techŜtep

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

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

Select from TECHSTEP.COM	NEW PROJECT
Q. Search projects and folders	
RECENT ALL	
Name	ID
🗸 🐌 My Project 70234 🔞	silver-impulse-274416
My Project 29015	genuine-citron-235714
techstep.com 🕜	826821783126
• TECHSTEP	famoc-32004

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".

Product details		
	Android Device Provisioning Partner A	\PI
	Automates Android zero-touch enrollment for device resellers and EMMs.	s, customers,
	ENABLE TRY THIS API	
OVERVIEW	DOCUMENTATION	
Overview		
Automates Androi and EMMs	d zero-touch enrollment for device resellers, customers,	Additional details
and Livinis.		Type: SaaS & APIs
About Google		Last updated: 7/22/22
Google's mission i universally access	s to organize the world's information and make it ible and useful. Through products and platforms like	Category: <u>Mobile</u> Service name: androiddeviceprovisioning.googleapis.con

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**).

API	APIs & Services
«»	Dashboard
Ш	Library
0-	Credentials
92	OAuth consent screen
	Domain verification
Ξe	Page usage agreements

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

A second s		
before your users authenticate, this consent screen will all	low them to choose	About the consent screen
whether they want to grant access to their private data, as	well as give them a link	The consent screen tells your users who is
to your terms of service and privacy policy. This page conf	igures the consent	requesting access to their data and what kind of data
screen for all applications in this project.		you're asking to access.
Application type		
Public		OAuth verification
Any Google Account can grant access to the scopes require	ed by this app.	
Learn more about scopes		To protect you and your users, your consent screen
• Internal		Verification is required if your app is marked as
 Internal Only years with a Coople Assault is your preceivation and 	mant season to the second	Public and at least one of the following is true
requested by this app.	grant access to the scopes	and and a wast one of the following is not.
		 Your app uses a sensitive and/or restricted scope
Application name		Your app displays an icon on its OAuth consent
The name of the app asking for consent		screen
TECHSTEP		Your app has a large number of authorised
		domains
Application logo		You have made changes to a previously verified
An image on the consent screen that will help users recognise y	rour app	OAuth consent screen
icon.png	Browse	The verification process may take up to several
		weeks, and you will receive email updates as it
		progresses. Learn more about verification.
		Before your consent screep and application are
		Before your consent screen and application are verified by Google, you can still test your application
C		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will
G		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.
S		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.
S		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth
S		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience.
Apport email @ hown on the consent screen for user support		Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience.
Aupport email O hown on the consent screen for user support support@techsten.no		Before your consent screen and application are verified by Google, your an still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits
Support email support email support@techstep.no	×	Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our 0.Auth experience. OAuth grant limits Token grant rate
Support email	×	Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits Token grant rate Your current per minute token grant rate limit is 100
Support email Shown on the consent screen for user support support@techstep.no support@techstep.no scopes for Google APIs Scopes allow your application to access your user's private data	*	Before your consent screen and application are verified by Google, your application with limitations. Learn more about how your application behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits Token grant rate Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate
Bupport email Movement Support email Movement Support@techstep.no Boopes for Google APIs Boopes allow your application to access your user's private data Prove did a sensitive score, such as scores that aire you full	Learn more coress to Calendar or Drive.	Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our 0Auth experience. OAuth grant limits Token grant rate Your current per minute token grant rate limit is 100 grants per minute. Your current per day token grant resets every minute. Your current per day token grant
Support email Support email Support enail Support@techstep.so Su	• . Learn more ccess to Calendar or Drive,	Before your consent screen and application are verified by Goole; you can still test your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits Token grant rate Your ourrent per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token
Support email	• Learn more ccess to Calendar or Drive,	Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your application behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits Token grant rate Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token grant rate resets every day.
Bupport email Comparing the consent screen for user support support@techstep.no Support@techstep.no Support@techstep.no support@techstep.no support@techstep.such as scopes that give you full a soogle will verify your consent screen before it's published. email	• Learn more ccess to Calendar or Drive,	Before your consent screen and application are verified by Google, your can still test your application with limitations. Learn more about how your application with limitations. Learn more about how your app will behave before it's verified. Let us know what you think about our OAuth experience. OAuth grant limits Taken grant rate Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate were yrants per day token grant rate resets every day. Raise limit
Bupport email Compared to the consent screen for user support Support@techstep.no Support@techstep.no Coopes allow your application to access your user's private datu f you add a sensitive scope, such as scopes that give you full a Soogle will verify your consent screen before it's published. email profile	• Learn more ccess to Calendar or Drive,	Before your consent screen and application are verified by Google, your can still test your application with limitations. Learn more about how your application with limitations and how your applicat

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:



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 URIs (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.

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 <u>Setting up OAuth 2.0</u> 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.
• The domains of the URIs you add below will be automatically added to your <u>OAuth consent screen</u> as <u>authorised domains</u> .
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 clien Services	t ID and secret can always be accessed from Credentials in APIs &	2
0	OAuth is limited to 100 <u>sensitive scope logins</u> until the <u>OAuth</u> <u>consent screen</u> is published. This may require a verification process that can take several days.	
Your Cli	ent ID	
711782	2125315-klb5rcnop29qan6o20c28h1eqs7l9rbt.apps.gc	٦
Your Cli	ent Secret	
kb0Tcr	nhrzx-04tCJJWdQqLtW	Б

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

ок

OAu	th 2.0 Client IDs					
	Name	Creation date 🛛 🕹	Туре	Client ID		
	Web client 3	12 May 2020	Web application	711782125315-klb5	Ū	î ±

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.

tec	hŜtep Monitoring Urządzenic	v Użytko	ownicy Aplikacje ~	Konfiguracje	Polityki ~ Kampan	ie beta Zaa	wansowane	¢ [™] ≥ :
✓.	+ Q Szukaj						Sesja wygaśni	e za 117 minut.
	Dodaj urządzenie		Numer telefonu	Metoda rejestracji	Tryb urządzenia	Ostatni kontakt	Utworzone	Ostatnio zmieniane
C	Utwórz wpis (dodaj później)	0-0b34- 8d-273		КМЕ	COSU	2023-06- 09 14:49:09	2023-05-04 10:12:41	2023-06-09 08:40:54
0	Samsung SM- Added S901B from Galaxy startup S22 5G 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	
	××××	
D	odaj nowe i fabrycznie zresetowane urządzenia do MDM, by pracowr byli gotowi do pracy od pierwszego uruchomienia urządzenia.	licy
он • •	wne korzyści: Dodanie urządzenia po wyjęciu z pudełka Brak możliwości usunięcia MDM Uproszczone rozpoczęcie pracy z urządzeniem	
/bierz metodę: Apple DEP	Android Zero-Touch	Samsung KME
Ć	*	SAMSUNG
Program rejestracji urządzeń pozwala na automatyczne dodawanie i skonfigurowanie urządzeń iOS Twojej organizacji.	Android zero-touch pozwala na bezproblemową konfigurację i wdrażanie Androidowych urządzeń firmowych.	Usiuga 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:

	Inte	egracja zero-touch	ı	>
Zaloguj się	Wybierz konto	Dodatkowe ustawienia	Wybierz urządzenia	Potwierdź
	:	Zaloguj się do portalu zero-touc	ch.	
Zostaniesz poprosza	ony o pozwolenie aplikacji Es touc	ssentials MDM na zarządzanie u ch i konfiguracjami EMM w orga	rządzeniami z Androidem do re nizacji	ejestracji typu zero-
		Autoryzuj Google		

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

techdemo.no wants access to your Google Account
S Terrardischgrad con
When you allow this access, techdemo.no will be able to
 Manage Android zero-touch enrollment devices and EMM configurations for your organization. Learn more
Make sure you trust techdemo.no
You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.
Learn how Google helps you share data safely.
See techdemo.no's Privacy Policy and Terms of Service.

Po pomyślnej autoryzacji Essentials MDM będzie mógł zarządzać integracją zerotouch. Z rozwijanej listy wybierz konto zero-touch, z którym chcesz się zintegrować (jeśli konto administratora jest połączone z więcej niż jedną firmą w konsoli zerotouch). 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

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

	0				
Zaloguj się	Wybierz konto	Dodatkowe ustawi	enia Wybierz	urządzenia	Potwierdź
	Wybierz konto zero	-touch, z którym chcesz	zintegrować Essent	ials MDM	
Nazwa konta					
FancyFon ZT Test					
		- 4			
Domyślny użytkownik in admin.techstep, admin.te	echstep (admin.techst	ep)			
oomyślny użytkownik in admin.techstep, admin.te Metoda dodawania Urządzenie w pełni zarządzane (COBO)	echstep (admin.techst Urządzenie profilem do	en ep) e służbowe z pracy (WPC)	ądzenie dedykowa (COSU)	ne Urządzeni	e współdzielone BETA
Domyślny użytkownik in admin.techstep, admin.te Metoda dodawania Urządzenie w pełni zarządzane (COBO) Metoda uwierzytelniania	urządzenie profilem do	en ep) e służbowe z pracy (WPC)	ądzenie dedykowa (COSU)	ne Urządzeni	e współdzielone BETA
Domyślny użytkownik in admin.techstep, admin.te Metoda dodawania Urządzenie w pełni zarządzane (COBO) Metoda uwierzytelnianic Brak uwierzytel	urządzenie Urządzenie profilem do	en ep) e służbowe z pracy (WPC) Poświadczenia użytka	ądzenie dedykowai (COSU) wnika	Ne Urządzeni Kod start	e współdzielone BETA
Domyšlny użytkownik in admin.techstep, admin.te Metoda dodawania Urządzenie w pełni zarządzane (COBO) Metoda uwierzytelnianic Brak uwierzytel Grupy urządzeń	nporowanych urządze echstep (admin.techst Urządzenie profilem do a Đ Iniania	en ep) esłużbowe z pracy (WPC) Poświadczenia użytka	ądzenie dedykował (COSU) wnika	ne Urządzeni Kod start	e współdzielone BETA

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

Wybiorrykente	Dedetkewe usterwienie	Wybiorsuradzopia	Detwierd
wybierz konto	Dodatkowe ustawienia	wybierz urządzenia	Potwieru
		≑ 75% 🔒	
		Urządzenie jest zarządzane. test skonfigurował urządzenie do	
aziału wsparcia		pełnego zarządzania. Jeśli uważasz, że to błąd, skontaktuj się w następujący	
		sposób:	
ału wsparcia		@ test@test.com	
n		Wiadomość od test	
		Informacje o urządzeniu	
macja		adjusting of and destanted in par-	
		LJ	
	Wybierz konto działu wsparcia ału wsparcia macja	Wybierz konto Dodatkowe ustawienia działu wsparcia	Wybierz konto Dodatkowe ustawienia Wybierz urządzenia działu wsparcia * 75% * Urządzenie jest zarządzane. działu wsparcia • • macja • •

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.

Zaloguj się	Wybierz konto	Dodatkowe ustaw	vienia Wyb	ierz urządzenie	a I	Potwierdź
Wybierz urz	adzenia do importu lub po:	zwól, aby Essentials MDI	1 importował wsz	ystkie nieprzyp	pisane urządze	nia
Jeśli masz urza	ądzenia powiązane z innym	i konfiguracjami EMM, n	nusisz je wybrać r	ęcznie, aby zos	stały zaimporto	owane
Szukaj		Auto	omatyczny impor	t 🔽 Zaznacz w	/szystko (4) 🔲	< >
^ IMEI	Producent Numer set	nyjny Metoda uwierzy	Importuj do tryb Do	odaj do trybu I	Dodaj do trybu	Status
		Domyślna	•			INNY
		Domyślna	•			INNY
		Domyślna	•			INNY
		Domyślna	•			INNY

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



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.

Zero Touch	Devices			III 2 🦃
Fancyfon	Search for devices using IMEI, ME	ID or Serial Number		
Configurations	Search		Select identifier 👻	Q SEARCH
Manage People				
Resellers	Devices (Total: 6)			:
Send feedback				
	IMEI / Serial Number	Configuration	Unregister	
	2012/02/12/14	No config	- UNREGISTER	
		No config	- UNREGISTER	
		No config	✓ UNREGISTER	
	101000-0111	No config	- UNREGISTER	
	1010010010010	No config	✓ UNREGISTER	
	101210-0108	Barents Company S	- UNREGISTER	

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.