

# FAMOC<sup>®</sup>

## Przewodnik integracji SAML Azure



[www.famoc.com](http://www.famoc.com)

PUBLISHED BY

FAMOC S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

Copyright© 2008-2021 by Famoc S.A.

Wszystkie prawa zastrzeżone. Cała zawartość dokumentu stanowi wyłączną własność firmy Famoc S.A. i nie może być powielana ani dystrybuowana bez pisemnej zgody wydawcy. Publikacja może zawierać marki i nazwy produktów będące znakami towarowymi lub zarejestrowanymi znakami towarowymi poszczególnych właścicieli.

SPECYFIKACJE I INFORMACJE DOTYCZĄCE PRODUKTÓW I USŁUG PRZEDSTAWIANYCH W INSTRUKCJI PODLEGAJĄ ZMIANOM. WSZELKIE INFORMACJE I ZALECENIA ZAMIESZCZONE W DOKUMENCIE SĄ WŁAŚCIWE JEDNAKŻE WSZELKA ODPOWIEDZIALNOŚĆ ZA IMPLEMENTACJĘ I UŻYTKOWANIE PRODUKTÓW I USŁUG LEŻY PO STRONIE UŻYTKOWNIKÓW.



## Spis treści

|                                           |    |
|-------------------------------------------|----|
| Jak działa protokół SAML?                 | 4  |
| Dodawanie nowej aplikacji w portalu Azure | 4  |
| Konfiguracja SAML Azure w FAMOC           | 8  |
| Znane problemy                            | 9  |
| Podsumowanie                              | 10 |

## 1 Jak działa protokół SAML?

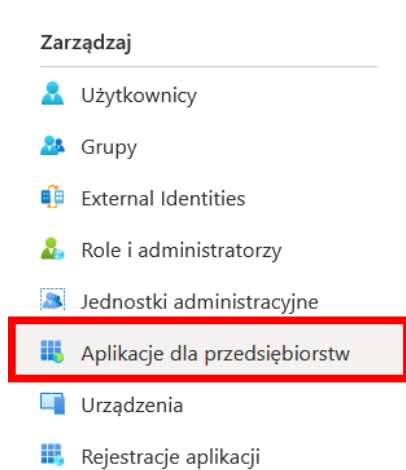
Protokół SAML umożliwia logowanie się do konsoli administracyjnej FAMOC manage za pośrednictwem usług zewnętrznych (Identity Provider).

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.

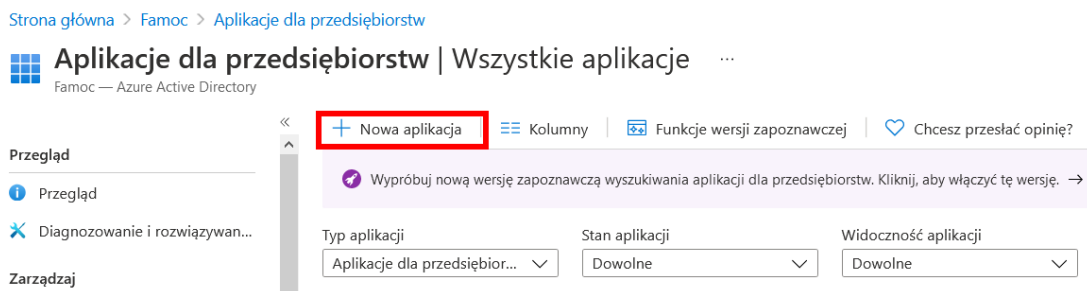
## 2 Dodawanie nowej aplikacji w portalu Azure

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

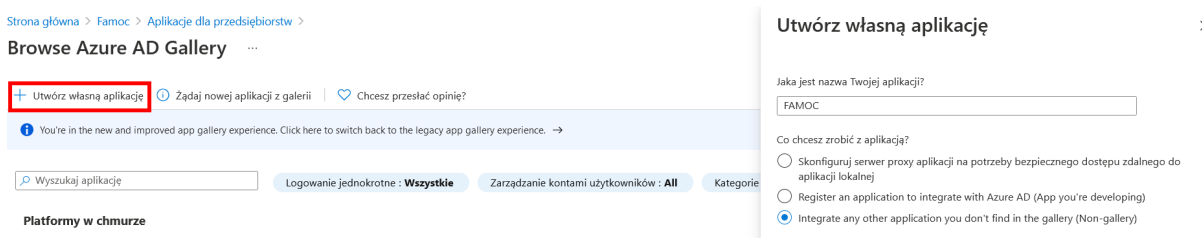
1. Zaloguj się do portalu Microsoft Azure za pośrednictwem adresu URL <https://portal.azure.com>.
2. Wybierz Azure Active Directory. Następnie wybierz opcję Aplikacje dla przedsiębiorstw z panelu po lewej stronie.



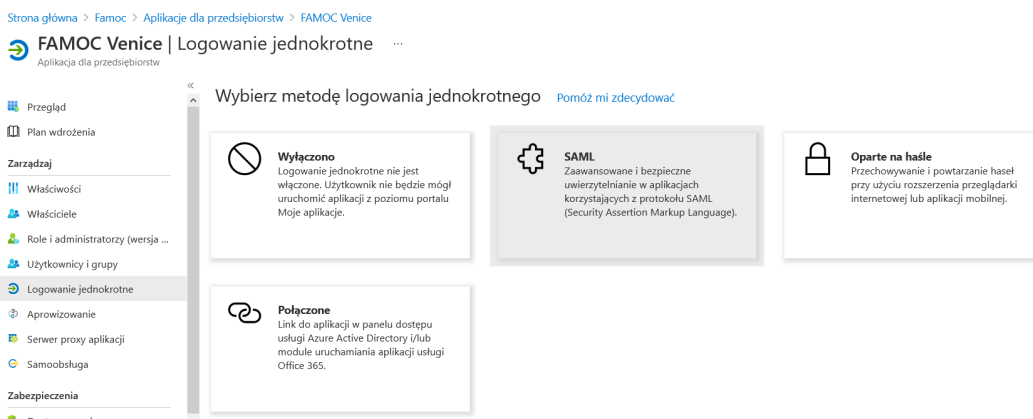
3. Aby dodać aplikację, kliknij Nowa aplikacja.



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).

## Podstawowa konfiguracja protokołu SAML

Zapisz

Identyfikator (identyfikator jednostki) \* ⓘ

Domyślny identyfikator będzie odbiorcami odpowiedzi SAML dla logowania jednokrotnego zainicjowanego przez dostawcę tożsamości

https://venice.fancyfon.com/ui/ ✓ ⓘ 🗑️

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

Domyślny adres URL odpowiedzi będzie obiektem docelowym w odpowiedzi SAML dla logowania jednokrotnego zainicjowanego przez dostawcę tożsamości

https://venice.fancyfon.com/ui/ ✓ ⓘ 🗑️

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”.

**Zarządzanie oświadczeniem** ... ✕

Zapisz ✕ Odrzuć zmiany

Nazwa: nameidentifier

Przestrzeń nazw: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Wybór formatu identyfikatora nazwy

Kwalifikowana nazwa domeny systemu Windows ▼

Źródło \*  Atrybut  Przekształcenie

Atrybut źródłowy \* user.userprincipalname ▼

Warunki oświadczenia

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

Certyfikat podpisywania SAML Edytuj

Stan: Aktywne

Odcisk palca: 865AD531EB41B808EA24C626B71EB35E36CC32  
41

Wygaśnięcie: 29.03.2024, 15:31:32

Wiadomość e-mail z powiadomieniem: mike.ross@therealfamoc.onmicrosoft.com

Adres URL metadanych federacyjnych aplikacji: <https://login.microsoftonline.com/d6e0ff...>

Certyfikat (base64) [Pobierz](#)

Certyfikat (nieprzetworzony) [Pobierz](#)

Kod XML metadanych federacji [Pobierz](#)

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.

**FAMOC Venice | Użytkownicy i grupy** ...

Aplikacja dla przedsiębiorstw

[+ Dodaj użytkownika/grupę](#) [Edytuj](#) [Usuń](#) [Aktualizuj poświadczenia](#) | [Kolumny](#) | ...

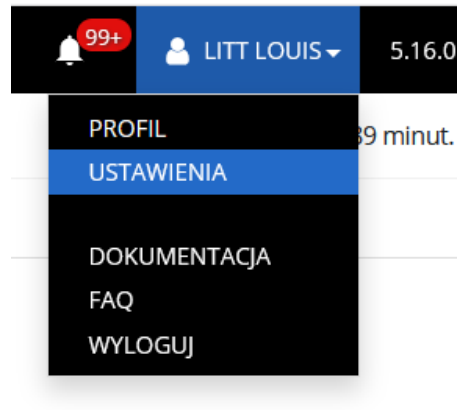
**i** Aplikacja będzie widoczna na Panelu dostępu dla przypisanych użytkowników. Aby temu zapobiec, ustaw we właściwościach opcję „widoczne dla użytkowników?” na wartość „nie”. →

Pokazano pierwszych 100 pozycji. Aby przeszukać wszystkich użytkowników i wszystkie grupy, wprowadź nazwę wyświetlaną.

| Nazwa wyświetlana           | Typ obiektu | Przypisana rola |
|-----------------------------|-------------|-----------------|
| <input type="checkbox"/> BL | Użytkownik  | User            |

### 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.

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:



## Ustawienia SAML

[Pokaż szczegóły](#)

Włącz autentykację przez SAML

---

Certyfikat X.509

```
-----BEGIN CERTIFICATE-----
MIIC8DCAdigAwIBAgIQGQv93VmPRIFMkZBvmB2cJANBgkqhkiG9w0BAQsFADA0MTwMAYDVQQD
EylNaWVyb3NvZnZnQgXp1cmUgRmVkbWVkdjhdGvkiFNTTYbDZlX0aWZpY2FOZTAeFw0yMTAzMjMxMz
MzjaFw0yNDAzMjMxNDMxMzjaMDQxMjAwMDQxMjAwMDQxMjAwMDQxMjAwMDQxMjAwMDQxMjAwMDQx
U1NPIENlcncRzmljYXRIMiBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAg2oRdl9fqlt
O3Y5Op9UNvzMMDSesnXAKKSLHbaaf09q3aF1QWd/3qydAT1Lul6fA+OIFFgq/18Dyhy66s13m6
DloeNzyVgioFaZRS5LhwNaVMIMSbtqPKX4kbNrEjgAa/VLxot+5rHxWjhOvv+fzUHN0ZUvQta
XimQbcPEEltIezidijokmuS2EWVkrE25gybz/nFHY4TcBAPWfTdG5a5UoJAONeBpVQgCk6-H
n7N7sm5HekrXAu7H+Z/CKAVHOB+VydLyeedQpZ3rcbnjm76bmjlyW245B7dEK1n8U6xW7qg
g4q7K8T08Y1oC5g3ngFg1yQjDAQABNIA0GCSg55h3DQEQbcwUA44B4BQbzrh80CRV8WMMArmuav
IevCLokCHHvZp9BEjIQ+DywyjC3h2nbvL4aYb55SjQo5h8Bf00QhjwDAFAH57NFRWUJp2k0
FDIWDHHzGluHqXE4dGTvHDozDC0ld3ycsWOL6ANF1GqmHwLjLrLduDoC7ngYHus8BvEET3xl
8l0eeLUEkhy0YD7mmP1XHURfivemM1Ej1gQmmWj648pMjN5mBqEuz3VvFM9E6vryCwyzrYILHN
qWhvKNi8Yrin02y0EdbU95jfgzrUAeCpUI4eh848rBN5093Y1oqJLTeZ7fv3Qcg1Wh5oFC1k8
fzpmSUVB9U1JmFkpq4o
-----END CERTIFICATE-----
```

---

Identyfikator https://venice.fancyfon.com/ui/

Login URL https://account.activedirectory.windowsazure.com

Znacznik XML użytkownika saml2:NameID

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

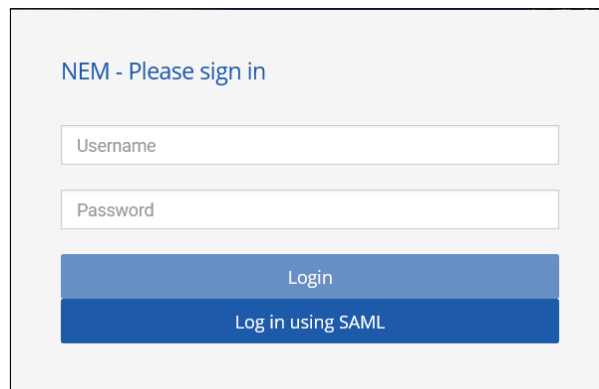
|                                       |                                             |                                  |
|---------------------------------------|---------------------------------------------|----------------------------------|
| Pole użytkownika: Imię                | <input type="text" value="user.givenname"/> | <input type="checkbox"/>         |
| Pole użytkownika: Nazwisko            | <input type="text" value="user.surname"/>   | <input type="checkbox"/>         |
| Pole użytkownika: Email               | <input type="text" value="user.mail"/>      | <input type="checkbox"/>         |
| Wybierz pole użytkownika              | <input type="button" value="Dodaj"/>        |                                  |
| Automatycznie twórz użytkowników      | <input checked="" type="checkbox"/>         |                                  |
| Domyślna rola dla nowych użytkowników | Administrator systemu FAMOC                 | <input type="button" value="↓"/> |

## 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.



NEM - Please sign in

Username

Password

Login

Log in using SAML