



Techstep

Essentials MDM

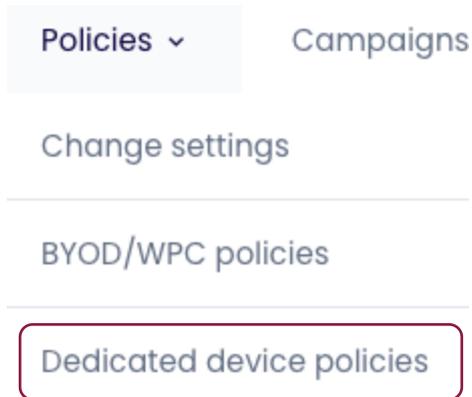
Dedicated Device Policies

Date: 17/11/2023



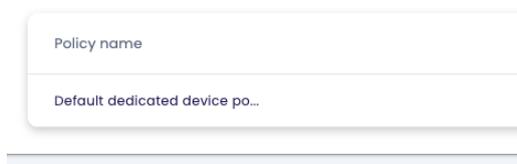
Dedicated device policies – Launcher customization

New option on Policies tab – Dedicated device policies, on which default and custom policies list is displayed. In current version list allows to customize columns and open details of the policy.



You will then have to choose between editing the existing default policy or create a completely new one.

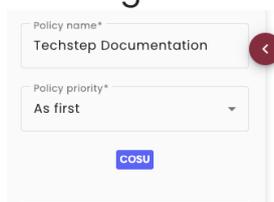
Default dedicated device policy



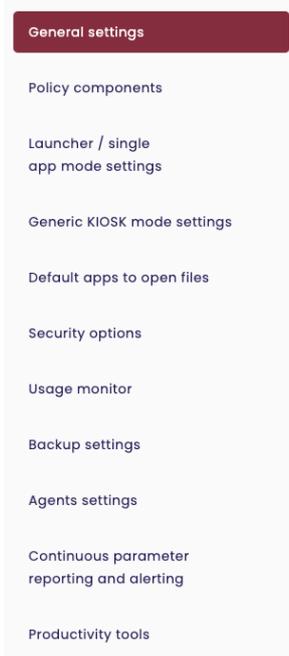
Dedicated device policies



To create a new dedicated device policy, tap the +-sign to the left. When creating a new one, you will have to give it a name and set a Policy priority:



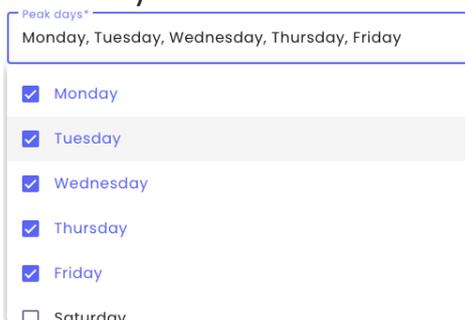
On the left side you will find several options available:



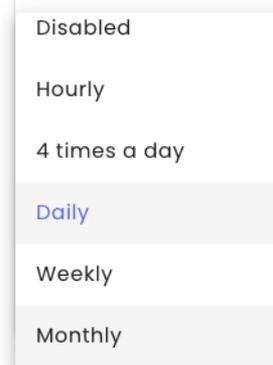
General settings

In the **General settings** you will find the following options:

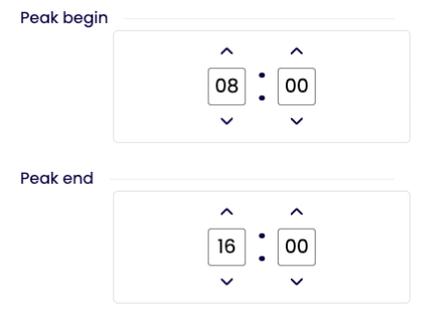
- Reinstall base agent (Yes/No)
- Uninstall not compatible policy components automatically (Yes/No)
- Mark as wiped on Base Agent uninstallation (Yes/No)
- Enable remote access services (Yes/No)
- Enable location services (Yes/No)
- Report additional data about apps (app size, cache size, data size)
(This option requires the Usage Access permission to be enabled)
- Report all applications
 - Report all applications
 - Report only managed applications
- Peak days



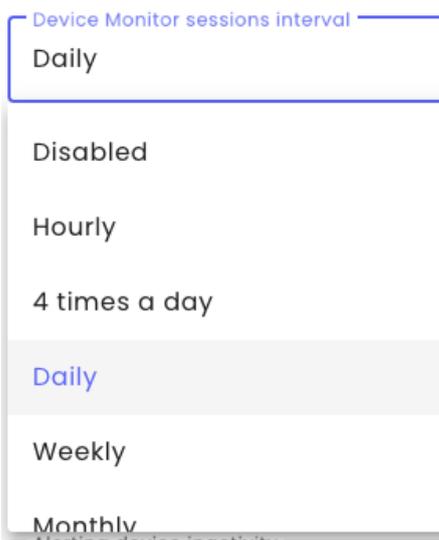
- Device Monitor sessions interval



- Peak time



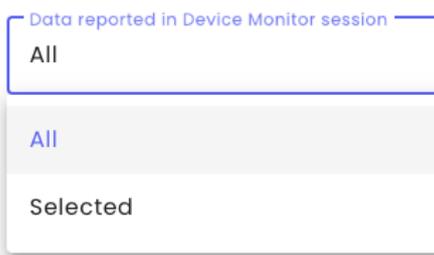
- Device Monitor sessions interval



- Number of stored Device Monitor sessions

- 5-50

- Data reported in Device Monitor session (Android)



- Wipe on exceeded device inactivity (Yes/No)
- Marked as wiped on exceeded device inactivity (Yes/No)
- Time sync interval

Disabled

1 hour

6 hours

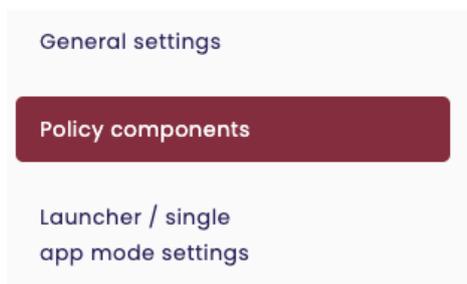
12 hours

1 day

1 week

- Sim change notify (for example if device was stolen) (Yes/No)
SMS Gateway number (SIM change notification)
- Device limit per user (Numeric, 1-999.999)

Policy Components



Here you can add components to your policy. You can chose between application or configuration.

 Add application

 Add configuration

Launcher/single app mode settings

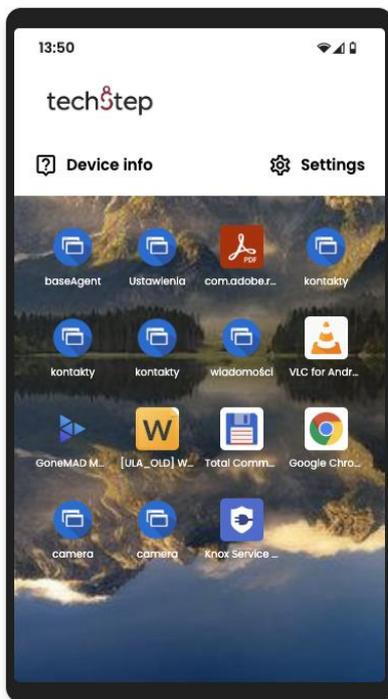
When Launcher is selected, preview of the Launcher view on the device is displayed. Preview is automatically changed based on the selected settings.

Apps/web clips can be reordered on the device preview using drag & drop function.

🔍 Search

Lock mode

Essentials MDM Launcher with allowed apps



- ① You can drag the icons to change their order.
- ② You can drag the settings bar to change its position.

Launcher settings are split into the four subtabs:



General Launcher settings

- Wallpaper - possibility to set custom wallpaper
- Start first application after reboot - if set, first app on the list will be launched automatically after reboot of the device
- Inactivity timeout - time after which the device will be locked (options: Disabled, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes)
- App list theme - light or dark mode background of apps & web clip part
- App list background transparency - allows to set transparency of the app list background (0%, 25%, 50%, 75%, 100%)



If Header settings are enabled - new area that can be displayed on the device, with options:



- Icon - possibility to set custom icon on the header bar
- Color - color of the header bar background (can be set directly with RGB values or picked up with the mouse click)
- Transparency - allows to set transparency of the header (0%, 25%, 50%, 75%, 100%)

Custom settings bar

- Settings bar position - allows to change position of the settings bar (top of the screen, below the header or bottom of the screen)
- Settings bar transparency - allows to set transparency of the settings bar (0%, 25%, 50%, 75%, 100%)
- Settings bar theme - available options: light or dark theme
- Show device info button - optional button on the left side of the settings bar
 - Optional device info button text - optional text displayed next to the device info icon on settings bar
 - Show device info in separate view
If set, device info fields will be shown on the separate page.
In addition we can provide short description (max 64 chars) which will be displayed on that view and phone number.
When provided and device will have a sim card there will be button displayed that will invoke call to the provided phone number.
Call functionality is available since Android 9.0.
 - Up to 8 fields about the device (device, sim card, user of the device + all types of custom fields) that will be displayed on separate view.
- Show settings button:
 - Optional settings button text - optional text displayed next to the settings button on settings bar
 - Show Bluetooth toggle - enables the Bluetooth connection
 - Show WiFi toggle - enables the WiFi
 - Show torch toggle - enables the torch
 - Show restart option - allows to restart the device
 - Show brightness slider - allows user to change the brightness on the device
 - Show rotate toggle - possibility to rotate the view
 - Show volume slider - allows user to change the volume on the device
 - Show grid/list switch - possibility to switch the view between grid and list
 - Show zoom toggle - possibility to zoom the view (both grid or list)

Launcher grid elements

- Apps & webclips:

New app / webclip can be added to the view with "Add new element" button on the right side.

We can select application shortcut or web clip.

When application shortcut will be selected we can provide:

- Package name - when clicked, hints with all apps from the organization will be displayed.
- Name - application name displayed on the device
- Description - optional text displayed in the second line visible on the list view
- Primary icon - icon displayed on the device in a normal view (not zoom)
- Zoom-mode icon - optional icon displayed in zoom mode (if not provided, primary one will be displayed)

Add new element ×

New item type:

Application shortcut	Webclip	Intent
----------------------	---------	--------

Package name* ▼
e.g. com.android.chrome

Name*

Description

Primary icon

+

Zoom-mode icon

+

Cancel Save

- When web clip will be selected, we can provide:
 - URL - link to the web clip
 - Name - name displayed on the device
 - Description - optional text displayed in the second line visible on the list view
 - Primary icon - icon displayed on the device in a normal view (not zoom)
 - Zoom-mode icon - optional icon displayed in zoom mode (if not provided, primary one will be displayed)

Add new element ×

New item type:

Application shortcut	Webclip	Intent
----------------------	---------	--------

URL*

The URL must contain the type of protocol, e.g. <https://company.com>

Name*

Description

Primary icon

+

Zoom-mode icon

+

Cancel Save

In order to change / remove already added app/web clip hover the app on the device preview, edit and delete icons will be shown.

In order to apply all the changes on the device, "Save" button need to be clicked. (Will appear on the left bottom part of the view when any change will be performed).

- With the Intent functionality we are able to open specific files via provided in uri application and also make a clickable icon:
 - Activity – new activity will be launched
 - Service – request for that a given application service can be started
 - Send a broadcast – broadcast the given intent to all interested BroadcastReceivers.

Add new element ×

New item type:

Application shortcut	Webclip	Intent
----------------------	---------	--------

Intent type:

Activity	Service	Broadcast
----------	---------	-----------

Intent*

Name*

Description

Primary icon

+

Zoom-mode icon

+

[Cancel](#) Save

- Select widgets is also possible. You can choose from a list from the tenant.

Generic KIOSK mode settings

- Keyguard (Enabled/Disabled)
- Volume change (Enabled/Disabled)
- Long press power button (Enabled/Disabled)
- System info on status bar (Enabled/Disabled)
- Home button (Enabled/Disabled)
- Recent apps (Enabled/Disabled)
(Not available if home button is disabled)
- Notifications (Enabled/Disabled)
(Not available if home button is disabled)

Default apps to open files

Here you have the option to choose which app to open files.

Add default application

The screenshot shows a form titled "Add default application" with two main sections. The top section is a list of applications categorized by type:

- Word-writing programs**
 - + Google Docs
 - + Microsoft Word
- Spreadsheets**
 - + Google Sheets
 - + Microsoft Excel
- Presentation apps**
 - + Google Slides
 - + Microsoft Powerpoint
- PDF readers**
 - + Adobe Acrobat Reader

The bottom section is a form for selecting a default application for a specific MIME type:

- Select MIME data type from the list or fill manually:** A dropdown menu with ".doc" selected.
- MIME data type*:** A text input field containing "application/msword". Below it, it says "This field is required".
- Package name*:** A dropdown menu with "Word (com.microsoft.office.word)" selected.
- Activity*:** A text input field containing "Word files". Below it, it says "This field is required".

Security options

There are several security options to secure the devices in the dedicated device policy. You are also able to perform a search or filter on Android models.

Filters ▼

Android

- Samsung SDK
- Huawei SDK
- Device Owner

- Wipe policy:
 - Data wipe on SIM card change (Yes/No)
 - Wipe on no SIM card detection (Yes/No)
(Data wipe on SIM card change must be enabled)
 - Wipe memory card (Yes/No)
(Data wipe on SIM card detection must be enabled)
 - Wipe on root detection (Yes/No)
 - Factory reset lock (Yes/No)
 - Factory reset protection (FRP)

Disabled
✓

- Unlock the device with an active device account
- Unlock the device with an account from the list
- Remove FRP after device wipe

- Network policy:
 - Wi-Fi lock (Yes/No)
 - Manual Wi-Fi configuration lock (Yes/No)
(Wi-Fi lock must be enabled)
 - Keep Wi-Fi on in sleep mode (Yes/No)
 - Prevent Wi-Fi from being turned on (Yes/No)
 - Bluetooth lock (Yes/No)
 - Cellular data lock

Do not lock
✓

- Enable package data and block possibility to disable
- Disable package data and block possibility to enable

- Cellular data lock in roaming

Do not lock ✓

Disable and block possibility to enable

- Wi-Fi tethering lock (Yes/No)
- USB tethering lock (Yes/No)
- Block incoming MMS (Yes/No)
- Disable Network Settings Reset (Yes/No)
- Disable VPN settings (Yes/No)
- Block private DNS settings (Yes/No)
- Block incoming calls

Do not block ✓

All

Pattern

(Pattern will let you set patterns of blocked numbers, see examples in the console)

- Block incoming SMS messages

Do not block ✓

All

Pattern

(Pattern will let you set patterns of blocked numbers, see examples in the console)

- Monitor list of managed Wi-Fi configurations (Yes/No)
- Disallow cellular 2G (Yes/No)
- Disallow Ultra-Wideband (UWB) (Yes/No)

- Location policy:

- Android location lock

Do not lock ✓

Disable location and block possibility to enable

Disable location

Enable location and block possibility to disable

Enable location

- Hardware policy

- Camera lock (Yes/No)
 - USB media player lock (Yes/No)
 - Development mode lock (Yes/No)
 - Task manager lock (Yes/No)

- NFC lock (Yes/No)
- Disallow outgoing beam using NFC (Yes/No)
- Storage card lock (Yes/No)
- Screen capture lock (Yes/No)
- USB file manager (Yes/No)
- Block multiwindow mode (Yes/No)
- Block safe mode (Yes/No)
- Block airplane mode (Yes/No)
- Prevent users from configuring credentials in the managed keystore
- Encryption policy (Yes/No)
 - Internal storage encryption (Yes/No)
- Installer policy
 - Application installer lock (Yes/No)
 - Allow USB debugging (Yes/No)
 - Unknown sources lock (Yes/No)
 - Disable application control (Yes/No)
 - Accounts creation using Google Play (Yes/No)
- Application restrictions
 - Application voice recording lock (Yes/No)
 - Do not force Google Play Protect (Yes/No)
 - Force automatic date and time (Yes/No)
 - Disable accounts modification (Yes/No)
 - Disable user accounts management (Yes/No)
 - Disallow config default applications (Yes/No)
- Application policy
 - Device Owner application policy
 - No application policy ✓
 - Allow only applications from the list
 - Block applications on the list
 - Device Owner runtime permission policy
 - Managed by user ✓
 - Allow
 - Deny

- Application permissions exceptions

Add new exception

Package name*

Calendar As global

Read calendar

Write calendar

Camera As global

Camera

Contacts As global

Read contacts

Write contacts

Read accounts

- The auto-update Managed Google Play apps policy settings

Enable auto updates

Enable auto updates only when the device is connected to Wi-Fi

Allow the user of device to configure the app update policy

Disable auto updates

- Applications availability in the MGP store

All applications from the GP store

Only enabled applications

Usage Monitor

- Enable usage monitor services (Yes/No)

The Android Usage agent monitors and reports user activity to the Essentials server, records outgoing and incoming voice calls, and gives insight into outgoing and incoming text and MMS messages. Essentials Usage Monitor installation is like Base Agent installation.

- Report device data after restart of the device (Yes/No)
- Package data settings
 - Report data traffic using Wi-Fi

Do not report

Every 15 minutes

Every 30 minutes

Every hour

Every 6 hours

Every day

Every 3 days

Every week

Every 2 weeks

Every month

Every 3 months

o Extended reporting settings

o Report device state (Yes/No)

o Report screens unlock/lock time (Yes/No)

o Report application usage (Yes/No)

Report extended parameter

Report extended parameters

Every day

Do not report

Every 15 minutes

Every 30 minutes

Every hour

Every 6 hours

Every day

Every 3 days

Every week

Every 2 weeks

Every month

Every 3 months

Backup settings

- Backup synchronization settings

Backup items – sets the backup items that will be included in policy
(Supported only backup of the contacts)

- Backup interval

Disabled

Once a day

Once a week

Once a month

- Business contact synchronization

- Basic synchronization type

None of the contacts

Contacts only from user groups

Contacts from all groups

- Contacts synchronization of the additional groups

This will let you add users from the user groups in the system

Contacts synchronization of the additional groups

0 ^

No results

+

- Business contacts sync interval

Disabled

Once a day

Once a week

Once a month

- Default mobile number of business contacts

Mobile number

Office phone

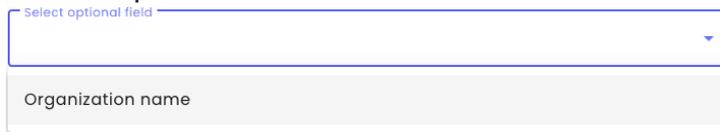
Agent settings

Here you are able to set a handful of values to be displayed in the agent.

- Organization name displayed on the device
 - This makes you able to configure the organizations name on the device, i.e., Techstep



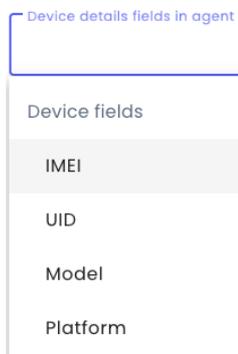
- Select optional field



- Show additional filed on agent's main panel (Yes/No) (Available for Android and macOS devices)
 - Value of the additional field on agent's main panel



- Device details fields in agent





Continuous parameter reporting and alerting

This will let the system report several parameters from the device, like Charger state, Battery level, Memory RAM Free, Battery voltage, Battery temperature, Battery condition and low battery level.

- Parameter reporting

Disabled

Report only in peak

Report all the time

- Report only in peak

Parameter list

Parameter	Interval	Alerting condition
Charger state	15 minutes	different from: Not conne..

+

- Report all the time

Parameter list

Parameter	Interval	Alerting condition
Charger state	15 minutes	different from: Not conne..

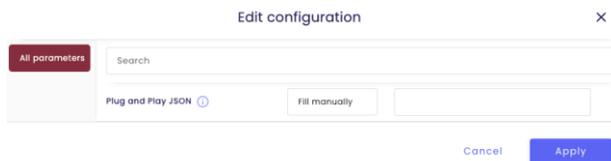
+

Productivity tools

- This makes you install two applications for productivity

- Enable Plug&Play (Yes/No)

Plug & Play application offers effective way to establish connection between Bluetooth-enabled devices and an Android device, but also the ability to use a device's built-in camera as a scanner. This app is added by default to the Managed Kiosk product. You can edit the configuration when activated



- Enable FileViewer (Yes/No)

FileViewer application enables a secure and flexible way to present different types of documents, images and movies on the device. You can edit the configuration when activated

