



# Techstep

## Essentials MDM

### Zgodność z RODO

Data: 18/10/2023



## Spis treści

1	RODO a system Techstep Essentials MDM .....	4
2	Kontrola dostępu do danych z urządzeń mobilnych.....	5
3	Odseparowanie danych służbowych od prywatnych .....	8
4	Dostęp do zasobów firmowych dla urządzeń będących w terenie .....	9
4.1	Urządzenia Android.....	9
4.2	Urządzenia Apple.....	10
5	Dostęp do zasobów firmowych .....	11
5.1	Dostęp do zasobów firmowych dla urządzeń będących w zasięgu firmowej sieci Wi-Fi .....	11
5.2	Bezpieczny dostęp do poczty firmowej.....	11
6	Wsparcie w przypadku wystąpienia wycieku danych.....	12
6.1	Wyczyszczenie danych.....	12
6.2	Zlokalizowanie skradzionego lub zgubionego urządzenia .....	12
6.2.1	Urządzenia Android .....	12
6.2.2	Urządzenia Apple .....	13
6.3	Automatyczne usuwanie danych.....	13
6.4	Przegląd operacji wykonanych z poziomu konsoli www .....	14
6.5	Przegląd uprawnień użytkowników.....	15

OPUBLIKOWANY PRZEZ:

Techstep Poland S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

Chroniony prawem autorskim © 2008-2023 Techstep Poland S.A. Wszelkie prawa zastrzeżone.

Cała treść dokumentu stanowi wyłączną własność Techstep Poland S.A. i nie może być powielana ani rozpowszechniana bez pisemnej zgody wydawcy. Publikacja może zawierać marki i nazwy produktów, które są znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli.

SPECYFIKACJE ORAZ INFORMACJE DOTYCZĄCE PRODUKTÓW I USŁUG PRZEDSTAWIONE W NINIEJSZEJ INSTRUKCJI MOGĄ ULEC ZMIANIE. WSZELKIE INFORMACJE I ZALECENIA ZAWARTE W NINIEJSZYM DOKUMENTIE SĄ ISTOTNE, JEDNAKŻE WSZELKA ODPOWIEDZIALNOŚĆ ZA WDROŻENIE I KORZYSTANIE Z PRODUKTÓW I USŁUG PONOSI UŻYTKOWNIK.

## 1 RODO a system Techstep Essentials MDM

Rozporządzenie o Ochronie Danych Osobowych (RODO) nakłada na organizacje przetwarzające i przechowujące dane osobowe dodatkowe obowiązki w zakresie ochrony danych. By pozostać w zgodzie z rozporządzeniem, należy zwrócić także uwagę na zabezpieczenie danych na urządzeniach mobilnych wykorzystywanych w celach służbowych. Organizacje zarządzające urządzeniami mobilnymi poprzez system Techstep Essentials MDM mają gotowe, opisane poniżej narzędzia, dzięki którym mogą zadbać o bezpieczeństwo danych, które się na nich znajdują. Należy jednak zaznaczyć, że RODO określa wyłącznie ramy, ale nie daje szczegółowych instrukcji. Finalnie, to do każdego administratora należy decyzja, które zabezpieczenia uzna za wystarczające dla potrzeb swojej organizacji.

## 2 Kontrola dostępu do danych z urządzeń mobilnych

Dostęp do danych przechowywanych na urządzeniu można chronić na kilka sposobów. Jednym z podstawowych jest zabezpieczenie urządzenia mobilnego poprzez kod blokady. System Techstep Essentials MDM wymusza ustawienie kodu blokady urządzenia poprzez dedykowaną konfigurację, którą można dodać do polityki podstawowej. W takim przypadku organizacja ma pewność, że wszystkie zarządzane urządzenia mobilne w systemie Techstep Essentials MDM mają ustawiony kod blokady.

Wymuszenie kodu blokady jest domyślnym ustawieniem systemu Techstep Essentials MDM i jest elementem domyślnej polityki w systemie. Wymuszenie kodu blokady można dodać do dowolnej polityki wykorzystywanej w organizacji.

Konfiguracje wymuszające kod blokady znajdują się w szczegółach polityki w zakładce Elementy polityki.

Nazwa	Wersja	Ustawienia	Ignoruj błąd	Niezależny
Require 4 chars lock code on iOS			<input type="checkbox"/>	<input checked="" type="checkbox"/>
Require 4 chars lock code on Android			<input type="checkbox"/>	<input checked="" type="checkbox"/>
Require 6 chars lock code for work profile on Android BYOD devices			<input type="checkbox"/>	<input checked="" type="checkbox"/>

Wymagania kodu blokady można zmienić poprzez edycję konfiguracji dla danej platformy na zakładce Konfiguracje.

np. dla platformy Android: 'Require 4 chars lock code on Android'.

Edycja parametrów konfiguracji: Require 4 chars lock code on Android

Wszystkie parametry

Główne parametry

Wymagania zabezpieczeń blokowania ekranu

Wygaśnięcie kodu blokady

Zarządzanie zabezpieczeniami ekranu b...

Szukaj

Złożoność hasła do blokady ekranu użytkownika ⓘ Niska

Wymagania zabezpieczeń blokowania ekranu ⓘ Hasło lub PIN

Minimalna długość kodu blokady ⓘ 4

Maksymalna ilość błędnych prób ⓘ 0

Zapisz i odśwież status przypisanej polityki Zapisz

Szyfrowanie pamięci urządzenia mobilnego jest kolejnym sposobem na ochronę danych przechowywanych na urządzeniach mobilnych. Urządzenia sprzedawane z systemem Android w wersji co najmniej 6 oraz iOS 10 mają domyślnie szyfrowaną pamięć wewnętrzną. Jednakże, aby w pełni chronić dane przechowywane w pamięci urządzenia zalecane jest, aby wymusić kod blokady, który pełni funkcję dodatkowego klucza szyfrującego pamięć.

Wszystkie urządzenia z systemem Android wcześniejszym niż wersja 6 muszą zostać poddane procesowi wymuszenia szyfrowania pamięci, podczas którego należy zdefiniować kod blokady.

Szyfrowanie można wymusić, włączając odpowiednią pozycję w polityce bezpieczeństwa:

Polityki > Zmień ustawienia > Polityka szyfrowania pamięci a następnie wybrać 'Szyfrowanie pamięci wewnętrznej'.

## Zarządzanie ustawieniami polityk



Wybierz sekcję ustawień

Ustaw wartość

Wybierz polityki

Podsumowanie

Szukaj

## Polityka szyfrowania pamięci

☒ Szyfrowanie pamięci wewnętrznej

Pełne zarządzanie BYOD/WPC COSU

☐ Wyłącz tryb bezpiecznego uruchamiania

Pełne zarządzanie

☐ Aktywacja trybu Common Criteria

Pełne zarządzanie

Cofnij

Dalej

Po każdej zmianie polityki należy odświeżyć zmiany dla zarządzanych urządzeń.

## 3 Odseparowanie danych służbowych od prywatnych

### 3.1 Urządzenia Android

Dane służbowe można oddzielić od prywatnych za pomocą konteneryzacji dostępnej w systemie Techstep Essentials MDM. Do tego celu można użyć profilu służbowego (Android Enterprise), obsługującego wszystkie urządzenia Android 8 i nowsze.

Jednym z kluczowych elementów, które ograniczają możliwość wycieku danych przy korzystaniu w konteneryzacji jest blokada przenoszenia danych (kopiuj wklej) pomiędzy środowiskiem służbowym a prywatnym oraz rozdzielenie aplikacji takich jak kalendarz czy kontakty.

Ustawienia można włączyć lub zablokować w polityce profilu służbowego:  
Polityki > Zmień ustawienia > Ograniczenia profilu do pracy

### 3.2 Urządzenia Apple

W przypadku urządzeń działających pod kontrolą systemu Apple iOS dane służbowe są odseparowane domyślnie od momentu zarządzania przez system Techstep Essentials MDM. Dostęp do danych służbowych można dodatkowo ograniczyć do aplikacji służbowych, tzn. takich, które są zarządzane przez system Techstep Essentials MDM. Oznacza to, że załącznik pobrany z firmowego konta e-mail (klient pocztowy) może zostać otwarty tylko w aplikacji firmowej, zatwierdzonej do tego celu przez dział bezpieczeństwa. Analogicznie można zawęzić dostęp do kontaktów biznesowych tylko dla aplikacji i kont służbowych (zarządzanych przez system Techstep Essentials MDM).

W celu osiągnięcia powyższego efektu należy ustawić wartości parametrów:

- 'Nie zezwalaj na udostępnianie zarządzanych dokumentów za pomocą AirDrop' na 'Tak'
- 'Nie zezwalaj na udostępnianie danych z niezarządzanych aplikacji' na 'Tak'
- 'Nie zezwalaj na udostępnianie danych z zarządzanych aplikacji' na 'Tak'

Powyższe parametry znajdują się w Polityki > Zmień ustawienia > Ograniczenia aplikacji.



## 4 Dostęp do zasobów firmowych dla urządzeń będących w terenie

Dane przechowywane na urządzeniach to jeden z elementów, który należy chronić. Należy mieć na uwadze, że urządzenia mobilne umożliwiają dostęp do sieci firmowej oraz jej zasobów. W celu bezpiecznego i kontrolowanego dostępu do firmowej sieci zalecamy integrację z bramą Techstep Essentials VPN, która bazuje na protokole IPsec IKEv2.

System Techstep Essentials MDM umożliwia zdefiniowanie, które aplikacje powinny móc korzystać z połączenia VPN (tzw. Per-app VPN), wymuszenie korzystania z VPN przez całe urządzenie lub tylko przez kontener (czyli część służbową).

### 4.1 Urządzenia Android

Wymagany jest klient Strongswan VPN zainstalowany przez system Techstep Essentials MDM. Konfiguracja klienta Strongswan znajduje się w:

Konfiguracje > Nowa konfiguracja > Android > VPN > Strongswan VPN.

Nowa konfiguracja

Wybór platformy   Typ konfiguracji   Parametry konfiguracji   Podstawowe dane   Sklep firmowy   Polityka instalacji   Podsumowanie

Wybierz typ kategorii, którą chcesz dodać

Typy konfiguracji z kategorii: **VPN**

<input type="radio"/> Konfiguracja VPN (tylko dla urządzeń Samsung)	Android 14.0 - Samsung, Android 13.0 - Samsung, Android 12.0 - Samsung... (17)
<input type="radio"/> Konfiguracja VPN Cisco AnyConnect Konfiguracja klienta VPN Cisco AnyConnect	Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (63)
<input type="radio"/> Ogólna konfiguracja VPN dla urządzeń Samsung	Android 14.0 - Samsung, Android 13.0 - Samsung, Android 12.0 - Samsung... (14)
<input checked="" type="radio"/> Strongswan VPN Konfiguracja Strongswan VPN	Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (36)
<input type="radio"/> Ustawienia VPN trybu zawsze włączony	Android 13.0, Android 14.0 - Samsung, Android 13.0 - Samsung... (20)

Cofnij   **Dalej**

W konfiguracji można zdefiniować, które aplikacje powinny korzystać z połączenia VPN. Jeżeli połączenia VPN ma obejmować całe urządzenie, konfiguracja musi znaleźć się w polityce pełnego zarządzania, jeżeli dotyczyć ma kontenera to musi znaleźć się jako element polityki BYOD / WPC.

## 4.2 Urządzenia Apple

W przypadku urządzeń iOS wykorzystujemy natywnego klienta VPN, którego można skonfigurować za pomocą konfiguracji podstawowego profilu iOS, która znajduje się w:

Konfiguracje > Nowa konfiguracja > Apple > iOS, iPadOS albo macOS > VPN

Parametr Użycie Per-App VPN umożliwia zdefiniowanie nazw poszczególnych aplikacji oraz listy domen dla przeglądarki Safari, które będą się łączyć z siecią firmową poprzez VPN.

## 5 Dostęp do zasobów firmowych

### 5.1 Dostęp do zasobów firmowych dla urządzeń będących w zasięgu firmowej sieci Wi-Fi

Dzięki integracji systemu Techstep Essentials MDM z infrastrukturą i siecią firmową organizacja może mieć dodatkową kontrolę nad próbującymi się podłączyć do firmowej sieci urządzeniami. Dostęp do sieci firmowej powinny mieć tylko urządzenia zarządzane i zabezpieczone. Taka weryfikacja jest możliwa dzięki połączeniu w lokalnej sieci systemu Techstep Essentials MDM oraz punktu dostępowego Cisco ISE lub Extreme Networks.

### 5.2 Bezpieczny dostęp do poczty firmowej

Poprzez użycie Techstep Essentials Exchange Active Sync Proxy dostęp do pocztowych serwerów w organizacji jest ograniczony do urządzeń zarządzanych, zabezpieczonych i zgodnych z polityką bezpieczeństwa w systemie Techstep Essentials MDM. W takim przypadku firma ma pewność, że urządzenie spoza organizacji nie będzie miało dostępu do poczty służbowej, a w przypadku wystąpienia takiej sytuacji o takiej próbie zostanie powiadomiony administrator systemu Techstep Essentials MDM.

## 6 Wsparcie w przypadku wystąpienia wycieku danych

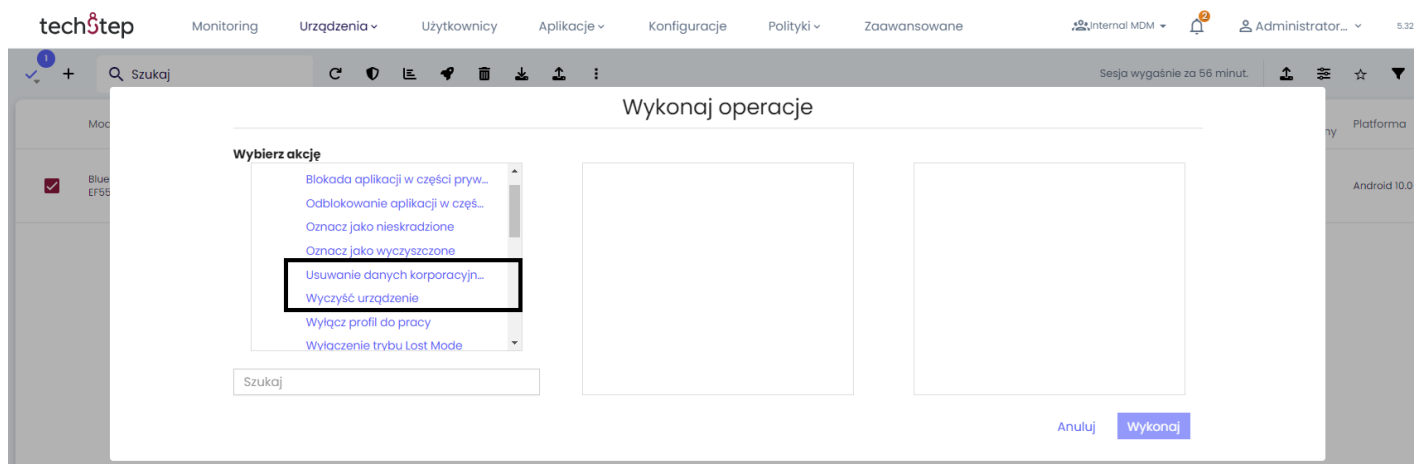
In case of the device theft or loss, the employee should report this to the IT administrator in the company. Devices that are managed and secured by Techstep Essentials MDM do not pose a threat of data leakage. The administrator can remotely locate stolen or lost device and, if necessary, send a command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

W przypadku kradzieży lub zgubienia urządzenia mobilnego pracownik powinien jak najszybciej zgłosić ten fakt administratorowi w swojej firmie. Gdy urządzenia są zarządzane i zabezpieczone przez system Techstep Essentials MDM, nie jest to powód do obaw. Administrator może zdalnie zlokalizować skradzione lub zgubione urządzenie, ewentualnie wysłać komendę wyczyszczenia danych służbowych lub wszystkich danych znajdujących się na urządzeniu.

### 6.1 Wyczyszczenie danych

Dane z urządzenia można zdalnie usunąć wysyłając komendę 'wipe'. Można to zrobić z poziomu widoku listy urządzeń Zarządzanie > Urządzenia > szczegóły danego urządzenia > wyślij komendę:

- 'Wyczyść urządzenie', aby usunąć wszystkie dane z urządzenia
- 'Usuwanie danych korporacyjnych', aby usunąć dane firmowe (kontener)

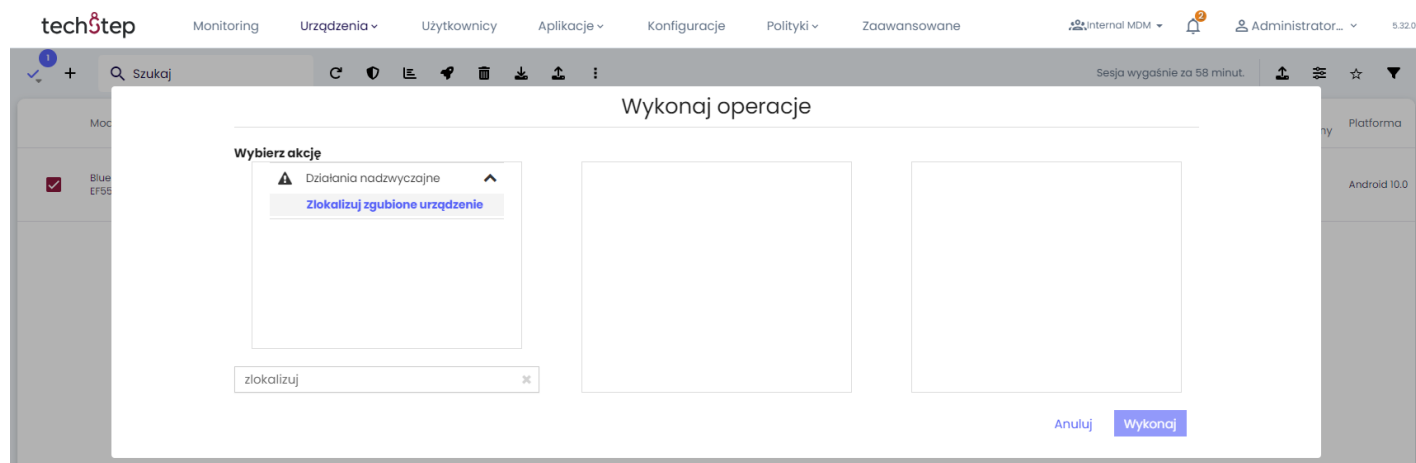


### 6.2 Zlokalizowanie skradzionego lub zgubionego urządzenia

#### 6.2.1 Urządzenia Android

Urządzenie musi mieć zainstalowany moduł lokalizacji: Polityki > Zmień ustawienia > Ustawienia podstawowe > Włącz usługi lokalizacyjne

Jeżeli zarządzane urządzenie ma zainstalowany moduł lokalizacji, to w przypadku kradzieży lub zgubienia administrator systemu Techstep Essentials MDM może zlokalizować takie urządzenie. Można to zrobić z poziomu widoku listy urządzeń: Zarządzanie > Urządzenia > szczegóły danego urządzenia > wyślij komendę > Zlokalizuj zgubione urządzenie.



## 6.2.2 Urządzenia Apple

W celu zlokalizowania skradzionego lub zgubionego urządzenia iOS, urządzenie musi zostać wprowadzone w tryb utracony (tylko dla urządzeń w trybie nadzorowanym). Od tego momentu będzie można je zlokalizować.

W celu wprowadzenia urządzenia w tryb utracony, należy przejść do widoku listy urządzeń:

Zarządzanie > Urządzenia > szczegóły danego urządzenia > wyślij komendę > Włączenie trybu Lost Mode, a następnie:

Zarządzanie > Urządzenia > szczegóły danego urządzenia > wyślij komendę > Zlokalizuj zgubione urządzenie

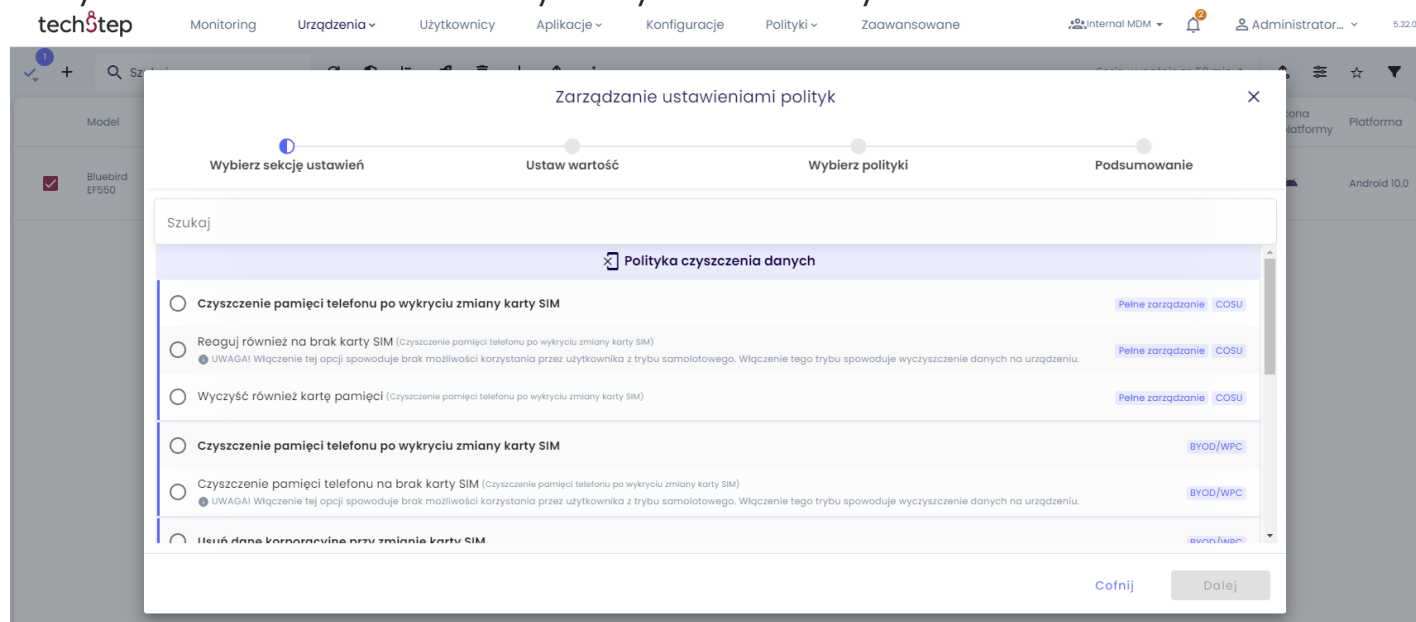
W momencie włączenia trybu utraconego urządzenie jest zablokowane dla użytkownika końcowego do momentu odblokowania go przez administratora systemu Techstep Essentials MDM.

## 6.3 Automatyczne usuwanie danych

Pamięć urządzenia może zostać wyczyszczona w przypadku kradzieży bez dodatkowej ingerencji administratora. Polityka Techstep Essentials MDM może zawierać konieczność usunięcia danych w przypadku wykrycia zmiany karty SIM lub jej braku.

Dodatkowo dane firmowe mogą zostać automatycznie usunięte w przypadku wykrycia złamania zabezpieczeń iOS (tzw. Jailbreak) lub Android (root).

## Polityki > Zmień ustawienia > Polityka czyszczenia danych



## 6.4 Przegląd operacji wykonanych z poziomu konsoli www

Wszystkie operacje w systemie Techstep Essentials MDM (inicjowane przez administratora lub wygenerowane przez system na podstawie ustawionych preferencji) są zapisywane i dostępne z poziomu logu operacji. Widok logu umożliwia zweryfikowanie, jaki rodzaj operacji został wykonany, przez kogo, kiedy i jaki jest status operacji. Aby otworzyć listę operacji, należy przejść do zakładki log:

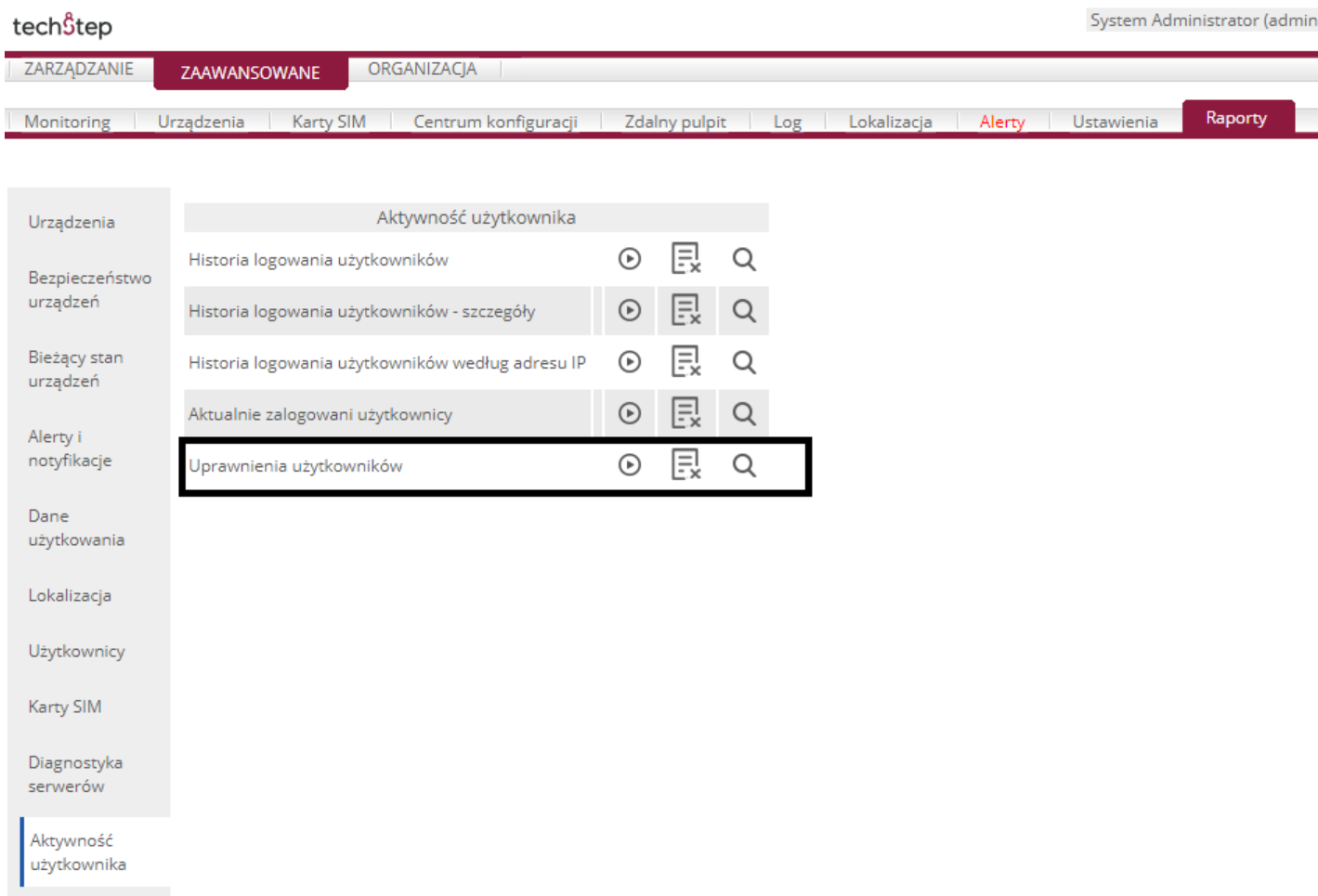
Urządzenia > Log

techStep Monitoring <span>Urządzenia</span> <span>Użytkownicy</span> <span>Aplikacje</span> <span>Konfiguracje</span> <span>Polityki</span> <span>Zaawansowane</span> <span>Internal MDM</span> <span>Administrator...</span> <span>5.32.0</span>															
Ostatnie odświeżenie: 14:47:36 <span>Sesja wygaśnie za 59 minut.</span>															
Przedział ilości rekordów: 1-9															
Akcja	Komponent	Target	Utworzono	Utworzył	Ostatni status	Status	Wiadomość	ID	Użytkownik telefonu	Numer telefonu	IMEI	Opis telefonu	Numer seryjny urządzenia	UID urządzenia	Identyfikator urządzenia
Uruchomiony	Agent Zdalny dostęp	Urządzenie	2 lata temu		2 lata temu	1		2182	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Uruchom	Agent Zdalny dostęp	Urządzenie	2 lata temu	Administrator, System	2 lata temu	1		2181	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Uruchom	Agent Zdalny dostęp	Urządzenie	2 lata temu	Administrator, System	2 lata temu	1		2180	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Uruchomiony	Agent Zdalny dostęp	Urządzenie	2 lata temu		2 lata temu	1		2179	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Uruchom	Agent Zdalny dostęp	Urządzenie	2 lata temu	Administrator, System	2 lata temu	1		2178	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957
Odśwież politykę	Polityka Default policy	Urządzenie	2 lata temu	Administrator, System	2 lata temu	3		2175	admin@tech		356661460045957	Added in Device Owner mode ...	EF550RA4LAWBC319		356661460045957

## 6.5 Przegląd uprawnień użytkowników

Każdy użytkownik mogący logować się do systemu Techstep Essentials MDM posiada uprawnienia nadane przez administratora organizacji. Uprawnienia te mogą umożliwiać potencjalny dostęp do danych osobowych. W prosty sposób można wyświetlić uprawnienia i ich zakres przypisane do danego użytkownika w systemie Techstep Essentials MDM.

Aby wyświetlić raport uprawnień dla każdego z użytkowników należy przejść do: Zaawansowane > Raporty > Aktywność użytkownika > Uprawnienia użytkowników



The screenshot displays the Techstep Essentials MDM web interface. At the top, the 'techStep' logo is on the left, and 'System Administrator (admin)' is on the right. Below the header, there are two main navigation tabs: 'ZARZĄDZANIE' and 'ZAAWANSOWANE'. Under 'ZAAWANSOWANE', there are several sub-tabs: 'Monitoring', 'Urządzenia', 'Karty SIM', 'Centrum konfiguracji', 'Zdalny pulpit', 'Log', 'Lokalizacja', 'Alerty', 'Ustawienia', and 'Raporty'. The 'Raporty' tab is currently selected. On the left side, there is a sidebar with a list of navigation items: 'Urządzenia', 'Bezpieczeństwo urządzeń', 'Bieżący stan urządzeń', 'Alerty i notyfikacje', 'Dane użytkowników', 'Lokalizacja', 'Użytkownicy', 'Karty SIM', 'Diagnostyka serwerów', and 'Aktywność użytkownika'. The 'Aktywność użytkownika' item is highlighted. The main content area shows a section titled 'Aktywność użytkownika' with a list of user activity logs. The logs are organized into a table with columns for the activity name, a play button icon, a document icon, and a search icon. The 'Uprawnienia użytkowników' (User Permissions) entry is highlighted with a black border.

Aktywność użytkownika			
Historia logowania użytkowników	▶	📄	🔍
Historia logowania użytkowników - szczegóły	▶	📄	🔍
Historia logowania użytkowników według adresu IP	▶	📄	🔍
Aktualnie zalogowani użytkownicy	▶	📄	🔍
<b>Uprawnienia użytkowników</b>	▶	📄	🔍