



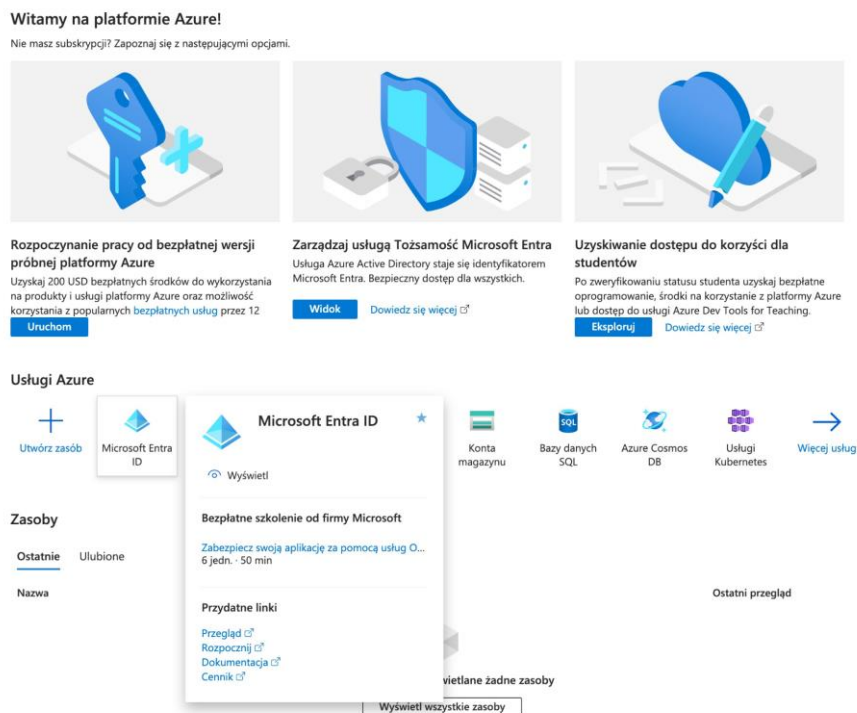
# Integracja z Azure Active Directory

Data: 4/12/2023



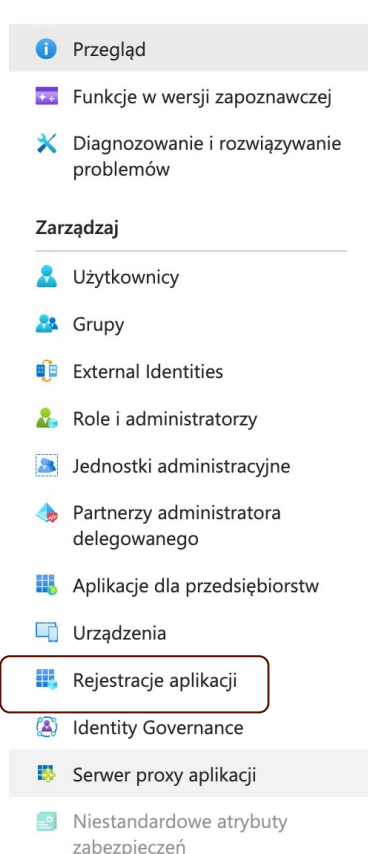
### 1. Rozpoczęcie – rejestracja aplikacji

Aby dokonać integracji systemu Essentials MDM z Azure Active Directory należy najpierw zarejestrować aplikację na naszym koncie Azure. W tym celu logujemy się do portalu <https://portal.azure.com/> i następnie z usług Azure wybieramy Azure Active Directory.

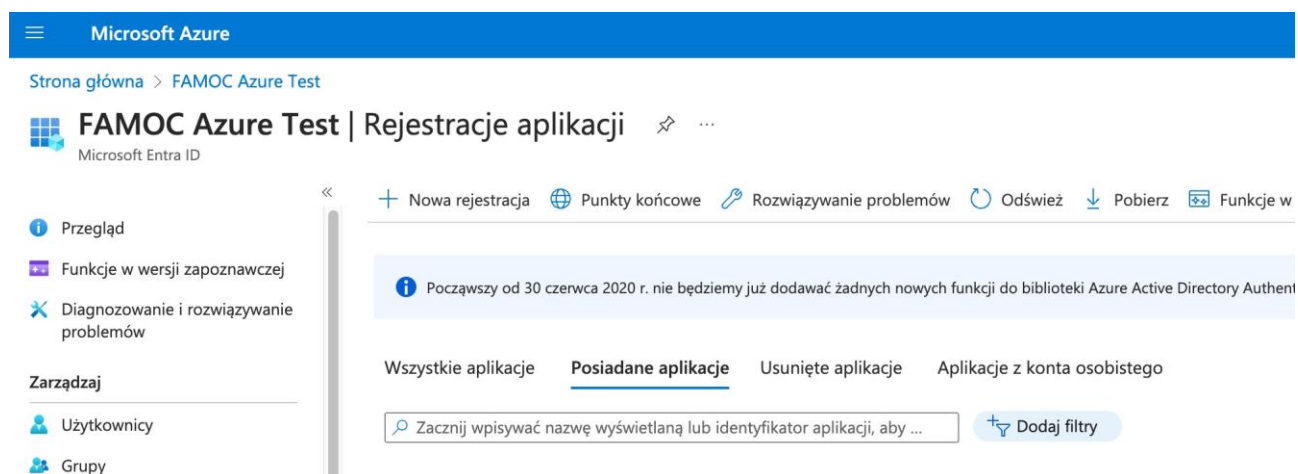


### Rejestrowanie Essentials MDM na platformie Azure

Po przejściu do zakładki Azure AD, z menu po lewej stronie wybierz Rejestrację aplikacji (App registration).



Następnie wybierz opcję Nowa rejestracja (New registration).



W kolejnym kroku wprowadź nazwę Aplikacji i określ, czy dostęp do niej mają mieć konta z jednej domeny, czy z większej liczby domen – wybierz **pojedyncza dzierżawa** lub **wiele dzierżaw**. Możemy także podać URI, na który użytkownik ma zostać przekierowany po pomyślnym uwierzytelnieniu (jest to opcjonalne i można to zrobić później). Naciśnij Zarejestruj (**Register**).

### Zarejestruj aplikację ...

#### \* Nazwa

Nazwa wyświetlana tej aplikacji widoczna dla użytkowników (można ją później zmienić).

Techstep Essentials 

#### Obsługiwane typy kont

Kto może korzystać z tej aplikacji lub uzyskiwać dostęp do tego interfejsu API?

- ☒ Konta tylko w tym katalogu organizacyjnym (tylko FAMOC Azure Test — pojedyncza dzierżawa)
- ☐ Konta w dowolnym katalogu organizacyjnym (dowolna dzierżawa usługi Microsoft Entra ID — wiele dzierżaw)
- ☐ Konta w dowolnym katalogu organizacyjnym (dowolna dzierżawa usługi Microsoft Entra ID — wiele dzierżaw) i osobiste konta Microsoft (np. Skype, Xbox)
- ☐ Tylko osobiste konta Microsoft

[Pomóż mi wybrać...](#)

#### Identyfikator URI przekierowania (opcjonalnie)

Pod ten identyfikator URI zostanie zwrócona odpowiedź uwierzytelniania po pomyślnym uwierzytelnieniu użytkownika. Podanie teraz tego identyfikatora URI jest opcjonalne i można go później zmienić, ale wartość jest wymagana w przypadku większości scenariuszy uwierzytelniania.

Wybierz platformę 

np. <https://example.com/auth>

Następnie przejdź do zakładki **API permissions**, aby skonfigurować uprawnienia aplikacji.


#### Zarządzaj

 Znakowanie i właściwości


 Uwierzytelnianie

 Certyfikaty i klucze tajne

 Konfiguracja tokenu

 Uprawnienia interfejsu API

 Uwidocznij interfejs API

 Role aplikacji

Możemy usunąć domyślne uprawnienia użytkownika, klikając ikonę trzech kropek, a następnie Usun uprawnienia (**Remove permissions**).

## Integracja z Azure ActiveDirectory

+ Dodaj uprawnienie    ✓ Wyraż zgodę administratora dla katalogu FAMOC Azure Test

Interfejs API / Nazwa uprawnień	Typ	Opis	Wymagana zgoda a...	Stan
▼ Microsoft Graph (1)				
User.Read	Delegowa...	Loguj się i odczytuj profil użytkownika	Nie	

Usun wszystkie uprawnienia

Aby wyświetlić uprawnienia ze zgodą dla poszczególnych aplikacji i zarządzać nimi, a także ustawienia zgody dzierżawy, wypróbuj [aplikację dla przedsiębiorstw](#).

Następnie klikamy Dodaj uprawnienie (**Add a permission**). Wybieramy Microsoft Graph, a następnie Uprawnienia aplikacji (**Application permissions**).

◀ Wszystkie interfejsy API



Microsoft Graph

<https://graph.microsoft.com/> [Dokumentacja](#)

Jakiego typu uprawnień wymaga Twoja aplikacja?

Delegowane uprawnienia

Aplikacja musi uzyskiwać dostęp do interfejsu API jako zalogowany użytkownik.

Uprawnienia aplikacji

Aplikacja działa jako usługa w tle lub demon bez zalogowanego użytkownika.

W sekcji Katalog (**Directory**) wybierz directory.read.all i potwierdź, klikając Dodaj uprawnienia (**Add permissions**).

▼ Directory (1)

<input checked="" type="checkbox"/>	Directory.Read.All ⓘ Read directory data	Tak
<input type="checkbox"/>	Directory.ReadWrite.All ⓘ Read and write directory data	Tak
<input type="checkbox"/>	Directory.Write.Restricted ⓘ Manage restricted resources in the directory	Tak

W sekcji Uprawnienia API (API permissions) wymagane jest również udzielenie zgody administratora na utworzoną aplikację (**Grant Admin consent**).

+ Dodaj uprawnienie    ✓ Wyraż zgodę administratora dla katalogu FAMOC Azure Test

Interfejs API / Nazwa uprawnień	Typ	Opis	Wymagana zgoda a...	Stan
▼ Microsoft Graph (1)				
Directory.Read.All	Aplikacja	Read directory data	Tak	✓ Udzielono dla FAMOC A...    ...

Następnie przejdź do zakładki Certyfikaty i klucze tajne (**Certificates & secrets**), aby dodać nowy klucz tajny klienta. Kliknij przycisk Nowy klucz tajny klienta (**New client secret**), wprowadź jego opis i określ czas wygaśnięcia.

# Integracja z Azure ActiveDirectory

Strona główna > FAMOC Azure Test > Rejestracja aplikacji > Techstep Essentials

Techstep Essentials | Certyfikaty i klucze tajne

Wyszukaj

Chcesz przesłać opinię?

Poświadczenia umożliwiają poufny aplikacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adresem internetowym (przy użyciu schematu HTTPS). W celu zapewnienia wyższego poziomu bezpieczeństwa zalecane jest używanie certyfikatu (zamiast klucza tajnego klienta) jako poświadczenia.

Certyfikaty rejestracji aplikacji, wpisy tajne i poświadczenia federacyjne można znaleźć na poniższych kartach.

Certyfikaty (0) | Wpisy tajne klienta (0) | Poświadczenia federacyjne (0)

Ćciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako hasło aplikacji.

+ Nowy klucz tajny klienta

Opis	Wygasa	Wartość	Identyfikator wpisu tajnego
Nie utworzono żadnych wpisów tajnych klienta dla tej aplikacji.			

Dodaj klucz tajny klienta

Opis

Wygasa

Rekomendowane: 180 dni (6 miesięcy)

Następnie MUSISZ skopiować jego wartość (nie będzie ona wyświetlona ponownie).

+ Nowy klucz tajny klienta

Opis	Wygasa	Wartość	Identyfikator wpisu tajnego
Hasło	27.05.2024	a6u8Q~8XQrPXsNQQLyC7kstjfuMg5c1...	f5f5c496-217f-4fcb-83db-afaaac918235

Następnie zaloguj się do konsoli Essentials. Przejdź do ustawień organizacji, sekcji Użytkownicy i poświadczenia, a następnie znajdź sekcję Integracja z Azure Active Directory. Kliknij przycisk Aktywuj.

TE Testowa

Zarządzane urządzenia  
0  
Limit urządzeń  
Bez limitu  
Ważna do  
Bez limitu

Szczegóły

Użytkownicy i poświadczenia

Apple

Android

Powiadomienia

Grupy

Weryfikacja dwuetapowa

Uwierzytelnianie dwuskładnikowe stanowi dodatkową warstwę zabezpieczającą konta użytkowników podczas logowania do systemu Essentials MDM.

Aktywuj

Integracja z usługą Azure Active Directory

Zintegruj Essentials MDM z Azure Active Directory i zsynchronizuj użytkowników oraz grupy.

Aktywuj

Integracja SAML

Zintegruj Essentials MDM z zewnętrzną usługą autoryzacji SAML (np. Azure AD, Office 365).

Aktywuj

Uwierzytelnianie Swivel

Adres URL Swivel

Brak wartości

Sprawdź poprawność adresu

W następnym kroku wprowadź następujące dane pobrane z Azure Portal:

- Wyświetlana nazwa (może być dowolna)
- Identyfikator aplikacji (klienta)
- Identyfikator katalogu (dzierżawy)
- Sekret aplikacji



Szczegóły

Wprowadź poświadczenia Zweryfikuj integrację Mapowanie pól użytkownika Mapowanie pól grupy Ustawienia

W Azure portal przejdź do "Azure Active Directory" > "App registrations" > "New registration". Następnie w "API permissions" utwórz nowe uprawnienie oraz w sekcji "Directory" zaznacz "directory.read.all". Przejdź do zakładki "Certificates & secrets" i utwórz client secret.

Wyświetlana nazwa\*

Identyfikator aplikacji\*

Identyfikator katalogu (dzierzawy)\*

Wpis tajny aplikacji\*

Dalej

Po kliknięciu Dalej Twoja integracja zostanie zweryfikowana.

Szczegóły

Wprowadź poświadczenia Zweryfikuj integrację Mapowanie pól użytkownika Mapowanie pól grupy Ustawienia

Użytkownicy stworzeni przez Azure: 1914  
Grupy stworzone przez Azure: 11  
Użytkownicy:

Adriana Wabbin [Adriana.Wabbin@kancelariahadmali.onmicrosoft.com]

Adriana Philippson [Adriana.Phillipson@kancelariahadmali.onmicrosoft.com]

Alia Khou [Alia.Khou@kancelariahadmali.onmicrosoft.com]

Alison Flawley [Alison.Flawley@kancelariahadmali.onmicrosoft.com]

Allyn Windbush [Allyn.Windbush@kancelariahadmali.onmicrosoft.com]

Almae Domonelli [Almae.Domonelli@kancelariahadmali.onmicrosoft.com]

Cofnij Dalej

W ostatnim kroku można zdefiniować ustawienia integracji. Najpierw można przypisać atrybuty z Azure AD, aby automatycznie dopasować je do odpowiednich wartości w Essentials MDM (np. adres e-mail, imię, nazwisko, numer telefonu lub stanowisko).

Szczegóły

Wprowadź poświadczenia

Zweryfikuj integrację

Mapowanie pól użytkownika

Mapowanie pól grupy

Ustawienia

Atrybut Essentials MDM	Atrybut Azure	Przekształcenie RegExp	Przekształcenie wartości
Login do Essentials MDM *	userPrincipalName	Przekształcenie RegExp	Przekształcenie wartości
Imię	givenName	Przekształcenie RegExp	Przekształcenie wartości
Nazwisko	surname	Przekształcenie RegExp	Przekształcenie wartości
Stanowisko	jobTitle	Przekształcenie RegExp	Przekształcenie wartości
Telefon do biura	businessPhones	Przekształcenie RegExp	Przekształcenie wartości

Dalej

W następnym kroku możesz zrobić to samo z atrybutami grup.

Szczegóły

Wprowadź poświadczenia

Zweryfikuj integrację

Mapowanie pól użytkownika

Mapowanie pól grupy

Ustawienia

Atrybut Essentials MDM	Atrybut Azure	Przekształcenie RegExp	Przekształcenie wartości
Nazwa grupy *	displayName	Przekształcenie RegExp	Przekształcenie wartości
Opis grupy	description	Przekształcenie RegExp	Przekształcenie wartości

Dodaj nowe pole

Cofnij

Dalej

W ostatnim kroku można również zdefiniować filtry, aby ograniczyć importowane dane zgodnie z określonymi parametrami dla użytkowników i/lub grup. Można również zdefiniować interwał synchronizacji (domyślnie 60 minut, maksymalnie 24 godziny) i Powiadomienie o niepowodzeniu synchronizacji.



Szczegóły

×

Wprowadź poświadczenia

Zweryfikuj integrację

Mapowanie pól użytkownika

Mapowanie pól grupy

Ustawienia

Filtry

Typ filtru

Podstawowy filtr grup

Zaawansowany filtr użytkowników i grup

Importuj użytkowników tylko z odfiltrowanych grup (zostaw puste pole by zaimportować wszystkich użytkowników)

Test

Sales

Interwał synchronizacji

Interwał synchronizacji\*

60 minut

Powiadomienie o niepowodzeniu synchronizacji

Powiadomienie o niepowodzeniu synchronizacji\*

Przy każdym błędzie synchronizacji

Cońnij

Zapisz i uruchom synchronizację

Szczegółowy opis składni filtra można znaleźć w dokumentacji Microsoft:

<https://docs.microsoft.com/en-us/graph/query-parameters#filter-parameter>

Dodatkowo możliwe jest również korzystanie z zaawansowanych zapytań:

<https://docs.microsoft.com/en-us/graph/aad-advanced-queries>

Microsoft udostępnia narzędzie do sprawdzania poprawności wprowadzonych filtrów:

<https://developer.microsoft.com/en-us/graph/graph-explorer>

Aby zakończyć proces, kliknij Zapisz i uruchom synchronizację.

Jeśli proces przebiegł poprawnie, zobaczysz krótkie podsumowanie zaimportowanych użytkowników, jak na poniższym obrazku. Możesz wprowadzić zmiany w integracji, klikając "Edytuj".

### Integracja z usługą Azure Active Directory

[Synchronizuj teraz](#)[Usuń integrację](#)[Edytuj](#)

Zintegruj Essentials MDM z Azure Active Directory i zsynchronizuj użytkowników oraz grupy.

Nazwa: Tehcstep Essentials

Status synchronizacji: **wykonana poprawnie**

Ostatnia synchronizacja: 17 minut temu 

Następna synchronizacja: za 43 minuty 

Użytkownicy stworzeni przez Azure: **2** (do usunięcia: **1** 

Grupy stworzone przez Azure: **2**