FAMOC®

Konfiguracja atestacji SafetyNet

www.famoc.com

PUBLISHED BY
FAMOC S.A.
Ul. Wajdeloty 12A
80-437 Gdańsk

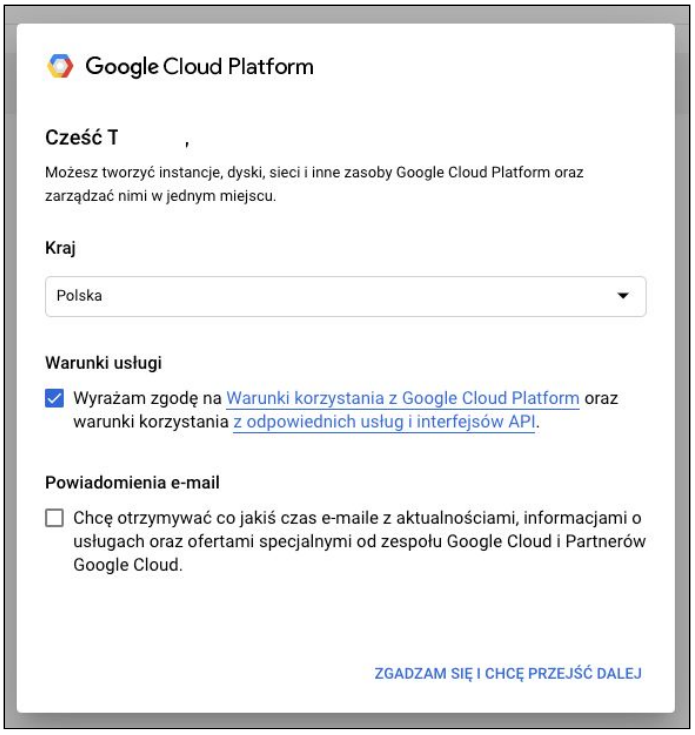
Spis treści

1 Uzyskanie klucza SafetyNet API

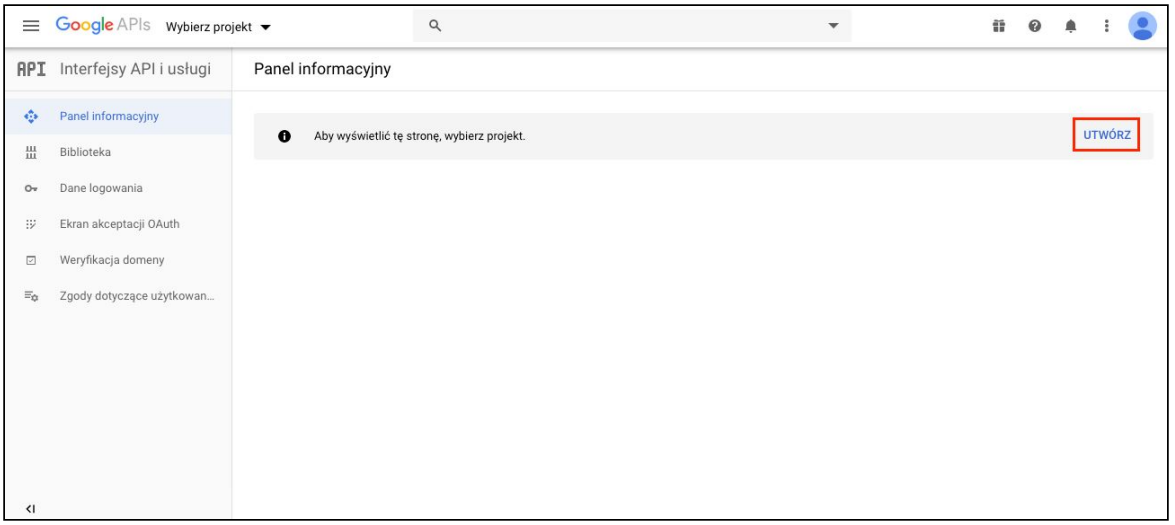
Wymagania:

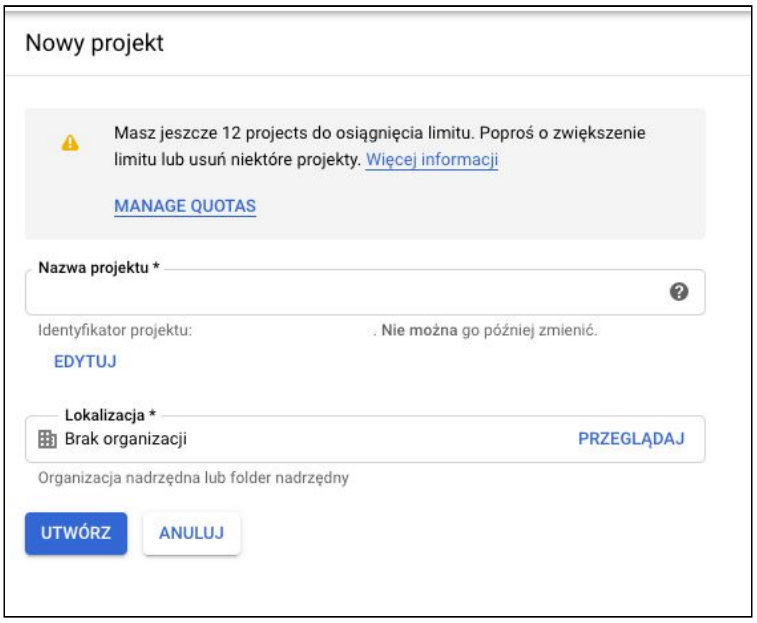
- aktywne konto Google

Aby wygenerować klucz SafetyNet API należy wejść na stronę https://console.developers.google.com/ i zalogować się na na swoje konto Google. Następnie zaakceptuj warunki korzystania z Google Cloud Platform i warunki korzystania z odpowiednich usług i interfejsów API



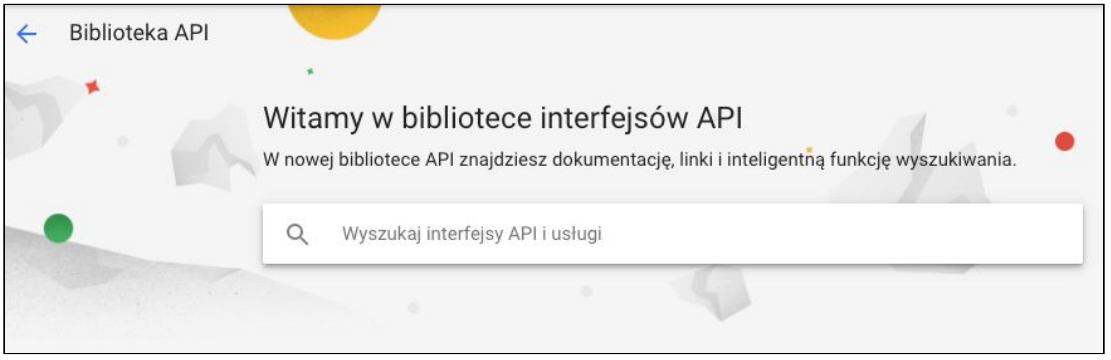
Utwórz nowy projekt i wprowadź jego nazwę (w Lokalizacji może być ustawiony ‘Brak organizacji’)

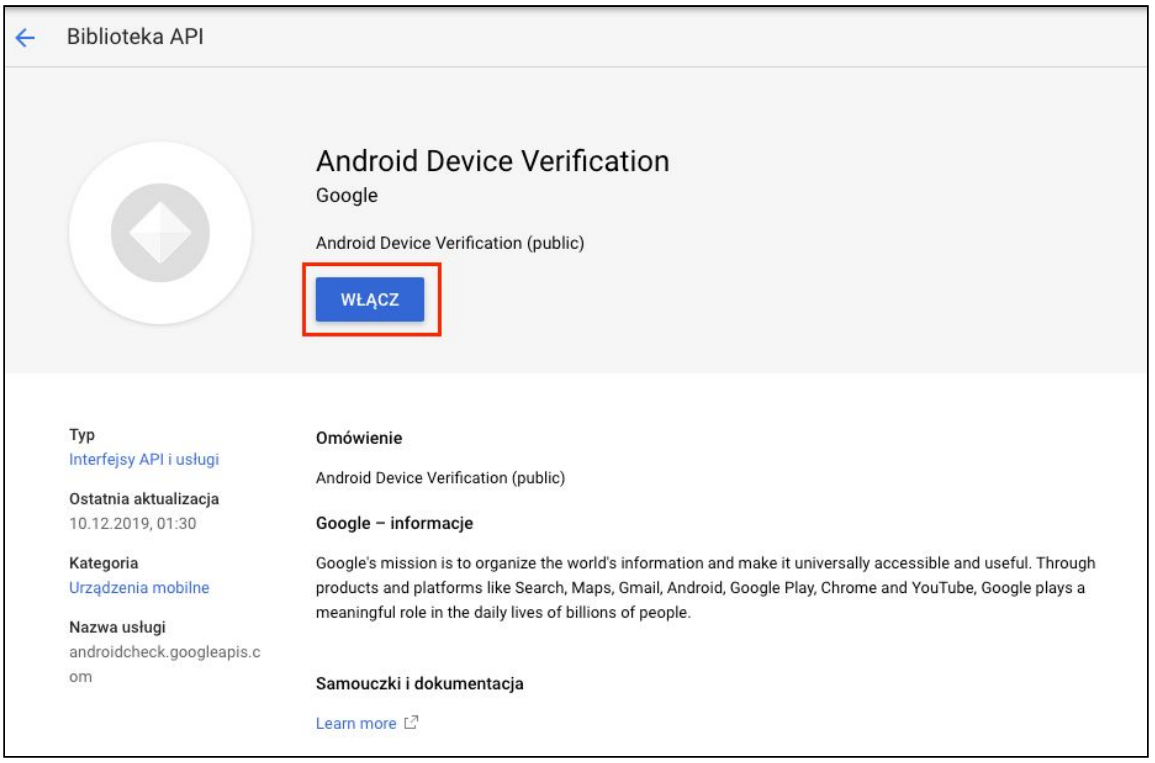




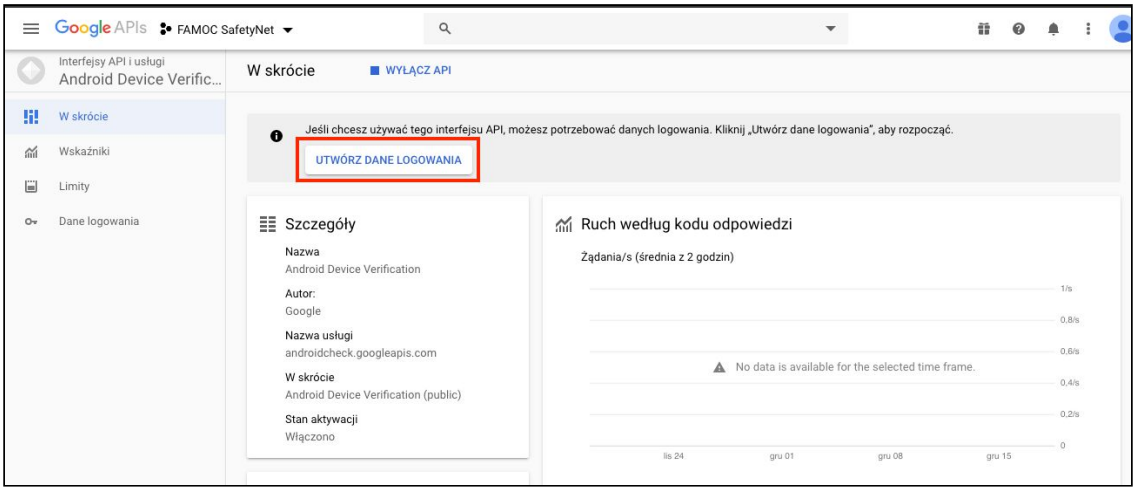
Przejdź na stronę https://console.developers.google.com/apis/library

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

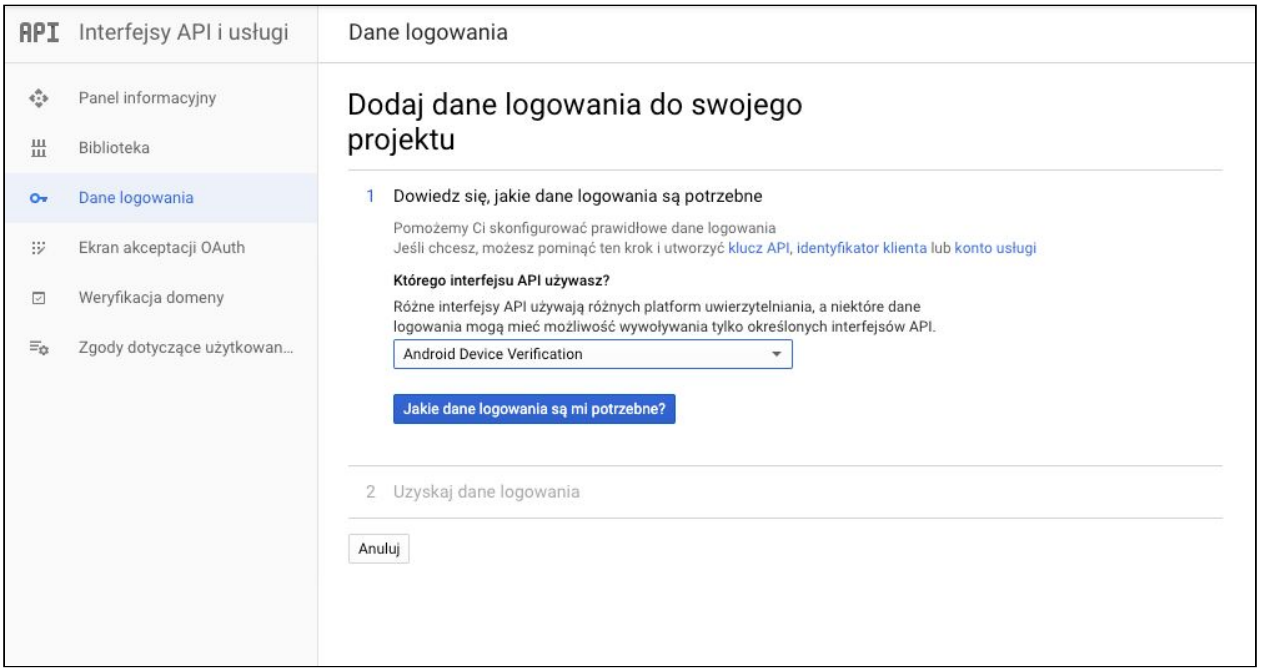




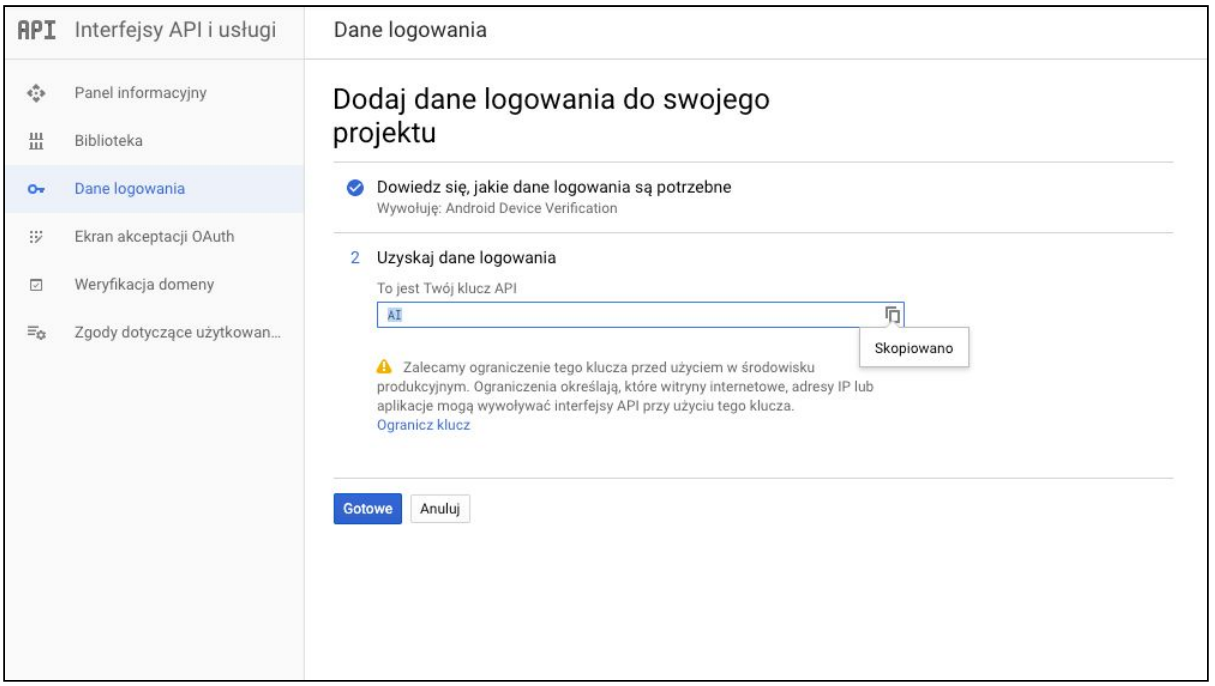
Zostaniesz przeniesiony na nową stronę, gdzie należy utworzyć dane logowania.



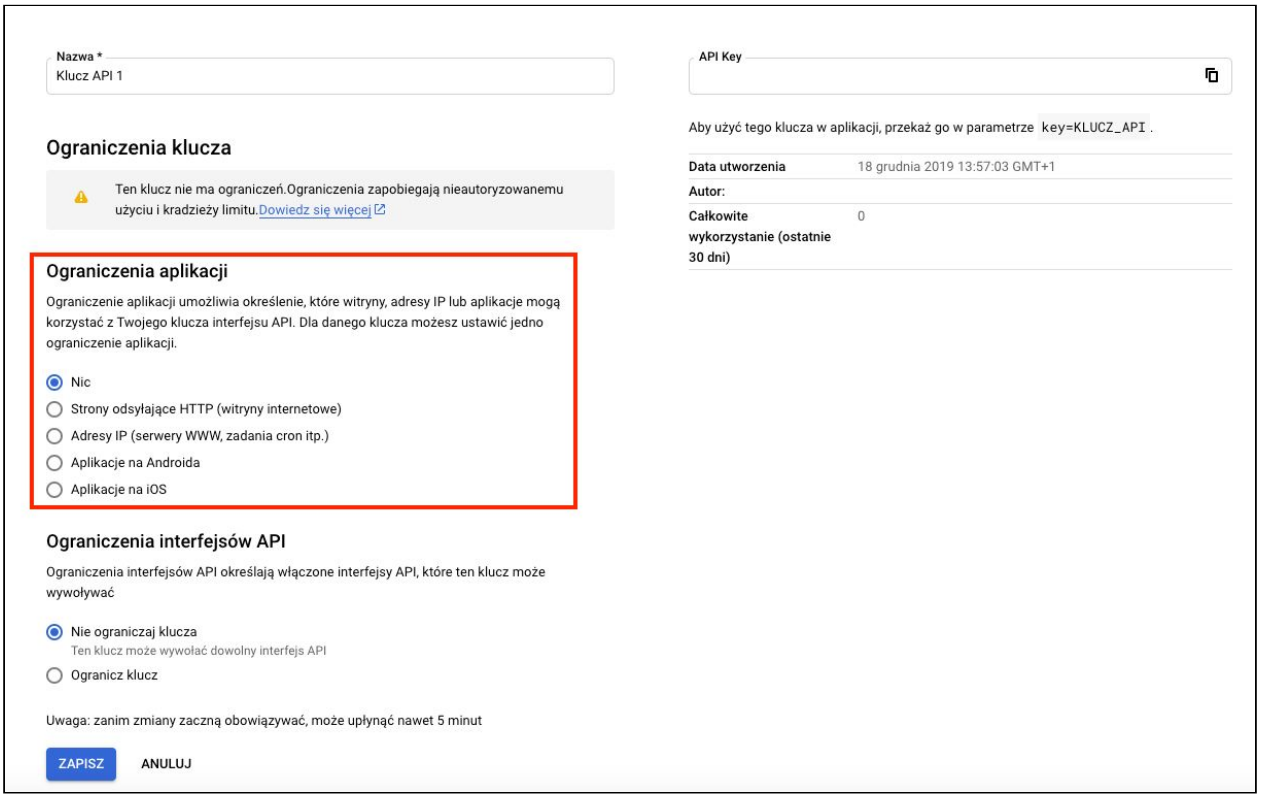
Wybierz ‘Android Device Verification’ i następnie kliknij ‘Jakie dane logowania są mi potrzebne?’



Zostanie wygenerowany klucz API, skopiuj go i kliknij ‘Gotowe’.

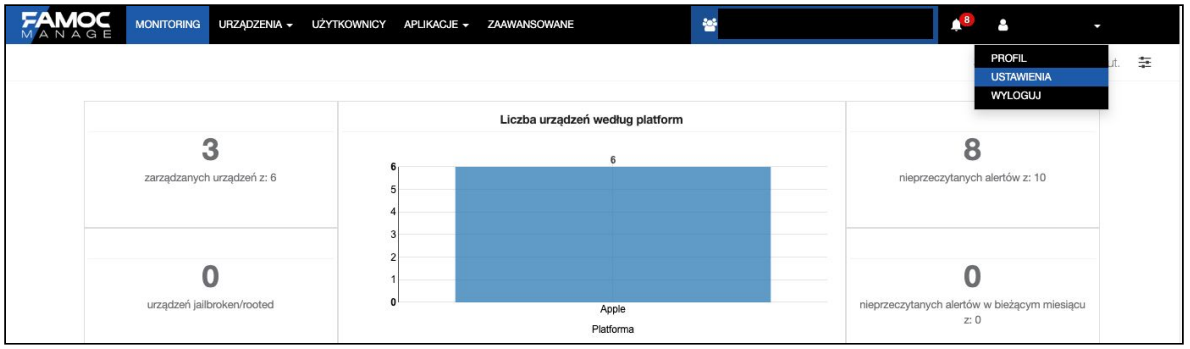


W ograniczeniach klucza upewnij się że ‘Ograniczenia aplikacji’ są ustawione na ‘Nic’

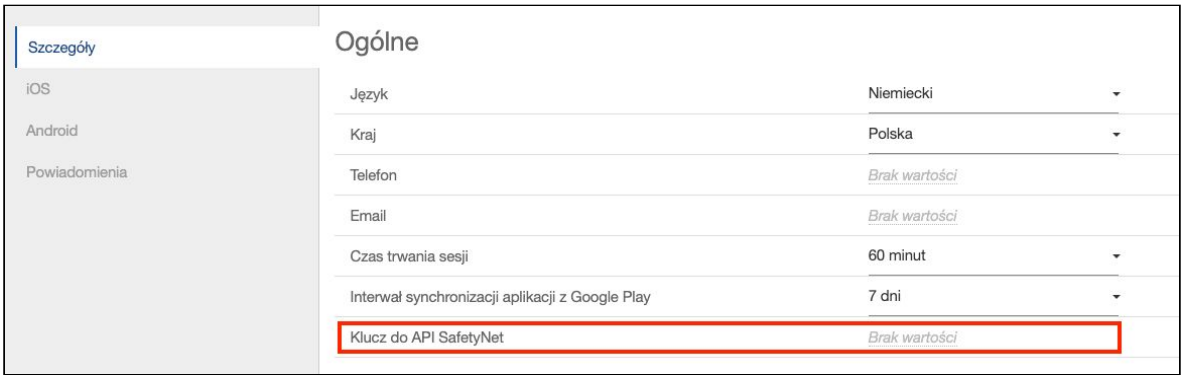


2 Aktywacja SafetyNet w systemie FAMOC

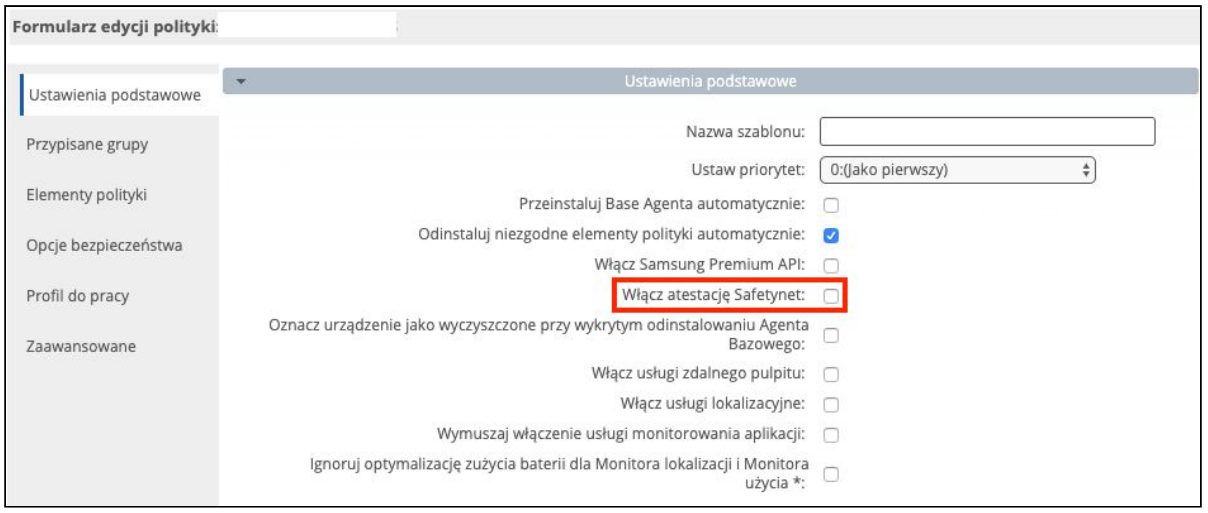
Po zalogowaniu do FAMOC-a wybierz ustawienia organizacji.

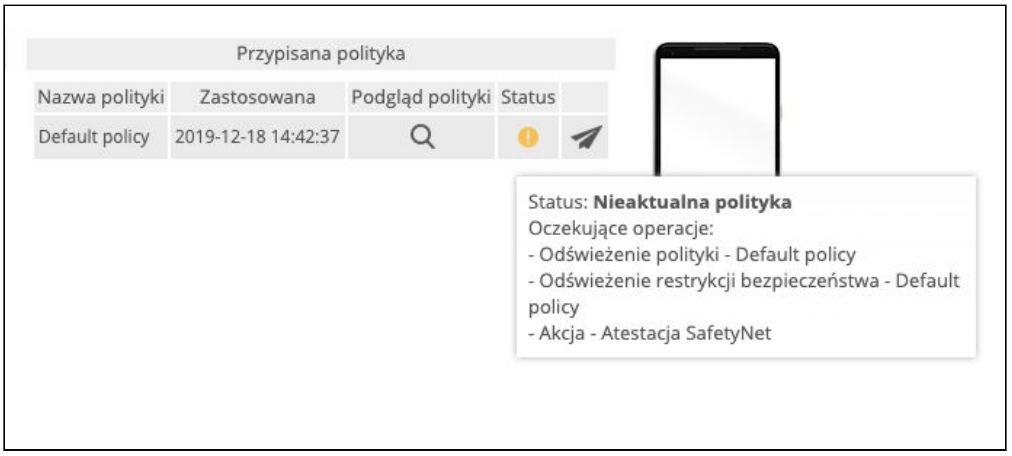


W zakładce ‘Szczegóły’, w polu ‘Klucz do API SafetyNet’ wklej wygenerowany klucz.



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.



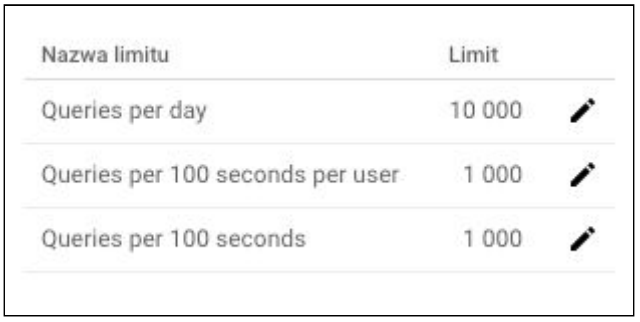


Podczas enrollmentu jeśli wynik atestacji będzie negatywny to komponenty polityki generalnej i profilu do pracy nie zostaną zainstalowane. Wynik atestacji zależy od statusu urządzenia (np. czy jest zrootowane, posiada odblokowanego bootloadera), możliwe przypadki (musi być przynajmniej jedno ‘false’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

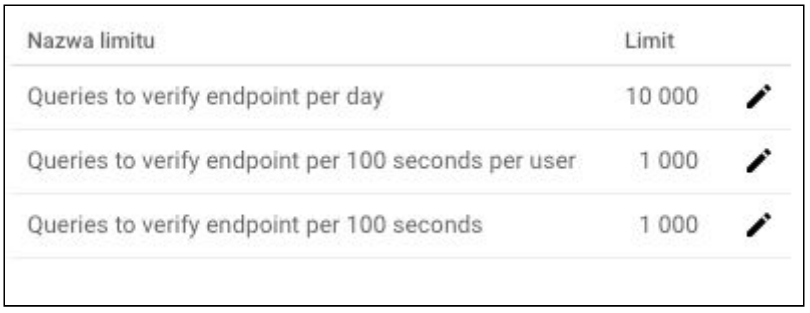
Table 1. Examples of how device status could affect the values of `basicIntegrity` and `ctsProfileMatch`

Device Status	Value of ctsProfileMatch	Value of basicIntegrity
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.