

FAMOC[®]

System Management Guide



www.famoc.com

PUBLISHED BY

Famoc Software Ltd

Grand Union House

Drurys Avenue

Midleton, co. Cork, Ireland

Copyright © 2008-2022 by Famoc Software Ltd

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Famoc™ and FAMOC™ are either registered trademarks or trademarks of Famoc Software Ltd.

This publication may contain the trademarks and service marks of third parties and such trademarks and service marks are the property of their respective owners.

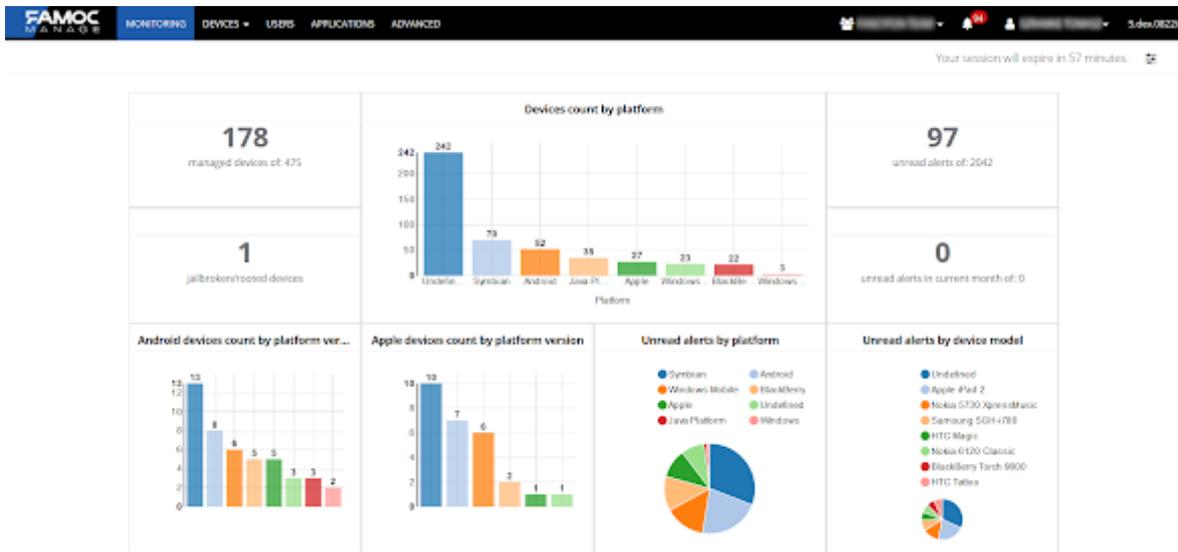
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS AND SERVICES. THE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT AND SERVICES ARE SET FORTH IN THE FAMOC TERMS AND CONDITIONS AND ARE INCORPORATED HEREIN BY THIS REFERENCE.

1. MONITORING	6
Report types	6
Functions of the Chart Action Menu	7
Managing reports	9
Changing layout	10
Saving changes	10
2. DEVICES	10
Customizing devices list	10
Filtering devices list	11
Adding a new device to FAMOC	12
Device details	19
Management actions	21
Adding many devices to FAMOC	23
Apple DEP	23
Android zero-touch	26
KME	26
Remote Access Support	27
3. USERS	29
Customizing Users list	30
Adding a user	30
4. APPLICATIONS	32
Customizing applications list	34
Application details	35
Managed Configurations	38
Adding a new application to FAMOC	39

Application reputation	41
Managed Google Play	42
5. CONFIGURATIONS	43
6. POLICIES	47
7. LOCATIONS	48
The map interaction	49
Customizing locations list	50
Filtering locations list	51
Export locations data to a file	52
Location tab on a device details view	52
Filters in location tab of device details	53
8. LOGS	54
Customizing logs list	54
Filtering logs list	55
Export logs data to a file	56
9. NEWS AND NOTIFICATIONS	57
10. USER MENU	58
General	58
Users & authentication	60
Apple panel	63
Registering a new APNs certificate	64
Android panel	65
Notifications	69
Groups	70
Translations	72

1. MONITORING

In this section the user can view the status of devices and applications managed by FAMOC and monitor system alerts.



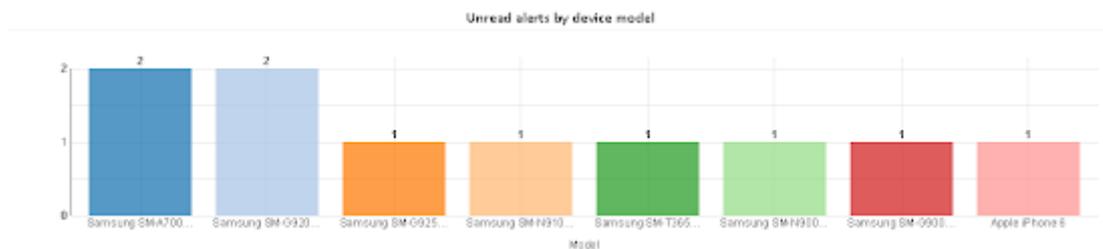
There are multiple reports that can be added to the monitoring interface. Reports can be shown as a chart, table or number.

Report types

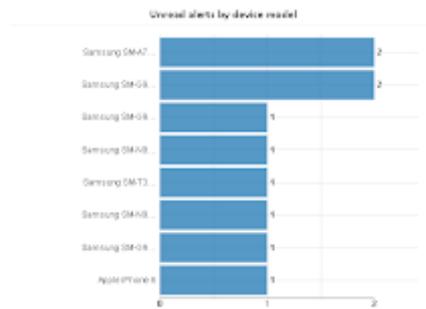
Number – displays desired report as a number (sometimes with additional information like total amount)



Bar chart – chart that uses vertical bars to show comparisons between categories.



Bar horizontal chart - chart that uses horizontal bars to show comparisons between categories.



Pie chart - a circular chart divided into sectors, illustrating numerical proportion.

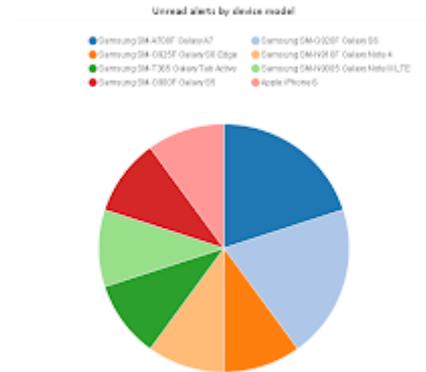


Table - displays data in rows and columns.

Device Model	Count	Total
Samsung SM-A700F Galaxy A7	2	2
Samsung SM-G920F Galaxy S6	2	2
Samsung SM-G925F Galaxy S6 Edge	1	1
Samsung SM-N910F Galaxy Note 4	1	1
Samsung SM-T365 Galaxy Tab Active	1	1
Samsung SM-N9005 Galaxy Note III LTE	1	1
Samsung SM-G900F Galaxy S5	1	1
Apple iPhone 6	1	1
Total	10	10

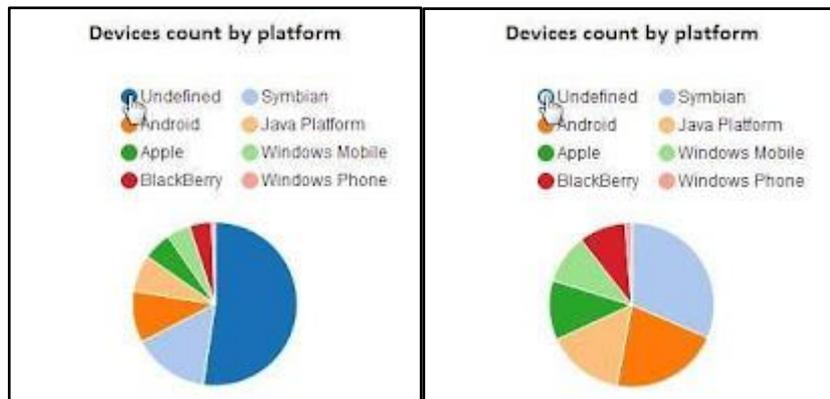
At the top of each report in the Monitoring tab there's an action menu that allows users to perform the following actions: export reports to pdf, send an email with pdf attached, check for details or refresh data. Menu appears after user points the mouse on top of the report.

Functions of the Chart Action Menu

-  show/hide legend (available only for pie chart) – click to show/hide legend
-  export to pdf – save the report as a pdf file to the computer
-  send report – send an email with a pdf file attached
-  show details – display information about the report in the Reports tab
-  refresh – update status of the report

NOTE: For "number" type of report, only "show details" and "refresh" buttons are available.

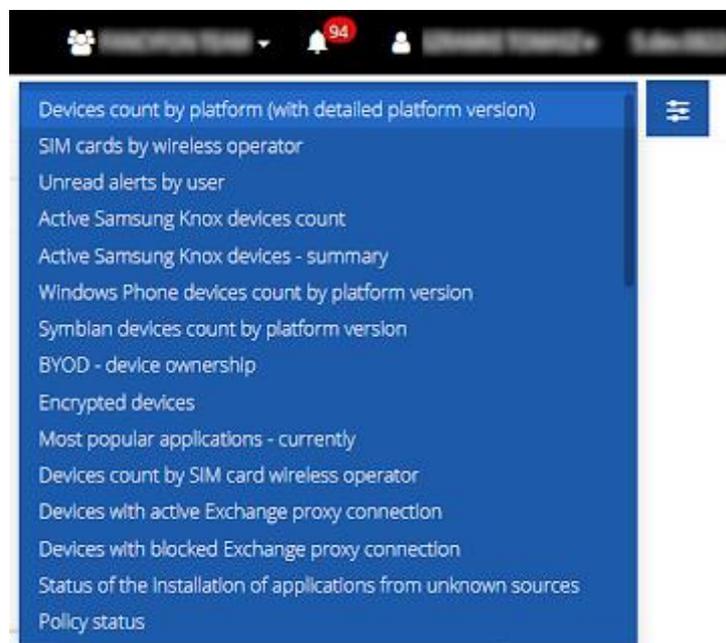
The user can customize information shown on the pie chart by checking/unchecking positions in the chart legend.



Using the Settings icon in the upper right corner of the screen the user can define which reports are displayed in the Monitoring section, resize and change the layout of reports.



Clicking the Settings icon causes the display of additional button: add report +. Click or tap to expand the list of available reports.



Managing reports



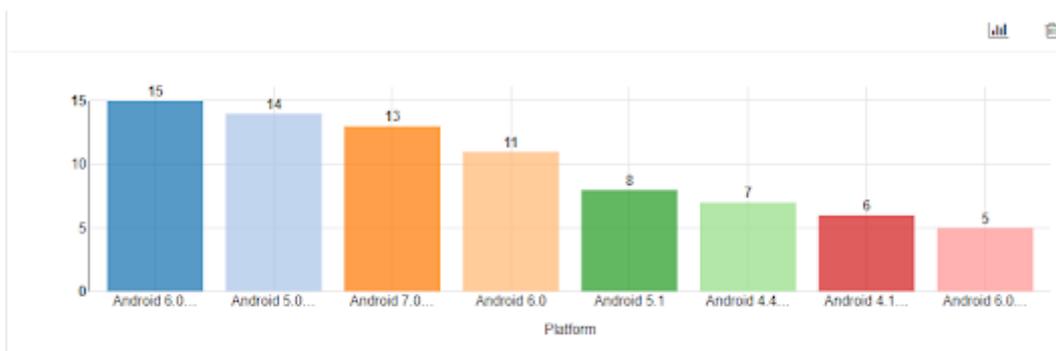
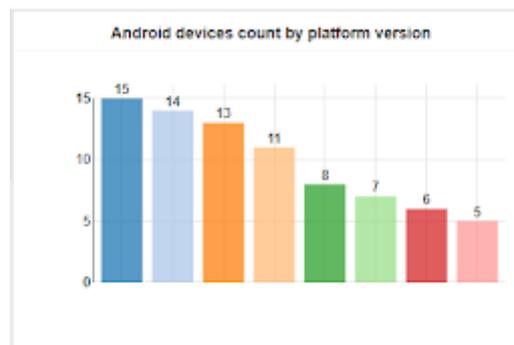
Change report type – This widget allows the user to change a report type. Click on it and select the desired report type to be displayed. Available report types: bar chart, bar horizontal chart, pie chart, table.



Remove report – By clicking this widget the user will remove report from monitoring

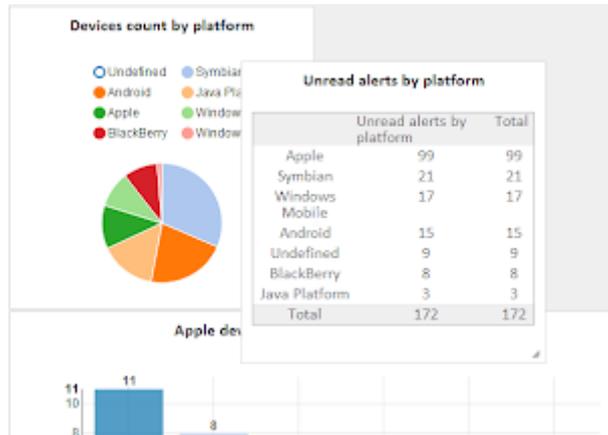
Resize – The user can set the size of the report by grabbing one of the 4 corners and moving it to resize as desired. Such change has some restrictions: must meet the requirements of ratio size. Requirements are different for each type of the report. While resizing the green color informs if the current size meets the requirements of the ratio.

The larger the chart, the more details and information it displays. In case of the small report the user must move the cursor to the selected bar to see the detailed information.



Changing layout

To change the position of the report, the user must drag it and move to the desired position.



Saving changes

All changes done in the “Settings” mode will be saved after clicking/tapping on the “Settings” button. Exiting Monitoring settings straight to the other tab will not save changes.

2. DEVICES

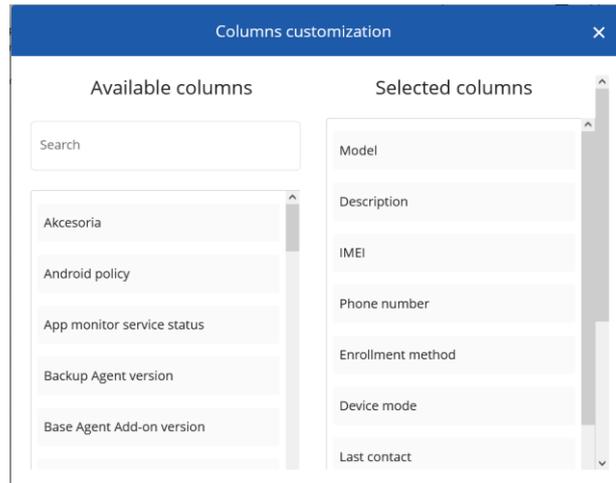
In the Devices tab the user can remotely perform various operations: add new devices, install agents or applications, configure some functionalities, apply policies etc.

The screenshot shows the FAMOC MANAGE interface with the 'DEVICES' tab selected. The interface includes a navigation bar with options like MONITORING, DEVICES, USERS, APPLICATIONS, CONFIGURATIONS, POLICIES, and ADVANCED. A search bar and session expiration notice are also visible. The main content is a table with the following columns: Model, Description, IMEI, Phone number, Enrollment method, Device mode, Last contact, Created on, Last modification, User, Login, Platform icon, Platform, Policy name, and Policy status. The table lists various devices such as Motorola Moto G100, Huawei MediaPad T5, Apple iPad 9, Samsung SM-G960F Galaxy S9, Nokia 7.1, Samsung SM-A105F Galaxy A10, Samsung SM-A225F Galaxy A22, Apple iPad 9, Samsung SM-A415 Galaxy A41, Apple iPhone 11, and Apple iPad 6.

Customizing devices list

Clicking a column name allows you to sort by any property in the list view. There is also a possibility to customize which columns are displayed, by using **Customize table view** button . All available columns are grouped on the left side of the Action box, while columns currently visible in the Devices list are displayed on the right side. The administrator can drag and drop any column to change the

order or the list of displayed columns. To accept changes confirm by pressing **Save**.

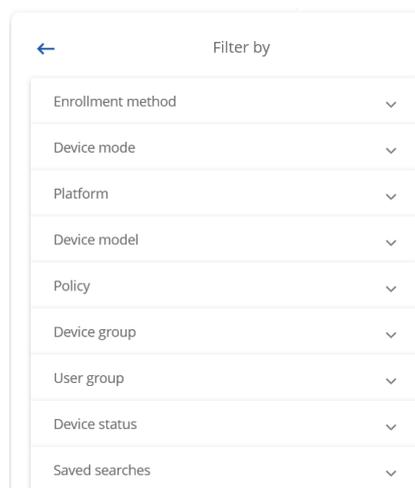


Next to the customization icon, there is a star icon (☆). It allows the user to save the search results in the form of a list. For example you can search for a specific model or user and save the results to quickly come back to them later.

Filtering devices list

Use filters to display only the list of devices meeting certain parameters. Click the icon  and then specify device properties from the menu on the right:

- Enrollment method
- Device mode
- Platform
- Device model
- Policy Device group
- User group
- Device status



After applying the filters, you can save the displayed results by clicking on the star icon. This way you will be able to access them quickly later.

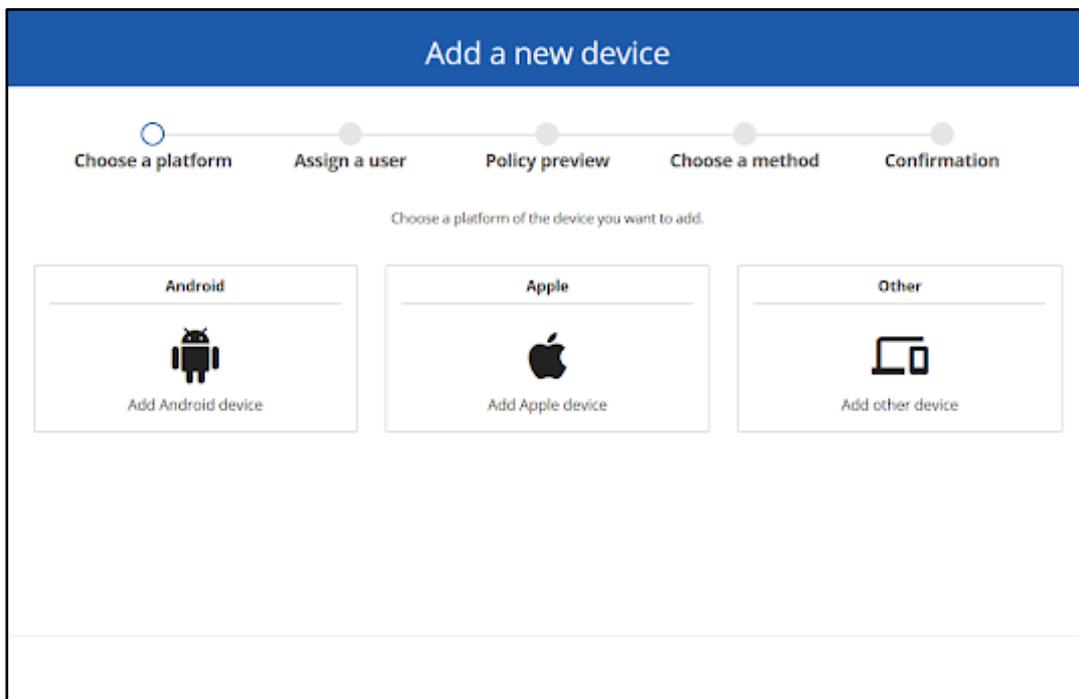
Your session will expire in 83 minutes.

1 - 50 of 116

Model	Description	IMEI	Phone number	Enrollment method	Device mode	Created on	Last modification	User	Login	
<input type="checkbox"/>	Motorola Moto G100	Added in WPC mode (QR code)	354001151306057 48694866457	WPC QR	WPC	2022-07-27 08:06:05	2022-03-30 12:44:30	2022-07-27 08:06:03	Ross, Mike	mike.ross@famoc
<input type="checkbox"/>	Huawei MediaPad T5	Added in COSU mode (QR code)	E4268B76C73A	COSU QR	COSU	2022-07-26 14:42:16	2022-07-26 14:05:00	2022-07-26 14:42:16	Specter, Harvey	h.specter@famoc

Adding a new device to FAMOC

This feature allows you to enroll a single device using various methods: email, phone number or QR code; or set the device up in Device Owner mode using NFC or a QR code. To add a single device to the system, hover over the **+** button in the **DEVICES** tab and choose the **'Enroll a device'** option. A step-by-step modal window will appear and guide you through the enrollment process.



First, select a platform. You can choose between Android, Apple, or other devices (e.g. Windows). Next steps will differ slightly depending on the chosen platform.

Add a new device x

● Choose a platform
○ Assign a user
● Policy preview
● Choose a method
● Confirmation

Enrollment method

Fully managed device (COBO)

Device with work profile (BYOD, WPC)

Dedicated device (COSU)

Shared device BETA

User authorization required ⓘ

No authentication

Any user

Selected user only

User name

Louis Litt (l.litt) -

Email

l.litt

Phone number

48600123123

Description

Enter description

Device groups

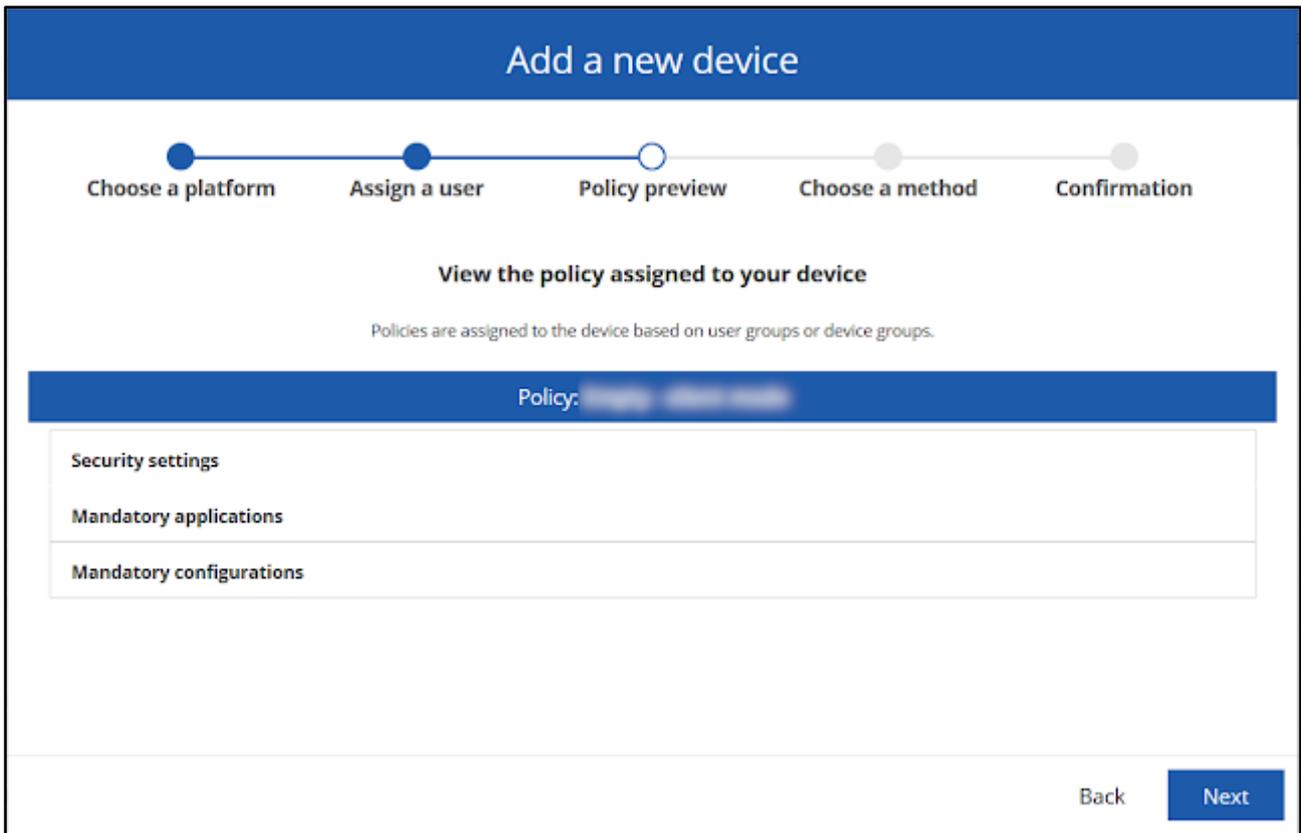
Select group

ⓘ User missing? [Add a new one here.](#)

Back
Next

In the second step select the device user and, if needed, edit the user's email and phone number. You can also force a user to log in by selecting **User authorization required**. During enrollment, it will be necessary to provide login data for the FAMOC manage console or SAML credentials (if authorization has been configured). For Android devices, you can choose the method of adding here - full management (COBO), device with a work profile (BYOD / WPC), dedicated device (COSU) or a shared device (a special mode that allows you to create several user profiles on the device). For Apple devices you can select COBO or BYOD method (Managed Apple ID is required).

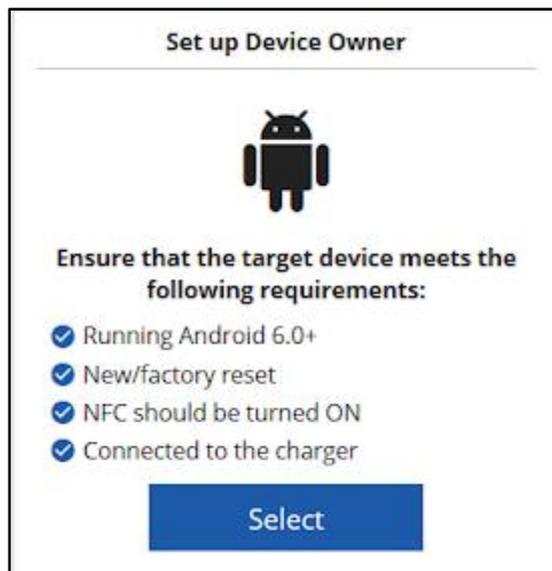
The third step displays policy and apps that will be assigned to the device. This is based on the device group or user group.



In the penultimate step select the desired enrollment method. The choices depend on the selected platform.

Platform	Enrollment mode	Available enrollment methods
Android	Fully managed device (COBO)	Device Owner (recommended) Device Admin (legacy option)
	Device with work profile (BYOD, WPC)	Work profile on company-owned device Private device with work profile
	Dedicated device (COSU)	Device Owner
	Shared device	User profile
Apple	Fully managed device (COBO)	Enrollment link QR Code
	User enrolled device BYOD	Enrollment link QR Code
Other	Fully managed device	Enrollment link QR Code

For fully managed Android devices it is recommended to use Device Owner mode. It requires new or factory reset device but gives you access to more features.



Set up Device Owner

This choice allows you to enroll an Android device in the Device Owner mode. The first step of this process is optional and allows the administrator to configure a WLAN connection on the device during enrollment (Keep in mind that the device will require Internet access to communicate with FAMOC to properly configure and finish the enrollment process.) Then, select one of the two methods for enrollment in the Device Owner mode: NFC or QR enrollment.

The NFC method requires an NFC-enabled, admin-assigned device already enrolled (not necessarily in DO mode) to FAMOC. You need to select such a device for use as a master device for scanning. Choose the device and click 'Start'. The master device will receive a request to start the NFC scan. Use the target device to scan the new device by positioning the devices back to back. When the new device is detected by the master device, tap the screen on the master device to start the enrollment process. The new device will be assigned to the selected user. Note: This method requires both devices to be NFC-enabled, with the functionality turned on master device. The new device must be factory reset or new with Android 6.x or higher.

NOTE: For devices with Android 10 or later, NFC registration has been replaced with QR code registration.

The QR method does not require an additional device enrolled. The QR Reader can be easily accessed by tapping the welcome screen on a factory reset/new device 6 times. Upon scanning the code, the enrollment process will begin.

NOTE: This method is available only for devices with Android 7.x or higher.

Add a new device

Progress bar: Choose a platform (selected), Assign a user, Policy preview, Choose a method, Confirmation

Step 1: Set up a WiFi (optional)

This enrollment method requires internet connection. If there's no SIM card in the device, fill in WiFi settings below.

Network name:

Password:

Step 2: Choose NFC or QR code

NFC

Go to master device
Method unavailable. To enroll a device using NFC you need a master device enrolled using a different method (sms, email, QR code). Make sure your Android device has active NFC and set yourself as the device user.

QR Code

Go to the target device
The target device needs to stay on the welcome screen. Tap the screen 6 times to download QR code scanner and enroll the device.

[Back](#)

Other options of enrollment include sending enrollment link via e-mail or SMS or scanning QR code. This is default option for iOS and Windows devices. For android devices select **Show legacy options** to access those ways of enrollment.

[Show legacy options](#)

Send enrollment link

Email

Phone number

[Send](#)

Scan QR Code



[Copy link](#) | [Refresh](#)

Send Enrollment Link

A link to the enrollment page will be sent to the user's email address or phone via SMS. Note: To use the SMS option you need to have the SMS gateway in place.

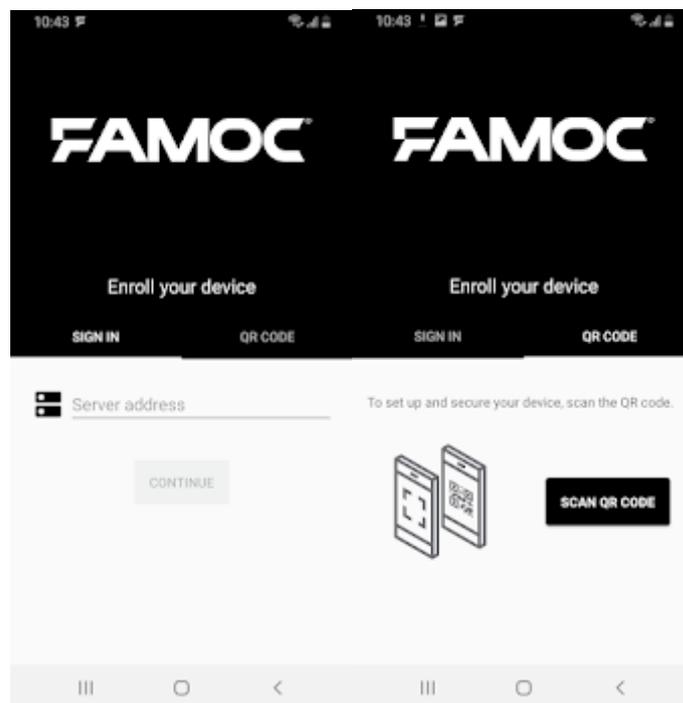
Scan QR Code

You can scan the QR code using a device camera or QR code reader apps. Note: set the QR reader apps to open links automatically. Otherwise, the QR code will be counted as used before opening the link in the web browser. After scanning, the device displays the enrollment page.

After downloading the FAMOC app a new device record is automatically created in the system and the device is assigned to the selected user.

Adding device directly from Base Agent

Another possibility to add a device is installing a Base Agent from Google Play or with a .apk file. Once you run the Base Agent you will see two options - signing in to the server or scanning QR code. The first option requires a valid server address. Second option allows you to scan QR code received via e-mail or directly from the FAMOC system as described above.

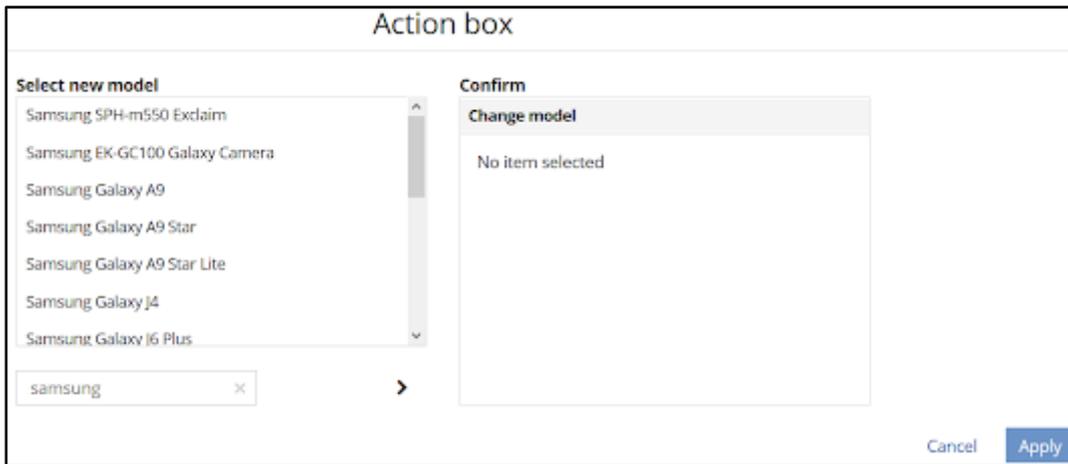


Creating a device entry for future enrollment

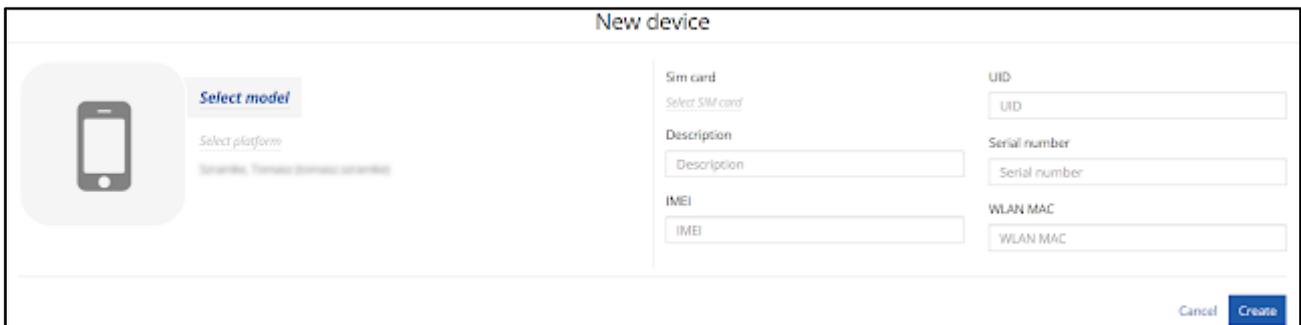
Another option is to create a new device entry in the system and enroll it after providing basic data about it. To do so, hover over the **+** button in the **DEVICES** tab and choose the 'Create entry (enroll later)' option.

Follow these steps to create entry:

1. Select the device model and platform (optionally) from the Action box list and press **Apply**. It is possible to use the search box to specify these parameters:

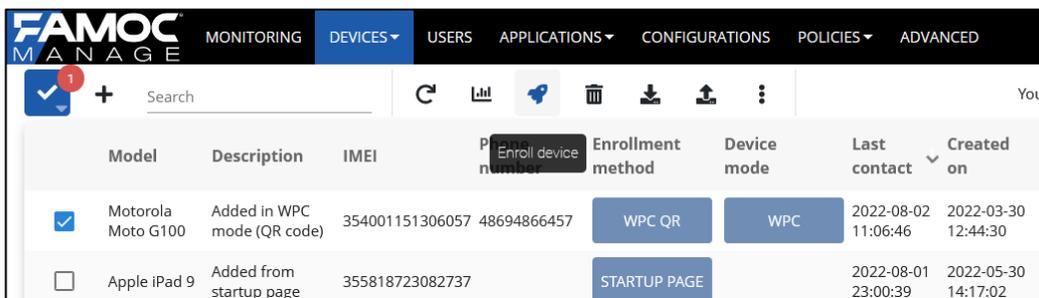


2. Fill in other fields to describe the device (optionally).
3. Assign a predefined SIM card.
4. Assign the device user.
5. Finish by pressing **Create**.



When all device details are ready, you can start the enrollment process, either from the list of **DEVICES** tab, or from the chosen device details view:

1. Select the device from the list or click on the device.
2. Use **Enroll device** button .



3. When Action box appears, one of the **Notification delivery methods** needs to be selected:
 - Automatic selection

- Email only
 - SMS only
 - No notification
4. You can also select if you want to clear device information from previous enrollment.
 5. Choose enrollment method:
 - Fully Managed device
 - Device with work profile (BYOD)
 - Dedicated device (COSU)
 - Corporate-owned device with work profile (WPC)
 6. In the last section choose enrollment mode - Device Owner or Device Admin and select the device system version.
 7. Select whether the enrollment should start **Now** or be **Scheduled** for later.
 8. The status of the enrollment operation can be checked in the device details in the **Log** tab.

Action	Component	Target	Created on	Created by	Last status	Status	Message ID	Phone user	Phone number	IMEI	Phone description	Device serial number	Device UID	Device identifier
Run	Agent Location Monitor	Device	about 23 hours ago	Administrator, System	about 23 hours ago	1	Sent	37130 h.specter@famoc.com		354838352569615	Added in Device Owner mode ...	R5BR7044SAA		354838352569615
Running	Agent Remote Access	Device	about 23 hours ago		about 23 hours ago	1		37129 h.specter@famoc.com		354838352569615	Added in Device Owner mode ...	R5BR7044SAA		354838352569615
Run	Agent Remote Access	Device	about 23 hours ago	Administrator, System	about 23 hours ago	1	Sent	37128 h.specter@famoc.com		354838352569615	Added in Device Owner mode ...	R5BR7044SAA		354838352569615
Running	Agent Remote Access	Device	about 24 hours ago		about 24 hours ago	1		37127 h.specter@famoc.com		354838352569615	Added in Device Owner mode ...	R5BR7044SAA		354838352569615

9. After the device receives the enrollment message, the user starts the installation of FAMOC agents.

When the enrollment process is completed, you can view the device details and perform management actions.

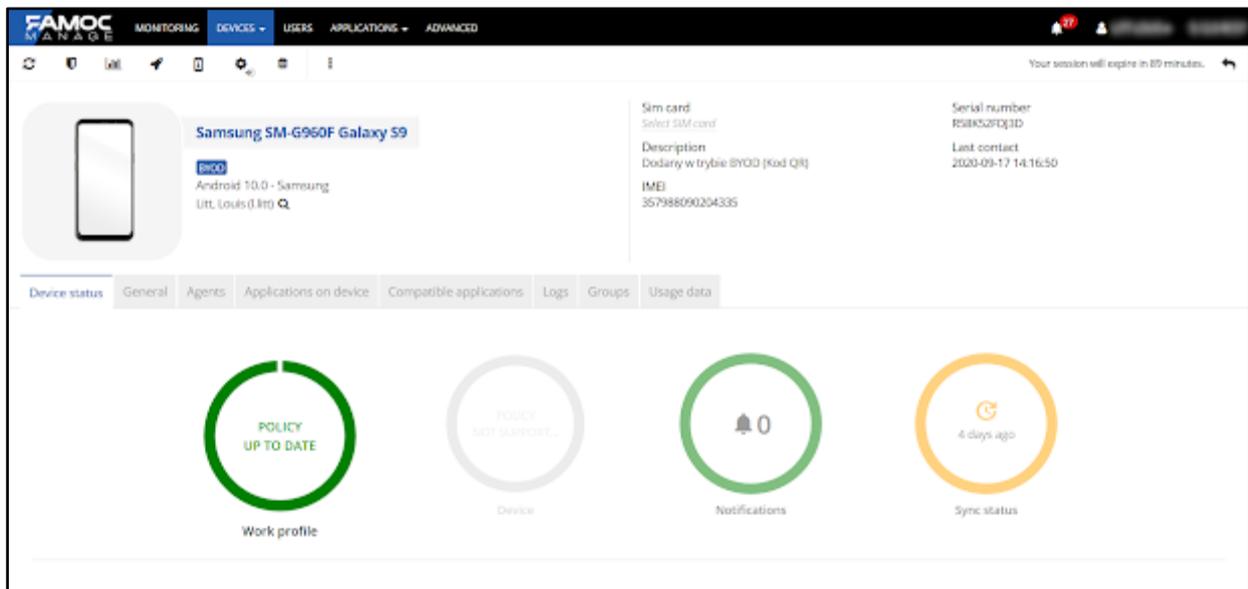
Device details

In the device details view you can see information about the device including user name, sim card number, description, IMEI, WLAN MAC number, serial number and date of last contact. In the tabs below you can also see the status of the device, general parameters, applications, logs and assigned groups.

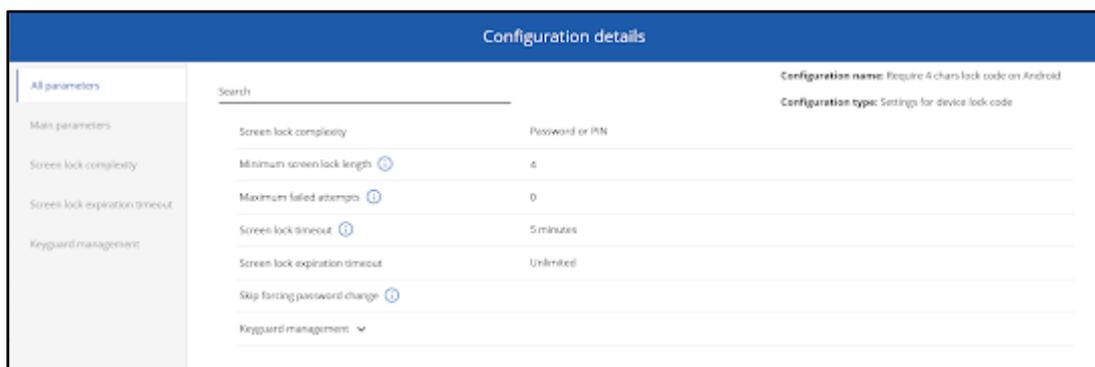
In the device status tab you can see graphic representation of Policy, Work profile, Notifications and Sync status. Green color of the circle means everything is ok, Yellow - moderate warning, Red - important warning, Grey - n/a. Clicking each circle displays additional details.

- **Device:** detailed information about the status of the policy applied on the device including

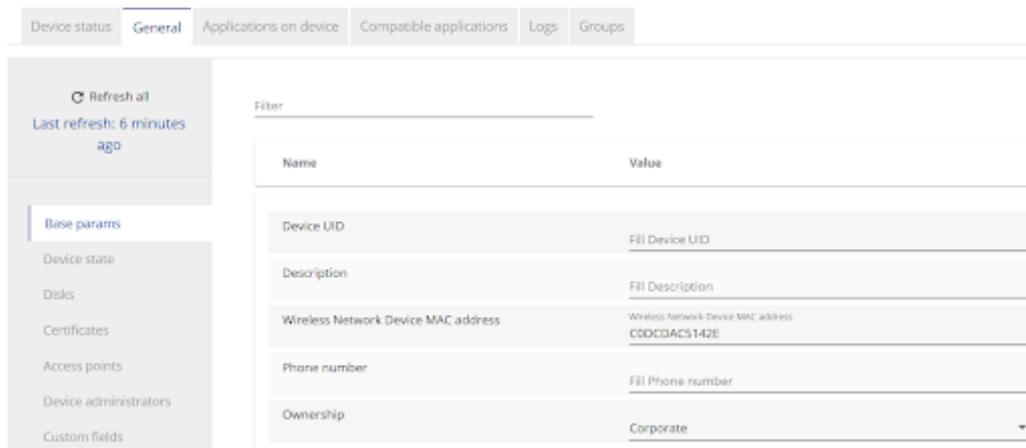
- security restrictions, mandatory apps and configurations
- **Work profile:** detailed information about the status of the container on device, applied security restrictions, apps and configurations
- **Notifications:** alerts related to the device
- **Sync status:** information about device synchronization schedule including data and location monitoring as well as contacts synchronization
- **Exchange proxy status:** detailed information about the connection and applied policy (only devices with Exchange proxy enabled)



In the section below, you can also view the policy settings such as Basic Parameters, Restrictions, Mandatory Applications and Configurations. In the case of some restrictions and configurations, we can view its details using the  icon.



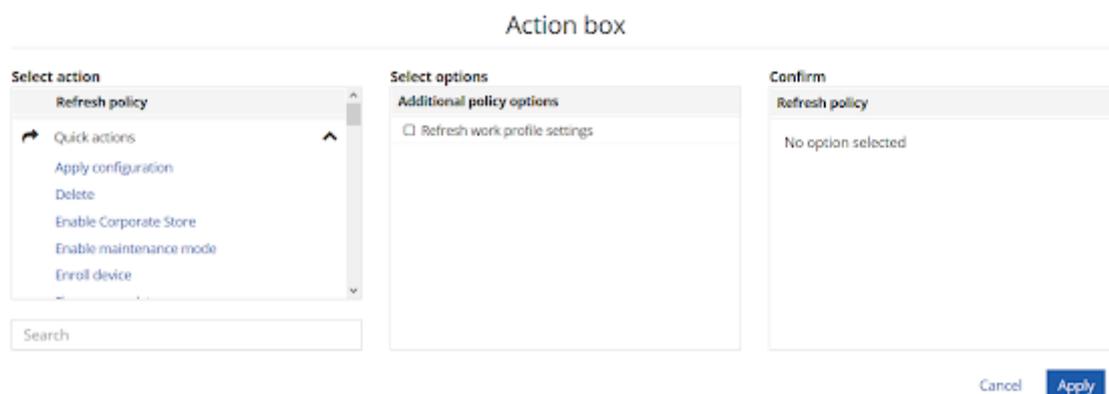
In the General tab you can find many useful details about the device including Base parameters like IMEI, Serial number, OS version as well as information about device state, disks, certificates, access points, device administrators and custom fields.



Applications on device tab lists all the apps currently installed on the device. **Compatible applications** includes all the apps added to FAMOC which are compatible with the device model and OS. In the **Logs** tab you can see all the operations performed on the device with the possibility to customize displayed columns and export table to txt or csv format. In the Groups tab you can see the groups to which the device has been assigned. If the device has a Usage monitor installed you will also see a Usage data tab - it displays details such as list of calls and messages, data used, device state and used applications.

Management actions

Basic actions are available on the menu above the device description. All management operations can be found in the Action Box which can be accessed from the menu by pressing  .



Devices Menu	Description
	Select
	Add new device
	Customize table view
	Refresh general policy
	Refresh restrictions
	Get device monitor data

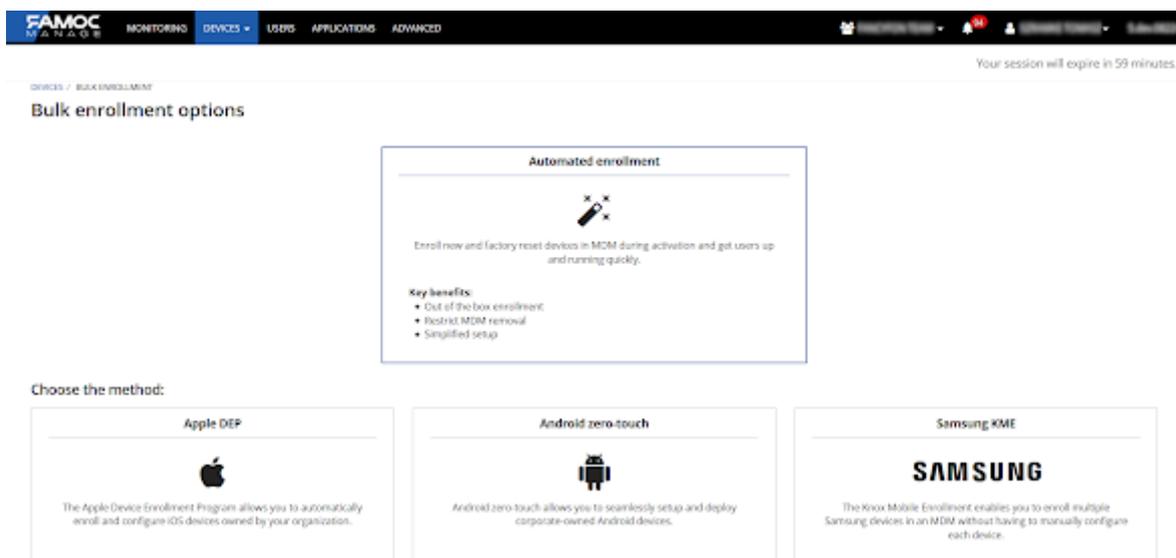
	Enroll device
	Install application (Select All allows you to install all compatible applications)
	Apply configuration
	Delete
	Action Box
 Quick actions	<ul style="list-style-type: none"> • Apply configuration <ul style="list-style-type: none"> • Delete • Enroll device • Firmware update • Fixed asset disposal report • Fixed asset transfer report <ul style="list-style-type: none"> • Get current location • Get device monitor data (there is a possibility to download full or selected data from the device) <ul style="list-style-type: none"> • Install application • Install certificate • Remove configuration <ul style="list-style-type: none"> • Reset lock code • Restart device • Run Remote Support <ul style="list-style-type: none"> • Send message • Run application <ul style="list-style-type: none"> • Send message • Shutdown device • Synchronize contacts • Uninstall application
 Emergency operations	<ul style="list-style-type: none"> • Disable Android Work Profile <ul style="list-style-type: none"> • Disable Lost Mode • Enable Android work profile <ul style="list-style-type: none"> • Enable Lost Mode • Enterprise wipe • Locate lost device <ul style="list-style-type: none"> • Lock device • Mark as wiped • Remove stolen device status <ul style="list-style-type: none"> • Report stolen device <ul style="list-style-type: none"> • Wipe Device • Suspend personal apps
 Assignment	<ul style="list-style-type: none"> • Assign to group • Change user • Detach from group
	<ul style="list-style-type: none"> • Refresh policy

Policy	<ul style="list-style-type: none"> Refresh restrictions
 KNOX	<ul style="list-style-type: none"> Lock KNOX container Reset KNOX lock code Unlock KNOX container Wipe KNOX container
 Device logs	<ul style="list-style-type: none"> Disable logging Enable logging Get device logs (possibility to download logs in .zip format in Logs tab)
 Agents	<ul style="list-style-type: none"> Generate Base Agent access code <ul style="list-style-type: none"> Install Base Agent Install Location Monitor Install Remote Access Install Usage Monitor Uninstall Location Monitor Uninstall Remote Access Uninstall Usage Monitor

Table - Functions available in the DEVICES tab and Action Menu.

Adding many devices to FAMOC

This feature allows you to automatically enroll devices in bulk by utilizing the Device Enrollment Program (for Apple devices), Android zero-touch (for Android devices) or KME (for Samsung Android devices). The process is easy and intuitive. To add many devices hover over the **+** button in the Devices tab and choose the Bulk enrollment option.



Apple DEP

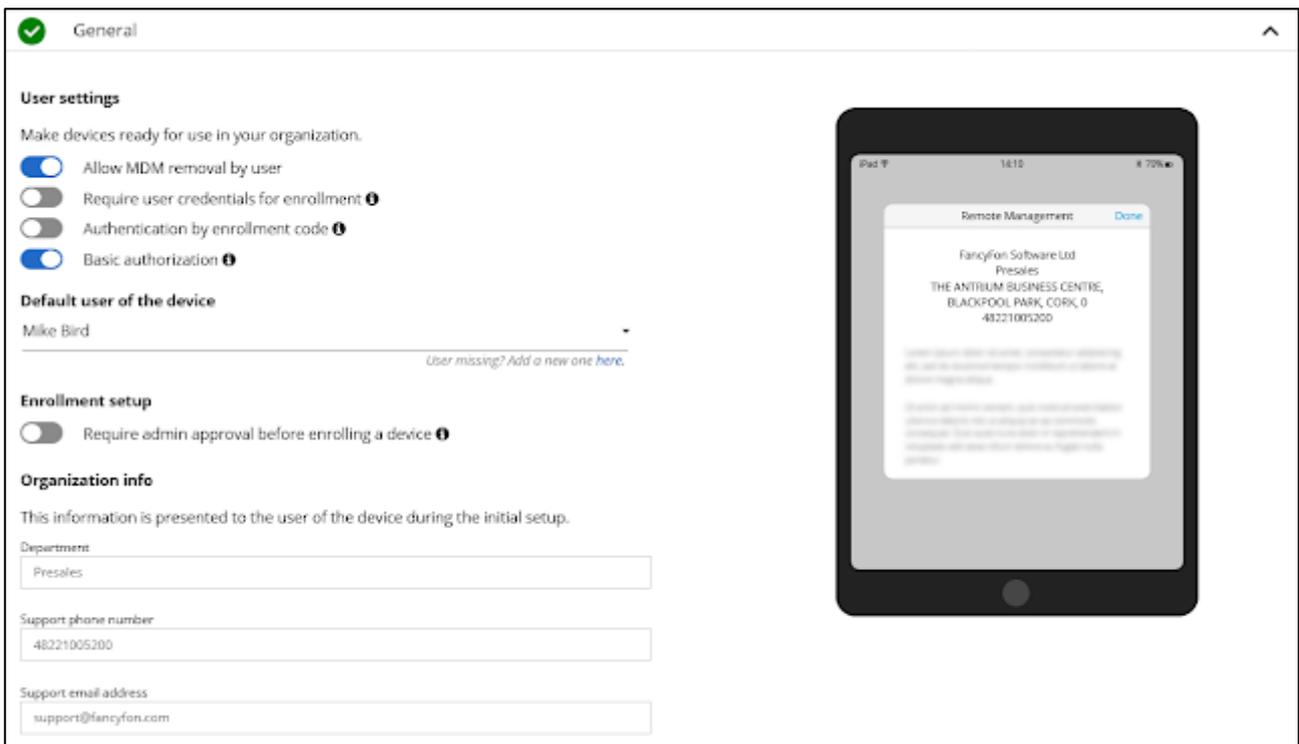
To synchronize a new DEP account, first, select the Apple DEP method. Then, click the Start now button. A familiar window will appear, guiding you through the process. After uploading the DEP token to FAMOC, a summary will display the basic information on the account: name, Apple ID of the

administrator and the number of devices available on the account. After closing the modal window you will be able to edit specific settings for the account.

In the General section:

- If the 'Allow MDM removal by user' option is enabled, the users will not be able to manually remove the MDM profile from the device.
 - If the 'Require user credentials for enrollment' option is enabled, during enrollment the user will have to provide login details for FAMOC manage or SAML authorization (if configured). Devices will be automatically attached to users upon enrollment, otherwise the 'Default users of the device' selection will be used for new devices.
 - To add an additional level of verification, you can use the 'Authentication by enrollment code' option. This means that the user will have to enter upon registration a unique code assigned to a given user. If you check this option you will be able to adjust the code requirements in the organization settings. You can read more about it [here](#).
 - Then generate the codes by clicking **Generate enrollment code for users**. **Show enrollment codes** option allows you to display the generated codes, and to export them as a .txt file.
 - If **Basic Authorization** is selected, the user can only log in with the FAMOC manage console login credentials.
- If the option 'Require admin approval' is enabled, an alert is generated during the enrollment process. Administrator has to approve the device to finish the setup. When the enrollment is not authorized, administrator can select wipe device or enable lost mode actions as a result of the alert.
- The 'Organization info' fields are optional, their contents will be displayed on the device during enrollment.

The Startup settings section allows you to select which panes of the setup assistant should be displayed after the profile installation.

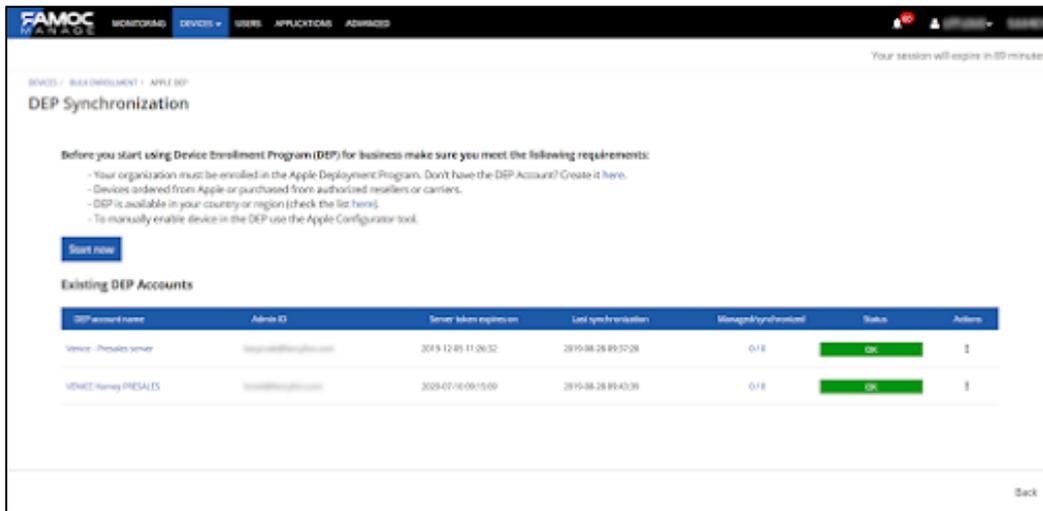


After configuring the DEP account settings according to your needs, press the Synchronize button. The profile information will be sent to Apple and assigned to the devices belonging to the DEP account and the entries for these devices will be created in FAMOC. At this point, the devices are ready for enrollment, and the number of successfully synchronized devices will be displayed along with the server's token expiration date. If you return to the Apple DEP screen, a DEP accounts table will be displayed.

FAMOC allows multiple DEP accounts within an organization. All account synchronizations will be displayed here.

The DEP account table displays: the names of available DEP accounts, Apple ID used to create the accounts, DEP accounts token expiration date, last synchronization dates, the number of devices currently enrolled and managed, the number of devices synchronized with DEP in total and the status of synchronizations. The  button allows you to perform certain operations for any DEP account: edit the account's settings, delete the account, stop the synchronization schedule, restart the synchronization, synchronize the account now and renew the server token. Any changes in the account's settings require a synchronization (scheduled or manual) to take effect on the devices.

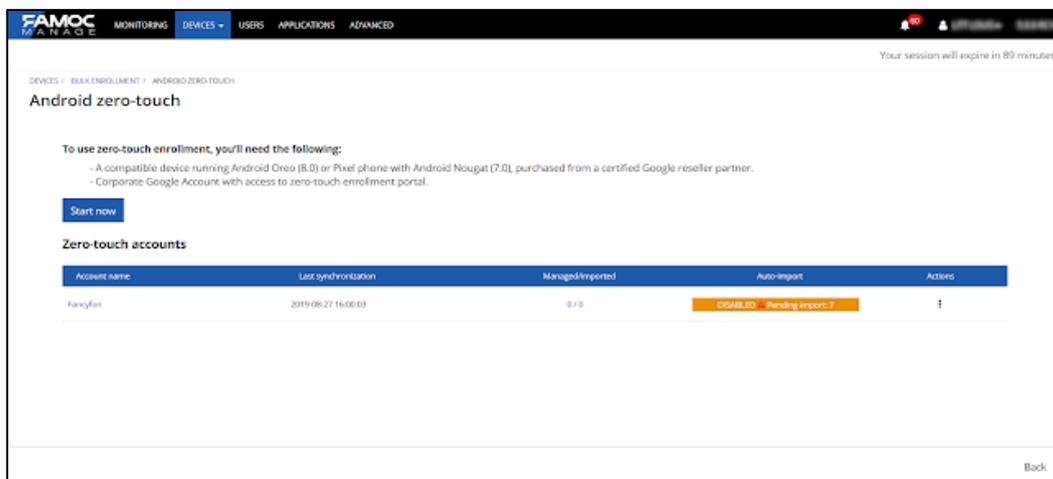
For further details concerning DEP read the FAMOC Apple DEP documentation.



Android zero-touch

To import an Android device to your zero-touch account, first, select the Android zero-touch. Then, click the Start now button. On the first step you will be asked to authorize your account with proper email. Next step is deciding which information will be displayed on the device during enrollment (e.g. company name). After selecting the devices to import, press Synchronize to import your devices.

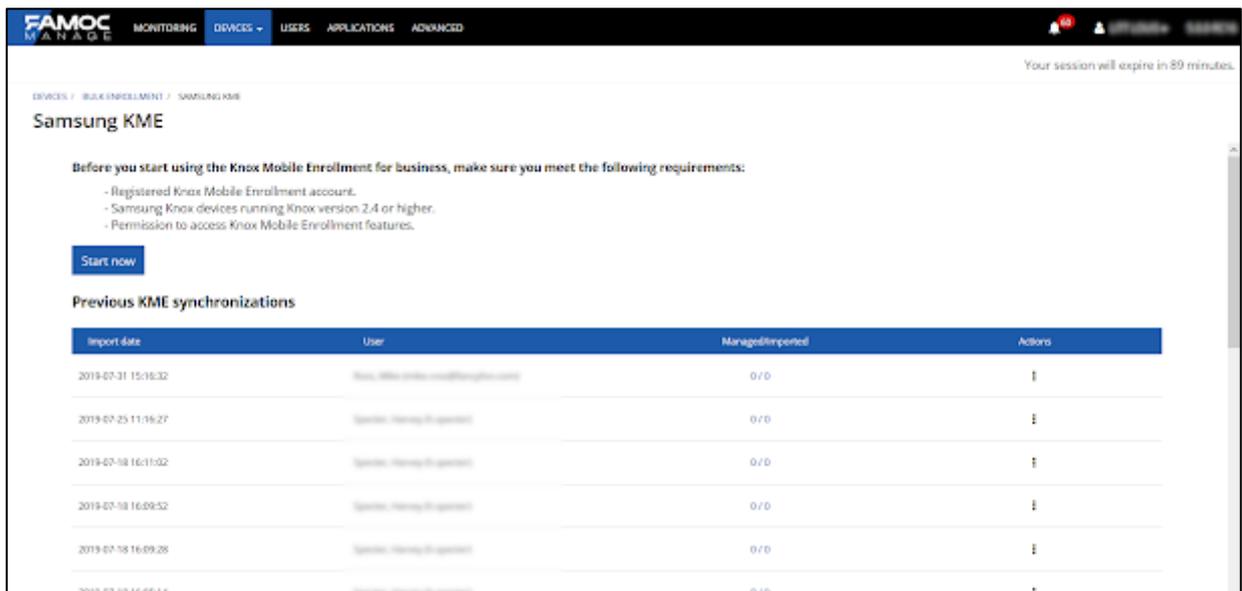
For more information read 'Android Enterprise zero-touch integration guide'.



KME

To enroll Samsung Android devices in bulk using Knox Mobile Enrollment, first, select the Samsung KME method. Then, click the Start now button. A familiar window will appear, guiding you through the process. After uploading CSV to FAMOC and then back to Samsung KNOX, a device import history table will be displayed from which you can redownload the device list CSV file if needed.

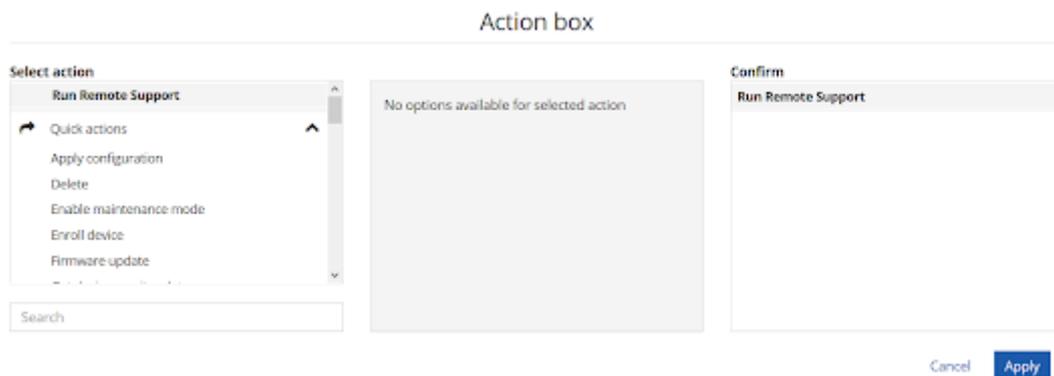
For further details concerning KME read the FAMOC KNOX Mobile Enrollment documentation.



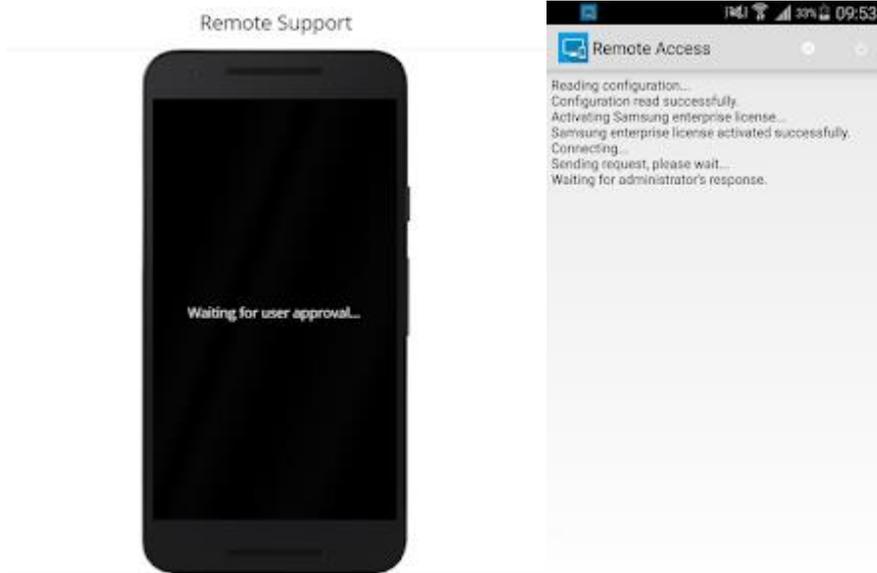
Remote Access Support

Remote Access is a tool that allows administrators to remotely manage the end user's device. The solution provides a real time view of the remote device screen and allows the administrator to take control of the keyboard after being granted consent by the user.

To run **Remote Access** go to devices list view, select a device and press  in the Action Box. Now select **Run Remote Support** and click **Apply**.



You will see the "Waiting for user approval" message on your screen and "Reading configuration" message on your device. After a while you will be asked if you agree for a Remote Access, so click "Yes" and the device' screen will appear on your computer.



Once the device is connected to FAMOC you can see the screen and make all necessary changes.

Additionally, on the bottom right corner there are four useful buttons.

Clicking the wrench button () allows you to enter Maintenance mode which is useful for COSU mode devices. It allows you to exit COSU mode and regain access to the Settings for example.

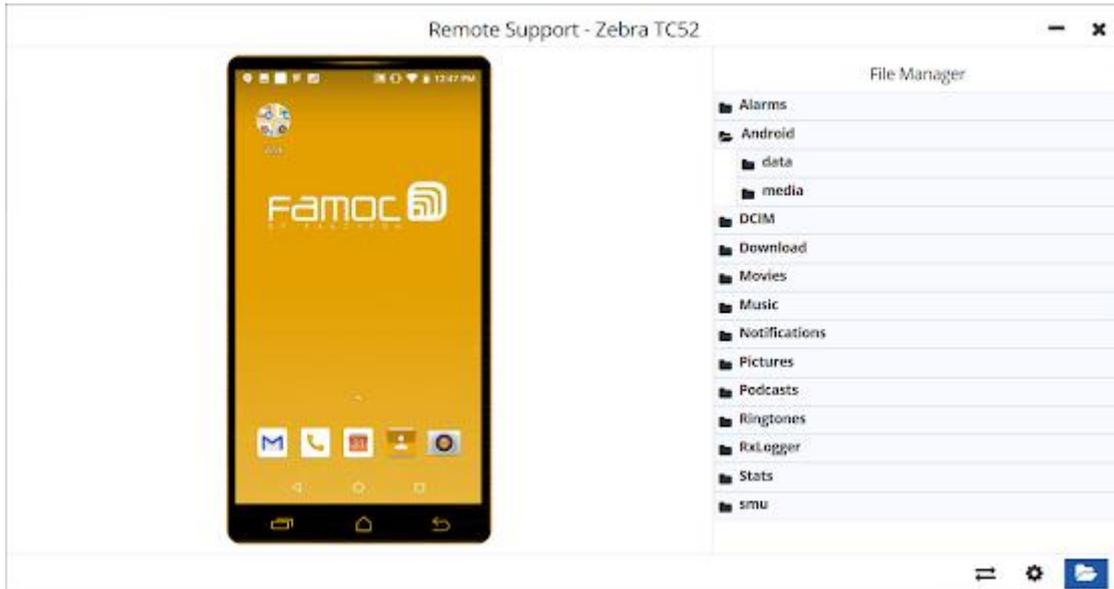
Button  refreshes the connections with the device.

By clicking **Settings** icon  a new tab appears on the right side of the screen where you can decide about the quality of the displayed device' screen. Save all changes by clicking **Apply**.



When you click the File Manager  you will be able to see all the folders and files that are on the device you are currently accessing. In this section you can download the files to your computer, put the files from your computer to the device, add folders on the device and replace files among

device's folders.



You can minimize the window and close session by using the buttons in the top right corner   and maximize the screen with  in the right bottom corner.

3. USERS

This section allows managing all user accounts. Clicking the column name allows you to sort by any property in the list view.

A screenshot of the FAMOC MANAGE web interface. The top navigation bar includes "MONITORING", "DEVICES", "USERS", "APPLICATIONS", and "ADVANCED". The "USERS" tab is active. Below the navigation bar is a search bar and a session timer that says "Your session will expire in 59 minutes." The main content area displays a table of users with the following columns: Login, Name, Surname, Email, Can login, SLA, Created on, Last modification, and Devices. The table contains seven rows of user data.

Login	Name	Surname	Email	Can login	SLA	Created on	Last modification	Devices
<input type="checkbox"/> PK	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-01-21 09:16:06	2019-08-27 14:03:10	
<input type="checkbox"/> AD	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-07-01 08:21:23	2019-08-27 14:03:57	
<input type="checkbox"/> AU	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-06-24 09:54:58	2019-08-27 14:03:57	
<input type="checkbox"/> TK	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-04-29 15:22:38	2019-08-27 14:03:57	
<input type="checkbox"/> OF	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-03-25 14:26:35	2019-08-27 14:03:57	
<input type="checkbox"/> AM	www.kamrad	Kamrad	www.kamrad@famoc.com	YES		2019-02-28 11:20:00	2019-08-27 14:03:57	

 Select button – by clicking this button you will select all users on the page.

Selected users count is visible next to the "Select" button.

 Add user – this button opens the user creator. (See 2.1 Adding users)

Search module – allows to search for users by name or login.

 Table settings – allows to add or remove columns from the users tab view.

Selecting users from the list allows administrator to perform actions for multiple users at the same time.

	Login	Name	Surname	Email	Can login	SLA	Created on	Last modification	Devices
<input checked="" type="checkbox"/>	AD	Jan	Janowski	jan.janowski@famoc.com	YES		2019-07-01 08:21:23	2019-08-27 15:06:14	
<input checked="" type="checkbox"/>	PLU	Jan	Janowski	jan.janowski@famoc.com	YES		2019-06-24 09:54:58	2019-08-27 15:06:14	
<input checked="" type="checkbox"/>	TW	Jan	Janowski	jan.janowski@famoc.com	YES		2019-04-20 15:22:38	2019-08-27 15:06:14	
<input type="checkbox"/>	DR	Jan	Janowski	jan.janowski@famoc.com	YES		2019-03-25 14:26:35	2019-08-27 15:06:14	

Customizing Users list

Clicking a column name allows you to sort by any property in the list view. There is also a possibility to customize which columns are displayed, by using **Customize table** view button . All available columns are grouped listed on the left side of the Action box, while columns currently visible in the Users list are displayed on the right side. The administrator can drag and drop any column to change the order or the list of displayed columns. To accept changes confirm by pressing Save.

Customize table view

Available columns

Search

User fields ▼

Custom user fields ▼

Selected columns

Search

- Photo ✕
- Login ✕
- Name ✕
- Surname ✕
- Email ✕
- Can login ✕
- SLA ✕
- Created on ✕

Cancel Save

Adding a user

There are many ways to add users to FAMOC manage. You can import users from file (.txt.; .xls; .csv) (described in separate article), import from Azure Active Directory catalogue (described in Organization settings section) or add them manually.

Click the Add user button  to open user creator. In the first step add basic user information such as: name, surname, login, email, country and language.

New User



Surname

Name

Login

This field is required

Email

Country
Poland

Language
English

Can login
 Enable user login

Cancel Create

Once the user is created, administrator can fill additional information in user sub-tabs: Details, Groups & roles, Settings and Certificates.

user1
user1
user1
Enter email

Can login: No
Account status: UNLOCKED
Country: No value

Language: English
User password: Change password
Force password change: Set expiration date

Details Settings Certificates Groups & roles

Basic data

Company: user1
Department: admin
Job title: No value
Employee ID: user1@wp.pl
Email username: No value
Mobile number: 48123456789
Office phone: Enter mobile number

Exchange data

Exchange username: No value
Exchange email: No value
Exchange domain: No value
Password: No value

Click the field in order to add or edit information.

Basic data

Company: user1 ✓ ✕
Department: admin
Job title: No value
Employee ID: user1@wp.pl
Email username: No value
Mobile number: 48123456789
Office phone: Enter mobile number

All user management actions can be performed in the menu above the user avatar and the Action box.

Your session will expire in 58 minutes.

Action box

Select action

- Quick actions
- Edit users
- Groups and roles

Search

Cancel Apply

user1
user1
user1
Enter email

Can login: No
Account status: UNLOCKED
Country: No value

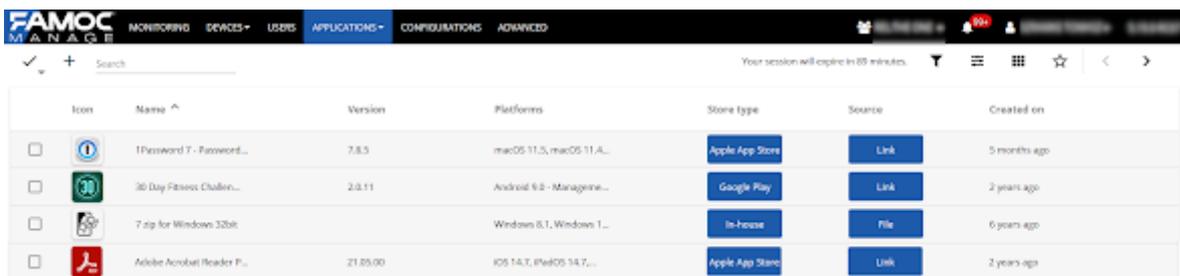
Language: English
User password: Change password
Force password change: Set expiration date

Action box group name	Available actions
 Quick actions	<ul style="list-style-type: none"> • Delete user • Enroll device • Force password change • Lock user account • Unlock user account • Change platform
 Edit users	<ul style="list-style-type: none"> • Change country • Change password • Change SIM card
 Groups and roles	<ul style="list-style-type: none"> • Assign to group • Assign to role • Detach from group • Detach from role

Table - Actions available in the USERS tab and Action Menu.

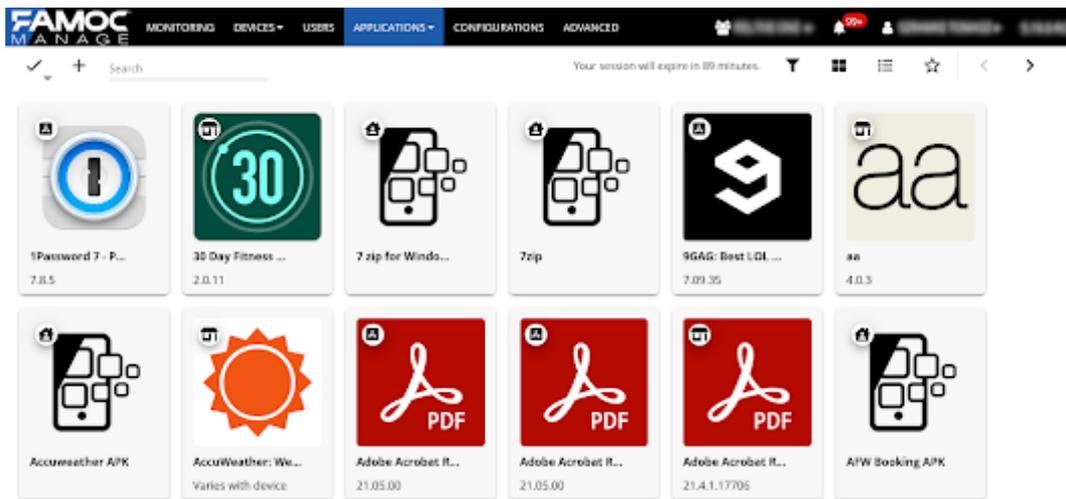
4. APPLICATIONS

The Applications tab enables FAMOC user to manage components, which may be installed on mobile devices. All applications added to the system can be sorted by using the chosen column. At first glance, it is possible to notice details such as application's icon, version, group, target platform or source. It is possible to customize which columns are displayed.



Icon	Name	Version	Platforms	Store type	Source	Created on
	1Password 7 - Password...	7.8.5	macOS 11.5, macOS 11.4L...	Apple App Store	Link	5 months ago
	30 Day Fitness Challen...	2.0.11	Android 9.0 - Manage...	Google Play	Link	2 years ago
	7.zip for Windows 32bit		Windows 8.1, Windows 1...	In-house	File	6 years ago
	Adobe Acrobat Reader P...	21.05.00	iOS 14.7, iPadOS 14.7...	Apple App Store	Link	2 years ago

Applications list view



Applications list – grid view

✓ Select button – by clicking this button you select all applications from the list.

✓ Selected applications count – visible when activated.

+ Add new application – opens the action box.

Search Search module – allows to search for applications by name.

Export data - allows to create list of selected apps with selected data from columns in .csv or .txt format.

Filters - allows to filter app list by Installation source (Google Play Store, App Store, Managed Google Play, In-house app), Major app groups (Application groups to which the most applications have been assigned), User groups, Installation destination (Work Profile or Personal part), Policy (to which app is assigned), Configuration (apps with defined configuration), Installations (apps that are or are not installed on the device).

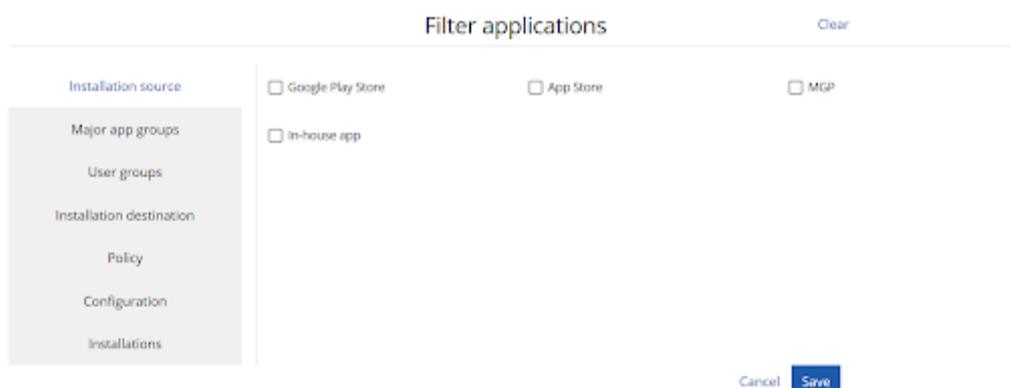
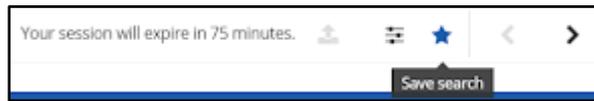


Table settings – allows to add or remove columns from the applications tab view.

Select grid view - changes the view of applications list to icons grid view.

FAMOC also allows you to save search and filter results for easy access later. For example, you can

save all custom applications or all applications with managed configurations to quickly return to the created list later. To do this, click the star icon and enter a name for the list being saved. Saved results will be available later by hovering over the star icon or from the level of filters.

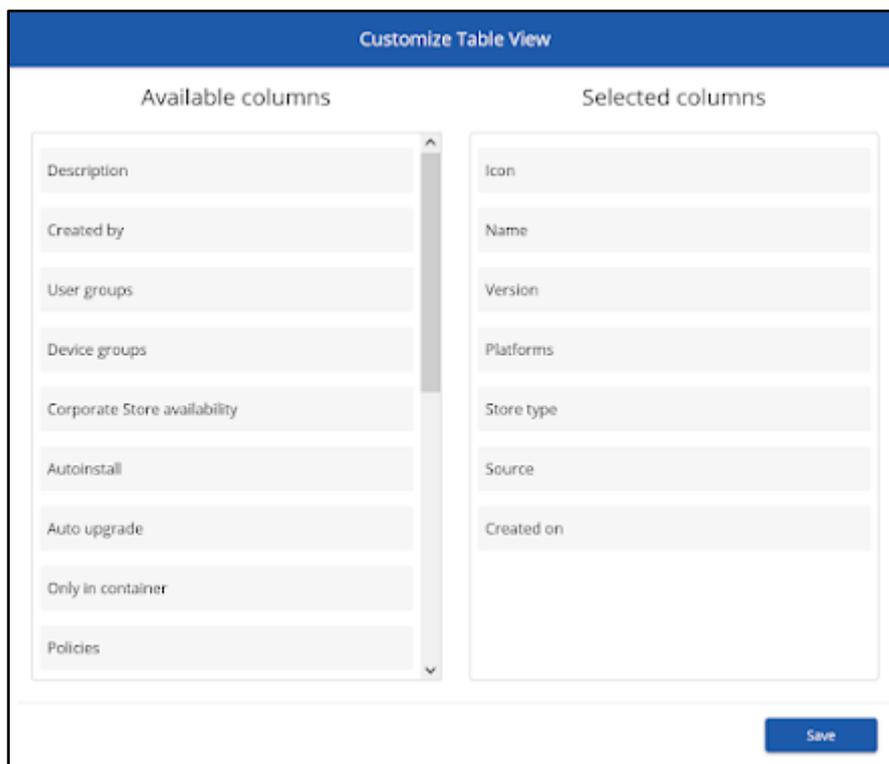


Selecting an application from the list allows the administrator to perform actions for multiple components at the same time.

Icon	Name	Version	Platforms	Store type	Source	Created on
<input checked="" type="checkbox"/>	Google Maps - Navigate...	Varies with device	Android 9.0 - Manage...	Google Play	Link	about a month ago
<input checked="" type="checkbox"/>	Google Maps - Navigate...	Varies with device	Android 9.0 - Manage...	Google Play	Link	about a month ago
<input checked="" type="checkbox"/>	Google Sheets	Varies with device	Android 9.0 - Manage...	Google Play	Link	2 years ago
<input checked="" type="checkbox"/>	Google Slides	Varies with device	Android 9.0 - Manage...	Google Play	Link	2 years ago

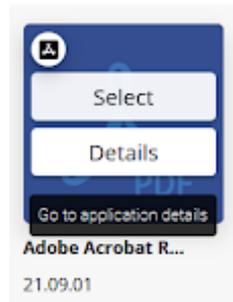
Customizing applications list

There is a possibility to customize which columns are displayed, by using the **Customize table view** button . All available columns are listed on the left side of the Action box, while columns currently visible in the Applications list are displayed on the right side. The administrator can drag and drop any column to change the order or the list of displayed columns. To save changes press **Save**.



Application details

To go to the application details, click on its name (list view) or hover over its icon and click Details (grid view).

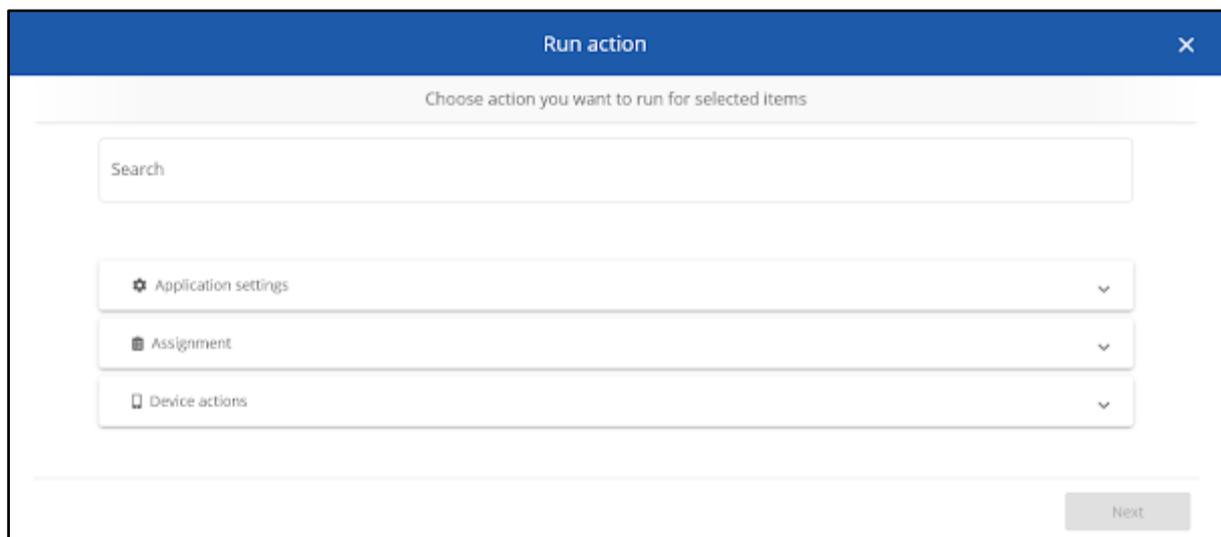


Basic operations are available on the navigation bar. They are (from left) -

- Install the app
- Uninstall the application
- Launch the application
- Remove application¹



The three dots icon  allows access to advanced operations.



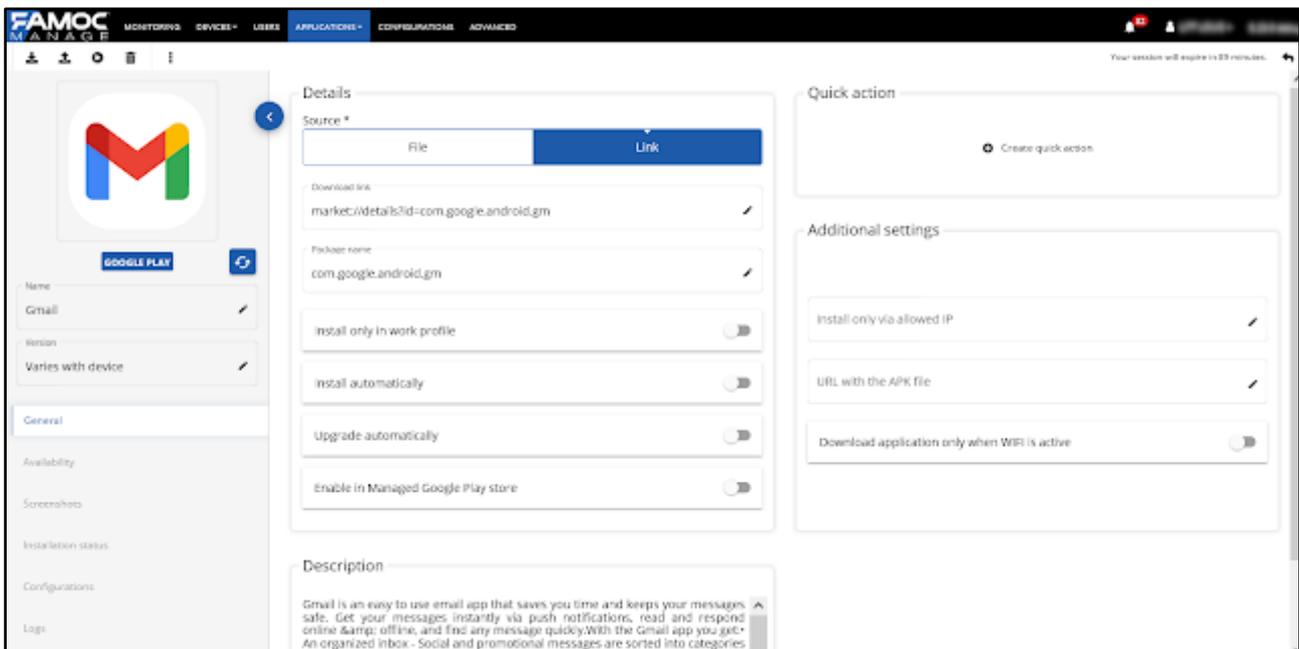
Actions category	Available actions
------------------	-------------------

¹ Some pre-installed applications e.g. Launcher, Zebra apps (used when Zebra OTA integration is available), Strongswan, cannot be removed from FAMOC.

Device actions	<ul style="list-style-type: none"> • Uninstall application • Get configuration feedback <ul style="list-style-type: none"> • Run application • Reapply managed configuration <ul style="list-style-type: none"> • Install application
Assignment	<ul style="list-style-type: none"> • Assign policies • Detach Policies • Create quick action • Set corporate store availability • Set the application groups • Set platforms for the application <ul style="list-style-type: none"> • Change device models
Application settings	<ul style="list-style-type: none"> • Set automatic upgrade • Set automatic installation • Remove application

Clicking on an application name allows you to edit it. Refresh button  allows us to update app data from the store.

From the menu on the left, you can then select a section to manage the detailed settings of the application.

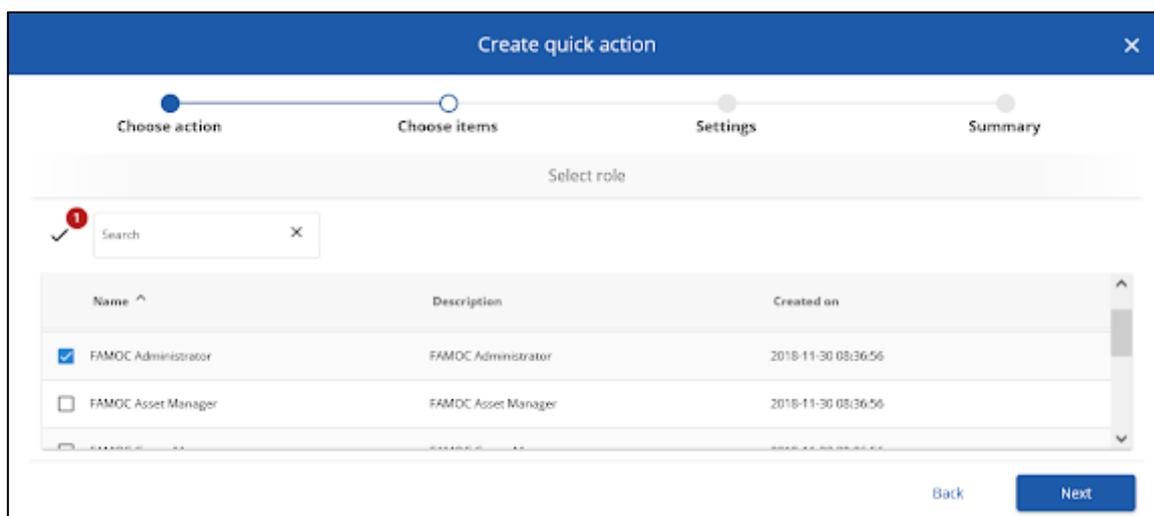


In the General section, we can change the source of the application (file or link to the application), change the package name and specify the following installation parameters:

- Installation only in the work profile - it will only be possible to install the application in the work profile
- Automatic installation - the application will be installed on all devices, regardless of the policy

- Automatic update - the application will be automatically updated with new versions
- Enable on Managed Google Play Store - The app will be available on the Managed Google Play Store
- Application policy accepted - accept application policy automatically

You can also add the application installation to the Quick Actions menu. If you do, the operation will be available from the Device details screen. You can edit the action name and select the roles that will be able to perform the created operation.



You can also define the allowed IP from which the app can be installed, define an external source of the app by providing the URL of the APK file, and only allow the app to be installed when Wi-Fi is active.

In the **Availability** tab, you can assign platforms and device models to the application, define for which user groups the application will be available in the company store and assign the application to an application group. You can also assign or detach an application to policies.

In the **Screenshots** tab, you can add or remove screenshots that will be displayed in the store.

In the **Installation status** tab, you can check on which devices the application was installed, its version on the device, installation date and last run.

In the **Configurations** tab, you can preconfigure applications to be installed on a device with specific settings.

For the iOS apps you can upload file with configuration parameters (xml file in .plist format) and maintain the custom values (nested parameters are supported)².

² You can read more about iOS app config here: <https://www.appconfig.org/ios/> You can also check the example for Google Chrome configuration <https://www.chromium.org/administrators/ios-mdm-policy-format>



For the Android apps you can use Managed configuration which are explained below.

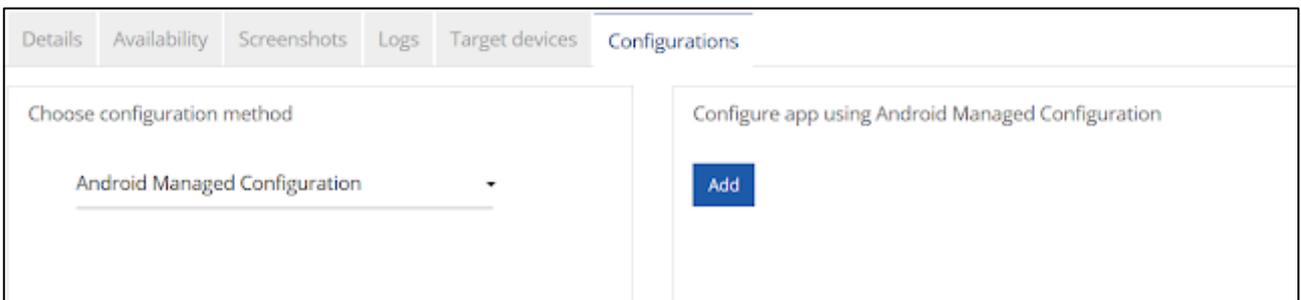
Managed Configurations

Some apps include built-in settings templates, which can be configured and implemented remotely on a device. This option is available only for apps that:

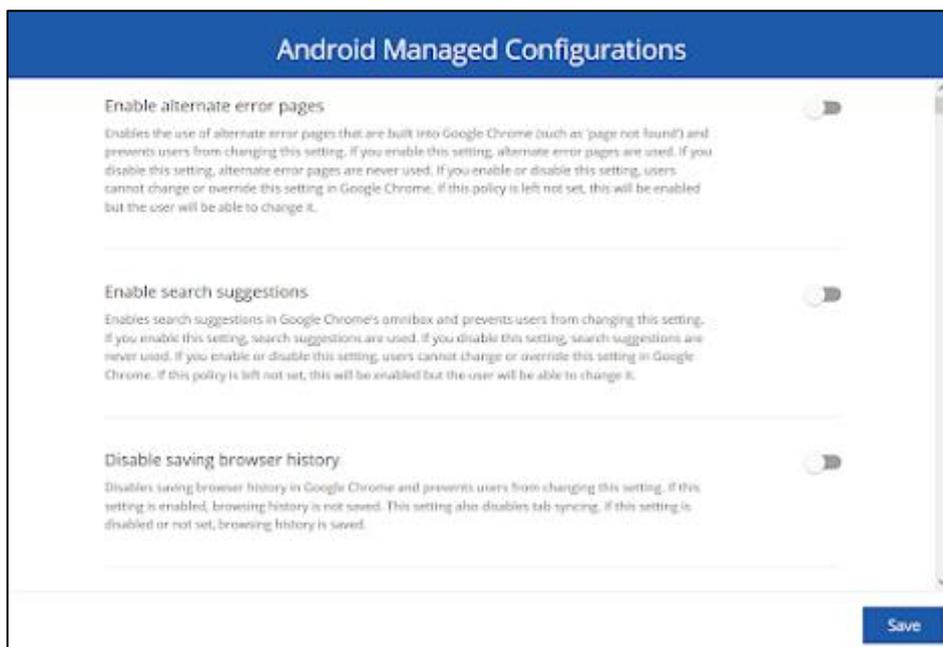
- a. have this feature enabled by its developer;
- b. have been enabled for Managed GooglePlay store in FAMOC (refresh the page once you have marked appropriate field).



To use this settings choose **Android Managed Configuration** method and click **Add** in the section on the right.



Available settings depend on the app. On the screenshot below you can see an example of settings for the Chrome browser.



Managed Configurations are available only for apps that support this feature. App developers define which features and settings will be available in Managed Configurations template. FAMOC administrator can freely specify this configuration within given options. Once the settings are configured according to your needs click Save. Configuration will be imported to Managed Google Play and app will be updated on all devices with the new configuration.

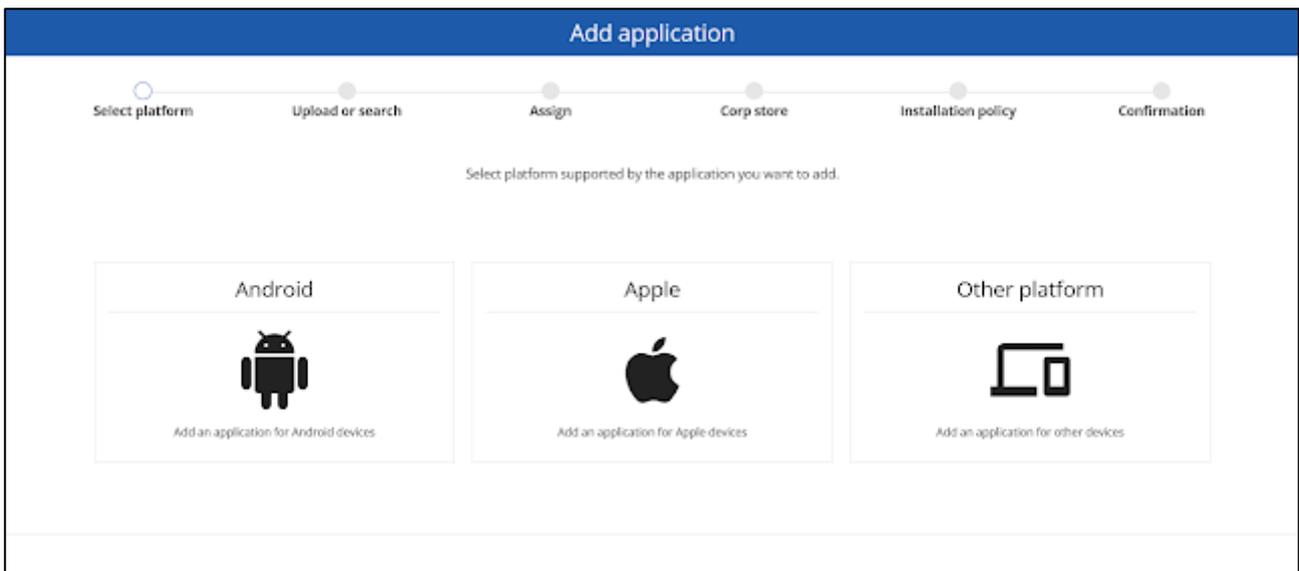
In the **Logs** tab you can check all operations (Installation, Uninstallation, Application configuration) related to the given application.

In the case of applications for iOS / macOS, the **VPP Licenses** tab will also be visible, where you can check the status and assignment of the license for a given application.

Adding a new application to FAMOC

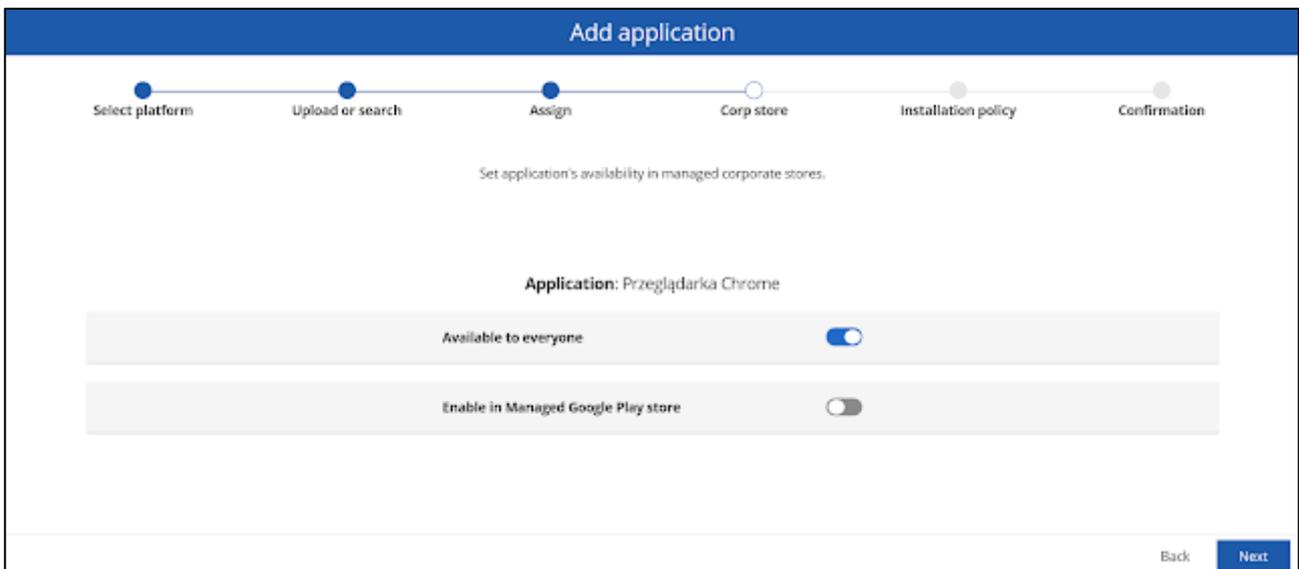
To add an application to the system, use **Add application** button **+** in the **APPLICATIONS** tab. It will trigger a modal window which will guide you through the process of adding new app.

In the first step select the platform of an application (Android, Apple or other).

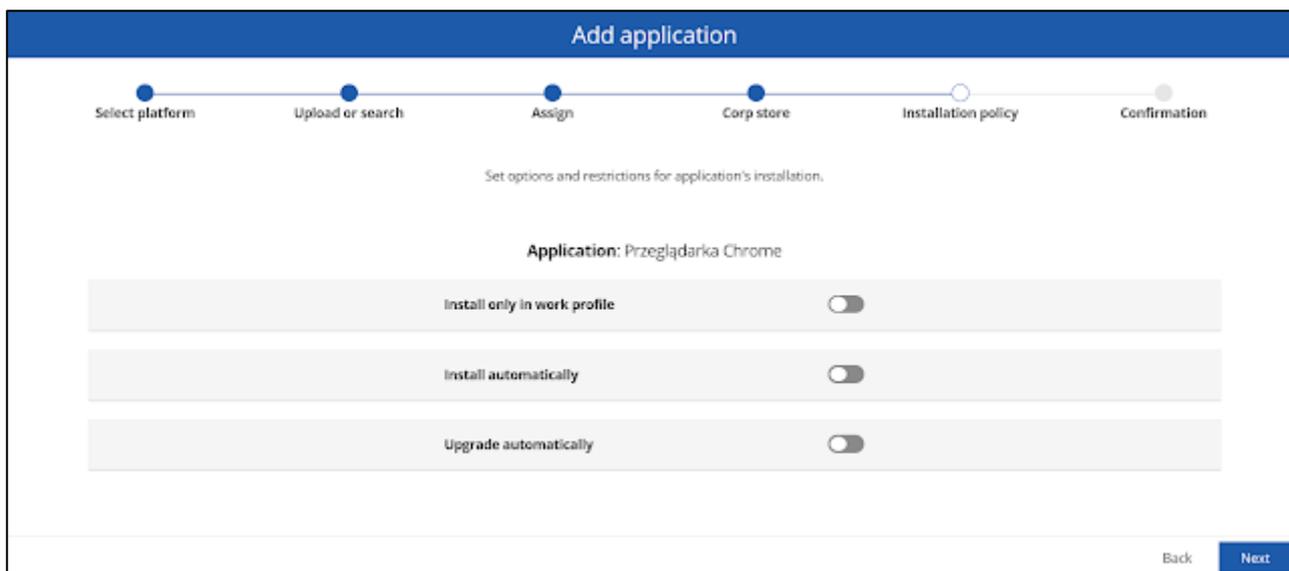


Then, depending on your choice search for an app in a store (Google Play, App store), upload a file with an app (supported formats - .apk for Android or .app; .pkg; .ipa. for iOS or macOS; .xap or .msi for Windows) or provide a link to an app file (file will be uploaded to FAMOC from that link). If you choose 'Add in-house application' option you will see an additional step to enter general information about the application and upload the application file. Required fields are marked with messages.

In the next step assign your application to appropriate app group. Then, select if the app should be available for all users or only users from selected groups of users or devices. You can also add the app to a Managed Google Play store (Android only).



Finally, set app installation policy - Install only in work profile - app will be possible to install only in corporate part of the device, Install automatically - app will be installed on all compatible devices, regardless of policy, Upgrade automatically - app will be automatically updated once new version is available.

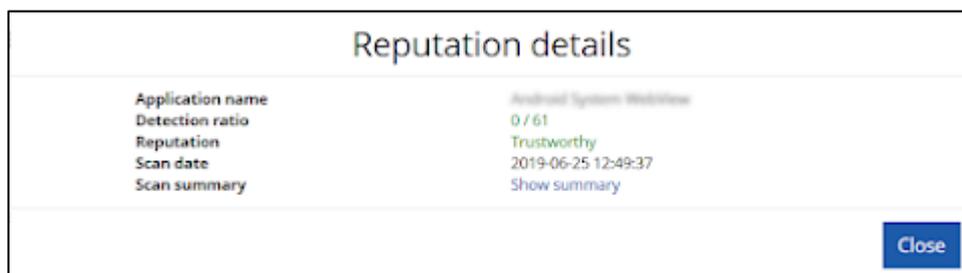


In the last step confirm adding application by clicking **Create application**. newly created app can be found in the **Applications** tab.

Application reputation

FAMOC uses VirusTotal services to validate apps security reputation. Information about package including package_name and md5 hash are sent to VT servers which generates app report.

Report is based on a result of many antivirus scans. Downloaded information consist of number of performed scans and risk detections. Depending on the results, app is given appropriate security reputation level.



For each VT report you can view a summary ([example](#)).

There are five reputation levels:

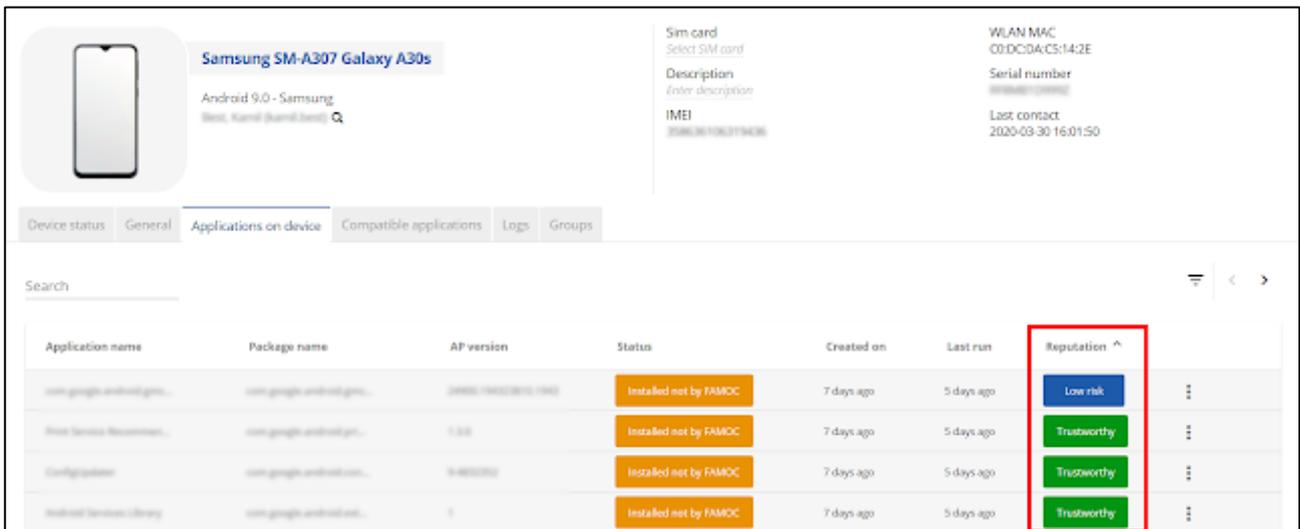
- UNKNOWN - (grey)
- OK - (green) Trustworthy
- INFO - (blue) Low risk
- WARNING - (yellow) Suspicious
- ERROR - (red) Dangerous

Reputation levels are based on the following thresholds:

- 0 positive detections: OK

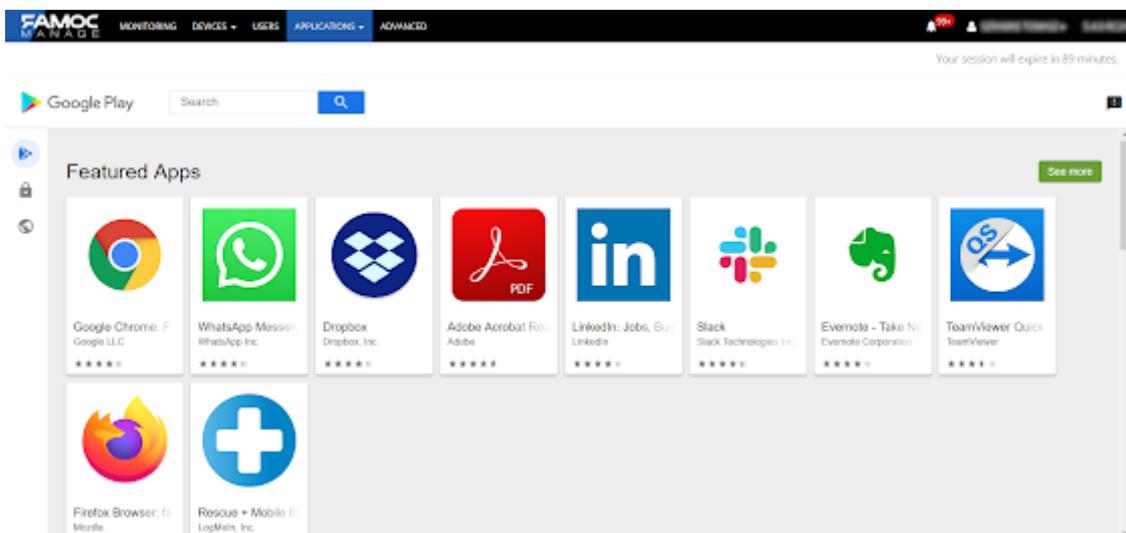
- up to 10% INFO
- 10% -50% WARNING
- 50% ERROR

You can see app reputation in Device details, under Applications tab. Click the shield icon on the apps list. Color of the shield corresponds to the level of risk.



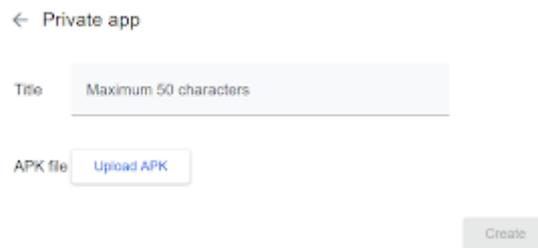
Managed Google Play

This subtab allows previewing Managed Google Play. You can search for any apps, add private apps and publish web apps (website shortcuts as apps). In the search field you can search apps by name.

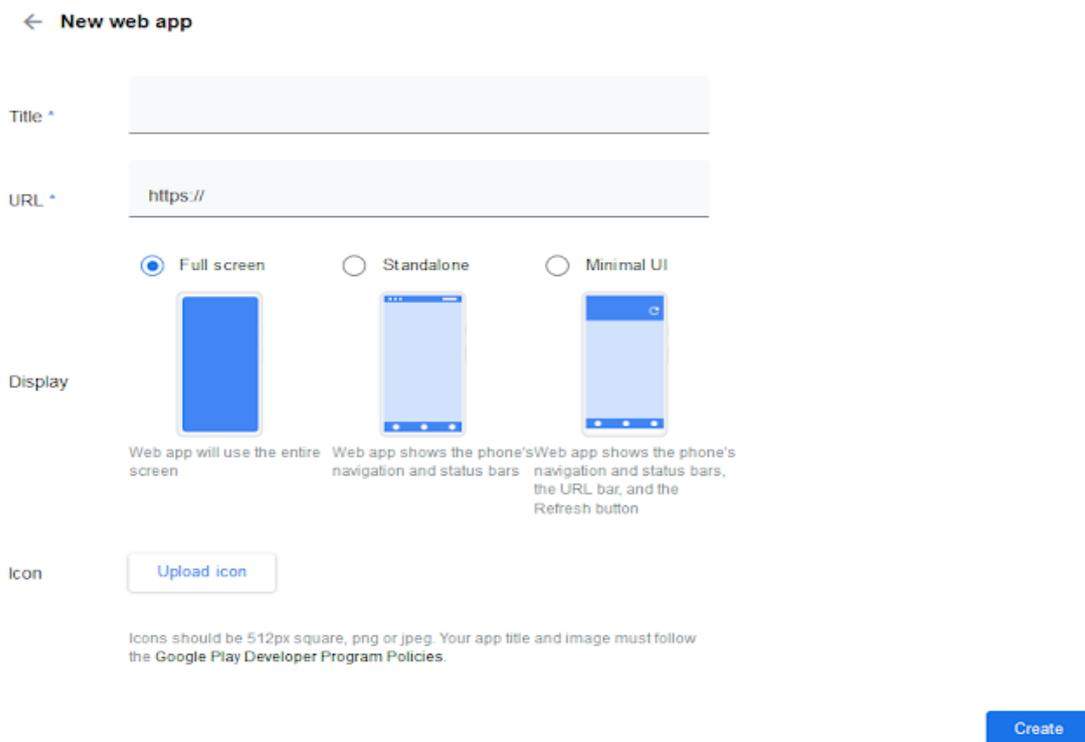


Once you found the app you are looking for you can preview its permissions and approve them so the app will not be asking for permissions on a device. When you do it, you will be asked to decide whether you wish to keep the app approved when the app requests new permissions or to revoke app approval when this app requests new permissions. Once the permissions are approved you can add the app to Managed Google Play by clicking **Select**. Then you will be automatically redirected to the app details page. Clicking **Unapprove** will revoke app permissions and remove it from the store.

In the Private apps tab, you can add your own .apk applications to the store. To do this, click the plus icon in the bottom right corner of the screen, then enter the application name and upload the APK file. To confirm adding the application, click the **Create** button.



In the Web apps tab you can create a shortcut to a specific URL that will be displayed on the device in the form of an application. The tab allows you to enter the Title, URL, specify the display of the application on the device and send the icon in .png or .jpg format, under which the application will be displayed on the screen of the device.

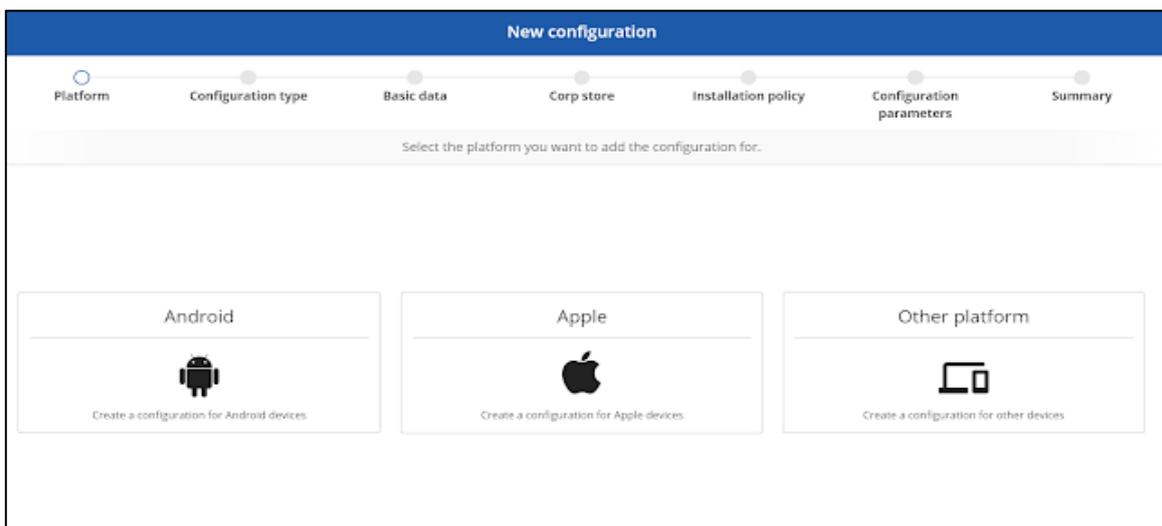


5. CONFIGURATIONS

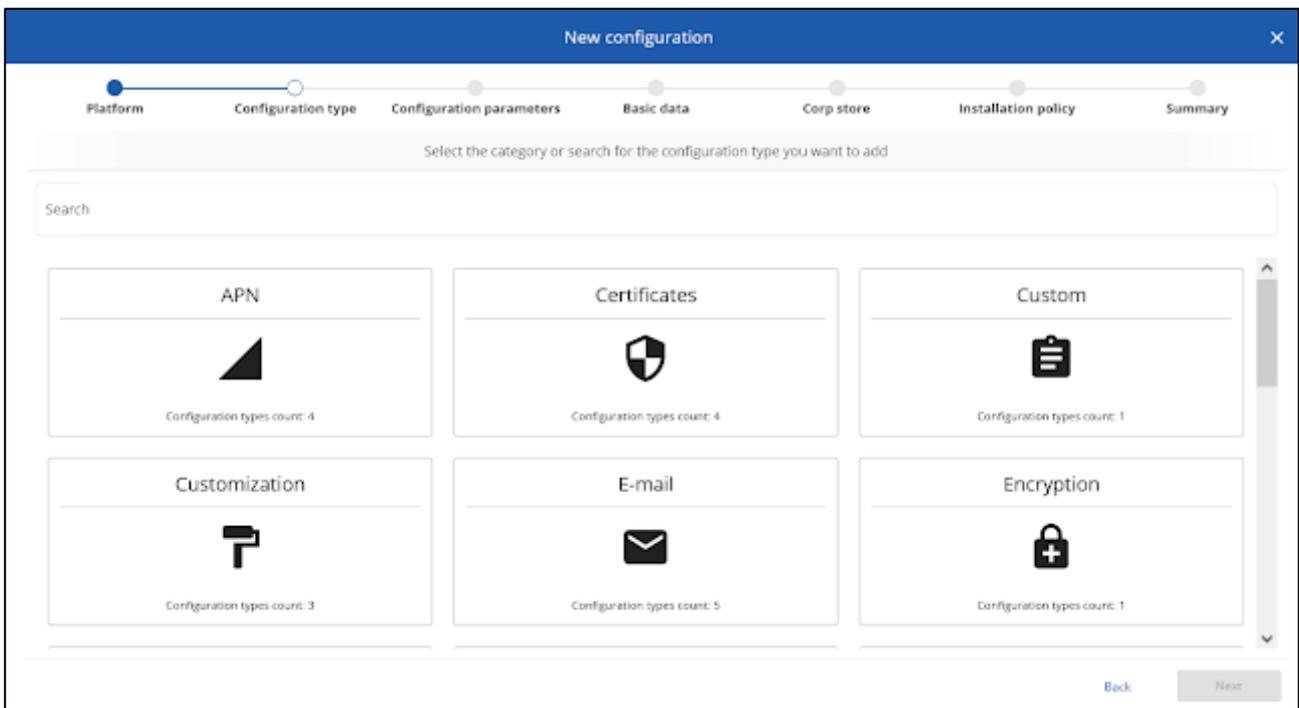
Configurations tab allows you to quickly and easily manage all configurations in FAMOC.

Name	Type	Created by	Created on	Platforms	Available in corpstore	Only in container	
<input type="checkbox"/> APN	Access point configuration	Harvey Specter	3 days ago	Android 10.0, Android ...	No	No	⋮
<input type="checkbox"/> Wine CA	Install certificate	Mike Ross	28 days ago	Android 10.0, Android ...	No	No	⋮
<input type="checkbox"/> pwa	COSU mode settings	Mike Ross	about a month ago	Android 10.0, Android ...	No	No	⋮

To add a new configuration click the PLUS button (+). When clicked, the configuration wizard window will open. In the first step select the platform - Android, Apple (iOS, macOS, tvOS) or Other (Windows).



Then, select the Type: APN, Certificates, E-mail, Lock code, SD Card lock, Tools, VPN, WLAN) or use search field.



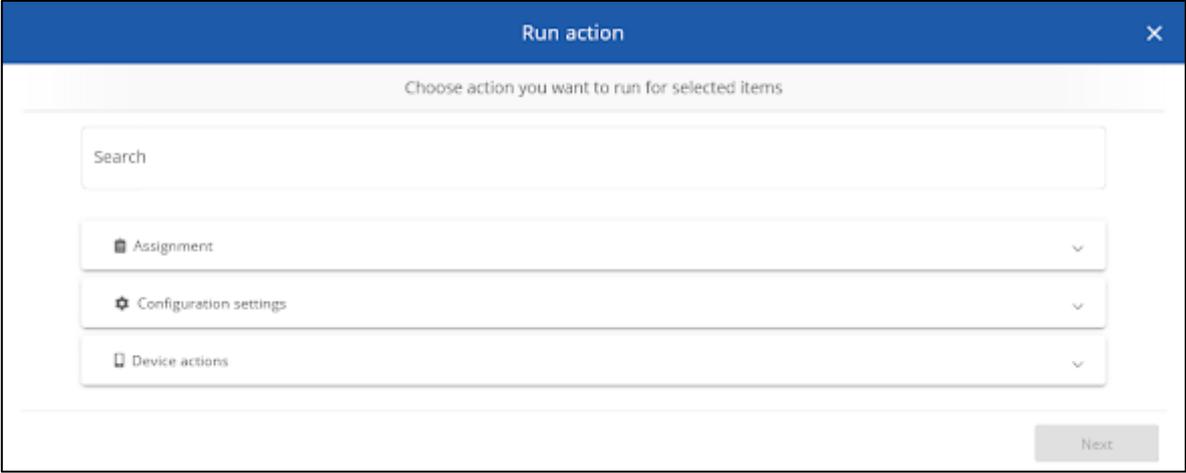
For some categories it is possible to select an even more specific type. In the following steps provide the Name of the configuration and description (optional), specify its availability in the company store and installation settings.

Then specify the configuration parameters, check the summary and click Create Configuration to complete the process.

On the navigation bar there are also more options to manage configurations

Icon	Action
✓	Select all / select all configurations on the page
+	Add new configuration
⌵	Filter configurations list. You can filter by the Configuration type groups, Configuration types, Platforms, Policy (all policies to which configuration is assigned), Availability (Corpstore, Only in Container, Installed on devices) The saved search results will also appear here.
☰	Customizing table view
☆	Save search results - saved results will be available after hovering over the star icon or on the filter list.

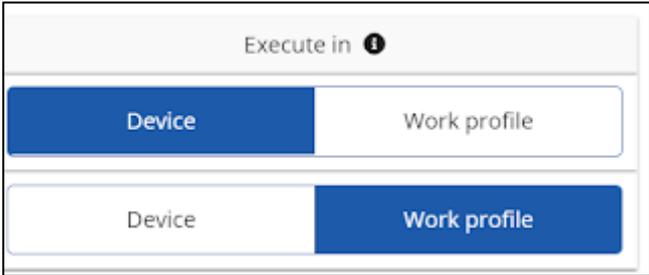
To manage the configuration, select one or more of them and then click the three dots icon on the top bar. A window will appear that will guide you through the selected action process.



Select an operation to perform and the wizard will guide you through the steps.

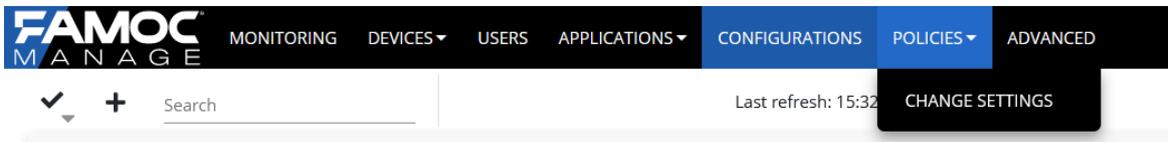
Actions	
Assignment	<ul style="list-style-type: none"> • Assign policies • Create quick action • Detach policies • Save as • Set corporate store availability • Set platforms for configuration
Configuration settings	<ul style="list-style-type: none"> • Delete • Set automatic installation • Set automatic upgrade
Device actions	<ul style="list-style-type: none"> • Apply on device • Uninstall from device

In the case of configurations that can be used both in a work profile and for the entire device, it will be possible to choose where the configuration should be applied.



6. POLICIES

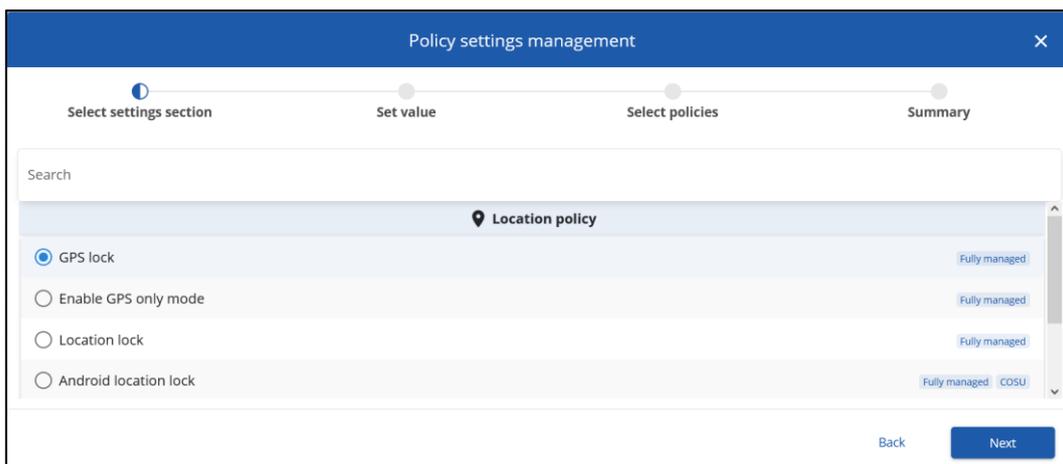
The policies tab allows you to quickly edit policies by adding new settings or restrictions. To do this, hover over the tab and select Change settings.



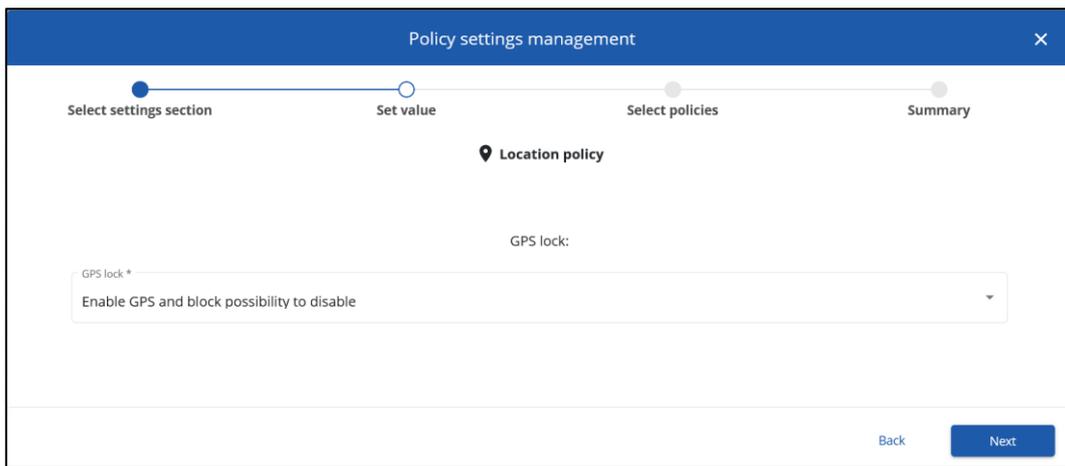
The edit wizard screen will be displayed. Then select the category of settings you want to change:

- Application policy
- Application restrictions
- COSU settings
- Enabled applications
- Encryption policy
- General settings
- Hardware policy
- Installer policy
- Location policy
- Network policy
- Update policy
- Wipe policy
- Work profile restrictions

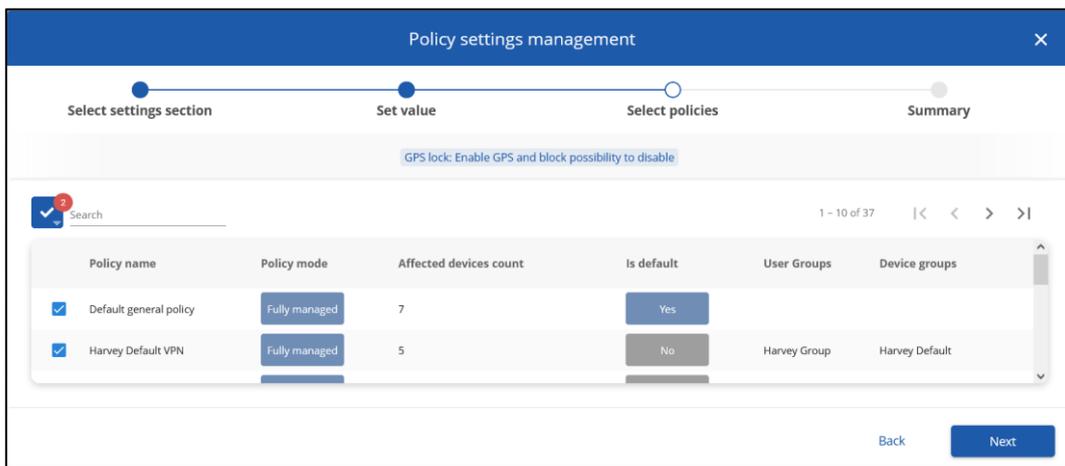
Depending on the category selected, specific settings will be displayed. Select the parameter you are interested in and click Next.



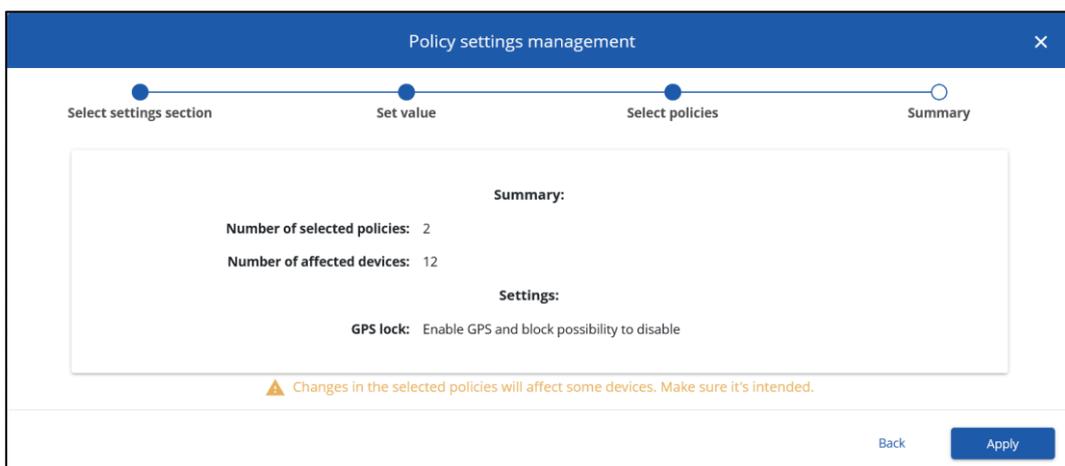
Then specify the value of the selected parameter and click Next.



In the next step, select the policies to be applied with the change. You can select any number of policies from the list.



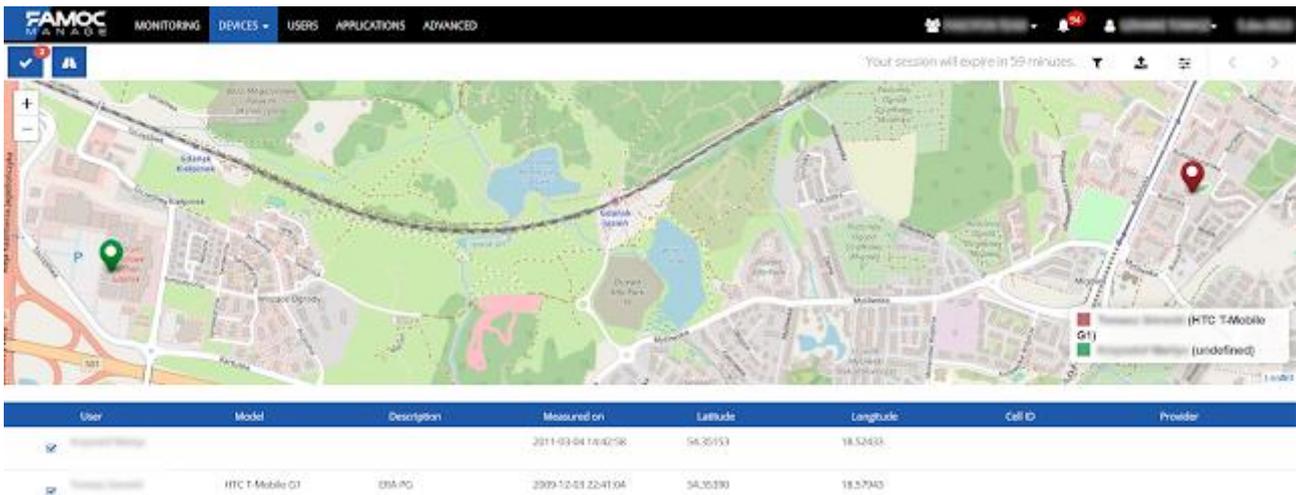
In the last step, a summary will be displayed. You will see how many policies will be changed and how many devices will be affected by the change. Click Apply to complete the process.



7. LOCATIONS

The Locations tab enables FAMOC user to monitor devices' or users' positions, which may be retrieved from a mobile device. The administrator can see on the map the last position of every

mobile device, which retrieves location data. All listed devices can be sorted on the list by using the chosen column and clicking on the column name.



Action button	Description
	Customize table view
	Filters
	Export data
	Previous page
	Next page
	Select/Unselect
	Draw/Do not draw paths

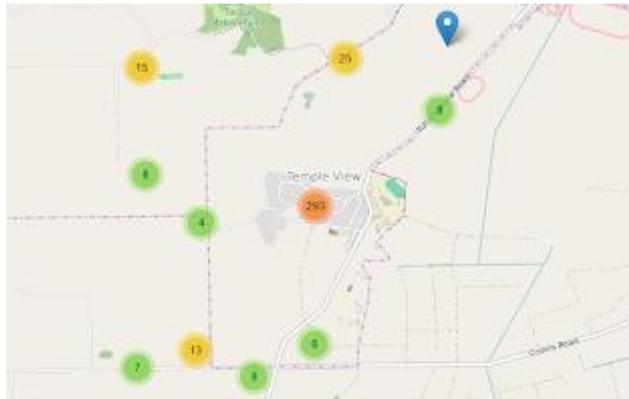
Table - Actions available in the Location tab

The map interaction

The administrator can mark any device on the list to see its positions on the map. On the right side of the map there is a legend with assigned marker colors for a clearer view of different devices in similar positions. You can freely select and unselect devices shown on the map, up to 14 devices at the same time. For each device you can see last retrieved location and another 20 previous locations.

Number on Select/Unselect button informs how many devices are marked on the list.

Position markers, which are close to each other, are shown on the map as groups. The administrator can click on the markers group or zoom in the map to see a single device location. The number displayed on the group icons shows how many locations are grouped there.



Markers of the single device can be linked to show a path of motion and changes in the device position in time. It may be turned on and off with Draw/Do not draw paths button on the action bar.

User	Model	Description	Measured on	Latitude	Longitude	Cell ID	Provider
...	Apple iPhone 6	Added from startup page	2019-05-06 19:42:51	54.20281	18.60357	4	QPS
...	Apple iPhone 6	Added from startup page	2019-09-05 13:31:54	54.31117	18.57528	4	QPS
...	Apple iPhone 6	Added from startup page	2019-07-04 15:00:07	54.31136	18.58177	4	QPS

By clicking on the tag of a single device, you can view its basic information, such as the assigned user, device model, date of location download, IMEI number, serial number and coordinates, and go to the details.



Customizing locations list

There is a possibility to customize which columns are displayed, by using **Customize table view** . All available columns are listed on the left of the Action box, while columns currently visible in the Logs list are displayed on the right side. The administrator can drag and drop any column to change order or a list of displayed columns. To confirm changes press **Save**.

Customize table view

Available columns

- Altitude (meters)
- Horizontal accuracy (meters)
- Vertical accuracy (meters)
- Course (degrees)
- Speed (m/s)

Selected columns

- User
- Model
- Description
- Measured on
- Latitude
- Longitude
- Cell ID
- Provider

Filtering locations list

Filters

Show last:
2 weeks

Records per page:
10

Filter by:
User

Model

Description

From: 14-08-2019 10:42

To:

2019-Aug						
Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

2019-Aug						
Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

There is a possibility to filter locations data which is displayed on the map, by using the Filters button . With active filters, only 20 last locations for each device will be shown on the list and the map. Administrator can choose various filter options:

Show last - if chosen, you can see only locations from chosen time frame; possible options to choose are: one day, two days, three days, one week, two weeks, one month and full history.

Date range - you can choose specific dates (with hours and minutes) in calendars from and to which locations will be shown on the list. ;

Filter by - three possible fields: Model, User and Description, by which administrator can filter devices on the list;

Records per page – the administrator can change the number of devices shown on a single page.

To confirm all chosen settings, click Save.

51

Export locations data to a file

Export data

Available columns

- Altitude (meters)
- Horizontal accuracy (meters)
- Vertical accuracy (meters)
- Course (degrees)
- Speed (m/s)

Selected columns

- User ✕
- Model ✕
- Description ✕
- Measured on ✕
- Latitude ✕
- Longitude ✕
- Cell ID ✕
- Provider ✕

File format

Chosen file format:

- CSV comma separated
- CSV semicolon separated
- TXT tab separated
- Use filters**

From: 2019-08-14 10:42 +0200
To:

There is a possibility to export locations data by clicking the Export data button . You can export data with specific order of columns previously chosen in Customize table view options or choose another order of columns by dragging and dropping columns from the Available columns and Selected columns lists.

You can choose the format of exported file from three options:

CSV comma separated - .csv file, in which records are separated with “,” character;

CSV semicolon separated - .csv file, in which records are separated with “;” character;

TXT tab separated - .txt file, in which records are separated by tabulators.

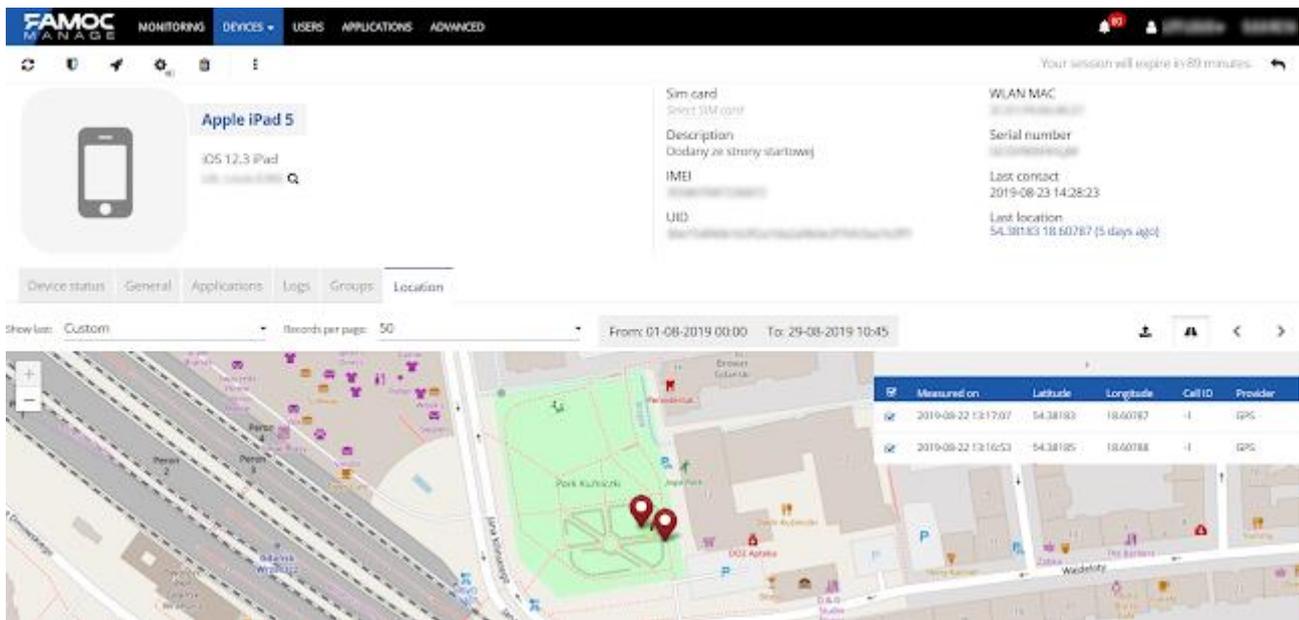
Use filters checkbox allows you to export data with previously chosen and confirmed filters (e.g. device model or time frame).

To confirm all settings, click **Save**.

In locations tab you can export all data retrieved from mobile devices in a single file.

Location tab on a device details view

After clicking on a single device record in the general location list the administrator is redirected to a device details view. You can see all location data for the device in the Location tab.



Action button	Description
	Expand a table
	Hide a table
	Previous page in table
	Next page in table
	Draw/Do not draw paths

Table - Actions available in the Location tab on Device page

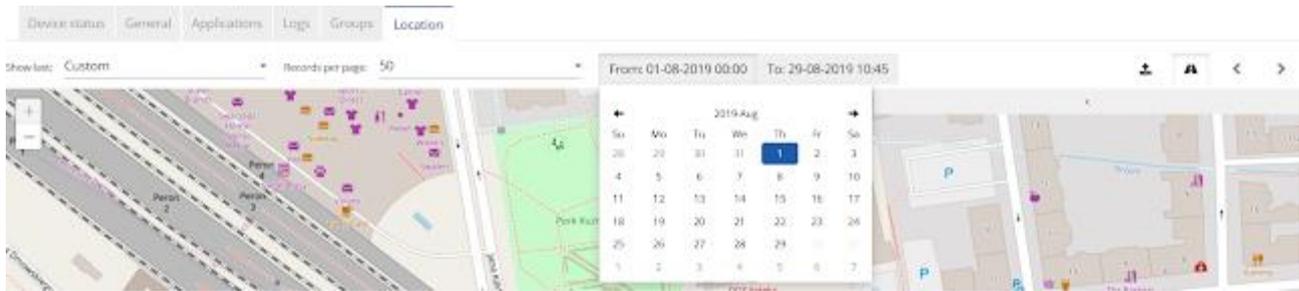
Filters in location tab of device details

There is a possibility to filter locations data which is displayed on the map and in the data table. You can choose from the following filter options:

Show last - if chosen, displays locations from chosen time frame; possible options to choose are: one day, two days, three days, one week, two weeks, one month and full history.

Date range – you can choose specific dates (with hours and minutes) by using From and To buttons.

Records per page – you can change the quantity of locations records shown in the single page in the table, available after unfolding the **Expand** button. By pressing **Next page** and **Previous page** buttons, you can see all stored location data for a device. You can freely select and deselect them to be shown or hidden on the map.



8. LOGS

The Logs tab enables you to monitor the status of operations, which were executed on all mobile devices in the organization in one place. The administrator can customize, sort, or filter operations shown on the list to monitor operation only from specific device groups, or show only operations with specific status of operation. The administrator can also export data from the table to popular data type file. The Logs list is refreshed automatically, so there is no need to refresh a page to see new operations or changes in operations statuses.

Action button	Description
	Customize table view
	Filters
	Export data
	Previous page
	Next page

Table - Actions available in the LOGS tab.

Operations with sub-operations can be extended on the list by clicking on.

Customizing logs list

There is a possibility to customize which columns are displayed, by using Customize table view button . All available columns are listed on the left side of the Action box, while columns currently visible in the Logs list are displayed on the right side. You can drag and drop any column to change order or list of displayed columns. To confirm press Save.

FAMOC M.A.N.A.G.E. MONITORING DEVICES USERS APPLICATIONS ADVANCED

Your session will expire in 59 minutes.

Customize table view

Available columns

Search

All columns selected

Selected columns

Search

- Action ✕
- Model ✕
- Component ✕
- Created on ✕
- Created by ✕
- Last status ✕
- Status ✕
- Message ✕

Cancel Save

Action	Model	Component	Created on	Created by	Last status	Status	Message
Refresh policy	Apple MacBook Air	Policy Default general policy	2019-08-28 08:02:51		2019-08-28 08:02:51	1 1	
Apply security restrictions	Apple MacBook Air	Policy Default general policy	2019-08-28 08:02:42		2019-08-28 08:02:44	1	

Filtering logs list

Filters

Show last:

2 weeks

Records per page:

10

Filter by:

From: 14-08-2019 11:16

2019-Aug						
Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

To:

2019-Aug						
Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Cancel Apply

There is a possibility to filter which operations are displayed, by using the **Filters** button . You can filter operation by various settings:

- **Show last** - if chosen, the system displays only operations from chosen period; possible options to choose are: one day, two days, three days, one week, two weeks, one month and full history;
- **Date range** - you can choose specific dates (with hours and minutes) on calendars from and to which operations will be shown on the list;
- **Filter by operation status** - you can choose status of operations, which you want to see on the list.

Filter by:

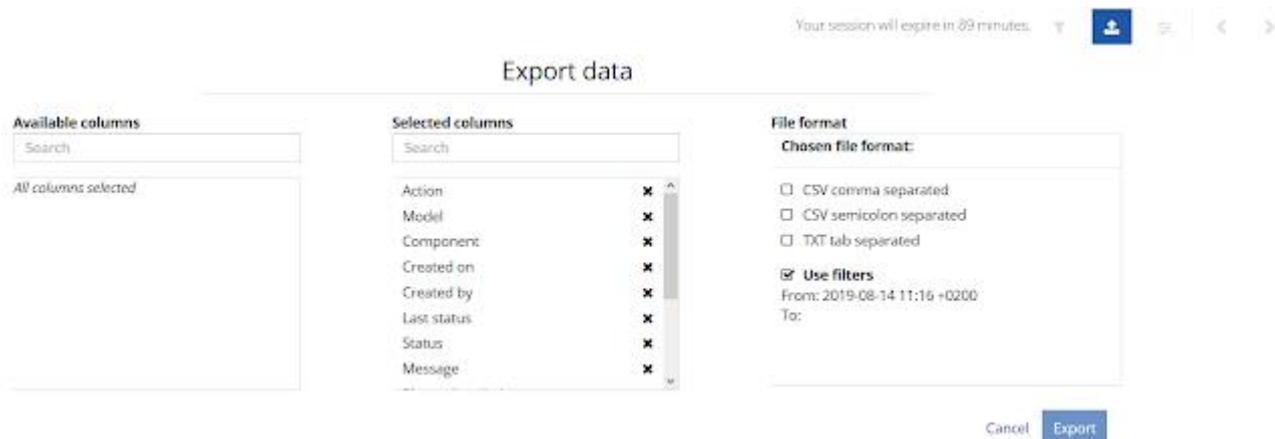


Cancel Apply

Records per page - you can change the quantity of operations shown on a single page.

To confirm settings, press **Save**.

Export logs data to a file



There is a possibility to export logs data by clicking the **Export data** button . You can export data with order of column previously chosen in **Customize table** view options or choose another order of columns by dragging and dropping columns from the **Available columns** and **Selected columns** lists.

You can choose the format of exported file from three options:

CSV comma separated - .csv file, in which records are separated with “,” character;

CSV semicolon separated - .csv file, in which records are separated with “;” character;

TXT tab separated - .txt file, in which records are separated by tabulators.

Use filters checkbox allows you to export data with previously chosen and confirmed filters (e.g. operation status).

To confirm settings, press **Save**.

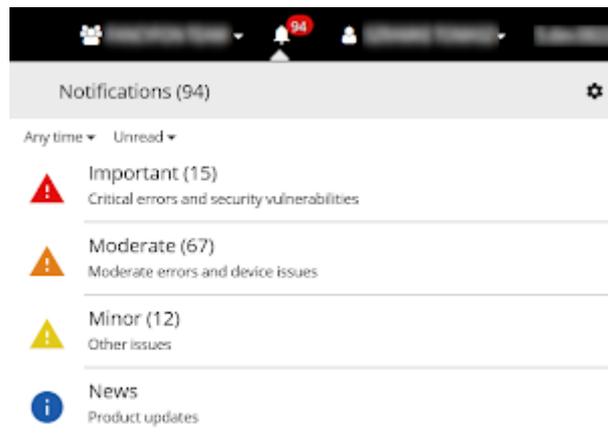
In the logs tab administrator can export operations in a single file only with records, which are displayed on a single page, for exporting operations with many pages, it is necessary to export one

file for each page with records.

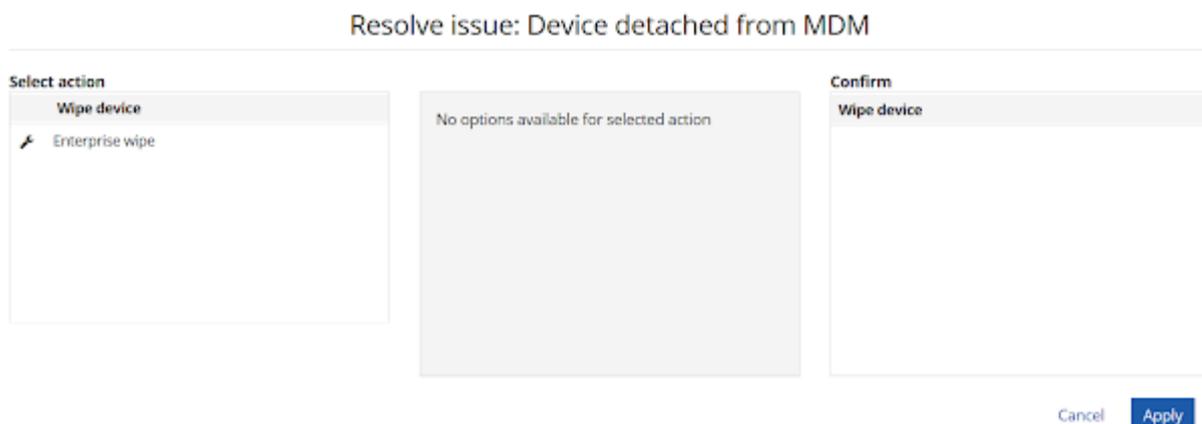
9. NEWS AND NOTIFICATIONS

The Notifications icon located on the top left side of the USER MENU allows the user (with required roles attached) to view and manage issues reported via alerts. The notification system also handles news. This feature informs the user about the recent changes in FAMOC, as well as other important information i.e. server maintenance.

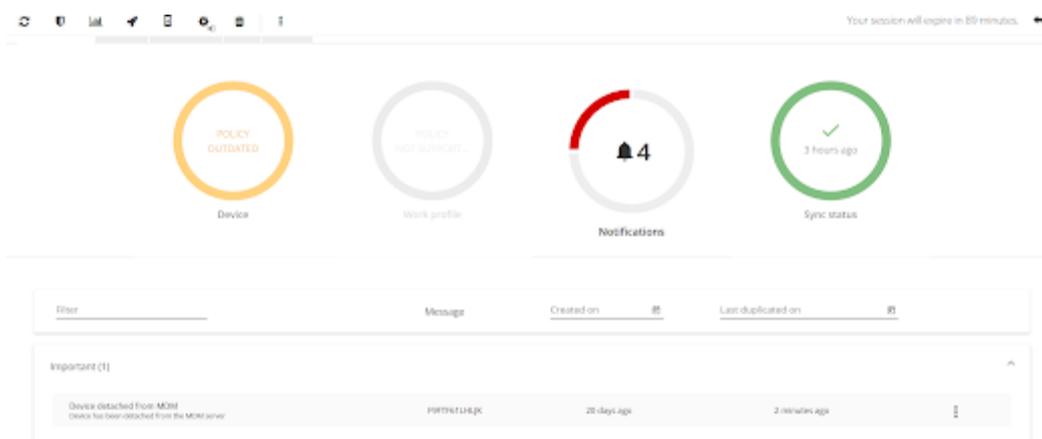
After clicking the icon, the notification panel will appear. Additional options for actions will be displayed on Notifications bar (if one or more items are selected), as well as Settings, which sends the user to the notifications settings tab (within the details panel of the User Menu, see below).



The alerts are grouped by their priority. To see what type of alerts are listed as Important/Moderate/Minor click the specific item on the list. Then you'll see the list of different alerts. By clicking on a specific alert type you'll see what devices are affected by this issue. Depending on the level and alert type, some actions may be taken, such as **mark as read, mark as unread, mark as ignored, resolve issue, show details**. The list of alerts can be filtered by time of occurrence and status (**read, unread, ignored, resolved**) for convenience. Certain alerts can be easily resolved using the resolve issue function and selecting the desired action.



The notification system can also be accessed from the Notifications tab within the device details view. The contents will be automatically filtered to display only alerts generated for the specific device.



10. USER MENU

The user and organization settings can be accessed by clicking the user icon and name on the right side of the menu.

Profile

The profile tab displays details of the currently logged in user and allows him to change his avatar, default organization, name, surname, email address, language, password and two-factor authorization settings if they are enabled for the organization.

Settings

The settings tab displays the organization's details such as the number of managed devices, device limit and the organization's license status. The administrator can also change the organization's avatar here.

Details panel

The details panel allows the administrator to modify certain options, including the organization's language, country, phone number, email address and session timeout. Additionally, log preferences can be set here.

General

General settings are listed in the table below:

Parameter	Description
Language	Possibility to select default language of the organization
Phone	Default phone number for organization
Email	Default email address for organization
Session Timeout	Period of inactivity after which user will be automatically logged out (Default: 90 minutes)
App Store / Google Play app synchronization	Interval of automatic app synchronization from Google Play

interval	and AppStore (Default: 7 days)
SafetyNet API key	If you wish to use SafetyNet attestation, provide a proper API key here.

Enrollment code settings

If you wish to use the enrollment code for the DEP method you can configure it here.

Parameter	Description
Code complexity	You can select to generate Numeric or Alphanumeric codes
Code length	You can define the number of characters in the generated code. Possible values: 6, 8 or 10
Code expiration time	The period during which the codes will be active. Possible values: 30 minutes, 60 minutes, 1 day or 3 days.

After making changes to the above settings, you have the option of saving and deactivating existing codes or updating them.

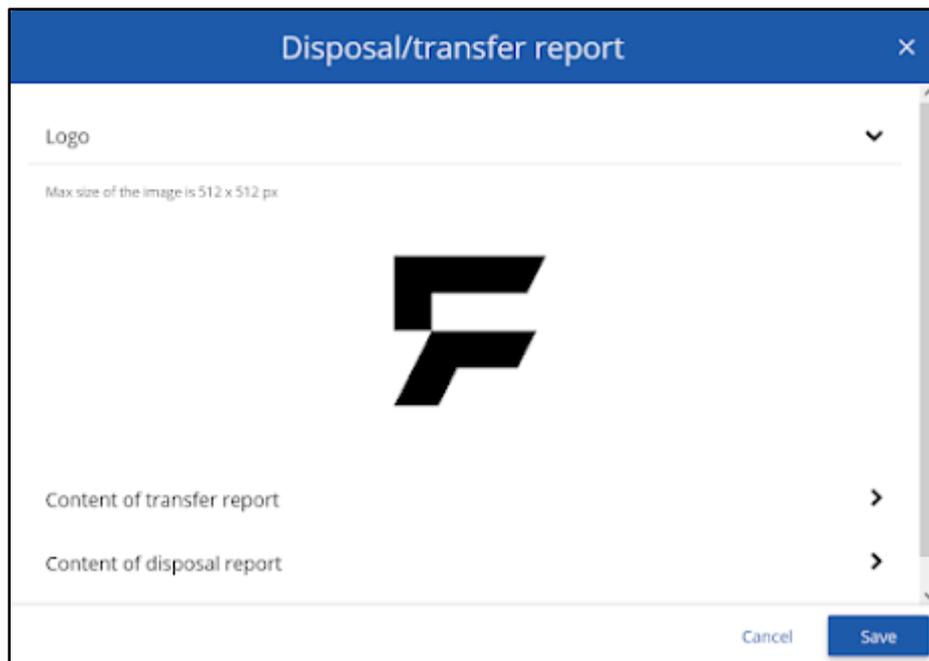
Device operations settings

Device operations settings are listed in the table below:

Parameter	Description
Hide operations executed on deleted devices	If set, operations executed on deleted devices will no longer be displayed in logs.
Hide operations executed before the last enrollment	If set, operations executed before the last enrollment will no longer be displayed in logs.
Default operation timeout	Period during which operation will automatically be retried.

Disposal/transfer report

Click Edit to change the default appearance and content of the devices release / collection protocol.

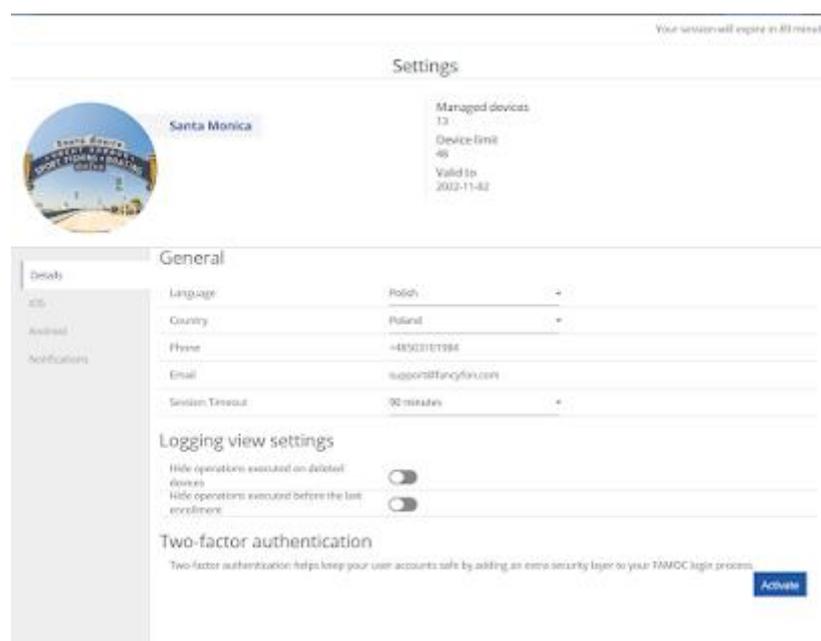


The protocol supports markdown syntax. You can freely edit the content of the protocol using the listed tags. At the moment of generating the protocol, the tags will be replaced with appropriate values taken from the user or device data.

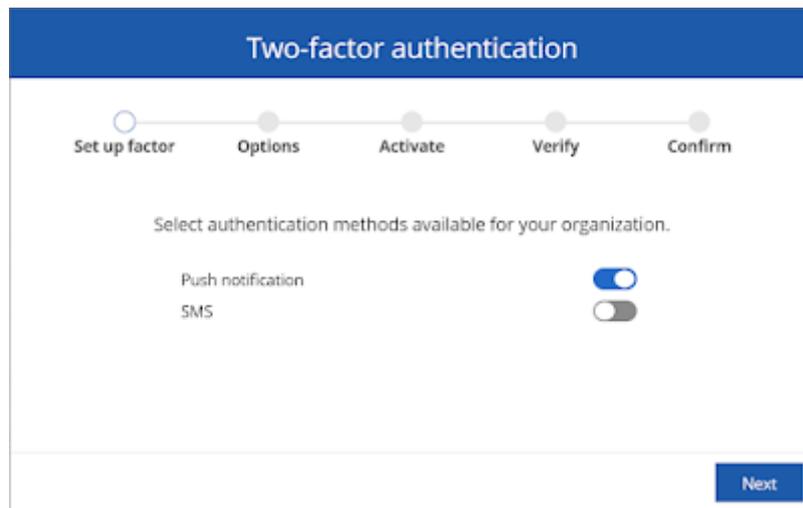
Users & authentication

Two-factor authentication

This function enables using a second factor to log in to FAMOC. The administrator may add an extra layer of protection for the organization.



To enable two-factor authentication, click the **Activate** button. Two-factor authentication window will be displayed.



There is a possibility to choose authentication methods:

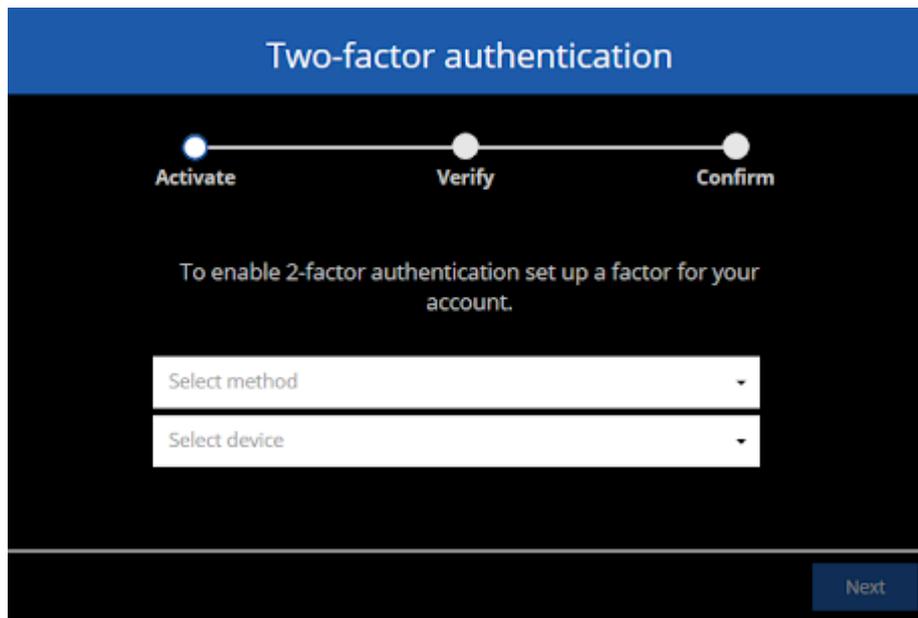
Push notification - user receives message in FAMOC application,

SMS - user gets an SMS message with specific code to confirm login (This method is disabled by default and needs to be activated on the server side. To enable SMS, please contact your FAMOC Server Administrator).

In the next step decide if you wish to **Enforce two-factor authentication for all users in the organization**. verify your method of authentication and, after a successful verification, two-factor authentication will be enabled for the organization and your account as well.



At this point any user in the organization can set up two-factor authentication for login to FAMOC account, either during login (if enforce is enabled) or at any time in the User Profile settings.



Two-Factor authentication on login page



Two-Factor authentication settings in the User Profile

Integration with Azure Active Directory

Integration with Azure Active Directory allows you to import users and groups from the Azure directory to the FAMOC system. The process requires an active account on the Azure portal and the creation of a FAMOC registration on this portal. The entire procedure is described in a separate document available at the [link below](#).



SAML settings

Select if you wish to use SAML protocol for user authentication. SAML protocol enables login via external SSO services such as Okta, Azure etc. After configuring the FAMOC application on the service provider's server, enter the following data:

- X.509 Certificate
- Entity ID
- Login URL
- User XML tag

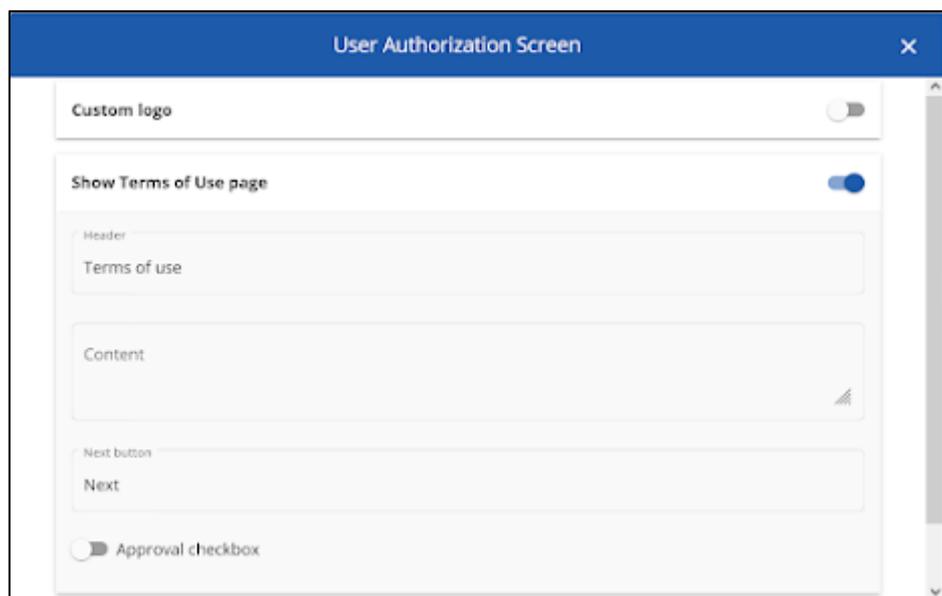
You can also select the option to automatically create users based on login and assign the default role of users created in this way. If you want to map user fields based on saml server data, check the select user field option and choose which field to be completed.

Swivel authentication

If you wish to use Swivel two-factor authentication provide Swivel endpoint and Shared secret (password that must be entered on the Swivel server agent and the device that will be making agent requests).

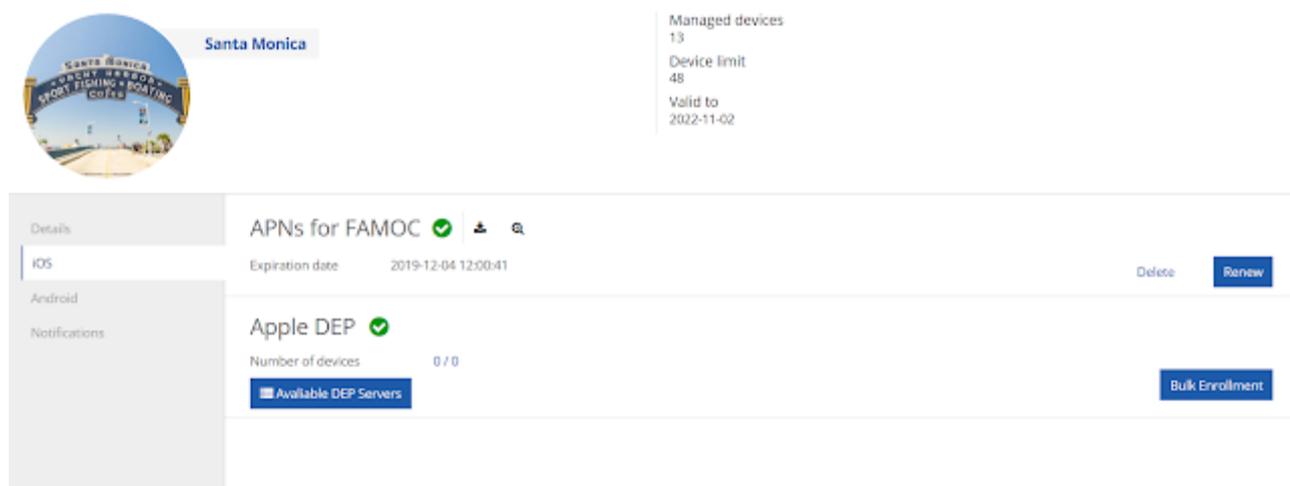
User Authorization Screen

It allows you to customize the content and appearance of the EULA statement (e.g. adding a company logo) displayed during device enrollment.



Apple panel

This panel allows the administrator to manage the Apple Push Notification Service (**APNs**) certificates, Apple DEP enrollment and applications purchased via VPP program.



Santa Monica

Managed devices
13
Device limit
48
Valid to
2022-11-02

Details

APNs for FAMOC ✓

Expiration date 2019-12-04 12:00:41

Delete Renew

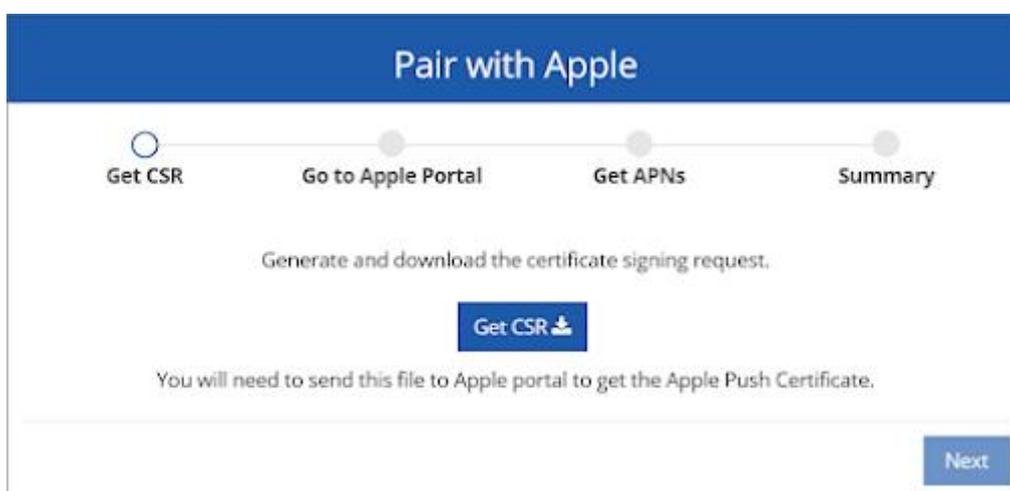
Apple DEP ✓

Number of devices 0 / 0

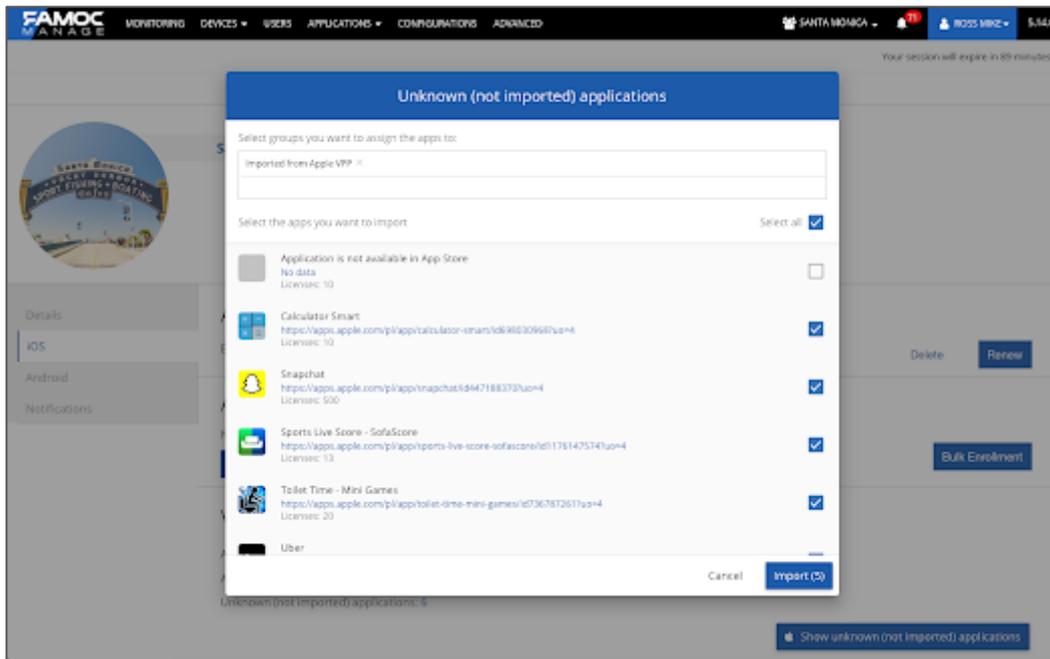
Available DEP Servers Bulk Enrollment

Registering a new APNs certificate

To register a new certificate, you will need a valid Apple ID. Click **GET APNs** to proceed. A **Pair with Apple** window will appear allowing you to download a Certificate Signing Request (**CSR**). Download this file and click **Next** then **Go to Apple portal** (the Apple website will open in a new browser tab). Sign in with your Apple ID credentials and click **Create a certificate**. Click choose file and select the previously downloaded CSR file, then click **Upload**. When the operation is completed click **Download** and save the .pem file. Close the Apple website's tab, this will bring you back to FAMOC and click **Next** in the **Pair with Apple** window. Drag and drop the previously downloaded .pem file into the Upload certificate box and click Next. Enter the email address for the Apple ID used above and click Finish.



In the **VPP licenses** section you can manage iOS applications purchased via VPP program. If you wish to import them to FAMOC, click Show unknown (not imported) applications. It will display a list of all applications with VPP codes. Select the apps by clicking the checkmark on the list and click Import. It is also necessary to provide the name of the group to which the selected applications are to be assigned.



Android panel

Managed Google Play Account	Managed Google Play	Manage Apps	Unenroll
Administrator: fanyfondamian@gmail.com			
Android Zero-Touch	Zero-touch accounts	Bulk Enrollment	
Number of devices: 1/1			
Android Management API ✔	Edit integration settings		
Project identifier: projectamapi-356110 Enterprise identifier: enterprises1.C00.usostm			
Samsung KME	Previous KME synchronizations	Bulk Enrollment	
Number of devices: 0/0			
Samsung E-FOTA	Activate		
E-FOTA lets you control how and when to update firmware on Samsung devices.			
Zebra OTA updates ⚠	Remove integration	Edit integration settings	
ⓘ This service is available for devices running Android Nougat (7.0) or newer with MX 9.2 or higher Registered devices number: 0			

Managed Google Play Account

This section allows you to enroll Managed Google Play Account. Managed Google Play allows you to publish, manage and distribute applications in your enterprise's Google Play Store. Enrollment of Managed Google Play Account is described in detail in a separate document [here](#).

Android zero-touch

This section allows you to integrate a zero-touch account with FAMOC. Android zero-touch allows out-of-the-box automatic enrollment of devices to FAMOC. To integrate FAMOC with zero-touch you will need:

- SSH access to your FAMOC application machine
- Google account

The process is described in detail in a separate document which can be found [here](#).

Android Management API

In this section, you can configure the Android management API if you want to use it. The process is described in a separate article which can be found [here](#).

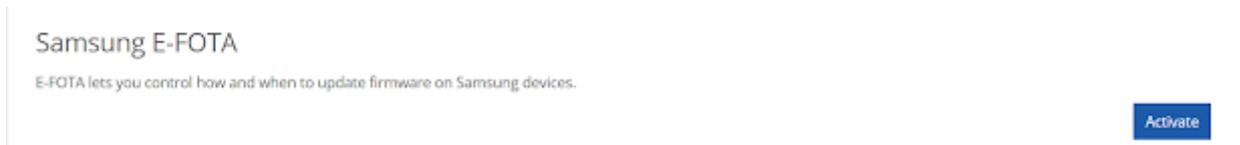
Samsung KME

This section allows you to integrate Samsung KME account with FAMOC. Samsung Knox Mobile Enrollment is a dedicated solution for Samsung devices which allows automatic enrollment to FAMOC. The process is described in detail in a separate document which can be found [here](#).

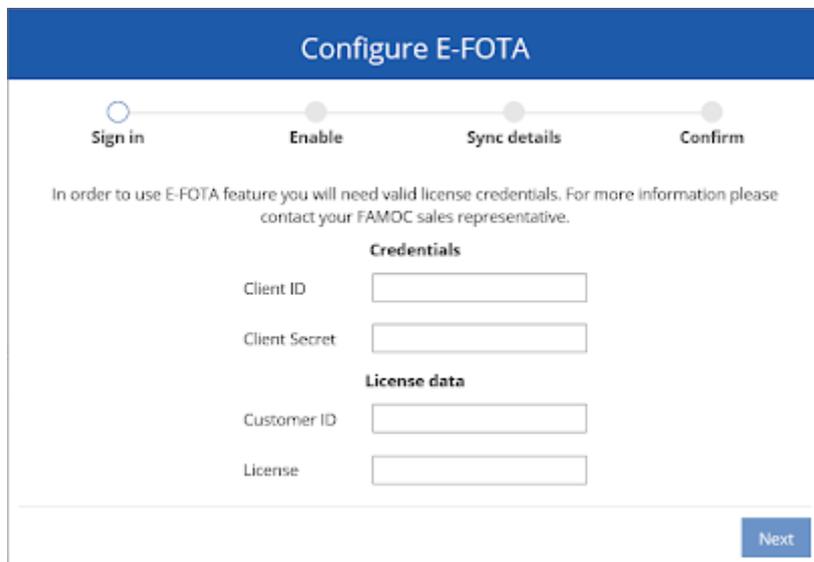
Samsung E-FOTA

Enterprise FOTA (Firmware-Over-The-Air) is a management service that lets you control how and when firmware updates are performed on Samsung mobile enterprise devices.

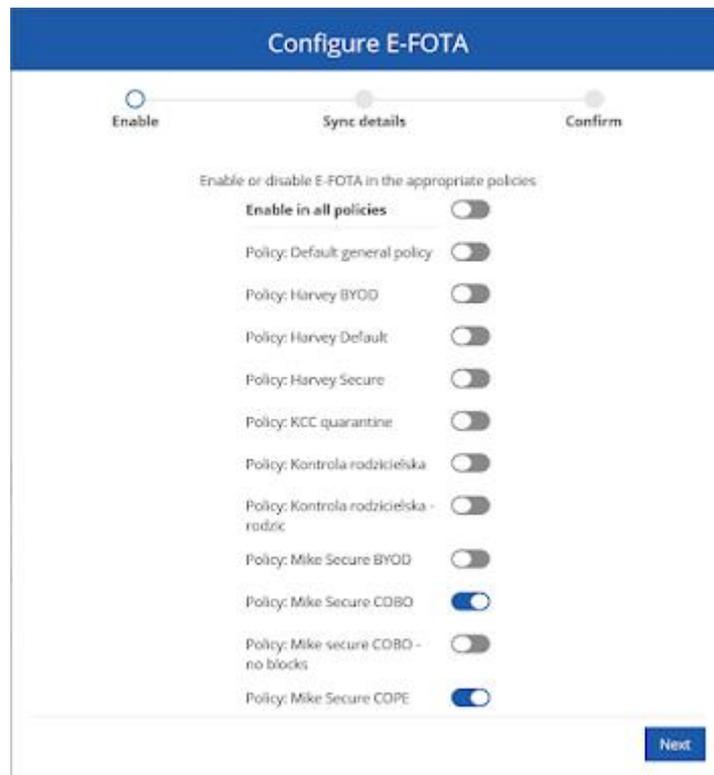
To activate this service go to Settings and enter the Android tab.



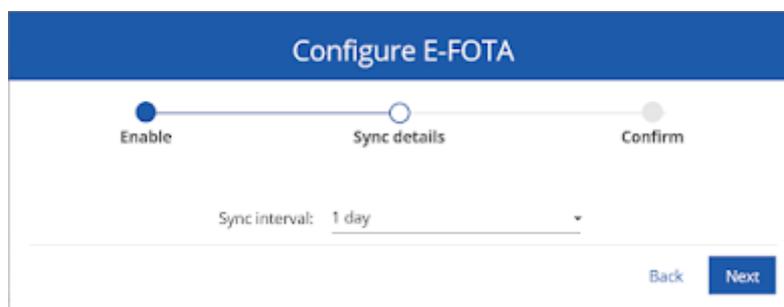
After clicking Activate button go through all steps to configure E-FOTA.



After providing all the credentials you have to define which FAMOC security policies should have the E-FOTA option enabled.



Then decide how often FAMOC will check if the new updates are ready to be downloaded to the specific devices (sync interval).



Now you can finish the process of establishing E-FOTA configuration and check all the available updates for your Samsung devices by clicking Show available updates button.

Samsung E-FOTA ✔

Expiration date: 2019-12-05 00:00:00

Device limit: 22

Last synchronisation: 2019-08-25 01:40:42

Registered devices: 6

Up to date devices: 1

In progress: 0

[Hide available updates](#)

Mark groups with

Phone model	Device count	Current version	Target version	Actions	Release date
SM-G955F Galaxy S8 Plus	1	G955F00LHDSBA/G955FD0MMDGBA/G95...	G955F00LSDSFB/G955F00MMSDGB/G95...	i c	2019-07-30 04:16:23
SM-A510F Galaxy A5 2016	1	A510F00S7CSAZW51DF0XA/CRL2W510F...	A510F00S8CSFA510F0XARCSFA510FL...	i c	2019-07-26 08:22:36
SM-G955F Galaxy S8 Plus	1	G955F00LHDSBA/G955FD0MMDGBA/G95...	G955F00SDSFB/G955FD0MMSDGB/G95...	i c	2019-06-26 06:22:50

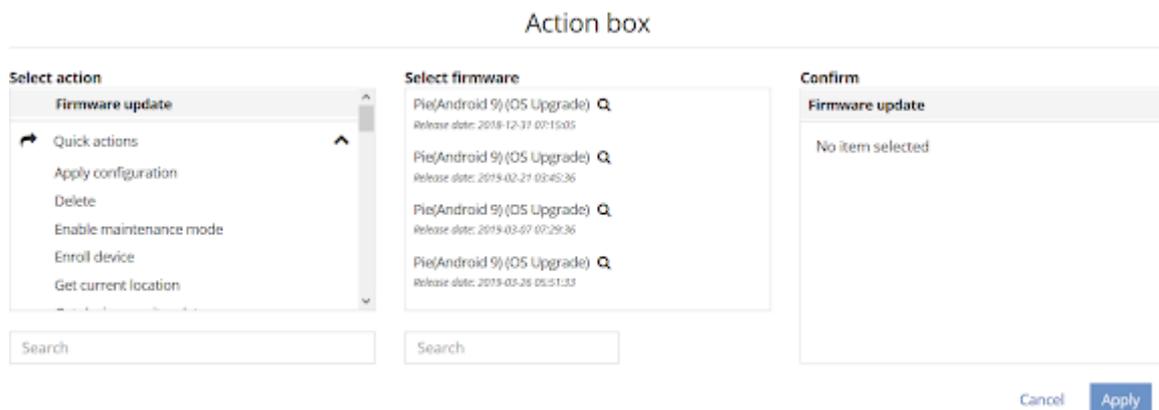
Firmware update via E-FOTA

First of all, please make sure that the security policy with E-FOTA has been refreshed on all assigned devices.

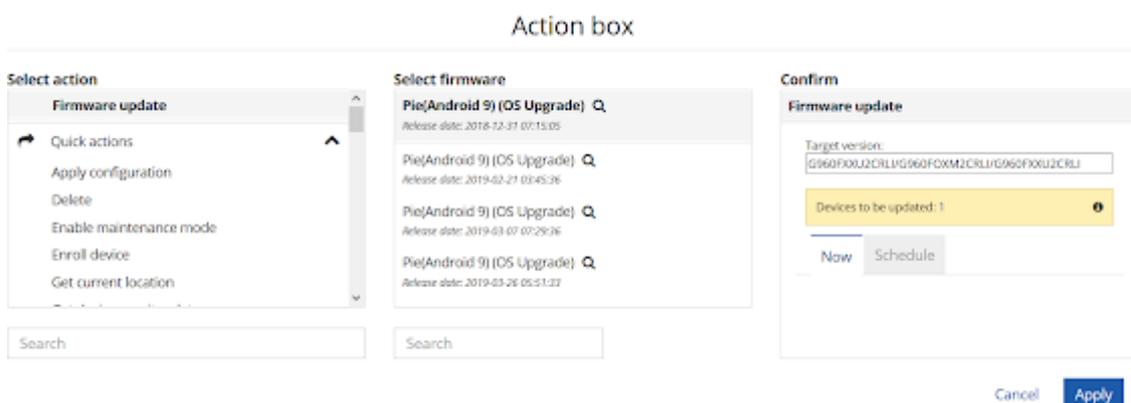
You can perform the firmware update in three ways:

1. Go to the Samsung device view, click More Actions , then go to Quick Actions and select Firmware Update.
2. On a general devices view, mark the left tick box of the device that you want to complete the firmware update on and then click More Actions and proceed as in step 1.
3. Go to Android Panel, expand **Show available updates**, and click .

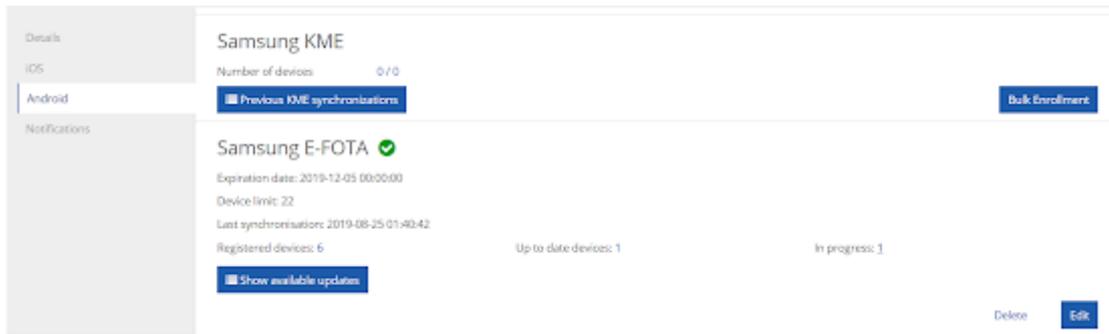
Please note that you can execute the firmware update only on one type of devices (the same model and firmware in the same security policy) at the same time.



After a short while you will see the list of available updates dedicated to your specified type of devices. Select the one you want to implement and decide if the update should be performed now (which means as soon as possible + 3 days) or in the selected min. 3 days peak schedule in the future.



Now you can go to the Settings tab and check how many of your devices are being updated at the moment and how many are up to date.



After clicking on the highlighted number you get a detailed report with all devices' data.

Devices currently being updated

Identifier	Phone model	Platform	User	Description	OS version	Target version	Period	Time Interval
359603080592...	SM-J730F	Android 7.0 - S...	...	Added using D...	J730F00U2ARF...	J730F00U3BRJ...	2019-08-28 - 2...	9:00 - 10:00

Once the firmware update is done, on the updated device there will pop up the information that the device's software has been updated.

Zebra OTA updates

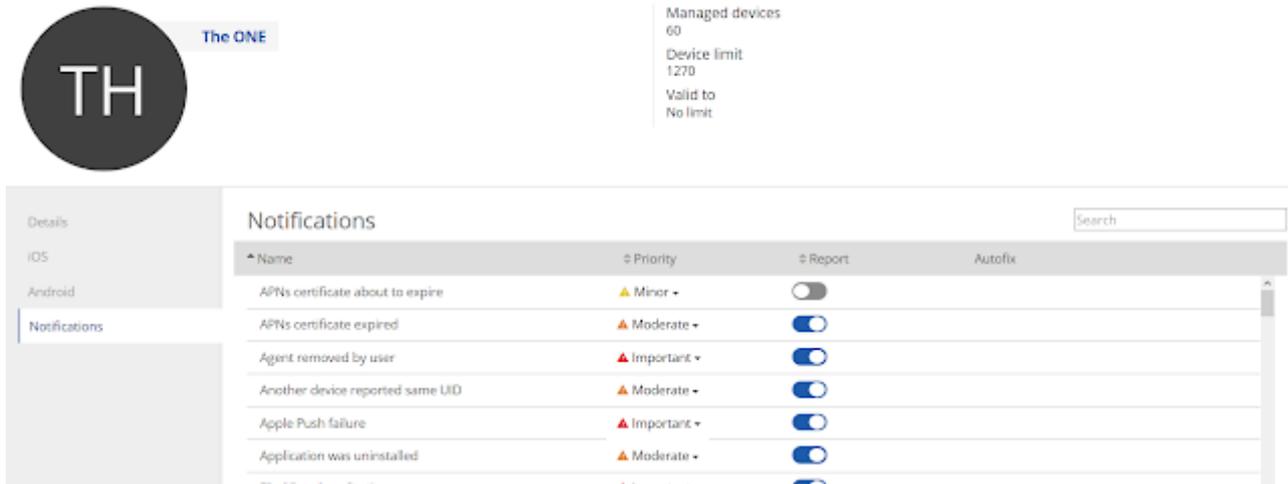
Zebra OTA updates are available for devices running Android Nougat (7.0) or newer with MX 9.2 or higher. To integrate FAMOC with Zebra OTA click **Enable integration**. A modal window will guide you through the process. First, go to Zebra portal and log into your client account. Then, approve integration with verification code copied from FAMOC. During the setup, Zebra Enrollment Manager and Zebra Common Transport Layer app will be imported to FAMOC. Directly from the setup screen it is possible to enable this feature in selected policies (mentioned above apps will be automatically installed and configured on compatible devices assigned to the selected policies).

Once it is done the integration is complete. From now on you will have a possibility to update Zebra devices remotely once any update is made available from the manufacturer. You also have a possibility to upload your own update by using Upload your own update³.

Notifications

In this section a user (with required role attached) can review and manage the settings for the notification system relating to issue alerting, such as disabling and enabling the reporting of each alert, as well as changing each alert's priority.

³ You can read more about Zebra OTA integration in a separate document available at support.famoc.com.



Managed devices
60

Device limit
1270

Valid to
No limit

Notifications

Name	Priority	Report	Autofix
APNs certificate about to expire	Minor	<input type="checkbox"/>	<input type="checkbox"/>
APNs certificate expired	Moderate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Agent removed by user	Important	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Another device reported same UID	Moderate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Apple Push failure	Important	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application was uninstalled	Moderate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Blacklisted application	Important	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

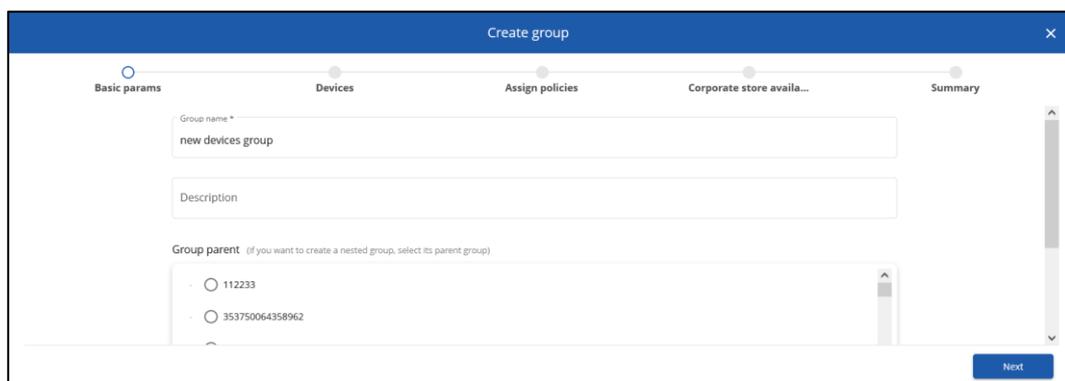
Groups

This tab allows you to manage all the groups in your organization - Users, Devices or Applications.

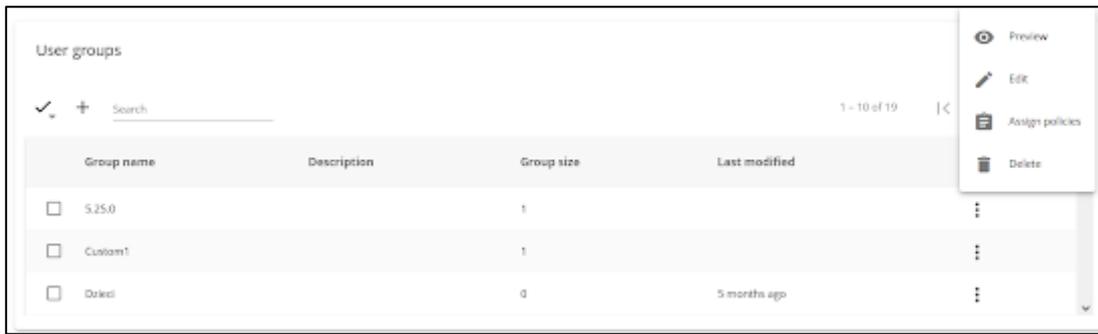
Clicking on the arrow will expand the list of groups. In the displayed table you will find basic information such as Group name, Description, Number and Date last modified.

After expanding the list of groups, we can add a new group by clicking the plus icon. It will open a modal window which will guide you through the process:

1. Basic params - provide the name of the group and its description. If you want to create a nested group, please also select the parent group.
2. Users/Devices - add users or devices to the group by clicking the checkboxes
 - a. Roles - for Users groups you can assign Role for all members of the group
3. Assign policies - assign the policy which will be applied for all members of the group
4. Corporate store availability - select which applications and configurations will be available for all members of the group
5. Summary - displays a summary with all the details of the created group.



We can also edit or delete groups by clicking on the three dots icon next to a specific group.



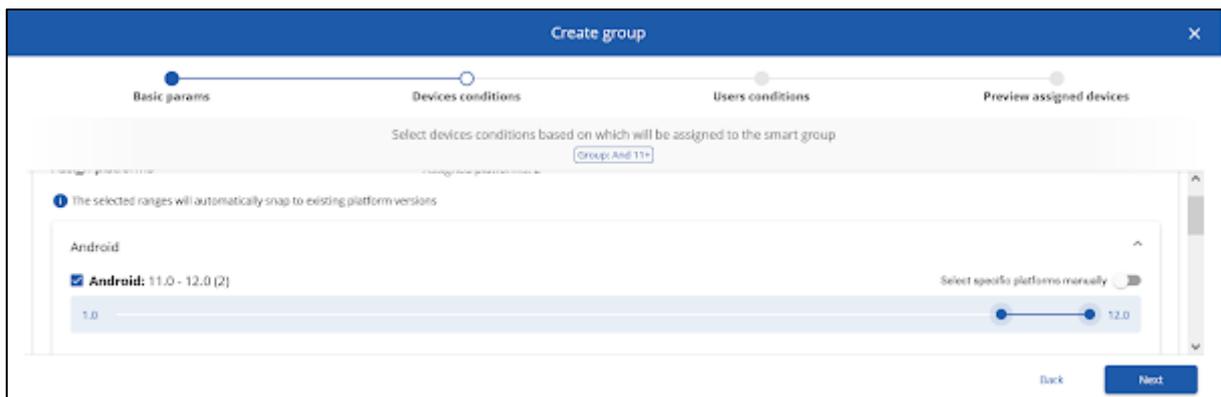
Smart groups

Smart groups is a method that allows you to automatically assign a device to a given group based on specific parameters. Assignment is dynamic, which means that if the device parameters are changed (e.g. system version change after updating), the device will automatically change the assigned group.

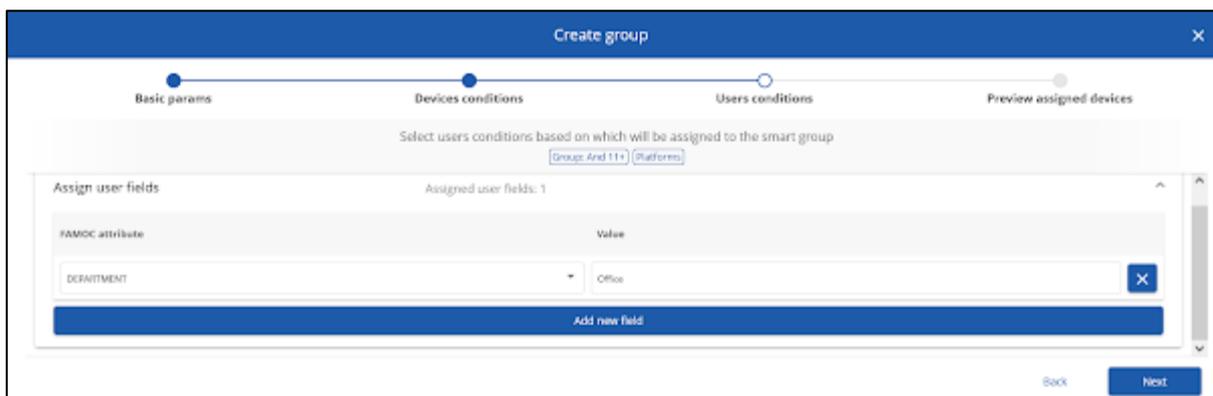
To define a smart group, expand the list and click the plus icon.



In the next step, define the group parameters. The example below shows creating a group for devices with Android 11 or later.

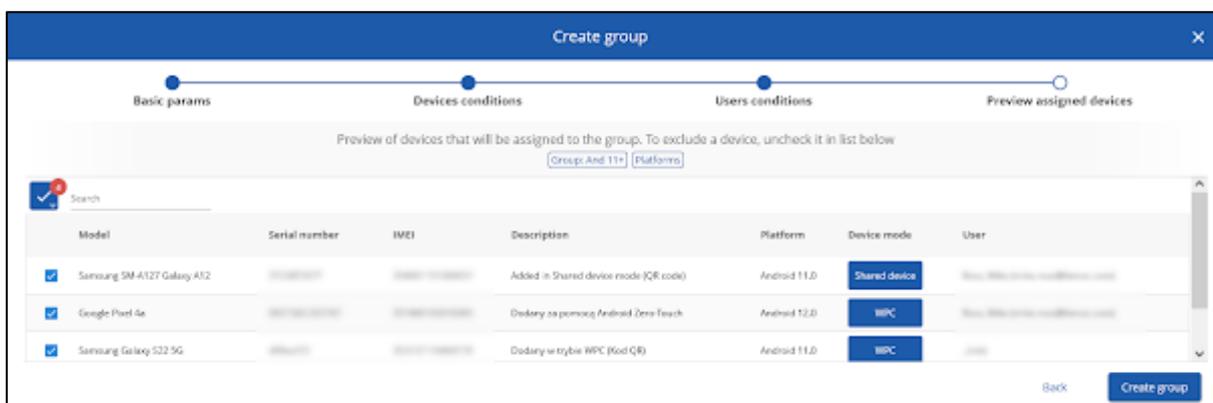


Additionally, you can define user parameters based on which devices will also be assigned to the group. For example, they can be all devices of employees from the Office group as in the example below.



In the last step, a preview of all devices that meet the defined parameters will be displayed and, on this basis, will be assigned to the newly created group.

To confirm your selection, click Create group.



Translations

To add new translation go to the Translations tab. Enter the name of the new language and click **Save**. New language version will be now displayed on the list.

Language	Status	Translation status	Assigned organizations	Assigned users	Last change	Import	Actions
English (Default language)		100%	1	13	2019-12-05 12:03:03		
Dutch		95.00%	3	15	2019-12-05 12:04:03		
German		1.04%	0	0			
<input type="text" value="Angerški"/>		0%	0	0		<input type="button" value="Import"/> New hybrid language	<input type="button" value="Export"/> <input type="button" value="Disable"/>
<input type="text" value="Pisny"/>		0%	0	0		<input type="button" value="Import"/> New hybrid language	<input type="button" value="Export"/> <input type="button" value="Enable"/>
<input type="text"/>							
<input type="text"/>							
<input type="text"/>							
<input type="text"/>							
<input type="text"/>							
<input type="text"/>							

You can import or export translation files in .csv format. New translation will be available for selection in user menu once you click **Enable**.

You can select the language from the left side menu and manually edit specific fields.

Languages

Angielski

New

| << | < | 1 | 2 | 3 | ... | 10 | ... | 20 | ... | 30 | ... | 100 | ... | 200 | ... | 300 | ... | 510 | all (12743) | > | >> | 25 items per page

English	New	
English	New	
Build version	<input type="text"/>	<input type="button" value="Save"/>
- Functionality supported from iOS 5.x	<input type="text"/>	<input type="button" value="Save"/>
- Functionality supported from iOS 6.0	<input type="text"/>	<input type="button" value="Save"/>
already exist	<input type="text"/>	<input type="button" value="Save"/>
Already exists The requested Add command failed because the target already exists.	<input type="text"/>	<input type="button" value="Save"/>
already exists.	<input type="text"/>	<input type="button" value="Save"/>
Available	<input type="text"/>	<input type="button" value="Save"/>
Command failed Non-specific errors created by the recipient while attempting to complete the comman	<input type="text"/>	<input type="button" value="Save"/>