techstep

Techstep Essentials MDM

GDPR Compliance

Date: 18/10/2023

Contents

PUBLISHED BY:

Techstep Poland S.A.
Ul. Wajdeloty 12A
80-437 Gdańsk

SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES INTRODUCED IN THIS MANUAL ARE SUBJECT TO CHANGES. ANY INFORMATION AND RECOMMENDATIONS PROVIDED IN THIS DOCUMENT IS RELEVANT, HOWEVER, ALL RESPONSIBILITY FOR THE IMPLEMENTATION AND USE OF THE PRODUCTS AND SERVICES IS WITH THE USERS

1 Essentials MDM & GDPR

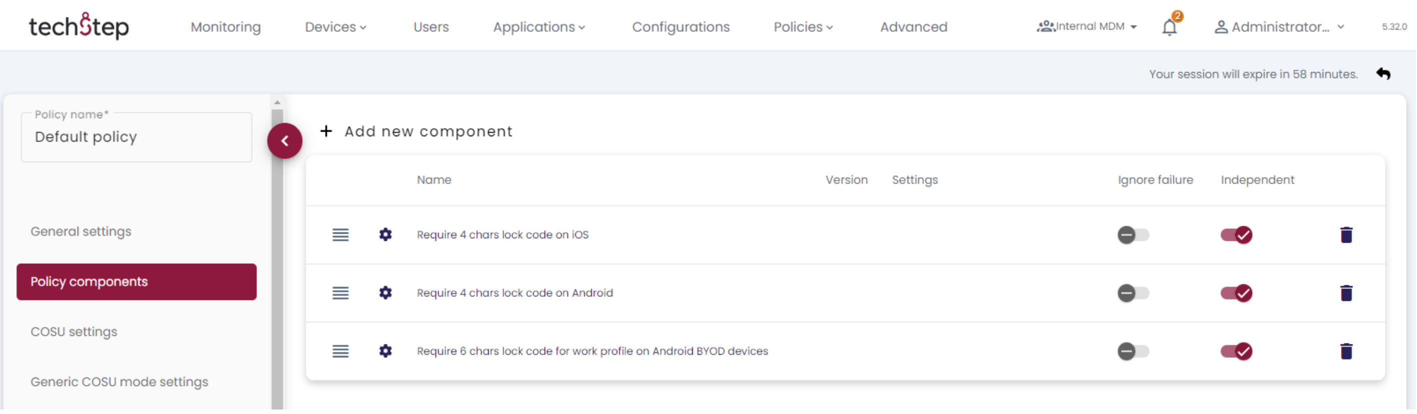
The General Data Protection Regulation (GDPR) imposes additional obligations on data protection for organizations that process and store personal data. In order to comply with new regulations, you should also analyse risks connected with mobile data security. Organizations that manage their mobile devices with Techstep Essentials MDM have all the tools they need to achieve security required by the new law at hand. Note that the GDPR gives guidelines not detailed instructions. At the end of the day, it is up to the administrator to decide which security measures are sufficient to meet organization needs.

2 Mobile data access control

Access to data stored on a mobile device can be protected in multiple ways. The basic security can be achieved by imposing a lock code: Techstep Essentials MDM system enforces the lock code through a configuration, which you can later add to the policy. This way the organization can be certain that mobile devices enrolled in Techstep Essentials MDM require lock code.

Device lock is a default setting and also a component of a default policy in Techstep Essentials MDM. Lock code can be enforced using every policy in the organization.

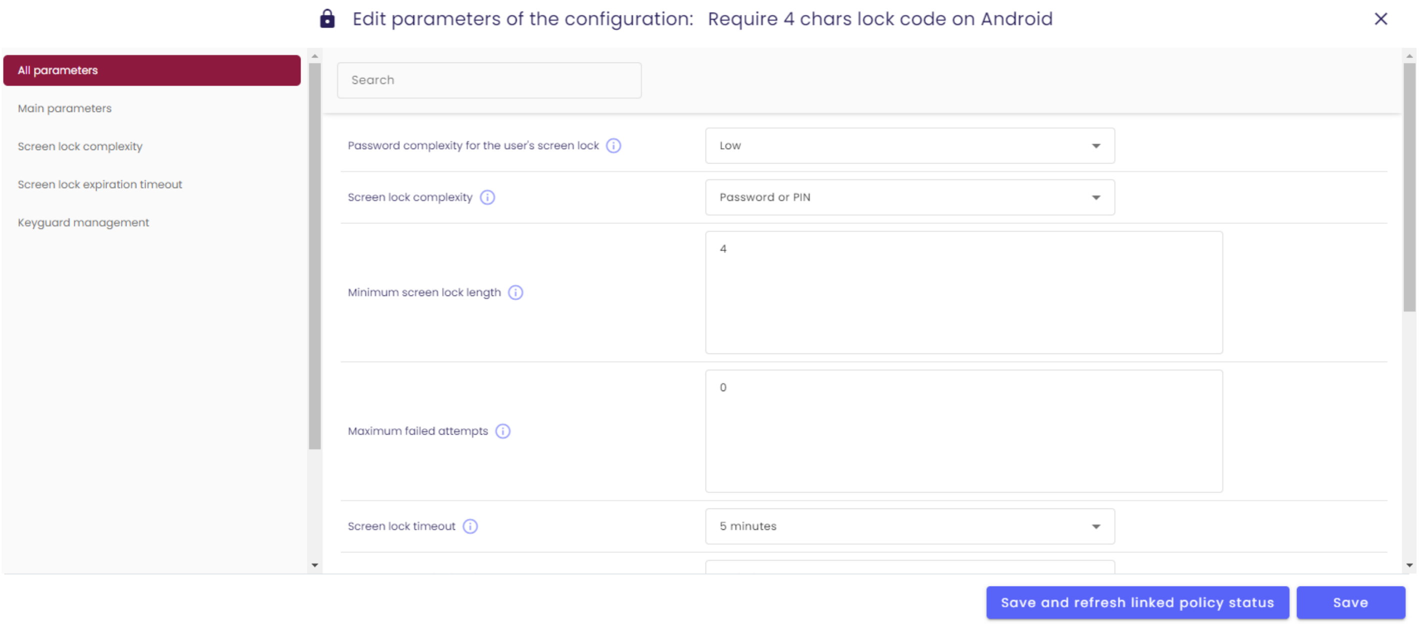
To enforce lock code go to policy details tab and add lock code configuration on Policy components tab.



Policy name*: Default policy

Name	Version	Settings	Ignore failure	Independent
Require 4 chars lock code on iOS			○	✓
Require 4 chars lock code on Android			○	✓
Require 6 chars lock code for work profile on Android BYOD devices			○	✓

Lock code requirements can be changed by editing the configurations for a given platform on Configurations tab.
i.e. for the Android platform: ‘Require 4 chars lock code on Android’.



Edit parameters of the configuration: Require 4 chars lock code on Android

Password complexity for the user's screen lock: Low

Screen lock complexity: Password or PIN

Minimum screen lock length: 4

Maximum failed attempts: 0

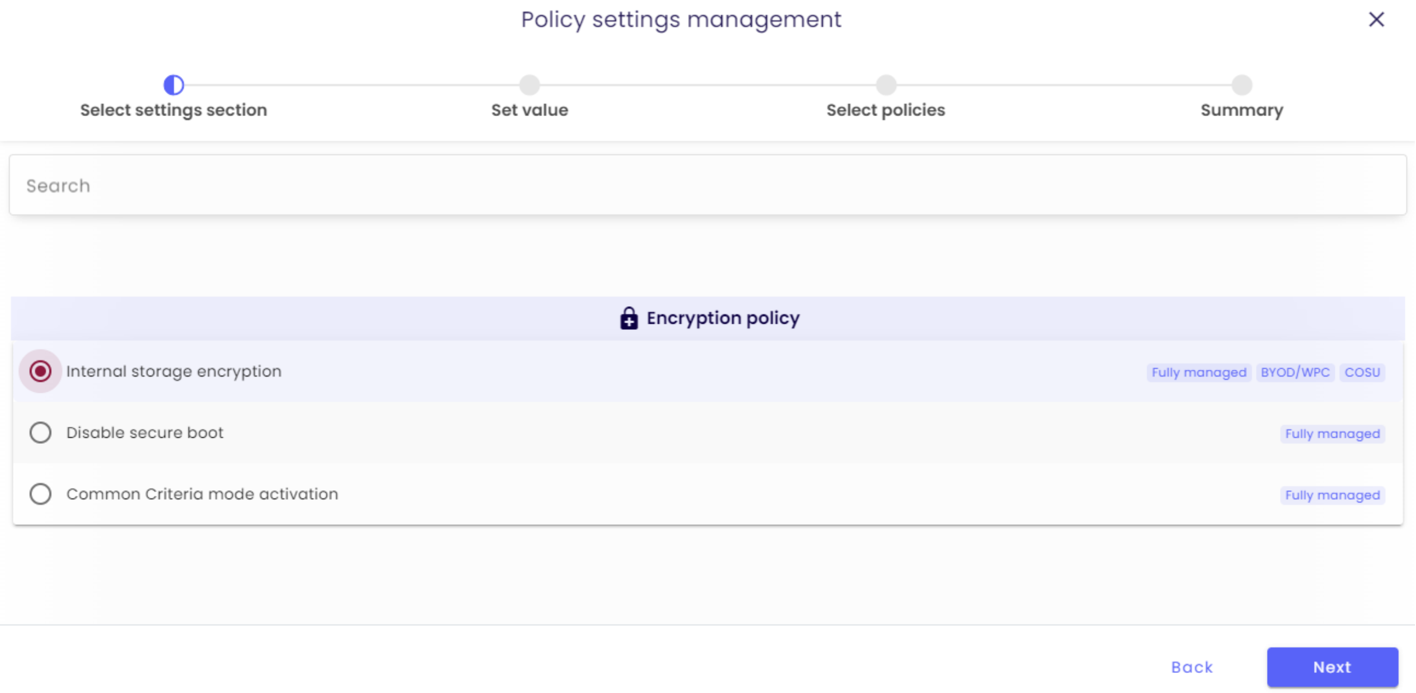
Screen lock timeout: 5 minutes

Another method to enhance data security on a mobile device is by internal storage encryption. Devices that launched with Android 6.0 and higher or with iOS 10 have a built-in internal storage encryption. However, to fully protect data stored on a mobile device, it is recommended to enforce the lock code as an additional way to encrypt your data.

All devices with Android previous to the version 6.0 have to go through the process of enforcing an internal storage encryption. During that process the lock code needs to be set up.

Encryption can be enforced by selecting a checkbox in a security policy:

Policies > Change settings > Encryption policy and then select 'Internal storage encryption'.



Encryption policy

● Internal storage encryption — Fully managed, BYOD/WPC, COSU

○ Disable secure boot — Fully managed

○ Common Criteria mode activation — Fully managed

Each policy change needs to be refreshed to be applied.

3 Separation of the corporate and private data

3.1 Android devices

With Techstep Essentials MDM, corporate data can be separated from private data using containerization. The container solution is available with Android Enterprise work profile (all Android 7.0 devices and higher).

Two key elements to prevent data leakage using container solutions are blocking data transfer (copy - paste) between the company's and private environments and blocking access to given applications (such as calendar or contacts).

Settings can be changed or blocked in the policy of the company's profile:
Policies > Change settings > Work profile restrictions

3.2 Apple devices

With iOS devices, company's data is separated from private by default if the Techstep Essentials MDM profile is installed on the device. In addition, company's data access can be restricted in a way that only corporate applications managed by Essentials MDM can be installed on the device (Supervised mode only). For example, an attachment downloaded from company's mail account can be opened only by an application that has been approved by the security department. Access to business contacts can also be limited in the same way.

In order to achieve this, parameters below should be changed:

- 'Do not allow to share managed documents using AirDrop' to 'No'
- 'Do not allow to share data from unmanaged apps' to 'No'
- 'Do not allow to share data from managed apps' to 'No'

These parameters can be found in Policies > Change settings > Application restrictions.

4 Access to company resources for devices in the field

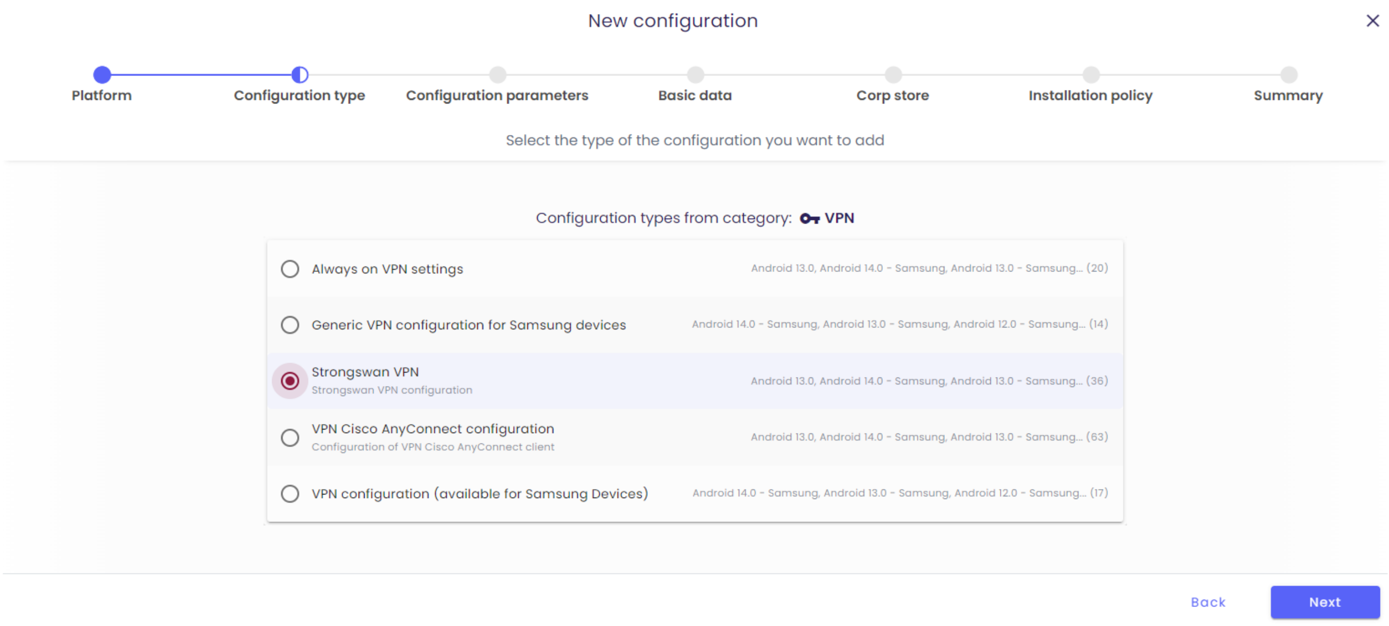
Data stored on devices used in the field also require protection. You need to keep in mind, that mobile devices enable access to company's network and its resources. In order to safely access the corporate network, it is advised to integrate with Techstep Essentials VPN network gateway, which is based on IPsec IKEv2 protocol.

Techstep Essentials MDM helps you decide, which applications should use VPN connection (Per-app VPN). It can also force the use of VPN by the whole device or only by the container (business-related part of the device).

4.1 Android devices

On Android devices, you need to install Strongswan VPN using the Techstep Essentials EMM. The Strongswan configuration can be found in:

Configurations > Add new > Android > VPN > Strongswan VPN.



Select the type of the configuration you want to add

Configuration types from category: VPN

○ Always on VPN settings — Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (20)

○ Generic VPN configuration for Samsung devices — Android 14.0 - Samsung, Android 13.0 - Samsung, Android 12.0 - Samsung... (14)

● Strongswan VPN — Strongswan VPN configuration — Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (36)

○ VPN Cisco AnyConnect configuration — Configuration of VPN Cisco AnyConnect client — Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (63)

○ VPN configuration (available for Samsung Devices) — Android 14.0 - Samsung, Android 13.0 - Samsung, Android 12.0 - Samsung... (17)

In this configuration you can decide which applications should require VPN connection. If VPN connection is to be used for the whole device, use the configuration in the general default policy. If you want to apply it to the container, then it has to be set up as a component of a BYOD / WPC policy.

4.2 Apple devices

On Apple devices we use native VPN client, which can be configured in the Apple VPN configuration which can be found in:

Configurations > Add new > Apple > iOS, iPadOS or macOS > VPN.

“Use Per-App VPN” allows you to define applications and list of domains for Safari browser that will require VPN connection.

5 Access to corporate resources

5.1 Access to corporate resources within its Wi-Fi

With the integration of the Techstep Essentials MDM system and the corporate network infrastructure, the company can have an additional control over devices that try to connect to internal network. Only devices that are managed and secure are allowed to access company’s network. The compliance verification is possible with Essentials MDM acting as External Compliance Checker integrated with CISCO ISE or Extreme Networks.

5.2 Secure access to corporate email

Techstep Essentials Exchange ActiveSync Proxy grants access to corporate email servers to managed, secured and Essentials MDM-compliant devices only. This way the company can be certain, that no external device will access company’s email. If anyone from the outside attempts to do it, the Essentials MDM system administrator will be notified about such an incident.

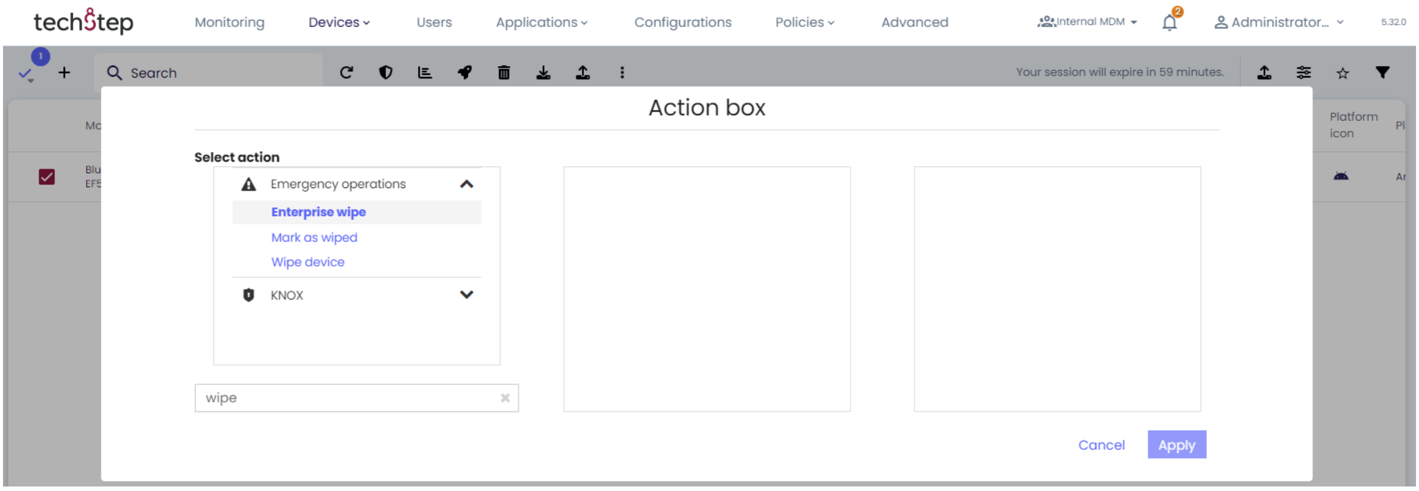
6 Data leakage prevention

In case of the device theft or loss, the employee should report this to the IT administrator in the company. Devices that are managed and secured by Techstep Essentials MDM do not pose a threat of data leakage. The administrator can remotely locate stolen or lost device and, if necessary, send a command to wipe the device or selectively wipe corporate data only.

6.1 Wipe device

Data on the device can be deleted remotely by sending a ‘wipe’ command. It can be done from the list of the devices tab: Management > Devices > device details > Select action

- ‘Wipe device’, to erase all data on the device
- ‘Enterprise wipe’, to delete corporate data (container)

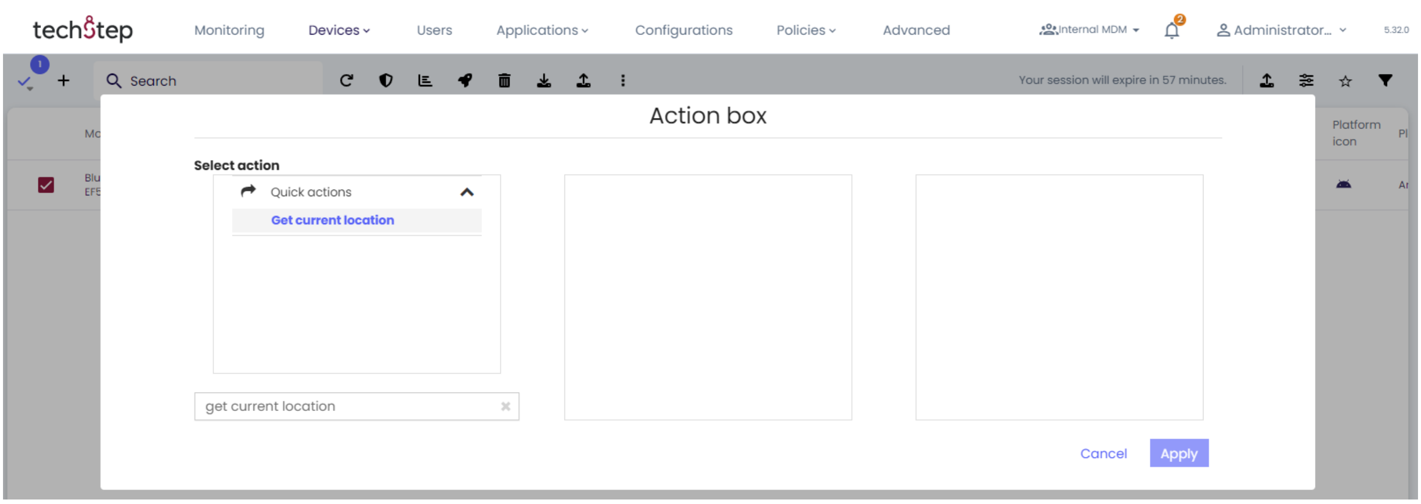


6.2 Locate stolen or lost device

6.2.1 Android devices

The device should have a location module installed: Policies > Change settings > General settings > Enable location services

If the managed device has the location module installed and gets stolen or lost, the Essentials MDM system administrator can locate the device. It can be done by accessing the list of the devices tab:
Management > Devices > device details > send a command > Get current location.



Your session will expire in 57 minutes.

6.2.2 Apple devices

In order to locate stolen or lost Apple device, it has to be set into a ‘lost mode’ - from this moment on, it can be located.

You can set a device into a lost mode (Supervised mode only) by accessing the list of the devices tab: Management > Devices > Device details > Select action > Enable Lost mode

And then:

Management > Devices > Device details > Select action > Get current location.

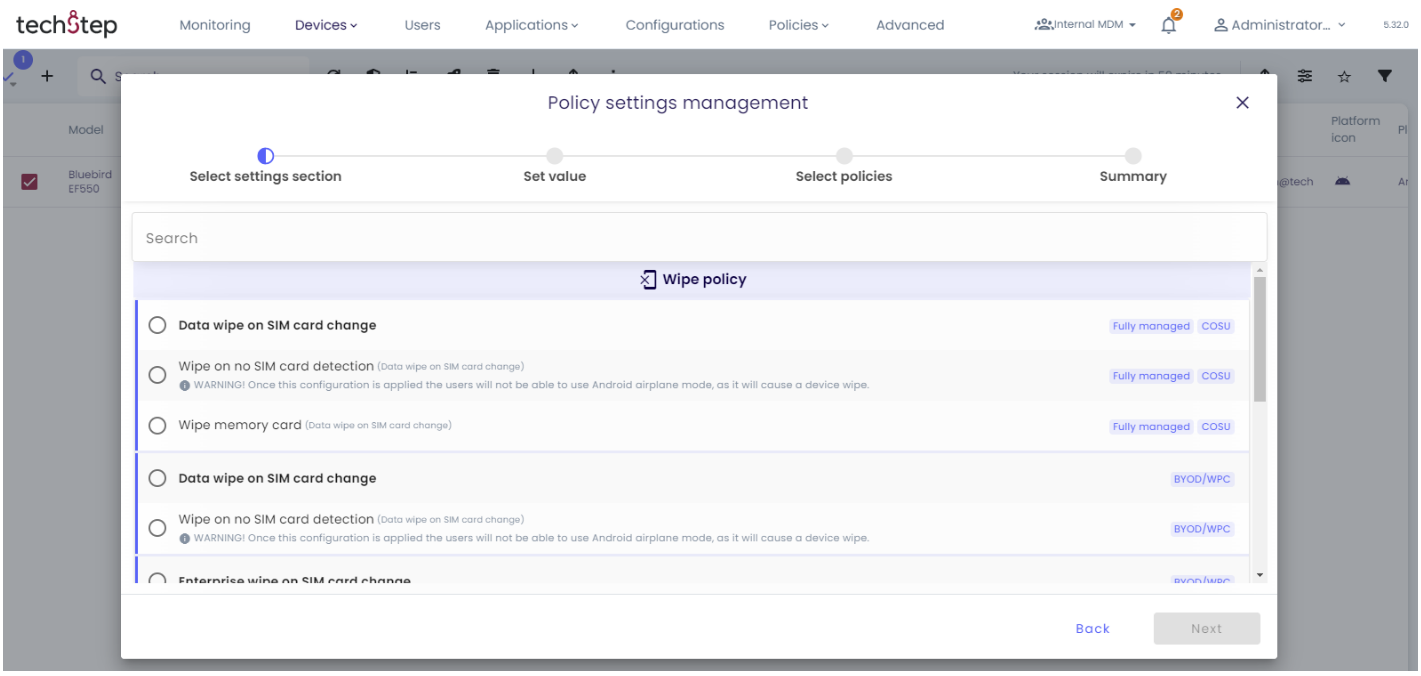
When the lost mode is on, the device is locked for the end user, until it’s unlocked by the Essentials MDM administrator.

6.3 Automatic data removal

Internal storage of the device can be wiped in case of the device being stolen or lost without any additional actions on the side of the administrator. The Essentials MDM policy can be set to automatically wipe the device in the event of the SIM card removal or change.

In addition, company’s data can be automatically deleted when the security is compromised on iOS (Jailbreak) or on Android (root).

Policies > Change settings > Wipe policy



Policy settings management

Select settings section | Set value | Select policies | Summary

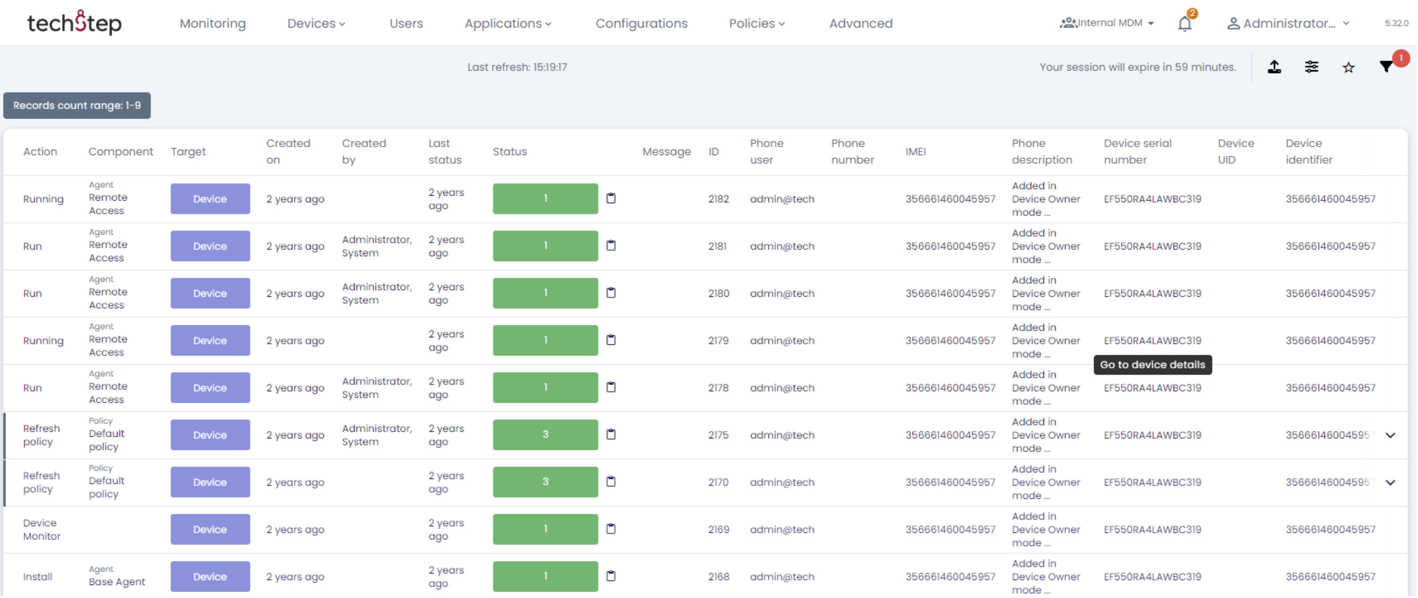
Search

Wipe policy

- ○ Data wipe on SIM card change — Fully managed, COSU
- ○ Wipe on no SIM card detection (Data wipe on SIM card change) — Fully managed, COSU
  WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe.
- ○ Wipe memory card (Data wipe on SIM card change) — Fully managed, COSU
- ○ Data wipe on SIM card change — BYOD/WPC
- ○ Wipe on no SIM card detection (Data wipe on SIM card change) — BYOD/WPC
  WARNING! Once this configuration is applied the users will not be able to use Android airplane mode, as it will cause a device wipe.
- ○ Enterprise wipe on SIM card change — BYOD/WPC

6.4 An overview of operations in the web console

All operations in the Essentials MDM system performed by the administrator or generated by the system based on the preferences are saved and available in the operation log. Log view allows verification the type of operation, who activated it, and when was it done and what's its status. To open the list of operations, go to the tab log: Devices > Log.



Last refresh: 15:19:17

Your session will expire in 59 minutes.

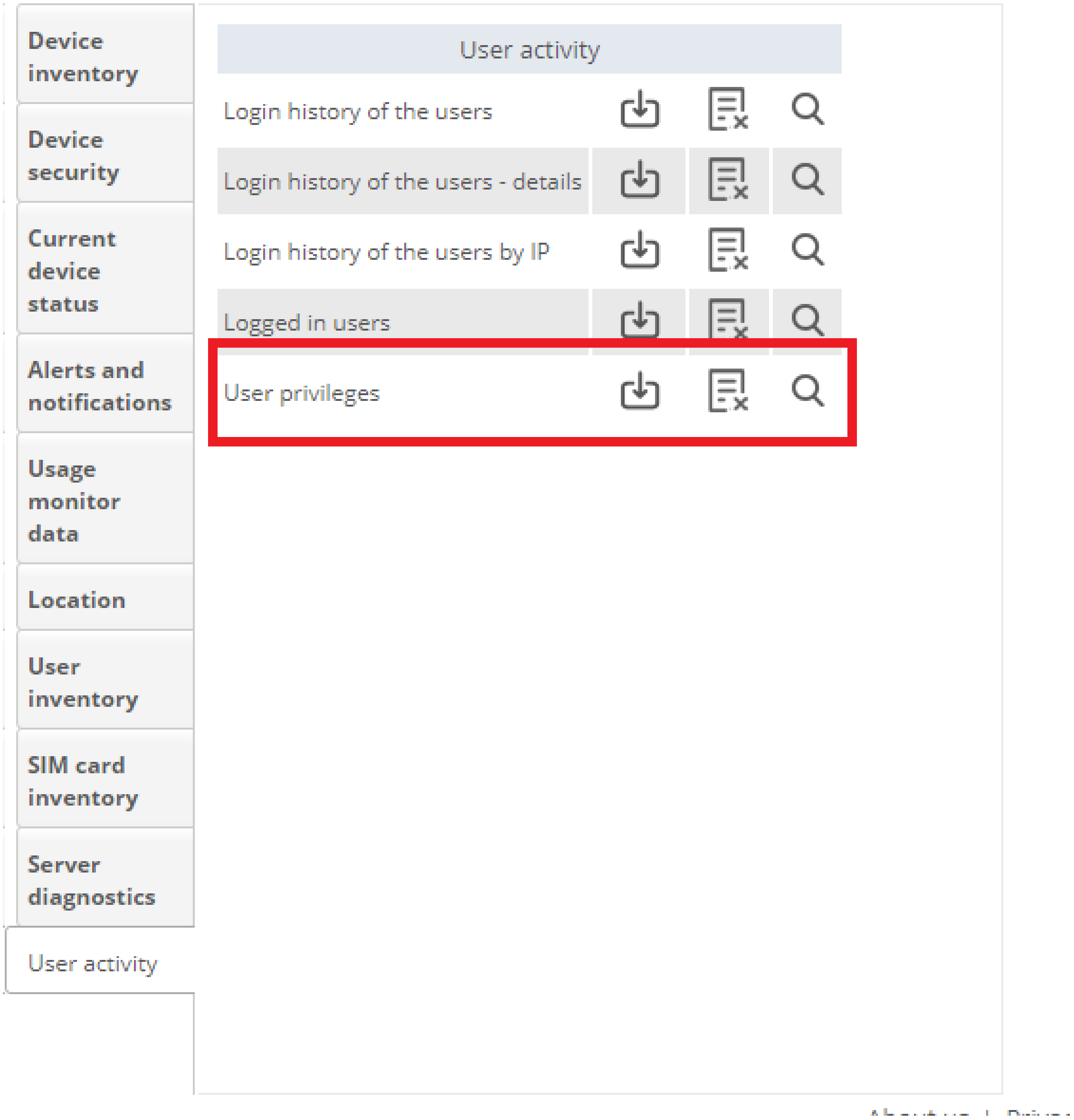
Records count range: 1-9

Action	Component	Target	Created on	Created by	Last status	Status	Message	ID	Phone user	Phone number	IMEI	Phone description	Device serial number	Device UID	Device identifier
Running	Agent Remote Access	Device	2 years ago		2 years ago	1		2182	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Run	Agent Remote Access	Device	2 years ago	Administrator, System	2 years ago	1		2181	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Run	Agent Remote Access	Device	2 years ago	Administrator, System	2 years ago	1		2180	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Running	Agent Remote Access	Device	2 years ago		2 years ago	1		2179	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Run	Agent Remote Access	Device	2 years ago	Administrator, System	2 years ago	1		2178	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Refresh policy	Policy Default policy	Device	2 years ago	Administrator, System	2 years ago	3		2175	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Refresh policy	Policy Default policy	Device	2 years ago		2 years ago	3		2170	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Device Monitor		Device	2 years ago		2 years ago	1		2169	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Install	Agent Base Agent	Device	2 years ago		2 years ago	1		2168	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957

6.5 An overview of user permissions

Each user that can log into the Techstep Essentials MDM system has permissions granted by the IT administrator of the company. These permissions can give a potential access to private data. In an easy way, you can review the permissions assigned to a given user in the Essentials MDM system.

To display a report for each user, go to: Advanced > Reports > User activity > User privileges


Device inventory
Device security
Current device status
Alerts and notifications
Usage monitor data
Location
User inventory
SIM card inventory
Server diagnostics
User activity
User activity
Login history of the users
Login history of the users - details
Login history of the users by IP
Logged in users
User privileges