



# Techstep

## Essentials MDM

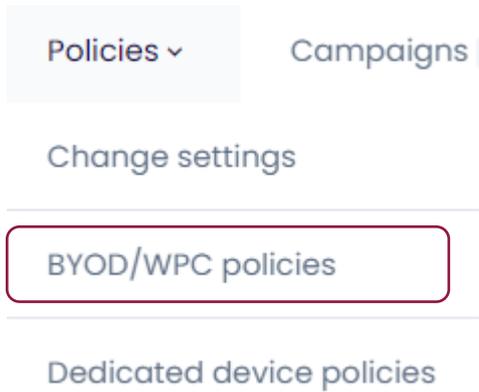
### BYOD/WPC Policies

Date: 30/11/2023

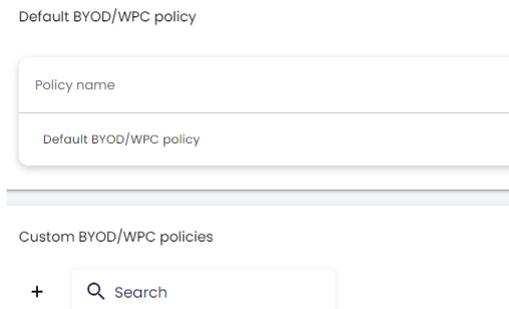


## BYOD / WPC policies

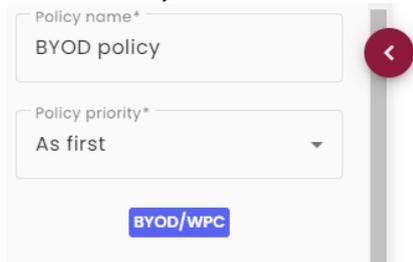
New option on Policies tab – BYOD/WPC policies, on which default and custom policies list is displayed. In current version list allows to customize columns and open details of the policy.



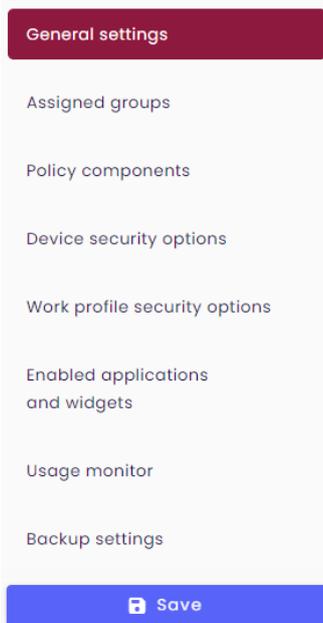
You will then have to choose between editing the existing default policy or create a completely new one.



To create a new BYOD / WPC 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)
- Enable Samsung Premium API
  - When set, Premium license field, Premium license expiry date and Enable Samsung attestation additional options appears.
  - Premium license and expiry date are required.
- SafetyNet attestation
  - Enabling this option will make impossible to enroll devices with unlocked Bootloader.
  - Administrator can set the interval of the device attestation.
- Mark as wiped on Base Agent uninstallation (Yes/No)
- Enable remote access services (Yes/No)
  - When set, administrator can set visibility of the remote session initialization consent with such values:
    - Managed by user
    - Require on every connection
    - Automatic connection
- Enable location services (Yes/No)
  - When set, administrator can set:
    - Location interval
    - Disable location reporting on off-peak
    - Disable location reporting after agent installation
- Ignore battery optimization for Location monitor and Usage monitor

- Selecting this option sends an operation that requires user confirmation
- Report additional data about apps (app size, cache size, data size)  
(This option requires the Usage Access permission to be enabled)
- Report all applications (option available for iOS devices)
  - Report all applications
  - Report only managed applications

○ Peak days

Peak days\*

Monday, Tuesday, Wednesday, Thursday, Friday

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

○ Device Monitor sessions interval

Disabled

Hourly

4 times a day

Daily

Weekly

Monthly

○ Peak time

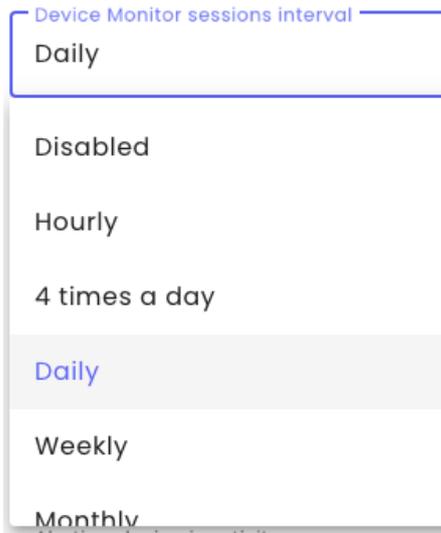
Peak begin

08 : 00

Peak end

16 : 00

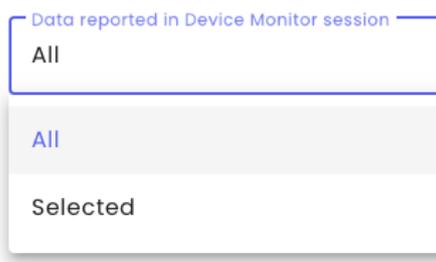
- Device Monitor sessions interval



- Number of stored Device Monitor sessions

- 5-50

- Data reported in Device Monitor session (Android)

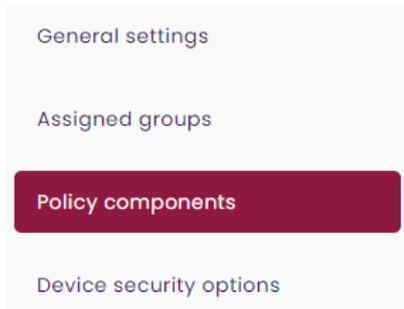


- Wipe on exceeded device inactivity (Yes/No)
- Marked as wiped on exceeded device inactivity (Yes/No)
- Time sync interval



- 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 choose between application or configuration.

 Add application

 Add configuration

## Security options

Security Options are divided into “Device security options” and “Work profile security options”

On BYOD devices, only work profile security options are applied, on WPC devices (work profile on company owned devices) both options are applied.

There are several security options to secure the devices in the BYOD/WPC. You are also able to perform a search or filter on BYOD, WPC, iOS, iPadOS and MacOS.

Filters

### Device security options

- 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 on root detection (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)
  - Prevent Wi-Fi from being turned on (Yes/No)
  - Bluetooth lock (Yes/No)
  - Cellular data lock in roaming
 

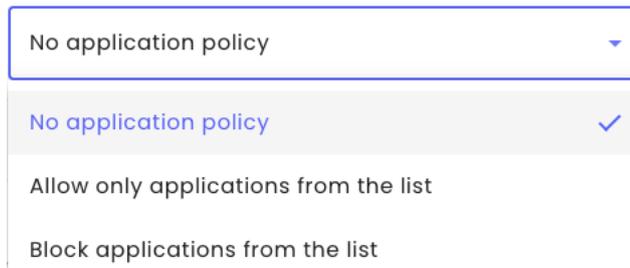
Do not lock ✓

Disable and block possibility to enable
  - Block outgoing calls



A screenshot of a dropdown menu. The top item is "Do not block" with a blue checkmark to its right. Below it are "All" and "Pattern".

- Block Bluetooth config (Yes/No)
- Block tethering config (Yes/No)
- Block mobile networks config (Yes/No)
- Block cell broadcast config (Yes/No)
- Disable SMS messages (Yes/No)
- Disallow cellular 2G (Yes/No)
- Disallow Ultra-Wideband (UWB) (Yes/No)
  
- Location policy:
  - Disable location config on device (Yes/No)
  - Disable location sharing on device (Yes/No)
  
- Update Policy
  - Enable Zebra OTA updates (Yes/No)
  
- Hardware policy
  - Block safe mode (Yes/No)
  - Block airplane mode (Yes/No)
  - Enable UB debugging (Yes/No)
  - Block screen capture (Yes/No)
  - Block USB file transfer (Yes/No)
  - Disable mounting on the physical external media (Yes/No)
  
- Installer policy
  - Unknown sources lock (Yes/No)
  
- Application restrictions
  - Block application voice recording on device (Yes/No)
  - Force automatic date and time (Yes/No)
  - Application policy on WPC device



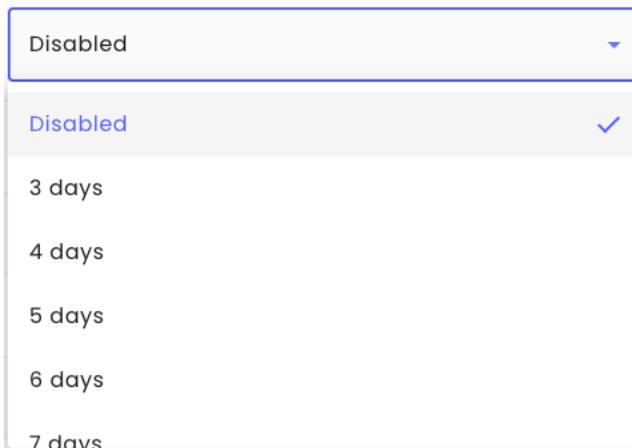
- Disable content capture on device (Yes/No)
- Disable content suggestions on device (Yes/No)

## Work profile security options

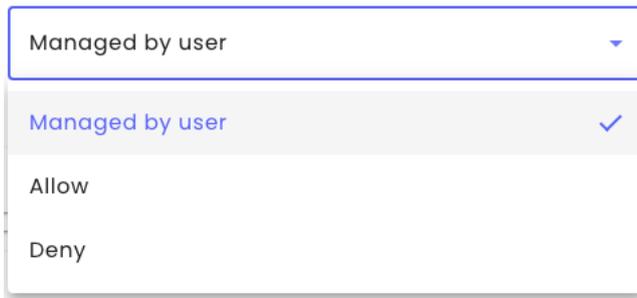
- Wipe policy:
  - Enterprise wipe on SIM card change (Yes/No) **(WPC/BYOD)**
  - Enterprise wipe on no SIM card detection (Yes/No) **(WPC/BYOD)**  
(Data wipe on SIM card change must be enabled)
  - Enterprise wipe on root detection (Yes/No) **(WPC/BYOD)**
- Network policy:
  - Disable VPN settings (Yes/No) **(WPC/BYOD)**
  - Disable managed networks settings change (Yes/No) **(WPC/BYOD)**
  - Monitor list of the managed Wifi configurations (Yes/No) **(WPC/BYOD)**
- Hardware policy
  - Disable Siri (Yes/No)
  - Disable Siri when device is locked (Yes/No)
  - Disable connections to Siri servers for the purpose of dictation (Yes/No)
  - Disable connections to Siri servers for the purpose of translation (Yes/No)
  - Disable automatically submitting diagnostic reports to Apple (Yes/No)
  - Disable Control Center from appearing on the Lock screen (Yes/No)
  - Disable backup of Enterprise books (Yes/No)
  - Disable Enterprise Book metadata sync (Yes/No)
  - Disable notifications history view on the lock screen (Yes/No)
  - Disable today notifications history view on the lock screen (Yes/No)
  - Disable managed applications to use the iCloud (Yes/No)
  - Force devices receiving AirPlay requests from this device to use a pairing pass (Yes/No)
  - Force encrypted backup (Yes/No)
  - Force wrist detection on Apple Watch (Yes/No)

- Force to set lock code (Yes/No)
  
- Encryption policy (Yes/No)
  - Internal storage encryption (Yes/No)
  
- Installer policy
  - Application installer lock (Yes/No)
  - Accounts creation using Google Play (Yes/No)
  
- Application restrictions
  - Application voice recording lock (Yes/No)
  - Do not allow to share managed documents using AirDrop (Yes/No)
  - Do not allow to share data from unmanaged apps (Yes/No)
  - Do not allow to share data from managed apps (Yes/No)
  - Allow unmanaged apps reading from managed contacts accounts (Yes/No)
  - Enable 'Do not allow to share data from unmanaged / managed apps' restrictions for copy and paste functionality (Yes/No)
  - Disable app uninstallation (yes/No)
  - Enable Safari fraud warning (Yes/No)
  - Disallow config default applications (Yes/No)
  
- Application policy
  - 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 ✓
  
- Work profile restrictions
  - Enable unknown sources (Yes/No)
  - Block screen capture (Yes/No)
  - Disable accounts modification (Yes/No)
  - Block creation of the mail account (Yes/No)

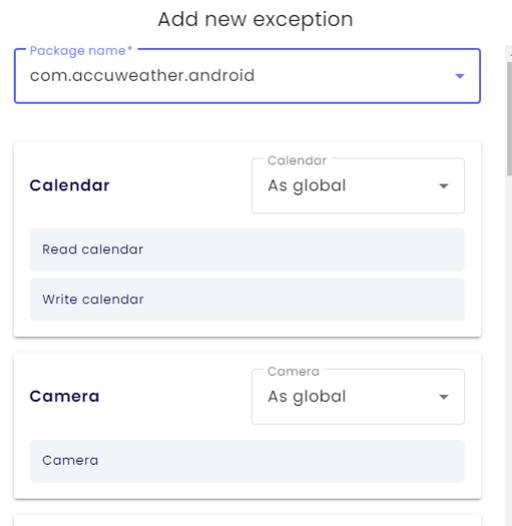
- Block creation of LDAP account (Yes/No)
- Block creation of Samsung account (Yes/No)
- Disable camera (yes/No)
- Disable cross profile copy-paste (Yes/No)
- Disable application control (Yes/No)
- Disable one lock code (Yes/No)
- Allow moving apps to work profile (Yes/No)
- Block NFC (Yes/No)
- Disallow outgoing beam using NFC (yes/No)
- Allow moving files from device to work profile (Yes/No)
- Allow moving files from work profile to device (Yes/No)
- Block change of the sharing of the calendar to the personal mode (Yes/No)
- Block change of the sharing of the calendar to work profile (Yes/No)
- Enable Bluetooth (Yes/No)
- Enable file sharing via Bluetooth in work profile (yes/No)
- Block Share Via List (Yes/No)
- Prevent users from configuring credentials in the managed keystore (Yes/No)
- Maximum time the work profile is allowed to be turned off



- Enable the ability to restore of the backup from the Google account (yes/No)
  - Disable location config (Yes/No)
  - Disable location sharing (Yes/No)
  - Disable content capture (Yes/No)
  - Disable content suggestions (Yes/No)
- Work profile applications permissions
    - Runtime permission policy



- Application permissions exceptions
  - Administrator can add exceptions to the global permission policy. For each application we can set exceptions for permissions categories:
    - Calendar
    - Camera
    - Contacts
    - Location
    - Microphone
    - Phone
    - Sensors
    - SMS
    - Storage
    - Physical activity



- Samsung KSP
  - Enable Samsung Knox Service Plugin (Yes/No)
    - When set, we can option configuration of the Samsung Knox Service Plugin

## Enable applications and widgets

- Enabled applications – applications available in work profile after device deployment, possible options:
  - Gmail
  - Microsoft Outlook
  - Google Calendar
  - Google Camera
  - Google Photos
  - Phone
  - Messages
  - Google Drive
  - Contacts
  - Downloads
  - Google Maps
  - Clock
  - Bixby
  - Samsung Galaxy Store
  - Netflix
  - One Drive
  - Youtube
  - Facebook
  - Google Chrome
  - Your Phone Companion – Link to Windows
  - Google Duo
  - Files
  - Samsung Internet Browser
  - Samsung Notes
- Enabled widgets of work profile applications – list of enabled widgets available in work profile

## Usage Monitor

- Enable usage monitor services (Yes/No)

The Android Usage agent monitors and reports user activity to the Essentials MDM server, records outgoing and incoming voice calls, and gives insight into outgoing and incoming text and MMS messages. Essentials MDM 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

- Extended reporting settings
  - Report device state (Yes/No)
  - Report screens unlock/lock time (Yes/No)
  - 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

Organization name displayed on the device

Available for Android devices

- Select optional field

Select optional field

Organization name

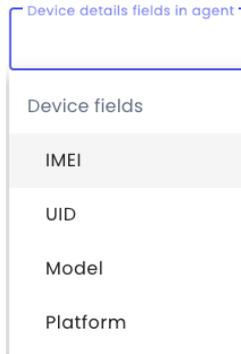
- Show additional filed on agent's main panel (Yes/No)  
(Available for Android and macOS devices)
  - Value of the additional field on agent's main panel

Value of the additional field on agent's main panel \*

Organization name

Organization name ✓

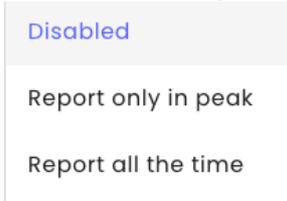
- Device details fields in agent (Available for Android and macOS devices)



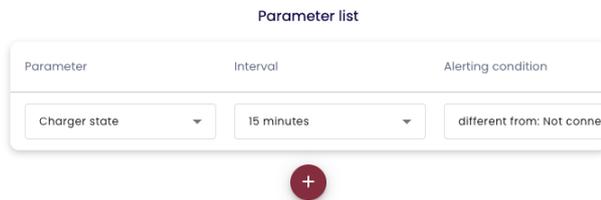
## Continuous parameter reporting and alerting

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



- Report only in peak



- Report all the time

