



# **PRADEO SECURITY Mobile Threat Defense Quick Start Guide**

Integration with Samsung Knox Manage



# TABLE OF CONTENTS

---

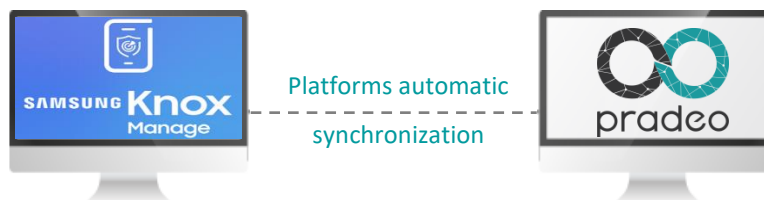
Overview.....	2
Requirements.....	3
Get started.....	4
1. Platforms connection .....	4
1.1 In Samsung Knox Manage .....	4
1.2 In Pradeo Security .....	5
2. Configuration of the integration level.....	6
2.1 By default.....	6
2.2 Ease administrators and users experience.....	7
2.3 Enforce the security policy in Samsung Knox Manage.....	7
3. Pradeo Security agent .....	9
3.1 Overview.....	9
3.2 0-touch enrollment.....	9

## OVERVIEW

The integration between Pradeo Security Mobile Threat Defense and Samsung Knox Manage offers two levels of deployment.

### 1 Automatic apps lists population

Synchronize the platforms to automatically empower the apps security capability.



### 2 On- Device Apps, Network & OS protection

Deploy the Pradeo Security agent on devices to block Apps before the first use, protect from device and network threat protection and dynamically enforce Samsung Knox Manage compliance policy.



## REQUIREMENTS

Pradeo Security Mobile Threat Defense integration with Samsung Knox Manage requires the following configuration:

- Apple devices with iOS 8+
- Android devices with OS 5+

# GET STARTED

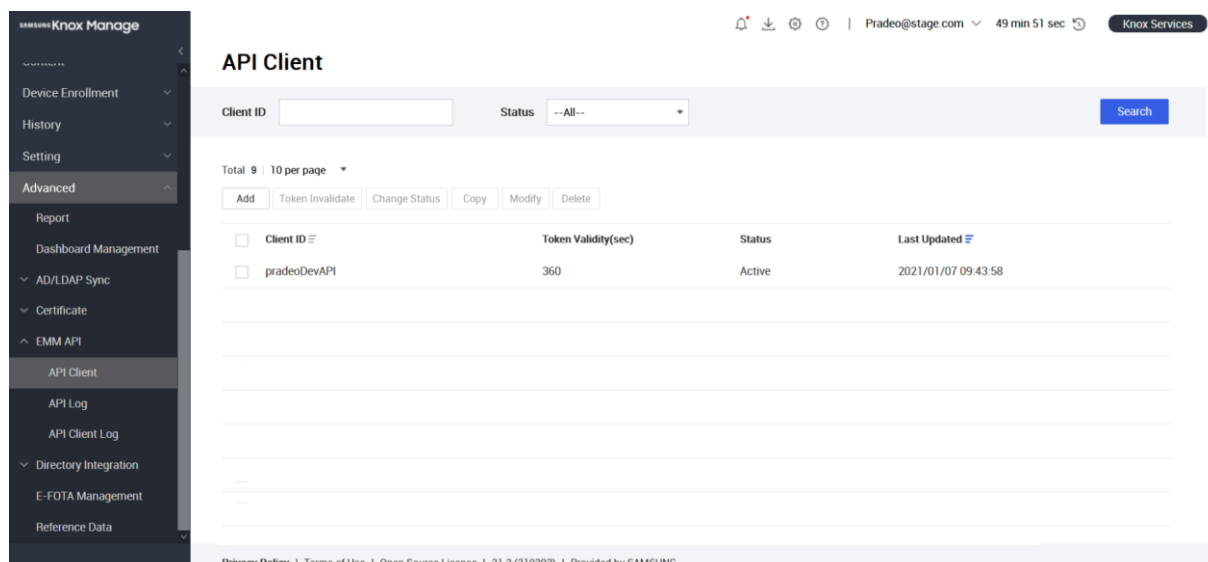
## 1. Platforms connection

### 1.1 In Samsung Knox Manage

Pradeo Security will interact with Samsung Knox Manage through the API REST. In order to allow the interaction between the 2 consoles a new API Client needs to be generated.

In order to generate the and retrieve the **Client Id** and **Password** necessary for the connection to Pradeo's platform, please proceed to:

From the Samsung Knox Manage console, select **Advanced** → **EMM API** → **API Client** → **Add**



A pop-up window will appear asking you to fill a few fields:

**Add API Client**
✕

**Client ID \***

The entered client ID cannot be changed.

**Password \***

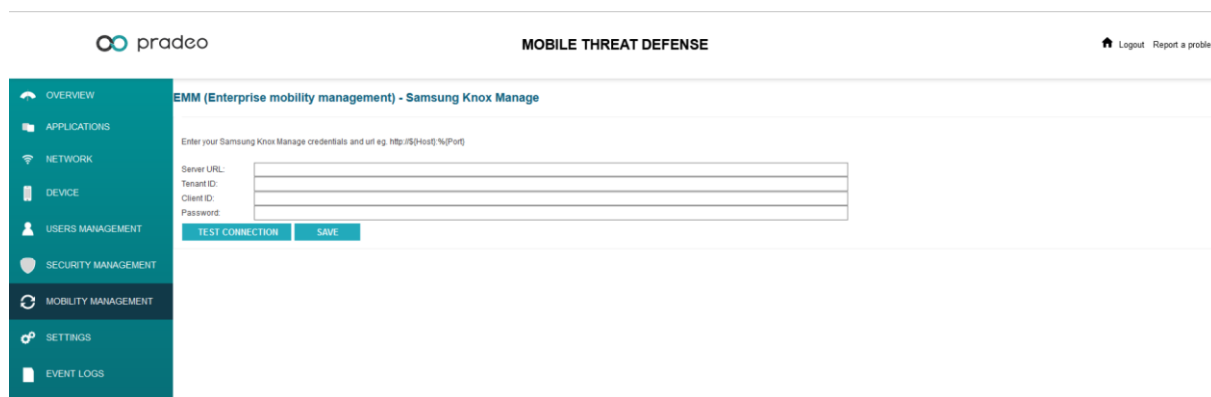
**Token Validity(sec) \***

This user will be inactive due to exceeding the number of licenses.

Please, make sure to note the ID and Password since they will be needed on Pradeo's console.

## 1.2 In Pradeo Security

On the Pradeo Security platform, click on the Mobile Threat Defense service then open the menu and go to **Mobility Management - Enterprise Mobility Management** and click on the Samsung Knox Manage logo.



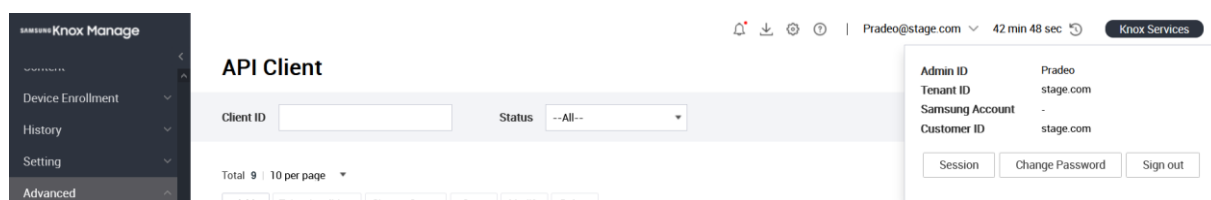
A form allows you to enter the parameters necessary to establish the connection with Workspace ONE powered by AirWatch.

You will need the following information:

- **Server URL**
- **Tenant ID**
- **Client ID**
- **Password**

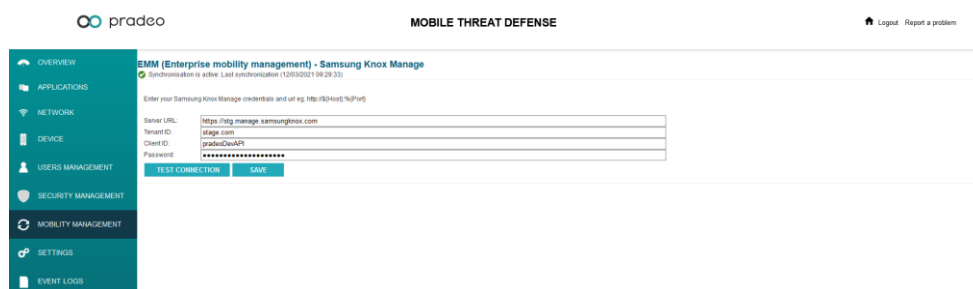
The **Server URL** is self-explanatory;

The **Tenant ID** can be retrieved from the Samsung Knox Manage console by clicking on the user id on the top right of the screen



**Client ID and Password** have been created on the step 1.1 of this guide.

Click "Save" to validate the settings. A synchronization status is displayed at the top of the page to indicate if the synchronization is active as well as the date of the last synchronization.



## 2. Configuration of the integration level

Pradeo provides a custom configuration of the integration to match each company's requirements.

The Pradeo support team will activate the platform-to-platform synchronization based on your preferences.

### 2.1 By default

#### *2.1.1 Synchronization of device information*

By default, devices enrolled on the Pradeo Security platform are anonymized: the self-enrollment process adds the terminals to the platform with a standard name (for example, the name of your company).

Then, the synchronization process automatically updates on Pradeo console: user's informations (first name, last name, e-mail address, device id) available in Samsung Knox Manage referring to the UDID or Serial Number as a unique identifier to match each device.

#### *2.1.2 Synchronization of monitored applications*

The synchronization process imports applications monitored in Samsung Knox Manage in the Pradeo Security platform to get them processed against the security policy and trigger required security measures.



For Android devices, the Pradeo Security agent, when installed, takes over the synchronization process to report installed/updated applications in real-time and trigger an immediate security response depending on security level that has been configured.

## 2.2 Ease administrators and users experience

### 2.2.1 Pre-import groups and devices

Groups and devices existing in Samsung Knox Manage can be pre-imported in the Pradeo Security platform in order to smoothen the enrollment process and the administration of devices.

Once devices are pre-imported, virtual instances of devices are created on the Pradeo Security platform. When the Pradeo Security agent is launched for the first time on a device, it connects to the Pradeo Security platform and matches its virtual instance becoming the effective instance of the device.

The pre-import of devices is one option to **allow a 0-touch enrollment relying** on Pradeo Security applications available on stores.

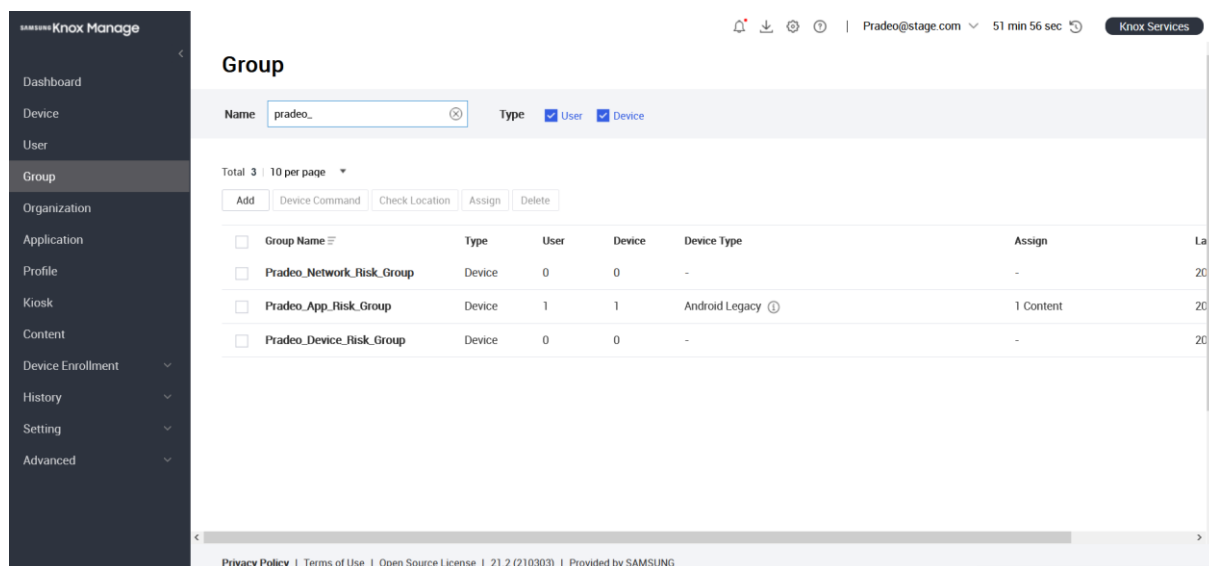
For more details on 0-touch enrollment methods, refer to section 3.2 *0-touch enrollment*.

## 2.3 Enforce the security policy in Samsung Knox Manage

The security context captured by Pradeo Security allows to dynamically enforce security measures on Samsung Knox Manage. Actions from permission denial to access to managed applications and even a wipe could be automatically triggered and ensure company's data protection.

### 2.3.1 Set compliance policies

When the synchronization begins Pradeo will automatically generate 3 Groups on Samsung Knox Manage Console. The Synchronization will also allow to automatically move the users into those 3 Groups if they fall on a non-compliance status



The screenshot shows the Samsung Knox Manage console interface for managing groups. The left sidebar contains navigation options: Dashboard, Device, User, Group (selected), Organization, Application, Profile, Kiosk, Content, Device Enrollment, History, Setting, and Advanced. The main content area is titled 'Group' and shows a search bar with 'pradeo\_' entered. Below the search bar, there are filters for 'Type' with checkboxes for 'User' and 'Device'. A table lists three groups:

Group Name	Type	User	Device	Device Type	Assign	La
<input type="checkbox"/> Pradeo_Network_Risk_Group	Device	0	0	-	-	20
<input type="checkbox"/> Pradeo_App_Risk_Group	Device	1	1	Android Legacy	1 Content	20
<input type="checkbox"/> Pradeo_Device_Risk_Group	Device	0	0	-	-	20

At the bottom of the page, there is a footer with links for Privacy Policy, Terms of Use, Open Source License, version 21.2 (210303), and a note 'Provided by SAMSUNG'.

- **Pradeo\_Network\_Risk\_Group** - dedicated to devices that have at least one severe Network Alert identified with Pradeo Security agent.
- **Pradeo\_App\_Risk\_Group** - dedicated to devices that have at least one severe application Alert identified with Pradeo Security agent.



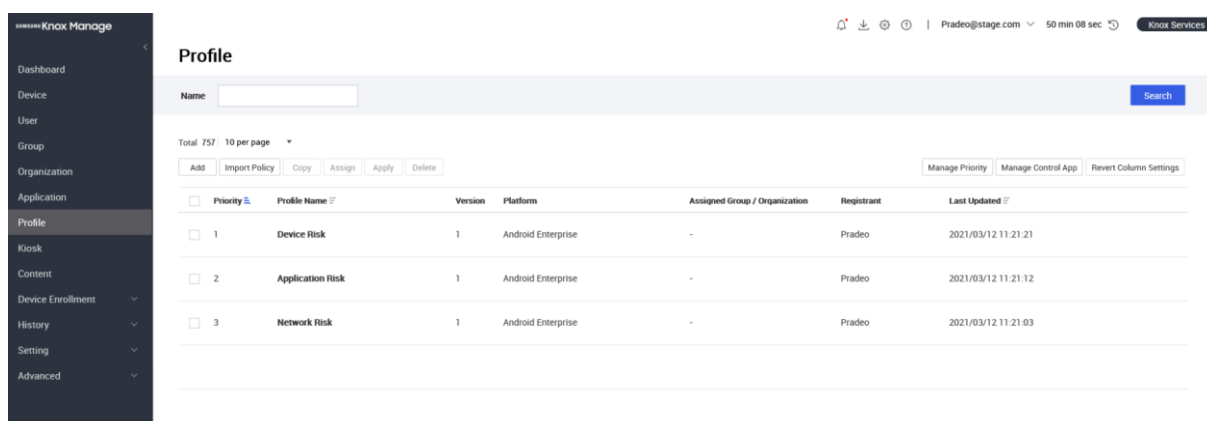
- **Pradeo\_Device\_Risk\_Group** - dedicated to devices that have at least one severe application Alert identified with Pradeo Security agent.

### 2.3.2 Set group Profile Policy

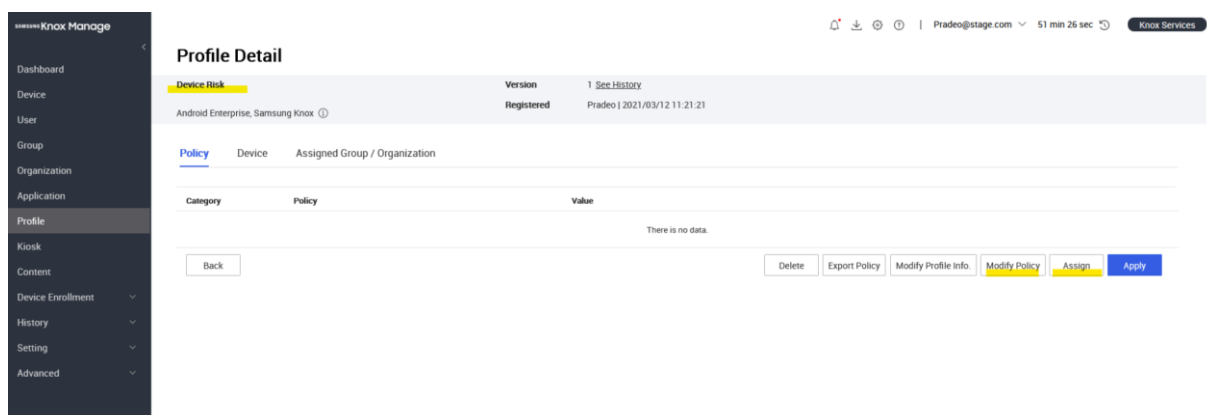
From Samsung Knox Manage console, it is possible to create profiles that can be assigned to specific groups such as:

- **Pradeo\_Network\_Risk\_Group** - dedicated to devices that have at least one severe Network Alert identified with Pradeo Security agent.
- **Pradeo\_App\_Risk\_Group** - dedicated to devices that have at least one severe application Alert identified with Pradeo Security agent.
- **Pradeo\_Device\_Risk\_Group** - dedicated to devices that have at least one severe application Alert identified with Pradeo Security agent.

In order to create a profile, navigate to **Profile** → **Add**, and create a profile for each one of the 3 Groups that Pradeo automatically generate.



To each Profile, the administrator can set a specific Policy that includes a whole set of restrictions that can be imposed to the device who falls in a non-compliant status.



Once the policy set, the Profile needs to be assigned to the corresponding Group pre-generated by Pradeo.

## 3. Pradeo Security agent

### 3.1 Overview

The Pradeo Security agent provides the on-device detection and protection from application, network and device threats. It instantaneously triggers remediation actions as per the security policy associated to the device and reports threats to the Pradeo Security platform.

When launched for the first time, the Pradeo Security agent syncs the overall security context of the device with the Pradeo Security platform (all applications, network and device parameters). This initialization process might take a few minutes. Thereafter, the amount of information to be synchronized is negligible and is processed in real-time.

### 3.2 0-touch enrollment

#### *3.2.1 Store agent or Agent pushed already pre-configured.*

Two different deployment options are availables:

The first option consists in using the Pradeo Security applications available on stores and manually filling all the necessary fields (the process may be simplified by using a QR code or a link that will automatically fill all the necessary fields), the second one allows to push directly the agent VIA the MDM as a preconfigured application.

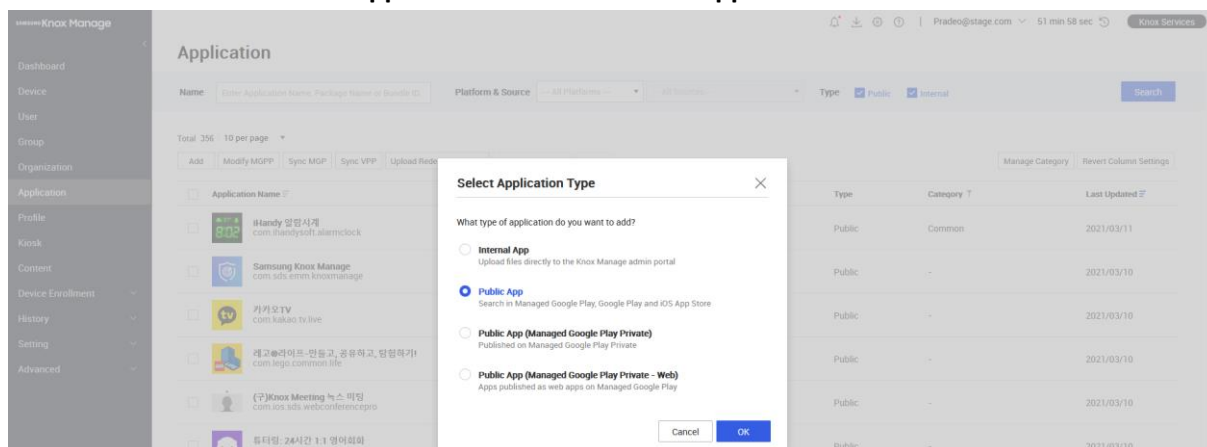
#### *3.2.2 Automatic deployment*

To smoothen the user experience and facilitate the implementation of the solution, the Pradeo Security agent can be deployed from Samsung Knox Manage.

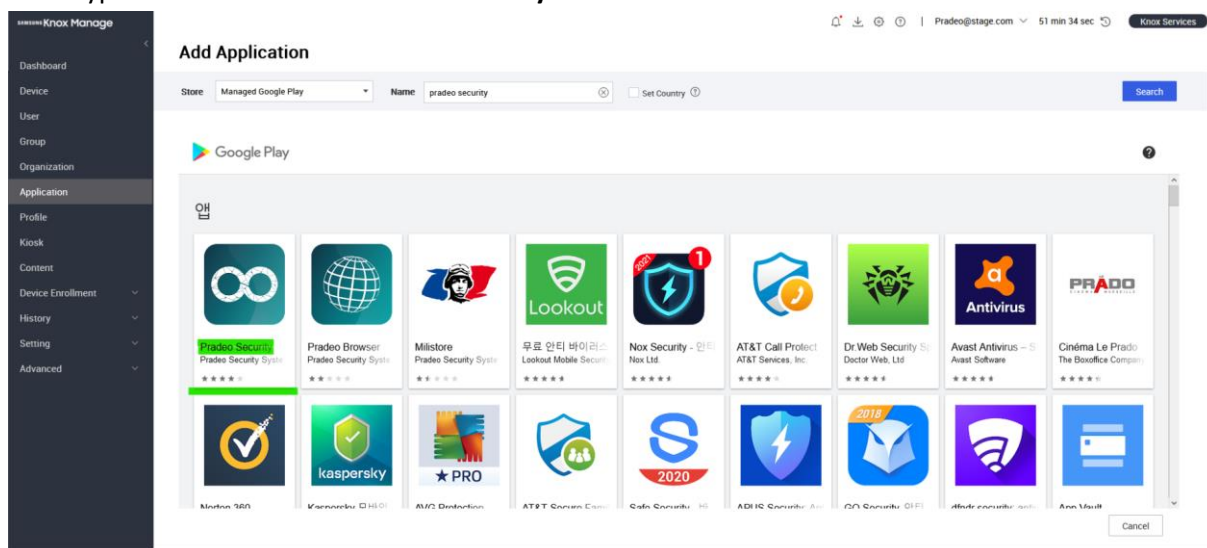
To do so, from the Samsung Knox platform:

### 3.2.3 On Android

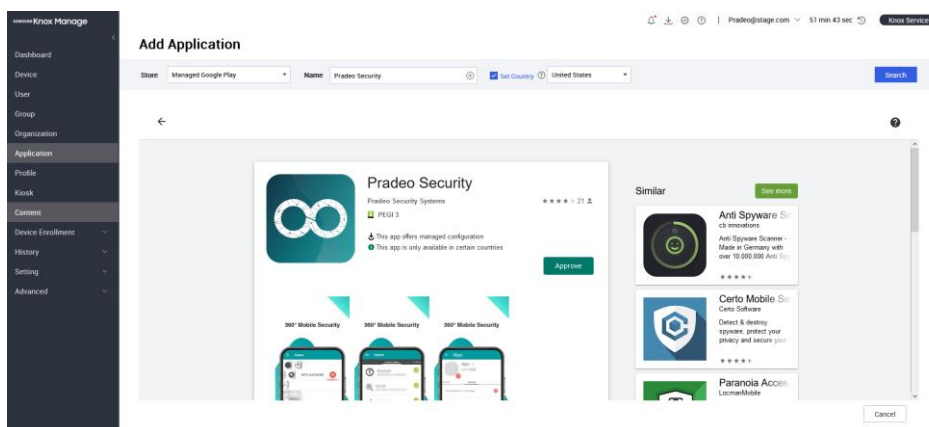
From the main menu select: **Application** → **Add** → **Public App**



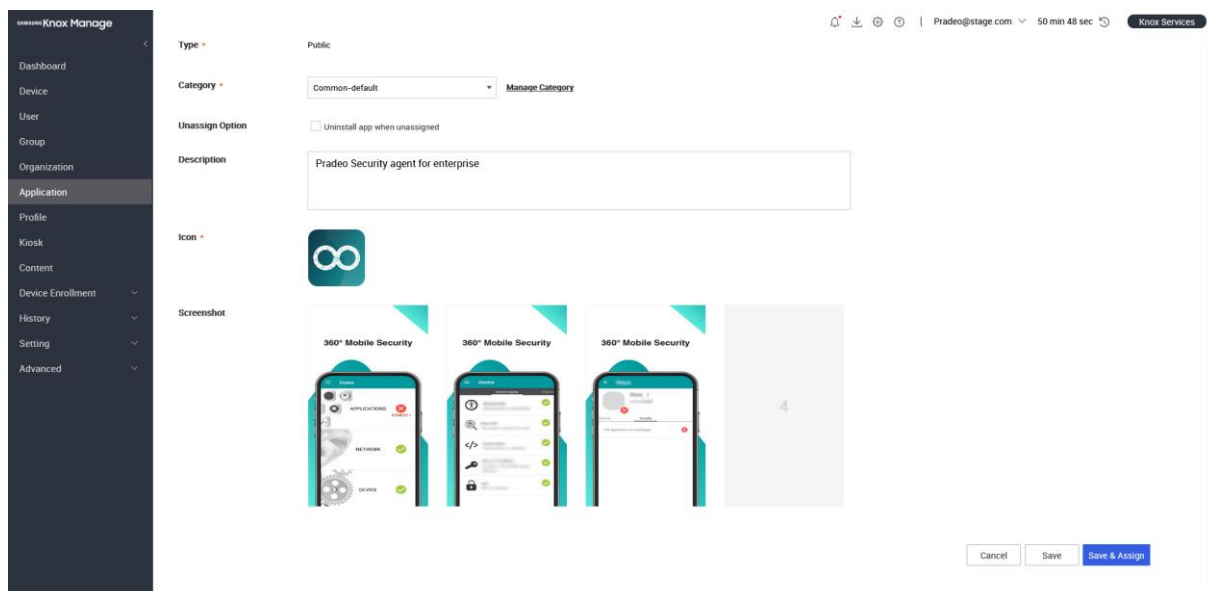
Then type on the search bar: **Pradeo security**



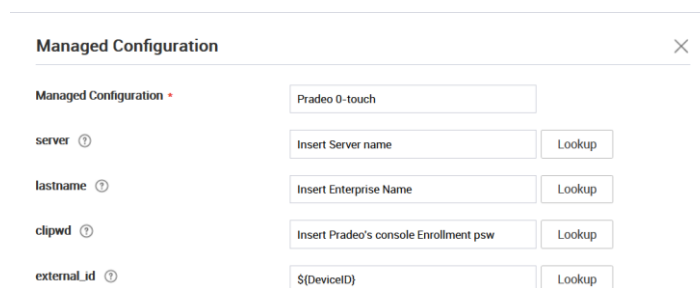
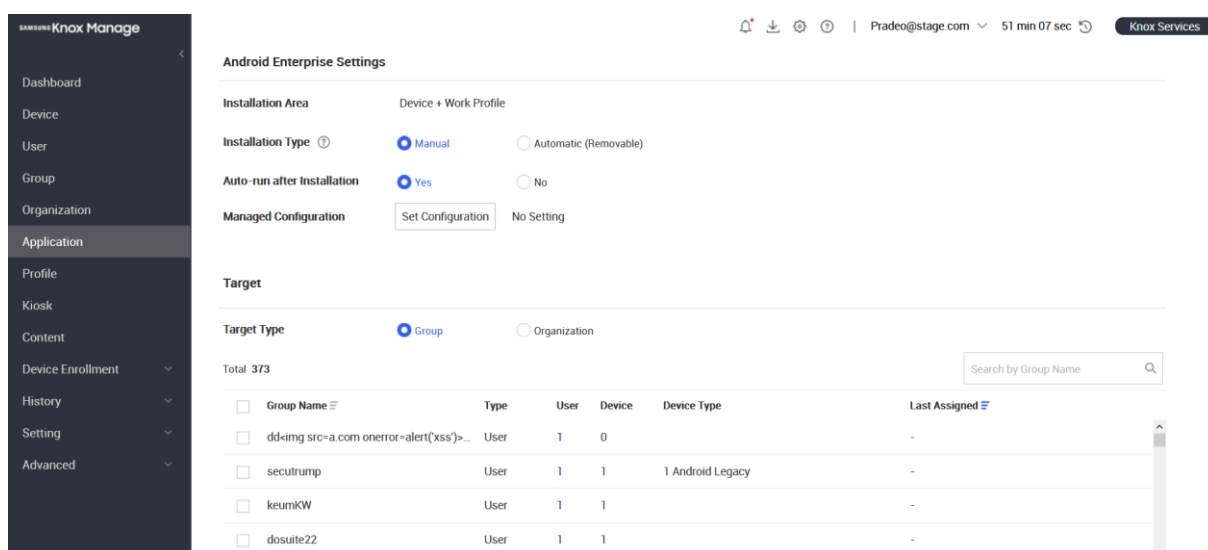
Select the application and then select **Approve** and proceed to approve the permissions requested.



From the next screen, scroll down and click on **Save&Assign**



For Android Enterprise devices, you can pre-fill all the necessary enrolment fields in order to grant à 0 touch experience to the user. In order to do so, from the **Assignment** menu find the **Android Enterprise Settings** and on **Managed Configuration** select **Set Configuration**.



On the Managed Configuration, the administrator needs to fill the enrolment fields that will allow users to automatically receive the configuration on their devices:

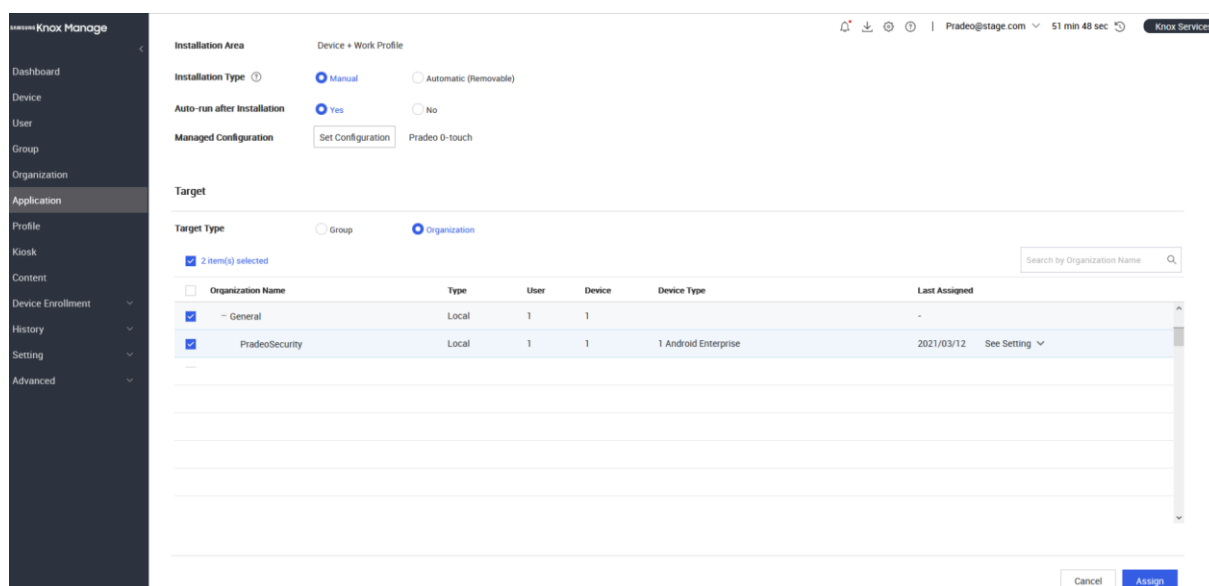
**Server:** this field must be filled with Pradeo's device endpoint (For the Cloud SaaS environment the standard is checkmyappscloud.com)

**LastName:** this field must be filled with the generic Enterprise Name. The synchronisation will make sure to modify the name of each device to make it correspond to his owner corresponding to what is set on the SKM.

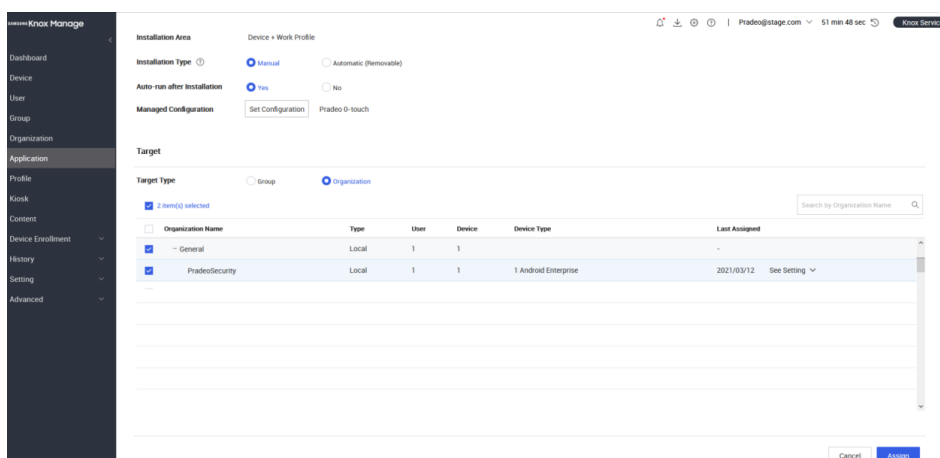
**Clipwd:** this field must be filled with the enrolment password that can be retrieved from Pradeo's console under **User Management → Mobile device Registration → Display Password**.

**External id:** this field must be filled with the variable **#{DeviceID}** which automatically allow to send to the agent the DeviceId of the user granting the synchronisation process.

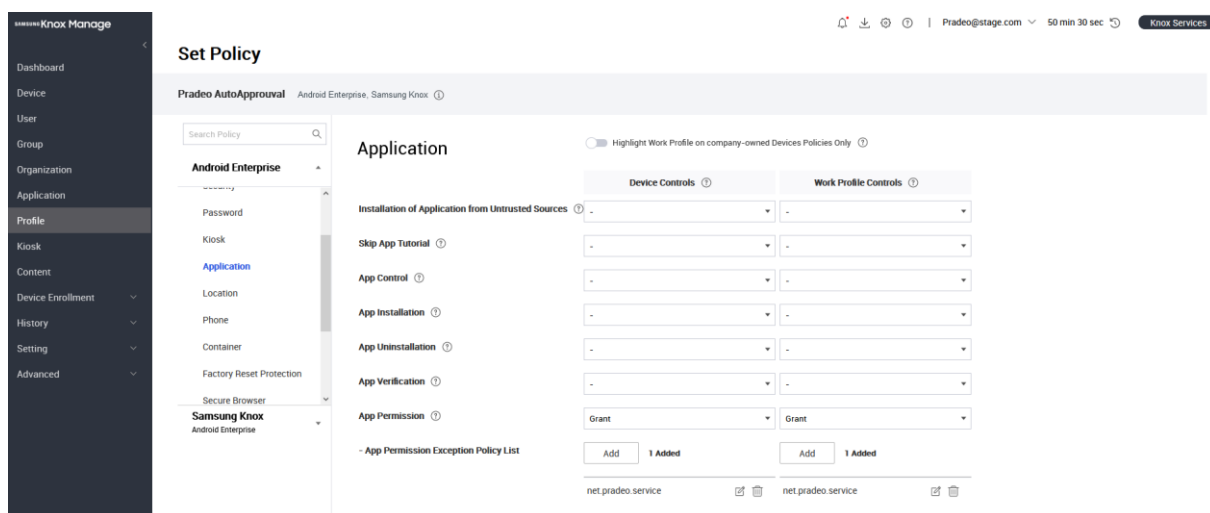
You can then proceed with the assignment to the Groups of users as needed:



Administrators can also create a specific profile to automatically grant to Pradeo Security all the necessary permissions. In order to do so, select **Profile → Add** and after setting a name for the **Profile** select **Android Enterprise** then **Save & Set Policy**



On the **Set Policy** screen, select **Applications** then under **App permission** select **Grant** and add **Pradeo Security** application on from the list:

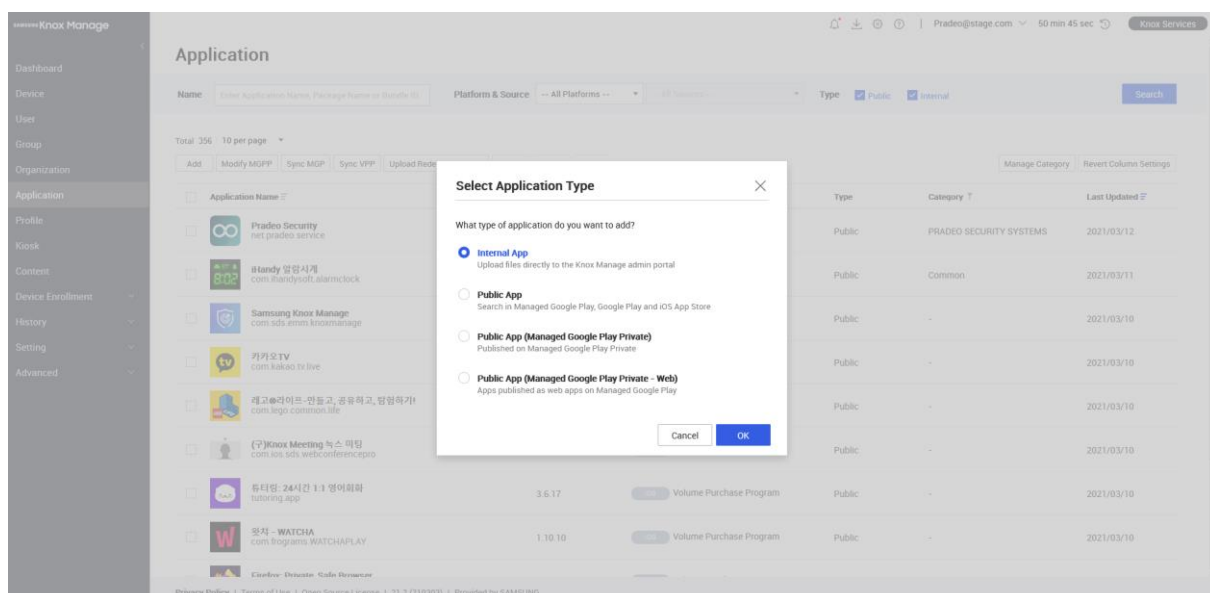


**Important Note:** For Android devices Pradeo Security needs the device administrator permission in order responsively block threats on the applications level. If your security policy does not allow to activate the device administrator permissions, you can create an exception specifically for Pradeo Security application.

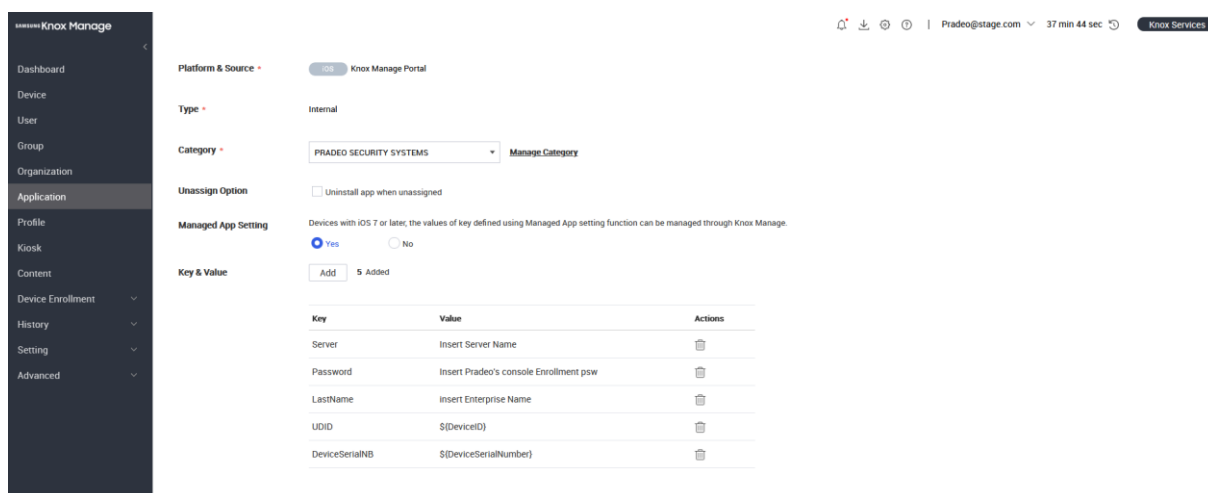
In order to do so, please refer to SKM guidelines: <https://docs.samsungknox.com/admin/knox-manage/kbas/kba-360044739273.htm>

### 3.2.4 On iOS

For iOS devices, Pradeo will provide to their customers a specific ipa. In order to deploy it navigate to the main menu then select: **Application** → **Add** → **internal App**



Select then iOS and add the Pradeo Security ipa. Once added, it will be possible to proceed to the 0-touch configuration. In order to do so, find the **Managed App** setting field and select **Yes** the Add the **Keys and Values** as below :



**Server:** this field must be filled with Pradeo’s device endpoint (For the Cloud SaaS environment the standard is checkmyappscloud.com)

**Password:** this field must be filled with the enrolment password that can be retrieved form Pradeo’s console under **User Management → Mobile device Registration → Display Password.**

**LastName:** this field must be filled with the generic Enterprise Name.The synchronisation will make sure to modify the name of each device to make it correspond to his owner corresponding to what is set on the SKM.

**UDID:** this field must be filled with the variable **`\${DeviceID}`** which automatically allow to send to the agent the DeviceId of the user granting the synchronisation process.

**DeviceSerialNB :** this field must be filled with the variable **`\${DeviceSerialNumber}`** which automatically allow to send to the agent the Serial Number of the user granting the synchronisation process.

Once everything is set, proceed to the assignment.