

FAMOC®

Konfiguracja atestacji SafetyNet



www.famoc.com

PUBLISHED BY

FAMOC S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

Copyright© 2008-2020 by Famoc S.A.

Wszystkie prawa zastrzeżone. Cała zawartość dokumentu stanowi wyłączną własność firmy Famoc S.A. i nie może być powielana ani dystrybuowana bez pisemnej zgody wydawcy. Publikacja może zawierać marki i nazwy produktów będące znakami towarowymi lub zarejestrowanymi znakami towarowymi poszczególnych właścicieli.

SPECYFIKACJE I INFORMACJE DOTYCZĄCE PRODUKTÓW I USŁUG PRZEDSTAWIANYCH W INSTRUKCJI PODLEGAJĄ ZMIANOM. WSZELKIE INFORMACJE I ZALECENIA ZAMIESZCZONE W DOKUMENCIE SĄ WŁAŚCIWE JEDNAKŻE WSZELKA ODPOWIEDZIALNOŚĆ ZA IMPLEMENTACJĘ I UŻYTKOWANIE PRODUKTÓW I USŁUG LEŻY PO STRONIE UŻYTKOWNIKÓW.



Spis treści

Uzyskanie klucza SafetyNet API	3
Aktywacja SafetyNet w systemie FAMOC	8

1 Uzyskanie klucza SafetyNet API

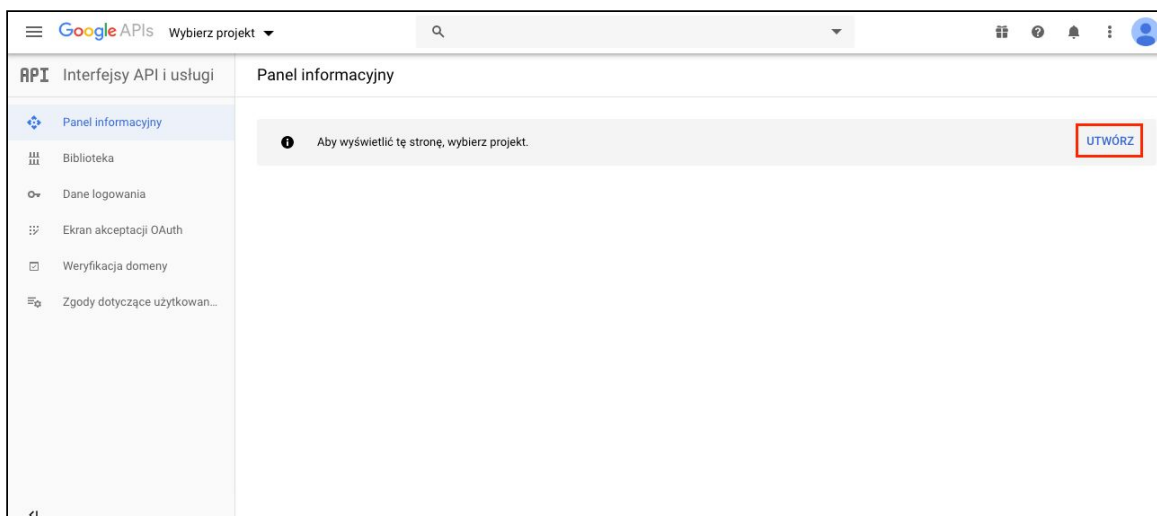
Wymagania:

- aktywne konto Google

Aby wygenerować klucz SafetyNet API należy wejść na stronę

<https://console.developers.google.com/> i zalogować się na swoje konto Google. Następnie zaakceptuj warunki korzystania z Google Cloud Platform i warunki korzystania z odpowiednich usług i interfejsów API

Utwórz nowy projekt i wprowadź jego nazwę (w Lokalizacji może być ustawiony 'Brak organizacji')



Nowy projekt

⚠ Masz jeszcze 12 projects do osiągnięcia limitu. Poproś o zwiększenie limitu lub usuń niektóre projekty. [Więcej informacji](#)

[MANAGE QUOTAS](#)

Nazwa projektu *

?

Identyfikator projektu: . Nie można go później zmienić.

[EDYTUJ](#)

Lokalizacja *

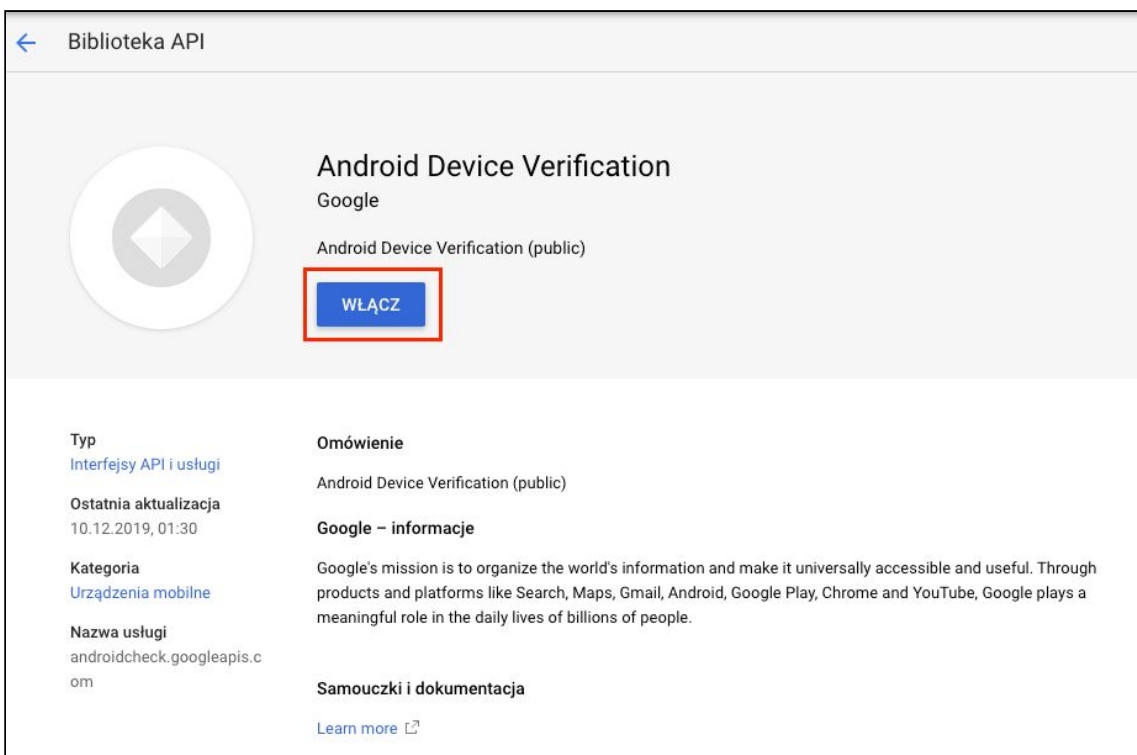
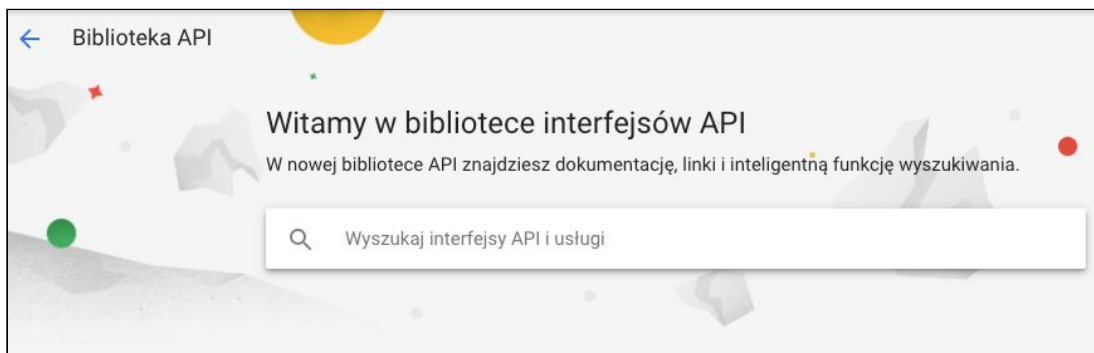
📁 Brak organizacji [PRZEGLĄDAJ](#)

Organizacja nadrzędna lub folder nadrzędny

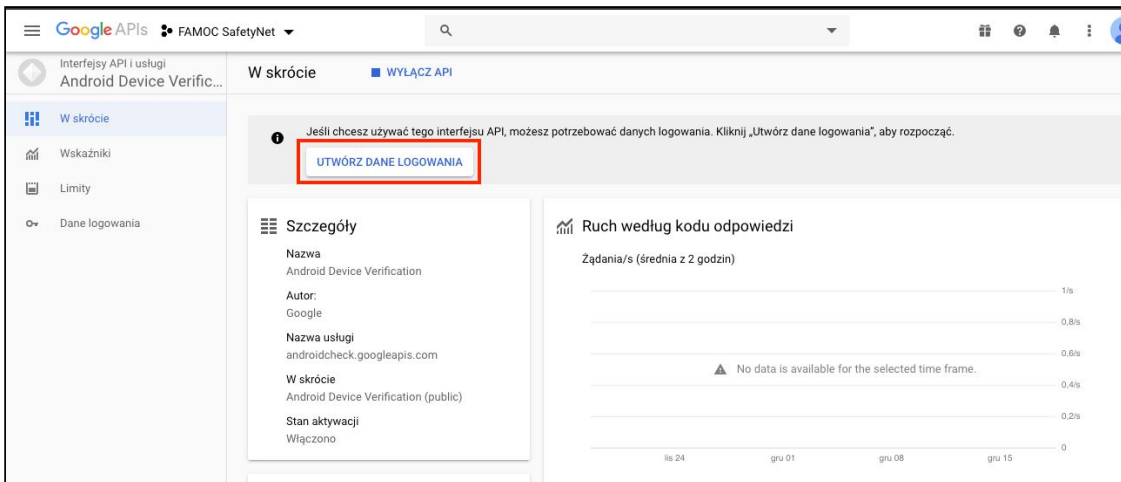
UTWÓRZ
ANULUJ

Przejdź na stronę <https://console.developers.google.com/apis/library>

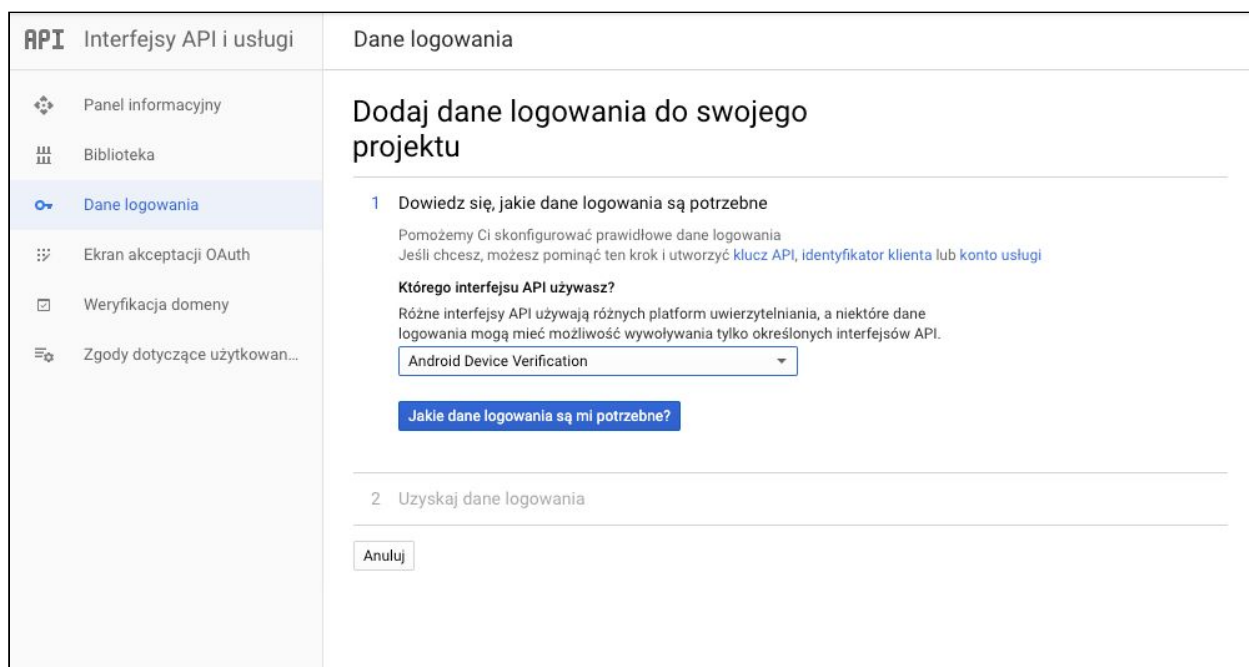
Na podanej stronie wyszukaj w bibliotece Android Device Verification API i kliknij przycisk 'Włącz'



Zostaniesz przeniesiony na nową stronę, gdzie należy utworzyć dane logowania.



Wybierz 'Android Device Verification' i następnie kliknij 'Jakie dane logowania są mi potrzebne?'



Zostanie wygenerowany klucz API, skopiuj go i kliknij 'Gotowe'.

RPI Interfejsy API i usługi

- Panel informacyjny
- Biblioteka
- Dane logowania
- Ekran akceptacji OAuth
- Weryfikacja domeny
- Zgody dotyczące użytkow...

Dane logowania

Dodaj dane logowania do swojego projektu

Dowiedz się, jakie dane logowania są potrzebne
Wywołuję: Android Device Verification

2 Uzyskaj dane logowania

To jest Twój klucz API

AI
Skopiowano

⚠ Zalecamy ograniczenie tego klucza przed użyciem w środowisku produkcyjnym. Ograniczenia określają, które witryny internetowe, adresy IP lub aplikacje mogą wywoływać interfejsy API przy użyciu tego klucza.
[Ogranicz klucz](#)

Gotowe
Anuluj

W ograniczeniach klucza upewnij się że 'Ograniczenia aplikacji' są ustawione na 'Nic'

Nazwa *

API Key

Aby użyć tego klucza w aplikacji, przekaż go w parametrze `key=KLUCZ_API`.

Data utworzenia

Autor:

Całkowite wykorzystanie (ostatnie 30 dni)

18 grudnia 2019 13:57:03 GMT+1

0

Ograniczenia klucza

⚠ Ten klucz nie ma ograniczeń. Ograniczenia zapobiegają nieautoryzowanemu użyciu i kradzieży limitu. [Dowiedz się więcej](#)

Ograniczenia aplikacji

Ograniczenie aplikacji umożliwia określenie, które witryny, adresy IP lub aplikacje mogą korzystać z Twojego klucza interfejsu API. Dla danego klucza możesz ustawić jedno ograniczenie aplikacji.

- Nic
- Strony odsyłające HTTP (witryny internetowe)
- Adresy IP (serwery WWW, zadania cron itp.)
- Aplikacje na Androida
- Aplikacje na iOS

Ograniczenia interfejsów API

Ograniczenia interfejsów API określają włączone interfejsy API, które ten klucz może wywoływać

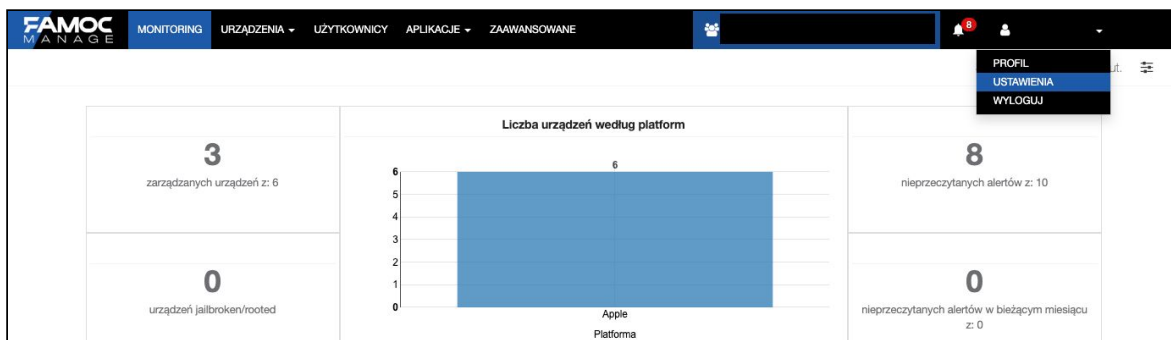
- Nie ograniczaj klucza
Ten klucz może wywołać dowolny interfejs API
- Ogranicz klucz

Uwaga: zanim zmiany zaczną obowiązywać, może upłynąć nawet 5 minut

ZAPISZ
ANULUJ

2 Aktywacja SafetyNet w systemie FAMOC

Po zalogowaniu do FAMOC-a wybierz ustawienia organizacji.



W zakładce 'Szczegóły', w polu 'Klucz do API SafetyNet' wklej wygenerowany klucz.

The screenshot shows the 'Szczegóły' (Details) settings page. The left sidebar lists 'iOS', 'Android', and 'Powiadomienia'. The main content area is titled 'Ogólne' (General) and contains the following settings:

Język	Niemiecki
Kraj	Polska
Telefon	Brak wartości
Email	Brak wartości
Czas trwania sesji	60 minut
Interwał synchronizacji aplikacji z Google Play	7 dni
Klucz do API SafetyNet	Brak wartości

The 'Klucz do API SafetyNet' field is highlighted with a red border.

W 'Ustawieniach podstawowych' polityki generalnej ('Zaawansowane' -> 'Ustawienia') pojawiła się opcja 'Włącz atestację SafetyNet' - po włączeniu jej i zapisaniu polityki generalnej, podczas enrollmentu pojawi się nowa operacja 'Atestacja SafetyNet'. Dla urządzeń, które wcześniej były dodane do FAMOCa, status polityki zmieni się na 'Nieaktualny' i podczas następnego odświeżenia polityki zostanie wykonana operacja atestacji.

Formularz edycji polityki:

Ustawienia podstawowe

Nazwa szablonu:

Ustaw priorytet: 0:(jako pierwszy)

Przeinstaluj Base Agenta automatycznie:

Odinstaluj niezgodne elementy polityki automatycznie:

Włącz Samsung Premium API:

Włącz atestację SafetyNet:

Oznacz urządzenie jako wyczyszczone przy wykrytym odinstalowaniu Agenta Bazowego:

Włącz usługi zdalnego pulpitu:

Włącz usługi lokalizacyjne:

Wymuszaj włączenie usługi monitorowania aplikacji:

Ignoruj optymalizację zużycia baterii dla Monitora lokalizacji i Monitora użycia *:

Przypisana polityka

Nazwa polityki	Zastosowana	Podgląd polityki	Status
Default policy	2019-12-18 14:42:37		

Status: **Nieaktualna polityka**

Oczekujące operacje:




- Odświeżenie polityki - Default policy
- Odświeżenie restrykcji bezpieczeństwa - Default policy
- Akcja - Atestacja SafetyNet


Podczas enrollmentu jeśli wynik atestacji będzie negatywny to komponenty polityki generalnej i profilu do pracy nie zostaną zainstalowane. Wynik atestacji zależy od statusu urządzenia (np. czy jest zrootowane, posiada odblokowanego bootloadera), możliwe przypadki (musi być przynajmniej jedno 'false' aby atestacja nie przeszła):

Table 1. Examples of how device status could affect the values of `basicIntegrity` and `ctsProfileMatch`

Device Status	Value of <code>ctsProfileMatch</code>	Value of <code>basicIntegrity</code>
Certified, genuine device that passes CTS	true	true
Certified device with unlocked bootloader	false	true
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	false	true
Device with custom ROM (not rooted)	false	true
Emulator	false	false
No device (such as a protocol emulating script)	false	false
Signs of system integrity compromise, one of which may be rooting	false	false
Signs of other active attacks, such as API hooking	false	false

Każdy projekt posiada swoje limity dot. liczby zapytań do API, domyślnie wyglądają one następująco (są to maksymalne wartości):

Nazwa limitu	Limit	
Queries per day	10 000	
Queries per 100 seconds per user	1 000	
Queries per 100 seconds	1 000	

Nazwa limitu	Limit	
Queries to verify endpoint per day	10 000	
Queries to verify endpoint per 100 seconds per user	1 000	
Queries to verify endpoint per 100 seconds	1 000	

Można je zmienić wchodzą na stronę <https://console.developers.google.com/apis/dashboard>, następnie wybierając 'Android Device Verification' -> zakładka Limity.