

Aby móc korzystać z integracji FAMOC zero-touch, administrator FAMOC musi zintegrować i autoryzować cały serwer FAMOC Server do odpowiedniego Enterprise Google API. Jako administrator FAMOC będziesz potrzebował:

- Dostępu SSH do twojego komputera aplikacji FAMOC
- Aktywnego konta Google

Tworzenie projektu Google Developer

Do zalogowania się do Konsoli Developera Google należy użyć danych konta Google.

- <https://console.developers.google.com>

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

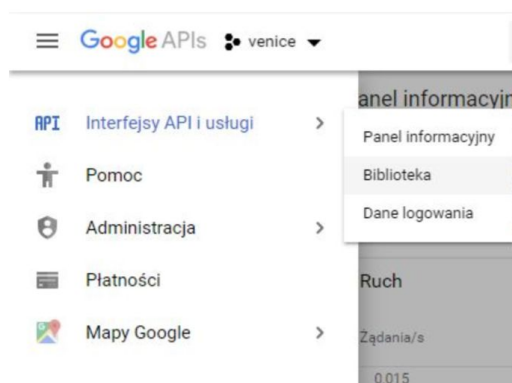


Wybierz nazwę swojego projektu. To pomoże ci zidentyfikować to w przyszłości. Gdy ikona powiadomienia wskazuje, że projekt jest gotowy - można przystąpić do włączenia Enterprise API.

Uruchomienie Enterprise API

Upewnij się, że wybrałeś swój projekt, a następnie przejdź do:

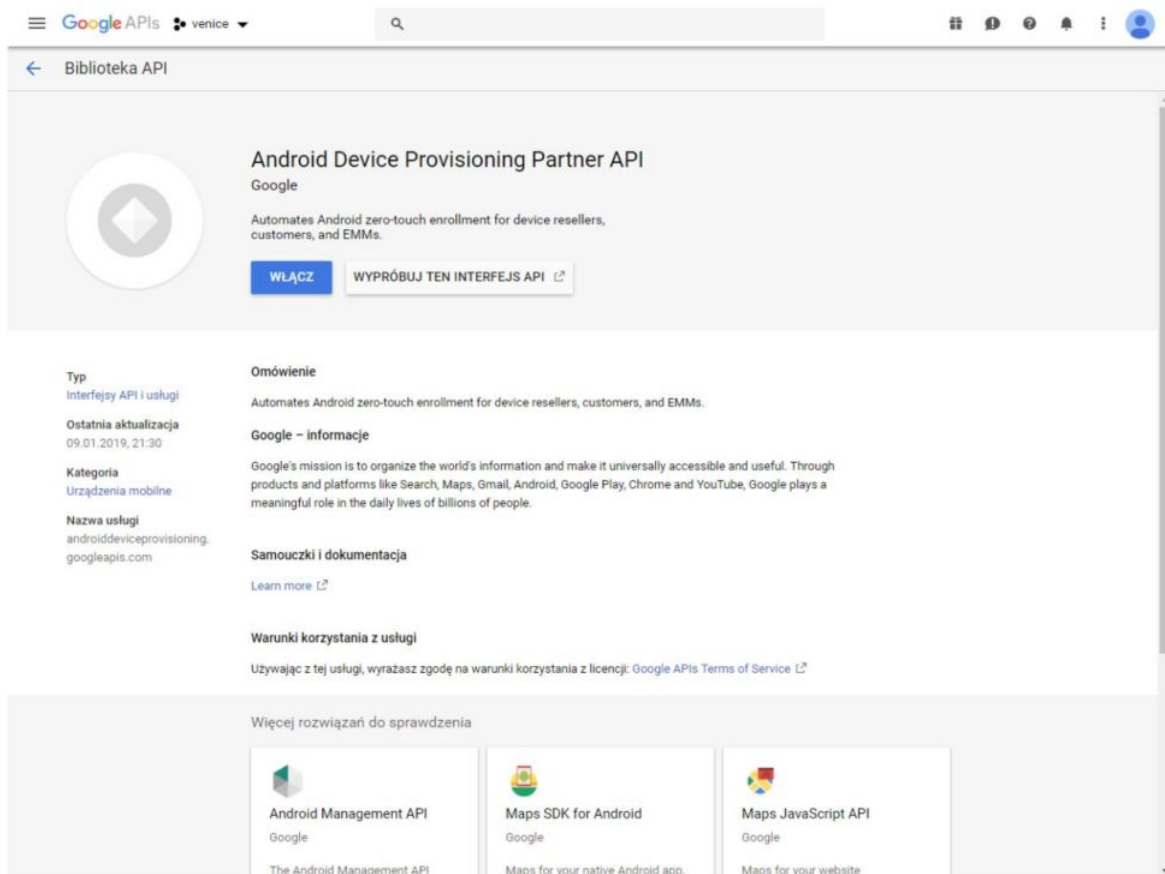
- "Menu" -> "API i usługi" -> "Biblioteka"
- lub kliknij "WŁĄCZ API I USŁUGI"



Aby obsługiwać funkcję "zero-touch", Google Project, który właśnie utworzyłeś, musi mieć włączony następujący interfejs API:

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

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



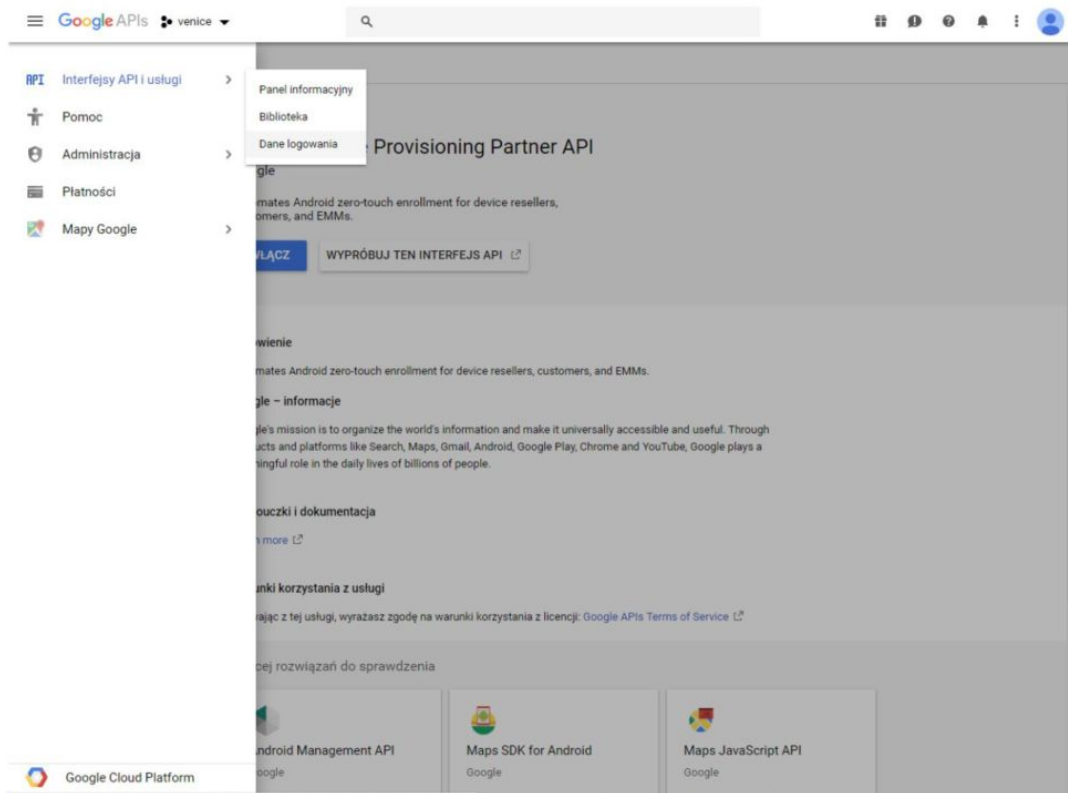
Konfiguracja poświadczeń interfejsu API

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

Konfiguracja ekranu zgody OAuth

Upewnij się, że wybrałeś swój projekt, a następnie przejdź do:

- "Menu" -> "APIs i usługi" -> "Poświadczenia" -> "Ekran zgody OAuth"



Ten ekran zgody OAuth zostanie przedstawiony administratorowi, który dodaje konto zero-touch do organizacji w FAMOC. Wypełnij odpowiednie informacje, zwracając szczególną uwagę na pola:

- Nazwa aplikacji (wymagane)
- E-mail pomocy (wymagane)
- Autoryzowane domeny (wymagane)
- Musi to być domena najwyższego poziomu, na której hostowany jest serwer FAMOC (np. Jeśli komputer jest hostowany na "emm.company.com", domeną najwyższego poziomu będzie "company.com")
- Logo aplikacji (opcjonalnie)
- Link do strony domowej aplikacji, link do Polityki prywatności aplikacji
- wymagane, jeśli chcesz używać logo, w przeciwnym razie - opcjonalnie

Dane logowania

Dane logowania **Ekran akceptacji OAuth** Weryfikacja domeny

Zanim Twoi użytkownicy się uwierzytelnią, ten ekran akceptacji pozwoli im wybrać, czy chcą zezwolić na dostęp do swoich prywatnych danych, jak również udostępnić im linki do warunków korzystania z usługi oraz do polityki prywatności. Ta strona pozwala Ci konfigurować ekran akceptacji dla wszystkich aplikacji w tym projekcie.

Stan weryfikacji

Nie opublikowano

Nazwa aplikacji [?]

Nazwa aplikacji, która prosi o akceptację

FAMOC venice

Logo aplikacji [?]

Obraz na ekranie akceptacji, który ułatwi użytkownikom rozpoznanie Twojej aplikacji

Plik lokalny do przesłania

Przełóżaj



Adres e-mail pomocy [?]

Wyświetlany na ekranie akceptacji jako kontakt dla użytkowników potrzebujących pomocy

Zakresy dla interfejsów API Google

Zakresy umożliwiają aplikacji dostęp do prywatnych danych użytkownika. [Więcej informacji](#)

Jeśli dodasz wrażliwy zakres, na przykład zakres zapewniający pełny dostęp do Gmaila lub Dysku, Google zweryfikuje ekran akceptacji przed opublikowaniem.

email

profile

openid

Dodaj zakres

Autoryzowane domeny [?]

Po zakończeniu konfiguracji kliknij Zapisz na dole strony

Skonfiguruj identyfikator klienta OAuth

Po skonfigurowaniu ekranu zgody OAuth możesz wygenerować poświadczenia dla swojego serwera FAMOC. Upewnij się, że wybrałeś swój projekt, a następnie przejdź do:

- "Menu" -> "APIs i usługi" -> "Poświadczenia" -> "Poświadczenia"

Z menu wybierz "OAuth Client ID" i wybierz "Aplikacja internetowa":

Wypełnij odpowiednie informacje, zwracając przede wszystkim uwagę na pola:

- Imię (wymagane)

Nazwa wewnętrzna dla poświadczeń (nie będzie wyświetlana użytkownikom)

- Autoryzowane źródła kodu JavaScript (wymagane)

Adres serwera FAMOC w formacie: ``https://emm.twojafirma.com``. Musi się zgadzać z autoryzowaną domeną najwyższego poziomu na skonfigurowanym ekranie zgody na OAuth.

- Autoryzowane identyfikatory URI przekierowania (wymagane)
- Adres zwrotny używany podczas rejestracji zero-touch. Ma format: ``https://emm.twojafirma.com/ui/devices/enrollment/zeroTouch``. Musi się zgadzać z autoryzowaną domeną najwyższego poziomu na skonfigurowanym ekranie zgody na OAuth.

Google APIs venice

← Identyfikator klienta – Aplikacja internetowa POBIERZ JSON ZRESETUJ KLUCZ TAJNY USUŃ

Identyfikator klienta	890215448461-malbm6ng3s6sl2cp7gfubi4rrnc80di8.apps.googleusercontent.com
Tajny klucz klienta	30U6288Xc72DK0kD7DcGrP6o
Data utworzenia	28 sty 2019, 12:42:24

Nazwa

Klient sieci Web

Ograniczenia

Wpisz źródła JavaScript, identyfikatory URI przekierowania lub oba te elementy. [Więcej informacji](#)

Domeny źródeł i domeny przekierowań trzeba dodać do listy autoryzowanych domen w ustawieniach akceptacji protokołu OAuth.

Autoryzowane źródła JavaScript

Do zastosowania z zadaniami z przeglądarki. Jest to pierwotny identyfikator URI aplikacji klienckiej. Nie może zawierać symbolu wieloznacznego (`https://*.example.com`) ani ścieżki (`https://example.com/subdir`). Jeśli używasz niestandardowego portu, musisz uwzględnić go w pierwotnym identyfikatorze URI.

`https://emm.adresserwera.pl`

`https://www.example.com`

Autoryzowane identyfikatory URI przekierowania

Do użycia z zadaniami z serwera WWW. Jest to ścieżka w aplikacji, do której przekierowywani są użytkownicy po uwierzytelnieniu przez Google. Ścieżka jest uzupełniana kodem autoryzacji pozwalającym na dostęp. Musi uwzględniać protokół. Nie może zawierać fragmentów adresów URL ani ścieżek względnych. Nie może też być publicznym adresem IP.

`https://emm.adresserwera.pl/ui/devices/enrollment/zeroTouch`

`https://www.example.com`

Zapisz Anuluj

Po skonfigurowaniu kliknij "ZAPISZ" u dołu strony. Pobierz swoje dane uwierzytelniające, klikając przycisk "Pobierz JSON" obok poświadczeń, które właśnie skonfigurowałeś.

Dodaj dane uwierzytelniające do komputera z serwerem FAMOC

Ostatnim krokiem, aby zintegrować zero-touch z serwerem FAMOC Server, jest dodanie danych uwierzytelniających z poprzedniego kroku do serwera. Aby to zrobić, najpierw zaloguj się do serwera FAMOC przez SSH jako użytkownik z uprawnieniami roota. Po autoryzacji edytuj ten plik za pomocą edytora, np.:

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

W pliku znajdź sekcję rozpoczynającą się od ``/*--BEGIN CUSTOM GLOBAL--*/`` i dodaj odpowiednio zawartość pobranego pliku:

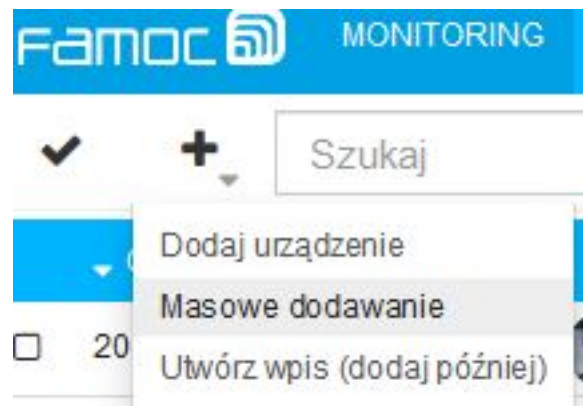
```
/*--BEGIN CUSTOM GLOBAL--*/  
$cons_zt_json='CONTENT_OF_JSON_CREDENTIALS_FILE';  
/*--END CUSTOM GLOBAL--*/
```

Zapisz plik i zamknij sesję SSH. Twój serwer FAMOC jest skonfigurowany, a twoi administratorzy mogą zacząć korzystać z zalet integracji zero-touch.

Dodanie konta zero-touch do organizacji FAMOC

Aby zacząć dodawać urządzenia zero-touch do twojej organizacji FAMOC, musisz dodać do niej swoje firmowe konto zero-touch. Możesz to zrobić za pomocą naszego kreatora rejestracji zbiorowej w widoku urządzeń. Po zalogowaniu się jako administrator do swojej organizacji, przejdź do:

"Nowy interfejs użytkownika" -> "Urządzenia" -> "+" -> "Zbiorowa rejestracja"




Następnie wybierz metodę "Android zero-touch".

URZĄDZENIA / MASOWE DODAWANIE

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:

<h4>Apple DEP</h4>  <p>Program rejestracji urządzeń pozwala na automatyczne dodawanie i skonfigurowanie urządzeń iOS Twojej organizacji.</p>	<h4>Android zero-touch</h4>  <p>Android zero-touch pozwala na bezproblemową konfigurację i wdrażanie Androidowych urządzeń firmowych.</p>	<h4>Samsung KME</h4> <h3>SAMSUNG</h3> <p>Usługa Knox Mobile Enrollment pozwala dodawać wiele urządzeń Samsung do systemu MDM bez konieczności ręcznej konfiguracji.</p>
---	--	---

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

Integracja zero-touch



Zaloguj się do portalu zero-touch.

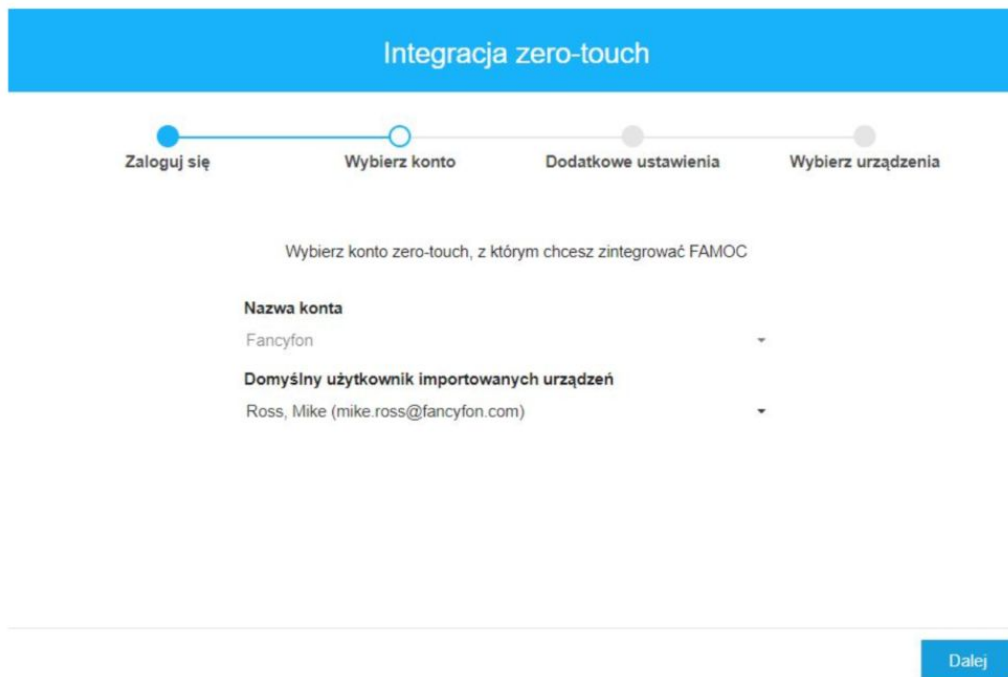
Zostaniesz poproszony o pozwolenie aplikacji FAMOC na zarządzanie urządzeniami z Androidem do rejestracji typu zero-touch i konfiguracjami EMM w organizacji

[Autoryzuj Google](#)

Zaloguj się na swoje konto administratora zero-touch i nadaj odpowiednie uprawnienia FAMOC:



Po udanej autoryzacji, FAMOC będzie mógł zarządzać twoją integracją zero-touch. Z rozwijanej listy wybierz konto zero-touch, z którym chcesz przeprowadzić integrację. (jeśli twoje konto administratora jest połączone z więcej niż jedną firmą na konsoli zero-touch). Możesz również wybrać domyślnego użytkownika przypisanego do urządzenia w FAMOC i przypisane Grupy urządzeń:



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

The screenshot shows the 'Integracja zero-touch' screen in the FAMOC application. The progress bar indicates the current step is 'Dodatkowe ustawienia'. The form fields are as follows:

- Nazwa klienta: Twoja firma
- Numer telefonu działu wsparcia: 48221005200
- Adres e-mail działu wsparcia: support@addresserwera.com
- Dodatkowa informacja: Witaj na firmowych serwerze do zarządzania urządzeniami!

The smartphone mockup displays the following text:

Urządzenie jest zarządzane.
Twoja firma skonfigurowała urządzenie do pełnego zarządzania. Jeśli uważasz, że to błąd, skontaktuj się w następujący sposób:
☎ 48221005200
@ support@addresserwera.com

Wiadomość od Twojej firma
Witaj na firmowych serwerze do zarządzania urządzeniami!

Informacje o urządzeniu

Na koniec wybierz urządzenie, które chcesz zaimportować do FAMOC. Na koniec wybierz urządzenie, które chcesz zaimportować do FAMOC. Możesz wybrać żądane urządzenia ręcznie lub wybrać opcję "Autoimport", która będzie okresowo (w odstępach 30-minutowych) synchronizować nowe urządzenia od zera-dotknięcia do FAMOC.

Urządzenie można ustawić w jednym z trzech stanów, w oparciu o przypisaną konfigurację zero-touch:

- "NIEPRZYPISANE" - urządzenie nie ma konfiguracji "zero-touch" (która zostanie przypisana jeśli urządzenie zostanie wybrane lub włączona zostanie opcja autoimport)
- "AKTUALNE" - urządzenie ma przypisaną aktualną konfigurację zero-touch (i nie otrzyma nowej konfiguracji podczas synchronizacji)
- "INNE" - urządzenie ma przypisaną inną konfigurację zero-touch EMM. Nie otrzyma domyślnie nowego profilu podczas automatycznego importu. Aby zastąpić inny profil EMM, musisz wybrać dane urządzenia na tym etapie.

Zero-touch integration



Select the devices to import or let FAMOC auto-import all unassigned devices

If you have devices assigned to other EMM configurations, you must select them manually to import them

Search Auto-import Select all (5) < >

	IMEI	Model	Serial number	Status
<input checked="" type="checkbox"/>	353378096525426	HMD Global		NOT ASSIGNED
<input checked="" type="checkbox"/>	358544080747848	HMD Global		NOT ASSIGNED
<input checked="" type="checkbox"/>	358549081897476	HMD Global		NOT ASSIGNED
<input checked="" type="checkbox"/>	359140090022147	K-touch		NOT ASSIGNED
<input checked="" type="checkbox"/>	867981023206686	Huawei		NOT ASSIGNED

Synchronize


Po wybraniu konfiguracji kliknij "Synchronizuj", aby dodać urządzenia do swojego konta FAMOC. Zostaniesz przekierowany do ekranu podsumowania.





Import completed

Available devices: 5 / 5

What do you want to do next?

Add many devices 

Go to the device list 

Go to settings 

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

The screenshot displays the 'Devices' management page. On the left, a sidebar contains navigation options: 'Zero Touch', 'Fancyfon', 'Configurations', 'Devices' (highlighted with a red box), 'Manage People', 'Resellers', and 'Send feedback'. The main content area has a blue header with the title 'Devices' and a notification badge '2'. Below the header is a search bar with the text 'Search for devices using IMEI, MEID or Serial Number'. The search bar includes a text input field, a 'Select identifier' dropdown, and a 'SEARCH' button. Below the search bar, a table lists devices. The table has three columns: 'IMEI / Serial Number', 'Configuration', and 'Unregister'. The table shows 6 devices in total. The first five devices have 'No config' in the Configuration column and 'UNREGISTER' in the Unregister column. The sixth device has 'Barents Company S' in the Configuration column and 'UNREGISTER' in the Unregister column.

IMEI / Serial Number	Configuration	Unregister
[REDACTED]	No config	UNREGISTER
[REDACTED]	No config	UNREGISTER
[REDACTED]	No config	UNREGISTER
[REDACTED]	No config	UNREGISTER
[REDACTED]	No config	UNREGISTER
[REDACTED]	Barents Company S	UNREGISTER

© 2018 Google | [Terms of Service](#)

"Dostępne urządzenia" podaje informację o: liczbie pomyślnie zaimportowanych urządzeń/liczbie wybranych urządzeń.

W przypadku jakichkolwiek problemów z importem sprawdź log systemu, aby uzyskać więcej szczegółów. Po zakończeniu synchronizacji - wszystko gotowe! Urządzenia będą rejestrować się do FAMOC po uruchomieniu.