



# Techstep

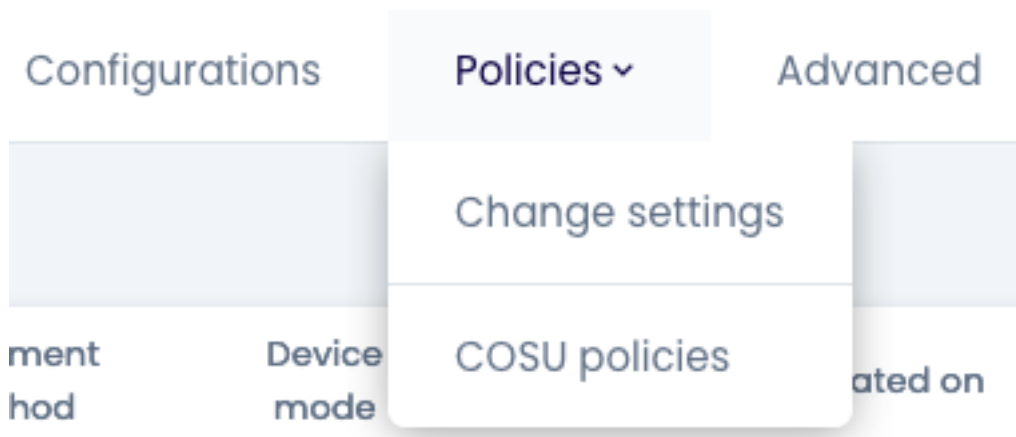
## Essentials MDM

### General policy settings

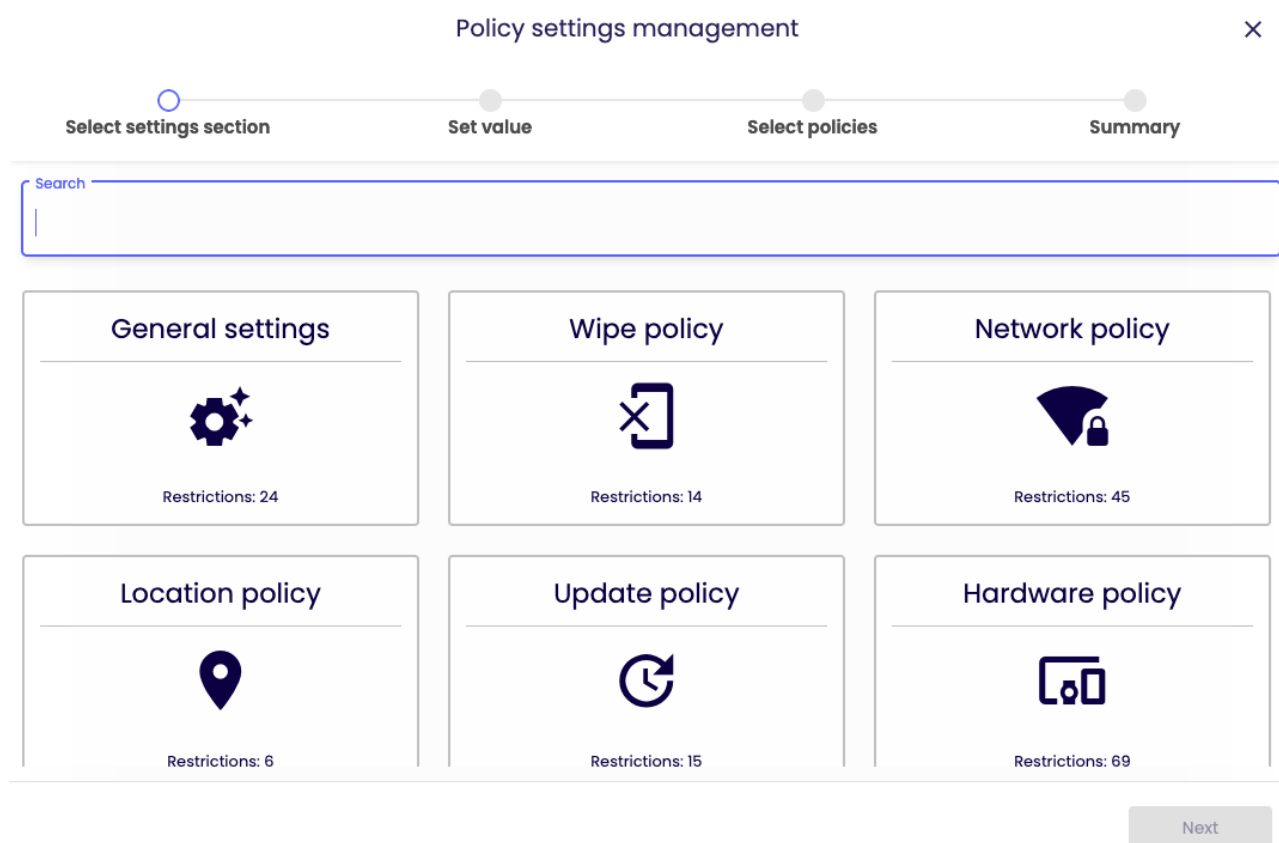
Date: 01/03/2023



To edit the general policy settings click Policies -> Change Settings



Choose the General Settings category



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

Policy settings management ×

Select settings sectionSet valueSelect policiesSummary

Search

General settings

☐ Reinstall Base Agent automaticallyFully managedBYOD/WPCCOSUShared device

☐ Uninstall not compatible policy components automaticallyFully managedBYOD/WPCCOSUShared device

☐ Mark as wiped on Base Agent uninstallationFully managedBYOD/WPCCOSUShared device

☐ **Enable remote access**Fully managedBYOD/WPCCOSU

☐ Remote Access session initialization consent (Enable remote access)Fully managedBYOD/WPCCOSU

☐ **Enable location monitor**Fully managedBYOD/WPCCOSU

☐ Location interval (Enable location monitor)Fully managedBYOD/WPCCOSU

☐ Location report only on peak (Enable location monitor)Fully managedBYOD/WPCCOSU

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	Explanation	Compatibility
General Settings		
<b>Reinstall Base Agent automatically</b>	When new Base Agent version appears in the system, it will be automatically reinstalled on devices (policy will be set as outdated). Default value: not checked.	Fully Managed BYOD/WPC COSU Shared Device
<b>Uninstall not compatible policy components automatically</b>	If set, not matching policy components from current policy will be uninstalled if device will be moved to other policy. Default value: not checked.	Fully Managed BYOD/WPC COSU Shared Device

<b>Mark as wiped on Base Agent uninstallation</b>	If set, the device will be marked as wiped in the Essentials MDM console if Base Agent is uninstalled.	Fully Managed BYOD/WPC COSU Shared Device
<b>Enable remote access</b>	If this option is marked, Remote Access will be installed with the policy.	Fully Managed BYOD/WPC COSU
<b>Remote Access session initialization consent (Enable remote access)</b>	Configure how to connect to a device for remote control. Chooses if the connection is going to be automatic or the user has to accept an admin to connect to the device.	Fully Managed BYOD/WPC COSU
<b>Enable location monitor</b>	If this option is marked, Location Monitor will be installed with the policy.	Fully Managed BYOD/WPC COSU
<b>Location Interval (Enable location monitor)</b>	Select how often the device should report its location to the Essentials MDM server.	Fully Managed BYOD/WPC COSU
<b>Location report only on peak (Enable location monitor)</b>	If Peak schedule interval is configured, the device can be configured to report location data only during the configured interval.	Fully Managed BYOD/WPC COSU
<b>Disable location reporting after agent installation (Enable location monitor)</b>	The device will stop reporting location services when the agent is reported installed on the device.	Fully Managed BYOD/WPC COSU
<b>Force the app monitor service to turn on</b>	When set, an additional operation included in the general policy, called "Enable app monitor service", will be added to the queue and sent to the device asking the user to turn the Essentials MDM Accessibility Service on.	Fully Managed
<b>Ignore battery optimization for Location monitor and Usage monitor (Selecting this option sends an operation that requires user confirmation)</b>	If battery optimization is activated on the device, this setting will make sure that location services are not stopped to save battery.	Fully Managed BYOD/WPC

<b>Report additional data about apps (app, size, cache size, data size. (This option requires the Usage Access Permission to be enabled))</b>	You will see additional information about apps installed on the device on the Essentials MDM admin console	Fully Managed BYOD/WPC COSU
<b>Reported applications (Available for iOS devices)</b>	Choose if the device should report all applications (Including user installed apps) or just applications installed by Essentials MDM	Fully Managed BYOD/WPC COSU Shared Device
<b>Peak schedule interval</b>	The interval of Base Agent server connection: 5 min./15 min./30 min. /1h/4h/12h/Once a day/Once a week/Once a month Default value: Once a day	Fully Managed BYOD/WPC COSU Shared Device
<b>Peak days (Peak schedule interval)</b>	Days of week during which Base Agent reports to Essentials MDM server Default value: Monday - Friday	Fully Managed BYOD/WPC COSU Shared Device
<b>Peak begin (Peak schedule interval)</b>	What time during peak days should Base Agent start reporting Default value: 8:00	Fully Managed BYOD/WPC COSU Shared Device
<b>Peak end (Peak schedule interval)</b>	What time during peak days should Base Agent stop reporting Default value: 16:00	Fully Managed BYOD/WPC COSU Shared Device
<b>Device monitor sessions interval</b>	Sets the interval of Device Monitor sessions: Off/Hourly/4 times a day/Daily/Weekly/Monthly Default value: Daily	Fully Managed BYOD/WPC COSU Shared Device
<b>Alerting device inactivity</b>	Alerting inactivity of the Base Agent after: 1-5 days/Week/Month/3 months. In case Base Agent doesn't	Fully Managed BYOD/WPC COSU Shared Device

	<p>report to server within this period, Essentials MDM generates an alert with three possible reaction options:</p> <ul style="list-style-type: none"> <li>• Remove device from Essentials MDM</li> <li>• Reinstall Base Agent</li> <li>• Mark device as stolen</li> </ul> <p>Default value: After week</p>	
<b>Wipe on exceeded device inactivity (Alerting device inactivity)</b>	If this option is marked and Base Agent doesn't report to server within a specified period of time, in addition to generated alert, the device will be wiped.	Fully Managed BYOD/WPC COSU Shared Device
<b>Mark as wiped on exceeded device inactivity. (Alerting device inactivity)</b>	If set, the device will be marked as wiped in the Essentials MDM console if it exceeds device inactivity period.	Fully Managed BYOD/WPC COSU Shared Device
<b>Confirmation mode for Base Agent</b>	Choose how/if information should be prompted to the user on the device.	Fully Managed
<b>Device monitor sessions stored count</b>	Configure how often the device should send information to the Essentials MDM server.	Fully Managed BYOD/WPC COSU Shared Device
<b>Archived device monitor sessions count</b>	Configure how many of the monitor sessions should be stored to be able to review on the server.	Fully Managed BYOD/WPC COSU Shared Device

Configure the setting to the wanted value and click next.

Policy settings management

Select settings section

Set value

Select policies

Summary

General settings

Reinstall Base Agent automatically:

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

Reinstall Base Agent automatically: Yes

2

Q Search

1 – 10 of 16

	Policy name	Policy mode	Affected devices count	Is default	User Groups	Device groups
<input checked="" type="checkbox"/>	Default policy	Fully managed	1	<div>Yes</div>		
<input checked="" type="checkbox"/>	Default BYOD/WPC policy	BYOD/WPC	0	<div>Yes</div>		
<input type="checkbox"/>	Default COSU policy	COSU	3	<div>Yes</div>		
<input type="checkbox"/>	TS Kiosk mode	Fully managed	0	<div>No</div>		Kiosk Devices

Back

Next

You will be 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: 1

Settings:

Reinstall Base Agent automatically: Yes

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

Back

Apply