

# FAMOC<sup>®</sup>

## FAMOC Admin Guide



[www.famoc.com](http://www.famoc.com)

## PUBLISHED BY

Famoc Software Limited  
Atrium Business Centre  
The Atrium, Blackpool Park  
Cork, Ireland

Copyright© 2008-2021 by Famoc Software Limited

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 Limited.

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.



**Table of Contents**

<b>About This Guide</b>	<b>5</b>
<b>What Is FAMOC?</b>	<b>6</b>
<b>FAMOC Components</b>	<b>7</b>
FAMOC Server	7
FAMOC Client Components	7
<b>Security</b>	<b>8</b>
<b>Customer Device Compatibility</b>	<b>8</b>
<b>FAMOC Administration Console</b>	<b>9</b>
<b>Using FAMOC</b>	<b>10</b>
<b>Adding New Organization/Department</b>	<b>11</b>
Organizations	11
Admins	12
Role Templates	13
Custom fields	14
Translations	15
Server status	15
<b>FAMOC Wizard</b>	<b>16</b>
<b>Adding New Users</b>	<b>17</b>
Adding Single Users	17
Adding Multiple Users (Import)	19
Server Synchronization	20
<b>Organization</b>	<b>22</b>
Users	22
Org. Details	22
User details	22
Groups	22
Adding Single Groups	22
Adding Multiple Groups (Import)	23
Imports	24
LDAP Import	24
File Import	24
Import Schemas	25
Dictionaries	25
Roles	25
<b>Monitoring</b>	<b>26</b>
<b>Device Inventory</b>	<b>26</b>

Adding Single Devices	28
Adding Multiple Devices (Import)	29
Working with Single Devices	29
Device Details	30
Users	30
Applications	30
Policies	31
Agents	31
Alerts	32
Log	32
Location	32
Security	32
Backup	33
Data backup/restore	33
Data import	33
SIM Cards	33
Device Monitor	33
Repairs	34
Usage data	34
Recorded connections	34
Installing Certificates and Base Agent on Individual Devices	34
<b>SIM Cards</b>	<b>35</b>
<b>Config Center</b>	<b>36</b>
Agents	37
Certificate Installation	37
FAMOC Agent Installation	38
Application	40
Adding applications from Apple App Store	40
Adding applications from Google play	40
Adding custom applications	40
Managing Application Groups	42
Installing Applications on Mobile Phones	42
Configurations	42
Adding Configurations	44
Sending Configurations to Mobile Phones	45
Messages Tab	45
Backup Tab	45
<b>Remote Access</b>	<b>46</b>
Remote Access Installation	46
Remote Access tab	47
Remote Access Panel	47
Device Monitor	48
File Manager	49

Configuration	49
<b>Log</b>	<b>49</b>
<b>Location</b>	<b>50</b>
<b>Alerts</b>	<b>50</b>
<b>Settings</b>	<b>51</b>
Policies	52
Alerts	53
Alerts Types	53
Alert Forwarding	53
Blacklisted Applications	54
Whitelisted Applications	55
Servers	55
System advanced	59
Enrollment	60
Custom Fields	62
Configuration Types	63
Reference Policies	63
Apple Certificates	63
VPP Settings	64
iOS DEP settings	65
Apple Configurator	67
Exchange proxy	67
External compliance checker	68
Manage Application Groups	69
Manage Device Groups	69
Android Enterprise settings	70
Knox Mobile Enrollment settings	70
Reports	71
Available operations on reports	72
<b>Additional Information</b>	<b>73</b>

## 1 About This Guide

After reading this administrator's guide, you will be able to:

- Understand how and why FancyFon Mobility Center(FAMOC™) can help you
- Understand how FAMOC will work for your company, end-users or your customers
- Identify the main FAMOC components and features
- Create multiple, separate organizations / departments within the FAMOC server and grant diverse management prerogatives to different system administrators
- Customize the FAMOC console by e.g. adding new system translations and custom fields, preparing package operations corresponding to specific company needs, or changing FAMOC Agent configuration
- Add single users and devices to FAMOC or perform bulk imports via server synchronization, or file import and data mapping
- Remotely manage end-users' devices (install applications, perform over-the-air configurations, initiate data backup, etc.)
- Gain an overview of the mobile infrastructure, monitor device parameters, instantly identify failures, and troubleshoot devices using dashboard, inventory, action log, alerts and reports
- Make a connection to a customer's phone using FAMOC Remote Access
- Use Location Monitor to locate devices and users
- Monitor server status and FAMOC licenses
- Know where to look for more detailed information and support

## 2 What Is FAMOC?

FAMOC is a comprehensive solution enabling users to remotely manage any number of mobile devices over the Internet. Company administrators as well as service providers can use FAMOC to ensure instant remote support to end users and employees.

FAMOC manages any mobile device running Android OS, iOS, Windows Phone 8, Windows Mobile 5.x & 6.x or higher, Symbian OS v9.x (both S60 and UIQ platforms), BlackBerry devices starting with OS version 4.3, Java feature phones with the appropriate Java Mobile Edition enhancements (see FAMOC Functionality Matrix).

FAMOC provides comprehensive mobile device lifecycle management and an unparalleled level of security support. The system's functionality is divided into five main building blocks:

### **Asset management**

FAMOC detects all assets within the mobile fleet, and stores all collected data, providing a library of information on company assets, including hardware, software, SIM cards, users and processing information. FAMOC Asset Manager gives a real time view into the organization's mobile environment, and is a highly useful resource for future planning.

### **Configuration management**

FAMOC enables administrators to perform all tasks related to over-the-air configuration provisioning, and supports a wide array of devices and operating systems. The solution tracks data for both individual assets and the entire system (version and model number, baseline performance, relations to other assets), empowering the remote configuration of parameters and corporate policy deployment.

### **Application management**

FAMOC automatically discovers and reports on the organization's mobile device inventory, providing a real-time view of the health and usage of all applications. Moreover, it synchronizes data stored on mobile devices to provide backup and common access to shared resources, and enables remote administration as well as over-the-air data synchronization.

### **Security management**

FAMOC provides an unparalleled level of security support across multiple mobile platforms, managed centrally, over the air. The solution ensures secure communication between the server and mobile devices, protecting stored data and enabling the seamless deployment of corporate policy.

### **Remote access**

FAMOC Remote Access is a highly secure and easy to use solution that troubleshoots mobile devices remotely, empowering the administrator to take remote control of mobile devices over a data connection (e.g. GPRS/EDGE/3G, WiFi), to view the device screen and use the device keyboard over the air.

### **What Will You Gain With FAMOC?**

- Remote control over smartphones
- Reduced support costs
- Increased user satisfaction
- Accelerated adoption of new services
- Better troubleshooting and a decrease "no trouble found" device returns
- Proven helpdesk technology
- Ability to solve difficult issues for your highly valued customers

## 3 FAMOC Components

FAMOC consists of a number of components designed to enable the efficient management of a mobile device through its lifecycle.

### 3.1 FAMOC Server

The FAMOC server is at the heart of the solution, providing the device inventory, managing communication with mobile devices, and handling the administration sessions via a web-based GUI. FAMOC server components may consist of more than one physical server, depending on the configuration, additional fail-over, load-balancing or database server may be included. Please contact [support@fancyfon.com](mailto:support@fancyfon.com) for more information.

### 3.2 FAMOC Client Components

Agents (software applications) that are installed on smartphones communicate with the server via secure data connections. Various agents perform different functions. A short description of individual agents can be found below.

#### **Base Agent**

The Base Agent is responsible for installing and uninstalling applications, configuration deployment, device wipe and the launching of applications including other FAMOC agents. It also ensures that appropriate security configurations are in place on the device. Functions include locking the Bluetooth connectivity on the phone, banning the user from installing applications, and restricting access to certain applications on the device. Base Agent also collects details about device parameters such as a WLAN Mac address, running processes, installed applications and many more.

#### **Backup Agent**

Backup Agent means that copies of data from mobile devices can be centrally stored on the FAMOC server and easily restored after data has been lost or a device has been replaced.

#### **Remote Access**

Remote Access allows the administrator to connect to a mobile device and control the keyboard and screen remotely. Administrator can also browse through the file system remotely, as well as download and upload files to and from a mobile device, over the air.

#### **Location Monitor**

Location Monitor tracks and locates end users' mobile devices.

#### **Usage Monitor**

Usage Monitor monitors and reports user activity to the FAMOC server.

## 4 Security

FAMOC addresses the following security concerns:

- By default, FAMOC is based on standard HTTPS, which means that no extra ports on corporate firewalls need to be opened for FAMOC to function. The Remote Access function needs one additional port enabled on firewalls – this port is configurable and can be adapted to specific needs.
- Encrypted connection is established between the administrator and customer, using well established Internet protocols (256-bit SSL).
- Support sessions are initiated by a customer: The administrator cannot examine a customer's device without being invited to do so by the customer, or without the user's explicit consent.
- Once the support session has ended, all access rights to the customer's device are removed.
- Sessions can be recorded to provide an audit trail of the administrator's actions.

## 5 Customer Device Compatibility

- Android (phones and tablets)
- Apple iPhone and iPad
- Apple tvOS, MacOS
- Microsoft Windows Phone 8 and Windows Phone 8.1
- Windows 10 Mobile
- Windows 8.1+

For more detailed information on compatibility see the *FAMOC Functionality Matrix*.

## 6 FAMOC Administration Console

The administration console is used for functions such as security settings, user authentication, communication, logging, and reporting.

1. To login to the FAMOC server, direct your browser to `https://<your server address>`

Use your Login and Password provided by your administrator.

2. After logging in, the device inventory of the current organization is displayed.

**NOTE:** First log in requires approval of "FAMOC End User License Agreement".

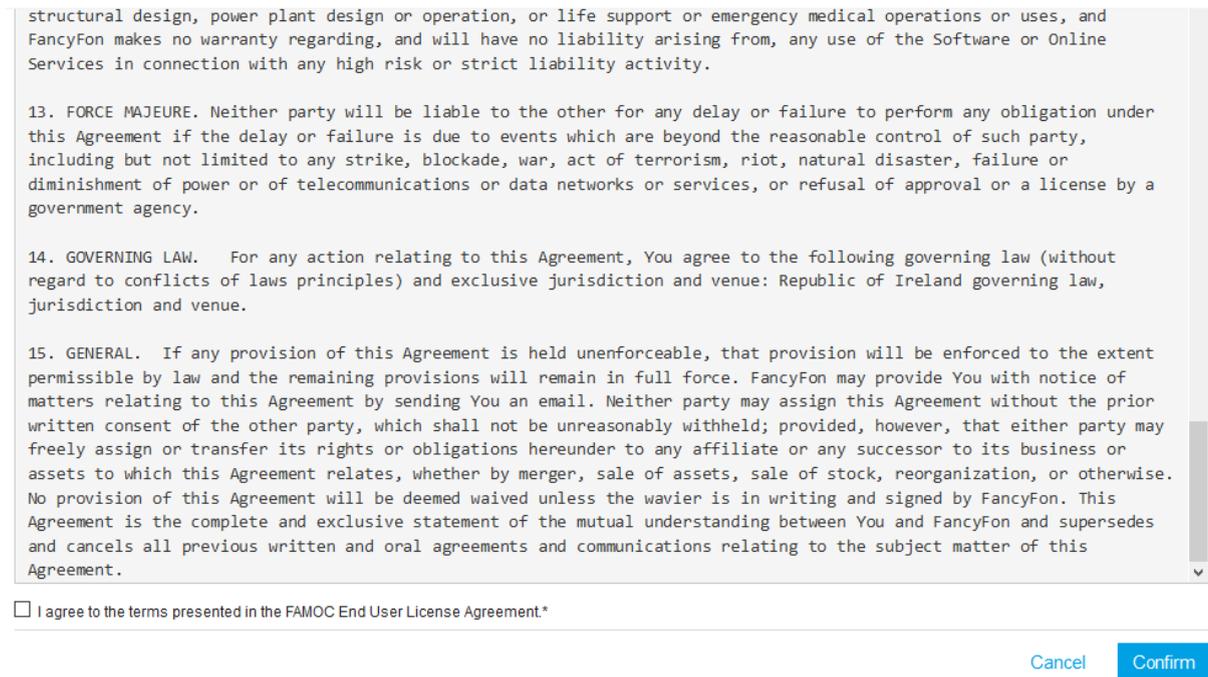


Figure 1 End User License Agreement

Go to **ADVANCED** Famoc view.



The top menu bar includes three entries **MANAGEMENT**, **ADVANCED** and **ORGANIZATION**.

**ORGANIZATION** allows managing users, groups and their privileges to access FAMOC functions.

**ADVANCED** provides access to the Mobile Device Advanced specific functionality.

**MANAGEMENT** leads to the new interface.

## 7 Using FAMOC

Below you will find a brief description of all FancyFon Mobility Center tabs.

ORGANIZATION	
<b>Users</b>	Add new users and grant them access to ORGANIZATION and FAMOC
<b>Org. Details</b>	Insert and modify company details

<b>User Details</b>	Edit user details such as name or language, and change the login and password
<b>Groups</b>	Create groups, assign users to groups. (This is useful when managing a large number of handsets.)
<b>Imports</b>	Import files, schemas or users, using OpenLDAP server, Active Directory server or file import
<b>Dictionaries</b>	Create additional dictionaries enabling more comprehensive description of devices and SIM cards added to the system. (This option is useful when using the advanced search function)
<b>Roles</b>	Create role templates with pre-defined user privileges
<b>ADVANCED</b>	
<b>Monitoring*</b>	New GUI feature. Customizable overview of FAMOC reports, showing current status of the system, giving general information of FAMOC and managed devices
<b>Devices</b>	Add single devices or bulk import of devices. Perform agent installations and show device details
<b>SIM cards</b>	List of all the SIM cards included in the FAMOC system
<b>Config center</b>	Management of agents, profiles, applications, configurations, operations, SMS and packages. Descriptions of the individual tabs can be found below
<b>Remote access</b>	Take remote control of phones registered with FAMOC
<b>Log</b>	Overview of operations performed on phones
<b>Location</b>	Track and locate users' mobile devices
<b>Alerts</b>	Insight info alerts reported to the system
<b>Settings</b>	Synchronize external servers with FAMOC, define custom fields and settings for FAMOC client components
<b>Reports</b>	Generate reports based on statistics included in FAMOC
<b>MANAGEMENT*</b>	
<b>Monitoring</b>	Customizable overview of FAMOC reports, showing current status of the system, giving general information about FAMOC and managed devices
<b>Users</b>	New users management tab
<b>Devices</b>	New device management tab
<b>Applications</b>	New application management tab
<b>Advanced</b>	Leads to more advanced functionalities of FAMOC
<b>Server management</b>	FAMOC UI translations tab is available under this tab

Table 1 FAMOC tabs

\* See FAMOC UI Guide to learn more about the new interface separate document:

## 8 Adding New Organization/Department

The FAMOC administrator may be allowed to create, edit and delete FAMOC organizations and administrators. If the FAMOC administrator is granted such privilege, when logging in to the system, and clicking the  icon, several server management tabs will be displayed:

- **Organizations** – allows new organizations/departments to be added FAMOC. Creating a FAMOC organization means creating a separate space/unit on the FAMOC server with an appropriate group of users, an administrator, and an adequate set of management prerogatives
- **Admins** – allows users to be granted access and management prerogatives to the newly created organizations
- **Roles** – allows new administrative roles to be added to FAMOC (sets of management prerogatives)
- **Custom fields** – allows to add custom fields for the organization
- **Translations** – allows new language versions to be added, by translating FAMOC tabs, subtabs and commands
- **Server status** – provides detailed information on service status, server licenses and SSL certificates

If an administrator is granted access to a number of departments, this section allows you to switch between them

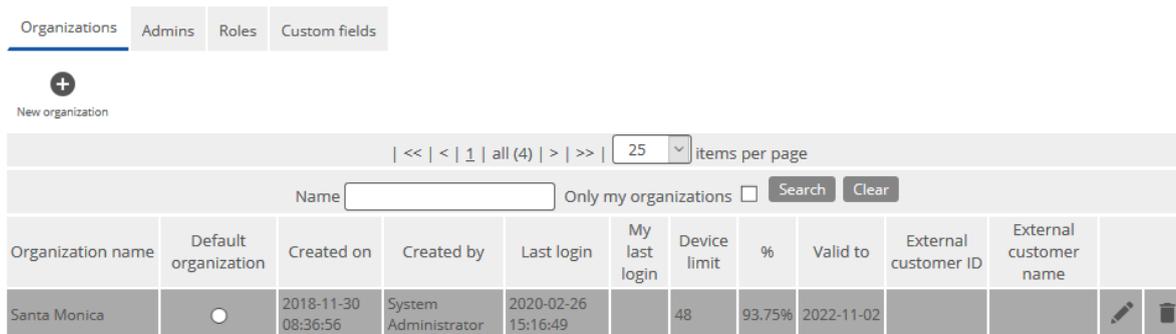


Figure 2 Adding organizations

### 8.1 Organizations

1. To create a new FAMOC organization, press the **New organization** button.
2. Define company/unit name, introduce the necessary data and grant organization administrator adequate management privileges by marking the correct role(s). The system provides four default templates:
  - **FAMOC Administrator** – grants full access and management powers
  - **FAMOC Security Manager** – grants access to security restrictions deployment and management

- **FAMOC Asset Manager** - grants access to information on company assets, including hardware, software, SIM cards, users and processing data
  - **FAMOC Group Manager** – grants access to manage specific groups of users and devices
  - **FAMOC Web Services** – gives access to the organization’s web services
3. Additional settings for organization:
- **Hide operations executed on deleted devices** - hides deleted devices entries in the log tab.
  - **Hide operations executed before the last enrollment** – hides entries in the log tab for operations executed before the last enrollment.
  - **Enable FAMOC Lite mode in organization** - for more information about FAMOC Lite please refer to the “FAMOC Lite Guide”.
4. To assign an administrator to the newly created organization, input their login and password in **Organization admin** tab. The password should be changed when the administrator logs in to their unit for the first time.
5. To finish, press **Save**.

The screenshot displays the 'Organizations' tab in the FAMOC Admin interface. At the top, there are navigation tabs: 'Organizations', 'Admins', 'Roles', and 'Custom fields'. Below these are 'Back' and 'Save' buttons. The main section is titled 'New organization:' and contains a form with the following fields: Name (text input), Country (dropdown menu with 'Select country ...'), Default language (dropdown menu with 'English'), Province (text input), City (text input), Street (text input), Postcode (text input), E-mail (text input), and Phone number (text input). Below the form are 'Additional settings' with three checkboxes: 'Hide operations executed on deleted devices', 'Hide operations executed before the last enrollment', and 'Enable FAMOC Lite mode in organization'. At the bottom, there are two tabs: 'Roles' and 'Organization admin'. The 'Organization admin' tab is selected, showing a list of roles: 'Roles', 'FAMOC Administrator', and 'FAMOC Security Manager', each with a 'View details' link.

Figure 3 Adding new institution

## 8.2 Admins

The **Admins** tab enables administrative users to be added to FAMOC, and provides comprehensive details on FAMOC administrators, such as login, name, surname, default organization, and a list of organizations they have access to. This section allows additional management privileges to be granted, extending or limiting powers of access to additional organizations, or deleting a user.

Figure 4 FAMOC admins

## 8.3 Role Templates

The **Roles** tab allows the administrator to create role templates with pre-defined sets of privileges, and attribute them to different organizations so that it will be available for selection while managing these organizations.

To add a new role to FAMOC:

1. Press **Add role** in the **Roles** tab.
2. Input **Name** and **Description** of the role.
3. Use the **Select** button to create a list of organizations for which the template will be available for selection.
4. To assign management and access prerogatives, mark the checkboxes in the **Privileges** table.
5. To finish press **Save**.

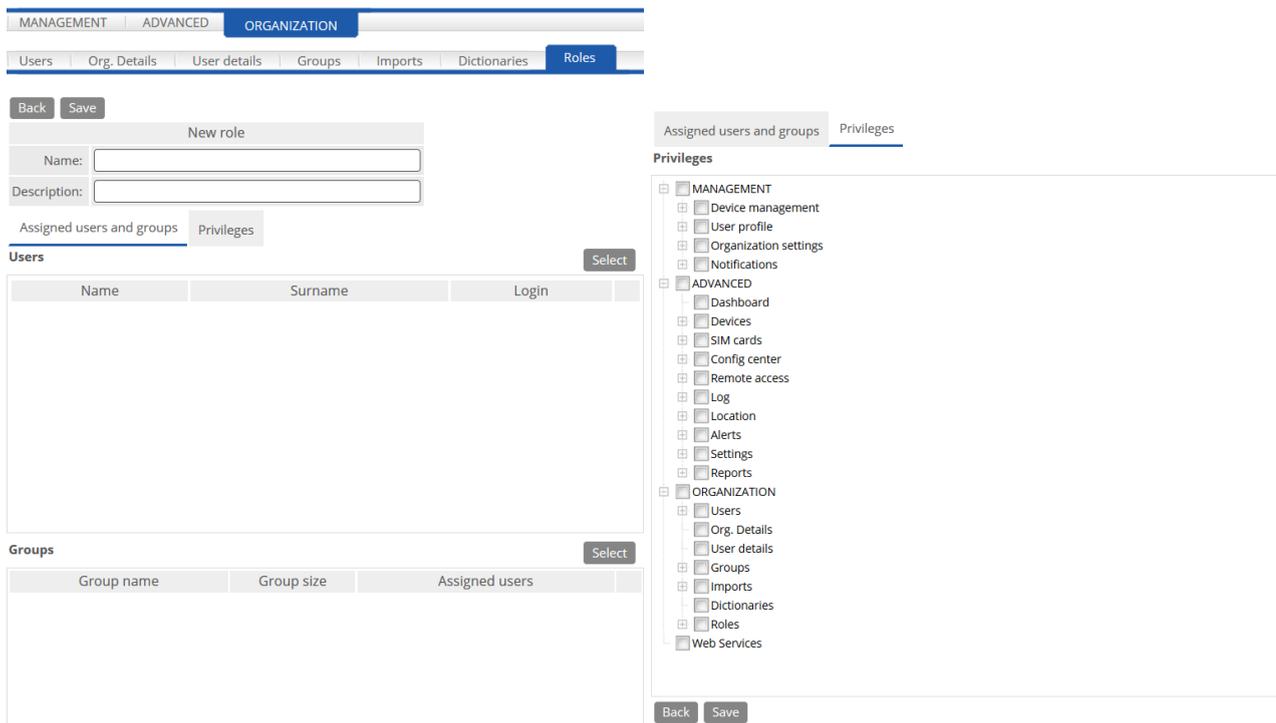


Figure 5 FAMOC role templates

## 8.4 Custom fields

The Custom fields tab allows the administrator to create fields for the organizations. When creating custom field, administrator can select:

- **Name:** name of the custom field
- **Table:** Organization or License
- **Type:** text, number, date, password

To add a Custom field:

1. Press **Add custom field** in the **Custom fields** tab.
2. Input **Name** of the custom field.
3. Select **Table** and **Type**.
4. To finish press **Save**.

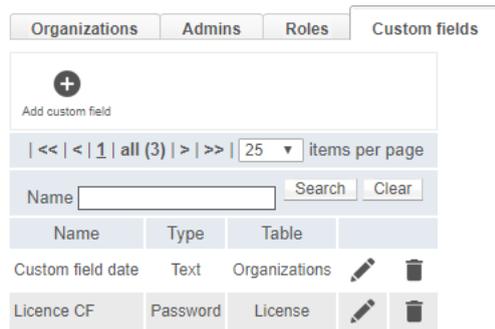


Figure 6 Custom fields tab

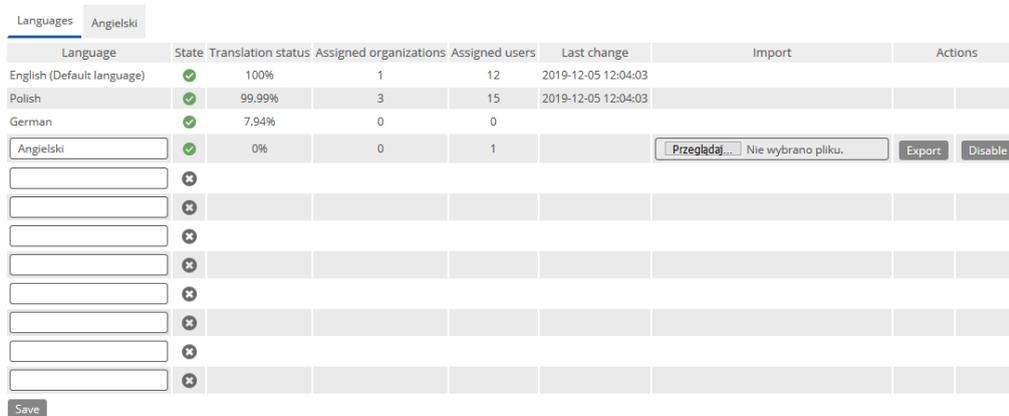
## 8.5 Translations

FAMOC provides multi-language support<sup>1</sup>, allowing administrators to create new translations of the console. Translations tab is available for semi-admin, administrator and superadmin roles.

To create a new language version:

1. Go to **Translation** → **Languages** tab.
2. Input **Language** name and press **Save** to create a new subtab enabling FAMOC console translation.
3. Go to the newly created language tab and translate the enlisted terms, each time clicking OK to add translation to the dictionary.

Marking **Enabled** next to a language version, makes it available for selection in each FAMOC organization.



<sup>1</sup>Currently supported language versions: English, German, Spanish and Polish.

Figure 7 Translations

## 8.6 Server status

This section displays the following subtabs:

- **Services status** – provides detailed information on the services covered by FAMOC license and services status
- **Server licenses** – gives an overview of licenses purchased within FAMOC (number of devices that can be managed within the platform) with the license expiration date
- **Reports** – shows a list of server reports (including license reports that enlists organizations created by the super admin with numbers of devices managed within the department and license limits). This section allows the administrator to generate reports on licenses per institution. Administrator is able to view detailed information on e.g. active devices within each organization, number of sent text and binary SMSes, iOS and Android push, download a text, .csv or detailed binary report file, and create a schedule for report that will send a report as an email.
- **SSL certificates** – provides details on SSL certificates in use

Services status | Server licenses | Reports | SSL certificates

Start services | Stop services | Restart services

FancyFon services status						Refresh
Program name	Details		Description	Status	License status	
FAMOC Proxy	Is running	OK	Proxy server	OK	-	
	localhost	OK				
	localhost:11030	OK				
Remote Access	Is running	OK	Remote Access server	OK	Covered	
	localhost:11010	OK				
	localhost:11012	OK				
	localhost:11023	OK				
	/var/drad.http	OK				
	/var/dmd-drad	OK				
Device Monitor	Is running	OK	Device Monitor server	OK	Covered	
	localhost:11014	OK				
	localhost:11015	OK				
	/var/rda	OK				
	/var/rda-param	OK				

Figure 8 Server status

## 9 FAMOC Wizard

After logging in to the system (if wizard steps are not proceeded or ignored), administrator will be displayed a popup with pending wizard steps. Additionally, the wizard popup can be invoked at any time by clicking on the Wizard tab (placed on the top right corner of the FAMOC console).

Wizard				✕
Wizard steps	Status			
<b>Add more users and groups</b>	✓	hide		
Add single user	✓			
<b>Configure LDAP/AD</b>	✗	proceed	ignore	
Import users and groups from file	✓			
Add group of users	✓			
<b>System configuration</b>	✓	hide		
Install Apple APNS certificate	✓			
<b>Add devices to the system</b>	✓	hide		
Add single device	✓			
Add devices to the system by accessing bootstrap page	✓			
<b>Define mobile devices policies</b>	✓	hide		
Define policies for groups of users or group of devices	✓			

Show pending steps | Close

Figure 9 Wizard popup

Full list of wizard steps:

- **Add more users and groups** – provides several ways of adding users and groups to the system. Step will not be shown, in case organization contains more than one user and group. FAMOC suggests the following options:
  - **Add single user** – proceed button opens ORGANIZATION → Users → Add user form
  - **Configure LDAP/AD** – proceed button opens ORGANIZATION → Imports → LDAP import tab
  - **Import users and groups from file** – proceed button opens ORGANIZATION → Imports → File import tab
  - **Add group of users** – proceed button opens ORGANIZATION → Groups → Add group form
- **System configuration** – provides the list to the Apple APNS certificate form. The step will not be shown in case an Apple certificate has already been uploaded to the system.
- **Add devices to the system** – provides several ways of adding devices to the system. FAMOC offers the following methods:
  - **Add single device** – proceed button opens FAMOC → Devices → Add device form.
  - **Add devices to the system by accessing bootstrap page** – proceed button opens FAMOC → Settings → System advanced → Startup settings tab where the link to the startup page is shown.
- Define mobile devices policies – provides links to define general and security policies for groups of users. FAMOC offers the following methods:
  - Define policies for groups of users or group of devices – proceed button opens FAMOC → Settings → Policies → General policies tab.

On the bottom of the Wizard popup there are two buttons:

- **Show all steps** – opens popup enlisting all steps with its status (pending, proceeded, ignored).
- **Close** – closes the wizard popup.

## 10 Adding New Users

The FAMOC administrator can add new users manually to the system or perform bulk imports by uploading an import file or synchronizing Open LDAP or Active Directory Server with FAMOC. Users can also be automatically added upon synchronization with a BlackBerry Enterprise Server.

### 10.1 Adding Single Users

1. To add a new user, click **Add user** in the **Users** tab under **ORGANIZATION**, or in the **Devices** section under the **ADVANCED** tab.
2. You will be asked to provide **Name** and **Surname** of the **New User**. In addition a **Login** can be assigned as well. The tabs below allow **WLAN Access** and employees' details to be defined. Optionally users can be added to **Groups**. Afterwards click **Save**.

The screenshot shows the 'Edit user data' form with the following fields and values:

- Name: default
- Surname: (empty)
- Login: default
- Can login:
- Password: (empty)
- Force user to change password after next login:

The 'WLAN Access' tab is active, showing the following fields:

- Country: Poland
- Company: (empty)
- Department: (empty)
- Job title: (empty)
- Office phone: (empty)
- Mobile number: (empty)
- Employee ID#: (empty)
- Email address: (empty)
- Email user name: example@famoc.com

The 'WLAN Access' tab also shows the following fields:

- Username for EAP: default
- Password for EAP: (masked with dots)
- Realm for EAP: default

Figure 10 Add user details

- To grant a user access to **ORGANIZATION** and **ADVANCED** tabs, administrator needs to first define sets of prerogatives to FAMOC management features in **ORGANIZATION** → **Roles** tab ([see 12.7](#)). Roles will be available for selection, after marking the **Can login** checkbox.
- When **Can login** feature is selected, there is also the possibility to enable the feature **Force user to change password after next login**, which forces a user to change their password.

The screenshot shows the 'User password settings' form with the following fields and values:

- Name: default
- Surname: (empty)
- Login: default
- Can login:
- Password: (masked with dots)
- Force user to change password after next login:

Figure 11 User password settings

- To introduce parameters for Instant Messenger, IBM Lotus Notes Traveler, Microsoft Exchange, VPN and AgitoRoamAnywhere, go to the **Applications** tab.

User details	Groups	Roles	WLAN Access	APN configuration	Applications	Certificates	Custom fields
Instant Messenger:							
IM user name:	<input type="text" value="john.doe"/>						
Lotus Notes:							
User ID:	<input type="text" value="john.doe"/>						
Microsoft Exchange:							
User name:	<input type="text" value="john.doe"/>						
E-mail address:	<input type="text" value="john.doe@exchange.company.com"/>						
Domain:	<input type="text" value="exchange.company.com"/>						
Password:	<input type="password" value="....."/>						
ShoreTel RoamAnywhere:							
User name:	<input type="text" value="john.doe"/>						
Password:	<input type="password" value="....."/>						
Directory Number:	<input type="text" value="44.20"/>						
Enterprise Number:	<input type="text" value="273954079"/>						
VPN:							
VPN User name:	<input type="text" value="john.doe"/>						
VPN Password:	<input type="password" value="....."/>						
<input type="button" value="Back"/>		<input type="button" value="Save"/>					

Figure 12 User application tabs

6. FAMOC allows the administrator to assign a certificate to a user. To upload the correct pem/der or pkcs#12 certificate file, go to the **Certificates** tab. It is also possible to input the issuer details, validity and expiry date (if uploading pem/der file, the data will be provided automatically). Once the changes have been saved, a certificate icon appears on the user list. The icon presents certificate details. The uploaded file can be used to send various configuration details to the user’s device, e.g. WiFi or APN authorization.

**NOTE:** FAMOC does not provide certificate verification. Providing a correct file is the responsibility of the administrator.

7. The **Users** tab also allows user details to be modified or deleted.

**NOTE:** If FAMOC is synchronized with any BlackBerry Enterprise Server ([see 11.3](#)), the **Add user** button appears in the device inventory tab ([see14](#)). On clicking it, a pop up is displayed. Choosing an option from **Adding user to FAMOC** or **Adding user to BES** navigates to the proper tab.

## 10.2 Adding Multiple Users (Import)

To perform a bulk import of users, select the **Users** tab under **ORGANIZATION** and click **Import users**.

You will be asked to input import description/name, define file format (parameters separated by a colon, semicolon, comma, or tab), and upload a previously prepared file.

If you have previously imported a parameter mapping schema to FAMOC, it will be accessible for selection while importing a file. Otherwise, select **Create new schema** option. To proceed, press **Next**.

The next step is to create a mapping schema, which means matching the parameters of the imported file with the FAMOC fields. Before saving the schema, input the schema map name.

**NOTE:** To ensure proper data upload and mapping, the schema should include FAMOC user logins.

Figure 13 Users import

Press **Save** to save the mapping schema. Import file details and mapping schema details will be displayed. Mapping schema and file source preview will be available. The system provides four options:

- **Back button** – saves the schema but postpones the import (the schema will be available for import into **ORGANIZATION** → **Imports** → **File Import** tab)
- **Import button** – enables file import and data mapping to be automated, according to the created schema
- **Validate data button** - enables the data to be validated prior to performing the import
- **Delete** – deletes the schema

**NOTE:** If the imported file is not validated successfully, it will be necessary to abort the operation and go through the process again, with a correct file format.

The imported file and the mapping schema will be available in **Imports** under **ORGANIZATION** tab ([see 12.5](#)).

### 10.3 Server Synchronization

1. The FAMOC administrator can add Open LDAP or Active Directory server to the system and synchronize it with FAMOC. To do this, select the tab **Imports** under **ORGANIZATION** and click **New Open LDAP server** or **New Active Directory server**.

2. Provide for the following data:

- **Connection data** – here all the details necessary to establish connection with the server need to be introduced, e.g. server type and name, connection interval, port and address.

FAMOC enables user LDAP authentication which means that users will be able to log in to FAMOC using a company server password.

You can select **Assign user group based on LDAP attribute** to automatically assign users to specific groups when the value of this field will be set in synchronization. Administrator can select the LDAP class name and attribute name. Then choose a group to which the users should be assigned<sup>2</sup>.

FAMOC generates startup code for imported device. To choose sending option select delivery method for startup code: Auto, Email, SMS, No notification.

- **Mapping** – allows administrator to define which fields should be collected from LDAP/Active Directory server and assigned to corresponding fields in FAMOC. The Assign button displays server’s dependency tree.
  - **Group mapping** – enables users to be assigned to groups previously created in LDAP/Active Directory server and then uploaded to FAMOC.
  - **Devices mapping** – enables devices import from LDAP/Active Directory to FAMOC.
3. To finish, press **Save and test settings** or **Save and synchronize**.

Figure 14 Server synchronization

**Global catalog support**

<sup>2</sup> This setting can be used eg for the quarantine. User group can be assigned to the specific policy with limited settings. When the LDAP flag will be set, user’s devices will be moved to the specific policy.

This service is available on port 3268. It should be used in Ldap import settings as connection port and allowed on the system firewall.

**Class list distinguished name** field should be empty and **Filter** need to contain information about the common users group, e.g. *'memberof=CN=Global\_group,CN=Users,DC=exchange,DC=com'*.

## 11 Organization

ORGANIZATION tab allows the administrator to edit company and user details, set interface language, add groups of users, create additional device descriptions in the system, manage user privileges and manage file import.

### 11.1 Users

The **Users tab** gives an overview of all FAMOC users and enables the administrator to add single or import multiple users to the system, manage user details and grant access to **ORGANIZATION** and **ADVANCED**. To edit user details press the **Edit** button appropriate to the user.

### 11.2 Org. Details

The **Org. Details tab** allows the administrator to edit company details such as Name, Country, and Address etc. After submitting any changes please click **Save**.

### 11.3 User details

User details such as **Name**, **Surname**, **Email address** and **Password** can be changed at **ORGANIZATION** → **Users Details**. Additionally, a language selection can be made here.

### 11.4 Groups

The **Groups tab** is useful when managing a large number of devices and users as it allows users to be grouped by similar requirements and group actions to be carried out.

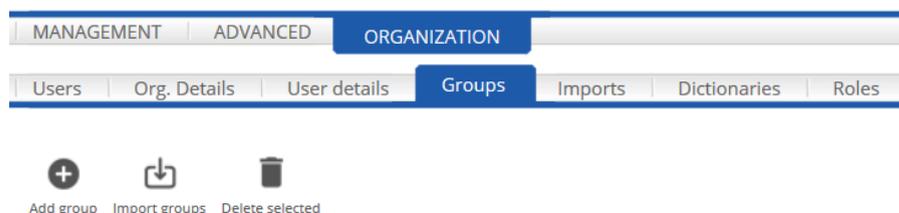


Figure 15 Groups tab view

### 11.4.1 Adding Single Groups

Groups can be added by pressing **Add group** at the **Groups** tab.

Provide a **Name** for the group. The name should be directly associated with group’s features, such as: London Employees, Sales Staff etc. This will make the administrator’s work more efficient. It is also possible to define Service Level Agreement (SLA). The system provides four SLA templates: Basic, Gold, Platinum or VIP, for different support priorities. Once the SLA is set, the following icons appear in the device inventory, allowing devices to be sorted according to the level of support:

- Basic Service Level Agreement
- Gold Service Level Agreement
- Platinum Service Level Agreement
- VIP Service Level Agreement

Using the **Staff** tab, select users to be included in this group and **Save** the changes.

Each group can also be granted privileges. To select them, use the **Roles** tab. FAMOC provides template roles, however it is also possible to create a new set of privileges ([see 10.7](#)). To finish, press **Save**.

A new group has been created and is shown in the **Groups** tab. Groups can be modified and deleted from FAMOC by pressing the respective buttons.

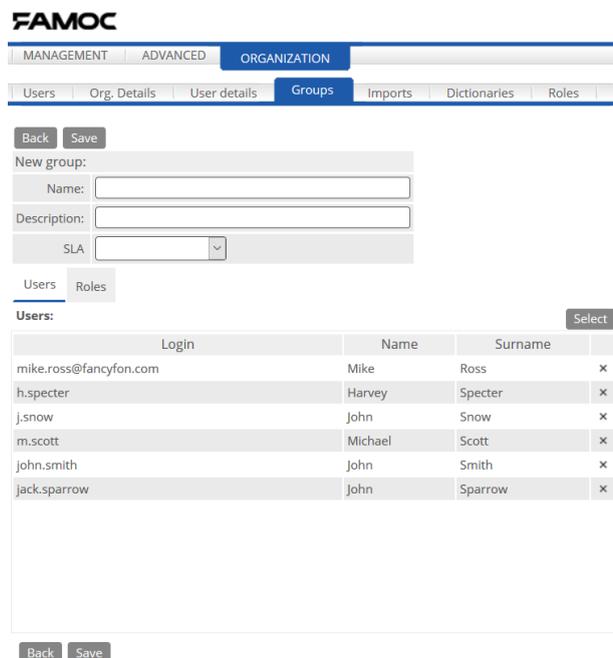


Figure 16 Creating groups

## 11.4.2 Adding Multiple Groups (Import)

To perform bulk import of groups, use the **Import groups** button in **Groups** under **ORGANIZATION** tab. File import requires a description to be added, a file format to be selected, and the file to be uploaded. If you have previously created a parameter mapping schema to FAMOC, it will be accessible for selection when importing a file. Otherwise, select **Create new schema** option. The operation is similar to bulk import of users ([see 10.2](#)).

## 11.5 Imports

The **Imports** tab allows the administrator to perform bulk import of users, groups, SIM cards, devices and bills to FAMOC.

### 11.5.1 LDAP Import

This section allows the administrator to add Open LDAP or Active Directory server to the system and synchronize it with FAMOC ([see 10.3](#)).

### 11.5.2 File Import

This section displays a list of previously uploaded files with file details. Using this tab, administrator can preview the file, import it in case the import was postponed while uploading the file to FAMOC, or delete the file. It is also possible to perform a new import.

1. To import a new file, use the **New import** button.
2. You will be asked to input import description/name, define file format (parameters separated by a colon, semicolon, comma or tab), and import type.
3. Upload a previously prepared file.
4. If you have previously imported a parameter mapping schema to FAMOC, it will be accessible for selection when importing a file. Otherwise, select **Create new schema** option. To proceed, press **Next**.
5. The next step is to create a mapping schema, which means matching parameters from the imported file with FAMOC fields. Before saving the schema, input **Schema map name**.

**NOTE:** To ensure that the data is uploaded and mapped correctly, the schema should include FAMOC user logins.

6. After saving the data, the uploaded file will be verified for correctness. If the file format is correct, the status will change to Verified and the import icon (  ) will appear on the list. After clicking it, the parameters will be automatically imported and mapped in accordance with the prepared schema.

NOTE: If the entered data turns out to be incorrect (  icon), the entire data importing process will have to be repeated with the correct file format.

7. Both the loaded and imported files are available in the **ORGANIZATION** → **Imports** → **Import from file** tab.

8. To delete the import scheme, click the  icon.

### 11.5.3 Import Schemas

This section displays a list of previously uploaded parameter mapping schemas. Using this tab, the administrator can preview or delete import schemas, or create a new pattern.

1. To create a new schema, use the **New schema** button.
2. You will be asked to input import description/name, define file format (parameters separated by a colon, semicolon, comma or tab), and upload a previously prepared file.
3. The next step is to define an import type. To continue press **Next**.
4. Input schema map name and match parameters from the imported file with FAMOC fields.

**NOTE:** To ensure the data is correctly uploaded and mapped, the schema should include FAMOC user logins.

5. To finish press **Save**.

### 11.6 Dictionaries

Creating additional **Dictionaries** in FAMOC enables a more comprehensive and personalized description of devices that are added to the system. This option is useful when using the advanced search function.

1. Dictionaries can be added by pressing **Add dictionary** in the **Dictionaries** tab.
2. Provide a **Name** and **Description** for the Dictionary.
3. Use the **Add** button to assign each word to the new dictionary.
4. Optionally, a description can be added next to each word.
5. To finish press **Save**.

**NOTE:** The **Dictionaries** tab serves to define additional categories with groups of words included in those groups. To be able to use them as device description it is also necessary to create **Custom Fields** in the system. To learn how to generate these see [21.4.2](#).

## 11.7 Roles

The **Roles tab** allows the administrator to create role templates with predefined user privileges so that while adding a new user, it is not necessary to manually grant a set of privileges each time, but it is possible to use a previously defined template.

The system provides 4 role templates:

- **FAMOC System Administrator** – with full access and management powers
- **FAMOC Security Manager** – with full privileges for security restrictions deployment and management
- **FAMOC Asset Manager** – with access to information on company assets, including hardware, software, SIM cards, users and processing data
- **FAMOC Group Manager** – grants access to manage specific groups of users and devices
- **FAMOC Web Services** – gives access to the organization's web services

However, the administrator can create custom sets of privileges:

1. To create a new template press **Add role** in **ORGANIZATION** → **Roles** tab.
2. Input **Name** and **Description** of the role.
3. To assign privileges, mark the checkboxes next to FAMOC tabs and functions in the **Available privileges** table. Once you assign privileges, they will appear in the **Assigned privileges** table.
4. To finish press **Save**.

List of available privileges can be found in *FAMOC Privileges Guide*.

## 12 Monitoring

The **Monitoring** displays an overview of FAMOC reports, shows current status of the system, and gives general statistics on FAMOC and managed devices. See FAMOC UI Guide to learn more about Monitoring and the new interface.

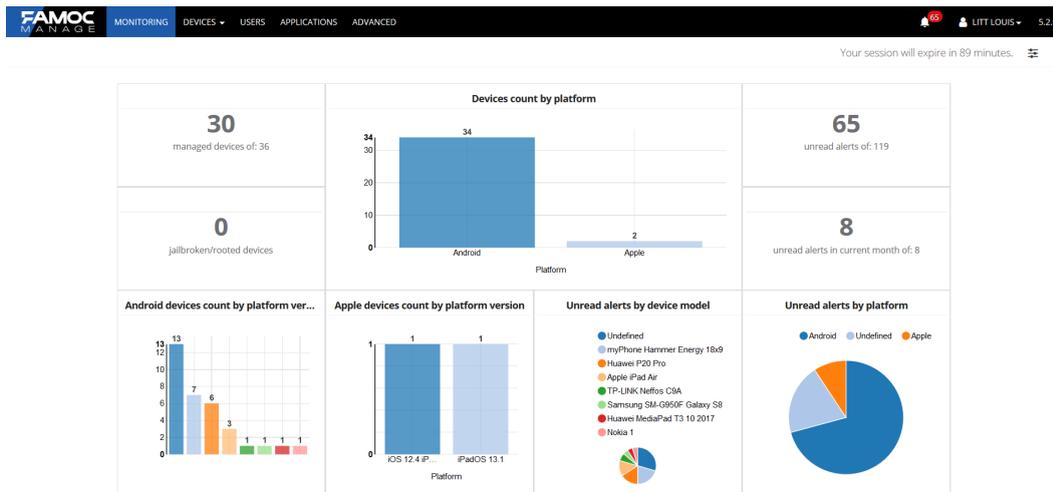


Figure 17 Monitoring

## 13 Device Inventory

The device inventory provides information such as username, telephone number, description, device model and time of last contact with the devices.

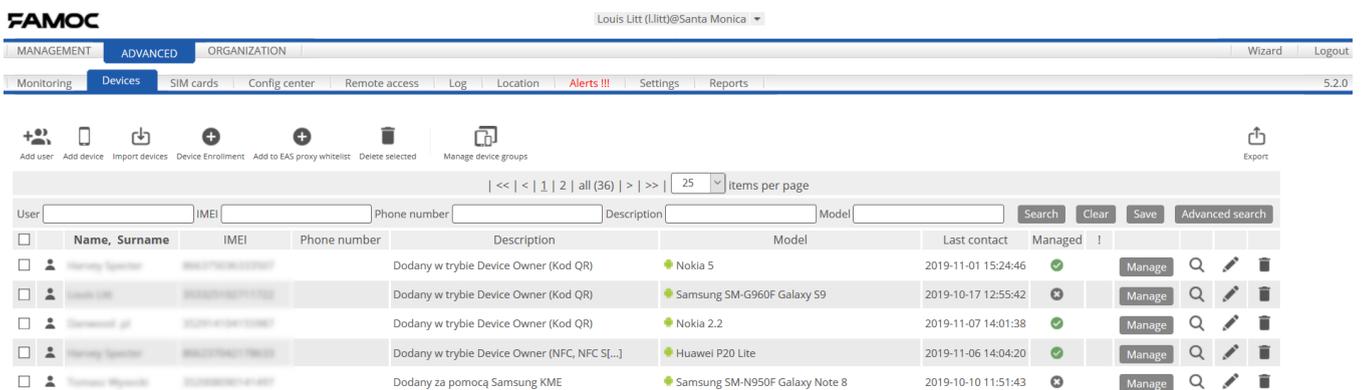


Figure 18 Device inventory

The device **search bar** helps to locate a mobile phone in the system. The **Save search result** function makes search parameters available in a search scroll. When clicking **Advanced search** button, additional search fields appear on the screen. Previously defined **Custom fields** are also accessible here.

**Connected to RA** option under **Advanced search** button, devices connected to Remote Access are displayed. Remote Access enables the administrator to take remote control of a mobile device screen and keyboard. Once the **Advanced search** option is selected, checkboxes appear next to all the search fields. Marking a checkbox next to an item adds a column to the device list with corresponding data.

Figure 19 Device search bar

Device inventory tab also includes functional icons:

- **Add user** – directs to **ORGANIZATION** → **Users** → **Add user** tab
- **Add device** – enables new devices to be added to FAMOC
- **Import devices** – enables bulk imports of users using CSV files
- **Device Enrollment** – enables generating startup code for selected devices, allowing users to access bootstrap page
- **Add to EAS proxy whitelist** – enables selected device identifiers(IMEI, device UID, serial number) to be added to the EAS proxy whitelist. Option available only if EAS proxy is defined. For more detailed information, refer to [21.4.6](#).
- **Delete selected** – enables previously marked devices to be deleted
- **Manage device groups** – redirects to settings tab with possibility to manage device groups
- **Export** – enables data to be exported to a .csv file separated by comma, .csv separated by semicolons or .txt files, and also cancels exports



Figure 20 Device inventory functional icons

## 13.1 Adding Single Devices

To add a new phone use Add device button in the Device inventory and provide the following information:

1. Phone number in the **SIM card** sub tab<sup>3</sup>
2. Select user from the user pop up list in the **Device** sub tab
3. Model (not necessary for all platforms supported by FAMOC Base Agent)
4. Device group – add new one, or select existing from the list

<sup>3</sup> Phone number format: Country Direct Number + Phone number (e.g. for an Irish number 353509483726)

5. Other information can be provided but is optional

The **Device** sub tab contains device details. Some of the parameters will be provided to FAMOC automatically, others may be added manually, but are optional.

The **SIM card** tab contains asset information concerning contract details and the telecom operator. If you want to add a new SIM card to a device already included in the system, use **Add new card** button. If using a SIM card already included in FAMOC, press the **Use existing card** button. The **Remove SIM card** button removes the connection between the SIM card and device, which means the SIM card is no longer inserted into this particular device.

Figure 21 Add device

### 13.2 Adding Multiple Devices (Import)

Large numbers of devices can be imported into FAMOC using **Import devices** button in Device inventory or **Import** tab under **ORGANIZATION**. FAMOC supports different import file formats. To learn more about FAMOC import, refer to [12.5](#).

### 13.3 Working with Single Devices

Once devices are available in the device list, the installation of **Certificates**, **Base Agent**, **DM Profile** or other **FAMOC client components** on each of the managed devices can begin. For more information on these

functions refer to [14.4](#). Details of individual devices can be seen and modified by pressing the **Manage** button next to a device.

After pressing the **Manage** button, device details and management tabs are displayed. This section allows various actions to be performed or information to be searched for, for the selected device.

In the main view, next to device details table, there is information about policy currently assigned to the device. **Policy preview** displays the policy settings and assignment status. If the policy is not applied on the device or it is outdated there is possibility to refresh it on the device.

Underneath the device picture certain functions can be accessed: **Restart Device** (for Custom Android and supervised Apple devices), **Shutdown Device** (for Samsung Android and supervised Apple devices) and **Run Remote access** (if the proper agent is installed; refer to chapter [17](#) for details).

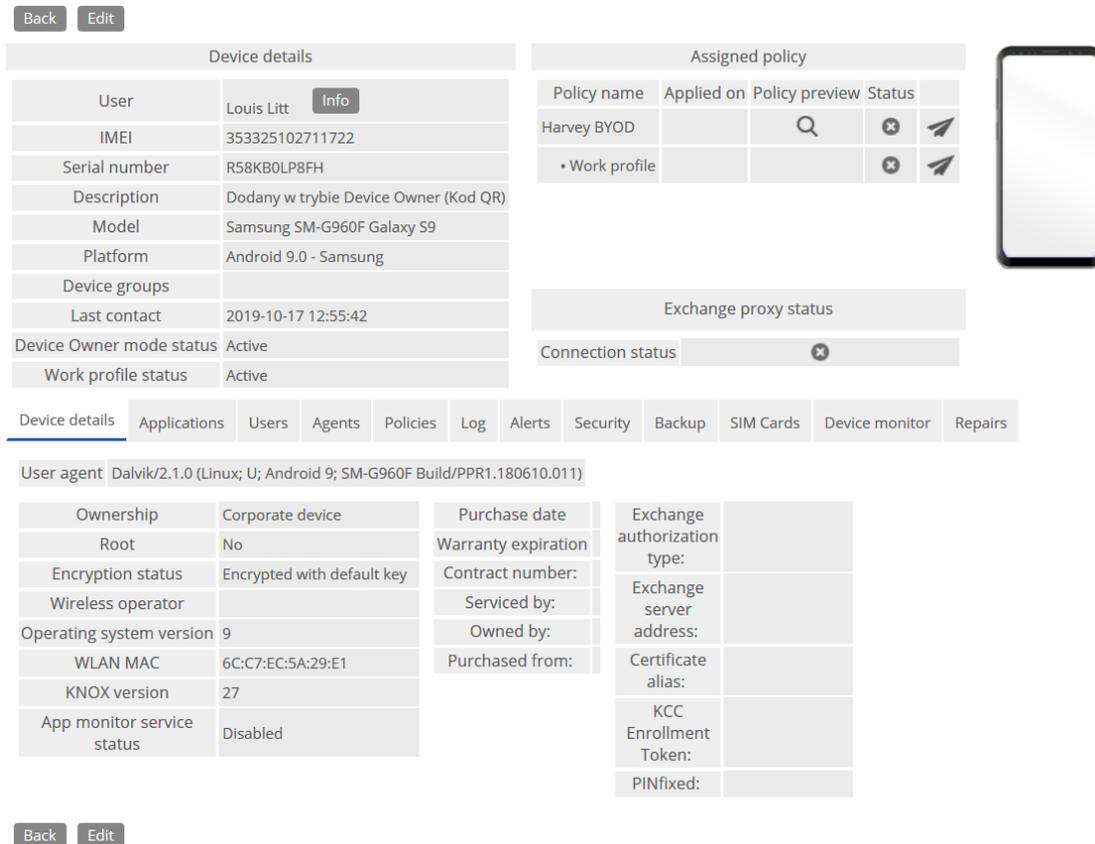


Figure 22 Single device management

### 13.3.1 Device Details

This section gives general information about the device, e.g. ownership of the device, jailbreak / root status, encryption status, MAC address, detailed operating system version, when and from where it was purchased, the contract number, warranty expiration date, which partner it is serviced by and who the owner is.

### 13.3.2 Users

This section provides mobile device user history if it had different owners in the past.

### 13.3.3 Applications

Left menu of the section manages the following functionalities:

- **Installed applications** – The tab displays all applications installed via FAMOC console, and those reported by Device Monitor, with application details and application reputation. Each of them can be Run or Removed from the device. Applications highlighted in green are the ones installed using FAMOC and confirmed by the device monitor. Applications highlighted in red were installed using FAMOC but are not reported by the Device Monitor (e.g. the user uninstalled it manually). Reinstall all button enables repeated installation on FAMOC applications.
- **Work Profile applications** – The tab shows applications installed in container.
- **Available in Store** – The tab displays preview of corporate store with applications available for installation. Application list contains all compatible applications that are available for all devices or are included in specific corporate store, assigned to a group of users. The table also includes an installation status icon and several action buttons: install, reinstall, run, uninstall.
- **All compatible** – The tab displays all applications available in FAMOC that are compatible with a certain device. Applications list contains an installation status icon and several action buttons: install, reinstall, run, uninstall.
- **Uninstalled applications** – The tab displays all applications that were uninstalled from the device, with possibility to view details of the application and its reputation.

### 13.3.4 Policies

The tab displays policy and configurations applied to the device. The first table shows assigned policy including the name, date of the assignment, date of the last modification, date when the policy was applied on device, policy preview, status of the policy installation and action icon allowing to refresh the policy (if policy is not applied or is outdated). The second table shows list of the applied configurations.

Assigned policy						
Policy name	Created on	Last modified	Applied on	Policy preview	Status	
Harvey Default	2018-12-06 14:32:39	2019-08-29 13:10:24	2019-11-01 08:38:17			

Applied configurations						
Name	Type	Installed in	Created on	Created by	Last status	Disabled
Tapeta FF 1080p	Set wallpaper on the device screen	Device	2019-10-28 10:21:56		2019-10-28 10:23:44	

Back Edit

Figure 23 Policies tab

### 13.3.5 Agents

This section gives insight into all agents installed on the device, their install version, the latest available version, date of last execution, creation and download. In the Agents tab administrator can generate access code for Maintenance mode or Recovery mode on the device, enable or disable diagnostic agents logs and download them remotely.



Figure 24 Device Agents tab

### 13.3.6 Alerts

The tab gives insight into alerts reported to the system by FAMOC clients installed on the device. The table presents time and details of the event. Data is listed in chronological order. Alerts are divided into four groups – read, unread, ignored and resolved. Once the administrator has become familiar with the alert, it should be marked as **Read, Ignored or Resolved**.

### 13.3.7 Log

Log displays all actions performed on the device along with status and details.

### 13.3.8 Location

The tab gives details on the last location of a user’s device. To be able to locate the device, it is necessary to first install Location Monitor and run the applet in the **ADVANCED** → **Manage** → **Agents** tab. To update data, use Get actual location button in the **Location** subtab.

### 13.3.9 Security

FAMOC provides an unparalleled level of security support across multiple mobile platforms, managed centrally or individually on a device. Data security section shows operations log with action name, used application/agent, status, date of creation and last status, and SMS status.

Left menu of the section manages the following functionalities:

- **Data wipe** - The device can be reported stolen and wiped at this tab. In addition, for iOS devices, FAMOC allows an **Enterprise Wipe** option, which removes all the enterprise data installed by FAMOC profile. There is also a button **Mark as wiped** for devices on which wipe was done manually. For Samsung devices with KNOX container there is additional button – **Enterprise wipe – KNOX container**, which removes container from the device. For devices with Android for Work container there is an additional button - **Enterprise wipe – container**, which removes container from the device.
- **Device lock** – The device can be remotely locked/unlocked and the lock code can be reset at this tab. These options are available for Symbian, Android and iPhone. In addition, for Samsung devices with KNOX container there are separate buttons for **Lock KNOX container** and **Reset KNOX lock code**.
- **Certificate management** – For even better mobile infrastructure security, FAMOC offers a unique system that uses individual certificates for each device, with a remote invalidation option. When transferring data between a phone and FAMOC server, the certificate request comes from the device, the key never leaves the device, so it is not possible to impersonate the device by copying the certificate. This tab displays a list of installed certificates along with their details and allows generating and installing, renewing or revoking a certificate on the device.
- **EAS proxy whitelist** - displays list of Exchange ActiveSync proxy addresses.

### 13.3.10 Backup

The tab displays type of backup, its status, path, date of last run and creation. Backup and restore can be performed from this tab. Additionally, it is possible to import data from one device to another.

**NOTE:** Performing backup and restore is only possible if the Backup Agent is first installed on a mobile device.

#### Data backup/restore

Performing data backup/restore requires a backup pattern to be created by pressing **Add new** button:

1. Select what type of data to include in the backup pattern (contacts, calendar, folders, SMS). For folders, select access path from a pop up list. It is also possible to provide filters such as file types to include or exclude and maximum file or folder size. Press **Add item**.
2. To execute data backup mark proper items and press **Backup** button.
3. Pressing Restore button can restore files stored on the server.

#### Data import

1. To import files from one device to another press the **Import** button.
2. Select device and mark files to be imported. Press **Next** to proceed.
3. The selected files will appear in the backup data table as imported. Mark them and press **Restore**.

**NOTE:** It is only possible to import data from devices belonging to the same user. It is also possible to import data from devices removed from the system for the period of one month.

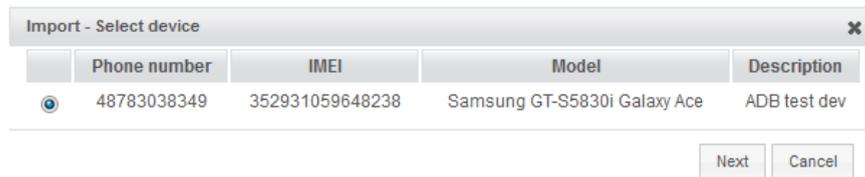


Figure 25 Data import

### 13.3.11 SIM Cards

The tab displays information on the current active SIM card, gives access to SIM cards history, IMSI, tariff name and additional description.

### 13.3.12 Device Monitor

Device monitor gives detailed information concerning the mobile phone, e.g. device details, hardware, processes, applications, Bluetooth parameters, disks or access points.

### 13.3.13 Repairs

The tab provides details concerning past repairs and allows new ones to be reported.

### 13.3.14 Usage data

The tab presents connection details reported by the Usage monitor for Android, such as connection type, date, phone number, application usage<sup>4</sup>, browser history and device usage. This section enables the download of outgoing/incoming text messages and voice connections.

### 13.3.15 Recorded connections

The tab presents connection details reported by the Symbian Audit Agent, such as connection type, date or phone number. This section enables the download of outgoing/incoming text messages and voice connections.

**NOTE:** FAMOC records voice calls in AMR<sup>5</sup> file format, therefore software supporting AMR files is required to play the recording.

<sup>4</sup> For Android 6.0 and higher, application usage reporting requires the Application Monitor Service on the device to be turned on.

<sup>5</sup> The Adaptive Multi-Rate audio codec is a patented audio data compression scheme optimized for speech coding.

## 13.4 Installing Certificates and Base Agent on Individual Devices

Installing certificate, FAMOC Base Agent, FAMOC Remote Access, FAMOC Backup Agent or FAMOC Security Agent on a single device can be done directly from the Advanced device tab, by pressing the **Install** icon under the **Agents** tab.

Logging status: Enabled

Agents List								
Agent	Name	Version	Latest version	Last run	Created on	Downloaded	Uninstalled on	Status
Certificate								✘
Base Agent								✔
Remote Access								✔
Backup Agent								✔
Security Agent								✔
Location Monitor								✔
Usage Monitor								✔
SecureSource								✘
Base Agent Add-on								✘

Figure 26 Install agents on single device

The recommended order for the installation is:

1. Certificate (for untrusted server certificate)
2. Base Agent (with Security monitor)
3. Remote Access
4. Backup Agent
5. Location Monitor
6. Usage monitor
7. Call Recorder

Agents repository also displays the installation status:

- agent was successfully installed
- new version of agent is available
- device lacks the agent
- user refused installation
- application has been sent
- application is being installed
- start Remote Access session
- send configuration to the device in case automatic configuration process fails

Further details on the installation process can be found in [16.1](#).

## 14 SIM Cards

The **SIM cards** tab provides information on each SIM card that is included in the FAMOC system, which means it also includes the SIM cards which aren't inserted into any mobile device.

This section enables SIM card details to be edited, as well as adding or removing them from the system.

**Add new SIM card** button enables new cards to be registered with the system. Using the **Import SIM card** function performs bulk imports by uploading formatted files. The **Insert** button enables the SIM card to be attributed to a selected mobile device.

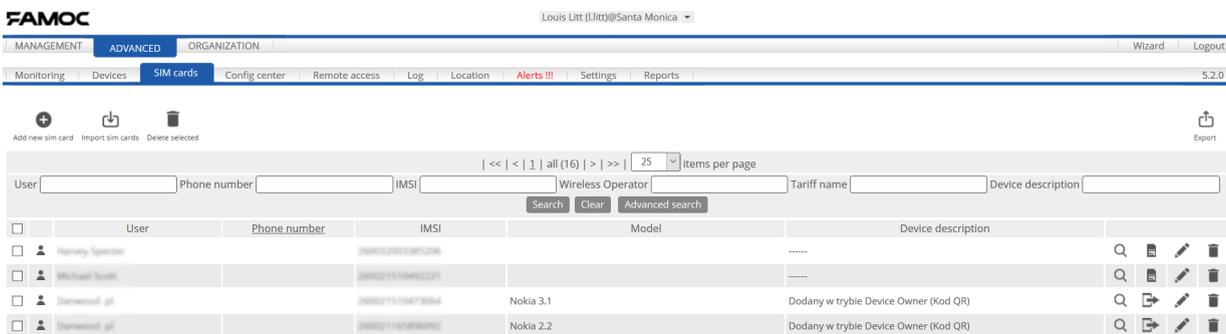


Figure 27 SIM cards tab

Next, the admin may go to Advanced/ Devices and click export, the custom fields are included in the export data dialogue window.

When the admin wants to add custom fields in the Sim Cards should go to Advanced / Settings / System advanced and add in custom fields tab a custom field to the SIM Cards table.

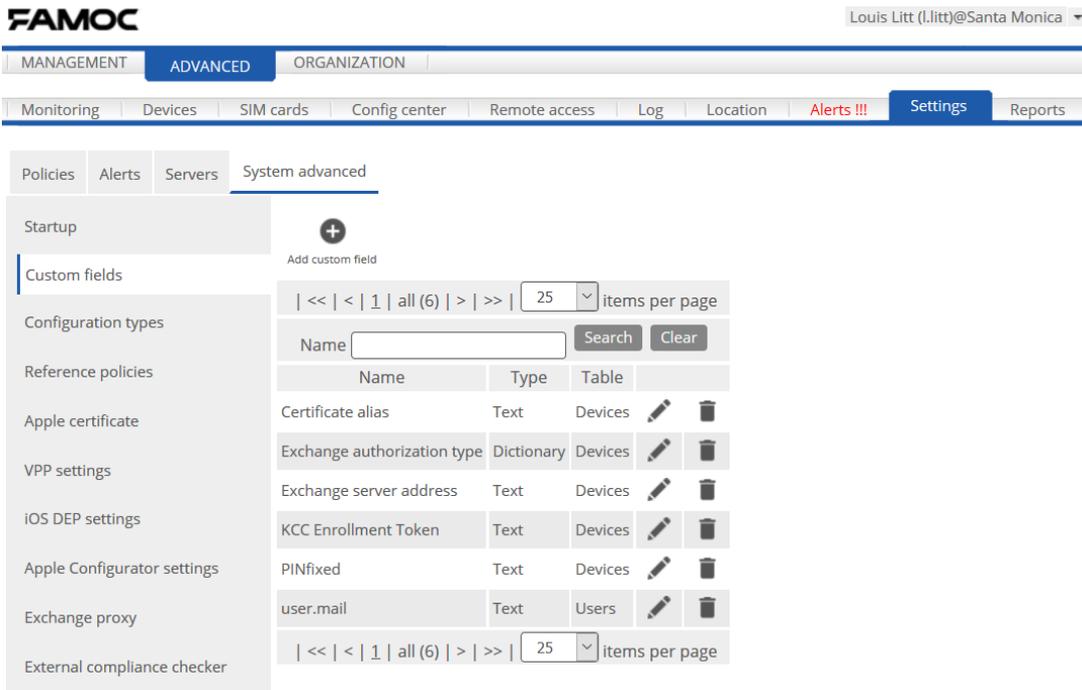


Figure 28 Custom fields

Next, the admin may go to Advanced / Devices and click export, the custom fields are included in the export data dialogue window.

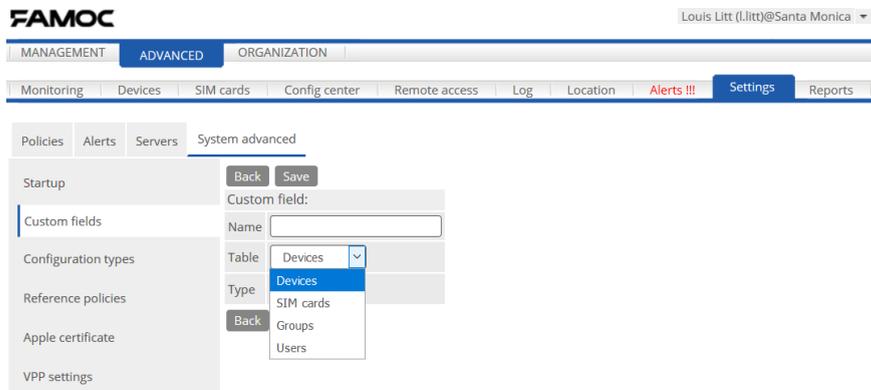


Figure 29 Custom field creation

## 15 Config Center

The FAMOC **Config center** allows bulk operations to be performed on the managed phones. This includes the installation of applications, performing backups as well as configuring devices.

The Config center section consists of eight modules: **Agents, Applications, Corporate store, Configurations, Messages, Backup, Packages** and **Sets of Packages**.

## 15.1 Agents

The **Agents tab** allows **certificates, Base Agent, Remote Access, Backup Agent, Security Agent, Location Monitor, Usage Monitor, Call Recorder and Add-on** to be installed on any number of devices simultaneously. Details of each item, including the version number and the number of successful installations, are shown here. For phones with different operating systems, such as Symbian, Windows Mobile or UIQ, the correct version of the application needs to be chosen before installation. This section also displays a list of operations related to each agent and allows the applet to be configured.

### 15.1.1 Certificate Installation

The **Certificate** function provides secure data transfer between mobile phones and the FAMOC server. Its installation is necessary for any other FAMOC Agents to work properly. As with all the other applications, certificate may be installed separately for each device or as a mass operation on a group of mobile phones simultaneously.

**NOTE:** If the server uses certificate as a preinstalled function on mobile devices (e.g. VeriSign), this step can be omitted.

1. Press **Install** icon to send certificate to mobile devices.
2. Next the mobile devices on which the certificate shall be installed need to be selected by pressing the **Add phones** button.
3. Select devices from the pop up window showing all managed devices. Group selections can be done by pressing the **Groups** button. Filters can be applied to ease the device selection.
4. Before sending the list of selected devices can be checked. FAMOC also allows you to choose whether the installation should be performed immediately or at a later time.

Operation: ? help

Install

Devices:

Teszt Telek	DEMO: Teszt Telek	Motorola Q9h	X
System Administrator	DEMO: Administrator System	BenQ E72 Smartphone	X
Pedro Perez	DEMO: Pedro Perez	Asus MyPal A636N	X
John Smith	DEMO: John Smith	Fujitsu-Siemens LOOX T830	X
John Doe	DEMO: John Doe	Nokia E71	X
Joe Borg	DEMO: John Borg	Nokia 5310 XpressMusic	X
Jean Dupont	DEMO: Jean Dupont	BlackBerry 7100g	X
Jan Novak	DEMO: Jan Novak	SonyEricsson W958c	X
Jan Kowalski	DEMO: Jan Kowalski	Samsung SGH-D720	X
Ivan Horvat	DEMO: Ivan Horvat	HTC Touch Diamond	X

Select option to install:

**Make sure that built-in browser is used on the device. Some browsers will not be able to install the certificate.**

Certificate

Certificate (alternative)

Installation method:

WAP-push link  Use https

Perform operation now

Perform on:  at  + random

Figure 30 Certificate installation

### 15.1.2 FAMOC Agent Installation

Agent installation is similar to previously presented certificate and manual DM Profile installation.

1. Select the mobile devices on which the installation will be performed by pressing the **Select phones** button.
2. Select installation option (FAMOC Agents require the correct platform assignment). If you want the system to decide which software version should be supplied to a handset, mark **Auto Selection**.
3. Define where the applet should be installed (device memory, memory card, disc) and select installation method.

**NOTE:** After certificate and Base Agent installation, which can only be performed via WAP-push link, an additional method is available – installation via Base Agent. It is recommended to use the Base Agent method as the installation requires less user interactions than using the SMS method.

FAMOC default communication is based on HTTPS standard. If the administrator allows an HTTP option during the server installation, it becomes the default setting for sending WAP-push links during FAMOC agent

installation. In such situations, it is also possible to switch to HTTPS by marking *Use https* option. Once the FAMOC agents have been installed, the system does not allow HTTP communication.

If the server doesn't allow HTTP to be used as standard, the option will not be visible in the FAMOC interface.

4. You can perform the operation immediately, postpone it or schedule it for when the handset next connects to the server.

The screenshot shows a web interface for FAMOC Agent installation. At the top, there is a header 'Device list (23)' and a 'Select devices' button. Below this is a table listing 23 devices with columns for device name, IMEI, ICCID, and model. Each row has a small 'X' icon in the rightmost column, indicating that all devices are selected. Below the table is a section titled 'Additional operation settings:'. This section contains three radio button options: 'Perform operation now' (which is selected), 'Perform on:' (with a date and time picker set to 2019-11-07 at 15:49 and a random interval of 0), and 'Schedule operation for later, starting at:' (also with a date and time picker set to 2019-11-07 at 15:49 and a random interval of 0). At the bottom of the settings section are 'Back' and 'Send' buttons.

Device Name	IMEI	ICCID	Model	Action
Harvey Secure (harvey.secure)	353857080043694	17069522502169	Zebra TC51 TC56	X
Harvey Specter (h.specter)	354788082627730	6TEQBVDIMB[...]	myPhone Hammer Energy 18x9	X
Donna Paulsen (donna.paulsen@famoc.com)	869814035283773	869814035283773	Huawei Mate 20 Lite	X
Harvey Specter (h.specter)	355661081875437	ZY3228LH2Q	Motorola Moto G	X
Donna Paulsen (donna.paulsen@famoc.com)	356437085292062		Samsung SM-J530G Galaxy J5 2017	X
Donna Paulsen (donna.paulsen@famoc.com)	354263100797857	R58KB5ZL67W	Samsung SM-J415FN Galaxy J4 Plus	X
Donna Paulsen (donna.paulsen@famoc.com)	356642108417170	R58M430DH2B	Oppo A5	X
Donna Paulsen (donna.paulsen@famoc.com)	353317100004309	353317100004309	Nokia 3	X

Figure 31 FAMOC Agent installation

5. To finish, press **Send**. A text message will be sent to the selected phones with step by step instructions on how to install the certificate.

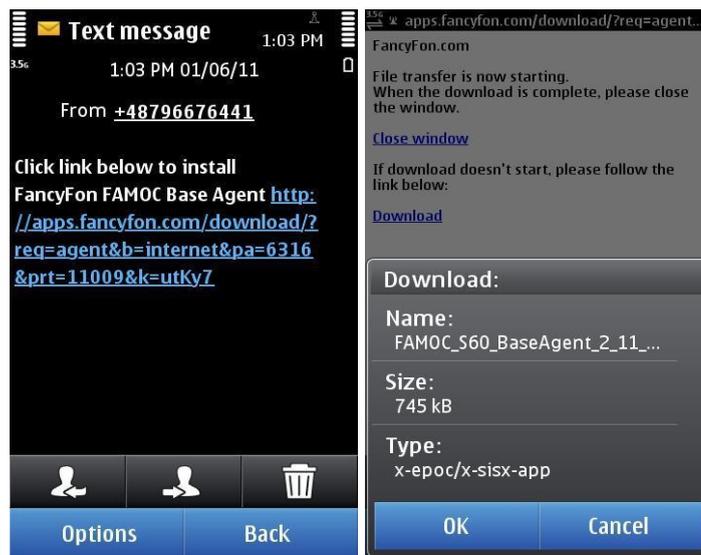


Figure 32 Base Agent installation - phone screens

**NOTE:** Backup Agent installation process includes automatic contacts and calendar backup pattern (see [16.5](#)).

## 15.2 Application

The Applications tab allows maintaining an application repository per organization. Further functions include installing, removing, executing and reporting on applications (viewing a list of operations related to each application, and a list of devices with the application installed). Additionally, this section displays application licenses.

### 15.2.1 Adding applications from Apple App Store

1. On the **Applications tab** press **Add application**.
2. Select option **Add application from Apple App Store**.
3. Type in application name and click **Next**.
4. List of matching applications from Apple App Store will be shown.
5. Select proper application and click **Next**.
6. Application details will be shown with possibility to:
  - a. Select to which FAMOC application group this application should be assigned
  - b. Enable application in corporate store
7. Click **Save** to add application to the repository or click **Save & Edit** to add application and open edit form.

**NOTE:** It is possible to create custom configuration for each application: Configuration tab in edit form of application.

### 15.2.2 Adding applications from Google play

1. On the **Applications tab** press **Add application**.
2. Select option **Add application from Google Play**.
3. Type in application name and click **Next**.
4. List of matching applications from Google Play will be shown.
5. Select proper application and click **Next**.
6. Application details will be shown with possibility to:
  - a. Select to which FAMOC application group this application should be assigned
  - b. Enable application in corporate store
7. Click **Save** to add application to the repository or click **Save & Edit** to add application and open edit form.

### 15.2.3 Adding custom applications

1. On the **Applications tab** press **Add application**.
2. Select option **Add custom application**.
3. Insert application **Name**, **Description** and **Version**.
4. Select **Application group** from the available options or create a new group using the "+" icon.
5. In the **Corporate store availability** section check if the application should be visible for all devices (**Available to everyone** checkbox) or assign user groups or device groups for which application should be available. You can also select options to **Install automatically** or **Upgrade automatically**.
6. Use the **Select file** button to add an application file from your local computer. To install applications on Java handsets it is necessary to upload **.jad** installation file to the system. To enable users to download applications from Apple AppStore and Google Play, mark **the Installation from store** option and input the **Download link**<sup>6</sup>.
7. FAMOC offers a template app icon. To replace it with a different graphics, use the **Change** button.
8. Each application requires the correct platforms and phone models to be assigned. Use the **Platforms** and **Phone models** subtabs and the **Select** button to choose any platform and device model the selected application it is compatible with. Some platforms will be chosen automatically by the system as a suggestion – they may be altered.
9. The **Screenshot manager** subtab allows you to upload exemplary application screenshots.
10. In the **Advanced options** subtab, the administrator is able to add Terms & Conditions and configure some additional settings. If using Windows Mobile handsets, define **Start command** (file UID3 for Symbian

<sup>6</sup> Currently available for Android and iOS devices

devices, application name for Windows Mobile devices) for Base Agent to launch the application. If using Symbian OS, this field will be filled automatically. It is also possible to introduce introductory and closing text message that will appear on end user's device.

11. In **Configuration** subtab, administrator is able to select: custom configuration parameters or predefined configuration (possibility to select one configuration from the list). For some apps (availability depends on the app) it is possible to use Android Managed Configurations. After successful installation of the app, related configuration is sent to the device (based on platform compatibility). Each time application is reinstalled the configuration is sent.

12. In the **Licenses** subtab, administrator is able to add application licenses. Additionally, application redemption codes for Apple Volume Purchase Program (VPP) can be applied in this section. License can be uploaded from a file or pasted directly using the **Paste** button.

Format of an uploaded file or a pasted license:

- The first line should contain license key header (separated by semicolon if there are more parts of the license key),
- The following lines – license keys

Apple redemption codes should contain one column (first line with some license key header, following lines with redemption codes).<sup>7</sup>

Example file contents:

```
Code
CCXFJ8989PQA
ZSPAJ7979NFF
```

15. Click **Save** to add the application to the application repository.

#### 15.2.4 Managing Application Groups

This button directs to the **ADVANCED** → **Settings** → **System advanced** → **Manage application groups** tab, where administrator is able to create and manage groups of application ([see 21.4.7](#))

#### 15.2.5 Installing Applications on Mobile Phones

Application installation is very similar to FAMOC Agent installation ([see 16.1](#))

1. To select an application to install, press the **Install** button next to an application

<sup>7</sup> For more details on getting started with VPP, please refer to Apple's documentation: <http://www.apple.com/business/vpp>

2. Click **Add phones** to select the mobile phones. If the Base Agent is already installed on the selected devices, the recommended installation method is 'Using Base Agent'. Define where the applet should be installed and schedule the operation. By clicking **Send**, administrator sends the required application.<sup>8</sup>
3. Depending on the Base Agent mode on the devices (Confirmation, Information, Silent), users might be prompted to confirm the action on their handsets.
4. The status of the installation can be checked in the **Log** tab.

## 15.3 Configurations

The **Configurations** tab allows the administrator to define and send configurations to any number of devices. The main configuration window shows a list of pre-prepared configurations, categorized and grouped accordingly to the mobile platform, ready to be sent to mobile devices. The dependency tree in the left menu provides easy access to available configurations.

The **show policy status** icon (in the **Configurations** table) displays details about the configuration (type, description, etc.) and the policy status (number of compliant devices, devices with an outdated policy, devices that failed to implement the policy) with an option to **resend** a policy in case it is outdated or in case of a failed installation.

The screenshot shows the 'Configurations' tab in the FAMOC admin interface. At the top, there are navigation tabs: Agents, Applications, Corporate store, Configurations (selected), Messages, Backup, Packages, and Sets of packages. Below these are buttons for 'Add configuration' and 'Delete selected'. A filter section shows 'All platforms' selected, with sub-tabs for Android, Apple, and Windows Phone. The main table lists configurations with the following data:

Name	Type	Method	Description	Server	Platform	Created by	Created on	Actions
Android work profile lock code	Settings for Android work profile lock code	Base Agent			Android 10.0, Android 10.0 - Custo[...]	Harvey Specter	2018-12-07 16:06:33	[Edit] [Send] [Search] [Flag]
Android work profile lock code	Settings for Android work profile lock code	Base Agent			Android 10.0, Android 10.0 - Custo[...]	Harvey Specter	2019-05-13 10:27:30	[Edit] [Send] [Search] [Flag]
Automatic SIM card unlock	Automatic SIM card unlock	Base Agent			Android 10.0 - Samsung, Android 4,[...]	Mike Ross	2019-04-04 14:52:39	[Edit] [Send] [Search] [Flag]
Strongswan VPN	Strongswan VPN	Base Agent			Android 10.0, Android 10.0 - Custo[...]	System Administrator	2018-12-06 11:12:47	[Edit] [Send] [Search] [Flag]
Install certificate	Install certificate	Base Agent			Android 10.0, Android 10.0 - Custo[...]	Mike Ross	2019-06-12 12:33:54	[Edit] [Send] [Search] [Flag]

<sup>8</sup> Installation of Java applications via the Base Agent is only available for Symbian S60 phones.

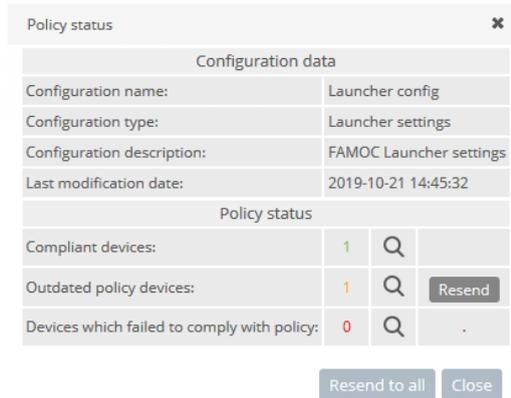


Figure 33 Adding configurations

The configurations accessible in FAMOC are arranged into the following groups:<sup>9</sup>

Configurations Types	
<b>Policy imported from BES</b>	Enables policies to be imported from BlackBerry Enterprise Server
<b>Connectivity/ Networking</b>	Includes configurations such as SyncML Http server synchronization, access point configuration, setting VoIP and Bluetooth parameters as well as various WLAN configurations
<b>Security</b>	Includes setting parameters for antivirus protection and taking actions to provide device security such as device encryption, data wipe out data, device lock and many others
<b>Mail</b>	Includes TouchDown, MailForExchange and IBM Lotus Notes Traveler configurations enabling phone users to synchronize their Email, Tasks, Calendar and Contacts to their phones over the air, using 3G/HSDPA mobile carrier network or WiFi
<b>Tools</b>	Enables numerous device tools, such as camera, clock, alarm, browser or registry key, to be managed
<b>iOS</b>	Includes general iOS configuration
<b>KNOX</b>	Includes configurations that can be applied in the KNOX container
<b>Device customization</b>	Provides configurations enabling the branding and customizing users handsets, e.g. adding operator logo, wallpaper, managing home screen layout
<b>Exchange policies</b>	Provides configurations for Microsoft Exchange ActiveSync mailbox policies <sup>10</sup>

<sup>9</sup> To learn more about FAMOC configurations refer to FAMOC Administrator Guide Appendix: FAMOC Configurations.

<sup>10</sup> To learn more about Microsoft Exchange ActiveSync configuration, please refer to the FAMOC Administrator Guide Appendix: FAMOC Exchange Web Service Addon Installation Guide

Table 2 Configuration types

### 15.3.1 Adding Configurations

1. To add a new position to the list, click the **Add configuration** button.
2. Click **Select configuration type** to choose a configuration template.
3. Every configuration requires a unique name (from now on, visible in the system under this name), the configuration specific parameters need to be provided.

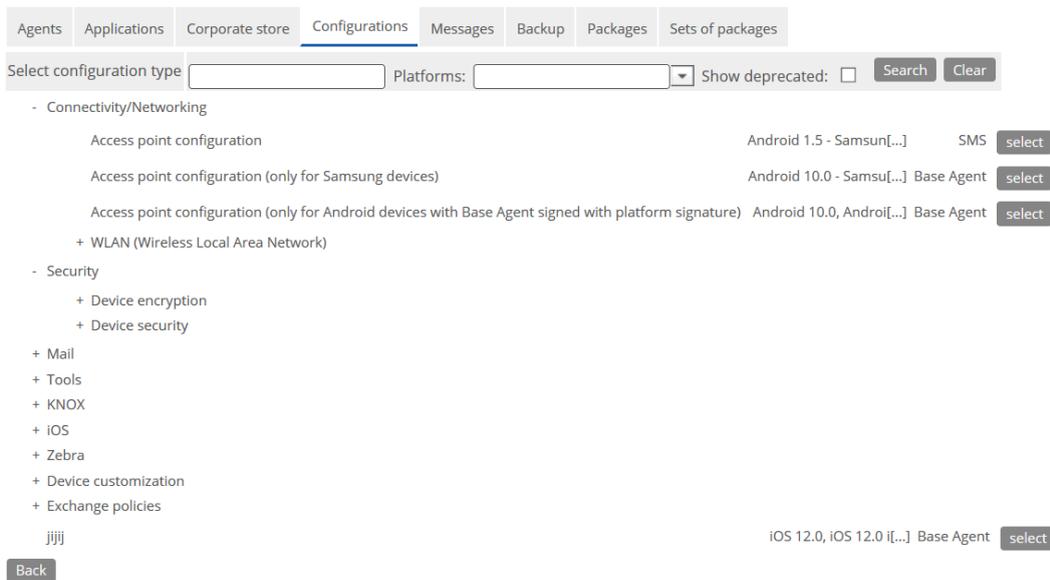


Figure 34 Adding configurations

4. In the **Corporate store** tab you can select if you wish the configuration should be available to everyone or only assigned user groups or device groups. You can also select to **Install** or **Upgrade** configuration **automatically** (it will be automatically installed or updated once any changes are made).



Figure 35 Corporate store availability

### 15.3.2 Sending Configurations to Mobile Phones

Predefined configurations can be sent to mobile phones using the **Send** button. Select mobile devices to be used, by clicking the **Add phones** button. Select Installation method: Personal part or Container. The operation is similar to any other previously described installation<sup>11</sup>.

## 15.4 Messages Tab

The **Messages** tab allows FAMOC administrators to send messages to any number of devices. FAMOC provides bootstrap SMS informing mobile device users about the system's implementation.

1. To create a new message click **Add message**.
2. Provide a **Name**.
3. Select **Message type: SMS** or **Push message**.

For Push message: select **Type: Information** or **Confirmation**

4. Enter the text of the **Message**.
5. To send a message press the **Send** button next to respective message and add phones.

## 15.5 Backup Tab

The **Backup** tab stores copies data from mobile devices onto the central FAMOC server. This allows a restore to be performed after data has been lost or a device has been replaced.

1. To create a new backup template click **Add backup pattern**.
2. Provide a **name** for the backup configuration.
3. Select the type of data to include in the backup pattern. Supported data types include contacts, calendar, SMS messages and folders. It is possible to provide filters such as maximum total size, maximum file size and file types to include or exclude.
4. Press **Add item**.
5. Click **Save** to add the pattern to backup pattern repository.
6. To perform backup press **Execute** button on the repository.

---

<sup>11</sup> For more information refer to [16.1](#)

Agents Applications Corporate store Configurations Messages **Backup** Packages Sets of packages

Back Save

New backup pattern:

Name:

Type	Path	Max total size	Max file size	Files included in backup	Files excluded from backup	
Contacts		<input type="text" value="20"/> MB				X
Calendar		<input type="text" value="20"/> MB				X
Sms		<input type="text" value="20"/> MB				X
Folder	/home/data	<input type="text" value="500"/> MB	<input type="text"/>	<input type="text"/>	<input type="text"/>	X

Add new item:

Data type:

folder path  eg. /home/data C:/PHOTO/

Add item

Back Save

Figure 36 Define backup pattern

**FAMOC backup supports the following platforms:**

- Android
- Apple iPhone
- RIM BlackBerry
- Symbian S60
- Microsoft Windows Mobile
- JAVA
- Samsung Bada
- Symbian UIQ

## 16 Remote Access

Remote Access is a highly secure and easy to use solution, allowing the administrator to troubleshoot mobile devices remotely, over a data connection (e.g. the Internet), empowering the administrator to view the screen and take control over the keyboard.

Remote Access requires the **Base Agent** to already be installed on the phone. For information on how to install a Base Agent refer to [16.1](#).

### 16.1 Remote Access Installation

Remote Access can be installed from the **Device inventory** tab, **Config center** → **Agents** tab or under **Manage** section in **Device** tab (see [14](#) and [16.1](#)) The process is similar to the installation of other FAMOC client components.

## 16.2 Remote Access tab

To start a remote access session, go to the **Remote Access** tab. Phones with Remote Access successfully installed will have the **Run** button enabled.

MANAGEMENT							
ADVANCED		ORGANIZATION					
Monitoring	Devices	SIM cards	Config center	Remote access	Log	Location	Alerts !!!
Settings	Reports						
Sessions							
Other available devices							
Nr	Device model	Platform name	User	Description	IMEI	Number of sessions	
1	Zebra TC51 TC56	Android 6.0	Harvey Secure	Added from startup page	353857080043694		Run
2	myPhone Hammer Energy 18x9	Android 7.0	Harvey Specter		354788082627730		Run
3	Huawei Mate 20 Lite	Android 8.1	Donna Paulsen		869814035283773		Run
4	Motorola Moto G	Android 7.1	Harvey Specter		355661081875437		Run
5	Samsung SM-J530G Galaxy J5 2017	Android 7.0 - Samsung	Donna Paulsen	Dodany ze strony startowej	356437085292062		Run
6	Samsung SM-J415FN Galaxy J4 Plus	Android 8.1 - Samsung	Donna Paulsen	Dodany ze strony startowej	354263100797857		Run
7	Oppo A5	Android 9.0	Donna Paulsen		356642108417170		Run
8	Nokia 3	Android 8.1	Donna Paulsen	Added from startup page	353317100004309		Run

Figure 37 Remote Access tab

Remote Access can be started on mobile phones by:

- Clicking the **Run** link next to the phone
- The device owner by starting Remote Access on the phone

Once a connection between the phone and the FAMOC server has been established, a **Start session** link will be available to start the Remote Access session.

It is also possible to run Remote Access under the **Manage** section in the Device inventory tab.

## 16.3 Remote Access Panel

Clicking the Start session link activates the Remote Access panel. Once the administrator is connected to the end user's device, remote diagnostic and management tools give the administrator even more capabilities over the air than a physical presence. The phone user is able to view all actions on the screen and can terminate the connection at any time by disconnecting or closing the Remote Access agent on the phone.

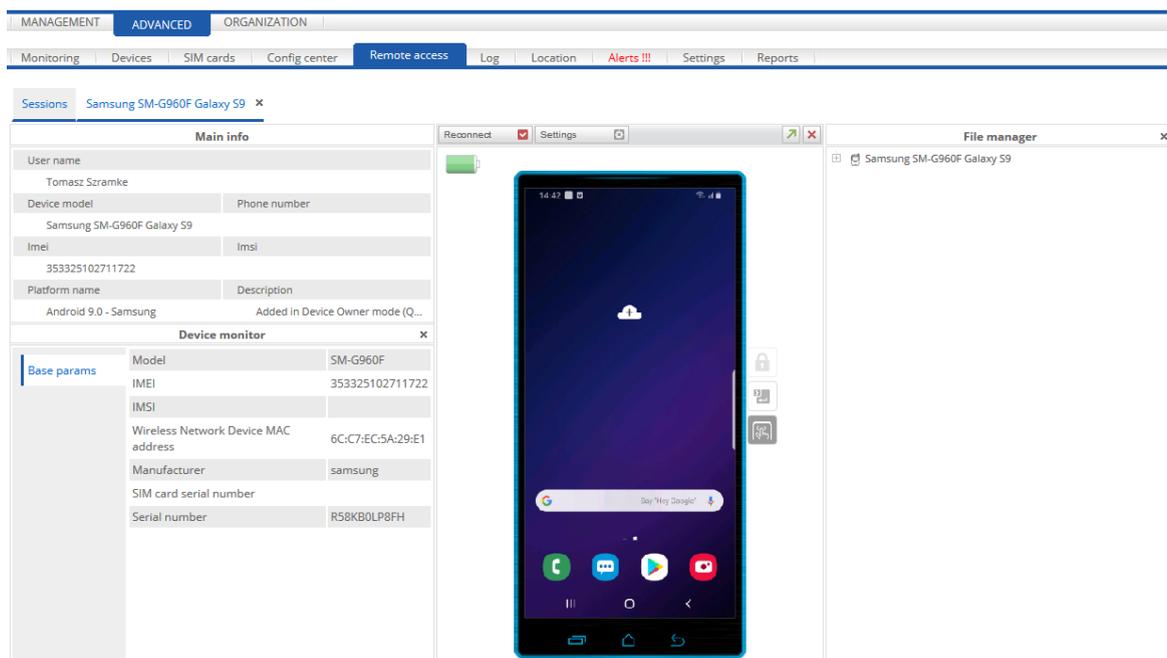


Figure 38 Remote Access panel

A **Lock phone / Unlock** button allows the mobile phone's keyboard to be locked or unlocked remotely. This function is especially useful when, during an idle period in a Remote Access session, the phone switches to standby and locks the keyboard automatically.

Remote Access also allows a **PC keyboard** to be used, for example, entering configuration parameters in a more convenient way than using the phone keyboard.

The **touch screen** symbol enables a touch screen handset to be managed via the FAMOC Remote Access panel.

The panel also displays mobile phone side buttons as well as device **battery charge status** and the **signal strength**.

### 16.3.1 Device Monitor

The Device Monitor<sup>12</sup> provides technical details about the connected mobile device. It can be used to, e.g. analyze and resolve performance and incompatibility issues. The amount of parameters provided through the Device Monitor is dependent on the respective phone platform.

<sup>12</sup> Device Monitor is currently supported on Apple iOS, Android, Windows 10 Mobile, Windows 8.1+, RIM BlackBerry, Symbian S60, Windows Mobile and Symbian UIQ

### 16.3.2 File Manager

The **File Manager**<sup>13</sup> allows files and folders on the remote device to be managed. Next to file operations, such as copy, delete, rename, the File Manager allows files to be uploaded and downloaded. This function can be used to, e.g. replace configuration files or analyze log files of applications.

### 16.3.3 Configuration

Remote Access panel allows administrator to enable/disable phone skin button highlight and to set screenshot quality to adopt the bandwidth requirements to slower connections.

## 17 Log

FAMOC logs any activity performed on phones in a system log by organization. The organization **Log** can be accessed on the **Log** tab and provides the following information:

- Action
- Application/Agent
- Created: date and time of creation
- Last status: date and time of last status
- Status: operation successful/request sent/operation failed
- Message: sent/sending failed
- Phone description
- IMEI
- Phone number
- Phone user
- Operation ID: identifier of the operation
- Actions: possible actions on specific operation (Retry, Cancel)

To organize the log according to a specific issue, scroll through the list at the top, which includes the following categories: unfinished, successful, failed, waiting, waiting for dependent operation, cancelled, operations in progress, request sent, download started, and application started.

It is possible to move directly to device details page by clicking on the IMEI column.

---

<sup>13</sup> File Manager is currently supported on Android, Symbian S60, Windows Mobile and Symbian UIQ.

Activity logs for individual devices can be accessed via the **Devices** tab by clicking the **Manage** button next to the selected phone.

The screenshot displays the 'Device details' and 'Assigned policy' sections for a device. The 'Device details' table includes fields like User (Harvey Specter), IMEI (866237042178633), Serial number (9WVDU18C07004263), Description (Dodany w trybie Device Owner (NFC, NFC Single)), Model (Huawei P20 Lite), Platform (Android 9.0), Device groups, Last contact (2019-11-06 14:04:20), Device Owner mode status (Active), and Work profile status (Does not exist). The 'Assigned policy' section shows 'Policy name' (Harvey Default) and 'Applied on' (2019-11-06 14:04:17). Below these is the 'Exchange proxy status' and 'Connection status' section. A mobile phone icon is shown with the text 'Run Remote access'. At the bottom, there is a navigation bar with tabs: Device details, Applications, Users, Agents, Policies, Log, Alerts, Location, Security, Backup, SIM Cards, Device monitor, Repairs. The 'Log' tab is selected, showing an 'Operations log' table with columns: Action, Component, Create date, Created by, Last status, Status, Message, ID, Group ID, and Actions. The log entries include 'Get device logs', 'Policy refresh', 'Apply security restrictions', 'Device Monitor', and 'Install', all with a status of 'Operation successful'.

Figure 39 Single device log

## 18 Location

The Location tab enables mobile devices to be tracked and the route travelled to be marked out, by handset users over the past days or complete location history. Location history can be also exported to the CSV or TXT file.

The screenshot shows the 'Location' tab in the FAMOC interface. On the left is a map of Gdansk, Poland, with various districts and landmarks labeled. On the right is a table of location history. The table has columns: User, Model, Last measured on, Latitude, Longitude, Cell ID, and Provider. The table contains 14 rows of data for a 'default' user with a 'Lenovo TAB M10' model. The 'Last measured on' column shows dates from 2019-11-08 to 2019-11-06. The 'Latitude' and 'Longitude' columns show coordinates. The 'Cell ID' and 'Provider' columns show network information. The table is paginated with 25 items per page. At the top of the interface, there is a navigation bar with tabs: Monitoring, Devices, SIM cards, Config center, Remote access, Log, Location, Alerts, Settings, Reports. The 'Location' tab is selected. There is also an 'Export' button in the top right corner.

Figure 40 Location tab

## 19 Alerts

The **Alerts** tab gives insight into alerts reported to the system such as for example wrong device configuration, blacklisted application detection or user support request. The table presents time and details of the event as well as device details. Data is listed in chronological order. The system gives possible problem resolution options. On clicking **fix this** button, a list of recommended actions will be displayed.

The top menu groups alerts accordingly to the following categories: unread, read, ignored, and resolved. Once the administrator has become familiar with the alert, it should be **marked as read, unread, ignored or resolved** using an appropriate button.

FAMOC allows filtering alerts accordingly to specific fields (Details, Message, Phone Number, IMEI, User, Description, Model, Platform) and alert types.

Clicking on the alert redirects it to the given phone's details.

Alerts are also visible in the device inventory list under the **Device** tab. Each problem reported to the system is marked in red and by an **!** icon.

Alert		Device							
Created on	Last duplicated on	Details	Message	Phone Number	IMEI	User	Description	Model	Platform
2019-11-08 09:42:22	2019-11-08 09:47:21	Device inactivity time exceeded	866375036333507		866375036333507	Harvey Specter	Dodany w trybie Device Owner (Kod QR)	Nokia 5	Android 9.0
2019-11-08 08:32:50	2019-11-08 08:33:15	KNOX reported license status change.	Internal error.		357988090204335	Mike Ross	Dodany ze strony startowej	Samsung SM-G960F Galaxy S9	Android 9.0 - Samsung
2019-11-07 13:25:44	2019-11-08 09:47:21	Device inactivity time exceeded	357870103761610		357870103761610	default	Dodany ze strony startowej	Samsung SM-A405F Galaxy A40	Android 9.0 - Samsung
2019-11-07 13:05:47	2019-11-08 09:47:21	Device inactivity time exceeded	868862030017390		868862030017390	Mike Ross	Dodany w trybie Device Owner (Kod QR)	Huawei MediaPad T3 10 2017	Android 8.0

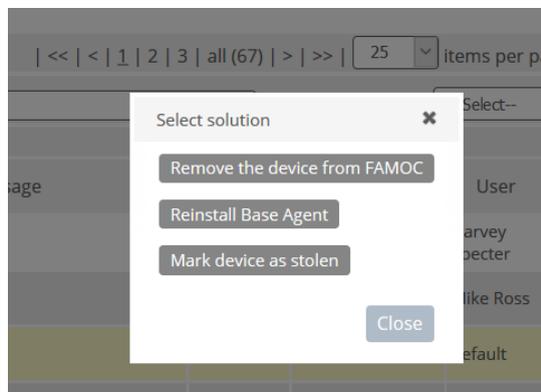


Figure 41 Alerts tab

Types of alerts reported to FAMOC, can be defined under ADVANCED→Settings→Alerts (see section 21.2).

## 20 Settings

The **Settings** tab enables FAMOC settings such as Agent configuration, synchronizations of external servers or alerts reported to the system to be set. It includes the following sections: Policies, Alerts, Server, System advanced.

### 20.1 Policies

This section allows administrator to define FAMOC policy and configure FAMOC Base Agent. It is possible to create several policy templates for specific group of users or devices. Besides the Base Agent settings, you can also attach to the policy configurations, applications and agents<sup>14</sup>.

The default general policy will be applied to the devices that do not belong to any group that have general policy assigned.

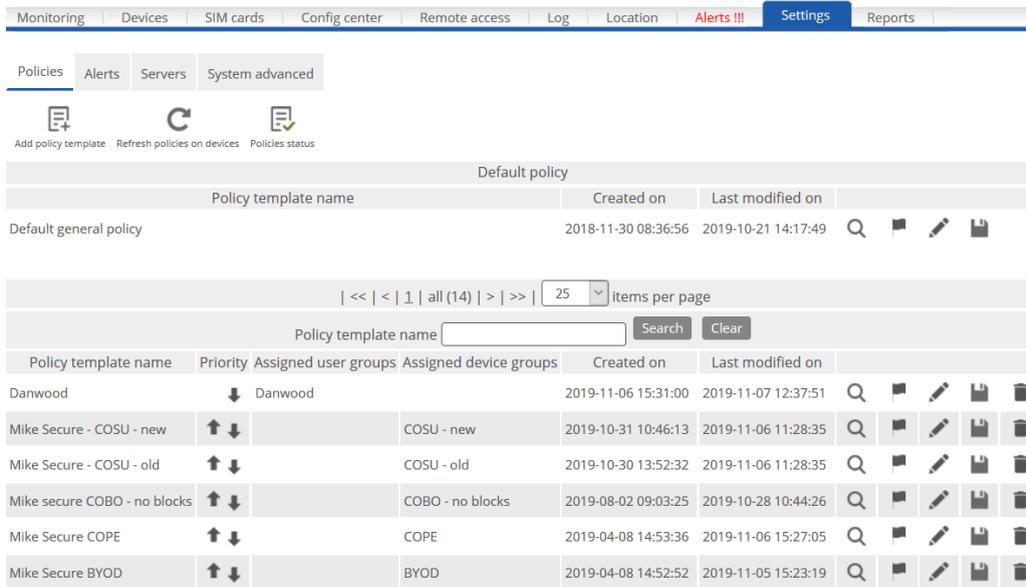


Figure 42 Main policies view

Every policy is divided into several sections:

- **General settings** - basic settings like name, priority, services enabled or schedules
- **Assigned groups** - groups of devices and/or users assigned to the policy

<sup>14</sup> For more information, please refer to *FAMOC Administrator Guide Appendix: Policy Templates*.

- **Policy components** - apps and configurations assigned to the policy
- **Security options** - various security settings including e.g. possibility to lock Bluetooth, phone settings, time settings, file manager, web browser, application installer.
- **Work profile** - possibility to enable and configure container on a device<sup>15</sup>
- **Advanced** - advanced policy settings, device details fields in Base Agent, backup and usage policy

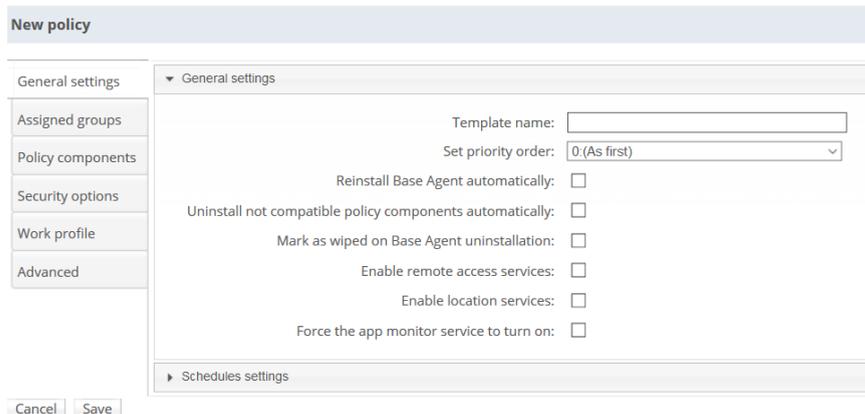


Figure 43 Policy - General settings

## 20.2 Alerts

The Alerts tab allows administrator to manage FAMOC alerts setting.

### 20.2.1 Alerts Types

This subtab displays a list of alerts detected by FAMOC and allows administrator to select which of them should be reported to the system and visible both in the device inventory list and in the **Alerts** tab and in the Log tab.

### 20.2.2 Alert Forwarding

The section provides alerts forwarding rules to be set (e.g. alerts can be forwarded to device owner). Administrator can define which alerts should be automatically directed to specific users. FAMOC also allows setting instant SMS and email notification, as well as forward the alerts to an external SNMP or syslog system.

In order to forward the alerts to a user (or a group of users) each user needs to have a mobile number/email address assigned. In order to forward the Alerts to an SNMP server an appropriate server needs to be defined in the **ADVANCED** → **Settings** → **Servers** tab.

Alerts can be forwarded to external Syslog server. In order to **forward** alerts to external syslog an appropriate server needs to be defined in the **ADVANCED** → **Settings** → Servers tab.

<sup>15</sup>For more information, please refer to *FAMOC Android Work profile Guide*.

It is possible to specify custom message fields like: from (name & email), reply to email, email subject, email message, SMS message. These fields will be used in email / SMS notifications while specified alert appears in the system.

In addition it is possible to use several tokens (such token will be replaced with the data fetched from FAMOC server); allowed tokens are:

- in email subject field: `_ALERT_ID_` which will be replaced with FAMOC alert ID
- in email content field: `_ALERT_ID_` - FAMOC alert ID

`_ALERT_CREATED_ON_` - alert creation date

`_ALERT_DESCRIPTION_` - alert description

`_ALERT_MESSAGE_` - alert message

`_PHONE_NUMBER_` - phone number of the device

`_IMEI_` - IMEI of the device

`_MODEL_` - model of the device

`_USER_` - "Name Surname" of the user

`_COMPANY_` - company of the user

`_USERGROUPS_` - list of the user groups

`_DEVICE_DESCRIPTION_` - description of the device

`_GEN_POLICY_` - name of the general policy of the device

`_SEC_POLICY_` - name of the security policy of the device

- in SMS message: `_ALERT_ID_` - FAMOC alert ID

`_ALERT_DESCRIPTION_` - alert description

`_ALERT_MESSAGE_` - alert message

`_USER_` - "Name Surname" of the user

The screenshot displays the 'Alert forwarding settings' configuration page. The interface includes a navigation menu with 'Policies', 'Alerts', 'Servers', and 'System advanced'. The 'Alerts' section is active, showing 'Alert types' and 'Alert forwarding' options. The 'Alert forwarding' section is expanded, revealing a 'New destination' form with a 'Name' field. Below this, the 'Message settings' section includes fields for 'From (name)', 'From (email)', 'Reply to (email)', and 'Subject'. The 'Email content' field contains a template for an email message, and the 'SMS message' field contains a template for an SMS message. The 'Syslog message' field contains a template for a syslog message. The page also includes 'Back' and 'Save' buttons.

Figure 44 Alert forwarding settings

### 20.2.3 Blacklisted Applications

The section manages list of forbidden applications, preventing the mobile phone coming under attack from malware, spyware or viruses. The Blacklisted Application Alerting is based on Device Monitor reported data and verifies whether certain applications are installed on the device and alerts the administrator accordingly. In order to have up-to date reports it is advisable to schedule device monitor sessions to e.g. once a day or once a week (**Settings** → **Agents** → **Base Agent**).

To add an item to the blacklist:

1. Press **Add blacklisted application** button.
2. Provide the **Name** of the application.
3. Select a proper **platform** which should it be applied to.
4. Define phrases on the basis of which the application will be searched on the device during a Device Monitor session. Depending on the mobile platform, Device Monitor monitors different application parameters:

- BlackBerry: Application Full Name
- Symbian S60: Application UID, Application Full Name, Application Short Name, Application File
- Apple iOS: Process Name
- Android: Application Full Name, Application File

- Windows Mobile: Application Full Name
5. To finish press **Save**.

## 20.2.4 Whitelisted Applications

The section manages list of allowed applications based on Device monitor data. It verifies whether applications not from the list are installed on device and alerts the administrator accordingly.

To add an item to the whitelist:

1. Press **Add whitelist** button.
2. Provide a **Name** of the whitelist.
3. Select a proper **platform** to apply to.
4. Set list as **Active**.
5. Select applications:
  - Manually, by clicking on the **Add** button (popup with text field will appear).
  - From Device monitor data, by clicking on **Select from Device monitor** button. In this case popup with list of existing Device monitor sessions for devices will appear. On the popup there is possibility to preview the list of applications and **Select** button. After pressing on it, all the applications reported it selected Device monitor session will be linked to the whitelist.

In alerting, all active whitelists for the specific platform will be used.

## 20.3 Servers

The **Servers** tab allows an external server repository to be maintained. The section enables Exchange, SNMP, Certificate Authority, SecureSource, servers to be added to the system. Further functions include synchronization and removing the servers.

1. Press **Add server** to set **Exchange, SNMP, Certificate Authority, SecureSource or Syslog** configuration and introduce the necessary parameters.
2. Once the settings are saved, the server can be synchronized by pressing **Synchronize now** button on the server list.

On the server list, next to the Certificate Authority server(second icon from the right)it is possible to generate and install CA certificates on multiple devices. In addition there is a possibility to preview devices with generated certificates (last icon). Certificate list is sorted by **Expires** column. Popup provides an option to renew several certificates.

Parameter	Description
-----------	-------------

<b>Name</b>	Name of the server
<b>Address</b>	The IP address of the given Exchange server
<b>Port</b>	The port of the given Exchange server
<b>Interval</b>	The FAMOC-Exchange server synchronization interval
<b>Number of stored Exchange synchronizations</b>	Number of synchronized data packages stored on the server available for browsing in data synchronization history/log.
<b>Web Service user</b>	Name of a Web Service user
<b>Web Service user password</b>	Web Service user password
<b>Synchronization type</b>	Type of synchronization data: all data (users and devices)/devices of the existing users
<b>Synchronize only existing devices in FAMOC</b>	Yes/No
<b>Synchronize devices that contacted Exchange within the last..</b>	Additional synchronization of devices that contacted Exchange within the last: Day/Three days/Week/Two weeks/ Month/Year

Table 5 Exchange configuration parameters

Parameter	Description
<b>Name</b>	Name of the server
<b>Address</b>	The IP address of the given SNMP server
<b>Port</b>	The port of the given SNMP server
<b>Interval</b>	The FAMOC-SNMP server synchronization interval

Table 6 SNMP configuration parameters

Parameter	Description
<b>Type</b>	Type of the server (Microsoft CA)
<b>Name</b>	Name of the server
<b>Address</b>	The IP address of the given CA server
<b>Port</b>	The port of the given CA server
<b>Synchronization interval</b>	The FAMOC-Certificate Authority server synchronization interval
<b>Revoke certificates after wipe of the device</b>	If checked, certificates will be revoked on device wipe.
<b>Certificate request key size</b>	Size of the request key (1024, 2048 ...). iOS and Symbian devices accepts only 1024 or 2048 key size. If greater value will be set, 2048 key size will be used.

<b>Server machine name</b>	Server machine name
<b>Certificate Authority name</b>	Certificate Authority name
<b>Web Service user</b>	Web Service user
<b>Web Service user password</b>	Web Service user password
<b>Certificate Authority domain</b>	Domain of the Certificate Authority
<b>Certificate template</b>	Template of the certificate
<b>Common name (CN)</b>	<p>Certificate common name. Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required):</p> <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> <li>• Separator (like dot, colon or at)</li> <li>• Second field from FAMOC db</li> </ul>
<b>Country (C)</b>	Country
<b>Locality (L)</b>	Locality
<b>State or province (ST)</b>	State or province
<b>Organization (O)</b>	Organization name
<b>Organizational unit (OU)</b>	Organizational unit name
<b>Additional SAN attribute (DNS)</b>	<p>Subject Alternative Name, DNS field.</p> <p>Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required):</p> <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> <li>• Separator (like dot, colon or at)</li> </ul> <p>Second field from FAMOC db</p>
<b>Additional UPN attribute</b>	<p>User Principal Name.</p> <p>Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required):</p> <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> <li>• Separator (like dot, colon or at)</li> </ul> <p>Second field from FAMOC db</p>
<b>Certificate source</b>	Downloaded from file / Generated and signet by CA
<b>Certificate file (.PFX)</b>	Upload the certificate file
<b>PFX file password</b>	Set the PFX file password

Table 7 Microsoft Certificate Authority configuration parameters

Parameter	Description
<b>Type</b>	Type of the server (FAMOC CA)
<b>Name</b>	Name of the server
<b>Address</b>	The IP address of the given CA server
<b>Port</b>	The port of the given CA server
<b>Synchronization interval</b>	The FAMOC-Certificate Authority server synchronization interval
<b>Revoke certificates after wipe of the device</b>	If checked, certificates will be revoked on device wipe.
<b>Certificate request key size</b>	Size of the request key (1024, 2048 ...). iOS and Symbian devices accepts only 1024 or 2048 key size. If greater value will be set, 2048 key size will be used.
<b>PKCS#12 CA certificate file</b>	Certificate file
<b>PKCS#12 CA certificate file password</b>	Password for certificate file
<b>Period</b>	Issued certificates validity period
<b>Common name (CN)</b>	Certificate common name. Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required): <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> <li>• Separator (like dot, colon or at)</li> <li>• Second field from FAMOC db</li> </ul>
<b>Country (C)</b>	Country
<b>Locality (L)</b>	Locality
<b>State or province (ST)</b>	State or province
<b>Organization (O)</b>	Organization name
<b>Organizational unit (OU)</b>	Organizational unit name
<b>Additional SAN attribute (DNS)</b>	Subject Alternative Name, DNS field. Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required): <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> <li>• Separator (like dot, colon or at)</li> </ul> Second field from FAMOC db
<b>Additional UPN attribute</b>	User Principal Name. Field can be filled with custom value or selected from FAMOC db. It is possible to select 3 parts (not required): <ul style="list-style-type: none"> <li>• Field from FAMOC db (e.g. user login or some custom field)</li> </ul>

	<ul style="list-style-type: none"> <li>Separator (like dot, colon or at)</li> </ul> Second field from FAMOC db
<b>Key usage</b>	User can mark sections which will need certificate to unlock
<b>Extended Key Usage</b>	User can mark more advanced sections which will need certificate to unlock
<b>OID (Add extension)</b>	User can define custom section by OID code which will need certificate to unlock
<b>Certificate source</b>	Downloaded from file / Generated and signed by CA
<b>Certificate file (.PFX)</b>	Upload the certificate file
<b>PFX file password</b>	Set the PFX file password

Table 8 FAMOC Certificate Authority configuration parameters

Parameter	Description
<b>Name</b>	Name of the server
<b>File server type</b>	SecureSource server type (currently available only a WebDav Server)
<b>Address</b>	The IP address of the given File Repository server
<b>Port</b>	The port of the given File Repository server
<b>Synchronization interval</b>	The FAMOC-SecureSource connector synchronization interval
<b>Path to the resources</b>	Path to file repository

Table 9 SecureSource configuration parameters

Parameter	Description
<b>Name</b>	Name of the server
<b>Address</b>	The IP address of the given Syslog server
<b>Port</b>	The port of the given Syslog server
<b>Interval</b>	The FAMOC-Syslog server synchronization interval

Table 10 Syslog configuration parameters

## 20.4 System advanced

The System advanced subtab allows administrator to manage general FAMOC server parameters, such as enrollment page configuration, custom fields, configuration types or reference policies.

## 20.4.1 Enrollment

This section provides the system installation on mobile devices using a web interface. If the standard WAP-push link installation is not applicable, it is possible to download FAMOC client components from the FAMOC enrollment webpage, using the built-in phones web browser.

Once a user logs on the website using their mobile device, he is allowed to download the certificate, FAMOC Base Agent and Base Agent configuration file.

Parameter	Description
<b>General settings</b>	
<b>Enabled/Disabled</b>	Sets if installation on mobile devices using a web interface is allowed. Default value: Enabled
<b>Enrollment address</b>	Easy URL to the bootstrap webpage. Default value: server address/Organization Name Recommended bootstrap address.
<b>Advanced settings</b>	
<b>Alternative full address</b>	Alternative URL to the bootstrap webpage. Option is deprecated
<b>Server name for VirtualHost in Apache</b>	An easier domain name, which is an alternative link to access bootstrap webpage.
<b>Enrollment page title</b>	Custom bootstrap page title Default value: FAMOC
<b>Preferred agent installation source</b>	Sets agent installation source. Possible to choose: FAMOC and Application store.
<b>Enrollment page header</b>	Custom bootstrap page header Default value: FAMOC
<b>Device description required</b>	Require device description on bootstrap page. Default value: this option is not checked
<b>Show certificate on enrollment page</b>	Sets if certificate download link is shown on startup page. Possible values: <ul style="list-style-type: none"> <li>Based on server certificate – global setting will be used (if certificate on the server is trusted – certificate will not be shown)</li> <li>Do not show certificate</li> <li>Show certificate</li> </ul>

<b>Enrollment code expiry period</b>	Sets enrollment code expiry period: by default not set Possible values: 1 day, 1 week, 2 weeks, 1 month.
<b>Login settings</b>	
<b>User authentication required</b>	If marked, the user will be required to provide his login and password to FAMOC in order to access the website (LDAP/AD details will be used if synchronization was enabled). If unmarked, two additional options appear: Global password or startup code and Only startup code. Default value: this option is checked
<b>Global password or enrollment code</b>	Global password to the bootstrap website. If the administrator inputs a password, end-users will be asked to provide it to access the website. This password (in contrast to the User Authentication) is the same for all users. With this option, it is also possible to provide startup code of the device. If the radio button is marked and password field is left empty then no login restrictions will be applied.
<b>Only enrollment code</b>	Access to the bootstrap page only with startup code for device, generated from ADVANCED→Devices list tab.
<b>User settings</b>	
<b>Default user</b>	Selects the default user to whom the devices will be assigned. If none is selected, the user will be asked to choose an option from the list upon accessing the startup website.
<b>Device group settings</b>	
<b>Default device group</b>	The device group selection enables the administrator to select the default device group upon enrollment or ask the user during enrollment process. 'none' means that no group is selected and the user will be asked to choose an option from the list upon accessing the startup page.
<b>Package settings</b>	
<b>Only Base Agent with policies</b>	Only Base Agent with its configuration will be available on enrollment page. Default value: This option is selected by default
<b>Use selected package</b>	Allows a single package to be defined ( <a href="#">see 16.6</a> ) that will be automatically installed on the device, which accesses the enrollment webpage.
<b>Automatic package selection based on device platform</b>	Allows a package set to be defined, including a number of packages for different mobile platforms. FAMOC will automatically detect devices accessing the website and provide the proper installation set.
<b>Let user choose package</b>	Enables user to manually select the desired installation package.

Welcome page settings	
<b>Show welcome page</b>	Enabled/Disabled Default value: option is not checked
<b>Welcome message</b>	Text that appears once the user opens an enrollment page. It's possible to add HTML code to this text field: [LINK]...[/LINK] and [EMAIL]...[/EMAIL]. In case no text is entered in this field, the enrollment welcome page will not be displayed to a user. He will be directed to a standard bootstrap page with links to download FAMOC client components.
<b>Welcome message link</b>	Link tags in "Welcome message" will be replaced with address provided in this field
<b>Welcome message email address</b>	Email tags in "Welcome page" will be replaced with address provided in this field.
<b>Welcome button</b>	Text that will be displayed on button enabling users to proceed with the bootstrap process e.g. Next / Continue / Accept
<b>Welcome page with approval checkbox</b>	Enables the creation of an approval checkbox that users must select in order to enroll the device.
<b>Approval message</b>	Customizable message for Approval checkbox. By default: Accept terms of use.
Enrollment message settings	
<b>From (name)</b>	Sender name. By default: FAMOC Server
<b>From (email)</b>	Sender email address.
<b>Reply to (email)</b>	Reply email address.
<b>Subject</b>	Subject of the message.
<b>Email content</b>	Customizable email message content with a possibility to use tokens.
<b>SMS message</b>	Customizable SMS message content.

Table 11 Startup

When package settings are configured to "Use selected package", "Automatic package selection" or "Let the user choose package" it is necessary to first create **Bootstrap Packages** and **Set of Packages** (see 16.7). While creating a Package it is crucial to mark **Allow Bootstrap** to make it available in the Startup section.

## 20.4.2 Custom Fields

This section enables customized fields to be added to the system. The administrator is allowed to create additional descriptions in: **Users, Groups, Devices** and **SIM Cards** section. This option is helpful when using

the advanced search function. If adding a dictionary field to FAMOC, it is necessary to create additional dictionaries in **Dictionaries** tab under **ORGANIZATION** ([see 12.6](#)).

1. To add a custom field press **Add**.
2. Provide a **Name** of the field.
3. Select a **table** which should it be applied to (Devices, SIM Cards, Groups, Users).
4. Define data format (text/number/password/date/dictionary).
5. To finish press **Save**.

### 20.4.3 Configuration Types

The main repository displays a tree of existing groups of configuration types (predefined and custom) with custom configuration types. The administrator is allowed to perform some operations on each tree item (excluding predefined items). The list can be expanded or collapsed using „-“/ „+“ marks (on the left of the group name); by default it is expanded.

The tab allows administrator to add new configuration types and groups of configuration types to FAMOC. It is also possible to create types of configuration using custom files or files from iPhone Configuration Utility tool.<sup>16</sup>Created templates will appear in the **ADVANCED**→ **Config Center**→ **Configuration**→ **Add configuration** section.

### 20.4.4 Reference Policies

This section enables benchmark security policies to be added to the system. To define a new set of standard device management procedures:

1. Press **Add policy** button
2. Provide a **Name** for the policy
3. Define specified parameters such as inactivity timeout, required password length, memory encryption rules, backup schedule etc.
4. Press **Save** to finish

### 20.4.5 Apple Certificates

To be able to make use of the FAMOC Mobile Device Management capabilities it is necessary to:<sup>17</sup>

- Register on the Apple website and create an Apple ID<sup>18</sup>.

<sup>16</sup> To learn more about FAMOC configuration types refer to *Custom Configuration Types* guide.

<sup>17</sup> For more information on generating an SSL certificates for the Apple Push Notification Service, please refer to *FAMOC iOS Configuration Guide*.

<sup>18</sup> To create an Apple ID, go to: <https://appleid.apple.com/>

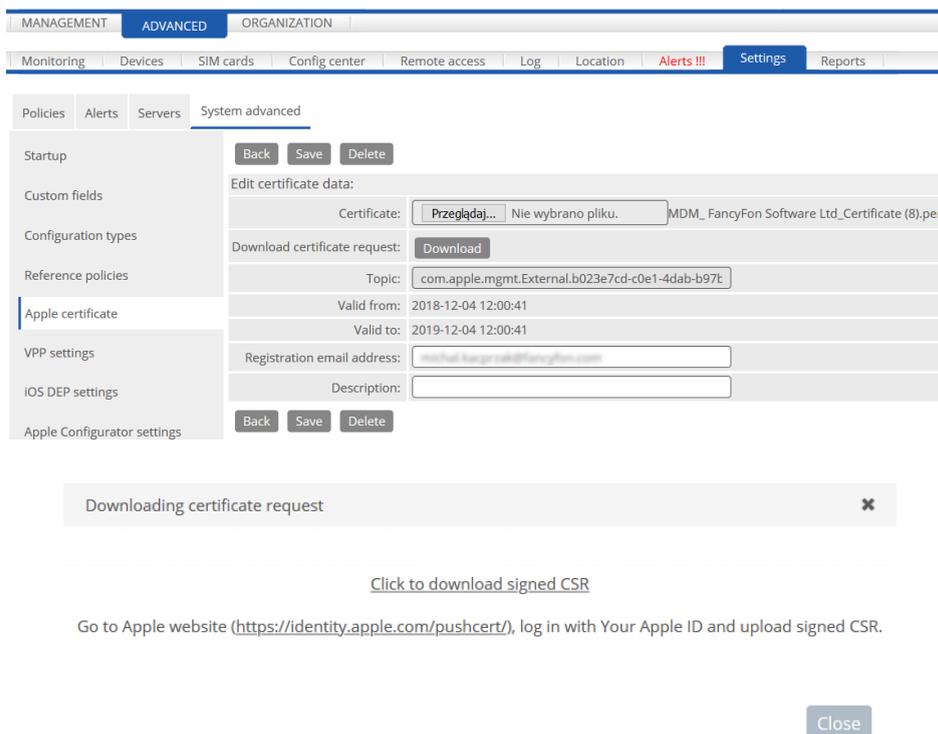
- Generate CSR (Certificate Signing Request) using the FAMOC console.
- Sign the certificate request file on the FancyFon Partner Portal. (This step is not necessary if license with certificate is applied on server).
- Upload the signed CSR on the Apple website and generate an Apple certificate.
- Upload the Apple certificate to the FAMOC console.

This section describes how to generate a CSR (Certificate Signing Request) and upload Apple Certificates to FAMOC.

To generate a CSR, click on the **Generate certificate request** button.

To upload Apple certificate, use the **Browse** button and press **Save**.

The **Delete** button allows administrator to remove the certificate, however this option is only available if none of the devices uses this certificate, since after deleting a certificate being in use, it is no longer possible to communicate with such device.



**Figure 45 Apple Certificates**

## 20.4.6 VPP Settings

VPP token implementation allows administrator to synchronize licenses of the VPP account. To manage VPP settings, go to **ADVANCED** → **Settings** → **System advanced** → **VPP settings**.

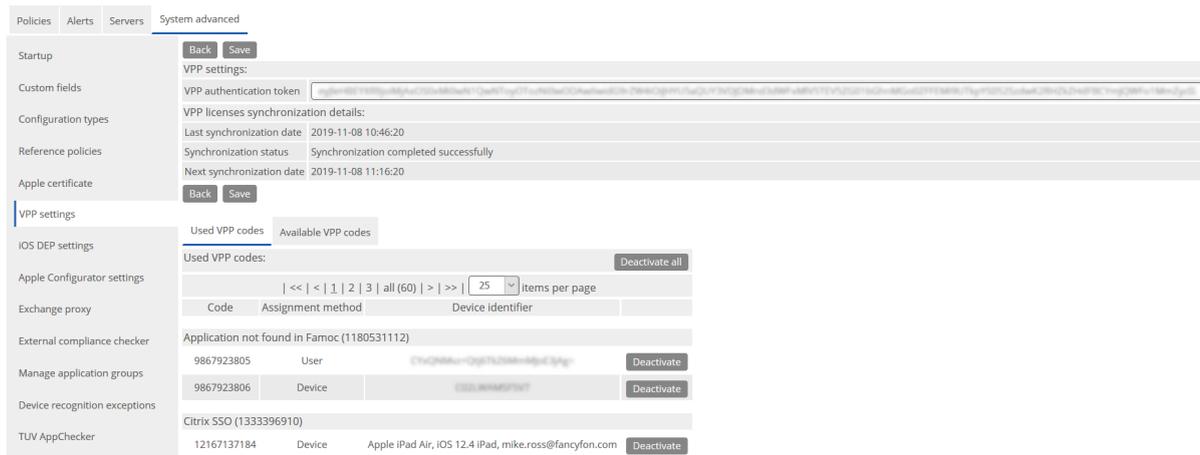


Figure 46 VPP settings

1. Generate token on your VPP account.
2. Paste token in FAMOC VPP settings.
3. **Save** settings.
4. List of Available/Used VPP codes is available after synchronization.
5. It is possible to manage used VPP codes and deactivate them.

Used VPP codes		Available VPP codes	
Code	Assignment method	Device identifier	
Application not found in Famoc (1180531112)			
9867923805	User	CYxQNMvz+Qtj6TkZ6MmMJoE3jAg=	Deactivate
9867923806	Device	C02LWAMSF5V7	Deactivate
Citrix SSO (1333396910)			
12167137184	Device	Apple iPad Air, iOS 12.4 iPad, mike.ross@fancyfon.com	Deactivate
Mirror to Mac or Windows PC (1350663974)			
12321539065	Device	Apple iPad Air, iOS 12.4 iPad, mike.ross@fancyfon.com	Deactivate
Facebook (284882215)			
4946658109	User	CYxQNMvz+Qtj6TkZ6MmMJoE3jAg=	Deactivate
4946658110	Device	Apple iPad Air, iOS 12.4 iPad, mike.ross@fancyfon.com	Deactivate
4946658111	Device	FK1WTM1QJCLH	Deactivate
Application not found in Famoc (307868751)			
466352033	Device	GCGV92CKHP9X	Deactivate
466352034	Device	Apple iPad Air, iPadOS 13.1, mike.ross@fancyfon.com	Deactivate
466352035	Device	Apple iPad Air, iOS 12.4 iPad, mike.ross@fancyfon.com	Deactivate
466352036	Device	C8QWJ5FYJWF7	Deactivate

Figure 47 VPP Token

## 20.4.7 iOS DEP settings

Synchronization with Apple Device Enrollment Program provides a fast and easy way to deploy MDM profile on your corporate iOS devices.

A DEP account synchronization can be configured in section **ADVANCED** → **Settings** → **System advanced** → **iOS DEP settings**:

1. Click **Add account**.
2. Generate a public/private key pair.
3. Download public key.
4. Create virtual server on <https://deploy.apple.com> and upload public key.  
**NOTE:** Public key filename is required: PublicKey.pem
5. Upload server token in **FAMOC's iOS DEP account settings**.
6. Assign devices to virtual MDM server on the Apple portal.
7. In **FAMOC's iOS DEP account settings** select default user of the devices.
8. Setup device synchronization interval.
9. Setup panes configuration and press **Save**.

- 10. After configuration is saved, **Start initial synchronization** to synchronize all currently assigned devices on virtual MDM server. FAMOC synchronizes devices as scheduled.
- 11. **Initial synchronization** button is now replaced by **Force synchronization**, **Stop synchronization** and **Restart synchronization** buttons to control device synchronization.

Figure 48 iOS DEP account settings

## Setup panes configuration<sup>19</sup>

<b>Enable Supervised mode on devices</b>	Possibility to enable Supervised mode on the devices. Supervised mode enables additional MDM features on iOS.
<b>Disable removal of the MDM using UI on device</b>	If checked, MDM profile can't be removed by user. Option available only if 'Enable Supervised mode on devices' option is on.
<b>Department</b>	MDM profile information: department.
<b>Support phone number</b>	MDM profile information: support phone number.
<b>Support email address</b>	MDM profile information: support email address
<b>Hide and disable the passcode pane</b>	Possibility to disable the passcode pane.
<b>Disable Location Services</b>	Possibility to disable location services.
<b>Disable restoring from backup</b>	Possibility to disable restoring device from backup.
<b>Disable signing into Apple ID and iCloud</b>	Possibility to disable signing into Apple ID and iCloud.
<b>Skip Terms and Condition</b>	Possibility to skip Terms and Condition pane.
<b>Skip Touch ID setup</b>	Possibility to skip Touch ID setup pane.
<b>Skip Apple Pay setup</b>	Possibility to skip Apple Pay setup pane.

<sup>19</sup> For more info about DEP please refer to Apple documentation at <http://www.apple.com/business/dep/>

<b>Skip zoom setup</b>	Possibility to skip zoom setup pane.
<b>If the Restore pane is not skipped, remove Move from Android option from it</b>	If set, removes "Move from Android" option from restore pane.
<b>Disable Siri</b>	Possibility to disable Siri.
<b>Disable automatically sending diagnostic information</b>	Possibility to disable diagnostic information sending.

Table 12 iOS DEP settings

### 20.4.8 Apple Configurator

This section allows administrator to generate tokens that will be used during iOS device enrollment using Apple Configurator.

For more information, please refer to Apple Configurator Enrollment in FAMOC.

### 20.4.9 Exchange proxy

This section allows administrator to use FAMOC as a proxy to Exchange server.

1. Press **Add forwarding address** button.
2. Select **external address** and **port**. The list of available external addresses and ports can be created only using FAMOC reconfigurator<sup>20</sup>.
3. **Authorization cache timeout** - specifies how often to refresh the security-related caches (available options - (No timeout or between 2 minutes - 1 hour)
4. Input the **forwarding address**.
5. Define **access policy** (allow access for all devices or managed devices with one or more policies from the list below).
6. Press **Save**.

Available access policies that can be used with the main policy:

1. Allow access for all devices
2. Allow access for managed devices Allow access for devices from whitelist
  - a. Allow access for devices which last contact was not before ...
  - b. Allow access for devices from the list
  - c. Block access for jailbroken devices

<sup>20</sup> For more information, please refer to *Exchange ActiveSync Proxy Configuration* document.

- d. Block access for devices on which general policy failed
  - e. Block access for devices on which security restrictions failed
  - f. Block access for devices on which alert occurs
  - g. Allow access for KNOX identifiers only\*
3. Additional list of authorized identifiers - administrator can define a list of the identifiers that are allowed to communicate with EAS proxy, even if the EAS proxy policy allows only managed devices. (List can be defined in the "Additional list of authorized identifiers" section. If option "Alert about connection attempt by unmanaged device" is set in EAS proxy settings - there will be possibility to add the identifier reported in alert directly to this list.)

It is allowed to set several policies simultaneously.

When selecting a policy allowing access for devices from Whitelist, it is possible to define a list of identifiers allowed when accessing the Exchange. Identifiers (IMEI, device UID, serial number or Exchange ID) can be added manually via **Add identifier** which opens the popup with a text field.

Once the settings are saved, FAMOC will be used as a proxy to Exchange server. FAMOC identifies devices using IMEI, serial numbers, UID or Exchange ID. In case a device, which attempted to connect to Exchange, could not be identified, FAMOC generates alerts to all of the devices assigned to the user. Assigning Exchange ID to each device can fix the alerts.

When selecting a policy of blocking access for devices on which the alert was detected, multiple alerts can be selected from the list. Each reported alert from the list will block access to Exchange. Alerts can be marked as ignored or resolved which means that access to Exchange will not be blocked.

**There are additional alert settings:**

- 1. Alert on connection attempt by blocked device – if marked, alerts will be generated in admin interface when blocked device tries to connect to Exchange.
- 2. Alert on connection attempt by unmanaged device – if marked, alert will be generated in admin interface when unmanaged device tries to connect to Exchange.

#### 20.4.10 External compliance checker

This section allows administrator to use FAMOC as a compliance checker for some external environment like CISCO ISE, Checkpoint or any other.

- 1. Press **Add compliance checker** button.
- 2. Provide checker name and select checker type from the list.
- 3. Checker identifier will be automatically generated (it should be used as a checker instance identifier).

4. Define **compliance policy**.
5. Press **Save**.

Available compliance policies:

1. Allow access for devices managed in FAMOC
2. Allow access for device which last contact was not earlier than selected period of time
3. Block access for jailbroken/rooted devices
4. Block access for devices on which selected alerts occur

It is allowed to set several policies simultaneously.

It is required to configure CISCO ISE with compliance checker identifier (mentioned above) and FAMOC web service user credentials.

For more details about FAMOC integration with CISCO ISE please refer to FAMOC CISCO ISE Integration guide.

Checkpoint, or any other external environment that wants to verify compliance of the device can use FAMOC web service – checkDevice which returns the compliance status.

For more details about checkDevice web service usage please refer to FAMOC WebService APIs guide.

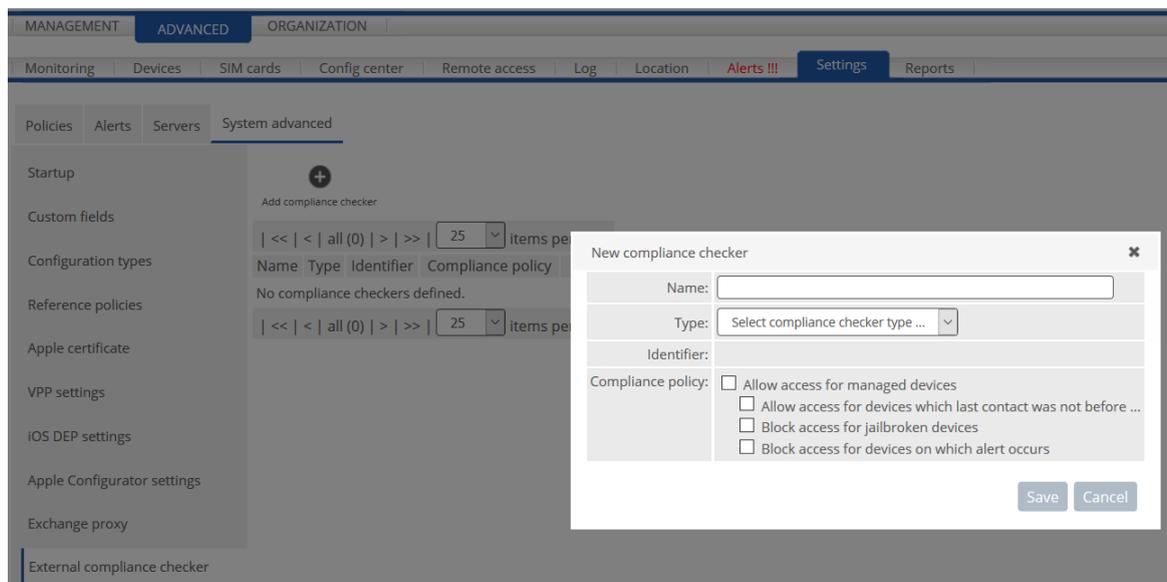


Figure 49 External compliance checker

## 20.4.11 Manage Application Groups

This section allows administrator to create, delete or edit name and icon of application groups available for selection afterwards while adding new applications to FAMOC. It is also possible to view all the applications included in each group. While deleting a group, administrator is prompted to move all the applications included in this group to a different one.

### 20.4.12 Manage Device Groups

This section allows administrator to create, delete or change device groups. It is also possible to view devices included in each group.

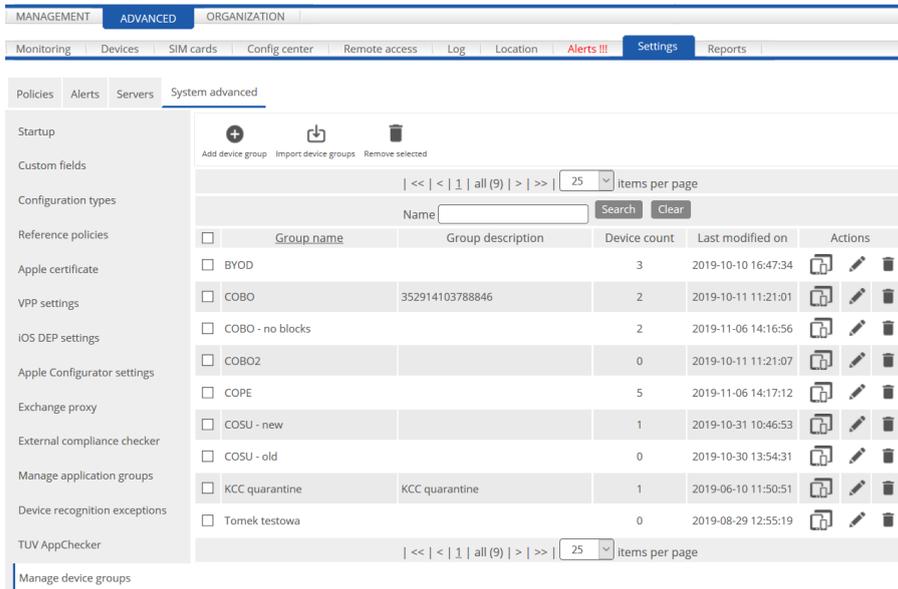


Figure 50 Manage device groups

### 20.4.13 Android Enterprise settings

This section allows the administrator to enroll and synchronize a Managed Google Play account for use with Android Work Profile (see 'Android Work Profile Guide' for more details).

### 20.4.14 Knox Mobile Enrollment settings

This section allows administrator to generate/regenerate Base Agent apk link for Knox Mobile Enrollment. It is also possible to export device list needed to activate KME in next steps.

For more details please see KME Documentation.

System advanced				
Startup	MDM Server URI	MDM agent apk link	Custom JSON Data	Options
Custom fields	venice.fancyfon.com	venice.fancyfon.com/kme/index.php/54hShnevBYtvhmVyzzeF5SimX1k6yL6Q	Not required.	Export device list
Configuration types				
Reference policies				
Apple certificate				
VPP settings				
IOS DEP settings				
Apple Configurator settings				
Exchange proxy				
External compliance checker				
Manage application groups				
Device recognition exceptions				
TUV AppChecker				
Manage device groups				
Android Enterprise settings				
Knox Mobile Enrollment settings				
Samsung E-FOTA				

Figure 51 Knox Mobile Enrollment settings

## 21.5 Reports

Reports are used for collecting data and statistics concerning FAMOC, devices and users included in the system, and operations performed on the handsets. The tab generates statistics on: device inventory, device security, current device status, alerts and notifications, SIM card inventory, user inventory, billings, server diagnostics and user activity.

Device inventory		Device inventory		
Device inventory	Devices added in ...			
Device security	Devices count by platform			
Current device status	Devices count by platform (detailed platform version)			
Alerts and notifications	Android devices count by platform version			
	Apple devices count by platform version			
Usage monitor data	Symbian devices count by platform version			
	Windows Phone devices count by platform version			
Location	Phone count by model			
User inventory	Phones without SIM card			
	BYOD - device ownership			
SIM card inventory	List of WLAN MAC addresses			
	Devices firmware version			
Server diagnostics	Devices older than ...			
	Devices repaired in ...			
User activity	Devices in repair			
	Devices repairs by service partner			
	Devices in repair - overdue			
	Stolen/lost devices			
	Devices count by SIM card wireless operators			
	Devices count by user's company			
	Apple devices count by OS version			
	Devices count by build number			
	Activated devices in ...			

Figure 52 Reports

### 21.5.1 Available operations on reports

In order to generate a report click the Generate icon on the reports list. If the report requires parameters (e.g. Start – end dates) a popup will appear. After generating the report, an additional icon will appear allowing you to download the last report.

Device inventory		Device inventory			
Device inventory	Devices added in ...				
Device security	Devices count by platform				

Figure 52 Action on reports

It is possible to define schedules for the reports and send them to email recipients. In order to create a schedule click **Add schedule** icon. In **Schedule creation** popup set:

1. Schedule interval – how often the report will be generated (every day, every weekday, every week, every month)
2. Start date – date and time when the report will be sent for the first time
3. Report schedule recipients – list of the email addresses separated by semicolon
4. Activate schedule – if schedule will be active just after saving it
5. Report parameters – section appears if report has parameters (e.g. Report Device added in ... has parameters: start date, end date and as a parameter value can be selected first and last day of the previous month)
6. Message settings – section with fields required in email as: from, reply to email, subject, email content. Custom values can be set. In the subject field, name of the report will be replaced with token `_REPORT_NAME_`.

Figure 53 Reports – schedule creation

## 21 Additional Information

If you face any difficulties or need support please contact [support@fancyfon.com](mailto:support@fancyfon.com).

For more information about FAMOC and other FancyFon products please visit [www.fancyfon.com](http://www.fancyfon.com).