

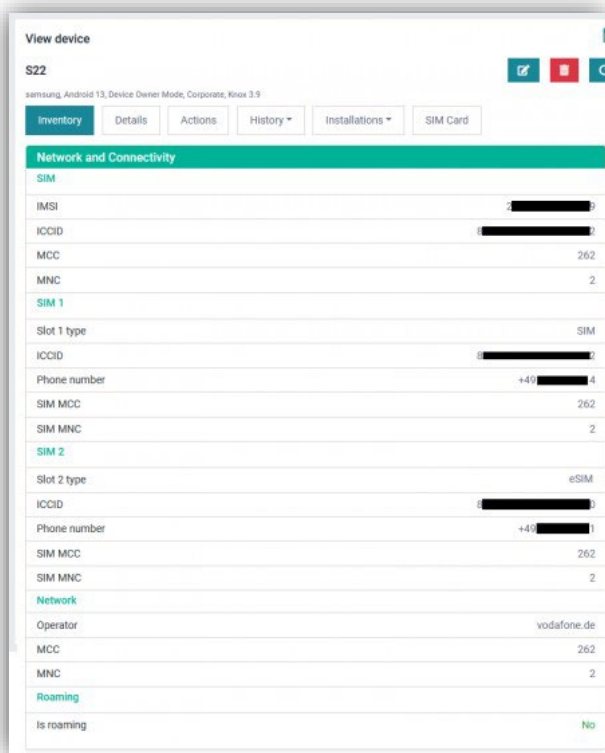
Release Bulletin

IKARUS mobile.management – Server

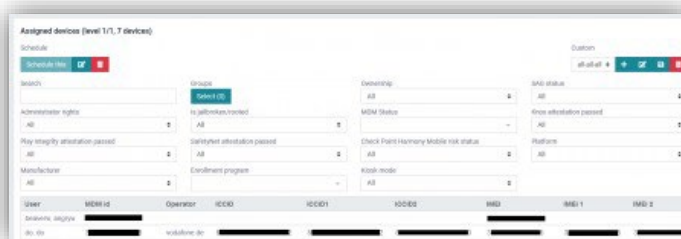
Version 6.12.xx
Release date 28.11.2023

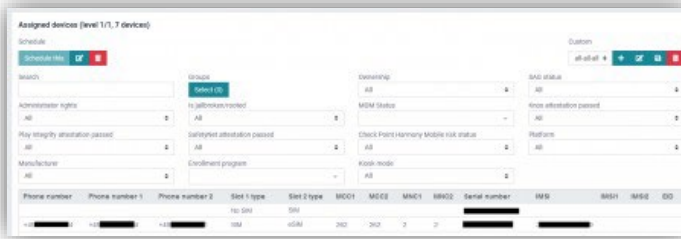
Dual SIM support

Dual SIM support has been added. Information of each SIM and eSIM is shown separately.



In Organization > Users and devices > Network and Connectivity data of each SIM card and eSIM is listed separately.



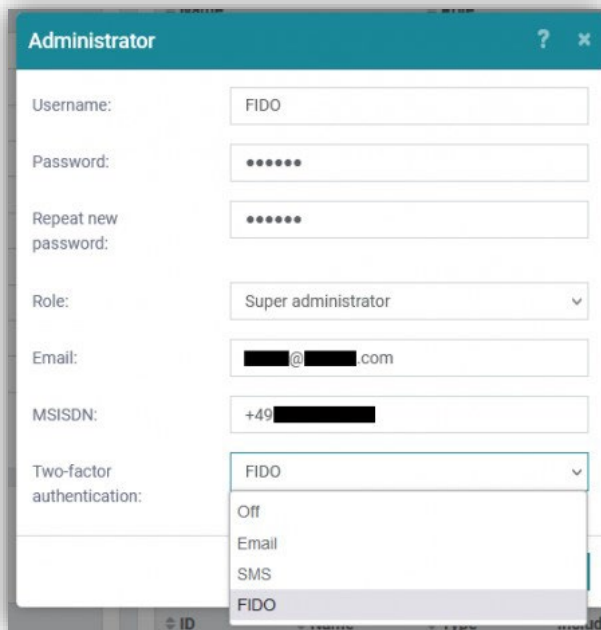


In Reports the values of each SIM card has its own number (e.g. IMEI1, IMEI2, ...). The value without a number (e.g. IMEI) is the one of the currently active SIM / eSIM.

On iOS devices it is now possible to disable the Activation Lock remotely via the MDM or directly on device by entering the username and password or by entering the bypass code.

FIDO2 support

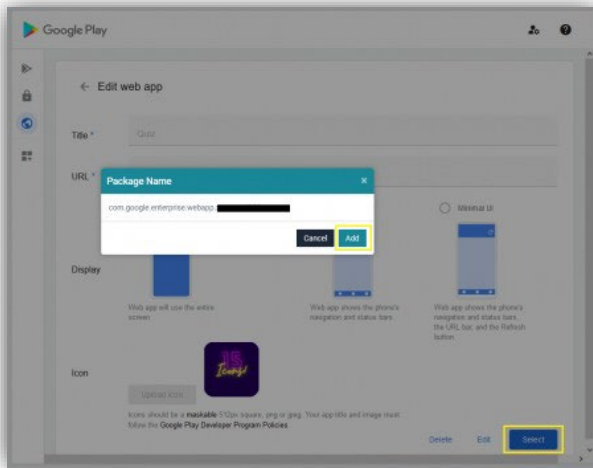
Two-factor-authentication via FIDO2 have been added. A login can be done via e.g. an USB dongle / token.



When adding a new administrator account, now "FIDO" can be selected from "Two-factor-authentication" drop-down menu.

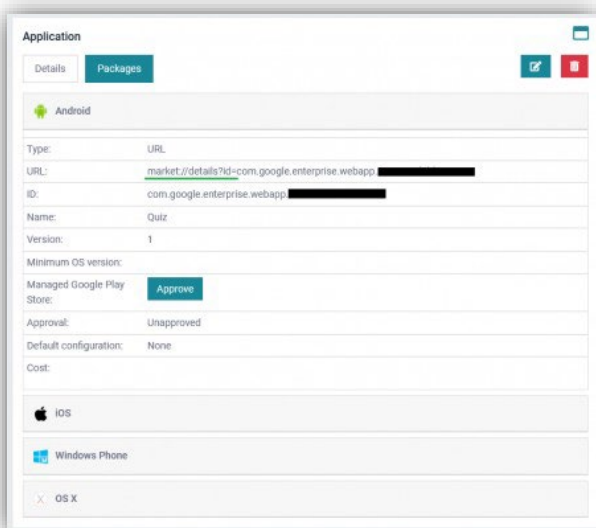
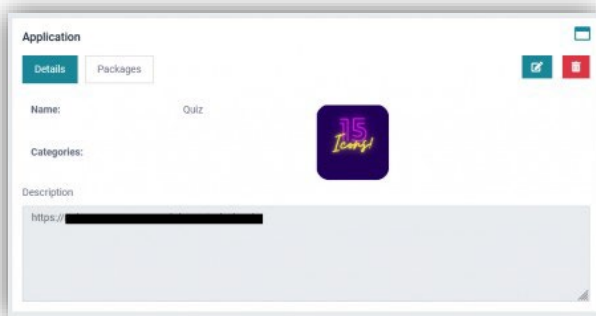
Adding WebApps with one click

WebApps can be added with on click now.



Select a WebApp from Infrastructure > Managed Google Play and click on the "Select" button. The pop-up "Package Name" will appear.

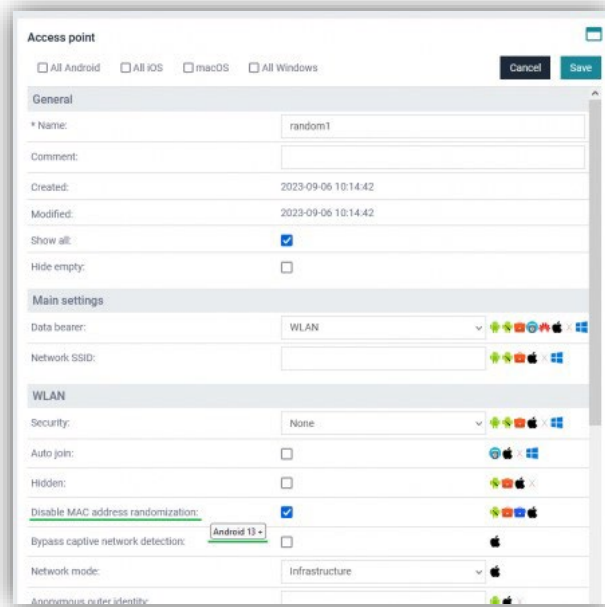
Now click on the "Add" button.



The WebApp has been added automatically to Applications.

Disabling MAC address randomization for Android

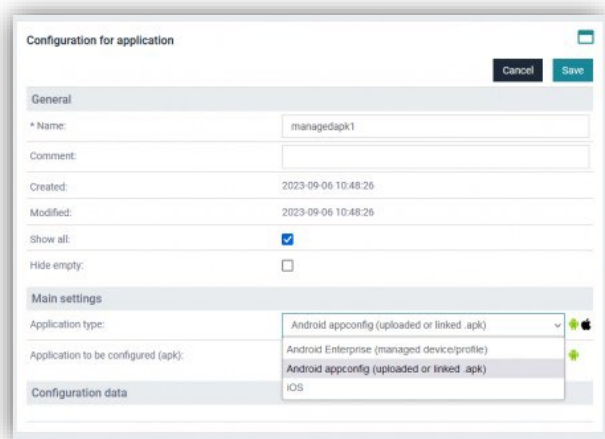
Disabling randomized WiFi MAC address via an Access Point configuration is now possible for Android devices with Android 13 or higher.



If the option is enabled, the hardware MAC address will be used instead of a random generated one.

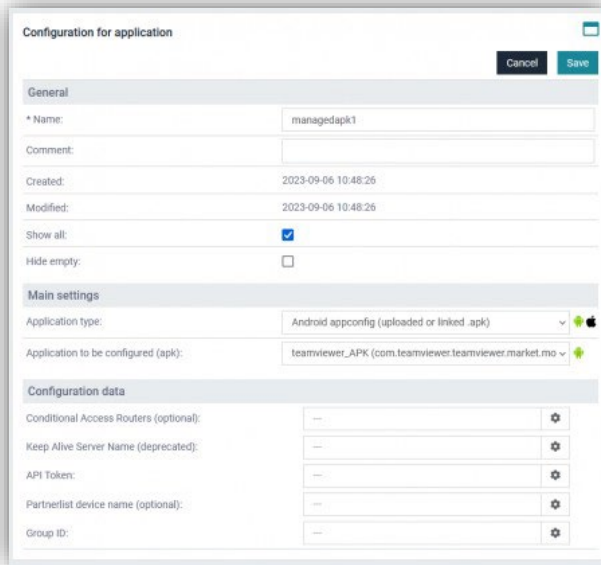
Support managed configuration for APK files

Now a managed configuration can be added to an APK file that supports managed configuration.



First, you need to add an APK file or the URL to the APK of an application that supports managed configuration to Applications.

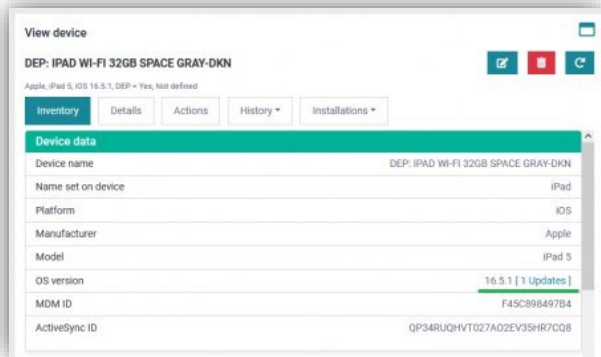
Then add a "Configuration for application" and select "Android appconfig (uploaded or linked .apk)" for "Application type".



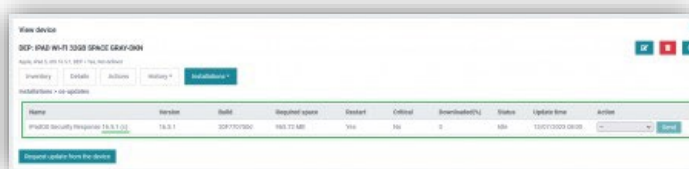
Select the uploaded or linked apk from the drop-down menu "Application to be configured (.apk)". New fields for these values that can be added will appear under "Configuration data".

Rapid Security Responses for Apple devices

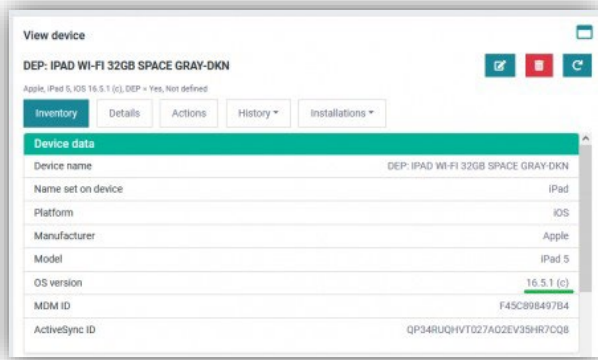
Available Rapid Security Responses for Apple devices are shown.



If a software or a Rapid Security Responses update is available for an Apple device, a notification will appear in brackets next to the OS version number.



A click on that notification will show details about the available update. A letter in brackets in the version number indicates that the available update is a Rapid Security Responses.



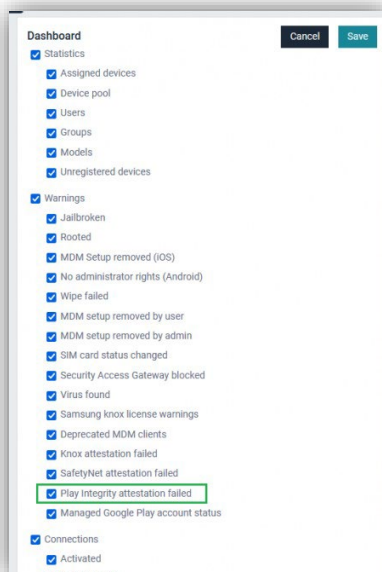
After the update, the new version number with the letter in brackets is shown.

Play Integrity API Support (replacing SafetyNet)

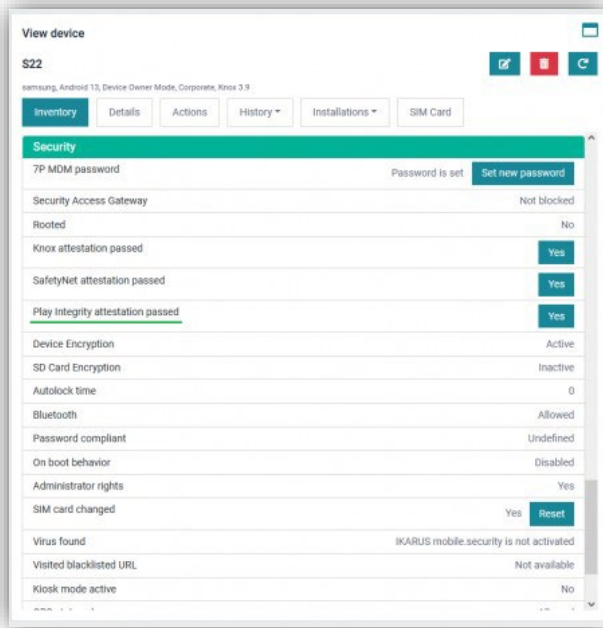
Google Play Integrity API support has been implemented.

Warnings	
Jailbroken	0
Rooted	0
MDM Setup removed (iOS & Win)	6
No administrator rights (Android)	0
Wipe failed	0
MDM setup removed by user	5
MDM setup removed by admin	1
SIM card changed	2
Security Access Gateway blocked	2
Virus found	0
Samsung Knox	2
Deprecated MDM clients (<6.10.00)	32
Knox attestation failed	0
SafetyNet attestation failed	0
<u>Play Integrity attestation failed</u>	4
Managed Google Play account status	1

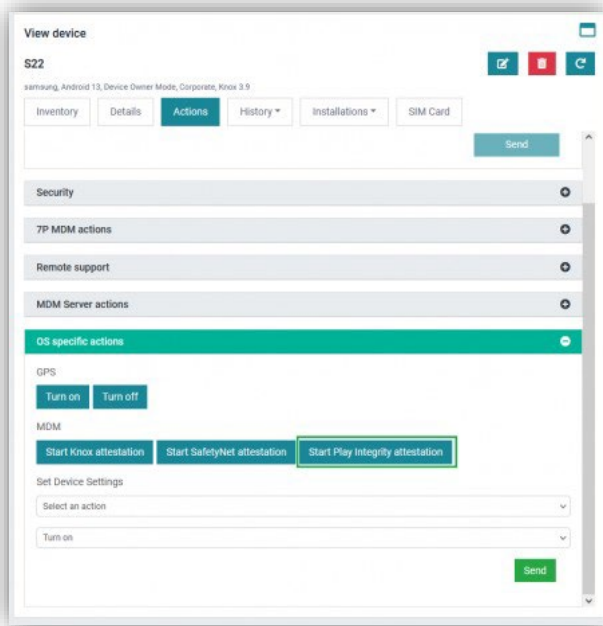
Dashboard: Failed Play Integrity attestation is shown in Dashboard > Warnings.



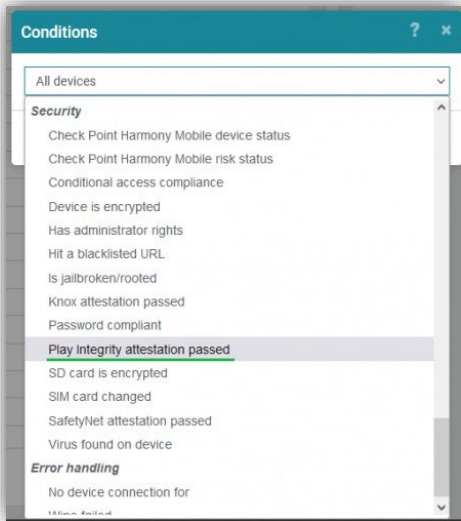
Settings: Displaying this warning can be enabled or disabled in Settings > System > Dashboard.



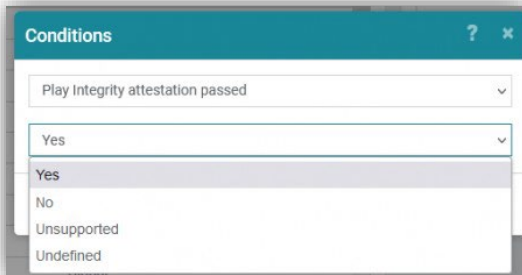
Device inventory: The status of the Play Integrity attestation is also displayed in the Security tab in Organization > Users and devices > Inventory > Security.



The attestation can be started manually in Organization > Users and devices > Actions > OS specific actions.

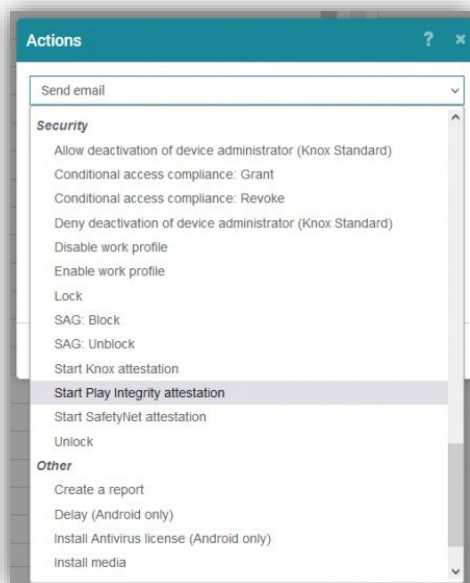


Operations: A condition has been added to filter out devices with different Play Integrity status.



Play Integrity attestation status can be:

- Yes (attestation passed)
- No (Play Integrity attestation failed)
- Unsupported (Play Integrity attestation not supported)
- Undefined (Play Integrity attestation support unknown)



The action "Start Play Integrity attestation" has been added.

In this operation the Play Integrity attestation will be started on all devices where it failed.

User	Device name	Model	Knox attestation passed	Play Integrity attestation passed	SafetyNet attestation passed
beachone_angryw	ax02a	TC57	Undefined	Undefined	Unsupported
do, do	plm7fa	Pixel 7a	Undefined	Yes	Yes
do, do	S22	SM-S901B	Yes	Yes	Yes
do, do	Pixel6a	Pixel 6a	Undefined	No	Yes
wp, wp	S7	SM-G930F	Unsupported	Unsupported	Unsupported
wpcv_wpcvo	NB1apco	Nokia 8.1	Undefined	No	Yes
wpcv_wpcvo	S10	SM-G970F	Yes	Yes	Yes
wpcv_wpcvo	TabA	SM-T290	Undefined	No	Yes

Reports: A column that shows the Play Integrity attestation has been added.

Android managed system updates improved

The restriction "System update policy" has been improved.

These are the improved options of the restriction "System update policy":
Install windowed: The fields "Start time" and "End time" have been added.

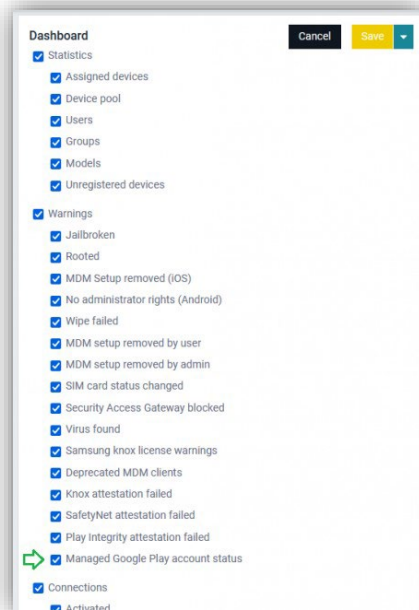
No policy: Removes the policy and enables manual system updates again.

Google Play Errors in Dashboard

Managed Google Play errors are now displayed in Dashboard for a quick overview.

Warnings	
Jailbroken	0
Rooted	0
MDM Setup removed (iOS & Win)	6
No administrator rights (Android)	0
Wipe failed	0
MDM setup removed by user	5
MDM setup removed by admin	1
SIM card changed	2
Security Access Gateway blocked	2
Virus found	0
Samsung Knox	2
Deprecated MDM clients (<6.10.00)	32
Knox attestation failed	0
SafetyNet attestation failed	0
Play Integrity attestation failed	4
<u>Managed Google Play account status</u>	1

The amount of Android devices that have Managed Google Play errors is displayed here.



If the line is not visible in Dashboard, it needs to be enabled in Settings.

User	Device	MDM ID	MDM IDSN	Platform	Model	MDM Version	Manufacturer
lastname, firstnames	frankem	Samsung A6 (Gionee Test)		Android	SM-A600FN	6.05.02	samsung

MDM Setup removed by user	5	Knox	24
MDM Setup removed by admin	1	Zero Touch	21
SIM card changed	2	QIP	15
Security Access Gateway blocked	2	Android enterprise	67
Virus found	0	Device pool	8
Samsung Knox	2	Running in Knox mode	4
Deprecated MDM clients (<6.10.00)	32	Devices in Lost mode	1
Knox attestation failed	0		
SafetyNet attestation failed	0		
Play Integrity attestation failed	4		
Managed Google Play account status	1		

A click on the number will show a list of affected devices.

Setup data	
MDM Status	Overdue
7P MDM	6.05.02
Android Enterprise status	Managed device
AE account support	Status: Failure Info: EXCEPTION_ADDING_ACCOUNT
AE working environment	success
Extended MDM support	SAFE4: LicenseAccepted
Knox API version	3.5
Push configuration	FCM (OK)
Auto update policy	Not available

In Device Inventory > Setup data status of the AE account is also shown.

Android enterprise (level 1/1, 1 devices)			
User	Device name	Model	Managed Google Play account status
lastemil.firstemil	Samsung A6 Simon Test	SM-A600FN	Status: Failure. Info: EXCEPTION_ADDING_ACCOUNT

In Reports there is a column that also shows the status.

Connecting company and private apps

Data sharing between company calendar and private calendar is now possible with the restriction "Connected work & personal calendar".

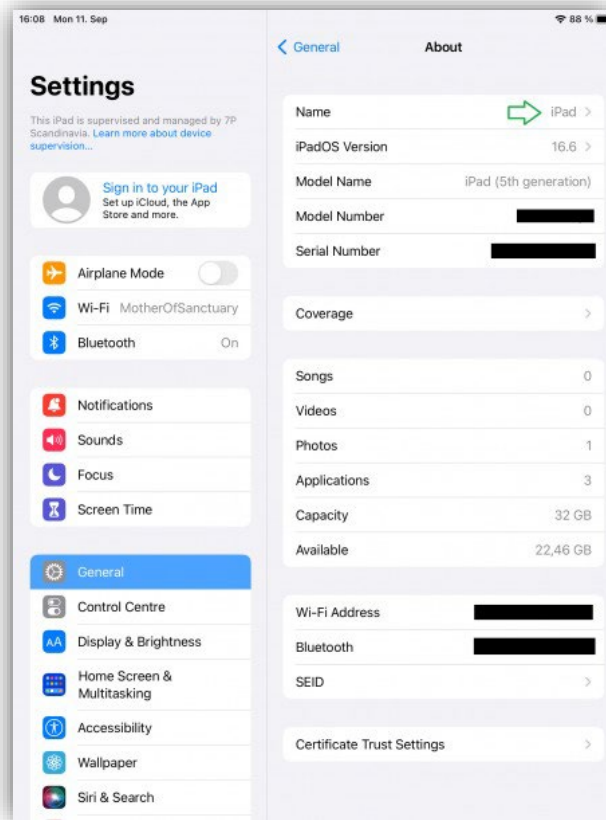
Data sharing between company apps and private apps is also possible with the restriction "Connected work & personal apps".

Restriction	
Classroom	Connected work & personal apps
Allow teacher to lock apps or device without prompting the student:	Allow
Allow to observe student's screen without prompting:	WhitelistGroup
Force automatic join to classes:	Allow
Force permission request to leave the class:	
Enterprise app trust modification:	

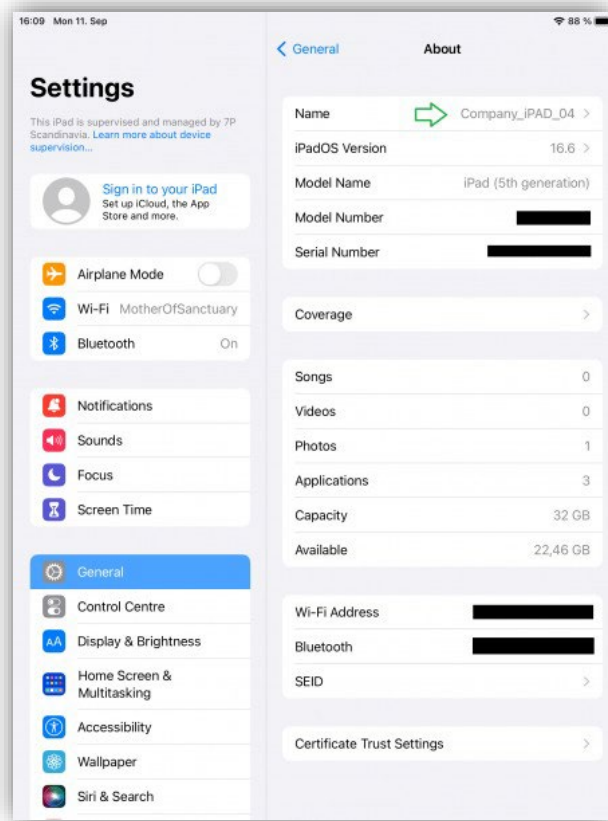
Minimum Android version is 13.

Set iOS device name

An option to change the name of the device for supervised iOS devices has been added to the Apple device configuration. Instead of entering a name manually, a custom parameter can be selected as the device name.

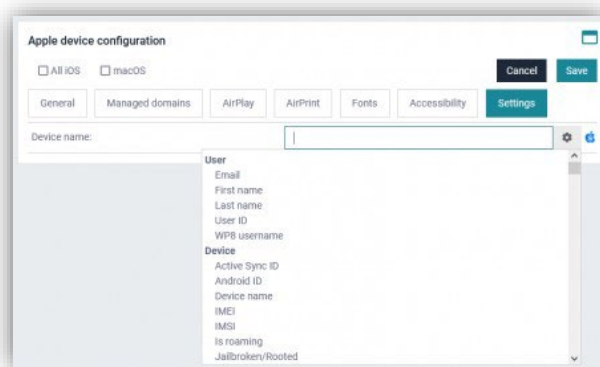


The name of supervised Apple devices can be changed via the "Apple device configuration".



Via the "Apple device configuration", a supervised Apple device will be renamed to the value entered in the configuration.

After entering a value in Settings > Device name and applying the configuration to the device, the name is changed to the new value.

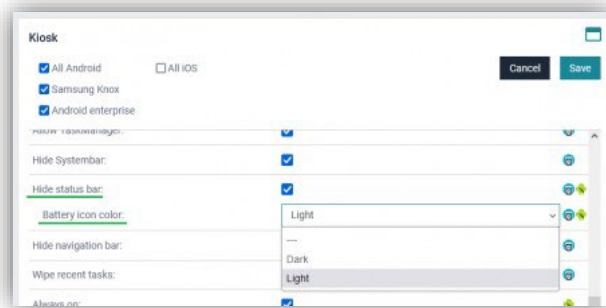


To add a custom parameter as device name, click on the gear icon and select a custom parameter.

New Kiosk features and improvements

Kiosk configuration: Color of the battery icon (Samsung)

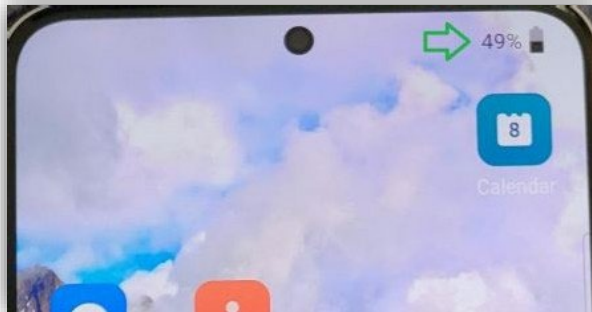
If hiding the status bar is enabled in the Kiosk configuration, the battery icon will also be hidden on Samsung devices.. A battery icon will be displayed for those devices. Depending on the color of the background image, a light or dark colored battery icon can be selected.



After enabling "Hide status bar" in the Kiosk configuration, the second option "Battery icon color" will appear.

The values for "Battery icon color" are:

- -- (default value, white color)
- Dark (black color)
- Light (white color)



Example of the battery icon in black (Dark).



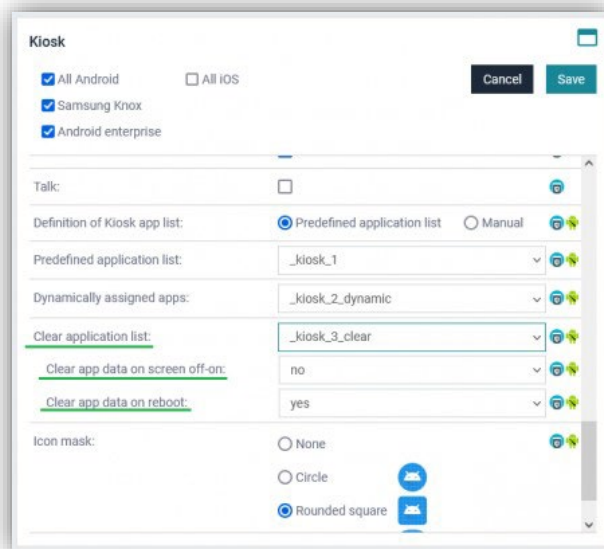
Example of the battery icon in white (default, Light).

Kiosk configuration: Improved "Clear app data"

The way app data (browser history, open web pages) should be cleared can be selected separately. There are two options:

"Clear app data on screen off-on": This will clear history of visited URLs and will close open browser pages if device screen time out turns the screen off or screen gets turned off manually.

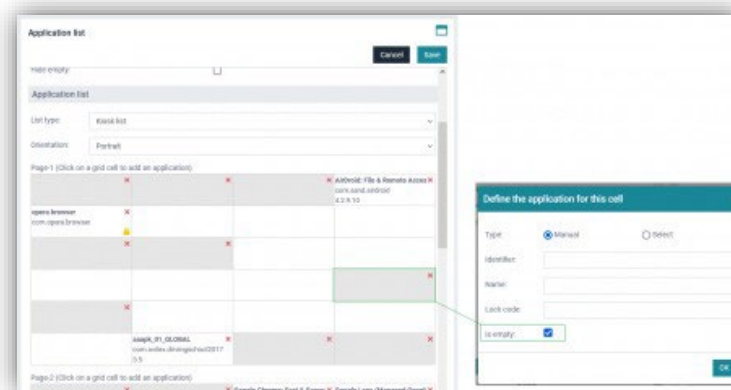
"Clear app data on reboot": This will clear history of visited URLs and will close open browser pages on device reboots.



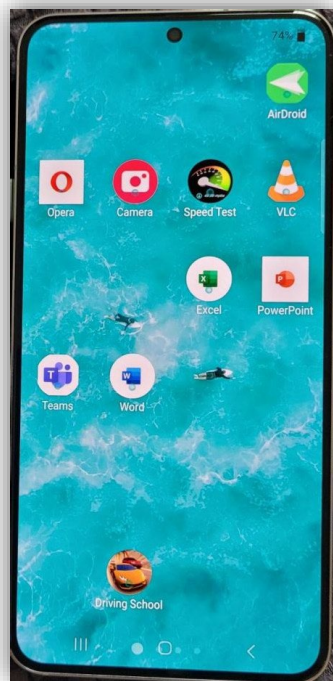
If an application list (type: Recommended list) is selected instead of None, two additional options appear. The available values are "Yes" and "No".

Application List configuration: Define a Grid position to be reserved as "Empty"

Grid positions can be defined as "Empty". These grid positions will remain empty even if apps from the dynamically assigned app list are installed after the device is in Kiosk mode.



In the Application List configuration (type: Kiosk list), you can click on a position and tick the "Is empty" check box. This position in the grid remains empty on devices in Kiosk mode if it has been selected in the "Predefined application list" in the Kiosk configuration.



This is an example how positions marked as "Is Empty", remain empty on a device in Kiosk mode.