



Network Device Management System

NDMS

System Architecture

Overview

Boxlight's Networked Device Management System (NDMS) is a cloud-based system. Every device that is to be managed by the NDMS must be able to connect to at least the NDMS server.

In an application where it is desired that the device to be managed should not have internet access, the device still needs to be able to connect to the Boxlight NDMS server. The recommended approach is to allow access but configure the firewall to whitelist (meaning allow access to) only the Boxlight NDMS server.

Create and Register a New Account

Overview

Creating and registering a new account and beginning to connect devices is a simple process.

<https://Boxlight.glbth.com/glbth/v1/login.html?register>

Before we start, it is important to understand the terminology used by Boxlight's Network Device Management System, hereafter referred to as NDMS, and explain the different fields, roles, and concepts.

Domain: Also known as the **Account**. This is your actual account name and will follow you everywhere when you log in, create users, connect devices, and such. A domain can be any text that the server will respond to as legal or available during registration.

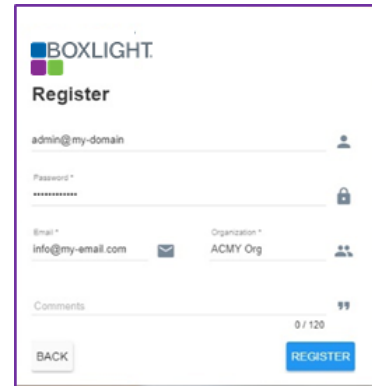
Server: The address of the server is composed of the main domain and the subdomain: <https://Boxlight.glbth.com/glbth/v1/> where Boxlight can appear under different names. When signing in to the console, the address should also contain /glbth/v1/. When connecting a device, make sure you leave the server address as the default, which is <https://Boxlight.glbth.com>.

User: The user is the entity that manages devices. The format of a user will always be **xxxx@your-domain**, with xxxx being the user and your-domain as the account name you enrolled. The default user name will be admin@your-domain and cannot be changed. Each user can be assigned from the admin account.

Register a new account

Navigate to the registration page at <https://boxlight.glbth.com/v1/login.html> and fill in the details as explained above.

Once done, you should receive an email containing an account activation link. Make sure you click the link to activate the account.



Sign in to your account

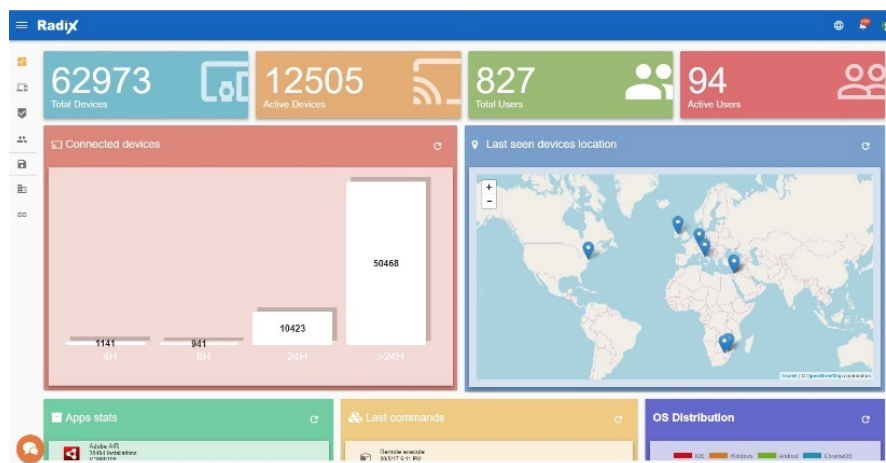
Navigate to the NDMS console page [here](#) and enter all details as registered. Remember, the username format is **admin@my-domain** (no extra suffixes, such as .com).



Dashboard

Overview

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



Each tile represents a block of information.

Tile	Description
Total devices	Total number of registered devices
Active devices	Total number of devices checked in the last 24 hours
Total users	Total number of users registered with the domain
Active users	Number of users logged on (except yourself)
Connected devices	Number of devices according to their last check in
Last seen location	Location of the last device's reported connection
Apps stats	The most frequently used apps
Last commands	List of the last commands committed
OS distribution	Chart showing the device operating systems

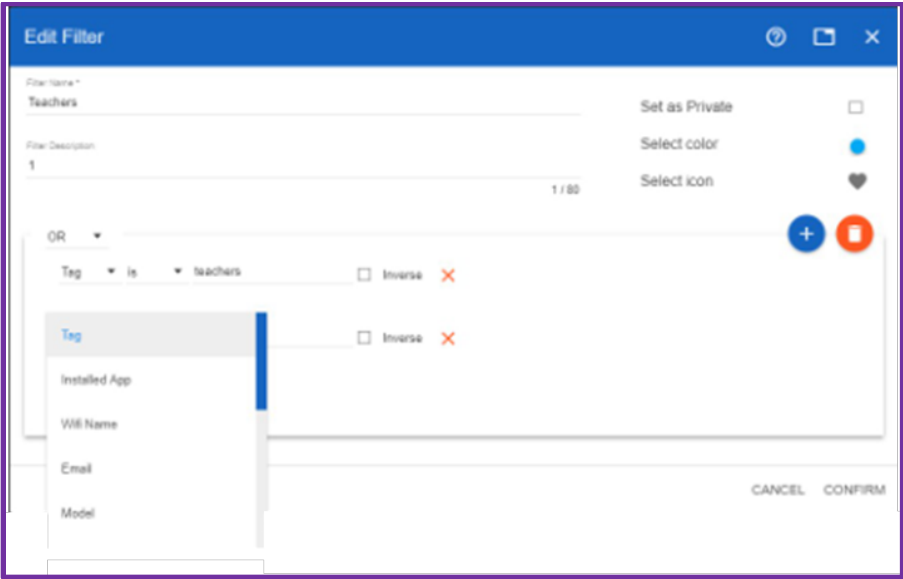
Manage Groups and Filters

Overview

Grouping and filtering devices is a very useful method of managing many devices with different locations and purposes. A group contains devices that are dynamically filtered by specific criteria.

The “All” group is a master group containing all the devices enrolled to the domain that are authorized to be viewed by the current user. There is no limit to the number of groups you can create in an account, and a device may be a member of more than one group. If a device falls under a filter criterion, it will immediately appear in a group and be applied with all rules and tasks relevant to that group.

In this case, the filter group called “Teachers” filters all devices containing a tag called “teachers” and set with a standout color and icon that represents the group. The use of a specific icon and color makes it easy to visually pick out group members.



The following listing shows all devices tagged with “teachers” in the “Teachers” group.

The screenshot shows the BOXLIGHT interface. At the top, there is a search bar and a 'Filter Groups' sidebar on the right. The main area displays a table of devices under the 'Teachers' group. The table has columns for Os, HardwareID, Name, Email, Last Seen, Policies, and Tags. The 'Teachers' filter is selected in the sidebar.

Os	HardwareID	Name	Email	Last Seen	Policies	Tags
Android	54275999	Mike	mike@gmail.com	26/7/17 3:30 PM		lenovo TB3-X70L teacher educate
Android	5404A62	Mike	mike@gmail.com	26/7/17 2:40 PM		mike teachers
Android	94a1a23	Mike	mike@gmail.com	26/7/17 11:12 AM		mike teachers
Android	1074262	Mike	mike@gmail.com	25/7/17 6:29 PM		teachers mike
Android	94a1a23	Mike	mike@gmail.com	24/7/17 5:48 PM		teachers mike
Android	C44202	Mike	mike@gmail.com	7/7/17 2:50 PM		dov teachers
Android	a032998	Mike	mike@gmail.com	11/5/17 12:40 PM		Lenovo yoga

Filter conditions

There are currently 12 conditions that you can use to filter devices:

1. **Tag:** Text tags that can be applied to a device (either agent or server side) and can describe the device
2. **Installed apps:** According to an installed app (app label or app package name)
3. **Wi-Fi name:** Wi-Fi SSID that the device is currently connected to
4. **Email:** Main device account
5. **Model:** Model name of device
6. **Permissions:** What OS permission is available:
 - Root
 - System
 - Limited privilege
7. **Last seen:** The last time a device was seen connected and online
8. **Is locked:** According to the anti-theft lock status of the device
9. **Policy:** Policy that is applied on the device
10. **Available internal storage:** The amount of available space (MB) on the embedded Android system
11. **OS version:** Operating system version (number)
12. **Hardware ID:** The internal hardware ID, typically represented by the MAC address

Filter criteria

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

- Is
- Starts with
- Ends with
- Contains

A group can also be filtered by combining several groups of criteria separated by “And” or “Or” operators.

For example

Some devices contain the tag “Class_A” and some devices contain the tag “Class_B,” while others may contain both of the tags.

Option A: Can create a group to filter all devices that have Class_A.

Option B: Can create a group to filter all devices that have Class_B.

Option C: Can create a group to filter all devices that have Class_B or Class_A.

Option D: Can create a group to filter all devices that have Class_B and Class_A.

One can assign some conditions with “And” or “Or” operators.

Also, one can create a group of conditions and put it in an “Or” or “And” condition to another group.

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

1. Have tag “Class_A” and Chrome software is installed.

OR

2. Have tag “Class_B” and Gmail software is installed.

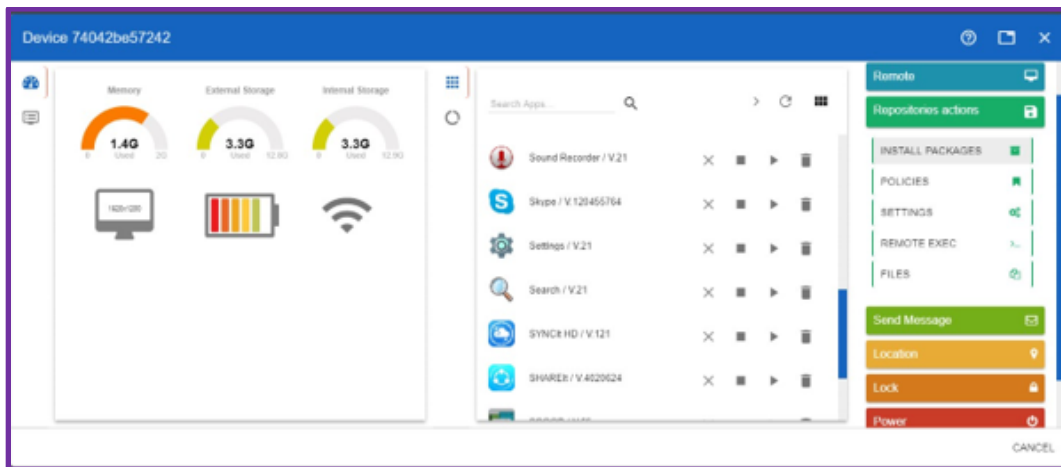
Apply Commands and Operations to Devices

Overview

One of the main purposes of a device management system is to command and operate the devices. Applying commands to devices can be done on a single device, a group of devices, one or more selected devices that are not in a group, or all available devices at once.

Applying commands to a single device

Applying commands to a single device is done on the device control panel. Open the device to which you would like to apply the task and navigate the right “command” column to apply the desired task. When working on a single device, all commands are immediate and cannot be scheduled. There are some tasks that are unique to a 1-to-1 operation, such as “Remote control” commands that can only be started from the device control panel.



Group-level commands

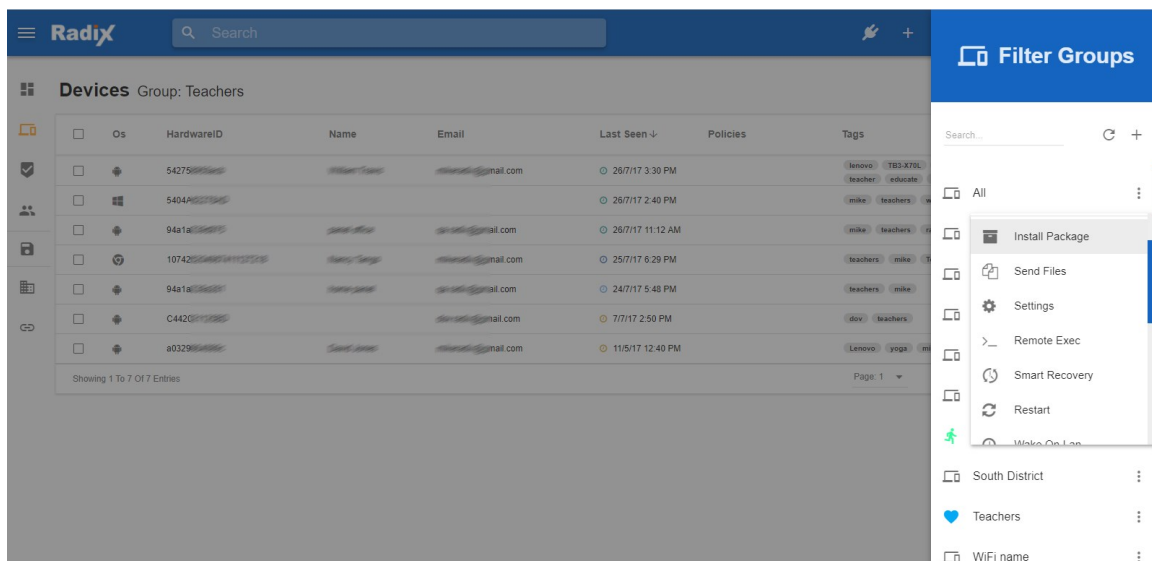
Most of the commands that can be applied on a single device can also be applied to a group. Here is a list of group-level commands you can apply on more than one device.

Function	Repository	Ad-Hoc	Comments
Install Package	x		
Send Files	x		
Remote Exec	x		
Workflow	x		
Restart		x	
Wake on LAN		x	
Tags		x	

Function	Repository	Ad-Hoc	Comments
Policies	x		
Shut Down		x	
Send Message		x	
Sound Siren		x	
Change the Agent Password		x	
Uninstall Package		x	
App Usage Report		x	
New Command (Set Trigger)		x	

Applying commands to a group

Locate the group you would like to apply the task to and click the “Actions” menu represented by the downward pointing arrow. Select the relevant task from the menu and apply it to the group.



Applying commands to selected devices

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

BOXLIGHT Search

Devices Group: Teachers 3 Devices Selected

Os	HardwareID	Name	Email	Last Seen
<input checked="" type="checkbox"/>	5427589	William Taylor	wtaylor@gmail.com	26/7/17 3:30 PM
<input checked="" type="checkbox"/>	540462	James Taylor	jtaylor@gmail.com	26/7/17 2:40 PM
<input checked="" type="checkbox"/>	94a1a23	James Taylor	jtaylor@gmail.com	26/7/17 11:12 AM
<input type="checkbox"/>	1074262	James Taylor	jtaylor@gmail.com	25/7/17 6:29 PM
<input type="checkbox"/>	94a1a23	James Taylor	jtaylor@gmail.com	24/7/17 5:48 PM
<input type="checkbox"/>	C442021	James Taylor	jtaylor@gmail.com	7/7/17 2:50 PM
<input type="checkbox"/>	a032998	James Taylor	jtaylor@gmail.com	11/5/17 12:40 PM

Showing 1 To 7 Of 7 Entries

Page: 1 Items Per Page: 20

Install Package
Send Files
Settings
Remote Exec
Smart Recovery
Restart
Wake On Lan

FILTER GROUPS

novov (T83-X70L) mike teachers test tab3
jsher educate radix
ike teachers windows
ike teachers radix
achers mike Teachers!
teachers mike
gov teachers
Lenovo yoga mike teachers

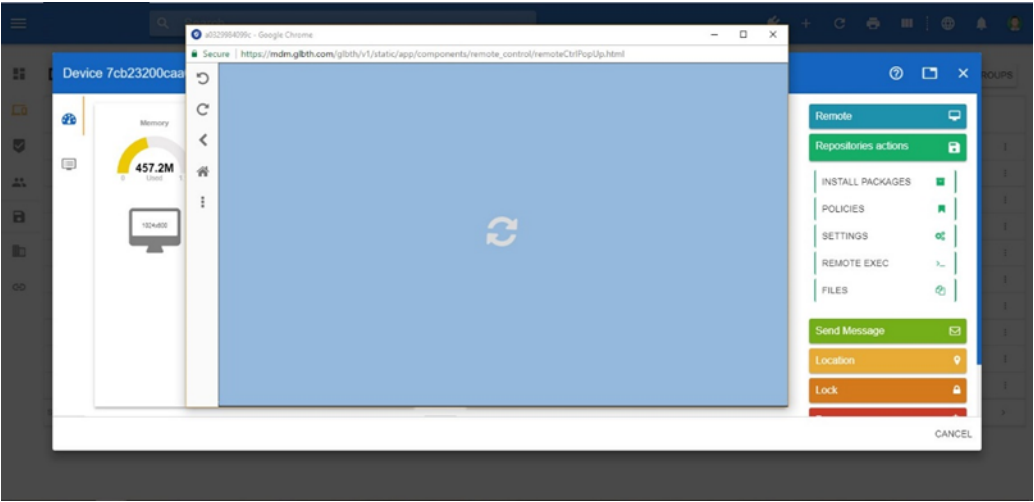
Remote Screen View and Control

Overview

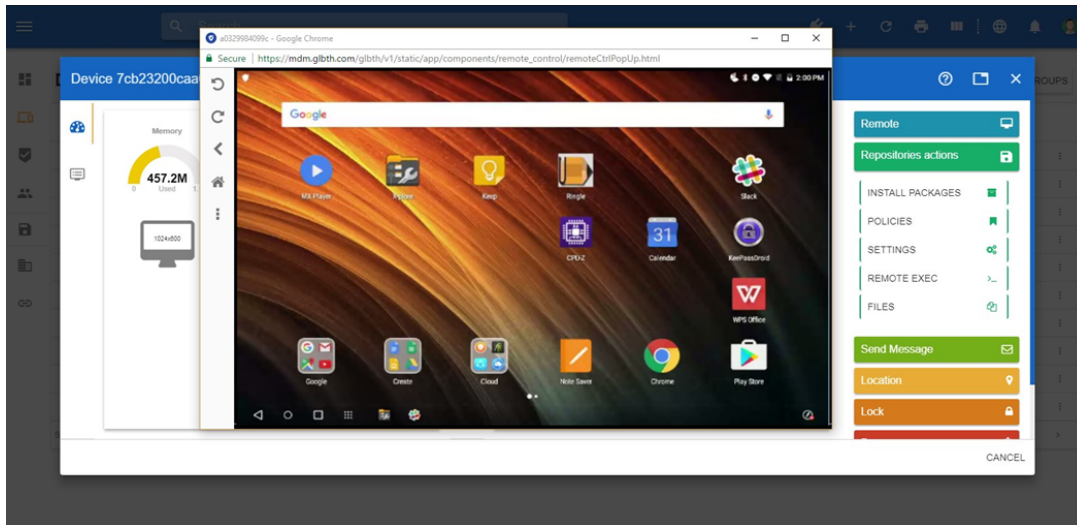
Remote control is a very powerful function that makes remote assistance easy and effective.

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

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



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



Requesting user confirmation

In order to request user confirmation for remote control session:

- Navigate to the **domain settings** menu option
- Set: **Require users permission for remote control** Yes/No

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

Supported environments and conditions

Android

- **User permissions:** Remote view only
- **System permissions:** Remote view and control
- **Root permissions:** Remote view and control

Android Device Settings Repository

Overview

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

To apply the setting bundles, see [Apply commands and operations on devices](#) below.

Every single settings item can be set separately by turning “on” or “off” the slider buttons.

There are two types of slider buttons: a two-way button and a three-way button.

Three-way slider button



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



The “on” mode means that this settings option will be turned on in this bundle



The “off” mode means that this settings option will be turned off in this bundle

Two-way slider button



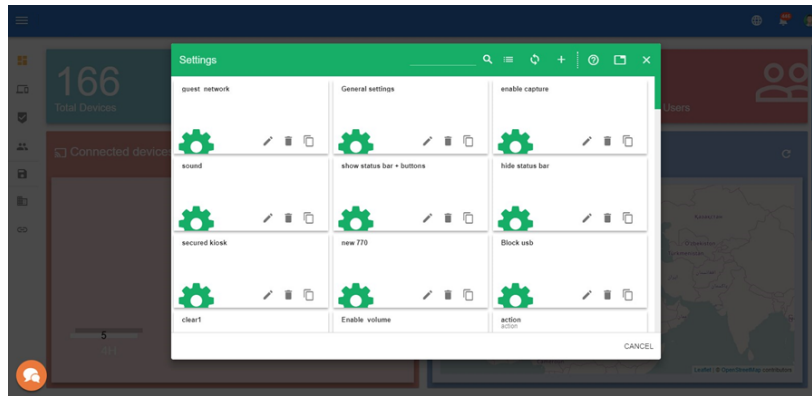
The “off” mode means that this settings item is ignored in this bundle



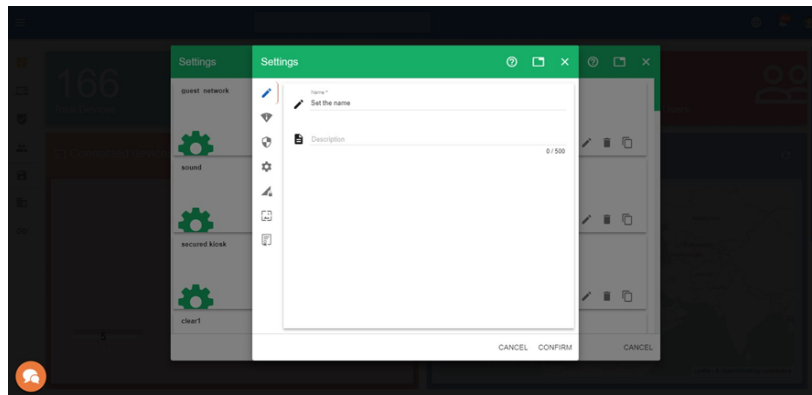
The “on” mode means that this settings option will be turned on in this bundle and you can set values to it

Creating a new settings bundle








Open the repositories and click the “Settings” section. A list of existing settings bundles will be displayed.



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

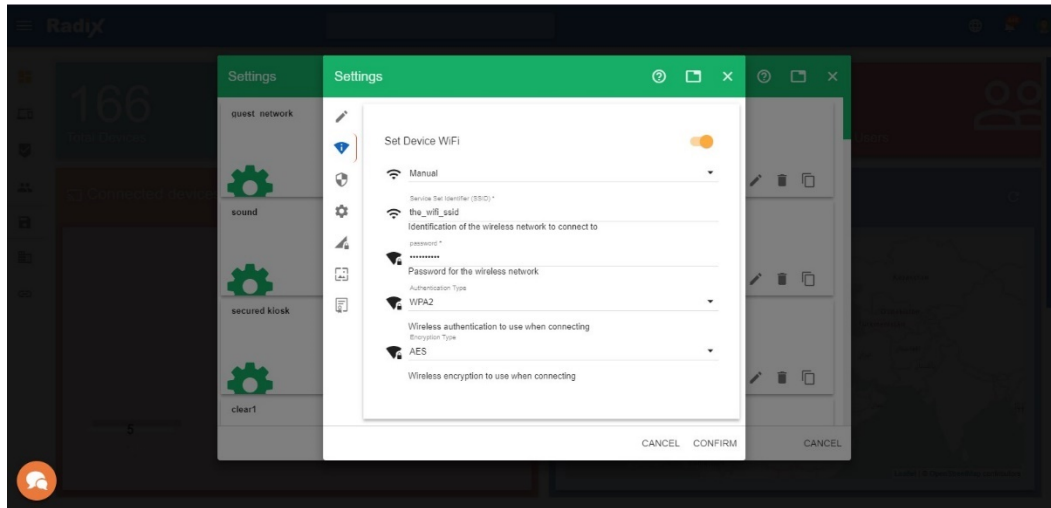


The “Settings” tabs

	Name and description
	Set Wi-Fi SSIDs
	Set security settings
	Set different “general” settings
	APN settings
	Set device desktop wallpaper
	Add CA certificates

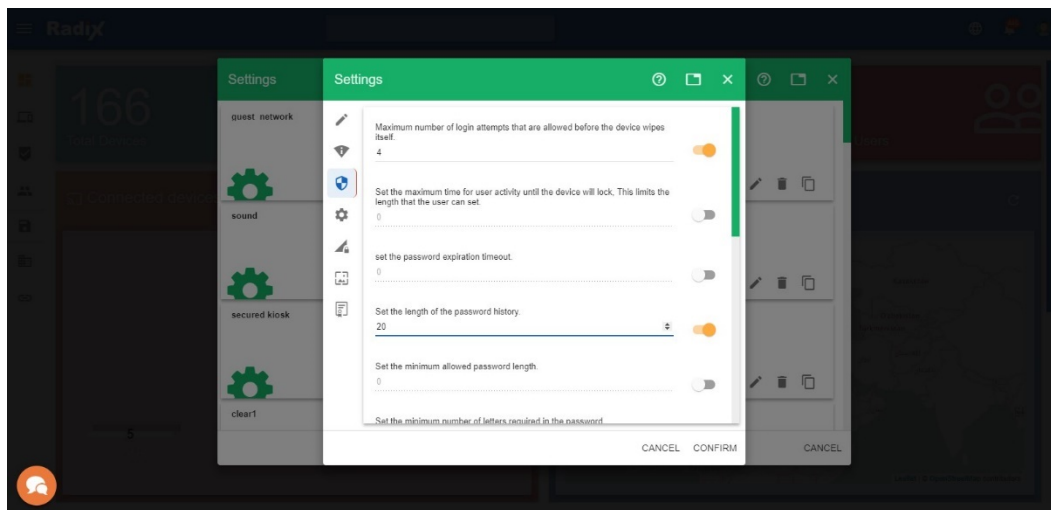
The “Set device Wi-Fi” tab

Turn on the slider button to set the Wi-Fi settings and enter the Wi-Fi SSID details. You can manually enter the fields or use the import functions to load a Wi-Fi profile (for Windows only).



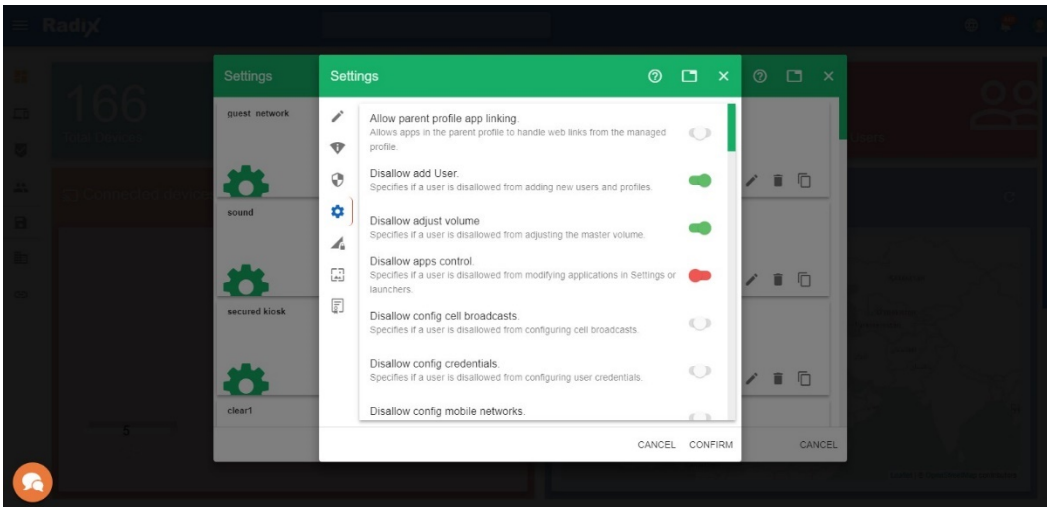
The “Security” tab

Turn on the slider button to set the different settings and set values.



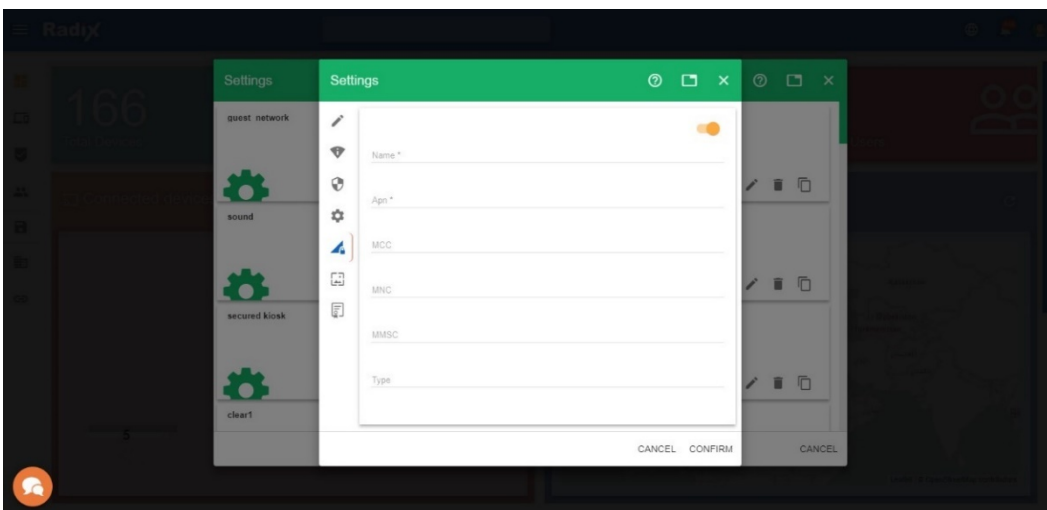
The “General” tab

Turn on/off settings you want to enable or disable. Notice the wording on each function, for example: “Disallow adjust volume.” When set to on, the volume button will be disabled. When turned off, the volume button will be enabled.



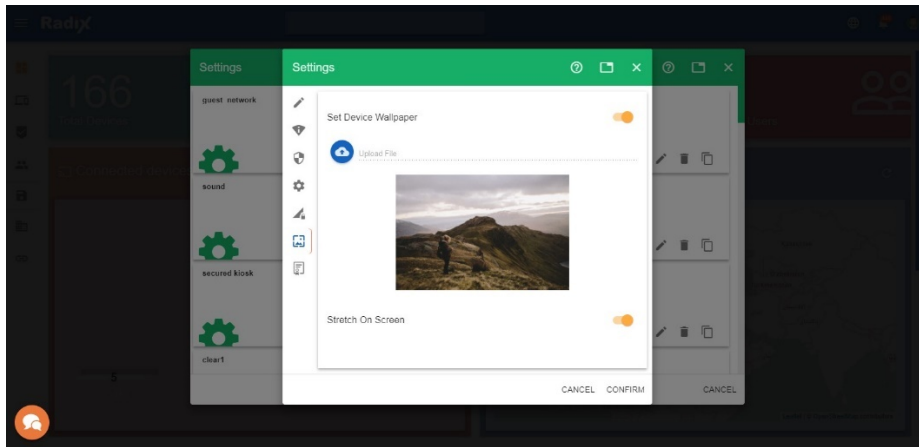
The “APN” tab

Turn on the slider button to set the APN settings



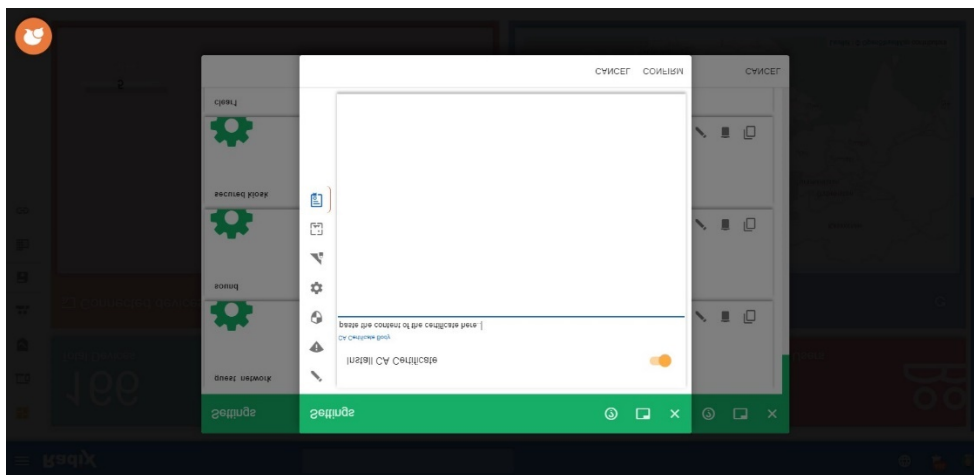
The “Wallpaper” tab

Turn on the slider button to set the wallpaper. Upload a picture (PNG or JPG) and choose whether the picture will be stretched or centered.



The “Certificate” tab

Turn on the slider button to set the CA certificate. Paste the certificate content in the text field below.

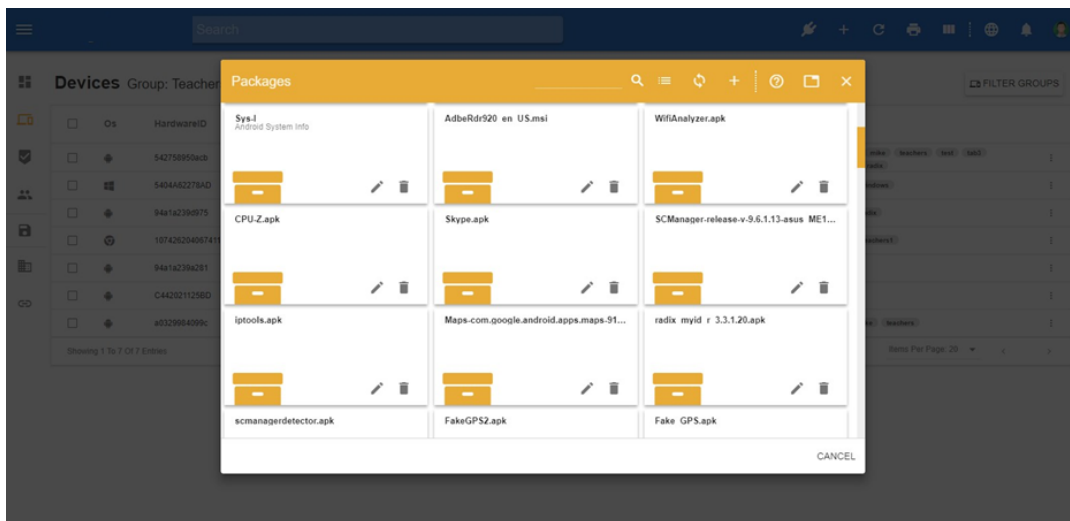


Remote Software Installation

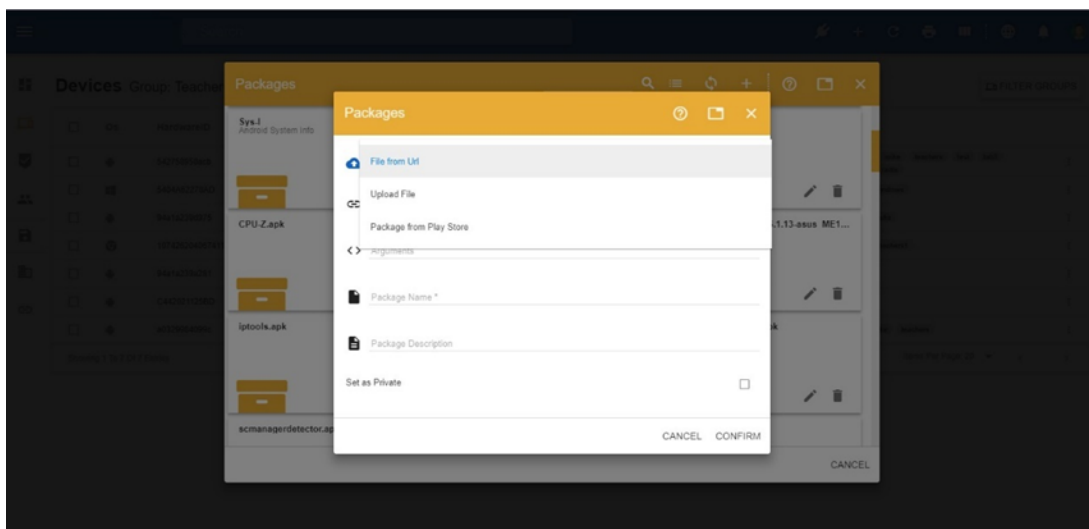
Overview

Installing applications remotely to one or many devices is done by first creating a repository “installation package.”

Open the repositories and click the “Packages” section. A list of existing packages will be displayed.



Click the “+” button to add a new package.



Select the package source

1. The first option is a URL reachable from the web (HTTP or direct FTP link). This allows storing the installation file anywhere on the web for quick download.
Note: A link cannot be an address of the application on Google Play or any other installation marketplace, it must be a link to a file.
2. Upload an installation package to the server on your account.
Note: this option will deduct the size of the installation package from your total account server storage space.

Supported installation package formats



Windows install packages supported: MSI Windows installer and EXE setup files



Android installation packages are APK files

Set the installation arguments/parameters

The installation arguments are different from one setup package to another—these are usually advertised by the app manufacturer. The common ones are “/s” and “/silent” along with many more.

Note: Android installers do not require arguments.

Name and description

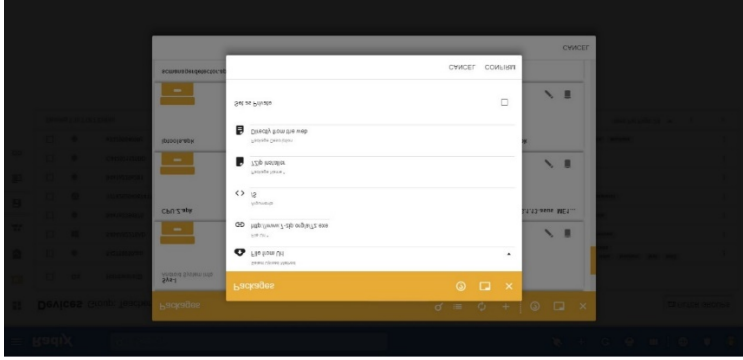
Give a name that best describes the installation package. This can be any name you desire, it does not have to be the name of the file. A description will make it easier for other users to understand what this installation package does.

Set as private

In a multitenancy environment where there are several users on your domain, you may want to set the package you create as “private” so it will only be visible to your account. If not selected, all domain users will have access to the installation package.

Package example

The following is an example of a Windows installation package for “7zip” with an unattended silent installation parameter “/S”.

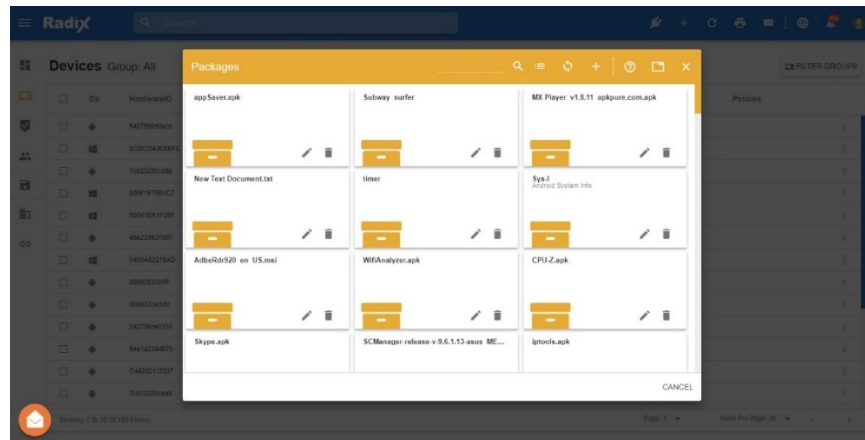


Install Package Directly From Google Play

Installing applications directly from Google Play to one or many devices is done by first creating a repository “installation package.” Direct installation is possible only for free apps. There is no need to have Google Play services or even to have a Google account on the devices to which you wish to install the apps.

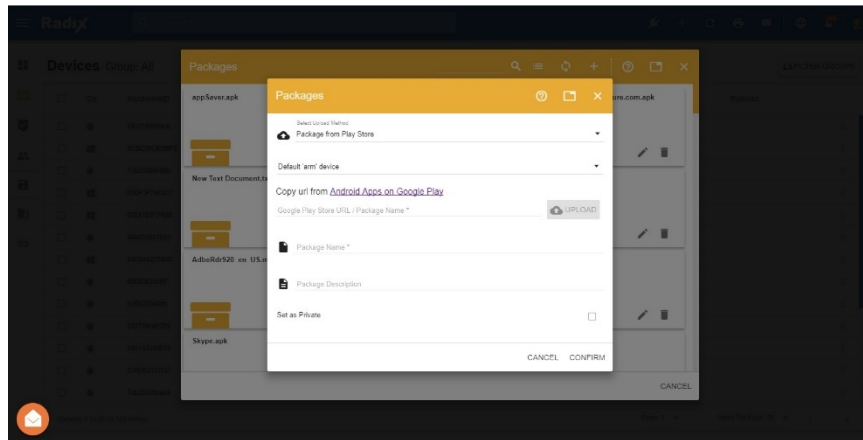
Note: When installing from Google Play, you should be aware that the updates will not occur automatically. Whenever there is an update, you will need to repeat the process and create a new package as you are not actually installing directly from Google Play, but rather from the NDMS server.

Open the repositories and click the “Packages” section. A list of existing packages will be displayed.

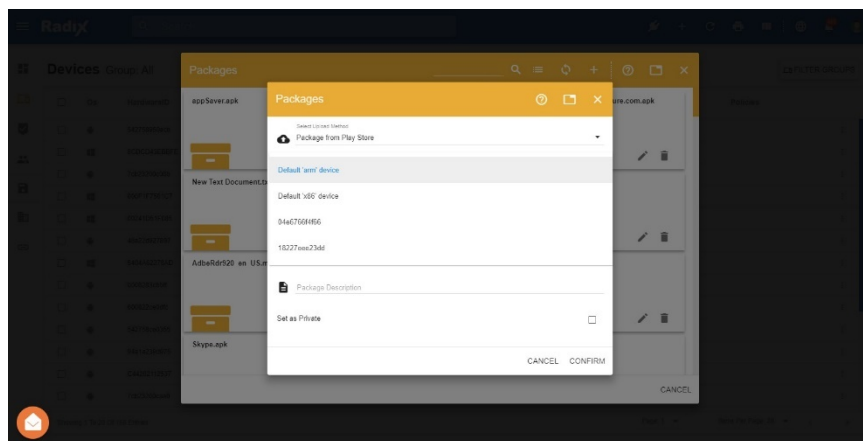


Click “Add New” to add a new package.

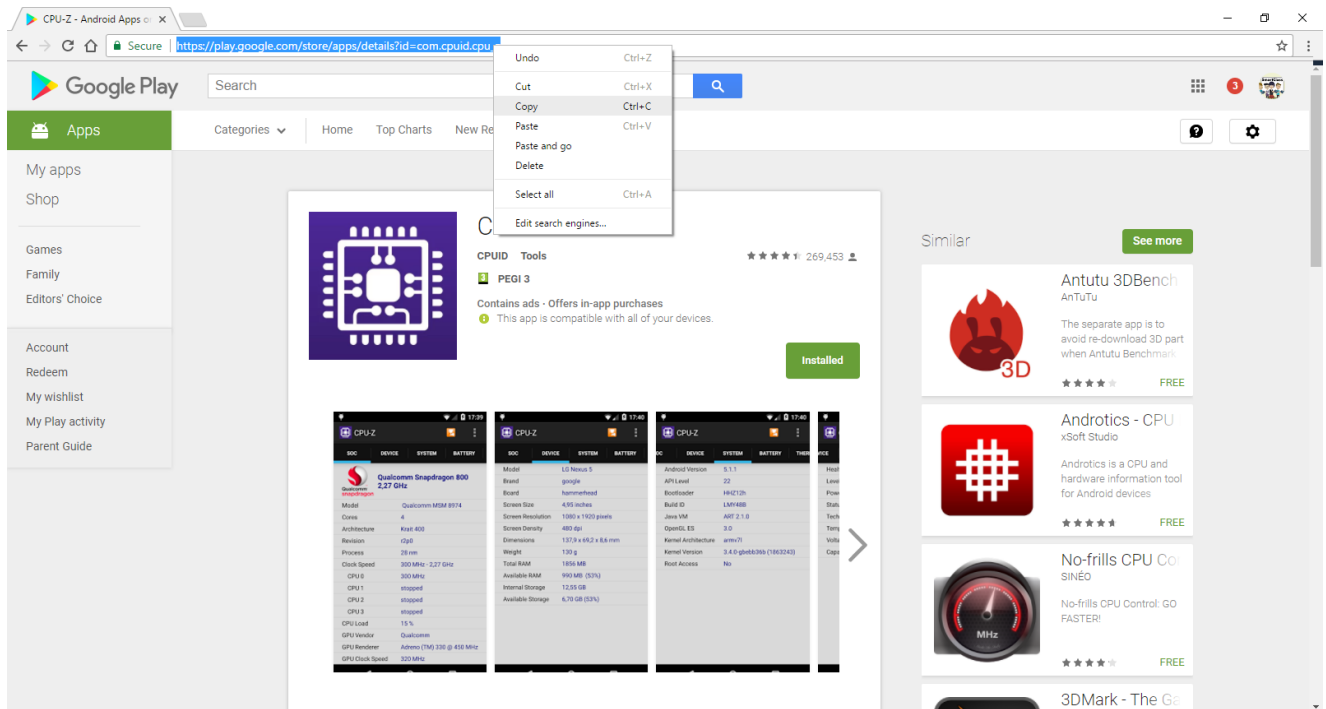
Select “Package from Play store” and click to open the Google Play website. Note: If you know the exact name of the APK bundle, there is no need to open Google Play.



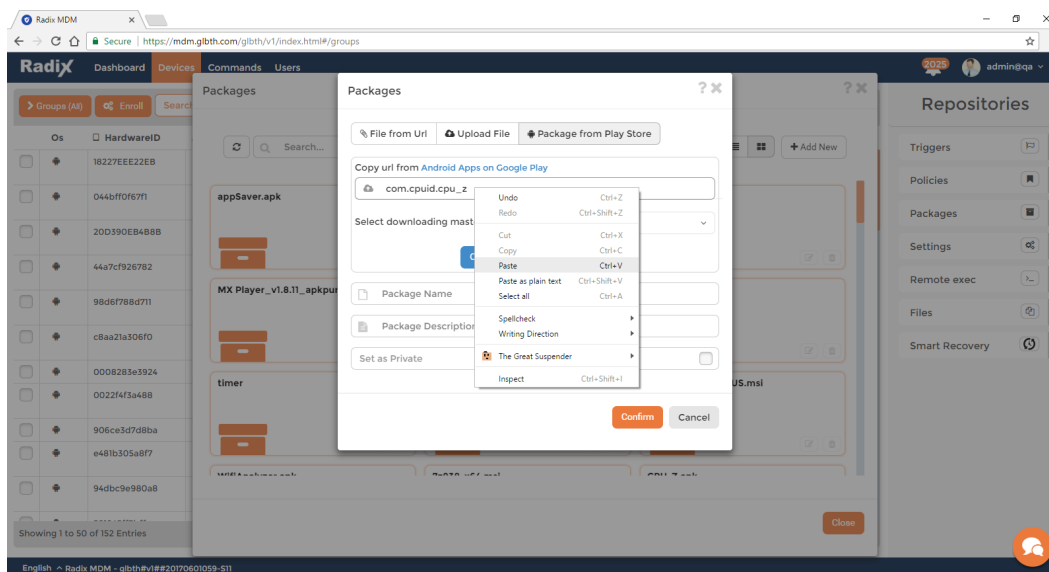
Select the relevant “Master Device.” Use the default **ARM** or **x86** device if the application you are installing is platform version and dependencies agnostic. Read more on how and why set a master device.



Search Google Play for the desired app and make sure it is free. Copy the URL of the app.

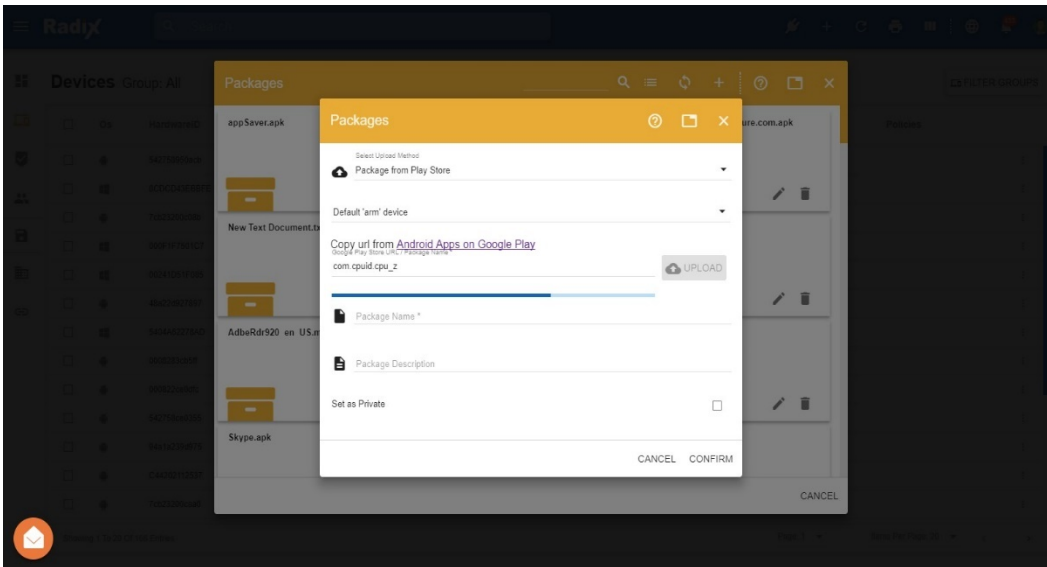


Paste the URL in the Google Play package name field. Note: The system will automatically trim the link and use only the relevant package name of the APK.



Select the “master device” that resembles the target devices (ARM devices, x86 devices, or a custom device you can add on the “domain settings”). The reason is that some apps install different APK for different platforms.

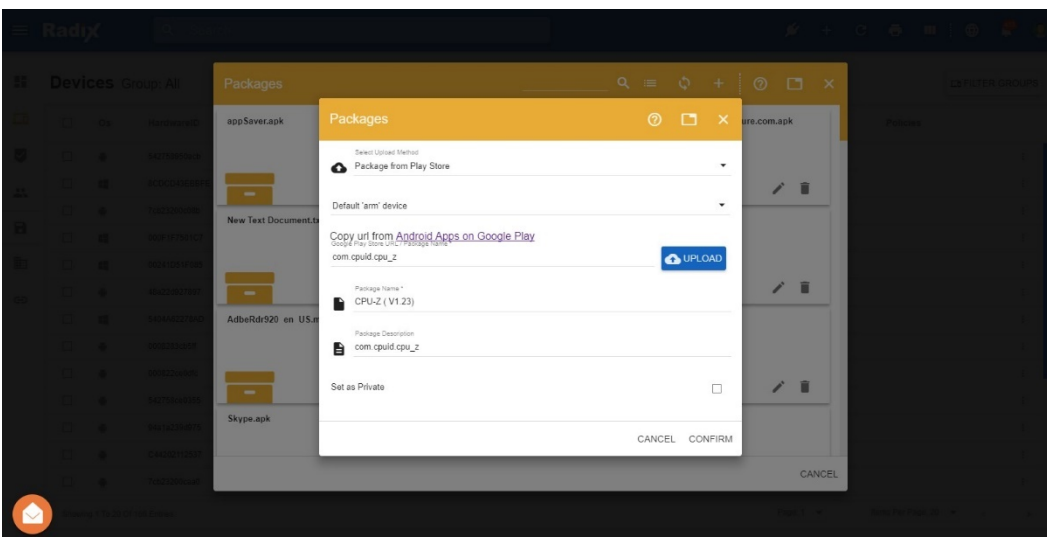
Click the “upload” button and the NDMS will retrieve the package from Google Play and store it on the NDMS server.



If the upload fails, try to repeat the process once or twice. If it still fails, try to change the master device. If the upload still fails, this package may not be suitable for direct install.

When the progress bar finishes, the package is ready with a default name as retrieved from Google Play. You may change the displayed name and description.

Click “confirm” and the package will be ready for installation.



In order to install the package, see the “Apply commands and operations on devices” guide.

Setting up a Master Device

Installing applications directly from Google Play to one or many devices is done by first creating a repository “installation package.” Direct installation is possible only for free apps. There is no need to have Google Play services or even to have a Google account on the devices you wish to install the apps to.

In order to be able to retrieve the right installation package from Google Play, the device that retrieves the APK must have as close (and in some cases identical) to the platform preconditions as the rest of the target devices. For example, if you have 200 Samsung Galaxy devices with x86 CPU, apps from Google Play that depends on the CPU type must install the relevant x86 APK (and therefore the Google Play entry will have two options that are transparent to the user installing it), but when the user installs the app, the device local play app will choose the relevant APK automatically. The same is true for the Android OS versions dependencies—if your master device is Android 6 and the target devices are Android 4.44, there are apps that have different internal versions for different OS platforms.

This is why we allow you to set your own master devices. You can set more than one master device according to your needs.

The master device will not be dedicated to being a master device—it is just a logical connection with Google Play.

Preparing the master device

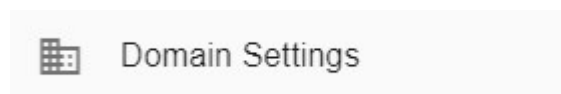
Choose one of your devices that resembles the rest of the target devices.

Set a Google account (can be specially registered for this task, does not have to be one of your existing accounts). Make sure this account does not have two forms of identifications, but rather only a password.

Enroll the device to the NDMS platform normally and copy the **device ID** as displayed in the console.

Setting the master device on the NDMS platform

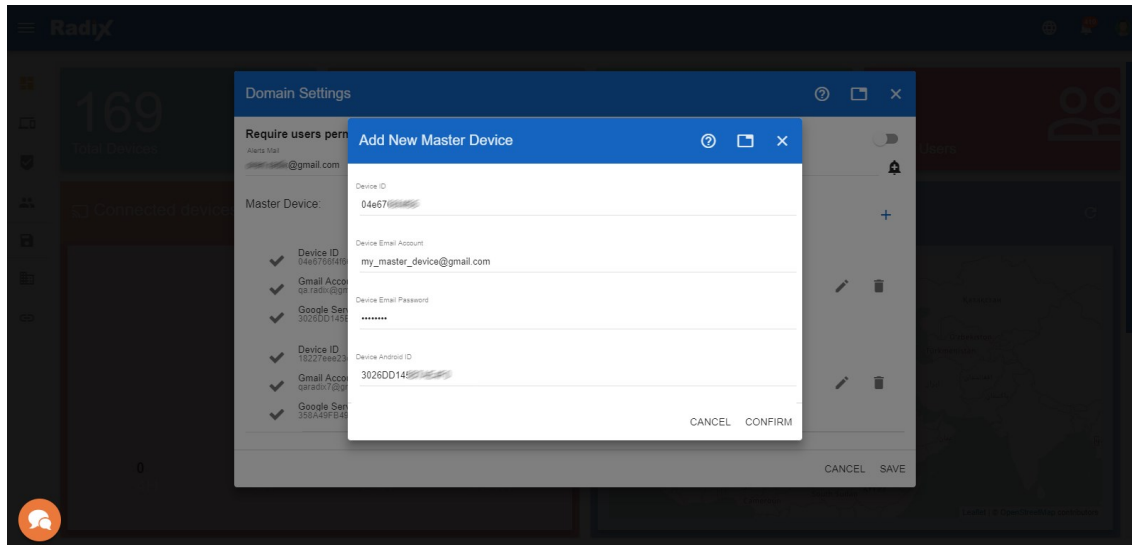
Open the Domain Settings



Click the “+” button to add a new master device

1. Add the Google account of the master device and open the Google Play app.
2. Enter the device ID of the master account (as appears on the device dashboard).

Once you enter the device ID, the system will pull the unique Device Android ID automatically as collected by the NDMS agent when the device enrolled.



Confirm to save the new master device.

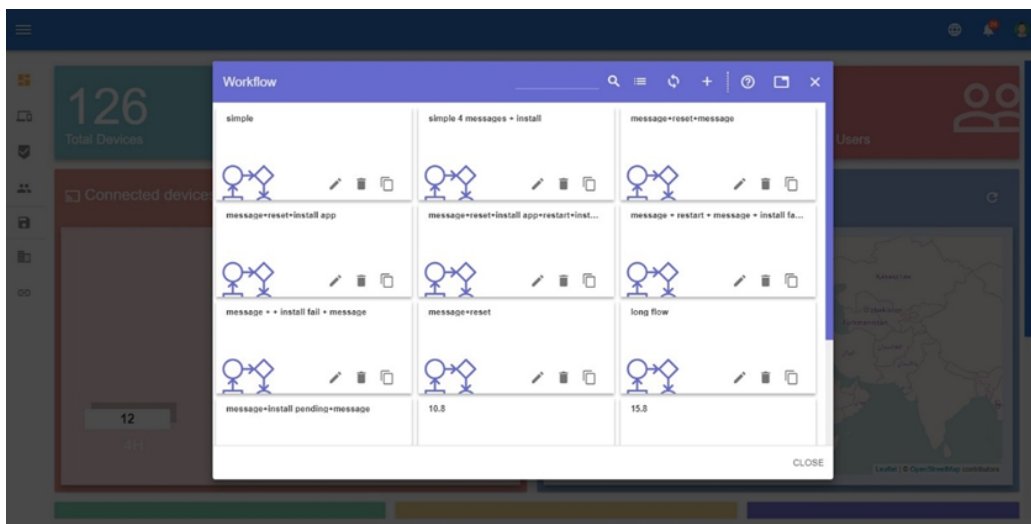
Workflow Repository

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

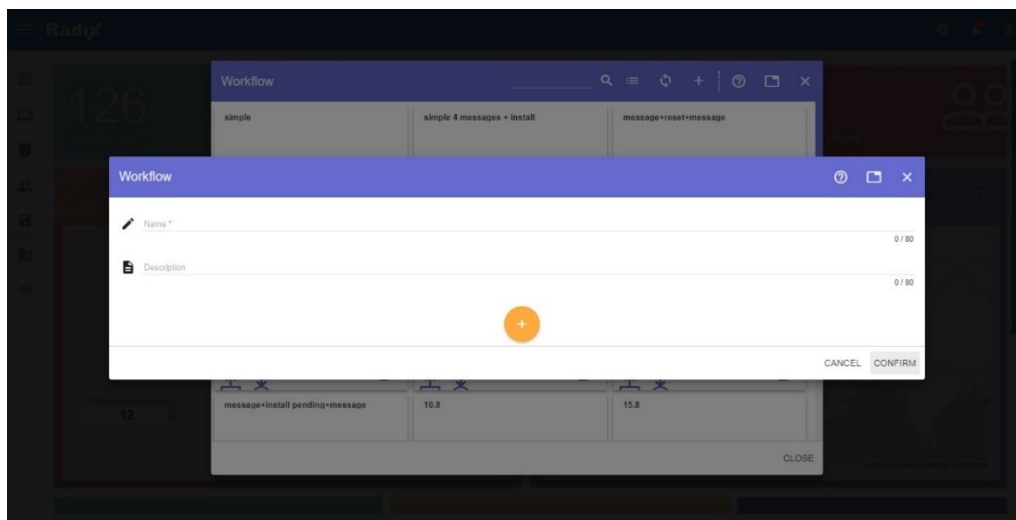
Note: This method can also be applied to a newly enrolled device for quick onboarding.

Creating a new workflow

Open the workflow repository item.



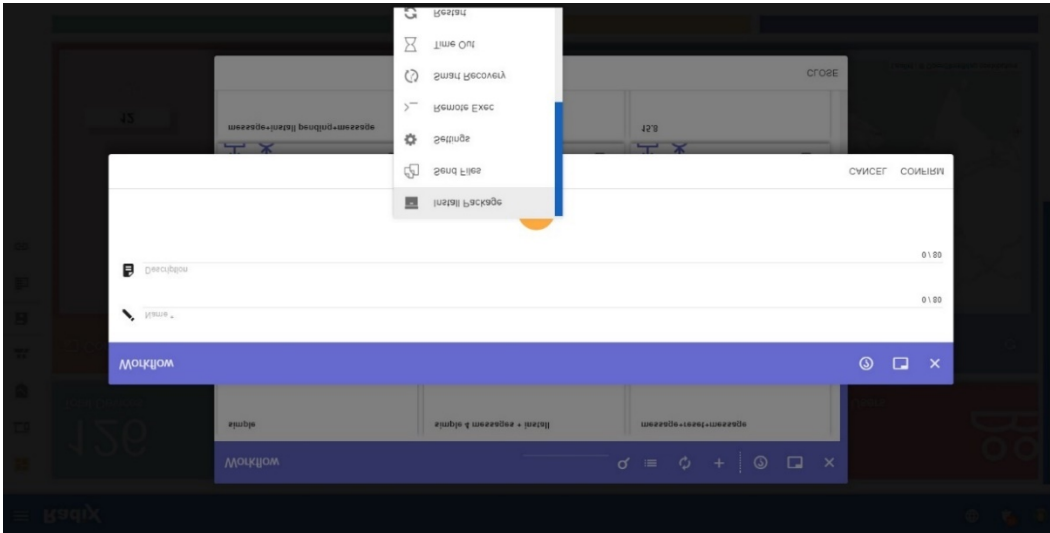
Click the “+” button to add a new workflow.



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

Add a workflow step (item)

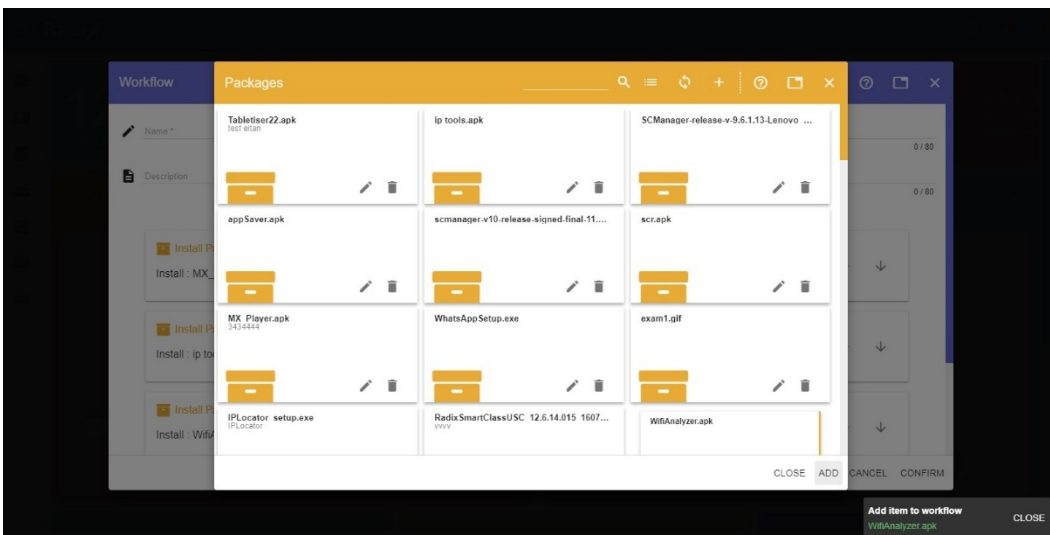
Click on the “+” button and select an action from the list.



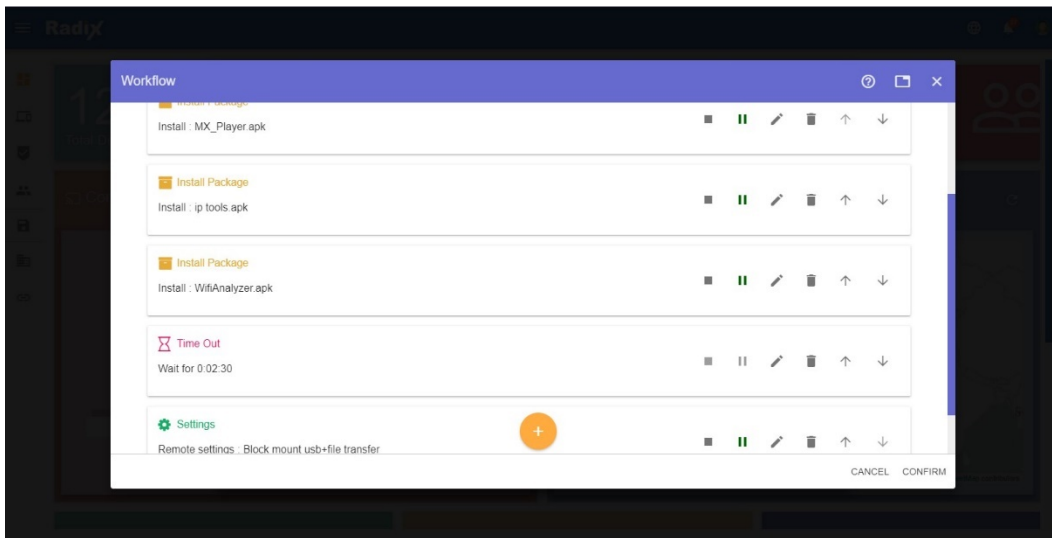
In this example, we selected the “Install Package” repository, so all packages on the repository show up.

Select a package and click “add” to add it to the sequence. You may add several packages, then click the “close” button to close the packages repository screen. Notice the message on the bottom right side indicating that the item was added.











Repeat the “add commands to workflow” with all desired commands.



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



Workflow steps configuration

-   Do not wait for this step—all these types of steps can even happen simultaneously if the general queue is not busy or the device can handle it.
-   Wait for this step to **finish** before proceeding to the next step. This step can fail or succeed and flow will continue.
-   Wait for this step to **finish successfully** before proceeding to the next step. If this step fails, flow will not continue.
-   Edit or delete the workflow step.
-   Send the workflow item step sequence up and down, before or after the current location.

Execute Commands

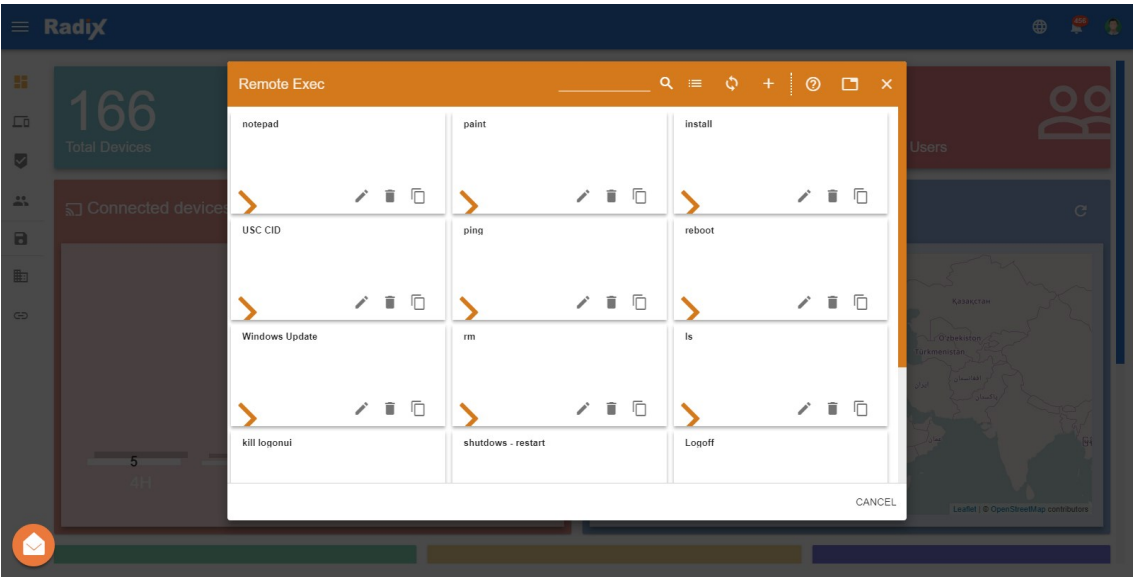
Overview

If you need to execute a more advanced command or a script, or even apply commands that are not currently available on the NDMS interface, using the Remote Execute commands repository is the best option. This works for both Android and Windows.

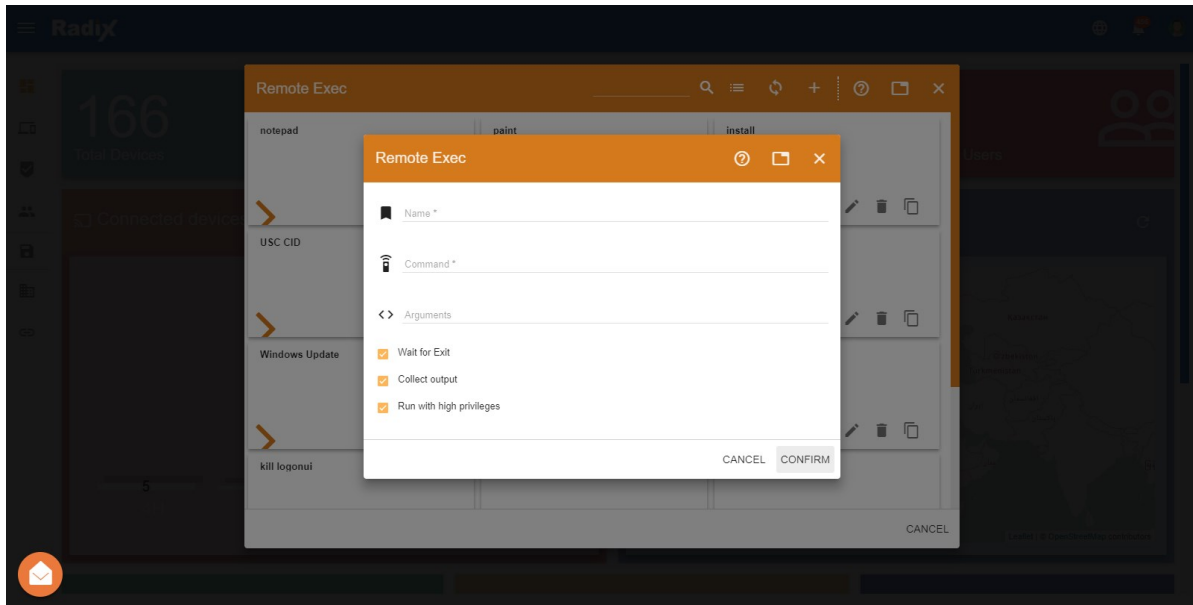
Creating a new command

Note: You may run the commands with high local device privileges, so please use this only if you are familiar with writing batches and scripts and you know what you are doing.

Open the repositories and click the “Remote Exec” section. A list of existing commands bundles will be displayed.



Click the “+” to add a new command and set a name to the new command.



Creating a new command can be done in several levels with different outcomes.

Command: This is where you write the main command

Arguments: This is where you write the command arguments

Wait for exit: Will indicate if the command result should be sent after the command finishes to run on the remote device or not

Collect output: This will indicate if the process standard result output is collected back as part of the command result

Run with high privileges: Run the command with higher local device privileges

Examples

Android command examples

	What will it do?	Command	Arguments	Wait	Collect	Priv
1	Disable Google Play	pm	disable com.android.vending	×	×	×
2	Get a list of running apps and display result	top	-n 1	×	×	×
3	Open a website using default browser	am	start -a android.intent.action.VIEW -d https://www.radix-int.com			
4	Run the calculator	start	-user 0 -n com.android.calculator2/ com.android.calculator2.Calculator			×

Result example

Result example for item #2

Open the command status results, navigate to your command, and click the “!” for result info.

The screenshot shows the Radix interface with a 'Commands' table. A modal window titled 'Command' is open, displaying a table with the following data:

ID	Time	Status
William (Team: 54273995)	17/8/17 17:15:22	Command Executed Successfully!
William (Team: 54273995)	17/8/17 17:15:05	Command sent

The modal also features a pie chart showing the status distribution: Success - 1, Failed - 0, and Pending - 0. A red box highlights the exclamation mark icon in the status column of the first row.

The screenshot shows the Radix interface with a 'Commands' table. A modal window titled '54273995' is open, displaying a detailed log output. The log shows various system processes and their status, including 'system_server', 'com.google.android.gms', and 'migrate/2'. The log output is as follows:

```
pid pkk cp 0% S 7717K 135S 104436K fg system system_server
2172 1 3% S 113 1942952K 104436K fg system system_server
23345 0 2% S 87 2683072K 163704K bg u0_a56 com.google.android.gms
27136 2 1% R 1 14076K 1528K fg system top
248 3 0% S 6 25428K 4584K fg logd /system/bin/logd
3307 3 0% S 58 1303496K 84196K fg u0_a9 com.google.android.gms.persistent
161 2 0% S 1 OK OK fg root mmccqd/0
26959 3 0% S 1 OK OK fg root kworker/u8:4
26966 0 0% S 1 OK OK fg root kworker/u8:8
26906 0 0% S 1 OK OK fg root kworker/u8:1
26878 0 0% S 1 OK OK fg root kworker/0:2
2270 2 0% S 38 59136K 988K fg radio /system/bin/mtkrild
2337 0 0% S 10 23056K 720K fg radio /system/bin/vianild
26954 2 0% S 1 OK OK fg root kworker/u8:2
26960 3 0% S 1 OK OK fg root kworker/u8:5
261 0 0% S 1 14088K 932K fg system /system/bin/servicemanager
24413 1 0% S 1 OK OK fg root kworker/1:1
24555 3 0% S 1 OK OK fg root kworker/3:0
2610 0 0% S 1 OK OK fg root tx_thread
1149 2 0% S 1 OK OK fg root kworker/2:3
14 1 0% S 1 OK OK fg root kworker/1:0H1
1708 0 0% S 10 29084K 1480K fg root /system/bin/netd
94 0 0% S 1 OK OK fg root hps_main
2972 0 0% S 37 1140484K 35196K fg radio com.android.phone
15 2 0% S 1 OK OK fg root migrate/2
1928 3 0% S 1 OK OK fg root ksdioirqd/mmc2
3 0 0% S 1 OK OK fg root ksoftirqd/0
57 0 0% S 1 OK OK fg root cinteractive
1726 0 0% S 2 11648K 516K fg system /system/bin/thermal
3178 2 0% S 15 1157572K 25880K bg u0_a9 com.google.process.gapps
```

Create and Apply Triggers

Overview

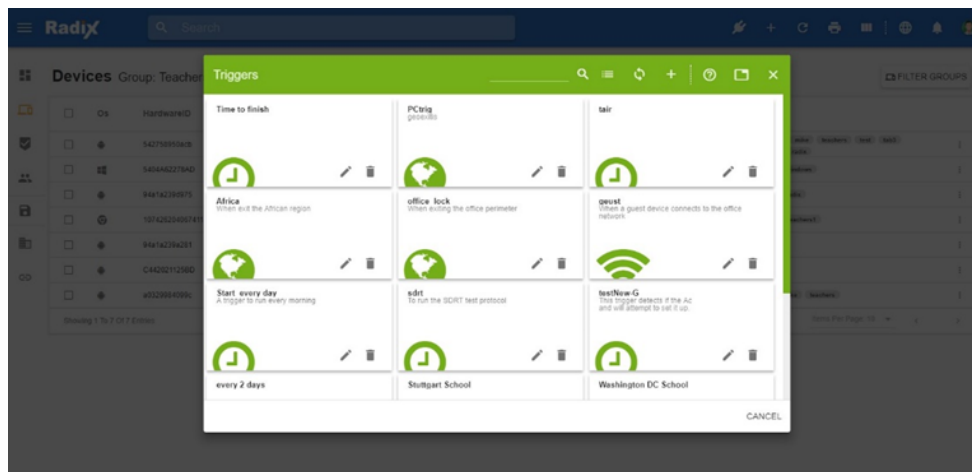
In order to automate commands and act on events, open the triggers repository and create triggered events. You can set different events and their thresholds, and selectively apply different triggered events accordingly.

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

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

Setting up a new trigger

Open the “Triggers” repository and select “+” to add new.



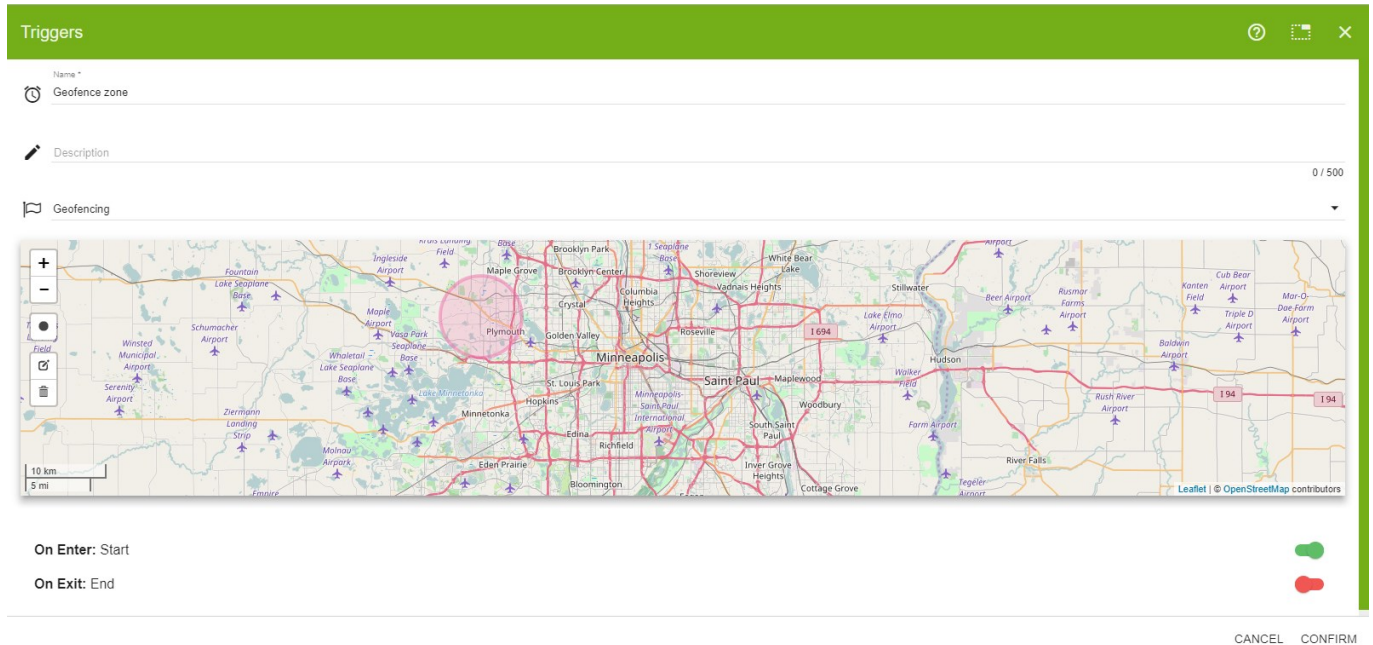
Select the type of trigger

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

Geofencing

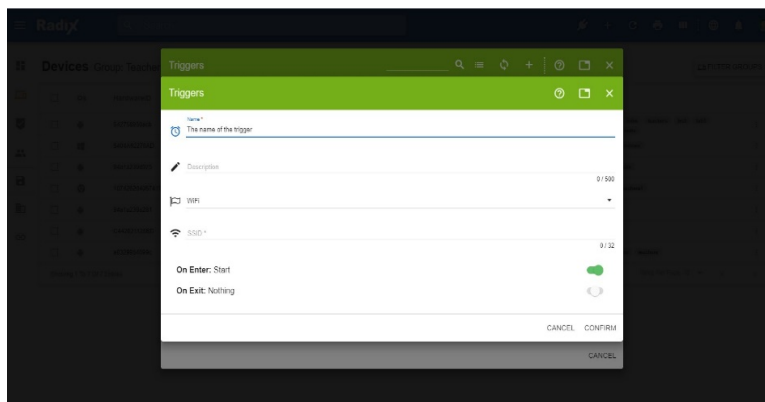
- Name the trigger and add a description

- Select a region by zooming in to the relevant area (minimum 20 mile radius)
- Select what will happen “On Enter” and “On Exit.” It can either be:
 - Nothing: Nothing will happen
 - Start: Start the mode (like start a policy or start locking the device)
 - End: Stop the mode (like stop a policy or unlock the device)



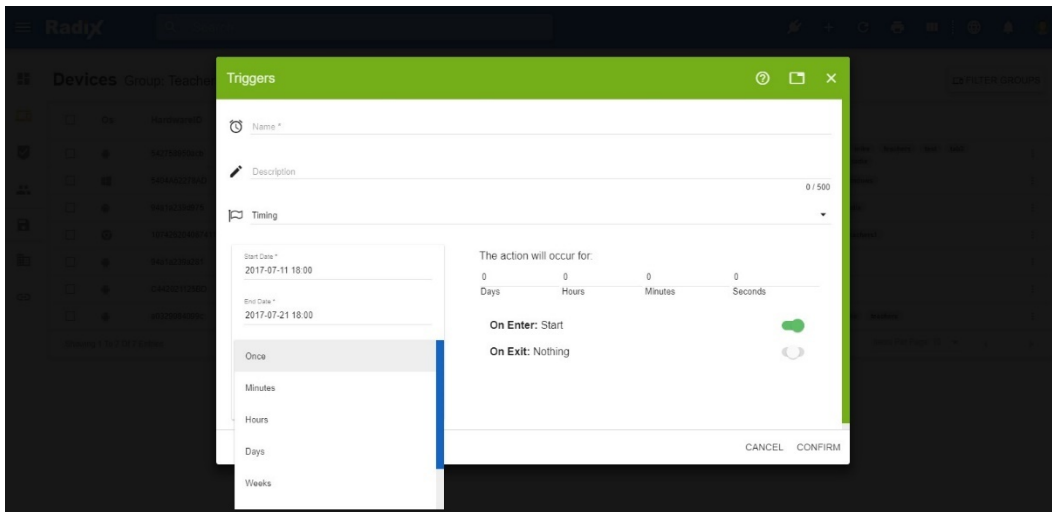
Wi-Fi

- Name the trigger and add a description
- Select an SSID to be triggered when connected
- Select what will happen “On Enter” and “On Exit.” It can either be:
 - Nothing: Nothing will happen
 - Start: Start the mode (like start a policy or start locking the device)
 - End: Stop the mode (like stop a policy or unlock the device)



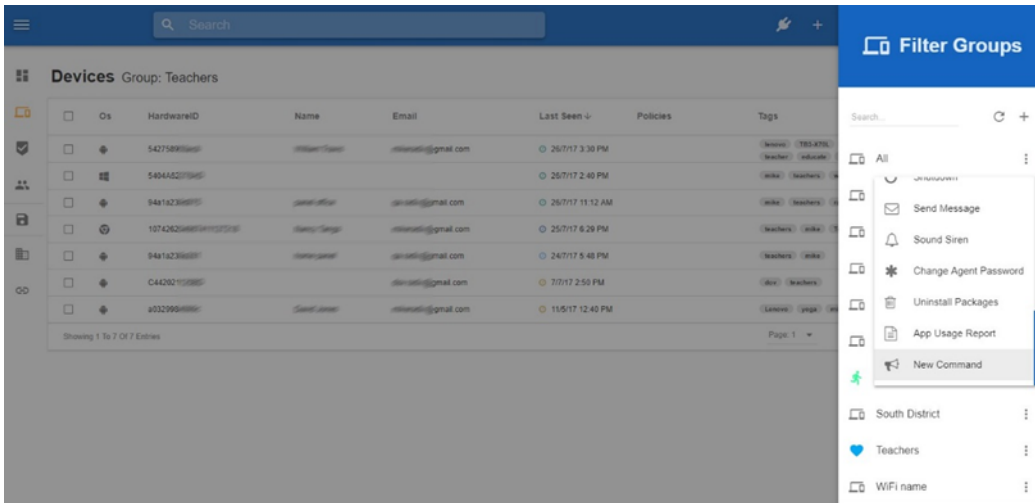
Timing

- Name the trigger and add a description
- Select the time interval that will trigger the task:
 - Once
 - Every minute, hour, day, week, month
 - Set if the trigger repeats and for how long
 - Set the time range—for example, if this is set to “daily” trigger a task, set it to work for 10 days and stop
 - Set the TTL (time to live) for when the triggers become irrelevant and will no longer apply

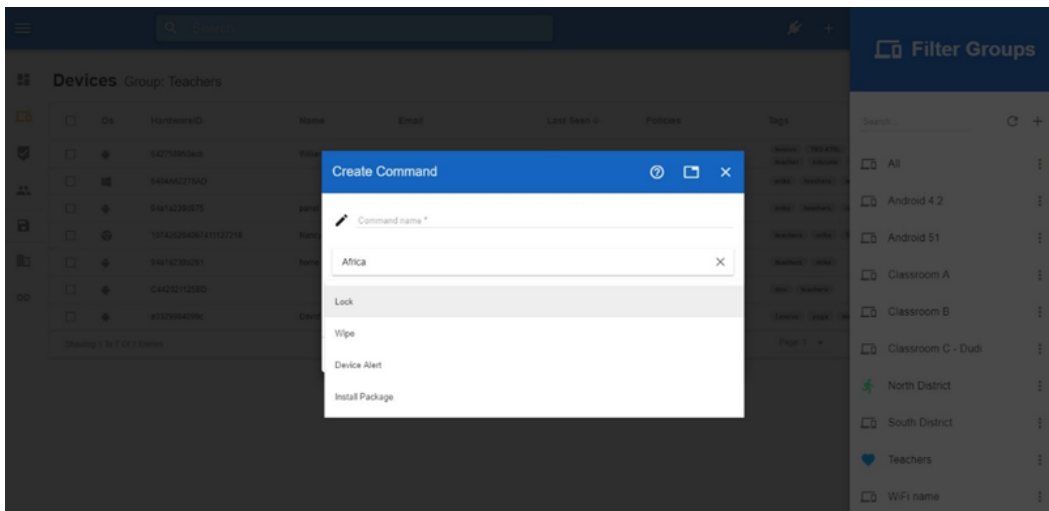


Create trigger-based commands

Locate the group you would like to create a triggered command for and click the “Actions” menu represented by the arrow facing down. Then, select “New Command” menu option.



- Name the command
- Select the trigger created earlier
- Select the command you would like to apply

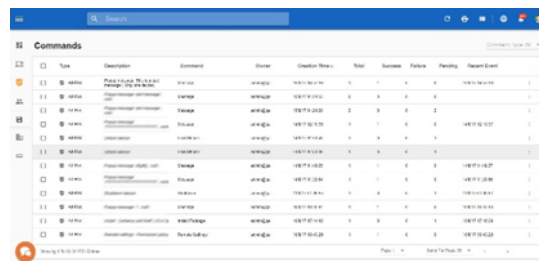


Commands History

Overview

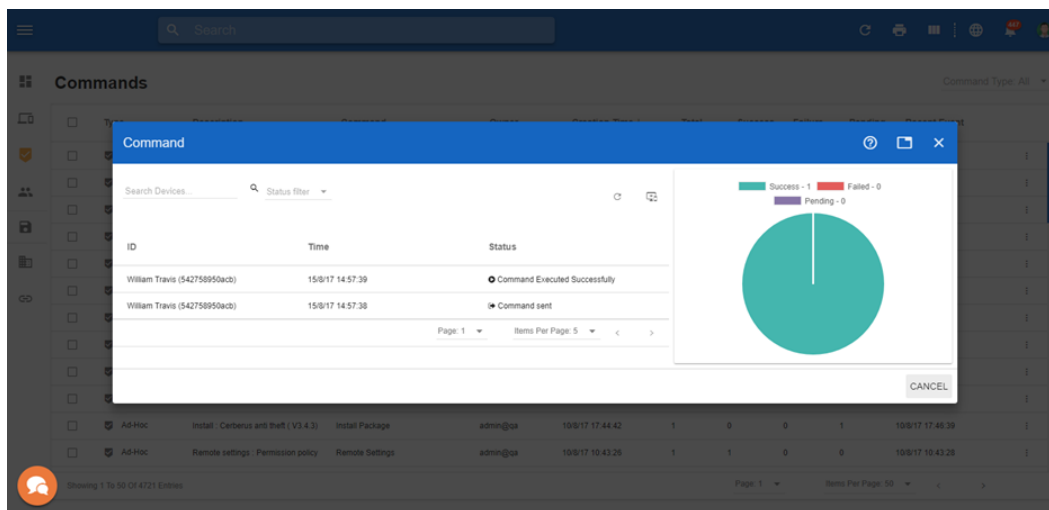
After applying commands to devices, groups, or creating a triggered command, you may want to query command results and perhaps manage the ongoing commands.

Open the “Commands” on the left and you will be presented with a command history summary. You may sort and search results by any column.



ID	Type	Description	Command	Owner	Creation Time	Time	Success	Failure	Pending	Repeat Count
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1
11	Ad-Hoc	Push Package (Push Package)	cmd.exe	admin@qa	15/8/17 14:57:39	15/8/17 14:57:39	1	0	0	1

By clicking any line (Command), you can see more in-depth information about the command itself. In this case, the command to send a message was delivered successfully to all devices (in this case, only one device).

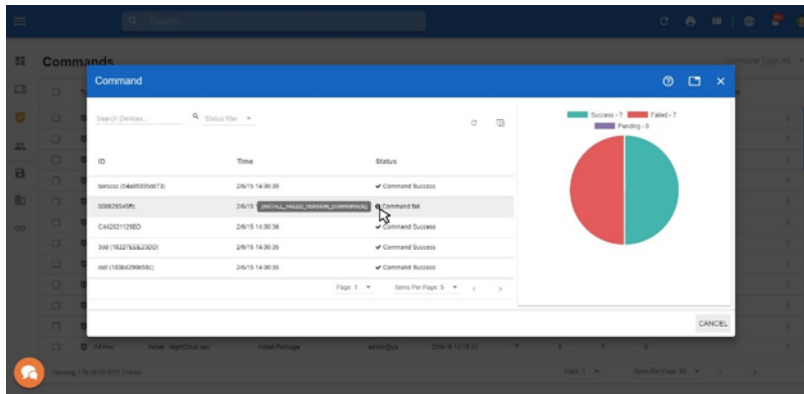


The screenshot shows a modal window titled "Command" with a search bar and a status filter. Below is a table of command results:

ID	Time	Status
William Travis (542758950acb)	15/8/17 14:57:39	Command Executed Successfully
William Travis (542758950acb)	15/8/17 14:57:38	Command sent

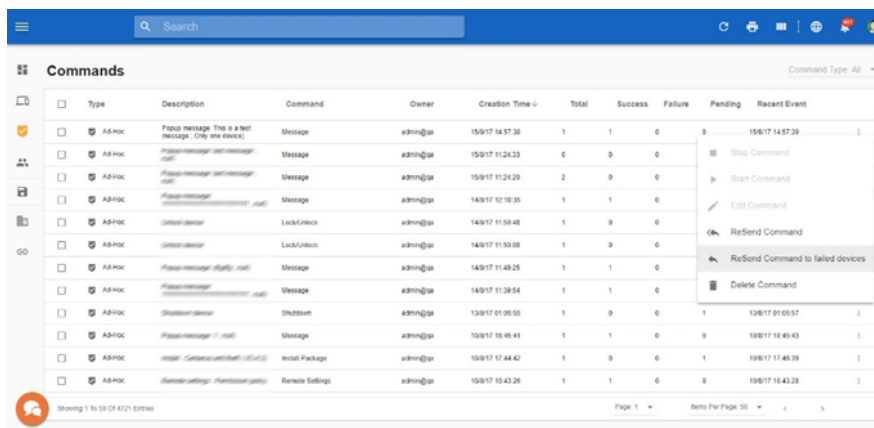
To the right of the table is a pie chart showing the status distribution: Success - 1 (teal), Failed - 0 (red), and Pending - 0 (purple). A "CANCEL" button is located at the bottom right of the modal.

In this case, the command to install a new package was delivered successfully to seven devices out of 14 devices in total. If you set the mouse over the failed command, it will prompt with the failure reason. In this case, the indication is that the current installed version is already higher than the attempted one.



You may always stop, start, edit, resend, or delete any commands.

Note: The Resend command to failed devices is particularly useful and saves much time.



Ad-Hoc One-Time Session

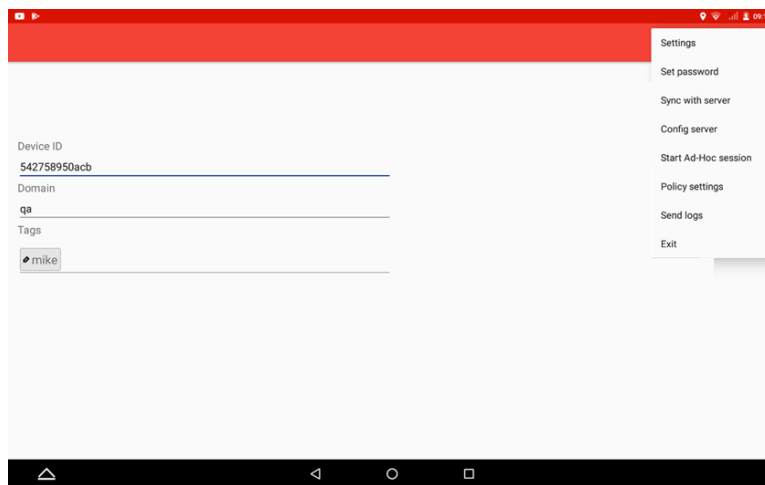
Overview

The ad-hoc session was introduced in order to allow management of devices across different accounts and domains. You may temporarily add a device for remote support or remote control without enrolling the device to your account.

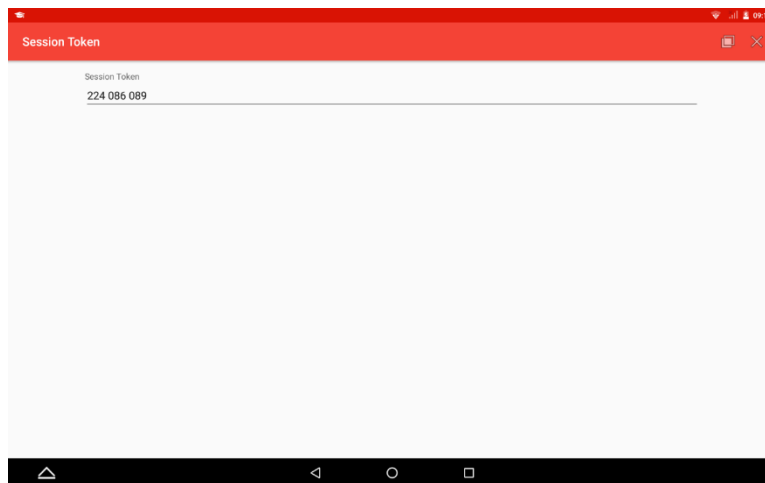
Note: The remote management session can be terminated at any time by the **remote user** or by the **admin**.

User side: Starting an ad-hoc session and obtaining a session ID

Open the NDMS agent and select “Start Ad-Hoc session” on the menu.

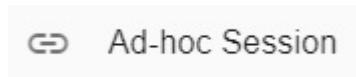


Send the session ID number to your admin.

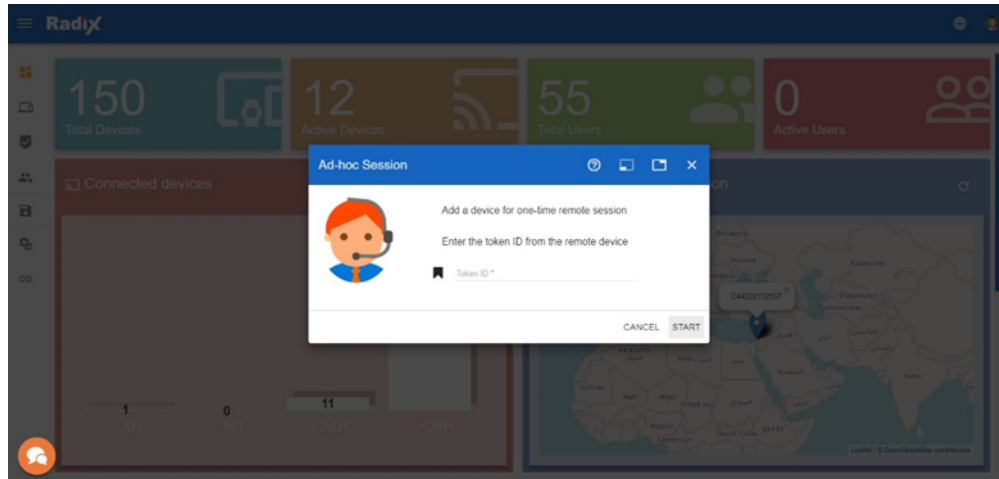


Admin side: Adding a remote device using an ad-hoc session ID

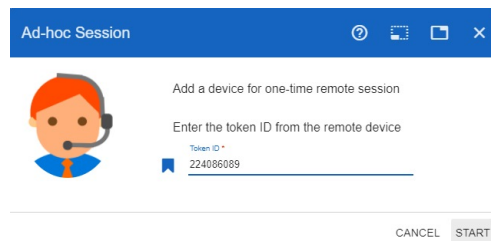
Open the Ad-hoc menu



Initiate remote ad-hoc session.

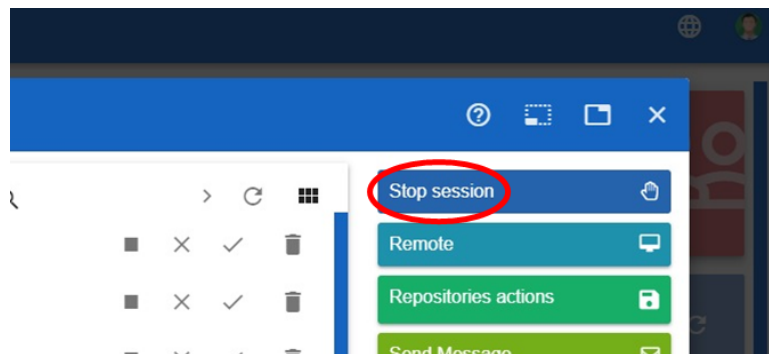


Enter the session ID code as given to you by the user and click "Start."



Once the session starts, the user device will be visible in your list just like any other device. You may apply any command, install apps, remote control the device, and so on.

To end the session, simply click the "Stop session" button on the device dashboard:



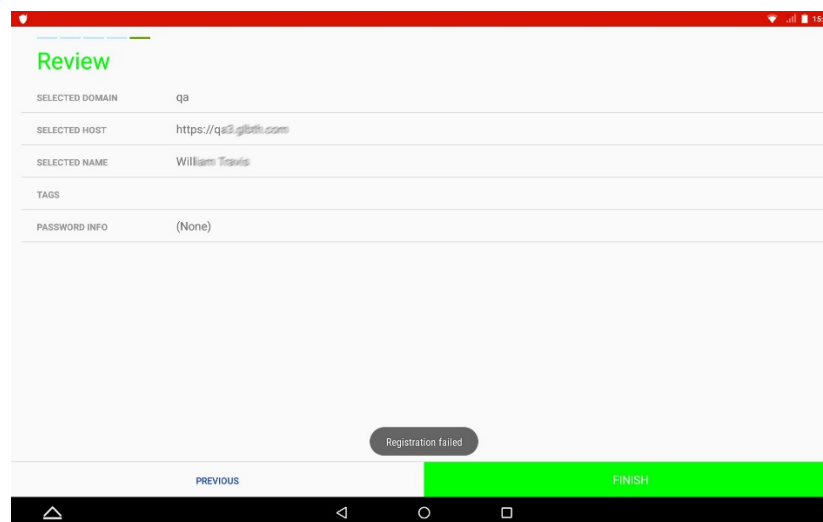
Authentication Token

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

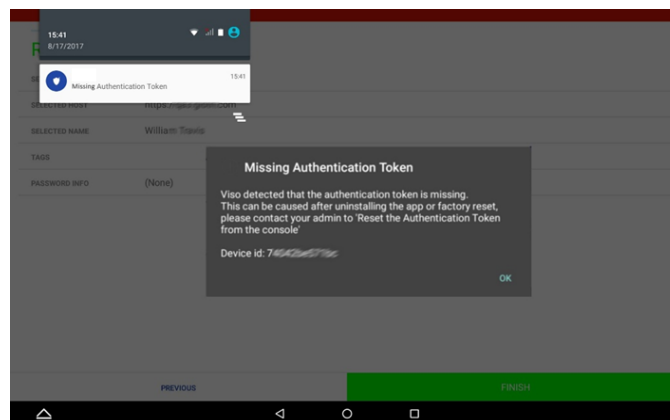
Missing authentication token

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

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



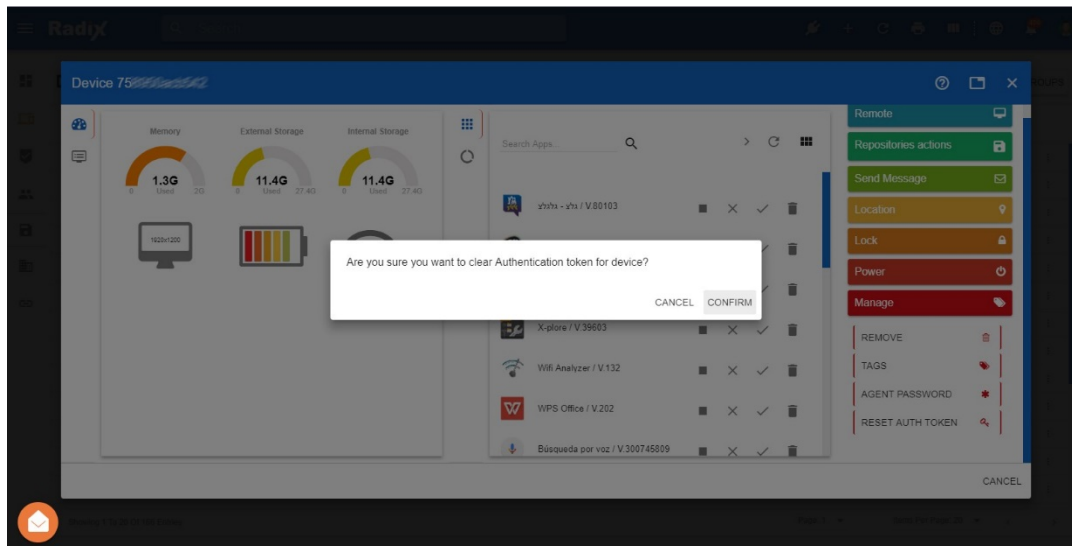
When clicking on the notification for more information, you will see a detailed note



Reset authentication token

Navigate to the specific device control panel on the domain it was originally enrolled to and select “Reset Auth Token” under the “Manage” tab.

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



Adding a New User

Overview

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

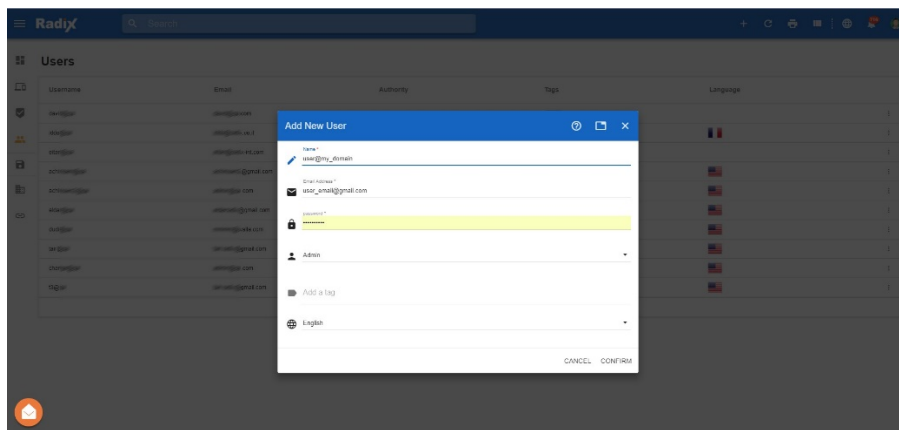
Note: This user is an NDMS console user and has no relations to the local device user.

Adding a new user

Open the Users menu



Click the “+” button to add a new user.



Name

By default, any username will be added with your domain name as a suffix: user@my_domain. This is also the proper name format when you log on.

Email

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

Password

Password must be at least eight characters with a combination of letters Aa-Zz, numbers, and symbols.

User type

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

Admin@my_domain default users	The default mandatory user found in every account; has all rights
Admin rights	Rights for all functions
User rights	Rights for all functions but user management
Observer rights	Rights to view device locations
Teacher rights	Can use the Teacher mode functionality

Tag

By setting tags to users, the users are then able to see only devices with corresponding tags. The devices must contain all the tags in order for the user to be able to see them.

For example:

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

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

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

Language

Sets the default console interface language for that user.

Boxlight Customer Support

The Boxlight Customer Support team cannot actively assist in configuring the Network Device Management System to your specific network and complement of devices. However, they can assist with general questions, technical background, and general information. Boxlight Customer Support can be reached at 877.696.4646 ext. 1 or CustomerCare@boxlight.com.