FAMOC®

Przewodnik integracji SAML Azure

www.famoc.com

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

Spis treści

1 Jak działa protokół SAML?

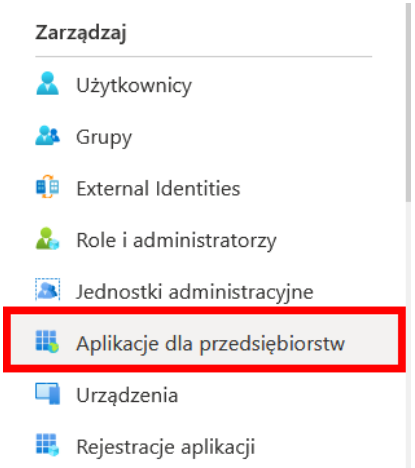
Protokół SAML umożliwia logowanie się do konsoli administracyjnej FAMOC manage za pośrednictwem usług zewnętrznych (Identity Provider).

Użytkownik może zalogować się do IdP i wybrać spośród aplikacji FAMOC manage. Zostanie w tym momencie automatycznie zalogowany do FAMOC z poświadczeniami dostawcy tożsamości. Jeżeli użytkownik nie posiada konta w zarządzaniu FAMOC, takie konto może zostać utworzone automatycznie (pod warunkiem, że w ustawieniach zarządzania FAMOC wybrana jest opcja Automatycznie twórz użytkowników). Po wylogowaniu się z FAMOC manage, użytkownik może zalogować się ponownie za pomocą przycisku Zaloguj przez SAML, który przekieruje Cię do strony logowania w IdP. Jednym z takich dostawców tożsamości jest Microsoft Azure.

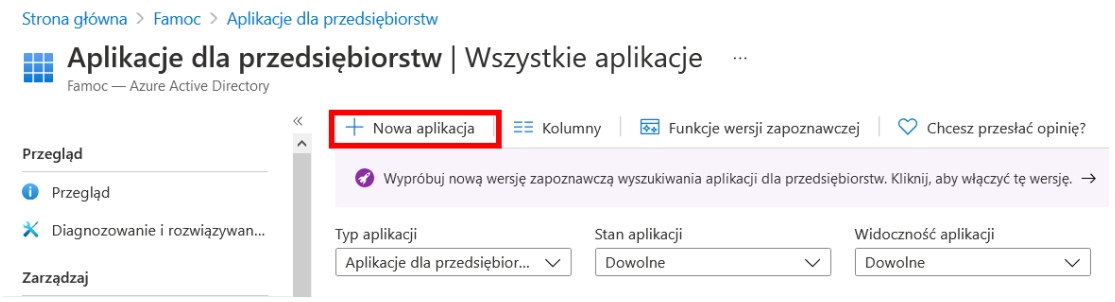
2 Dodawanie nowej aplikacji w portalu Azure

Aby zintegrować FAMOC manage z Azure SAML, musisz utworzyć aplikację FAMOC na platformie Azure, a następnie skonfigurować dane z platformy Azure.

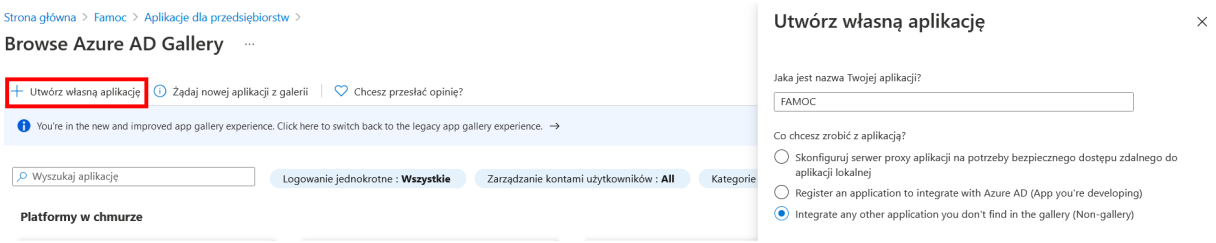
1. Zaloguj się do portalu Microsoft Azure za pośrednictwem adresu URL https://portal.azure.com.
2. Wybierz Azure Active Directory. Następnie wybierz opcję Aplikacje dla przedsiębiorstw z panelu po lewej stronie.



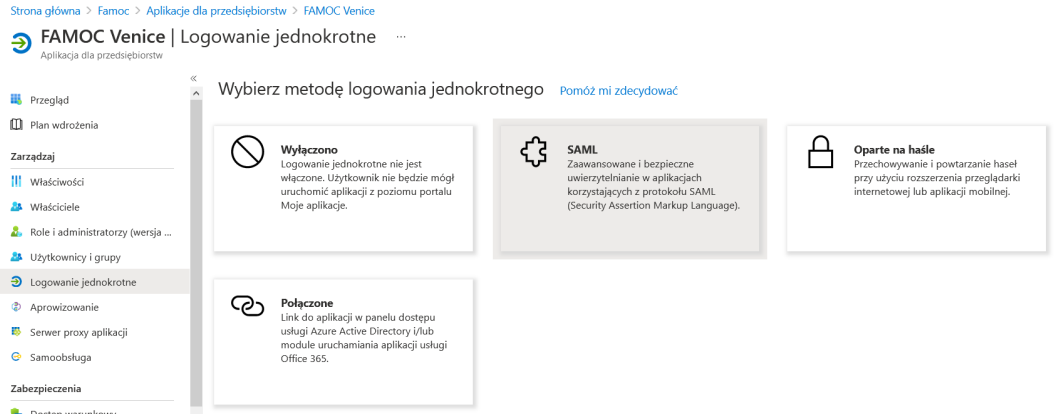
3. Aby dodać aplikację, kliknij Nowa aplikacja.



4. Wybierz Utwórz własną aplikację, wprowadź nazwę aplikacji (dowolna nazwa, np. FAMOC manage) i kliknij Stwórz



5. Przejdź do Logowanie jednokrotne -> SAML

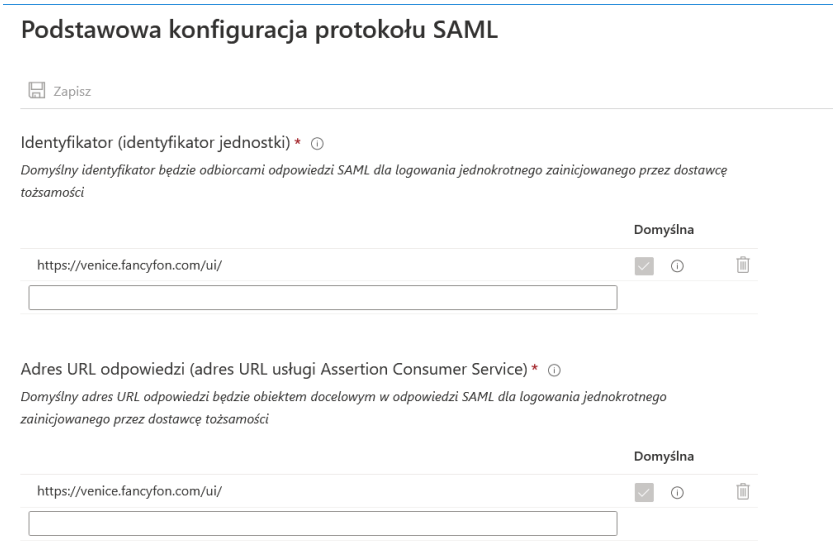


6. Wypełnij następujące pola:

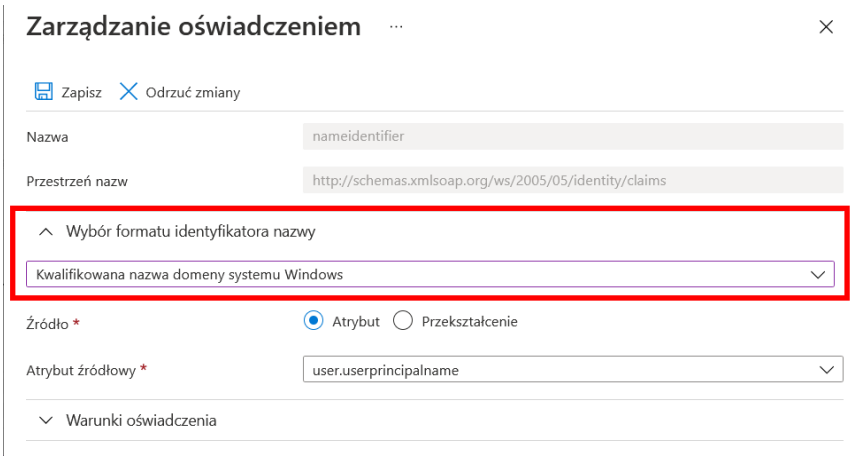
Identyfikator (identyfikator jednostki) - może to być adres URL Twojego serwera zarządzającego FAMOC lub dowolna inna wartość, np. famoc.yourorganization.com (tę samą wartość należy podać jako parametr EntityId w ustawieniach SAML zarządzania FAMOC)

Adres URL odpowiedzi (adres URL usługi Assertion Consumer Service):

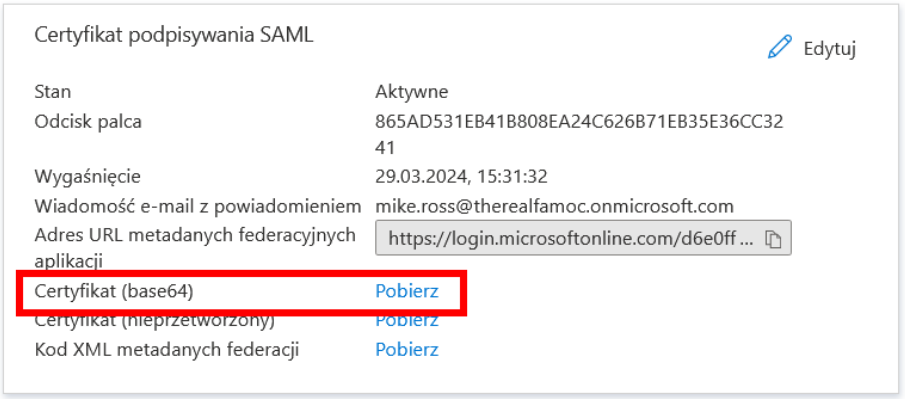
https://adreserwera.com/ui/ (koniecznie z / ui / na końcu).



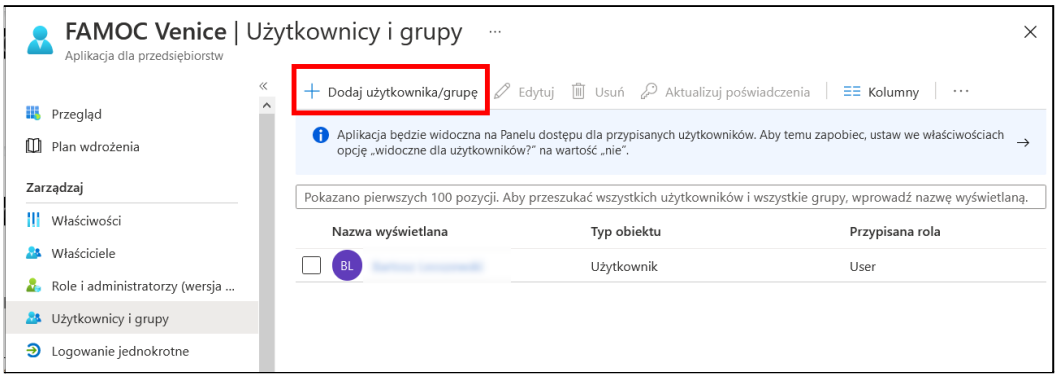
7. W sekcji Atrybuty i oświadczenia użytkowników pozostaw tylko Unikatowy identyfikator użytkownika - pozostałe identyfikatory można usunąć. Ten musi pozostać, a dodatkowo, edytując ten identyfikator, należy ustawić domenę Windows ... w „Wybierz format identyfikatora nazwy”.



8. Pobierz także certyfikat (Base64). Będzie służyć jako cert X509 w ustawieniach SAML w konsoli FAMOC manage.

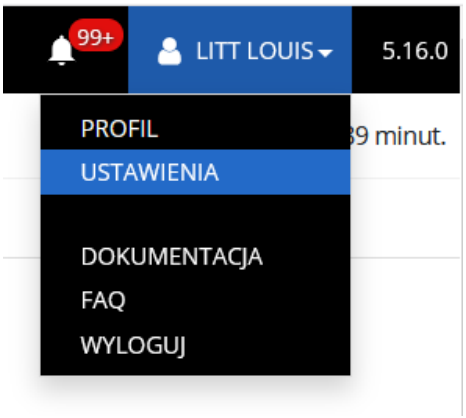


Należy również pamiętać, że do aplikacji muszą być przypisani użytkownicy i / lub grupy użytkowników, którzy będą mogli logować się tą metodą. Aby to zrobić, przejdź do sekcji Użytkownicy i grupy, a następnie kliknij Dodaj użytkownika / grupę.



3 Konfiguracja SAML Azure w FAMOC

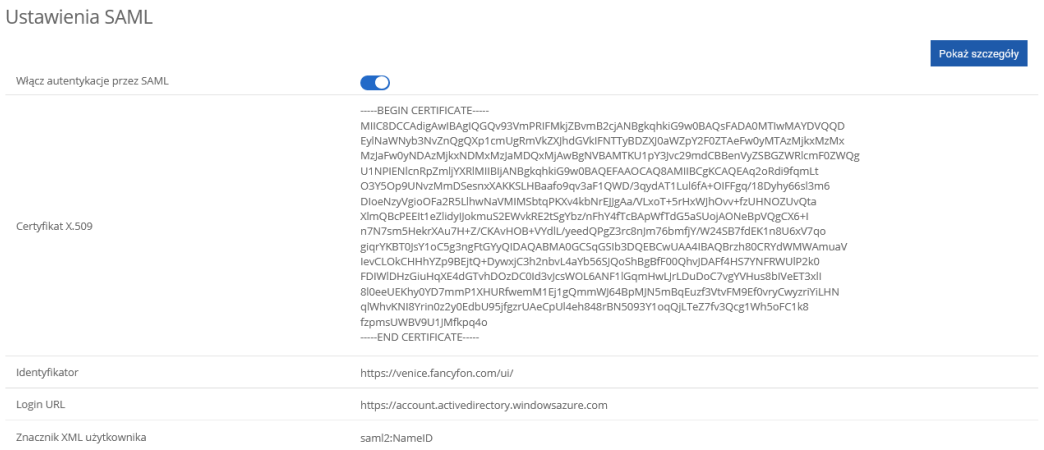
Aby skonfigurować SAML Azure AD w FAMOC, przejdź do ustawień organizacji:



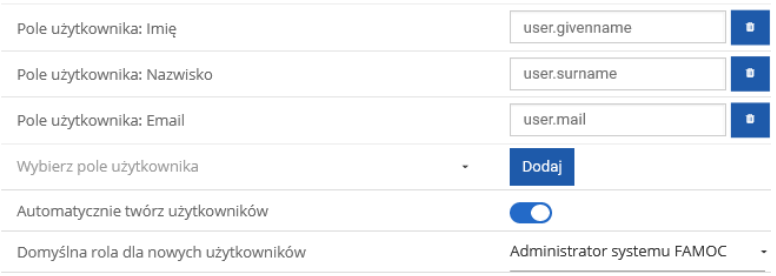
1. Następnie znajdź sekcję ustawień SAML i kliknij Włącz autentykację przez SAML.

2. Otwórz pobrany wcześniej Certyfikat (Base64) w dowolnym edytorze tekstu (np. NotePad), skopiuj całą zawartość i wklej ją w polu Certyfikat X.509.
3. Wprowadź ten sam identyfikator jednostki, który został wprowadzony w witrynie Azure Portal
4. Adres URL logowania to https://account.activedirectory.windowsazure.com (uwaga: nie ten z ustawień aplikacji). Z tej strony możesz również zalogować się do FAMOC.

Poprawnie edytowane dane wyglądają następująco:



Pozostałe pola są opcjonalne. Są używane do mapowania atrybutów z usługi Azure AD do zarządzania FAMOC. Mapowanie atrybutów umożliwia automatyczne tworzenie użytkownika w FAMOC z tymi samymi danymi, co w usłudze Azure AD. Dzięki temu użytkownik może automatycznie mieć przypisane wartości takie jak adres e-mail czy domena, co pozwoli na łatwiejszą konfigurację np. konta e-mail.
Możesz także zaznaczyć opcję automatycznego tworzenia użytkowników w FAMOC i przypisać im domyślną rolę



Znane problemy

W niektórych przypadkach podczas próby zalogowania się do konsoli FAMOC manage może pojawić się błąd 400. Może się to zdarzyć, jeśli jesteś już zalogowany w tej samej przeglądarce. Aby temu zapobiec, wyloguj się i wyczyść pliki cookie przeglądarki.

Podsumowanie

Od teraz logując się z tego samego komputera i tej samej przeglądarki będzie pamiętane, że logowałeś się do FAMOC manage poprzez Azure AD i zostanie to zasugerowane po wejściu na stronę logowania do zarządzania FAMOC manage.