



Techstep

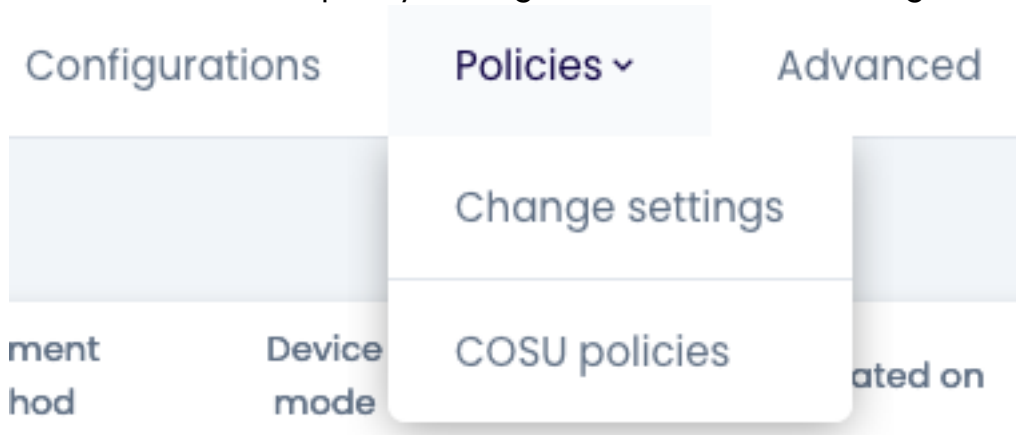
Essentials MDM

Installer policy

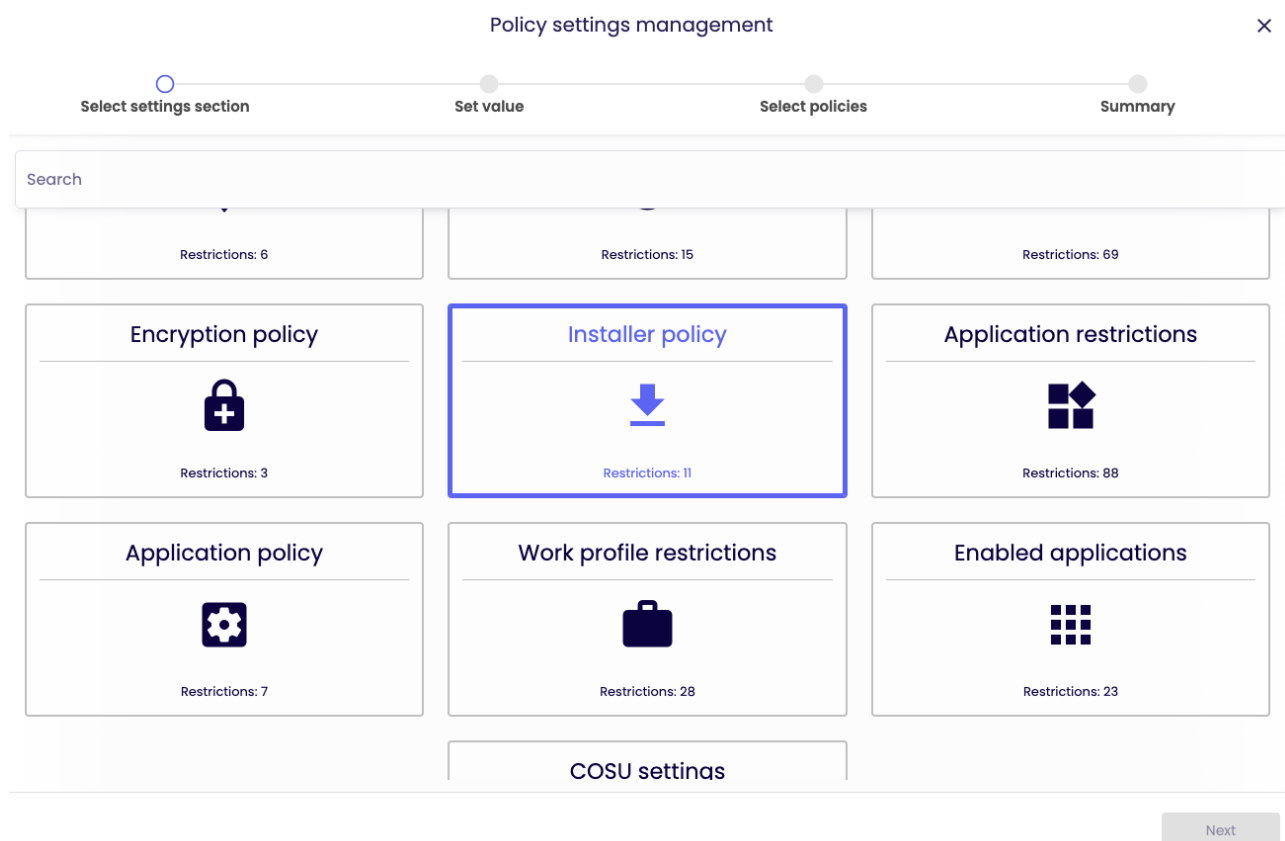
Date: 06/03/2023



To edit the Installer policy settings, click Policies -> Change Settings



Choose the Installer policy category



Within Installer policy there are several settings that you can add to your policies.

Policy settings management ×

Select settings section Set value Select policies Summary

Search

↓ Installer policy

- ☐ **Application installer lock** Fully managed BYOD/WPC COSU
- ☐ Notification when application installation is blocked (Application installer lock) Fully managed BYOD/WPC
- ☐ Allow USB debugging (Application installer lock) Fully managed COSU
- ☐ Unknown sources lock (Application installer lock) Fully managed BYOD/WPC COSU
- ☐ Disable application control (Application installer lock) Fully managed COSU
- ☐ Accounts creation using Google Play (Application installer lock) Fully managed BYOD/WPC COSU
- ☐ Allow USB debugging on Windows 10 Mobile devices Fully managed
- ☐ Unknown sources lock on Windows 10 Mobile devices Fully managed
- ☐ Manual installation of the root certificate lock Fully managed
- ☐ Disable the App Store Fully managed
restriction.desc-monitored.function331
- ☐ Prohibit the user from installing configuration profiles and certificates interactively Fully managed

[Back](#) [Next](#)

Choose the setting you want to configure and click next.

Below is a table of all the settings you can configure within this category with an explanation.

Parameter	Value	Compatibility
General Settings		
Application installer lock	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed COSU BYOD/WPC
Notification when application installation is blocked (Application installer lock)	Possible options: Enter text for notification	Fully Managed BYOD/WPC
Allow USB debugging (Application installer lock)	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed COSU
Unknow sources lock (Application installer lock)	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed COSU BYOD/WPC

Disable application control (Application installer lock)	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed COSU
Accounts creation using Google Play (Application installer lock)	Possible options: <input type="radio"/> Enabled or disabled Default value: Enabled	Fully Managed COSU BYOD/WPC
Allow USB debugging on Windows 10 Mobile devices	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed
Unknown sources lock on Windows 10 Mobile devices	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed
Manual installation of the root certificate lock	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed
Disable the App Store	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed
Prohibit the user from installing configuration profiles and certificates interactively	Possible options: <input type="radio"/> Yes or no Default value: No	Fully Managed

Configure the setting to the wanted value and click next.

Policy settings management

×

Select settings section

Set value

Select policies

Summary

↓ Installer policy

Prohibit the user from installing configuration profiles and certificates interactively:

☒ Yes

Back

Next

Select the policies you want to add the setting to (You can choose multiple policies) and click next.

Policy settings management

×

●

Select settings section

●

Set value

○

Select policies

●

Summary

Prohibit the user from installing configuration profiles and certificates interactively: Yes

2

✓

Search

1 – 10 of 10

|<

<

>

>|

Policy name	Policy mode	Affected devices count	Is default	User Groups	Device groups
<input checked="" type="checkbox"/> Default policy	Fully managed	0	Yes		
<input checked="" type="checkbox"/> TS Kiosk mode	Fully managed	0	No		Kiosk Devices
<input type="checkbox"/> Ssavers Norway	Fully managed	0	No		Specsavers
<input type="checkbox"/> Apple_KioskDevice	Fully managed	0	No	OUS Renhold	Apple_FunctionDevice
<input type="checkbox"/> RetailDemo	Fully managed	0	No		RetailX Techstep Test
<input type="checkbox"/> Lovisenberg	Fully managed	0	No	Lovisenberg	
<input type="checkbox"/> Ascom Myco	Fully managed	0	No	Ascom	Ascom Myco 3
<input type="checkbox"/> LDS-Telefonkiosk-std	Fully managed	0	No	LDS-Telefonkiosk-std	LDS-Telefonkiosk-std
<input type="checkbox"/> Meny	Fully managed	0	No	Meny	DG_Meny

Back

Next

You will then be showed a summary of your applied settings and if there are devices affected by the change.

Click Apply to set your configuration change into effect.

Note: When pressing apply, the settings will be applied on the affected devices immediately.

Policy settings management

×

●

●

●

○

Select settings section

Set value

Select policies

Summary

Summary:

Number of selected policies: 2

Number of affected devices: 0

Settings:

Prohibit the user from installing configuration profiles and certificates interactively: Yes

Back

Apply