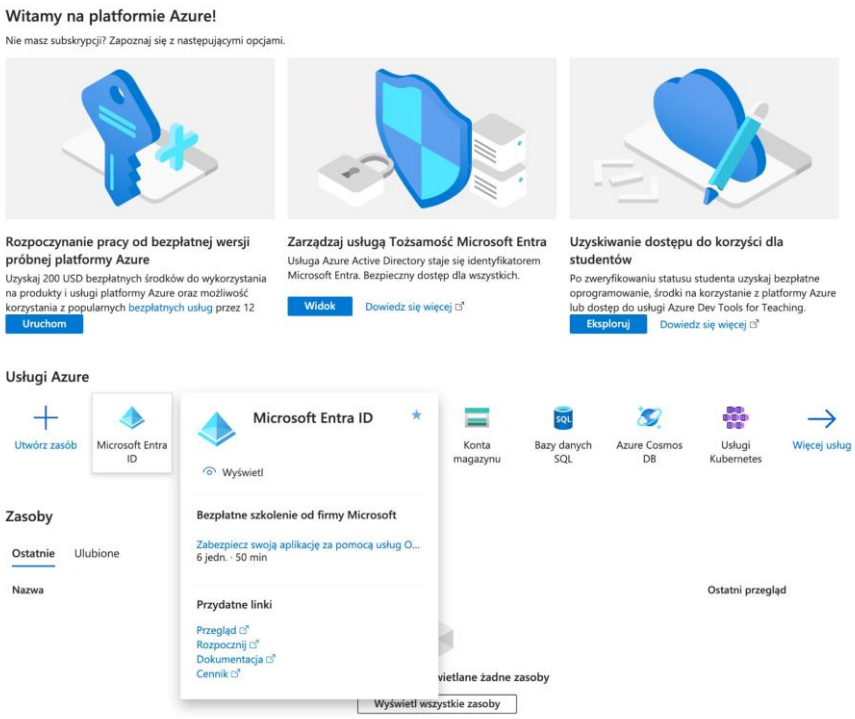
tech8tep

Integracja z Azure Active Directory

Data: 4/12/2023

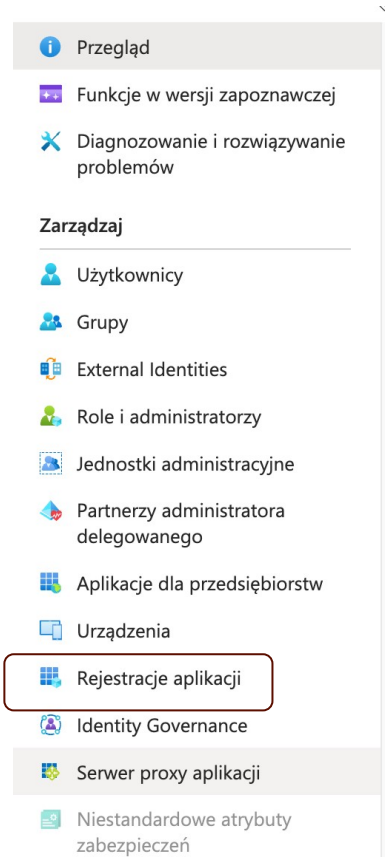
1. Rozpoczęcie – rejestracja aplikacji

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.

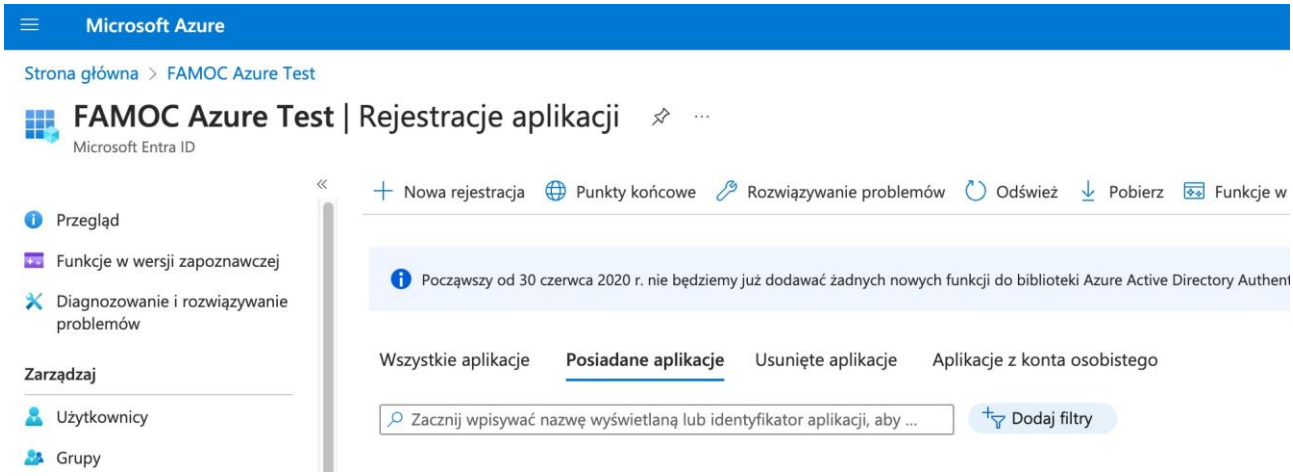


Rejestrowanie Essentials MDM na platformie Azure

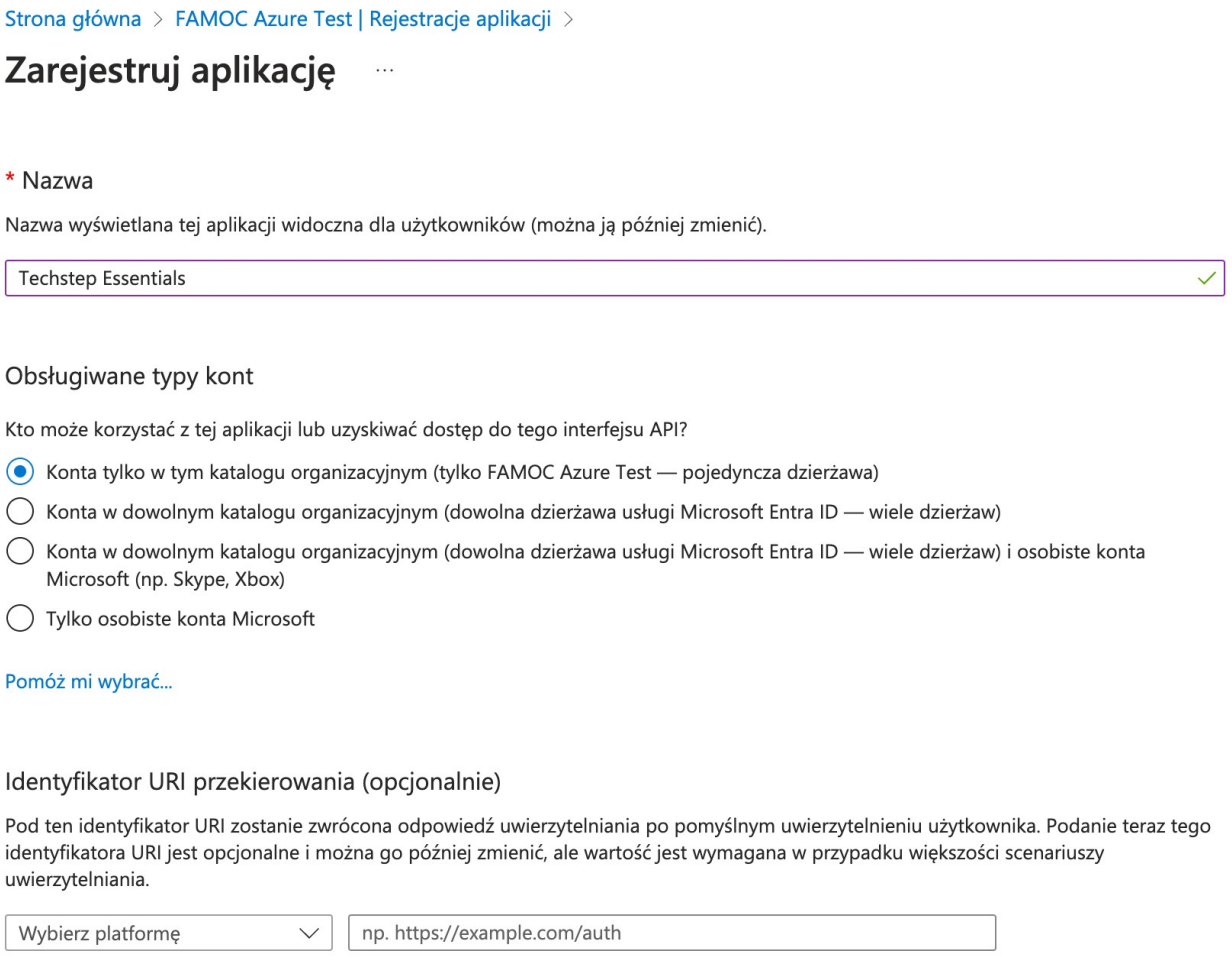
Po przejściu do zakładki Azure AD, z menu po lewej stronie wybierz Rejestracje aplikacji (App registration).



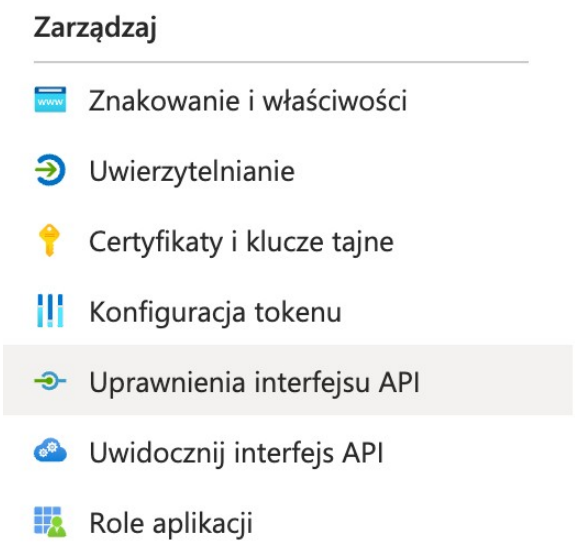
Następnie wybierz opcję Nowa rejestracja (New registration).



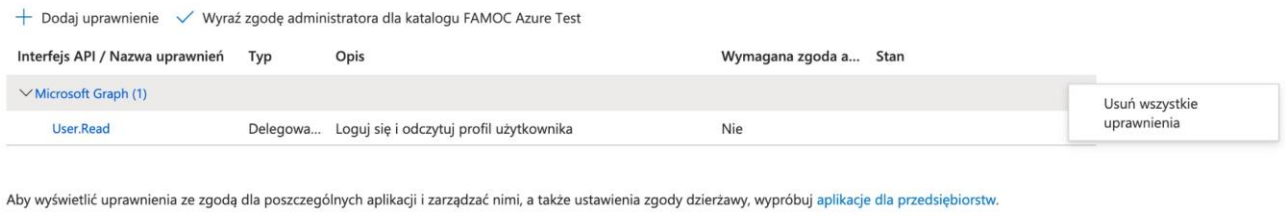
W kolejnym kroku wprowadź nazwę Aplikacji i określ, czy dostęp do niej mają mieć konta z jednej domeny, czy z większej liczby domen - wybierz **pojedyncza dzierżawa** lub **wiele dzierżaw**. Możemy także podać URI, na który użytkownik ma zostać przekierowany po pomyślnym uwierzytelnieniu (jest to opcjonalne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



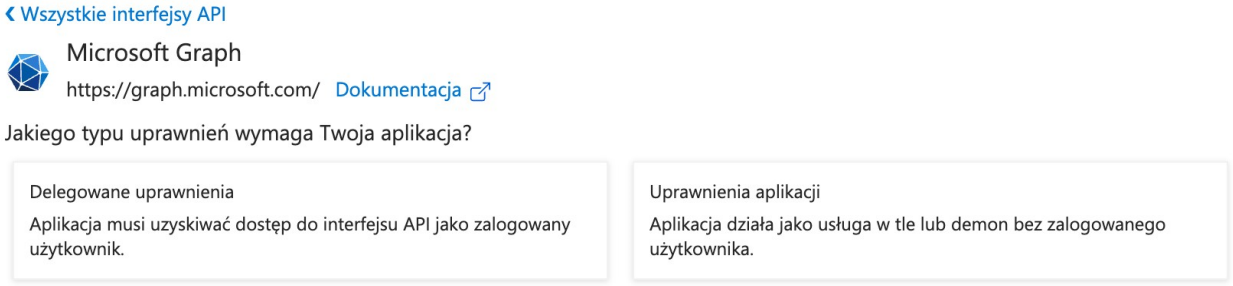
Następnie przejdź do zakładki **API permissions**, aby skonfigurować uprawnienia aplikacji.



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

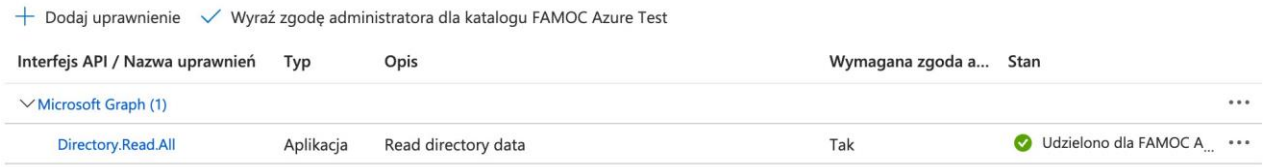


Następnie klikamy Dodaj uprawnienie (**Add a permission**). Wybieramy Microsoft Graph, a następnie Uprawnienia aplikacji (**Application permissions**).

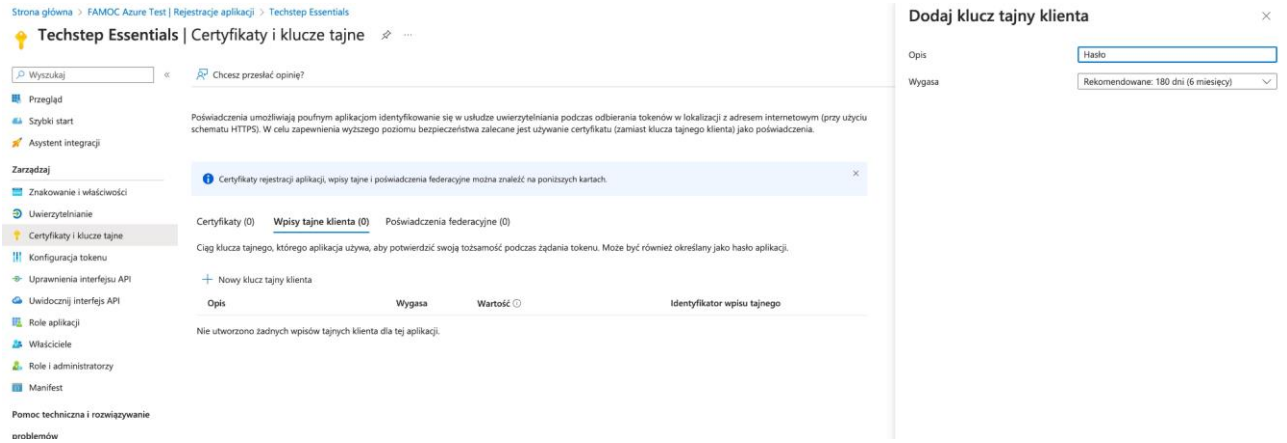


W sekcji Katalog (**Directory**)wybierz directory.read.all i potwierdź, klikając Dodaj uprawnienia (**Add permissions**).

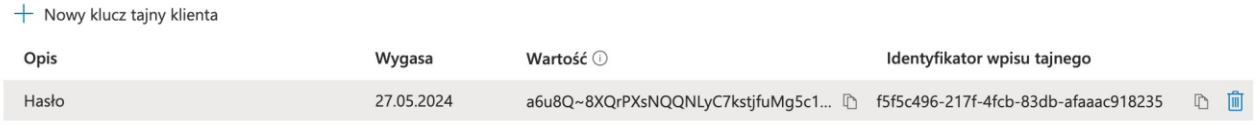
W sekcji Uprawnienia API (API permissions) wymagane jest również udzielenie zgody administratora na utworzoną aplikację (**Grant Admin consent**).



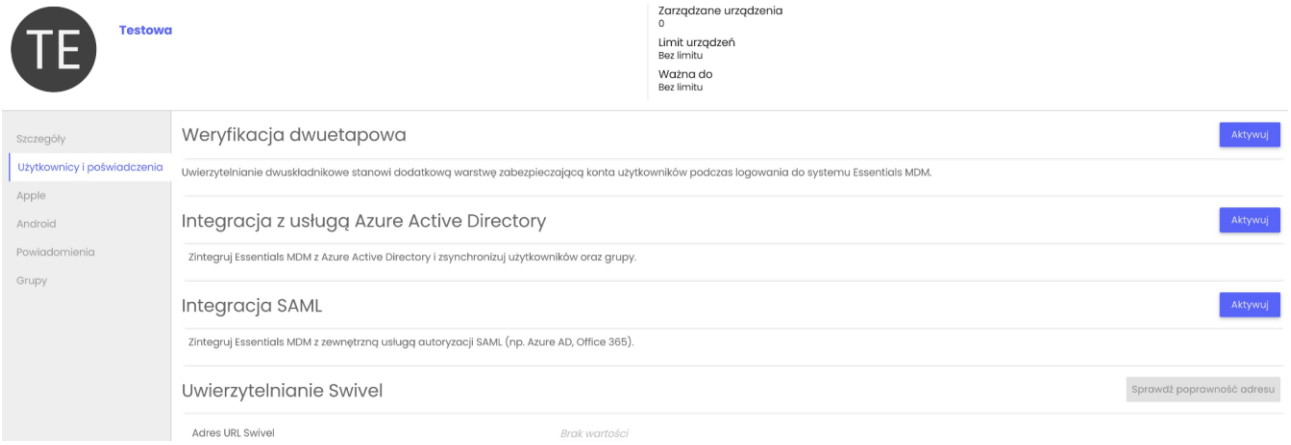
Następnie przejdź do zakładki Certyfikaty i klucze tajne (**Certificates & secrets**), aby dodać nowy klucz tajny klienta. Kliknij przycisk Nowy klucz tajny klienta (**New client secret**), wprowadź jego opis i określ czas wygaśnięcia.



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

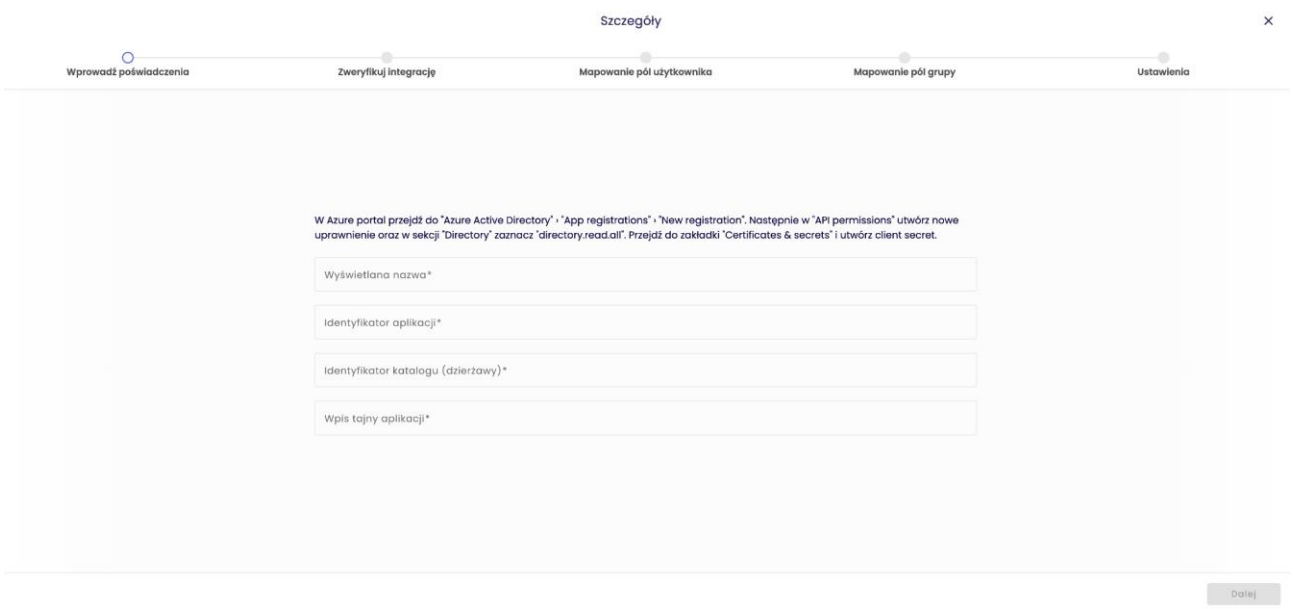


Następnie zaloguj się do konsoli Essentials. Przejdź do ustawień organizacji, sekcji Użytkownicy i poświadczenia, a następnie znajdź sekcję Integracja z Azure Active Directory. Kliknij przycisk Aktywuj.

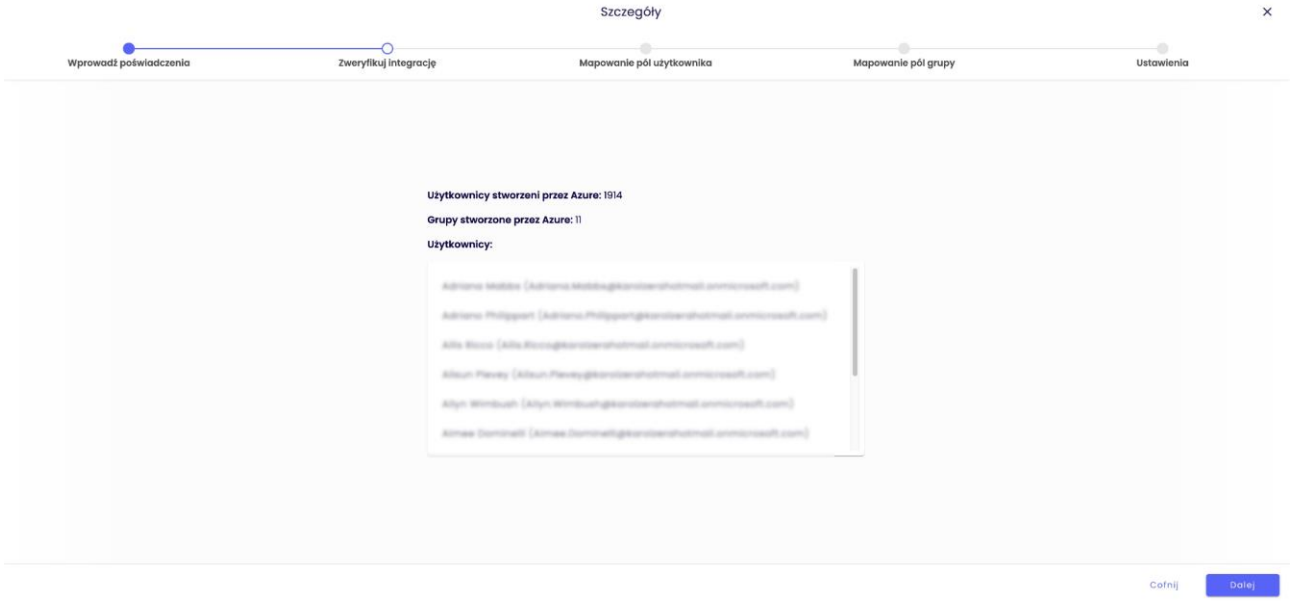


W następnym kroku wprowadź następujące dane pobrane z Azure Portal:

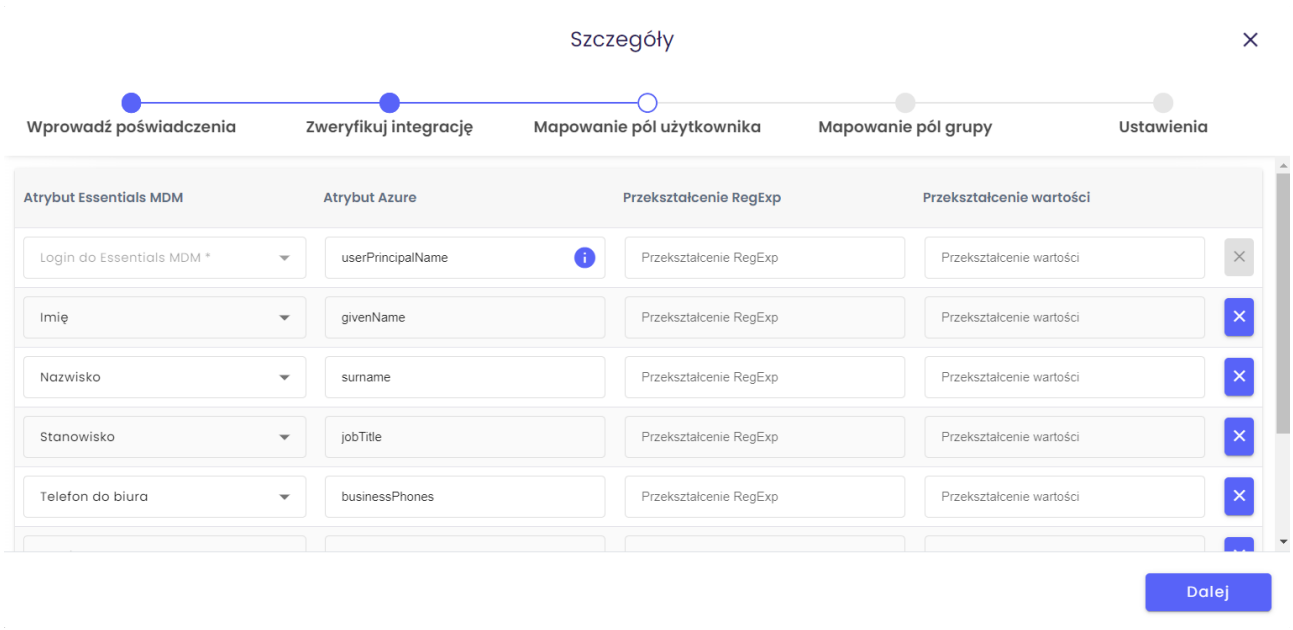
- Wyświetlana nazwa (może być dowolna)
- Identyfikator aplikacji (klienta)
- Identyfikator katalogu (dzierżawy)
- Sekret aplikacji



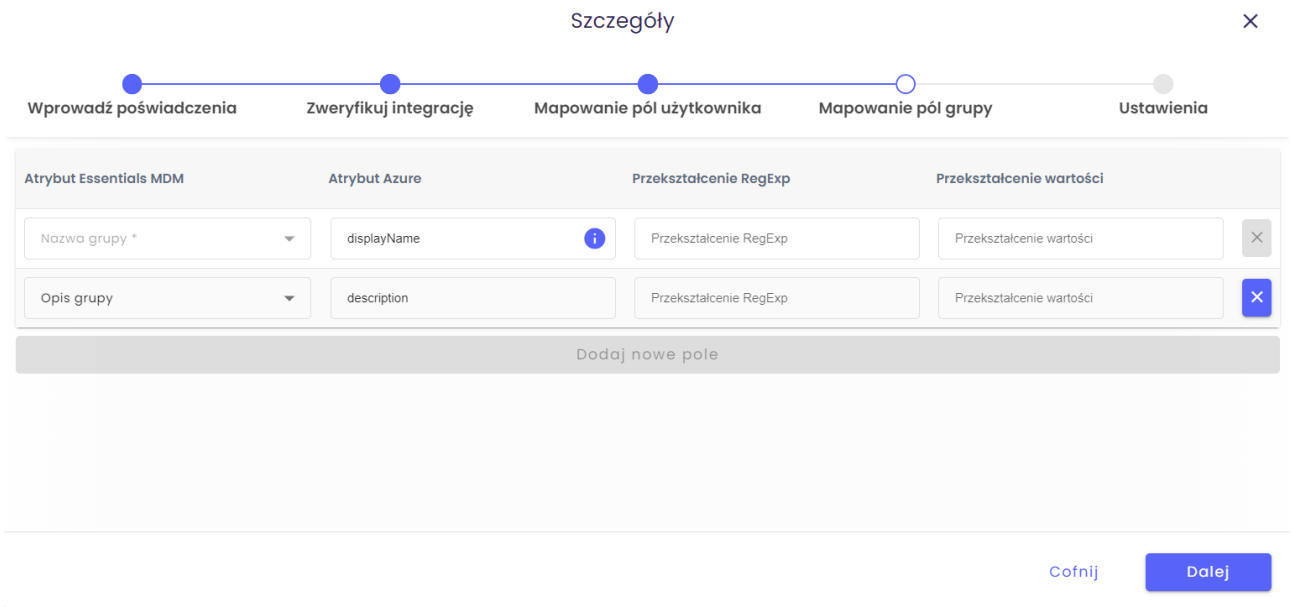
Po kliknięciu Dalej Twoja integracja zostanie zweryfikowana.



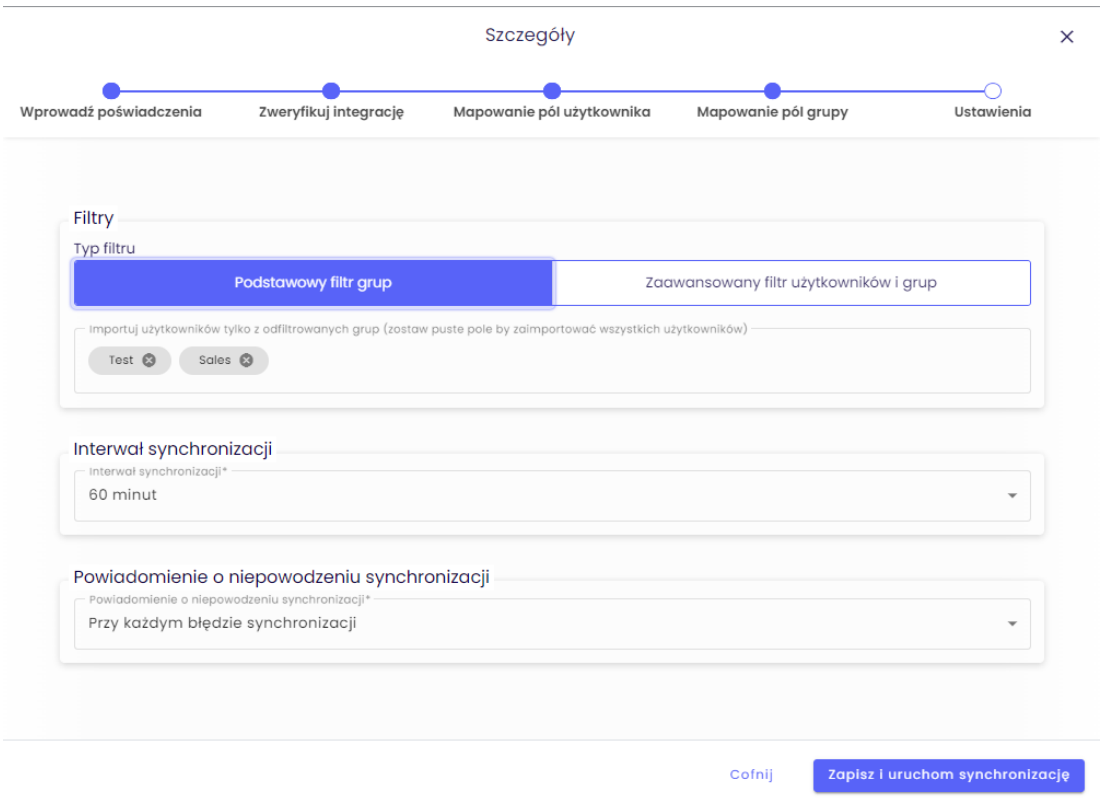
W ostatnim kroku można zdefiniować ustawienia integracji. Najpierw można przypisać atrybuty z Azure AD, aby automatycznie dopasować je do odpowiednich wartości w Essentials MDM (np. adres e-mail, imię, nazwisko, numer telefonu lub stanowisko).



W następnym kroku możesz zrobić to samo z atrybutami grup.



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.



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".