techstep

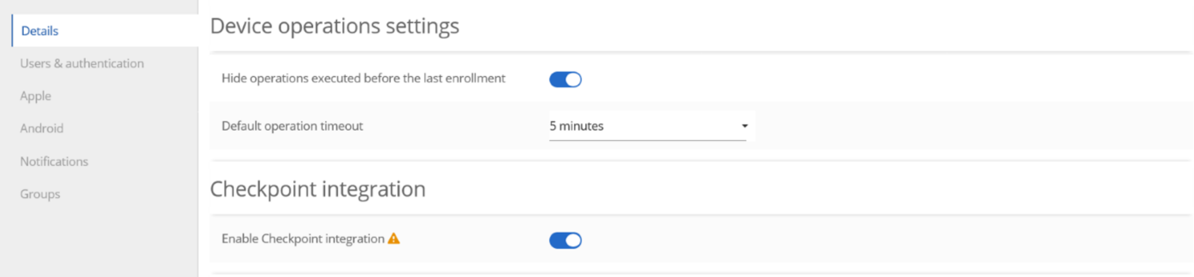
Integration with Checkpoint Harmony

Date: 11/04/2023

Check Point Harmony is the industry's first solution to unify device, user and remote access security.
It protects devices and Internet connection against the most sophisticated attacks, ensuring access to corporate applications in accordance with the principles of Zero Trust.
Essentials MDM allows the system to be integrated with the Check Point Harmony service, ensuring constant monitoring of devices to protect against potential threats.

Step 1

Activate Checkpoint integration in Essentials MDM.



Device operations settings

Hide operations executed before the last enrollment: on

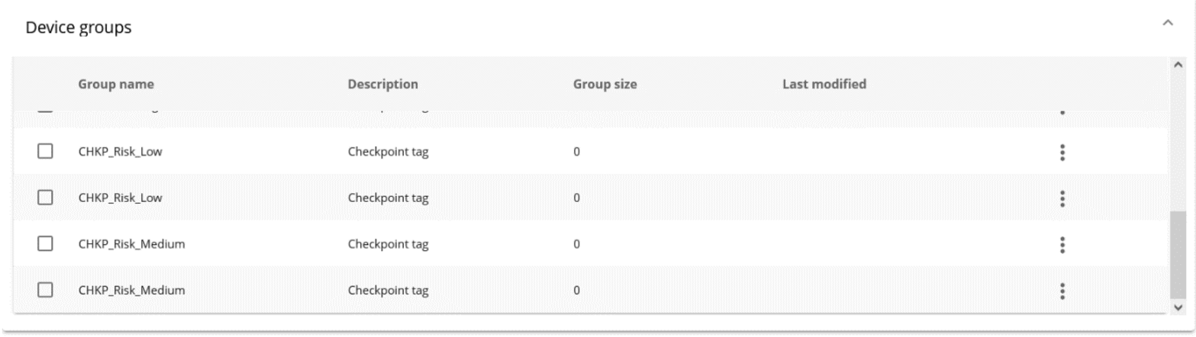
Default operation timeout: 5 minutes

Checkpoint integration

Enable Checkpoint integration ⚠: on

Step 2

After activation, the organization will automatically create groups corresponding to the Checkpoint threat levels and a role that gives access rights to webservices responsible for integration support.

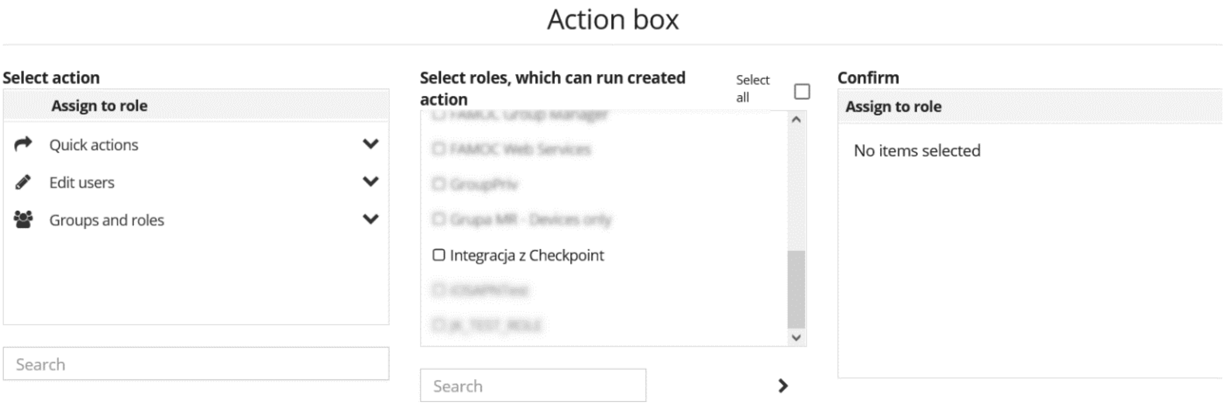


Device groups

	Group name	Description	Group size	Last modified	
□	CHKP_Risk_Low	Checkpoint tag	0		⋮
□	CHKP_Risk_Low	Checkpoint tag	0		⋮
□	CHKP_Risk_Medium	Checkpoint tag	0		⋮
□	CHKP_Risk_Medium	Checkpoint tag	0		⋮

Step 3

Then create a new user or give the existing user Checkpoint integration role.



Action box

Select action

Assign to role

Select roles, which can run created action

Select all □

[redacted]
[redacted]
[redacted]
[redacted]
□ Integracja z Checkpoint
[redacted]
[redacted]

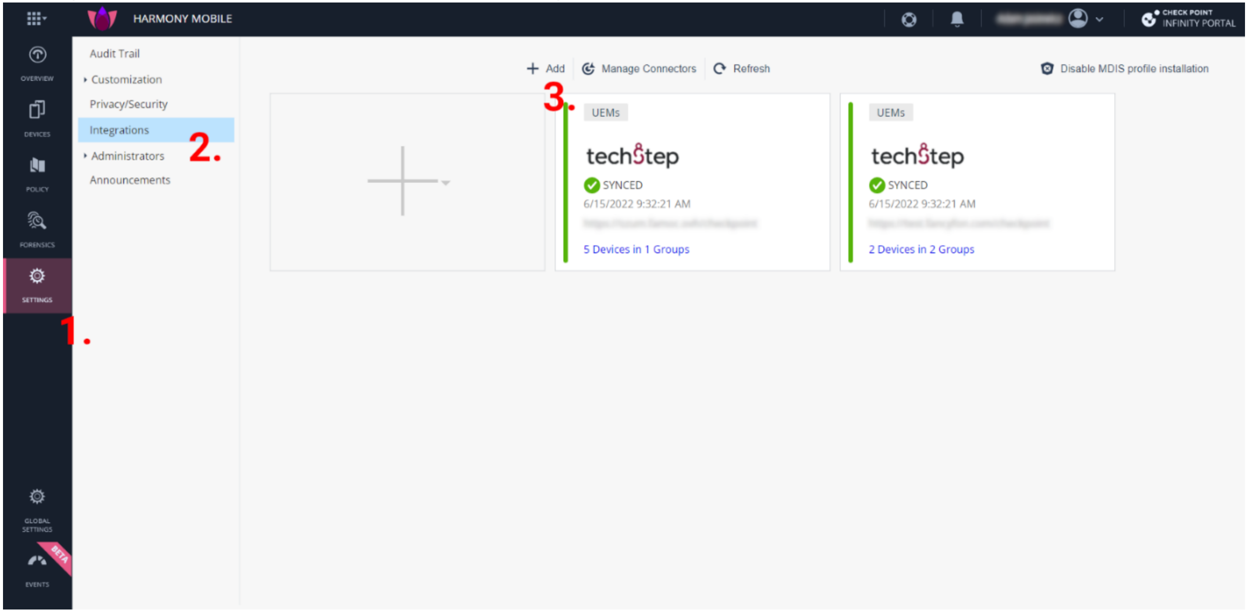
Confirm

Assign to role

No items selected

Step 4

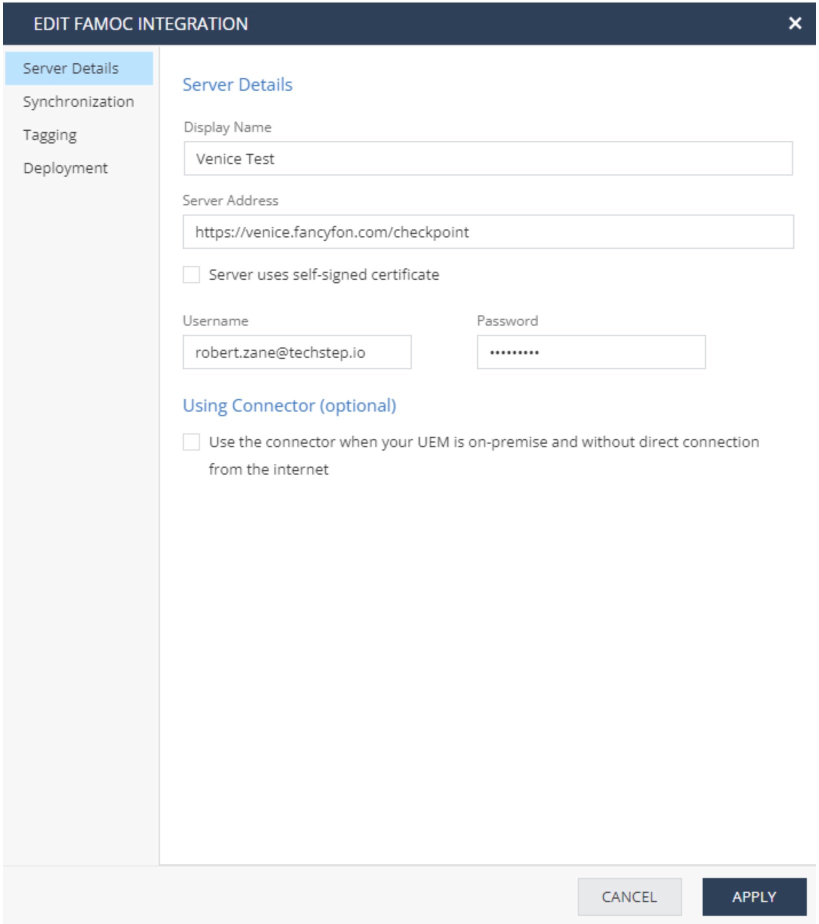
Then go to the Checkpoint portal, log in and go to settings (1.). Click Integrations (2.) and add new integration (3.).



SYNCED
6/15/2022 9:32:21 AM
[redacted]
5 Devices in 1 Groups

SYNCED
6/15/2022 9:32:21 AM
[redacted]
2 Devices in 2 Groups

Select Techstep from the list of UEMs and provide the URL of server and login and password of the user with the Checkpoint integration role. Then proceed with the next steps.



Server Details

Display Name: Venice Test

Server Address: https://venice.fancyfon.com/checkpoint

□ Server uses self-signed certificate

Username: robert.zane@techstep.io

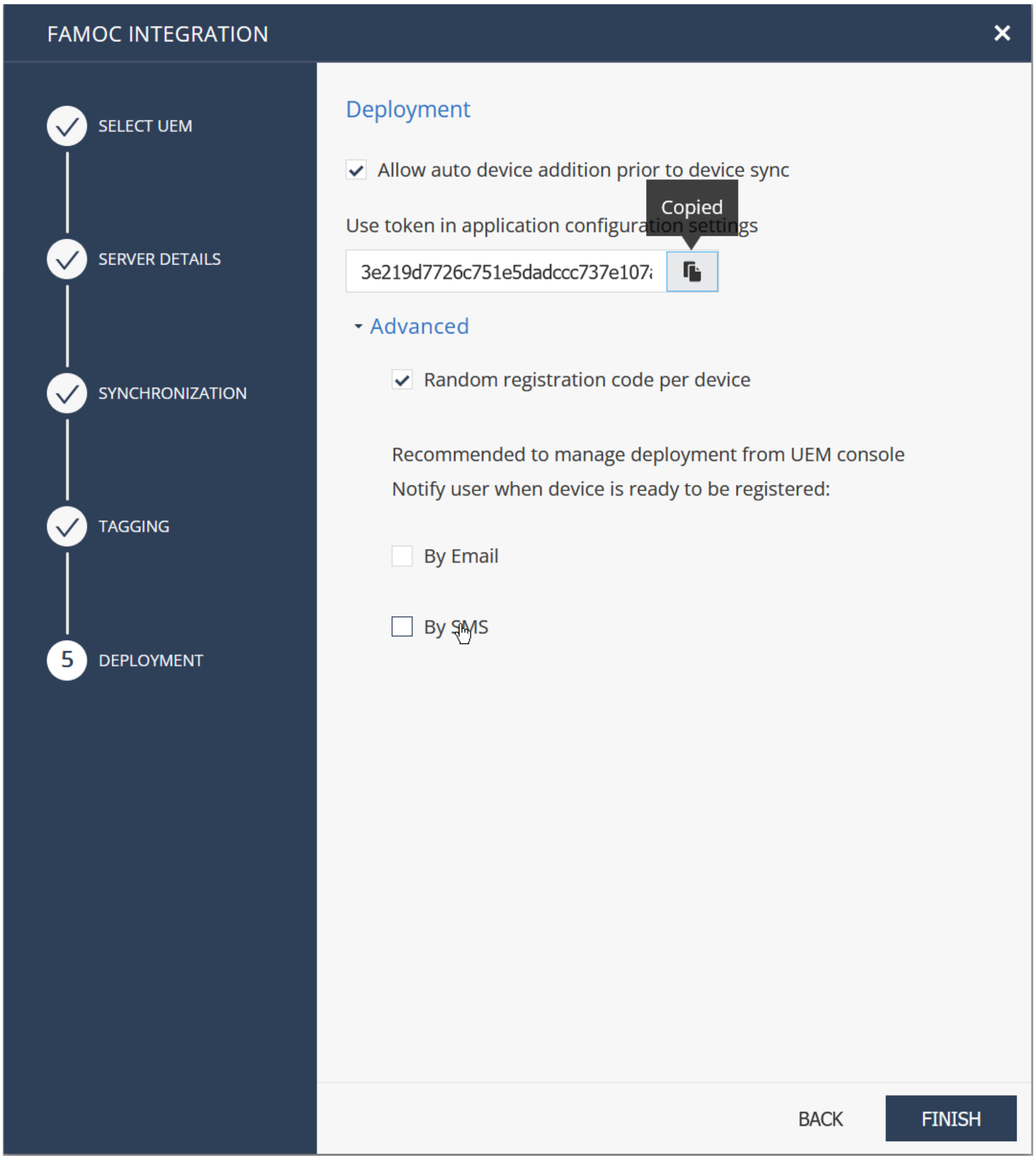
Password: •••••••••

Using Connector (optional)

□ Use the connector when your UEM is on-premise and without direct connection from the internet

Step 5

In the last step of integration, the generated token should be additionally copied. It will be needed to configure the application in the Essentials MDM console.



Deployment

☑ Allow auto device addition prior to device sync

Use token in application configuration settings

3e219d7726c751e5dadccc737e107

Advanced

☑ Random registration code per device

Recommended to manage deployment from UEM console

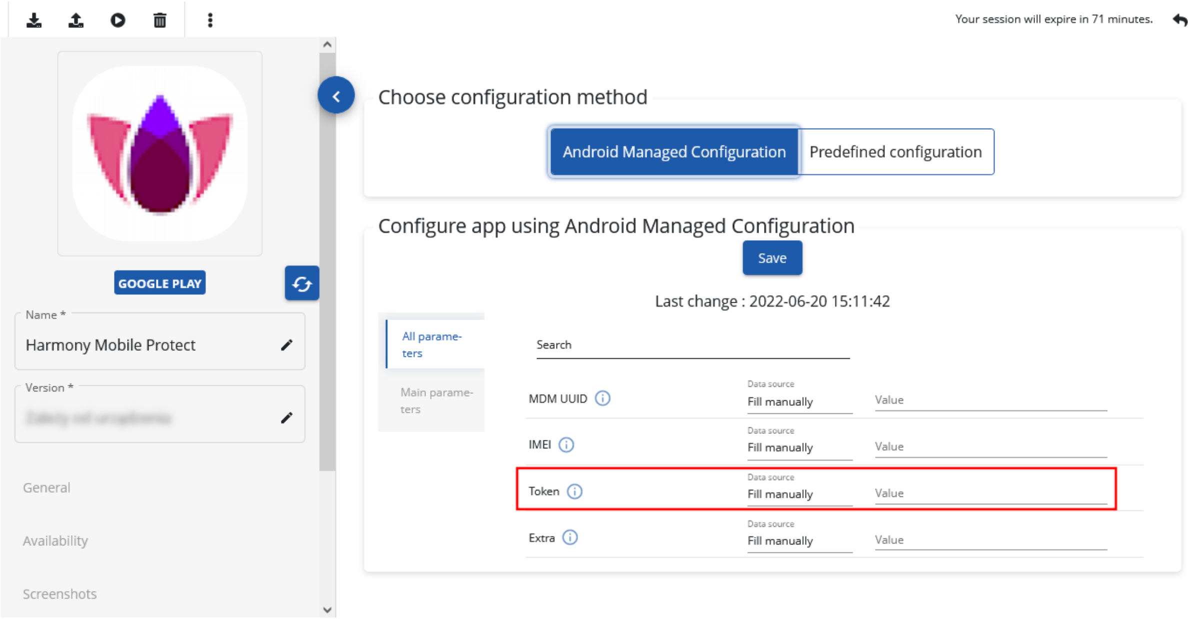
Notify user when device is ready to be registered:

□ By Email

□ By SMS

Step 6

Then add the Harmony Mobile Protect application from the Google Play store to the Essentials MDM system. After adding, go to the application details, then to the Configurations tab and edit the Android Managed Configuration. Paste the copied token in the appropriate field.



Your session will expire in 71 minutes.

GOOGLE PLAY

Name *
Harmony Mobile Protect

Version *
[redacted]

General

Availability

Screenshots

Choose configuration method

Android Managed Configuration | Predefined configuration

Configure app using Android Managed Configuration

Save

Last change : 2022-06-20 15:11:42

All parameters

Main parameters

Search

	Data source	
MDM UUID ⓘ	Fill manually	Value
IMEI ⓘ	Fill manually	Value
Token ⓘ	Fill manually	Value
Extra ⓘ	Fill manually	Value

Step 7

Finally, all you have to do is assign the groups created in Essentials MDM (they are based on the danger level set by Checkpoint Harmony) to the appropriate policies. If a potential threat is detected, devices will be automatically assigned to selected groups, and thus their policy will change (e.g. access to corporate networks will be limited for them to be quarantined).