Release Bulletin

IKARUS mobile.management – Server

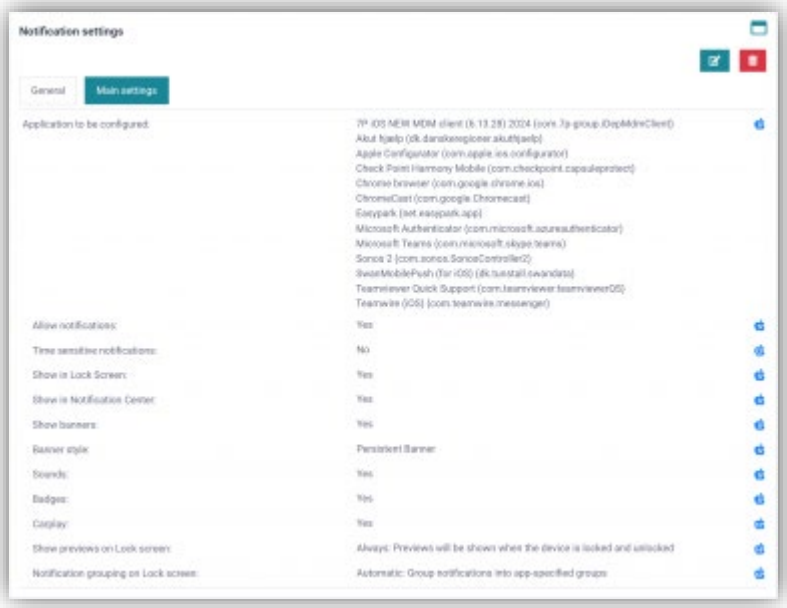
Version	6.16.xx
Release date	14.01.2025

Single Sign On (SSO) with 7P EMM

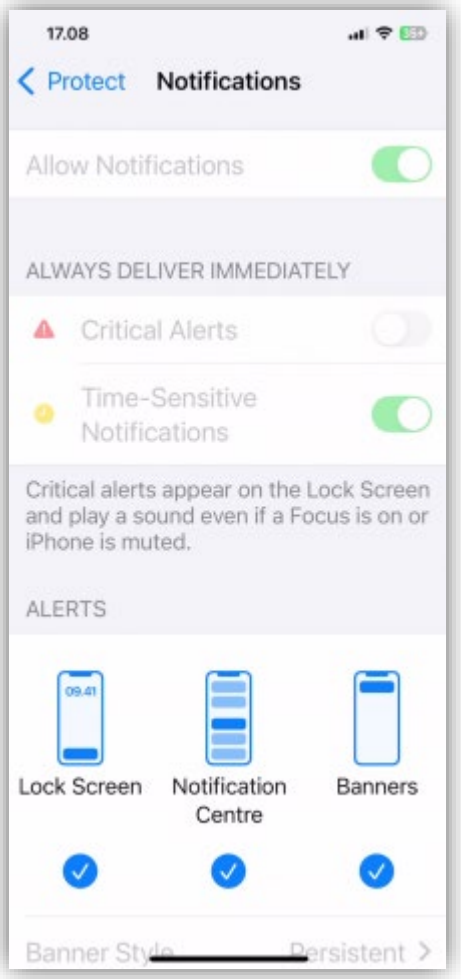
For a detailed guide on how to set up Single Sign On with our EMM solution, please refer to HowTo – Single Sign On (SSO) with 7P EMM.

iOS - New configuration "Notification settings"

With the release of 6.16.05 we now have a new configuration type named “Notification settings” which is to be used for Supervised iOS devices.
Depending on the OS version of the Supervised iOS device there are more or less compatible settings.
The purpose of this notifications settings is to select one or multiple iOS apps, where you then preset how notifications should behave on these apps when notifications arrive to the device to these apps.
When applied these settings are greyed out for the user and cannot be modified by the user.
Example of a Notification settings configuration:



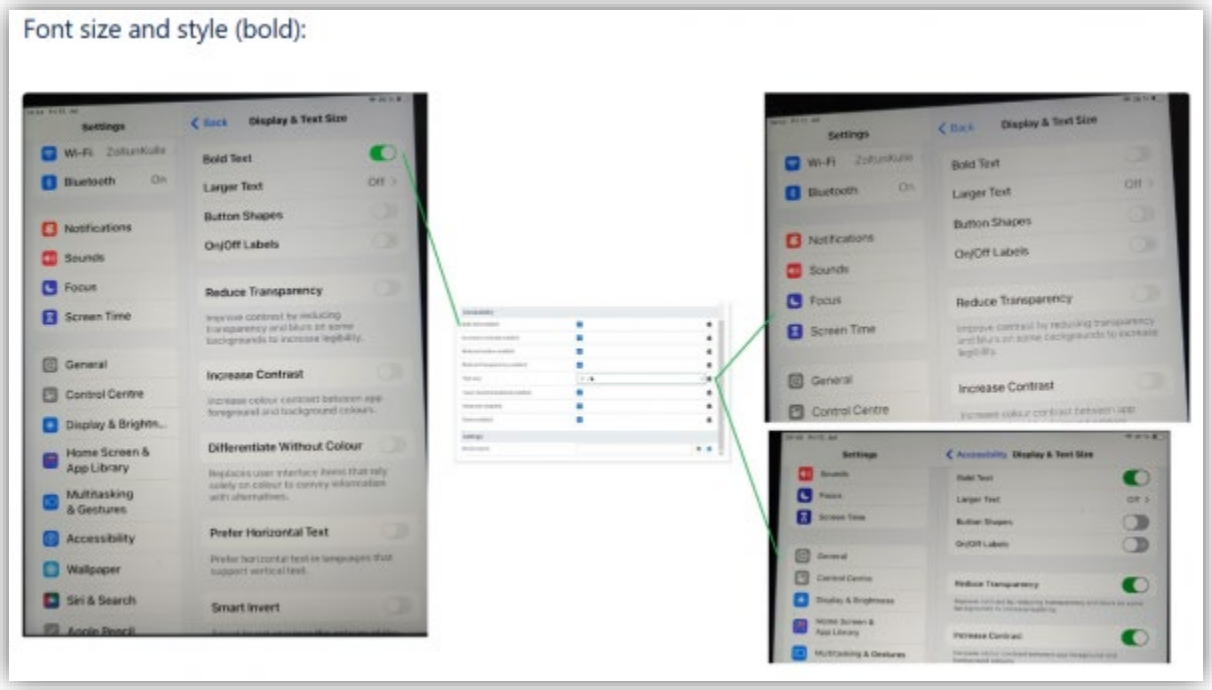
Example of an iOS device when this is applied to a selected app:

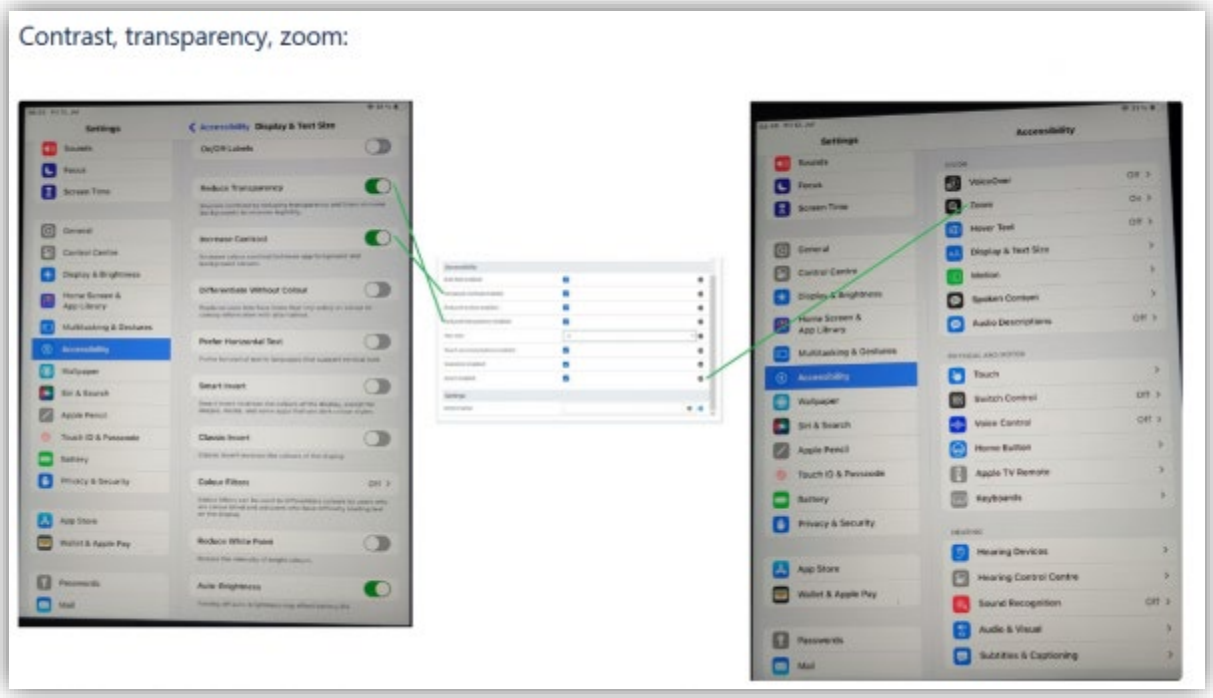


Note: Only one configuration of this type can be used at a time on a device. If a configuration is already applied and you want to apply a new or update the existing.
Then the old must be removed first before the new can become applied.

iOS - Accessibility settings in "Apple device configuration"

With this new configuration options you can pre-define settings with the iOS device of Settings -> Accessibility, with the purpose to easy the usage of the iOS user experience.
Like Increase text size or bold text and many other settings. When this config is applied to a device, this changes the Accessibility settings immediately.



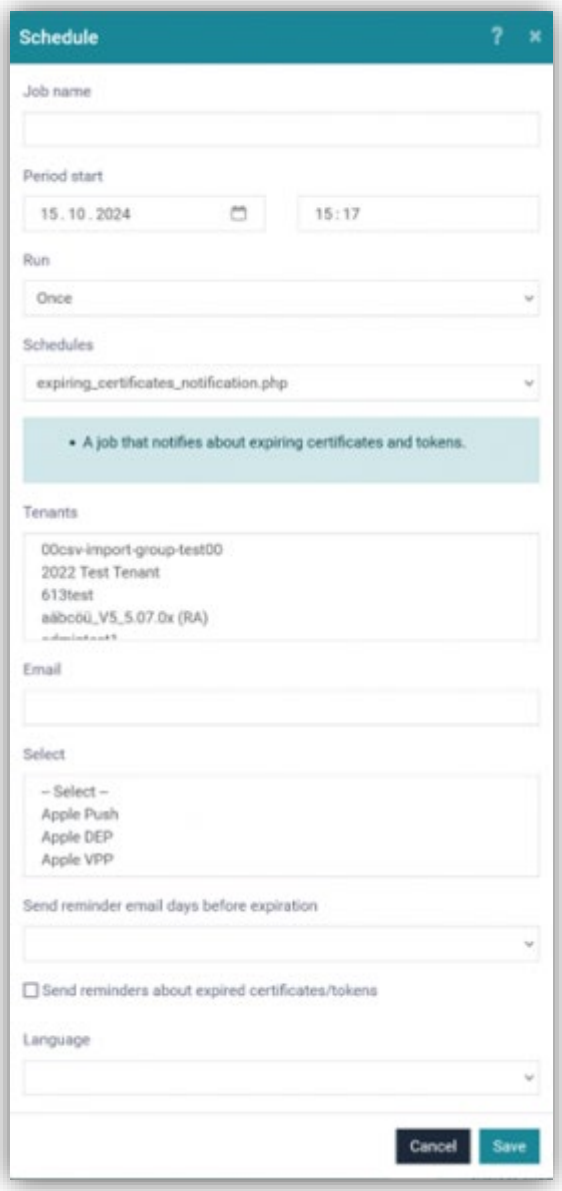


When you try to remove the config, the settings remain in the state of when the config was applied and will not return to default.

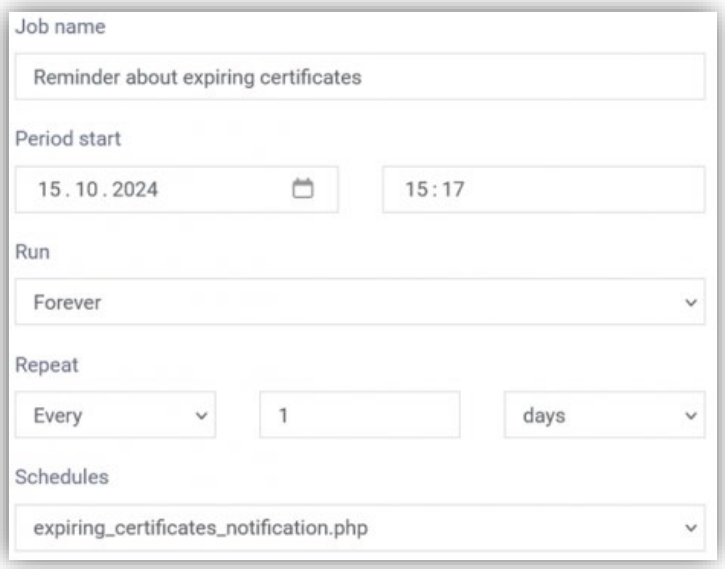
Certificate Expiration Notification

The EMM Server can now send an email notification for certificates or certain tokens that are about to expire. This can be especially useful for Apple Push and DEP and VPP tokens.
[Global] -> Operations -> Scheduler

Click on the “+” to add a new schedule and select “expiring_certificates_notification.php” from the drop-down menu “Schedules”.



Job name: Provide a name for the schedule, e.g. “Reminder about expiring certificates”.
Period start: Select the start of the scheduler run period.
Run: configure how often the schedule should run. We recommend to set it up to run once per day:



Tenants: select the tenants that that should be checked for expired certificates/tokens.

Note: Multi-select is possible with CRTL or SHIFT keys.

Email: enter the email address where the reminder should be sent to. Multiple addresses can be set using comma as a separator.
Select: Select the certificates/tokens you would like to receive a reminder:

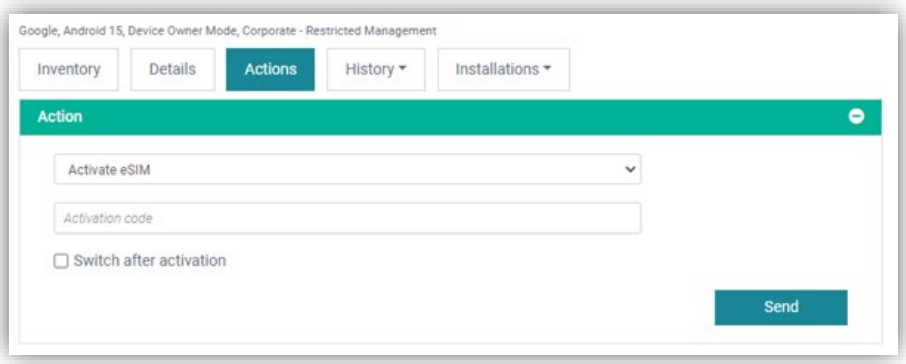
- Apple Push: a reminder for the Apple Push token
- Apple DEP: a reminder for the Apple DEP token
- Apple VPP: a reminder for the Apple VPP token
- Other certificates/tokens: a reminder for trust or identity certificates that have been uploaded to infrastructure -> certificates

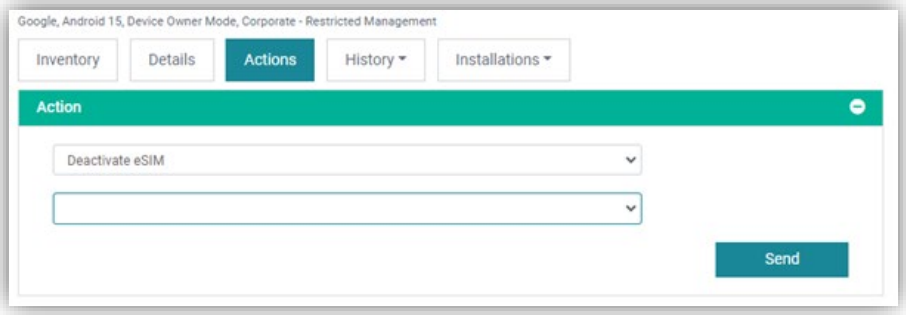
Note: Multi-select is possible with CRTL or SHIFT keys.
Send reminder email days before expiration: select the notification period. Example: „30 days before“ would send the notification email 30 days bevor a certificate/token expires.
Send reminders about expired certificates/tokens: by default, if selected, the email will also be sent if there are certificates/tokens that have already expired.
Language: Select the language for the email.

New eSIM options

1 Android eSIM actions

In 6.16 we now have the capability to activate eSIM on Android devices directly through the MDM platform. This new feature simplifies device provisioning and enhances the flexibility for managing mobile connectivity.
Administrators can now remotely activate and deactivate eSIM profiles on supported Android devices:



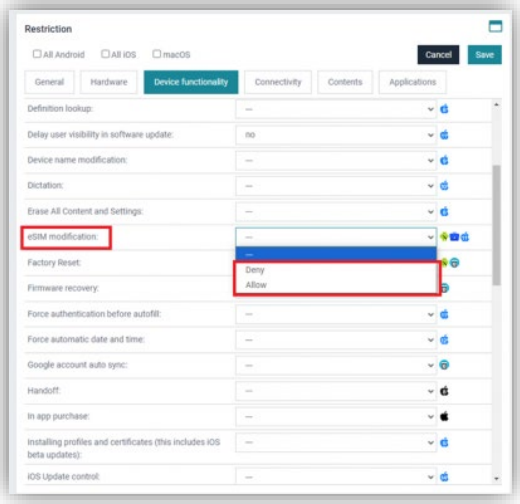


Prerequisites:

- A device running Android 15 Beta 2 or later and supports eSIM
- Valid eSIM activation code (Example: LPA:1$RSP-0003.OBERTHUR.NET$5XEHC-3W9E4-XIQ4F-EEBAR)
- MDM client 6.16.XX or higher

2 eSIM restriction

Administrators can now restrict users from adding, removing, or altering eSIM profiles on enrolled Android devices.



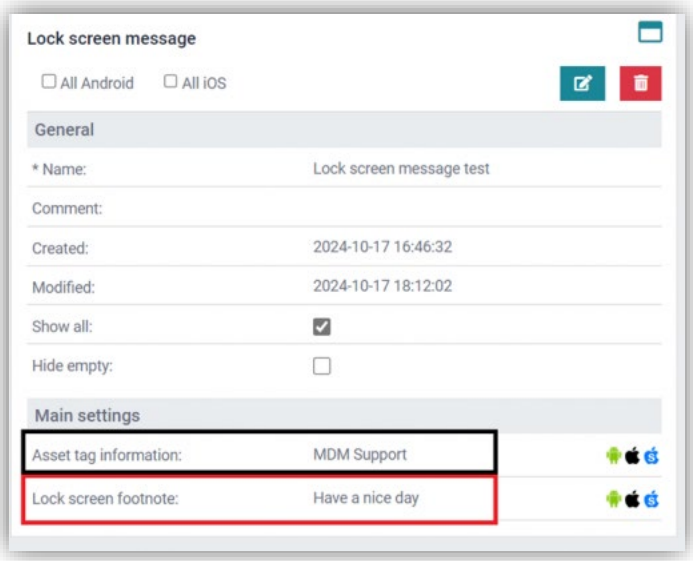
This new feature adds an extra layer of control, preventing unauthorized changes to eSIM settings and profiles, thus ensuring device security and compliance with organizational policies.

Android lock screen message configuration

It is now also possible to change the messages in the lock screen on Android devices.

The display name of the organization can be used --> Asset tag information (black)

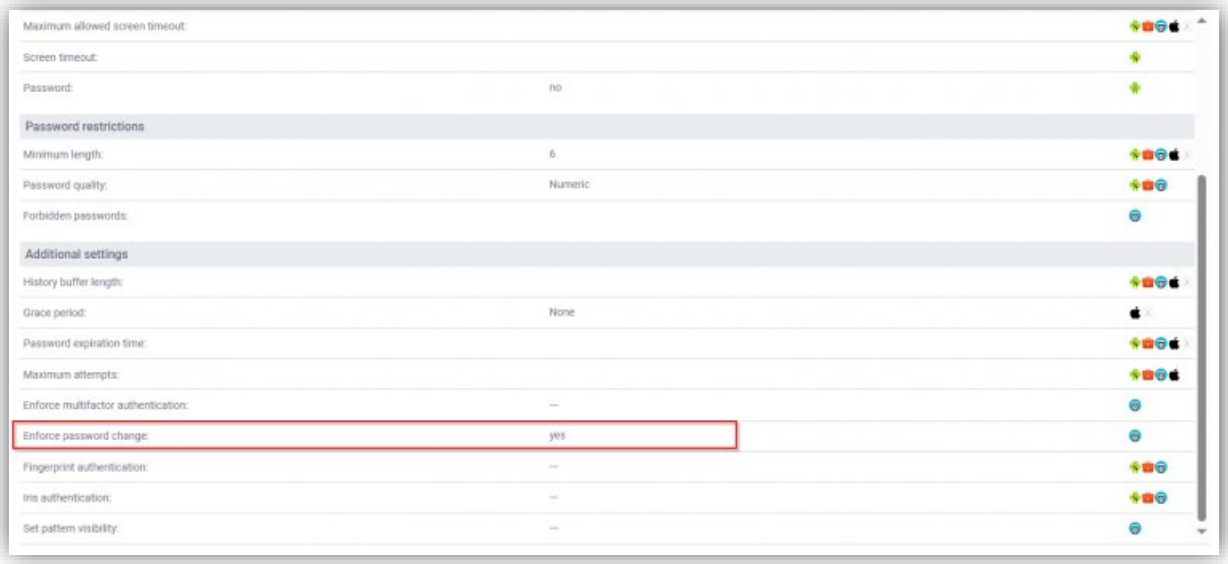
And the footnote can be changed (red)



It is also possible to use different parameters such as user ID or device name.

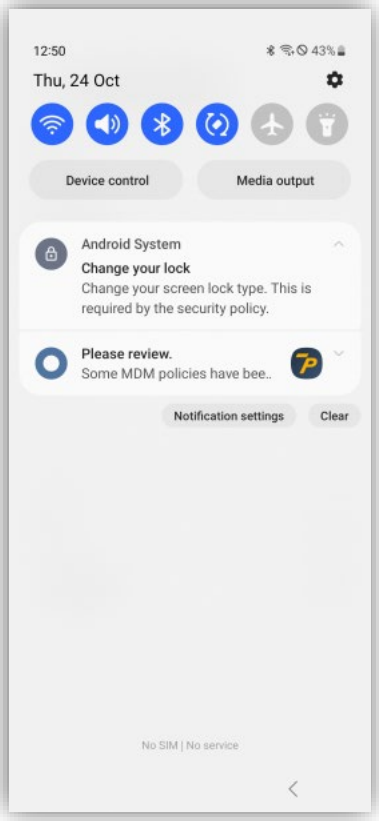
Samsung - Enforce password change option

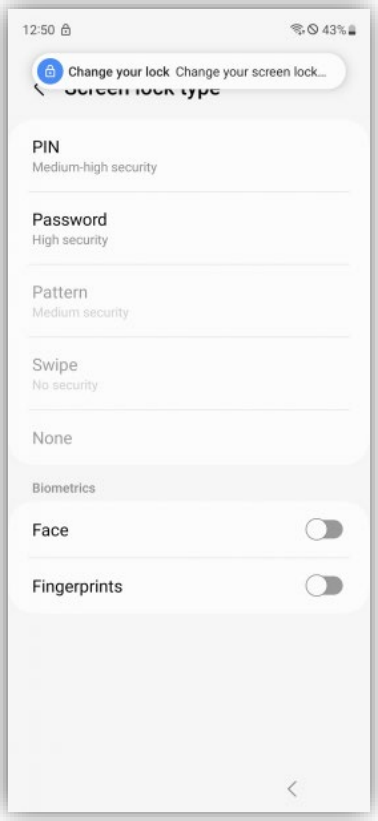
There is a new option in the Autolock configuration type called "Enforce password change":



If a configuration is sent to a device with this option set to "yes", the device will prompt the user to set their password in accordance to the password policies defined in the Autolock configuration.

On the device a message will be shown and the lock type settings will be opened and cannot be closed:



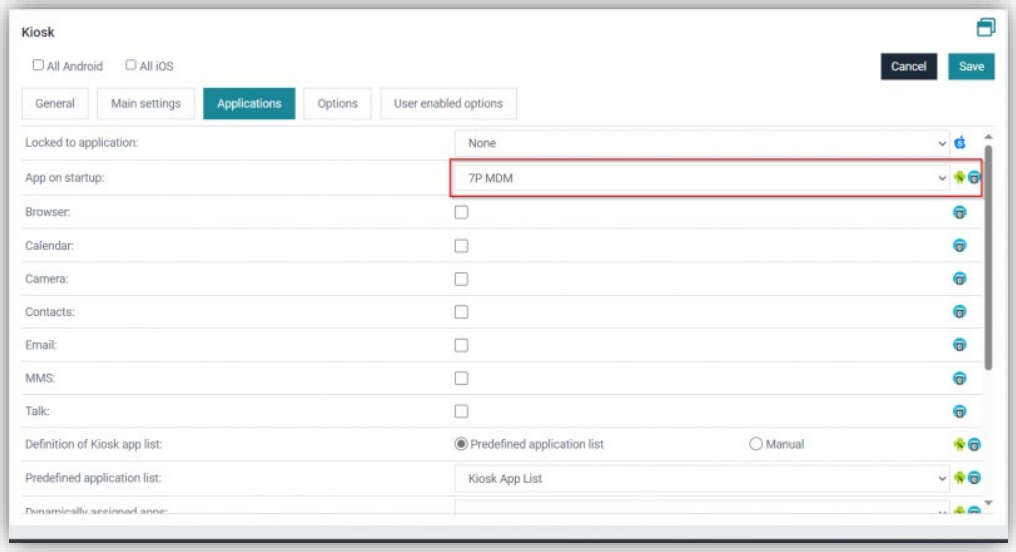


Note: It is important to keep in mind that this will prevent the user from utilizing other functions and apps until the lock code is set.

Therefore, applying the Autolock configuration automatically via an Operation should be done with caution to prevent locking you or the user out at an inconvenient time.

Start app in Kiosk mode

There is a new option in the Kiosk configuration type called "App on startup":



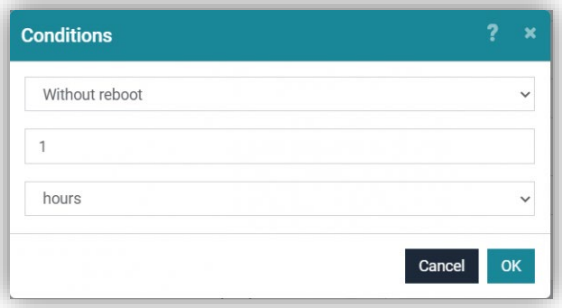
The app will be started when

- the Kiosk configuration is applied to the device.
- the device is rebooted.
- the device is turned on after being previously turned off.

This feature requires Kiosk client version 6.16 or newer in order to work.

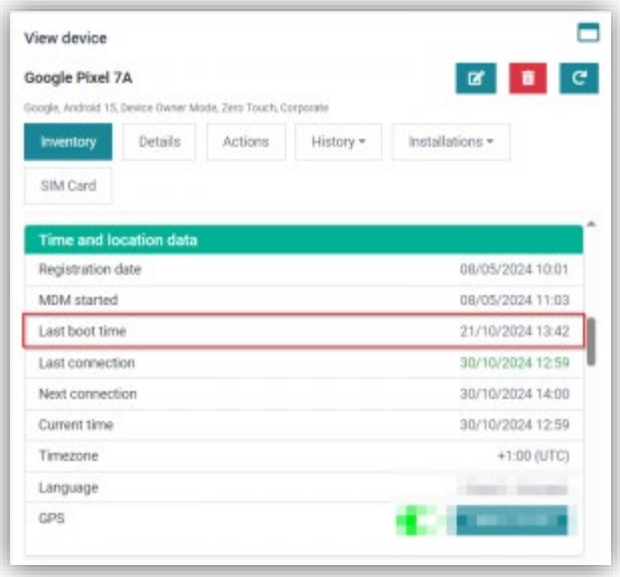
Android - New condition "Without reboot"

In Operations a new condition called "Without reboot" was added to the Device specific section:

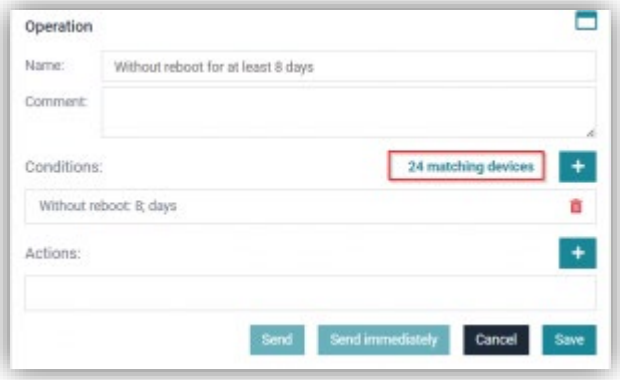


This condition can check for devices that haven't been rebooted for at least the entered amount of days or hours.

The relevant time stamp for the last reboot time of a device can be found in the device's inventory in Organization -> Users and devices:

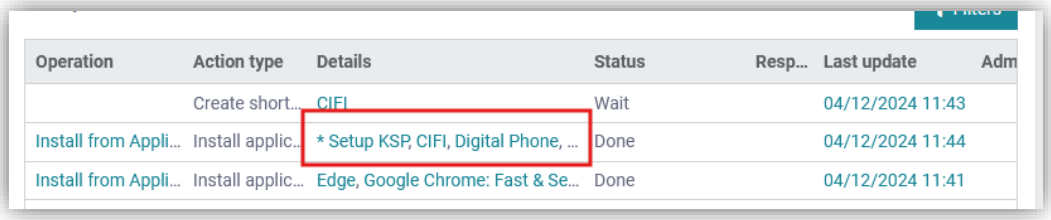


As the time of writing this article (30.10.24, 13:33) the device "Google Pixel 7A" was not rebooted for eight days. Therefore, if an operation with "Without reboot" condition aimed at devices that haven't been rebooted for at least eight days is created, the device will be included:



Android - additional Details on the History-> Actions Tab

In the 6.16 Release we implemented the possibility for most actions that apply multiple of items to devices to also store and show the list of those items in the action history. This means if you use an operation that installs mandatory apps from an applist, you can now easily see which App triggered the operation to run. This shows up to five apps at the moment.



When using a blacklist to uninstall/disable apps via an operation you can click on "Done" in the status to see details on which apps triggered the operation and were uninstalled/disabled.