


Release Bulletin

IKARUS mobile.management – Server

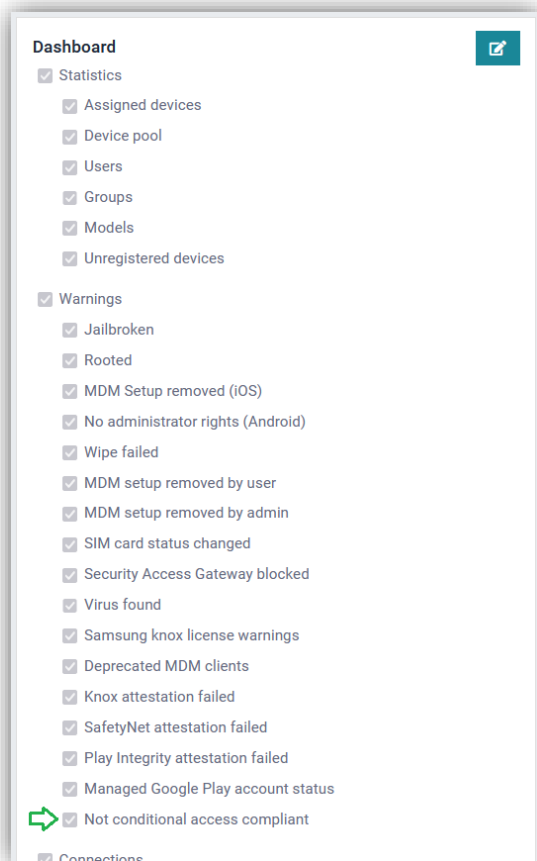
Version 6.13.xx
Release date 06.03.2023

Conditional Access

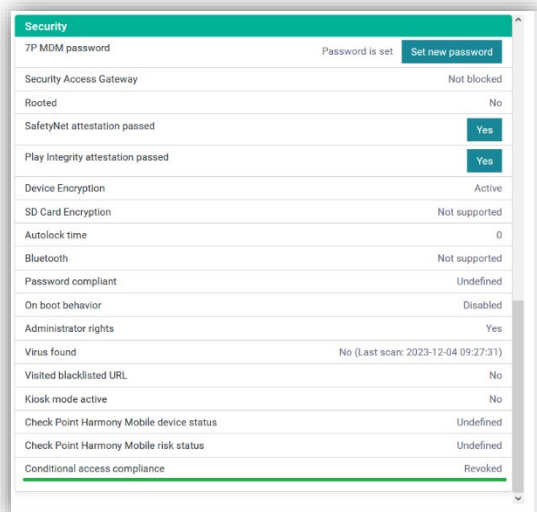
Conditional Access (Microsoft) has been implemented.

Warnings	
Jailbroken	0
Rooted	0
MDM Setup removed (iOS & Win)	7
No administrator rights (Android)	0
Wipe failed	0
MDM setup removed by user	7
MDM setup removed by admin	0
SIM card changed	0
Security Access Gateway blocked	2
Virus found	0
Samsung Knox	1
Deprecated MDM clients (<6.11.00)	32
Knox attestation failed	0
SafetyNet attestation failed	3
Play Integrity attestation failed	5
Managed Google Play account status	0
 Not conditional access compliant	96

On Dashboard > Warnings the number of non-compliant devices is displayed.





If this information is not visible in Dashboard, it must be enabled in Settings > System > Dashboard.



The current status of the conditional access compliance for each device is displayed on Organization > Users and devices > View device > Security.

Assigned devices (level 1/1, 8 devices)

Schedule Custom

Schedule this  

Search

Groups Select (0)

Ownership All

SAG status All

Administrator rights All

Is jailbroken/rooted All

MDM Status All

Knox attestation passed All

Play Integrity attestation passed All

SafetyNet attestation passed All

Check Point Harmony Mobile risk status All

Conditional access compliance All

Platform All

Manufacturer All


Enrollment program All

Kiosk mode All

User	Device name	Model	OS version	Platform	7P MDM version	Conditional access compliance	Conditional access authenticated
beaverw, angryw	zebra	TC57	8.1.0	Android	6.08.04		No
do, do	S22	SM-S901B	14	Android	6.13.00	Revoked	No
do, do	Pixel4	Pixel 4a	13	Android	6.13.00	Revoked	No
wp, wp	TabA	SM-T290	11	Android work profile	6.13.00	Revoked	No
wp, wp	S7			Android work profile			No
wp, wp	Nokia8			Android work profile			No
wpc0, wpc0	Nokia81	Nokia 8.1	11	Android work profile	6.13.00	Revoked	No
wpc0, wpc0	Pixel7	Pixel 7a	14	Android work profile	6.13.00	Revoked	No

Export as CSV Export for Excel Showing 1 to 8 of 8 entries

On the Reports page (Inventory > Assigned devices), a new filter "Conditional access compliance" and new columns "Conditional access compliance", "Conditional access authenticated" have been added.

Edit view 

Name

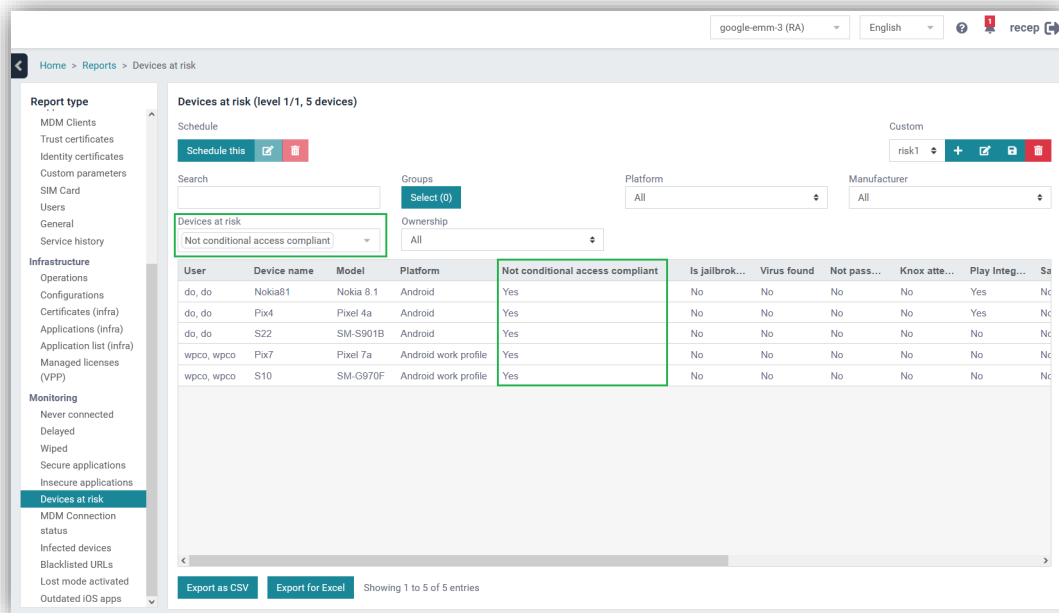
Columns

- ☒ 7P MDM version
- ☐ Android Enterprise status
- ☐ Apple VPP user status
- ☐ Apple VPP user tenant
- ☐ Certificate valid until
- ☐ Check Point Harmony Mobile device status
- ☐ Check Point Harmony Mobile risk status
- ☐ Comment
- ☒ Conditional access authenticated
- ☒ Conditional access compliance
- ☐ Creation date
- ☐ DEP profile status
- ☒ Device name
- ☐ EID
- ☐ Email
- ☐ Enrollment URL
- ☐ Enrollment program
- ☐ Enrollment token valid until
- ☐ Firmware
- ☐ Flash (free)
- ☐ Flash (total)
- ☐ Groups
- ☐ ICCID
- ☐ ICCID1
- ☐ ICCID2
- ☐ IMEI
- ☐ IMEI 1

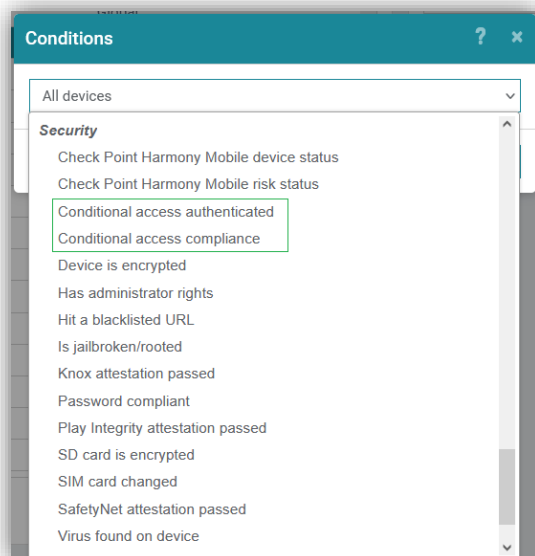
Filters

- ☒ Administrator rights
- ☒ Check Point Harmony Mobile risk status
- ☒ Conditional access compliance
- ☒ Enrollment program
- ☒ Groups
- ☒ Is jailbroken/rooted
- ☒ Kiosk mode
- ☒ Knox attestation passed
- ☒ MDM Status
- ☒ Manufacturer
- ☒ Ownership
- ☒ Platform
- ☒ Play Integrity attestation passed
- ☒ SAG status
- ☒ SafetyNet attestation passed
- ☒ Search

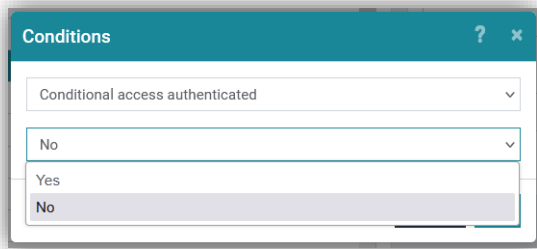
They can be enabled and disabled in the "Edit" option.



On Reports > Monitoring > Devices at risk, the filter and column "Not conditional access compliant" have been added.

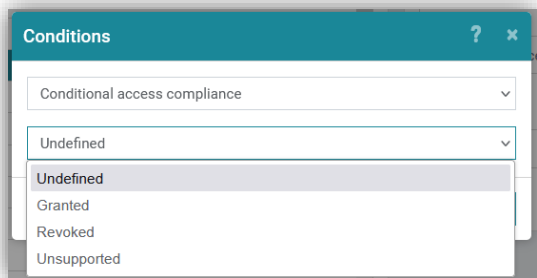


To manage devices with different conditional access authentication and compliance status, the two conditions "Conditional access compliance" and "Conditional access authenticated" have been added to Operations.



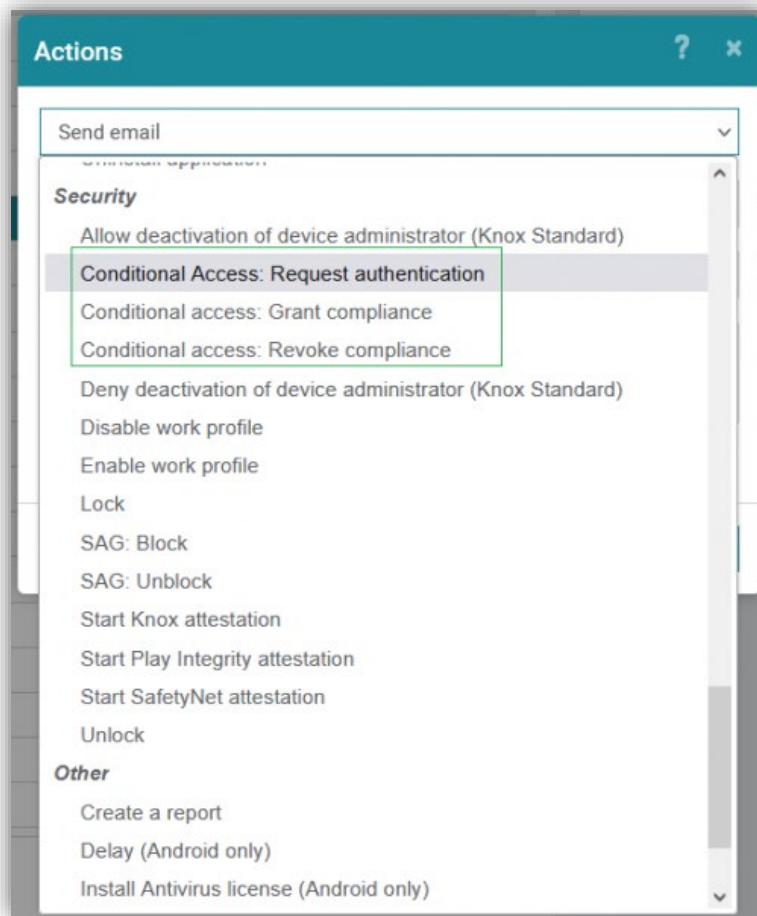
The condition "Conditional access authenticated" has the following values:

- Yes
- No



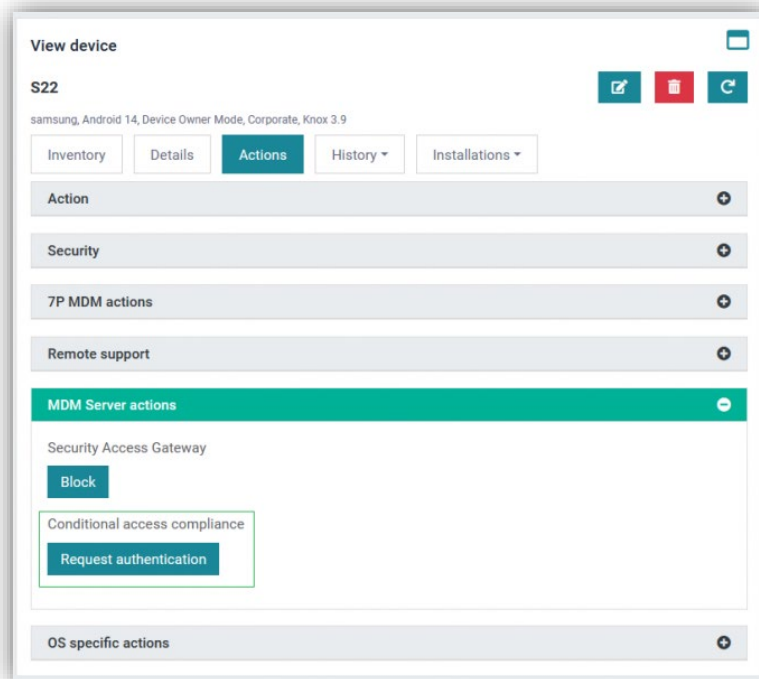
The condition "Conditional access compliance" has the following values:

- Undefined
- Granted
- Revoked
- Unsupported



To request authentication and change the conditional access compliance status of the devices, those three new actions have been added to Operations:

- Conditional access request authentication
- Conditional access grant compliance
- Conditional access revoke compliance



Requesting authentication and changing the conditional access compliance status of a selected device can also be done in Organization > Users and devices > MDM Server actions by clicking on the button under "Conditional access compliance". Depending on the current Conditional access compliance status of the device, one of those three buttons will be available:

- Request authentication
- Grant
- Revoke

Note: To use the conditional access feature, the latest MDM client (Android and iOS) and the Microsoft Authenticator app are required. To find out more, read our comprehensive guide (https://wiki.dmaas.de/index.php/Conditional_Access).

New condition "No application from blacklist installed"

To support the most common use cases for Conditional Access integration, a new condition "No application from blacklist installed" has been implemented. It can be used to filter devices that no longer match the condition "Application from blacklist is installed" without creating additional operations.

Operation

Name:

00-00-00test

Conditions:

4 matching devices

+

All devices

+

Conditional access compliance: Revoked

+

No application from blacklist installed: B-L-K

+

Actions:

+

Conditional access: Grant compliance

+

Send

Send Immediately

In this example, devices with a revoked conditional access compliance status but no blacklisted apps, will get their conditional access compliance status to "granted".

“Devices at risk” report improved

Check Point Harmony Mobile and Conditional Access reported risk values have been integrated into the "Devices at risk" report.

google-emm-3 (RA)

English

recep

s at risk

Devices at risk (level 1/1, 6 devices)

Schedule

Schedule this

+

-

Search:

Groups

Platform

Manufacturer

Search

Select (0)

All

All

Ownership

All

Custom

risk1

+

-

+

-

Search

SafetyNet attestation failed

Play Integrity attestation failed

Not password compliant

Not conditional access compliant

Check Point Harmony Mobile risk status

Hit a blacklisted URL

Virus found

Is jailbroken/rooted

Check Point Harmony Mobile device status

Check Point Harmony Mobile risk status

Not conditional access compliant

Is jailbroken/rooted

Virus f

Check Point Harmony Mobile device status	Check Point Harmony Mobile risk status	Not conditional access compliant	Is jailbroken/rooted	Virus f
	No	No	No	No
	Yes	No	No	No
	Yes	No	No	No
ork profile	Yes	No	No	No
ork profile	Yes	No	No	No
wpco, wpco	Yes	No	No	No

wpco, wpco

Pixel7

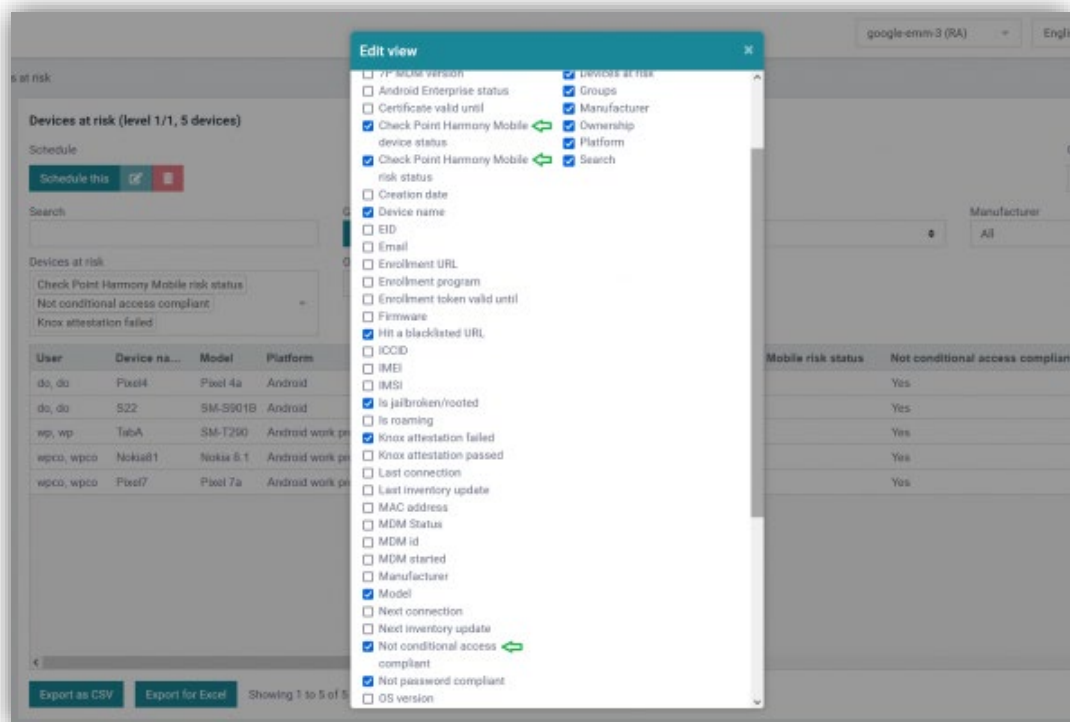
Pixel 7 a

Android work profile

Export as CSV

Export for Excel

Showing 1 to 6 of 6 entries



The filters and columns "Check Point Harmony Mobile device status", "Check Point Harmony Mobile risk status" and "Not conditional access compliant" have been added.
Admin roles and permissions improved

Now it is possible to create roles with more detailed levels of access.

Admin role

Name:

Help-1

Manage admin roles allowed:

☒

Manage admins of roles:

☐ All

Helpdesk administrator

Read-only administrator

000test000

00110011roles

00b00

00test00

01_restricted

Change own credentials allowed:

☒

Read-only:

☐

Access to user interface:

☐ All

☒ Dashboard

☒ Dashboard

☒ Logs

☐ Exception logging

☒ Organization

☒ Users and devices

☐ Hierarchies and groups

☐ User assignment

☐ Device pool

☐ Infrastructure

☒ Operations

☐ Operations

☒ Scheduler

☐ Reports

☐ Settings

Cancel

Save

Auditor roles or Help desk roles with different permissions can be added. Each level can be added or removed separately.

WiFi information added into QR code (Android)

Now it is possible to add the WiFi information into the enrollment QR code. If all or many devices should connect to the same WiFi access point, an Access Point configuration can be created and selected as the default WiFi access point during enrollment. This information will be embedded into the generated QR code. A device will connect to that access point automatically and will connect to the internet during enrollment. The step of manually entering the WiFi information can be skipped.

Zero Touch Enrollment Cancel Save

Default ownership (for DO only): Private

Android enrollment type: Work Profile On Company Owned

Wi-Fi configuration: access point - g

☒ Leave all system apps enabled

Activation JSON string to be used in ZTE portal:

Copy to clipboard

Zero Touch

For Zero Touch enrollment, the WiFi configuration can be set on Settings > Android > Zero Touch Enrollment. The default value is "None". In this case, the WiFi information will be asked during enrollment and should be entered manually.

Add device Cancel Save without enrolling

Choose a platform: Android iOS macOS Unknown

Enrollment program: None

Android enrollment type: Device Owner Mode

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

Ownership: Corporate

MDM ID:

Device name:

Phone number:

Email for enrollment:

Comment:

Serial number:

Activation parameters

Download URL:

Activation PIN:

Samsung Knox Premium: Do not activate

Wi-Fi configuration: access point - g

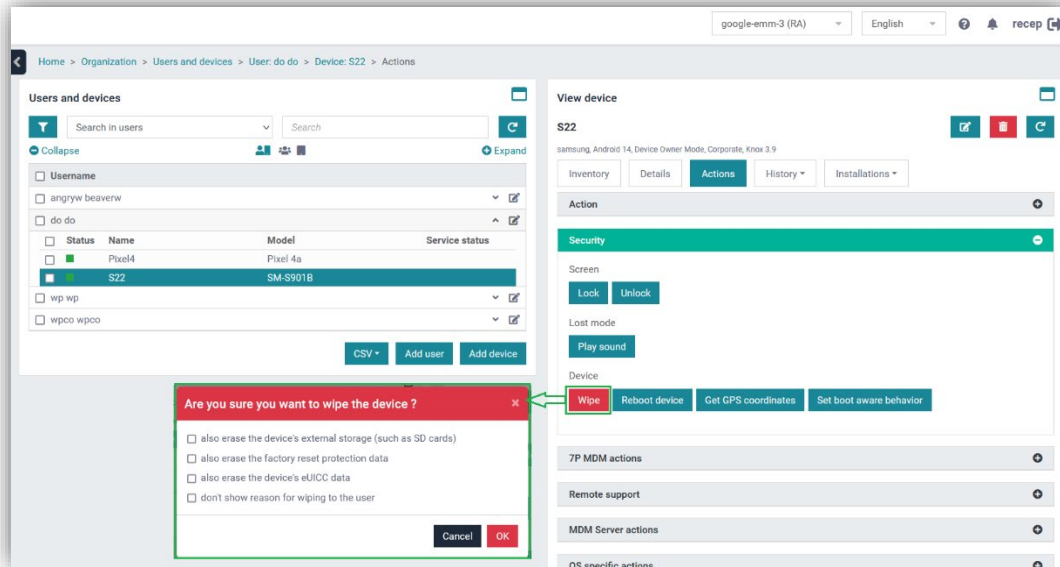
Enroll via email Activate with QR code

For any enrollment via QR code, the Access Point configuration can be selected here. The

QR code should be generated after selecting the Access Point configuration. "None" is the default value. If "None" is selected, the Access Point information must be entered manually during enrollment.

Additional options for "Wipe" (Android 11 and newer)

Additional Android wipe options for supported devices are now presented in the Wipe Device dialog.

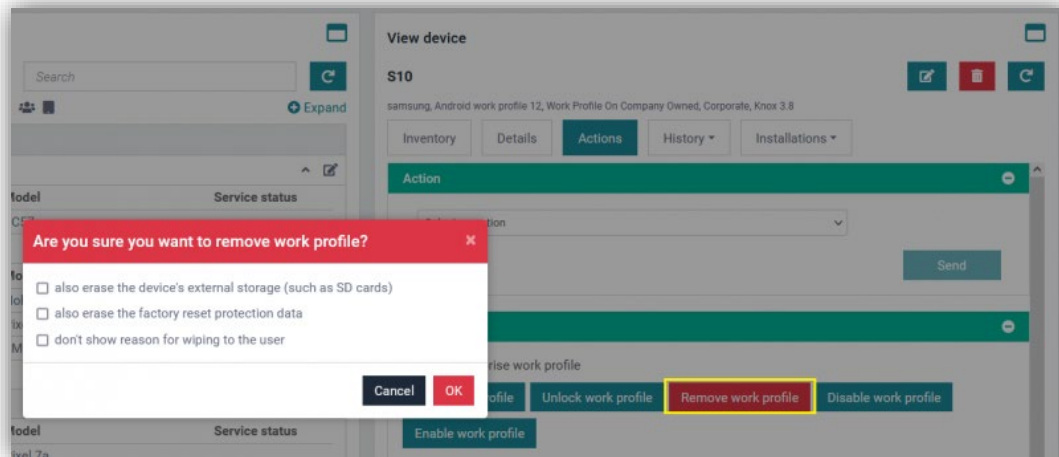


After clicking the "Wipe" button, a pop-up with four options will appear:

- also erase the device's external storage (such as SD cards)
- also erase the factory reset protection data
- also erase the device's eUICC data
- don't show reason for wiping to the user

Selected options that are not supported by the device will be ignored.

Additional options for "Remove work profile" (Android 11 and newer)



After clicking on the "Remove work profile" button, a pop-up with three options will appear:

- also erase the device's external storage (such as SD cards)
- also erase the factory reset protection data
- don't show reason for wiping to the user

Selected options that are not supported by the device will be ignored.

Kiosk changes and improvements

Those are the improvements made for Kiosk:

1. The option to disable Kiosk has been removed from the configuration. Disabling Kiosk mode can be done via a button on "MDM Server actions" or via an action in Operations.
2. The Kiosk client URL is already pre-filled based on the cloud information. A different URL can still be entered if needed.
3. A second wallpaper in landscape mode has been added. When rotating the device from portrait mode to landscape mode, the second wallpaper will be displayed.

Kiosk

☐ All Android ☐ All iOS Cancel Save

General

* Name:

Comment:



Created: 2023-12-06 12:52:53



Modified: 2023-12-06 12:52:53



Show all: ☒


Hide empty: ☐


Main settings


URL:  

Background image: ☒ URL ☐ Uploaded file  

Landscape background image: ☒ URL ☐ Uploaded file  

Allow multi-window mode: ☐ 

Allow TaskManager: ☐ 

Hide Systembar: ☐ 

Note: To be able to use the new Kiosk features, please use the latest 6.13.00 Kiosk client.

Infrastructure > Applications changes

Small changes have been made to the "Applications" page:

- Options have been regrouped to be tied and displayed with the appropriate package platforms.
- Options for different platforms are now separated and will not overwrite each other.
- On "Packages", each platform has its own description if the application has been added via an URL (AppStore, PlayStore). The text in this field cannot be edited.
- On "Details", there is still the "Description" field. Descriptions for apps added via file (apk, ipa) or also via URL and ID can be added and edited.
- The application icon has been moved from "Details" to "Packages".

Application

Details

Packages

Name

outlook

Categories

APPROVED, officetools, System Apps

Description

Application

Details

Packages

Android

Type:

URL

URL:

market://details?id=com.microsoft.office.outlook

ID:

com.microsoft.office.outlook

Name:

Microsoft Outlook

Description:

Connect and coordinate your busy life with Microsoft Outlook . Stay on top of your day through a secure email and calendar app that lets you manage your emails, files and calendar all in one place. Stay productive with whatever hits your inbox, whether it's from your work, school or your personal account. Organize your email intelligently, filtered into Focused and Other so you can easily see your most important messages. Keep your day organized by seeing multiple calendars at a glance.

Outlook is free for personal use. You can connect your various accounts, like Microsoft Exchange, Microsoft 365, Outlook.com, Gmail, Yahoo Mail, iCloud and more. And you can stay connected on the go. With Outlook.

Version:

4.2345.1

Minimum OS version:

9

Managed Google Play Store:

Undo approval

Approval:

Approved

Default configuration:

outlookconfig1

Cost:

Free