



Przewodnik integracji Android Enterprise Zero-Touch

Data: 29/11/2023



1- Na czym polega Android Enterprise zero-touch?

Android Enterprise zero-touch pozwala przedsiębiorstwu rejestrować urządzenia firmowe w systemie EMM z pominięciem ręcznej procedury rejestracji. Integracja Android Enterprise zero-touch z Essentials MDM daje możliwość automatycznej rejestracji wszystkich urządzeń z systemem Android 8 i nowszym.

Więcej informacji można znaleźć na stronie Android Enterprise zero-touch:

<https://www.android.com/enterprise/management/zero-touch/>

2- Integracja serwera Essentials MDM z usługą zero-touch

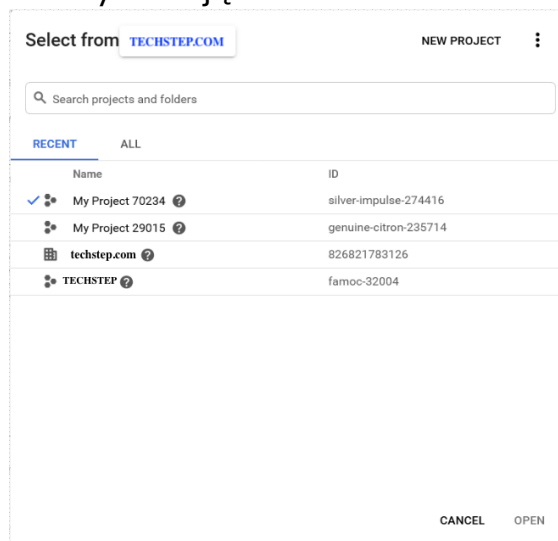
Aby móc korzystać z integracji Essentials MDM zero-touch, administrator Essentials musi zintegrować i autoryzować całą maszynę Essentials MDM Server do odpowiedniego API Enterprise Google. Wymagane jest posiadanie przez administratora Essentials

- Dostępu SSH do maszyny aplikacji Essentials
- Konta Google

2.1 Utwórz projekt Google Developer

Korzystając z konta Google zaloguj się do Google Developer Console - <https://console.developers.google.com>

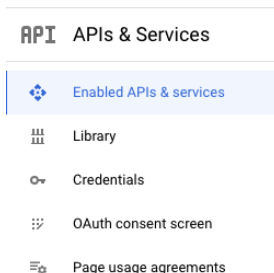
Po zalogowaniu utwórz nowy projekt. Będzie on zawierał wszystkie ustawienia zero-touch dla tej integracji serwera Essentials MDM, w tym odpowiednie dane uwierzytelniające.



Wybierz nazwę dla swojego projektu. Pomoże to zidentyfikować go w przyszłości. Gdy ikona powiadomienia wskazuje, że projekt jest gotowy – wszystko jest gotowe do włączenia Enterprise API.

2.2 Włączenie API Enterprise

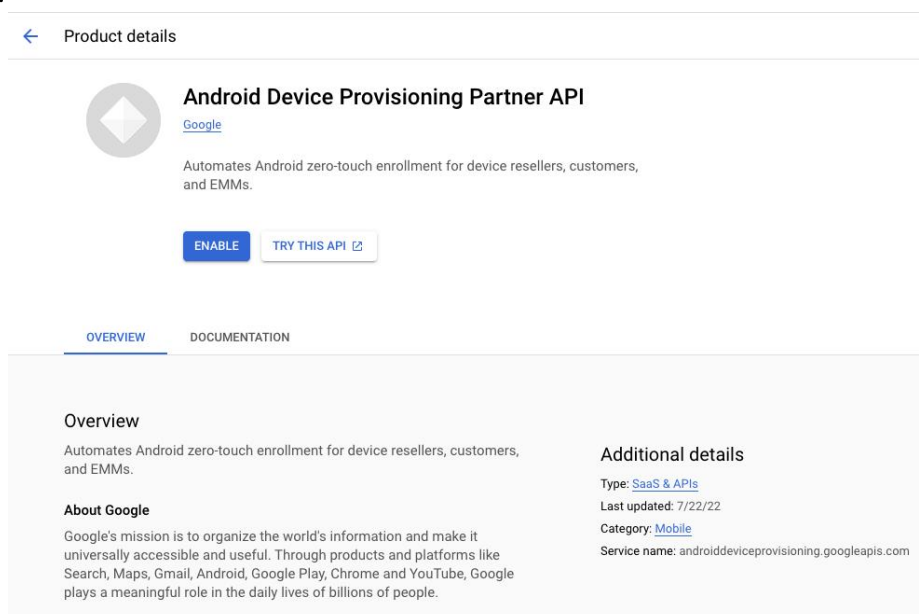
Upewnij się, że wybrałeś swój projekt, a następnie wybierz z menu po prawej stronie Biblioteka (Library) lub kliknij "WŁĄCZ APIS I USŁUGI" (ENABLE APIS AND SERVICES).



Aby obsługiwać usługę zero-touch, utworzony właśnie projekt Google wymaga włączenia następującego interfejsu API:

- Android Device Provisioning Partner API
(Nazwa usługi: *androiddeviceprovisioning.googleapis.com*)

Wyszukaj i wybierz ten interfejs API z biblioteki Google, a następnie kliknij "ENABLE".

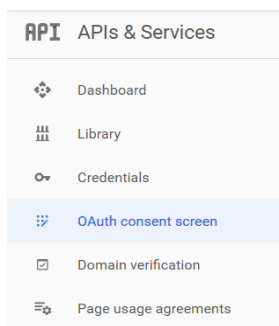


2.3 Konfiguracja poświadczeń API

Essentials zero-touch Integration wykorzystuje poświadczenia OAuth 2.0 do uwierzytelniania i autoryzacji. W tym kroku skonfigurujemy tę metodę.

2.3.1 Konfiguracja ekranu zgody OAuth

Upewnij się, że wybrałeś swój projekt, a następnie wybierz z menu po prawej stronie ekran zgody OAuth (**OAuth consent screen**).



Poniższy ekran zgody OAuth zostanie wyświetlony administratorowi, który dodaje konto zero-touch do organizacji w Essentials MDM. Najpierw należy wybrać typ użytkownika: Wewnętrzny/Internal (tylko użytkownicy z organizacji) lub Zewnętrzny/External (dowolny użytkownik z kontem Google). Wypełnij odpowiednie informacje, zwracając szczególną uwagę na pola:

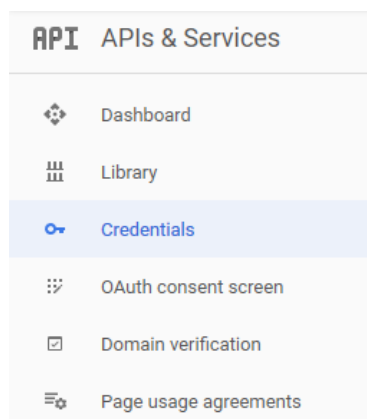
- Nazwa aplikacji/Application name (wymagane)
- E-mail działu wsparcia/Support e-mail (wymagane)
- Autoryzowane domeny/Authorized domains (wymagane) - musi to być domena najwyższego poziomu, na której hostowany jest serwer Essentials MDM (np. jeśli urządzenie jest hostowane na "emm.company.com", domeną najwyższego poziomu będzie "company.com").
- Logo aplikacji/Application logo (opcjonalne) wymagane, jeśli chcesz używać logo, w przeciwnym razie - opcjonalne
- Link do strony głównej aplikacji, link do polityki prywatności aplikacji/Application Homepage link, Application Privacy Policy link

The screenshot shows the 'OAuth consent screen' configuration page. It includes sections for 'Application type' (Public or Internal), 'Application name', 'Application logo', 'Support email', and 'Scopes for Google APIs'. The 'Internal' application type is selected. The application name is 'TECHSTEP'. The application logo is a red square with a white 'S' icon. The support email is 'support@techstep.no'. The scopes for Google APIs are 'email', 'profile', and 'openid'. On the right side, there is information about the consent screen, OAuth verification, and OAuth grant limits. The 'Raise limit' button is visible at the bottom right.

Po skonfigurowaniu kliknij przycisk ZAPISZ (SAVE) u dołu strony.

2.3.2 Konfiguracja identyfikatora klienta OAuth

Po skonfigurowaniu ekranu zgody OAuth można wygenerować dane uwierzytelniające dla serwera Essentials MDM. Upewnij się, że wybrałeś swój projekt, a następnie wybierz z menu po prawej stronie opcję Poświadczenia (**Credentials**).



Kliknij CREATE CREDENTIALS i z rozwijanego menu wybierz OAuth Client ID i wybierz Web application:

[+ CREATE CREDENTIALS](#) [DELETE](#)

API key
Identifies your project using a simple API key to check quota and access.

OAuth client ID
Requests user consent so that your app can access the user's data.

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

Wypełnij odpowiednie informacje, zwracając największą uwagę na szczegóły pól:

- Nazwa/Name (wymagane) – Wewnętrzna nazwa poświadczeń (nie będzie wyświetlana użytkownikom).
- Autoryzowane pochodzenie JavaScript/Authorized JavaScript origins (wymagane) – Adres komputera Essentials MDM Server, w formacie: `https://emm.yourcompany.com`. Musi być zgodny z autoryzowaną domeną najwyższego poziomu na skonfigurowanym ekranie zgody OAuth.
- Autoryzowane URI przekierowania/Authorized redirect URLs (wymagane) – adres zwrotny używany podczas rejestracji zero-touch. Ma format: `https://emm.yourcompany.com/ui/devices/enrollment/zeroTouch`. Musi być zgodny z autoryzowaną domeną najwyższego poziomu na skonfigurowanym ekranie zgody OAuth.

Przewodnik integracji Android Enterprise Zero-Touch

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

Application type *
Web application

[Learn more](#) about OAuth client types

Name *
Web client 3

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorised domains](#).

Authorised JavaScript origins **?**

For use with requests from a browser

+ ADD URI

Authorised redirect URIs **?**

For use with requests from a web server

+ ADD URI

CREATE

CANCEL

Po skonfigurowaniu kliknij CREATE u dołu strony. Pojawi się okno potwierdzenia z identyfikatorem klienta i tajnym hasłem klienta.

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is published. This may require a verification process that can take several days.


Your Client ID
711782125315-k1b5rcnop29qan6o20c28h1eqs719rbt.apps.gc

Your Client Secret
kb0Tcnhrzx-04tCJJWdQqLtw

OK

Pobierz swoje dane uwierzytelniające, klikając przycisk Pobierz JSON (Download JSON) obok danych uwierzytelniających, które właśnie skonfigurowałeś.

OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID				
<input type="checkbox"/>	Web client 3	12 May 2020	Web application	711782125315-k1b5...				

2.4 Dodawanie poświadczeń do serwera Essentials MDM

Ostatnim krokiem do integracji zero-touch z serwerem Essentials MDM jest dodanie poświadczeń z poprzedniego kroku do serwera. Aby to zrobić, należy najpierw zalogować się do serwera Essentials MDM Server przez SSH na użytkownika z uprawnieniami roota. Po autoryzacji edytuj ten plik za pomocą wybranego edytora, np:

```
[root@famoc-app /]# nano /var/www/aplikacje/config.php
```

W pliku należy znaleźć sekcję zaczynającą się od: `/*--BEGIN CUSTOM GLOBAL--*/` i odpowiednio dodać zawartość pobranego pliku:

```
/*--BEGIN CUSTOM GLOBAL--*/  
$cons_zt_json='CONTENT_OF_JSON_CREDENTIALS_FILE';  
/*--END CUSTOM GLOBAL--*/
```

Zapisz plik i zamknij sesję SSH. Serwer Essentials MDM jest gotowy, a administratorzy mogą zacząć korzystać z zalet integracji bezdotykowej.

3- Dodawanie konta zero-touch do organizacji Essentials MDM

Aby rozpocząć dodawanie urządzeń zero-touch do Essentials MDM, należy dodać firmowe konto zero-touch do organizacji. Można to zrobić za pomocą kreatora masowej rejestracji w zakładce Urządzenia. Po zalogowaniu się jako administrator organizacji przejdź do karty URZĄDZENIA, a następnie najedź kursorem na ikonę + i wybierz opcję Masowe dodawanie.

Przewodnik integracji Android Enterprise Zero-Touch

techStep Monitoring Urządzenia Użytkownicy Aplikacje Konfiguracje Polityki Kampanie BETA Zaawansowane

Sesja wygaśnie za 117 minut.

✓ + Szukaj

Dodaj urządzenie

Masowe dodawanie


Utwórz wpis (dodaj później)

	Numer telefonu	Metoda rejestracji	Tryb urządzenia	Ostatni kontakt	Utworzone	Ostatnio zmieniane
<input type="checkbox"/>	0-0b34-8d-273...	KME	COSU	2023-06-09 14:49:09	2023-05-04 10:12:41	2023-06-09 08:40:54
<input type="checkbox"/>	Samsung SM-S901B Galaxy S22 5G Added from startup page	STARTUP PAGE	BYOD	2023-03-08 09:50:47	2023-03-08 09:50:47	

Następnie wybierz metodę Android zero-touch:

Metody masowego dodawania

Dodawanie automatyczne



Dodaj nowe i fabrycznie zresetowane urządzenia do MDM, by pracownicy byli gotowi do pracy od pierwszego uruchomienia urządzenia.

Główne korzyści:

- Dodanie urządzenia po wyjęciu z pudełka
- Brak możliwości usunięcia MDM
- Uproszczone rozpoczęcie pracy z urządzeniem

Wybierz metodę:

Apple DEP



Program rejestracji urządzeń pozwala na automatyczne dodawanie i skonfigurowanie urządzeń iOS Twojej organizacji.

Android Zero-Touch



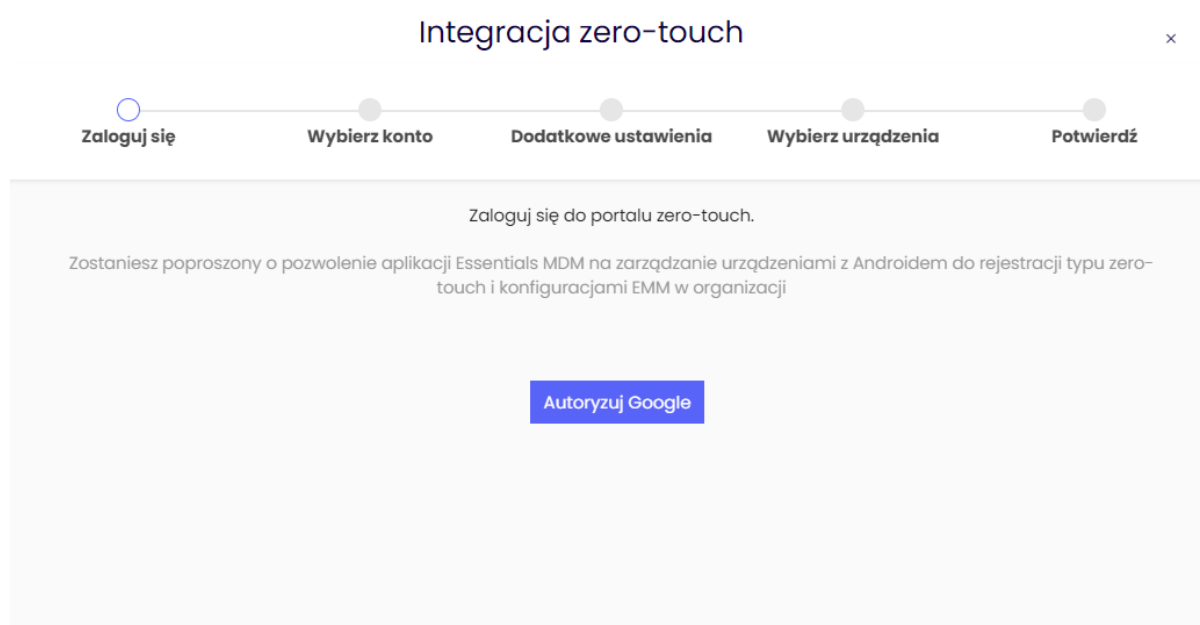
Android zero-touch pozwala na bezproblemową konfigurację i wdrażanie Androidowych urządzeń firmowych.

Samsung KME

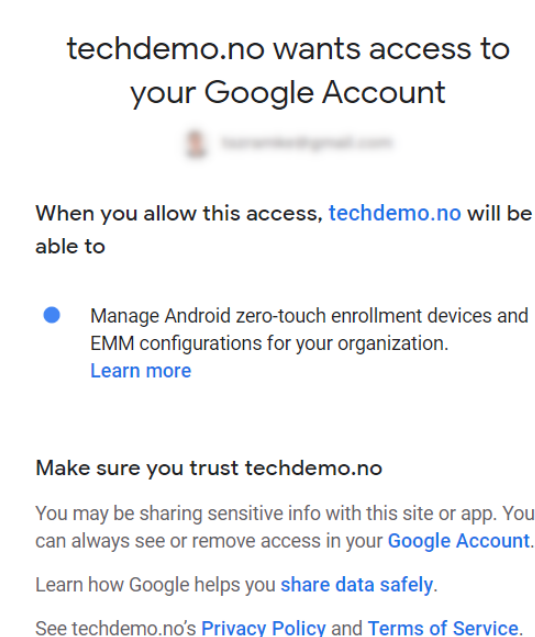
SAMSUNG

Usługa Knox Mobile Enrollment pozwala dodawać wiele urządzeń Samsung do systemu MDM bez konieczności ręcznej konfiguracji.

Aby dodać nową integrację zero-touch, użyj przycisku Rozpocznij. Otworzy się okno dialogowe, które poprowadzi Cię przez proces autoryzacji. Wybierz Autoryzuj Google:



Zaloguj się na swoje konto administratora zero-touch i przyznaj odpowiednie uprawnienia Essentials MDM:



Po pomyślnej autoryzacji Essentials MDM będzie mógł zarządzać integracją zero-touch. Z rozwijanej listy wybierz konto zero-touch, z którym chcesz się zintegrować (jeśli konto administratora jest połączone z więcej niż jedną firmą w konsoli zero-touch). Następnie wybierz domyślnego użytkownika urządzeń w Essentials MDM i przypisz grupy urządzeń. Możesz także zdecydować, czy chcesz zażądać poświadczeń od użytkownika podczas procesu rejestracji. Istnieje również

Przewodnik integracji Android Enterprise Zero-Touch

możliwość rejestrowania urządzeń w trybie BYOD (w tym trybie administrator Essentials MDM zarządza tylko częścią profilu roboczego urządzenia).

Integracja zero-touch

Zaloguj sięWybierz kontoDodatkowe ustawieniaWybierz urządzeniePotwierdź

Wybierz konto zero-touch, z którym chcesz zintegrować Essentials MDM

Nazwa konta

FancyFon ZT Test

Email administratora ⓘ

Domyślny użytkownik importowanych urządzeń

admin.techstep, admin.techstep (admin.techstep)

Metoda dodawania

Urządzenie w pełni zarządzane (COBO)

Urządzenie służbowe z profilem do pracy (WPC)

Urządzenie dedykowane (COSU)

Urządzenie współdzielone **BETA**

Metoda uwierzytelniania ⓘ

Brak uwierzytelniania

Poświadczenia użytkownika

Kod startowy

Grupy urządzeń

Wybierz grupę

Dalej

Na następnym ekranie podaj dane swojej firmy, które zostaną przedstawione użytkownikowi podczas procesu rejestracji urządzenia:

Integracja zero-touch

Zaloguj sięWybierz kontoDodatkowe ustawieniaWybierz urządzeniePotwierdź

Nazwa klienta

test

Numer telefonu działu wsparcia

4888888888

Adres e-mail działu wsparcia

test@test.com

Dodatkowa informacja

Urządzenie jest zarządzane.

test skonfigurował urządzenie do pełnego zarządzania. Jeśli uważasz, że to błąd, skontaktuj się w następujący sposób:

☎ 4888888888

@ test@test.com

Wiadomość od test

Informacje o urządzeniu

Cofnij

Dalej

techstep₁₁

Na koniec wybierz urządzenia, które chcesz zaimportować do Essentials. Możesz wybrać wymagane urządzenia ręcznie lub wybrać opcję Automatyczny import, dzięki której nowe urządzenia będzie okresowo (co 30 minut) synchronizować się z zero-touch do Essentials MDM. Jeśli chcesz zażądać autoryzacji użytkownika do rejestracji określonego urządzenia, wybierz opcję Wymagaj poświadczeń.

Urządzenie może znajdować się w jednym z 3 stanów, w oparciu o jego przypisanie do konfiguracji zero-touch:

- NIEPRZYPISANE – urządzenie nie ma konfiguracji zero-touch (i otrzyma ją, jeśli zostanie wybrana lub jeśli wybrano automatyczny import)
- AKTUALNA – urządzenie ma przypisaną aktualną konfigurację zero-touch (i nie otrzyma nowej konfiguracji podczas synchronizacji)
- INNY – urządzenie ma już przypisaną inną konfigurację EMM zero-touch. Domyślnie nie otrzyma nowego profilu zero-touch podczas automatycznego importu. Aby zastąpić inny profil EMM, musisz wybrać wymagane urządzenia w tym kroku.

Integracja zero-touch

Zaloguj sięWybierz kontoDodatkowe ustawieniaWybierz urządzeniaPotwierdź

Wybierz urządzenia do importu lub pozwól, aby Essentials MDM importował wszystkie nieprzypisane urządzenia

Jeśli masz urządzenia powiązane z innymi konfiguracjami EMM, musisz je wybrać ręcznie, aby zostały zaimportowane

Automatyczny import ☒Zaznacz wszystko (4) ☐

	IMEI	Producent	Numer seryjny	Metoda uwierzy...	Importuj do tryb...	Dodaj do trybu ...	Dodaj do trybu ...	Status
<input type="checkbox"/>				Domyślna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INNY
<input type="checkbox"/>				Domyślna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INNY
<input type="checkbox"/>				Domyślna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INNY
<input type="checkbox"/>				Domyślna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	INNY

Cofnij

Dalej

Po wybraniu konfiguracji kliknij przycisk Synchronizuj, aby dodać urządzenia do konta Essentials MDM. Nastąpi przekierowanie do ekranu podsumowania.

Integracja zero-touch

Zaloguj się

Wybierz konto

Dodatkowe ustawienia

Wybierz urządzenia

Potwierdź

Upewnij się że dane synchronizacji się zgadzają i kliknij przycisk Synchronizuj

Urządzenia do zaimportowania: 0

Urządzenia do odłączenia: 0

Cofnij

Synchronizuj

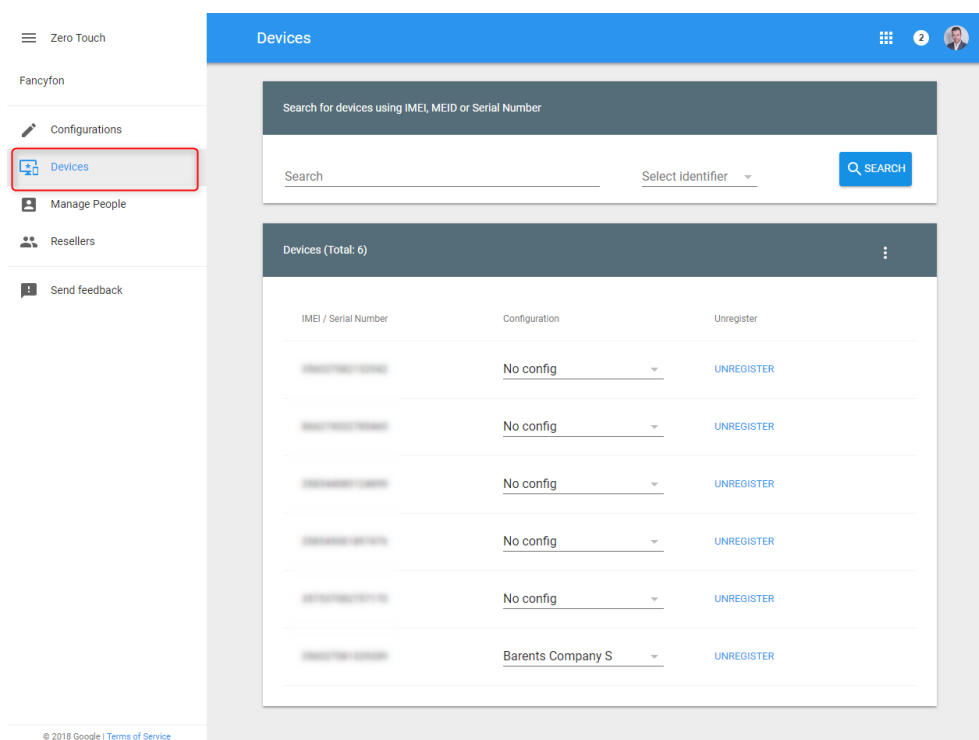
Co chcesz teraz zrobić?

Dodaj wiele urządzeń

Idź do listy urządzeń

Idź do ustawień

Przejdź do portalu Zero-Touch w przeglądarce i zaloguj się na swoje konto (<https://partner.android.com/zerotouch>). Przejdź do zakładki: Urządzenia. Zobaczysz urządzenia swojej organizacji.



Sekcja Dostępne urządzenia dostarcza informacji: liczba pomyślnie zaimportowanych urządzeń / liczba wybranych urządzeń.

W przypadku jakichkolwiek problemów z importem przejdź do dziennika systemowego, aby uzyskać więcej informacji.

Po zakończeniu synchronizacji – wszystko gotowe! Po włączeniu urządzenia zostaną zarejestrowane w Essentials MDM.