COPE mode combines some elements of BYOD and COBO mode. Device is fully managed by the company but personal use is accepted by permitting private Google accounts on a device. Corporate part is stored in a separate Work Profile container. Your organisation can, however, enforce policies across both - private and business parts of the device.

For COPE mode two policies templates will be necessary to prepare. Configuration of Work Profile policy might be similar to BYOD model, with little exceptions of course. Security policy will have to be adopted to ensure control over the device. It is also very important to inform employees about the rules of using the device for personal matters e.g. cases in which device might be remotely wiped.

Security policies settings

An example of case mentioned above might be rooting the device. Rooted devices are more vulnerable so we highly suggest selecting ***Wipe on root detection*** option. Make sure that users know that the device might be completely wiped if rooting is detected.

Network policy shouldn't be as strict as in COBO mode. Employees will probably use their home Wi-Fi so you should let them configure WiFi connection manually. You might, however, consider blocking data transfer in roaming (***Cellular data lock in roaming***) to avoid generating additional cost for a company. For the same reason you might block ***WiFi*** and ***USB tethering***.

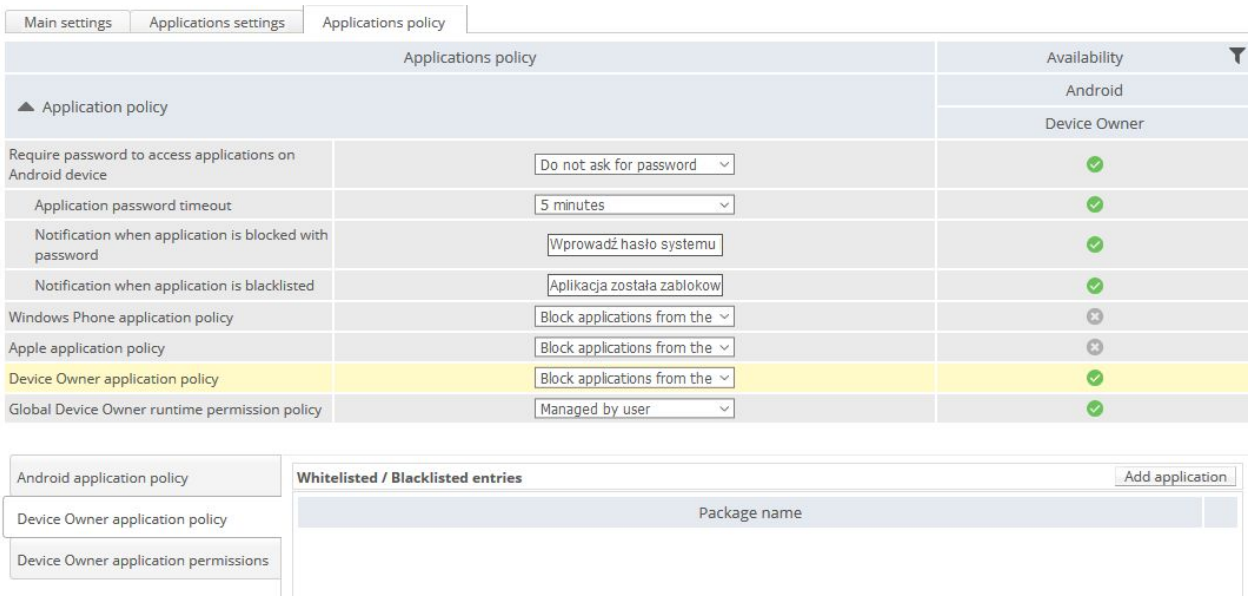
In the **Hardware policy** section note all the options that can pose some risks of security breach. You should definitely select ***Factory reset lock*** so users will not be able to wipe the device manually. Separate Work Profile part on the device is essential so ***Disable manual work Profile removal*** have to be selected.

We also suggest to select ***Development mode lock*** and ***Block safe mode***. In this modes users have access to some functions that should be left only for your IT staff.

Applications

Google Play Protect is a very useful tool that scans the device for any malware. Because users will install various applications on devices, this option should be enabled to prevent the risk of any damage caused by suspicious applications and sites. Therefore, we recommend selecting ***Force Google Play Protect*** in the **Application restrictions** section.

Another option that allows more control over applications can be a blacklist. In the **Applications policy** > **Device Owner application policy** tab you can add unwanted apps to the list and from the menu above select **Block applications from the list**.



Android Work Profile

In COPE mode it is important to keep corporate and personal part separate, however the policy might be not that strict, since both parts are controlled by company. These settings are recommended:

Disable account modification - within Work Profile only corporate account should be allowed. Private account should be kept outside to avoid, for example, using wrong mailboxes.

Disable cross profile copy-paste - user will not be able to transfer any information outside Work Profile using copy-paste method.

Disable application control - user will not be able to uninstall, disable or modify app data.

Runtime permission policy: Deny - user will not be able to change applications permissions.

In the **Policy components** section select apps that should be installed in Work Profile container.

You should definitely add **Work Profile lock code**, in the same manner as in BYOD mode. The process is described here under *Setting up security code*.

Once the policy is set up, click Save to finish configuration.

Now both policies can be implemented on devices. Administrator will have full control over the device, but the user will be able to customize private part according to his needs. Work Profile will be separate and safe and corporate data will be protected.

This configuration is, of course, only our suggestion but it should give you some perspective how COPE model should work.