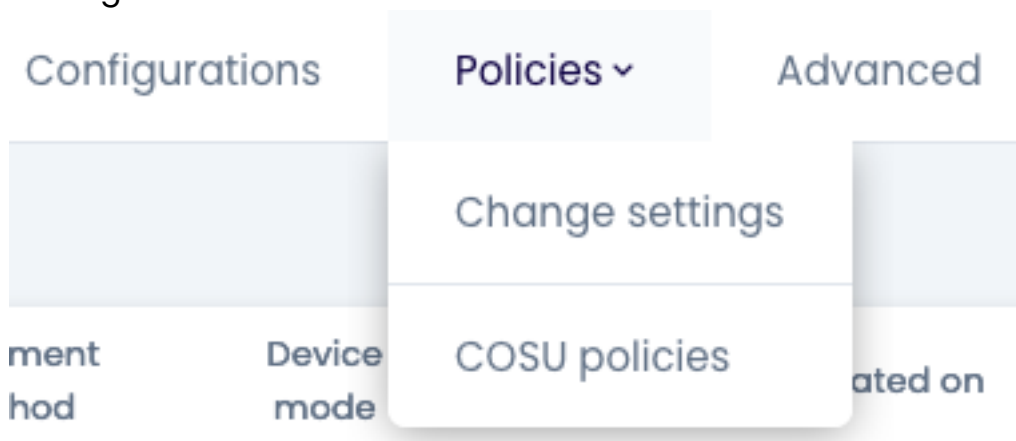# techstep

Techstep Essentials MDM

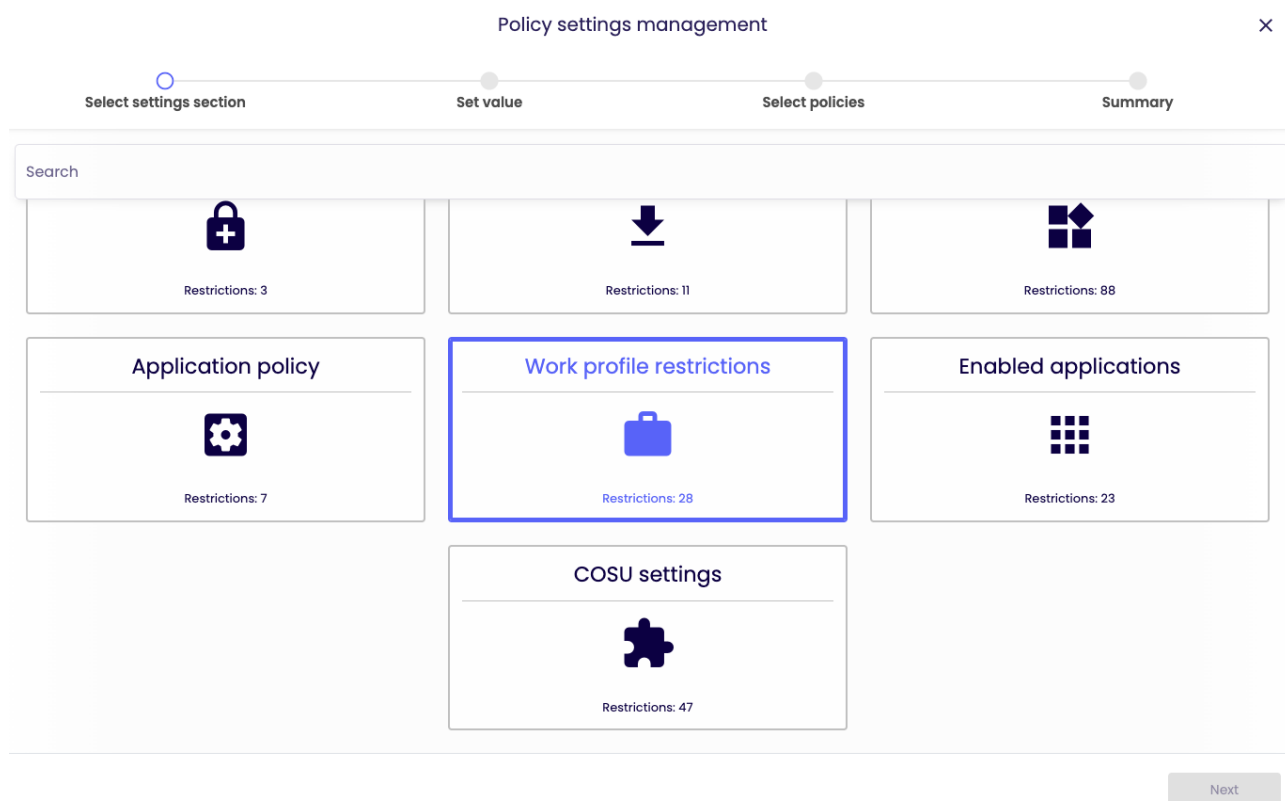## Work profile restrictions

Date: 16/03/2023

To edit the Work profile restrictions policy settings, click Policies -> Change Settings

Configurations   Policies ⌄   Advanced

Change settings

COSU policies

ment   Device   ated on
hod   mode

Choose the Work profile restrictions policy category

Policy settings management   ✕

○──────────────●──────────────●──────────────●
Select settings section   Set value   Select policies   Summary

Search

🔒
Restrictions: 3

⬇
Restrictions: 11

🔳
Restrictions: 88

Application policy
⚙
Restrictions: 7

Work profile restrictions
💼
Restrictions: 28

Enabled applications
⊞
Restrictions: 23

COSU settings
🧩
Restrictions: 47

Next

Within Work profile restrictions policy there are several settings that you can add to your policies.

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. In fully managed policy options are available only when policy has work profile defined (old COPE setup).

Parameter	Value	Compatibility
General Settings		
Enable unknown sources	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block screen capture	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Disable accounts modification	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block creation of the mail account (Disable account modification)	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block creation of LDAP account (Disable account modification)	Possible options: o Yes or no	Fully Managed BYOD/WPC

	Default value: No	
Block creation of Samsung account (Disable account modification)	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Accounts creation using Google Play	Possible options: o Enabled or disabled Default value: Enabled	Fully Managed
Disable camera	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Disable cross profile copy-paste	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Disable application control	Possible options: o Yes or no Default value: No (The following user actions will be denied when this restriction is enabled: apps uninstalling, disabling apps, clearing app caches, clearing app data, force stopping apps and clearing app defaults).	Fully Managed BYOD/WPC
Disable one lock code	Possible options: o Yes or no Default value: No (In order to disable active one lock code, Settings for work profile lock code configuration should be applied before).	Fully Managed BYOD/WPC
Allow moving apps to work profile	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block NFC	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Disallow outgoing beam using NFC (Block NFC)	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Allow moving files from device to work profile	Possible options: o Yes or no	Fully Managed BYOD/WPC

	Default value: No	
Allow moving files from work profile to device	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block change of the sharing of the calendar to the personal mode	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Block change of the sharing of the calendar to work profile	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Enable Bluetooth	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Enable file sharing via Bluetooth in work profile (Enable Bluetooth)	Possible options: o Yes or no Default value: No	BYOD/WPC
Block Share Via List	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Prevent users from configuring credentials in the managed keystore	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Maximum time the work profile is allowed to be turned off	Possible options: o Disabled o 3, 4, 5 or 6 days Default value: Disabled (The minimum value is 3 days)	Fully Managed BYOD/WPC
Enable the ability to restore of the backup from the Google account	Possible options: o Yes or no Default value: No	Fully Managed BYOD/WPC
Disable location config	Possible options: o Yes or no Default value: No	BYOD/WPC
Disable location sharing	Possible options: o Yes or no Default value: No	BYOD/WPC
Disable content capture	Possible options: o Yes or no Default value: No	BYOD/WPC
Disable content suggestions	Possible options: o Yes or no	BYOD/WPC

techstep

	Default value: No	

Configure the setting to the wanted value and click next.

Policy settings management   ✕

●━━━━━━━━━━○━━━━━━━━━━●━━━━━━━━━━●
Select settings section   Set value   Select policies   Summary

💼 **Work profile restrictions**

Block screen capture:

⬤ No

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

Block screen capture: No

🔍 Search   1 – 3 of 3 |< < > >|

	Policy name	Policy mode	Affected devices count	Is default	User Groups	Device groups
☑	Default BYOD/WPC policy	BYOD/WPC	3	Yes		
☐	Default shared device policy	Shared device	0	Yes		
☑	Test WPC Ricardp	BYOD/WPC	0	No	Test WPC Ricardo	

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: 3

Settings:

Block screen capture: No

⚠ Changes in the selected policies will affect some devices. Make sure it's intended.

Back   Apply