



Integracja z Azure SAML

Data: 01/12/2023



Jak działa protokół SAML?

Protokół SAML umożliwia logowanie się do konsoli administratora Essentials MDM za pośrednictwem usług zewnętrznych (Identity Provider).











Użytkownik może zalogować się do IdP i wybrać Essentials MDM spośród aplikacji, po czym zostanie automatycznie zalogowany do Essentials MDM przy użyciu poświadczeń IdP. Jeśli użytkownik nie ma konta w Essentials MDM, takie konto może zostać utworzone automatycznie (pod warunkiem, że w ustawieniach Essentials MDM wybrano opcję *Automatycznie twórz użytkowników*). Po wylogowaniu się z Essentials MDM, użytkownik może zalogować się ponownie za pomocą przycisku **Zaloguj używając SAML**, który przekieruje do strony logowania w IdP. Jednym z takich IdP jest Microsoft Azure.

Dodawanie nowej aplikacji w portalu Azure

Aby zintegrować Essentials MDM z Azure SAML, należy utworzyć aplikację Essentials MDM w Azure, a następnie skonfigurować dane z Azure.

1. Zaloguj się do Microsoft Azure Portal za pośrednictwem adresu URL <https://portal.azure.com>.
2. Wybierz Azure Active Directory. Następnie wybierz opcję **Aplikacje dla Przedsiębiorstw** (Enterprise Applications) z panelu po lewej stronie.

Zarządzaj

-  Użytkownicy
-  Grupy
-  External Identities
-  Role i administratorzy
-  Jednostki administracyjne
-  Partnerzy administratora delegowanego
-  **Aplikacje dla przedsiębiorstw**
-  Urządzenia
-  Rejestracje aplikacji
-  Identity Governance

3. Aby dodać aplikację, kliknij +Nowa aplikacja (New application).

[Strona główna](#) >

FAMOC Azure Test | Przegląd
Microsoft Entra ID

+ Dodaj > Zarządzaj dzierżawami Co now

- Użytkownik >
- Grupa
- Aplikacja dla przedsiębiorstw
- Rejestracja aplikacji

Informacje podstawowe

Nazwa FAMOC Azure Test

4. Wybierz Utwórz własną aplikację (Create your own application), wprowadź nazwę aplikacji (dowolna nazwa, np. Essentials MDM) i kliknij Utwórz. (Użyj Non-gallery)

Strona główna > FAMOC Azure Test | Przegląd > Przeglądanie galerii rozwiązań Microsoft Entra

Przeglądanie galerii rozwiązań Microsoft Entra

+ Utwórz własną aplikację Chcesz przesłać opinię?

Galeria aplikacji rozwiązań Microsoft Entra to wykaz typów aplikacji, które ułatwiają wdrażanie i konfigurowanie logowania jednokrotnego (SSO) oraz automatyczną aprobowanie użytkowników. Podczas wdrażania aplikacji z galerii aplikacji korzystasz ze wstępnie utworzonej aplikacji. Jeśli chcesz opublikować aplikację opracowaną w galerii rozwiązań Microsoft Entra w celu odnawiania i używania jej przez inne organizacje, możesz przesłać zadanie przy użyciu procesu opisanego w tym artykule.

Wyszukaj aplikację Logowanie jednokrotne: Wszystkie Zarządzanie kontami użytkowników: All Kategorie: Wszystkie

Platformy w chmurze

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle
- SAP

Utwórz własną aplikację

Chcesz przesłać opinię?

Jeśli tworzysz własną aplikację, korzystasz z serwera proxy aplikacji lub chcesz zintegrować aplikację, która nie znajduje się w galerii, możesz tutaj utworzyć własną aplikację.

Jaka jest nazwa Twojej aplikacji?

Wprowadź nazwę

Co chcesz zrobić z aplikacją?

- ☐ Skonfiguruj serwer proxy aplikacji na potrzeby bezpiecznego dostępu zdalnego do aplikacji lokalnej.
- ☐ Zintegruj aplikację, aby zintegrować ją z usługą Microsoft Entra ID (aplikacja, którą opracowujesz).
- ☒ Zintegruj dowolną inną aplikację, której nie można znaleźć w galerii (aplikację spoza galerii).

5. Przejdź do Zarządzaj (Manage) - Pojedyncze logowanie (Single Sign-On) - > SAML

Strona główna > FAMOC Azure Test | Przegląd > Przeglądanie galerii rozwiązań Microsoft Entra > Techstep

Techstep | Logowanie jednokrotne

Aplikacja dla przedsiębiorstw

Przegląd

Plan wdrożenia

Diagnozowanie i rozwiązywanie problemów

Zarządzaj

- Właściwości
- Właściciele
- Rola i administratorzy
- Użytkownicy i grupy
- Logowanie jednokrotne**
- Aprobowanie
- Serwer proxy aplikacji
- Samobsługa
- Niestandardowe atrybuty zabezpieczeń

Zabezpieczenia

Logowanie jednokrotne (SSO) zapewnia zabezpieczenia i wygodę, gdy użytkownicy logują się do aplikacji w usłudze Microsoft Entra ID, umożliwiając dodatkowo użytkownikom w organizacji logowanie się do każdej używanej aplikacji przy użyciu tylko jednego konta. Gdy użytkownik zaloguje się do aplikacji, to jego poświadczenie jest używane dla wszystkich innych aplikacji, do których potrzebuje dostępu. [Dowiedz się więcej.](#)

Wybierz metodę logowania jednokrotnego Pomóż mi zdecydować

- Wylączone**
Logowanie jednokrotne nie jest włączone. Użytkownik nie będzie mógł uruchomić aplikacji z poziomu portalu Moje aplikacje.
- SAML**
Zaawansowane i bezpieczne uwierzytelnianie w aplikacjach korzystających z protokołu SAML (Security Assertion Markup Language).
- Oparte na hasle**
Przechowywanie i powtarzanie haseł przy użyciu rozszerzenia przeglądarki internetowej lub aplikacji mobilnej.
- Połączone**
Link do aplikacji w rozszerzeniu Moje aplikacje i/lub module uruchamiania aplikacji usługi Office 365.

6. Wypełnij następujące pola:

Identyfikator (Entity ID) – może to być adres URL serwera Essentials MDM lub dowolna inna wartość, np. essentials.yourorganization.com (ta sama wartość będzie musiała zostać podana jako parametr EntityId w ustawieniach Essentials SAML); Uwaga, zaznacz tę wartość jako domyślną (Default).

Adres URL odpowiedzi (Assertion Consumer Service URL):
https://adresserwera.com/ui/ (koniecznie z / ui / na końcu).

Podstawowa konfiguracja protokołu SAML

 Zapisz |  Chcesz przesłać opinię?

Identyfikator (identyfikator jednostki) * ⓘ

Unikatowy identyfikator rozpoznający aplikację w usłudze Microsoft Entra ID. Ta wartość musi być unikatowa we wszystkich aplikacjach w dzierżawie usługi Microsoft Entra ID. Domyślnym identyfikatorem będą odbiorcy odpowiedzi SAML dla logowania jednokrotnego zainicjowanego przez dostawcę tożsamości.

Domyślna



[Dodaj identyfikator](#)

Adres URL odpowiedzi (adres URL usługi Assertion Consumer Service) * ⓘ

Adres URL odpowiedzi to miejsce, w którym aplikacja spodziewa się otrzymać token uwierzytelniania. Jest on także określany jako usługa ACS (Assertion Consumer Service) w standardzie SAML.

Ind...

Domyślna



[Dodaj adres URL odpowiedzi](#)

Zapisz zmiany i zamknij tę sekcję.

- W sekcji User Attributes & Claims należy pozostawić tylko Unique User Identifier – pozostałe identyfikatory można usunąć. Ten musi pozostać, dodatkowo w edycji tego identyfikatora należy ustawić "Nazwę kwalifikowaną domeny Windows" (Windows domain qualified name) w "Wybierz format identyfikatora nazwy" (Choose name identifier format).

 Zapisz |  Odrzuć zmiany |  Chcesz przesłać opinię?

Nazwa *	name
Przestrzeń nazw	Wprowadź identyfikator URI przestrzeni nazw
^ Wybierz format nazwy	
Format nazwy	Podstawowy
Źródło *	<input checked="" type="radio"/> Atrybut <input type="radio"/> Przekształcenie <input type="radio"/> Rozszerzenie schematu katalogu
Atrybut źródłowy *	user.userprincipalname
<div> <div>Warunki oświadczenia</div> <div>Zaawansowane opcje oświadczeń SAML</div> </div>	

Zapisz zmiany i zamknij tę sekcję.

- Następnie w sekcji SAML Certificate pobierz certyfikat (Base64). Będzie on służył jako certyfikat X509 w ustawieniach Essentials SAML.

Certyfikaty SAML

Certyfikat podpisywania tokenu

Stan	Aktywne	Edytuj
Odcisk palca	4F54ADF9D2D3BF259183107FEBBEAEF24AD74BE2	
Wygaśnięcie	1.11.2028, 17:03:27	
Wiadomość e-mail z powiadomieniem	karol.zera@hotmail.com	
Adres URL metadanych federacyjnych aplikacji	https://login.microsoftonline.com/abf77a0f-0016-...	
Certyfikat (base64)	Pobierz	
Certyfikat (nieprzetworzony)	Pobierz	
Kod XML metadanych federacji	Pobierz	

Certyfikaty weryfikacji (opcjonalne)

Wymagane	Nie	Edytuj
Aktywne	0	
Wygaśnięcie	0	

Należy również pamiętać, że użytkownicy i/lub grupy użytkowników, którzy będą mogli logować się za pomocą tej metody, muszą być przypisani do aplikacji. W tym celu należy przejść do sekcji Użytkownicy i grupy (Users and groups), a następnie kliknąć przycisk Dodaj użytkownika/grupę (Add user/group).

Strona główna > TestSAML

TestSAML | Użytkownicy i grupy

Aplikacja dla przedsiębiorstw

Przegląd

Plan wdrożenia

Diagnozowanie i rozwiązywanie problemów

Zarządzaj

Właściwości

Właściciele

Role i administratorzy

Użytkownicy i grupy

Logowanie jednokrotne

Aprobowanie

Serwer proxy aplikacji

Samoobsługa

« + Dodaj użytkownika/grupę | Edycja przypisania | Usuń | Aktualizuj poświadczenia | Kolumny | Chcesz przesłać opinię?

1 Aplikacja będzie widoczna w rozszerzeniu Moje aplikacje dla przypisanych użytkowników. Aby temu zapobiec, ustaw we właściwościach opcję „widoczne dla użytkowników?” na wartość „nie”. →

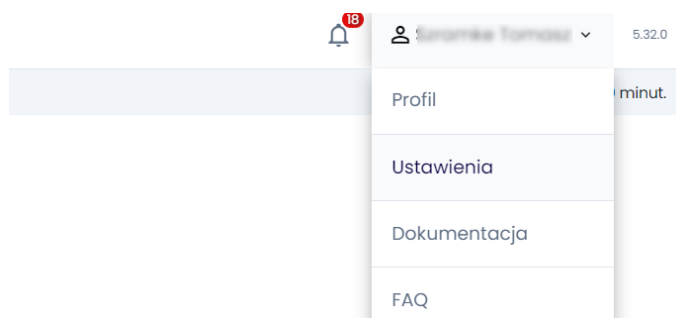
Tutaj przypisz użytkowników i grupy do ról aplikacji dla aplikacji. Aby utworzyć nowe role aplikacji dla tej aplikacji, użyj rejestracji aplikacji.

🔍 Pokazano pierwszych 200 pozycji. Aby prz...

	Nazwa wyświetlana	Typ obiektu
<input type="checkbox"/>	AM Adriana Mabbs	Użytkownik

Konfiguracja SAML w Essentials MDM

Aby skonfigurować SAML Azure w Essentials, przejdź do Ustawień organizacji:



1. Następnie znajdź integrację SAML w sekcji "Użytkownicy i uwierzytelnianie" i kliknij Aktywuj.
2. Prześlij wcześniej pobrany certyfikat (Base64).
3. Wprowadź ten sam identyfikator podmiotu, który wprowadziłeś w Azure Portal.
4. W polu Login URL wprowadź adres URL dostępu użytkownika z Azure Portal. Z tej strony możesz również zalogować się do Essentials MDM.

Właściwie wprowadzone dane powinny wyglądać następująco:

A screenshot of the 'Ustawienia SAML' (SAML Settings) configuration page in the Azure portal. The page has a title bar with 'Ustawienia SAML' and a close button. Below the title bar is a progress indicator with three steps: 'Wprowadź poświadczenia' (highlighted with a blue circle), 'Tworzenie użytkowników', and 'Mapowanie pól użytkownika'. The main content area contains three input fields: 'Login URL*' with the value 'https://myapps.microsoft.com/signin/2f17eefa-1864-4938-9dea-6b88fb74b19f?tenantId=ed66d488-3c7d-4237-842e-...', 'Identyfikator*' with the value 'https://fm.techdemo.no/ui/', and 'Certyfikat X.509*' with a file upload button labeled 'Plik z certyfikatem (1.066 kB)'. At the bottom right, there is a blue 'Dalej' (Next) button.

Naciśnij "Dalej".

Na następnej stronie włącz "Automatycznie twórz użytkowników i przypisz rolę dla tych użytkowników. Naciśnij "Dalej".

Na ostatniej stronie musisz zmapować login Essentials MDM do właściwego atrybutu SAML. Możesz dodać więcej atrybutów. Służą one do mapowania atrybutów z Azure AD do Essentials MDM. Mapowanie atrybutów pozwala na automatyczne utworzenie użytkownika w Essentials MDM z tymi samymi danymi, co w Azure AD. Dzięki temu użytkownik może mieć automatycznie przypisane takie wartości jak adres e-mail czy domena, co pozwoli na łatwiejszą konfigurację np. konta e-mail.

Ustawienia SAML

Wprowadź poświadczenia

Tworzenie użytkowników

Mapowanie pól użytkownika

Atrybut Essentials MDM

Atrybut SAML

Login do FAMOC *

saml2:NameID

Atrybut Essentials MDM

Atrybut SAML *

Dodaj nowe pole

Cofnij

Zapisz ustawienia

Znane problemy

W niektórych przypadkach podczas próby zalogowania się do Essentials MDM przy użyciu usługi Azure AD może zostać wyświetlony błąd 400. Może się tak zdarzyć, jeśli użytkownik jest już zalogowany w tej samej przeglądarce. Aby temu zapobiec, wyloguj się i wyczyść pliki cookie przeglądarki.

Podsumowanie

Od teraz przy logowaniu z tego samego komputera i tej samej przeglądarki będzie zapamiętywane, że zalogowałeś się za pomocą Azure AD i będzie to sugerowane po wejściu na stronę logowania Essentials MDM.

techStep

Zaloguj się

Nazwa użytkownika

Hasło

ZALOGUJ

lub

ZALOGUJ PRZEZ SAML