To maintain high security standards, it is sometimes necessary to implement very strict security policy. In COBO mode (Company Owned, Business Only) employees are limited to use their devices only for professional matters and have little (or even none) options of configuration. Though it may seem rather harsh, it keeps the risk of security breach to a minimum.

FAMOC gives you variety of options to protect your company device from potential hazards such as malware or phishing attempts. In this article we would like to give you some suggestions, how to define **Security options** in FAMOC policy for COBO mode. To begin, log in to FAMOC console and navigate to **ADVANCED > Settings > Policies** tab. Then **Edit** or **Add** new policy template and select **Security options** tab.

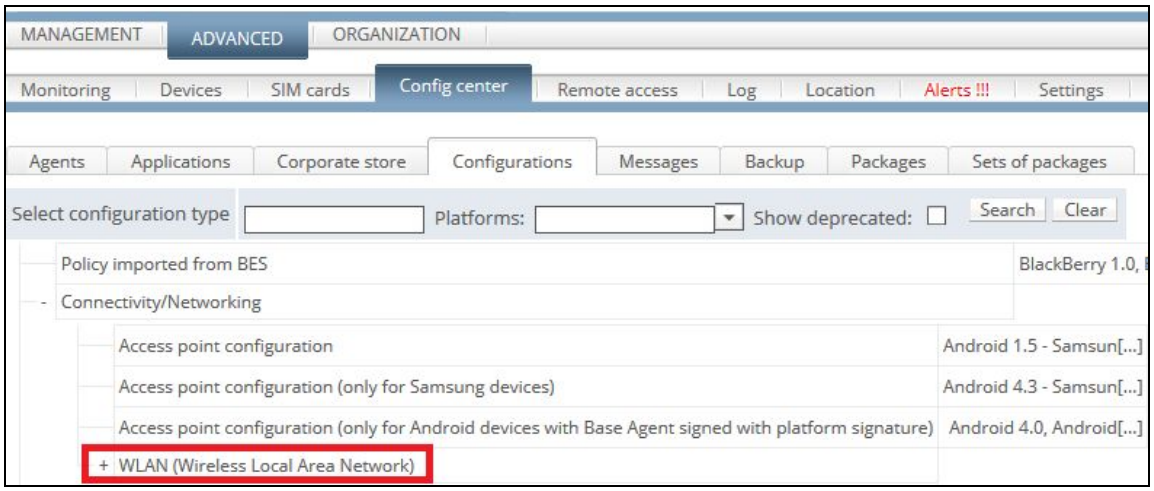
In COBO mode it is important to prevent user from re-configuring important settings or applications. We recommend following settings.

Wipe policy

Wipe on root detection: Rooting allows to bypass Android security and gain access to data that otherwise would be protected. Keeping sensitive data on rooted device is risky, so we suggest to select that option.

Network policy

Manual WiFi configuration lock: Blocks the possibility to manually configure WiFi connection. You can use **Configurations** to apply defined WiFi settings for e.g. office network.



Cellular data lock in roaming: Cellular data cost in roaming depends on the country you visit. Within the EU it should not be a problem, but in other countries it may generate bigger costs. You might consider blocking cellular data in roaming to avoid that problem.

WiFi tethering lock / USB tethering lock: This option blocks the possibility to use the phone as router or USB modem. It is highly recommended to use private APN (Access Point Name) for secure corporate network connection. That way, only authorized devices have access to your company's infrastructure. Creating mobile hotspot might pose some risk of hacking the network, especially when default settings are used.

Hardware policy

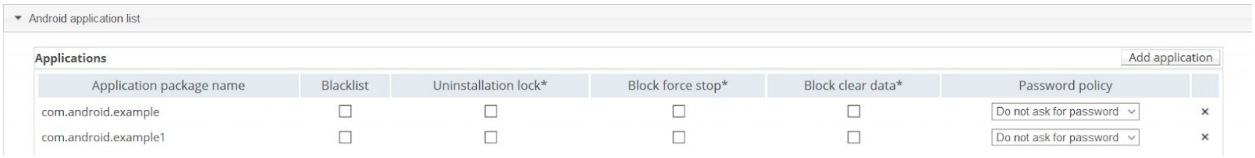
OTA update lock: This option blocks system updates for 30 days. It can give some time to ensure compatibility of your apps with new system version.
Factory reset lock: You don't want to have your precisely prepared configuration erased with one click. To ensure that the device works according to your policy, you can block possibility to restore factory settings.
Development mode lock: In development mode users have access to some low level functions for example fake GPS location. To keep control over the device, we suggest turning this feature on.
Unknown sources lock: In COBO mode users should have installed on the device only approved apps. Installation of .apk files from unknown sources can be dangerous and shouldn't be allowed.
Storage card lock: Enforcing all those security measures would be pointless if users could transfer files to external memory and open on other device. With plenty of possibilities to store your data in cloud you might consider to block usage of storage card slot.
USB file manager lock: This option blocks another way of data leak - for example, in case of using public charging slots. When it's turned on, transfer of data over USB cable will be blocked.
Block safe mode: Safe mode can be sometimes necessary to troubleshoot the device. However, in COBO mode you want only authorized personnel to deal with any errors or bugs. This is why we advise to block safe mode and leave troubleshooting for IT department.

Applications restrictions

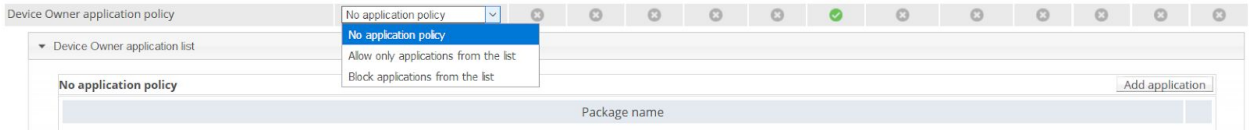
Force Google Play Protect: Google Play Protect is an answer to many threats that comes with malware and other suspicious apps. It scans your device every day in search for any dangerous software and helps to browse the Internet safely. This option activates protection on the device and prevents disabling it.
Disable application control: It prevents users from modifying apps permissions, clearing data or cache.
Disable accounts modification: Users will be able to use only predefined account on the device. Using another accounts will be forbidden.

Applications policy

In this tab you can set restrictions for specific apps. In the **Android application policy** section you can add apps and choose to **Blacklist** them, prevent **uninstalling**, **stopping** or **clearing data**. It is up to you to decide this part of policy. If some apps are necessary you should add them to the list and select **Uninstallation lock**, so user won't be able to remove it, even by mistake. On the other hand, if there is an app that should definetely be avoided you might consider adding it to **Blacklist**.



In the next section - **Device Owner application policy** you can create list of apps for Device Owner mode and select from the drop-down menu to Block them or decide that only apps from the list can be installed on a device.



Last section include permissions for apps. **Device Owner application permissions** tab allows you to configure predefined sets of permissions for apps so user will not be able to change it. If you wish, you can for example block some app access to location info, camera, calendar etc.

When you have all the above settings configured, you can save the policy and implement them on a device. They should be now secured and ready to work in COBO mode.