

Getting Started

- [What is KMM?](#)
- [Quick Start Guide](#)
- [Enrollment](#)
- [Zero-touch / Enrollment](#)
- [KMM Client](#)
- [Application Management](#)
- [Custom APK to Kiosk](#)

What is KMM?

KMM (Kuori Mobility Management) is an Android Enterprise Mobility Management (EMM) solution designed for managing Fully Managed Android devices. KMM provides organizations with centralized control over corporate-owned devices, allowing administrators to securely configure, manage, monitor, and deploy Android devices at scale.

KMM integrates directly with Google Android Enterprise services, including Managed Google Play and the Android Management API (AMAPI). Through these integrations, KMM can manage applications, device policies, security settings, and device configurations using Google's officially supported Android Enterprise framework.

Device policies created in KMM are distributed to devices through the Android Management API. These policies can include application management, device restrictions, password requirements, kiosk configurations, network settings, and other enterprise device management features commonly required for Fully Managed deployments.

Application distribution and lifecycle management are handled through Managed Google Play integration. Administrators can approve public applications from Google Play, upload private applications, manage application permissions, and silently deploy applications directly to managed devices.

KMM supports the core functionality expected from a modern Android EMM solution for Fully Managed devices, including:

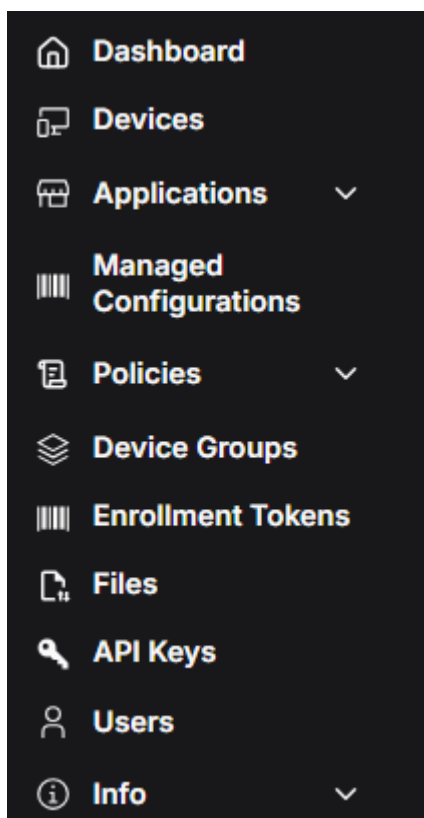
- Device enrollment and provisioning
- Application management and distribution
- Device policy management
- Kiosk and dedicated device configurations
- Remote device management actions
- Live client connection status and device location map (through the KMM Client app)
- Bulk actions on many devices at once
- Security and compliance controls
- Device grouping and policy assignment
- Android Enterprise integrations
- Live client connection status and device location map (through the KMM Client app)
- Bulk actions on many devices at once

In May 2025, Kuori successfully passed the Android Enterprise EMM Product Review for the Fully Managed Device solution set. As part of this approval, Kuori received authorization for production deployment, allowing KMM to be publicly deployed to customer environments as an officially reviewed Android Enterprise EMM solution.

Quick Start Guide

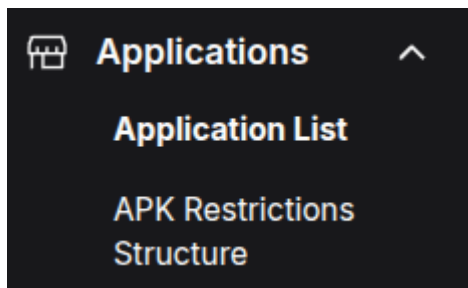
This quick start guide focuses on managing application distribution via KMM by selecting an application, creating your first application policy, and creating your first device group. This guide is intended for situations where your device or devices are already enrolled in the enterprise that you administer.

In KMM, once an enterprise is selected, navigation is handled through the menu on the left side of the screen. From there, users can create new policies, manage devices, create device groups, manage applications, and more.

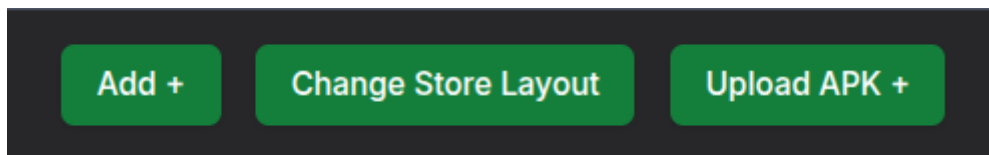


Creating and Applying Your First Policy

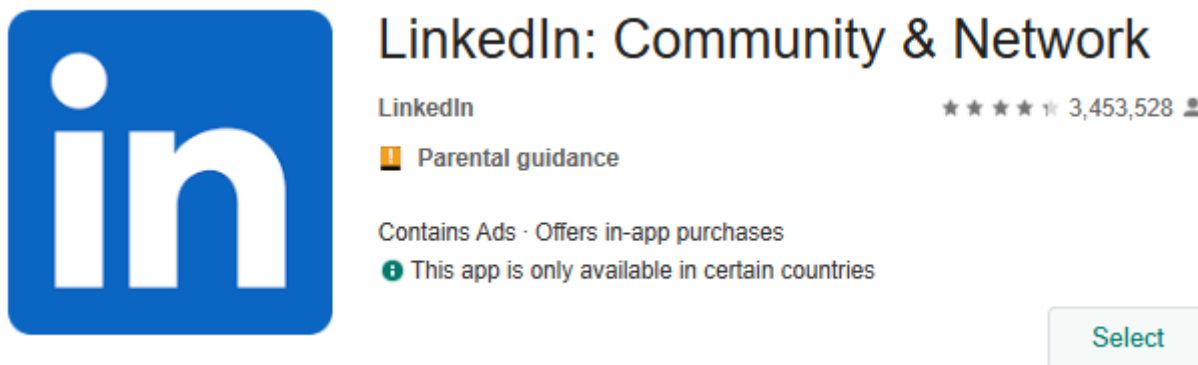
First, select an application to get started. Navigate to the Application List view from the left-side menu.



At the top of the view, select Add+ to choose an application from the Google Play Store, or select Upload APK+ to upload a custom APK package.



In this guide we will be selecting an LinkedIn application via the Google Play Store.



After selecting the application, navigate back to the Application List view and verify that the application appears in the list.

Add +Change Store LayoutUpload APK +

App name

Package name

Custom App

Search

←Page 1→Limit30

App name	Package
LinkedIn: Community & Network	com.linkedin.android
Kuori Security Service	tech.kuori.security.service.kuori
KMM Client	tech.kuori.kmmclientapp

Next, create an application policy. Navigate to Policies > Applications from the left-side menu. Select Create at the top of the page, then select Create New +.

KUORI

v1.3.0

Dashboard

Devices

Applications

Managed Configurations

Policies

Application

Device Function

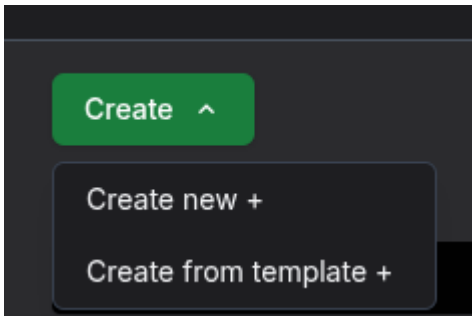
Create

Name

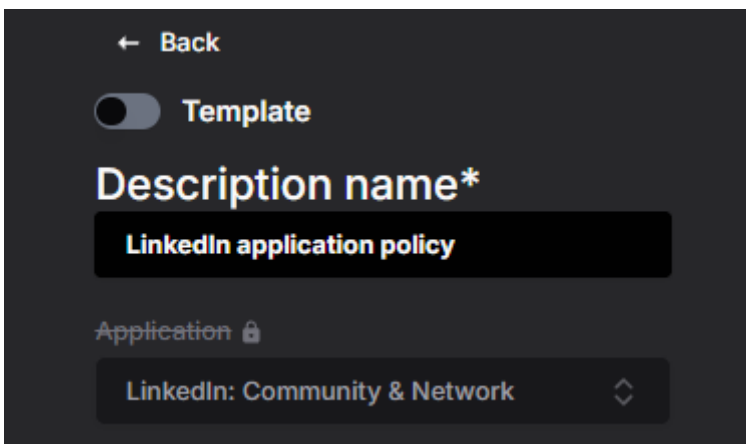
Advanced search

Search

←Page 1

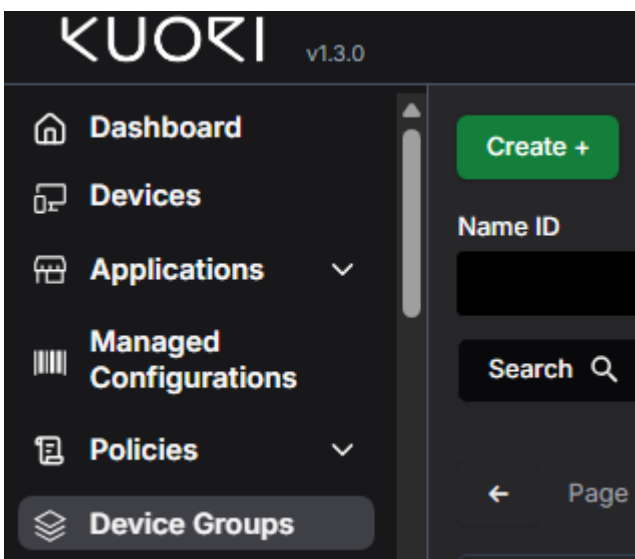


You can now select the application you just added from the dropdown menu. Fill in the Name ID field (Description name) for your new policy. Depending on the application, you may also want to modify some configuration settings. Once finished, press the Save button at the bottom of the page.



Creating a Device Group

Now that the application policy has been created, you need a device group where the policy will be applied. Navigate to the Device Groups page and press Create +.



Fill in the Name ID field. Note that the Name ID cannot contain whitespace characters. Under Applications, select the application policy you just created.

The **Use Client** switch is on by default and installs the KMM Client app on the group's devices. **Use Security Service** sits next to it and is off by default. The question mark beside each field explains what it does. You can read more about the client application [here](#).

Finally, press Save.

← Back

TestFiles ⓘ

Use Client ⓘ
☒ Yes

Use Security Service ⓘ
☐ Yes

Client Managed Config ⓘ
KMMClientToDSMGraniittiProd ⌵

Description ⓘ
For testing purposes

Device Functions ⓘ
⌵

Network and Connectivity Policy ⓘ
⌵

Files ⓘ
kiosk-config-prod-104.json ⌵

Applications ⓘ
FileExplorer ⌵

System Update Policy ⓘ
⌵

Interaction Policy ⓘ
⌵

Application Settings ⓘ
⌵

Administrative Policy ⓘ
⌵

Security Policy ⓘ
⌵

Edit

Assigning a Device to the Device Group

The final step is to attach a device to the newly created device group.

Navigate to the Devices page and select the eye icon for the device you want to assign to the group. In the device page, open the Actions tab and select the new device group you just created. To move several devices at once, tick their checkboxes in the device list and select **Change group**. The result is reported per device.

Finally press the save button next to the Device group.

After saving, KMM sends the updated policy information to Google AMAPI. Within approximately 10 minutes, the device will retrieve the updated policy and apply the required changes automatically.

Serial number	Display Name	Device Group	Android version	Brand	Model	Hardware number	Client Active	Last Report Time (UTC)	Actions
GRAN00001424	—	default	13	Kuori	KH3588S	—	X	2026-05-22 12:05:56	

CommandsActionsHardwareApplicationsPolicy ComplianceScreenshots

ⓘ Actions have delay from few seconds to maximum of ten minutes

Display name

Save

Device group

LinkedIndevicegroup

Save

Device state

Save

Hardware number

Save

Serial Number

Device Group

Client connection

Advanced search

Search

List

Map

3 devices selected

Change group

Reboot

←

Page 1

→

Limit

30

6 devices

☒	Serial number	Display Name	Device Group	Android version	Brand	Model	Client connection ⓘ	Client Last Connected (UTC)	Actions
☒	GRAN00001970	—	DSM_GRANIITTI	13	Kuori	KH3588S	●	2026-10-01 01:25:12	
☒	NUPITON00001008	—	DSM_NUPITON	11	Kuori	KH660	●	2026-10-01 01:25:12	
☒	RK356622110013	—	DSM_KIVI	11	Kuori	KH3566	●	—	
☐	GRAN00000923	R&D	DSM_GRANIITTI	13	Kuori	KH3588S	●	2026-09-30 10:31:44	
☐	GRAN00001139	—	DSM_GRANIITTI	13	Kuori	KH3588S	●	2026-09-30 10:31:44	
☐	GRAN00000990	—	TestFiles	13	Kuori	KH3588S	●	2026-09-30 10:31:24	

←

Page 1

→

Limit

30

Summary

In this guide, we went through the basic workflow for distributing applications with KMM. We selected an application, created an application policy, created a device group, and finally assigned a device to that group so the policy could be applied automatically.

This example demonstrates the basic concepts of how KMM policies, applications, and device groups work together. In a real production environment, device enrollment is typically handled through automated enrollment methods such as Zero-touch Enrollment or enrollment tokens.

You can read more about automated enrollment methods [here](#).

These enrollment methods allow devices to automatically enroll into KMM during setup, making large-scale deployments significantly easier and more efficient.

Enrollment

What does this do?

Enrollment is how an Android device joins KMM. During enrollment the device installs Android Device Policy, connects to your enterprise and lands in the device group you chose. From then on the device receives the policies, applications and settings of that group.

KMM supports three ways to enroll a device. All three start from the same thing: an **enrollment token** created in KMM.

- **Zero-touch enrollment.** The device enrolls by itself the first time it is switched on and connected to the internet. Nothing is typed on the device.
- **QR code enrollment.** The person setting up the device scans a QR code shown in KMM.
- **Token enrollment.** The person setting up the device types the token code shown in KMM.

Zero-touch is meant for fleets of new devices bought from a zero-touch reseller. QR code and token enrollment are meant for devices you set up by hand, one at a time.

Before You Start

- You need an editor or admin role to create or delete enrollment tokens. Viewers can open the page but cannot change anything.
- The device group the devices should join must already exist. Create it under **Device Groups** first.
- The device must be new or factory reset. Enrollment happens during the Android setup wizard and cannot be done on a device that is already in use.
- For zero-touch, the device must have been bought through a zero-touch reseller and be registered to your company in the zero-touch portal. Kuori manages the zero-touch portal on your behalf.

Zero-touch and manual enrollment do not mix

A device that is registered for zero-touch always enrolls through zero-touch. When such a device is switched on, Android fetches the zero-touch configuration before the setup wizard offers any other choice. You cannot skip it, scan a QR code or type a token on that device.

If you need to enroll a zero-touch device with a QR code or a token instead, ask your KMM administrators to remove the device from zero-touch first. Once the device has been removed, factory reset it and proceed with QR code or token enrollment as described below.

Creating an Enrollment Token

Every enrollment method needs a token, so create one first.

1. Open **Enrollment Tokens** in the side menu.
2. Select **Create +**.
3. Enter a **Display Name** so you recognize the token later.
4. Choose a **Duration**. This is how long the token stays valid, from half an hour up to five years, or **Forever**. Devices enrolled with the token stay enrolled after the token expires; only new enrollments stop.
5. Choose the **Device Group** the enrolled devices should join.
6. **Additional Data** is optional text saved with the token. You can leave it empty.
7. Switch **One Time Only** on if the token may be used for exactly one device. Leave it off for a token you will use for many devices.
8. **Management** and **Required Account Email** are only available for a Domain-Managed Enterprise. For other enterprises they are shown crossed out and the default is used. If you need them, upgrade the enterprise via the **Enterprise** page first.
9. **Management** and **Required Account Email** only works with domains where Enterprise has been binded to. For example if enterprise is binded to kuori.tech domain, only @kuori.tech emails will work with this.
10. Select **Save**.

The new token appears as a card on the **Enrollment Tokens** page. The card shows:

- **Expiration** as a UTC time.
- **Personal Usage**, **Required Account Email** and **Device Group** as chosen when the token was created.
- **Token**, the code used for token enrollment.
- **QR Code**, collapsed by default. Select the heading to show the code.
- **Zero Touch DPC Extras**, the text Kuori needs for zero-touch, with a **Copy to clipboard** button.

An expired token shows an **Expired** badge at the top of its card. Editors and admins can delete a token with the red delete button. Deleting a token does not unenroll devices that already used it.

Zero-touch Enrollment

With zero-touch the enrollment token is applied to the devices by Kuori, not on the device itself.

1. Create an enrollment token as described above. Use a long **Duration** or **Forever**, and leave **One Time Only** off, so the same token works for every device in the batch.
2. On the token card, select **Copy to clipboard** under **Zero Touch DPC Extras**.
3. Send the copied text to Kuori together with the list of devices that should use it. Kuori adds the configuration to your company in the zero-touch portal and assigns it to your devices.
4. Hand the devices to their users. When a device is switched on for the first time and connects to Wi-Fi or mobile data, it enrolls into the device group of the token without anyone doing anything on the device.

If a device was bought as zero-touch but has not been registered to your company yet, give Kuori the device serial numbers, manufacturer and model.

QR Code Enrollment

Use this when you set up devices by hand and have KMM open on a screen next to you.

1. Create an enrollment token as described above, or open an existing one that has not expired.
2. On the token card, select the **QR Code** heading to show the code.
3. Factory reset the device if it is not new, then switch it on.
4. On the Android **Welcome** screen, tap the same spot on the screen six times or in the email field, enter `afw#setup` and continue
5. The device asks to connect to Wi-Fi and then opens the QR code scanner. On some devices the scanner is offered directly on the Welcome screen.
6. Scan the QR code shown in KMM.
7. Follow the steps on the device. The device installs Android Device Policy, enrolls into KMM and applies the device group of the token.

Token Enrollment

Use this when you cannot scan a QR code, for example when the device has no camera or when you are giving instructions over the phone.

1. Create an enrollment token as described above, or open an existing one that has not expired.
2. Note the code shown under **Token** on the token card.
3. Factory reset the device if it is not new, then switch it on.
4. Go through the Android setup wizard until the Google sign-in screen.
5. In the email field, enter `afw#setup` and continue. The device installs Android Device Policy.
6. When asked for the enrollment code, type the **Token** exactly as shown in KMM.
7. Follow the remaining steps on the device. The device enrolls into KMM and applies the device group of the token.

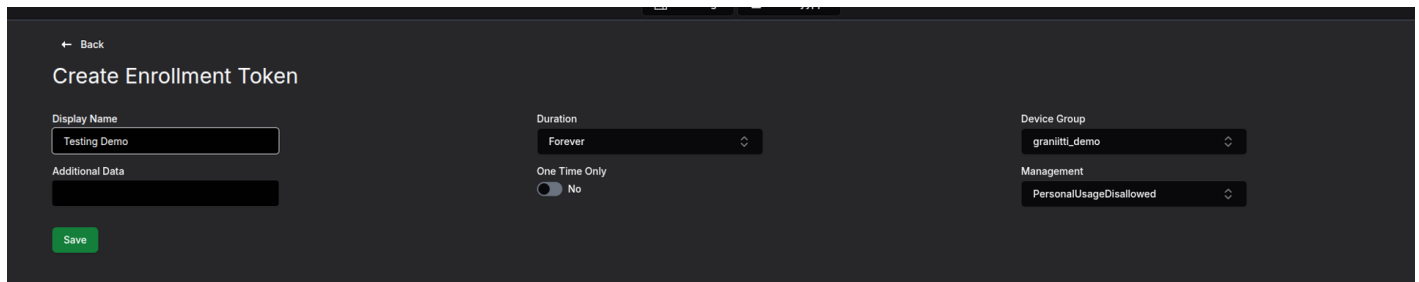
Zero-touch / Enrollment

Zero-touch enrollment is a deployment method that allows organizations to automatically configure and manage corporate devices right out of the box.

When a user powers on a new device and connects to the internet, it automatically downloads enterprise policies, apps, and security settings with no manual IT setup required.

Enrolling devices with Zero-touch

First, create an enrollment token in KMM



← Back

Create Enrollment Token

Display Name	Duration	Device Group
Testing Demo	Forever	granitti_demo
Additional Data	One Time Only	Management
	☐ No	PersonalUsageDisallowed

Save

Then you need to either have access to Zero-touch customer portal, or give the token to someone who has access to it.

Kuori usually manages zero touch portal and handles the initial device enrollment through it.

Zero-touch customer portal

Add Configuration: Go to the **Configurations** tab.

- **Set the EMM DPC:** Select your MDM application/agent (or `Android Device Policy`) as the EMM DPC.
- **Add DPC Extras:** Paste the JSON or setup token generated from your EMM dashboard into the DPC Extras box.
- **Assign:** Save the configuration and either set it as your **Default** profile or manually apply it to specific devices using their serial number in the **Devices** tab

KMM Client

KMM Client is a KMM Extension App. KMM Client extends the standard capabilities of Android Management API by enabling additional device management features directly on managed Android devices.

The application runs in the background on enrolled devices and allows KMM to perform advanced management actions that are not available through standard Android Management API policies alone.

Some of the features require a separate Kuori Security Service application that is available in Managed Google Play. This service provides privileged access to specific Android system APIs that are not available to standard Android applications.

The following sections describe the available features and how to enable KMM Client on enrolled devices.

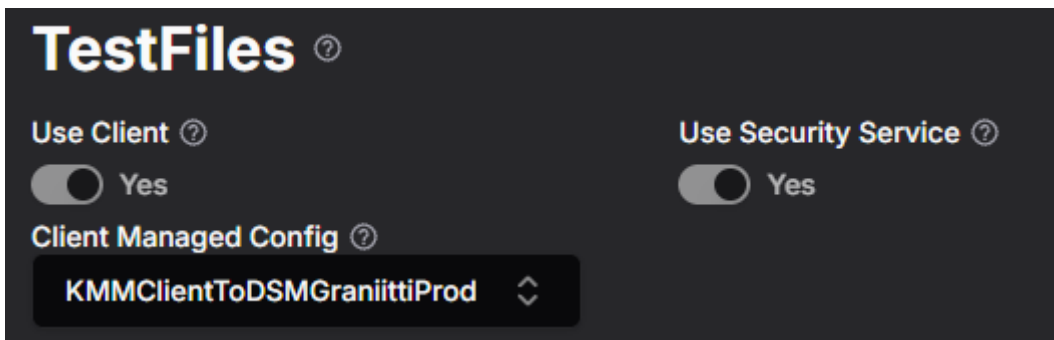
Features

- Device online status `0.1.0`
 - Pings KMM to tell if Client is currently active
- Background image change `0.1.0`
 - Change background image via managed configurations
- Enabling gesture navigation `0.1.0` `Requires Security Service`
 - Gesture navigation set on/off via managed configurations
- Custom application installation (APK) `0.2.0`
 - Get and install desired custom APKs from the server
- Screen capture (screenshot) `0.2.0` `Requires Security Service`
 - Server requests a screenshot and client sends image to the server
- Setting of landscape/portrait mode `0.2.0` `Requires Security Service`
 - Display Rotation set via managed configurations
- File upload from the server `0.3.0`
 - Upload files to specific locations on the device
- Automatically wake DSM client (if installed) `0.3.0`
 - KMM Client detects if DSM Client is installed and wakes it via broadcast
- Device location `0.6.0`
 - KMM Client reports the device position; KMM shows it on the device map and on the device page's Location tab.

How to enable KMM Client

When creating a Device Group, the **Use Client** option is enabled by default. Enabling this option automatically adds the KMM Client and required Setup Action to the new device group. The **Use Security Service** option is disabled on default. Enabling this option automatically adds the Kuori Security Service to the new device group. *These applications are added to the KMM enterprise by default.*

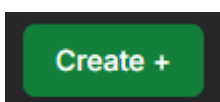
A Managed Configuration for the Client must also be selected. Default managed configuration is selected automatically. Custom managed configurations can also be created to modify the behavior and settings of the Client. These configuration options are described in detail in the following Features section.



Note: You can also manually create Application Policies for KMM Client and Security Service and Interaction Policy for the Setup Action, but this is the preferred way.

Adding Custom Managed Configurations

To add custom Managed Configurations, you need API key for KMM Client. Navigate to **API Keys** from the side navigation and click Create new API key:



Enter display name for the API key (this **can not** be edited later). Also save the actual API key to somewhere secure, you won't be able to see it again.

New API Key

This key will only be shown once. Save it somewhere secure before creating it — you won't be able to view it again.

Display Name

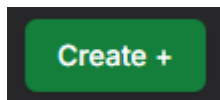
API Key

api_ece96d8854a0a5b8b264705fec4cd07f9a12
7861b21a09459c3a8f3941e2e69f

CopyCancelCreate Key

Next navigate to **Managed Configurations** from the side navigation:

You can choose to edit existing one or create a new one. To Create new, click the Create button:



Choose **KMM Client** from the package name dropdown:

Fetch by package name

⌵

Enter description name for the configuration and select the settings you want to configure (API key is mandatory).

tech.kuori.kmmclientapp

Description name*

KMM Client Configuration

Select settings

api_key, background_image, enable_gesture_navigation, display_rotation

api_key

api_4c899d981a40b9f2d76682425c03906

background_image

wallpaper.png

enable_gesture_navigation

☒ Yes

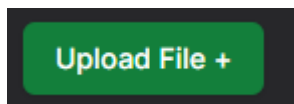
display_rotation

0°

Create

Gesture Navigation and Display Rotation can be chosen from this view.

The Background Image needs a filename for the desired image. The image needs to be uploaded to the KMM first. To upload image, navigate to **Files** from the side navigation and click **Upload File**:



For background image the description is optional and destination folder is **not needed**. Destination folder is used for file upload to the device. *More about file upload later in the Features Explained.*

Upload File

Choose File

wallpaper.png

Max file size: 1 GB

Selected: wallpaper.png (0.03 MB)

Description (Optional)

Enter description

Destination Folder (Optional)

Select folder

Cancel

Upload

Features Explained

Server ping / Online status

A connected client shows as a green dot in the **Client connection** row of the device page's Status section and in the **Client connection** column of the device list. Yellow means a weak connection (hover the dot for the response time), red means not connected, grey means the group does not use the client. **Client Last Connected (UTC)** shows when the client last connected or disconnected. The dot updates live; no reload is needed.

☐ Serial number	Display Name	Device Group	Android version	Brand	Model	Client connection ⓘ	Client Last Connected (UTC)	Actions
☐ GRAN00000990	—	default	13	Kuori	KH3588S		2026-09-30 10:15:27	 

Background image

Sets the background image shown on the device home screen. Choose an image that fits your device screens; the KMM Client applies it when the configuration is published to the device group. The image is set by the KMM Client together with its Security Service app, so both must be installed on the device.

Enable gesture navigation

Switches the device to gesture navigation instead of the three-button navigation bar. Its main purpose is to hide the taskbar when an application runs in kiosk mode, so the user sees only the kiosk app. Set it to ****Yes**** to hide the taskbar and ****No**** to keep the standard navigation bar. In the ready-made configuration this setting is ****Yes****.

Display rotation

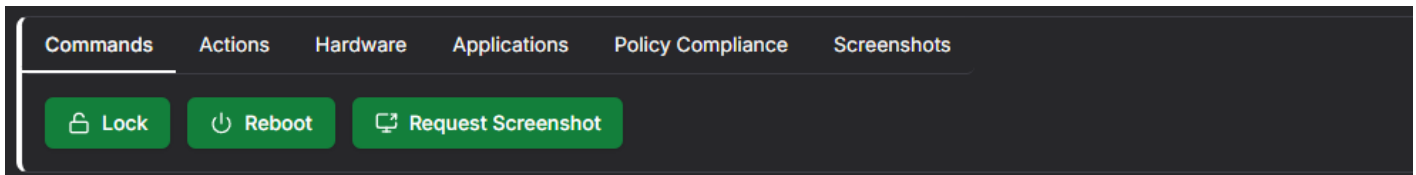
Fixes the orientation of the device screen. If the picture on the screen isn't oriented correctly from the start (for example, it's showing landscape content on a portrait-mounted totem, or it's simply upside down), you can fix this from the KMM client. The rotation setting only offers four fixed values — 0°, 90°, 180°, and 270° — so you just pick whichever of the four matches how the screen is physically mounted, and the display will reorient to match. It's not a fine-tune/free-angle adjustment, just one of those four positions.

Screen capture (screenshot)

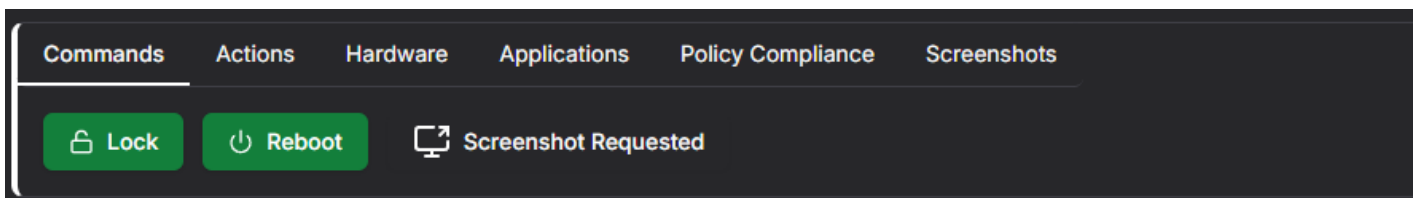
Screenshot can be requested from Device page. Navigate to **Devices** from side navigation and open the desired device from the View button:



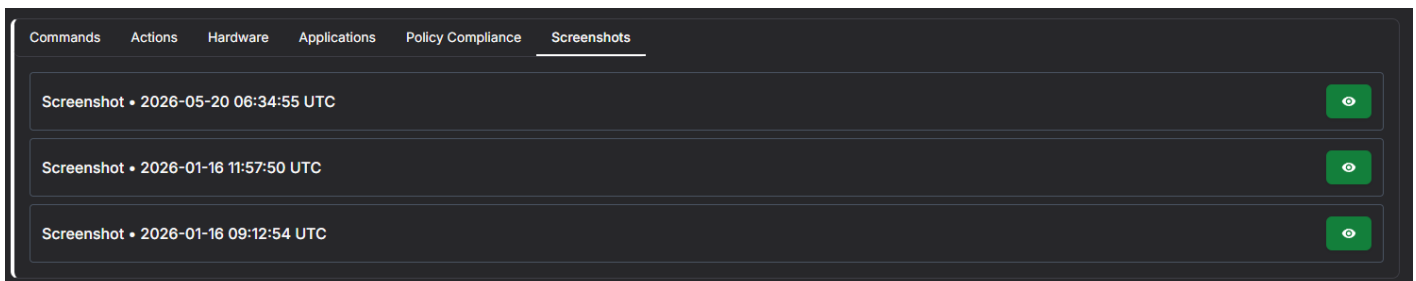
From the **Commands** tab you can find **Request Screenshot** button:



When requested, the button stays inactive until the screenshot is received from the Client:

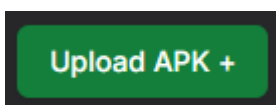


The screenshot appears in the Screenshots tab as soon as the device sends it, and the bell shows a **Screenshot Ready** notification. If the device could not take it, the bell shows **Screenshot Failed** with the reason and the button becomes available again. *Only the latest five screenshots are saved* :



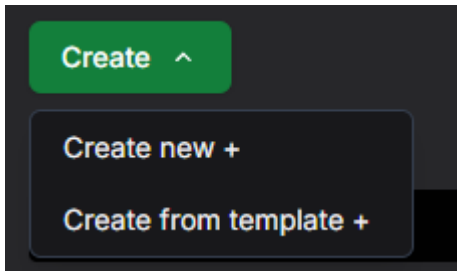
Custom APK installation

KMM Client installs desired APKs from KMM. To add custom APK to device group, navigate to **Applications** → **Application List** from the side navigation and click upload APK:



Choose the APK file and click Upload.

Next you need to create Application Policy for the Custom APK. Navigate to **Policies** → **Application** from the side navigation and click create new:



Enter description name and choose the application from the dropdown:

A dark-themed form titled 'Description name*'. It contains a text input field with the placeholder 'Enter Description name'. Below it is a dropdown menu labeled 'Application' with a downward arrow icon. Under the dropdown, the text 'Select application first...' is displayed. At the bottom of the form are two buttons: a green 'Save' button and a white 'Reset' button with a dark border.

When custom APK is chosen, the necessary settings are set by default. You can change the APK version code (if multiple versions of the same APK are uploaded to the KMM):

Description name*

Custom Application Policy

Application

DsmClientApp

Default Permission Policy

Grant

Delegated Scopes

Unspecified

Always On VPN Lockdown Exemption

Unspecified

User Control Settings

Unspecified

Charging Constraint

Unspecified

Signin Key Fingerprint SHA-256

7ba7a1c8fbc67541b6e817c7... x

Configuration

Select permissions (overrides default)

Install Type

Custom

Disabled

No

Accessible Track Ids

Credential Provider Policy

Unspecified

Network Type Constraint

Unspecified

Allow Uninstall By User

DisallowUninstallByUser

Role Type

Minimum Version Code

Auto Update Mode

Unspecified

Install Priority

Device Idle Constraint

Unspecified

APK Version Code

78

Save

Reset

Now that Application Policy can be added to the Device Group. Navigate to **Device Groups** from the side navigation and click open the desired Device Group from the list:



Click **Edit** and choose the Application Policy from the **Applications** dropdown:

← Back

NewDeviceGroup

Use Client

Yes

Use Security Service

Yes

Client Managed Config

KMM Basic config

Description

Demo Group

Device Functions

Network and Connectivity Policy

Files

Applications

Custom Application Policy

System Update Policy

Interaction Policy

Application Settings

Administrative Policy

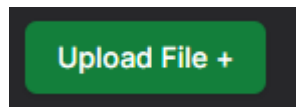
Security Policy

Edit

KMM Client installs the desired APKs assigned to its Device Group.

File upload

Upload files to specific locations on the device. First upload the desired files to KMM. Navigate to **Files** from the side navigation and click upload file:



Choose the file, and enter the description (optional). Destination folder offers Android's default folders and also a Custom folder. If Destination Folder is not provided, the file will be downloaded to */Downloads*:

Upload File

Choose File

demo_config.json

Max file size: 1 GB
Selected: demo_config.json (0.00 MB)

Description (Optional)

Enter description

Destination Folder (Optional)

Select folder

Q Search...

Default (/Downloads)

Pictures (/Pictures)

Videos (/Videos)

Audio (/Audio)

Documents (/Documents)

Custom

Next add that file to the Device Group. Navigate to **Device Groups** from the side navigation, click open the desired Device Group from the list:



Click **Edit** and choose the file(s) from the **Files** dropdown:

← Back

NewDeviceGroup ⓘ

Use Client ⓘ
☐ Yes

Use Security Service ⓘ
☐ Yes

Client Managed Config ⓘ
KMM Basic config ⌵

Description ⓘ
Demo Group

Device Functions ⓘ
⌵

Network and Connectivity Policy ⓘ
⌵

Files ⓘ
demo-config.json ⌵

Applications ⓘ
⌵

System Update Policy ⓘ
⌵

Interaction Policy ⓘ
⌵

Application Settings ⓘ
⌵

Administrative Policy ⓘ
⌵

Security Policy ⓘ
⌵

Edit

KMM Client downloads the desired files assigned to its Device Group.

Automatically wake DSM Client if installed on the device

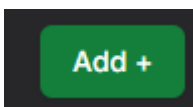
KMM Client detects if DSM Client is installed and wakes it up via broadcast.

Application Management

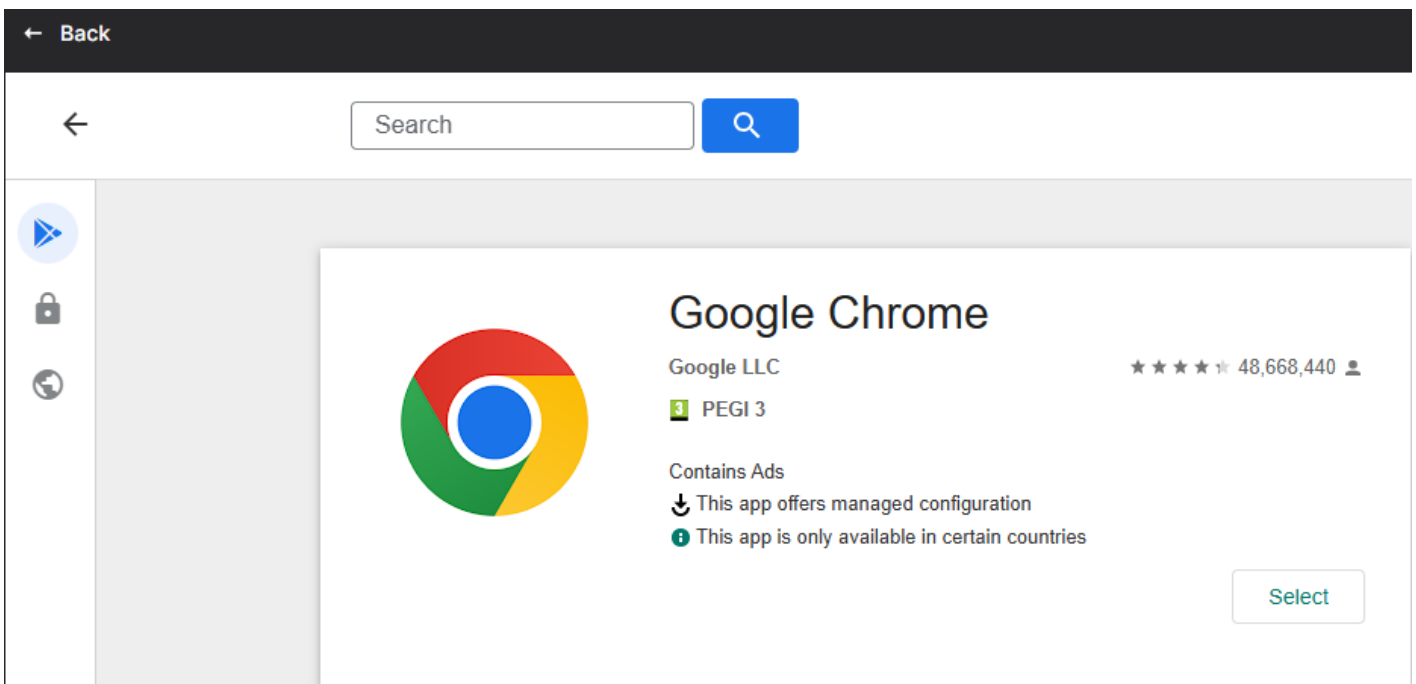
To install app on your device, you need to add the application to your enterprise in KMM. After that you need to create [Application Policy](#) for that application. That policy needs to be then added to the [Device Group](#) your Device belongs to in order to install the application.

Install application on device

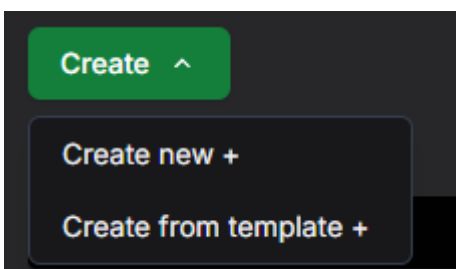
First navigate from the side navigation to [Applications](#) → [Application List](#) and click 'Add +'.



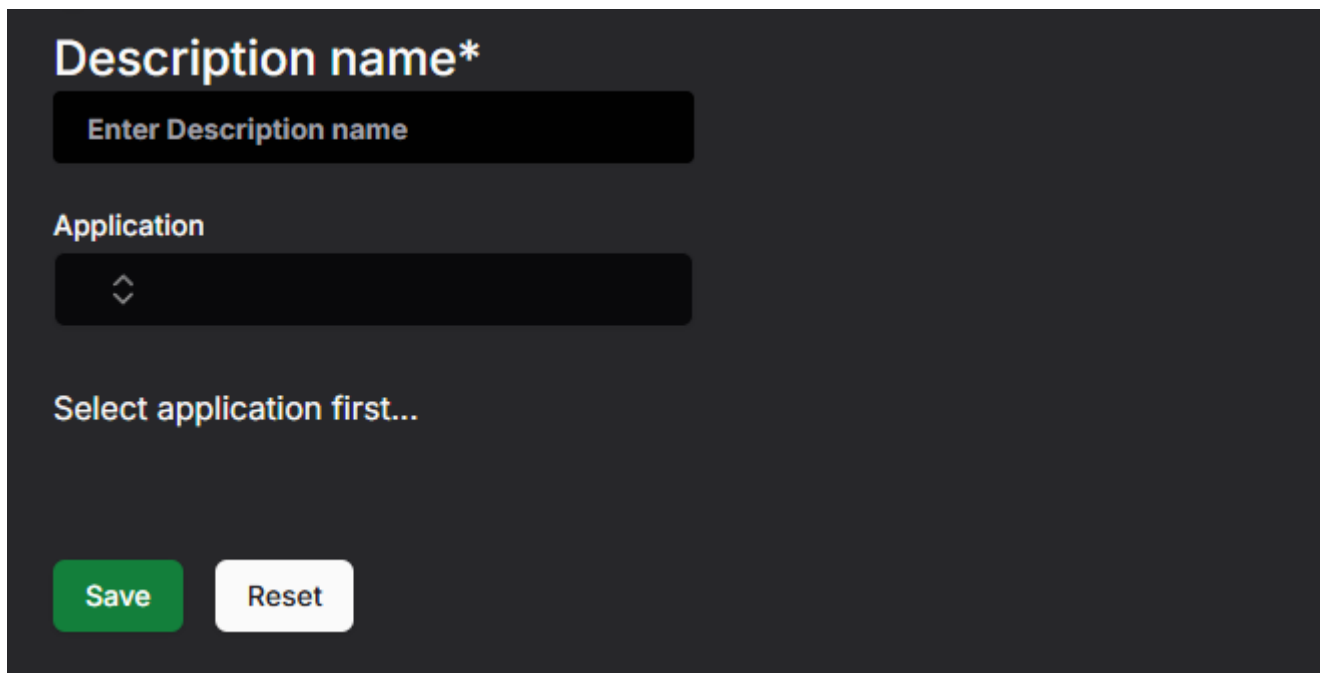
Select or search the desired application from Play Store and click 'Select':



Next the application needs [Application Policy](#) that can be added to the [Device Group](#). Navigate to Policies → Application from the side navigation and click 'Create new +':



Enter description name for the policy and choose your application from the dropdown:



Description name*

Enter Description name

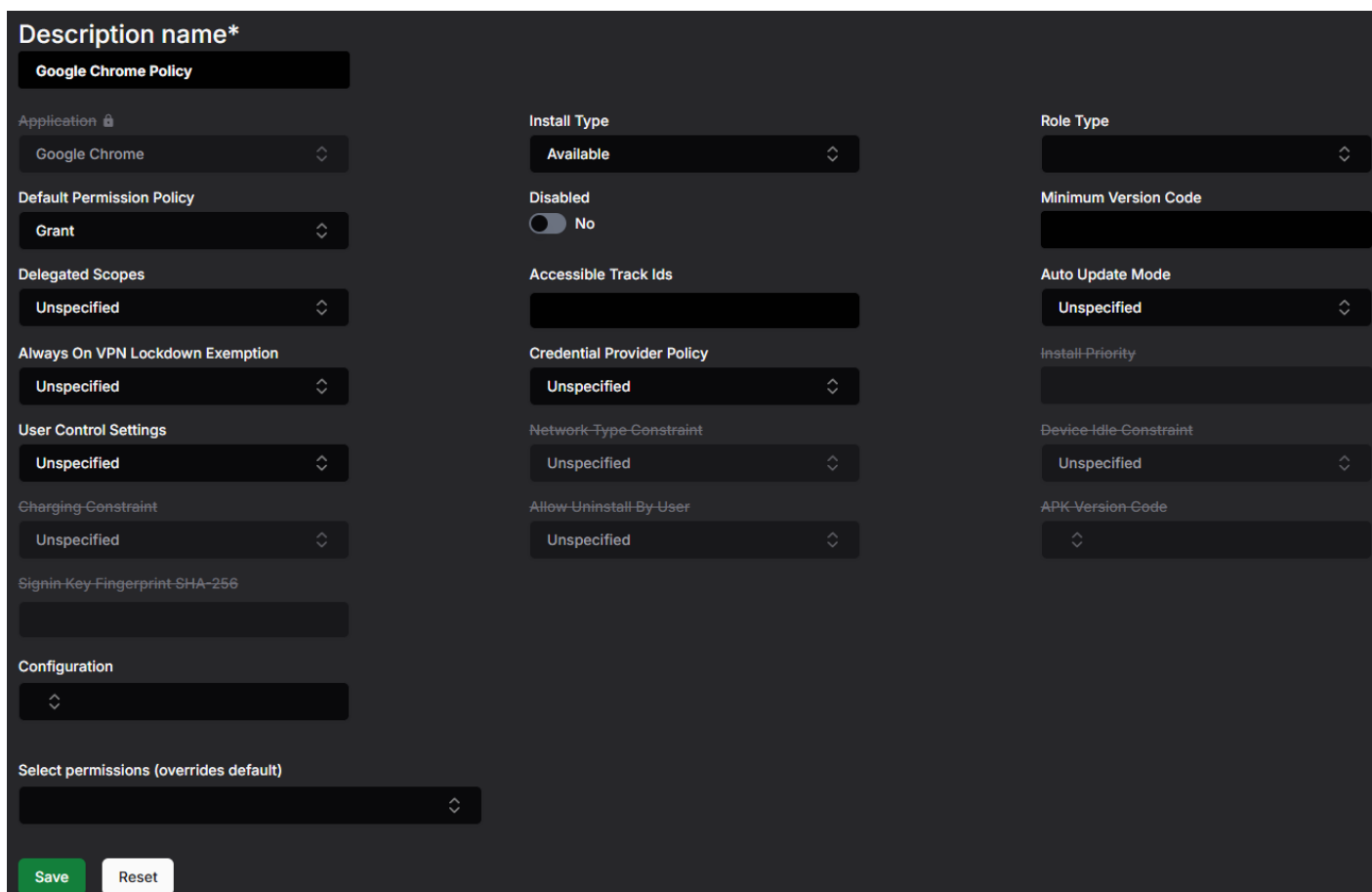
Application

⌵

Select application first...

Save **Reset**

Default values are provided for the configuration with Install Type 'Available':



Description name*

Google Chrome Policy

Application 

Google Chrome

Default Permission Policy

Grant

Delegated Scopes

Unspecified

Always On VPN Lockdown Exemption

Unspecified

User Control Settings

Unspecified

Charging-Constraint

Unspecified

Signin-Key-Fingerprint-SHA-256

Configuration

⌵

Select permissions (overrides default)

⌵

Install Type

Available

Disabled

☐ No

Accessible Track Ids

Credential Provider Policy

Unspecified

Network-Type-Constraint

Unspecified

Allow-Uninstall-By-User

Unspecified

Role Type

Minimum Version Code

Auto Update Mode

Unspecified

Install-Priority

Device-Idle-Constraint

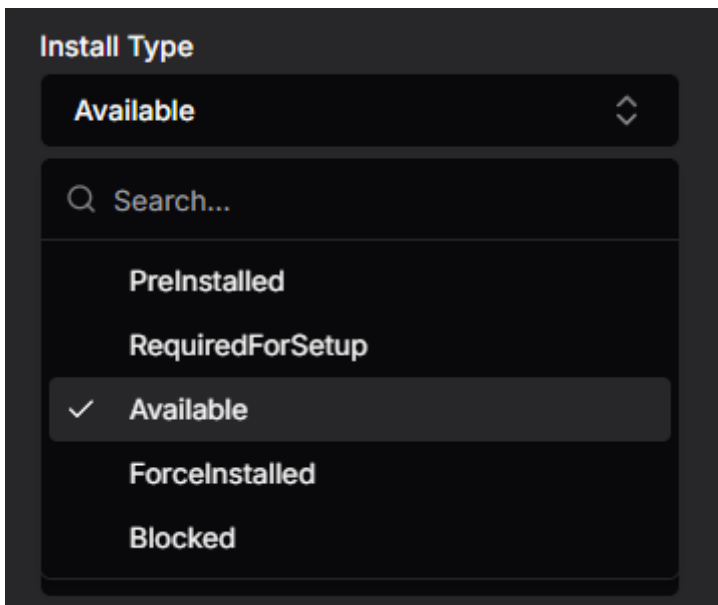
Unspecified

APK-Version-Code

⌵

Save **Reset**

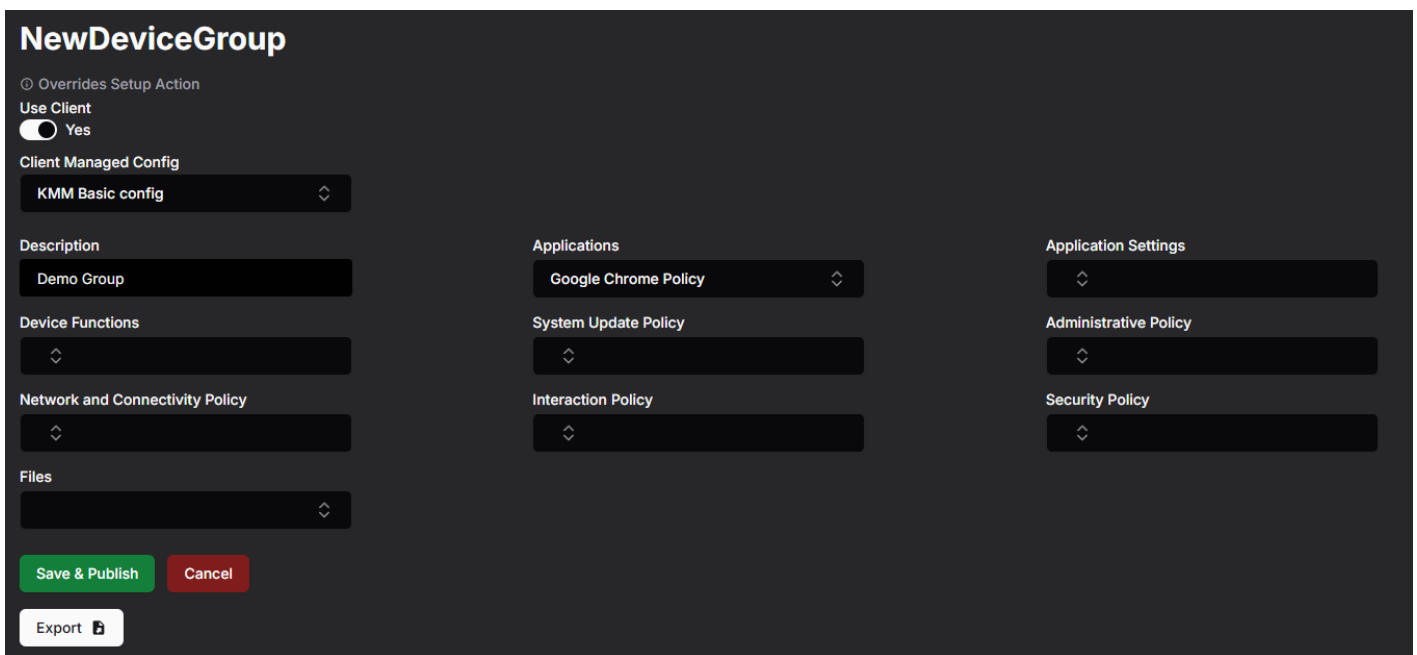
The Install Type can be changed on non-custom applications. **Available** means that the application can be freely installed from the Play Store on the device, but it is not installed automatically. Other options are:



The screenshot shows a dark-themed dropdown menu titled "Install Type". The menu is open, displaying a list of options: "Available", "PreInstalled", "RequiredForSetup", "Available" (with a checkmark), "ForceInstalled", and "Blocked". The "Available" option is currently selected.

ForceInstalled installs the application automatically when the policy is applied to the group that the device belongs to. The application can not be uninstalled manually from the device with this setting. **RequiredForSetup** installs the application automatically when the device is enrolled.

After the policy is created navigate to **Device Groups** from the side navigation and click open the desired group (or create a new one). Choose the policy from the Applications dropdown and save the group:



The screenshot shows the "NewDeviceGroup" form in a dark theme. The form includes several sections: "Overrides Setup Action" with a "Use Client" toggle set to "Yes"; "Client Managed Config" with a dropdown set to "KMM Basic config"; "Description" with a text field containing "Demo Group"; "Device Functions" with a dropdown; "Network and Connectivity Policy" with a dropdown; "Files" with a dropdown; "Applications" with a dropdown set to "Google Chrome Policy"; "System Update Policy" with a dropdown; "Interaction Policy" with a dropdown; "Application Settings" with a dropdown; "Administrative Policy" with a dropdown; and "Security Policy" with a dropdown. At the bottom, there are buttons for "Save & Publish" (green), "Cancel" (red), and "Export" (white with a download icon).

Install custom application on device

KMM Client installs desired APKs from KMM. To add custom APK to device group, navigate to **Applications** → **Application List** from the side navigation and click upload APK:

Upload APK +

Choose the APK file from your device and click Upload:

Upload APK

Choose File DSMClientAp...iitti_0_4_32.apk

Max file size: 1 GB

Selected: DSMClientApp_graniitti_0_4_32.apk
(3.27 MB)

Cancel

Upload

Next you need to create Application Policy for the Custom APK. Navigate to **Policies** → **Application** from the side navigation and click create new:

Create ^

Create new +

Create from template +

Enter description name for the policy and choose your custom application from the dropdown:

Description name*

Enter Description name

Application



Select application first...

Save

Reset

When custom APK is chosen, the necessary settings are set by default. Install Type is locked to **Custom** for custom applications. You can change the APK version code (if multiple versions of the same APK are uploaded to the KMM):

The screenshot shows the 'Custom Application Policy' configuration screen. It features a dark theme with various settings organized into columns. The settings include:

- Description name***: Custom Application Policy
- Application**: DsmClientApp
- Default Permission Policy**: Grant
- Delegated Scopes**: Unspecified
- Always On VPN Lockdown Exemption**: Unspecified
- User Control Settings**: Unspecified
- Charging Constraint**: Unspecified
- Signin Key Fingerprint SHA-256**: 7ba7a1c8fbc67541b6e817c7... x
- Configuration**: Unspecified
- Select permissions (overrides default)**: Unspecified
- Install Type**: Custom (locked)
- Disabled**: No
- Accessible Track Ids**: Unspecified
- Credential Provider Policy**: Unspecified
- Network Type Constraint**: Unspecified
- Allow Uninstall By User**: DisallowUninstallByUser
- Role Type**: Unspecified
- Minimum Version Code**: Unspecified
- Auto Update Mode**: Unspecified
- Install Priority**: Unspecified
- Device Idle Constraint**: Unspecified
- APK Version Code**: 78

At the bottom, there are 'Save' and 'Reset' buttons.

Now that Application Policy can be added to the Device Group. Navigate to **Device Groups** from the side navigation and click open the desired Device Group from the list (or create a new one). Choose the policy from the **Applications** dropdown and save the group:

The screenshot shows the 'NewDeviceGroup' configuration screen. It features a dark theme with various settings organized into columns. The settings include:

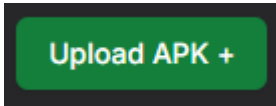
- Overrides Setup Action**: Use Client
- Use Client**: Yes
- Client Managed Config**: KMM Basic config
- Description**: Demo Group
- Device Functions**: Unspecified
- Network and Connectivity Policy**: Unspecified
- Files**: Unspecified
- Applications**: Custom Application Policy
- System Update Policy**: Unspecified
- Interaction Policy**: Unspecified
- Application Settings**: Unspecified
- Administrative Policy**: Unspecified
- Security Policy**: Unspecified

At the bottom, there are 'Save & Publish', 'Cancel', and 'Export' buttons.

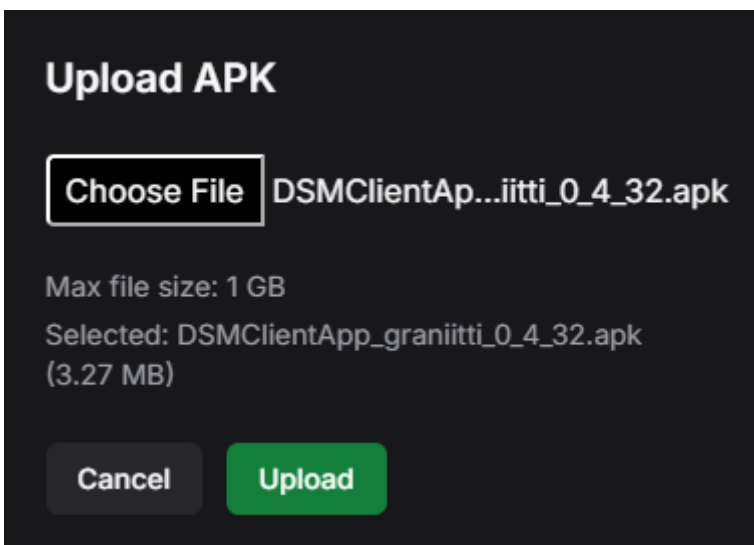
KMM Client installs the desired APKs assigned to its Device Group.

Custom APK to Kiosk

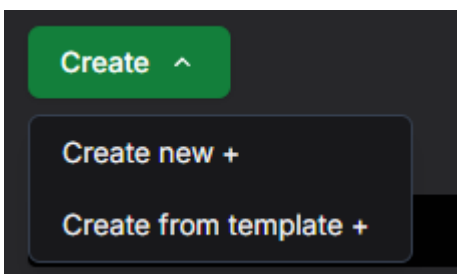
KMM Client installs desired APKs from KMM. To add custom APK with **Kiosk** mode to device group, first you need to navigate to **Applications** → **Application List** from the side navigation and click upload APK:



Choose the APK file from your device and click Upload:



Next you need to create Application Policy for the Custom APK. Navigate to **Policies** → **Application** from the side navigation and click create new:



Enter description name for the policy and choose your custom application from the dropdown:

Description name*

Enter Description name

Application

Select application first...

Save

Reset

When custom APK is chosen, choose **Kiosk** for the Role Type. Install Type is locked to **Custom** for custom applications. You can change the APK version code (if multiple versions of the same APK are uploaded to the KMM):

Description name*

Custom APK Kiosk

Application

DsmClientApp

Default Permission Policy

Grant

Delegated Scopes

Unspecified

Always On VPN Lockdown Exemption

Unspecified

User Control Settings

Unspecified

Charging Constraint

Unspecified

Signin Key Fingerprint SHA-256

7ba7a1c8fbc67541b6e817c7... x

Configuration

Install Type

Custom

Disabled

No

Accessible Track Ids

Credential Provider Policy

Unspecified

Network Type Constraint

Unspecified

Allow Uninstall By User

DisallowUninstallByUser

Role Type

Kiosk

Minimum Version Code

Auto-Update Mode

Unspecified

Install Priority

Device Idle Constraint

Unspecified

APK Version Code

78

Save

Reset

Now that Application Policy can be added to the Device Group. Navigate to **Device Groups** from the side navigation and click open the desired Device Group from the list (or create a new one). KMM Client is required for custom APK installs, so make sure **Use Client** is enabled with correct configuration. KMM Client installs the desired APKs assigned to its Device Group.

Choose the policy for the APK from the **Applications** dropdown and save the group:

The screenshot shows a configuration form titled "Name ID". At the top, there is a text input field containing "CustomKioskGroup". Below this, there is a section for "Overrides Setup Action" with a "Use Client" toggle switch set to "Yes". A note states: "Client Managed Config: A default config has been applied automatically. Update it if needed". Below this is a dropdown menu showing "KMMClientSettings". The form is organized into three columns. The first column contains: "Description" (text input: "Demo Group"), "Device Functions" (dropdown), "Network and Connectivity Policy" (dropdown), and "Files" (dropdown). The second column contains: "Applications" (dropdown: "Custom APK Kiosk"), "System Update Policy" (dropdown), and "Interaction Policy" (dropdown). The third column contains: "Application Settings" (dropdown), "Administrative Policy" (dropdown), and "Security Policy" (dropdown). At the bottom left is a green "Save" button.

Optionally, we can also create Interaction Policy for more Kiosk settings. Navigate to **Policies** → **Interaction** from the side navigation, and click Create:

The screenshot shows a green "Create" button with an upward arrow. A dropdown menu is open below it, showing two options: "Create new +" and "Create from template +".

Enter the description name and edit the desired settings. Here we can find Kiosk custom launcher enabled, Kiosk power button actions, Kiosk system error warnings, Kiosk system navigation, Kiosk status bar and Kiosk device settings. Save the policy when ready.

Description Name*

Kiosk Settings

Set user icon disabled

No

Screen brightness mode

Unspecified

Kiosk system error warnings

Unspecified

Kiosk device settings

Unspecified

Screen timeout

Set wallpaper disabled

No

Screen timeout mode

Unspecified

Kiosk system navigation

Unspecified

Credential provider policy default

Unspecified

Kiosk custom launcher enabled

No

Kiosk power button actions

Unspecified

Kiosk status bar

Unspecified

Screen-brightness-%

Support Messages

+ Add Support Messages

Setup Action

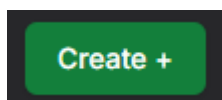
No setup action added yet.

+ Add Setup Action

Save Policy

The Interaction Policy can be added to the Device Group the same way the Application Policy was added previously.

Lastly, we need **Enrollment Token** for the new group. Navigate to **Enrollment Tokens** from the side navigation, and click Create:



KMM automatically generates new group with "initial_" prefix for the groups that have KMM Client and Custom APK with Kiosk mode enabled. Choose that and click Save:

Create Enrollment Token

Display Name

Custom APK Kiosk

Duration

Forever

Device Group

initial_CustomKioskGroup

Additional Data

One Time Only

No

Management

PersonalUsageDisallowedUserless

Save