



FUDO SECURITY

Nowoczesne zarządzanie dostępem uprzywilejowanym

Przewodnik po Fudo Enterprise 6.1



Spis Treści

01 Wstęp: Nowe wyzwania, prostsze rozwiązania

02 Tożsamość pod kontrolą

2.1 Sprawniejsza praca z wieloma domenami (Kerberos)

2.2 Usprawniona synchronizacja z dostawcami tożsamości (Entra ID i Okta)

03 Aktywna ochrona przed zagrożeniami

3.1 Wykrywanie skompromitowanych poświadczeń

3.2 Zarządzanie uprawnieniami w środowisku Linux (Sudo)

3.3 Nowoczesne metody uwierzytelniania i obsługa haseł

04 Codzienna wygoda (Dla użytkowników i IT)

4.1 Kontrolowany transfer plików w sesjach RDP

4.2 Ułatwienia dla zespołów administracyjnych

05 ShareAccess: Dostęp do zasobów w modelu chmurowym

06 Podsumowanie



Wstęp: Nowe wyzwania, prostsze rozwiązania

Współczesne środowisko biznesowe wymaga od organizacji ciągłego dostosowywania architektury IT do elastycznych modeli pracy. Rozwój modelu hybrydowego, migracja zasobów do chmury i współpraca z zewnętrznymi dostawcami zacierają tradycyjne granice sieci firmowej. Poleganie wyłącznie na klasycznych rozwiązaniach, takich jak szyfrowane tunele VPN czy podstawowe zapory sieciowe, może prowadzić do trudności organizacyjnych i luk w nadzorze.

Zapewnienie bezpieczeństwa w cyberprzestrzeni to proces ciągły, wymagający analizy potrzeb organizacji, oceny jej dojrzałości technologicznej i dopasowania narzędzi do specyfiki procesów biznesowych. Zbyt rygorystyczne ograniczenia, nieuwzględniające realiów operacyjnych, często skłaniają użytkowników do szukania obejść, co obniża odporność firmy na zagrożenia.

Fudo Enterprise 6.1 został zaprojektowany, aby wspierać organizację w procesie adaptacji. Nowa wersja systemu pomaga zachować równowagę między wymogami kontroli dostępu uprzywilejowanego (PAM) a wygodą pracy zespołów IT i partnerów zewnętrznych. Dzięki elastycznym mechanizmom zarządzania tożsamością, nowoczesnym metodom uwierzytelniania i usprawnieniom nadzoru sesji, Fudo 6.1 wspiera redukcję ryzyka w cyfrowym ekosystemie przedsiębiorstwa.



Tożsamość pod kontrolą

Zarządzanie tożsamością i uprawnieniami w rozproszonych strukturach wymaga spójności i minimalizacji ręcznych, podatnych na błędy operacji. Elastyczne mechanizmy integracji umożliwiają sprawne odwzorowanie struktur organizacyjnych w systemie dostępu.

2.1

Sprawniejsza praca z wieloma domenami (Kerberos)

Architektura bezpieczeństwa w dużych firmach często musi uwzględniać obsługę wielu niezależnych domen Active Directory, z których każda korzysta z własnej infrastruktury DNS. Fudo Enterprise 6.1 rozszerza wsparcie dla protokołu Kerberos, ułatwiając dopasowanie systemu do wymagań skomplikowanych sieci.

Granularna kontrola dostępu

Administratorzy mogą precyzyjnie określić, gdzie stosować uwierzytelnianie Kerberos. Konfiguracja pozwala niezależnie włączać lub wyłączać ten protokół dla logowania zewnętrznego, synchronizacji LDAP i połączeń RDP, co zwiększa elastyczność wdrożenia w różnych środowiskach sieciowych.

Ograniczenie automatycznego powrotu do starszych protokołów

Aby zwiększyć poziom bezpieczeństwa, system umożliwia wyłączenie automatycznego przełączania na mniej bezpieczne metody uwierzytelniania, takie jak NTLM czy prosty bind w LDAP. Zapobiega to przypadkowemu pominięciu polityki ochrony przez nieprzewidziane reakcje infrastruktury.

Obsługa środowisk wielodomenowych

Dedykowany, lokalny mechanizm obsługi DNS pozwala przypisać oddzielne serwery nazw dla poszczególnych domen. Ułatwia to stabilną pracę w złożonych strukturach bez konieczności wprowadzania istotnych zmian w konfiguracji sieciowej klienta.

Automatyczny przegląd sieci (Discovery)

Skanery sieciowe Fudo umożliwiają ciągłe mapowanie zasobów wykorzystujących WinRM i LDAP. Regularne skanowanie pomaga identyfikować nowe urządzenia i konta, wspierając aktualność informacji o infrastrukturze.

Przeniesienie zarządzania tożsamością do zewnętrznych dostawców chmurowych wymaga sprawnej wymiany informacji o zmianach uprawnień pracowników.

SCIM 2.0 Standard

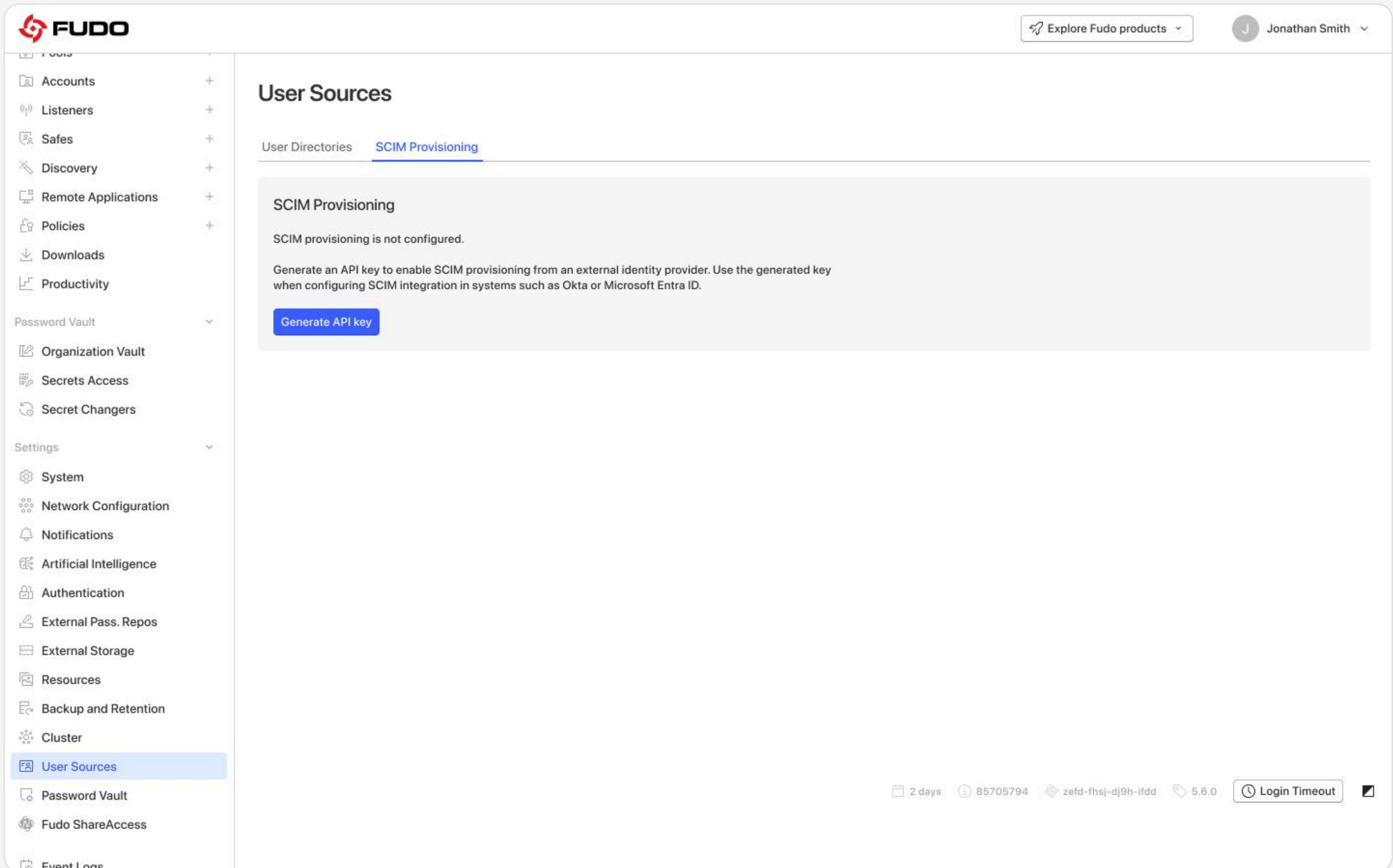
Obsługa protokołu SCIM umożliwia odbieranie informacji o zmianach tożsamości bezpośrednio od dostawców, takich jak Microsoft Entra ID czy Okta. System szybko reaguje na zdarzenia przesyłane przez dostawcę, eliminując potrzebę cyklicznego odpytywania bazy danych.

2.2

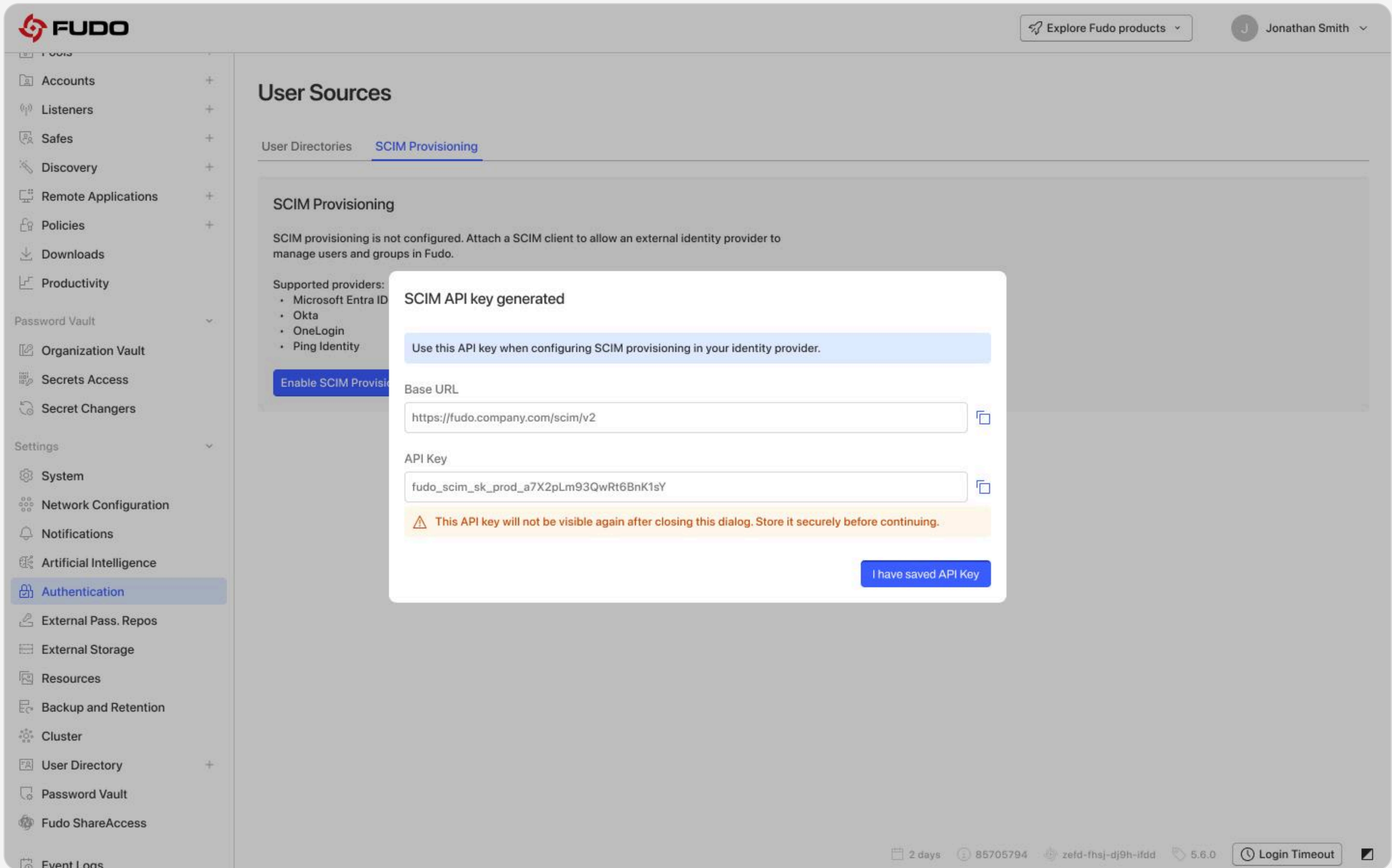
Usprawniona synchronizacja z dostawcami tożsamości (Entra ID i Okta)



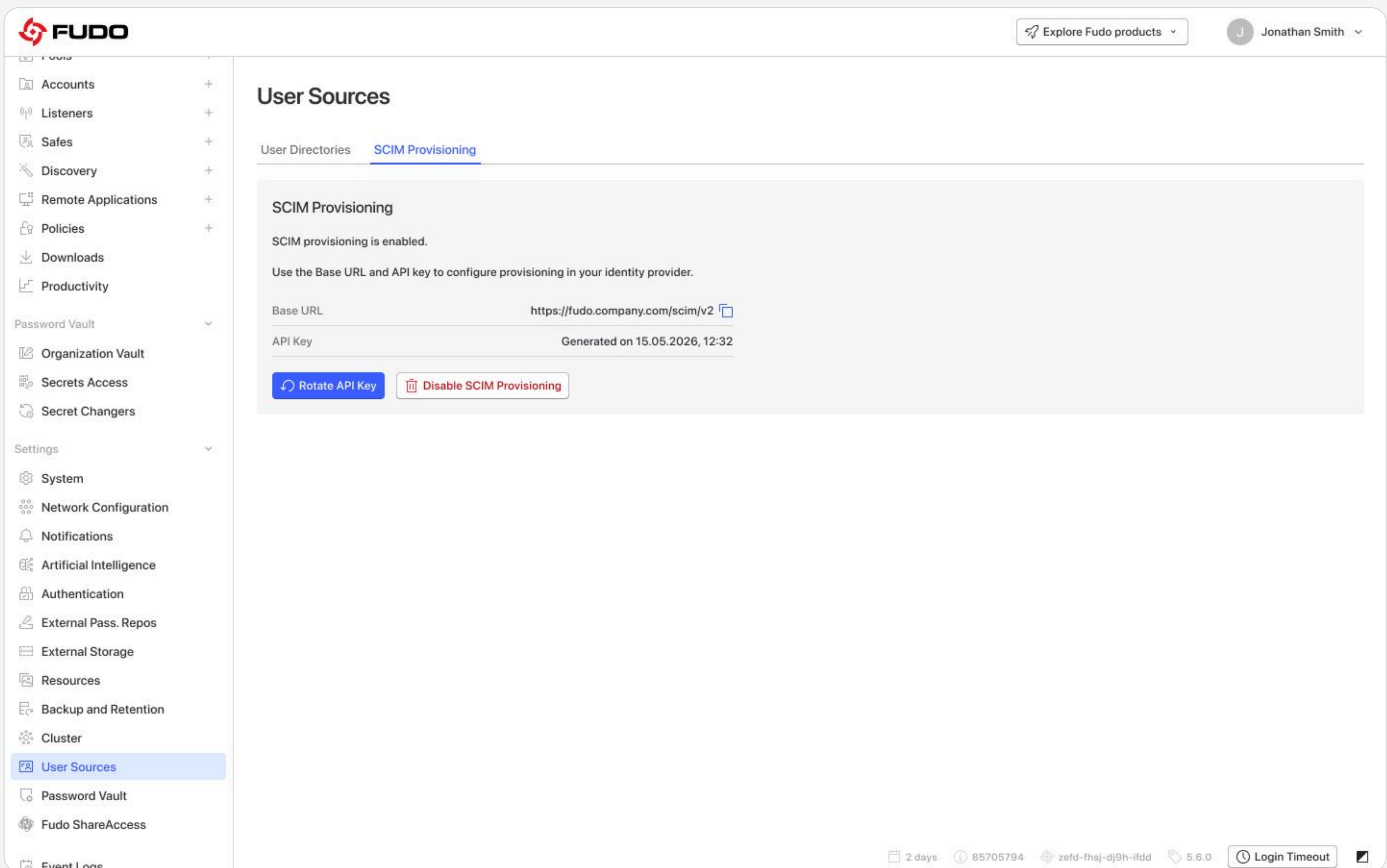
NOWOCZESNE ZARZĄDZANIE DOSTĘPEM UPRZYWILEJOWANYM



Nowa zakładka SCIM Provisioning w konsoli zarządzania Fudo. Wygenerowanie klucza API umożliwia integrację z zewnętrznym dostawcą tożsamości, takim jak Microsoft Entra ID czy Okta, i automatyzację apro wizacji użytkowników.

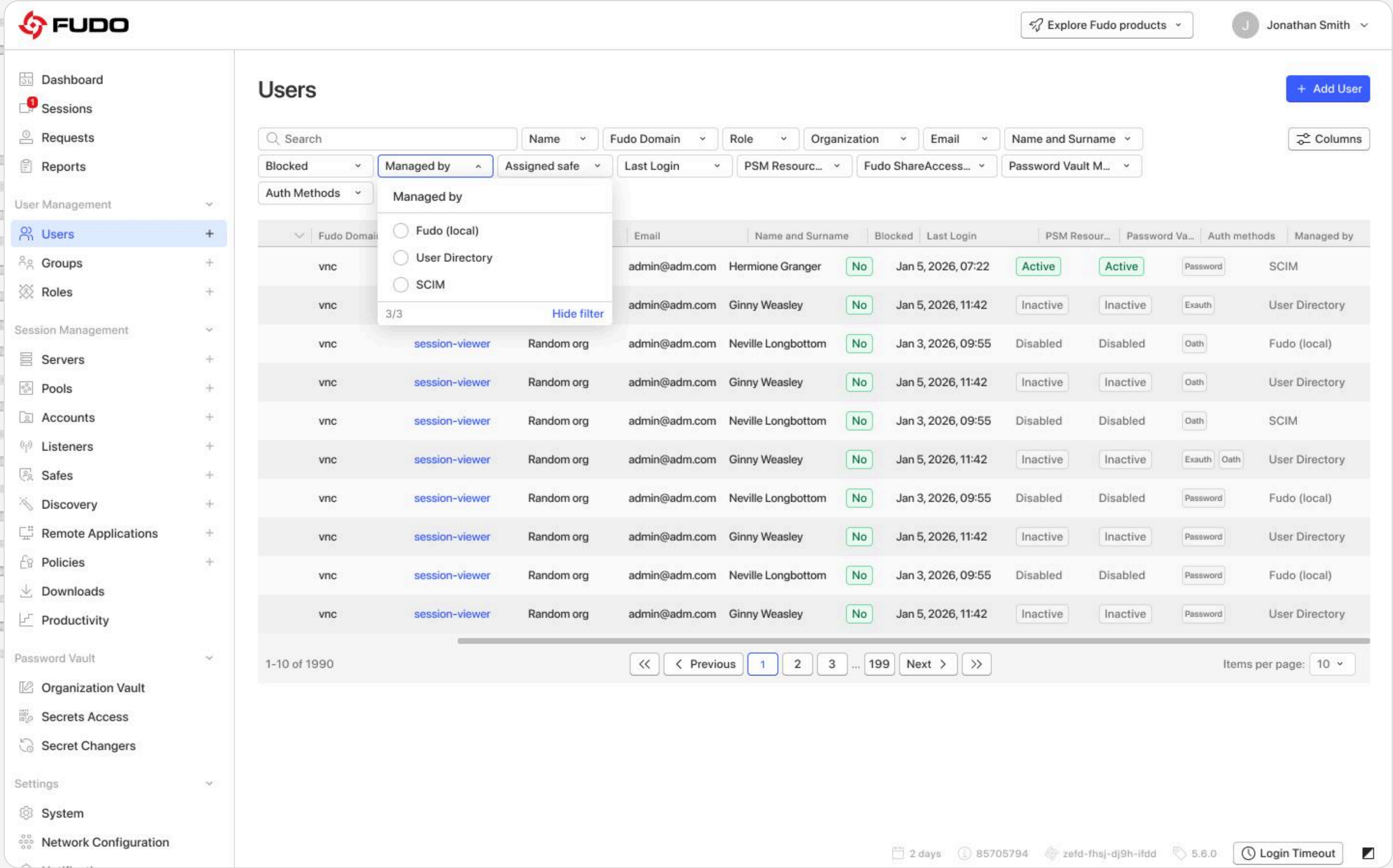


Widok wygenerowanego klucza API SCIM oraz adresu Base URL w panelu Fudo. Wprowadzenie tych parametrów w zewnętrznym dostawcy tożsamości (np. Entra ID czy Okta) umożliw ia bezpieczne zestawienie automatycznej synchronizacji kont.

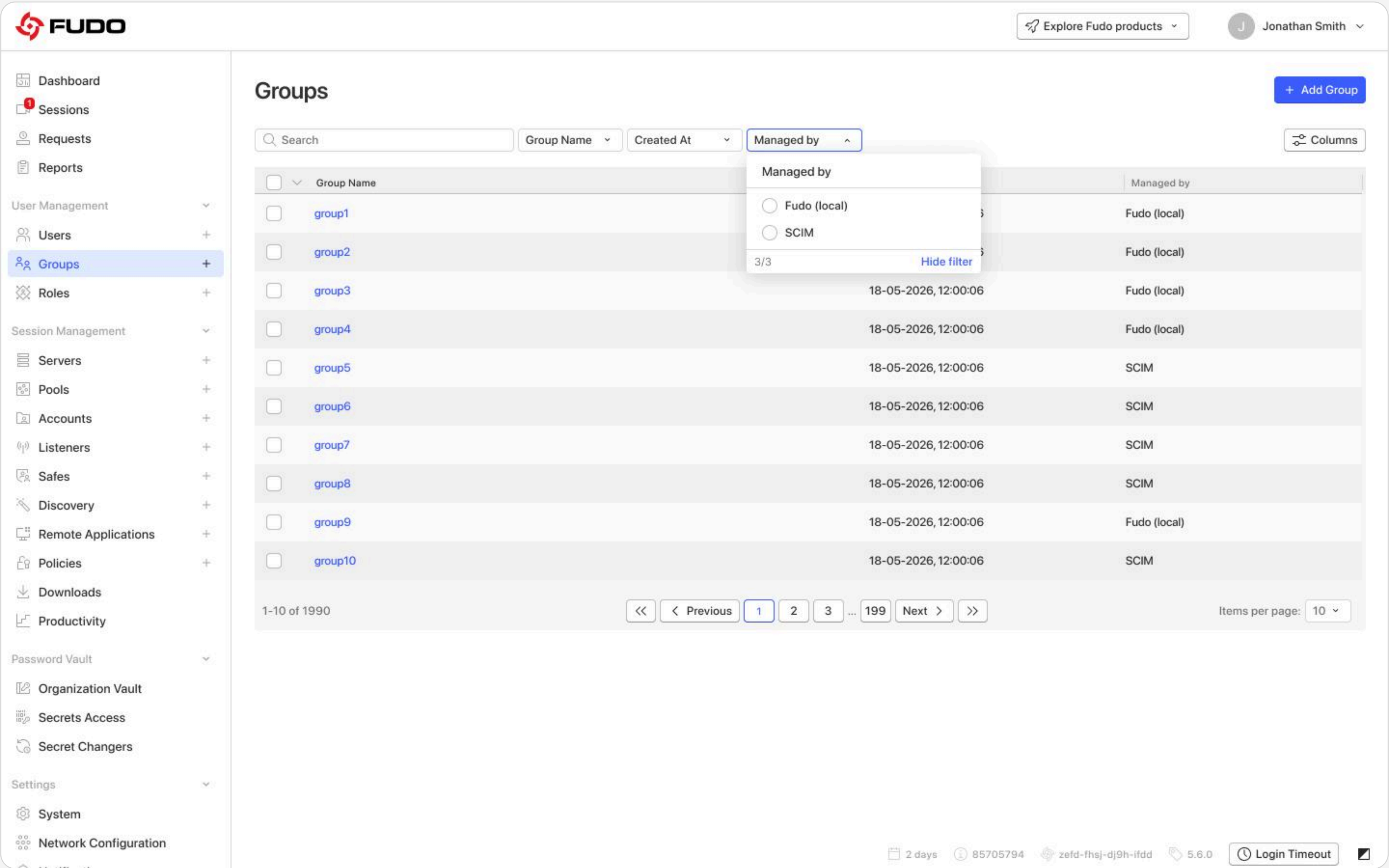


Ekran aktywnej usługi SCIM Provisioning w Fudo Enterprise 6.1, pozwalający na podgląd adresu punktu końcowego oraz sprawne zarządzanie kluczem uwierzytelniającym.

NOWOCZESNE ZARZĄDZANIE DOSTĘPEM UPRZYWILEJOWANYM



Lista użytkowników w Fudo Enterprise 6.1 z widocznym filtrowaniem według źródła tożsamości (Managed by).



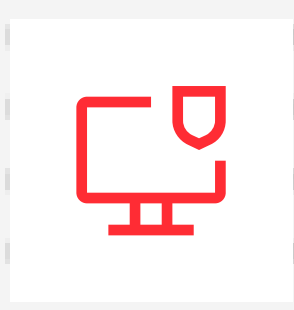
Widok zarządzania grupami użytkowników w Fudo 6.1 z opcją filtrowania według źródła pochodzenia (Managed by).

Wsparcie dla cyklu życia tożsamości

Zmiany statusu zatrudnienia, awanse czy przeniesienia między działami odnotowane w systemie głównym są natychmiast odzwierciedlane w systemie Fudo. W przypadku odejścia pracownika, reguły integracji umożliwiają szybkie wyłączenie konta i odebranie dostępu.

Ochrona spójności danych

Obiekty zsynchronizowane przez SCIM są chronione przed przypadkową lokalną modyfikacją w interfejsie Fudo. Centralne zarządzanie poświadczeniami ułatwia utrzymanie porządku w uprawnieniach w całej firmie.



Aktywna ochrona przed zagrożeniami

Nadzór nad dostępem uprzywilejowanym jest skuteczniejszy, gdy pasywna rejestracja jest wspierana przez rozwiązania umożliwiające wczesne wykrywanie nieprawidłowości.

3.1 Wykrywanie skompromitowanych poświadczeń

Wykorzystywanie przejętych lub słabych haseł to częsty wektor incydentów. Fudo Enterprise 6.1 oferuje funkcję wspierającą audyt poświadczeń przechowywanych w sejfie haseł (Password Vault).

Przetwarzanie bazy wycieków w środowisku lokalnym

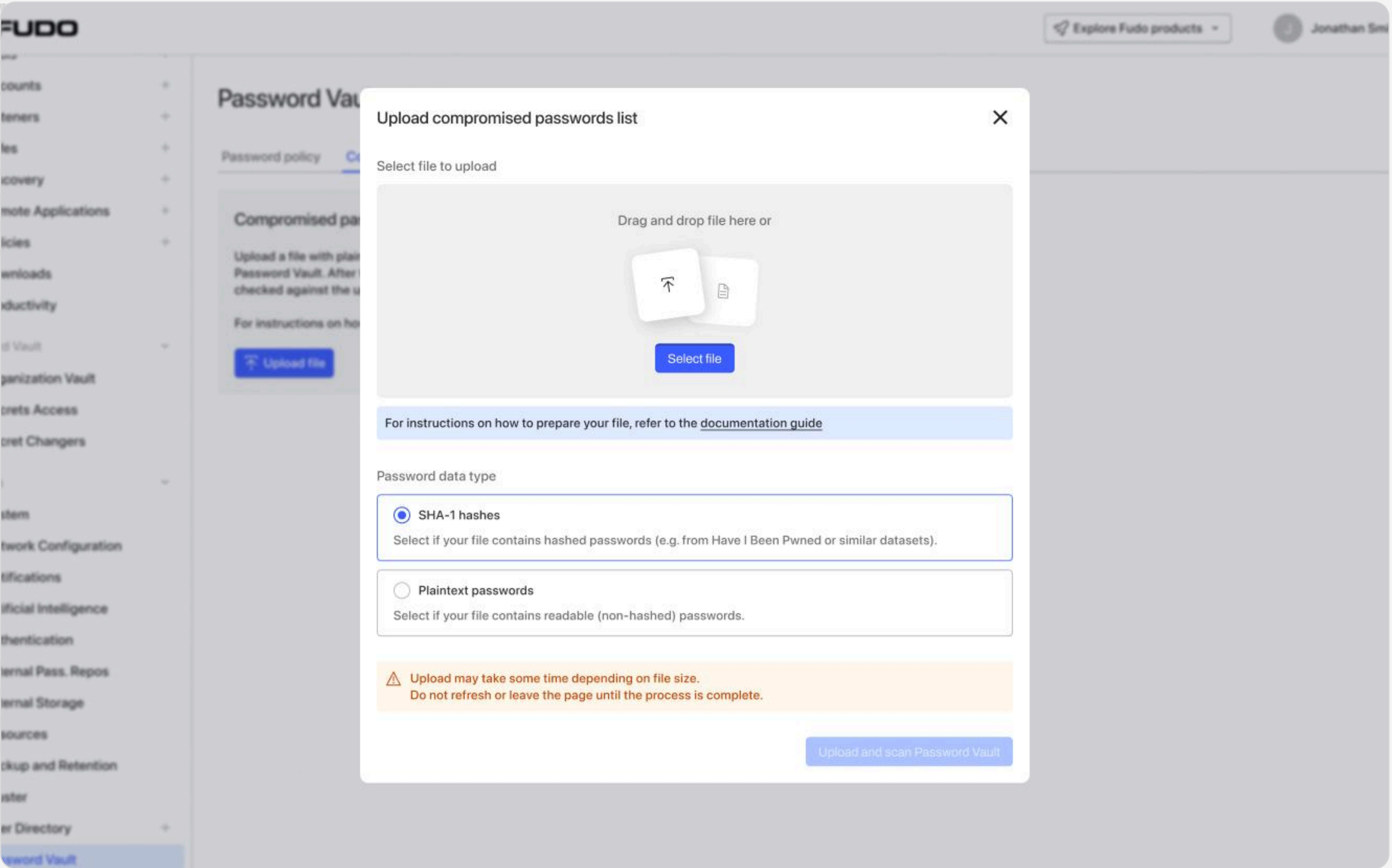
Administratorzy mają możliwość zasilenia systemu własnymi listami znanych wycieków poświadczeń. Odbywa się to bez ryzyka transmisji danych na zewnątrz – cała analiza porównawcza wykonywana jest lokalnie na urządzeniu, dzięki czemu prywatne dane oraz struktury są wykonywane w bezpiecznej strefie klienta.

Weryfikacja haseł w procesach operacyjnych

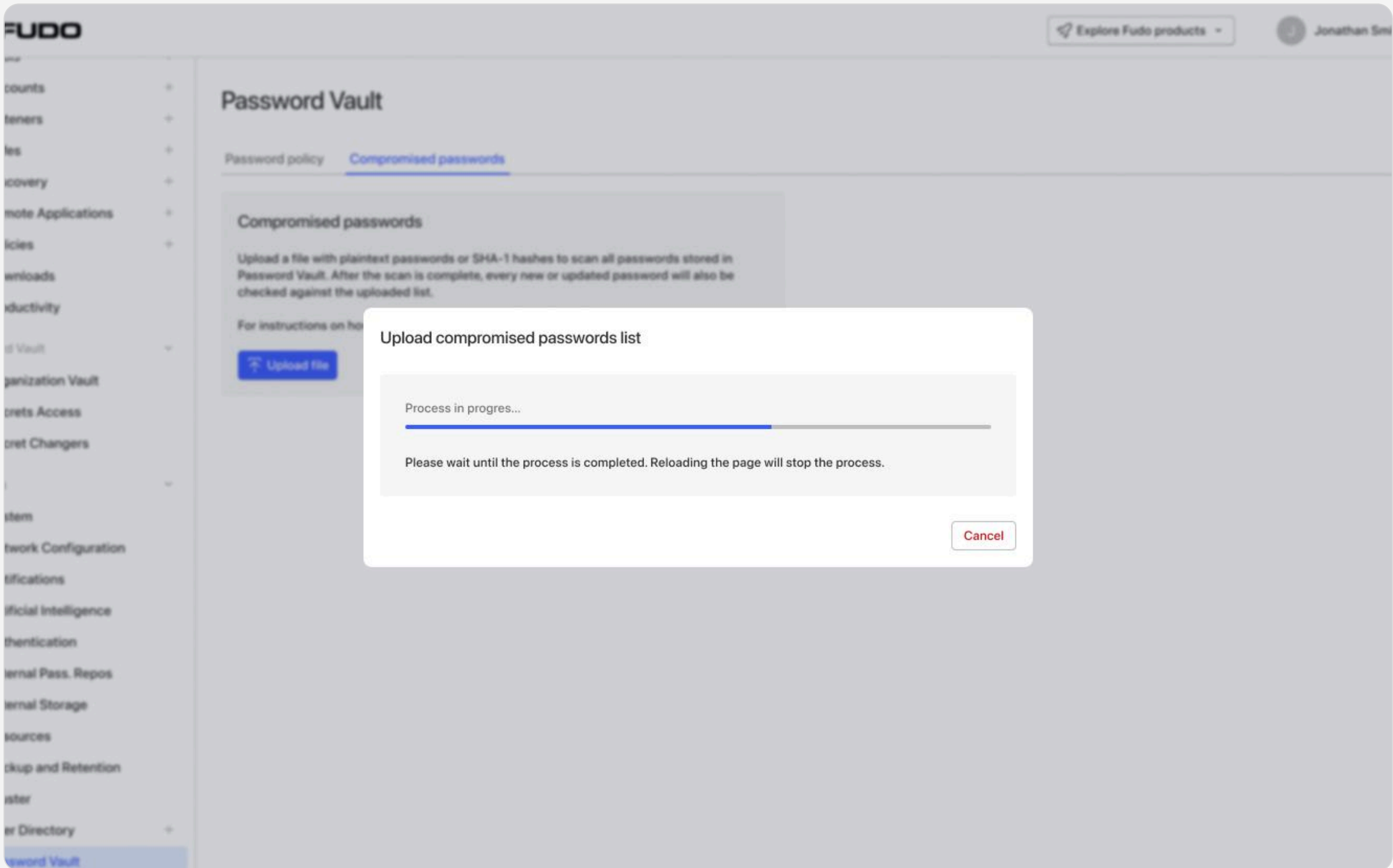
System weryfikuje poświadczenia podczas importu bazy wycieków oraz podczas tworzenia lub edycji rekordów. W przypadku wykrycia słabego lub ujawnionego hasła Fudo wyświetla ostrzeżenie wizualne, ułatwiając decyzję o zmianie hasła.

Zgodność z zaleceniami branżowymi

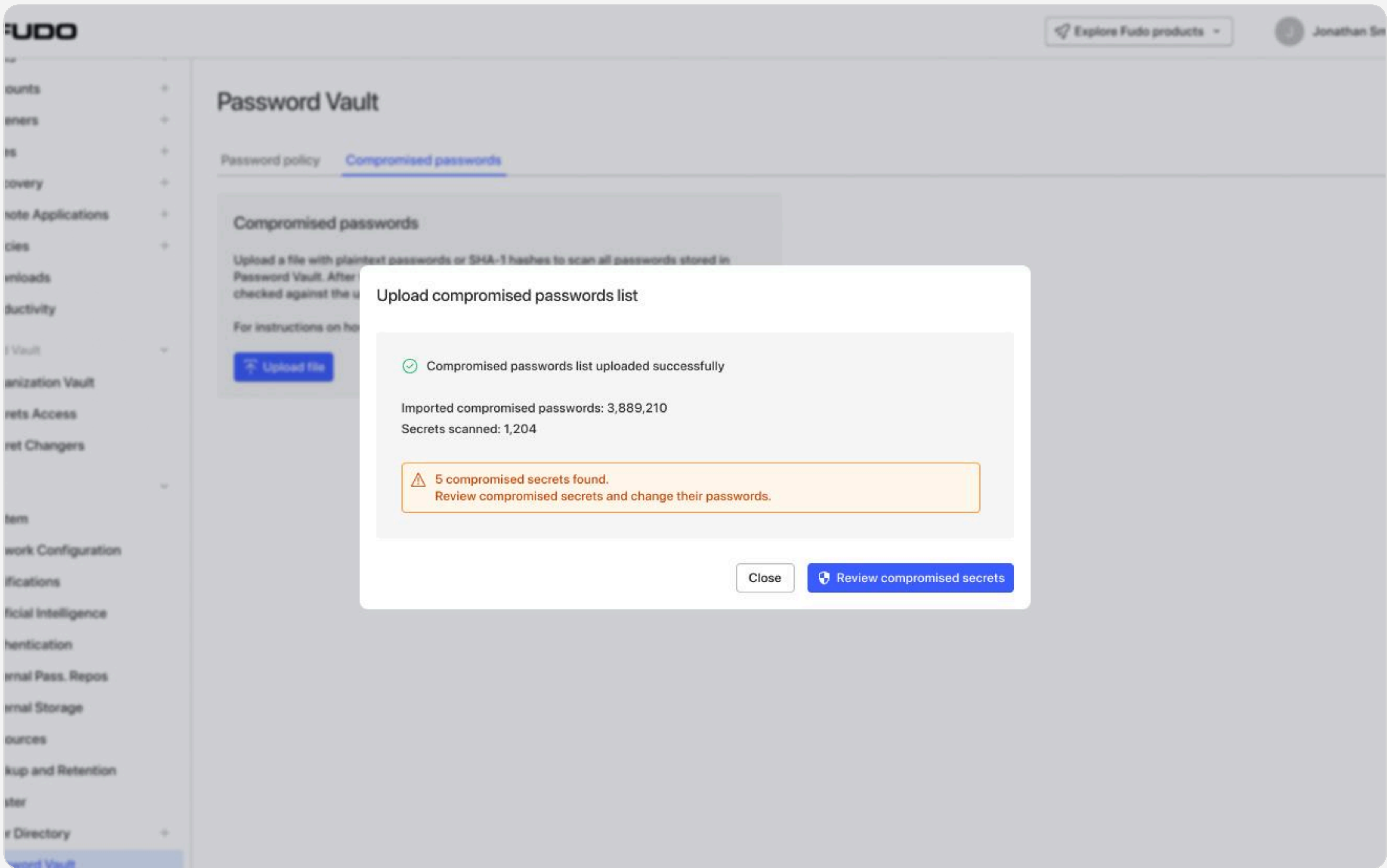
Funkcjonalność ta wpisuje się w realizację dobrych praktyk i wytycznych z zakresu zarządzania tożsamością, takich jak NIST SP 800-63B, które rekomendują weryfikację proponowanych poświadczeń w rejestrach znanych kompromitacji.



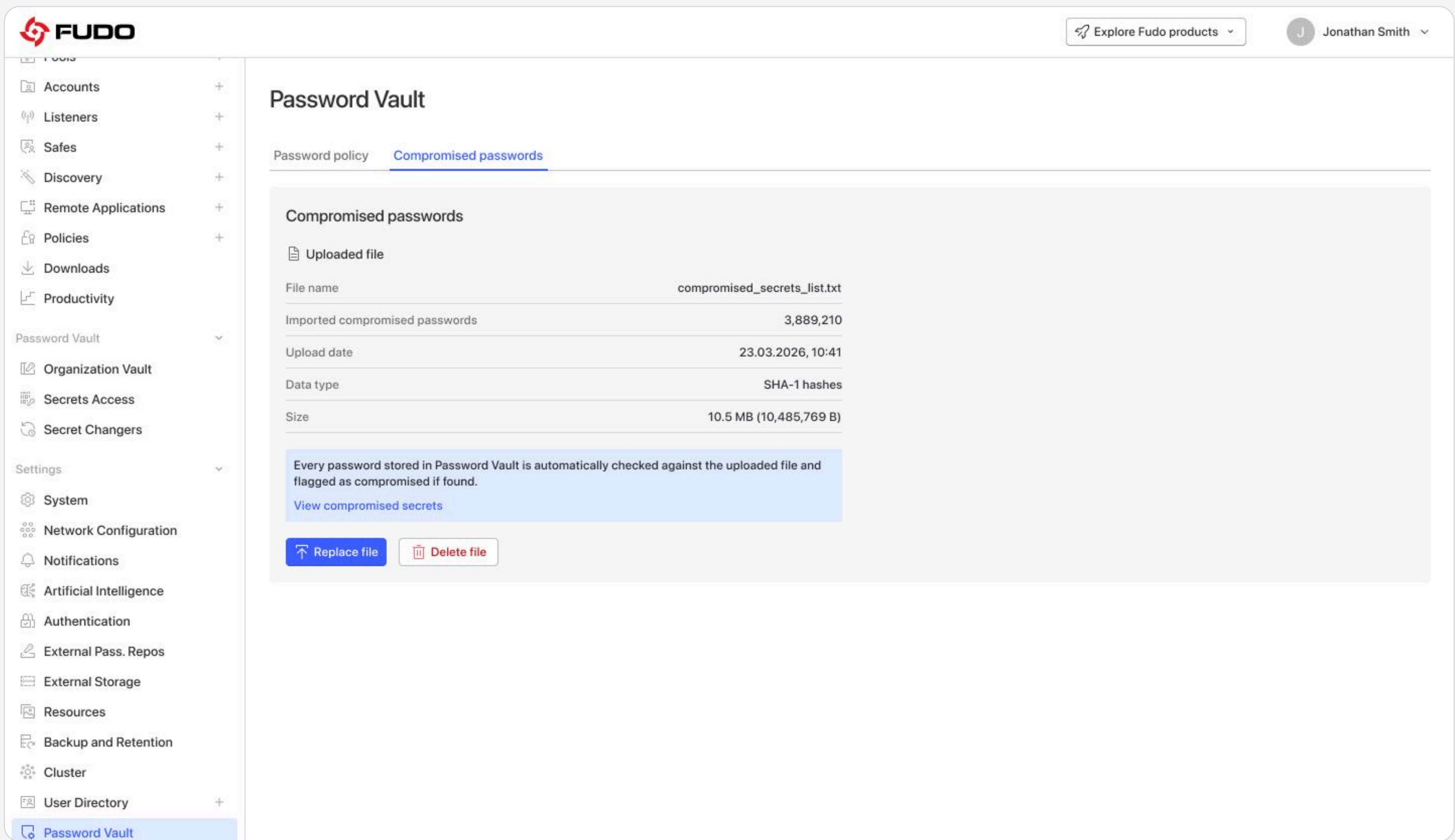
Ekran przesyłania listy ujawnionych poświadczeń w postaci skrótów SHA-1 lub tekstu jawnego. Uruchamia weryfikację sekretów przechowywanych w Password Vault z rejestrami znanych wycieków.



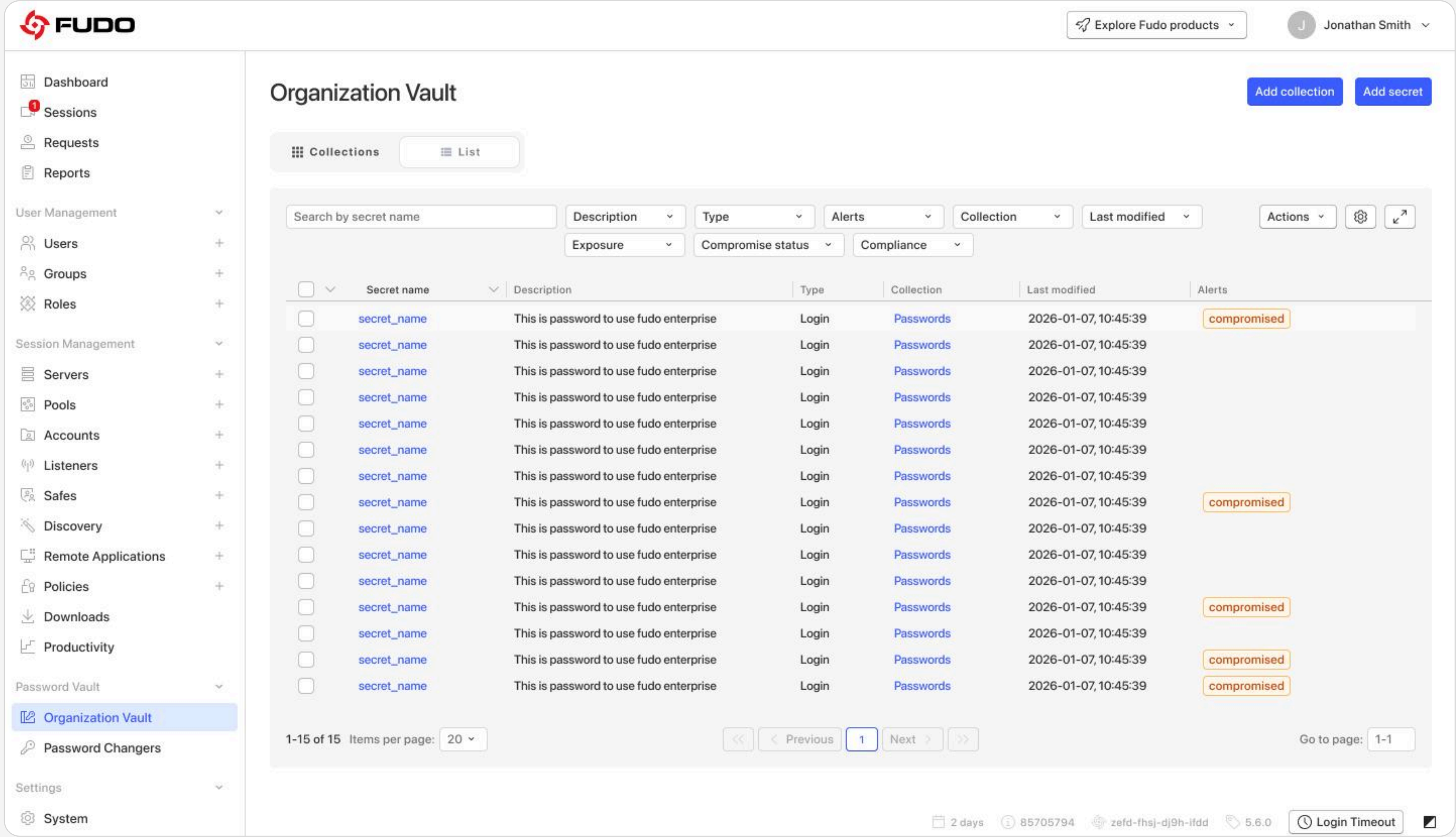
Ekran prezentujący postęp przesyłania listy wycieków oraz automatycznego skanowania sejfów haseł w Fudo Enterprise 6.1.



Podsumowanie skanowania sejfów haseł z widoczną informacją o identyfikacji ujawnionych poświadczeń oraz opcją ich szybkiej remediacji.



Ekran ze szczegółami wgranego pliku wycieków w Fudo Enterprise 6.1, prezentujący stan stałej, automatycznej weryfikacji haseł w sejfie.



Ekran listy sejfu organizacji (Organization Vault) w Fudo Enterprise 6.1 z widocznym oznaczeniem skompromitowanych poświadczeń.

3.2 Zarządzanie uprawnieniami w środowisku Linux (Sudo)

Kontrola uprawnień administracyjnych i na serwerach Linux jest wyzwaniem ze względu na rozproszenie plików konfiguracyjnych.

Model oparty na jawnej zgodzie (Whitelisting)

Dedykowana wtyczka do polecenia sudo umożliwia zmianę podejścia do przyznawania uprawnień. Zamiast blokować wybrane komendy, polityka bezpieczeństwa domyślnie ogranicza wykonywanie instrukcji i zezwala tylko na te, które zostały zaakceptowane przez administratorów.

Centralna autoryzacja żądań

Wtyczka komunikuje się z systemem Fudo przez API. Weryfikacja uprawnień odbywa się poza lokalnym systemem operacyjnym, co ogranicza możliwość obejścia reguł przez użytkownika końcowego.

Monitorowanie i rejestracja zdarzeń

Każde użycie komendy podnoszącej uprawnienia może być rejestrowane i powiązane z powiadomieniami e-mail lub wiadomościami w aplikacji mobilnej, co daje zespołom bezpieczeństwa lepszy wgląd w operacje na kluczowych serwerach.

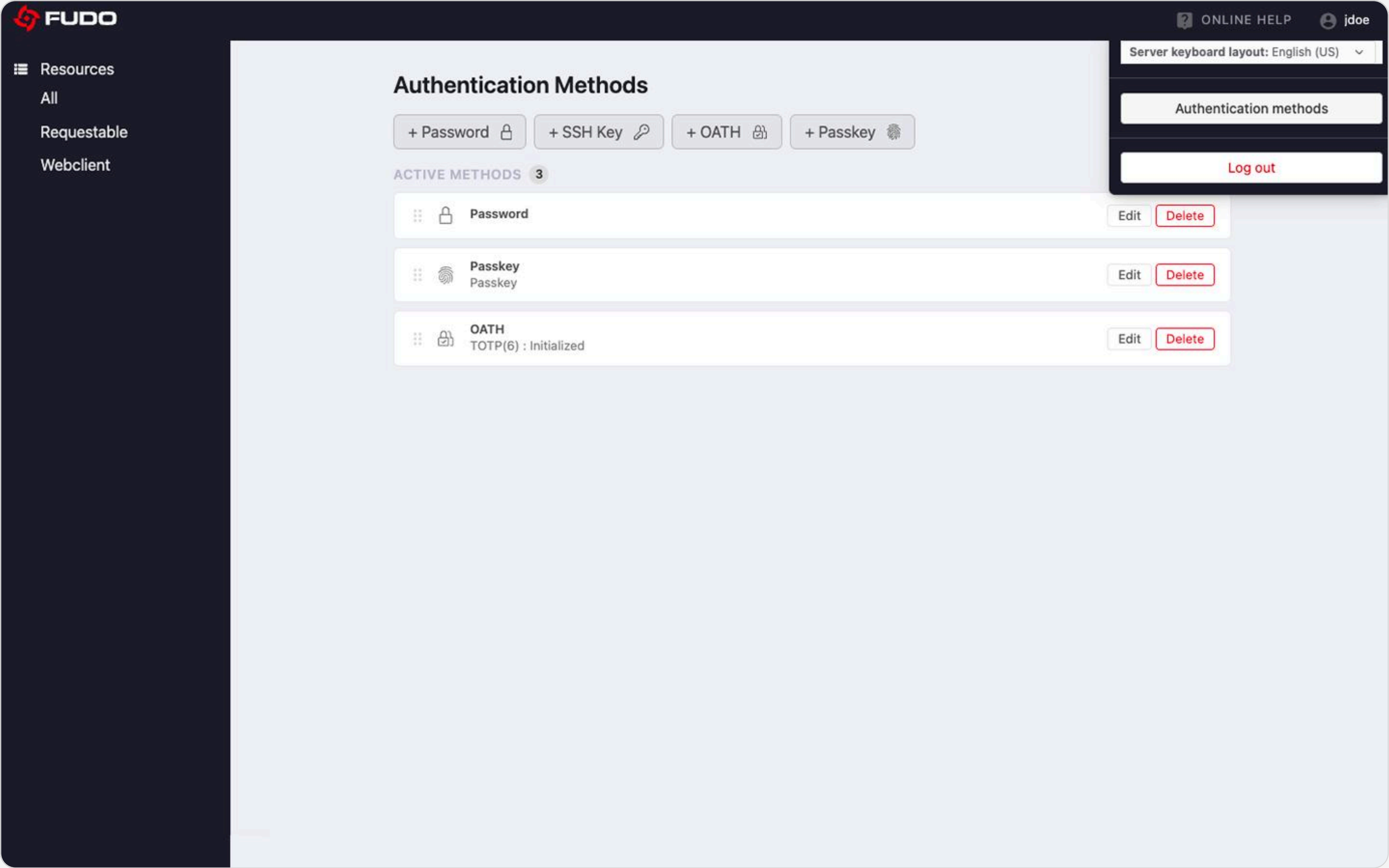
3.3

Nowoczesne metody uwierzytelniania i obsługa haseł

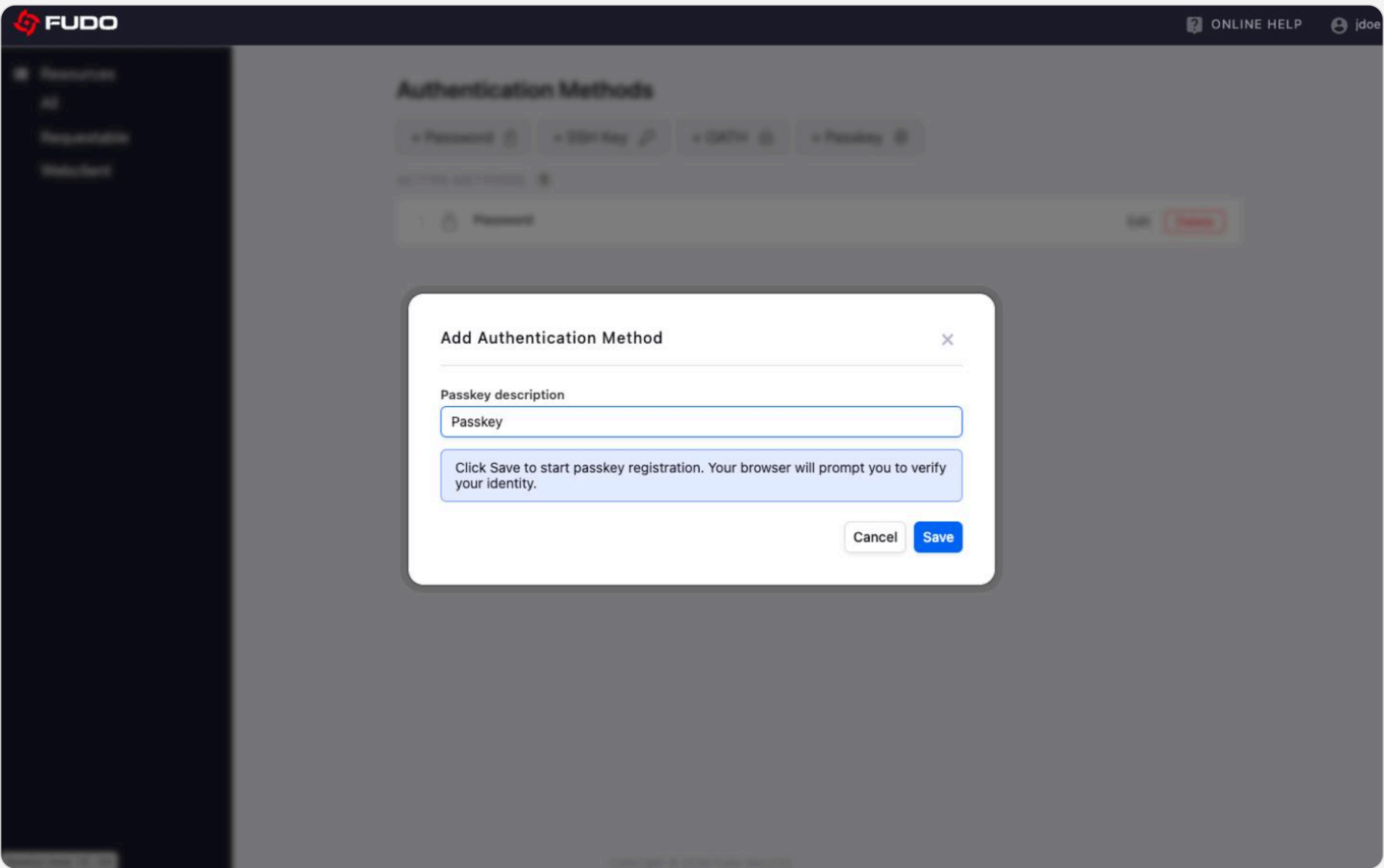
Wdrożenie metod uwierzytelniania odpornych na wyłudzenia poświadczeń jest kluczowe dla budowania odporności organizacji.

Standard FIDO2 i bezhasłowy dostęp

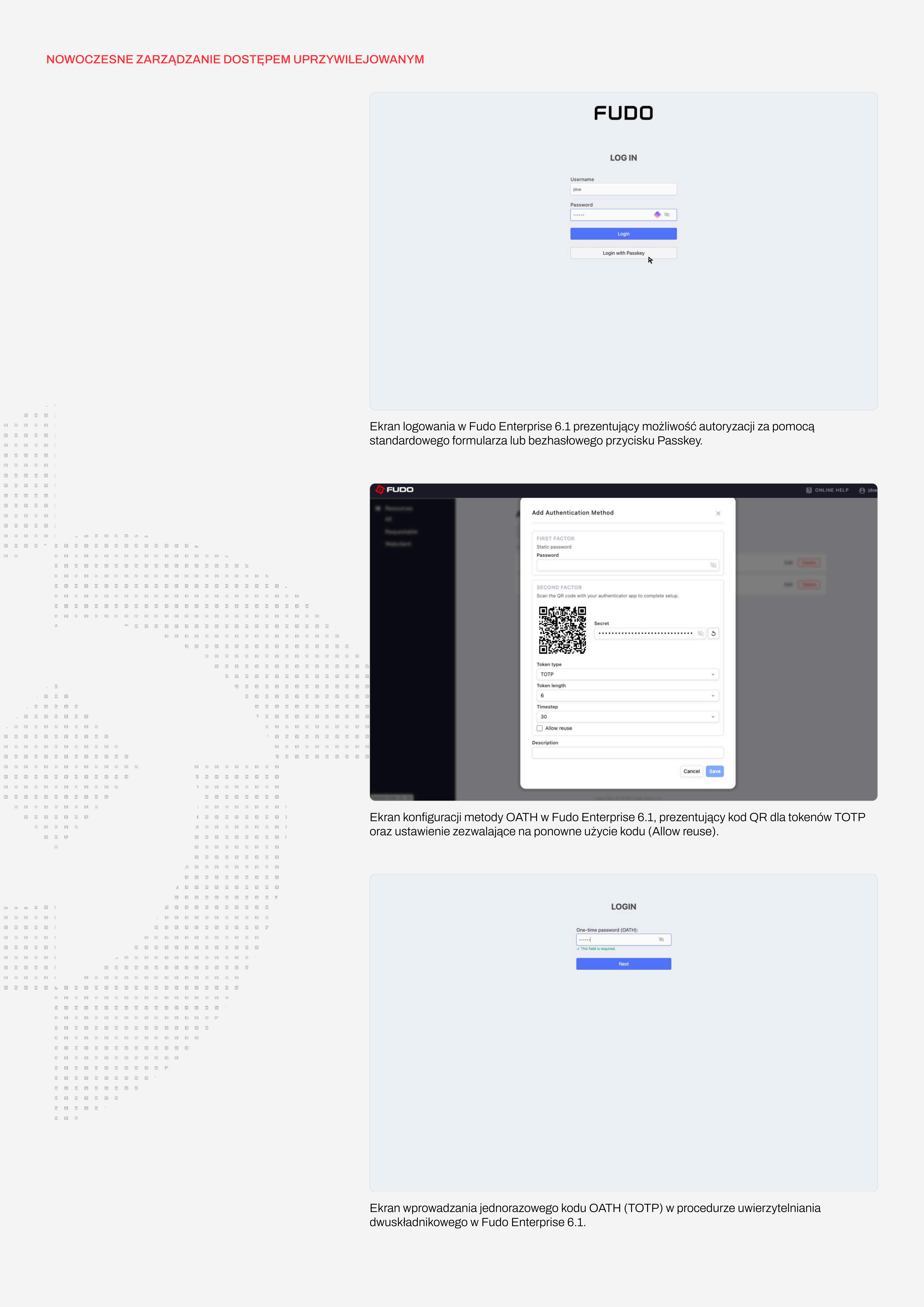
Fudo 6.1 obsługuje bezhasłowe logowanie zgodne ze standardem FIDO2. Użytkownicy mogą korzystać ze sprzętowych kluczy (np. YubiKey) i biometrii w urządzeniach końcowych oraz zarządzać poświadczeniami za pośrednictwem dedykowanego portalu samoobsługowego.



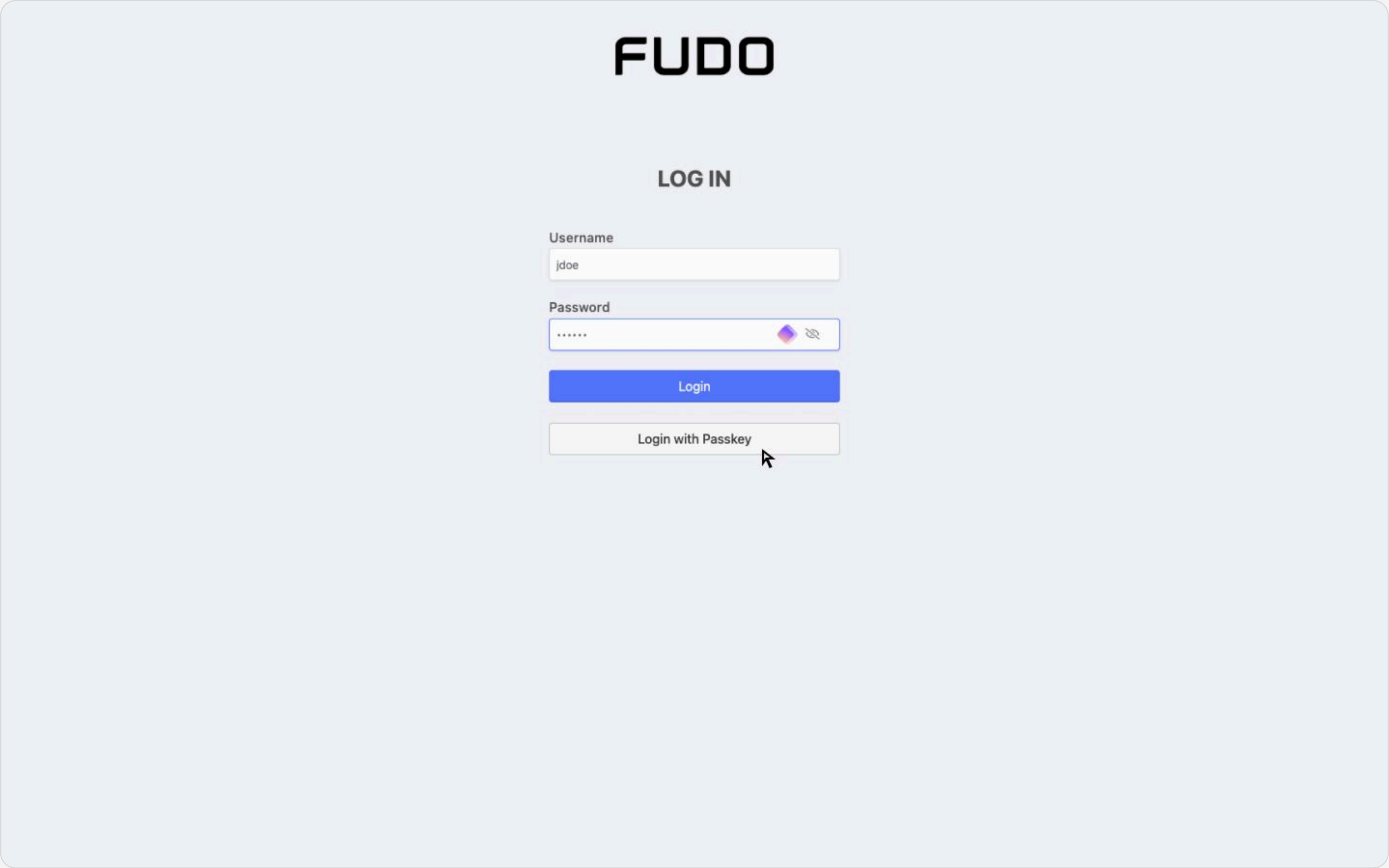
Ekran konfiguracji metod uwierzytelniania w portalu użytkownika Fudo Enterprise 6.1 z obsługą haseł, kluczy SSH, tokenów OATH oraz mechanizmów Passkey.



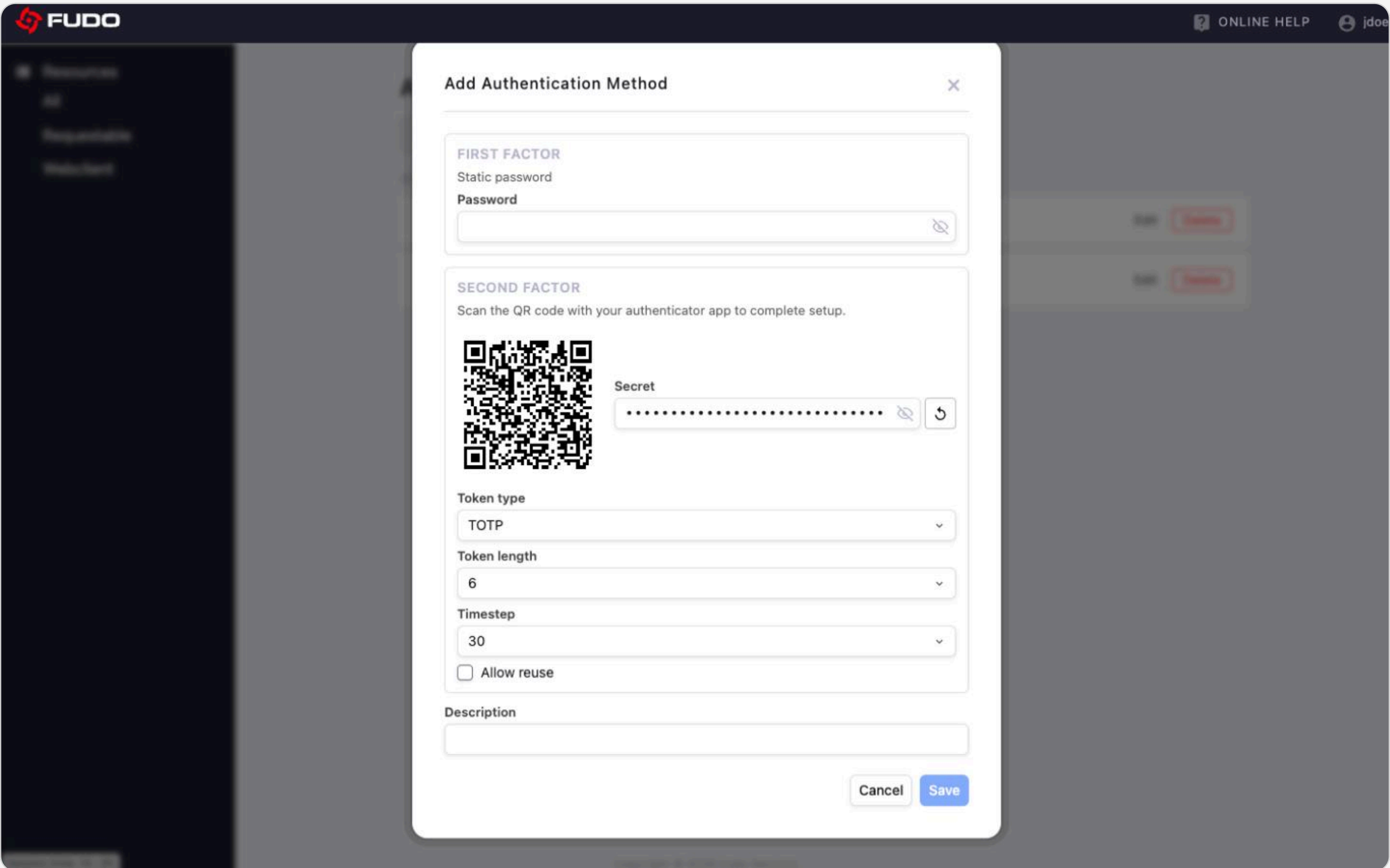
Okno konfiguracji nowej metody Passkey w Fudo Enterprise 6.1, prowadzący użytkownika przez proces parowania klucza sprzętowego lub autoryzacji biometrycznej.



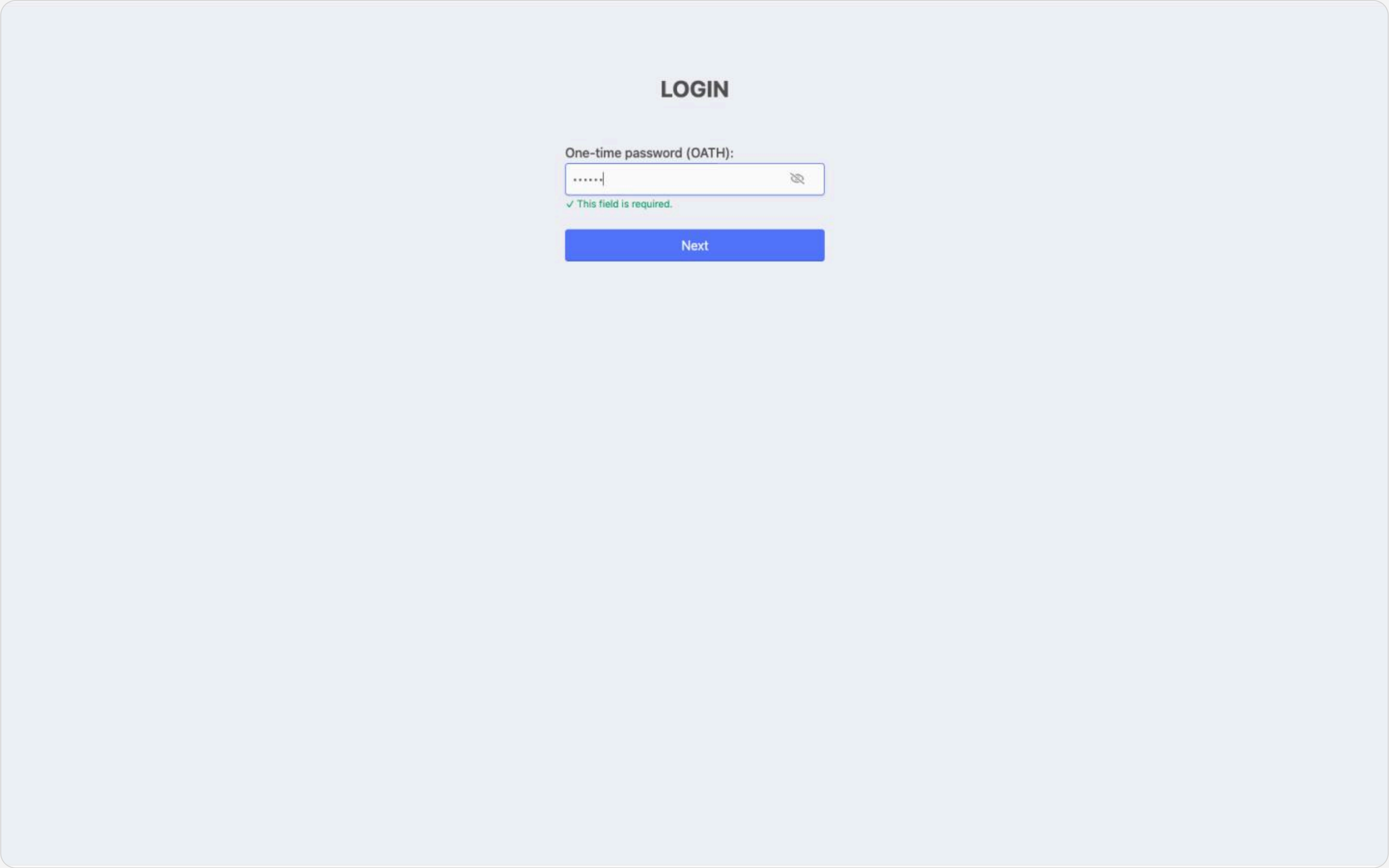
NOWOCZESNE ZARZĄDZANIE DOSTĘPEM UPRZYWILEJOWANYM



Ekran logowania w Fudo Enterprise 6.1 prezentujący możliwość autoryzacji za pomocą standardowego formularza lub bezhasłowego przycisku Passkey.



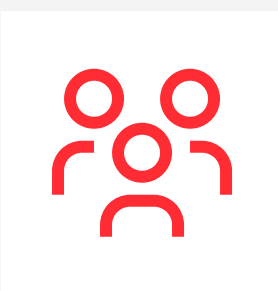
Ekran konfiguracji metody OATH w Fudo Enterprise 6.1, prezentujący kod QR dla tokenów TOTP oraz ustawienie zezwalające na ponowne użycie kodu (Allow reuse).



Ekran wprowadzania jednorazowego kodu OATH (TOTP) w procedurze uwierzytelniania dwuskładnikowego w Fudo Enterprise 6.1.

Automatyzacja logowania przez wtyczkę przeglądarkową

Wtyczka do przeglądarki współpracująca z Password Vault umożliwia bezpieczne uzupełnianie danych logowania w aplikacjach webowych. Rozwiązanie eliminuje potrzebę ręcznego przepisywania haseł lub ich przechowywania w niezabezpieczonych plikach.



Codzienna wygoda (Dla użytkowników i IT)

Skuteczne mechanizmy ochrony powinny być projektowane tak, aby nie nakładały na użytkowników i zespoły administracyjne nadmiernego obciążenia operacyjnego.

4.1 Kontrolowany transfer plików w sesjach RDP

Wymiana plików między środowiskiem lokalnym a zdalnymi zasobami jest częsta w codziennej pracy utrzymaniowej i wymaga odpowiedniego nadzoru.

Dedykowana przestrzeń transferowa

Fudo Drive umożliwia przesyłanie plików w sesjach RDP bezpośrednio z interfejsu przeglądarki. Interaktywne kontenery plików ułatwiają kontrolę nad materiałami wprowadzanymi i wyprowadzanymi ze środowiska docelowego.

Rejestracja i automatyczne czyszczenie zasobów

Transferowane pliki są rejestrowane w materiałach z przebiegu sesji. Po zakończeniu połączenia katalog transferowy może być automatycznie czyszczony, co zmniejsza ryzyko pozostawienia poufnych danych na serwerach docelowych.

4.2 Ułatwienia dla zespołów administracyjnych

Wraz ze skalowaniem infrastruktury rośnie liczba obiektów zarządzanych przez administratorów.

Operacje masowe

Interfejs zarządczy Fudo umożliwia zbiorcze edycje, zmiany statusu i przypisywanie polityk wielu obiektom jednocześnie. Usprawnia to rutynowe prace konfiguracyjne i skraca czas obsługi powtarzalnych zgłoszeń.

Okresowe kody jednorazowe

Wsparcie dla jednorazowych kodów OTP o wydłużonym czasie ważności (np. 60 sekund) ułatwia administratorom nawiązywanie równoległych połączeń do wielu zasobów bez konieczności ciągłego generowania nowych tokenów.



ShareAccess: Dostęp do zasobów w modelu chmurowym

Współpraca z zewnętrznymi podmiotami, takimi jak audytorzy, serwisanci czy dostawcy oprogramowania, wymaga bezpiecznego i prostego udostępniania zasobów.

Model bezinstalacyjny (SaaS)

Fudo ShareAccess w modelu chmurowym nie wymaga instalacji dodatkowych urządzeń w infrastrukturze klienta ani oprogramowania na komputerach dostawców zewnętrznych.

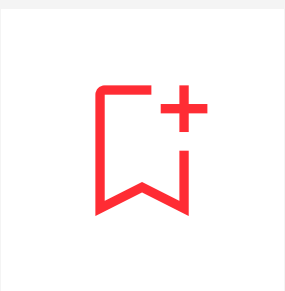
Dostęp do aplikacji bez udostępniania całej sieci

Zamiast szerokiego dostępu sieciowego przez tradycyjne połączenia VPN, ShareAccess pozwala wskazać konkretną aplikację lub serwer dostępny w przeglądarce. Ogranicza to widoczność pozostałych elementów infrastruktury.

Kontrola czasu dostępu i ochrona poświadczeń

Dostawca zewnętrzny uwierzytelnia się w portalu i realizuje zadania w określonym czasie. Poświadczenia do zasobów są przekazywane bez ujawniania ich użytkownikowi, co zmniejsza ryzyko niekontrolowanego wykorzystania poza wyznaczonym kanałem.





Podsumowanie

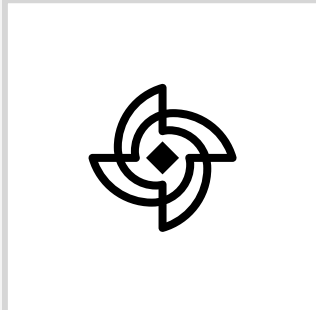
6.1

Nowoczesne zarządzanie dostępem uprzywilejowanym

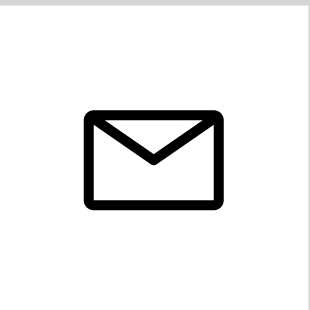
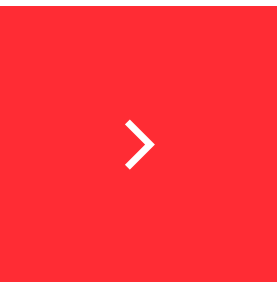
Wdrożenie rozwiązań zarządzania dostępem uprzywilejowanym powinno uwzględniać specyfikę i poziom dojrzałości technologicznej organizacji. Fudo Enterprise 6.1 oferuje elastyczne narzędzia wspierające budowę bezpiecznego środowiska IT: od nowoczesnych metod uwierzytelniania, przez integracje chmurowe, po usprawnienia codziennej pracy administratorów i użytkowników.

Sukces wdrożenia zależy od analizy potrzeb firmy, właściwej konfiguracji polityk i stopniowego wprowadzania zmian.

Fudo 6.1 zaprojektowano z myślą o elastyczności, umożliwiając stopniowe zwiększanie poziomu ochrony wraz ze wzrostem wymagań bezpieczeństwa, bez zakłócania bieżących procesów biznesowych.



www.fudosecurity.com



Zapytaj o ofertę

