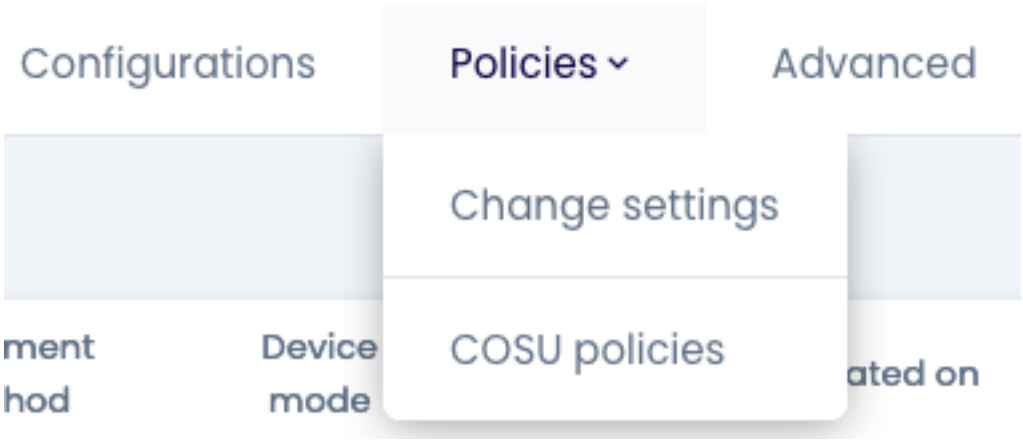
techstep

Techstep Essentials MDM

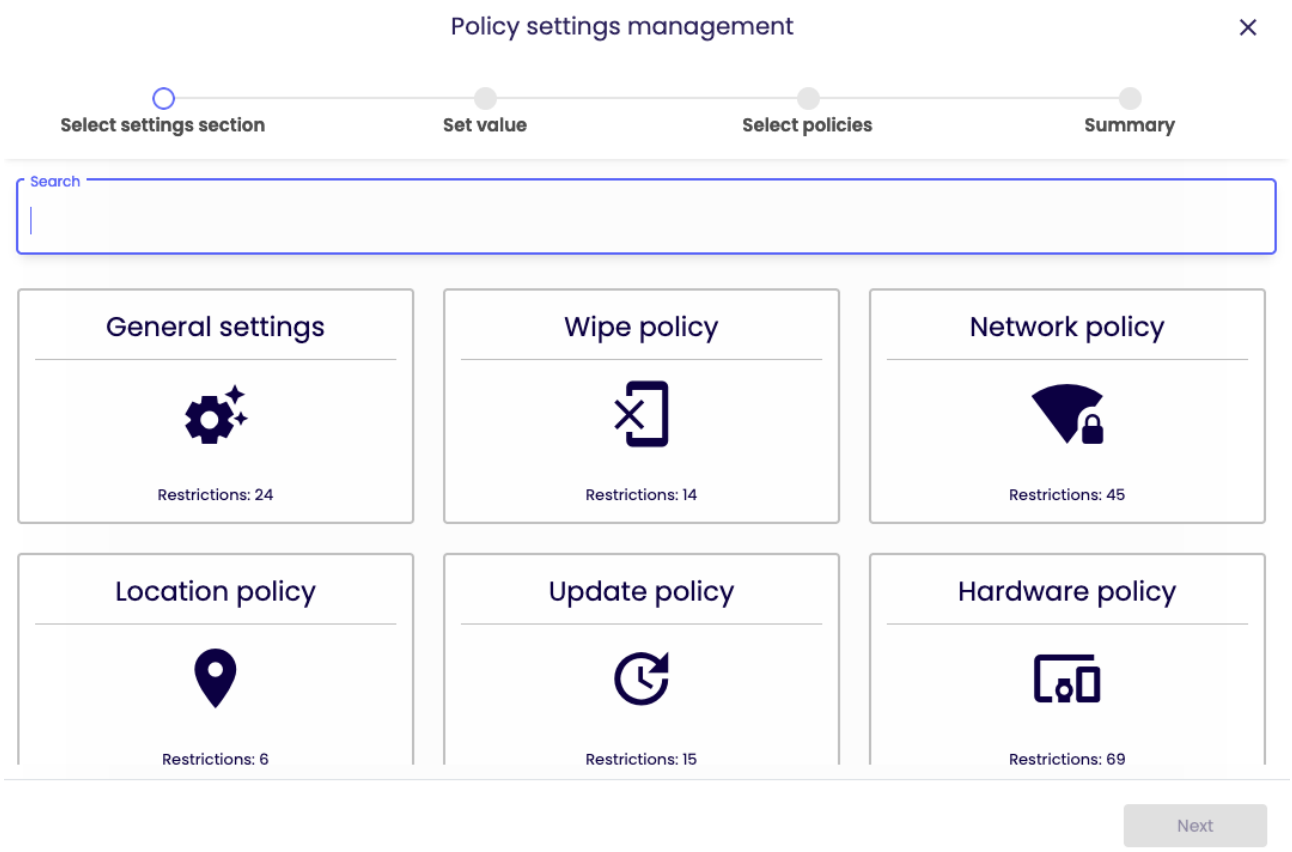
Network policy

Date: 23/11/2023

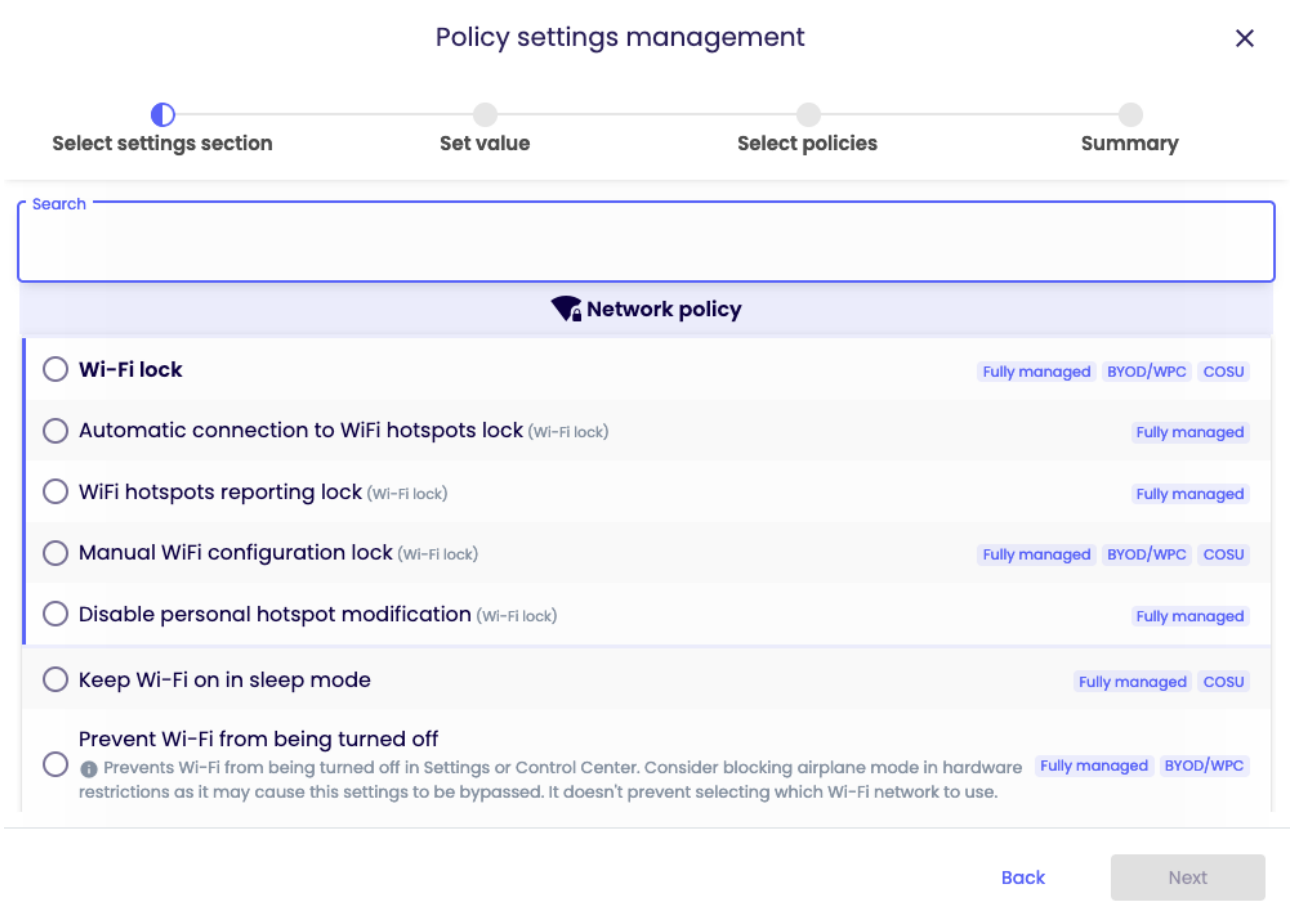
To edit the wipe Network policies click Policies -> Change Settings



Choose the Wipe policy category



Within Network policies there are several settings that you can add to your policyset.



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	Explanation	Compatibility
General Settings		
Wi-Fi lock	If set, Wi-Fi cannot be used on the device. Availability: Android and Windows Phone 8.1 / 10 devices	Fully Managed COSU BYOD/WPC
Automatic connection to Wifi hotspots lock	If set, the device will not connect automatically to the WiFi hotspots. Availability: Windows Phone 8.1 / 10	Fully Managed
Wifi hotspots reporting lock	If set, the device will not report WiFi hotspots. Availability: Windows Phone 8.1	Fully Managed
Manual wifi configuration lock	If set, there will be no possibility to configure WiFi connection manually. Availability: Device Owner, iOS devices in the Supervised mode, Windows Phone 8.1/10	Fully Managed COSU BYOD/WPC

Disable personal hotspot modification		Fully Managed
Keep wifi on in sleep mode		Fully Managed COSU
Prevent wifi from being turned off		Fully Managed BYOD/WPC
Bluetooth lock	If set, Bluetooth cannot be used on the device. Availability: Android, Windows Phone 8.1/10, iOS 11.3 and above in Supervised mode Possible options available for Android Samsung with Enterprise SDK from 2.0: • Enable Advanced Audio Distribution Profile (A2DP) • Enable Audio/Video Remote Control Profile (AVRCP) - when this profile is enabled with (A2DP) user will be able to use Media Audio connection additionally user will be able to use buttons on bluetooth device(Play/Stop/Next song). • Enable HandsFree Profile (HFP) - this profile works only with HSP profile. • Enable Headset Profile (HSP) - when this profile is enabled with (HFP) user will be able to use Call Audio connection additionally user will be able to use buttons on bluetooth device(Answer or terminate the call) • Enable Phone Book Access Profile (PBAP) - when this profile is enabled bluetooth device will have access to contacts saved on the phone or tablet. • Enable Serial Port Profile (SPP) - this profile needs to be selected for proper wireless connection between devices • Enable file sharing via Bluetooth	Fully Managed COSU BYOD/WPC

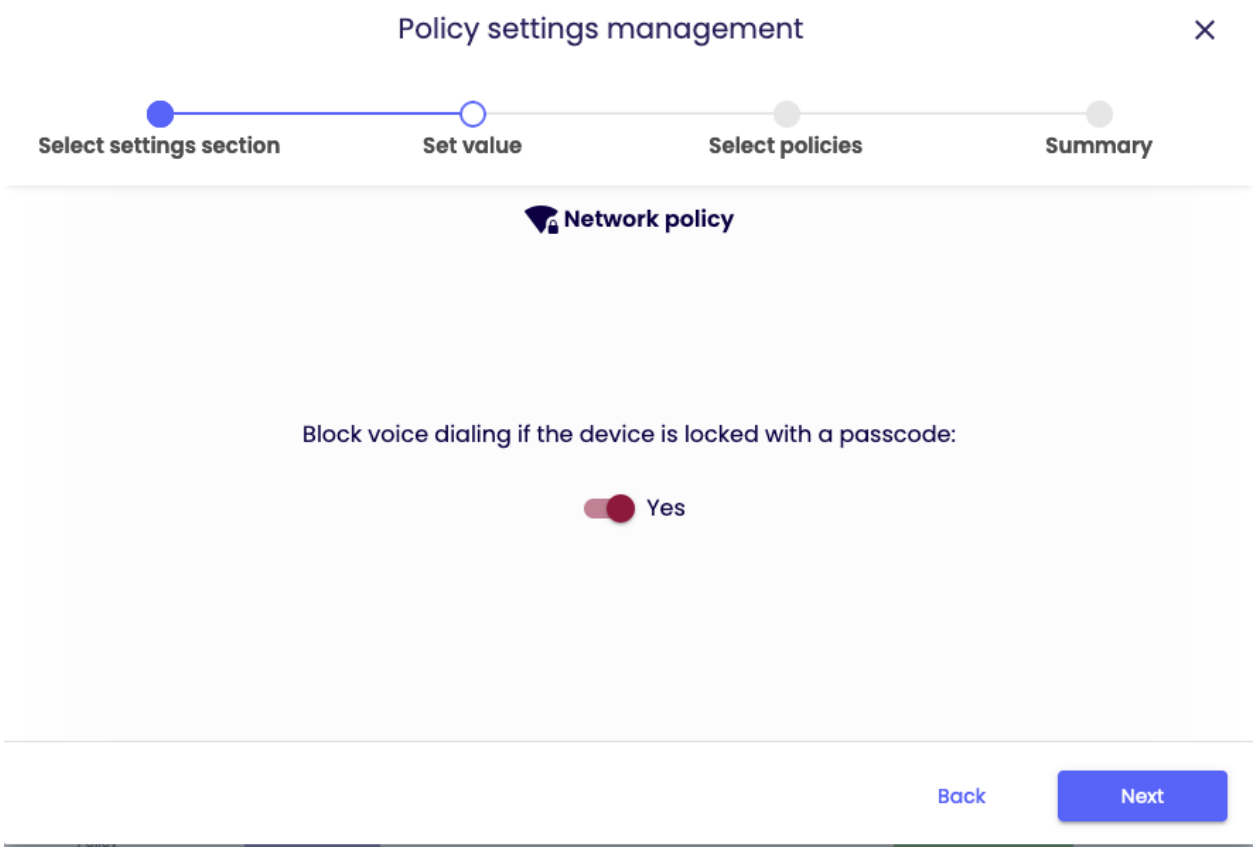
Enable Advanced Audio Distribution Profile (A2DP)		Fully Managed
Enable audio/Video Remote Control Profile (AVRCP)		Fully Managed
Enable HandsFree profile (HFP)		Fully Managed
Enable Headset profile (HSP)		Fully Managed
Enable Phone Book Access Profile (PBAP)		Fully Managed
Enable Serial Port Profile (SPP)		Fully Managed
Enable file sharing via Bluetooth		Fully Managed
Cellular data lock	Possible options: • Do not lock • Enable and block possibility to disable • Disable and block possibility to enable Availability: Android 4.x or better	Fully Managed COSU
Cellular datalock in roaming	Possible options: • Do not lock • Disable and block possibility to enable Availability: Android, Device Owner and Windows Phone 8.1/10 devices Default value: Do not lock.	Fully Managed COSU BYOD/WPC
Disable cellular plan modification		Fully Managed
Wifi tethering lock	If set, WiFi tethering is disabled. Availability: Android Samsung with Enterprise SDK from 2.0 and Device Owner	Fully Managed COSU
USB tethering lock	If set, USB tethering is disabled. Availability: Android Samsung with Enterprise SDK from 3.0, Device Owner and Windows Phone 8.1/10	Fully Managed COSU
VPN over cellular lock	If set, VPN cannot be used over cellular data. Availability: Windows Phone 8.1/10	Fully Managed
Device usage report to Microsoft block	If set, usage report sending to Microsoft is disabled. Availability: Windows Phone 8.1/10	Fully Managed
VPN over cellular in roaming lock	If set, VPN cannot be used over cellular data in roaming Availability: Windows Phone 8.1/10	Fully Managed
Disallow the creation of VPN configurations	If set, user cannot configure VPN settings. Available from iOS 11.0	Fully Managed

Block incoming MMS	If set, incoming MMS won't be delivered Availability: Android Samsung with Enterprise SDK from 3.0	Fully Managed COSU
Disable Network Settings Reset	If set, the 'Reset network settings' option won't be available Availability: Device Owner	Fully Managed COSU
Disable VPN settings	If set, the VPN settings can not be modified by the user.	Fully Managed COSU BYOD/WPC
Disable eSIM settings modification	If set, user cannot modify eSIM settings. Available from iOS 12.1	Fully Managed
Block private DNS settings	If set, user cannot modify private DNS settings.	Fully Managed COSU
Block outgoing calls	If set, the user will not be able to make outgoing calls on the device.	Fully Managed BYOD/WPC
Block incoming calls	If set, the user will not be able to receive incoming calls on the device.	
Pattern of blocked numbers (Block incoming calls)	If set, the administrator can block incoming calls from certain telephonenumber patterns. 820.* will block incoming calls from all numbers starting with 820. 820 [0-9]{7}$).* will block incoming calls from numbers starting with 820 and contains 7 digits.	Fully Managed COSU
Block incoming SMS messages	If set, the user will not be able to receive SMS messages to the device.	Fully Managed COSU
Pattern of blocked numbers (Block incoming SMS messages)	If set, the administrator can block incoming SMS from certain telephonenumber patterns. 820.* will block SMS from all numbers starting with 820. 820 [0-9]{7}$).* will block all SMS from numbers starting with 820 and contains 7 digits.	Fully Managed COSU

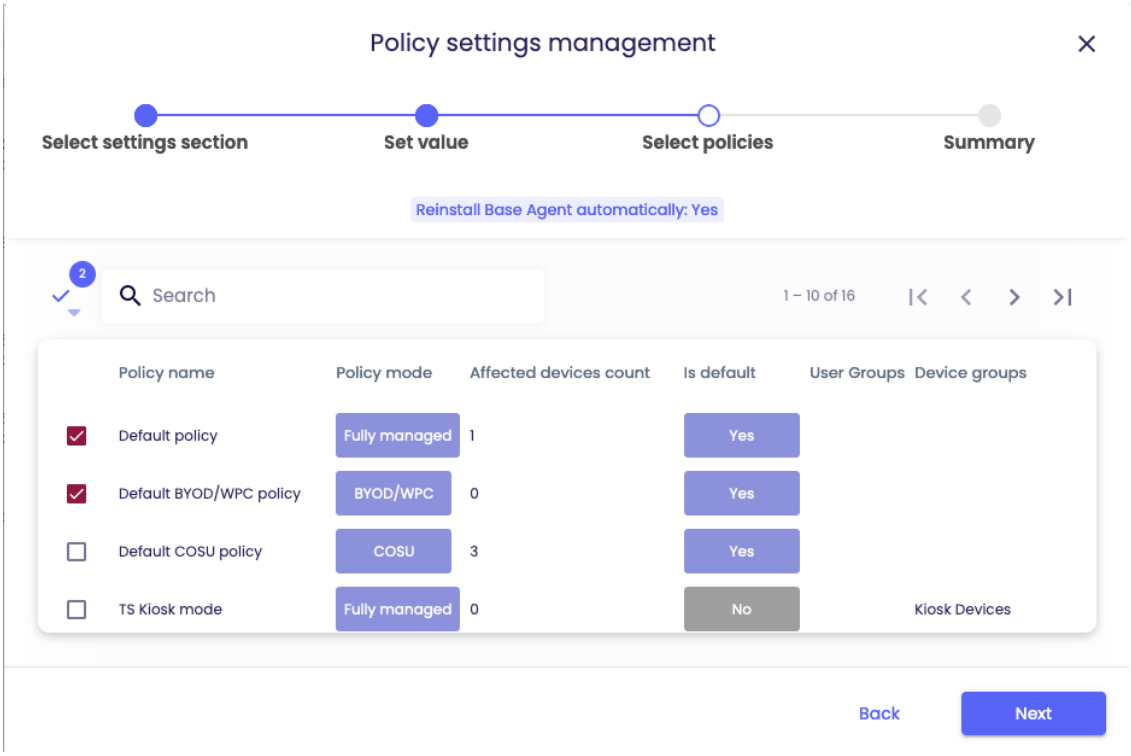
Disable managed networks settings change	If set, the user is not able to edit a wifi configuration that has been set by the Essentials MDM server.	Fully Managed BYOD/WPC
Monitor list of the managed Wifi configurations	If set, the administrator can see connection data about managed wifi config. Information like Acces point display name, Access point IP, Access Point MAC address and if the access point is currently in use or not	Fully Managed COSU BYOD/WPC
Block global background fetch when roaming	If set, apps can not fetch data in the background while the device is roaming.	Fully Managed
Block voice dialing if the device is locked with a passcode	If set, the user can not use voice dialing if the device is locked with a passcode.	Fully Managed
Disable apps cellular data modification	If set, the user can not modify apps data usage coniguration	Fully Managed
Disable host pairing	If set the device is unable to pair with any host computer	Fully Managed
Block Bluetooth config	If set, the Bluetooth config will be unavailable on the device	Fully Managed BYOD/WPC
Block tethering config	If set, the user will be unable to configure tethering on the device.	BYOD/WPC
Block mobile networks config	If set, it will not be possible to configure mobile settings on the device.	Fully Managed BYOD/WPC
Block cell broadcast config	If set, it will not be possible to configure cell broadcast on the device.	Fully Managed BYOD/WPC
Disable SMS messages	If set, SMS messages will be disabled.	Fully Managed BYOD/WPC
Disallow Ultra-Wideband (UWB)	When set, Settings → Connected devices → Connection preferences → Ultra-wideband(UWB) option on the device will be turned off Available from Android 14	Fully Managed, WPC, COSU (Not BYOD)

Disallow cellular 2G	When 'Disallow cellular 2G' option is enabled in COBO/WPC/COSU policy 'Allow 2G' option is blocked on the device Available from Android 14	Fully Managed, WPC, COSU (Not BYOD)

Configure the setting to the wanted value and click next.



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