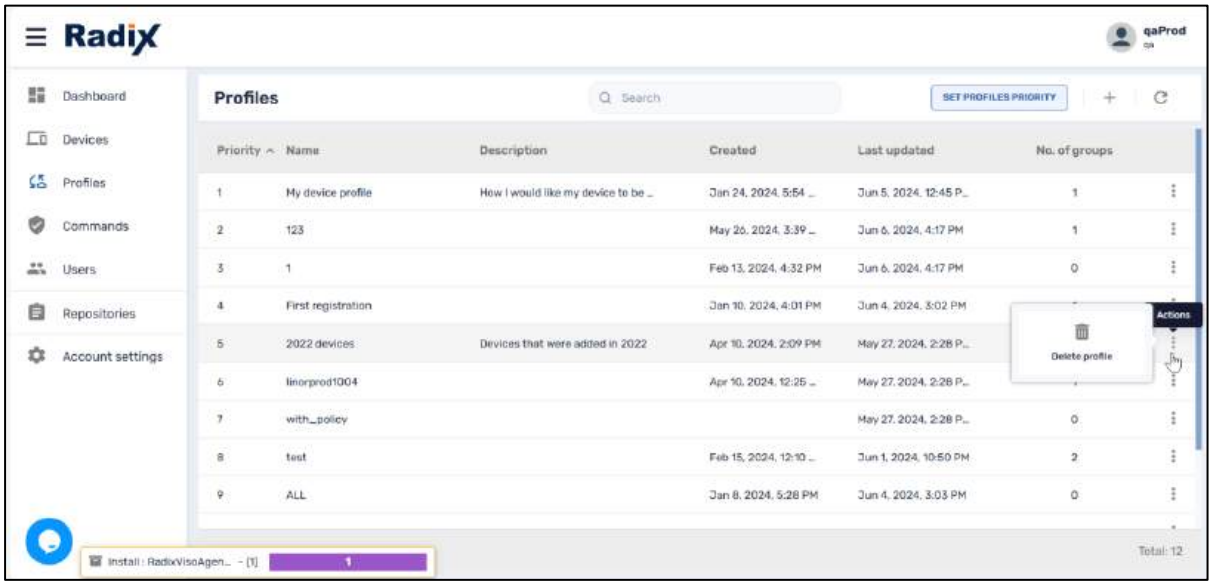
You can also delete a profile that you created.

To delete a profile:

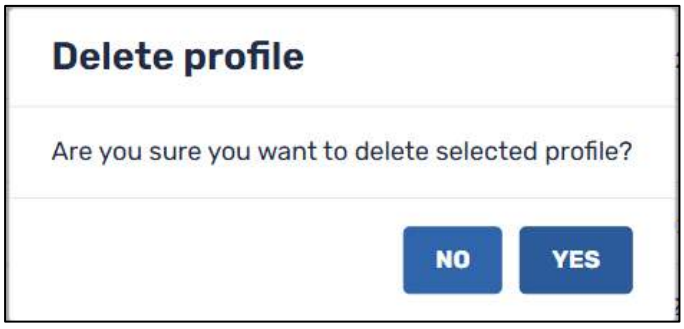
1. Click on the **Profiles** icon to open the Profiles Console.
2. Find the profile which you wish to delete from the list of profiles.
3. Click on the profile's three-dot menu (Actions) in the far-right column.



The **Delete Profile** tab opens.



4. Click on **Delete Profile** to remove the selected profile. You will be prompted before deleting the profile.



5. Check **Yes** to delete the profile. You will receive confirmation that the profile has been deleted:

Chapter 6. Commands Console

The **Commands** console 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.

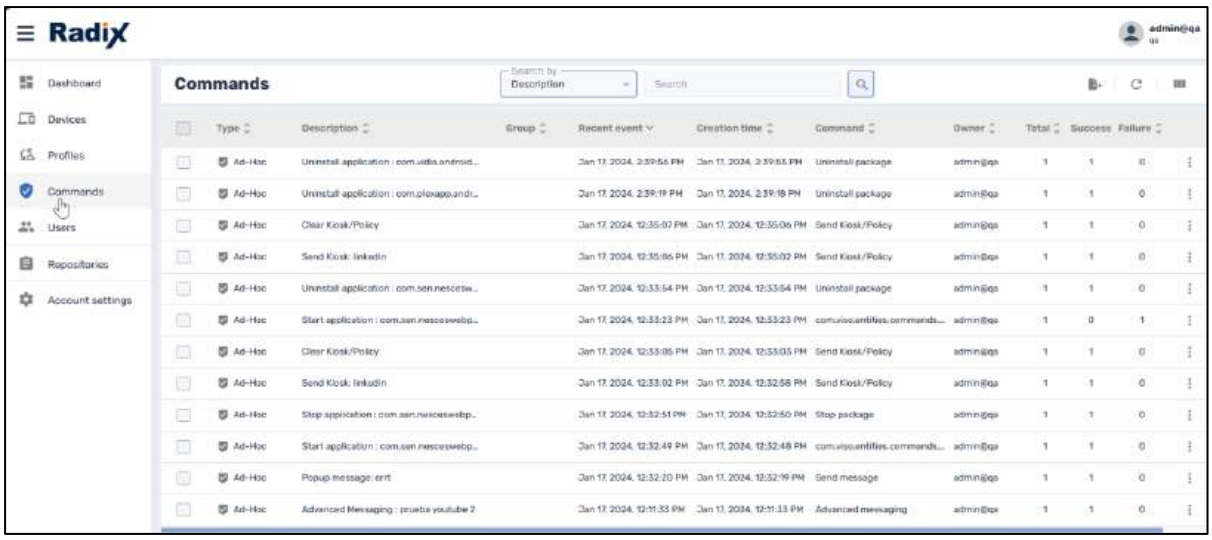


Figure 6-1: You can access the Commands Console via the Commands icon in the Overview Dashboard

6.1 Types of Commands in the Commands Console

In the **Type** column in the Commands console, 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 4.2.1.15**)), while an Ad-Hoc command is sent via the other Radix Device Manager 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.

6.2 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.

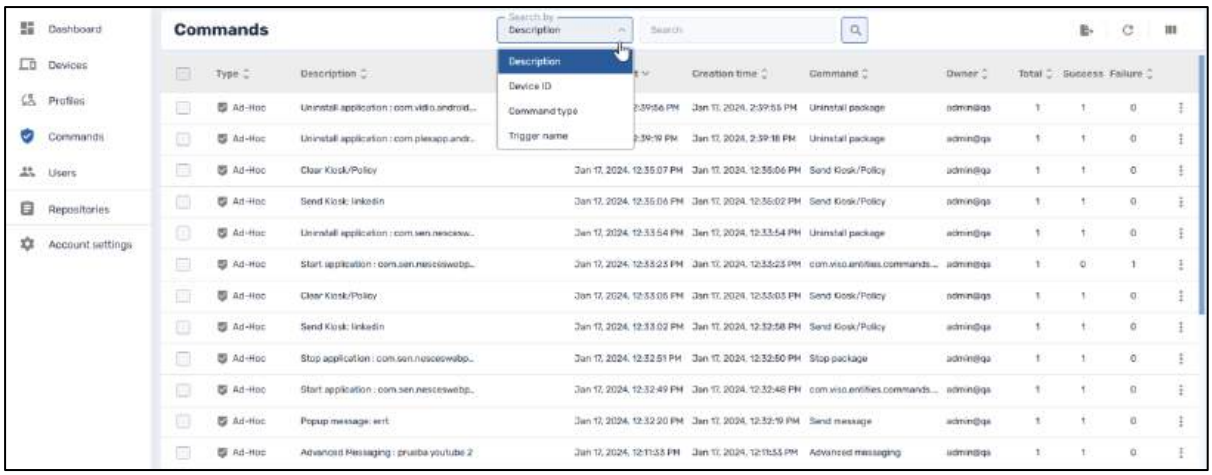


Figure 6-2: Various search criteria for commands

6.3 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.

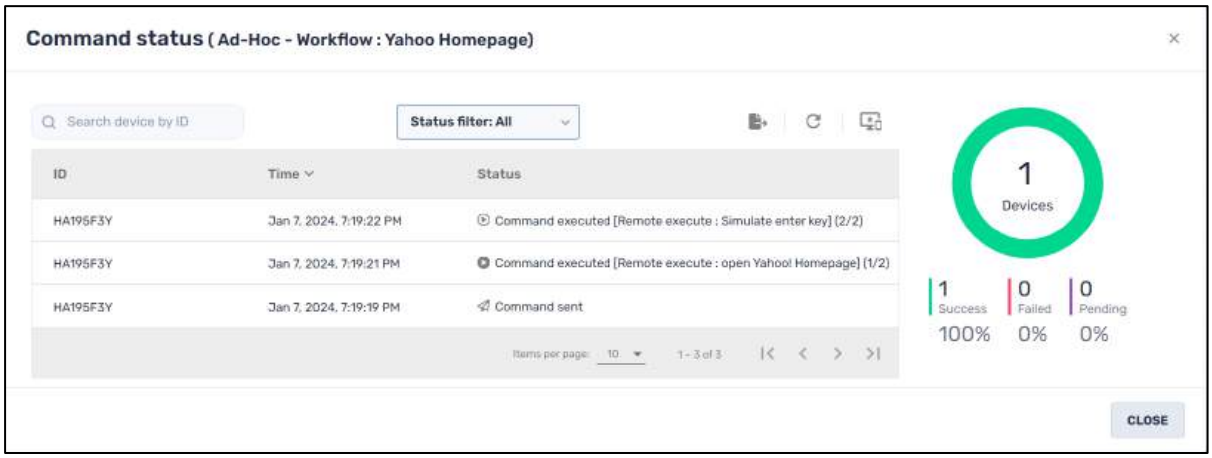


Figure 6-3: Command status of a "Successful" command

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.

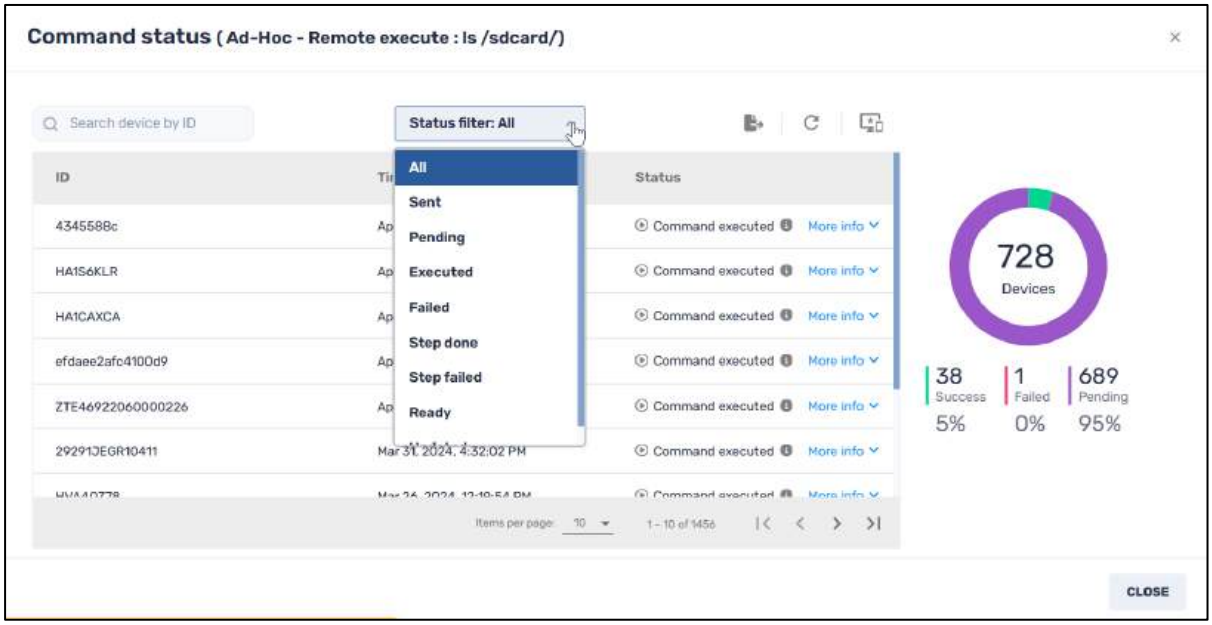


Figure 6-4: Command status window--Status Filter

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 very 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:

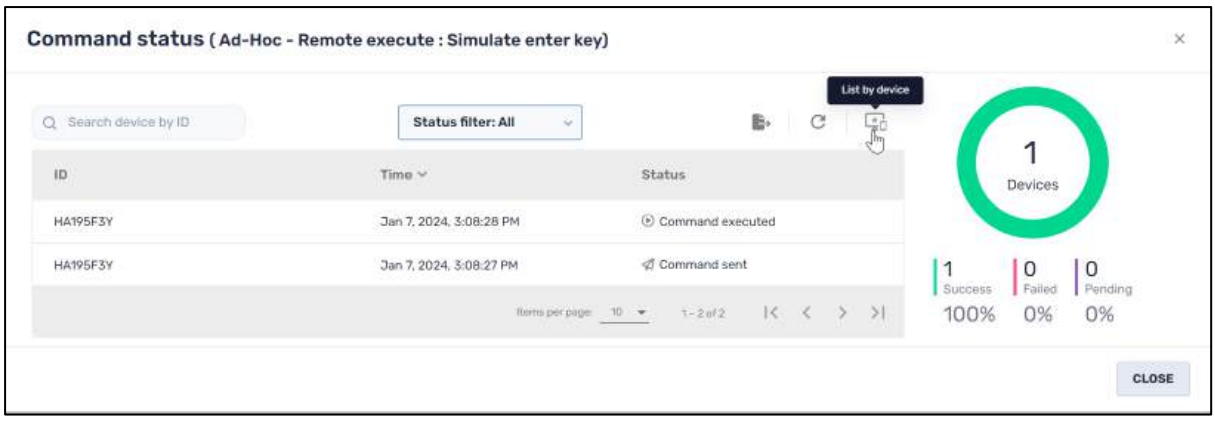


Figure 6-5: Commands listed by device

Figure 6-6: Commands listed by time sent

6.4 Executing Commands from the Commands Console

By clicking on the command's three-dot menu in the far-right column of the Commands Console you will see options to start, stop, edit, resend, or delete this command.

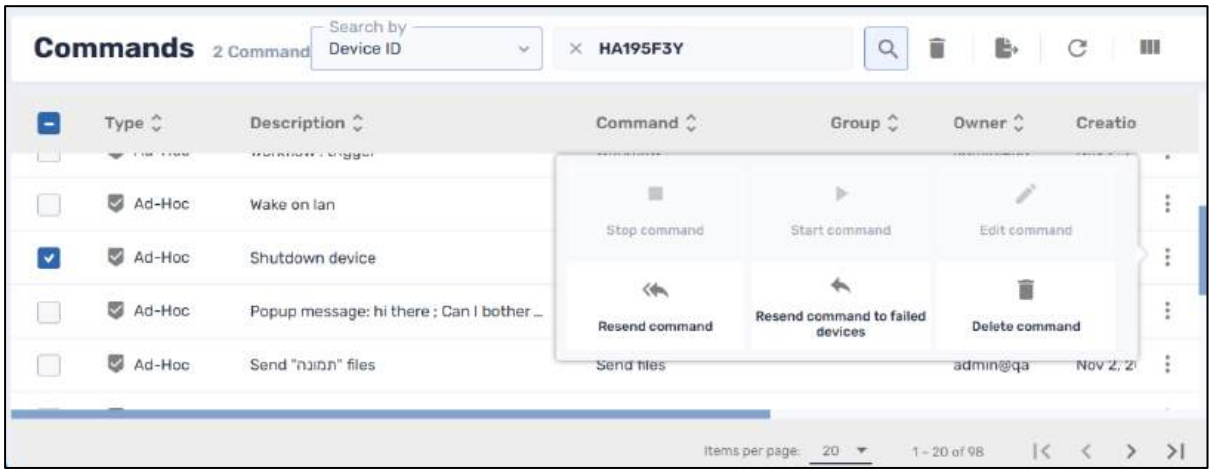


Figure 6-7: Options to start, stop, resend, or delete command

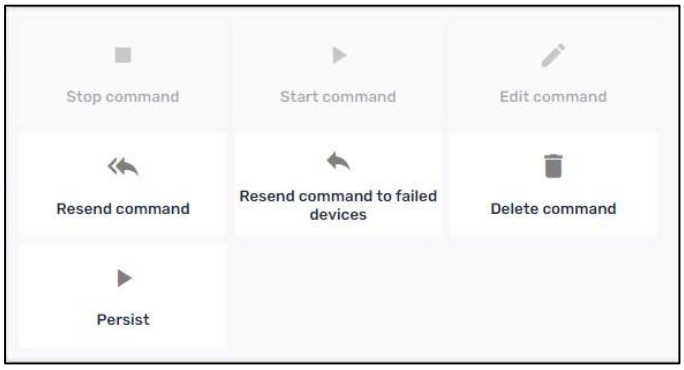
6.5 Use of the Persist Command for Groups

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.

   The Commands options grid opens.
2. Select **Persist**.



You will be prompted if you want to employ persistence.

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.

4. If for some reason you wish to disable persistence, select a group with persistence, and select **Stop persistence** from its three-dot menu.

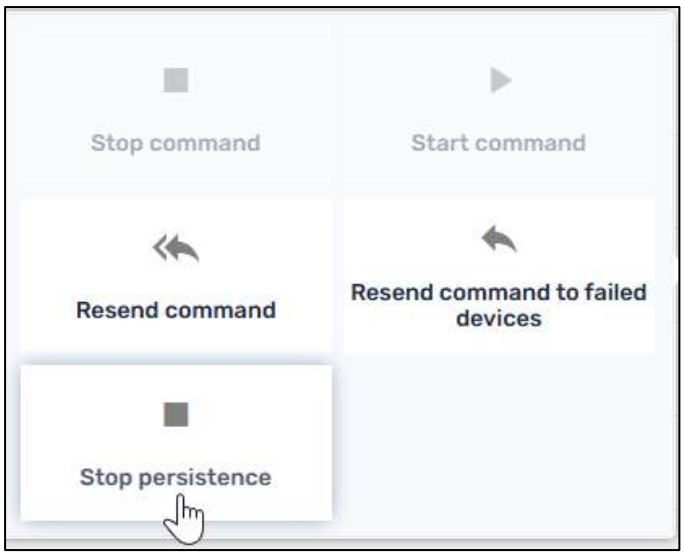
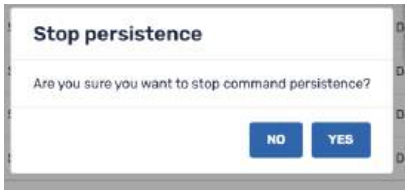


Figure 6-8: Stop Persistence option

5. You will be prompted if you wish to stop persistence. Click **Yes**.



The color of the command's icon in the Commands console will now revert from green to blue. This indicates that the command no longer has persistence.

Chapter 7. Users Console

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

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

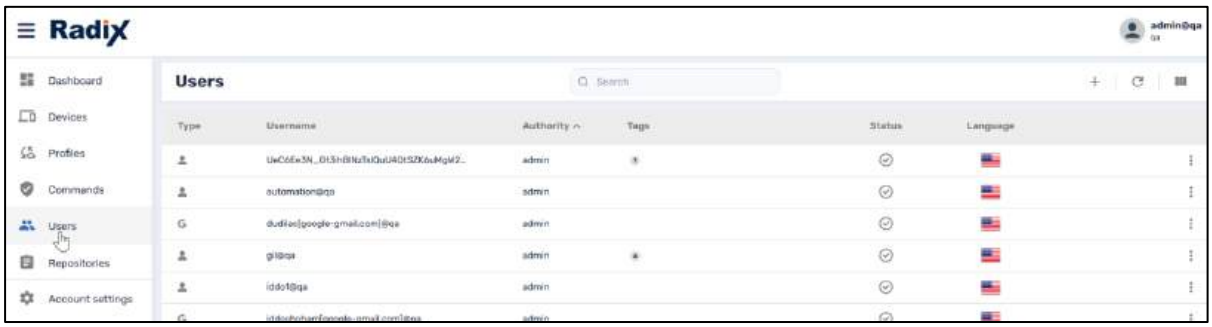
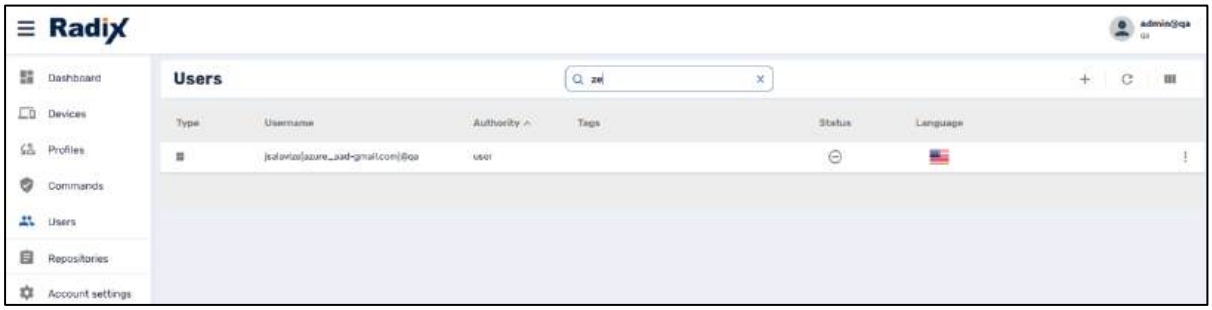


Figure 7-1: List of Users, as displayed in the User Console

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



7.1 Adding a New User

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

To add a new user:

1. Click on the **Users Console** icon in the Overview Dashboard. The Users Console opens, displaying all existing users.

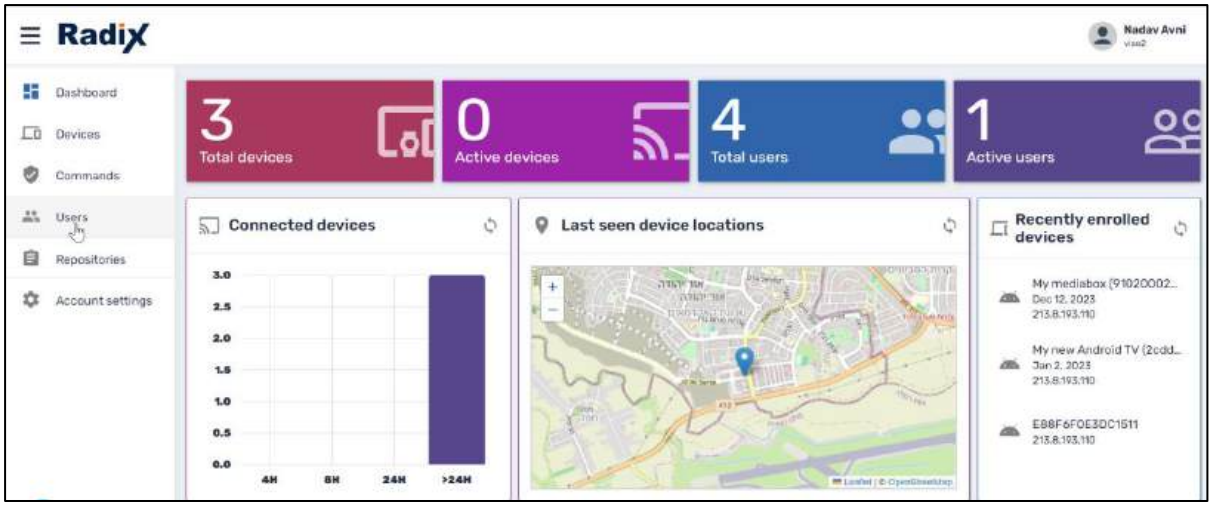


Figure 7-2: Users Console Icon in Overview Dashboard

2. In the upper right side of the Users Console, click on the **Add New User** + icon.

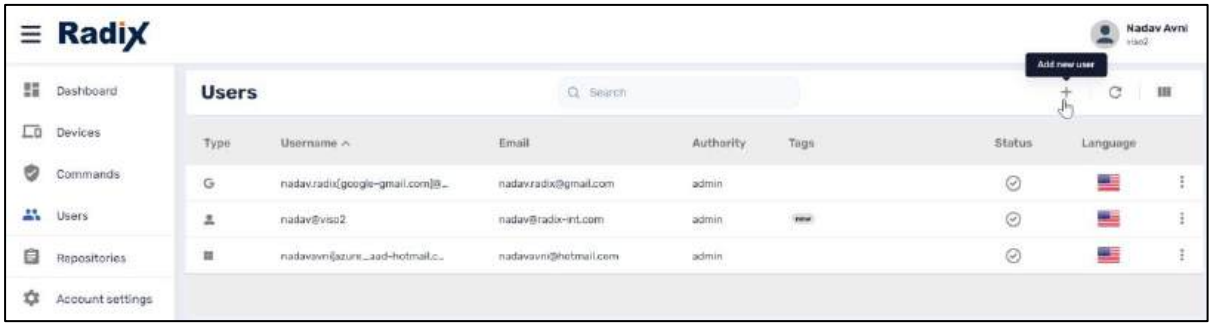
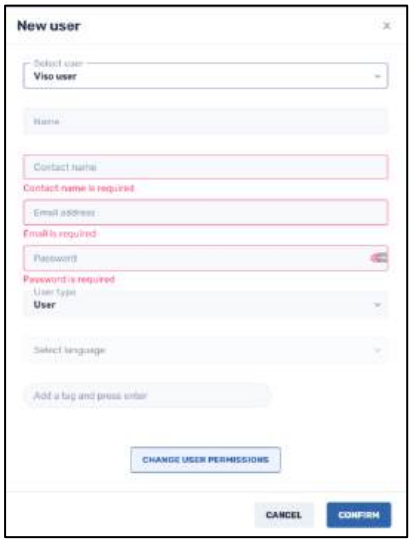


Figure 7-3: Placement of "Add New User" icon

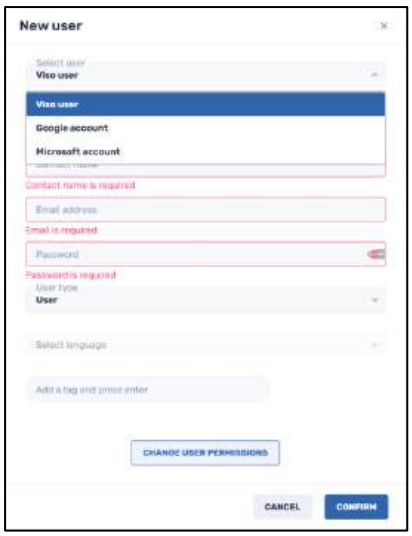
The **New User** dialog box opens.



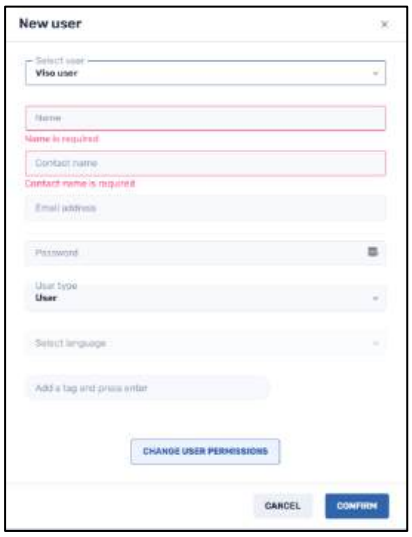
You will have to supply the following information to add a new user:

7.1.1 Select User

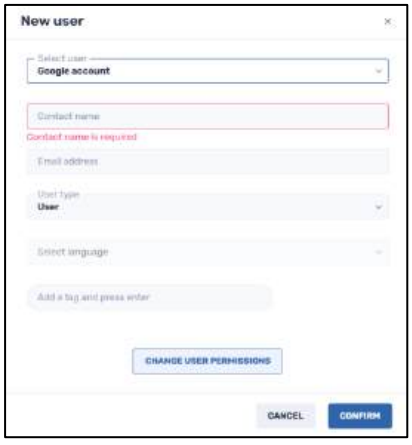
There are three options here:



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



- **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.



After supplying the required information and clicking **Confirm**, the user's account will appear in the Radix Device Manager Dashboard as being in "Pending" status.

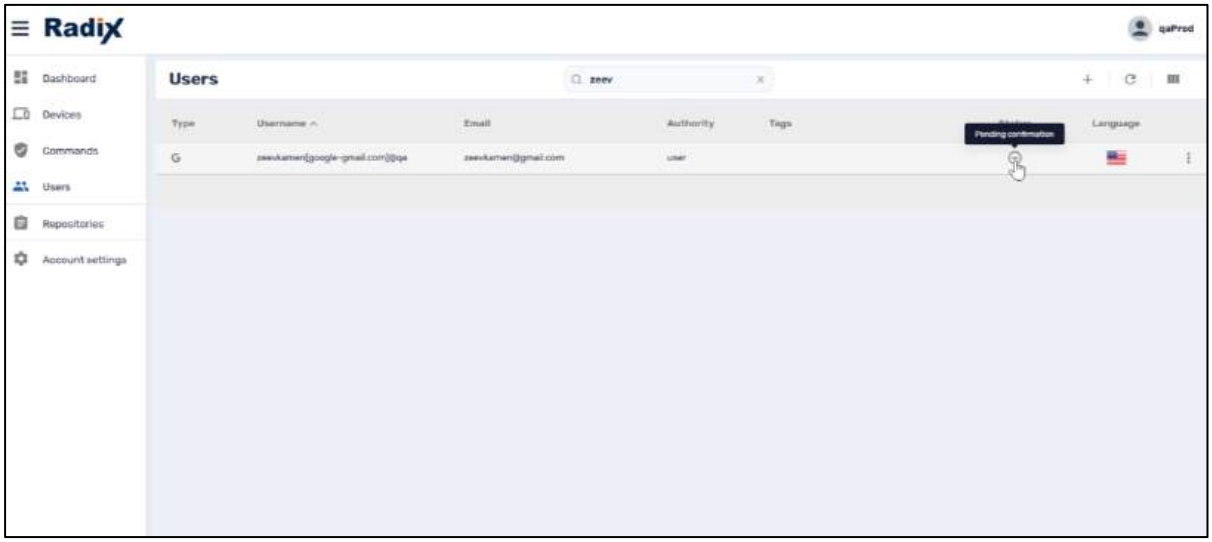


Figure 7-4: Appearance of user status, pending confirmation

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

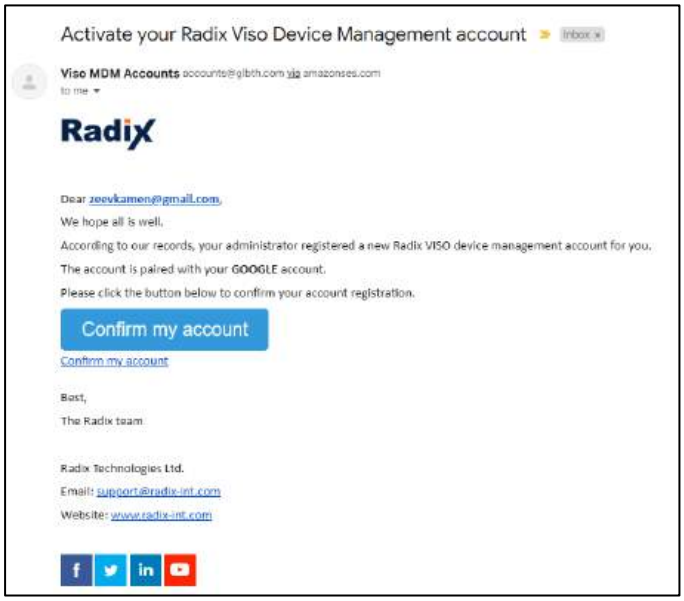


Figure 7-5: Google Account Confirmation E-mail

- **Microsoft account:** The sign-in requirements for a Microsoft account are the same as those for a Google account.

7.1.2 Name

This name will appear in the Radix Device Manager along with your device/s.

7.1.3 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.

7.1.4 Email Address

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

7.1.5 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.

7.1.6 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 User Console. Also, any user of the Radix Device Manager 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.)

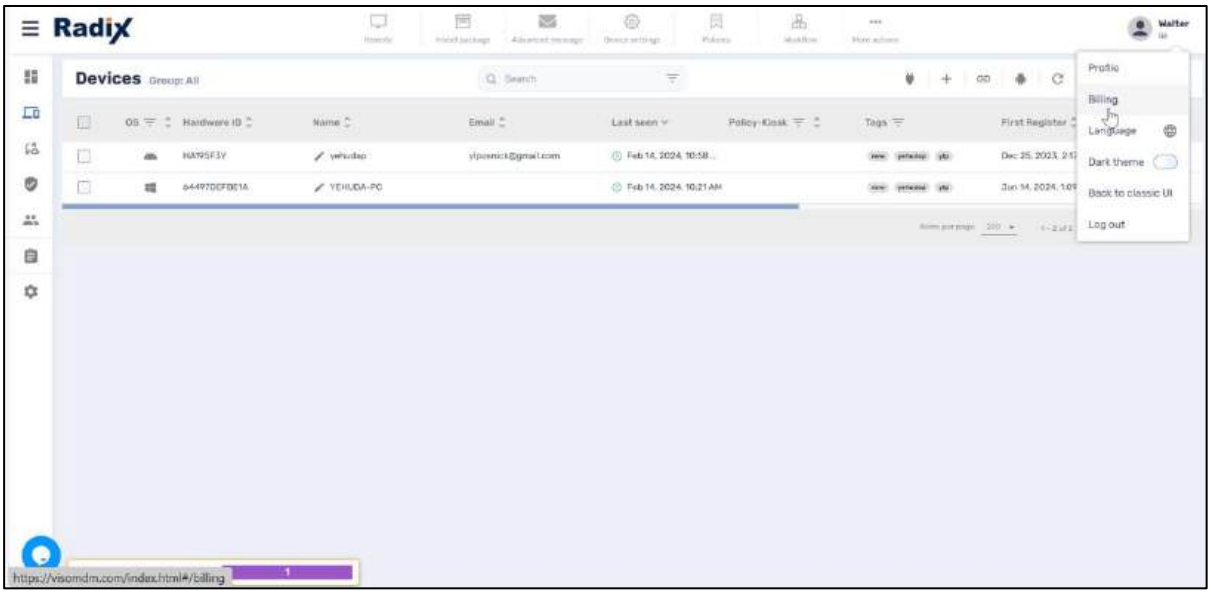


Figure 7-6: The interface of the user ("Walter") with Admin privileges

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

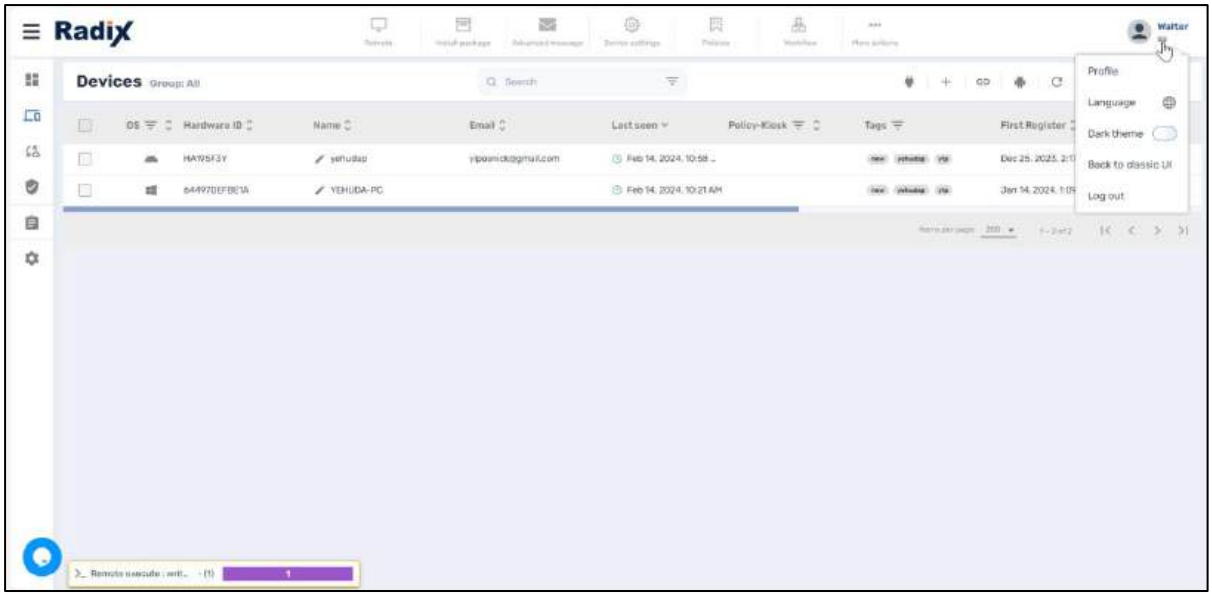


Figure 7-7: The same user as above, with only User privileges

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

Figure 7-8: View of Display of User with only Supporter Privileges

7.1.7 Select Language

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

7.1.8 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.

7.1.8.1 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.

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

7.2 Viewing a User's Profile

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

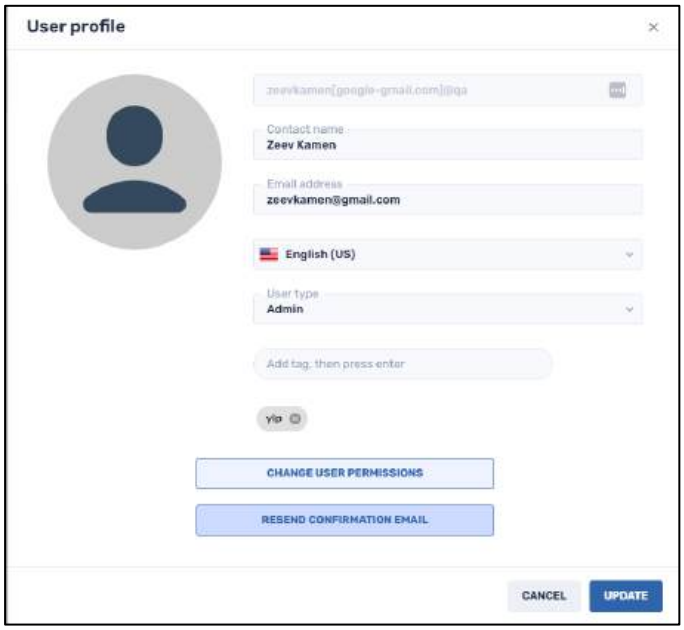
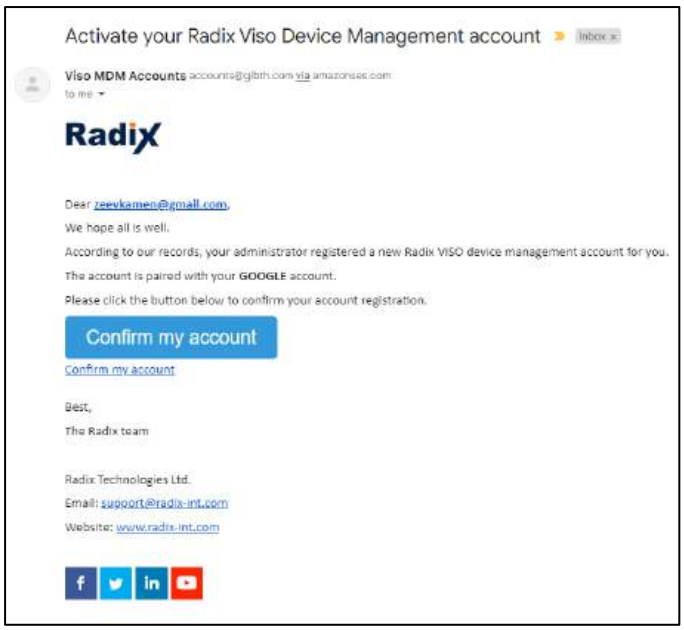


Figure 7-9: User Profile screen

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.



7.3 Changing the User's Interface Language

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

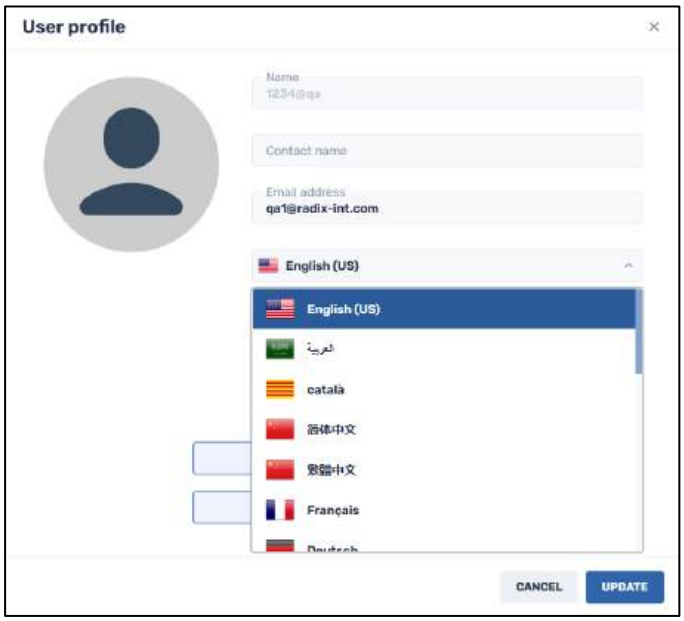


Figure 7-10: Selecting the language of the interface

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

7.4 Granting Administrator Privileges to a User

If a person has only User status, the **Users Console** icon will not appear in their Overview Dashboard:

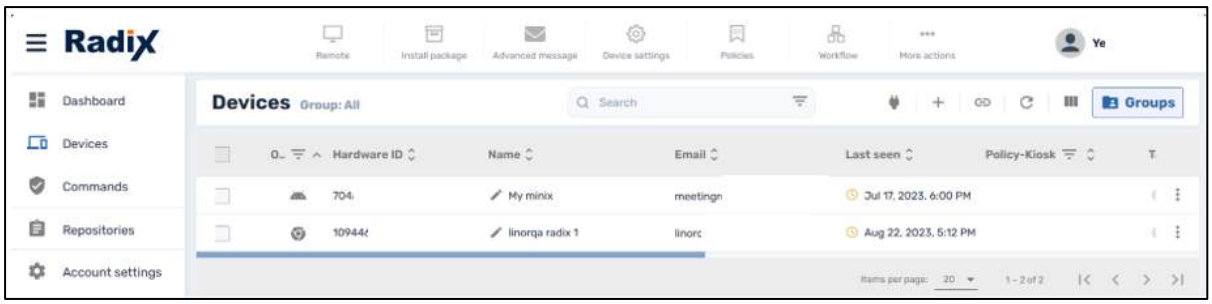


Figure 7-11: User Interface of Person with only "User" status

If the user's status is changed to **Administrator**, the **Users Console** icon option will reappear:

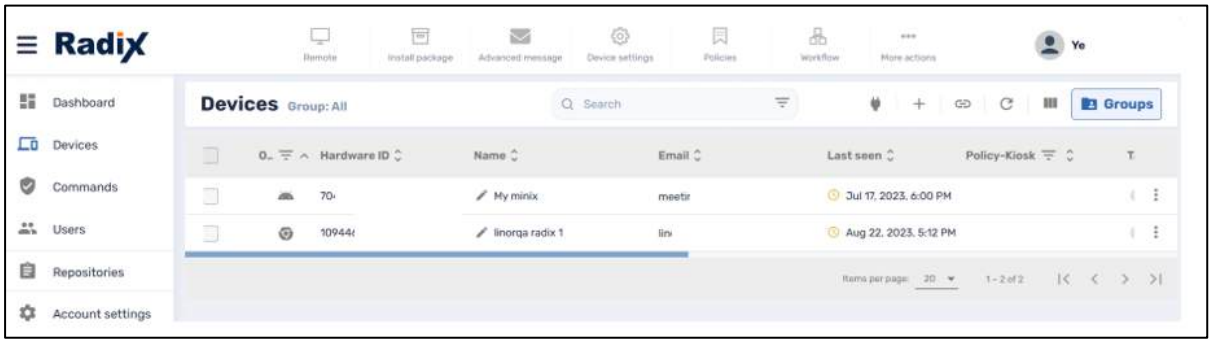


Figure 7-12: User Interface of person with "Admin" status. Note the "Users" icon in the sidebar

7.5 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:

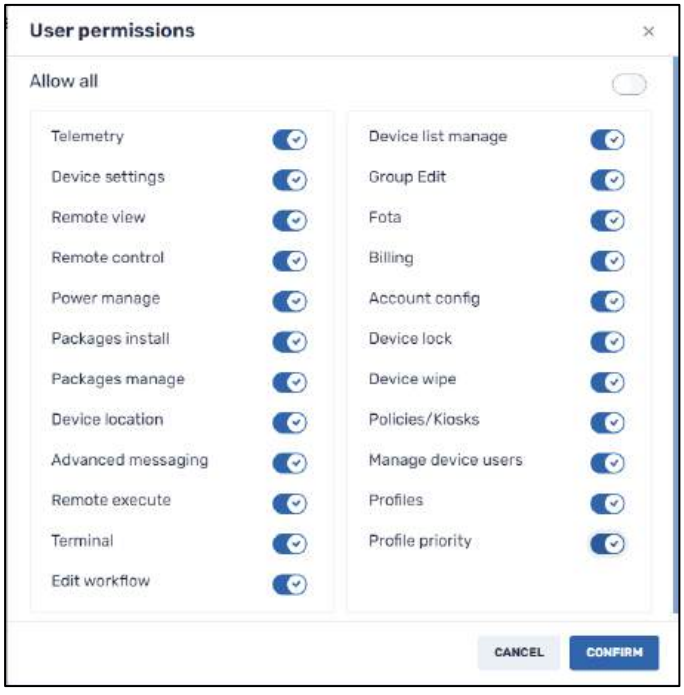


Figure 7-13: List of User permissions that can be granted

Note: This list of permissions is the Radix Device Manager 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. (See **Sections 3.1-3.3**.)
- **Device settings**: To show/hide repository items from Device Settings. (See **Section 9.79.7**.) The Device Settings option on the Dashboard will be disabled as well. (See **Section 4.1.4**.)
- **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 4.1.1**.)
- **Power manage**: To show/hide the **Shutdown**, **Restart**, and **Wake on LAN** actions. (See **Section 4.2.1.19**, **4.2.1.14**, and **4.2.1.23.**)
- **Packages install**: To enable/disable installing apps. (See **Section 4.1.2**.)
- **Packages manage**: To allow/disallow the user to start/stop/enable/disable/uninstall software packages. (See **Section 4.2.1.3**, **4.2.1.5**, and **4.2.1.22**.)
- **Device location**: To allow/disallow viewing the device location. (See **Section 4.4.3.7**.)
- **Advanced messaging**: To allow/disallow the **Advanced messaging (Section 4.1.3)** and **Assets** (**Section 9.6**) repository items.
- **Remote execute**: To enable/disable the **Remote execute** option. (See **Section 4.2.1.12**.)
- **Terminal**: To enable/disable the **Terminal** option in the Devices console. (See **Section 4.4.3.2**.)
- **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 4.1.6**.
- **Device list manage**: To show/hide the actions listed in the Device Dashboard under the **Manage** tab. (See **Section 4.4.3.10**.)
- **Group edit**: To enable/disable making any changes to a group, such as creating or deleting a group. (See **Section 4.3.8**.)
- **FOTA**: This allows/disallows the user to use the Firmware OTA (=Over-the-Air) update engine command, to install firmware updates. (See **Section 4.2.1.11.**)
- **Billing**: To enable/disable access to billing information to the user. (See **Section 3.4.2.**)
- **Account config**: To show/hide the account settings on the Overview Dashboard and shows/hides the panes to access the account settings. (See **Chapter 10**.)
- **Device lock**: To show/hide the device lock and unlock actions. (See **Section 4.4.3.8**.)
- **Device wipe**: To show/hide the option to wipe a device. (See **Section 4.4.3.8**.)
- **Policies/Kiosks**: To show/hide the **Policy** and **Kiosk** repository items. (See **Section 4.1.5** and **Section 4.2.1.8**.)

- **Manage device users**: To enable/disable the ability to create or remove users from the device in the Device Dashboard. (See **Section 4.2.1.8.4**.)
- **Profiles:** This will allow/disallow the user from creating, editing, or changing the priority of device profiles. (See **Section 5.1, Creating a New Profile**)
- **Profile priority:** This will allow/disallow the user from changing the priority level of the different device profiles. The **Set Profiles Priority** button will not appear in the Profiles console. (See **Section 5.4, Setting the Priority of Profiles**.)

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.

7.6 Deleting a User

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

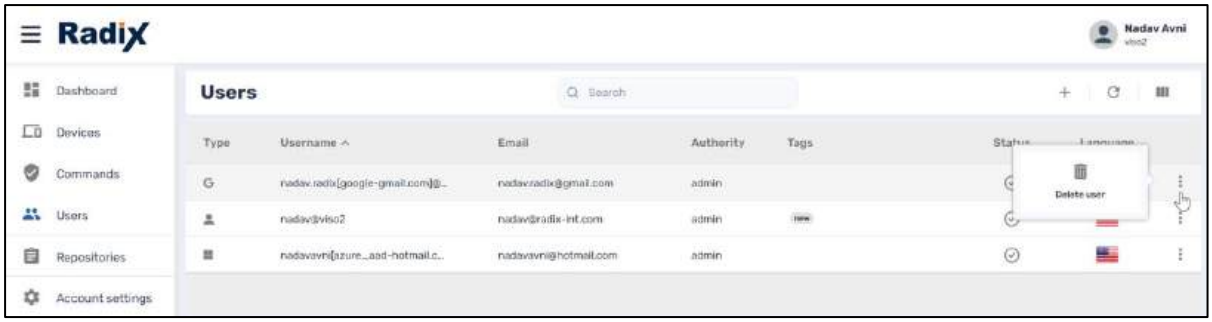


Figure 7-14: Option to delete a user

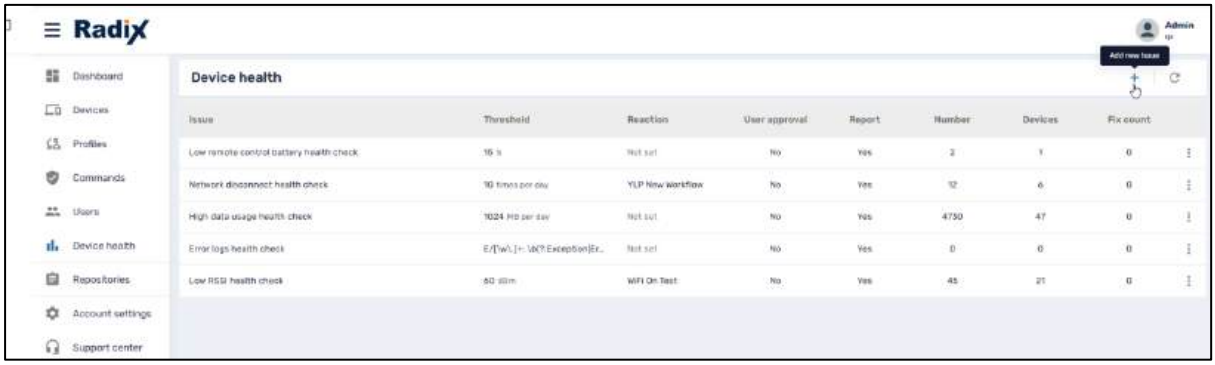
Chapter 8. Device Health Console

When you click on the **Device Heal**th icon in the Device Manager sidebar menu, the following window opens:

There are five device health settings options. In the screen capture above, all five of the options have been employed, and have already been set to the desired parameters. You can change these parameters at any time.

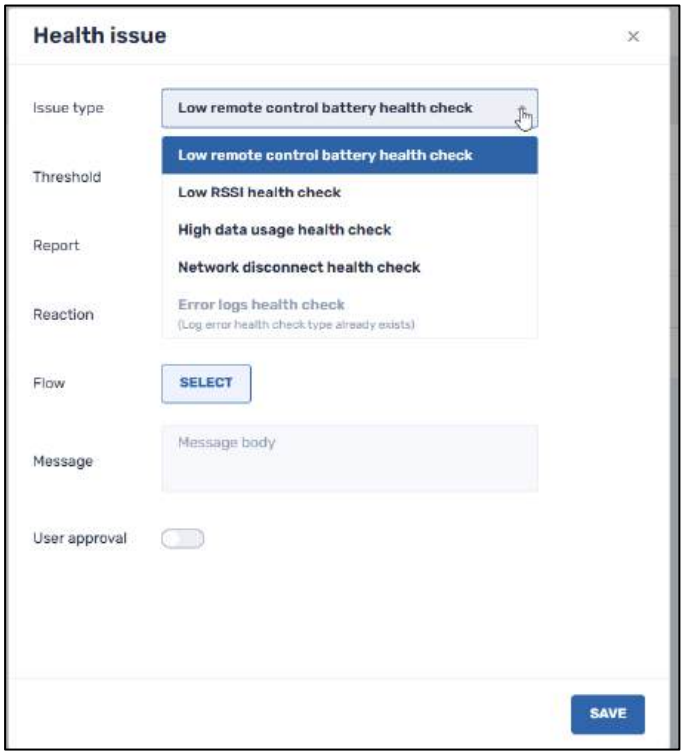
8.1 Creating a New Device Health Issue

If you wish to create a new Device Health issue, click on the **Add new issue** icon in the Device Health Console:



The Device Health Console will display a summary of your device health settings, the system's reaction, the number of devices involved, and more.

The following window opens. When you click on the **Issue type** drop-down list, you receive the following health issue options:



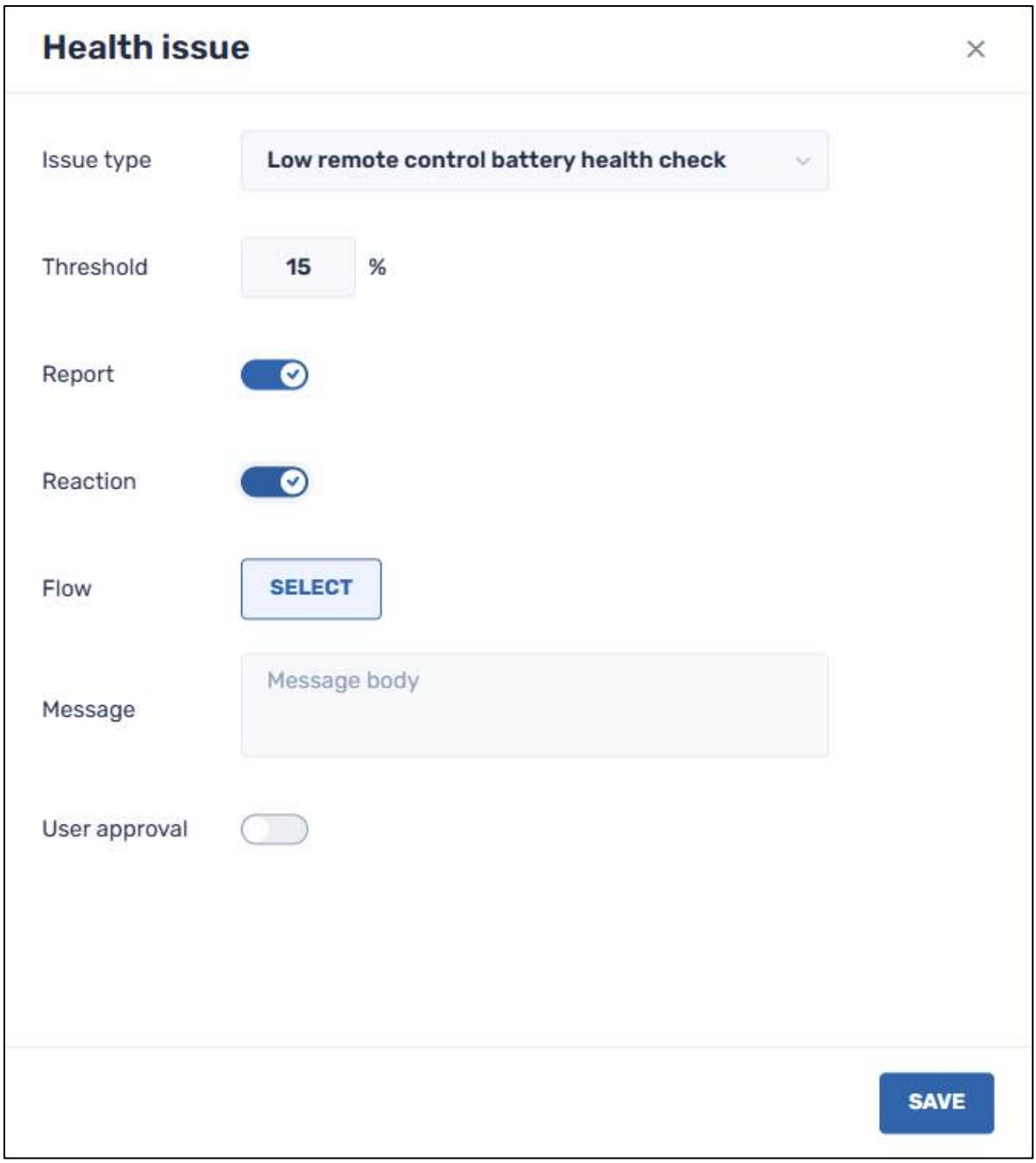
All five of the options have the following options to report any device health issues to the Radix Device Manager.

- **Report:** If you check the **Report** button, a report will be created when one of the remote devices exceeds the threshold health value.
- **Reaction:** If you check the **Reaction** button, you will activate the following three options, to serve as an additional reaction when a device exceeds the threshold value:
    - **Flow**: This allows you to create a workflow of commands (as in **Section 4.1.6, Workflow**) as a reaction to exceeding the device health threshold.
    - **Message**: This sends a text message to the Radix Device Manager device.
    - **User approval**: By clicking this, the user gives approval to receive a notification when a device health issue has occurred.

We will go through the device health options in turn.

8.2 Low remote control battery health check

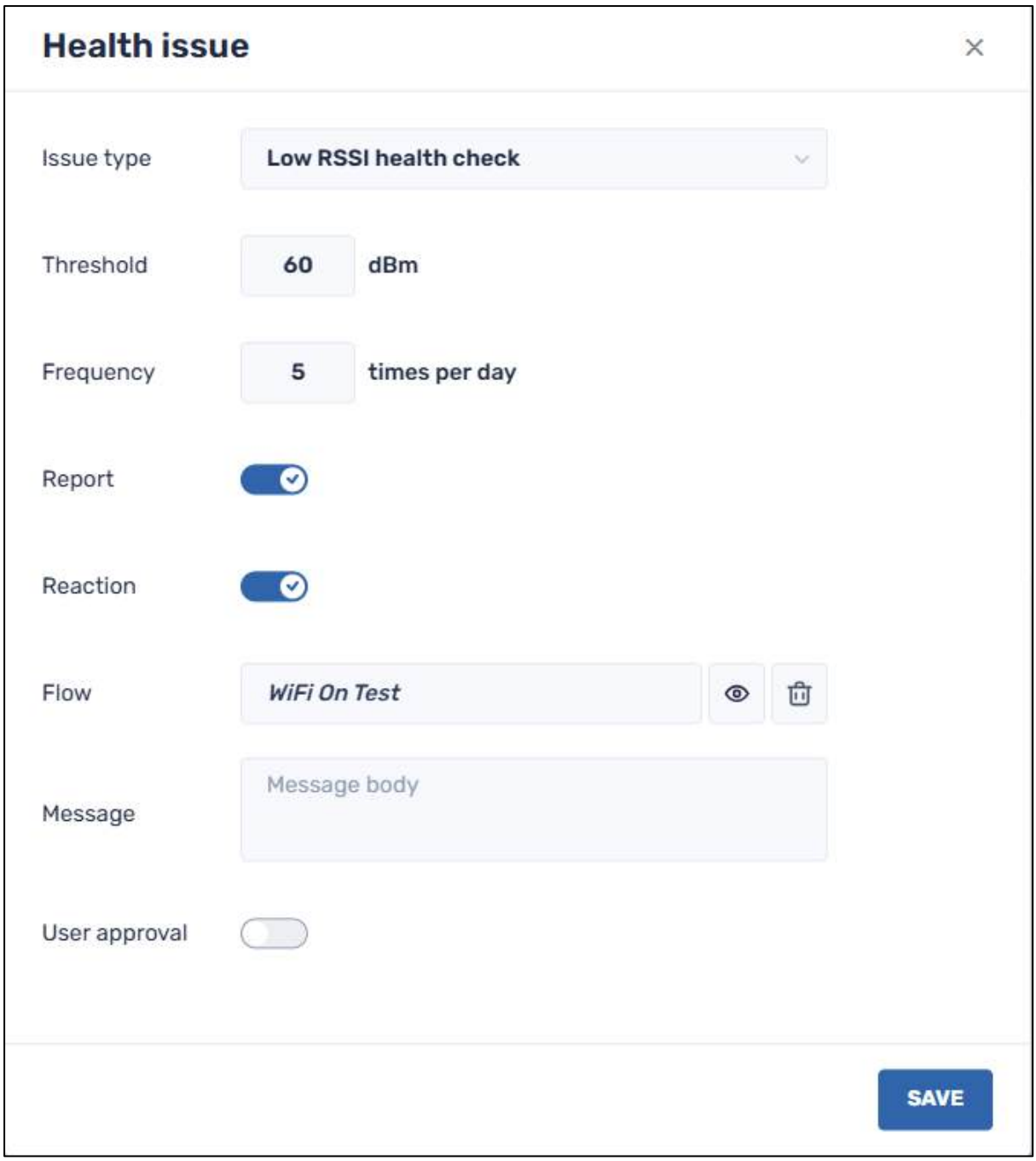
When you select this health issue option, the following window opens:



You supply a battery threshold level in the **Threshold** window. In the above example, a message will be sent to the Radix Device Manager if the battery level on a device drops below 15%.

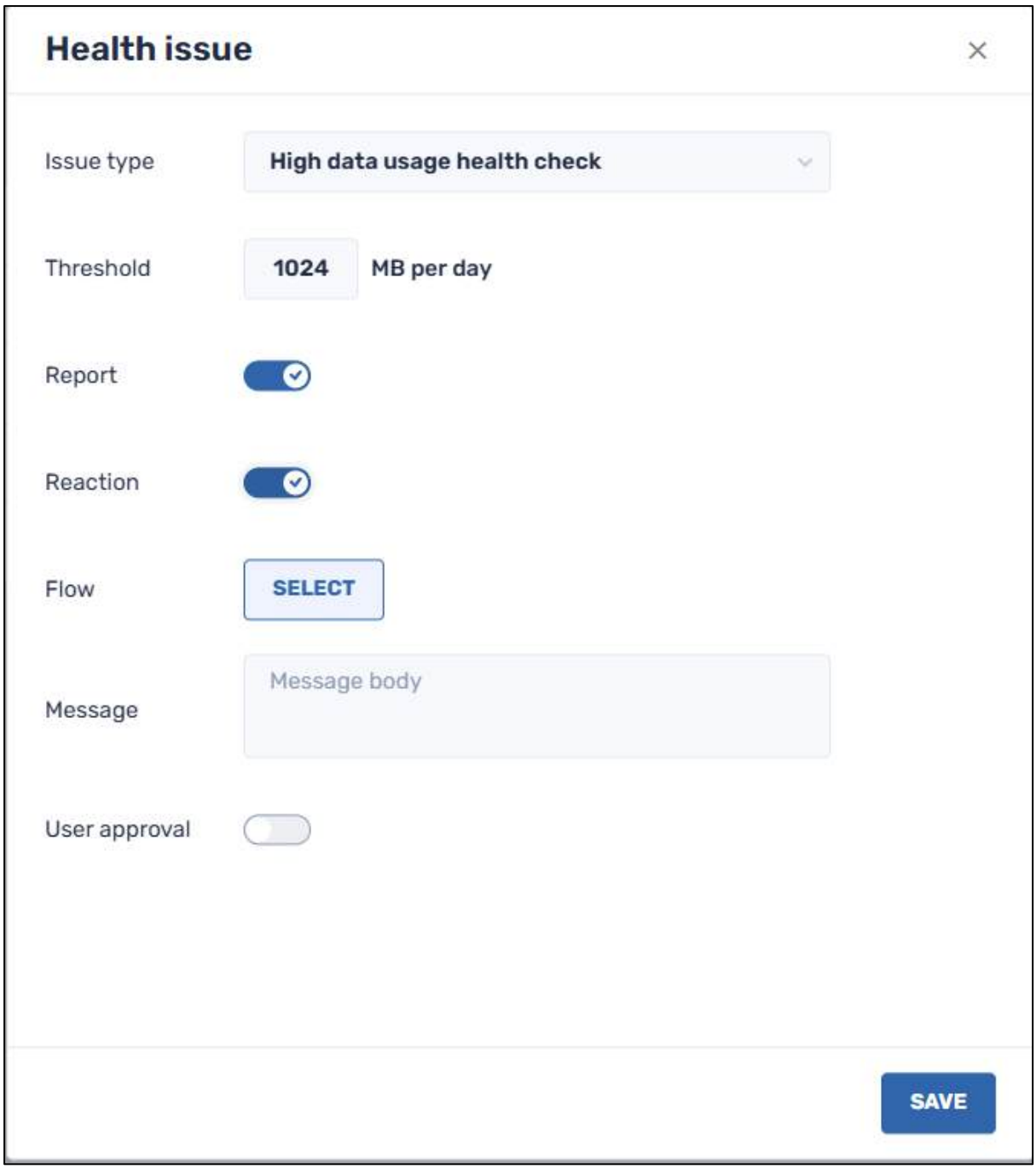
8.3 Low RSSI health check

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 60 dBm five times a day or more.



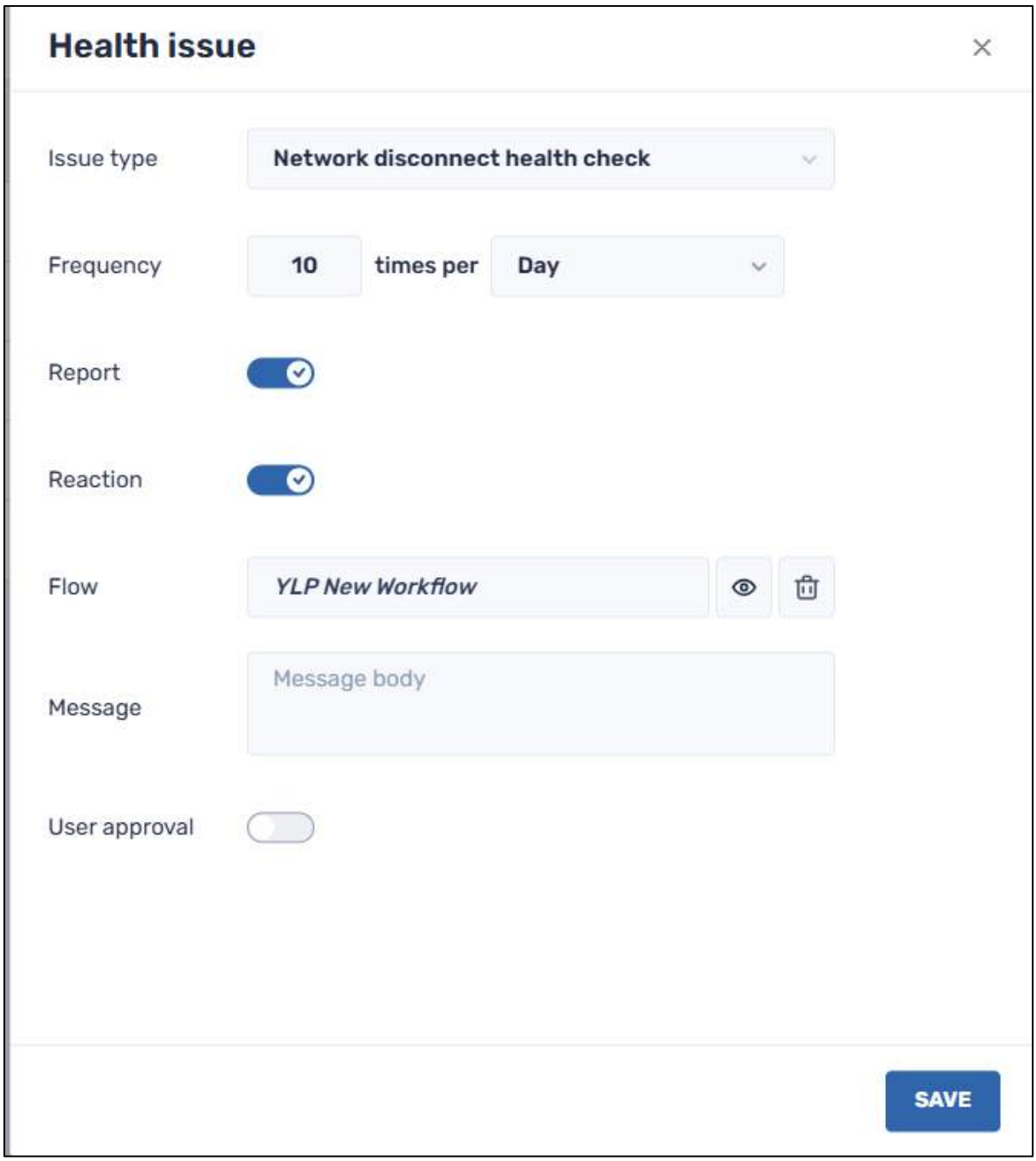
8.4 High data usage health check

This setting will send a message to the Device Manager if the data usage on a device exceeds a threshold amount. In the example below, the threshold was set at 1024 MB per day.

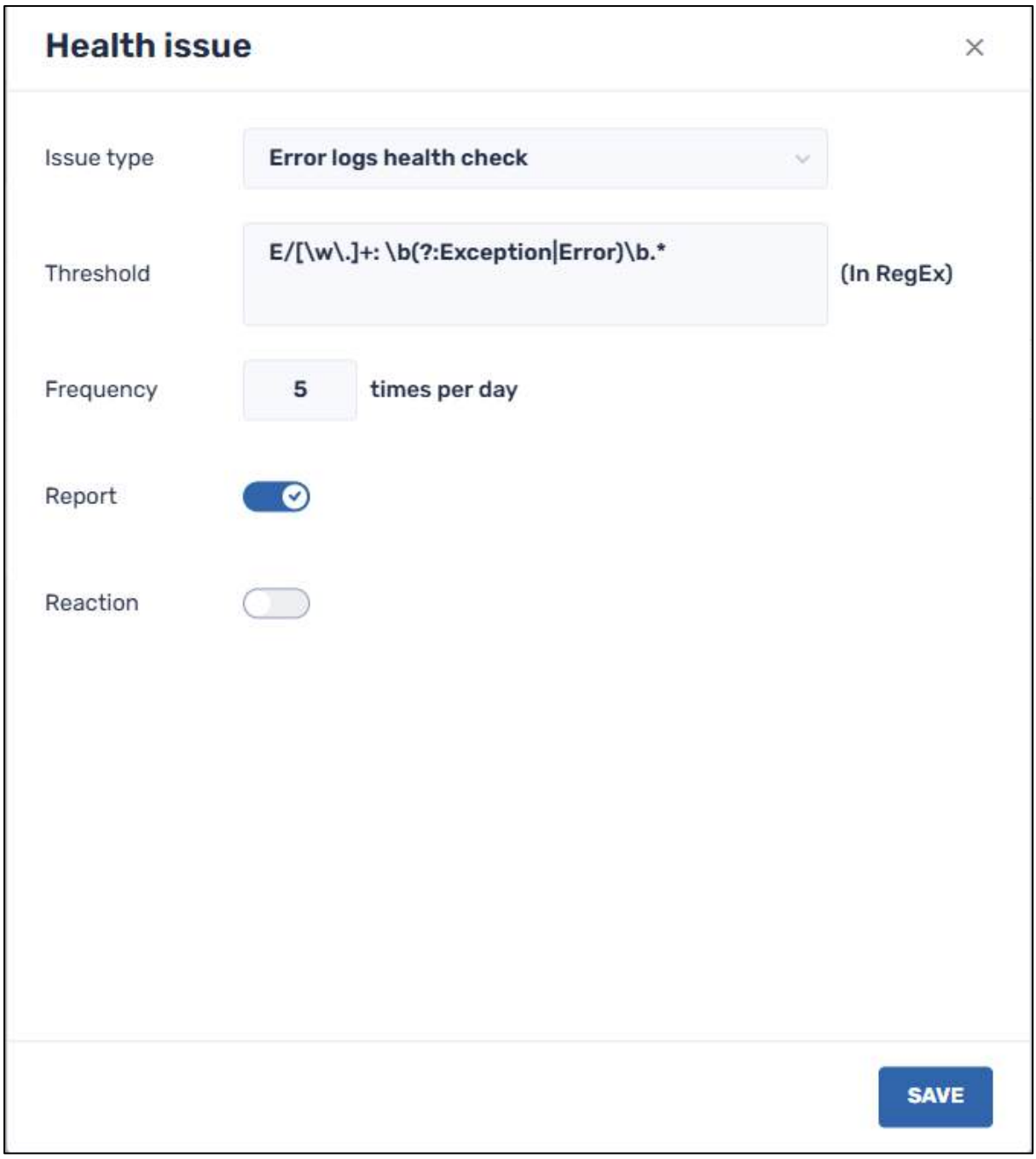


8.5 Network disconnect health check

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 Manager a message if a remote device disconnects from the network more than 10 times per day.



8.6 Error logs health check



Chapter 9. Repositories Console

In the Repositories Console, you can create and/or store software packages, scripts, device settings, workflows of commands, and more. Once these repositories are stored in the Radix Device Management system, they can be accessed and applied to selected devices elsewhere in the Radix Device Management interface.

When you select the **Repositories** icon in the Radix Device Management Dashboard, the grid of Repository options is displayed.

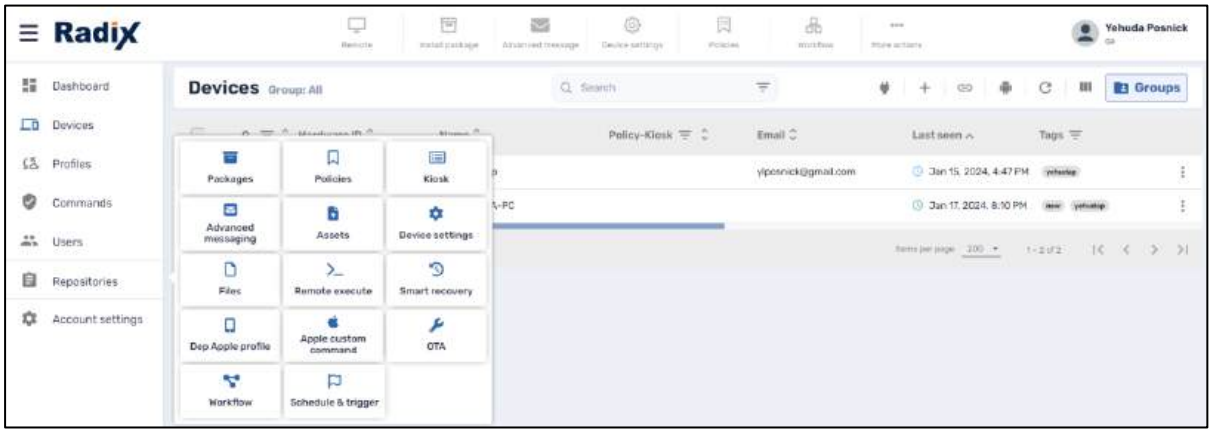


Figure 9-1: Repositories Options

Here is a summary of the Repository options:

Table 9-1: Repository Console Options

Icon	Description
Packages	Allows you to upload software packages into the Radix Device Management interface. These packages can be installed using the **Install Packages** command, as described in **Section 4.1.2**.
Policies	Allows you to create a software policy, blocking certain apps that may have security or performance issues. These policies can be applied to devices, using the **Policies** command. See **Section 4.1.5**.
Kiosk	Allows you to create a limited set of apps to be used on a device, so that the device functions only as a display in a kiosk. See **Section 4.2.1.8**, on how to apply a Kiosk option to a device.
Advanced messaging	Allows you to create a text message with an image, a sound file, a YouTube video, or even an interactive HTML form. See **Advanced Messaging** in **Section 4.1.3**, to see how an advanced message can be applied to a device.
Assets	Allows you to add an asset (= an image or audio file) to the Radix Device Management interface, for use in other consoles.

Device settings	Allows you create a list of settings to be applied to selected devices. See also **Device Settings** in **Section 4.1.4.**
Files	Allows you to create a repository of files to be sent to a device. They are sent with the **Send Files** command, as in **Section 4.2.1.16**.
Remote execute	Allows you to create specific command line arguments or scripts on a device. See **Remote Execute** in **Section 4.2.1.12** for information on how this is implemented.
Smart recovery	Allows you to select settings, to be implemented to restore a device's system configuration and settings to the latest system snapshot, or factory settings. See **Smart Recovery** in **Section 4.2.3.2**.
Dep Apple profile	Allows you to create a Device Enrollment Program (=DEP) for an Apple device. See also **DEP Apple Profile** in **Section 4.2.2.2**.
Apple custom command	Allows you to create a plist (=property list) file on a MacOS device. See also **Apple Custom Command** in **Section 4.2.2.1**, on how this plist is executed.
OTA	Allows you to remotely receive updates to an Android device's operating system or apps. See also **OTA** in **Section 4.2.1.11**, on how these OTA updates are applied.
Workflow	Allows you to create a series of commands to a device, to be executed sequentially. See also **Workflow** in **Section 4.1.6**, on how these Workflows are sent to a device.
Schedule & trigger	Allows you to create a command, as well as schedule when to execute the command by means of an assigned trigger. See also **Scheduler & trigger command** in **Section 4.2.1.15**.

9.1 Packages

This allows you to upload a software package from a URL, a file on your computer, a package from Google Play Store, or an iOS enterprise application. (The user of the device may have to complete the installation.) See **Section 4.1.2, Install Packages**.

9.2 Policies

This option allows you to create and apply a software policy to a device, blocking certain apps or software packages that either cause performance problems or security problems. After selecting the operating system (Android, iOS, MacOS, Windows, and ChromeOS), you then specify which apps to block, and how to activate the policy. See **Section 4.1.5, Policies**.

9.3 Kiosk

This option allows you to set up a device to be used as a display in a kiosk, such as in a storefront or hotel. You select particular apps that you want to be part of the kiosk display, as well as an appropriate background. See **Section 4.2.1.8** on how to apply a Kiosk option to a device.

9.4 Views

The **Views** repository option allows you to create a Kiosk option where you select allowed apps and access to single URL on the remote device. See **Views** in **Section 4.2.1.23**.

9.5 Advanced messaging

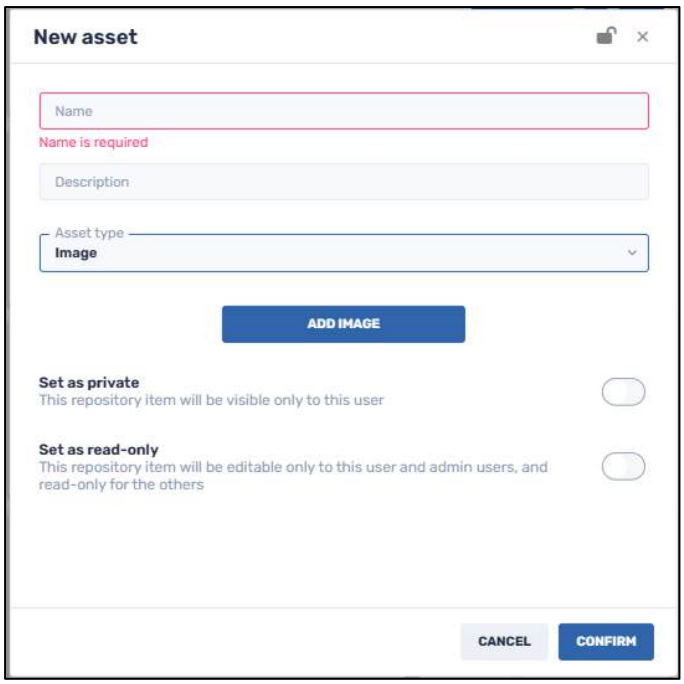
This option sends a text message with an image to a device. The message may be a "Welcome" message, a holiday greeting, or an emergency alert. See **Advanced Messaging** in **Section 4.1.3**.

9.6 Assets

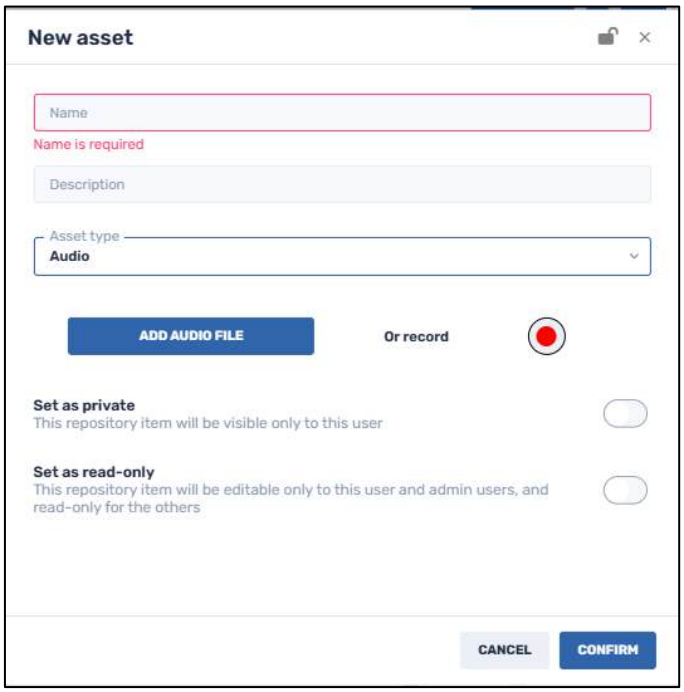
This option allows you to apply an asset, such as an image or audio file, to a device. This comes in handy if you wish to create an Advanced Message (**Section 4.1.3**). You may upload an audio file or record one using the Radix Device Management interface. You can then use these images or audio files in other Radix Device Management consoles.

To add a new asset:

1. Click on the **Add New** button at the lower left corner of the "Assets" screen. The "New asset" screen opens.



2. Assign a name and description to the new asset.
3. If you choose to add an image, click **Add Image**. You will be prompted to upload an image from your computer.
4. If you choose to add audio, you have the option of uploading an audio file by clicking **Add Audio File** or recording an audio file.



5. Click on the **Set as private** button if you want this new image or audio asset to be visible only to you (the creator of the item) when you log in to the Radix Device Manager.
6. Click on the **Set as read-only** button if you want to limit who can edit this asset. 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 **Confirm**. The new Asset will now appear in the Assets Repository.

9.7 Device Settings

This option allows the Radix Device Management user to create a configuration of device settings that can be saved and applied to a fleet of devices at once. The settings could include selecting a type of keyboard, enabling or disabling a screen saver, configuring a printer, or performing a reset on the device. See also **Device Settings** in **Section 4.1.4**.

9.8 Files

This option allows you to assign specific files to be sent to devices. The files can be from a computer, or from an URL. You will use the **Send Files** command as detailed in **Section 4.2.1.16** for sending files to devices.

9.9 Remote Execute

This allows you to create a command-line command or script and send it to a device. See **Section 4.2.1.12** for more details.

9.10 Smart Recovery

This allows you to select settings to be implemented to restore a device's system configuration and settings to the latest system snapshot, or factory settings. See **Smart Recovery** in **Section 4.2.3.2**.

9.11 DEP Apple profile

This allows you to set up a Device Enrollment Program (=DEP) for an Apple device. See also **DEP Apple Profile** in **Section 4.2.2.2**.

9.12 Apple Custom Command

This option allows you to create a plist (=property list) file to be applied to a MacOS device. See also **Apple Custom Command** in **Section 4.2.2.1**, on how this plist is executed.

9.13 OTA

This allows you to remotely receive updates to an Android device's operating system or apps. See also **OTA** in **Section 4.2.1.11**, on how these OTA updates are applied.

9.14 Workflow

This allows you to create a series of commands to a device, to be executed sequentially. See also **Workflow** in **Section 4.1.6**, on how these Workflows are sent to a device.

9.15 Schedule & Trigger

This allows you to create a command to be sent to a device, along with a trigger for when to implement the command. The trigger can be timing, geofencing, a Wi-Fi signal, or upon startup of the device. See also **Scheduler & trigger command** in **Section 4.2.1.15**.

Chapter 10. Account Settings Console

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

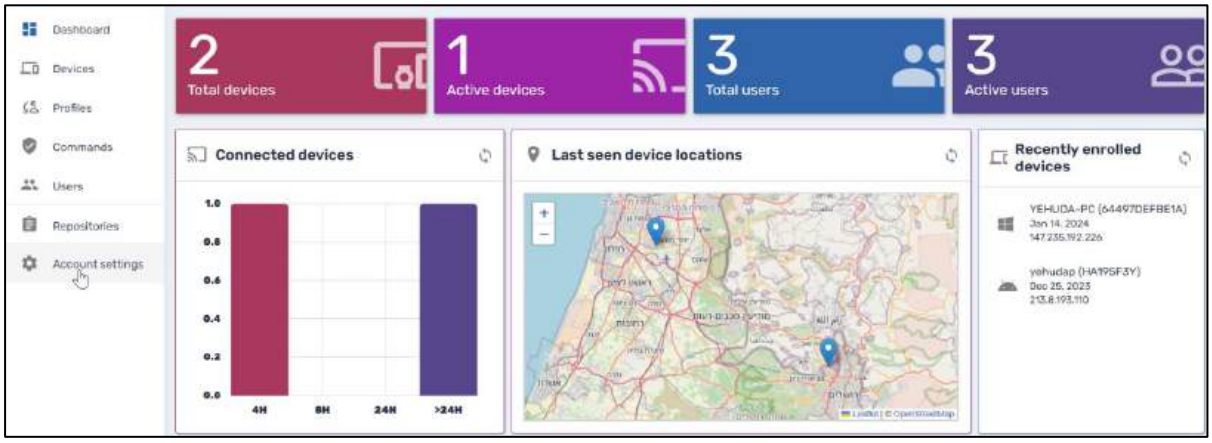
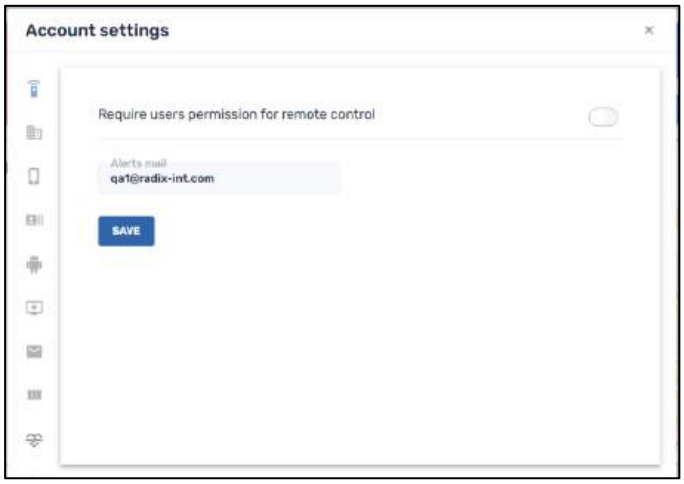


Figure 10-1: Account Settings icon in the Overview Dashboard

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



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

Table 10-1: Account Settings Options

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

We will go through the options in order.

10.1 Remote Control Option

Clicking on the "Remote Control" icon in the Account Settings Console gives the Radix Device Manager 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.

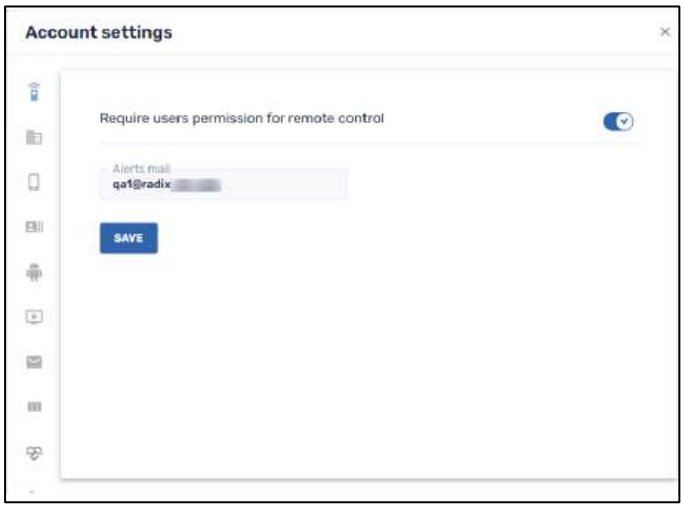


Figure 10-2: Account Settings Console, with permission for remote control option selected

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

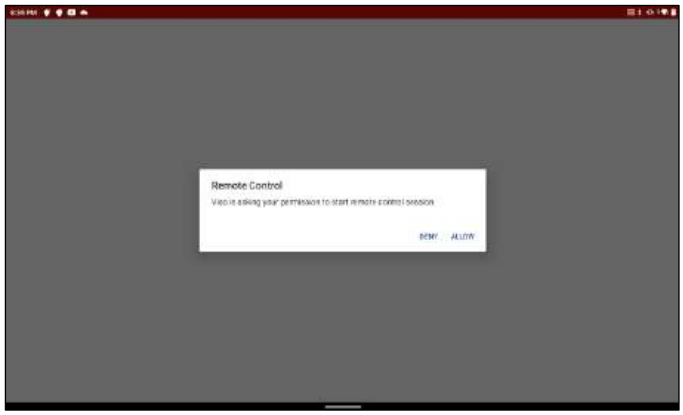


Figure 10-3:Prompt on the user's device, to allow remote control of a device

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:

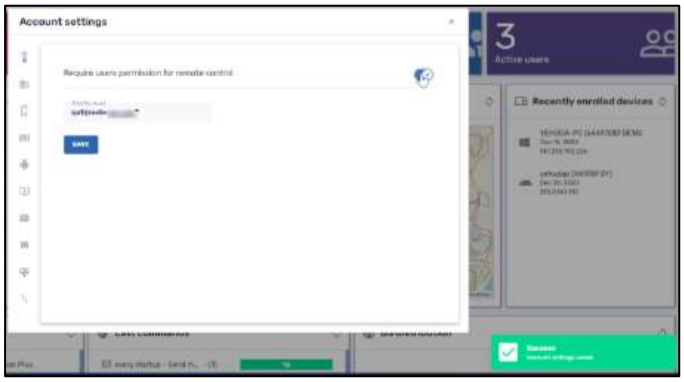


Figure 10-4: Notification of a successful change to the account

Note: This option is only for users with administrator privilegies. 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:

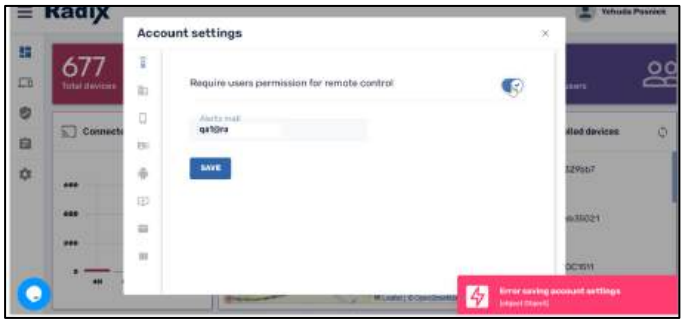


Figure 10-5: Error message for user without Admin privileges

10.2 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.

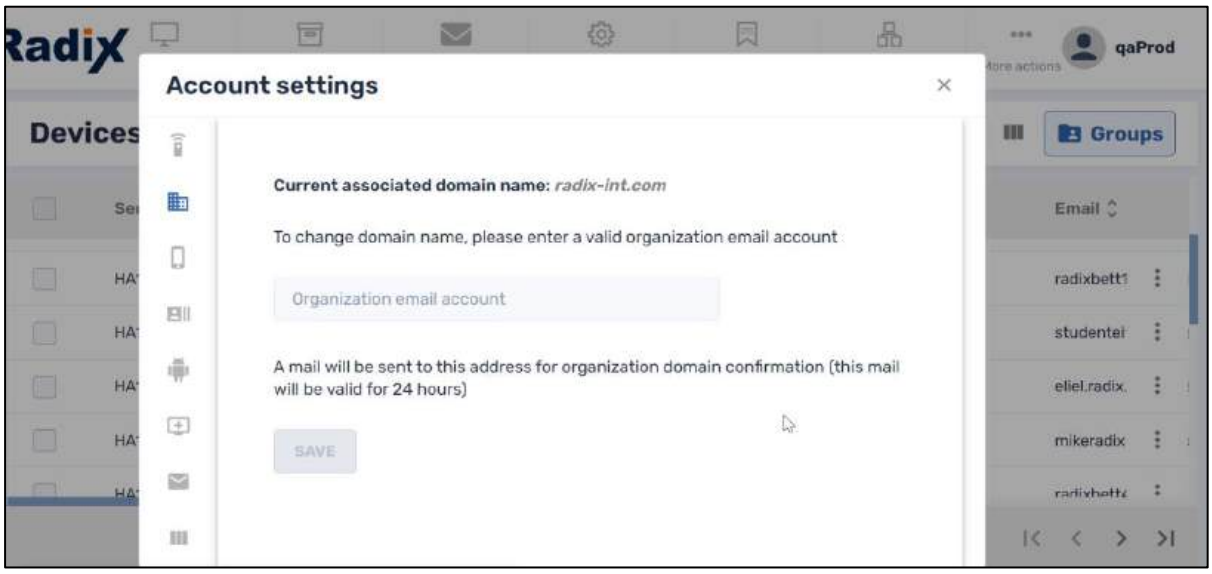
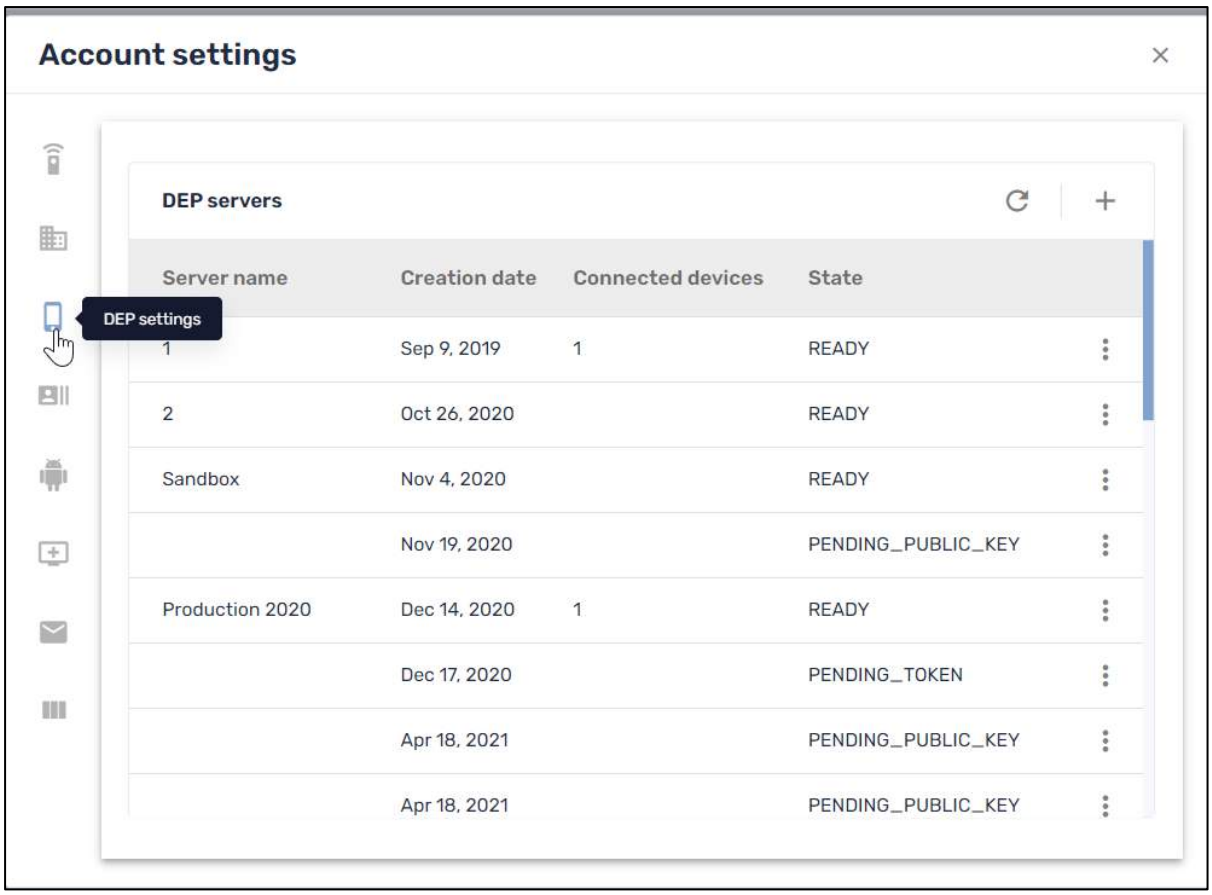


Figure 10-6: Dialog Box to select a domain

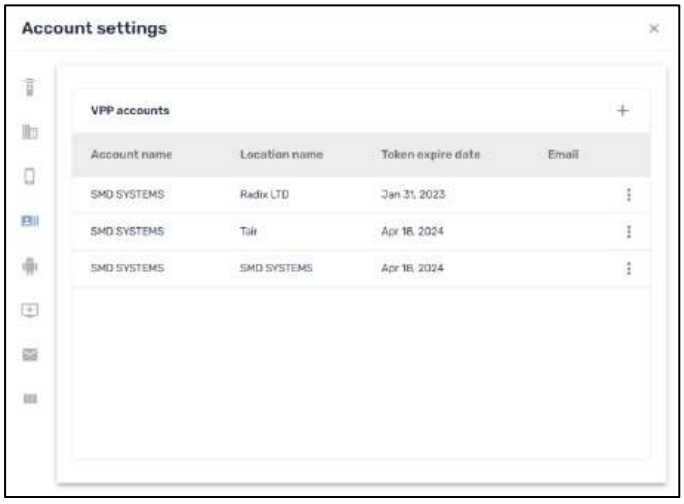
10.3 DEP Settings

There is also an option to use the Device Enrollment Program (=DEP) to connect your device.



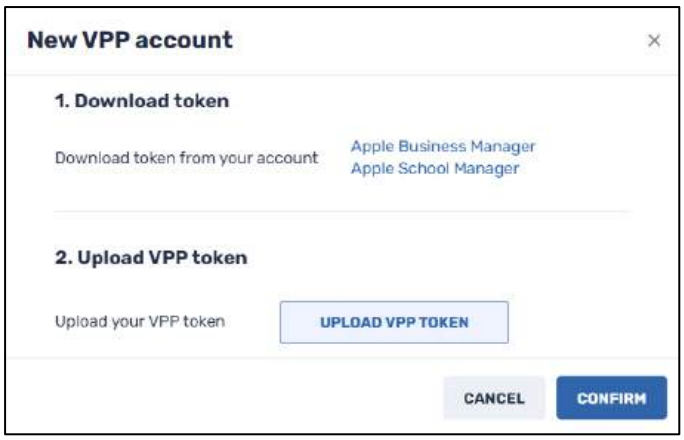
10.4 VPP Settings

This displays existing Apple VPP (=Volume Purchase Program) accounts, allows you to edit them, or add an additional VPP account.



To add a new VPP account:

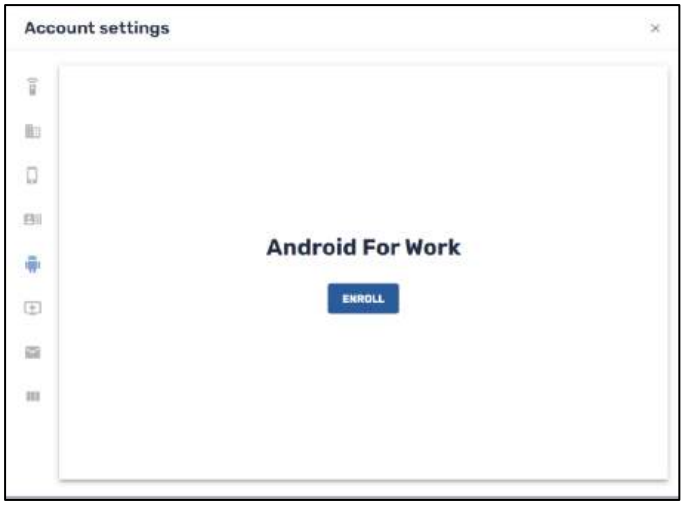
1. Click on the **Add VPP account** icon +. The **New VPP account** dialog box opens.



2. Download a VPP token from the Apple website after entering the Apple ID for your device.
3. Upload the VPP token from your computer by clicking on **Upload VPP Token**.
4. Click **Confirm** to apply the VPP token to your device.

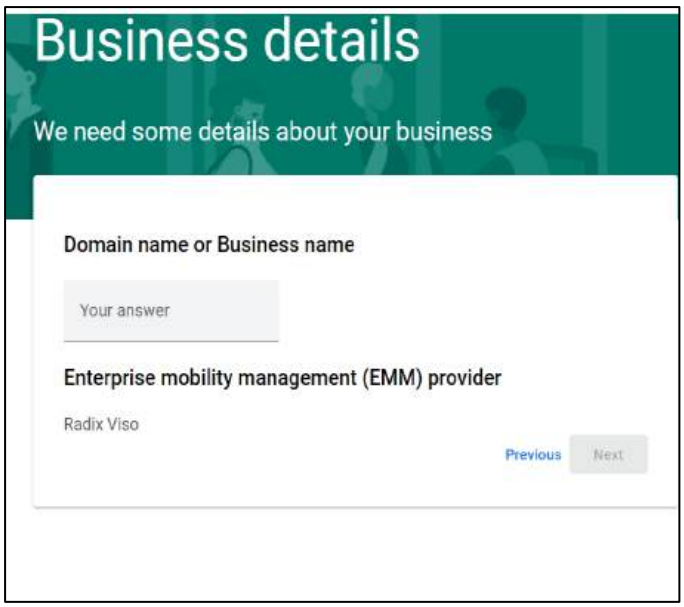
10.5 Android for Work

When you click on the **Android for Work** icon, you get a prompt to enroll your Android device. This will enable you to use Mobile Device Manager (=MDM) software on your Android device in a manner that is secure.

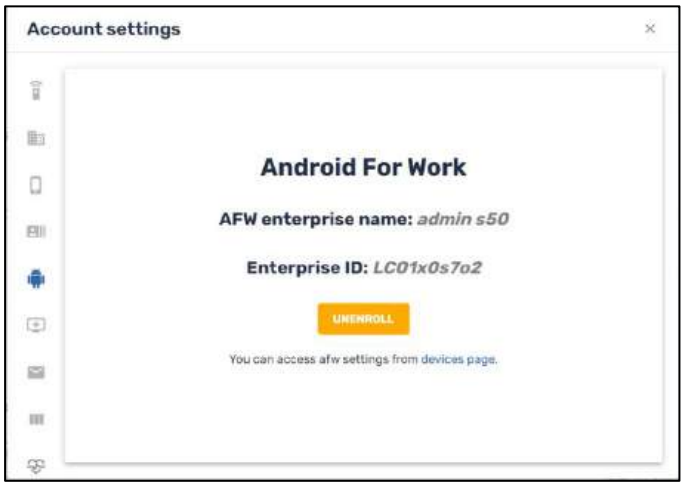


After you click on the **Enroll** prompt, the Google Play app opens:

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

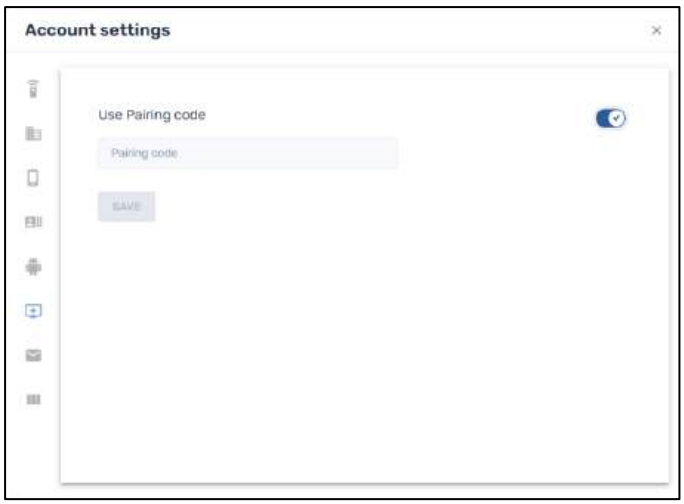


Once a device is enrolled in Android for Work, you will see the following screen in the account settings:



10.6 Device Pairing Option

This option adds another level of security to remote devices. When the Radix Device Manager 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.



10.7 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.

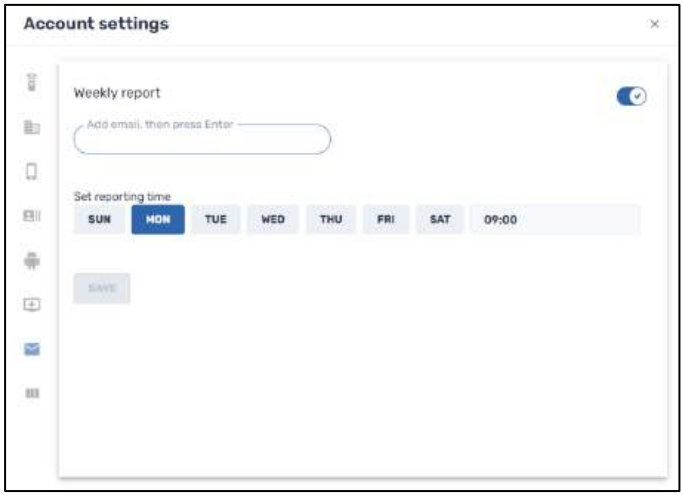


Figure 10-7: Interface to select email addresses, day, and time to send a weekly report

10.8 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.

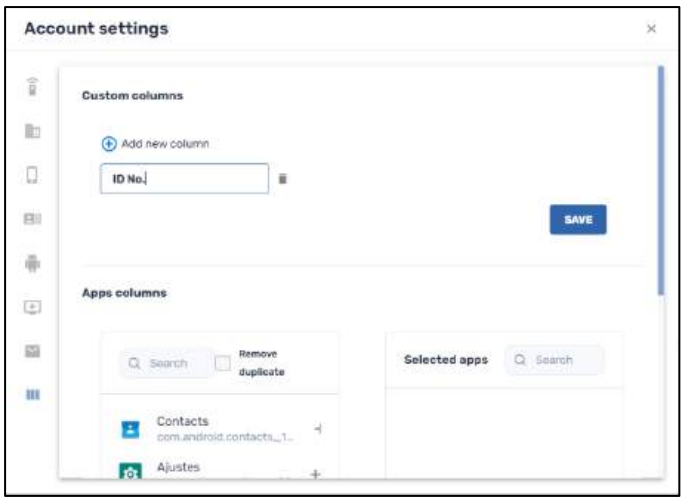


Figure 10-8: Window to select columns to be displayed

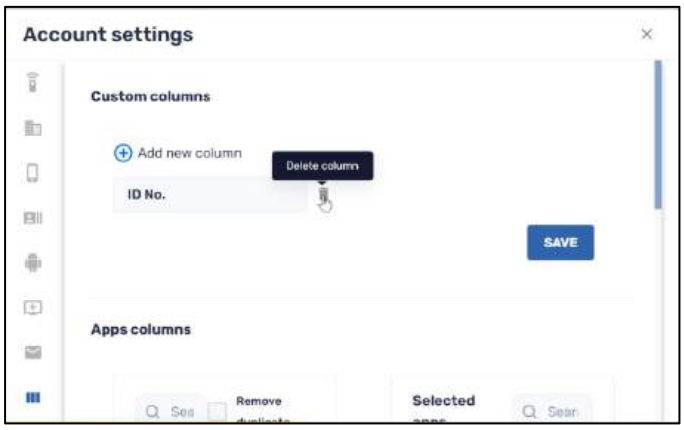
To add a new column heading:

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.

To delete a column that you have added:

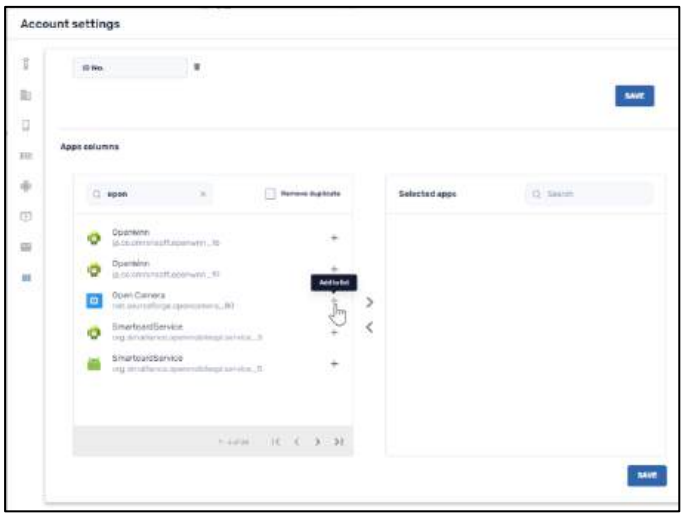
1. Click on **Add new column**. The "Type the column name" textbox appears.
2. Type in the name of the existing column heading that you want to delete and click on the Delete Column icon .



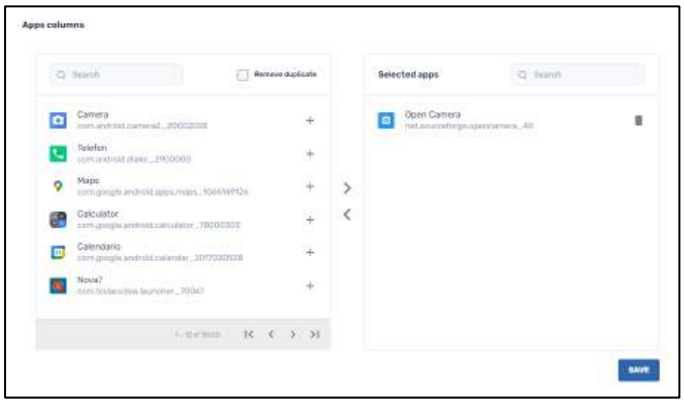
3. At the **Delete column** prompt, click **Yes**. The column name will be removed from the list of columns heading options.

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

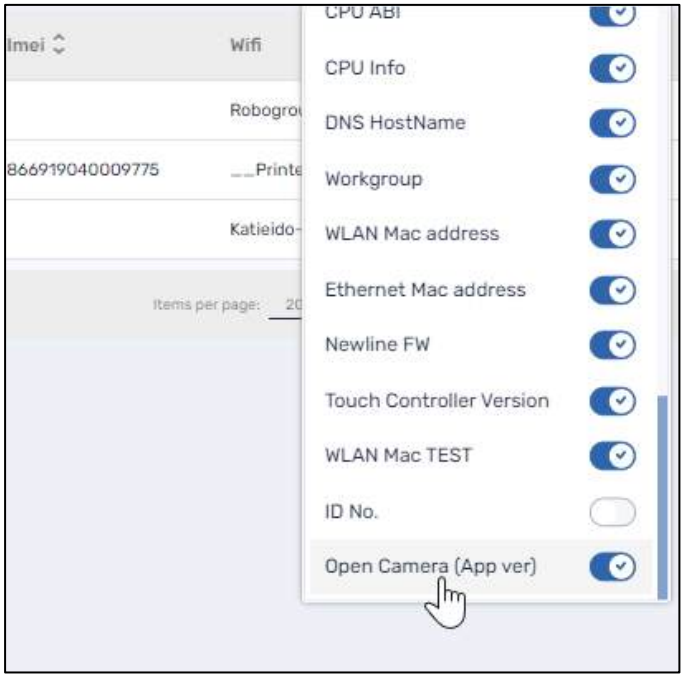
1. Search for the app from the list, either using the Search bar, or by scrolling through the options.



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.



10.9 Health Check Thresholds Option

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

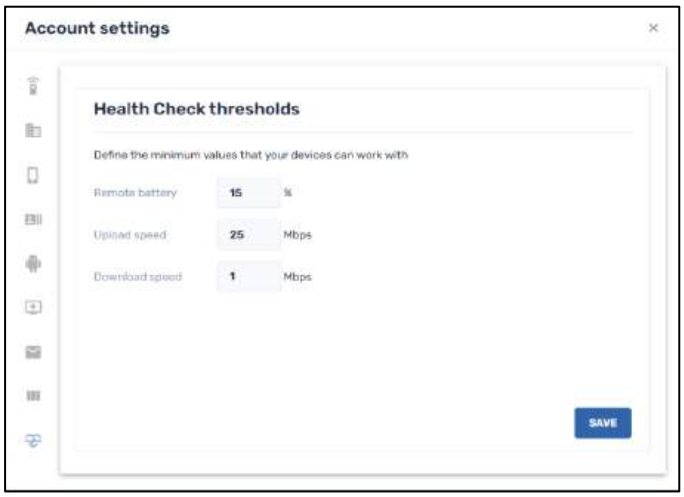


Figure 10-9: Health Check Thresholds Window

10.10 Import Tags and Labels

There is an option in the Radix Device Manager 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:

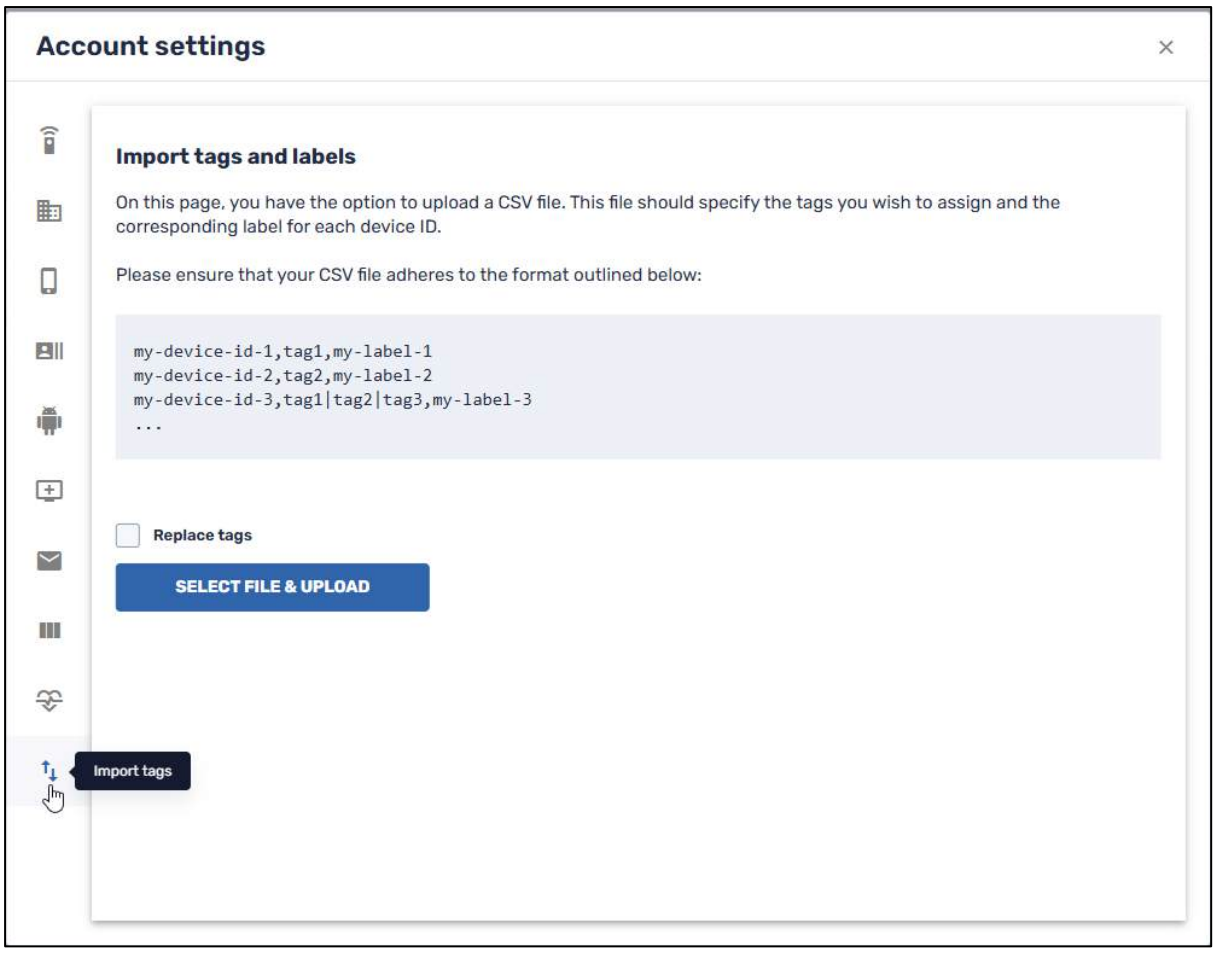
- Both the device name and its tags,
- Just the device names, or
- Just the tags.

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 Manager.

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. (A file created using Word or Excel may not work, even if you save it as a .txt file.)
3. If the upload is successful, you will receive a notification that it succeeded in the lower right-hand corner.

10.10.1 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:

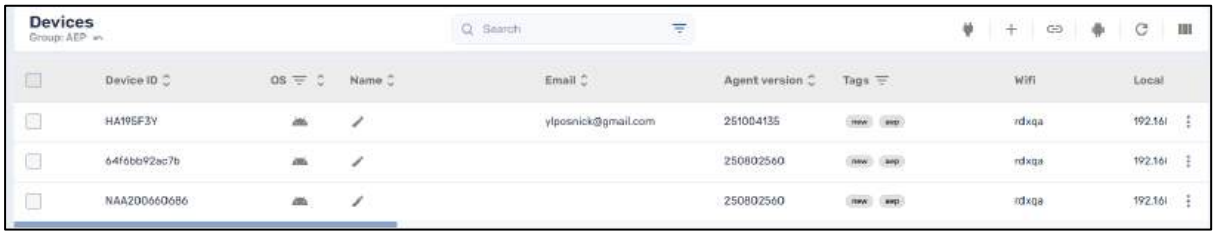
- You separate the fields for **Device ID**, **Device Label**, and **Tags** with a comma. In the option where you only assign tags, remember to put a comma at the end of the list of tags, even though you do not intend to assign a label the device.
- There should be **no** spaces between the various parameters.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

10.10.2 Practical Examples

10.10.2.1 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.

1. We have created a group "AEP," with the following three devices.



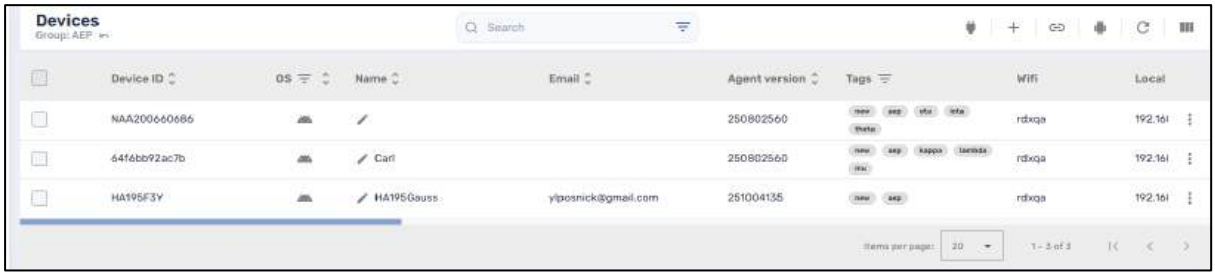
Initially, the data is as follows:

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

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

3. 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:

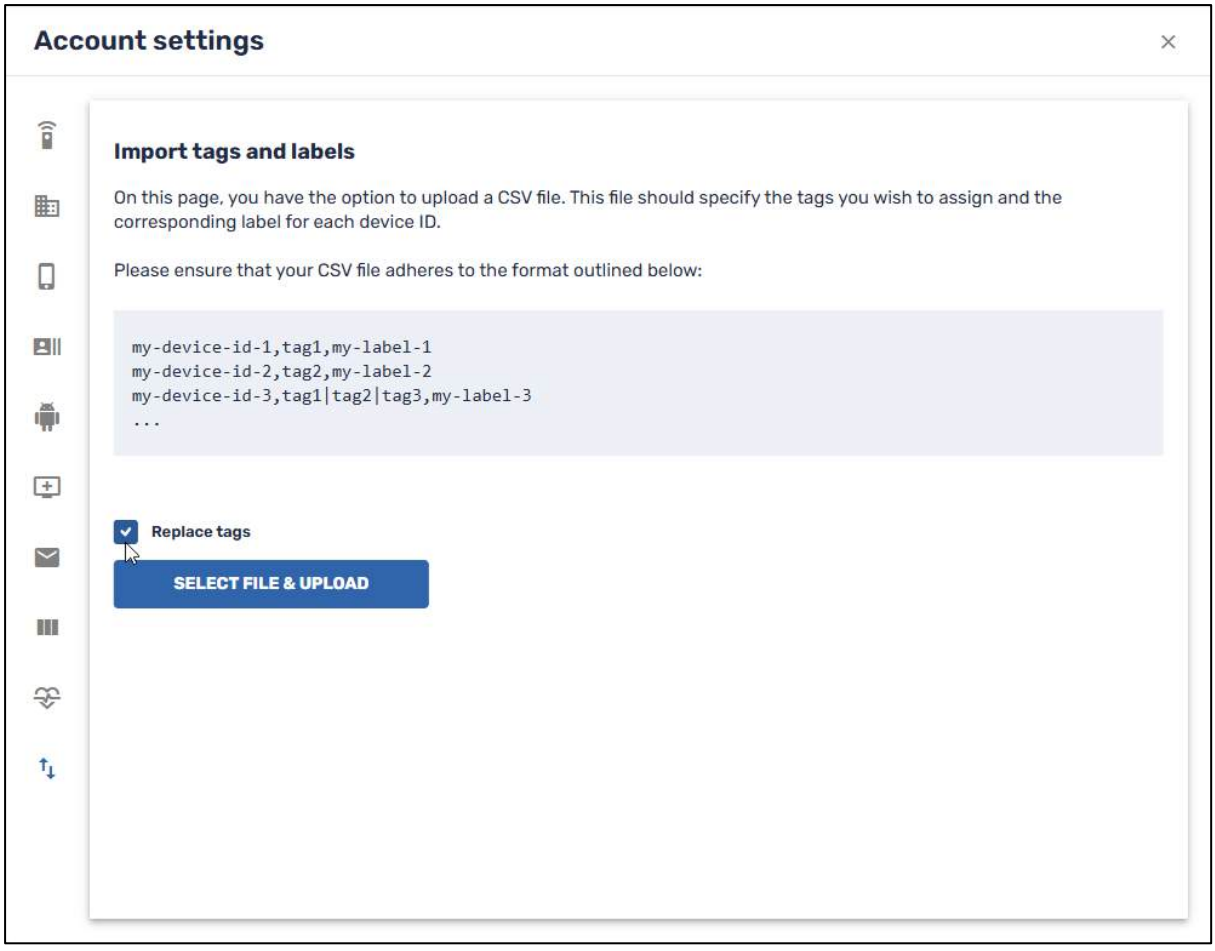


The labels and tags are now as follows:

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

10.10.2.2 Example 2: Overwriting Tags and Labels

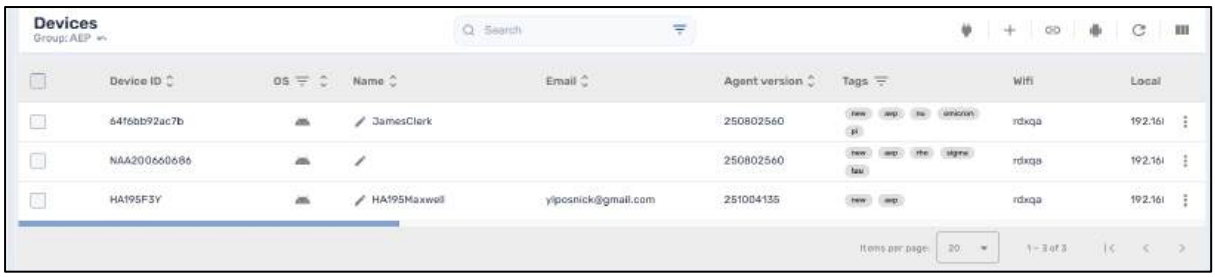
There is also an option to overwrite the existing tags on the devices, by clicking the **Replace Tags** box.



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

Note: We will have to retain the tags “new” and “AEP,” so that the devices remain in the group AEP. If we overwrite the existing tags, the devices will lose the “aep” tag and will no longer be members of the AEP group.

The group AEP will appear as follows in the Radix Device Manager:



Here is a summary of the results:

Device ID	Initial Device Label	Initial Device Tags
64f6bb92ac7b	JamesClerk	new, aep, nu, omicron, pi
HA195F3Y	HA195Maxwell	new, aep
NAA200660686		new, aep, rho, sigma, tau

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.

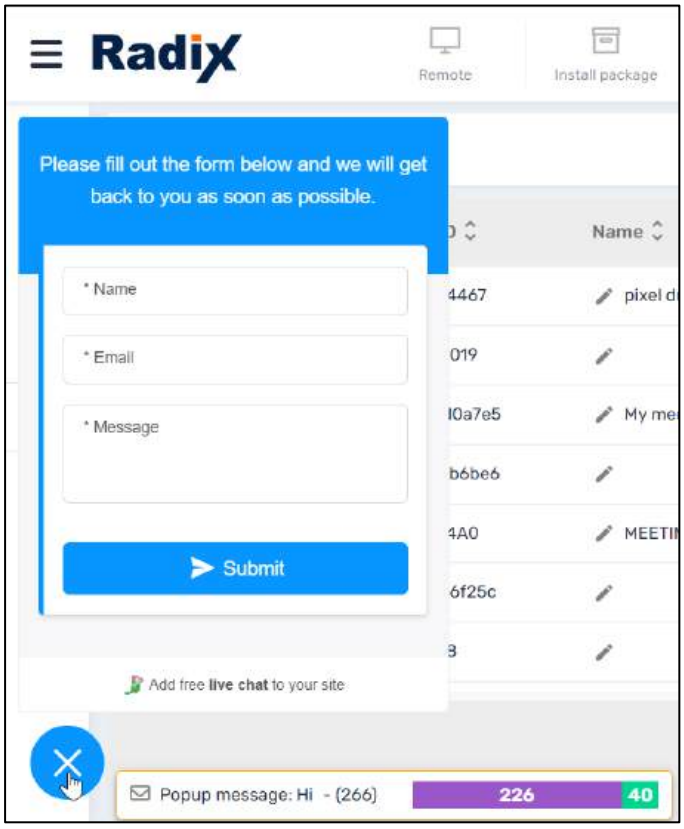


Figure 11-1: Customer Request Form

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 Manager, 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. The **Command Grid** opens.

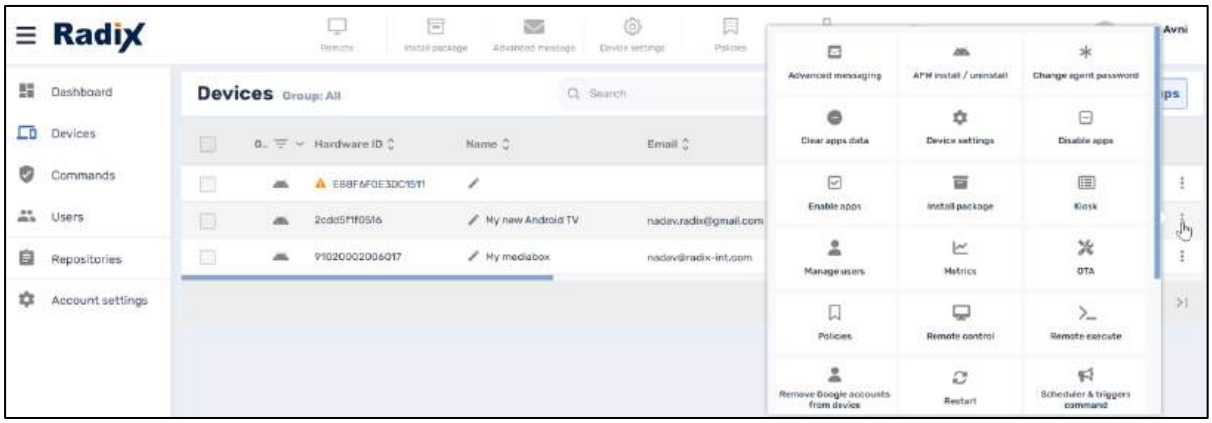
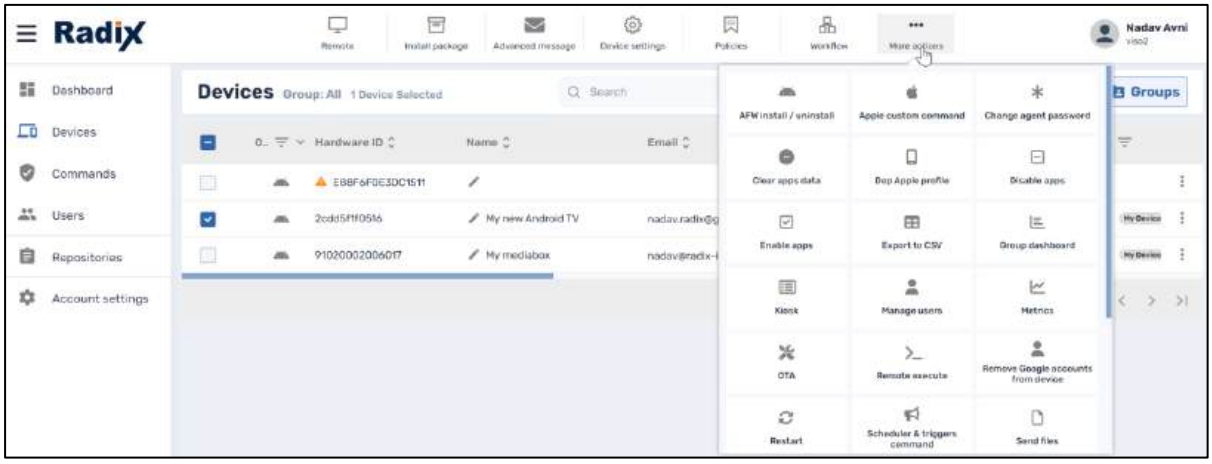


Figure 12-1: Commands Grid as accessed from the device's three-dot menu

Method 2: From the Devices Console Ribbon:

1. Click on the **Devices** icon on the left side of the Dashboard.
2. In the list of devices, select a particular device by checking its checkbox in the far-left column. The icons for commands in the Devices Console Ribbon will become active.
3. The Devices Console Ribbon already has icons for:
    - **Remote Control** of a device,
    - **Install Package**, to install a software package or app on a device,
    - **Advanced Messages**, to send a message that can combine audio and visual content,
    - **Device Settings**, to adjust a device's settings,
    - **Policies**, to block or allow particular applications, and
    - **Workflow**, to send a series of commands to be implemented in order.

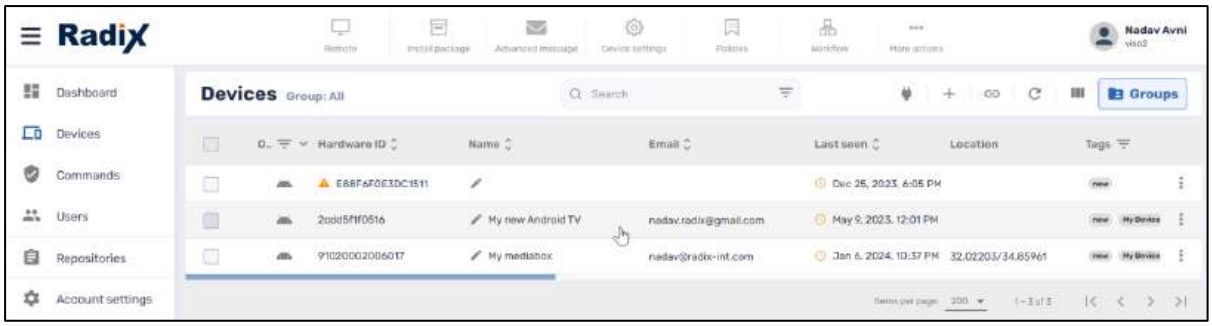
4. By clicking on the **More actions** icon, you can access all other available command options:



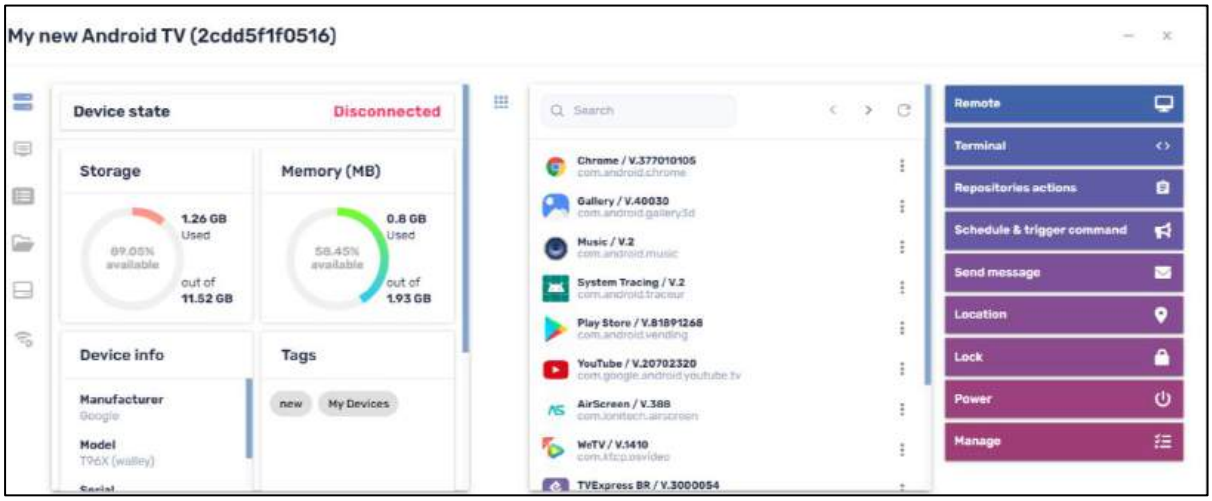
Method 3: From the Device Dashboard:

The Device Dashboard will allow you to access a sizeable number of the available commands. But only the previous two methods allow access to **all** available commands.

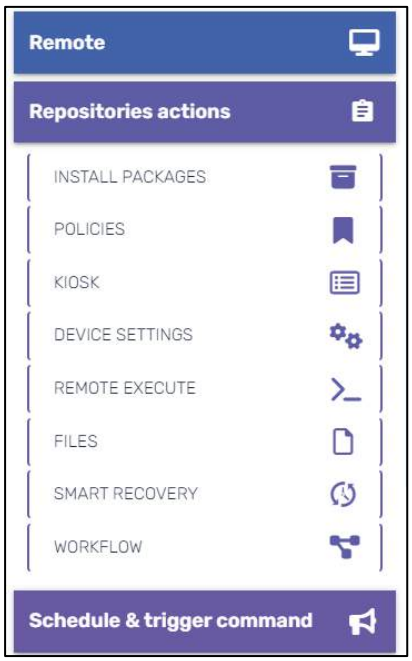
1. Click on the **Devices** icon on the left side of the Dashboard.
2. Click on the row of any of the devices listed.



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,
  - The Devices Console Ribbon under the **Advanced message** icon,
  - The Device Dashboard, under the **Repositories actions** tab, under **Advanced messaging**.
- **Further Details**: This is discussed in detail in **Section 4.1.3, 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,
  - The Devices Console Ribbon under the **More options** icon.
- **Further details**: This is discussed in detail in **Section 4.2.1.1, Android for Work (AFW) install/uninstall** as well as in **Section 10.5, Android for Work**.

12.1.3 Apple Custom Command

- **Function**: This option allows you to execute a plist (=property list) file on a MacOS or iOS device.
- **Access**: The Apple Custom Command feature can be accessed by:
  - The device's three-dot menu,

- The Devices Console Ribbon under the **Advanced message** icon,
- The Device Dashboard, under the **Repositories actions** tab, under **Apple Custom Command**.

- **Further details**: This is discussed in detail in **Section 4.2.2.1**, **Apple Custom Command**.

12.1.4 Change Agent Password

- **Function**: This allows you to change a user's password.
- **Access**: The Change Agent Password feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon under the **More Actions** icon,
  - The Device Dashboard, under the **Manage** tab, under **Change Agent Password**.
- **Further details**: This is discussed in detail in **Section 4.2.1.2, 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,
  - The Devices Console Ribbon, from the **More Actions** icon.
- **Further details**: This is discussed in detail in **Section 4.2.1.3, 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,
  - The Devices Console Ribbon, from the **More Actions** icon.
- **Further details**: This is discussed in detail in **Section 4.2.1.4, Clear Apps Data.**

12.1.7 Collect 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,
  - The Devices Console Ribbon, from the **More Actions** icon,
- **Further details**: This is discussed in detail in **Section 4.2.1.5, Collect Logs**.

12.1.8 DEP Apple profile

- **Function**: This allows you to set up a Device Enrollment Program (=DEP) for an Apple device.
- **Access**: The DEP Apple Profile command can be accessed from:
  - The device's three-dot menu,

- The Devices Console Ribbon, from the **More Actions** icon,
- The Device Dashboard, under the Repositories tab, under DEP Apple Profile.

- **Further details**: This is discussed in detail in **Section 4.2.2.2, DEP Apple profile.**

12.1.9 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.

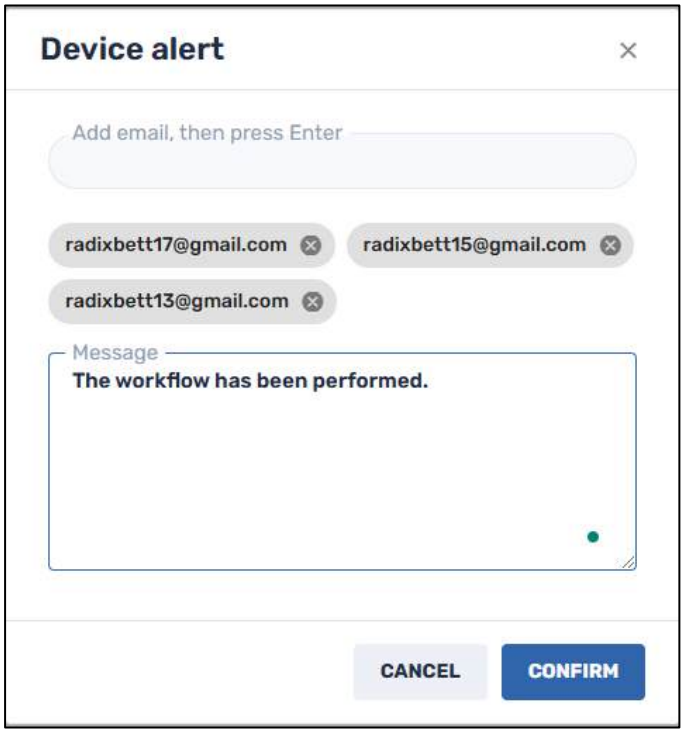


Figure 12-2: Window to send device alert

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.

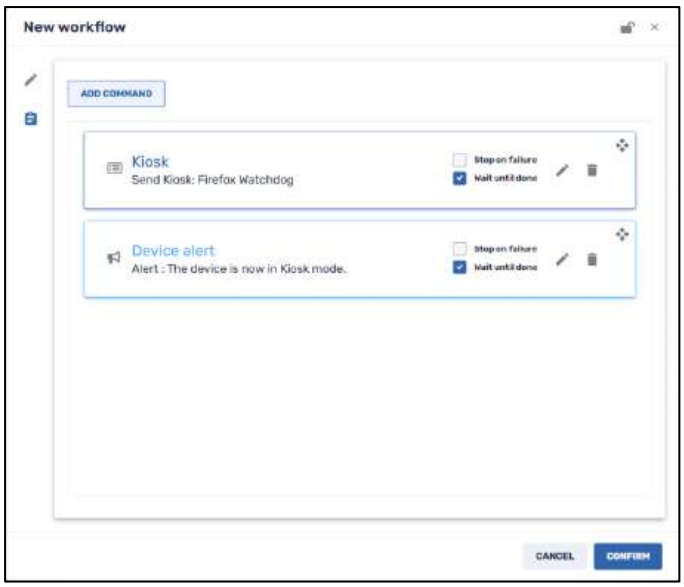


Figure 12-3: Workflow that illustrates use of Device Alert command

12.1.10 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
  - The Devices Console Ribbon from the **Device Settings** icon,
  - The Device Dashboard, from the **Repositories actions** tab under **Device Settings**.
- **Further details**: This is discussed in detail in **Section 4.1.4, Device Settings.**

12.1.11 Disable/Enable Apps

- **Function**: This allows you to remove an app from a device or reinstall it.
- **Access**: You can access the Disable/Enable Apps command by
  - The device's three-dot menu,
  - The Devices Console Ribbon, from the **More options** icon.
- **Further details**: This is discussed in detail in **Section 4.2.1.6, Disable/Enable apps.**

12.1.12 Export Blue Screen Data (Windows Devices Only)

- **Function**: This sends information about a system crash in Windows. The data comes in the form of an Excel spreadsheet, listing the Device ID, details of the blue screen error, and when the blue screen appeared.
- **Access**: You can access the Export Blue Screen Data command from a Windows device's three-dot menu.
- **Further details**: This is discussed in detail in **Section 4.2.3.1, Export Blue Screen Data**.

12.1.13 Export 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
  - The Devices Console Ribbon, from the **More options** icon,

- In the Groups three-dot menu, from the pane of commands on groups,
- In the Commands console, and in other windows where data is displayed.

You can choose to display all columns available, or only the columns currently shown in the **Devices** table.

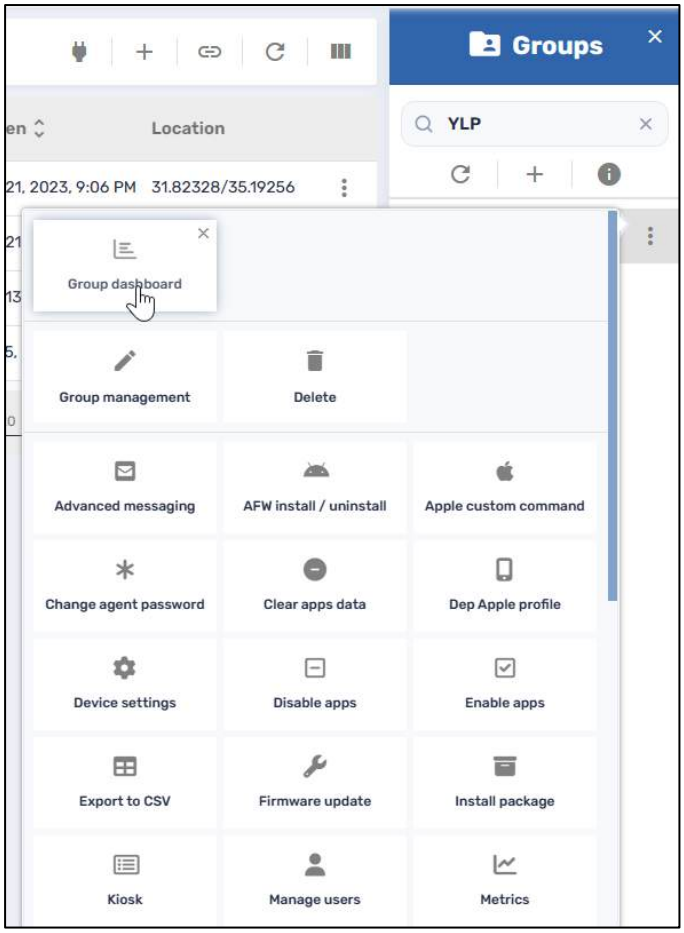
Figure 12-4: Export to CSV selection options

12.1.14 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,
  - The Devices Console Ribbon from the **Device Settings** icon.
  - The Device Dashboard, under **Manage>Firmware Update**.
- **Further details**: This is discussed in detail in **Section 4.2.1.7, Firmware Update.**

12.1.15 Group Dashboard

- **Function**: The **Group Dashboard** command displays the statistics for the devices in a group.
- **Access**: This can be accessed from the three-dot menu of a group in the **Groups** window.



The Group Dashboard appears as follows:

- **Further details**: Creating and managing groups is described in greater detail in **Section 4.3.8, Grouping Devices**.

12.1.16 Group Management

- **Function**: If you have created a group, but want to perform modifications, use the **Groups Management** command tile. This is especially useful for installing mandatory applications on many devices simultaneously.
- **Access**: You can access the Group Management command from a Group's three-dot menu in the Device Console:

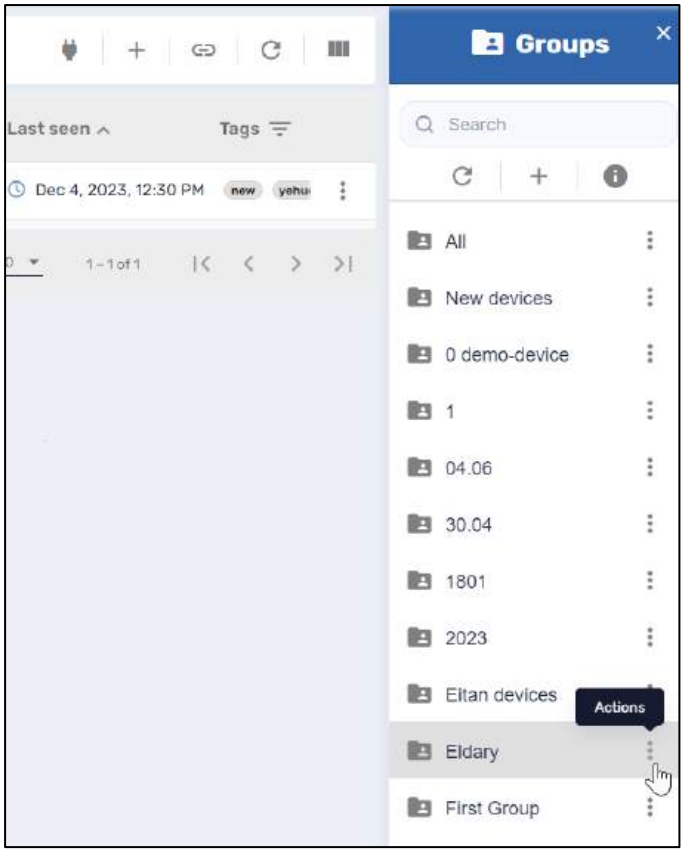


Figure 12-5: Three-dot menu for the Group "Eldary"

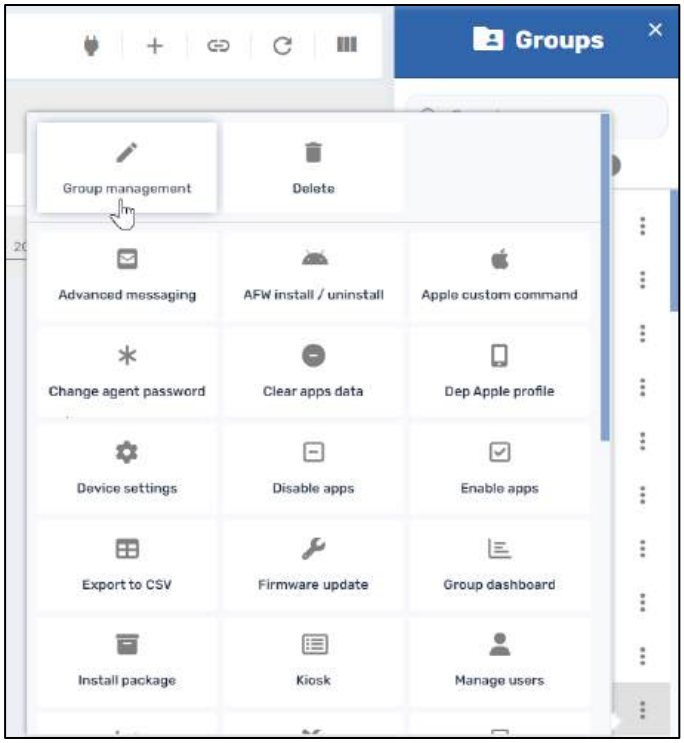


Figure 12-6: Group Management tile in the Groups commands

- **Further details**: The Group Management option is discussed in **Section 4.3.8.3, Group Management Options**.

12.1.17 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
  - The Devices Console Ribbon, under the **Install package** icon,
  - The Device Dashboard, from the **Repositories** tab, under **Install Packages**.
- **Further details**: The Install Packages command is treated in **Section 4.1.2, Install Package**.

12.1.18 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,
  - The Devices Console Ribbon, under the **More actions** icon,
  - The Device Dashboard, from the **Repositories** tab, under **Kiosk**.
- **Further details**: The Kiosk command is treated in **Section 4.2.1.8, Kiosk**.

12.1.19 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,
  - The Devices Console Ribbon,
  - The Device Dashboard, under **Manage Users**.
- **Further details**: The Manage users command is discussed in **Section 4.2.1.9, Manage users**.

12.1.20 Metrics

- **Function**: This provides graphical displays of app usage on a device, to see the frequency with which apps are used on a device.
- **Access**: The Metrics feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, under **More actions**.
- **Further details**: The Metrics command is discussed in **Section 4.2.1.10, Metrics**.

12.1.21 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Repository actions** tab, under **OTA**.
- **Further details**: The OTA command is discussed in **Section 4.2.1.11, OTA**.

12.1.22 Policies

- **Function**: The 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 Policies feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, under **Policies**,
  - The Device Dashboard, under the **Repositories actions** tab, under **Policies**.
- **Further details**: Creating and applying policies to devices is dealt with in **Section 4.1.5, Policies**.

12.1.23 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,
  - The Devices Console Ribbon from the **Remote** icon,
  - The Device Dashboard, from the **Remote** tab.
- **Further details**: This command is discussed in **Section 4.1.1, Remote Control**.

12.1.24 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Repositories Actions** tab under **Remote Execute**.
- **Further details**: The Remote Execute command is treated in **Section 4.2.1.12, Remote Execute**.

12.1.25 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Manage** tab.
- **Further details**: The Remove Google Accounts command is treated in **Section 4.2.1.13, Remove Google Accounts from Device**.

12.1.26 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Power** tab, under **Restart**.

- **Further details**: The Restart command is treated in **Section 4.2.1.14, Restart**.

12.1.27 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Schedule & trigger command** tab.
- **Further details**: The Scheduler & Trigger Command is treated in **Section 4.2.1.15, Scheduler & Triggers Command**.

12.1.28 Screen settings

- **Function**: This allows you to adjust the brightness and volume on flat panel devices.
- **Access**: The **Send Files** feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, under the Manage tab.
- **Further details**: The **Screen settings** command is treated in **Section 4.2.1.16, Screen Settings.**

12.1.29 Send 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Repositories action** tab, under **Files**.
- **Further details**: The Send Files command is treated in **Section 4.2.1.17, Send Files.**

12.1.30 Send Message

- **Function**: This command allows you to send a simple text message, with a message title and body, to a device.
- **Access**: The **Send Message** feature can be accessed by:
  - The device's three-dot menu.
  - The Devices Console Ribbon, under **More actions**.
  - The Device Dashboard, from the **Send Message** tab.
- **Further details**: The Send Message command is discussed in **Section 4.2.1.18, Send Message**.

12.1.31 Shutdown

- **Function**: This command shuts the device down remotely.
- **Access**: The **Shutdown** feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Power** tab, under **Shutdown.**
- **Further details**: The Shutdown command is treated in **Section 4.2.1.19, Shutdown**.

12.1.32 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 Devices Console Ribbon, under **More actions**.
- **Further details**: This command is discussed in **Section 4.2.3.2, Smart Recovery**.

12.1.33 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, or
  - The Devices Console Ribbon, under **More actions**.
- **Further details**: The Sound Siren command is treated in **Section 4.2.1.20, Sound Siren**.

12.1.34 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,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Manage** tab, under **Tags.**
- **Further details**: The Tags command is treated in **Section 4.2.1.21, Tags**.

12.1.35 Timeout

- **Function**: You can use this as part of the Workflow command (see **Section 4.1.6, 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 **Workflow>Add New Workflow>Add Command>Time out**.

12.1.36 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,
  - The Devices Console Ribbon, under **More actions**.
- **Further details**: For more information about the Uninstall Packages command, see **Section 4.2.1.22, Uninstall Packages**.

12.1.37 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,
  - The Devices Console Ribbon, under **More actions**,

- The Device Dashboard, from the **Repositories Actions** tab, under **Views.**

- **Further details**: This command is dealt with at length in **Section 4.2.1.23, Views.**

12.1.38 VPP Install/Uninstall

- **Function**: This allows you to install or uninstall a program via the Apple Volume Purchase Program (=VPP).
- **Access**: The **VPP Install/Uninstall packages** feature can be accessed by the Devices Console Ribbon, under **More actions**.
- **Further details**: For more information about the VPP Install/Uninstall options, see **Section 4.2.2.3, VPP Install/Uninstall**.

12.1.39 Wake on LAN

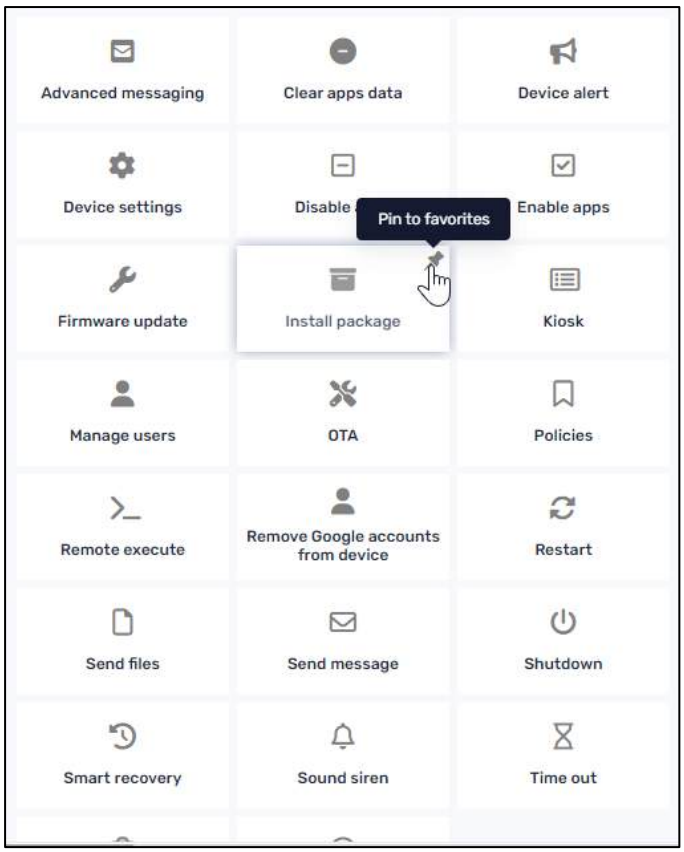
- **Function**: This option allows a device (or group of devices) to be turned on or "awakened" by means of a network message or a time trigger.
- **Access**: The **Wake on LAN** feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, under **More actions**,
  - The Device Dashboard, from the **Power** tab, under **Wake on LAN.**
- **Further details**: This command is dealt with at length in **Section 4.2.1.24, Wake on LAN.**

12.1.40 Workflow

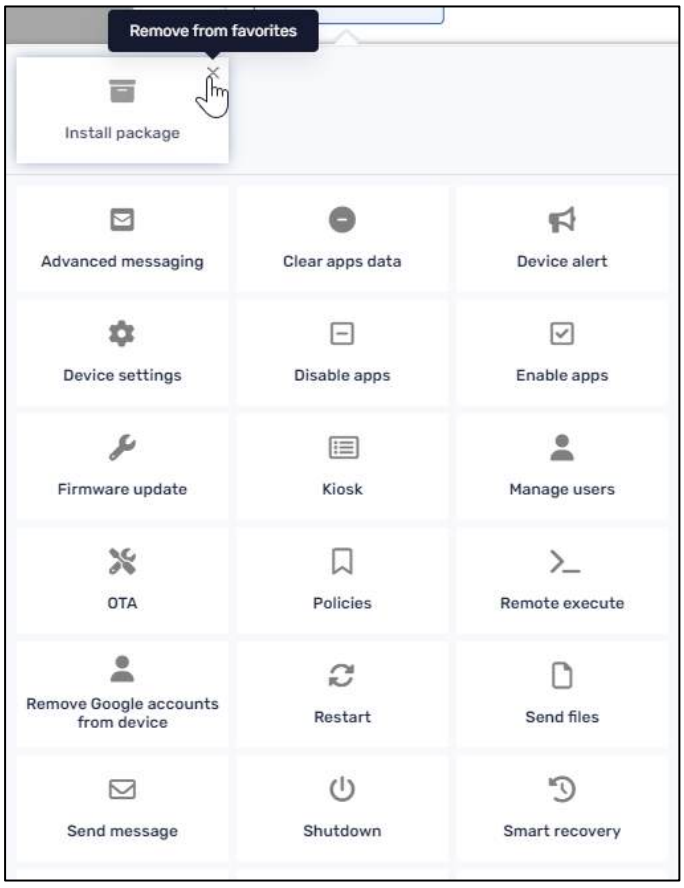
- **Function**: The Workflow command allows you to send a series of commands to be executed, one after the other, to a single device or group of devices.
- **Access:** The **Workflow** feature can be accessed by:
  - The device's three-dot menu,
  - The Devices Console Ribbon, from the **Workflow** icon,
  - The Device Dashboard, from the **Repositories actions** tab, under **Workflow**.
- **Further details**: The Workflow option is treated at length in **Section 4.1.6, Workflow.**

12.2 Pinning and Unpinning 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 Console Tile options

12.3 Console 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.

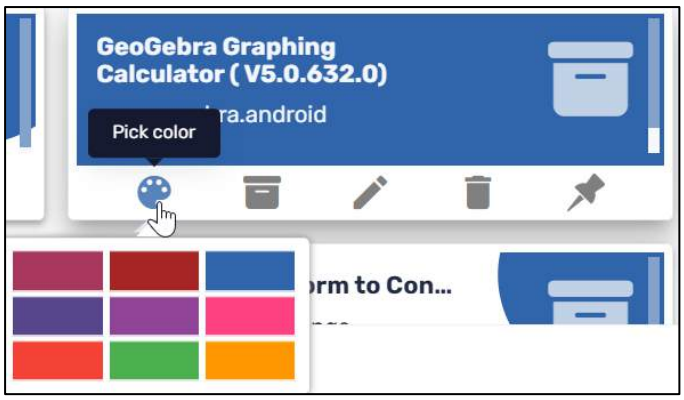
Figure 12-8: Sample Kiosk Tile, with six editing options

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.

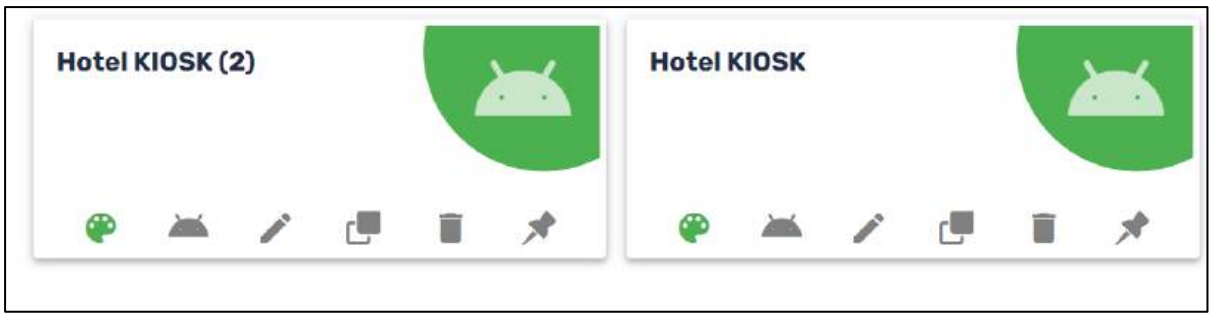
12.3.3 Edit Icon

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):

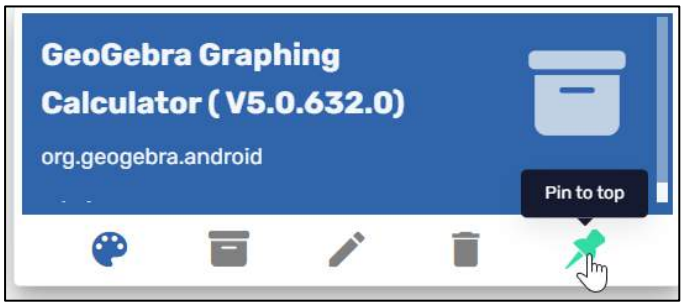


12.3.5 Delete

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 Manager 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	iOS	MacOS	Windows
	Advanced Messaging	Android				
	AFW Install/Uninstall	Android				
	Apple Custom Command			iOS	MacOS	
	Change agent password	Android				Windows
	Clear apps cache	Android				
	Clear apps data	Android				
	Collect logs	Android				
	Dep Apple Profile			iOS	MacOS	
	Device Settings	Android				Windows
	Disable apps	Android				
	Enable apps	Android				
	Export Blue Screen Data					Windows
	Export to CSV	Radix Device Management Interface Feature				
	Firmware update	Android				
	Group Dashboard	For managing groups of devices/users				
	Group Management	For managing groups of devices/users				
	Install Packages	Android		iOS	MacOS	Windows
	Kiosk	Android	Chrome	iOS	MacOS	Windows
	Manage Users	Android				

	Metrics	Android	Chrome			Windows
	OTA	Android				
	Policies	Android	Chrome	iOS	MacOS	Windows
	Remote Control	Android				Windows
	Remote Execute	Android				Windows
	Remove Google accounts from device	Android				
	Restart	Android		iOS	MacOS	Windows
	Scheduler & triggers command	Android				Windows
	Screen settings	Android				
	Send files	Android				Windows
	Send message	Android	Chrome			Windows
	Shutdown	Android		iOS	MacOS	Windows
	Smart Recovery					Windows
	Sound Siren	Android				
	Tags	Android	Chrome	iOS	MacOS	Windows
	Timeout	Feature in Workflow Command				
	Uninstall packages	Android				Windows
	Views	Android	Chrome	iOS	MacOS	
	VPP install/uninstall			iOS	MacOS	
	Wake on LAN	Android				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 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