Release Bulletin

IKARUS mobile.management - Server

Version 6.13.xx Release date 06.03.2023

Conditional Access

Conditional Access (Microsoft) has been implemented.

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.

Dashboard	1
Statistics	
Assigned devices	
Device pool	
Users	
Groups	
Models	
Unregistered devices	
Warnings	
Jailbroken	
Rooted	
MDM Setup removed (iOS)	
No administrator rights (Android)	
Wipe failed	
MDM setup removed by user	
MDM setup removed by admin	
SIM card status changed	
Security Access Gateway blocked	
Virus found	
Samsung knox license warnings	
Deprecated MDM clients	
Knox attestation failed	
SafetyNet attestation failed	
Play Integrity attestation failed	
Managed Google Play account status	
🔿 🗹 Not conditional access compliant	

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

7P MDM password	Password is set Set new password		
Security Access Gateway	Not blocked		
Rooted	No		
SafetyNet attestation passed	Yes		
Play Integrity attestation passed	Yes		
Device Encryption	Active		
SD Card Encryption	Not supported		
Autolock time	0		
Bluetooth	Not supported		
Password compliant	Undefined		
On boot behavior	Disabled		
Administrator rights	Yes		
Virus found	No (Last scan: 2023-12-04 09:27:31)		
/isited blacklisted URL	No		
Kiosk mode active	No		
Check Point Harmony Mobile device status	Undefined		
Check Point Harmony Mobile risk status	Undefined		
Conditional access compliance	Revoked		

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

Schedule											Custom	
Schedule this	Ô										attest 🗢 🕂	g 8 1
Search			Groups				Ownership			SAG st	atus	
			Selec	ct (0)			All	\$		All		:
dministrator rights			ls jailbr	roken/rooted			MDM Status			Knox a	ttestation passed	
All		¢	All		\$			~		All		
lay Integrity attestatio	on passed		Safety	Net attestation	passed		Check Point Ha	rmony Mobile risk status		Conditi	onal access complian	ce
All		¢	All		\$		All	¢		All		
Platform			Manufa	acturer			Enrollment prog	jram	_ '	Kiosk r	node	
All		\$	All		\$			~		All		:
User	Device name	Mode	əl	OS version	Platform	7P	MDM version	Conditional access compl	iance	c Co	nditional access aut	henticated
beaverw, angryw	zebra	TC57		8.1.0	Android	6.0	8.04			No)	
do, do	S22	SM-S	901B	14	Android	6.1	3.00	Revoked		No)	
do, do	Pixel4	Pixel	4a	13	Android	6.1	3.00	Revoked		No		
wp, wp	TabA	SM-T	290	11	Android work profile	6.1	3.00	Revoked		No)	
wp, wp	S7				Android work profile					No		
wp, wp	Nokia8				Android work profile					No)	
wpco, wpco	Nokia81	Nokia	a 8.1	11	Android work profile	6.1	3.00	Revoked		No		
	Dive 17	Pixel	7a	14	Android work profile	6.1	3.00	Revoked		No)	

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.



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

	do at not										
Report type	Devices at ris	k (level 1/1, 5 dev	vices)								
MDM Clients	Schedule								Custom		
Trust certificates	Cohestula daia								alata 🔺 🔒		
Identity certificates	Schedule this								nski 👻		
Custom parameters	Search			Groups	Platform			Manufac	turer		
SIM Card				Select (0)	All		\$	All			
Conoral	Devices at risk		_	Ownership							
Service history	Not condition	al access compliant	-	All	Φ.						
Infrastructure	User	Device name	Model	Platform	Not conditional access compliant	ls jailbrok	Virus found	Not pass	Knox atte	Play Integ	
Configurations	do, do	Nokia81	Nokia 8.1	Android	Yes	No	No	No	No	Yes	
Certificates (infra)	do. do	Pix4	Pixel 4a	Android	Yes	No	No	No	No	Yes	
Applications (infra)	do do	S22	SM-S901B	Android	Yes	No	No	No	No	No	
Application list (infra)	wpco. wpco	Div7	Divol 7a	Android work profile	Vas	No	No	No	No	No	
Managed licenses	wpco, wpco	0.40	014.00705	Android work profile	165	NO	110	140	140	140	
(VPP)	wpco, wpco	\$10	SM-G970F	Android work profile	res	NO	NO	NO	NO	NO	
Monitoring											
Never connected											
Delayed											
Wiped											
Secure applications											
Devices at rick											
MDM Connection											
status											
010100											
Infected devices											

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.

Conditions	? >
Conditional access authenticated	~
No	~
Yes	
No	

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

- Yes
- No

conditions	? ×
Conditional access compliance	~
Undefined	~
Undefined	
Granted	
Revoked	
Unsupported	

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

- Undefined
- Granted
- Revoked
- Unsupported

ctions	- f
Send email	
Security	
Allow deactivation of device administrator (Knox Standard)	
Conditional Access: Request authentication	
Conditional access: Grant compliance	
Conditional access: Revoke compliance	
Deny deactivation of device administrator (Knox Standard)	
Disable work profile	
Enable work profile	
Lock	
SAG: Block	
SAG: Unblock	
Start Knox attestation	
Start Play Integrity attestation	
Start SafetyNet attestation	- 1
Unlock	
Other	
Create a report	
Delay (Android only)	
Install Antivirus license (Android only)	

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

View device					
S22					🗹 🧻 C
samsung, Android '	14, Device Owner	Mode, Corporate, Kr	10x 3.9		
Inventory	Details	Actions	History *	Installations -	
Action					0
Security					0
7P MDM act	ions				0
Remote supp	port				0
MDM Server	actions				٥
Security Acc	ess Gateway				
Block					
Conditional a	access compli	ance			
OC appaifu	actions				0

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 (<u>https://wiki.dmaas.de/index.php/Conditional_Access</u>).

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	
Conditio	ns:	4 matching devices +
All device	25	â
Condition	nal access compliance: Revoked	â
> No applie	cation from blacklist installed: B-L-K	â
Actions		+
Condition	nal access: Grant compliance	

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.

Custom risk1 \$ <mark>+ 126 6</mark>
risk1 🗢 🛨 🗹 🕯
risk1 💠 🕂 🗹 🖬
t is isilbroken/rooted
No

	Edit view ×	South sums (se)
k vices at risk (level 1/1, 5 devices) sobestule sobestule this arch vices at risk vices at risk vices at risk vices at risk so do 2022 SM-50018 Androd so, do 2021 SM-50018 Androd so, wpco Noka81 Nokis 8.1 Androd we spco, wpco Pisel7 Pisel 7a Androd we	Edit view × Priscus version Evences status Certificate valu until Manufacturer Check Point Harmony Mobile © Ownernabje device status Check Point Harmony Mobile © Search rick status Check Point Harmony Mobile © Search rick status Check Point Harmony Mobile © Search rick status Coretion date © Search rick status Device name © ED Email Envolkment URL Envolkment URL Envolkment token valid until Firmware Hits backstred URL Incode Is roaming Search Mab Search Last connection Last inventory update MAC address MDDM Status MDM Status	google-crim-3 (KA) + Eng Manufacturer All Mobile risk status Not conditional access compile Yes Yes Yes Yes Yes Yos

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.



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.

Lero Touch Enrollmen	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 approximation JSON string to Activation JSON string to	s enabled o be used in ZTE portal:

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.

8	Cancel Save without enrolling
Choose a platform	
	Onknown
Enrollment program	
None	,
Android enrollment type	
Device Owner Mode	
Leave all system apps enabled (Used in QR	code)
Ownership	
Corporate	· · · · · · · · · · · · · · · · · · ·
MDM ID	Device name
	Test-Device-1
Phone number	Email for enrollment
	recep.arsuzoglu@7p-group.com
Comment	Serial number
	<i>I</i>
Activation parameters	
Download URL	Activation PIN
1	
Samsung Knox Premium	
Do not activate	
Wi-Fi configuration	
access point - g	

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

IKARUS Security Software GmbH

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.

Home > Organization > Users at	nd devices > User: do do > Device: 522 > F	Actions		
Users and devices			View device	
Y Search in users	✓ Search	C	S22	B
Collapse	28 · · · · ·	O Expand	samsung, Android 14, Device Owner Mode, Corporate, Knox 3.9	
Username			Inventory Details Actions History - Installations -	
angryw beaverw		~ B	Action	
🗖 do do		^ B'		
Status Name	Model	Service status	Security	
Pixel4	Pixel 4a		Screen	
wp wp	01103010	~ 🗹	Lock Unlock	
wpco wpco		~ 2	Lost mode	
	001-		Play sound	
	CSV	Add user Add device	Davies	
	Are you sure you want to wipe the de	vice?	Neboli device Get GFS cooldinates Set boot aware behavior	
1	also erase the device's external storage (su	uch as SD cards)		
	also erase the factory reset protection data	a	7P MDM actions	
1	also erase the device's eUICC data		Remate suggest	
	I doubt a branches of a stability of the stability of		Remote support	

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)

		View device				
	• Expand	samsung, Android worl	k profile 12, Work Profile On Cor	mpany Owned, Corpor	rate, Knox 3.8	
	Copure	Inventory	Details Actions	History -	Installations *	
	~ 2	Action				•
Are you sure y	ou want to remove work profile? device's external storage (such as SD ca	× ards)			•	Send
Are you sure y	ou want to remove work profile? device's external storage (such as SD ca factory reset protection data	erds)			•	Send
Are you sure y	ou want to remove work profile? device's external storage (such as SD ca factory reset protection data ason for wiping to the user	x Irds)	rise work profile			Send
Are you sure y	ou want to remove work profile? device's external storage (such as SD ca factory reset protection data ason for wiping to the user	rds) Cancel OK	rise work profile	file Remove v	work profile Disable	Send 🗢

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.

All Android All iOS		Cancel	Save
General			
* Name:	Kiosk_Test_1	1	
Comment:			
Created:	2023-12-06 12	:52:53	
Modified:	2023-12-06 12	:52:53	
Show all:	~		
Hide empty:			
Main settings			
URL:	https://mdm.	7p-group.com/testmdmclient/7p-kiosk-	0 🕏
Background image:	O URL	O Uploaded file	0 👳
			0 🔅
Landscape background image:	O URL	O Uploaded file	@ 察
			@ 察
Allow multi-window mode:			0
Allow TaskManager:			0

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:

- 1. Options have been regrouped to be tied and displayed with the appropriate package platforms.
- 2. Options for different platforms are now separated and will not overwrite each other.
- 3. 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.
- 4. 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.
- 5. The application icon has been moved from "Details" to "Packages".

Application				
Details Pack	ages		ď	Î
Name	outloo	C		
Categories	APPRO	VED, officetools, System App	os	
Description				
				11.

opheation	
Details Package	s 🗹
📫 Android	4
Туре:	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 MAD plades usy Benjulity to the segmented on the see With pellulard.
Version:	4.2345.1
Minimum OS version:	9
Managed Google Play Store:	Undo approval
Approval:	Approved
Default configuration:	ootlookconfig1
Cost:	Free