techstep

Techstep Essentials MDM

Zgodność z RODO i NIS2

Data: 01/03/2024

Spis treści

OPUBLIKOWANY PRZEZ:

Techstep Poland Sp. Z o.o.

Ul. Wajdeloty 12A

80-437 Gdańsk

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. Dyrektywa NIS2 przez oprogramowanie Essentials MDM

Niniejszy dokument ma na celu przedstawienie sposobu, w jaki oprogramowanie Essentials MDM spełnia wymagania Dyrektywy o Bezpieczeństwie Sieci i Systemów Informacyjnych (NIS2).

Essentials MDM zostało zaprojektowane jako kompleksowe narzędzie do zarządzania urządzeniami mobilnymi w organizacjach. Jest to narzędzie niezbędne dla firm, aby skutecznie zarządzać, monitorować i zabezpieczać urządzenia mobilne w swojej infrastrukturze informatycznej.

2.1 Zgodność z Dyrektywą NIS2

Aby spełnić wymagania Dyrektywy NIS2, Essentials MDM zapewnia następujące funkcjonalności:

- Zarządzanie identyfikacją i autoryzacją: Oprogramowanie umożliwia centralne zarządzanie tożsamością i autoryzacją użytkowników, co pozwala na precyzyjne kontrolowanie dostępu do danych i zasobów w organizacji.

- Zarządzanie dostępem i uprawnieniami: Essentials MDM umożliwia administratorom ustalanie i kontrolowanie poziomów dostępu oraz uprawnień użytkowników do różnych funkcji i zasobów na urządzeniach mobilnych.

- Monitorowanie zdarzeń i incydentów: Oprogramowanie automatycznie monitoruje działania na urządzeniach mobilnych, identyfikując potencjalne zagrożenia i incydenty bezpieczeństwa. Dzięki temu administratorzy są w stanie szybko reagować na wszelkie nieprawidłowości.

- Zabezpieczenia techniczne: Essentials MDM oferuje szereg funkcji zabezpieczeń technicznych, takich jak szyfrowanie danych, zdalne blokowanie lub kasowanie danych w przypadku kradzieży lub utraty urządzenia oraz zdalne zarządzanie politykami bezpieczeństwa.

- Wymagania dotyczące raportowania: Oprogramowanie generuje szczegółowe raporty dotyczące aktywności użytkowników, zdarzeń bezpieczeństwa oraz stanu zabezpieczeń na urządzeniach mobilnych, co umożliwia organizacjom spełnienie wymogów dotyczących raportowania zgodnie z Dyrektywą NIS2.

2.2 Konsultacja z ekspertami ds. bezpieczeństwa

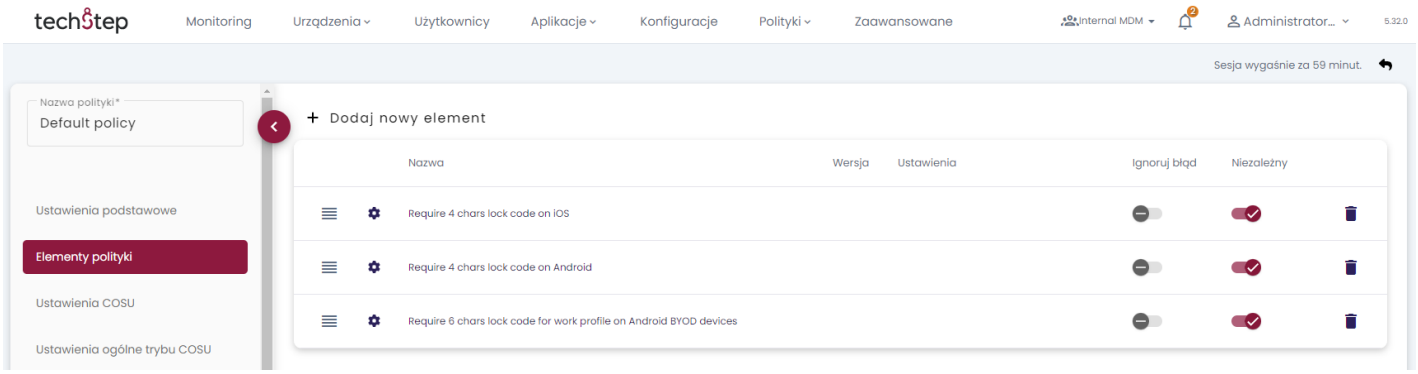
Essentials MDM zostało opracowane we współpracy z ekspertami ds. bezpieczeństwa informatycznego, aby zapewnić, że spełnia ono najwyższe standardy bezpieczeństwa i zgodności z obowiązującymi przepisami, w tym Dyrektywą NIS2.

1 Kontrola dostępu do danych z urządzeń mobilnych

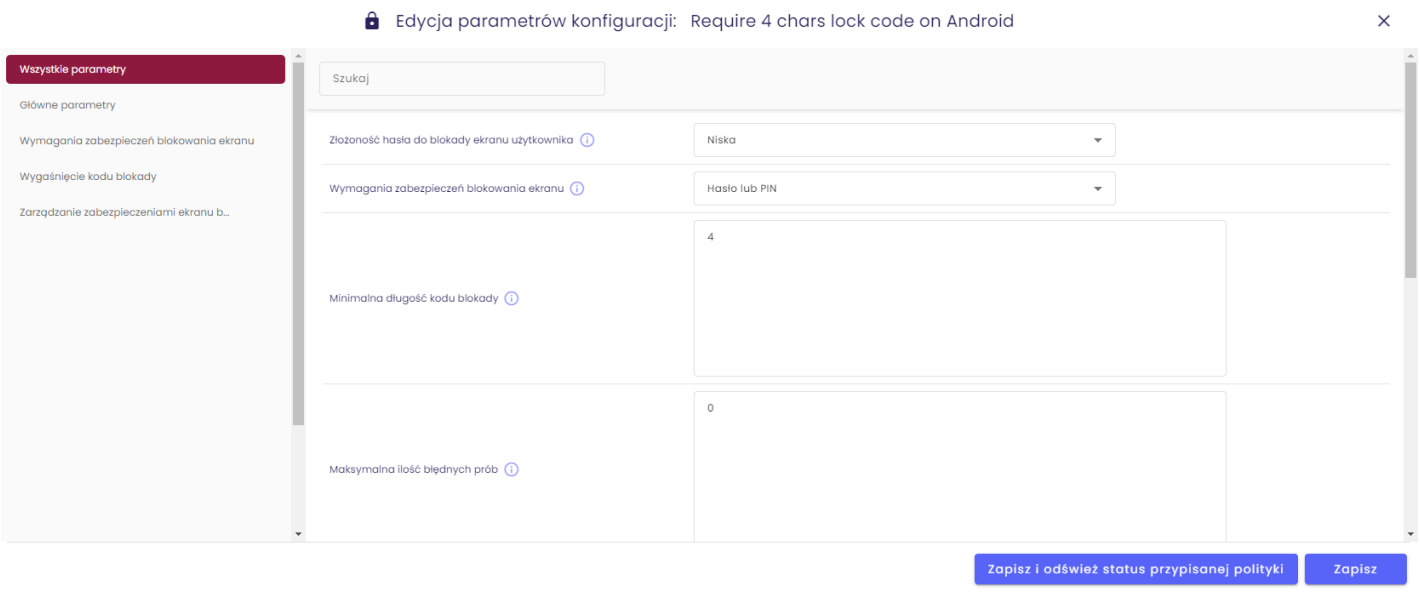
Dostęp do danych przechowywanych na urządzeniu można chronić na kilka sposobów. Jednym z podstawowych jest zabezpieczenie urządzenia mobilnego poprzez kod blokady. System Techstep Essentials MDM wymusza ustawienie kodu blokady urządzenia poprzez dedykowaną konfigurację, którą można dodać do polityki 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.



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’.

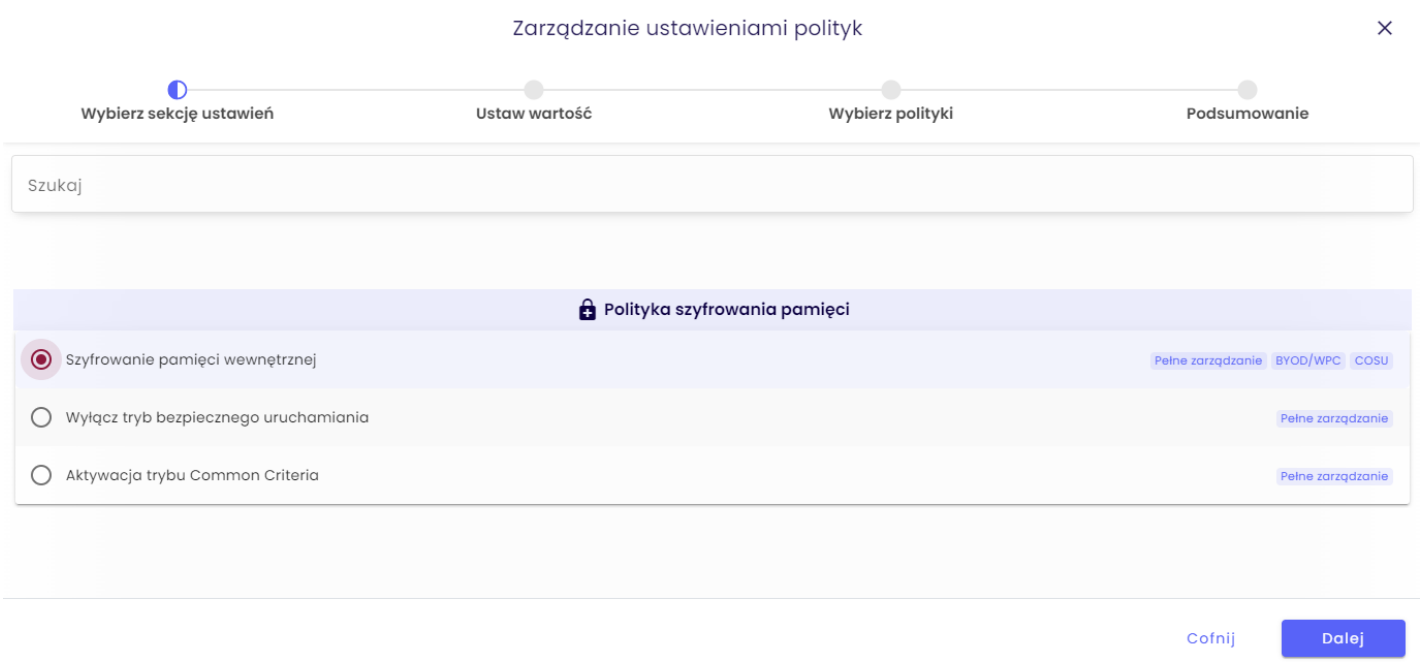


Szyfrowanie pamięci urządzenia mobilnego jest kolejnym sposobem na ochronę danych przechowywanych na urządzeniach mobilnych. Urządzenia sprzedawane z systemem Android w wersji co najmniej 6 oraz iOS 10 mają domyślnie szyfrowaną pamięć wewnętrzną. Jednakże, aby w pełni chronić dane przechowywane w pamięci 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’.



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.

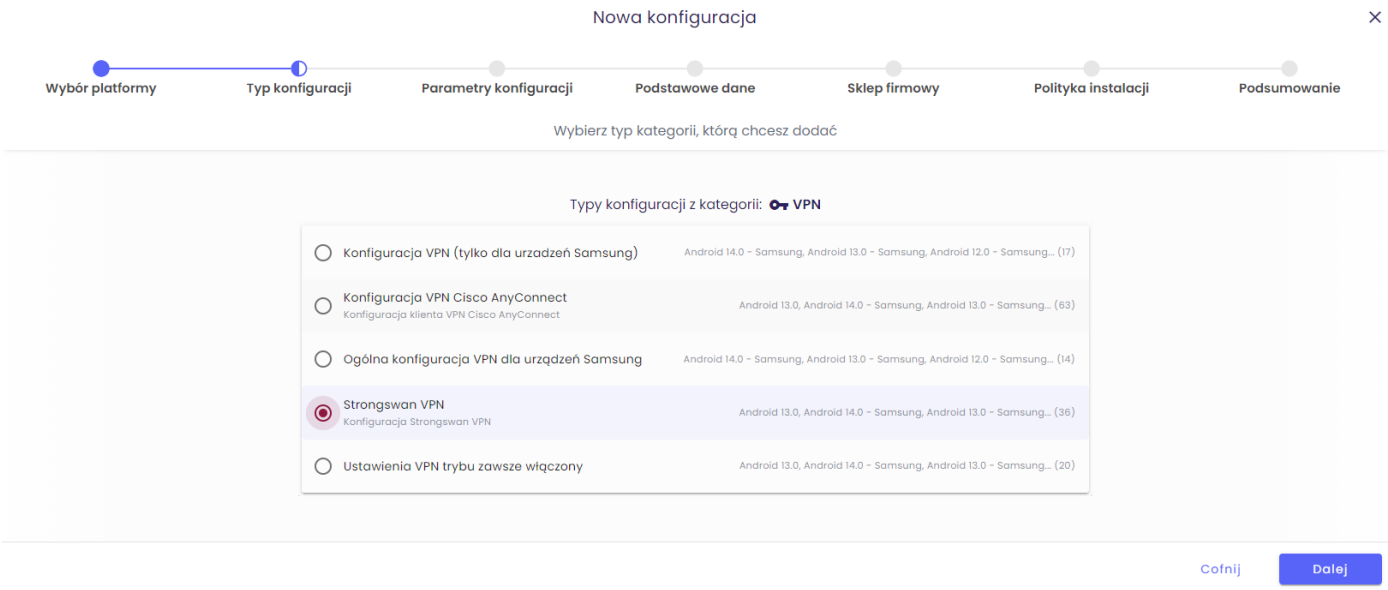
4. Dostęp do zasobów firmowych dla urządzeń będących w terenie

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.



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.

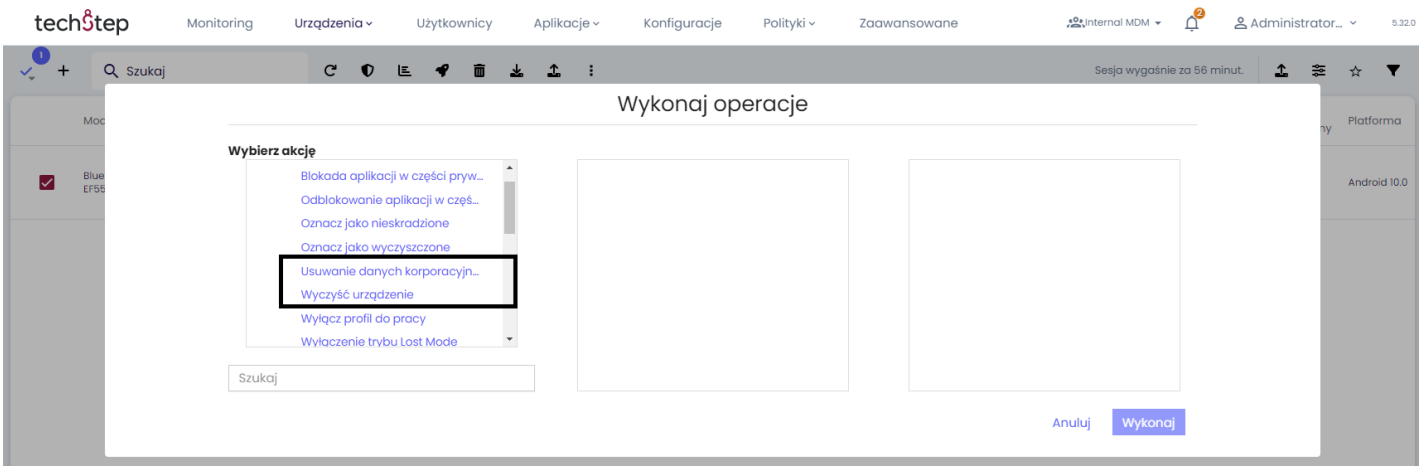
6. Wsparcie w przypadku wystąpienia wycieku danych

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)

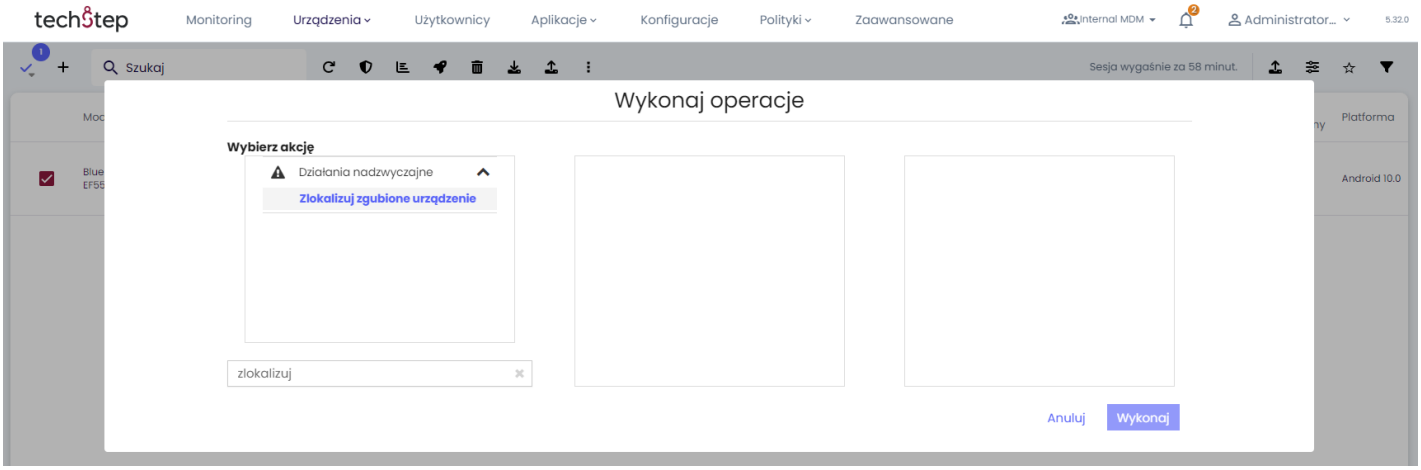


6.2 Zlokalizowanie skradzionego lub zgubionego urządzenia

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

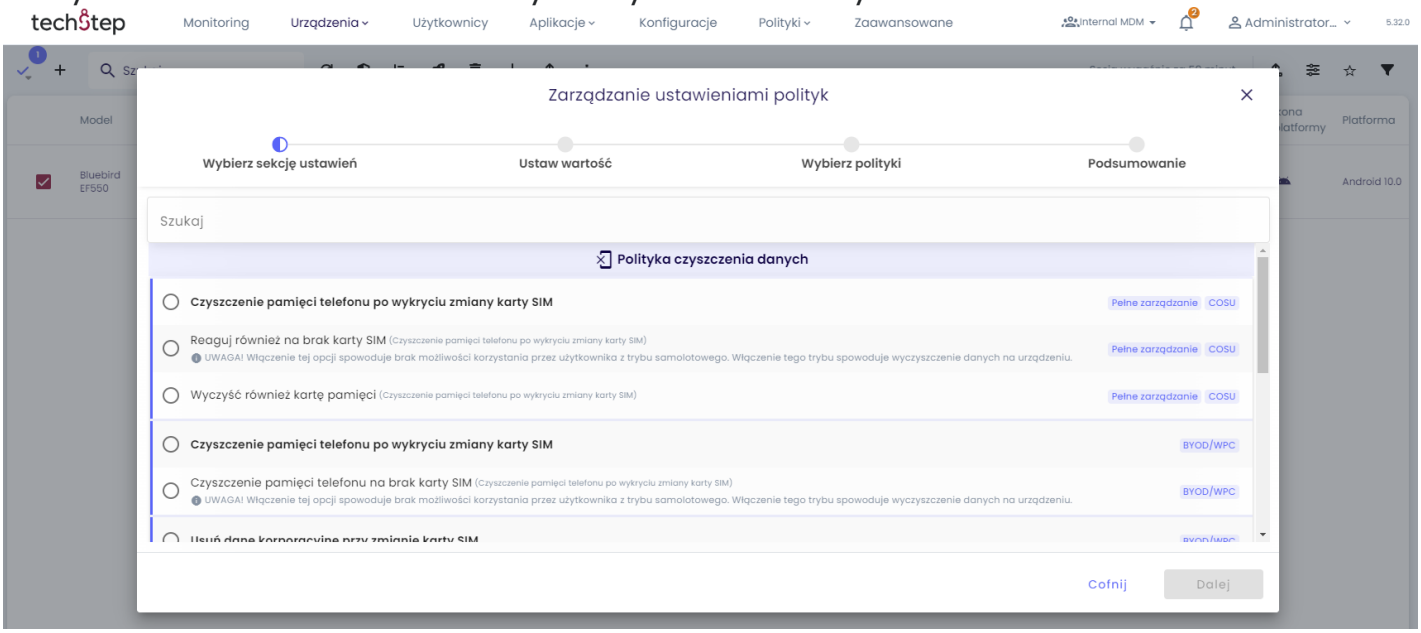
W momencie włączenia trybu utraconego urządzenie jest zablokowane dla użytkownika końcowego do momentu odblokowania go przez administratora systemu Techstep Essentials MDM.

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.

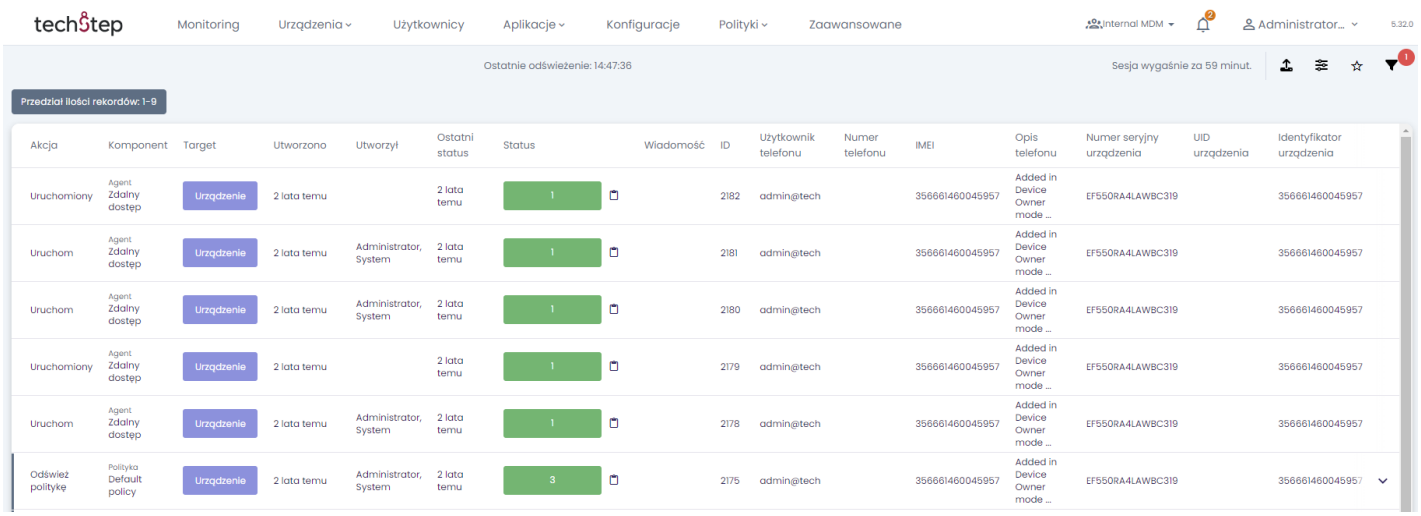
Dodatkowo dane firmowe mogą zostać automatycznie usunięte w przypadku wykrycia złamania zabezpieczeń iOS (tzw. Jailbreak) lub Android (root).

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



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