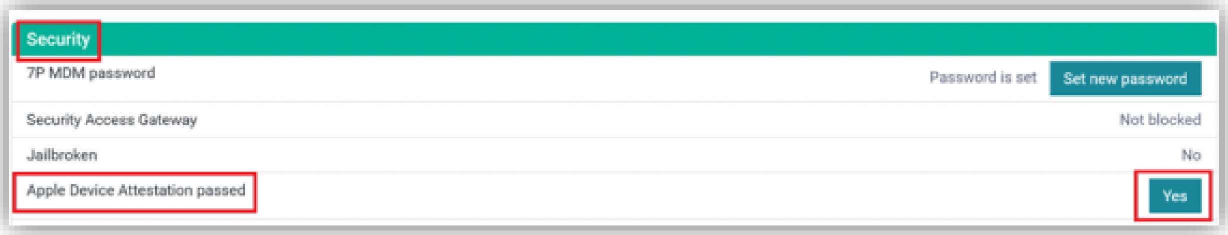
Release Bulletin

IKARUS mobile.management – Server

Version 6.14.xx
Release date 18.06.2023

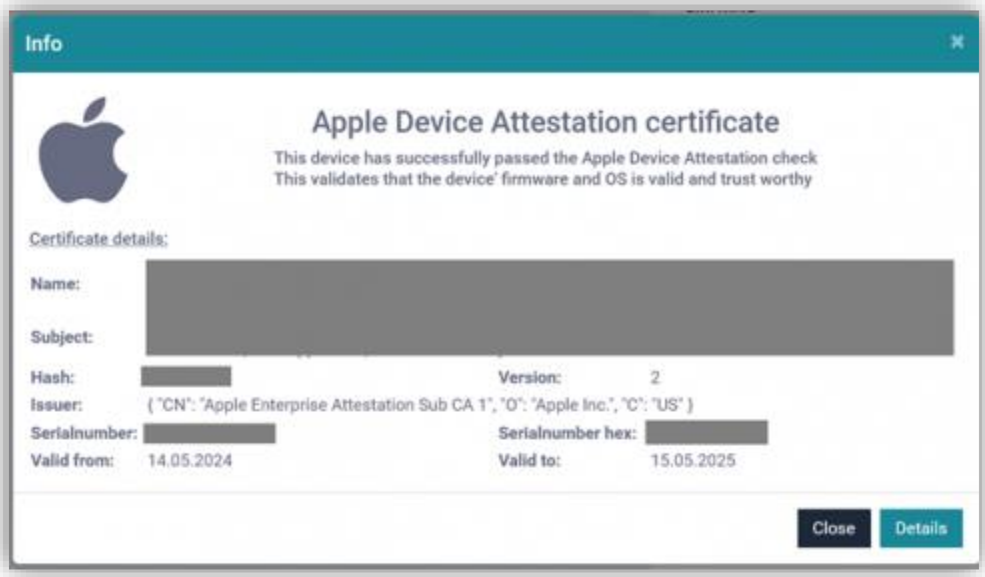
Apple Managed Device Attestation

We now support Apple Managed Device Attestation. The result can be seen on the inventory page of the Apple device:



Security	
7P MDM password	Password is set Set new password
Security Access Gateway	Not blocked
Jailbroken	No
Apple Device Attestation passed	Yes

Clicking on the button reveals further details about the attestation result:



Info ✖

Apple Device Attestation certificate

This device has successfully passed the Apple Device Attestation check
This validates that the device' firmware and OS is valid and trust worthy

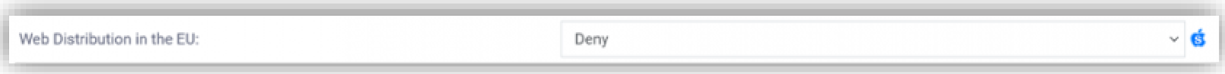
Certificate details:

Name: [redacted]
Subject:
Hash: [redacted] Version: 2
Issuer: { "CN": "Apple Enterprise Attestation Sub CA 1", "O": "Apple Inc.", "C": "US" }
Serialnumber: [redacted] Serialnumber hex: [redacted]
Valid from: 14.05.2024 Valid to: 15.05.2025

The Apple Managed Device Attestation replaces the Jailbreak detection, which will be removed from IKARUS mobile.management.

iOS Restriction for web distribution in the EU

iOS 17.5 introduces the distribution of apps through web pages in the EU. This can be prevented by the new restriction “Web Distribution in the EU”, which can be found in the configuration type “Restriction” in the section “Applications”.



Web Distribution in the EU:	Deny

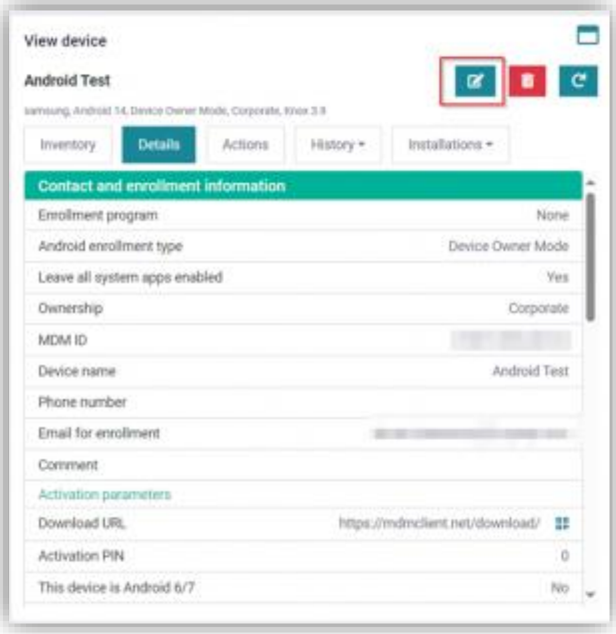
The restriction will only work with supervised iPhones.

Move active Android Enterprise devices between users

It is now possible to move devices with an active Android Enterprise account between users by changing the ownership and deleting the managed Google Play account on the device.

Important: This only works on Device Owner devices.

First, the ownership of the device needs to be changed from "Corporate" to "Private", so that IKARUS mobile.management does not try to activate the managed Google Play account again
This is done by going to “Details” tab and editing the device entry:

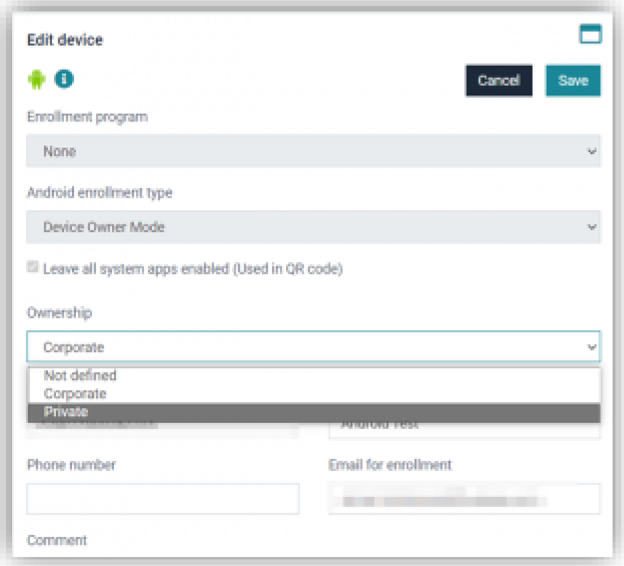


Android Test

samsung, Android 14, Device Owner Mode, Corporate, Knox 3.9

Contact and enrollment information	
Enrollment program	None
Android enrollment type	Device Owner Mode
Leave all system apps enabled	Yes
Ownership	Corporate
MDM ID	[redacted]
Device name	Android Test
Phone number	
Email for enrollment	[redacted]
Comment	
Activation parameters	
Download URL	https://mdmclient.net/download/
Activation PIN	0
This device is Android 6/7	No

Set the ownership to “Private” and save the entry:



Edit device

Enrollment program: None

Android enrollment type: Device Owner Mode

□ Leave all system apps enabled (Used in QR code)

Ownership: Corporate

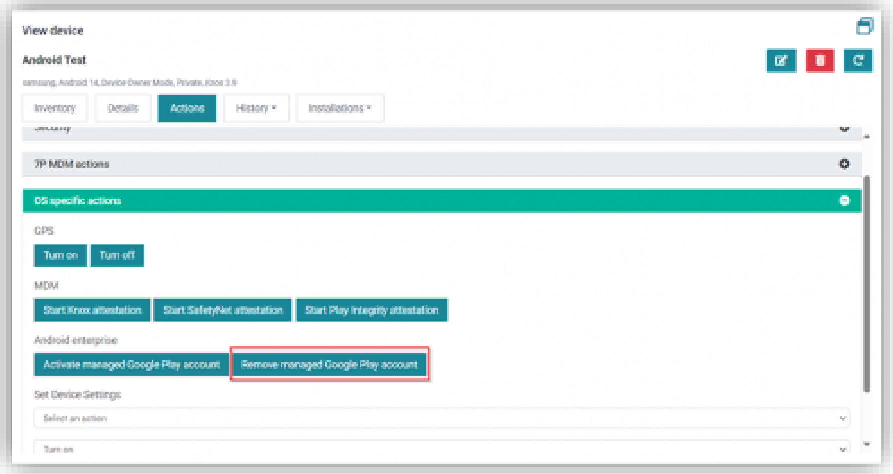
- Not defined
- Corporate
- Private

Phone number:

Email for enrollment: [redacted]

Comment

Now the managed Google Play account can be removed by navigating to Actions and selecting "Remove managed Google Play account" in "OS specific actions":

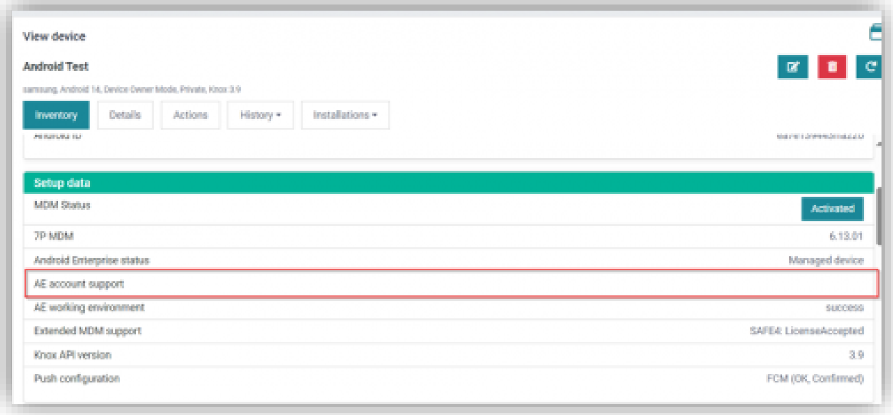


View device

Android Test

samsung, Android 14, Device Owner Mode, Private, Knox 3.9

If successfully executed, the "AE account support" in Inventory of the device should be cleared and no longer display the managed account data:



View device

Android Test

samsung, Android 14, Device Owner Mode, Private, Knox 3.9

Setup data

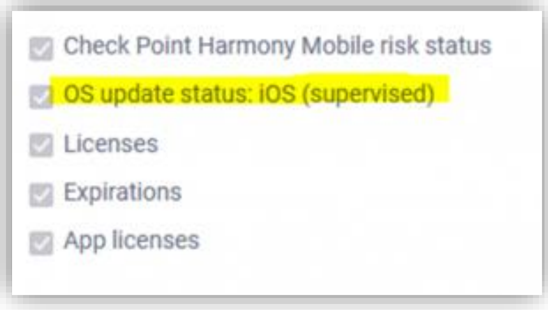
MDM Status	Activated
7P MDM	6.13.01
Android Enterprise status	Managed device
AE account support	
AE working environment	success
Extended MDM support	SAFE4: LicenseAccepted
Knox API version	3.9
Push configuration	FCM (OK, Confirmed)

The device can now be moved to a different user. To activate the managed Google Play account again, the ownership needs to be changed back to “Corporate”. This will automatically trigger the activation of the account.

An additional force connection might be needed to properly display the new account.

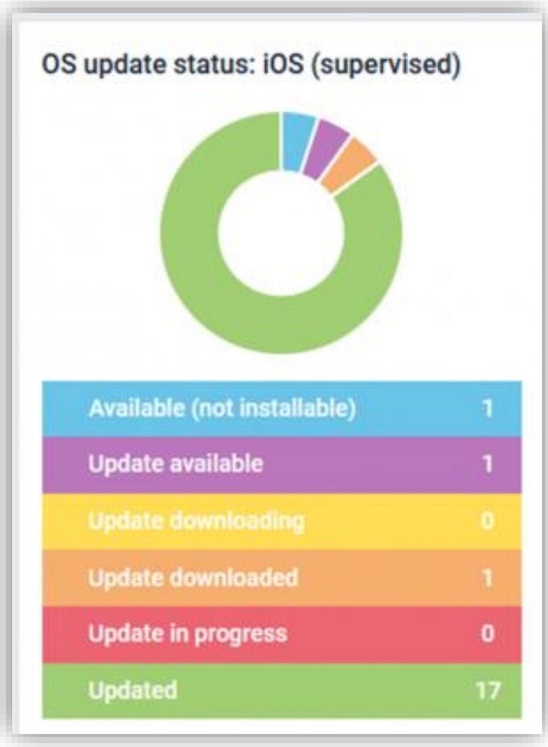
iOS Update pie chart in Dashboard

In Global view or local tenant inside Settings -> System -> Dashboard you can now enable an additional graphical view on OS update status on supervised iOS devices



☑ Check Point Harmony Mobile risk status
☑ OS update status: iOS (supervised)
☑ Licenses
☑ Expirations
☑ App licenses

When this is enabled, then inside your dashboard on either Global and/or tenant level is a new Pie chart overview of supervised iOS devices and their OS update status



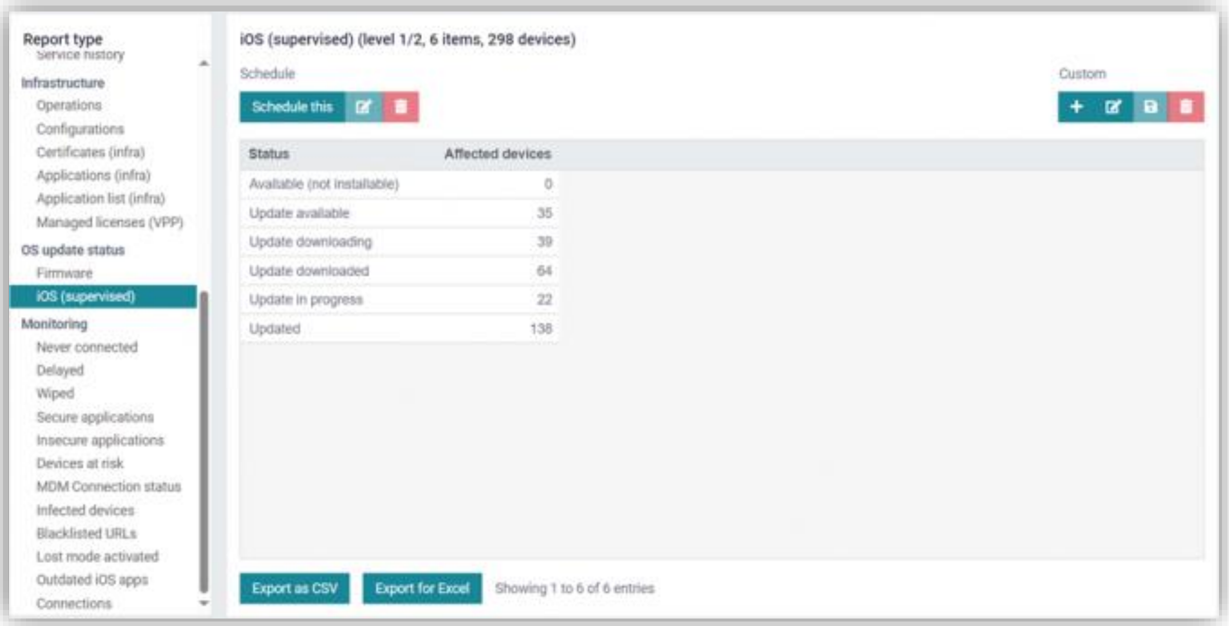
OS update status: iOS (supervised)

Available (not installable)	1
Update available	1
Update downloading	0
Update downloaded	1
Update in progress	0
Updated	17

Clicking on the numerical values in the table below the pie chart directs you to the new OS update status section within Reports as well into the report named iOS (supervised)

New report “iOS (supervised)”

There is a new report type in “OS update status” section called “iOS (supervised)”, which shows the different update statuses:



iOS (supervised) (level 1/2, 6 items, 298 devices)

Status	Affected devices
Available (not installable)	0
Update available	35
Update downloading	39
Update downloaded	64
Update in progress	22
Updated	138

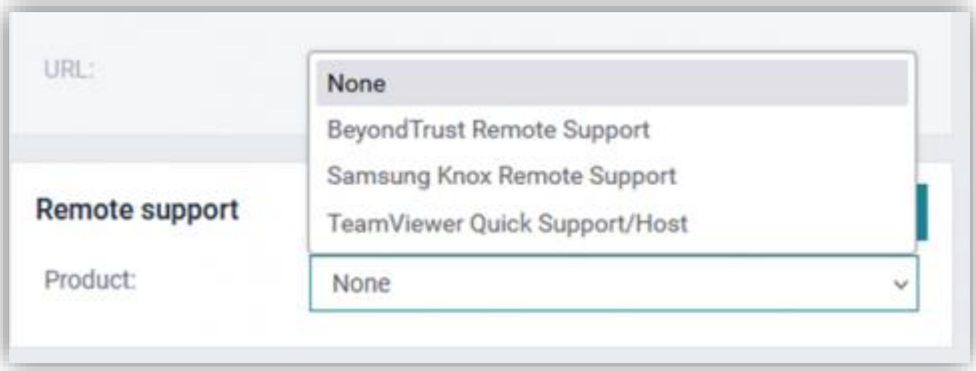
Showing 1 to 6 of 6 entries

By selecting one of these statuses the devices where the OS update is in that status are displayed.

New Remote Support options

In 6.14.xx server we have in Global view within Settings -> Connections -> Remote support added following changes:

You can now choose which Remote support solution you are using as default in combination with our MDM solution.


URL:
None
BeyondTrust Remote Support
Samsung Knox Remote Support
TeamViewer Quick Support/Host

Remote support

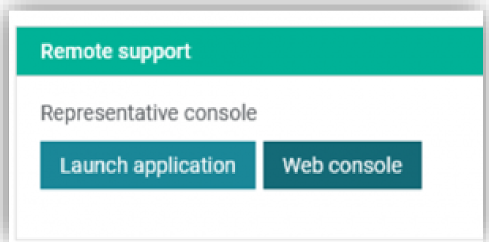
Product: None

With this choice you are able to benefit from these vendors remote support solution via a simple integration to MDM console.

If you choose:

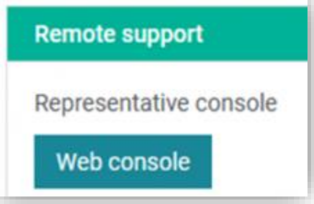
- Beyond Trust Remote support, then you must define some server settings for your Remote support appliance, whereafter devices with the Beyond Trust Remote support app on will have a button for remote starting the support session via email or SMS.

- Knox Remote support, then on those Android devices where the Knox Remote support app is installed on appears 2 new buttons.



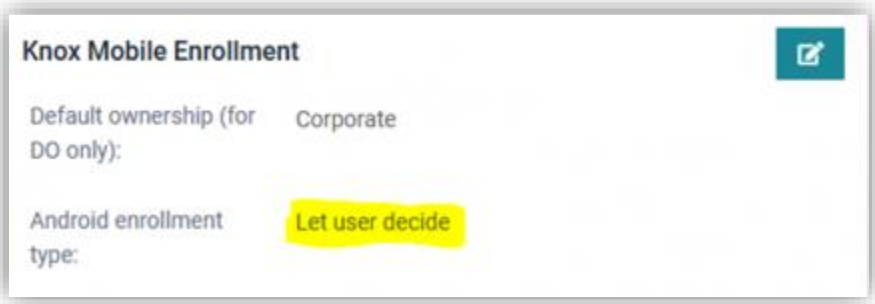
- Launch application, which means MDM server sends a remote-start application command for the Knox Remote support app. This button ONLY works on Samsung devices. On non-Samsung devices the user must start the app on the device.
- Web console, which in a new browser tab opens the Samsung Knox portal for entering your Knox admin account, whereafter you enter the Samsung Knox Remote support web console.

- TeamViewer Quick Support/Host, then you must secure that the TeamViewer Quicksupport app or TeamViewer Host app is installed on the device in advance. When this is done and MDM server can see this, then this Remote support option appears on the individual device within actions. From this web console you can access the TeamViewer web viewer console for remote supporting your devices with TeamViewer app on.



Allow users to decide the enrollment type for their device during KME enrollment

Inside Global view and Settings -> Android -> Knox Mobile Enrollment as well Settings -> Android -> Android Zero Touch Enrollment is a new Android Enrollment type available named “Let user decide”.



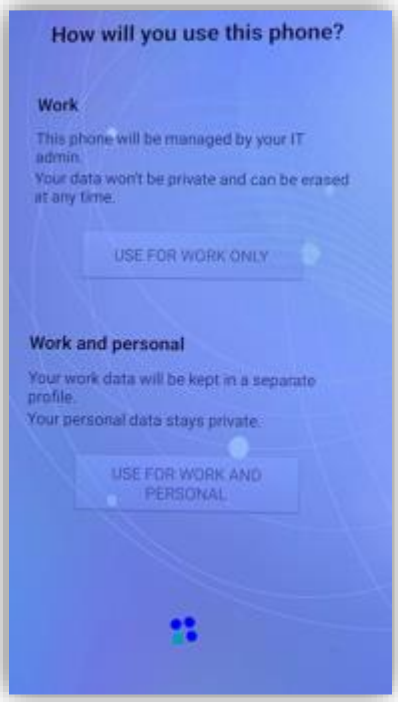
Knox Mobile Enrollment

Default ownership (for DO only): Corporate

Android enrollment type: Let user decide

This is available from server version 6.14.03 and requires the use of Android client 6.14.00 and higher and is available on Android devices from OS version 11 and up.

If this Android Enrollment type is selected in KME or Zero Touch and if a device is not pre-registered in MDM with it’s serial number or IMEI number, then during KME/Zero Touch Enrollment, the user will be prompted if the device is going the be used for Only corporate purpose, which means it will become added to MDM server as DO mode or if it is for corporate and private usage, which will enroll the device in MDM server in WPCO mode.



How will you use this phone?

Work

This phone will be managed by your IT admin.
Your data won't be private and can be erased at any time.

USE FOR WORK ONLY

Work and personal

Your work data will be kept in a separate profile.
Your personal data stays private.

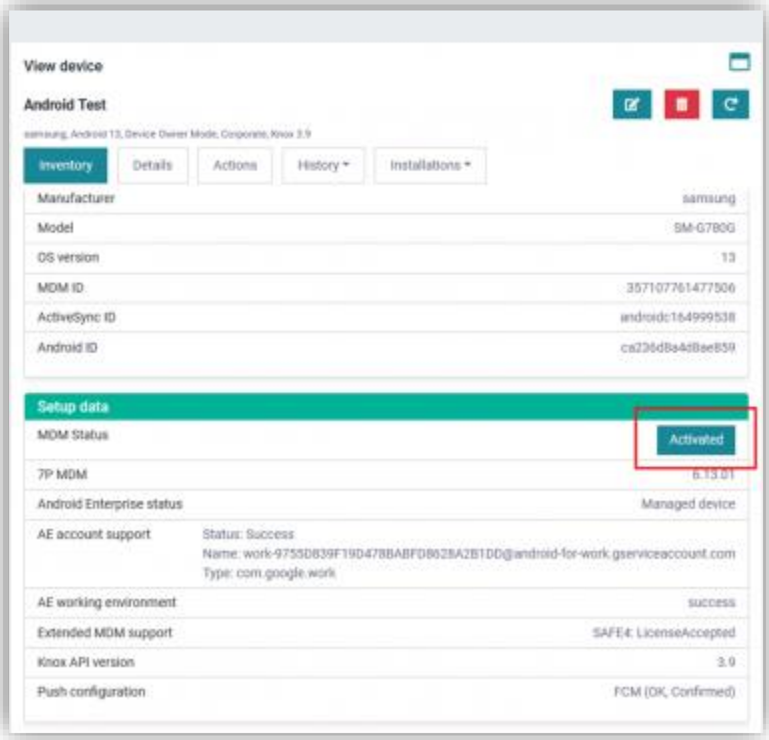
USE FOR WORK AND PERSONAL

Important: Once a device has been added to server in either DO or WPCO mode, then what is registered in MDM server counts and will be the mode the device is enrolled to. If wrong choice is made, then wipe the device and erase the device in server. Then at next new KME/Zero Touch Enrollment the user will be prompted again and added to server in correct Enrollment type mode.

Note: Please also be aware of that the Activation JSON string this option gives inside *Settings -> Android -> Knox Mobile Enrollment* or *Settings -> Android -> Zero Touch Enrollment* is different than when using DO or WPCO mode. If you want to use "*Let User decide*" check that you are using the correct JSON activation string.

MDM Status Improvement

With 6.14 an improved MDM Status Popup for Android Devices was added.



View device

Android Test

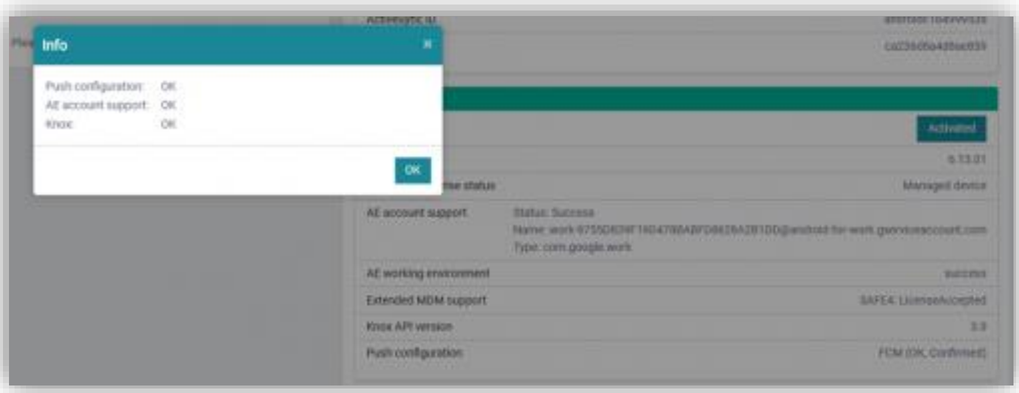
samsung, Android 13, Device Owner Mode, Corporate, Knox 3.9

Manufacturer	samsung
Model	SM-G780G
OS version	13
MDM ID	357107761477506
ActiveSync ID	androidc164999538
Android ID	ca236d8a4d8ae859

Setup data

MDM Status	Activated
7P MDM	6.13.01
Android Enterprise status	Managed device
AE account support	Status: Success Name: work-9755D839F19D478BABFD8628A2B1DD@android-for-work.gserviceaccount.com Type: com.google.work
AE working environment	success
Extended MDM support	SAFE4: LicenseAccepted
Knox API version	3.9
Push configuration	FCM (OK, Confirmed)

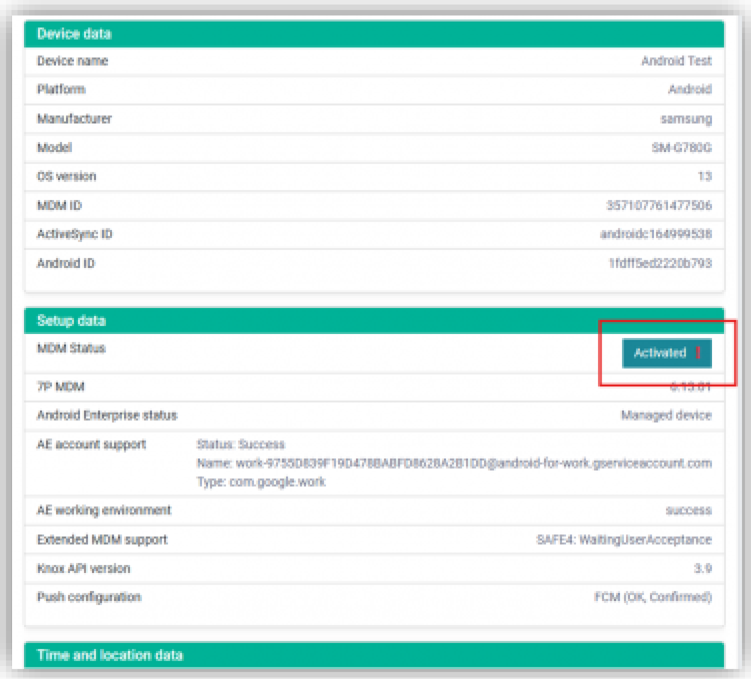
When you click on the MDM Status Button a popup shows the status of the push configuration, Android Enterprise Account Support and (if on a Samsung device) the Knox Status.



Info

Push configuration:	OK
AE account support:	OK
Knox:	OK

If any of the statuses for push configuration, Android Enterprise Account Support (and Knox if Samsung Device) is missing/ not properly activated, it is shown with a "!" on the MDM Status Button.

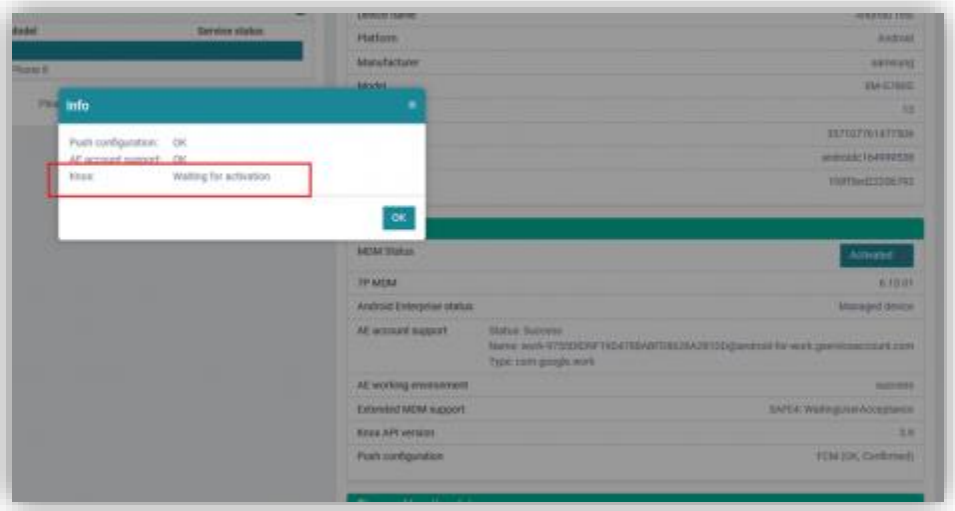


Device data	
Device name	Android Test
Platform	Android
Manufacturer	samsung
Model	SM-G780G
OS version	13
MDM ID	357107761477506
ActiveSync ID	androidc164999538
Android ID	1fdff5ed2220b793

Setup data	
MDM Status	Activated !
7P MDM	6.10.01
Android Enterprise status	Managed device
AE account support	Status: Success Name: work-9755D839F19D478BABFD8628A2B1DD@android-for-work.gserviceaccount.com Type: com.google.work
AE working environment	success
Extended MDM support	SAFE4: WaitingUserAcceptance
Knox API version	3.9
Push configuration	FCM (OK, Confirmed)

Time and location data

In this case you can click the button to see which part is not activated properly.



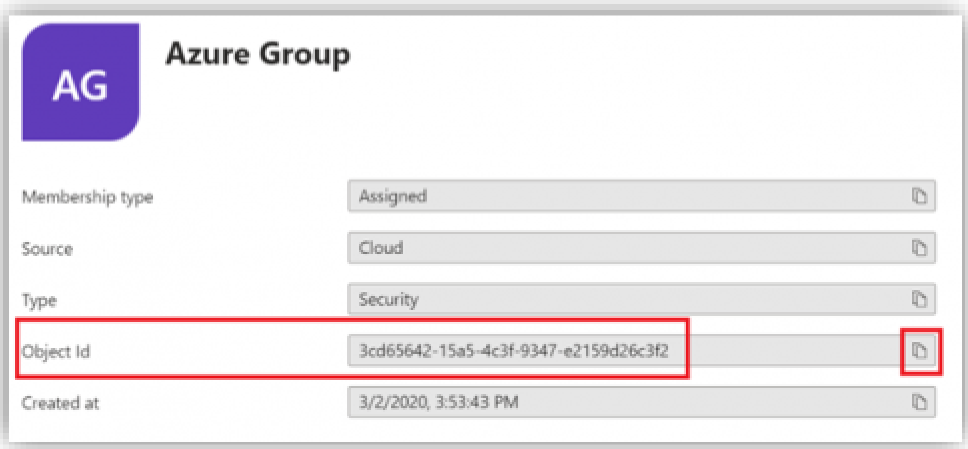
Info

Push configuration:	OK
AE account support:	OK
Knox:	Waiting for activation

Entra ID User sync now supports selection of groups

Our Entra ID user sync now supports to only sync users from selected Entra ID groups.

In Entra ID, the “Object ID” of a group can be copied using the button:



AG

Azure Group

Membership type: Assigned

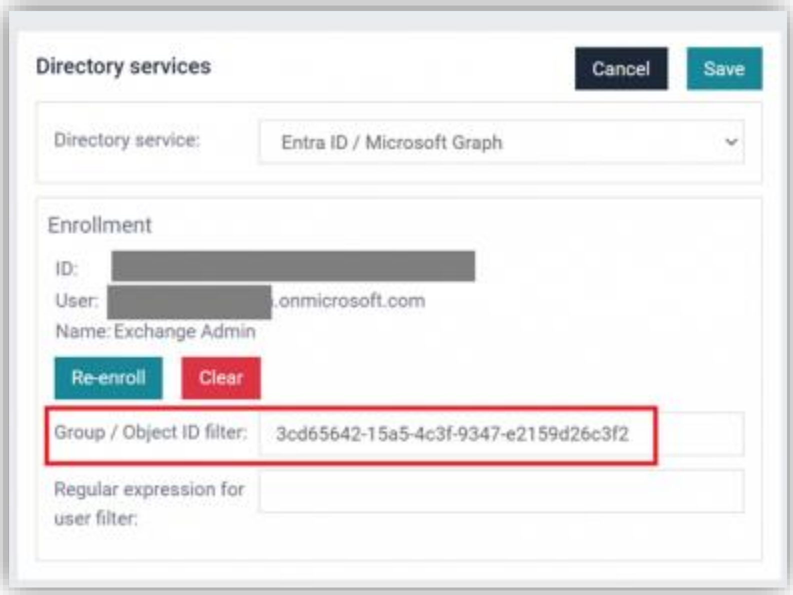
Source: Cloud

Type: Security

Object Id: 3cd65642-15a5-4c3f-9347-e2159d26c3f2

Created at: 3/2/2020, 3:53:43 PM

In IKARUS mobile.management, under [Tenant] - Settings – Connections – Directory services, where your Entra ID sync is configured, there is now a new field called "Group / Object ID filter":



Directory services

Directory service: Entra ID / Microsoft Graph

Enrollment

ID: [redacted]

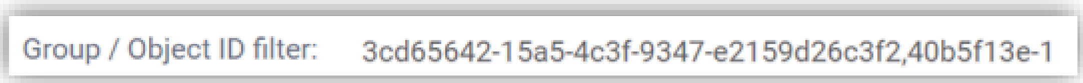
User: [redacted].onmicrosoft.com

Name: Exchange Admin

Group / Object ID filter: 3cd65642-15a5-4c3f-9347-e2159d26c3f2

Regular expression for user filter:

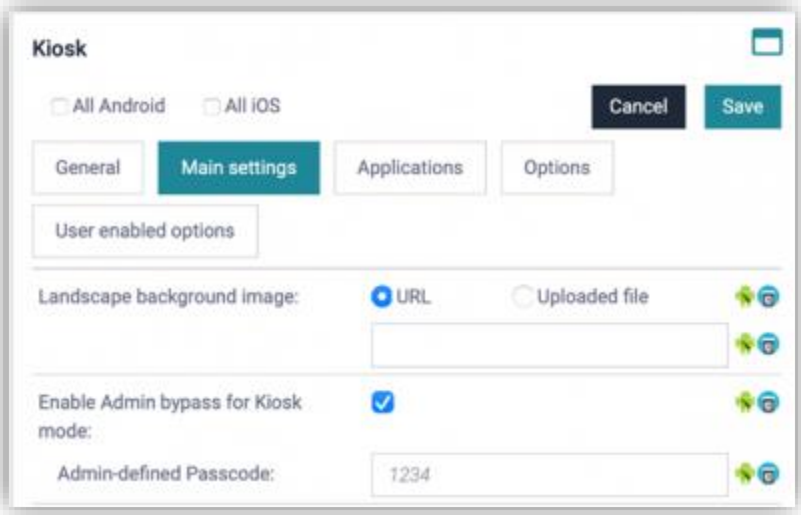
Additional groups can be added with a comma (no space after comma):



Group / Object ID filter: 3cd65642-15a5-4c3f-9347-e2159d26c3f2,40b5f13e-1

Android KIOSK: Admin bypass for KIOSK mode

The KIOSK configuration now has the possibility to set a PIN to bypass the KIOSK mode:



Landscape background image: ● URL ○ Uploaded file

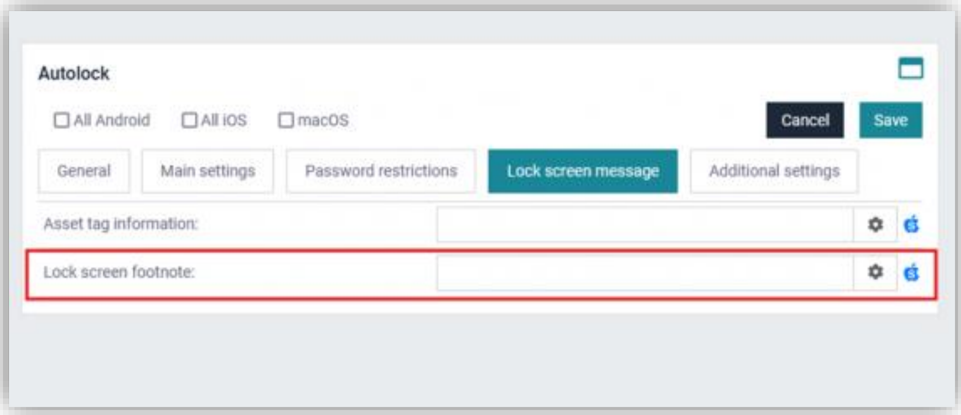
Enable Admin bypass for Kiosk mode: ☑

Admin-defined Passcode: 1234

The PIN can be entered in the settings of the MDM Client on the device (requires MDM Client 6.14).

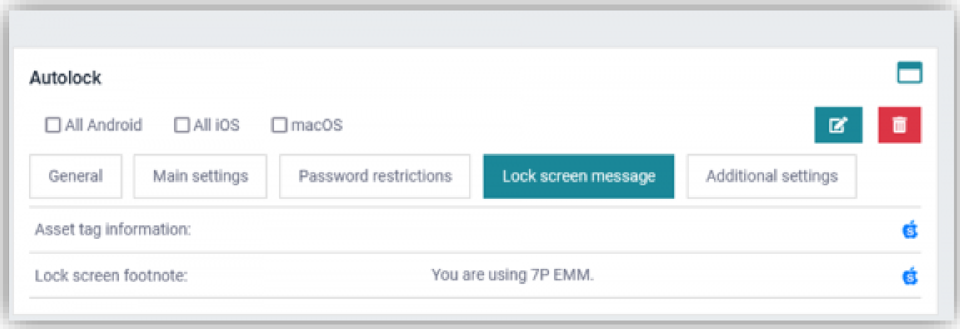
iOS: Lock screen footnote in Autolock configuration

We have added a new feature for iOS devices. Within the “Autolock” configuration you can now choose to display a unique lock screen footnote.



Asset tag information:

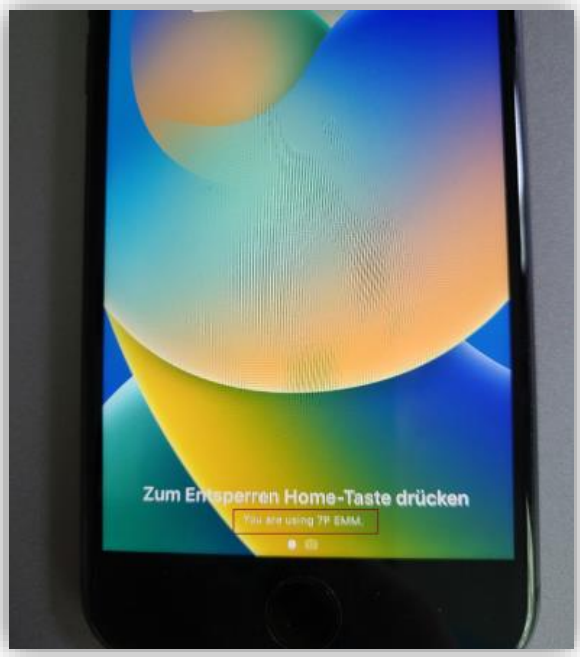
Lock screen footnote:



Asset tag information:

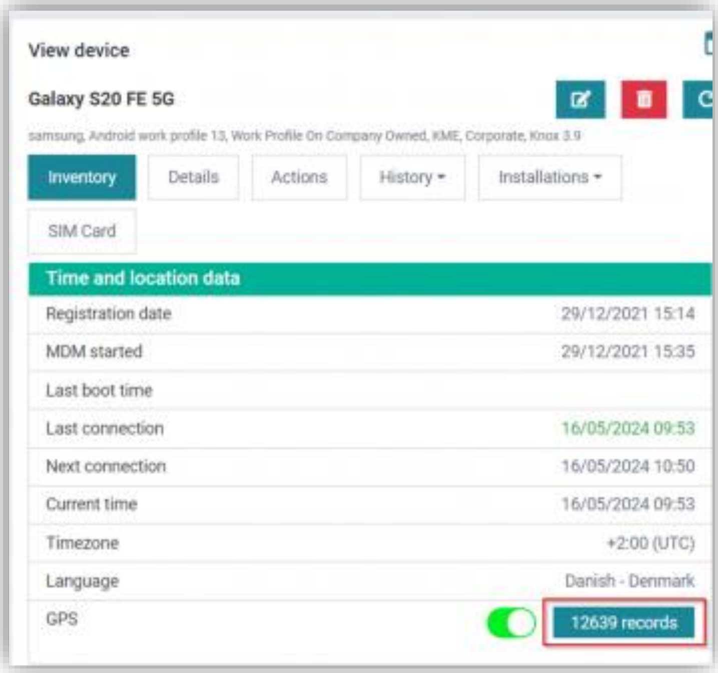
Lock screen footnote: You are using 7P EMM.

After entering your unique lock screen footnote and applying the autolock configuration, your footnote will be displayed on the lock screen of your device.



Modernization of GPS UI

When selecting the location record data in a device's inventory there is now a map directly integrated into the interface:



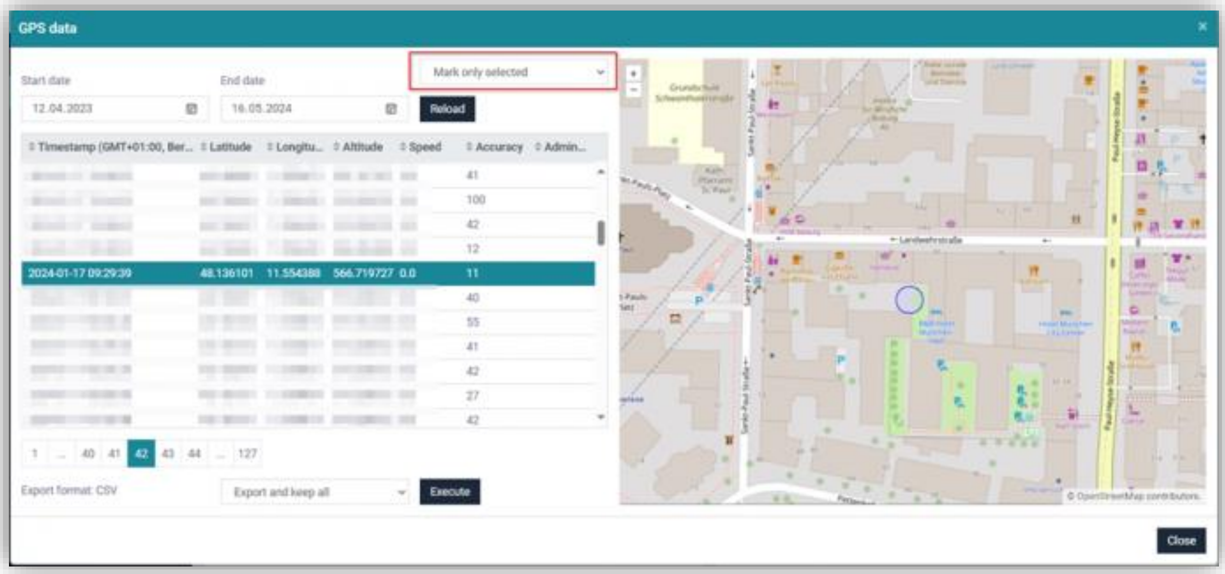
View device

Galaxy S20 FE 5G

samsung, Android work profile 13, Work Profile On Company Owned, KME, Corporate, Knox 3.9

Time and location data	
Registration date	29/12/2021 15:14
MDM started	29/12/2021 15:35
Last boot time	
Last connection	16/05/2024 09:53
Next connection	16/05/2024 10:50
Current time	16/05/2024 09:53
Timezone	+2:00 (UTC)
Language	Danish - Denmark
GPS	12639 records

By default, the map only shows a location pin for the currently selected location data:


GPS data

Start date: 12.04.2023

End date: 16.05.2024

Mark only selected

⇕ Timestamp (GMT+01:00, Ber...	⇕ Latitude	⇕ Longitu...	⇕ Altitude	⇕ Speed	⇕ Accuracy	⇕ Admin...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	41	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	100	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	42	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	12	
2024-01-17 09:29:39	48.136101	11.554388	566.719727	0.0	11	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	40	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	55	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	41	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	42	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	27	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	42	

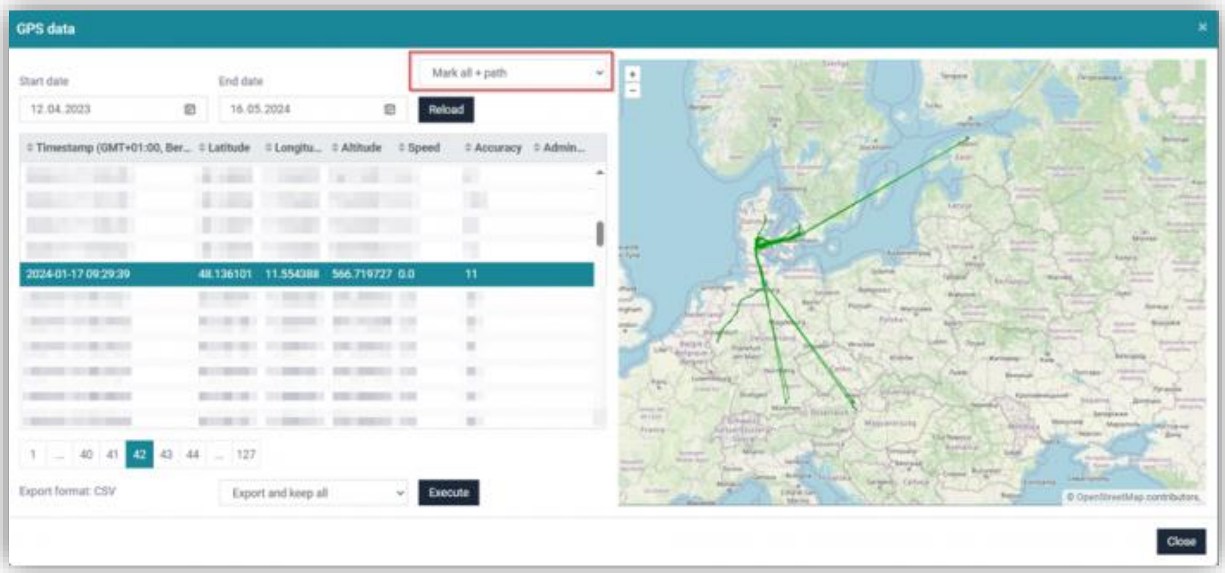
Export format: CSV

Export and keep all

Additionally, beside the default option “Mark only selected”, two new options called “Mark selected + path” and “Mark all + path” can be selected from the drop-down menu.

While the first option will only display a location pin for the currently selected location data, the latter one will display a pin for all available entries.

Both options will also show a path between all coordinates:


GPS data

Start date: 12.04.2023

End date: 16.05.2024

Mark all + path

⇕ Timestamp (GMT+01:00, Ber...	⇕ Latitude	⇕ Longitu...	⇕ Altitude	⇕ Speed	⇕ Accuracy	⇕ Admin...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
2024-01-17 09:29:39	48.136101	11.554388	566.719727	0.0	11	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

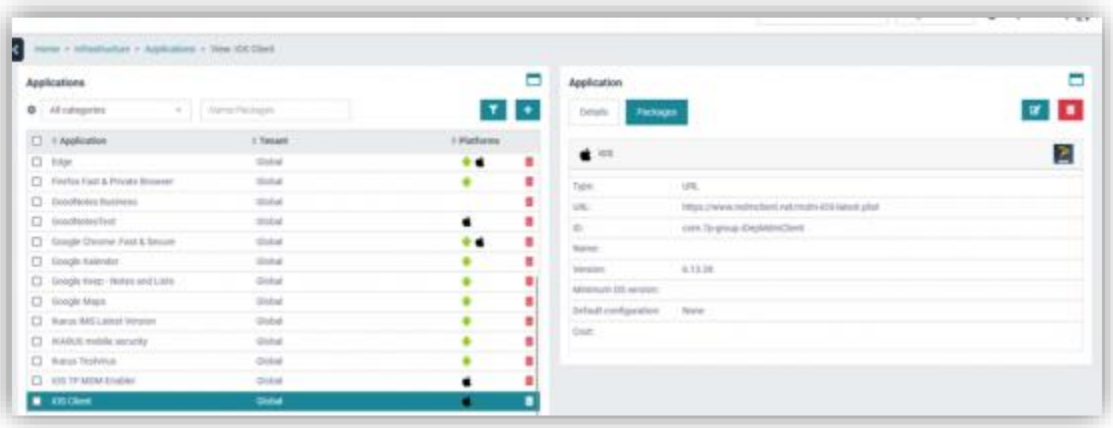
Export format: CSV

Export and keep all

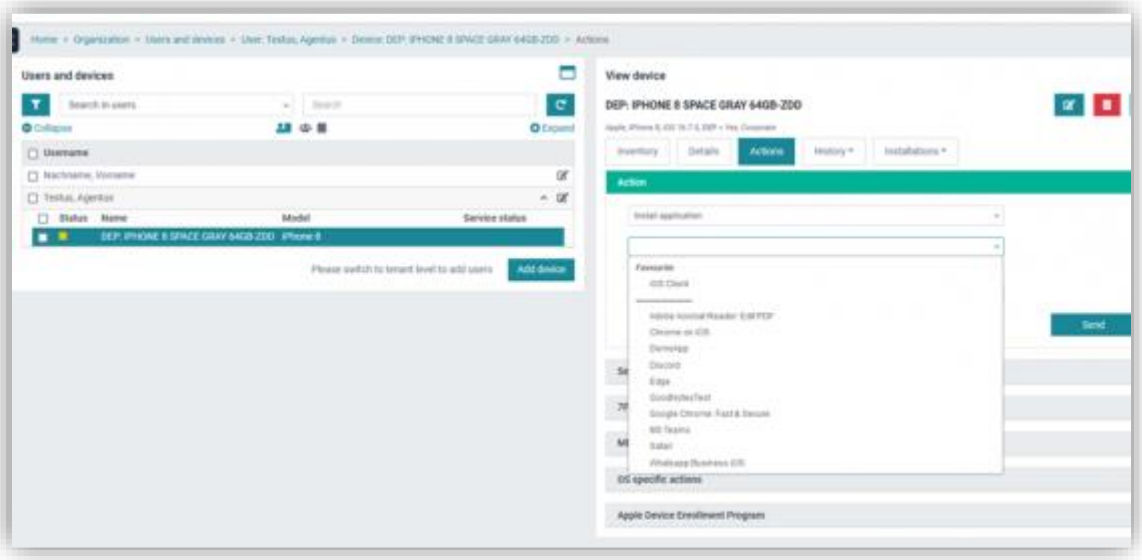
Favourite Apps

IKARUS Applications that are added under the infrastructure tab are now listed as “favourites” when using an “install application” command.

First, you must add the app in the infrastructure tab.

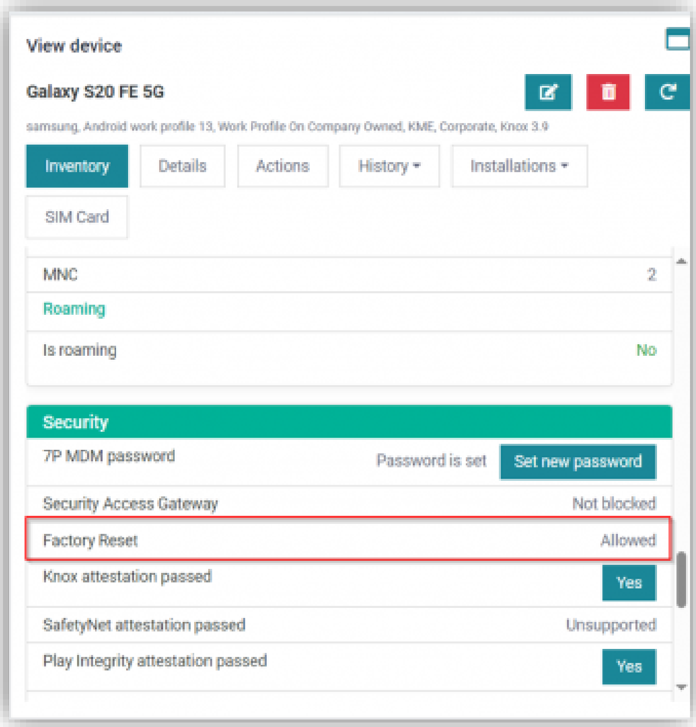


Then you should see it show up under “favourites” when using the “install application” command.



Android: Factory reset protection status

There is new attribute in “Security” section in device’s inventory called “Factory Reset”:



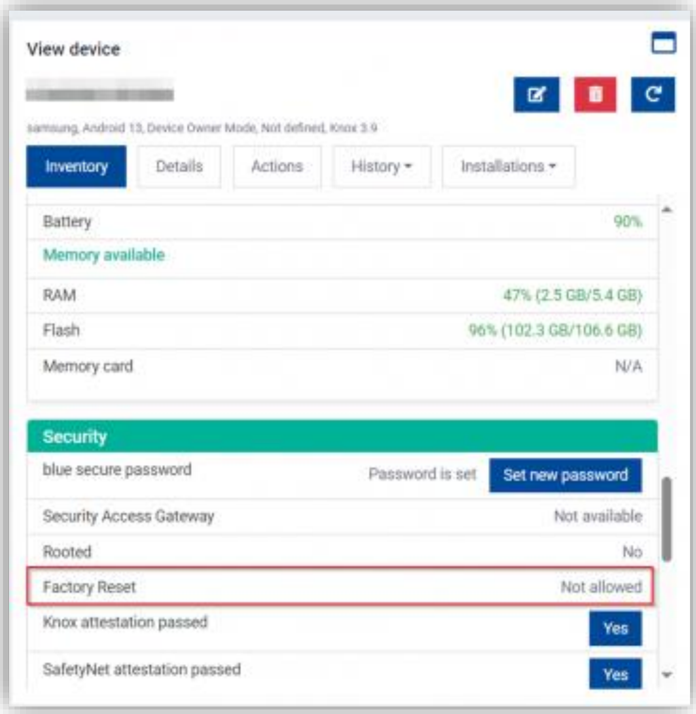
Galaxy S20 FE 5G

samsung, Android work profile 13, Work Profile On Company Owned, KME, Corporate, Knox 3.9

MNC	2
Roaming	
Is roaming	No
Security	
7P MDM password	Password is set
Security Access Gateway	Not blocked
Factory Reset	Allowed
Knox attestation passed	Yes
SafetyNet attestation passed	Unsupported
Play Integrity attestation passed	Yes

This attribute will show whether the factory reset of a device is currently allowed or if it is prohibited by a restriction in which the “Factory Reset” option was set to “Deny”.

If that’s the case, the value for the attribute will change to “Not allowed”:



[redacted]

samsung, Android 13, Device Owner Mode, Not defined, Knox 3.9

Battery	90%
Memory available	
RAM	47% (2.5 GB/5.4 GB)
Flash	96% (102.3 GB/106.6 GB)
Memory card	N/A
Security	
blue secure password	Password is set
Security Access Gateway	Not available
Rooted	No
Factory Reset	Not allowed
Knox attestation passed	Yes
SafetyNet attestation passed	Yes