

OpenText NetIQ Advanced Authentication

Bezpieczny dostęp w całej organizacji.

Uwierzytelnianie wieloskładnikowe i logowanie bez hasła.



Korzyści

- **Ochrona** przed phishingiem
- **Spójne zasady** uwierzytelniania
- **Lepsza ochrona dostępu** w Microsoft Active Directory® i Entra® ID
- **Niezależność** od jednego dostawcy

W wielu organizacjach tożsamość użytkowników potwierdza się na różne sposoby: za pomocą identyfikatorów i haseł, kart dostępu do budynków, kodów PIN czy dodatkowych pytań weryfikacyjnych. Często każdy z tych mechanizmów działa niezależnie od pozostałych.

OpenText™ NetIQ Advanced Authentication pozwala zarządzać tymi metodami z jednego miejsca. Ułatwia wdrożenie uwierzytelniania wieloskładnikowego i logowania bez hasła, ułatwiając spełnienie wymagań regulacyjnych oraz stosowanie wewnętrznych zasad bezpieczeństwa. Organizacja może dobrać poziom ochrony i sposób logowania do swoich potrzeb, dbając przy tym o wygodę użytkowników.

Dostosuj sposób uwierzytelniania do poziomu ryzyka. Połącz rozproszone rozwiązania w jeden system, który pozwala integrować aplikacje i zarządzać zasadami logowania.

Ochrona przed phishingiem

Cyberprzestępcy wiedzą, że użytkownicy często używają tych samych haseł w różnych usługach, zarówno na kontach prywatnych, jak i służbowych. Szkolenia z bezpieczeństwa są potrzebne, ale warto wzmocnić ochronę uwierzytelnianiem wieloskładnikowym oraz metodami logowania bez hasła. Takie rozwiązania mogą wykorzystywać biometrię, np. odcisk palca lub rozpoznawanie twarzy, oraz unikalne tokeny uwierzytelniające. Szczegółnej ochrony wymagają konta administratorów systemów i danych. Ich rozległe uprawnienia sprawiają, że przejęcie danych logowania może dać atakującemu dostęp do znacznej części zasobów organizacji.

„Dzięki rozwiązaniom Access and Identity Manager oraz Advanced Authentication szybko zabezpieczyliśmy dostęp przez VPN do aplikacji lokalnych i chmurowych dla wszystkich osób, które go potrzebowały”.

José Luis Rodríguez
Dyrektor operacyjny
i współzałożyciel ITechGrup

Spójne zasady uwierzytelniania

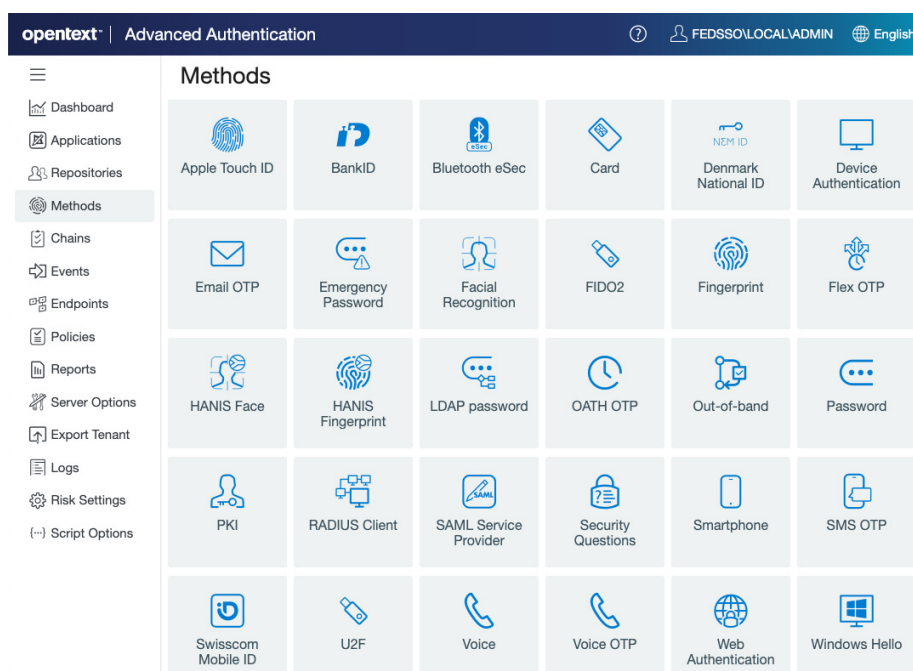
Kolejne wdrożenia często prowadzą do powstania wielu niezależnych mechanizmów uwierzytelniania. Taka fragmentacja utrudnia zarządzanie bezpieczeństwem i zwiększa ryzyko nieuprawnionego dostępu. Advanced Authentication łączy te mechanizmy w jednym systemie i pozwala zarządzać zasadami uwierzytelniania z jednej konsoli. Pomaga w ten sposób zwiększyć bezpieczeństwo i obniżyć koszty administracji. Szerokie możliwości integracji oraz obsługa nowoczesnych metod i urządzeń ułatwiają ujednolicenie rozwiązań działających w organizacji.

Lepsza ochrona dostępu w środowiskach Microsoft Active Directory® i Entra® ID

Coraz więcej organizacji korzysta z rozwiązań Microsoft dla przedsiębiorstw oraz usług opartych na Active Directory i Entra ID. Wraz z rozwojem tych środowisk trzeba zadbać o to, by sposób uwierzytelniania odpowiadał poziomowi ryzyka. Advanced Authentication integruje różne źródła danych o użytkownikach i ujednolica ochronę dostępu, zachowując wygodę logowania. Szeroki wybór metod pozwala dopasować je do potrzeb poszczególnych użytkowników. Niezależnie od tego, czy aplikacje działają lokalnie, czy w chmurze, rozwiązanie może wzmocnić ochronę systemów korzystających z ADFS przed nieuprawnionym dostępem.

Niezależność od jednego dostawcy

Otwarte standardy ułatwiają współpracę aplikacji i platform oraz pomagają zachować spójność architektury IT w dłuższej perspektywie. Rozwiązania oparte na zamkniętych protokołach mogą natomiast ograniczać wybór urządzeń do oferty jednego dostawcy. Utrudnia to dopasowanie sprzętu do potrzeb i budżetu organizacji. OpenText wspiera FIDO Alliance (Fast Identity Online) i opracowane przez tę organizację standardy. FIDO U2F (Universal 2nd Factor) pozwala użytkownikom zarządzać własnymi urządzeniami uwierzytelniającymi. Z kolei FIDO2 łączy specyfikację Web Authentication (WebAuthn) organizacji W3C z protokołem FIDO Client to Authenticator Protocol (CTAP). Dzięki kryptografii klucza publicznego umożliwia logowanie do witryn i aplikacji bez użycia hasła.



Platforma OpenText udostępnia liczne integracje i interfejsy uwierzytelniania.

Materiały

Strona rozwiązania NetIQ Advanced Authentication

[Poznaj rozwiązanie >](#)

Logowanie do Windows z FIDO2 i NetIQ Advanced Authentication

[Obejrzyj film >](#)

Więcej materiałów filmowych o MFA

[Zobacz materiały wideo >](#)

Z OpenText nie musisz zarządzać każdym urządzeniem uwierzytelniającym za pomocą osobnego oprogramowania producenta. Jedna platforma łączy aplikacje i metody uwierzytelniania, zastępując odrębne, niezależnie zarządzane rozwiązania. Ułatwia to stosowanie spójnych zasad bezpieczeństwa i zmniejsza nakład pracy administratorów.

Na tle konkurencyjnych rozwiązań OpenText wyróżnia się aplikacjami do silnego uwierzytelniania dla systemów Windows®, Mac OS® i Linux® oraz urządzeń mobilnych. Aplikacja mobilna obsługuje geofencing. Administratorzy mogą więc dobrać wymagany poziom zabezpieczeń na podstawie lokalizacji GPS użytkownika i innych czynników wpływających na ocenę ryzyka.

Funkcje produktu	Opis
Integracja oparta na standardach	Integracja aplikacji i metod uwierzytelniania w jednym systemie z obsługą HSPD11, PKI12, OAuth, FIDO, OATH, RADIUS, FIPS 140, NFC ISO/IEC i innych standardów, a także wybranych rozwiązań zamkniętych.
Geofencing	Geofencing wykorzystuje dane GPS, aby określić lokalizację dokładniej niż na podstawie adresu IP. Pozwala uzależnić zasady uwierzytelniania od tego, gdzie znajduje się użytkownik, np. czy przebywa w danym budynku lub na terenie kampusu.
Logowanie mobilne w trybie offline	Użytkownicy mogą potwierdzić tożsamość za pomocą drugiego składnika także bez połączenia z siecią. To przydatne m.in. podczas podróży.
Szyfrowanie FIPS 140-2	Szyfrowanie zgodne ze standardem FIPS 140-2 (Federal Information Processing Standard), opracowanym przez amerykański instytut NIST.
Uwierzytelnianie zależne od ryzyka	Wbudowany mechanizm ocenia ryzyko i na tej podstawie dobiera odpowiednią metodę uwierzytelniania.
Moduł helpdesk	Narzędzia do obsługi użytkowników: rejestracja i ponowna rejestracja, przypisywanie tokenów, wydawanie haseł awaryjnych i inne funkcje.
Pakiety SDK dla iOS i Androida	Interfejsy API i narzędzia do wdrażania uwierzytelniania w natywnych aplikacjach na iOS i Androida.