



Policy Templates Guide



www.famoc.com

PUBLISHED BY

Famoc Software Limited

Atrium Business Centre

The Atrium, Blackpool Park

Cork, Ireland

Copyright© 2008-2022 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

1. Device policy in FAMOC	5
1.1. Refresh Policies on Devices	7
1.2. Policies Status Popup	7
2. Fully managed policy Templates	9
2.1. General settings tab	9
2.1.1. Schedules settings	11
2.2 Assigned groups	12
2.3 Policy components	13
2.4 Security options	14
2.4.1 Restriction (time/geo/speed) rules	15
2.4.2 Wipe policy	17
2.4.3 Network policy	18
2.4.4 Location policy	20
2.4.5 Update policy	21
2.4.6 Hardware policy	22
2.4.7 Encryption policy	27
2.4.8 Installer policy	27
2.4.9 Application restrictions	28
2.4.10 Application policy	32
2.4.11 Samsung KSP	34
2.5 Advanced	35
3. BYOD/WPC policy templates	39
3.1. General settings tab	39
3.1.1. Schedules settings	41
3.2 Assigned groups	42
3.3 Policy components	42
3.4 Device security options	43
3.5 Work profile security options	46
3.6 Enabled applications and widgets	51
3.7 Advanced settings	52
4. COSU Policies	55
4.1. General settings tab	55

4.1.1. Schedules settings	56
4.2 Assigned groups	57
4.3 Policy components	58
4.4 COSU mode settings	59
4.5 Security options	60
4.5.1 Wipe policy	61
4.5.2 Network policy	62
4.5.3 Location policy	63
4.5.4 Update policy	63
4.5.5 Hardware policy	64
4.5.6 Encryption policy	64
4.5.7 Installer policy	65
4.5.8 Application restrictions	65
4.5.9 Application policy	66
4.5.9 Samsung KSP	67
4.6 Advanced	67
5. Shared device Policies	70
5.1. General settings tab	70
5.1.1. Schedules settings	70
5.2 Assigned device groups	71
5.3 Policy components	71
5.4 Security options on the device	72
5.4.1 Update policy	72
5.4.2 Hardware policy	73
5.5 User profile settings	73
5.5.1 Work profile restrictions	73
5.5.2 Enabled applications	74
5.6 Advanced	74
6. Policies Status on Device Details Page	75

1. Device policy in FAMOC

Since the 5.8 version of FAMOC, policy templates will be separated for Fully managed, BYOD/WPC and COSU devices. Depending on the enrollment process devices will have different type of policies applied.

To start policy configuration, go to **MANAGEMENT** → **Settings** → **Policies** tab. Possible main actions (buttons on the top of the list) are:

1. **Add policy template** - allows administrator to create a new policy template.
2. **Refresh policies on devices** - enables administrator to apply a policy on several devices.
3. **Policies status** - gives an overview of devices assigned to each policy, compliant devices, devices with an outdated policy and devices on which the policy has not yet been implemented.
4. **Unmerged/Deprecated policies** - if you have been using previous versions of FAMOC you can see here all the policies that are Unmerged and/or Deprecated.

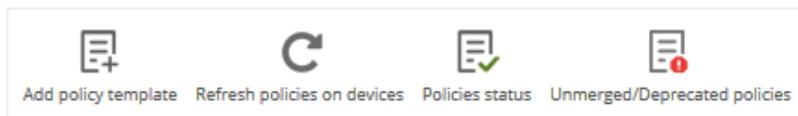


Figure 1 Main action buttons

If there are any previously used templates that have not yet been merged, you will see a warning.

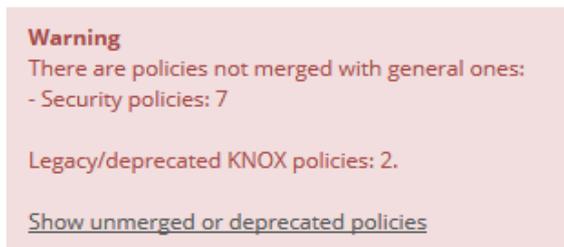


Figure 2 Unmerged/Deprecated policies warning

Merging process is described in detail [here](#).

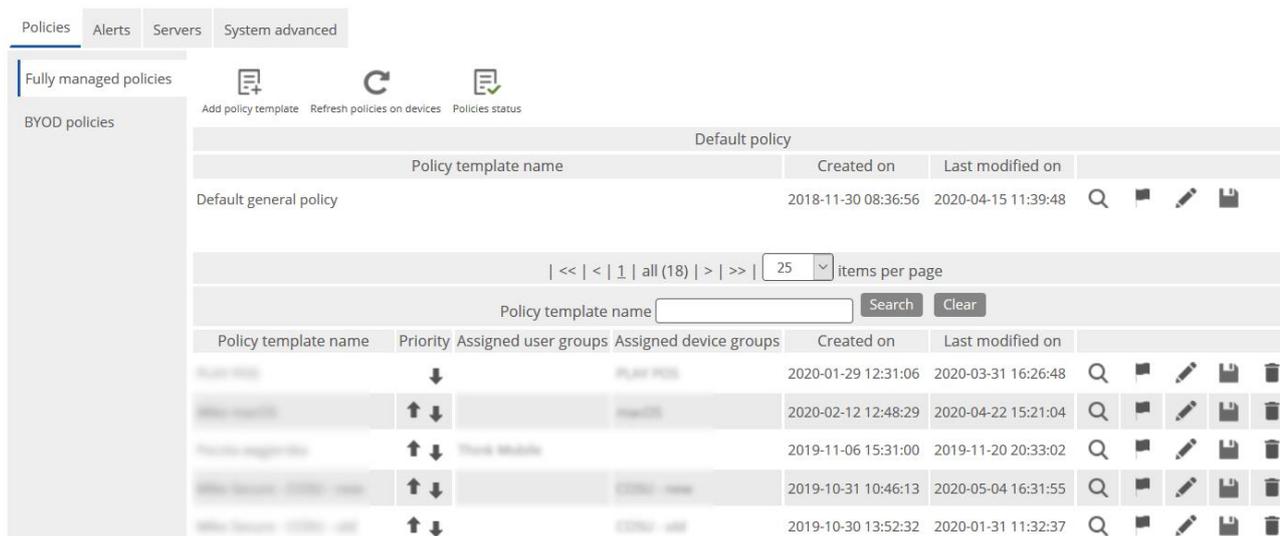


Figure 3 Policy templates

NOTE: Default policy is now on top of the list and groups can't be assigned to it. Policy is applied to devices that are not assigned to any other policy. There are separate default policies for both device groups (full management and BYOD).

Policy templates list columns description:

1. **Policy template name** – name of the policy template (clicking on the policy name, opens policy edit page)
2. **Priority** – order of the policy template selection for devices (if user is not assigned to any of the groups used in existing policy templates – last policy template will be applied for user's devices, if user is assigned to one of the groups used in existing policy templates – the highest policy template will be applied for user's devices). Clicking on the green arrows changes order.
3. **Assigned user groups** – user groups assigned to policy template
4. **Assigned device groups** – device groups assigned to policy template
5. **Created on** – date of the policy template creation
6. **Action column** – described in detail in the table below

Operation	Icon	Description
Preview		Shows the policy template details (without possibility to edit)
Show policy status		Opens popup with overview of devices assigned to policy, compliant devices, devices with an outdated policy and devices on which the policy has not yet been implemented
Edit		Opens edit form

Save as		Save existing policy as a new one
Delete		Adds possibility to delete policy template (only if policy template is not applied currently on any of the devices). If such policy template is applied currently - alert message will be shown ("Policy template is already applied on devices and cannot be deleted.")

1.1. Refresh Policies on Devices

Clicking on the **Refresh policies on devices** button, directs to operation page. Devices list is filled automatically with all devices that need to have the policy applied (devices with outdated policies and on which policies are not applied, but have agents installed).

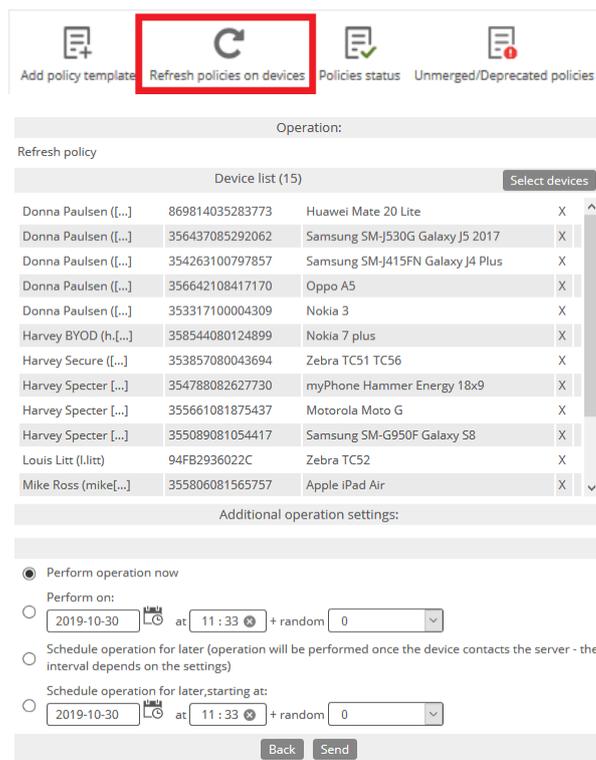


Figure 4 Refresh policies operation page

You can decide if you wish to perform the operation now or schedule it for later. To confirm your choice click **Send**.

1.2. Policies Status Popup

On clicking the **Policies status** button, popup with all policies status appears. The popup displays an overview of devices assigned to each policy, compliant devices, devices with an outdated policy and devices on which the policy has not yet been implemented.

Clicking on the preview icon, displays a list of devices.

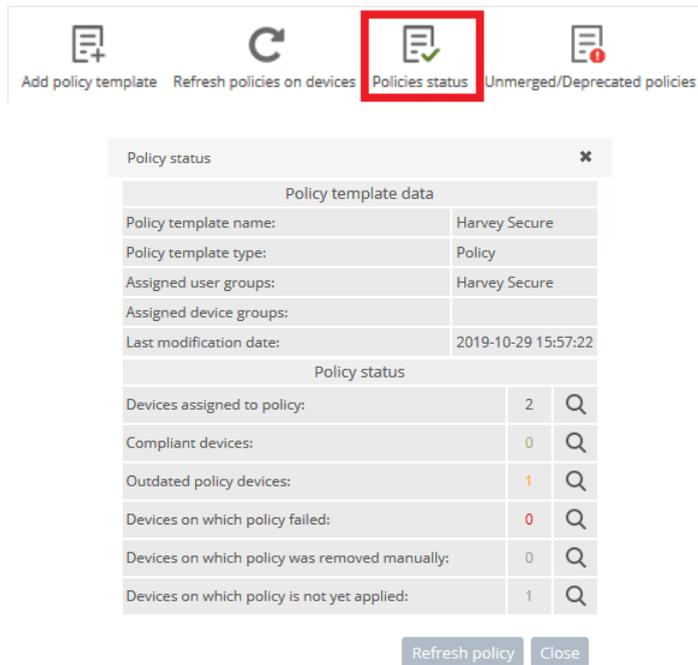


Figure 5 Policies status popup

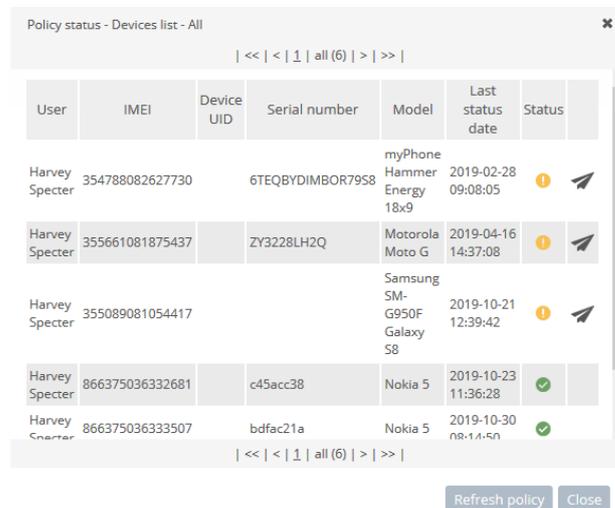


Figure 6 Policies status – devices list

The device list shows the following parameters:

1. **User** – user of the device
2. **IMEI, Device UID, Serial number** – identifier of the device
3. **Model** – model of the device
4. **Last status date** – date when the policy was successfully applied
5. **Current status icon**
6. **Action column** – with possibility to refresh policy on selected device (by clicking on ).

There is a possibility to refresh policy on all devices with outdated policy and on which policy is not applied yet (**Refresh policy** button on the bottom of the popup).

Policy status is described as follows:

- If the device has no policy template applied – its text colour is gray, and the status icon is 
- If the policy template was failed on the device – its text colour is red, and the status icon is 
- If the device has outdated policy template (policy template has been changed after the policy was applied on the device) – its text colour is orange, and the status icon is 
- If the device is compliant to the policy – its text colour is green, and the status icon is 

2. Fully managed policy Templates

To add new policy, click on the **Add policy template** button.

To edit an existing policy, click on the policy name or **Edit** button.

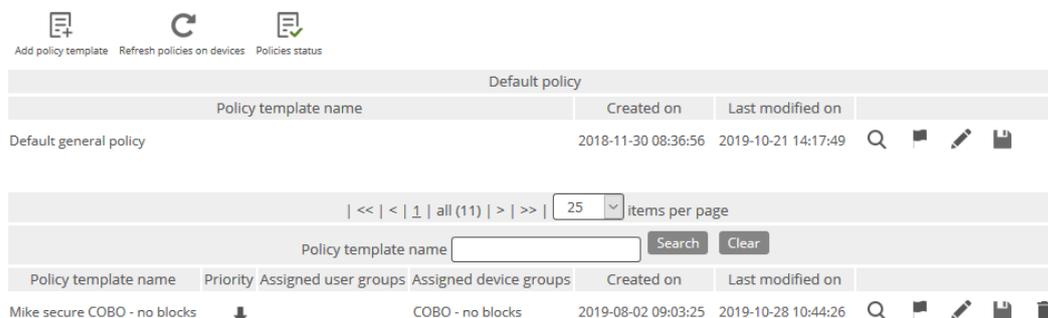


Figure 7 Policies main view

2.1. General settings tab

Below is the list of parameters on general settings tab:

Parameter	Value
General settings	
Template name	Input policy name (max 100 chars)
Set priority order	Specify position on the policy template list
Reinstall Base Agent automatically	When new Base Agent version appears in the system, it will be automatically reinstalled on devices (policy will be set as outdated). Default value: not checked.
Uninstall not compatible policy components automatically	If set, not matching policy components from current policy will be uninstalled if device will be moved to other policy. Default value: not checked.

Enable Samsung Premium API	To activate Samsung Premium API ¹ in the policy this option must be marked. Once it is selected a proper license key must be provided. Default value: not checked.
Premium license	Samsung license key can be added/changed/removed by using plus/minus icons next to the license key field.
Premium license expiry date	When set, 14,7,3,1 day before that date the alert in organization will be generated. Default value: not set.
Enable Samsung attestation	If set, an additional operation for Samsung KNOX attestation process will be added to the queue and will check the device's software integrity before creating the KNOX container. Default value: not checked.
SafetyNet attestation	The SafetyNet Attestation API is an anti-abuse API that allows to assess the Android device. Default value: not checked.
Mark as wiped on Base Agent uninstallation	If set, the device will be marked as wiped in the FAMOC console if Base Agent is uninstalled. Default value: not checked.
Enable remote access services	If this option is marked, Remote Access will be installed with the policy. Default value: not selected
Remote Access session initialization consent	Available options: <ul style="list-style-type: none"> • Managed by user • Require on every connection • Automatic connection Default value: Managed by user
Enable location services	If this option is marked, Location Monitor will be installed with the policy. Default value: not selected
Location interval	Interval in which location of the device is checked. Default value: Off
Disable location reporting on off-peak	When set, location will not be retrieved from the device in off-peak. Default value: not checked
Disable location reporting after agent installation	When set, location will not be retrieved just after the agent is installed. Default value: not checked
Force the app monitor service to turn on	When set, an additional operation included in the general policy, called "Enable app monitor service", will be added to the queue and

¹ You can read more about advantages offered by KPE Premium here: [Knox Platform for Enterprise | Advanced mobile security management](#)

	sent to the device asking the user to turn the FAMOC Accessibility Service on.
Ignore battery optimization for Location monitor and Usage monitor	Possibility to add Location and Usage monitor to ignore optimization battery app list, so that schedules, SMS, mms reporting works properly. Selecting this option sends an operation that requires user confirmation.
Report additional data about apps (app size, cache size, data size)	After selecting this option, FAMOC will collect information about the memory used by the application and its files. Default value: not checked
Reported applications	Options available: <ul style="list-style-type: none"> • Report all applications • Report only managed applications Option available only for iOS devices. Default value: Report all applications

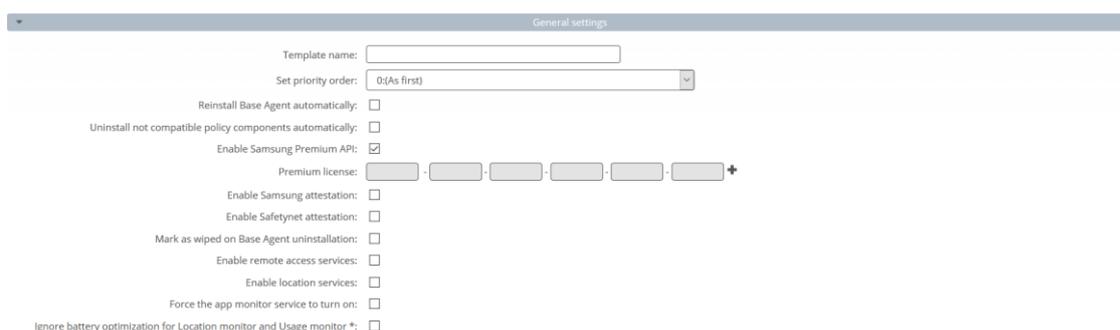


Figure 8 General settings tab

2.1.1. Schedules settings

Below is the list of parameters on schedules settings tab:

Parameter	Value
Schedules settings	
Peak schedule interval	The interval of Base Agent server connection: 5 min./15 min./30 min. /1h/4h/12h/Once a day/Once a week/Once a month Default value: Once a day
Peak days	Days of week during which Base Agent reports to FAMOC server Default value: Monday - Friday
Peak begin	What time during peak days should Base Agent start reporting Default value: 8:00
Peak end	What time during peak days should Base Agent stop reporting Default value: 16:00
Device Monitor sessions interval	Sets the interval of Device Monitor sessions: Off/Hourly/4 times a day/Daily/Weekly/Monthly

	Default value: Daily
Alerting device inactivity	Alerting inactivity of the Base Agent after 1-5 days/Week/Month/3 months. In case Base Agent doesn't report to server within this period, FAMOC generates an alert with three reaction options: <ul style="list-style-type: none"> • Remove device from FAMOC • Reinstall Base Agent • Mark device as stolen Default value: After week
Wipe on exceeded device inactivity	If this option is marked and Base Agent doesn't report to server within a specified period, in addition to generated alert, the device will be wiped.
Mark as wiped on exceeded device inactivity	If set, the device will be marked as wiped in the FAMOC console if it exceeds device inactivity period.

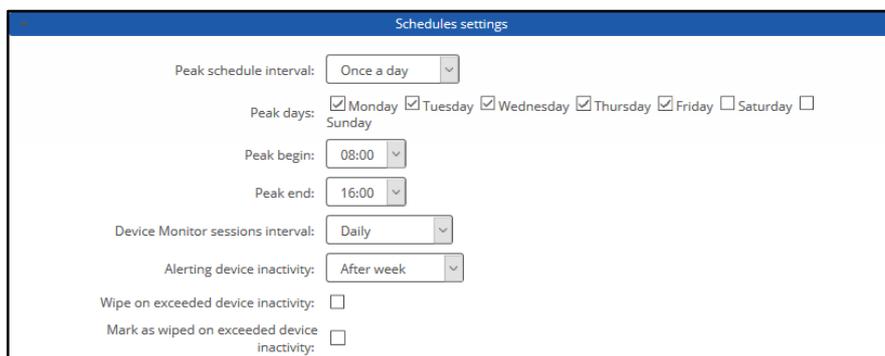


Figure 9 Schedules settings tab

2.2 Assigned groups

Each policy is assigned to certain groups of users or groups of devices, therefore each device receives a policy setting pre-defined to its group assignment. Devices not being members of any group and groups not being assigned to any policy receive a policy of the lowest priority (policy being at the bottom of the list). Devices being members of several groups receive the policy of the higher priority.

In the **Assigned Groups** tab administrator is allowed to assign groups to the policy. To select the group, click on the **Add device group** or **Add user group** button. Popup with group list will appear.

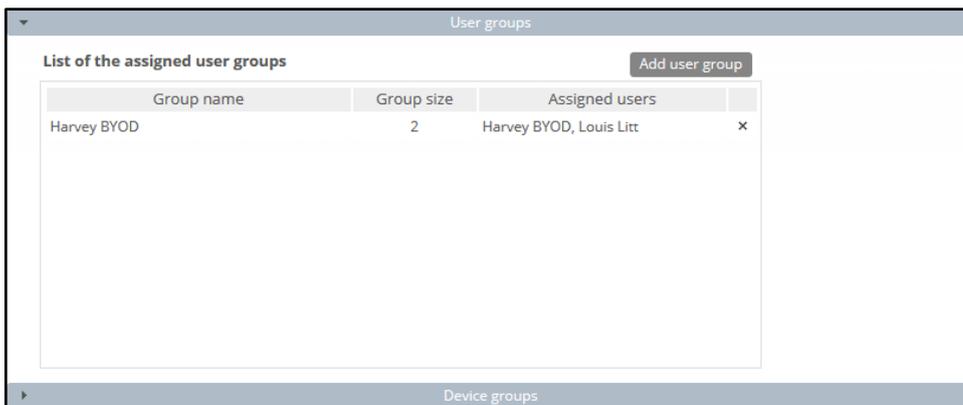
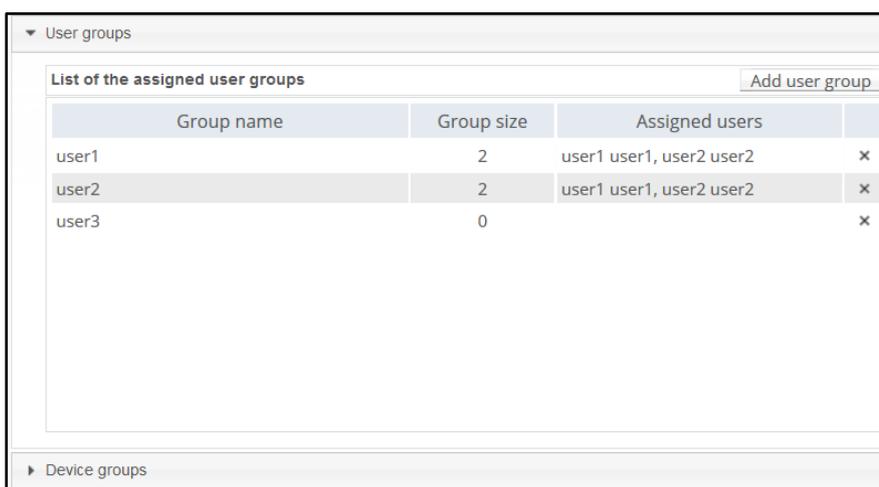


Figure 10 Groups tab

Mark checkboxes next to appropriate groups and click **Select**. Groups will be now assigned to the policy.



2.3 Policy components

In addition to general settings there is possibility to add configurations & applications to the policy.

To add configuration to the policy, click the **Select configuration** button. Popup with configuration list will appear.

Configuration can be set for:

- Peak – configuration will be applied in peak
- Off-peak – configuration will be applied in off-peak
- Always – configuration will be applied always

Every time a device connects to the server, it checks if proper policy is applied, and if the change is needed (e.g., there was the end of the peak and currently applied configuration is only for the peak) old configuration is removed and the appropriate is applied. The time-based policies can only be applied to iOS devices.

To add an application, click on the **Select application** button. Popup with application list will appear. Selected applications will be installed while applying the policy on the device. When the assigned to device policy is changed, the new policy will be applied, and the new list of applications will be installed. When selecting the application, it is possible to specify the number of installations retries (in case an application installation is cancelled by the user, FAMOC will retry the operation). Possible options:

- Installation obligatory (default option) – if installation is cancelled, it will be applied every next day.
- One installation attempt – if installation is cancelled, it will not be retried.
- Several installation attempts – installation will be retried a specified number of times.

Policy components can be set in custom installation order using down/up arrows in the **Order** column.

By default, each item is installed in a sequence (next item starts when previous has been successfully installed). It is possible to mark an item as independent (**Independent** column), which means the next action starts independently of the previous action, not waiting for its success report.

Select **Ignore failure** to execute the next action if the previous one failed.

Policy components		Select application	Select configuration			
Component name	Action	Ignore failure	Independent	Order		
Adobe Acrobat Reader	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↓	×	
Set wallpaper on device - Home and Lock	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Przeglądarka Chrome	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
strongswan 1.4.1.0	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Gmail	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Require 4 chars lock code on Android	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑	×	

Figure 11 Policy components tab

2.4 Security options

Security options include following settings:

1. Time/geo/speed rules
2. Wipe policy
3. Network policy
4. Location policy
5. Update policy
6. Hardware policy
7. Encryption policy

- 8. Installer policy
- 9. Application restrictions
- 10. Application policy
- 11. Samsung KSP

2.4.1 Restriction (time/geo/speed) rules

In this tab Administrator can define policy restrictions based on location (**Geofencing**), period and device’s movement speed. To implement time/geo/speed restrictions in your policy click **Add rule** and **New restriction** popup will appear.

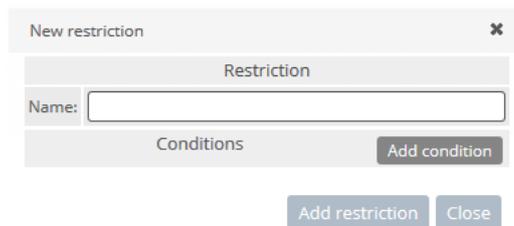


Figure 12 New restriction popup

Next, add condition for the restriction.

Condition type: Time - define when this restriction is valid. Two time periods are available: Peak and Off-peak

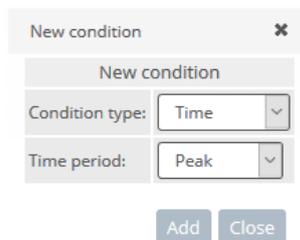


Figure 13 Condition type: Time

Condition type: Geofence - define the zone where policy is valid. Select radius from the list (from 500m to 5000m) and select the point from the map. When adding Geofence condition, previous selections are visible on the map.

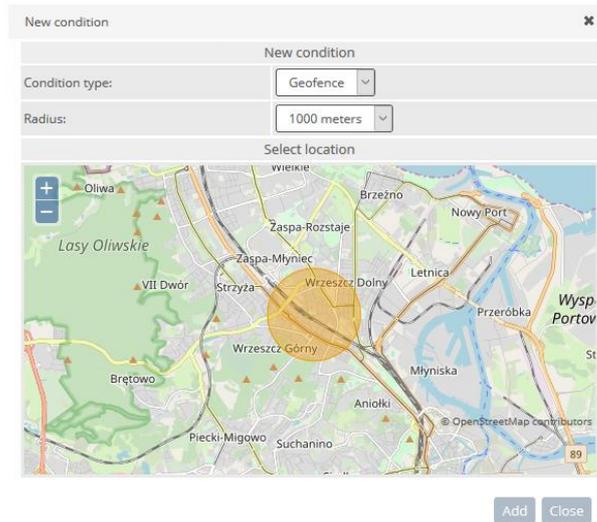


Figure 14 Condition: Geofence 500m radius

Only one Time and one Geofence condition can be defined in one restriction.



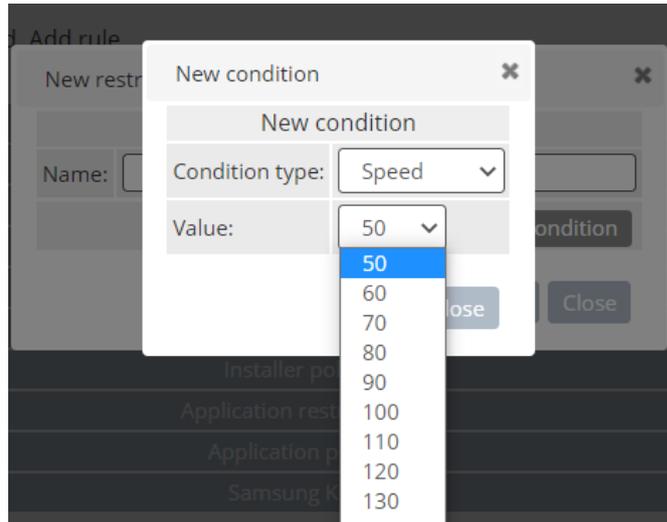
Figure 15 Time and Geofence conditions in one restriction

Speed restriction allows us to change policy settings according to the speed of movement of the device. Example:

- In our policy, we set a speed limit of 140 kmph.
- When the speed is exceeded, the policy changes e.g., social applications, camera, etc. are disabled
- We can also set the so-called allow list and specify that when a certain threshold is exceeded, only applications such as Maps will be available on the device.
- As soon as the speed drops below the specified limit, the default policy settings will be restored.

A 10% margin of error is used in the measurement.

NOTE: If the locating speed is not available and the last speed was above zero, we will decrease it by one km / h all the way to zero every second.



2.4.2 Wipe policy

Below is the list of parameters on Wipe policy settings tab:

Parameter	Description
Wipe policy	
Data wipe on SIM card change	If set, wipe will be performed when the SIM card change will be detected. Availability: Android devices
Wipe on no SIM card detection	If set, wipe will be performed when the SIM card is not detected. Option available when the first option is set (Data wipe on SIM card change). WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe. Availability: Android devices
Wipe memory card	If set, memory card will be wiped in addition when SIM card change will be detected. Option available when the first option is set (Data wipe on SIM card change). Availability: Android devices
Enterprise wipe on jailbreak detection	If set, the corporate data (all installed via FAMOC MDM) on device will be removed when jailbreak will be detected. Availability: iOS devices.
Wipe on root detection	If set, the device will be wiped when root will be detected. Availability: Android devices.
Allow Activation Lock	If set, Activation Lock option will be enabled on iOS devices. Availability: iOS devices in the Supervised mode
Factory reset lock	If set, factory reset cannot be performed. Availability: Device Owner, Android Management API, Android Samsung 4.x with Enterprise SDK 2.0, Android LG with Enterprise SDK from 1.0 , Windows Phone 8.1/10

<p>Factory reset protection (FRP)²</p>	<p>Factory Reset Protection is a solution that allows you to start the device after restoring factory settings only with a Google account that you have previously logged into the device. Available configuration options for this setting:</p> <ul style="list-style-type: none"> ● disable FRP (option will not be available on the device) ● unlock the device with an active account on device (the device can be unlocked with the previously used account) ● unlock the device with an account from the defined list (the device can be unlocked with an account from the list defined in FAMOC - user ID should be provided) ● remove the factory reset protection (FRP) after device wipe (deactivates the FRP after the wipe) <p>Availability: Device Owner</p>
----------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.4.3 Network policy

Below is the list of parameters on Network policy settings tab:

Parameter	Description
Network policy	
Wi-Fi lock	If set, Wi-Fi cannot be used on the device. Availability: Android and Windows Phone 8.1 / 10 devices
Automatic connection to WiFi hotspots lock	If set, the device will not connect automatically to the WiFi hotspots. Availability: Windows Phone 8.1 / 10
WiFi hotspots reporting lock	If set, the device will not report WiFi hotspots. Availability: Windows Phone 8.1
Manual WiFi configuration lock	If set, there will be no possibility to configure WiFi connection manually. Availability: Device Owner, iOS devices in the Supervised mode, Windows Phone 8.1/10
Disable personal hotspot modification	If set user cannot change personal hotspot settings. Availability: iOS 12.2
Keep Wi-Fi on in sleep mode	If set prevents Wi-Fi disconnecting in sleep mode. Availability: Device Owner
Prevent Wi-Fi from being turned off	Prevents Wi-Fi from being turned off in Settings or Control Center. Availability: Device Owner, iOS 13.0

² List of the unlock accounts must contain the valid Google user ID's. They can be obtained from the Google API, using the link below:

<https://developers.google.com/people/api/rest/v1/people/get>

By executing the API call and logging with valid Google account, response returns the 'id' field of the user.

<p>Bluetooth lock</p>	<p>If set, Bluetooth cannot be used on the device. Availability: Android, Windows Phone 8.1/10, iOS 11.3 and above in Supervised mode Possible options available for Android Samsung with Enterprise SDK from 2.0:</p> <ul style="list-style-type: none"> - Enable Advanced Audio Distribution Profile (A2DP) - Enable Audio/Video Remote Control Profile (AVRCP) - when this profile is enabled with (A2DP) user will be able to use Media Audio connection additionally user will be able to use buttons on bluetooth device(Play/Stop/Next song). - Enable HandsFree Profile (HFP) - this profile works only with HSP profile. - Enable Headset Profile (HSP) - when this profile is enabled with (HFP) user will be able to use Call Audio connection additionally user will be able to use buttons on bluetooth device(Answer or terminate the call) - Enable Phone Book Access Profile (PBAP) - when this profile is enabled bluetooth device will have access to contacts saved on the phone or tablet. - Enable Serial Port Profile (SPP) - this profile needs to be selected for proper wireless connection between devices - Enable file sharing via Bluetooth
<p>Cellular data lock</p>	<p>Possible options:</p> <ul style="list-style-type: none"> - Do not lock - Enable and block possibility to disable - Disable and block possibility to enable <p>Availability: Android 4.x, on Samsung devices only option Disable and block possibility to enable option is available.</p>
<p>Cellular data lock in roaming</p>	<p>Possible options:</p> <ul style="list-style-type: none"> - Do not lock - Disable and block possibility to enable <p>Availability: Android 4.x, Device Owner and Windows Phone 8.1/10 devices Default value: Do not lock.</p>
<p>Disable cellular plan modification</p>	<p>It blocks the possibility of changing the current tariff plan. Availability: iOS supervised</p>
<p>WiFi tethering lock</p>	<p>If set, WiFi tethering is disabled. Availability: Android Samsung with Enterprise SDK from 2.0 and Device Owner</p>
<p>USB tethering lock</p>	<p>If set, USB tethering is disabled. Availability: Android Samsung with Enterprise SDK from 3.0, Device Owner and Windows Phone 8.1/10</p>
<p>Device usage report to Microsoft lock</p>	<p>If set, usage report sending to Microsoft is disabled. Availability: Windows Phone 8.1/10</p>
<p>VPN over cellular lock</p>	<p>If set, VPN cannot be used over cellular data. Availability: Windows Phone 8.1/10</p>
<p>VPN over cellular in roaming lock</p>	<p>If set, VPN cannot be used over cellular data in roaming Availability: Windows Phone 8.1/10</p>
<p>Disallow the creation of VPN configurations</p>	<p>If set, user cannot configure VPN settings. Available from iOS 11.0</p>
<p>Block incoming MMS</p>	<p>If set, incoming MMS will not be delivered Availability: Android Samsung with Enterprise SDK from 3.0</p>
<p>Disable network settings reset</p>	<p>If set, the 'Reset network settings' option will not be available Availability: Device Owner</p>

Disable VPN settings	It blocks the possibility of changing the settings by the user Availability: Android, Device Owner
Disable eSIM settings modification	If set, user cannot modify eSIM settings. Available from iOS 12.1
Block private DNS settings	If set, user cannot set private DNS or turn off the DNS over TLS on the device. Availability: Device Owner, Android 10.0+
Block outgoing calls	Disables outgoing calls Availability: Device Owner
Block incoming calls	Allows you to block incoming calls. Available options: <ul style="list-style-type: none"> • Do not block • All • Pattern (The pattern of blocked numbers may contain e.g., numbers starting from 0700) Availability: Samsung SDK
Block incoming SMS messages	Allows you to block incoming text messages. Available options: <ul style="list-style-type: none"> • Do not block • All • Pattern (The pattern of blocked numbers may contain e.g., numbers starting from 0700) Availability: Samsung SDK
Disable managed networks settings change	Blocks the possibility to edit WiFi settings managed by FAMOC Availability: Android, Device Owner
Monitor list of the managed Wifi configurations	It monitors the status of managed networks and triggers an alert in case of their removal (forgotten on the device). Availability: Android, Device Owner
Block global background fetch when roaming	Disables background downloads when the device is roaming Availability: iOS
Block voice dialling if the device is locked with a passcode	Availability: iOS
Disable apps cellular data modification	Availability: iOS supervised
Disable host pairing	Availability: iOS supervised
Block Bluetooth config	Availability: Samsung SDK, Device Owner
Block mobile networks config	Availability: Device Owner (Android 8.0 +)
Block cell broadcast config	Availability: Device Owner (Android 8.0 +)
Disable SMS messages	Availability: Device Owner (Android 8.0+)

2.4.4 Location policy

Below is the list of parameters on Location policy settings tab:

Parameter	Description
Location policy	
GPS lock	Possible options: <ul style="list-style-type: none"> - Do not lock - Enable GPS - Enable GPS and block possibility to disable - Disable GPS - Disable GPS and block possibility to enable Availability: Android Samsung with Enterprise SDK 3.0 Default value: Do not lock
Enable GPS only mode	If set, the user cannot turn on power saving mode and high accuracy, only GPS is enabled and cannot be disabled.
Location lock	Allows you to grant the FAMOC agent access to the location and blocks the possibility of revoking these permissions. Possible options: <ul style="list-style-type: none"> - Do not lock - Enable location - Enable location and block possibility to disable - Disable location - Disable location and block possibility to enable Availability: Windows Phone 8.1/10
Android location lock	Allows you to grant the FAMOC agent access to the location and blocks the possibility of revoking these permissions. Possible options: <ul style="list-style-type: none"> - Do not lock - Enable location - Enable location and block possibility to disable - Disable location - Disable location and block possibility to enable Availability: Android 8.0+, Device Owner: Disable and block change option available from Android 8.0. Options: enable, disable, enable and block change available from Android 11.0.

2.4.5 Update policy

Below is the list of parameters on Update policy settings tab:

Parameter	Description
Update policy	
Delay user visibility of Software Updates	If enabled, no update information will appear on the device. The default delay will be 30 days unless a different period is selected in the "Delay software update" field. Availability: iOS supervised from 11.3, macOS from 10.13, tvOS from 12.2
Delay user visibility of non-OS Software Updates	If enabled, no information about non-OS updates will appear on the device. The default delay will be 30 days unless a different period is selected in the "Delay software update" field. Available from macOS 11

Delay software update by	Period in which the update will be postponed. Range: 1-90 days. Availability: iOS supervised from 11.3, macOS from 10.13, tvOS from 12.2
Delay minor software update by	Delays minor updates for a specified period after the release of these updates. Available from macOS 11.3
Delay non-OS software update by	Delays non-OS updates for a specified period after the release of these updates. Available from macOS 11.3
Force delayed major software updates	Delays major updates for a specified period after the release of those updates Available from macOS 11.3
Delay major software updates by	Period in which the update will be postponed. Range: 1-90 days. Available from macOS 11.3
Control system version (Samsung E-FOTA)	If set, E-FOTA is enabled. Availability: Android Samsung 7.x with Knox 2.7.1+
OTA update policy	Possibility to define OTA update policy. Available options are: <ul style="list-style-type: none"> • No policy • Automatic • Windowed • Postponed When Windowed option is selected, days and time range can be selected. Availability: Device Owner (blocks system updates for 30 days), Android Samsung with Enterprise SDK 3.0
Enable Zebra OTA updates	Possibility to enable OTA updates for Zebra devices. Availability: Zebra devices with Android 7 or higher and MX version 9.2 or newer.
Disable automatic software updates	When selected, the device firmware update from download mode is disabled Availability: Samsung SDK with premium license
Disable automatic checking for updates	If checked, the device will not automatically check for a new update. Availability: Samsung SDK with premium license

2.4.6 Hardware policy

Below is the list of parameters on Hardware policy settings tab:

Parameter	Description
Hardware policy	
Camera lock	If set, camera cannot be used on the device. Availability: Device Owner, Android 4.x, Android Samsung 2.3 – 4.x and Windows Phone 8.1/10, Apple devices

Disable manual unenrollment	If set, FAMOC Device administrator cannot be deactivated manually. Availability: Android Samsung with Enterprise SDK from 2.0, Android Sony with Enterprise SDK from 6.0, Android LG with Enterprise SDK from 1.0 and Windows 10 Mobile
Disable manual work profile removal	If set, work profile cannot be removed manually. Availability: Device Owner, Android 8.0
USB media player lock	If set and device is connected to PC using USB, device cannot be used in media player mode. Availability: Android Samsung 4.x with Enterprise SDK 3.0, Android Sony with Enterprise SDK from 5.0
Allow devices to be booted into recovery by an unpaired device	If checked, allows devices to be booted into recovery by an unpaired device. Available on iOS supervised devices.
Development mode lock	If set, development mode cannot be enabled. Availability: Device Owner, Android Samsung with Enterprise SDK 5.0
Task manager lock	If set, task manager will be blocked. Availability: Android Samsung with Enterprise SDK 3.0
NFC lock	If set, NFC cannot be used. Availability: Windows Phone 8.1/10, Android Samsung with Enterprise SDK from 2.0, iOS 14.2
Disallow outgoing beam using NFC	If set, user is not allowed to use NFC to transfer data from apps. Availability: Device Owner
Storage card lock	If set, disable Storage card socket. Availability: Device Owner, Android Samsung with Enterprise SDK from 2.0, Windows Phone 8.1/10
Copy & paste lock	If set, disable copy and paste function. Availability: Windows Phone 8.1/10
Screen capture lock	If set, there will be no possibility to capture screenshots Availability: Device Owner, Windows Phone 8.1/10, Android Samsung with Enterprise SDK from 2.0 and Apple devices
Disable remote screen observation by the Classroom app	Blocks the ability to see the screen in the Classroom app. Availability: iOS 12.0+, macOS 10.14.4+
Disable keyboard autocorrection	Users will not see suggestions for spelling correction. Availability: iOS supervised
Prevent Siri from querying user-generated content from the web	Siri will not query user-generated content such as Wikipedia Availability: iOS supervised
USB file manager lock	If set, there will be no possibility to browse files through USB connection. Availability: Device Owner, Windows Phone 8.1/10
Block multi-window mode	If set, multi-window mode will not be accessible on device Availability: Android Samsung with Enterprise SDK from 4.0

Block safe mode	If set, safe mode will not be accessible on the device. Availability: Device Owner, Android Samsung with Enterprise SDK from 4.0
Block airplane mode	If set, airplane mode will not be accessible on the device. Availability: Android Samsung with Enterprise SDK from 5.0, Device Owner from Android 9
Enable USB accessories while device is locked	If set, you allow your iOS device to always access USB accessories. Availability: iOS supervised 11.4.1
Disable the prompt to setup new nearby devices	If set, you can disable the option of using one device to set up new device by placing it next to each other. Availability: iOS supervised 11.0
Disable AirPrint	If set, AirPrint feature (printing via a wireless LAN) will be disabled. Availability: iOS supervised 11.0
Disable saving of AirPrint credentials on iCloud	If set, AirPrint credentials will not be saved on iCloud. Availability: iOS supervised 11.0
Require trusted certificates for TLS printing communication	If set, forces the device to use trusted certificates for TLS printing communication. Availability: iOS supervised 11.0
Disable iBeacon discovery of AirPrint printers	If set, iBeacon will not be locating and connecting to available printers. Availability: iOS supervised 11.0
Disable incoming AirPlay requests	If set, the device will reject incoming AirPlay streaming requests. Availability: tvOS
Disallow macOS auto unlock	If set, it will not be possible to unlock your device using Apple Watch. Availability: iOS supervised 14.5, macOS 10.12
Disallow macOS cloud desktop and document services	If set macOS cloud desktop and document services will be disabled. Availability: macOS 10.12.4
Prevent Touch ID from unlocking a device	If set, users will not be able to unlock the device using fingerprint recognition. Availability: iOS, iOS supervised, macOS 10.12
Disable biometric modification	If enabled, it will not be possible to change the biometric settings.
Enforced biometry timeout	Period after which users must enter their password, instead of TouchID. Available from macOS 12.
Disallow content caching	If set, content caching feature will be disabled. Availability: macOS 10.13 NOTE: This option is deprecated
Disable definition lookup	If set, built-in dictionary feature will be disabled. Availability: iOS supervised, macOS 10.11

Disable keyboard shortcuts	Blocks the use of keyboard shortcuts Availability: iOS
Disable QuickPath keyboard	If set QuickPath swipe keyboard will be disabled. Availability: iOS 13.0
Disable keyboard spell-check	Potentially misspelled words on user devices will not be underlined in red Availability: iOS
Prevent device from sleeping	If set, device will not go to a sleep mode after a period of inactivity. Availability: tvOS 13.0
Prevent users from configuring credentials in the managed keystore	If set, user will not have access to some Credential storage options such as: View user certificates, install certificates from device storage, Remove certificates Availability: Device Owner
Disable Siri	Possibility to disable Siri assistant Availability: iOS
Disable Siri when device is locked	Prevents Siri from starting on a locked device Availability: iOS
Disable connections to Siri servers for the purposes of dictation	If set, connections to Siri servers for the purposes of dictation will be disabled Availability: iOS 14.5
Disable connections to Siri servers for the purposes of translation	If set, connections to Siri servers for the purposes of translation will be disabled Availability: iOS 15.0
Block photo stream	If turned on, it blocks the transmission of photos in iCloud Availability: iOS
Disable Control Center from appearing on the Lock screen	If set, Control Center will not appear on Lock screen Availability: iOS
Disable automatically submitting diagnostic reports to Apple	If set, diagnostic report will not be automatically submitted to Apple Availability: iOS
Block the possibility of creating untrusted TLS connections	If set, prevents untrusted Transport Layer Security (TLS) certificates on devices Availability: iOS
Disallow updating certificate trust database	If set, prevents automatic certificates updates. Availability: iOS
Disables backup of Enterprise books	If set, backup of Enterprise books will be disabled Availability: iOS 8.0
Disables Enterprise Book metadata sync	If set, Enterprise Book metadata sync will be disabled Availability: iOS 8.0

Disable modification of notification settings	If set, it blocks the ability to change notification settings Availability: iOS supervised
Disables today notifications history view on the lock screen	If set, notifications history view on the lock screen will be disabled Availability: iOS 7.0
Disables notifications history view on the lock screen	If set, connections to Siri servers for the purposes of dictation will be disabled Availability: iOS 7.0
Disables managed applications to use the iCloud	If set, managed apps will not be able to use iCloud Availability: iOS 8.0
Force encrypted backup	Forces backup encryption Availability: iOS
Force devices receiving AirPlay requests from this device to use a pairing pass	If set, pairing pass will be required when device receives AirPlay requests from this device Availability: iOS
Disable pairing watches	After checking, it will disconnect from the currently used watch and clear its settings Availability: iOS supervised
Force wrist detection on Apple Watch	If checked, forces the paired Apple Watch to use Wrist Detection Availability: iOS
Disable passcode modification	Prevents password change Availability: iOS supervised, macOS 10.13+
Block device name modification	Prevents the device name from being changed Availability: iOS supervised, tvOS
Disable dictation	It prevents users from using the dictation feature on their device. Availability: iOS supervised, macOS
Disable diagnostic submission modification	If enabled, changing diagnostic data settings is not allowed. Availability: iOS supervised
Disable Screen Time	Disables the Screen Time feature Availability: iOS supervised
Disable wallpaper modification	Prevents the wallpaper from being changed Availability: iOS supervised, macOS 10.13+
Force assistant profanity filter	Siri profanity filter will be turned on Availability: iOS supervised, macOS

2.4.7 Encryption policy

Below is the list of parameters on Encryption policy settings tab:

Parameter	Description
Encryption policy	
Internal storage encryption	If set, encryption will be required. Availability: Android 4.x and Android Samsung with Enterprise SDK 2.0/3.0, iOS and Windows Phone 8.1/10
Disable secure boot	If set, secure boot of the device will be disabled. Availability: Android devices with FAMOC Add-On installed
Common Criteria mode activation	If set, device will be verified if it meets Mobile Device Fundamentals Protection Profile restrictions. Availability: Samsung SDK, Device Owner (KNOX Premium API required)

2.4.8 Installer policy

Below is the list of parameters on Installer policy settings tab:

Parameter	Description
Installer policy	
Application installer lock	If set, there will be no possibility to install applications on the device. Availability: Android, Apple, Windows Phone 8.1/10, Device Owner devices
Notification when application installation is blocked	You can set a notification that will appear on a device when a user tries to install an application. Default: Application installation is not allowed Availability: Android
Allow USB debugging	If set, USB debugging can be set on device. Available for Device Owner, Android Samsung from Enterprise SDK 3.0 and for Android Sony with Enterprise SDK from 5.0. USB debugging is blocked by default.
Unknown sources lock	If set, the possibility to change the unknown sources setting is blocked Availability: Device Owner, Android Samsung with Enterprise SDK 2.0
Disable application control	If set, users will not be able to modify the app (uninstall, stop, clear app data). Availability: Android Device Owner
Accounts creation using Google Play	Possibility to Disable/Enable accounts creation using Google Play When installer lock is set, accounts creation using Google Play is automatically disabled. Availability: Android Device Owner
Allow USB debugging on Windows 10 Mobile devices	If set, USB debugging can be set on device. Availability: Windows 10 Mobile USB debugging is blocked by default.

Unknown sources lock on Windows 10 Mobile devices	If set, the possibility to change the unknown sources setting is blocked Availability: Windows 10 Mobile
Manual installation of the root certificate lock	If set, there will be no possibility to install the root certificate manually. Availability: Windows Phone 8.1/10
Disable the App Store	Blocks access to the App Store Availability: iOS supervised
Prohibit the user from installing configuration profiles and certificates interactively	If set, prohibits the user from installing configuration profiles and certificates interactively Availability: iOS supervised

2.4.9 Application restrictions

Below is the list of parameters on Application restrictions tab:

Parameter	Description
Application restrictions	
Application voice recording lock	If set, microphone cannot be used on the device. Availability: Android Samsung 4.x devices with Enterprise SDK, Windows Phone 8.1/10
Do not force Google Play Protect	This option disables Google Play Protect scanning for any malicious software. It requires the newest Google Play services on Android 6.0, 7.0 with work profile enabled. Availability: Android
Phone settings lock	If set, there will be no possibility to enter the settings on the device. Availability: Android, Device Owner
Time settings lock	If set, there will be no possibility to enter time settings on the device. Availability: Android Samsung with Enterprise SDK 3.0
Force automatic date and time	If set, automatic date and time settings will be enforced on the device. Availability: Android, Device Owner, iOS supervised 12.0, tvOS 12.2
Web browser lock	If set, there will be no possibility to open a web browser on the device. Availability: Android, Apple, Windows Phone 8.1/10, Device Owner devices
Disable accounts modification	If set, the possibility to add, edit or delete an account will be locked Availability: Device Owner
Disable user accounts management	If set, additional user accounts cannot be created. Availability: Android Samsung with Enterprise SDK from 4.0
Email account creation lock	If set, there will be no possibility to create an email account on the device. Availability: Android (not available for Android 5.0) and Windows Phone 8.1/10 devices

Disable the ability to remove system apps from the device	If set, system apps cannot be deleted. Availability: iOS 11.0
Disable AirDrop	If set, AirDrop file sharing will be disabled. Availability: iOS supervised
Do not allow to share managed documents using AirDrop	If set, managed documents cannot be shared using AirDrop feature. Availability: iOS
Do not allow to share data from unmanaged apps	If set, sharing data from unmanaged apps will be forbidden. Availability: iOS
Disable passwords sharing with AirDrop Passwords feature	If set, it will not be possible to share passwords between devices using AirDrop feature. Availability: iOS 12.0, macOS 10.14
Do not allow to share data from managed apps	If set, sharing data from managed apps will be forbidden. Availability: iOS
Allow unmanaged apps reading from managed contacts accounts	If set, unmanaged apps will be allowed to read contacts from managed accounts. Availability: iOS 12.0
Allow managed apps to write contacts to unmanaged contacts accounts	If set, managed apps will be allowed to write contacts to unmanaged accounts. Availability: iOS 12.0
Enable 'Do not allow to share data from unmanaged / managed apps' restrictions for copy and paste functionality	Blocks the ability to copy data from unmanaged and managed applications Availability: iOS 15.0
Disable autofill passwords in apps	If set, passwords will not be autofilled in apps. Availability: iOS 12.0, macOS 10.14
Do not request passwords from nearby devices	If set, passwords will not be requested from nearby devices. Availability: iOS 12.0, macOS 10.14, tvOS 12.0
Authenticate Face ID/Touch ID before allowing autofill passwords or credit card information	If set, it will require to use face or fingerprint authentication before using autofill passwords or credit card information. Availability: iOS 11.0
Disable iCloud Private Relay	Availability: iOS 15.0, macOS 12.0
Disable iCloud Photo Library	Possibility to disable iCloud Photo Library. Availability: iOS, macOS 10.12
Disable Apple Music service	Possibility to disable Apple Music service. Availability: iOS supervised, macOS 10.12
Disable backing up the device to iCloud	Possibility to disable iCloud backups. Availability: iOS
Disable document syncing to iCloud	Possibility to disable iCloud documents synchronization. Availability: iOS supervised, macOS 10.11
Disable iCloud keychain synchronization	Possibility to disable iCloud keychain (Apple password manager) synchronization. Availability: iOS supervised, macOS 10.12
Disable macOS iCloud Bookmark sync	Possibility to disable macOS iCloud Bookmark synchronization. Availability: macOS 10.12
Disable macOS iCloud Mail services	Possibility to disable macOS iCloud Mail services. Availability: macOS 10.12

Disable macOS iCloud Calendar services	Possibility to disable macOS iCloud Calendar services. Availability: macOS 10.12
Disable macOS iCloud Reminder services	Possibility to disable macOS iCloud Reminder services. Availability: macOS 10.12
Disable macOS iCloud Address Book services	Possibility to disable macOS iCloud Address Book services. Availability: macOS 10.12
Disable macOS iCloud Notes services	Possibility to disable macOS iCloud Notes services. Availability: macOS 10.12
Disable iTunes	Availability: iOS supervised
Disable iTunes application file sharing services	Possibility to disable sharing files between your devices using iTunes. Availability: macOS 10.13
Force the user to enter their iTunes password for each transaction	Availability: iOS
Disable returning Internet search results by Spotlight	If set, Spotlight will not return results from Internet search. Availability: iOS supervised, macOS 10.11
Disable pairing of Apple TV with the Remote app or Control Center widget	If set, Apple TV will not be pairing with Remote app or Control Center widget. Availability: tvOS 10.12
Max level of movie content allowed on the device	Levels according to MPAA rating system. Options included: None, All, G, PG, PG-13, R, NC-17. Availability: iOS 11.3, tvOS 11.3
Max level of TV content allowed on the device	Levels according to TV Parental Guidelines rating system. Options included: None, All, TV-Y, TV-Y7, TV-G, TV-PG, TV-14, TV-MA. Availability: iOS 11.3, tvOS 11.3
Max level of app content allowed on the device	You can set age ratings for apps between 4+, 9+, 12+ and 17+ years of age. You can also select All or None apps allowed. Availability: iOS 11.3, tvOS 11.3
Disable Find My Device in the Find My app	If set Find My Device option will be disabled. Availability: iOS 13.0
Disable Find My Friends in the Find My app	If set Find My Friends option will be disabled. Availability: iOS 13.0
Disable changes to Find My Friends	Availability: iOS supervised
Disable activity continuation	If set, it will not be possible to continue your activities between devices. Availability: iOS, macOS 10.15
Lock possibility to leverage location information by Search	If set, search will not use location information. Availability: Windows Phone 8.1/10
Save As functionality in Microsoft Office lock	If set, disable "Save As" option in Microsoft Office. Availability: Windows Phone 8.1
Sharing files functionality in Microsoft Office lock	If set, disable "Share file" option in Microsoft Office. Availability: Windows Phone 8.1
Disable accounts modification on Apple devices	If set, the possibility to add, edit or delete an account will be locked. Availability: Supervised iOS devices
Allow use of TLS 1.0/1.1 in Safari	If set, use of TLS 1.0/1.1 in Safari browser will be possible. Availability: iOS 13.4, macOS 10.15

Prevent a user from adding any App Clips	If set, user cannot create any App Clips Availability: Supervised iOS devices
Limit Apple personalized advertising	Limits the display of interest-based advertising Availability: Supervised and non-Supervised iOS devices
Disable app uninstallation	Blocks the option to remove managed applications Availability: iOS 14.0, tvOS 14.0
Enable the ability to restore of the backup from the Google account	Restoring data from private accounts is disabled by default, check this option to enable it. Availability: Device Owner
Disable enterprise apps trust	Removes the Trust Enterprise Developer button in Settings > General > Profiles & device management Availability: iOS
Disable in-app purchases	Availability: iOS
Block Passbook notifications on the lock screen	Availability: iOS
Force limited ad tracking	Availability: iOS
Disable auto fill in Safari	Availability: iOS supervised, macOS
Disable JavaScript in Safari	Availability: iOS
Block pop-ups in Safari	Availability: iOS
Enables Safari fraud warning	Availability: iOS
Cookies accepted by Safari	Possible options: Always, Never, From visited websites
Disable Game Center	Availability: iOS supervised, macOS 10.13
Disable adding friends to Game Center	Availability: iOS supervised, macOS
Block multiplayer gaming	Availability: iOS supervised, macOS 10.13
Disable apps removal	Availability: iOS
Prevent automatic downloading of apps purchased on other device	Availability: iOS
Remove the Book Store tab from the Books app	Availability: iOS
Disable download of the Apple Books media that is tagged as erotica	Availability: iOS, macOS, tvOS
Disable iMessage app	Availability: iOS
Hide explicit music or video content purchased from the iTunes Store	Availability: iOS, macOS, tvOS 11.3
Disable connecting to network drives in the Files app	Availability: iOS 13.1

Disable connecting to any connected USB devices in the Files app	Availability: iOS 13.1
Disable News app	Availability: iOS supervised
Disable podcasts	Availability: iOS supervised, macOS
Disable Apple Music Radio	Availability: iOS supervised
Disable Shared Photo Stream	Availability: iOS
Hide the FaceTime app	Availability: iOS supervised
Force automatic class joining in Classroom	Availability: iOS supervised, macOS 10.14.4
Require permission to leave classes request in Classroom	Availability: iOS supervised, macOS 10.14.4
Force unprompted app and device lock in Classroom	Availability: iOS supervised, macOS 10.14.4
Force unprompted screen observation in Classroom	Availability: iOS supervised, macOS 10.14.4
Disable content capture on device	Availability: Android Device Owner
Disable content suggestions on device	Availability: Android Device Owner

2.4.10 Application policy

Below is the list of parameters on Application policy tab:

Parameter	Description
Application policy	
Applications policy for Android Device	<p>General setting of the application password policy.</p> <ul style="list-style-type: none"> Do not ask about password – if set, password will be required only for applications listed on “Applications password policy” list Ask about lock code – if set, lock code will be required for all applications (except those listed on “Applications password policy” list) Ask about administrator password – if set, administrator password will be required for all applications (except those listed on “Applications password policy” list) <p>Availability: Android devices default setting is “Do not ask about password” Default value: “Do not ask about password”</p>
Android application list	<p>Enter package name to set restrictions for specific applications:</p> <ul style="list-style-type: none"> Deny list Uninstallation lock - application cannot be uninstalled

	<ul style="list-style-type: none"> Block force stop - if set user will not be able to close the app using Force stop option Block clear data - if set user will not be able to clear app data using Clear data option Password policy - possible choices - Do not ask for password / Ask for lock code / Ask for admin password
Application password timeout	<p>Time after which prompt about the password will appear on device. It can be set to 1/5/10/15 minutes. Availability: Android devices Default value: 5 minutes</p>
Notification when application is blocked with password	<p>Customizable notification shown on the device when application is blocked with password. Default: Enter FAMOC Password. Availability: Android devices</p>
Notification when application is blacklisted	<p>Customizable notification shown on the device when application is blacklisted. Default: Application is not allowed. Availability: Android devices.</p>
Windows Phone application policy	<p>Can be set to:</p> <ul style="list-style-type: none"> “Block applications on the list” – will block all the applications defined in the “Whitelisted / Blacklisted entries” section “Allow applications on the list” – will allow all the applications defined in the “Whitelisted / Blacklisted entries” section
Apple application policy	<p>Can be set to:</p> <ul style="list-style-type: none"> “Block applications on the list” – will block all the applications defined in the “Allow list / Deny list entries” section “Allow applications on the list” – will allow all the applications defined in the “Allow list / Deny list entries” section <p>It is also possible to block webclips, to block/deny all webclips, enter com.apple.webapp Availability: iOS devices in the Supervised mode</p>
Device Owner application policy	<p>Can be set to:</p> <ul style="list-style-type: none"> “No application policy” - will provide no changes for all the applications defined in the “Allow list / Deny list entries” section “Allow only applications from the list” - will allow all the applications defined in the “Allow list / Deny list entries” section “Block applications from the list” - will block all the applications defined in the “Allow list / Deny list entries” section <p>Availability: Device Owner devices</p>
Global Device Owner runtime permission policy	<p>Possibility to define permissions (Calendar, Camera, Contacts, Location, Microphone, Phone, Sensors, SMS, Memory, Physical activity) for specific applications. Can be set to:</p> <ul style="list-style-type: none"> “Managed by user” - will let the user to choose which permission is denied or allowed “Allow” - will allow all the permissions for the applications defined in the “Application permissions exceptions” section “Deny” - will block all the permissions for the applications defined in the “Application permissions exceptions” section <p>Availability: Device Owner devices</p>

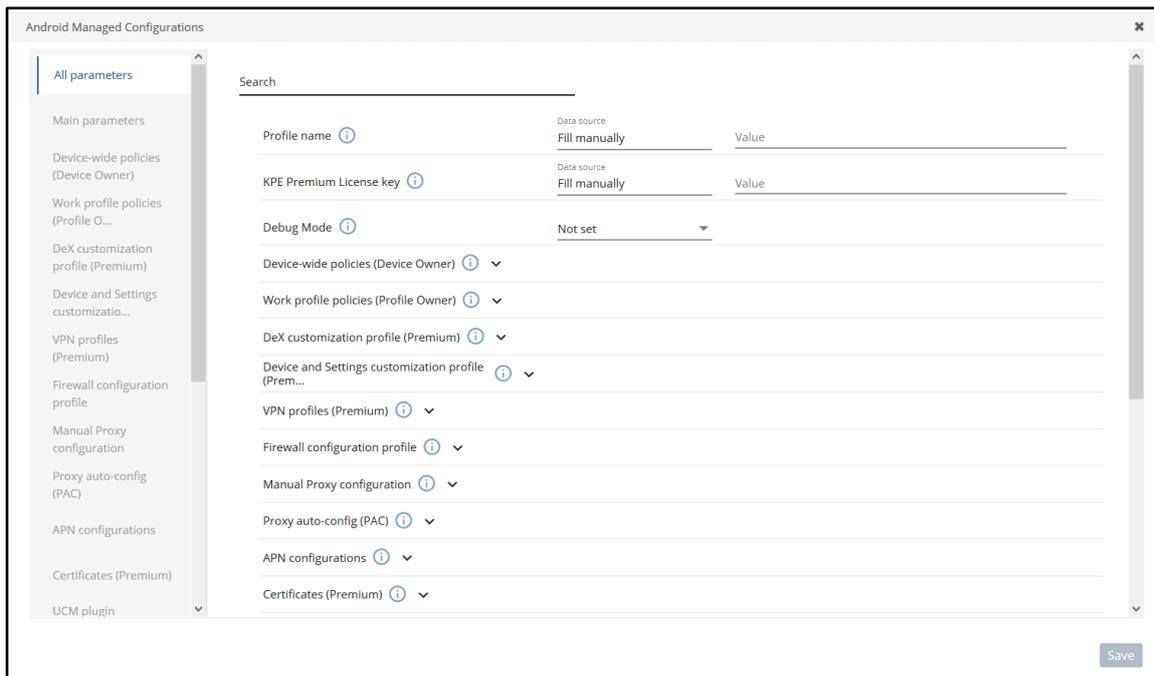
<p>The auto-update Managed Google Play apps policy settings</p>	<p>Can be set to:</p> <ul style="list-style-type: none"> ● Enable auto updates ● Enable auto updates only when the device is connected to WiFi ● Allow the user of device to configure the app update policy ● Disable auto updates <p>Availability: Android & Device Owner devices with Managed Google Play</p>
<p>Applications availability in the MGP store</p>	<p>This option determines the availability of the application in the Managed Google Play Store.</p> <p>Can be set to:</p> <ul style="list-style-type: none"> ● Only enabled applications (default) - only apps that are enabled and approved in Managed Google Play via FAMOC will be available ● All applications from the Google Play - all apps are displayed in Managed Google Play and allowed to install

2.4.11 Samsung KSP

Knox Service Plugin (KSP) is a solution that allows to set up policies and manage Samsung Knox Platform for Enterprise (KPE) enabled mobile devices. The KSP configuration procedure is described in a separate document available [here](#).

KSP settings are a part of the Security options section in the policy template. To use KSP settings in your policy click Enable Samsung KNOX Service Plugin. Then, click **Edit configuration**.

KSP provides several configurable parameters. To facilitate navigation in the settings, you can use the search field.



List of all available parameters can be found here: <https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm>

2.5 Advanced

In the Advanced policy settings, you can configure following parameters.

Parameter	Value
Advanced policy settings	
Confirmation mode for Base Agent	Base Agent confirmation mode: <ul style="list-style-type: none"> - Silent mode means the administrator can configure various options without bothering the user. - Information mode means the user will be informed each time the administrator wants to act. - Confirmation mode requires user confirmation each time the administrator wants to act Default value: Silent mode
FAMOC Base Agent administrator password	Password protection for Base Agent settings on the device (if left blank, no password is used) Default value: 12345
Number of stored Device Monitor sessions	Sets how many sessions of Device Monitor should be stored by FAMOC (1-10) Default value: 5
Number of archived Device Monitor sessions	Sets how many sessions of Device Monitor should be archived in logs (10-150) Default value: 20
Data reported in Device Monitor session	Select which data will be reported by the usage monitor. Default value: All (Choices: Base params; Applications; Bluetooth; Disks; Access points; Certificates; Device administrators; Device accounts; Software updates; SIM cards)
Time synchronization interval	Sets how often the system clock on the S60 device is synchronized with a Network Time Protocol Server Default value: Disabled
SIM change notify (for example if device was stolen)	Yes/No Default value: No
Device limit per user	Number of devices that user can add via the startup page when the user authentication option is set. If the limit is exceeded, specified user is not allowed to add any other device to the system using the startup page.
Organization name displayed on the device	The entered name will be displayed on the screen as - Your device is managed by (company name)
Show second line in header FAMOC Base Agent	Select if you want additional information about the name of the organization managing the device to be displayed in the Base Agent.

<p>Value of second line in header FAMOC Base Agent</p>	<p>The text displayed in the field described above.</p>
---------------------------------------------------------------	---------------------------------------------------------

Continuous parameter reporting and alerting

In this section you can define which battery parameters will be reported in real time. You can turn on continuous or peak reporting. If the battery status exceeds the specified threshold or status an alert will appear in the FAMOC manage console.

Available parameters are listed below:

- Battery condition - when the reported value is different from the specified (eg. specified: Good, reported: Overheat)
- Battery level - when the reported value is lower than specified 10%-50%
- Battery temperature - when the reported value is higher than specified 20-100 Celsius degree
- Battery voltage - when the reported value is higher than specified 2V-10V
- Charger state - when the reported state is different from the specified (eg. specified: Connected, reported: Not connected)
- Low battery level - when the reported value is equal to the specified (eg. reported and specified that the low battery level is reported)
- Memory RAM Free - when reported value is lower than specified 10-50%
- Signal strength - when reported value is lower than specified (eg. specified: -80dBm, reported: -107dBm)

Device details fields in Base Agent

Administrator can add custom fields which will be displayed in the Device Information Tab on the device.

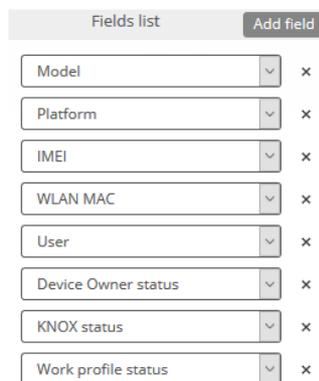


Figure 21 Device details fields

Backup settings

This section allows to set synchronization of all contacts or synchronization of data only within groups the user is a member of. In case of the latter option, administrator can specify additional groups, within which contacts are to be synchronized. To enlist groups of users for contact data

synchronization, use the Select button. You can also set contacts sync interval on a daily, weekly or monthly basis.

The screenshot shows a configuration window titled "Backup synchronization settings:". It contains several sections:

- Backup synchronization settings:** A dropdown menu for "Backup interval *" is set to "Off".
- Business contacts synchronization:** A dropdown menu for "Basic synchronization type" is set to "None of the contacts". Below it, another dropdown menu for "Business contacts sync interval" is set to "Off".
- Contacts synchronization of the additional groups:** A "Select" button is visible.
- Table:** A table with columns "Group name", "Group size", and "Assigned users". One row is visible: "Mike Group" with a size of "3" and assigned users "Mike Ross, Mike Bird, ff.michalk@outlook.com".

Figure 22 Contacts synchronization settings

Backup policy (deprecated)

This section enables backup policy settings like:

- Backup items – sets the backup items that will be included in policy (contacts, calendar, SMS, folders – based on platform).
- Backup frequency – sets the data synchronization frequency (daily/weekly/monthly/every X days). Under the **Add sample** button, FAMOC provides predefined backup patterns e.g., once a week on Monday or on the first day of each month.

Selecting Enable backup services checkbox activates backup policy. After that, Backup Agent will be installed with the policy and the backup policy will be applied.

The screenshot shows a configuration window titled "Backup policy". It contains several sections:

- Backup policy settings:** A checkbox for "Enable backup services" is currently unchecked.
- Backup items settings:** Includes an "Add new item" button and a table with columns "Type", "Path", "Total size", and "Total file size". The table lists "Contacts", "Calendar", and "SMS", each with a "20 MB" total size and a delete icon (x).
- Backup schedule settings *:** Includes "Add new" and "Add sample" buttons and a table with columns "Interval" and "Start at". The table lists five weekly schedules starting at 9:00 on Monday through Friday, each with a delete icon (x).

Figure 23 Backup policy settings

Usage policy

This section enables usage policy settings like:

- Reporting data traffic using WIFI
- Reporting data traffic using GPRS
- Reporting SMS content
- Reporting of the call type

Selecting the Enable usage monitor services checkbox activates the usage policy. After that, Usage Monitor will be installed with the policy and the usage policy applied.

Parameter	Description
Usage policy settings	
Enable usage monitor services	If this option is marked, Usage Monitor will be installed with the policy. Default value: not checked.
Report device data after restart of the device	If set, Usage Monitor will collect and send data on device restart.
Report data traffic using WIFI every	Interval of the WIFI data reporting (Do not report / 1 day / 3 days / 1 week / 2 weeks / 1 month / 3 months). Default value: 1 month.
Report data traffic using GPRS every	Interval of the GPRS data reporting (Do not report / 1 day / 3 days / 1 week / 2 weeks / 1 month / 3 months). Default value: 1 month.
Report SMS content	If set, content of the SMS will be reported. Default value: not checked.
Report device state	If set, reports device state. Default value: not checked.
Report screen unlock/lock time	Check to gather information about when the screen was unlocked.
Report application usage³	If set, reports application usage. Default value: not checked.
Report browser history	If set, reports browser history. Default value: not checked.
Report extended parameters every	Interval for reporting device state, application usage and browser history (Do not report / 15 minutes / 30 minutes / 1 hour / 6 hours / 1 day / 3 days / 1 week / 2 weeks / 1 month) Default value: 1 day.
Allow user to select the type of the call	If allow is selected, after the call the user will be prompted to select the type of the call. List of call types can be customized. By default, there are: Private, Corporate call types.

³ For Android 6.0 and higher, application usage reporting requires the Application Monitor Service on the device to be turned on.

	Default value: Do not allow.
--	------------------------------

3. BYOD/WPC policy templates

BYOD/WPC policies differ slightly from fully managed policies. In that approach most of the settings will affect only the work profile container on the device. All the components, restrictions and enabled applications will function only in the container. Private part of the device will function according to the user's settings (BYOD devices) or with low level of the control on WPC devices (work profile on company-owned devices).

3.1. General settings tab

Below is the list of parameters on general settings tab:

Parameter	Value
General settings	
Template name	Input policy name (max 100 chars)
Set priority order	Specify position on the policy template list
Reinstall Base Agent automatically	When the new Base Agent version appears in the system, it will be automatically reinstalled on devices (policy will be set as outdated). Default value: not checked.
Uninstall not compatible policy components automatically	If set, not matching policy components from current policy will be uninstalled if device will be moved to other policy. Default value: not checked.
Enable Samsung Premium API	To activate Samsung Premium API ⁴ in the policy this option must be marked. Once it is selected a proper license key must be provided. Default value: not checked.
Premium license	Samsung license key can be added/changed/removed by using plus/minus icons next to the license key field.
Premium license expiry date	When set, 14,7,3,1 day before that date the alert in organization will be generated. Default value: not set.
Enable Samsung attestation	If set, an additional operation for Samsung KNOX attestation process will be added to the queue and will check the device's software integrity before creating the KNOX container. Default value: not checked.
SafetyNet attestation	The SafetyNet Attestation API is an anti-abuse API that allows to assess the Android device. Default value: not checked.

⁴ You can read more about advantages offered by KPE Premium here: [Knox Platform for Enterprise | Advanced mobile security management](#)

Mark as wiped on Base Agent uninstallation	If set, the device will be marked as wiped in the FAMOC console if Base Agent is uninstalled. Default value: not checked.
Enable remote access services	If this option is marked, Remote Access will be installed with the policy. Default value: not selected
Remote Access session initialization consent	Available options: <ul style="list-style-type: none"> • Managed by user • Require on every connection • Automatic connection Default value: Managed by user
Enable location services	If this option is marked, Location Monitor will be installed with the policy. Default value: not selected
Location interval	Interval in which location of the device is checked. Default value: Off
Disable location reporting on off-peak	When set, location will not be retrieved from the device in off-peak. Default value: not checked
Disable location reporting after agent installation	When set, location will not be retrieved just after the agent is installed. Default value: not checked
Ignore battery optimization for Location monitor and Usage monitor	Possibility to add Location and Usage monitor to ignore optimization battery app list, so that schedules, SMS, mms reporting works properly. Selecting this option sends an operation that requires user confirmation.
Report additional data about apps (app size, cache size, data size)	Select to collect additional data about applications
Reported applications	Possible options: <ul style="list-style-type: none"> • Report all applications • Report only managed applications

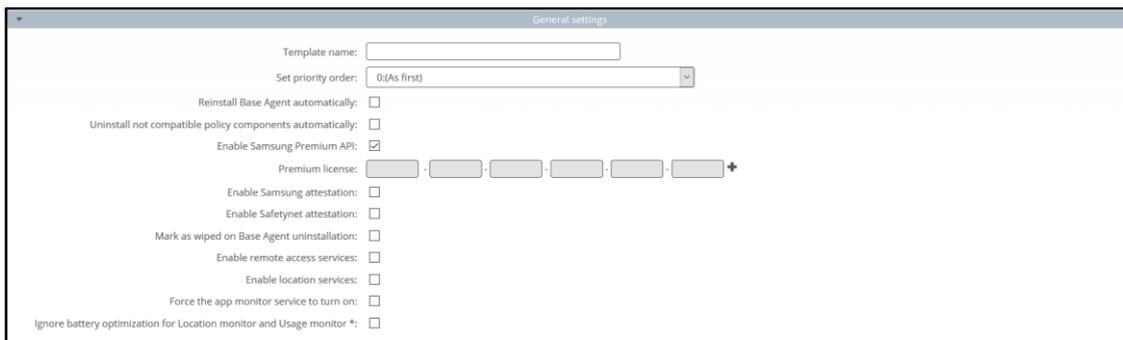


Figure 24 General settings tab

3.1.1. Schedules settings

Below is the list of parameters on schedules settings tab:

Parameter	Value
Schedules settings	
Peak schedule interval	The interval of Base Agent server connection: 5 min./15 min./30 min. /1h/4h/12h/Once a day/Once a week/Once a month Default value: Once a day
Peak days	Days of week during which Base Agent reports to FAMOC server Default value: Monday - Friday
Peak begin	What time during peak days should Base Agent start reporting Default value: 8:00
Peak end	What time during peak days should Base Agent stop reporting Default value: 16:00
Device Monitor sessions interval	Sets the interval of Device Monitor sessions: Off/Hourly/4 times a day/Daily/Weekly/Monthly Default value: Daily
Alerting device inactivity	Alerting inactivity of the Base Agent after 1-5 days/Week/Month/3 months. In case Base Agent does not report to server within this period, FAMOC generates an alert with three reaction options: <ul style="list-style-type: none"> ● Remove device from FAMOC ● Reinstall Base Agent ● Mark device as stolen Default value: After week
Wipe on exceeded device inactivity	If this option is marked and the Base Agent does not report to the server within a specified period, in addition to the generated alert, the device will be wiped.
Mark as wiped on exceeded device inactivity	If set, the device will be marked as wiped in the FAMOC console if it exceeds device inactivity period.

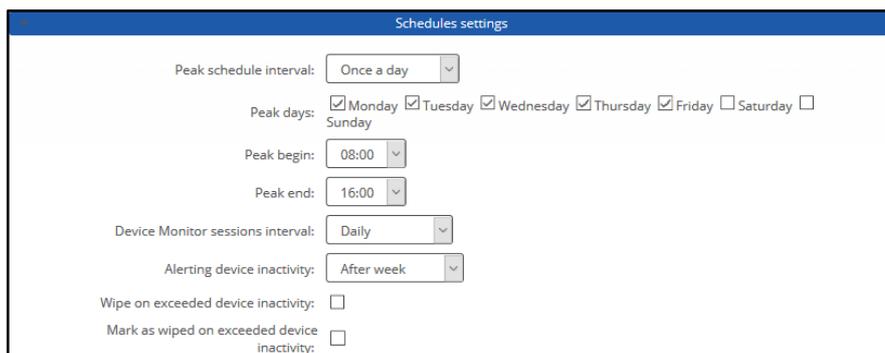


Figure 25 Schedules settings tab

3.2 Assigned groups

Each policy is assigned to certain groups of users or groups of devices, therefore each device receives a policy settings pre-defined to its group assignment. Devices not being members of any group and groups not being assigned to any policy receive a policy of the lowest priority (policy being at the bottom of the list). Devices being members of several groups receive the policy of the higher priority.

In the **Assigned Groups** tab administrator is allowed to assign groups to the policy. To select the group, click on the **Add device group** or **Add user group** button. Popup with a group list will appear.

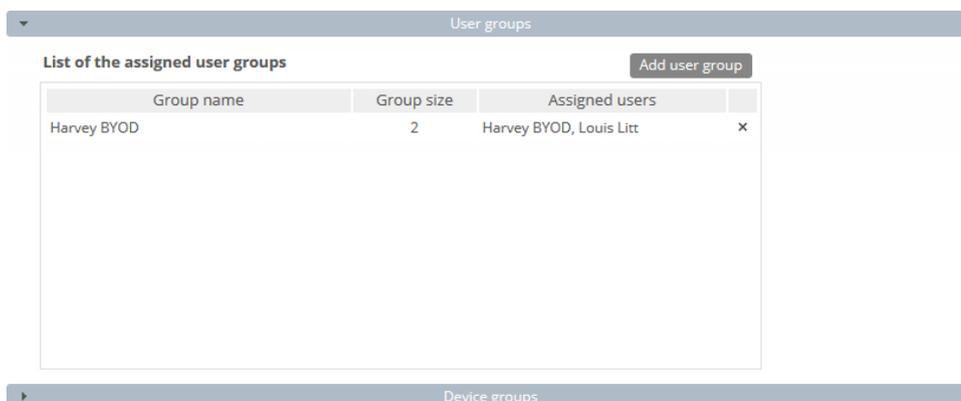


Figure 26 Groups tab

3.3 Policy components

In addition to general settings there is possibility to add configurations & applications to the policy. Please bear in mind that all those components and configurations will be installed in the work profile part of the device.

To add configuration to the policy, click the **Select configuration** button. Popup with configuration list will appear.

Configuration can be set for:

- Peak – configuration will be applied in peak
- Off-peak – configuration will be applied in off-peak
- Always – configuration will be applied always

Every time a device connects to the server, it checks if proper policy is applied, and if the change is needed (e.g., there was the end of the peak and currently applied configuration is only for the peak) old configuration is removed and the appropriate is applied. The time-based policies can only be applied to iOS devices.

To add application, click on the **Select application** button. Popup with application list will appear. Selected applications will be installed while applying the policy on the device. When the assigned to device policy is changed, the new policy will be applied, and the new list of application will be installed. When selecting the application, it is possible to specify number of installations retries (in

case an application installation is cancelled by user, FAMOC will retry the operation). Possible options:

- Installation obligatory (default option) – if installation is cancelled, it will be applied every next day.
- One installation attempt – if installation is cancelled, it will not be retried.
- Several installation attempts – installation will be retried specified number of times.

Policy components can be set in custom installation order using down/up arrows in **Order** column.

By default, each item is installed in a sequence (next item starts when previous has been successfully installed). It is possible to mark an item as independent (**Independent** column), which means the next action starts independently of the previous action, not waiting for its success report.

Select **Ignore failure** to execute the next action if the previous one failed.

Component name	Action	Ignore failure	Independent	Order
Adobe Acrobat Reader	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↓ ×
Set wallpaper on device - Home and Lock	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Przeglądarka Chrome	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
strongswan 1.4.1.0	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Gmail	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Require 4 chars lock code on Android	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ×

Figure 27 Policy components tab

3.4 Device security options

Device restrictions are applied to the whole device

Parameter	Value
Wipe policy	
Data wipe on SIM card change	If set, wipe will be performed when the SIM card change will be detected.
Wipe on no SIM card detection	If set, wipe will be performed when the SIM card is not detected. Option available when the first option is set (Data wipe on SIM card change). WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe.

Wipe on root detection	If set, the device will be wiped when root will be detected
Factory reset protection (FRP)	<p>Factory Reset Protection is a solution that allows you to start the device after restoring factory settings only with a Google account that you have previously logged into the device. Available configuration options for this setting:</p> <ul style="list-style-type: none"> • disable FRP (option will not be available on the device) • unlock the device with an active account on device (the device can be unlocked with the previously used account) • remove the factory reset protection (FRP) after device wipe (deactivates the FRP after the wipe)
Network policy	
Wi-Fi lock	If set, Wi-Fi cannot be used on the device. Availability: Android
Manual WiFi configuration lock	If set, there will be no possibility to configure WiFi connection manually. Availability: Android WPC
Prevent Wi-Fi from being turned off	Prevents Wi-Fi from being turned off in Settings or Control Center. Availability: Android WPC
Bluetooth lock	If set, Bluetooth cannot be used on the device. Availability: Android WPC
Cellular data lock in roaming	<p>Possible options:</p> <ul style="list-style-type: none"> - Do not lock - Disable and block possibility to enable <p>Availability: Android WPC 11+</p>
Block outgoing calls	Disables outgoing calls Availability: Android WPC 11+
Block Bluetooth config	Blocks possibility to change Bluetooth settings Availability: Android WPC
Block tethering config	Blocks possibility to change tethering settings Availability: Android WPC 11+
Block mobile networks config	Blocks possibility to change Bluetooth settings Availability: Android WPC 11+
Block cell broadcast config	Blocks possibility to configure Wireless Emergency Alerts (WEA), Amber Alerts Availability: Android WPC 11+
Disable SMS messages	Availability: Android WPC 11+
Location policy	
Disable location config on device	Availability: Android WPC

Disable location sharing on device	Availability: Android WPC 11+
Update policy	
Enable Zebra OTA updates	Availability: Zebra devices with: Android 7.0 and above, MX version 9.2 and above
Hardware policy	
Block safe mode	Availability: Android WPC 11+
Block airplane mode	Availability: Android WPC 11+
Enable USB debugging	Availability: Android both BYOD and WPC
Block screen capture	Availability: Android WPC
Block USB file transfer	Availability: Android WPC 11+
Disable mounting of the physical external media	Availability: Android WPC
Installer policy	
Unknown sources lock	Availability: Android BYOD and WPC
Application restrictions	
Block application voice recording on device	If set, microphone cannot be used on the device. Availability: Android WPC
Force automatic date and time	Availability: Android BYOD and WPC 11+
Application policy on device	Can be set to: <ul style="list-style-type: none"> • “No application policy” - will provide no changes for all the applications defined in the “Allow list / Deny list entries” section • “Allow only applications from the list” - will allow all the applications defined in the “Whitelisted / Blacklisted entries” section • “Block applications from the list” - will block all the applications defined in the “Whitelisted / Blacklisted entries” section Availability: Android WPC
Disable content capture on device	Availability: Android WPC 11+

Disable content suggestions on device	Availability: Android WPC 11+
----------------------------------------------	-------------------------------

3.5 Work profile security options

Parameter	Value
Wipe policy	
Enterprise wipe on SIM card change	If set, wipe will be performed when the SIM card change will be detected.
Enterprise wipe on no SIM card detection	If set, wipe will be performed when the SIM card is not detected. Option available when the first option is set (Data wipe on SIM card change). WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe.
Enterprise wipe on root detection	If set, the device will be wiped when root will be detected
Network policy	
Disable VPN settings	It blocks the possibility of changing the settings by the user Availability: Android BYOD and WPC
Disable managed networks settings change	Blocks the possibility to edit WiFi settings managed by FAMOC Availability: Android WPC 11 or higher
Monitor list of the managed Wifi configurations	It monitors the status of managed networks and triggers an alert in case of their removal (forgotten on the device). Availability: Android BYOD and WPC
Hardware policy	
Disable Siri	Possibility to disable Siri assistant Availability: iOS, iPadOS
Disable Siri when device is locked	Prevents Siri from starting on a locked device Availability: iOS, iPadOS
Disable connections to Siri servers for the purposes of dictation	If set, connections to Siri servers for the purposes of dictation will be disabled Availability: iOS, iPadOS

Disable connections to Siri servers for the purposes of translation	If set, connections to Siri servers for the purposes of translation will be disabled Availability: iOS, iPadOS
Disable automatically submitting diagnostic reports to Apple	If set, diagnostic report will not be automatically submitted to Apple Availability: iOS, iPadOS
Disable Control Center from appearing on the Lock screen	If set, Control Center will not appear on Lock screen Availability: iOS, iPadOS
Disables backup of Enterprise books	If set, backup of Enterprise books will be disabled Availability: iOS, iPadOS
Disables Enterprise Book metadata sync	If set, Enterprise Book metadata sync will be disabled Availability: iOS, iPadOS
Disables notifications history view on the lock screen	If set, notifications history view on the lock screen will be disabled Availability: iOS, iPadOS
Disables today notifications history view on the lock screen	If set, notifications history view on the lock screen will be disabled Availability: iOS, iPadOS
Disables managed applications to use the iCloud	If set, managed apps won't be able to use iCloud Availability: iOS, iPadOS
Force devices receiving AirPlay requests from this device to use a pairing pass	If set, pairing pass will be required when device receives AirPlay requests from this device Availability: iOS, iPadOS
Force encrypted backup	Forces backup encryption Availability: iOS, iPadOS
Force wrist detection on Apple Watch	If checked, forces the paired Apple Watch to use Wrist Detection Availability: iOS, iPadOS
Force to set lock code	If checked, forces the use of a lock code Availability: iOS, iPadOS
Encryption policy	
Internal storage encryption	If set, encryption will be required. Availability: Android
Installer policy	
Application installer lock	If set, there will be no possibility to install applications on the device. Availability: Android
Notification when application installation is blocked	You can set a notification that will appear on a device when a user tries to install an application. Default: Application installation is not allowed Availability: Android

Accounts creation using Google Play	Possibility to Disable/Enable accounts creation using Google Play When installer lock is set, accounts creation using Google Play is automatically disabled. Availability: Android
Application restrictions	
Application voice recording lock	If set, microphone cannot be used on the device. Availability: Android Samsung
Do not allow to share managed documents using AirDrop	If set, managed documents cannot be shared using AirDrop feature. Availability: iOS, iPadOS
Do not allow to share data from unmanaged apps	If set, sharing data from unmanaged apps will be forbidden. Availability: Android BYOD and WPC, iOS, iPadOS
Do not allow to share data from managed apps	If set, sharing data from managed apps will be forbidden. Availability: iOS, iPadOS
Allow unmanaged apps reading from managed contacts accounts	Availability: iOS, iPadOS
Enable 'Do not allow to share data from unmanaged / managed apps' restrictions for copy and paste functionality	Availability: iOS 15, iPadOS 15
Disable app uninstallation	Availability: iOS, iPadOS
Enables Safari fraud warning	Availability: iOS, iPadOS
Application policy	
The auto-update Managed Google Play apps policy settings	Can be set to: <ul style="list-style-type: none"> • Enable auto updates • Enable auto updates only when the device is connected to WiFi • Allow the user of device to configure the app update policy • Disable auto updates Availability: Android BYOD and WPC
Applications availability in the MGP store	This option determines the availability of the application in the Managed Google Play Store. Can be set to: <ul style="list-style-type: none"> • Only enabled applications (default) - only apps that are enabled and approved in Managed Google Play via FAMOC will be available • All applications from the Google Play - all apps are displayed in Managed Google Play and allowed to install Availability: Android BYOD and WPC

Work profile restrictions	
Enable unknown sources	Allows or blocks the possibility to install applications through .apk files to the Work Profile. The policy will not be active on Android 5.0 devices (installation of .apk is blocked)
Block screen capture	Allows to block screen capturing in application, which runs in the work profile to prevent from sharing data with that method. Availability: Android, Apple devices
Disable accounts modification	Blocks the possibility to add, edit or delete an account. Availability: Android BYOD and WPC
Block creation of the mail account	Availability: Samsung SDK only
Block creation of LDAP account	Availability: Samsung SDK only
Block creation of Samsung account	Availability: Samsung SDK only
Disable camera	Block the possibility to use the camera. Availability: Android BYOD and WPC
Disable cross profile copy-paste	Availability: Android BYOD and WPC
Disable application control	Blocks following actions: uninstalling & disabling apps, clearing app cache & data, force stopping apps and clearing apps defaults Availability: Android BYOD and WPC
Disable one lock code	Blocks the possibility to use one lock code for the device and Work Profile. Availability: Android BYOD and WPC
Allow moving apps to work profile	Availability: Samsung SDK only
Block NFC	Availability: Samsung SDK only
Disallow outgoing beam using NFC	Availability: Android BYOD and WPC
Allow moving files from device to work profile	Availability: Samsung SDK only
Allow moving files from work profile to device	Availability: Samsung SDK only
Block change of the sharing of the calendar to the personal mode	Availability: Samsung SDK only

Block change of the sharing of the calendar to work profile	Availability: Samsung SDK only
Enable Bluetooth	Availability: Samsung SDK only
Enable file sharing via Bluetooth in work profile	Availability: Android BYOD and WPC
Block Share Via List	Availability: Samsung SDK only
Prevent users from configuring credentials in the managed keystore	Availability: Android BYOD and WPC
Maximum time the work profile is allowed to be turned off	When the time is exceeded, the personal apps are blocked. Possible options: Disabled or 3-14 days Availability: Android WPC 11+
Enable the ability to restore of the backup from the Google account	Restoring data from private accounts is disabled by default, check this option to enable it Availability: Android BYOD and WPC
Disable location config	Blocks possibility to change location settings Availability: Android BYOD and WPC
Disable location sharing	Availability: Android BYOD and WPC
Disable content capture	Availability: Android BYOD and WPC
Disable content suggestions	Availability: Android BYOD and WPC
Work profile applications permissions	
Runtime permission policy	<p>Setting responsible for behaviour of applications, which asks for specific permission (Calendar, Camera, Contacts, Location, Microphone, Phone, Sensors, SMS, Memory, Physical activity) during its work. You can set three values:</p> <ul style="list-style-type: none"> ● Managed by user – default value, the user will be asked to give apps access to functions, which require specific permission. The user also will be able to change permissions for application. ● Allow – applications, which ask for permission, will have it granted automatically and the user will not be able to change it. ● Deny – applications, which ask for permission, will have it denied automatically and user will not be able to change it.

	<p>You can also set permissions for a specific application by clicking Add application. Then enter the package name and set the permissions for the application. Possible choices are:</p> <ul style="list-style-type: none"> ● As global ● Managed by user ● Allow ● Deny
<p>Samsung KSP for work profile</p>	
<p>Enable Samsung Knox Service Plugin</p>	<p>Knox Service Plugin (KSP) is a solution that allows to set up policies and manage Samsung Knox Platform for Enterprise (KPE) enabled mobile devices. The KSP configuration procedure is described in a separate document available here.</p> <p>KSP settings are a part of the Security options section in the policy template. To use KSP settings in your policy click Enable Samsung KNOX Service Plugin. Then, click Edit configuration.</p> <p>KSP provides a number of configurable parameters. To facilitate navigation in the settings, you can use the search field.</p> <p>List of all available parameters can be found here: https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm</p>

3.6 Enabled applications and widgets

In this section Admin can enable system applications in the work profile to be automatically accessible for users after profile activation. Enabled applications on the device may be different as some Android versions (especially branded versions) may not include all listed system applications. The admin can change the list of enabled applications and hide them according to needs. Default applications, which are always visible after profile activation are FAMOC Base Agent and managed Google Store. Currently available default apps:

Gmail (enabled by default in the policy), Contacts, Downloads, Google Maps, Google Calendar, Google Camera, Google Photos, Phone, Messages, Google Drive, Clock, Bixby, Samsung Galaxy Store, Netflix, One Drive, YouTube, Facebook, Google Chrome, Your Phone Companion – Link to Windows, Google Duo

New BYOD policy				
General settings			Availability	
			Android	Samsung SDK
Assigned groups	Google Maps	<input type="checkbox"/>	✓	✗
Policy components	Calendar	<input type="checkbox"/>	✓	✗
Security options	Camera	<input type="checkbox"/>	✓	✗
	Gallery	<input type="checkbox"/>	✓	✗
Enabled applications	Phone	<input type="checkbox"/>	✓	✗
Advanced	Messages	<input type="checkbox"/>	✓	✗
	Google Drive	<input type="checkbox"/>	✓	✗
	Contacts	<input type="checkbox"/>	✓	✗
	Downloads	<input type="checkbox"/>	✓	✗

Figure 28 System applications selection

In the widgets section, you can enable a widget of company apps - installed in Work Profile - to be used on the device Home Screen (they have to be added manually by the end user). The package name should be added to the list. The widgets of the application will now be available for adding on the home screen.

3.7 Advanced settings

In the Advanced policy settings, you can configure following parameters.

Parameter	Value
Advanced policy settings	
Number of stored Device Monitor sessions	Sets how many sessions of Device Monitor should be stored by FAMOC (1-10) Default value: 5
Number of archived Device Monitor sessions	Sets how many sessions of Device Monitor should be archived in logs (10-150) Default value: 20
Data reported in Device Monitor session	Select which data will be reported by the usage monitor. Default value: All (Possible choices: Base params; Applications; Bluetooth; Disks; Access points; Certificates; Device administrators; Device accounts; Software updates; SIM cards)
Time synchronization interval	Sets how often the system clock on the S60 device is synchronized with a Network Time Protocol Server Default value: Disabled
SIM change notify (for example if device was stolen)	Yes/No Default value: No
Device limit per user	Number of devices that user can add via startup page when user authentication option is set. If the limit is exceeded, specified user is not allowed to add any other device to the system using startup page.

Organization name displayed on the device*	The entered name will be displayed on the screen as - Your device is managed by (company name)
Show second line in header FAMOC Base Agent	Select if you want additional information about the name of the organization managing the device to be displayed in the Base Agent.
Value of second line in header FAMOC Base Agent	The text displayed in the field described above.

Continuous parameter reporting and alerting

In this section you can define which battery parameters will be reported in real time. You can turn on continuous or peak reporting. If the battery status exceeds the specified threshold or status an alert will appear in the FAMOC manage console.

Available parameters are listed below:

- Battery condition - when the reported value is different from the specified (eg. specified: Good, reported: Overheat)
- Battery level - when the reported value is lower than specified 10%-50%
- Battery temperature - when the reported value is higher than specified 20-100 Celsius degree
- Battery voltage - when the reported value is higher than specified 2V-10V
- Charger state - when the reported state is different from the specified (eg. specified: Connected, reported: Not connected)
- Low battery level - when the reported value is equal to the specified
- Memory RAM Free - when reported value is lower than specified 10-50%
- Signal strength - when reported value is lower than specified (eg. specified: -80dBm, reported: -107dBm)

Device details fields in Base Agent

Administrator can add custom fields which will be displayed in the Device Information Tab on the device.

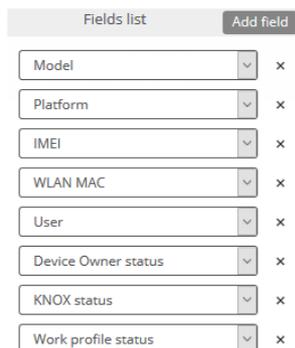


Figure 29 Device details fields

Backup settings

This section allows to set synchronization of all contacts or synchronization of data only within groups the user is a member of. In case of the latter option, administrator can specify additional groups, within which contacts are to be synchronized. To enlist groups of users for contact data synchronization, use the Select button. You can also set contacts sync interval on a daily, weekly or monthly basis.

Backup synchronization settings:

Backup interval *:

Business contacts synchronization:

Basic synchronization type:

Business contacts sync interval:

Contacts synchronization of the additional groups

Group name	Group size	Assigned users
Mike Group	3	Mike Ross, Mike Bird, ff.michalk@outlook.com <input type="button" value="x"/>

Figure 30 Contacts synchronization settings

Usage policy

This section enables usage policy settings like:

- Reporting data traffic using WIFI
- Reporting data traffic using GPRS
- Reporting SMS content
- Reporting of the call type

Selecting the Enable usage monitor services checkbox activates the usage policy. After that, Usage Monitor will be installed with the policy and the usage policy applied.

Parameter	Description
Usage policy settings	
Enable usage monitor services	If this option is marked, Usage Monitor will be installed with the policy. Default value: not checked.
Report device data after restart of the device	If set, Usage Monitor will collect and send data on device restart.
Report data traffic using WIFI every	Interval of the WIFI data reporting (Do not report / 1 day / 3 days / 1 week / 2 weeks / 1 month / 3 months). Default value: 1 month.
Report data traffic using GPRS every	Interval of the GPRS data reporting (Do not report / 1 day / 3 days / 1 week / 2 weeks / 1 month / 3 months). Default value: 1 month.
Report SMS content	If set, content of the SMS will be reported. Default value: not checked.

Report device state	If set, reports device state. Default value: not checked.
Report screen unlock / lock time	Check to gather information about when the screen was unlocked.
Report application usage⁵	If set, reports application usage. Default value: not checked.
Report browser history	If set, reports browser history. Default value: not checked.
Report extended parameters every	Interval for reporting device state, application usage and browser history (Do not report / 15 minutes / 30 minutes / 1 hour / 6 hours / 1 day / 3 days / 1 week / 2 weeks / 1 month) Default value: 1 day.
Allow user to select the type of the call	If Allow is selected, after the call the user will be prompted to select the type of the call. List of call types can be customized. By default, there are: Private, Corporate call types. Default value: Do not allow.

4. COSU Policies

COSU policies allow you to quickly configure dedicated use devices. Devices with this policy assigned will serve as single-use devices or will have only specific applications available.

4.1. General settings tab

Below is the list of parameters on general settings tab:

Parameter	Value
General settings	
Template name	Input policy name (max 100 chars)
Set priority order	Specify position on the policy template list
Reinstall Base Agent automatically	When a new Base Agent version appears in the system, it will be automatically reinstalled on devices (policy will be set as outdated). Default value: not checked.
Uninstall not compatible policy components automatically	If set, not matching policy components from current policy will be uninstalled if device will be moved to another policy. Default value: not checked.
Mark as wiped on Base Agent uninstallation	If set, the device will be marked as wiped in the FAMOC console if Base Agent is uninstalled. Default value: not checked.
Enable remote access services	If this option is marked, Remote Access will be installed with the policy. Default value: not selected

⁵ For Android 6.0 and higher, application usage reporting requires the Application Monitor Service on the device to be turned on.

Remote Access session initialization consent	<p>Available options:</p> <ul style="list-style-type: none"> • Managed by user • Require on every connection • Automatic connection <p>Default value: Managed by user</p>
Enable location services	<p>If this option is marked, Location Monitor will be installed with the policy. Default value: not selected</p>
Location interval	<p>Interval in which location of the device is checked. Default value: Off</p>
Disable location reporting on off-peak	<p>When set, location will not be retrieved from the device in off-peak. Default value: not checked</p>
Disable location reporting after agent installation	<p>When set, location will not be retrieved just after the agent is installed. Default value: not checked</p>
Report additional data about apps (app size, cache size, data size)	<p>After selecting this option, FAMOC will collect information about the memory used by the application and its files</p>
Reported applications	<p>Options available:</p> <ul style="list-style-type: none"> • Report all applications • Report only managed applications

4.1.1. Schedules settings

Below is the list of parameters on schedules settings tab:

Parameter	Value
Schedules settings	
Peak schedule interval	<p>The interval of Base Agent server connection: 5 min./15 min./30 min. /1h/4h/12h/Once a day/Once a week/Once a month Default value: Once a day</p>
Peak days	<p>Days of week during which Base Agent reports to FAMOC server Default value: Monday - Friday</p>
Peak begin	<p>What time during peak days should Base Agent start reporting Default value: 8:00</p>
Peak end	<p>What time during peak days should Base Agent stop reporting Default value: 16:00</p>

Device Monitor sessions interval	Sets the interval of Device Monitor sessions: Off/Hourly/4 times a day/Daily/Weekly/Monthly Default value: Daily
Alerting device inactivity	Alerting inactivity of the Base Agent after 1-5 days/Week/Month/3 months. In case Base Agent does not report to server within this period, FAMOC generates an alert with three reaction options: <ul style="list-style-type: none"> ● Remove device from FAMOC ● Reinstall Base Agent ● Mark device as stolen Default value: After week
Wipe on exceeded device inactivity	If this option is marked and Base Agent doesn't report to server within a specified period of time, in addition to generated alert, the device will be wiped.
Mark as wiped on exceeded device inactivity	If set, the device will be marked as wiped in the FAMOC console if it exceeds device inactivity period.

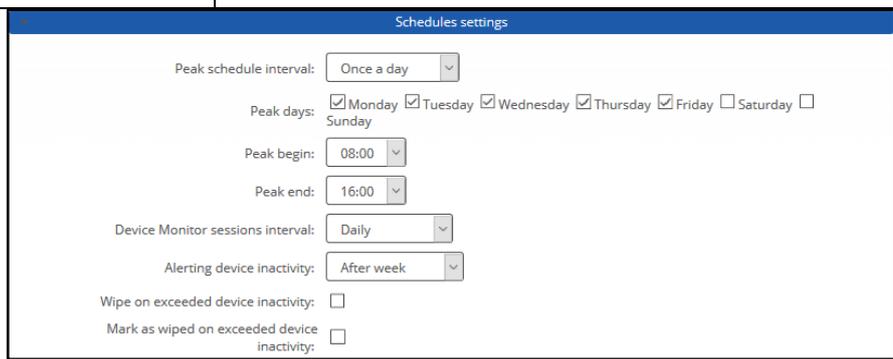
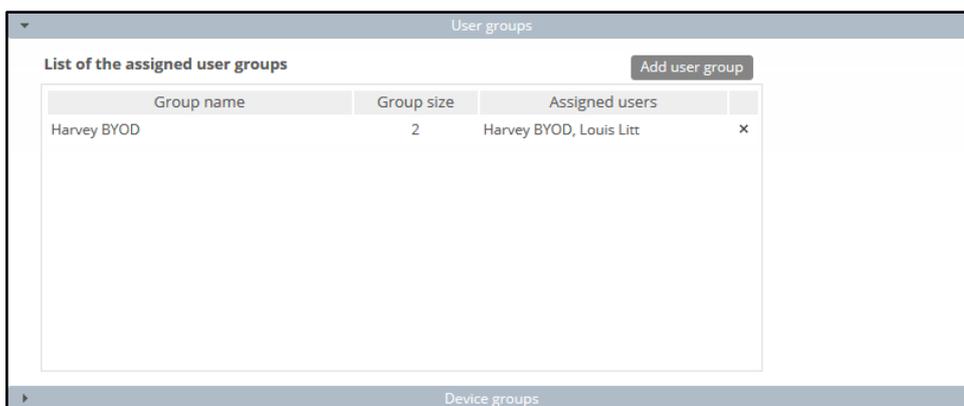


Figure 32 Schedules settings tab

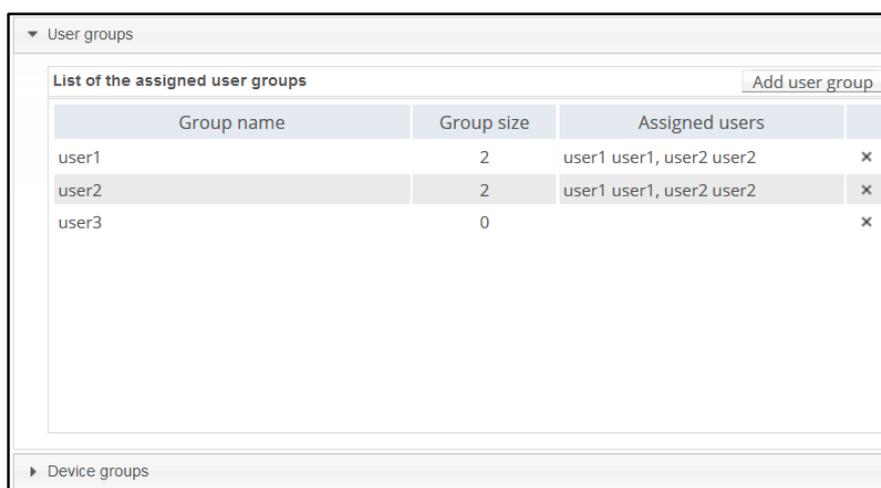
4.2 Assigned groups

Each policy is assigned to certain groups of users or groups of devices, therefore each device receives a policy settings pre-defined to its group assignment. Devices not being members of any group and groups not being assigned to any policy receive a policy of the lowest priority (policy being at the bottom of the list). Devices being members of several groups receive the policy of the higher priority.

In the **Assigned Groups** tab administrator is allowed to assign groups to the policy. To select the group, click on the **Add device group** or **Add user group** button. Popup with group list will appear.



Mark checkboxes next to appropriate groups and click **Select**. Groups will be now assigned to the policy.



4.3 Policy components

In addition to general settings there is possibility to add configurations & applications to the policy.

To add configuration to the policy, click the **Select configuration** button. Popup with configuration list will appear.

Configuration can be set for:

- Peak – configuration will be applied in peak
- Off-peak – configuration will be applied in off-peak
- Always – configuration will be applied always

Every time a device connects to the server, it checks if proper policy is applied, and if the change is needed (e.g., there was the end of the peak and currently applied configuration is only for the peak) old configuration is removed and the appropriate is applied. The time-based policies can only be applied to iOS devices.

To add an application, click on the **Select application** button. Popup with the application list will appear. Selected applications will be installed while applying the policy on the device. When the assigned to device policy is changed, the new policy will be applied, and the new list of applications will be installed. When selecting the application, it is possible to specify the number of installations retries (in case an application installation is cancelled by the user, FAMOC will retry the operation). Possible options:

- Installation obligatory (default option) – if installation is cancelled, it will be applied every next day.
- One installation attempt – if installation is cancelled, it will not be retried.
- Several installation attempts – installation will be retried specified number of times.

Policy components can be set in custom installation order using down/up arrows in **Order** column.

By default, each item is installed in a sequence (next item starts when previous has been successfully installed). It is possible to mark an item as independent (**Independent** column), which means the next action starts independently of the previous action, not waiting for its success report.

Select **Ignore failure** to execute the next action if the previous one failed.

Component name	Action	Ignore failure	Independent	Order
Adobe Acrobat Reader	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↓ ×
Set wallpaper on device - Home and Lock	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Przeglądarka Chrome	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
strongswan 1.4.1.0	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Gmail	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓ ×
Require 4 chars lock code on Android	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ×

Figure 34 Policy components tab

4.4 COSU mode settings

Here, you can configure kiosk mode settings. First, select **Lock mode** whether you wish to use FAMOC launcher only with apps from the allow list or a single application. Regardless of your choice, you will have to provide the name of a package or names of applications for a whitelist.

Rest of the settings is listed below:

Parameter	Value
COSU mode settings	
Lock mode	Settings: <ul style="list-style-type: none"> • FAMOC Launcher with allowed app list • Single application
FAMOC Launcher settings	

Wallpaper	Possibility to upload wallpaper
Start first application after reboot	Select Yes to automatically launch the first available application after device restart.
Inactivity timeout	Possible options: Disabled or between 30 seconds and 10 minutes
Show custom status bar	If set, a custom status bar will be displayed.
Show custom settings bar	If set, a custom settings bar will be displayed. Additional settings: <ul style="list-style-type: none"> ● Position - Location of the bar on the screen ● Theme - Light or dark ● Custom field - Possibility to display additional information taken from a selected custom field (up to 4 custom fields) ● Show Bluetooth icon ● Show WIFI icon ● Show torch icon ● Show restart icon
Allowed app list	Here you can provide a list of allowed apps in FAMOC Launcher
Shortcuts	Here you can provide a list of application shortcuts and webclips in FAMOC Launcher
Single app COSU settings	
Application package name	Provide the name of the app which will be used in COSU mode.
Other settings	
Volume change	Possible choices: Enabled/Disabled
Long press power button	Possible choices: Enabled/Disabled. Available from Android 9.0
Keyguard	Possible choices: Enabled/Disabled. Available from Android 9.0
Home button	Possible choices: Enabled/Disabled. Available from Android 9.0
Recent apps	Possible choices: Enabled/Disabled. Available from Android 9.0
Notifications	Possible choices: Enabled/Disabled. Available from Android 9.0
System info on status bar	Possible choices: Enabled/Disabled. Available from Android 9.0
Default applications to open files	Possibility to define a default application for opening documents (e.g. .pdf, .xls). To do this, expand the list and click Add default application. Then select the file type from the drop-down list and enter the appropriate parameters in the fields below. Default settings schemes can be used for the most popular applications.

4.5 Security options

Security options include following settings:

1. Wipe policy

2. Network policy
3. Location policy
4. Update policy
5. Hardware policy
6. Encryption policy
7. Installer policy
8. Application restrictions
9. Application policy
10. Samsung KSP

4.5.1 Wipe policy

Below is the list of parameters on Wipe policy settings tab:

Parameter	Description
Wipe policy	
Data wipe on SIM card change	If set, wipe will be performed when the SIM card change will be detected.
Wipe on no SIM card detection	If set, wipe will be performed when the SIM card is not detected. Option available when the first option is set (Data wipe on SIM card change). WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe.
Wipe memory card	If set, memory card will be wiped in addition when SIM card change will be detected. Option available when the first option is set (Data wipe on SIM card change).
Wipe on root detection	If set, the device will be wiped when root will be detected. Availability: Android devices.
Factory reset lock	If set, factory reset cannot be performed.
Factory reset protection (FRP)⁶	Factory Reset Protection is a solution that allows you to start the device after restoring factory settings only with a Google account that you have previously logged into the device. Available configuration options for this setting: <ul style="list-style-type: none"> ● disable FRP (option will not be available on the device) ● unlock the device with an active account on device (the device can be unlocked with the previously used account)

⁶ List of the unlock accounts must contain the valid Google user ID's. They can be obtained from the Google API, using the link below: <https://developers.google.com/people/api/rest/v1/people/get>

By executing the API call and logging with valid Google account, response returns the 'id' field of the user.

	<ul style="list-style-type: none"> • unlock the device with an account from the defined list (the device can be unlocked with an account from the list defined in FAMOC - user ID should be provided) • remove the factory reset protection (FRP) after device wipe (deactivates the FRP after the wipe) <p>Availability: Device Owner</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.5.2 Network policy

Below is the list of parameters on Network policy settings tab:

Parameter	Description
Network policy	
Wi-Fi lock	If set, Wi-Fi cannot be used on the device.
Manual WiFi configuration lock	If set, there will be no possibility to configure WiFi connection manually. Availability: Device Owner
Keep Wi-Fi on in sleep mode	If set prevents Wi-Fi disconnecting in sleep mode. Availability: Device Owner
Bluetooth lock	If set, Bluetooth cannot be used on the device.
Cellular data lock	Possible options: <ul style="list-style-type: none"> - Do not lock - Enable and block possibility to disable - Disable and block possibility to enable
Cellular data lock in roaming	Possible options: <ul style="list-style-type: none"> - Do not lock - Disable and block possibility to enable <p>Default value: Do not lock.</p>
WiFi tethering lock	If set, WiFi tethering is disabled. Availability: Android Samsung with Enterprise SDK from 2.0 and Device Owner
USB tethering lock	If set, USB tethering is disabled. Availability: Android Samsung with Enterprise SDK from 3.0, Device Owner
Block incoming MMS	If set, incoming MMS won't be delivered Availability: Android Samsung with Enterprise SDK from 3.0
Disable network settings reset	If set, the 'Reset network settings' option won't be available Availability: Device Owner
Disable VPN settings	If set, VPN settings change is not allowed.
Block private DNS settings	If set, the user cannot set private DNS or turn off the DNS over TLS on the device. Availability: Device Owner, Android 10.0+

Block incoming calls	<p>Allows you to block incoming calls. Available options:</p> <ul style="list-style-type: none"> • Do not block • All • Pattern (The pattern of blocked numbers may contain e.g., numbers starting from 0700) <p>Availability: Samsung SDK</p>
Block incoming SMS messages	<p>Allows you to block incoming text messages. Available options:</p> <ul style="list-style-type: none"> • Do not block • All • Pattern (The pattern of blocked numbers may contain e.g., numbers starting from 0700) <p>Availability: Samsung SDK</p>
Monitor list of the managed Wifi configurations	<p>It monitors the status of managed networks and triggers an alert in case of their removal (forgotten on the device).</p>

4.5.3 Location policy

Below is the list of parameters on Location policy settings tab:

Parameter	Description
Location policy	
Android location lock	<p>Allows to grant the FAMOC agent access to the location and blocks the possibility of revoking these permissions. Possible settings:</p> <ul style="list-style-type: none"> • Do not lock • Disable location and block possibility to enable <p>Availability: Android 8.0, Device Owner mode.</p>

4.5.4 Update policy

Below is the list of parameters on Update policy settings tab:

Parameter	Description
Update policy	
Control system version (Samsung E-FOTA)	<p>If set, E-FOTA is enabled.</p> <p>Availability: Android Samsung 7.x with Knox 2.7.1+</p>
OTA update lock	<p>Possibility to define OTA update policy. Available options are:</p> <ul style="list-style-type: none"> • No policy • Automatic • Windowed • Postponed <p>Availability: Device Owner (blocks system updates for 30 days), Android Samsung with Enterprise SDK 3.0</p>

4.5.5 Hardware policy

Below is the list of parameters on Hardware policy settings tab:

Parameter	Description
Hardware policy	
Camera lock	If set, the camera cannot be used on the device. Availability: Samsung SDK, Huawei SDK, Device Owner.
USB media player lock	If set, and the device is connected to PC using USB, the device cannot be used in media player mode. Availability: Android Samsung SDK 3.0
Development mode lock	If set, development mode can't be enabled. Availability: Device Owner, Android Samsung with Enterprise SDK 5.0
Task manager lock	If set, the task manager will be blocked. Availability: Android Samsung with Enterprise SDK 3.0
NFC lock	If set, NFC cannot be used. Availability: Android Samsung with Enterprise SDK from 2.0
Disallow outgoing beam using NFC	If set, user is not allowed to use NFC to transfer data from apps. Availability: Device Owner
Storage card lock	If set, disable Storage card socket. Availability: Device Owner, Android Samsung with Enterprise SDK from 2.0
Screen capture lock	If set, there will be no possibility to capture screenshots Availability: Device Owner, Android Samsung with Enterprise SDK from 2.0
USB file manager lock	If set, there will be no possibility to browse files through USB connection. Availability: Device Owner
Block multi-window mode	If set, multi-window mode won't be accessible on device Availability: Android Samsung with Enterprise SDK from 4.0
Block safe mode	If set, safe mode won't be accessible on the device. Availability: Device Owner, Android Samsung with Enterprise SDK from 4.0
Block airplane mode	If set, airplane mode won't be accessible on the device. Availability: Android Samsung with Enterprise SDK from 5.0
Prevent users from configuring credentials in the managed keystore	If set, user will not have access to some Credential storage options such as: View user certificates, install certificates from device storage, Remove certificates Availability: Device Owner

4.5.6 Encryption policy

Below is the list of parameters on Encryption policy settings tab:

Parameter	Description
Encryption policy	
Internal storage encryption	If set, encryption will be required. Availability: Android 4.x and Android Samsung with Enterprise SDK 2.0/3.0

4.5.7 Installer policy

Below is the list of parameters on Installer policy settings tab:

Parameter	Description
Installer policy	
Application installer lock	If set, there will be no possibility to install applications on the device. Moreover, selecting this option will cause the following options to be selected without the possibility to be changed. <ul style="list-style-type: none"> • Unknown sources lock • Disable accounts modification • Disable application control Availability: Android
Allow USB debugging	If set, USB debugging can be set on device. Available for Device Owner, Android Samsung from Enterprise SDK 3.0 and for Android Sony with Enterprise SDK from 5.0 USB debugging is blocked by default.
Unknown sources lock	If set, the possibility to change the unknown sources setting is blocked Availability: Device Owner, Android Samsung with Enterprise SDK 2.0
Accounts creation using Google Play	If set to Disabled, the possibility to add an account will be locked Availability: Device Owner
Disable application control	If set, users will not be able to modify app (uninstall, stop, clear app data). Availability: Android Device Owner

4.5.8 Application restrictions

Below is the list of parameters on Application restrictions tab:

Parameter	Description
Application restrictions	
Application voice recording lock	If set, the microphone cannot be used on the device. Availability: Android Samsung SDK
Do not force Google Play Protect	This option disables Google Play Protect scanning for any malicious software. It requires the newest Google Play services on Android 6.0, 7.0 with work profile enabled.

	Availability: Android
Phone settings lock	If set, there will be no possibility to enter the settings on the device. Availability: Android, Device Owner
Force automatic date and time	It automatically downloads time data from the network and blocks the possibility of manual changes.
Disable accounts modification	If set, the possibility to add, edit or delete an account will be locked Availability: Device Owner
Disable user accounts management	If set, additional user accounts can't be created. Availability: Android Samsung with Enterprise SDK from 4.0

4.5.9 Application policy

Below is the list of parameters on Application policy tab:

Parameter	Description
Application policy	
Device Owner application policy	<p>Can be set to:</p> <ul style="list-style-type: none"> • "No application policy" - will provide no changes for all the applications defined in the "Allow list/ Deny list entries" section • "Allow only applications from the list" - will allow all the applications defined in the "Allow list / Deny list entries" section • "Block applications from the list" - will block all the applications defined in the "Whitelisted / Blacklisted entries" section <p>Availability: Device Owner devices</p>
Global Device Owner runtime permission policy	<p>Possibility to define permissions (Calendar, Camera, Contacts, Location, Microphone, Phone, Sensors, SMS, Memory, Physical activity) for specific applications.</p> <p>Can be set to:</p> <ul style="list-style-type: none"> • "Managed by user" - will let the user to choose which permission is denied or allowed • "Allow" - will allow all the permissions for the applications defined in the "Application permissions exceptions" section • "Deny" - will block all the permissions for the applications defined in the "Application permissions exceptions" section <p>Availability: Device Owner devices</p>
The auto-update Managed Google Play apps policy settings	<p>Can be set to:</p> <ul style="list-style-type: none"> • Enable auto updates • Enable auto updates only when the device is connected to Wi-Fi • Allow the user of device to configure the app update policy • Disable auto updates

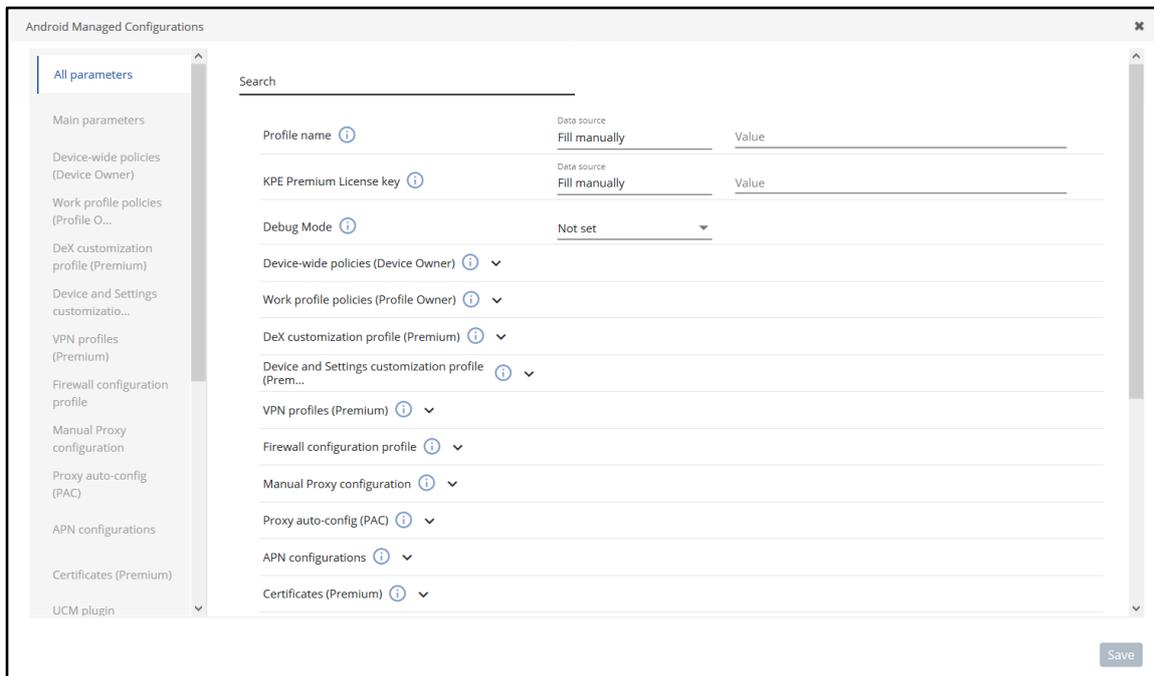
<p>Applications availability in the Managed Google Play store</p>	<p>This option determines the availability of the application in the Managed Google Store. Can be set to:</p> <ul style="list-style-type: none"> ● Only enabled applications (default) - only apps that are enabled and approved in Managed Google Play via FAMOC will be available ● All applications from the Google Play - all apps are displayed in Managed Google Play and allowed to install
--------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.5.9 Samsung KSP

Knox Service Plugin (KSP) is a solution that allows to set up policies and manage Samsung Knox Platform for Enterprise (KPE) enabled mobile devices. The KSP configuration procedure is described in a separate document available [here](#).

KSP settings are a part of the Security options section in the policy template. To use KSP settings in your policy click Enable Samsung KNOX Service Plugin. Then, click **Edit configuration**.

KSP provides several configurable parameters. To facilitate navigation in the settings, you can use the search field.



List of all available parameters can be found here: <https://docs.samsungknox.com/admin/knox-service-plugin/release-notes.htm>

4.6 Advanced

In the Advanced policy settings, you can configure following parameters.

Parameter	Value
-----------	-------

Advanced policy settings	
Number of stored Device Monitor sessions	Sets how many sessions of Device Monitor should be stored by FAMOC (1-10) Default value: 5
Number of archived Device Monitor sessions	Sets how many sessions of Device Monitor should be archived in logs (10-150) Default value: 20
Data reported in Device Monitor session	Select which data will be reported by the usage monitor. Default value: All (Possible choices: Base params; Applications; Bluetooth; Disks; Access points; Certificates; Device administrators; Device accounts; Software updates; SIM cards)
Time synchronization interval	Sets how often the system clock on the S60 device is synchronized with a Network Time Protocol Server Default value: Disabled
SIM change notify (for example if device was stolen)	Yes/No Default value: No
Device limit per user	Number of devices that user can add via startup page when user authentication option is set. If the limit is exceeded, specified user is not allowed to add any other device to the system using startup page.
Organization name displayed on the device*	The entered name will be displayed on the screen as - Your device is managed by (company name)
Show second line in header FAMOC Base Agent	Select if you want additional information about the name of the organization managing the device to be displayed in the Base Agent.
Value of second line in header FAMOC Base Agent	The text displayed in the field described above.

Continuous parameter reporting and alerting

In this section you can define which battery parameters will be reported in real time. You can turn on continuous or peak reporting. If the battery status exceeds the specified threshold or status an alert will appear in the FAMOC manage console.

Available parameters are listed below:

- Battery condition - when the reported value is different from the specified (eg. specified: Good, reported: Overheat)
- Battery level - when the reported value is lower than specified 10%-50%
- Battery temperature - when the reported value is higher than specified 20-100 Celsius degree
- Battery voltage - when the reported value is higher than specified 2V-10V

- Charger state - when the reported state is different from the specified (eg. specified: Connected, reported: Not connected)
- Low battery level - when the reported value is equal to the specified (eg. reported and specified that the low battery level is reported)
- Memory RAM Free - when reported value is lower than specified 10-50%
- Signal strength - when reported value is lower than specified (eg. specified: -80dBm, reported: -107dBm)

Device details fields in Base Agent

Administrator can add custom fields which will be displayed in the Device Information Tab on the device.

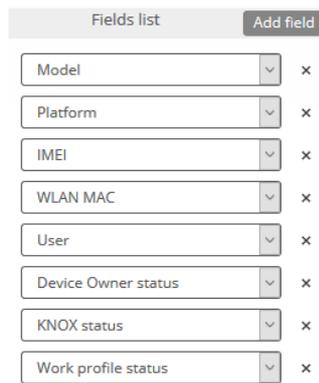


Figure 21 Device details fields

Backup settings

This section allows to set synchronization of all contacts or synchronization of data only within groups the user is a member of. In case of the latter option, administrator can specify additional groups, within which contacts are to be synchronized. To enlist groups of users for contact data synchronization, use the Select button. You can also set contacts sync interval on a daily, weekly or monthly basis.

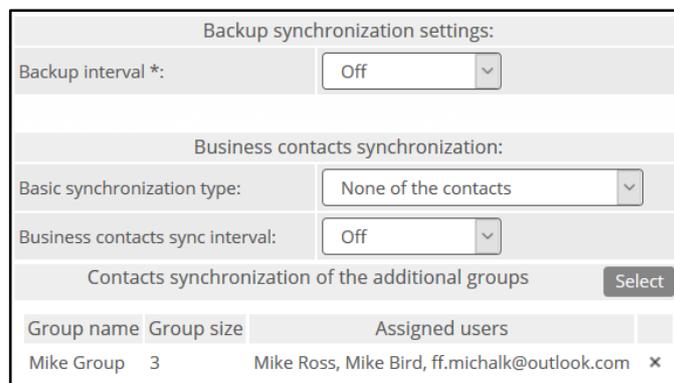


Figure 22 Contacts synchronization settings

5. Shared device Policies

Shared device policies allow you to place restrictions on devices running in shared mode.

5.1. General settings tab

Below is the list of parameters on general settings tab:

Parameter	Value
General settings	
Template name	Input policy name (max 100 chars)
Set priority order	Specify position on the policy template list
Reinstall Base Agent automatically	When a new Base Agent version appears in the system, it will be automatically reinstalled on devices (policy will be set as outdated). Default value: not checked.
Uninstall not compatible policy components automatically	If set, not matching policy components from current policy will be uninstalled if device will be moved to another policy. Default value: not checked.
Mark as wiped on Base Agent uninstallation	If set, the device will be marked as wiped in the FAMOC console if Base Agent is uninstalled. Default value: not checked.
Reported applications	Options available: <ul style="list-style-type: none"> • Report all applications • Report only managed applications

5.1.1. Schedules settings

Below is the list of parameters on schedules settings tab:

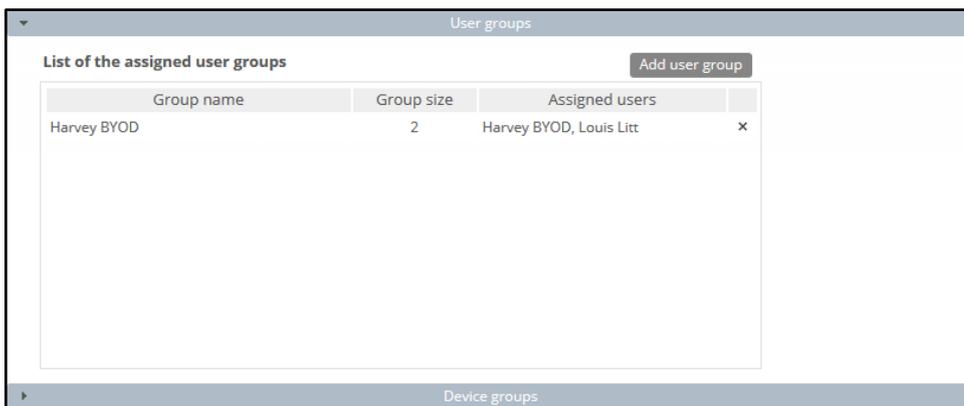
Parameter	Value
Schedules settings	
Peak schedule interval	The interval of Base Agent server connection: 5 min./15 min./30 min. /1h/4h/12h/Once a day/Once a week/Once a month Default value: Once a day
Peak days	Days of week during which Base Agent reports to FAMOC server Default value: Monday - Friday
Peak begin	What time during peak days should Base Agent start reporting Default value: 8:00
Peak end	What time during peak days should Base Agent stop reporting Default value: 16:00
Device Monitor sessions interval	Sets the interval of Device Monitor sessions: Off/Hourly/4 times a day/Daily/Weekly/Monthly

	Default value: Daily
Alerting device inactivity	Alerting inactivity of the Base Agent after 1-5 days/Week/Month/3 months. In case Base Agent does not report to server within this period, FAMOC generates an alert with three reaction options: <ul style="list-style-type: none"> • Remove device from FAMOC • Reinstall Base Agent • Mark device as stolen Default value: After week
Wipe on exceeded device inactivity	If this option is marked and Base Agent doesn't report to server within a specified period of time, in addition to generated alert, the device will be wiped.
Mark as wiped on exceeded device inactivity	If set, the device will be marked as wiped in the FAMOC console if it exceeds device inactivity period.

5.2 Assigned device groups

Each policy is assigned to certain groups of users or groups of devices, therefore each device receives a policy setting pre-defined to its group assignment. Devices not being members of any group and groups not being assigned to any policy receive a policy of the lowest priority (policy being at the bottom of the list). Devices being members of several groups receive the policy of the higher priority.

In the **Assigned Groups** tab administrator is allowed to assign groups to the policy. To select the group, click on the **Add device group** or **Add user group** button. Popup with group list will appear.



Mark checkboxes next to appropriate groups and click **Select**. Groups will be now assigned to the policy.

5.3 Policy components

In addition to general settings there is possibility to add configurations & applications to the policy.

To add configuration to the policy, click the **Select configuration** button. Popup with configuration list will appear.

Configuration can be set for:

- Peak – configuration will be applied in peak
- Off-peak – configuration will be applied in off-peak
- Always – configuration will be applied always

Every time a device connects to the server, it checks if proper policy is applied, and if the change is needed (e.g., there was the end of the peak and currently applied configuration is only for the peak) old configuration is removed and the appropriate is applied. The time-based policies can only be applied to iOS devices.

To add an application, click on the **Select application** button. Popup with the application list will appear. Selected applications will be installed while applying the policy on the device. When the assigned to device policy is changed, the new policy will be applied, and the new list of applications will be installed. When selecting the application, it is possible to specify the number of installations retries (in case an application installation is cancelled by the user, FAMOC will retry the operation). Possible options:

- Installation obligatory (default option) – if installation is cancelled, it will be applied every next day.
- One installation attempt – if installation is cancelled, it will not be retried.
- Several installation attempts – installation will be retried specified number of times.

Policy components can be set in custom installation order using down/up arrows in **Order** column.

By default, each item is installed in a sequence (next item starts when previous has been successfully installed). It is possible to mark an item as independent (**Independent** column), which means the next action starts independently of the previous action, not waiting for its success report.

Select **Ignore failure** to execute the next action if the previous one failed.

Policy components		Select application	Select configuration			
Component name	Action	Ignore failure	Independent	Order		
Adobe Acrobat Reader	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↓	×	
Set wallpaper on device - Home and Lock	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Przeglądarka Chrome	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
strongswan 1.4.1.0	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Gmail	Number of retries: Installation oblig: ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑ ↓	×	
Require 4 chars lock code on Android	Peak policy: Always ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑	×	

5.4 Security options on the device

5.4.1 Update policy

Below is the list of parameters on Update policy settings tab:

Parameter	Description
Update policy	
OTA update lock	Possibility to define OTA update policy. Available options are: <ul style="list-style-type: none"> • No policy • Automatic • Windowed • Postponed Availability: Device Owner (blocks system updates for 30 days), Android Samsung with Enterprise SDK 3.0

5.4.2 Hardware policy

Below is the list of parameters on Hardware policy settings tab:

Parameter	Description
Hardware policy	
USB file manager lock	If set, there will be no possibility to browse files through USB connection.
Block safe mode	If set, safe mode won't be accessible on the device. Availability: Device Owner, Android Samsung with Enterprise SDK from 4.0
Block airplane mode	If set, airplane mode won't be accessible on the device. Availability: Android Samsung with Enterprise SDK from 5.0

5.5 User profile settings

Here you can specify some restrictions for profiles created on a shared device.

5.5.1 Work profile restrictions

Parameter	Value
Work profile restrictions	
Enable unknown sources	Allows or blocks the possibility to install applications through .apk files to the Work Profile. The policy will not be active on Android 5.0 devices (installation of .apk is blocked)
Block screen capture	Allows to block screen capturing in application, which runs in the work profile to prevent from sharing data with that method.
Disable accounts modification	Blocks the possibility to add, edit or delete an account. <ul style="list-style-type: none"> • Block creation of the mail account (Samsung SDK only)
Block creation of the mail account	Available on Samsung devices

Disable camera	Block the possibility to use the camera.
Disable application control	Blocks following actions: uninstalling & disabling apps, clearing app cache & data, force stopping apps and clearing apps defaults

5.5.2 Enabled applications

In this section Admin can enable system applications in the work profile to be automatically accessible for users after profile activation. Enabled applications on the device may be different as some Android versions (especially branded versions) may not include all listed system applications. The admin can change the list of enabled applications and hide them according to needs. Default applications, which are always visible after profile activation are FAMOC Base Agent and managed Google Store.

5.6 Advanced

In the Advanced policy settings, you can configure following parameters.

Parameter	Value
Advanced policy settings	
Number of stored Device Monitor sessions	Sets how many sessions of Device Monitor should be stored by FAMOC (1-10) Default value: 5
Number of archived Device Monitor sessions	Sets how many sessions of Device Monitor should be archived in logs (10-150) Default value: 20
Data reported in Device Monitor session	Select which data will be reported by the usage monitor. Default value: All (Possible choices: Base params; Applications; Bluetooth; Disks; Access points; Certificates; Device administrators; Device accounts; Software updates; SIM cards)
Time synchronization interval	Sets how often the system clock on the S60 device is synchronized with a Network Time Protocol Server Default value: Disabled
SIM change notify (for example if device was stolen)	Yes/No Default value: No
Device limit per user	Number of devices that user can add via startup page when user authentication option is set. If the limit is exceeded, specified user is not allowed to add any other device to the system using startup page.
Organization name displayed on the device*	The entered name will be displayed on the screen as - Your device is managed by (company name)

6. Policies Status on Device Details Page

Policies status for device can be checked on main device details page or on “**Policies**” tab.

List of the policies shows:

- **Name** – name of the policy
- **Applied on** – date when the policy was applied on the device
- **Policy preview** – shows popup with current settings of the policy
- **Status** – shows status of the policy on device. When the mouse will be over the status icon, the list of missing policy items will be shown.
- **Action column** – if policy is not applied or outdated, there is a link to manually send configuration to device.

Assigned policy			
Policy name	Applied on	Policy preview	Status
Harvey Default	2019-10-30 10:48:37		

Figure 31 Assigned policy view