Fudo Enterprise 6.2 - Portal Użytkownika

Fudo Security

27.08.2026

Spis treści

ROZDZIAŁ 1

Spis treści

1.1 O dokumentacji

Konwencje i symbole

Poniższa sekcja opisuje konwencje nazewnicze użyte w dokumentacji.

kursywa

Element interfejsu graficznego użytkownika.

`przykład`

Przykładowa wartość parametru konfiguracyjnego.

Uwaga

Informacja uzupełniająca ściśle związana z opisywanym zagadnieniem, np. sugestia dotycząca postępowania; dodatkowe warunki, które należy spełnić.

Ostrzeżenie

Ostrzeżenie. Informacja istotna z punktu widzenia działania systemu. Nie zastosowanie się do zalecenia może mieć nieodwracalne skutki.

1.2 Opis systemu

Portal użytkownika umożliwia inicjowanie połączeń z serwerami docelowymi, do których użytkownik został uprawniony.

- System pozwala także na podglądanie haseł do wybranych kont a także przeglądanie historii haseł zarządzanych przez moduł skarbca haseł FUDO.

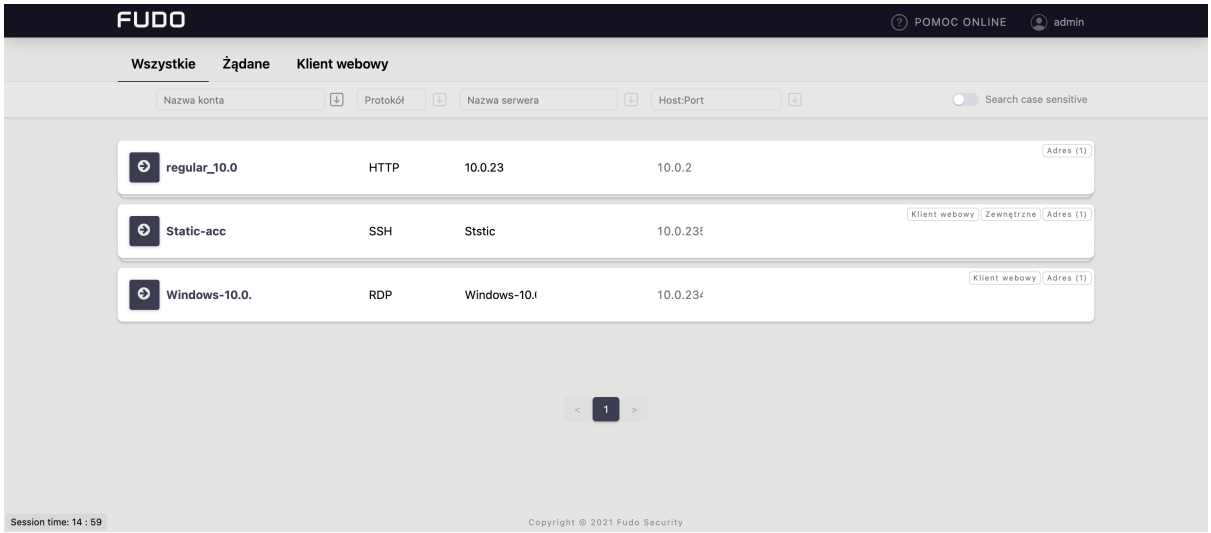
Uwaga

Więcej informacji na ten temat: *Podgląd historii haseł*.

- System umożliwia czasową rezerwację hasła do konta oraz jego automatyczne zdawanie po określonym czasie.

Uwaga

Więcej informacji pod linkiem *Wypożyczenie i zdawanie hasła dostępu*.



- Można także wybrać układ klawiatury serwera:
  - `English (US)` - Amerykański Angielski,
  - `German` - Niemiecki,
  - `German (Swiss)` - Szwajcarski Niemiecki,
  - `French` - Francuski (AZERTY),
  - `Norwegian` - Norweski,
  - `Turkish-Q` - Turecki.

Ostrzeżenie

Układy klawiatury na razie są dostępne tylko dla połączeń RDP w przeglądarce.

- Dostępne języki aplikacji: angielski, polski, rosyjski, ukraiński, kazachski, niemiecki oraz uzbecki.

Uwaga

Dostępność konkretnego języka jest określana podczas zakupu licencji.

Pokrewne tematy:

- *Logowanie do Portalu Użytkownika*
- *Metody uwierzytelniania*
- *Wypożyczenie i zdawanie hasła dostępu*
- *Podgląd historii haseł*
- *Podgląd i edycja notatek*
- *Nawiązywanie połączeń*
- *Rozwiązywanie problemów*

1.3 Logowanie do Portalu Użytkownika

Uwaga

- Portal Użytkownika jest kompatybilny z przeglądarkami Google Chrome, Mozilla Firefox oraz Microsoft Edge w systemach Microsoft Windows, Ubuntu i macOS.
- Portal Użytkownika wspiera funkcjonalność Single Sign On (SSO) do automatycznego uwierzytelnienia użytkowników Active Directory. Uruchomienie usługi SSO opisane jest w dokumentacji systemu.
- Do Portalu Użytkownika można też zalogować się za pomocą profilu w Azure albo Okta. Administrator może ustawić taki sposób logowania globalnie dla całego systemu.

1. Otwórz przeglądarkę internetową i wprowadź adres IP Portalu Użytkownika.

Uwaga

Adres IP uzyskasz od administratora systemu.

2. Potwierdź wyjątek bezpieczeństwa, aby wyświetlić stronę logowania.
3. Wprowadź nazwę użytkownika, hasło i kliknij *Zaloguj się*.

Tematy pokrewne:

- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Ubuntu*

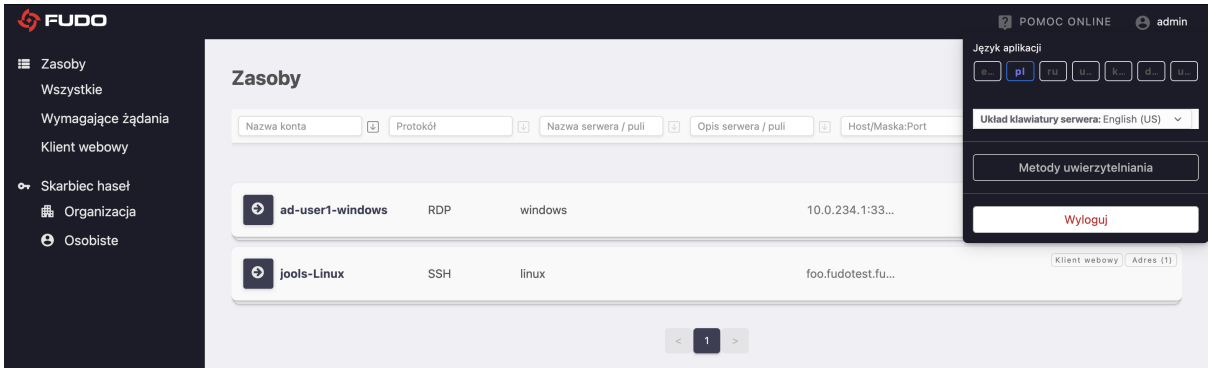
1.4 Metody uwierzytelniania

Portal umożliwia użytkownikom konfigurację własnych metod uwierzytelniania, w tym opcji uwierzytelniania wieloskładnikowego, takich jak OATH oraz FIDO2/Passkey.

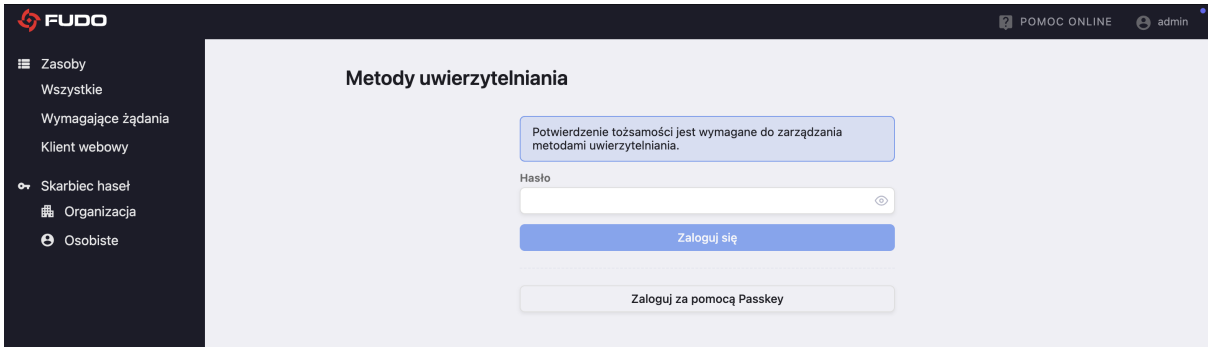
1.4.1 Dostęp do zarządzania metodami uwierzytelniania

Aby uzyskać dostęp do ustawień metod uwierzytelniania:

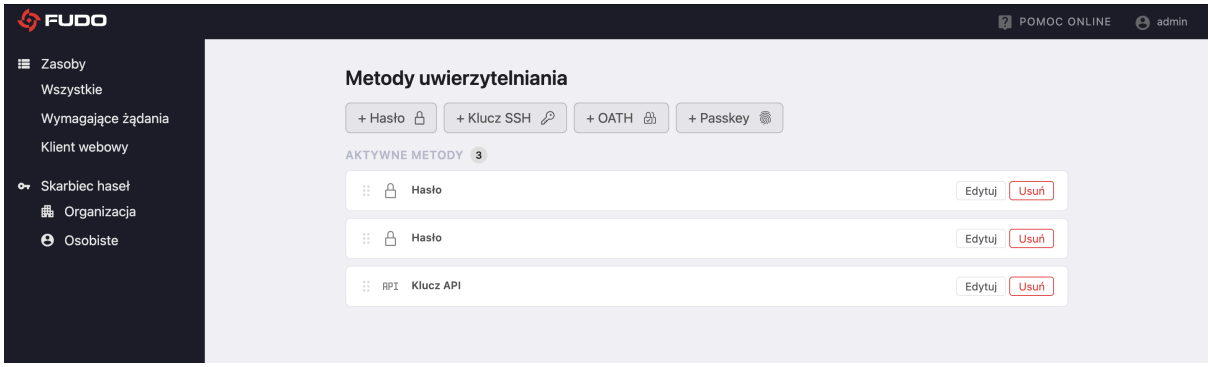
1. Zaloguj się do Portalu dostępu użytkownika
2. Otwórz menu użytkownika w prawym górnym rogu
3. Kliknij *Metody uwierzytelniania*



4. Wprowadź swoje aktualne hasło, aby uzyskać dostęp do ustawień



Po uwierzytelnieniu zobaczysz listę swoich aktualnych metod uwierzytelniania oraz możliwość dodania nowych.



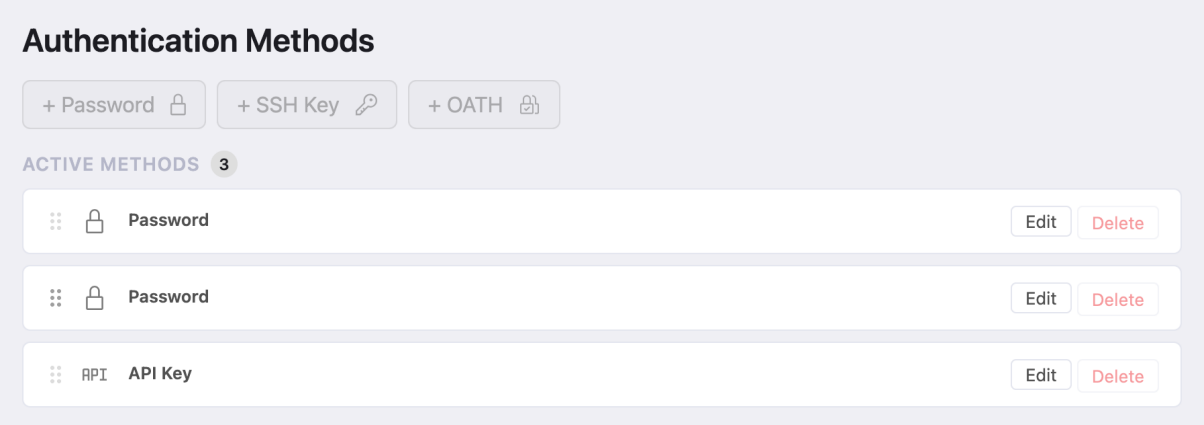
Uwaga

Dostęp do konfiguracji metod uwierzytelniania wymaga uwierzytelnienia dowolną metodą z wyjątkiem OpenID Connect.

1.4.2 Metody, którymi możesz zarządzać

Administrator decyduje, które typy metod uwierzytelniania możesz samodzielnie dodawać i usuwać. Ustawienie to jest wprowadzane w Panelu Administracyjnym i obowiązuje wszystkich użytkowników Portalu Użytkownika.

Jeśli dany typ metody nie jest dozwolony, przycisk jej dodania jest wyszarzony i wyświetla komunikat *Dodawanie i usuwanie tej metody uwierzytelniania zostało zablokowane przez administratora.* Przycisk *Usuń* przy każdej metodzie tego typu jest wyszarzony i wyświetla ten sam komunikat.



To ustawienie nigdy nie usuwa metod, które już posiadasz. Pozostają one na liście, nadal możesz się nimi logować i nadal możesz je edytować - na przykład zmiana hasła jest możliwa również wtedy, gdy dodawanie metody hasła jest zablokowane.

Uwaga

Niektóre metody są zawsze tworzone przez administratora i nigdy nie można ich usunąć w Portalu Użytkownika: *Klucz API*, *Certyfikat*, *DUO*, *SMS* oraz *Zewnętrzne uwierzytelnianie*. Ich przycisk *Usuń* jest wyszarzony i wyświetla komunikat *Tej metody uwierzytelniania nie można usunąć.* Edycja tych metod jest nadal możliwa.

Uwaga

Przycisk + Passkey w ogóle nie jest wyświetlany, jeśli administrator nie skonfigurował FIDO2. Różni się to od metody zablokowanej - metoda zablokowana jest widoczna jako wyszarzona, a nieskonfigurowana nie jest widoczna wcale.

Jeśli potrzebujesz metody, która nie jest dla Ciebie dostępna, skontaktuj się z administratorem systemu Fudo.

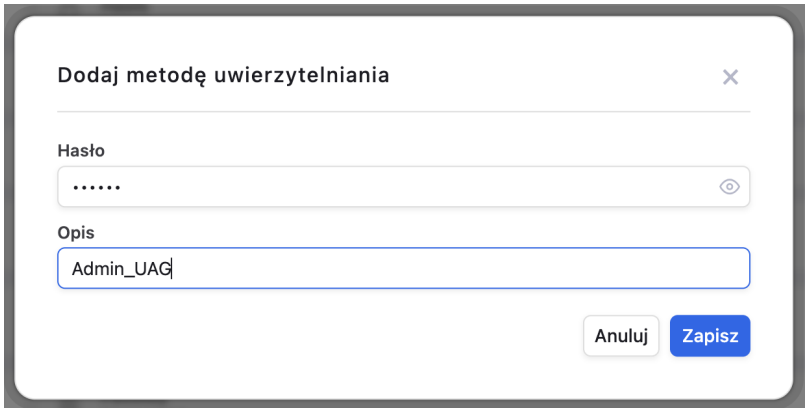
1.4.3 Uwierzytelnianie hasłem

Hasło jest podstawową metodą uwierzytelniania. Możesz zmienić swoje hasło w każdym momencie.

Zmiana hasła

Aby zmienić hasło:

1. W sekcji metod uwierzytelniania kliknij + *Hasło*
2. Wprowadź nowe hasło zgodnie z wymaganiami polityki bezpieczeństwa
3. Potwierdź nowe hasło
4. Kliknij *Zapisz*



Ostrzeżenie

Hasło musi spełniać wymagania określone w polityce złożoności haseł systemu.

Uwaga

Zmiana hasła wykonana w Portalu Użytkownika zaktualizuje również hasło zapisane w User Directory, jeśli włączona jest synchronizacja użytkowników. Funkcjonalność ta jest dostępna, jeśli w konfiguracji metody zewnętrznego uwierzytelniania w Panelu Admina Fudo Enterprise podamy dane konta z odpowiednimi uprawnieniami do zmiany haseł użytkowników w danym User Directory. Więcej informacji znajdziesz w rozdziale o konfiguracji zewnętrznego uwierzytelniania.

Uwaga

W przypadku użytkownika uwierzytelnionego metodą zewnętrznego uwierzytelniania **Active Directory**, gdy zmiana hasła jest wymuszana przez kontroler domeny, Fudo przeprowadza ją przy użyciu protokołu **Kerberos**, o ile Kerberos został użyty podczas uwierzytelniania tego użytkownika. Więcej informacji znajdziesz w rozdziale o ustawieniach uwierzytelniania Kerberos.

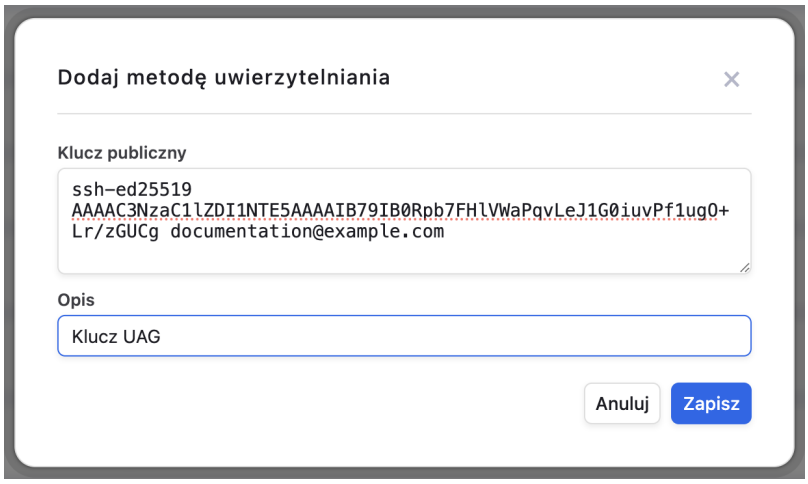
1.4.4 Uwierzytelnianie kluczem SSH

Klucze SSH pozwalają na bezpieczne uwierzytelnianie bez konieczności używania hasła podczas sesji SSH.

Dodawanie klucza SSH

Aby dodać klucz SSH:

1. W sekcji metod uwierzytelniania kliknij *+ Klucz SSH*
2. Wprowadź nazwę klucza (dla łatwej identyfikacji)
3. Wklej zawartość swojego publicznego klucza SSH
4. Kliknij *Zapisz*



1.4.5 Uwierzytelnianie OATH

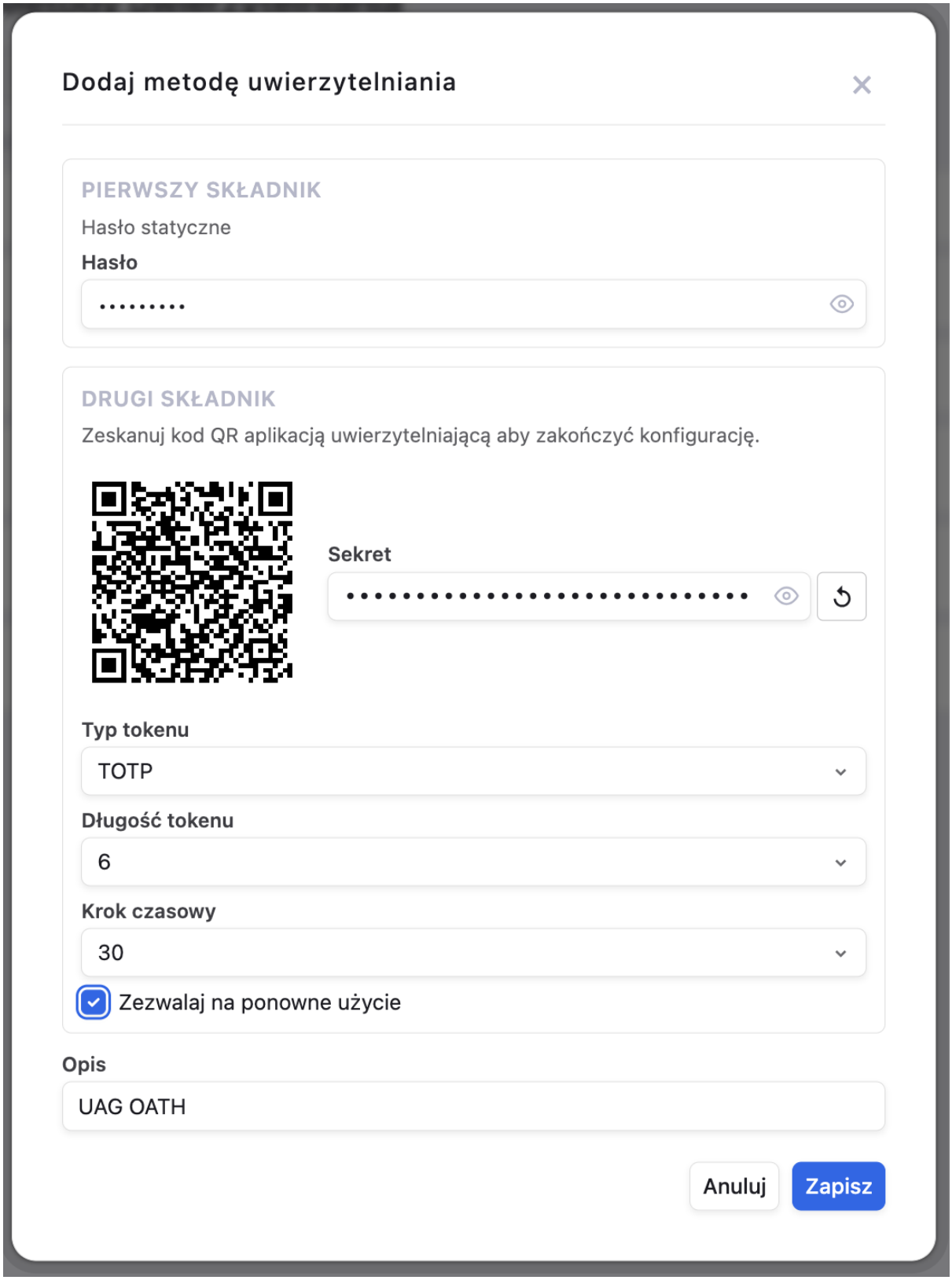
OATH to metoda uwierzytelniania dwuskładnikowego wykorzystująca kody czasowe generowane przez aplikację uwierzytelniającą.

Konfiguracja OATH

Aby skonfigurować metodę uwierzytelniania OATH:

1. W sekcji metod uwierzytelniania kliknij *+ OATH*
2. W sekcji *Pierwszy składnik* podaj statyczne hasło dla konta
3. W polu *Drugi składnik* wybierz `TOTP (czasowy)` lub `HOTP (licznikowy)` jako typ tokenu
4. Określ długość tokenu (zazwyczaj 6 cyfr)
5. Wybierz wymaganą wartość kroku czasowego (zazwyczaj 30 sekund)

6. (Opcjonalne) Włącz *Zezwól na ponowne użycie*, aby umożliwić akceptowanie tego samego kodu TOTP więcej niż raz w ramach aktualnego okna czasowego
7. Zeskanuj wyświetlony kod QR aplikacją uwierzytelniającą (np. Google Authenticator, Authy)
8. Wprowadź aktualny kod z aplikacji w celu weryfikacji
9. Kliknij *Zapisz*



Opcja Zezwól na ponowne użycie

Opcja `Zezwól na ponowne użycie` umożliwia akceptowanie tego samego prawidłowego kodu TOTP więcej niż raz w ramach aktualnego okna czasowego. Ta funkcja jest szczególnie przydatna w scenariuszach, w których wymagany jest równoległy dostęp.

Przypadki użycia:

- Skryptowany dostęp SSH
- Playbooki Ansible
- Równoległe operacje scp lub rsync
- Runnery CI łączące się z wieloma systemami
- Dostęp przez wiele hostów bastion
- Masowe przekazywanie połączeń RDP

Domyślne zachowanie:

Domyślnie opcja `Zezwól na ponowne użycie` jest wyłączona. Każdy kod TOTP może być użyty tylko raz. Po pomyślnej weryfikacji kolejna próba użycia tego samego kodu zostanie odrzucona.

Po włączeniu:

Gdy opcja `Zezwól na ponowne użycie` jest włączona:

- Ten sam kod TOTP może być akceptowany wielokrotnie w ramach aktualnego okna czasowego
- Możesz użyć tego samego kodu TOTP dla wielu równoległych połączeń w ramach jednego kroku czasowego
- Po wygaśnięciu kroku czasowego poprzedni kod staje się nieważny i wymagany jest nowy kod

Uwaga

Opcja `Zezwól na ponowne użycie` jest dostępna tylko dla tokenów TOTP (czasowych). Tokeny HOTP (licznikowe) nie obsługują ponownego użycia kodu.

Ostrzeżenie

Włącz tę opcję tylko wtedy, gdy jest to konieczne dla konkretnych przypadków użycia. Zezwolenie na ponowne użycie kodu TOTP zmniejsza poziom bezpieczeństwa w porównaniu z kodami jednorazowymi.

1.4.6 Uwierzytelnianie FIDO2 (Passkey)

FIDO2/Passkey to nowoczesna metoda uwierzytelniania bez hasła, wykorzystująca klucze sprzętowe, biometrię lub menedżery haseł.

Konfiguracja FIDO2/Passkey

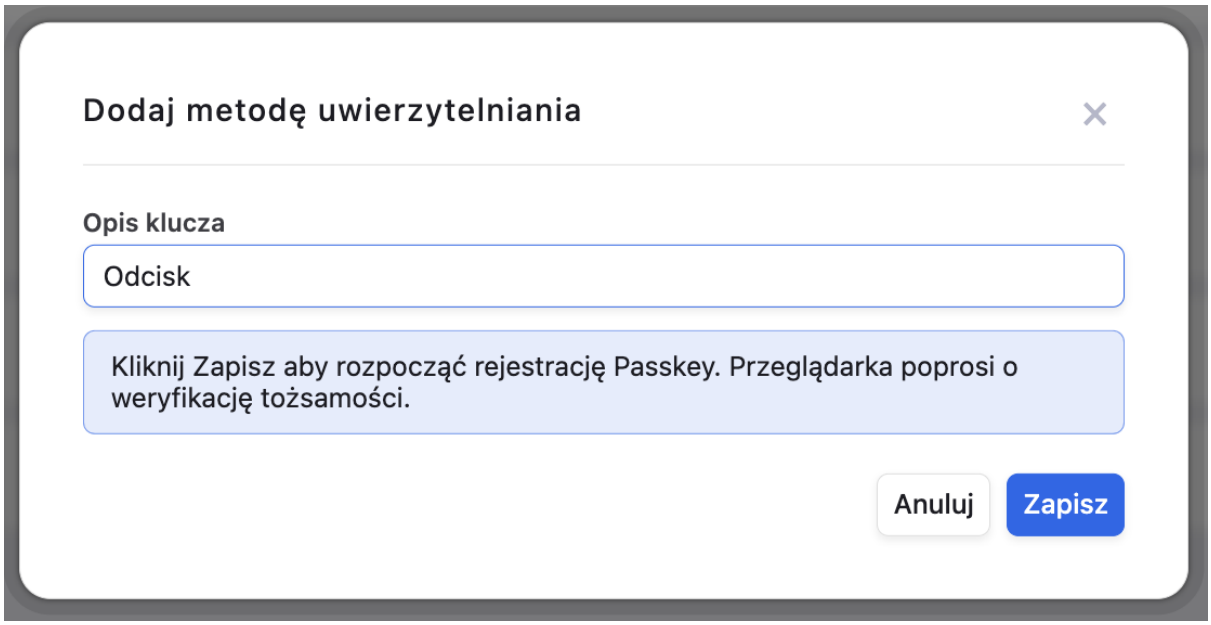
Uwaga

Aby móc skonfigurować i używać passkeyów w Portalu Użytkownika, administrator musi najpierw skonfigurować uwierzytelnianie FIDO2/Passkey w Panelu Administracyjnym oraz

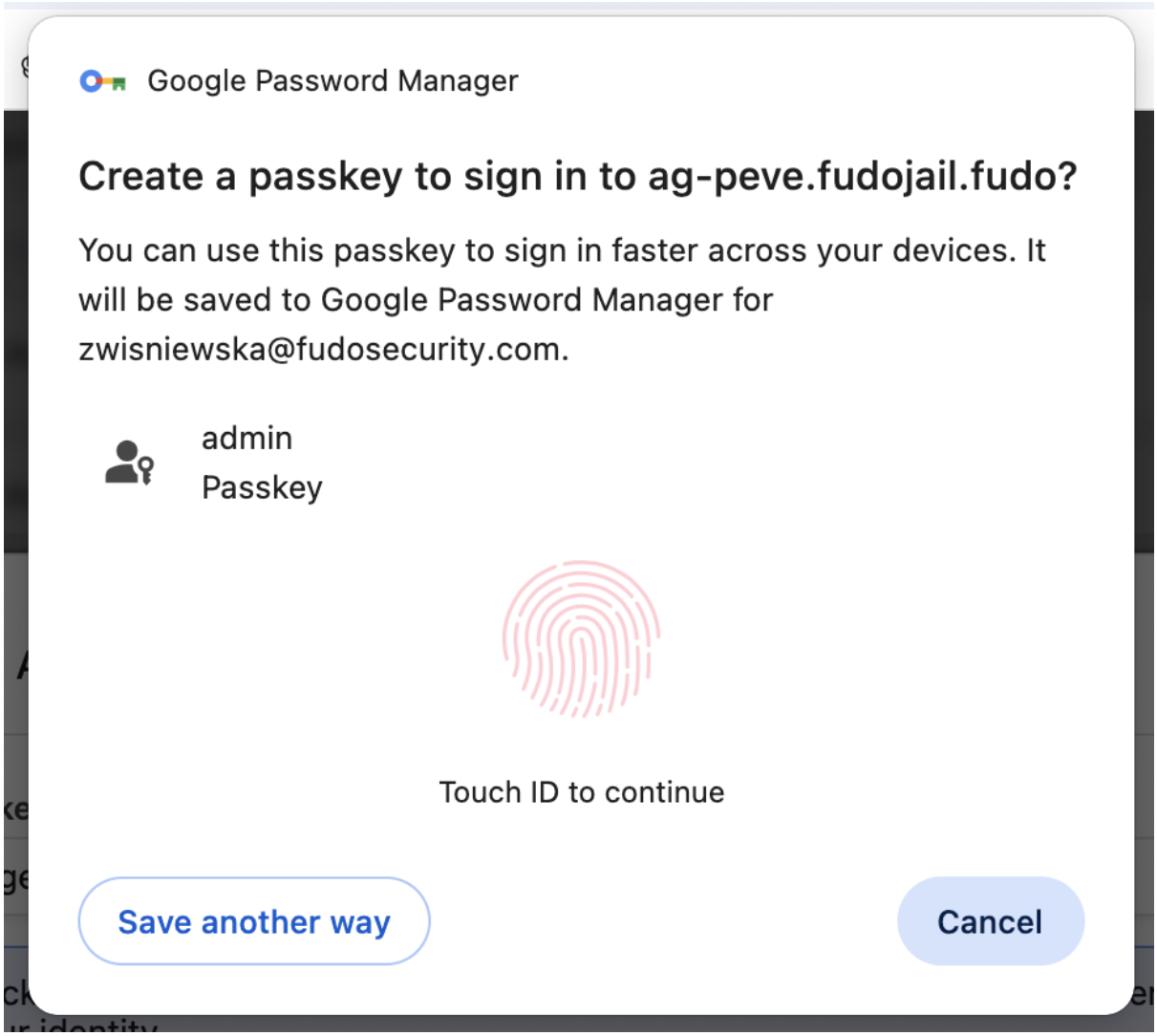
zezwolić użytkownikom na samodzielne zarządzanie metodą *Passkey*. Jeśli uwierzytelnianie za pomocą passkeyów nie jest dostępne, skontaktuj się z administratorem systemu Fudo.

Aby skonfigurować metodę uwierzytelniania FIDO2/Passkey:

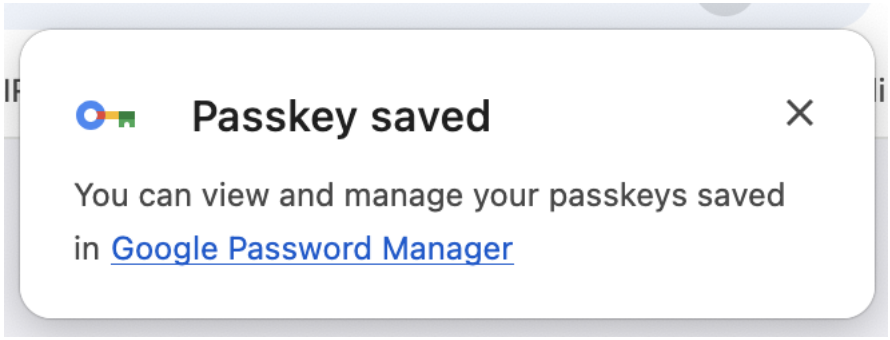
1. W sekcji metod uwierzytelniania kliknij *+ Passkey*



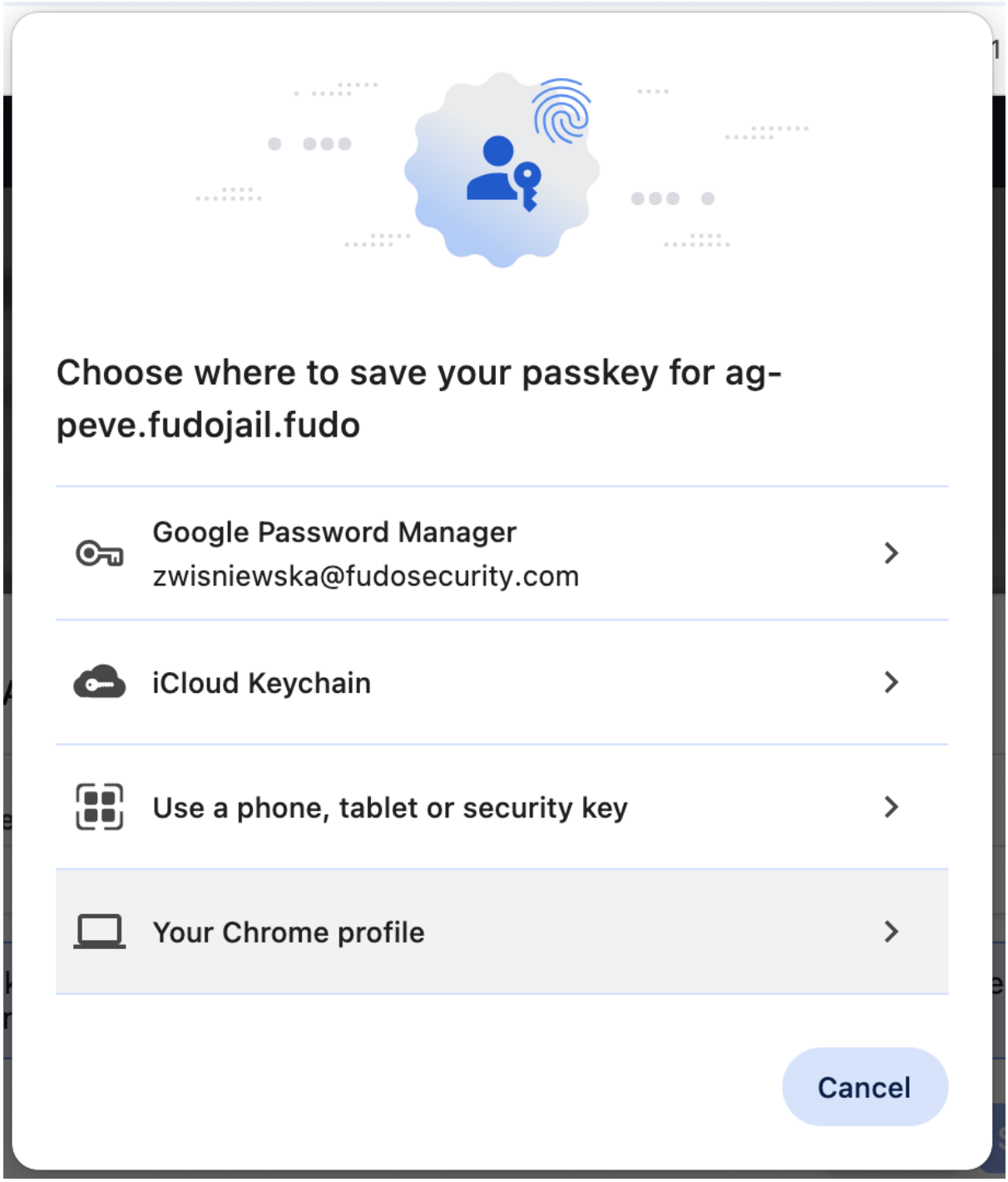
2. Postępuj zgodnie z instrukcjami przeglądarki lub menedżera haseł:
   - Wybierz metodę uwierzytelnienia (klucz sprzętowy, biometria, menedżer haseł)



3. Wprowadź nazwę dla swojego klucza Passkey



4. Potwierdź swoją tożsamość (dotknij klucza, użyj odcisku palca, Face ID) i zapisz klucz Passkey w wybranej lokalizacji
5. Po pomyślnym utworzeniu klucza zobaczysz potwierdzenie



Obsługiwane metody FIDO2

System wspiera następujące metody uwierzytelniania FIDO2:

- **Klucze sprzętowe** - YubiKey, Titan Security Key
- **Biometria wbudowana** - Touch ID (macOS), Windows Hello, Face ID
- **Menedżery haseł** - 1Password, Google Password Manager, Apple Passwords
- **Urządzenia mobilne** - używane jako klucze bezpieczeństwa przez Bluetooth/NFC

Używanie uwierzytelniania FIDO2/Passkey

Po skonfigurowaniu metody FIDO2:

1. Na stronie logowania wprowadź swoją nazwę użytkownika
2. Kliknij przycisk Zaloguj za pomocą Passkey (pojawia się tylko gdy FIDO2 jest skonfigurowane)
3. Potwierdź swoją tożsamość używając skonfigurowanej metody
4. System automatycznie zweryfikuje podpis kryptograficzny i udzieli dostępu

Ostrzeżenie

Klucze Passkey utworzone w Portalu Użytkownika nie mogą być wykorzystane w Panelu Administracyjnym ze względu na różne identyfikatory Relying Party.

1.4.7 Usuwanie metody uwierzytelniania

Aby usunąć jedną ze swoich metod uwierzytelniania:

1. W sekcji metod uwierzytelniania odszukaj metodę na liście *Aktywne metody*
2. Kliknij *Usuń*
3. Potwierdź usunięcie

Możesz usunąć wyłącznie taki typ metody, który wolno Ci również dodać. Jeśli przycisk Usuń jest wyszarzony, najedź na niego kursorem, aby poznać przyczynę:

- *Dodawanie i usuwanie tej metody uwierzytelniania zostało zablokowane przez administratora.* - administrator nie zezwolił na samodzielne zarządzanie tym typem metody. Poproś administratora o usunięcie metody lub o udostępnienie tego typu metody.
- *Tej metody uwierzytelniania nie można usunąć.* - metoda została utworzona przez administratora i nie ma swojego odpowiednika w samoobsłudze, dlatego może ją usunąć wyłącznie administrator.

Uwaga

Usuwanie metody jest celowo powiązane z jej dodawaniem. Zapobiega to sytuacji, w której usuniesz poświadczenie, którego nie mógłbyś samodzielnie utworzyć ponownie.

Tematy pokrewne:

- *Podgląd historii haseł*
- *Metody uwierzytelniania*

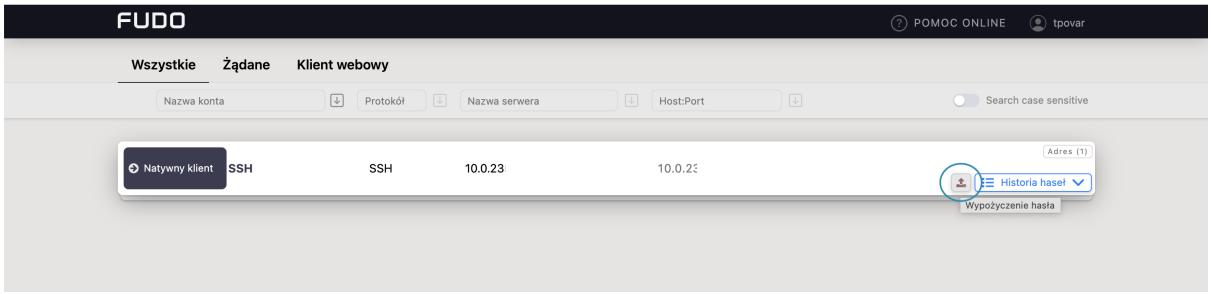
1.5 Wypożyczenie i zdawanie hasła dostępu

Przez Portal Użytkownika można czasowo wypożyczyć hasło dostępu innego konta. Jeśli dla danego użytkownika administrator ustawił określony okres dostępu do hasła, to jego „zwrot” odbędzie się automatycznie po upływie zdefiniowanego czasu. W przeciwnym wypadku, użytkownik jest zobowiązany „zwrócić” hasło manualnie.

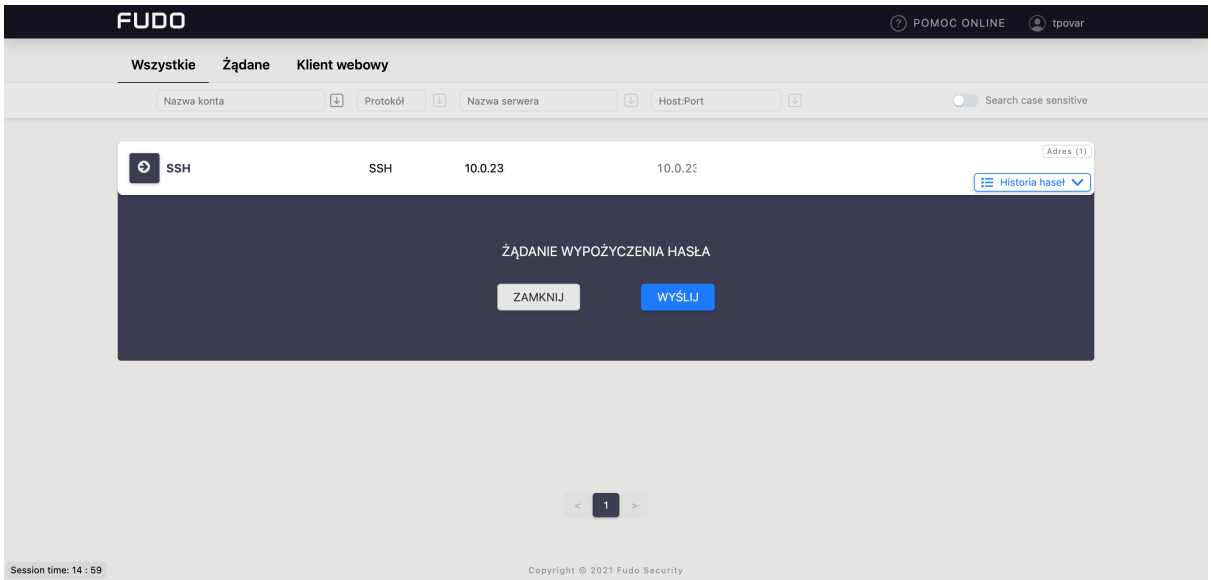
1.5.1 Wypożyczenie haseł

Aby wypożyczyć hasło, postępuj zgodnie z instrukcją:

1. Znajdź konto, którego hasło chcesz wypożyczyć. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
2. Kliknij ikonkę .



3. Kliknij *WYŚLIJ*.

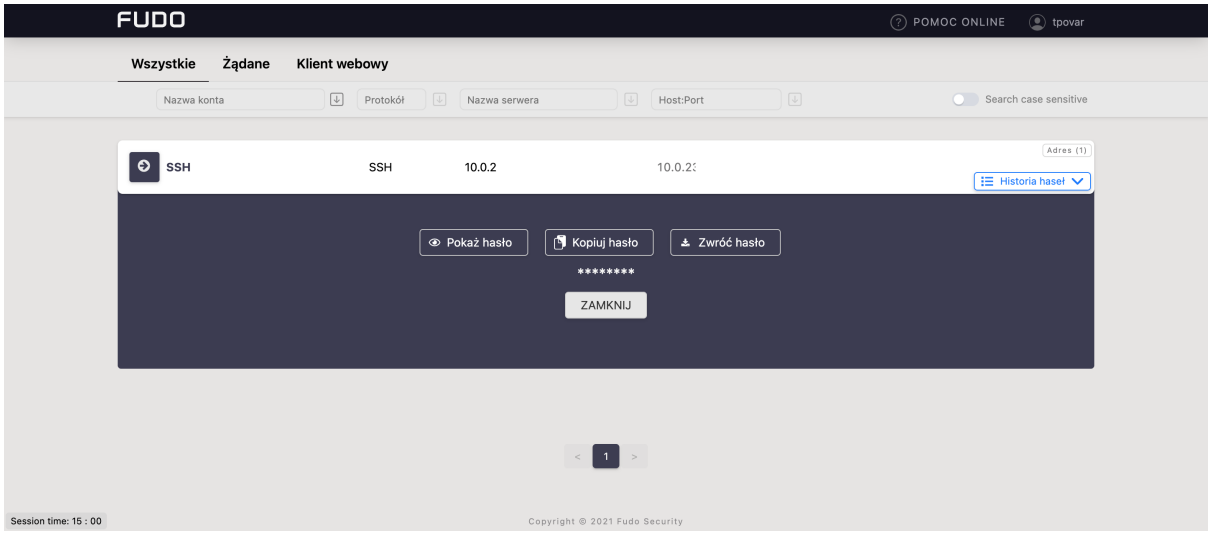


Jeśli powód jest wymagany, wprowadź go i kliknij *WYŚLIJ*.

Uwaga

- Wymaganie podania powodu logowania zależy od ustawień administracyjnych dla wybranego konta.
- W zależności od konfiguracji, żądanie wypożyczenia hasła może wymagać zatwierdzenia przez administratora.
- Jeśli hasło do konta jest aktualnie wypożyczone przez innego użytkownika, spróbuj ponownie później, lub skorzystaj z opcji *WYMUŚ REZERWACJĘ*.

4. Kliknij:
   - *Pokaż hasło*, aby wyświetlić hasło.
   - *Kopiuj hasło*, aby skopiować hasło do schowka.

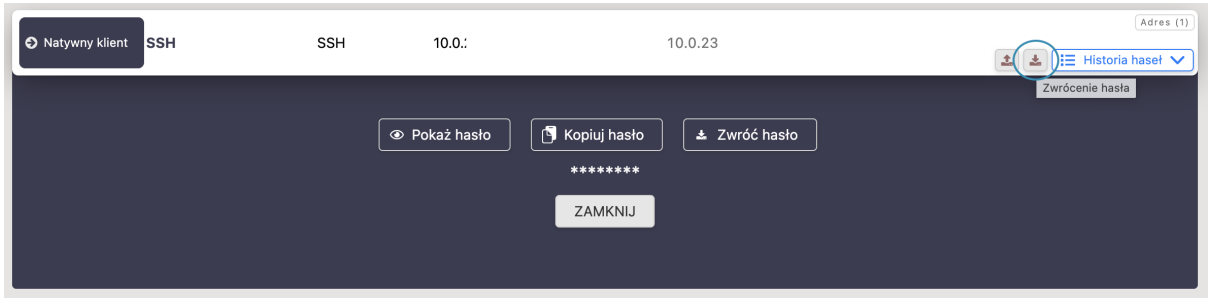


1.5.2 Zdawanie haseł dostępu

1. Znajdź konto, którego chcesz zdać hasło. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
2. Kliknij ikonkę ,

   lub

   kliknij ikonę i w oknie modalowym kliknij przycisk *Zwróć hasło*.



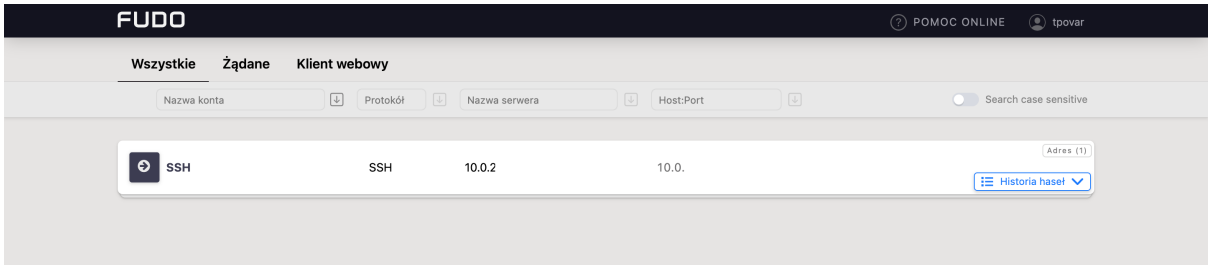
Pokrewne tematy:

- *Podgląd historii haseł*

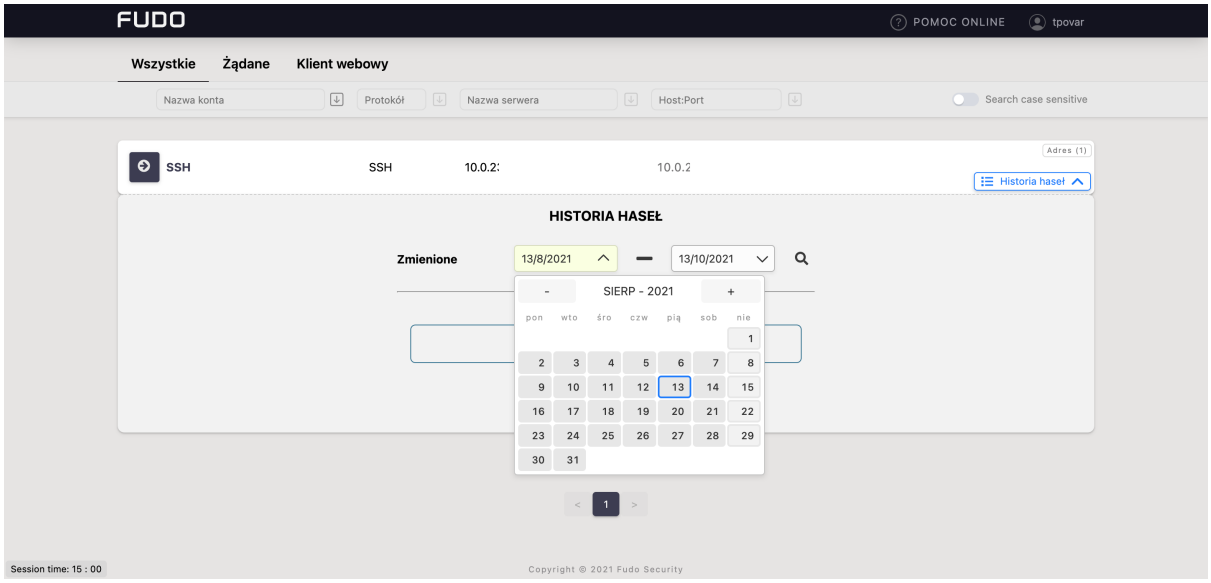
1.6 Podgląd historii haseł

Hasło dostępowe może zostać zmienione manualnie przez użytkownika, bądź automatycznie przez system Fudo Enterprise w zależności od ustawień skryptów oraz częstotliwości ich działania. Portal Użytkownika pozwala wyświetlić historię tych zmian. Postępuj zgodnie z instrukcją, aby je zobaczyć:

1. Znajdź konto, którego historię haseł chcesz przeglądać.
2. Kliknij przycisk *Historia haseł*.



3. Wybierz okres czasu, w ciągu którego hasło było zmieniane.



Pokrewne tematy:

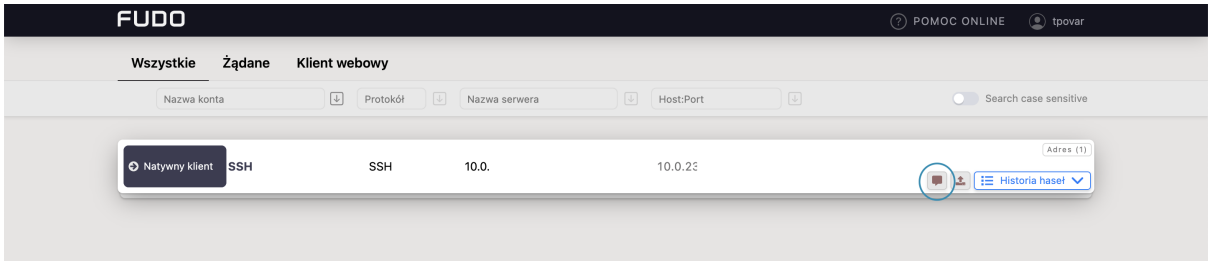
- *Podgląd historii haseł*
- *Metody uwierzytelniania*

1.7 Podgląd i edycja notatek

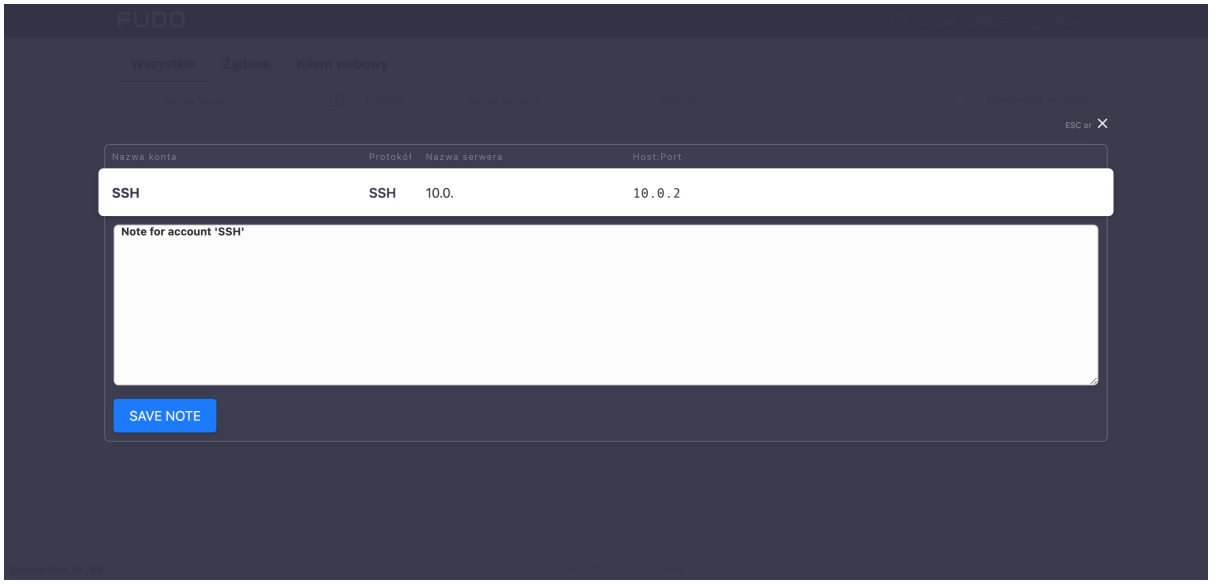
Notatki tworzone przez administratora mogą zawierać dodatkowe informacje dotyczące dostępu do serwerów.

> **Uwaga**
>
> Uprawnienia do przeglądania lub edytowania notatek nadawane są przez administratora na poziomie obiektu *sejf*.

1. Znajdź konto, którego notatkę chcesz zobaczyć.
2. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
3. Kliknij ikonę z notatką, aby wyświetlić jej treść.



4. Zmień lub wprowadź treść notatki i kliknij *ZAPISZ NOTATKĘ*, aby zapisać zmiany, lub zamknij modal krzyżykiem w prawym górnym rogu, albo klawiszem *Esc* na klawiaturze, aby zamknąć okno bez zapisywania zmian.



1.8 Skarbiec haseł

Moduł Skarbiec haseł w Portalu Użytkownika zapewnia bezpieczny, scentralizowany system do zarządzania hasłami i sekretami. Pozwala użytkownikom przechowywać, organizować i udostępniać dane logowania w obrębie organizacji, jednocześnie utrzymując osobiste sekrety oddzielnie.

Skarbiec haseł składa się z dwóch głównych komponentów:

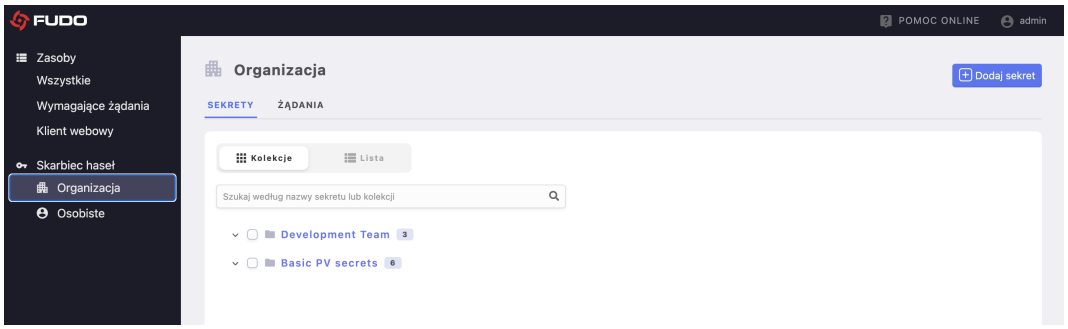
- **Skarbiec organizacji** - Zarządzany przez organizację, zawiera wspólne sekrety i kolekcje dostępne na podstawie uprawnień użytkownika.
- **Skarbiec osobisty** - Prywatna przestrzeń dla poszczególnych użytkowników do przechowywania ich osobistych danych logowania.

Poniższe sekcje opisują główne cechy Skarbca haseł oraz sposób pracy z sekretami i kolekcjami.

1.8.1 Przegląd

Dostęp do Skarbca haseł

1. Zaloguj się do Portalu Użytkownika przy użyciu swoich danych logowania.
2. W lewym panelu znajdź sekcję **Skarbiec haseł**.
3. Zobaczysz dwie opcje:
   - **Organizacja** - Dla sekretów współdzielonych w całej firmie.
   - **Osobisty** - Dla Twoich prywatnych danych logowania.



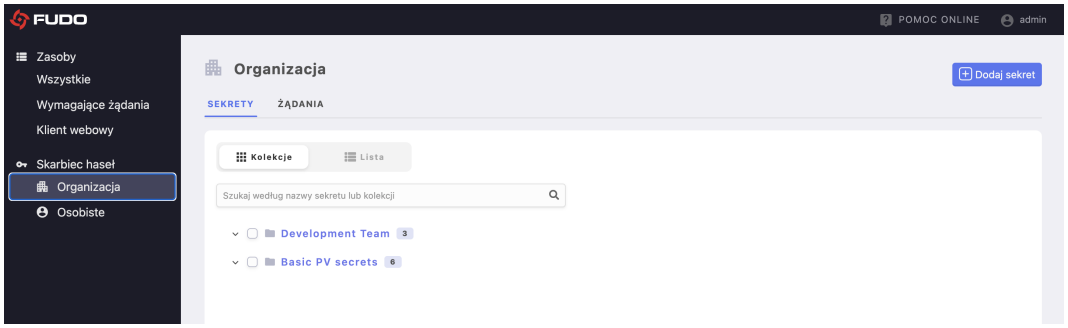
Przeglądanie sekretów i kolekcji

Interfejs zapewnia dwa tryby widoku:

- **Widok kolekcji** (domyślny) - Wyświetla sekrety zorganizowane w hierarchicznej strukturze kolekcji.
- **Widok listy** - Pokazuje wszystkie dostępne sekrety w formacie tabeli.

Widok kolekcji

Widok kolekcji to domyślny widok, wyświetlający sekrety zorganizowane w hierarchicznym drzewie kolekcji.



Wyszukiwanie i filtrowanie

Użyj paska wyszukiwania, aby szybko znaleźć sekrety:

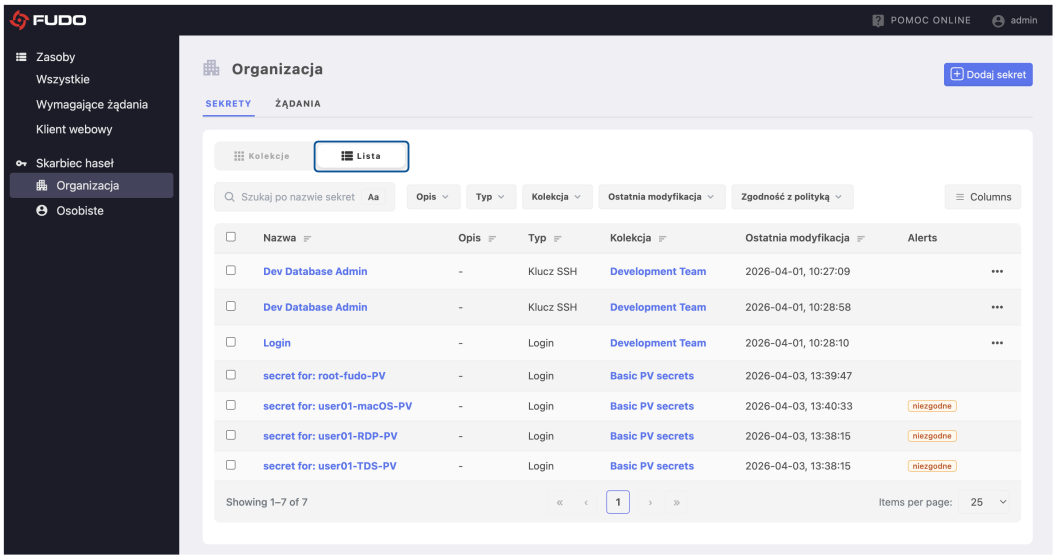
1. Wpisz nazwę sekretu lub nazwę kolekcji w polu wyszukiwania.
2. Użyj filtrów, aby zawęzić wyniki:
   - Kliknij na foldery kolekcji, aby filtrować według kolekcji.
   - Liczba obok każdej kolekcji pokazuje, ile sekretów zawiera.

Widok listy

Widok listy zapewnia kompleksową tabelę wszystkich dostępnych sekretów.

Przełączenie na widok listy

1. Kliknij przycisk **Lista** w przełączniku widoku.

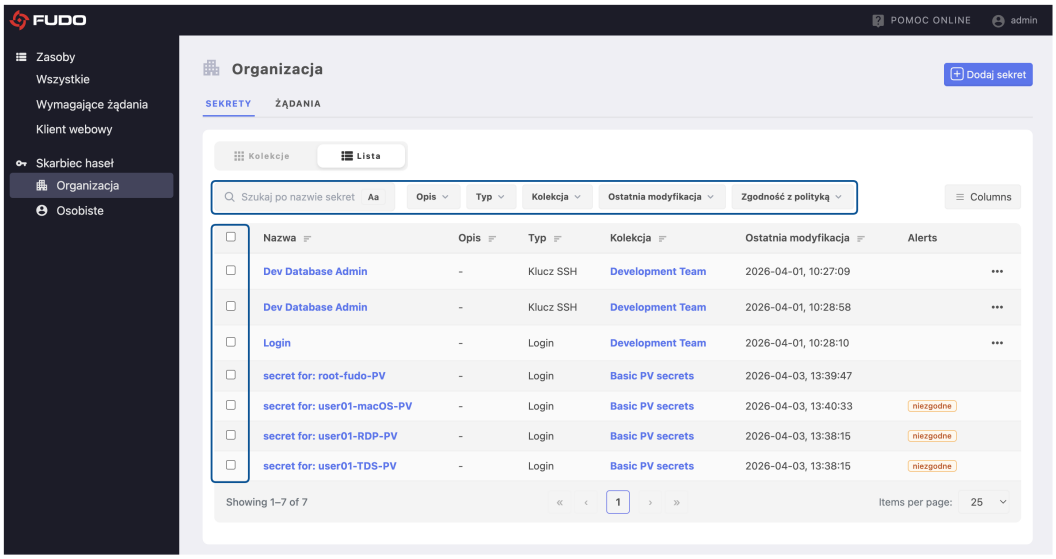


Sortowanie i filtrowanie

Tabela wyświetla:

- **Nazwa** - Nazwa sekretu (kliknij, aby otworzyć)
- **Opis** - Krótki opis
- **Typ** - Login, Klucz SSH, Notatka itp.
- **Kolekcja** - Nazwa kolekcji nadrzędnej
- **Ostatnia modyfikacja** - Data i czas ostatniej zmiany
- **Alerty** - Pokazuje, czy hasło spełnia polityki bezpieczeństwa

1. Kliknij w nagłówek danej kolumny, aby przesortować dane według jej zawartości rosnąco lub malejąco.
2. Użyj paska wyszukiwania, aby filtrować wyniki.
3. Wybierz wiele sekretów za pomocą pól wyboru jesli chcesz wykonać operację zbiorczą (np: usuwanie, przenoszenie).

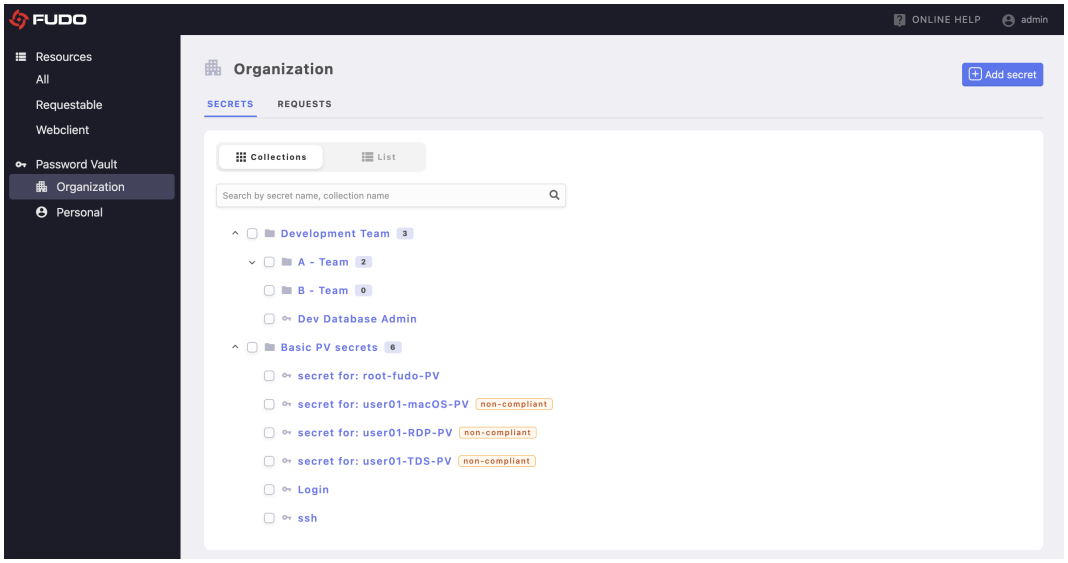


1.8.2 Skarbiec organizacji

Skarbiec organizacji zawiera sekrety i kolekcje zarządzane na poziomie organizacyjnym. Dostęp do tych sekretów jest kontrolowany przez system uprawnień.

Dostęp do Skarbca organizacji

1. Kliknij na **Organizacja** pod **Skarbiec haseł** w lewym panelu.
2. Główny widok otwiera się, pokazując dostępne kolekcje.



Rozumienie uprawnień użytkownika

W Skarbcu organizacji dostęp do sekretów jest zarządzany przez uprawnienia przydzielone przez administratora systemu. W zależności od poziomu uprawnień przyznanych dla kolekcji, użytkownicy mogą mieć możliwość przeglądania nazw sekretów, żądania dostępu do wartości sekretów, ujawniania i kopiowania danych sekretów lub pełnego zarządzania sekretami.

Widok na żądanie

- Przeglądanie nazw sekretów i kolekcji.
- Żądanie jednorazowego dostępu do wartości sekretów (wymaga zatwierdzenia administratora).
- Nie można modyfikować ani usuwać sekretów.

Widok

- Przeglądanie szczegółów wszystkich sekretów w kolekcji w dowolnym czasie.
- Ujawnianie i kopiowanie wartości sekretów.
- Nie można modyfikować ani usuwać sekretów.

Pełna edycja

- Wszystkie możliwości **Widok**, plus:
- Modyfikowanie istniejących sekretów.
- Przenoszenie sekretów między kolekcjami.
- Usuwanie sekretów.
- Dodawanie nowych sekretów do kolekcji.

Brak uprawnień

- Nie można przeglądać ani uzyskiwać dostępu do żadnych sekretów.

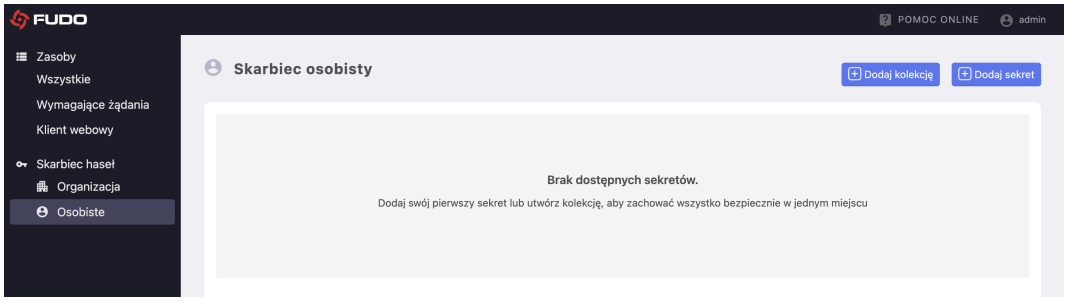
> **Uwaga**
>
> Jeśli potrzebujesz dostępu do Skarbca haseł lub dodatkowego dostępu do wybranych kolekcji, skontaktuj się z administratorem.

1.8.3 Skarbiec osobisty

Twój *Skarbiec osobisty* to prywatna przestrzeń do przechowywania osobistych danych logowania, do których tylko Ty masz dostęp, zapewniając Ci pełną prywatność, pełną kontrolę nad sekretami i domyślnie pełne uprawnienia do edycji.

Dostęp do Skarbca osobistego

1. Kliknij na **Osobisty** pod **Skarbiec haseł** w lewym panelu.
2. Zakładka skarbca osobistego pokazuje Twoje prywatne kolekcje i sekrety.
3. Jeśli otwierasz zakładkę po raz pierwszy, zobaczysz wiadomość powitalną, zachęcającą do stworzenia pierwszej kolekcji.



Kluczowe funkcje

Tworzenie i zarządzanie sekretami

W Twoim Skarbcu osobistym możesz:

- Dodawać dowolny typ sekretu (Login, Klucz SSH, Notatka, Klucz API, Certyfikat).
- Edytować i aktualizować informacje o sekrecie w dowolnym czasie.
- Przenosić sekrety między kolekcjami.
- Usuwać sekrety na stałe.

Uwaga

Szczegółowe instrukcje dotyczące zarządzania sekretami znajdziesz w *Dodawanie nowego sekretu*.

Organizowanie za pomocą kolekcji

Zarządzanie kolekcjami dostępne jest tylko w Skarbcu osobistym:

- Twórz nieograniczoną liczbę kolekcji i zagnieżdżonych struktur.
- Organizuj sekrety według projektów, klientów lub dowolnego systemu, który Ci odpowiada.
- Przenoś i reorganizuj kolekcje według potrzeby.
- Usuwaj puste kolekcje, gdy już nie są potrzebne.

Uwaga

Szczegółowe instrukcje dotyczące zarządzania kolekcjami znajdziesz w *Zarządzanie kolekcjami (Skarbiec osobisty)*.

Porównanie Skarbca osobistego ze Skarbcem organizacji

Funkcja	Skarbiec osobisty	Skarbiec organizacji
Kontrola dostępu	Pełna kontrola (tylko właściciel)	Oparta na uprawnieniach (zarządzana przez administratora)
Zarządzanie kolekcjami	Tworzenie/edycja/usuwanie przez Portal Użytkownika	Tylko zarządzanie przez administratora
Wymagana akceptacja	Nie	Tak (dla ograniczonego dostępu)
Widoczność	Prywatna dla użytkownika	Widoczna dla autoryzowanych użytkowników

Rozpoczęcie pracy

Aby rozpocząć korzystanie z Twojego Skarbca osobistego:

1. Utwórz pierwszą kolekcję - zobacz *Zarządzanie kolekcjami (Skarbiec osobisty)*.
2. Dodaj pierwszy sekret - zobacz *Zarządzanie sekretami*.

3. Organizuj i zarządzaj według potrzeby, używając funkcji opisanych powyżej.

1.8.4 Zarządzanie sekretami

Sekrety przechowują poufne informacje, takie jak dane logowania, klucze API, certyfikaty, klucze SSH i notatki. Każdy sekret jest przypisany do kolekcji w celu organizacji i kontroli dostępu.

Uwaga

Proces tworzenia sekretów jest identyczny w Skarbcu organizacji i Skarbcu osobistym. Główne różnice to:

- **Skarbiec organizacji**: Wymaga odpowiednich uprawnień od administratora. Potrzebujesz uprawnień *Pełna edycja* dla kolekcji docelowej.
- **Skarbiec osobisty**: Domyślnie masz pełną kontrolę. Nie potrzebujesz zatwierdzenia administratora dla swoich osobistych kolekcji.

Ostrzeżenie

Dla Skarbca organizacji: Musisz mieć odpowiednie uprawnienia, aby dodawać sekrety. Jeśli nie masz dostępu, skontaktuj się z administratorem Fudo.

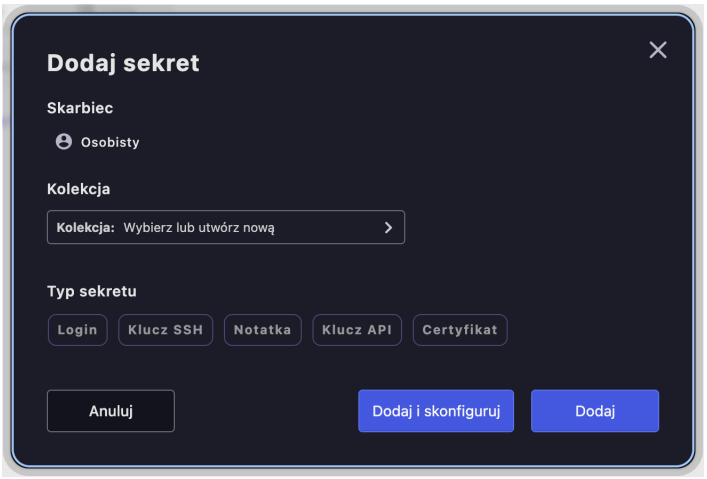
Dodawanie nowego sekretu

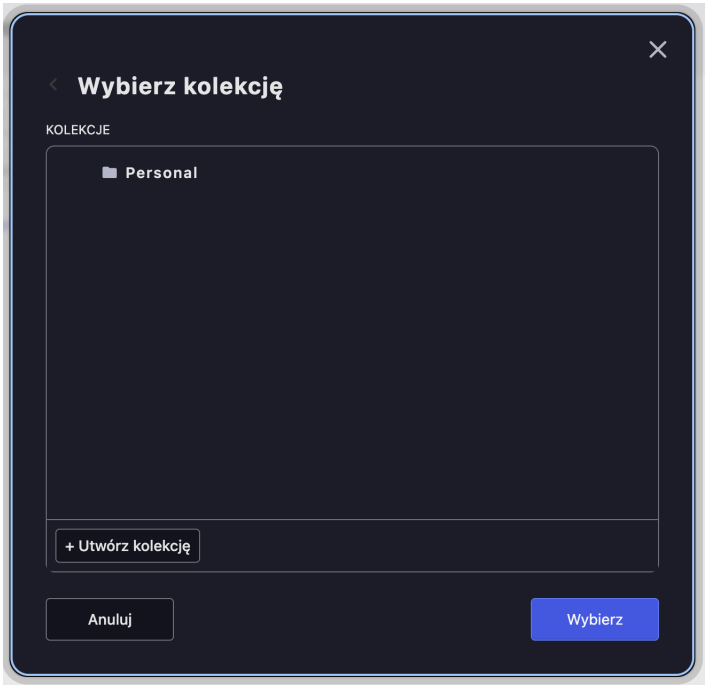
Uwaga

Dostępne typy sekretów:

- **Login**: Dane logowania nazwy użytkownika/hasła z informacjami o domenie i URL
- **Klucz SSH**: Prywatne klucze SSH do dostępu do serwerów
- **Notatka**: Notatki w postaci zwykłego tekstu do przechowywania informacji innych niż dane logowania
- **Klucz API**: Tokeny i klucze API do uwierzytelniania usług
- **Certyfikat**: Certyfikaty cyfrowe i klucze prywatne

1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.
2. Kliknij *Dodaj sekret*.

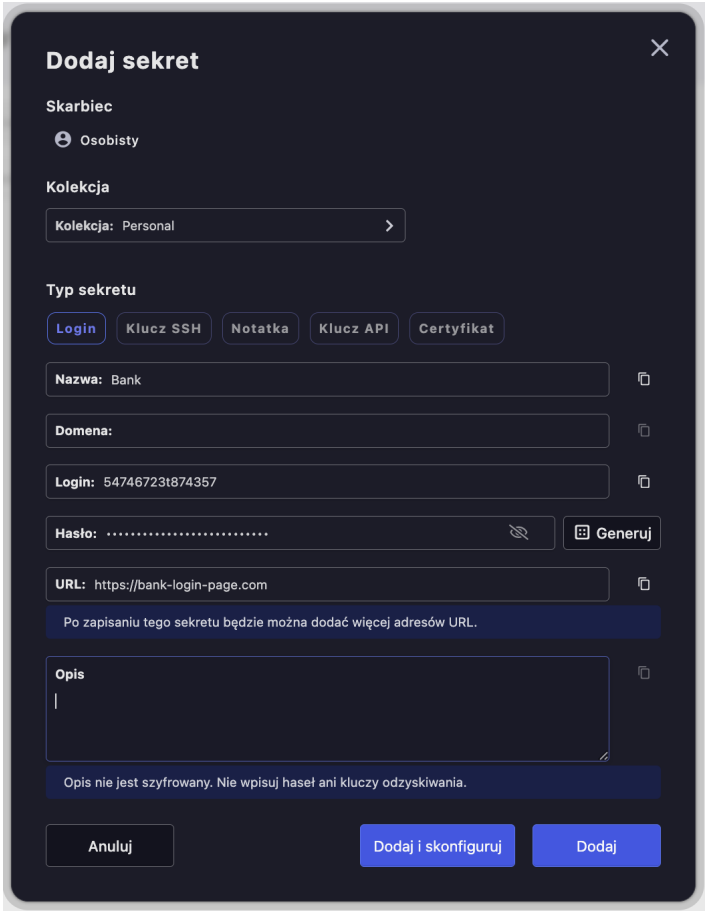




3. Wybierz kolekcję, w której zostanie przechowywany sekret, klikając listę rozwijaną *Kolekcja*.
4. Kliknij *Wybierz*.
5. Wybierz odpowiedni typ sekretu (Login, Klucz SSH, Notatka, Klucz API, Certyfikat).

Dla sekretów typu Login:

- Wypełnij wymagane pola:
  - *Nazwa*: Wprowadź opisową nazwę dla sekretu
  - *Domena*: Adres domeny docelowej lub serwera
  - *Login*: Nazwa użytkownika lub konta
  - *Hasło*: Możesz użyć przycisku *Generuj* dla bezpiecznych haseł
  - *URL*: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - *Opis*: Opcjonalne dodatkowe informacje (nieszyfrowane)

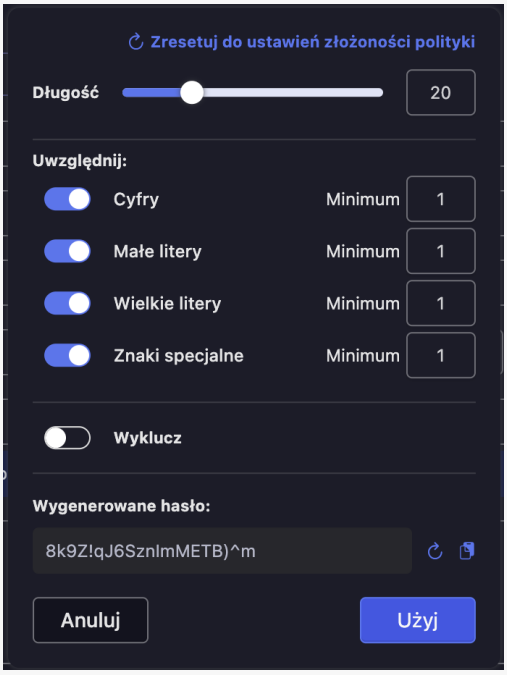


Uwaga

Generator haseł:

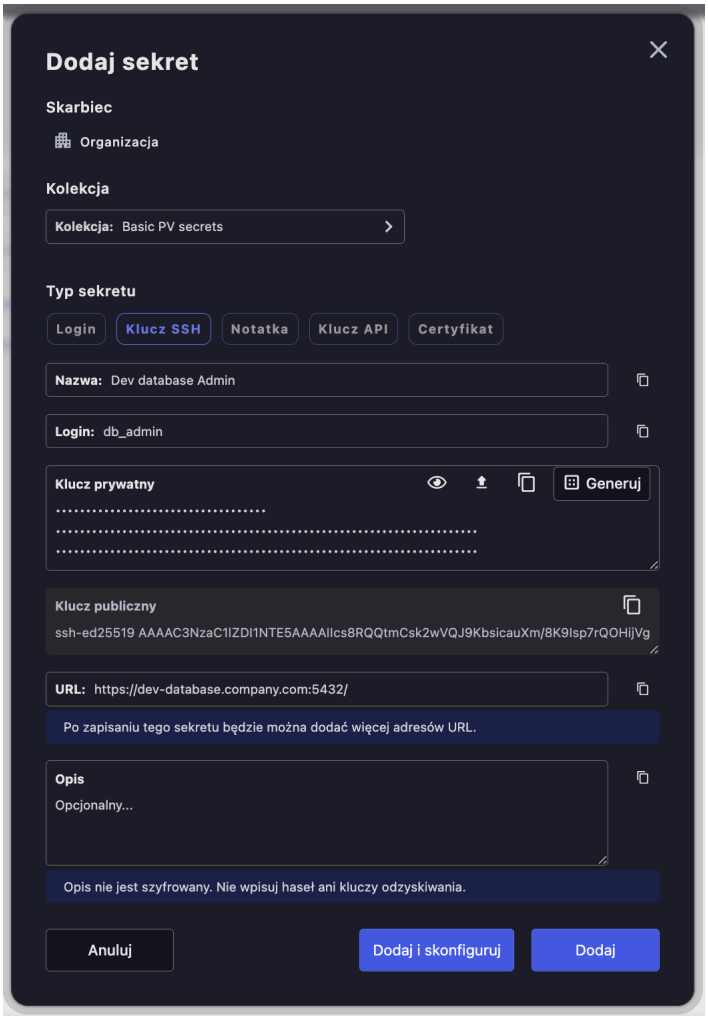
Zintegrowany generator haseł (przycisk *Generuj*) zapewnia bezpieczne tworzenie haseł z konfigurowalnym opcjami:

- **Długość**: Ustaw długość hasła (domyślnie: 20 znaków)
- **Typy znaków**: Uwzględnij cyfry, małe litery, wielkie litery, znaki specjalne
- **Minimalne wymagania**: Ustaw minimalną liczbę dla każdego typu znaku
- **Opcje wykluczania**: Wyklucz niejednoznaczne lub określone znaki
- **Wygenerowane hasło**: Podgląd i kopiowanie wygenerowanego hasła



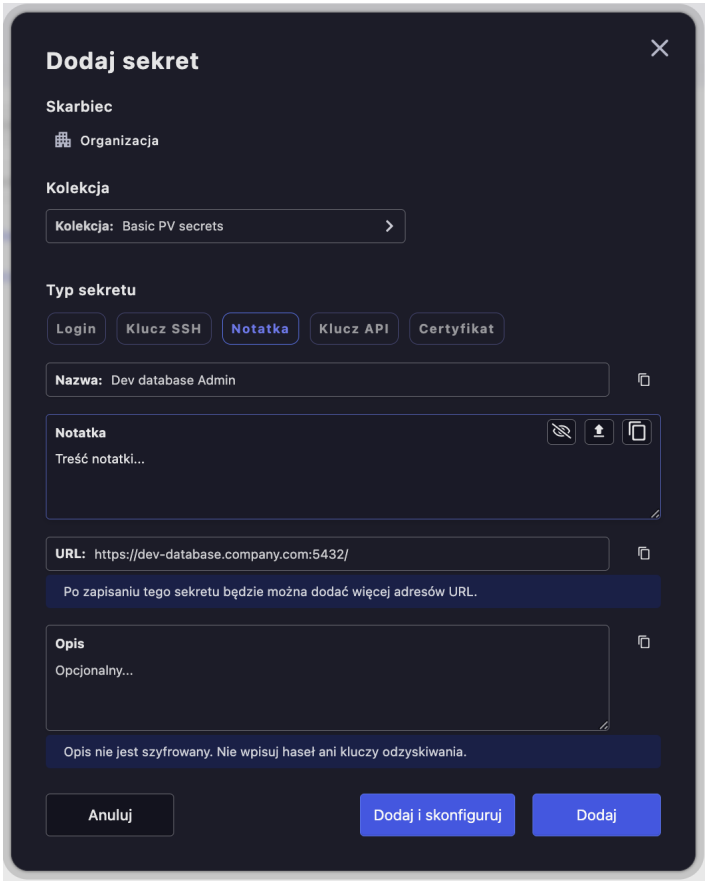
Dla sekretów typu Klucz SSH:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Login: Wprowadź nazwę użytkownika lub konta
  - Klucz prywatny: Wprowadź klucz prywatny lub kliknij *Generuj*, aby wygenerować klucze prywatny i publiczny
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



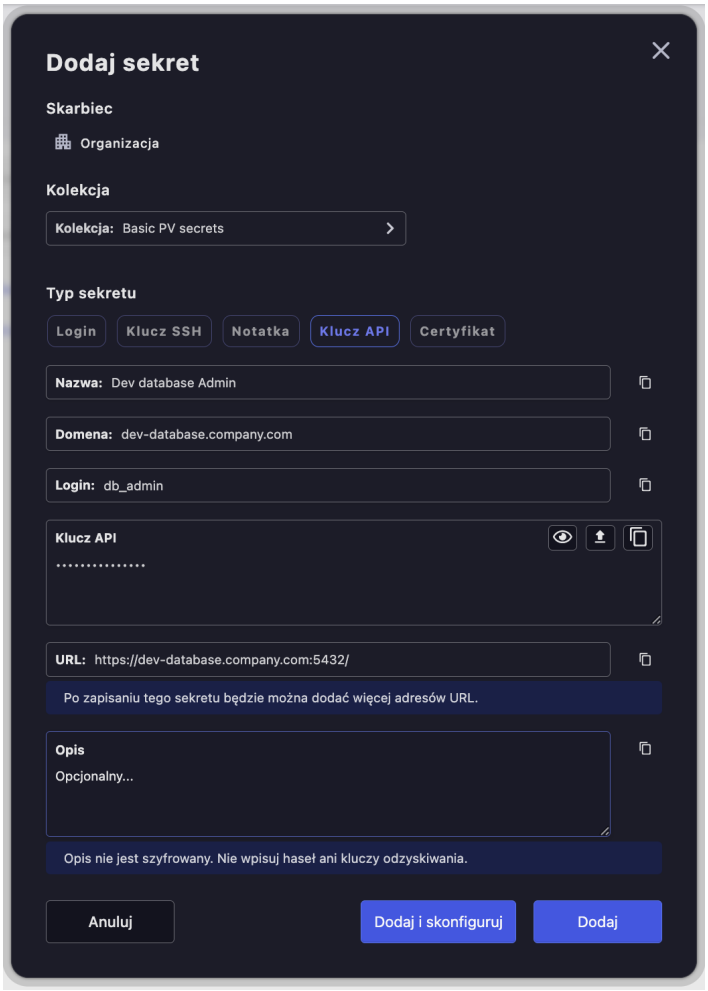
Dla sekretów typu Notatka:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Notatka: Wprowadź zawartość notatki
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



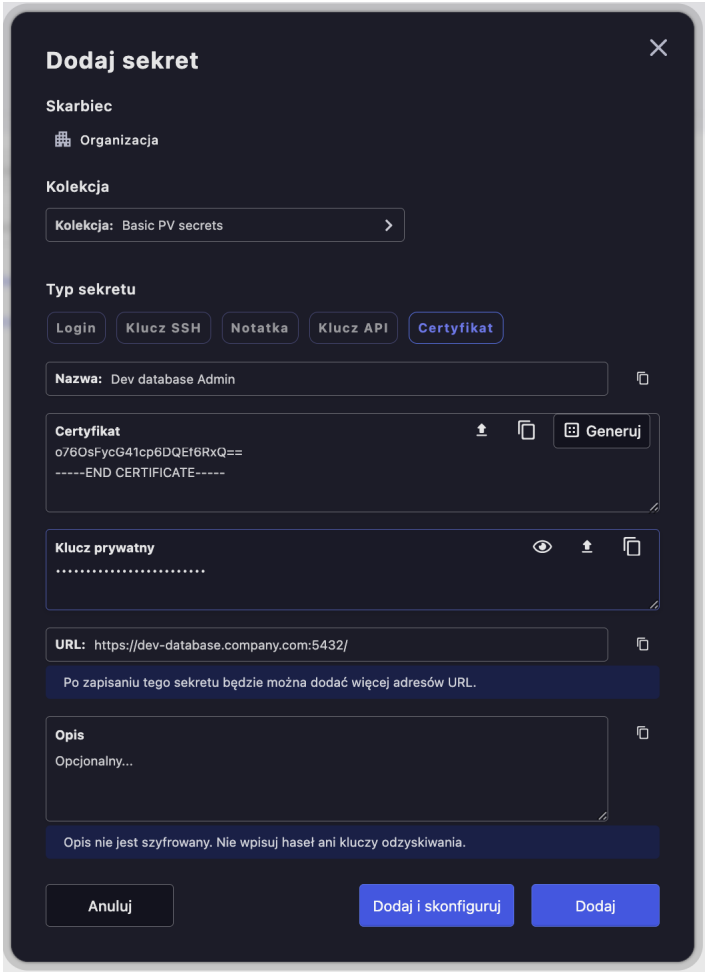
Dla sekretów typu Klucz API:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Domena: Wprowadź adres domeny docelowej lub serwera
  - Login: Wprowadź nazwę użytkownika lub konta
  - Klucz API: Wprowadź lub prześlij klucz API
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



Dla sekretów typu Certyfikat:

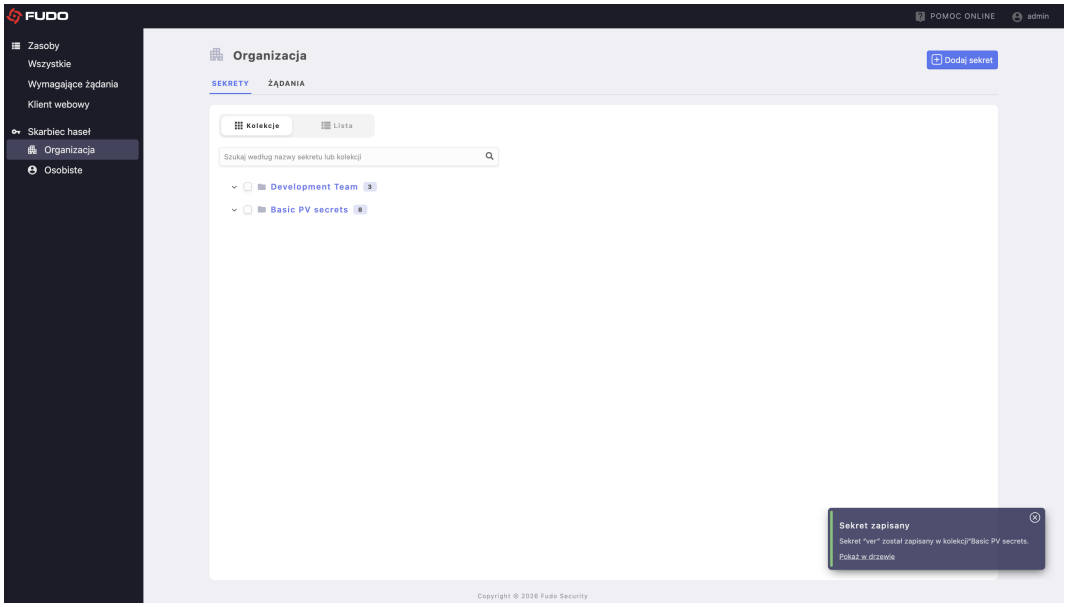
- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Certyfikat: Prześlij lub wygeneruj certyfikat
  - Klucz prywatny: Prześlij swój klucz prywatny
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



7. Kliknij *Dodaj*, aby utworzyć sekret i zamknąć okno, lub *Dodaj i skonfiguruj*, aby utworzyć sekret i otworzyć okno edycji, gdzie możesz kontynuować konfigurację.

Potwierdzenie sukcesu:

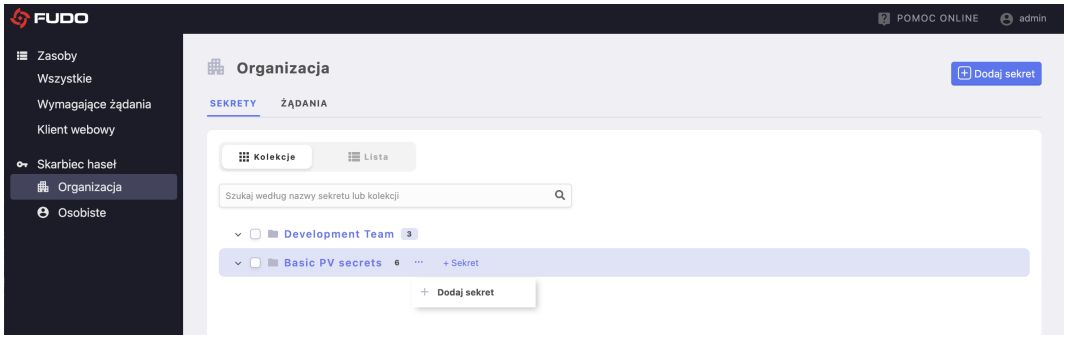
Po utworzeniu sekretu zobaczysz komunikat potwierdzający, a liczba sekretów w kolekcji zostanie zaktualizowana.



Alternatywne metody tworzenia sekretu:

Możesz również tworzyć sekrety za pomocą szybkich akcji:

1. **Z menu podręcznego po najechaniu na kolekcję**: Najedź na kolekcję i kliknij *+ Sekret*
2. **Z menu kontekstowego**: Kliknij menu trzech kropek (. . .) na kolekcji i wybierz **+ Dodaj sekret**



Dostęp do edycji sekretów

Sekrety można edytować w celu aktualizacji ich informacji, zmiany haseł, modyfikacji adresów URL lub aktualizacji opisów. Istnieje wiele sposobów dostępu do sekretów i ich edycji w Skarbcu haseł.

Metoda 1: Z widoku kolekcji

1. Przejdź do kolekcji zawierającej sekret.
2. Rozwiń kolekcję, aby wyświetlić jej sekrety.
3. Kliknij na nazwę sekretu, aby go edytować.

Metoda 2: Z widoku listy

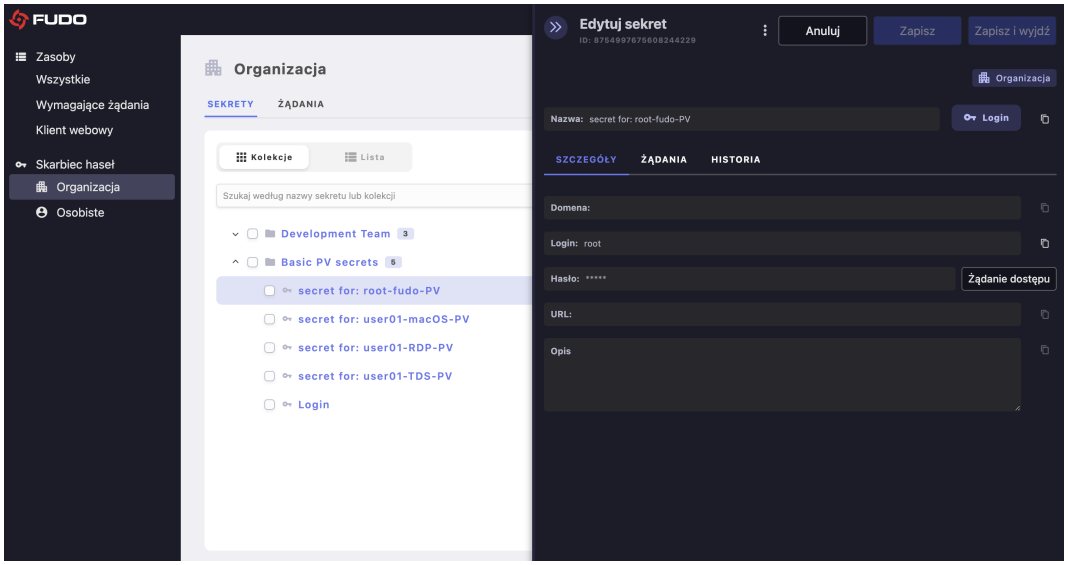
1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.
2. Kliknij *Lista*, aby przełączyć na widok listy.
3. Kliknij na nazwę sekretu, aby otworzyć panel edycji.

Panel edycji sekretu

Panel edycji sekretu zapewnia kompleksowe możliwości edycji z następującymi kartami:

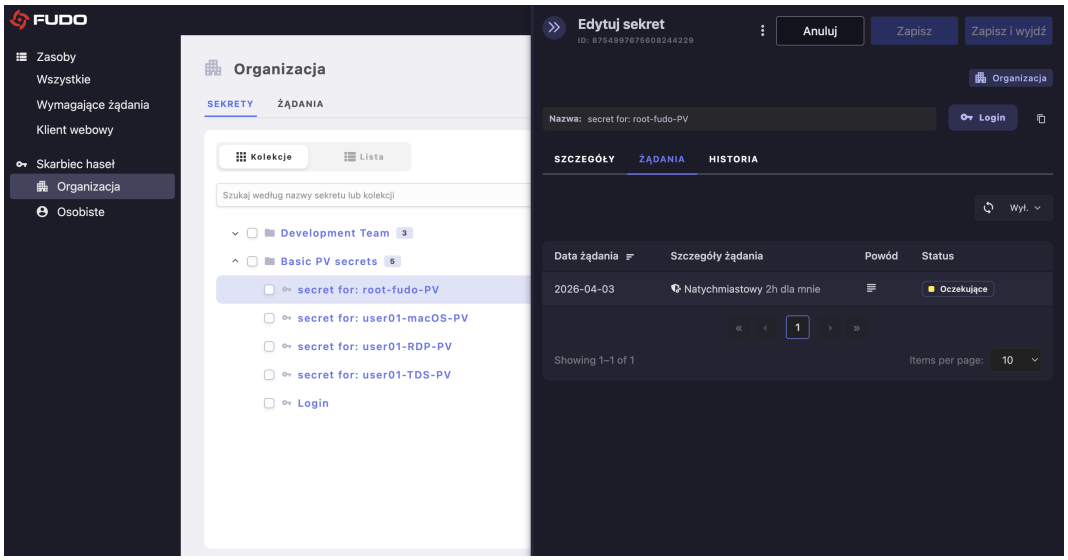
KARTA SZCZEGÓŁY

Karta Szczegóły to główny interfejs edycji informacji o sekrecie, gdzie możesz modyfikować wszystkie podstawowe atrybuty sekretu.



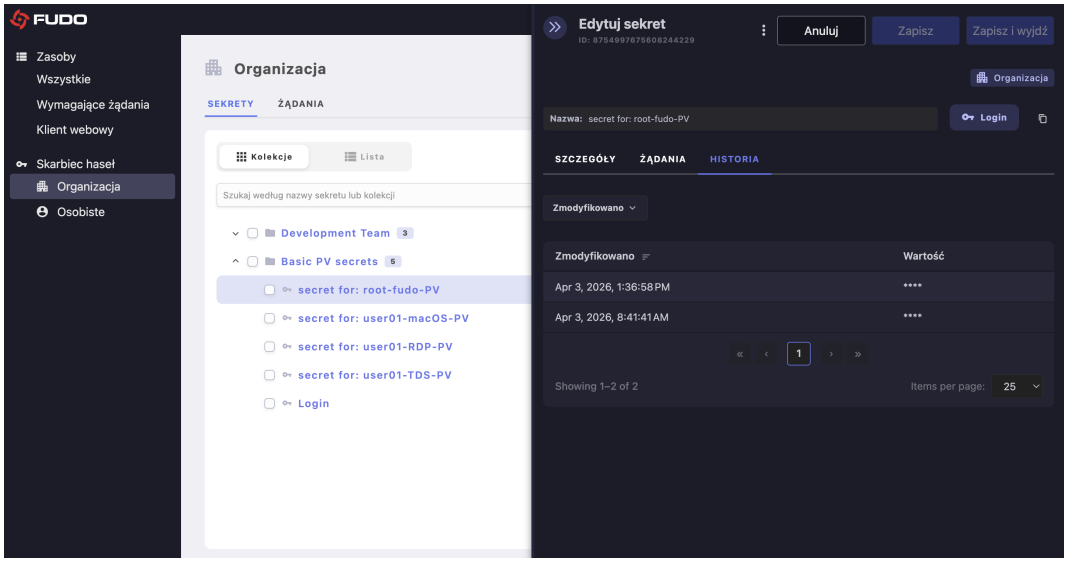
KARTA ŻĄDANIA

Karta Żądania pozwala przeglądać statusy żądań dostępu związane z wybranym sekretem.



KARTA HISTORIA

Karta Historia pozwala śledzić zmiany dokonane w wybranym sekrecie w czasie.



Przenoszenie sekretów między kolekcjami

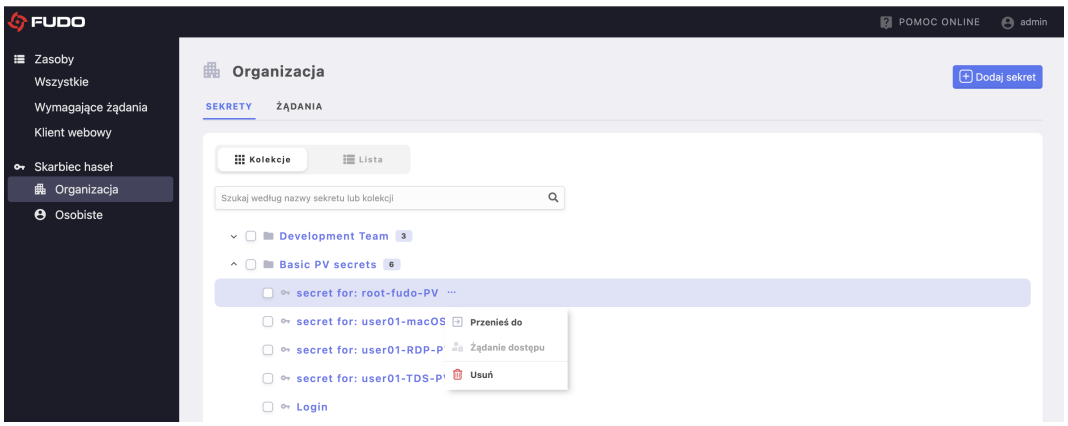
Sekrety można przenosić między kolekcjami w celu reorganizacji struktury skarbca haseł, dostosowania uprawnień dostępu lub odzwierciedlenia zmian w organizacji zespołu. Przeniesienie sekretów aktualizuje ich kontrolę dostępu na podstawie uprawnień kolekcji docelowej.

> **Uwaga**
>
> Przeniesienie sekretu do innej kolekcji zmieni jego uprawnienia dostępu na podstawie przypisań użytkowników i ról kolekcji docelowej.

Istnieje kilka metod przenoszenia sekretów między kolekcjami:

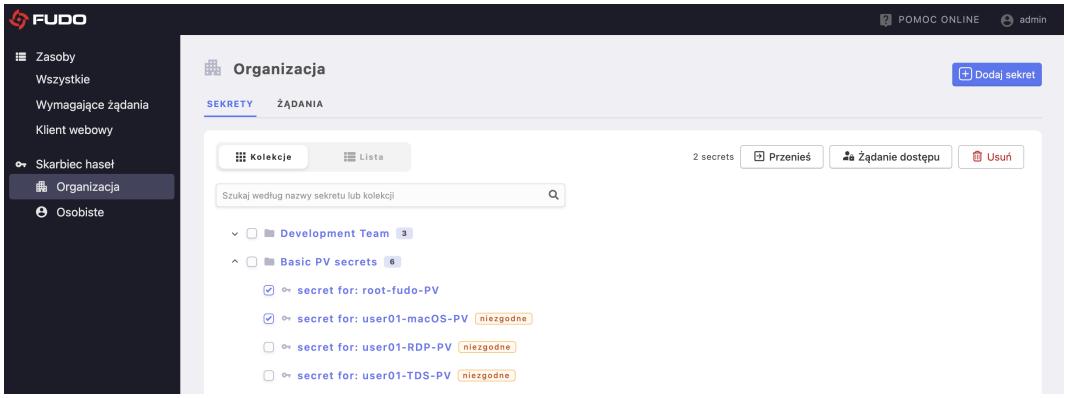
Metoda 1: Przenoszenie przy użyciu menu kontekstowego

1. Najedź kursorem na sekret, który chcesz edytować, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (...), aby otworzyć menu kontekstowe.
3. Wybierz *Przenieś do*.
4. Wybierz kolekcję docelową ze struktury drzewa.
5. Kliknij *Wybierz*, aby potwierdzić operację przeniesienia.



Metoda 2: Przenoszenie zbiorcze w widoku kolekcji

1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.
2. W widoku *Kolekcje* wybierz wiele sekretów, zaznaczając ich pola wyboru.
3. Kliknij przycisk *Przenieś*, który pojawi się na pasku akcji.
4. Wybierz kolekcję docelową ze struktury drzewa.
5. Kliknij *Wybierz*, aby potwierdzić operację przeniesienia.



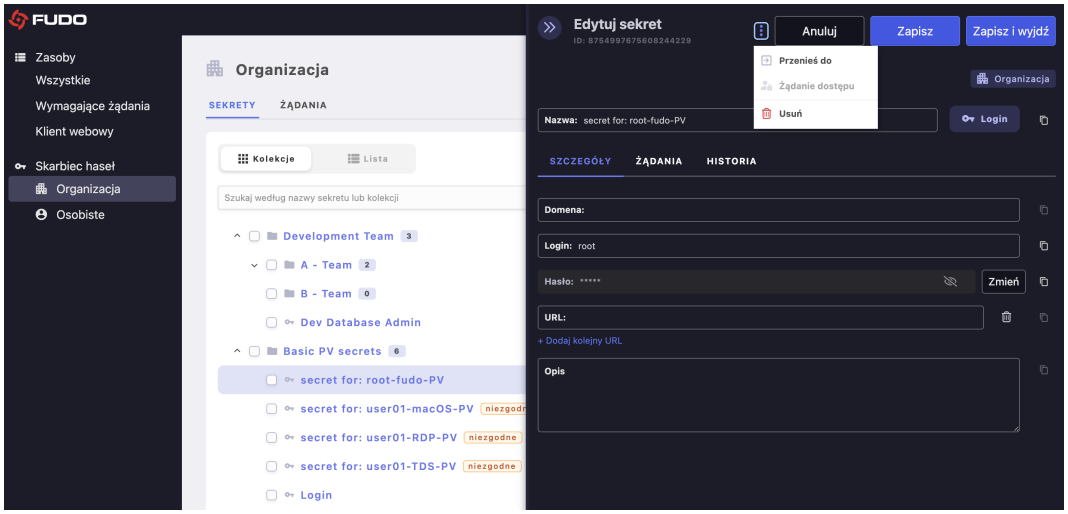
Metoda 3: Przenoszenie zbiorcze w widoku listy

Ta metoda pozwala przenosić wiele sekretów jednocześnie.

1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.
2. Kliknij *Lista*, aby przełączyć na widok listy.
3. Wybierz pola wyboru obok sekretów, które chcesz przenieść.
4. Kliknij przycisk *Przenieś*, który pojawi się na pasku akcji.
5. Wybierz kolekcję docelową ze struktury drzewa.
6. Kliknij *Wybierz*, aby potwierdzić operację przeniesienia.

Metoda 4: Przenoszenie podczas edycji

1. Otwórz dowolny sekret do edycji.
2. Kliknij przycisk trzech kropek (...) obok ID sekretu w panelu edycji i wybierz *Przenieś do*.
3. Wybierz kolekcję docelową ze struktury drzewa.
4. Kliknij *Wybierz*, aby potwierdzić operację przeniesienia.
5. Zapisz sekret.



Tematy powiązane:

- *Dodawanie nowego sekretu*
- *Dostęp do edycji sekretów*

Ujawnianie sekretu

Użytkownicy z uprawnieniami **Widok** lub **Pełna edycja** mogą ujawniać i kopiować wartości sekretów bezpośrednio z wybranego sekretu.

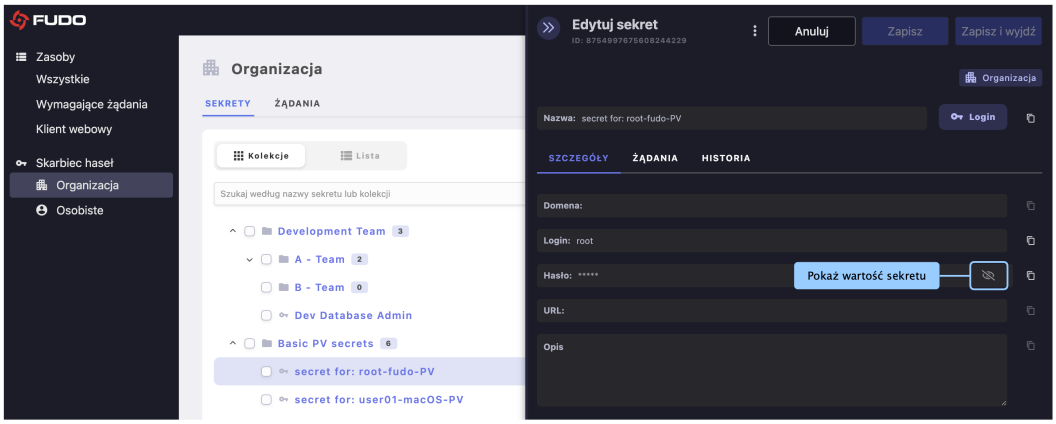
Ujawnianie ukrytych wartości

aby wywołać sekret:

1. Kliknij nazwę wybranego sekretu, aby otworzyć panel edycji sekretu.
2. Znajdź pole zawierające wartość sekretu dla wybranego typu sekretu.

> **Uwaga**
>
> Ze względów bezpieczeństwa wartości sekretów są domyślnie ukryte i są ujawniane tylko wtedy, gdy zdecydujesz się je wyświetlić.

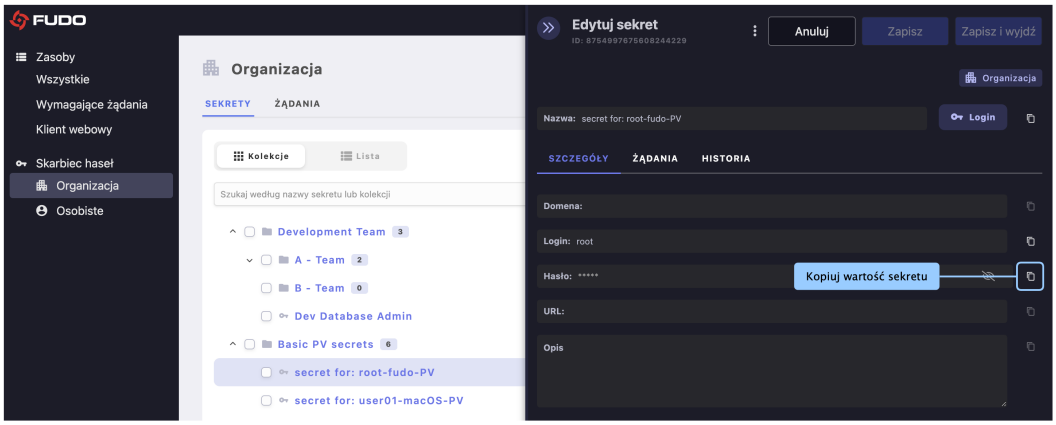
3. Kliknij **ikonę oka** obok pola wartości sekretu.
4. Sekret staje się widoczny w postaci tekstowej.
5. Kliknij ponownie ikonę oka, aby go ukryć.



Kopiowanie wartości

Aby skopiować wartość sekretu:

1. Kliknij nazwę wybranego sekretu, aby otworzyć panel edycji sekretu.
2. Znajdź pole zawierające wartość sekretu dla wybranego typu sekretu.
3. Kliknij ikonę [copy] obok pola wartości sekretu.
4. Wartość zostanie skopiowana do schowka.



Uwaga

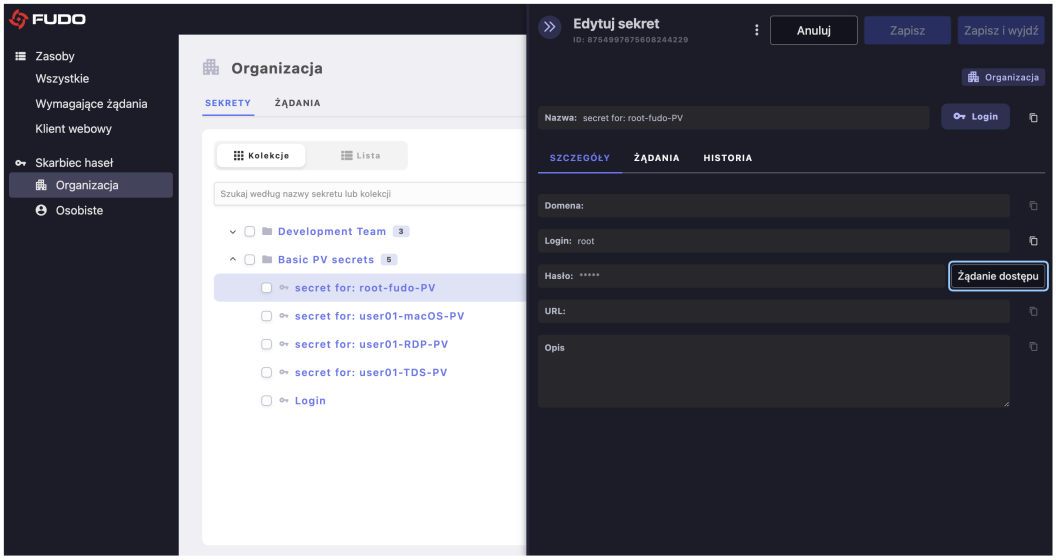
- Każda akcja ujawnienia i kopiowania jest rejestrowana w celach audytu bezpieczeństwa.
- Jeśli nie masz uprawnień **Widok** lub **Pełna edycja** dla sekretu, zobacz *Żądanie dostępu do sekretu*.

Żądanie dostępu do sekretu

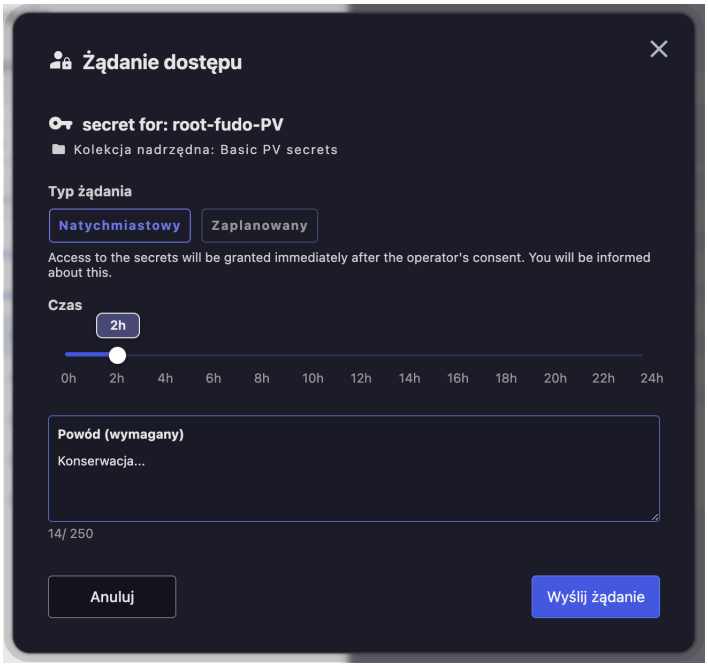
Użytkownicy z uprawnieniami **Widok na żądanie** nie mogą bezpośrednio przeglądać wartości sekretów. Aby uzyskać do nich dostęp, muszą złożyć wniosek dla wybranego sekretu. Wartości sekretów można przeglądać dopiero po zatwierdzeniu przez administratora.

Aby zażądać dostępu do sekretu:

1. Kliknij nazwę wybranego sekretu, aby otworzyć panel edycji sekretu.
2. Kliknij przycisk **Żądanie dostępu**.

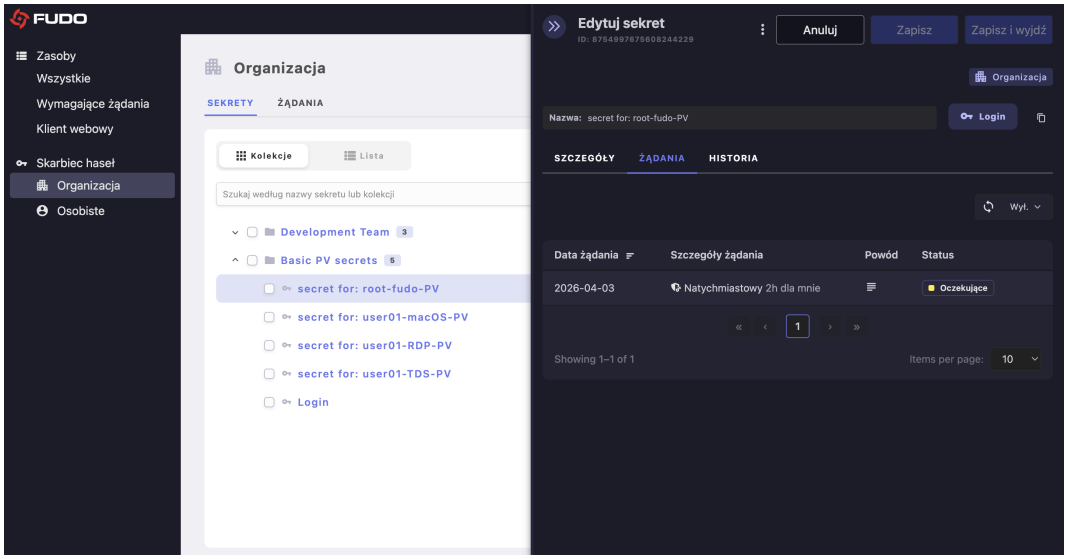


3. W oknie żądania skonfiguruj następujące pola:
   - **Typ żądania** – wybierz **Natychmiastowe** lub **Zaplanowane**
   - **Czas** – określ żądany czas dostępu
   - **Powód** – wprowadź powód żądania (wymagane)



4. Kliknij **Wyślij żądanie**.

Po wysłaniu żądania możesz śledzić jego status w karcie **ŻĄDANIA** wybranego sekretu.



Usuwanie sekretów

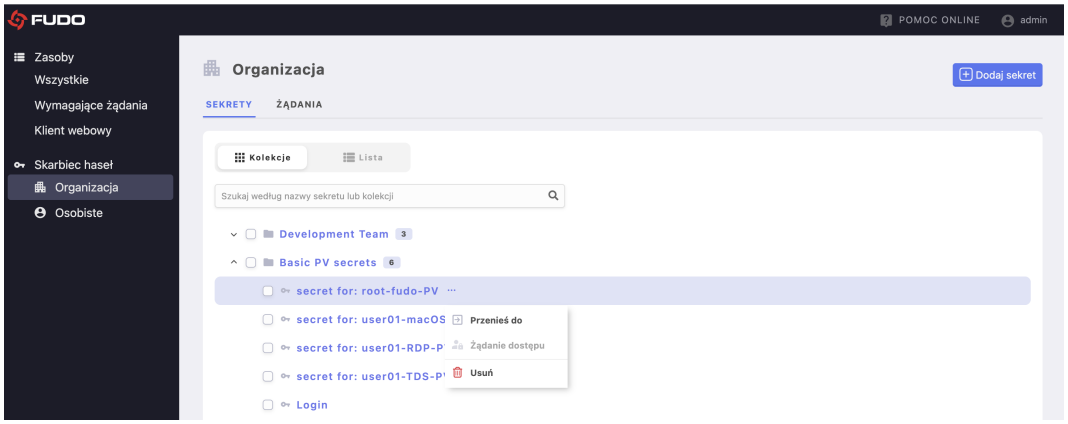
Sekrety można usuwać, gdy nie są już potrzebne lub gdy dane logowania zostały wycofane z użycia. Przed usunięciem sekretów upewnij się, że rozumiesz wpływ na użytkowników i aplikacje, które mogą od nich zależeć.

> **Ostrzeżenie**
>
> Usuwanie sekretu to trwała akcja, której nie można cofnąć. Upewnij się, że masz kopie zapasowe lub alternatywne metody dostępu przed przystąpieniem do usuwania.

Istnieje kilka metod usuwania sekretów ze Skarbca haseł:

Metoda 1: Używanie menu kontekstowego

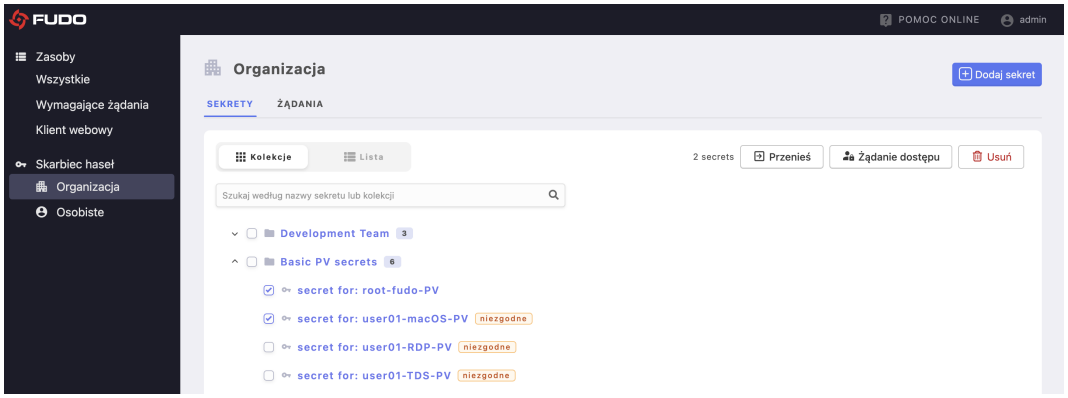
1. Najedź kursorem na sekret, który chcesz usunąć, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (...), aby otworzyć menu kontekstowe.
3. Wybierz *Usuń*.
4. Potwierdź usunięcie w oknie dialogowym ostrzeżenia.



Metoda 2: Usuwanie zbiorcze w widoku kolekcji

1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.

2. W widoku *Kolekcje* wybierz wiele sekretów, zaznaczając ich pola wyboru.
3. Kliknij przycisk *Usuń*, który pojawi się na pasku akcji.
4. Przejrzyj komunikat ostrzeżenia i potwierdź usunięcie.



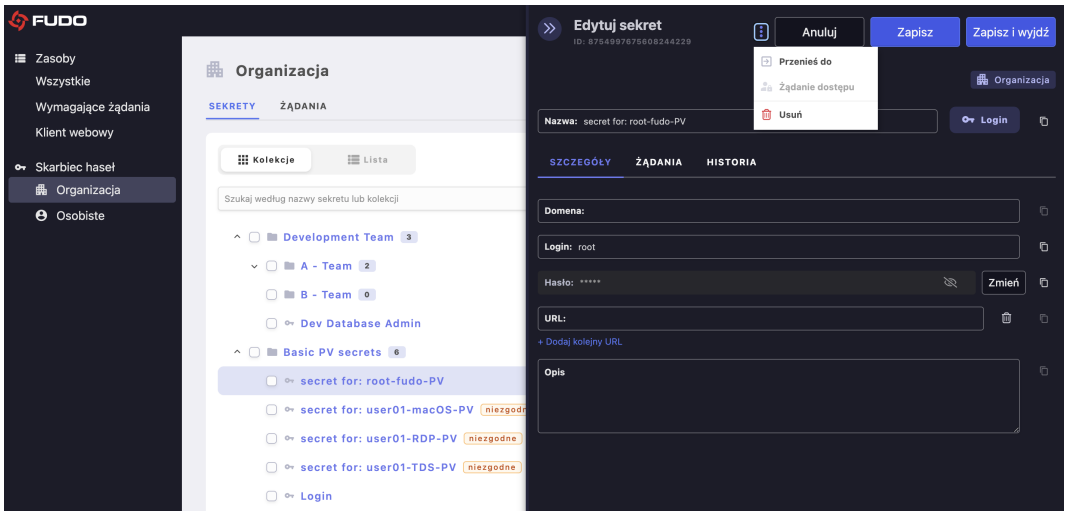
Metoda 3: Usuwanie zbiorcze w widoku listy

Ta metoda pozwala usuwać wiele sekretów jednocześnie.

1. Wybierz *Skarbiec haseł* > *Organizacja* lub *Osobiste*.
2. Kliknij *Lista*, aby przełączyć na widok listy.
3. Wybierz pola wyboru obok sekretów, które chcesz usunąć.
4. Kliknij przycisk *Usuń*, który pojawi się na pasku akcji.
5. Przejrzyj komunikat ostrzeżenia i potwierdź usunięcie.

Metoda 4: Usuwanie z panelu edycji

1. Otwórz dowolny sekret do edycji.
2. Kliknij przycisk trzech kropek (. . .) obok ID sekretu w panelu edycji.
3. Wybierz *Usuń* z menu rozwijanego.
4. Potwierdź usunięcie w oknie dialogowym ostrzeżenia.



Tematy powiązane:

- *Dodawanie nowego sekretu*
- *Dostęp do edycji sekretów*

Zgodność z polityką haseł

Polityki bezpieczeństwa haseł mogą być skonfigurowane w systemie, aby pomóc w utrzymaniu standardów organizacyjnych.

> **Uwaga**
>
> Sekret oznaczony jest statusem `niezgodny`, jeśli narusza jedną lub więcej polityk.

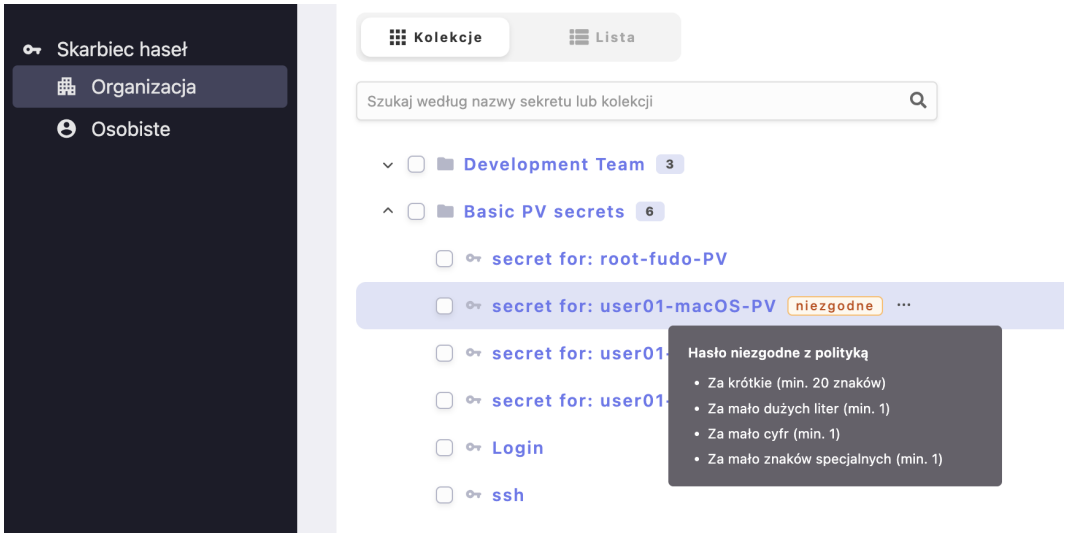
Powszechne naruszenia polityki

Sekret staje się niezgodny, gdy:

- Hasło jest za krótkie (wymóg minimalnej długości)
- Brakuje wymaganych typów znaków (wielkie litery, małe litery, cyfry, symbole)
- Hasło wygasło na podstawie harmonogramu rotacji
- Pasuje do znanych naruszonych haseł
- Ponownie używa poprzedniego hasła

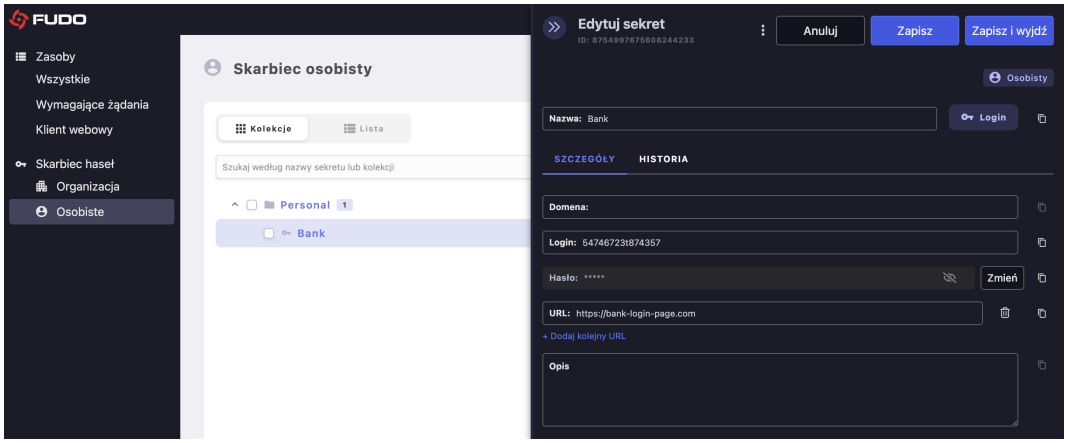
Aby zobaczyć, które wymagania polityki narusza sekret:

1. Najedź kursorem na wskaźnik `niezgodny`, aby wyświetlić podpowiedź z listą wymagań polityki, które nie są spełnione przez ten sekret.

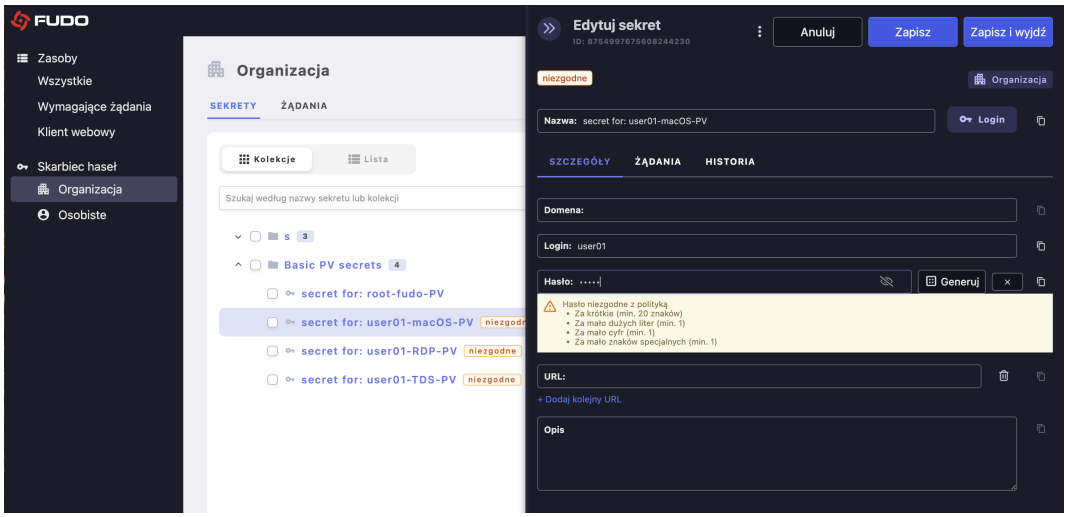


Naprawianie niezgodnych haseł

1. Otwórz niezgodny sekret.
2. Kliknij **Zmień**.



3. Lub:
   - Kliknij **Generuj**, aby uzyskać automatyczne zgodne hasło.
   - Ręcznie utwórz hasło zgodne z wyświetlanymi wymaganiami.



5. Zapisz zmiany.

1.8.5 Zarządzanie kolekcjami (Skarbiec osobisty)

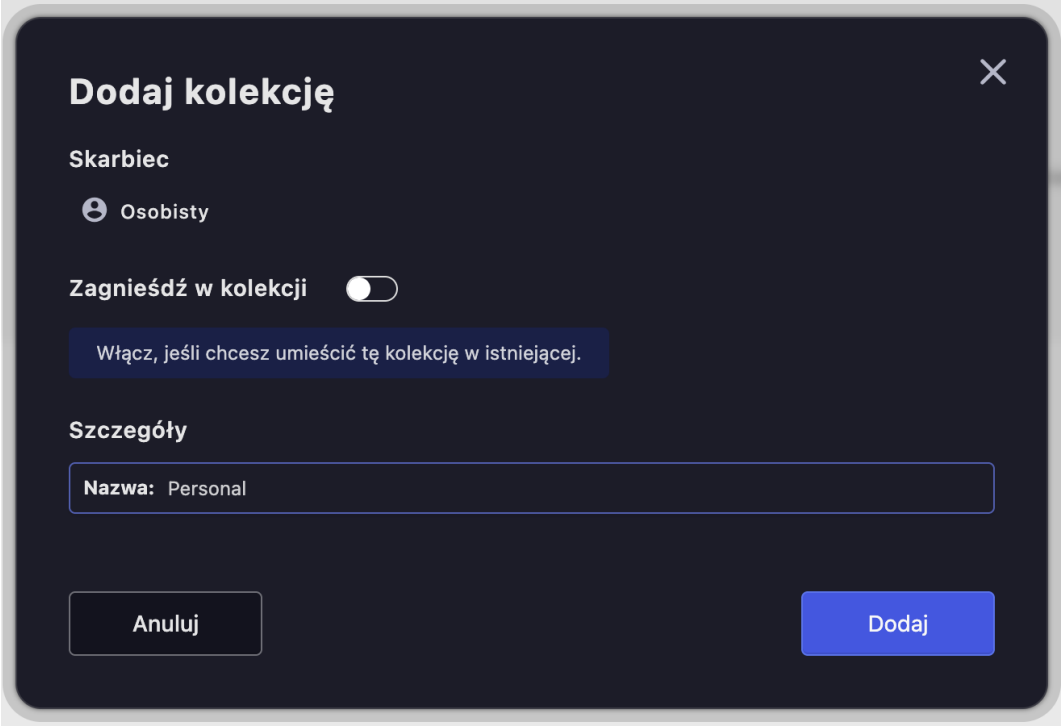
Kolekcje pomagają organizować osobiste sekrety w logiczne grupy. Zarządzanie kolekcjami jest dostępne tylko w Skarbcu osobistym.

> **Uwaga**
>
> **Kolekcje można tworzyć i zarządzać nimi tylko w Skarbcu osobistym.** Kolekcje Skarbca organizacji są zarządzane przez administratorów systemu Fudo Enterprise.

Tworzenie kolekcji

Kolekcje pomagają organizować osobiste sekrety w logiczne grupy.

1. Przejdź do *Skarbiec haseł* > *Osobiste*.
2. Kliknij *+ Dodaj kolekcję*.
3. Otwiera się okno dialogowe *Dodaj kolekcję*.



4. *Nazwa* (wymagane) - Wprowadź opisową nazwę kolekcji
5. *Zagnieździj pod kolekcją* (opcjonalne) - Przełącz na WŁĄCZONE, aby umieścić tę kolekcję w istniejącej:

- To tworzy hierarchiczną strukturę
- Pomaga organizować powiązane kolekcje

6. Kliknij Dodaj, aby utworzyć kolekcję

Edycja nazwy kolekcji

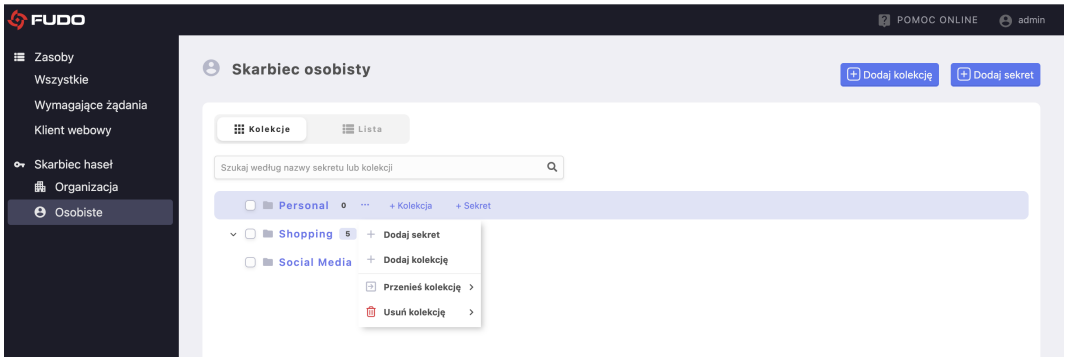
Aby edytować istniejącą kolekcję:

1. Przejdź do kolekcji w Twoim Skarbcu osobistym.
2. Kliknij na kolekcję, aby otworzyć panel edycji.
3. Zmień nazwę kolekcji.
4. Kliknij *Zapisz*, aby zastosować zmiany.

Przenoszenie kolekcji

Możesz reorganizować hierarchię kolekcji w dowolnym momencie:

1. Najedź kursorem na kolekcję, którą chcesz przenieść, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (...), aby otworzyć menu kontekstowe.
3. Wybierz *Przenieś kolekcję* z menu kontekstowego.
4. Następnie możesz wybrać, czy przenieść tylko zawartość kolekcji, czy kolekcję wraz z jej zawartością.



5. W oknie dialogowym wybierz kolekcję docelową, pod którą kolekcja zostanie zagnieżdżona, lub do której zostanie przeniesiona jej zawartość.
6. Kliknij *Wybierz*, aby na stałe usunąć kolekcję.

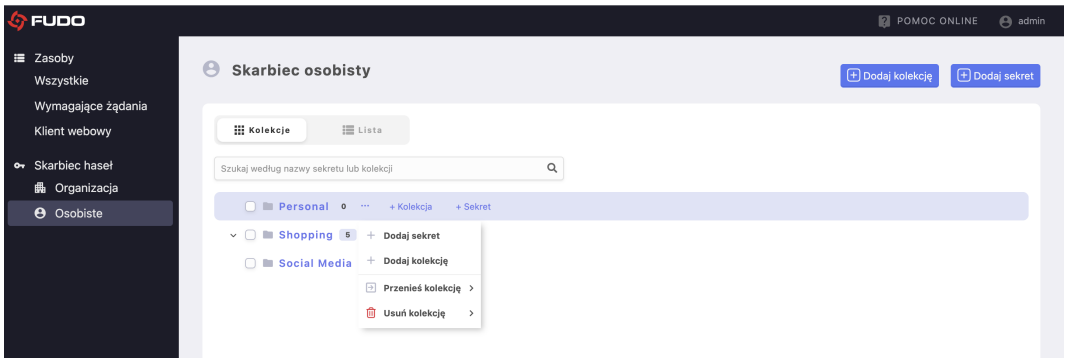
Usuwanie kolekcji

Kolekcje można usuwać, gdy nie są już potrzebne. Przed usunięciem kolekcji upewnij się, że wszystkie ważne sekrety zostały przeniesione do innych kolekcji lub zostały zarchiwizowane, ponieważ tej akcji nie można cofnąć.

Ostrzeżenie

Usuwanie kolekcji to trwała akcja, której nie można cofnąć. Wszystkie sekrety w kolekcji również zostaną usunięte, chyba że zostaną najpierw przeniesione do innej kolekcji.

1. Najedź kursorem na kolekcję, którą chcesz usunąć, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (. . .), aby otworzyć menu kontekstowe.
3. Wybierz *Usuń kolekcję* z menu kontekstowego.
4. Następnie możesz wybrać, czy usunąć tylko zawartość kolekcji, czy kolekcję wraz z jej zawartością.



5. W oknie dialogowym potwierdzenia przejrzyj nazwę kolekcji.
6. Kliknij *Usuń*, aby na stałe usunąć kolekcję.

Ostrzeżenie

Usuwanie kolekcji nadrzędnej wpływa na wszystkie zagnieżdżone kolekcje.

1.8.6 Rozszerzenie przeglądarkowe Fudo Password Vault

Rozszerzenie przeglądarkowe Fudo Password Vault umożliwia użytkownikom dostęp do sekretów przechowywanych w Fudo Enterprise bezpośrednio z obsługiwanych przeglądarek desktopowych: Chrome, Firefox i Safari.

Po zalogowaniu się przy użyciu poświadczeń użytkownika Fudo Enterprise oraz podaniu adresu Portalu Użytkownika użytkownicy mogą przeglądać dostępne kolekcje, wyszukiwać sekrety i otwierać powiązane strony internetowe bezpośrednio z poziomu rozszerzenia. Gdy formularz logowania zostanie rozpoznany, rozszerzenie może zaproponować autouzupełnienie pasującego sekretu, co przyspiesza i ułatwia dostęp do zasobów sieciowych.

Rozszerzenie obsługuje również procesy przyznawania dostępu w Skarbcu haseł. Jeśli sekret wymaga zatwierdzenia, użytkownik może poprosić o dostęp bezpośrednio z przeglądarki. Po przyznaniu dostępu na stronie wyświetlane jest powiadomienie. W przypadku sekretów z włączoną opcją rezerwacji na wyłączność rozszerzenie pokazuje, ile czasu pozostało do wygaśnięcia wypożyczenia.

Użytkownicy, którzy mają Skarbiec osobisty, mogą również tworzyć i edytować własne sekrety oraz kolekcje bezpośrednio w rozszerzeniu, bez otwierania Portalu Użytkownika w osobnej karcie.

Uwaga

Rozszerzenie jest dostępne dla klientów z pełną licencją Skarbca haseł. Obsługuje wyłącznie desktopowe wersje przeglądarek i jest dostępne w języku angielskim i polskim.

Instalacja

Zainstaluj rozszerzenie z oficjalnego sklepu z dodatkami swojej przeglądarki, a następnie przypnij je do paska narzędzi, aby mieć do niego szybki dostęp.

Chrome i inne przeglądarki oparte na Chromium

Zainstaluj rozszerzenie ze sklepu Chrome Web Store. Jeśli link jest niedostępny, wyszukaj w sklepie **Password Vault** firmy Fudo Security.

Firefox

Zainstaluj rozszerzenie ze sklepu Firefox Add-ons. Jeśli link jest niedostępny, wyszukaj w sklepie **Fudo Password Vault**.

Safari

Zainstaluj rozszerzenie ze sklepu Mac App Store, a następnie włącz je w *Safari* > *Ustawienia* > *Rozszerzenia*. Jeśli link jest niedostępny, wyszukaj w sklepie **Fudo Password Vault**.

Uwaga

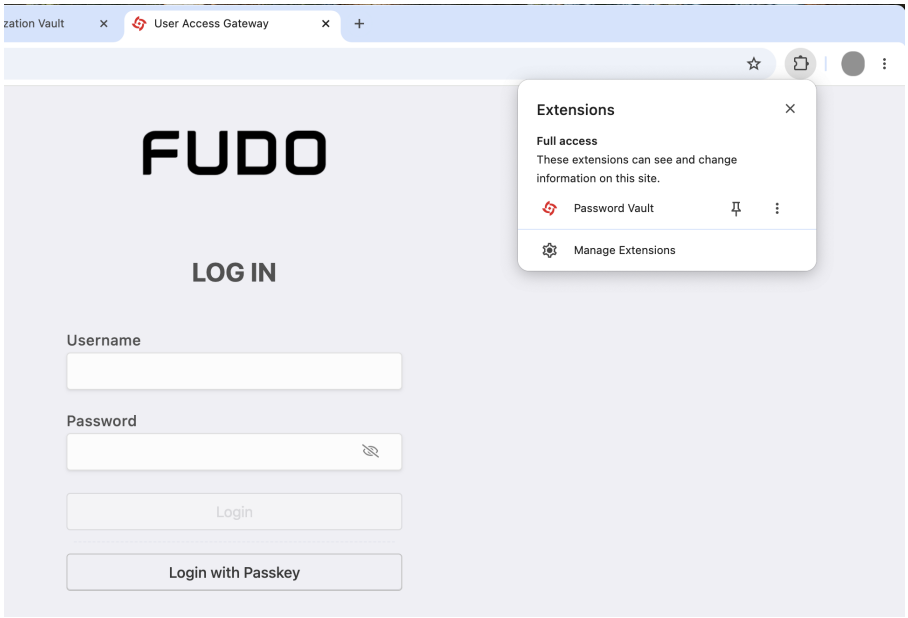
Safari wymaga dodatkowo nadania rozszerzeniu dostępu do witryn. Aby nadać dostęp:

1. Otwórz *Safari* > *Ustawienia* (*Cmd+,*) > *Rozszerzenia*.

2. Wybierz **Password Vault** na pasku bocznym po lewej stronie.
3. Kliknij **Edytuj witryny...**.
4. Na dole listy ustaw **Podczas odwiedzania innych witryn:** na **Zezwól**.
5. Zamknij Ustawienia.

Uruchamianie rozszerzenia

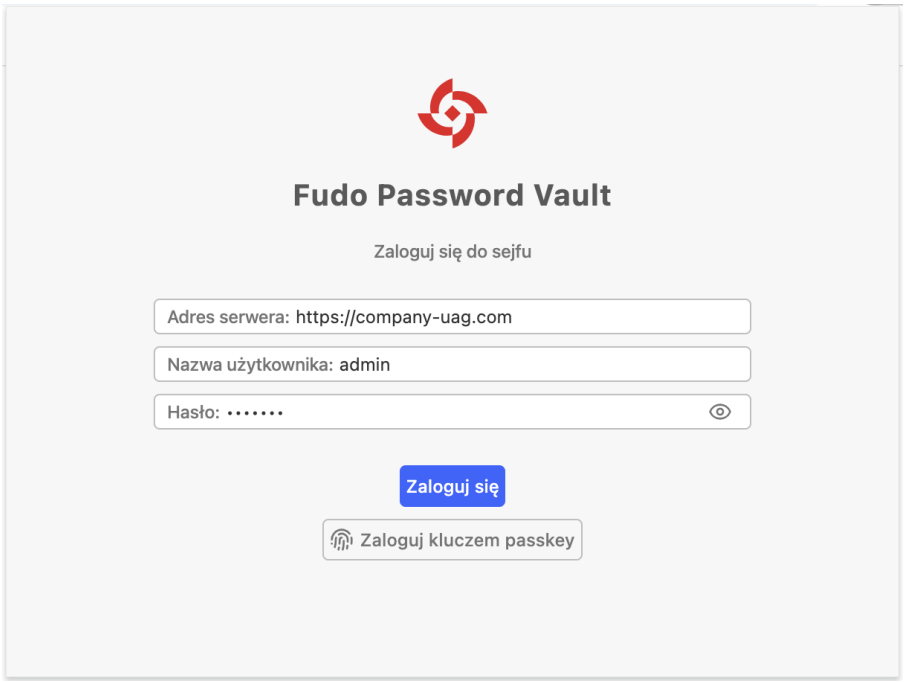
Po instalacji otwórz rozszerzenie z paska narzędzi przeglądarki. W przeglądarce Chrome kliknij ikonę **Rozszerzenia** (puzzel), a następnie wybierz **Password Vault**; możesz też przypiąć rozszerzenie do paska narzędzi, aby mieć do niego szybszy dostęp.



Logowanie

Aby rozpocząć korzystanie z rozszerzenia:

1. Otwórz rozszerzenie z paska narzędzi przeglądarki.
2. W polu **Adres serwera** wpisz adres Portalu Użytkownika swojej instancji Fudo Enterprise.
3. Podaj **Nazwę użytkownika** i **Hasło** użytkownika Fudo Enterprise.
4. Kliknij **Zaloguj się**.



Uwaga

Połączenie z Portalem Użytkownika musi używać protokołu HTTPS z publicznie zaufanym certyfikatem (wystawionym przez publiczny urząd certyfikacji).

Po zalogowaniu rozszerzenie łączy się z Portalem Użytkownika Fudo Enterprise i wyświetla sekrety, do których masz dostęp.

Logowanie kluczem passkey

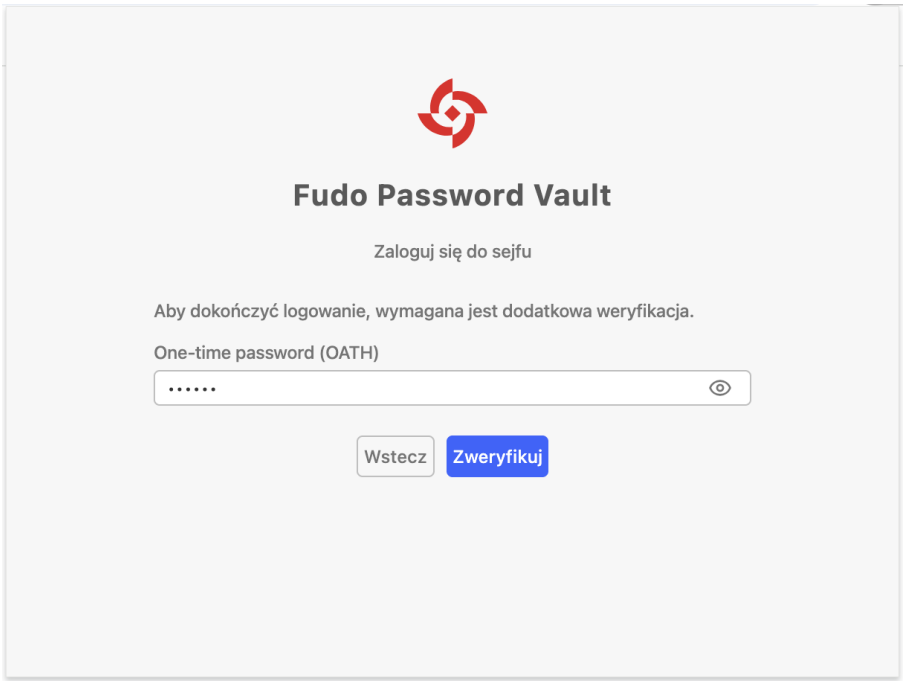
Jeśli Twoje konto jest skonfigurowane do uwierzytelniania FIDO2/Passkey, zamiast podawać hasło kliknij **Zaloguj kluczem passkey** pod przyciskiem **Zaloguj się**. Przeglądarka poprosi wtedy o klucz passkey i dokończy logowanie.

Uwaga

Logowanie kluczem passkey działa wyłącznie wtedy, gdy w polu **Adres serwera** podano nazwę hosta (FQDN), a nie adres IP - przeglądarka nie użyje klucza passkey dla adresu takiego jak `https://192.168.1.10/`. Szczegóły opisano w rozdziale o uwierzytelnianiu FIDO2/Passkey.

Podawanie drugiego składnika uwierzytelniania

Jeśli Twoje konto wymaga drugiego składnika uwierzytelniania, po wysłaniu poświadczeń rozszerzenie zastępuje formularz logowania ekranem weryfikacji. Ekran wskazuje metodę, której oczekuje serwer - na przykład **One-time password (OATH)** - i udostępnia pole na odpowiedź. Metody wymagające rejestracji tokenu wyświetlają dodatkowo kod QR do rejestracji tokenu.



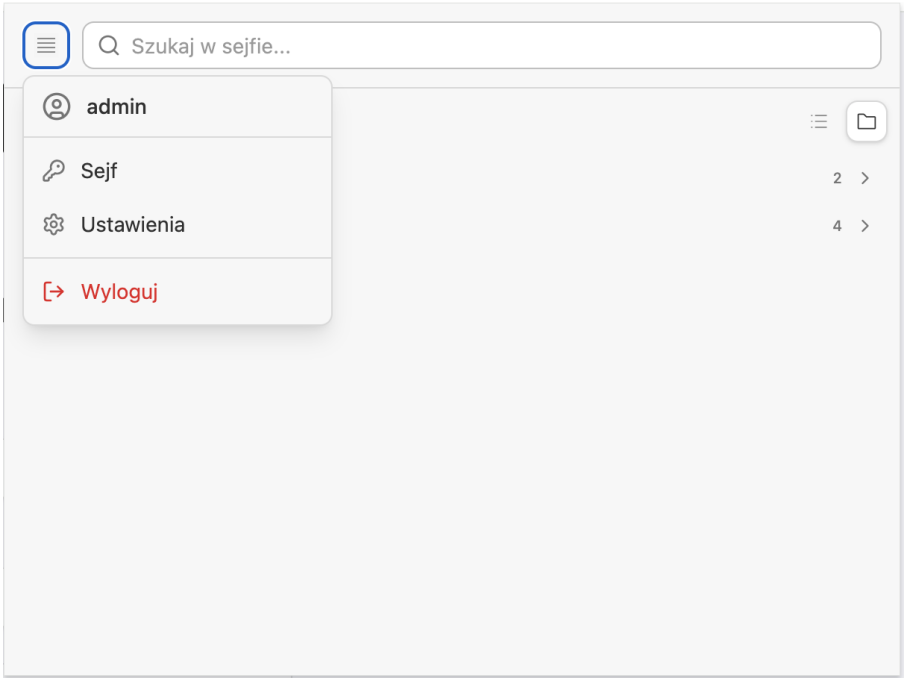
Wpisz kod z używanej metody uwierzytelniania i kliknij **Zweryfikuj** lub kliknij **Wstecz**, aby wrócić do formularza logowania. Jeśli kod nie zostanie zaakceptowany, próba logowania jest anulowana i trzeba zacząć od nowa przyciskiem **Wróć do logowania**.

Ważne

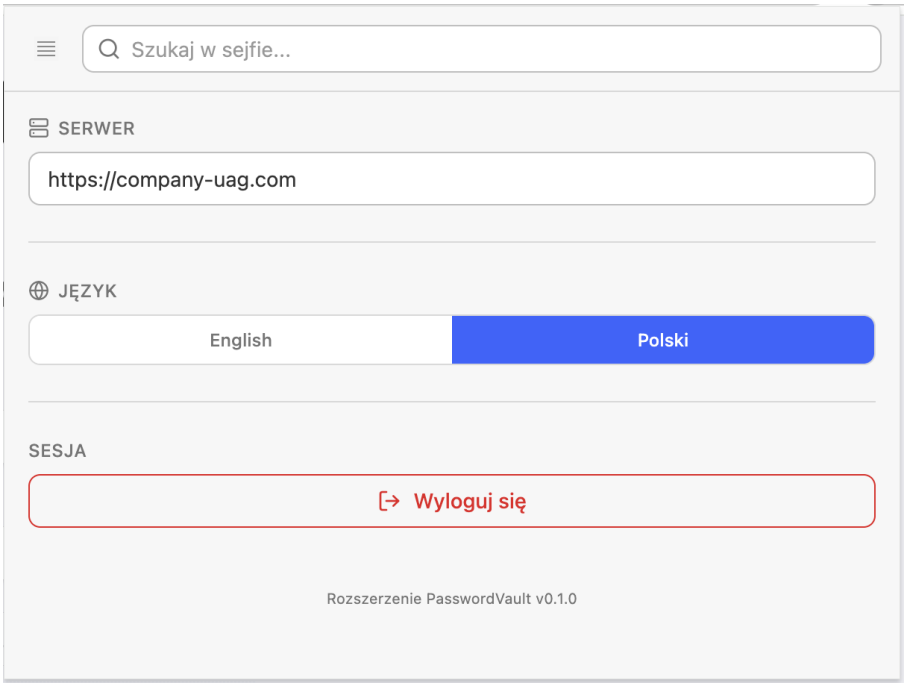
Dostępne metody drugiego składnika wynikają z konfiguracji Twojego konta w Panelu administracyjnym Fudo Enterprise. Rozszerzenie niczego nie konfiguruje - realizuje wyłącznie to, czego wymaga serwer.

Menu i ustawienia rozszerzenia

Przycisk menu w lewym górnym rogu otwiera menu rozszerzenia, które daje dostęp do **Sejfu**, **Ustawień** oraz opcji **Wyloguj**.

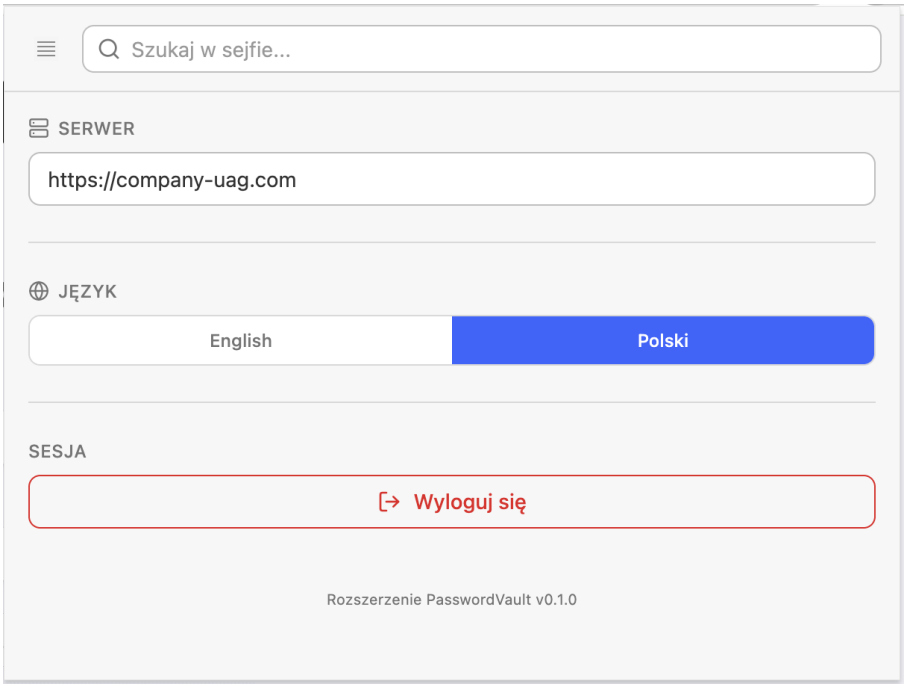


Na ekranie **Ustawienia** możesz sprawdzić adres **Serwera** (Portalu Użytkownika) oraz przełączyć **Język** interfejsu między angielskim a polskim.



Wylogowanie

Aby zakończyć sesję, otwórz menu rozszerzenia i wybierz **Wyloguj** lub kliknij **Wyloguj się** w obszarze **Sesja** na ekranie **Ustawienia**.



Przeglądanie kolekcji i sekretów

Po zalogowaniu możesz przełączać się między **widokiem kolekcji** a **widokiem listy sekretów** za pomocą przycisków w prawym górnym rogu, ograniczyć listę do jednego skarbca przyciskami **Wszystkie** / **Organizacja** / **Osobiste** oraz używać pola **Szukaj w sejfie**, aby znaleźć sekret po nazwie.

Ważne

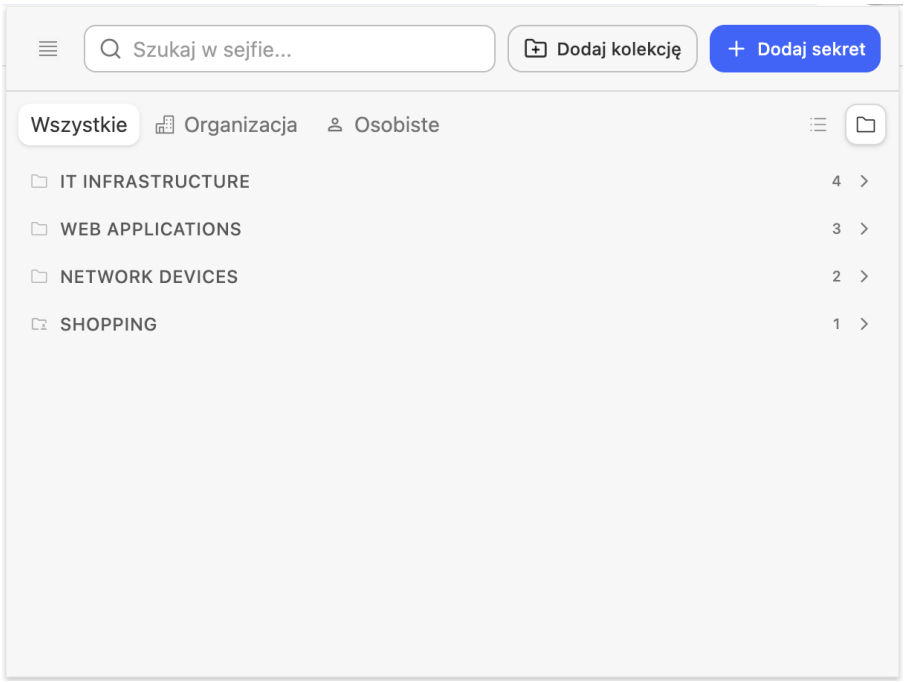
Rozszerzenie odzwierciedla te same uprawnienia, które skonfigurowano w Skarbcu haseł: widzisz wyłącznie te kolekcje i sekrety, do których przyznano Ci dostęp za pomocą praw do obiektu.

Filtrowanie według skarbca

Przyciski nad listą ograniczają ją do sekretów z jednego skarbca:

- **Wszystkie** - sekrety z obu skarbców. To ustawienie domyślne.
- **Organizacja** (ikona budynku) - wyłącznie sekrety ze Skarbca organizacji.
- **Osobiste** (ikona osoby) - wyłącznie Twoje sekrety ze Skarbca osobistego.

Przy aktywnym filtrze **Wszystkie** oba rodzaje nadal można rozróżnić: w widoku listy każdy sekret ma ikonę swojego skarbca, a w widoku kolekcji kolekcje osobiste mają inną ikonę folderu niż kolekcje organizacji.

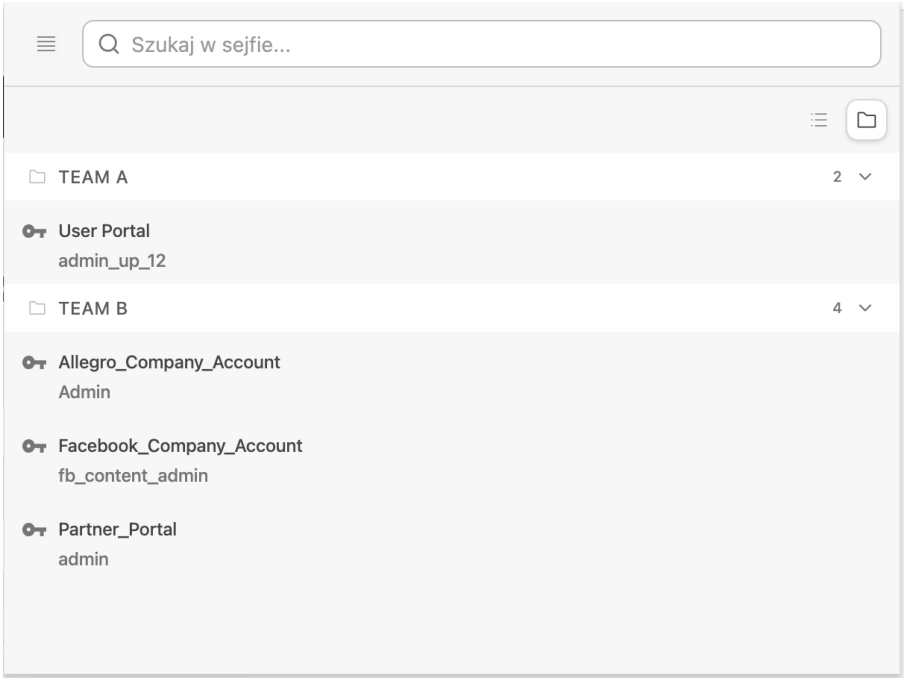


Ważne

Pole **Szukaj w sejfie** przeszukuje **wyłącznie wybrany skarbiec**. Przy wybranym filtrze **Osobiste** nie znajdziesz sekretu organizacji i odwrotnie. Jeśli w wynikach brakuje spodziewanego sekretu, przełącz filtr z powrotem na **Wszystkie**.

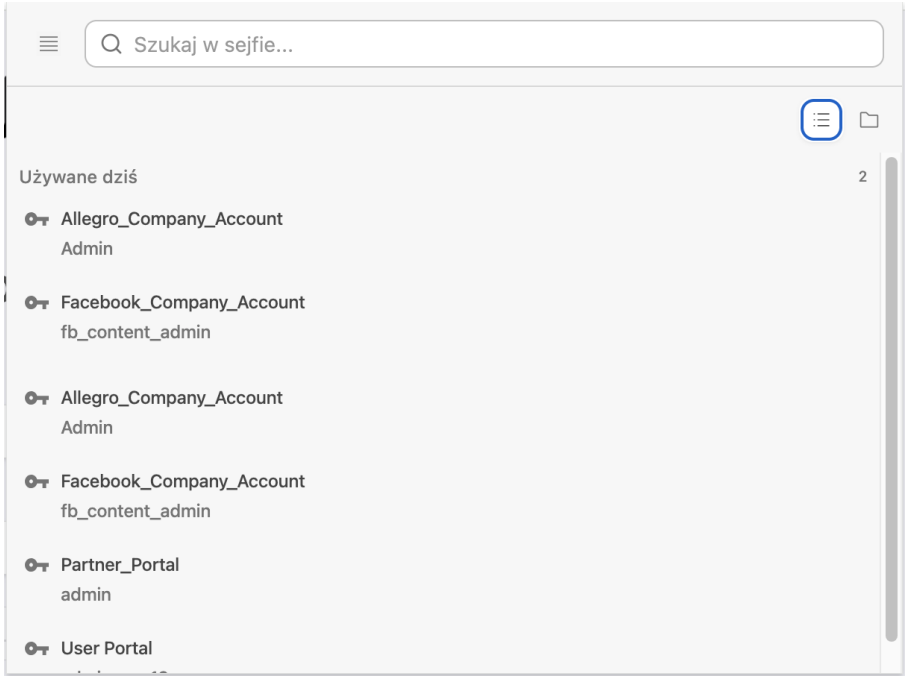
Widok kolekcji

Widok kolekcji grupuje sekrety w ramach kolekcji, do których należą.



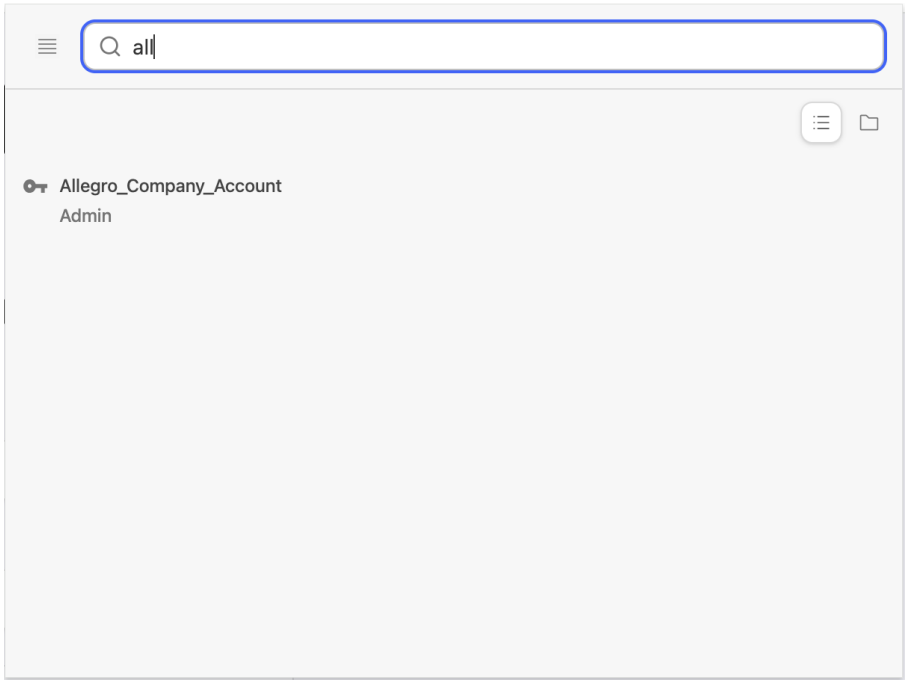
Widok listy sekretów

Widok listy pokazuje wszystkie dostępne sekrety na jednej płaskiej liście.



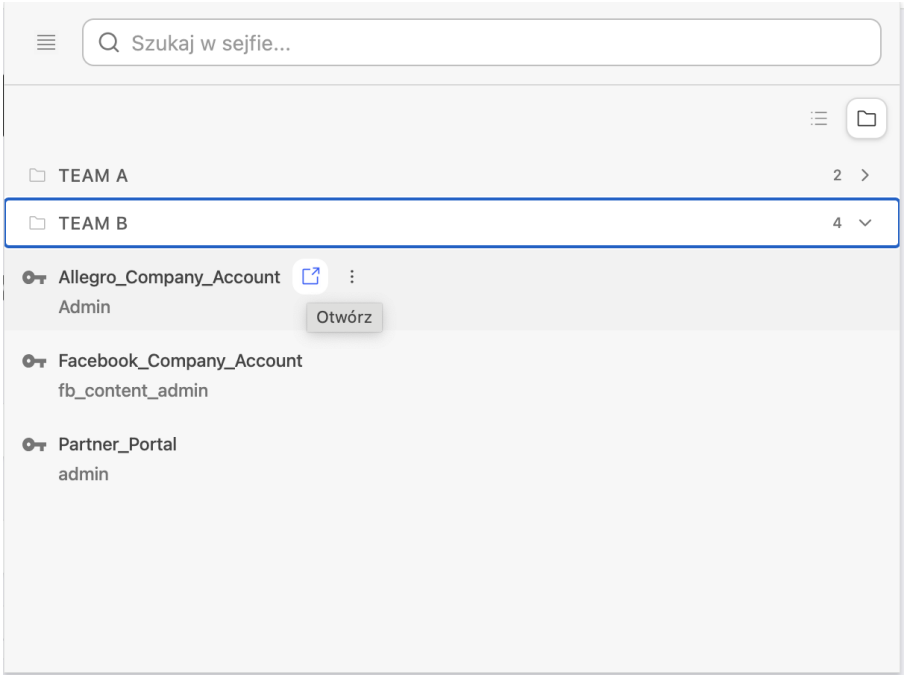
Wyszukiwanie

Wpisz tekst w polu **Szukaj w sejfie**, aby filtrować sekrety po nazwie. Wyszukiwanie obejmuje wyłącznie skarbiec wybrany przyciskami **Wszystkie** / **Organizacja** / **Osobiste**.



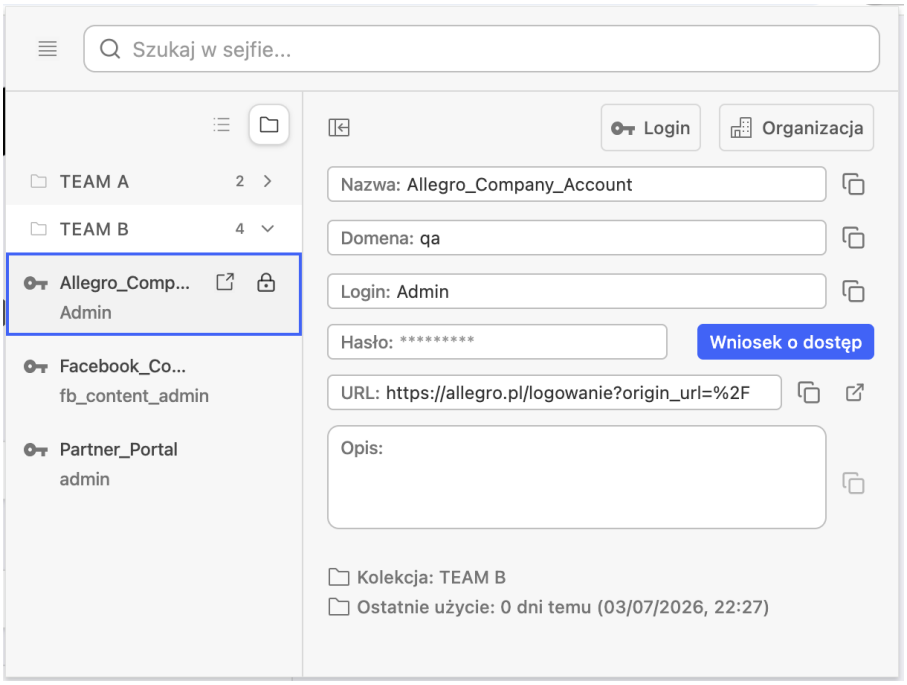
Otwieranie powiązanej strony

Przy każdym sekrecie widoczna jest ikona **Otwórz**, która prowadzi do strony powiązanej z sekretem. Kliknięcie jej otwiera powiązaną stronę bezpośrednio w przeglądarce.



Podgląd szczegółów sekretu

Wybranie sekretu otwiera jego szczegóły, gdzie możesz przejrzeć pola takie jak **Nazwa**, **Domena**, **Login**, **Hasło**, **URL** i **Opis** oraz skopiować poszczególne wartości do schowka.



Uwaga

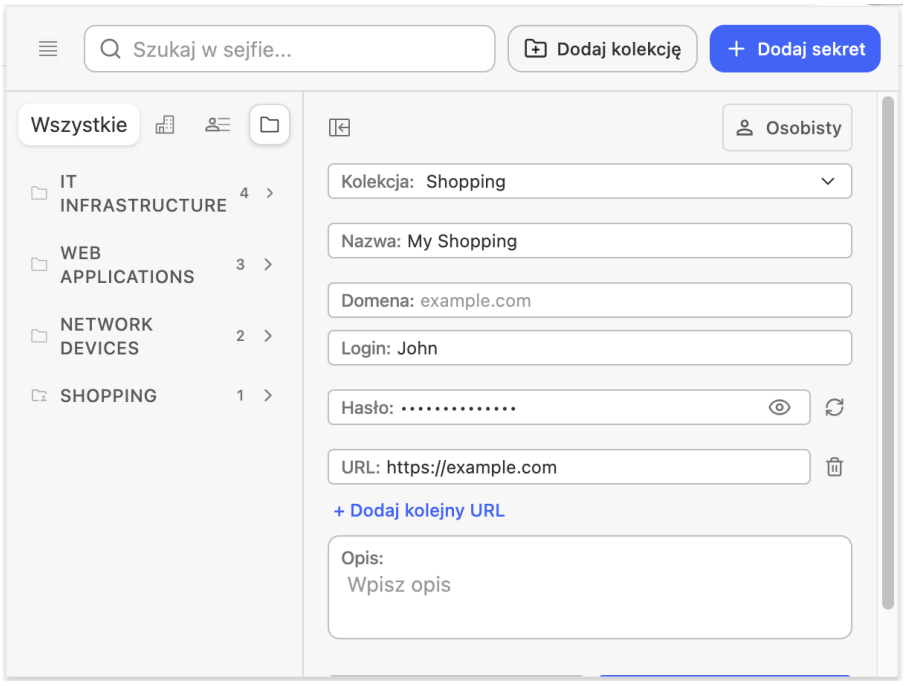
Hasło skopiowane do schowka jest automatycznie usuwane po 30 sekundach.

Tworzenie i edycja sekretów osobistych

Sekrety i kolekcje utworzone w rozszerzeniu zawsze trafiają do Twojego **Skarbca osobistego**. Zawartością Skarbca organizacji zarządzają administratorzy w Panelu administracyjnym Fudo Enterprise i nie można jej tworzyć ani edytować z poziomu przeglądarki.

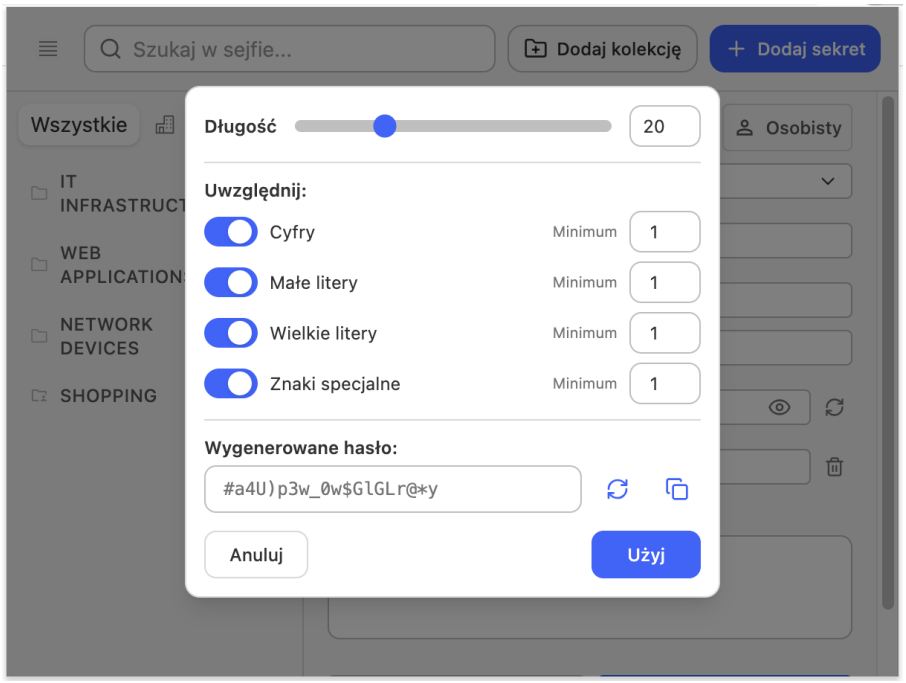
Tworzenie sekretu

1. Kliknij **Dodaj sekret** na górnym pasku.
2. Wybierz **Kolekcję**, do której ma trafić sekret. Na liście są wyłącznie kolekcje osobiste. Jeśli nie masz jeszcze żadnej, formularz wyświetla komunikat **Brak dostępnych kolekcji osobistych** - najpierw utwórz kolekcję.
3. Wypełnij pola sekretu:
   - **Nazwa** (wymagane) - nazwa, pod którą sekret jest widoczny na liście.
   - **Domena** - domena, do której należą poświadczenia.
   - **Login** (wymagane) - nazwa użytkownika zapisana w sekrecie.
   - **Hasło** (wymagane) - hasło zapisane w sekrecie.
   - **URL** - adres, z którym sekret jest dopasowywany podczas autouzupełniania. Kliknij + **Dodaj kolejny URL**, aby zapisać więcej adresów.
   - **Opis** - opcjonalne notatki.
4. Kliknij **Zapisz**.



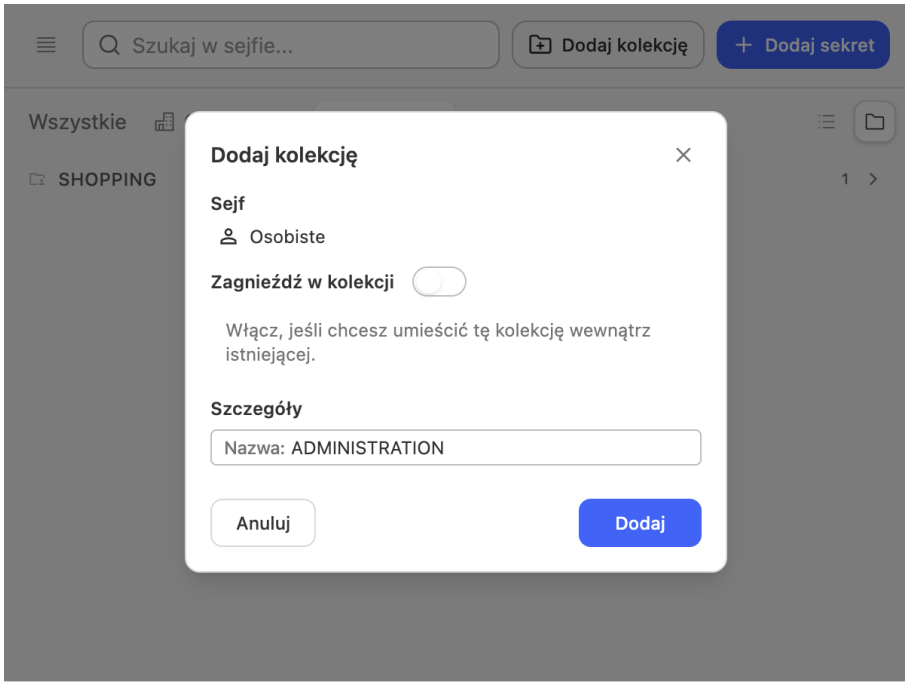
Generowanie hasła

Zamiast wpisywać hasło, kliknij ikonę generatora obok pola **Hasło**. W otwartym oknie ustaw **Długość**, włącz grupy znaków, które chcesz **Uwzględnić** (**Cyfry**, **Małe litery**, **Wielkie litery**, **Znaki specjalne**), oraz **Minimum** znaków z każdej z nich. Wynik pojawia się w polu **Wygenerowane hasło** - ikonami obok możesz wylosować kolejne hasło lub skopiować je do schowka, a przyciskiem **Użyj** wstawić je do formularza.



Tworzenie kolekcji

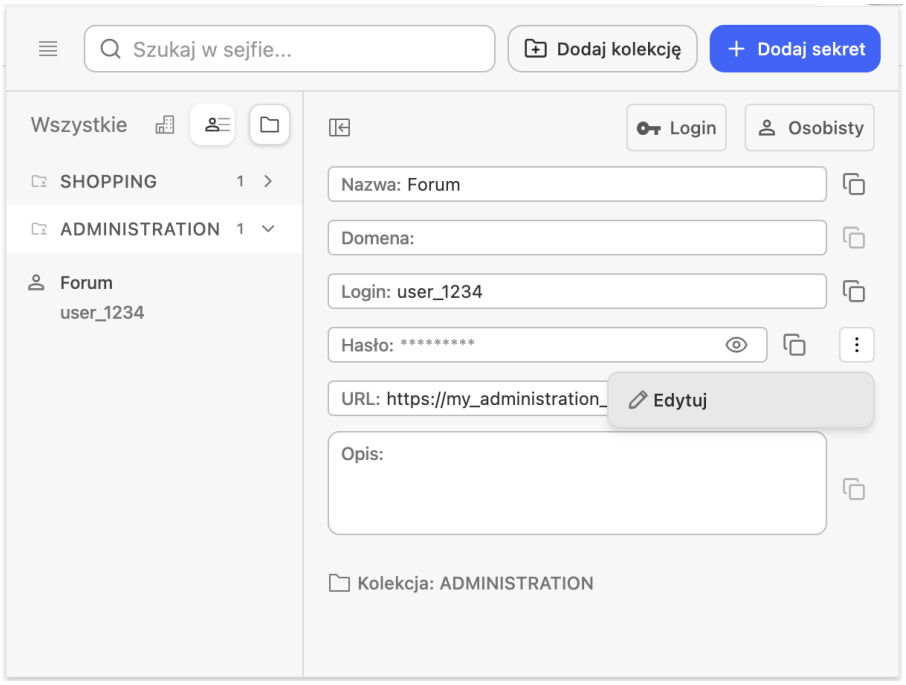
1. Kliknij **Dodaj kolekcję** na górnym pasku.
2. Pole **Sejf** ma zawsze wartość **Osobiste** i nie można go zmienić.
3. Aby umieścić nową kolekcję wewnątrz istniejącej, włącz opcję **Zagnieźdź w kolekcji** i wybierz kolekcję nadrzędną.
4. W sekcji **Szczegóły** wpisz **Nazwę** kolekcji.
5. Kliknij **Dodaj**.



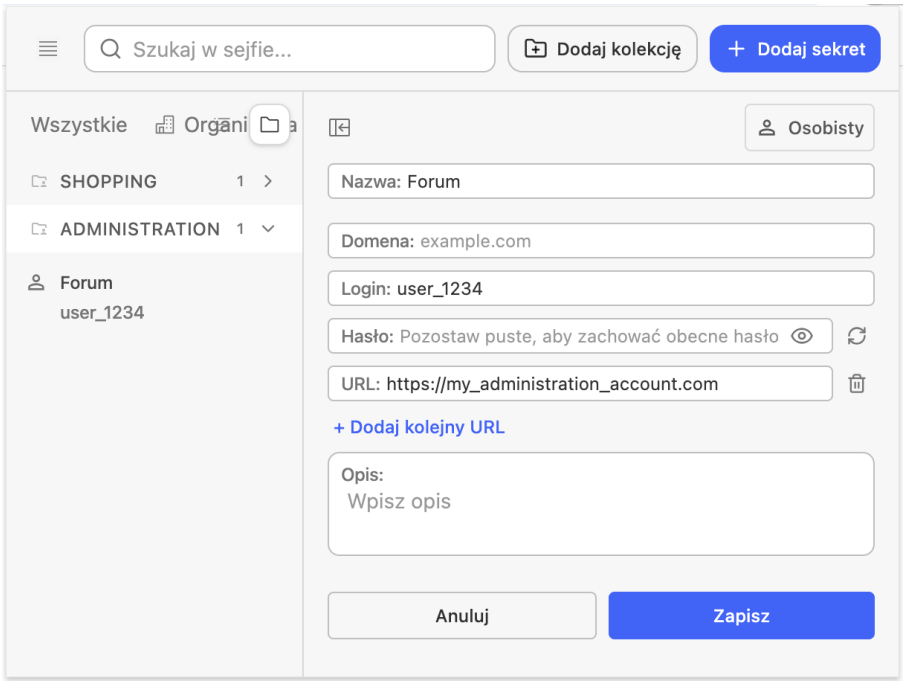
Edycja sekretu

Otwórz sekret osobisty, kliknij przycisk z trzema kropkami (**Więcej akcji**) obok pola **Hasło** i

wybierz **Edytuj**.



Formularz jest taki sam jak przy tworzeniu sekretu, z tą różnicą, że nie można zmienić kolekcji. Pozostaw pole **Hasło** puste, aby zachować obecne hasło.

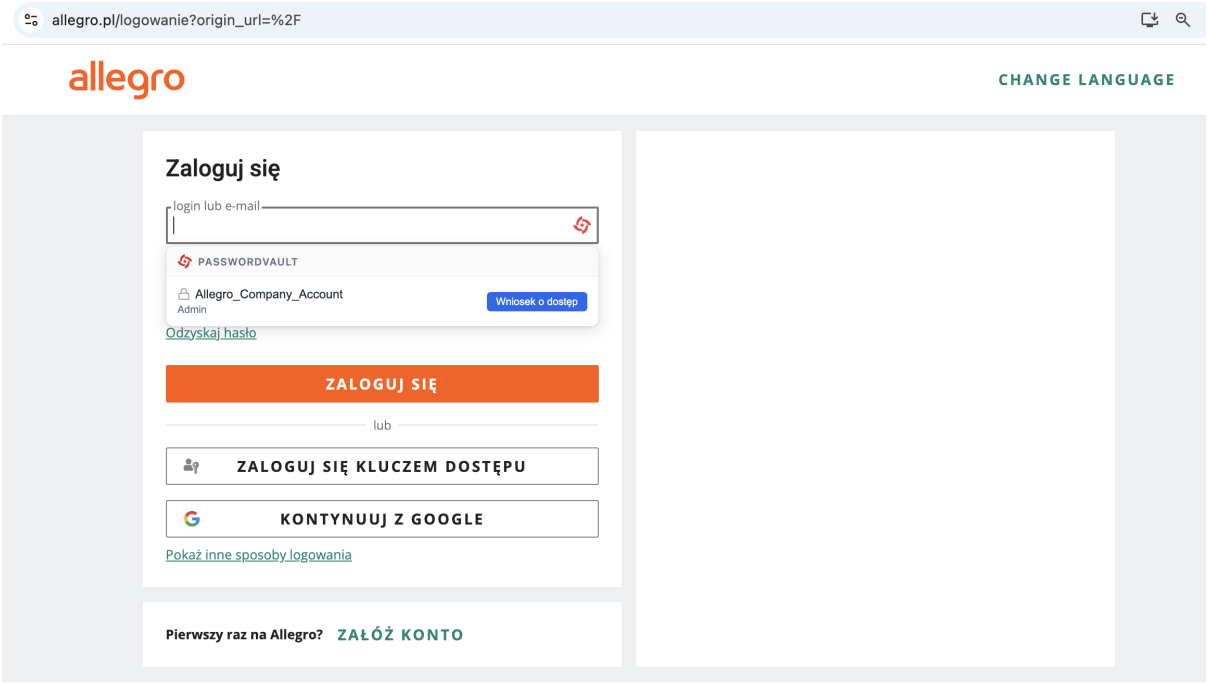


Uwaga

Opcja **Edytuj** jest dostępna wyłącznie dla sekretów ze Skarbca osobistego. Dla sekretów organizacji menu **Więcej akcji** nie zawiera pozycji **Edytuj**.

Autouzupełnianie danych logowania na stronach

Gdy otworzysz stronę, której formularz logowania zostanie rozpoznany, rozszerzenie wyświetla pasek podpowiedzi z propozycją autouzupełnienia pasującego sekretu. Wybranie podpowiedzi wypełnia zapisane poświadczenia, co przyspiesza i ułatwia dostęp do zasobów sieciowych.

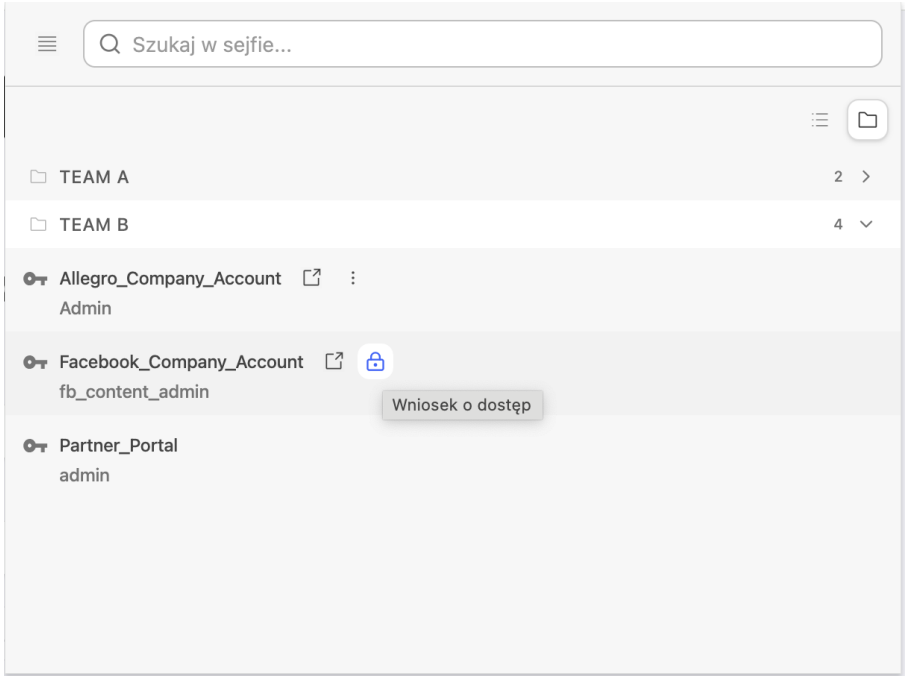


Wnioski o dostęp, rezerwacja na wyłączność i odebrany dostęp

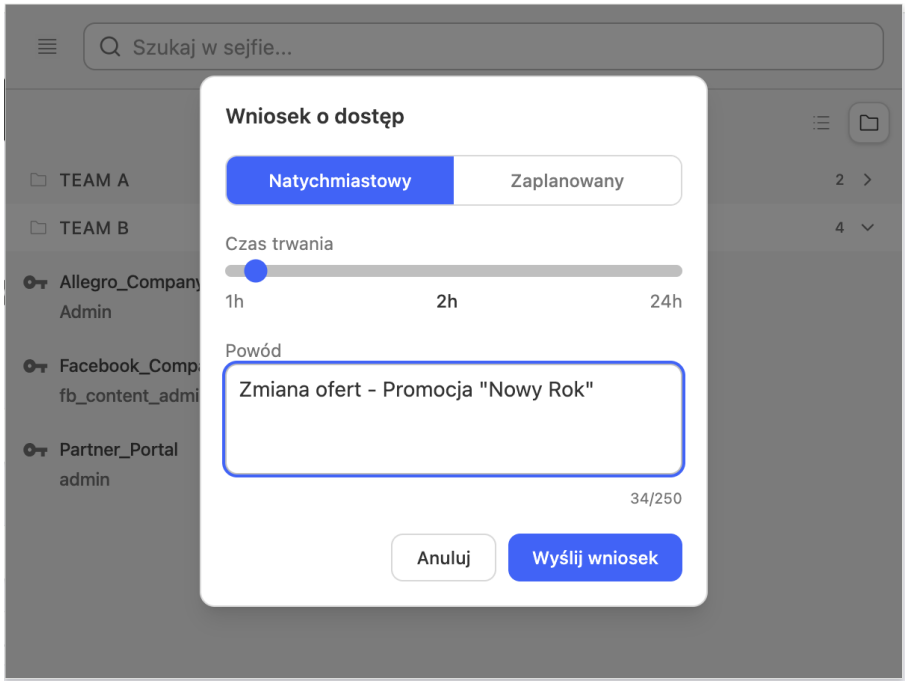
Rozszerzenie obsługuje procesy przyznawania dostępu w Skarbcu haseł bezpośrednio z przeglądarki.

Wnioskowanie o dostęp

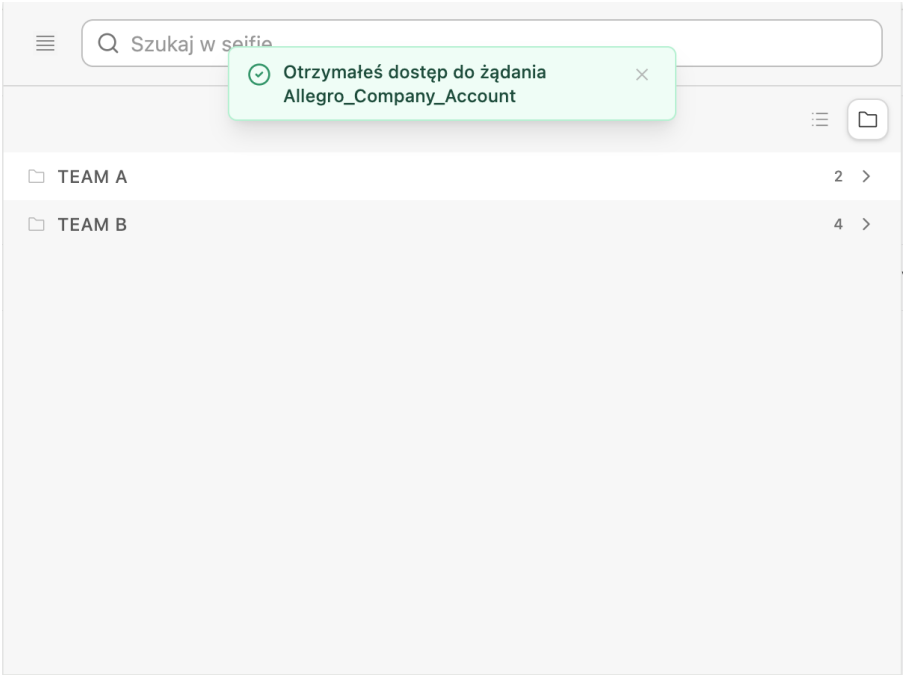
Jeśli sekret jest skonfigurowany z dostępem na żądanie, jest oznaczony ikoną kłódki (**Wniosek o dostęp**). Najedź na sekret i kliknij ikonę, aby poprosić o dostęp.



W formularzu **Wniosek o dostęp** wybierz, czy dostęp ma zostać przyznany **natychmiastowo** (Natychmiastowy), czy **zaplanowany** na później (Zaplanowany), ustaw **Czas trwania**, wpisz **Powód** wniosku i kliknij **Wyślij wniosek**.

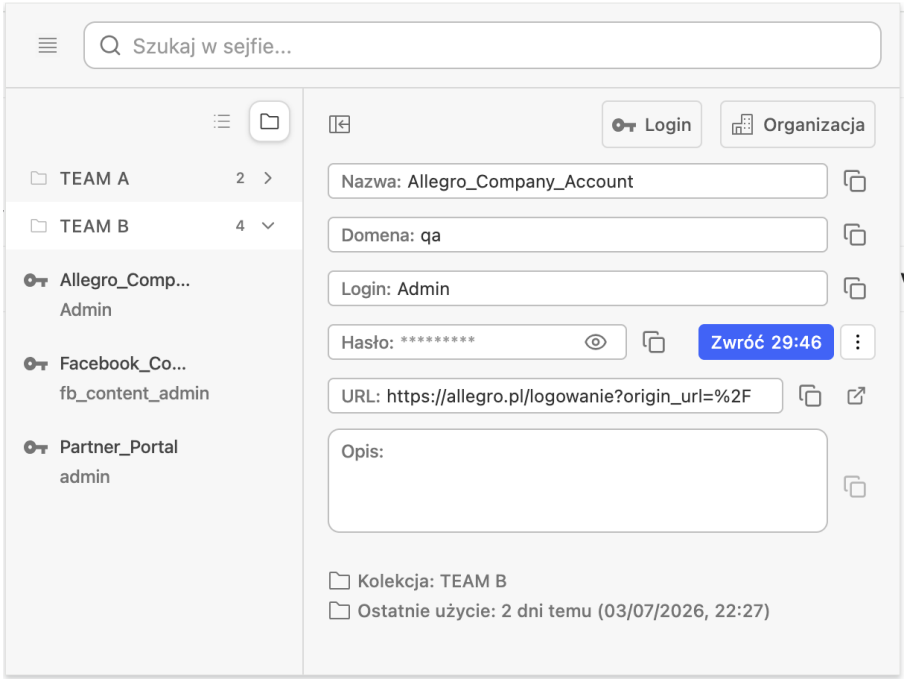


Po przyznaniu dostępu rozszerzenie wyświetla powiadomienie potwierdzające.



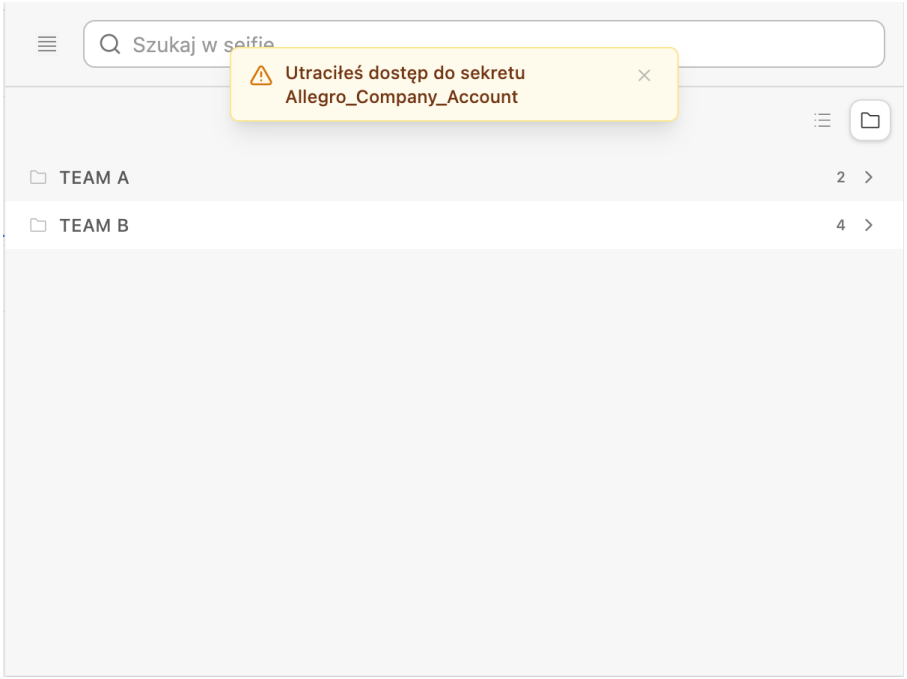
Rezerwacja na wyłączność

W przypadku sekretów z włączoną opcją rezerwacji na wyłączność przycisk **Zwróć** w szczegółach sekretu wyświetla licznik pokazujący, ile czasu pozostało do wygaśnięcia wypożyczenia.



Odebrany dostęp

Jeśli Twój dostęp do sekretu zostanie odebrany, przy sekrecie pojawia się przekreślona ikona, a na liście zostaje on oznaczony jako sekret z odmową dostępu. Rozszerzenie wyświetla również powiadomienie informujące o utracie dostępu.



1.9 Nawiązywanie połączeń

1.9.1 Połączenie przez żądanie o dostęp

Użytkownik może wysłać żądanie o dostęp do zasobów przez Portal Użytkownika.

Do dyspozycji użytkownika są dwa typy żądań: **natychmiastowy** oraz **zaplanowany**. W przypadku wybrania **natychmiastowego** typu żądania, użytkownik może ustalić okres dostępu od zaraz do maksymalnie 24 godzin. Okres dostępu użytkownika zaczyna się w momencie zatwierdzenia żądania przez administratora - wtedy ma się 24 godziny na rozpoczęcie sesji. W momencie rozpoczęcia sesji system odlicza czas dostępu i przerywa połączenie, kiedy czas ten się kończy. Natomiast, jeśli użytkownik nie łączy się w ciągu bliższych 24 godzin, jego dostęp zostaje cofnięty.

Zaplanowany typ żądania polega na wyborze okresu czasowego, podając czas oraz datę przyszłego dostępu.

Uwaga

Dla niektórych kont żądanie dostępu jest wymagane tylko w określonych godzinach. Jeśli administrator skonfigurował sejf do dostępu Just-in-Time zależnego od czasu, w godzinach objętych polityką codziennego dostępu można łączyć się bezpośrednio, a poza nimi trzeba wysłać żądanie dostępu. Takie konto nie jest oznaczane jako zablokowane poza swoimi godzinami - zamiast tego udostępniana jest opcja wysłania żądania. Wysłanie żądania jest możliwe także w objętych godzinach, mimo że nie jest wtedy wymagane.

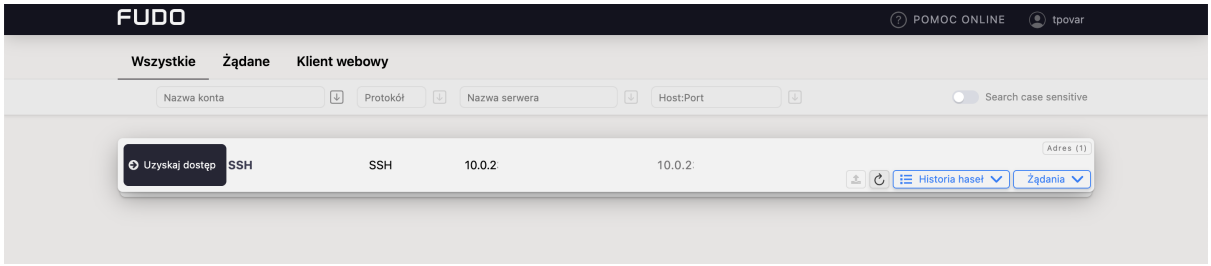
Ostrożnie

Sesja rozpoczęta w godzinach objętych polityką codziennego dostępu jest przerywana z chwilą ich zakończenia, chyba że zatwierdzone żądanie dostępu obejmuje pozostały czas.

Wysłanie żądania

Aby wysłać żądanie o dostęp, postępuj zgodnie z instrukcją:

1. Kliknij przycisk *Uzyskaj dostęp*, który jest widoczny po najechaniu myszką na konkretne konto.



2. Wybierz typ żądania: **natychmiastowy** lub **zaplanowany**.

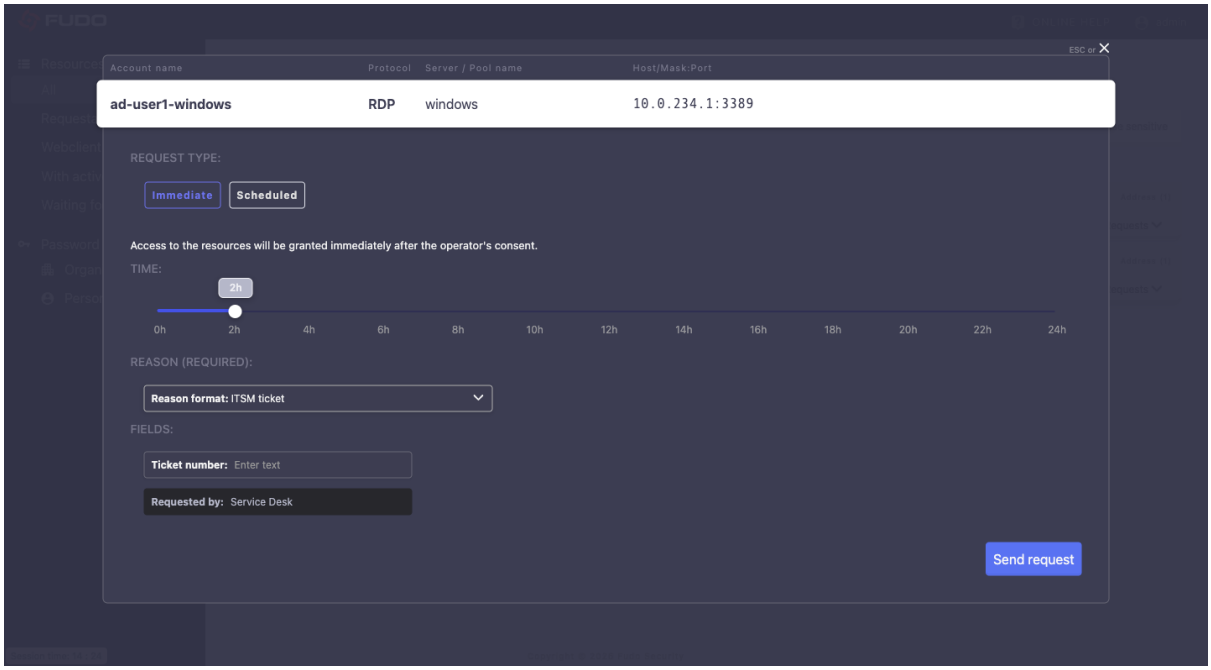
> **Uwaga**
>
> Dla obu typów żądań, pole *Powód* jest wymagane.

3. Ustaw okres dostępu.
4. Kliknij przycisk *Wyślij żądanie*.

Format powodu

Jeśli administrator zdefiniował formaty powodu, w oknie żądania pojawia się lista *Reason format*. Domyślną opcją jest *Free-form text*, która działa tak jak wcześniej — powód wpisujesz samodzielnie.

Wybranie formatu zastępuje pole tekstowe polami tego formatu. Wypełnij je, a powód zostanie złożony automatycznie.



Uwaga

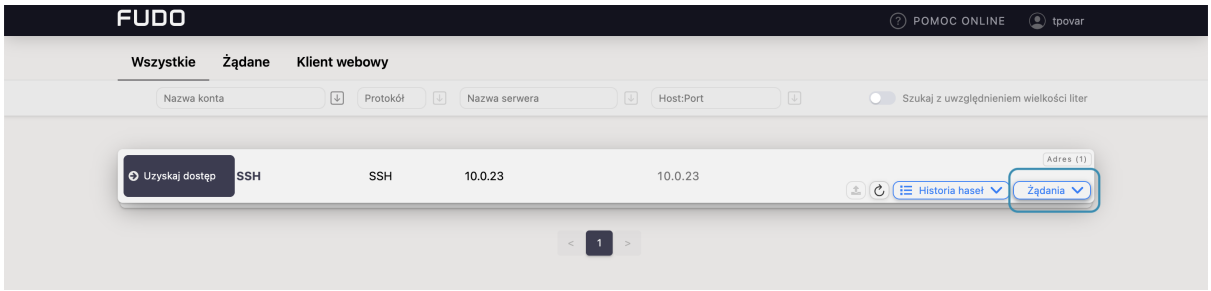
- **Wszystkie pola formatu muszą zostać wypełnione**, w przeciwnym razie nie da się wysłać żądania.
- Niektóre pola mogą już zawierać wartość, której nie można zmienić — administrator ustawił ją jako stałą część powodu.
- Pod nazwą formatu może pojawić się jego opis, jeśli administrator go wprowadził.
- Jeśli administrator zmieni format w trakcie wypełniania formularza, żądanie zostanie odrzucone z komunikatem *The reason does not match the selected format. Refresh the format and try again.* Odśwież stronę i wyślij żądanie ponownie.

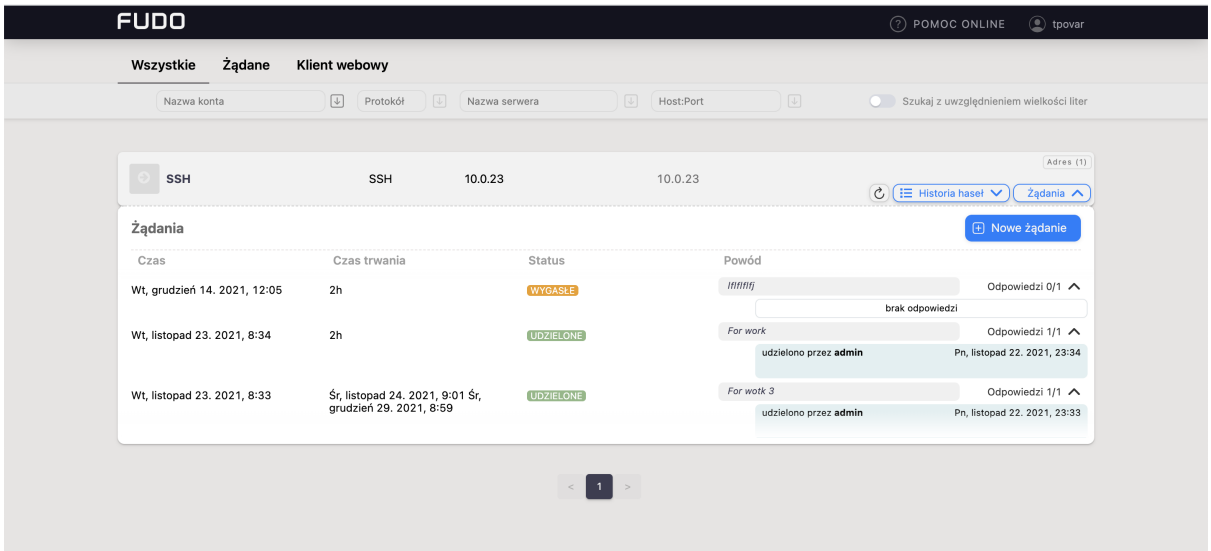
Monitorowanie statusu żądania

Możesz dostać dwa typy powiadomień o statusie swojego żądania:

- `Access Request accepted` - żądanie zostało zaakceptowane przez administratorów.
- `Access Request rejected` - żądanie zostało odrzucone.

Możesz sprawdzić status swojego żądania oraz postęp głosowania dla udzielenia dostępu pod przyciskiem *Żądania* na konkretnym koncie. Historia wszystkich żądań dostępu do zasobów konta też jest widoczna po wciśnięciu przycisku *Żądania* na koncie.





Uwaga

Możesz wysłać kolejne żądanie przez ten sam przycisk *Żądania*, wciskając następnie *+Nowe żądanie*.

1.9.2 RDP, VNC oraz SSH na połączeniu w przeglądarce

Na Portalu Użytkownika połączenia przez protokoły RDP, VNC oraz SSH mogą zostać nawiązane w przeglądarce. Do tego celu służy tak zwany, klient webowy. Lista kont, dla których został uruchomiony taki klient, jest dostępna pod odpowiednią zakładką *Klient webowy* na portalu.

Uwaga

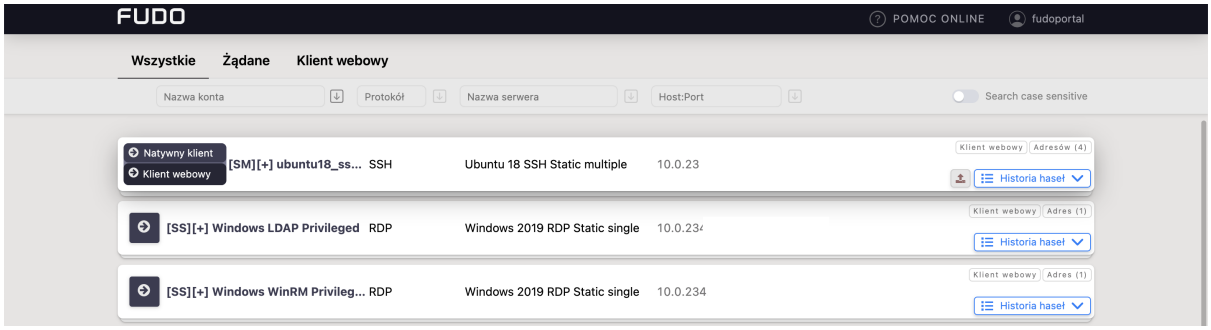
Dla połączeń w przeglądarce przez **protokół RDP** są dostępne następne układy klawiatury serwera.

- `English (US)` - Amerykański Angielski,
- `German` - Niemiecki,
- `German (Swiss)` - Szwajcarski Niemiecki,
- `French` - Francuski (AZERTY),
- `Norwegian` - Norweski,
- `Turkish-Q` - Turecki.

Wybiera się je z listy rozwijanej w prawym górnym rogu pod nazwą użytkownika.

Aby nawiązać połączenie w przeglądarce, postępuj zgodnie z instrukcją:

1. Znajdź konto i serwer, z którym chcesz się połączyć.
2. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
3. Kliknij przycisk *Klient webowy* obok wybranego konta w celu połączenia się z serwerem docelowym.



Uwaga

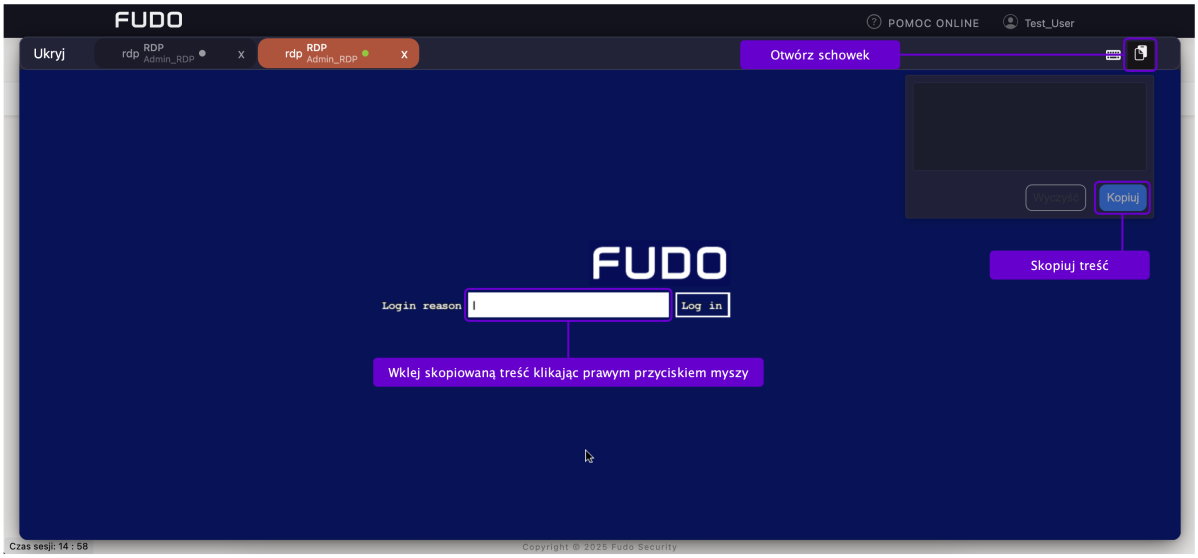
Każda sesja będzie otwarta w nowej zakładce przeglądarki.

Podawanie powodu logowania przy sesji RDP

Jeśli sesja RDP jest nawiązywana przy użyciu konta dodanego do Sejfu z włączoną opcją *Powód logowania*, użytkownik zostanie poproszony o podanie powodu przed zalogowaniem się do systemu docelowego.

Wklejanie tekstu powodu ze schowka:

Aby ułatwić wprowadzenie powodu logowania, możesz użyć funkcji **Schowek** dostępnej w prawym górnym rogu interfejsu Portalu Użytkownika.



1. Kliknij ikonę schowka w prawym górnym rogu ekranu.
2. Wklej lub wpisz tekst, który chcesz użyć jako powód logowania.
3. Kliknij przycisk **Kopiuj**, aby przenieść tekst do tymczasowego schowka sesji.
4. Przejdź do pola, w którym należy podać powód logowania.
5. Aby wkleić tekst, **kliknij prawym przyciskiem myszy** w pole tekstowe.

Uwaga

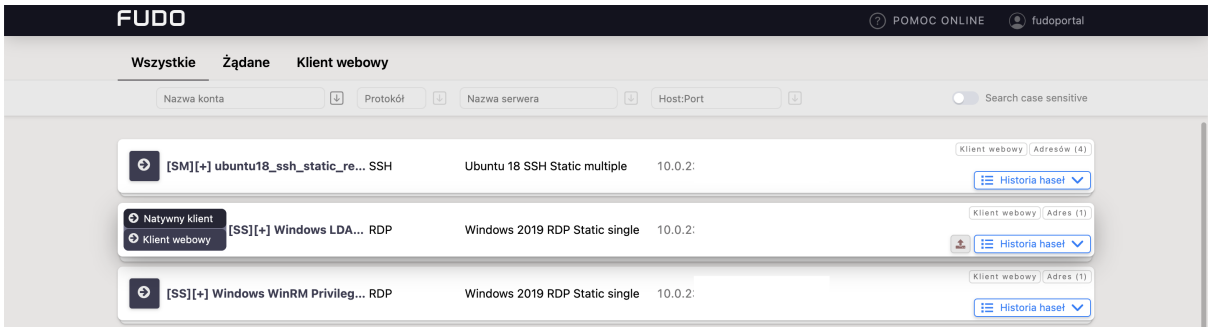
Należy pamiętać, że schowek ma ograniczenie długości kopiowanego tekstu do pola **Powód logowania**: maksymalnie **60 znaków** dla języka polskiego i angielskiego oraz **40 znaków** dla cyrylicy. Jeśli kopiowany tekst przekroczy ten limit, może zostać ucięty lub w ogóle nie zostanie skopiowany.

Tematy pokrewne:

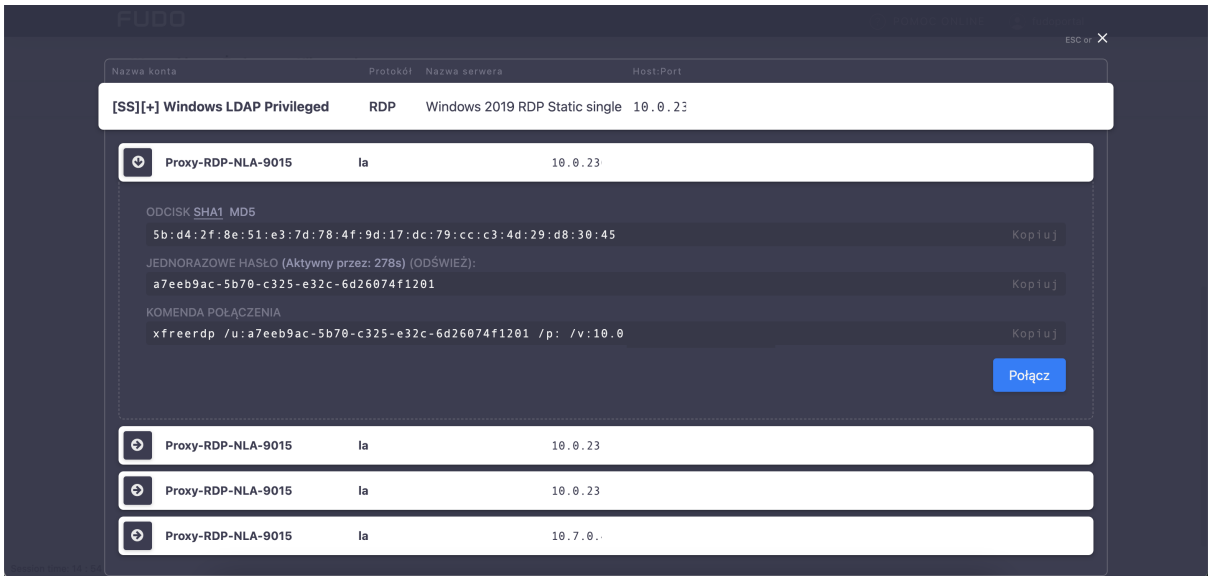
- *Funkcjonalności Webclienta*
- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*
- *RDP na systemie operacyjnym Ubuntu*

1.9.3 RDP na systemie operacyjnym Microsoft Windows 7 i 10

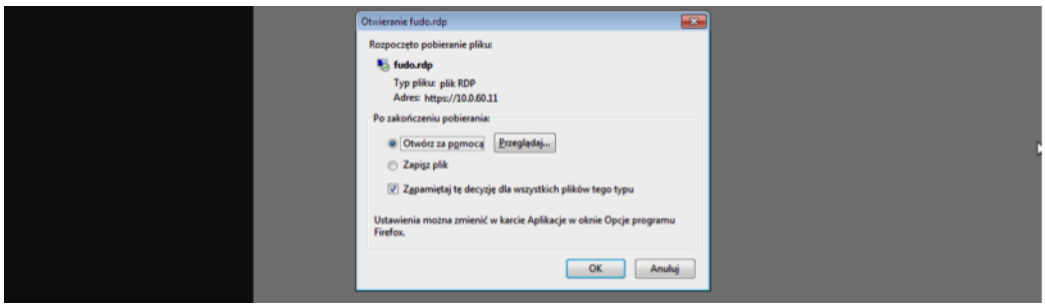
1. Znajdź konto i serwer, z którym chcesz się połączyć.
2. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
3. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.



4. Wybierz gniazdo nasłuchiwania, za pomocą którego chcesz się podłączyć.
5. Kliknij *Połącz*.



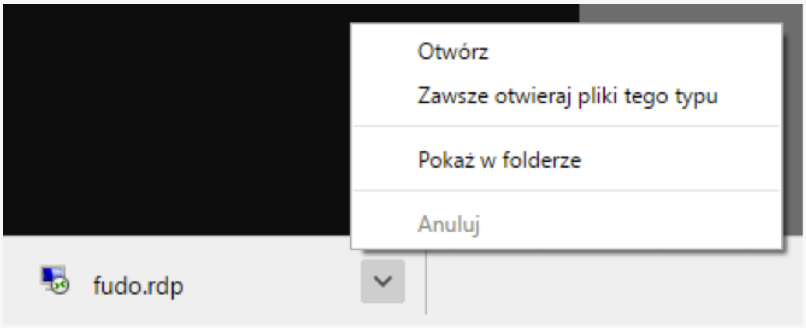
6. Zapisz plik definicji połączenia lub uruchom bezpośrednio klienta właściwego dla protokołu RDP.



Uwaga

- Przeglądarka *Chrome* zapisze plik automatycznie.

- Wybierz opcję *Zawsze otwieraj pliki tego typu*, aby automatycznie uruchamiać program kliencki.



7. Kontynuuj bez podawania hasła.
8. Kliknij *Tak*, aby zaakceptować informację dotyczącą nieznanego wystawcy certyfikatu.

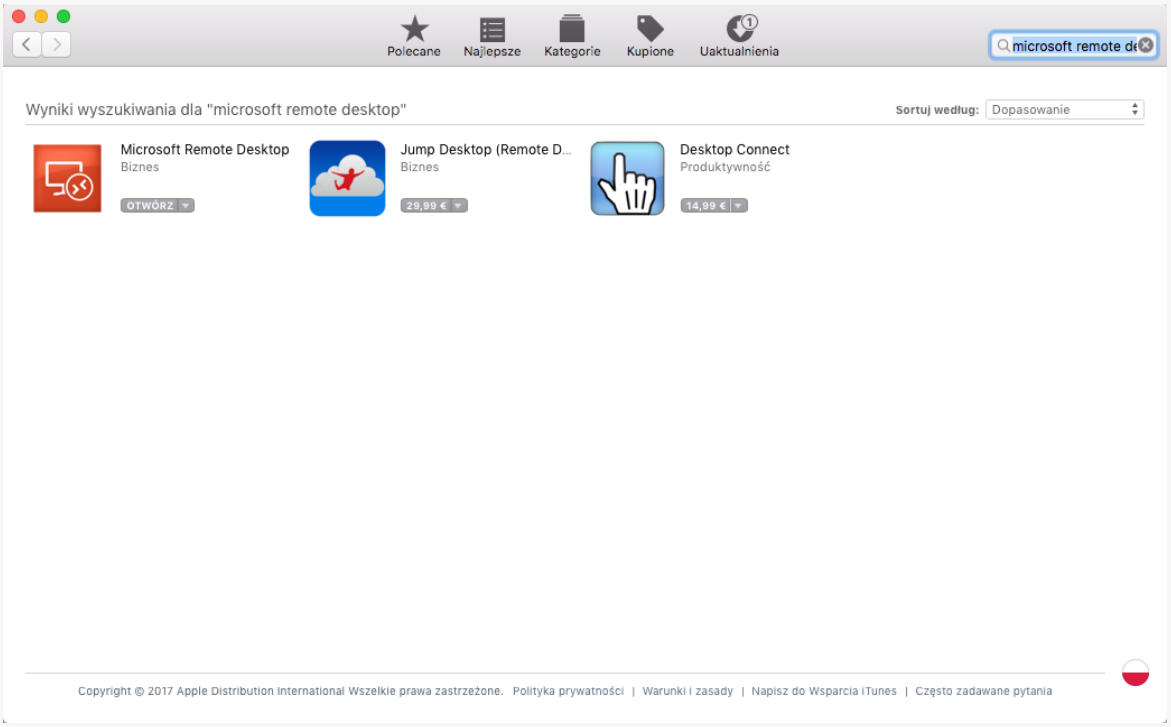
Tematy pokrewne:

- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Ubuntu*

1.9.4 RDP na systemie operacyjnym Mac OS

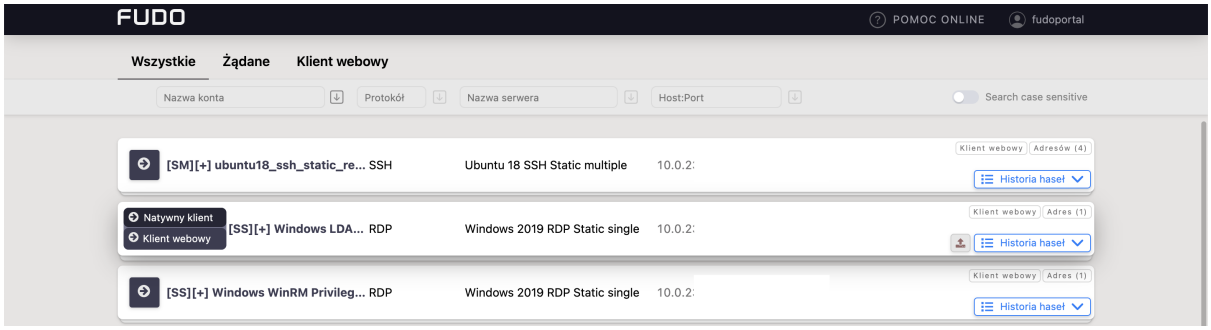
Uwaga

Aby nawiązywać połączenia RDP, pobierz z App Store i zainstaluj program Microsoft Remote Desktop.

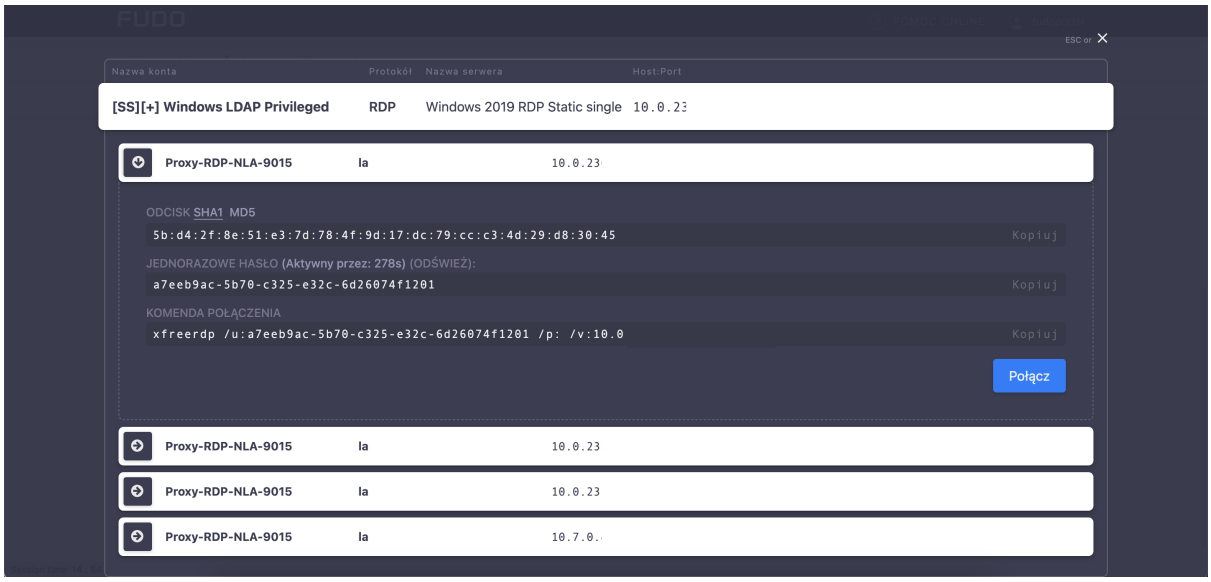


1. Znajdź konto i serwer, z którym chcesz się połączyć.

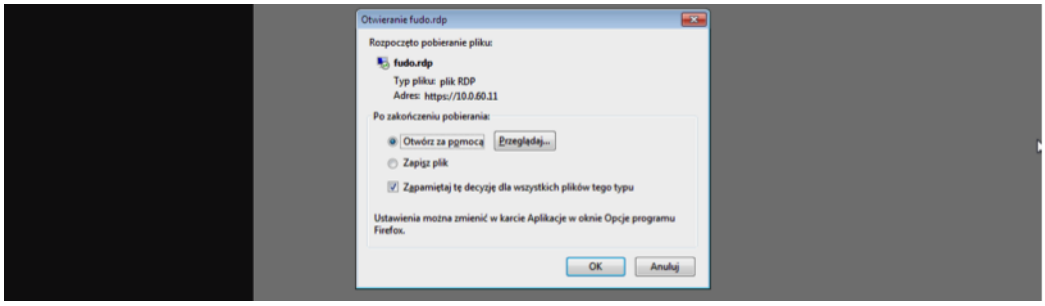
2. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
3. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.



4. Wybierz gniazdo nasłuchiwania, za pomocą którego chcesz się podłączyć.
5. Kliknij *Połącz*.

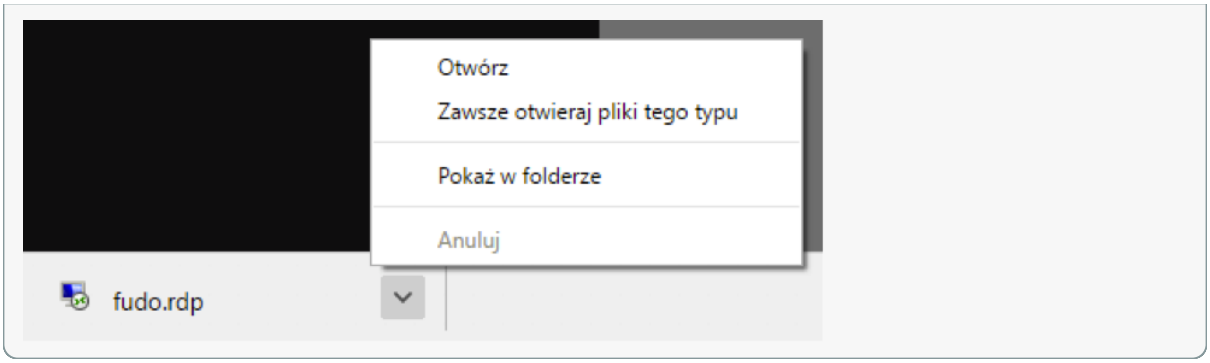


6. Zapisz plik definicji połączenia lub uruchom bezpośrednio klienta właściwego dla protokołu RDP.

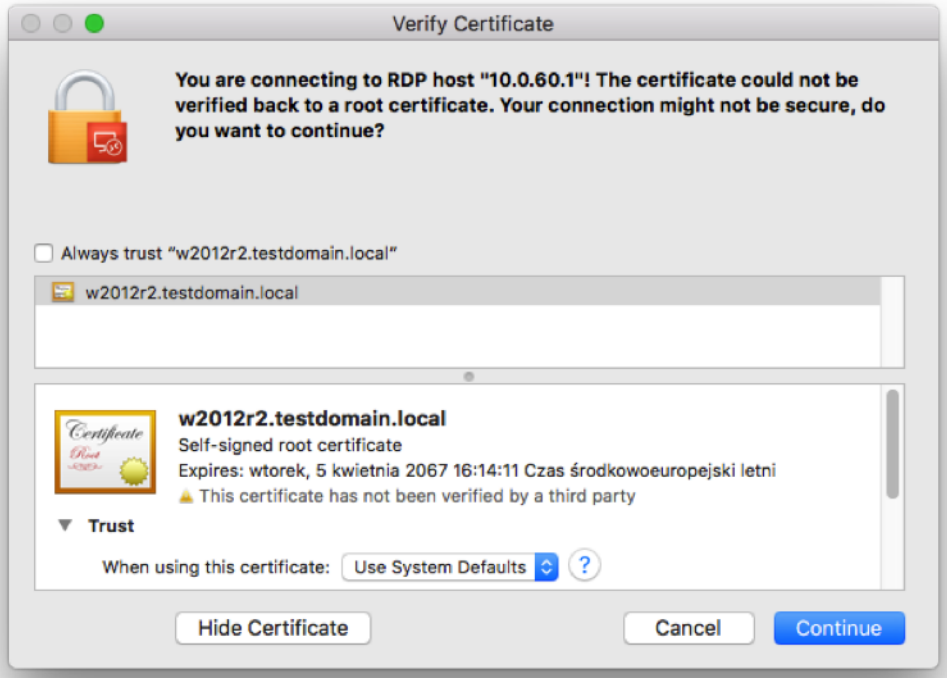


Uwaga

- Przeglądarka *Chrome* zapisze plik automatycznie.
- Wybierz opcję *Zawsze otwieraj pliki tego typu*, aby automatycznie uruchamiać program kliencki.



7. Kliknij *Continue*, aby zaakcpetować certyfikat i zainicjować połączenie z wybranym serwerem.



Tematy pokrewne:

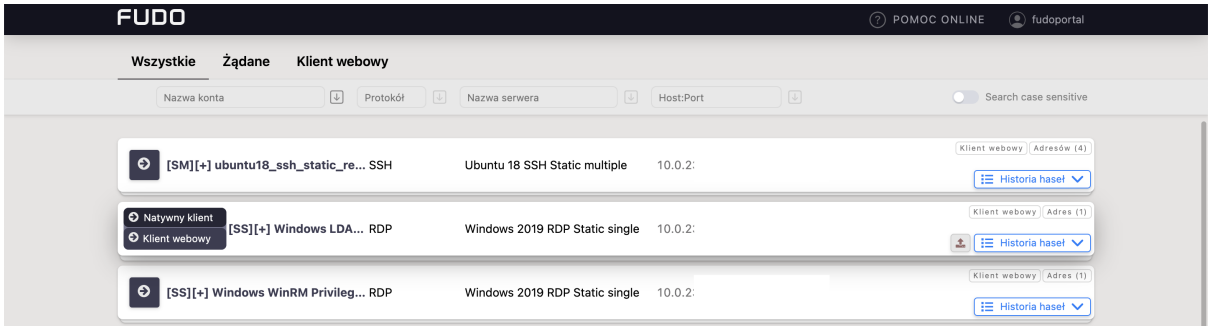
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*
- *RDP na systemie operacyjnym Ubuntu*

1.9.5 RDP na systemie operacyjnym Ubuntu

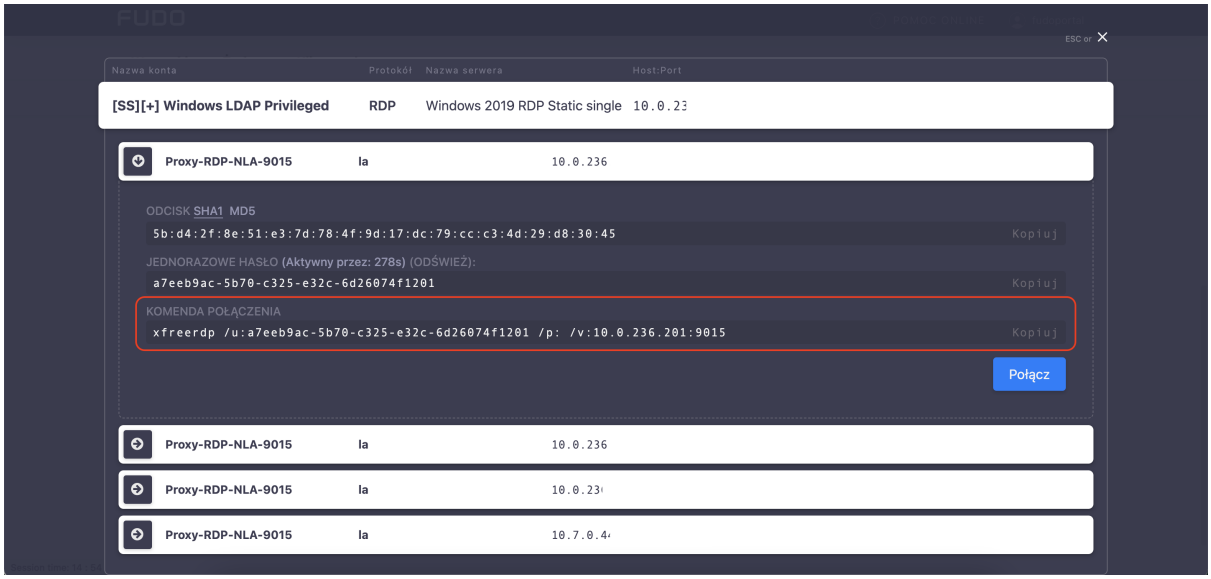
Uwaga

Prawidłowa obsługa połączeń RDP w systemie Ubuntu 16.04 LTS wymaga zainstalowania `xfreerdp`. Wykonaj polecenie `sudo apt-get install freerdp-x11`, aby zainstalować program.

1. Znajdź konto i serwer, z którym chcesz się połączyć.
2. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
3. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.



4. Wybierz gniazdo nasłuchiwania, za pomocą którego chcesz się podłączyć.
5. Skopiuj wygenerowany ciąg znaków stanowiący polecenie.



6. Wykonaj komendę w oknie terminala.

Tematy pokrewne:

- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*

1.9.6 SSH na systemie operacyjnym Microsoft Windows 7/10

Uwaga

Automatyczne inicjowanie połączeń SSH z poziomu Portalu Użytkownika wymaga zainstalowania programu *PuTTY* oraz skonfigurowania asocjacji pomiędzy protokołem a narzędziem. W tym celu zaleca się zainstalowanie razem z *PuTTY* programu *WinSCP*, który dokona wymaganych zmian konfiguracyjnych. Oba programy muszą być w tej same, 32 bitowej wersji.

1. Pobierz i zainstaluj program *WinSCP*.

   `https://winscp.net/download/WinSCP-5.19.2-Setup.exe`

Uwaga

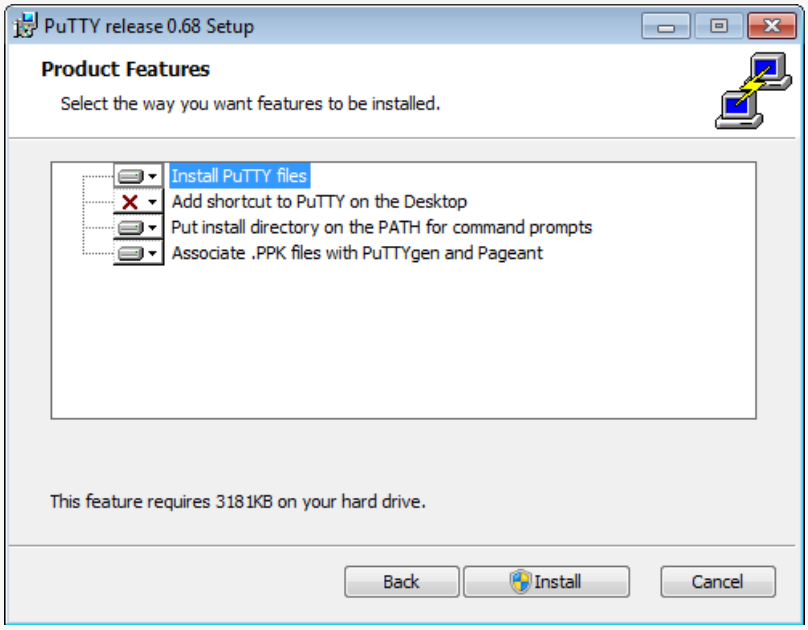
Sprawdź sumę kontrolną pobranego programu.

2. Pobierz i zainstaluj program *PuTTY*.

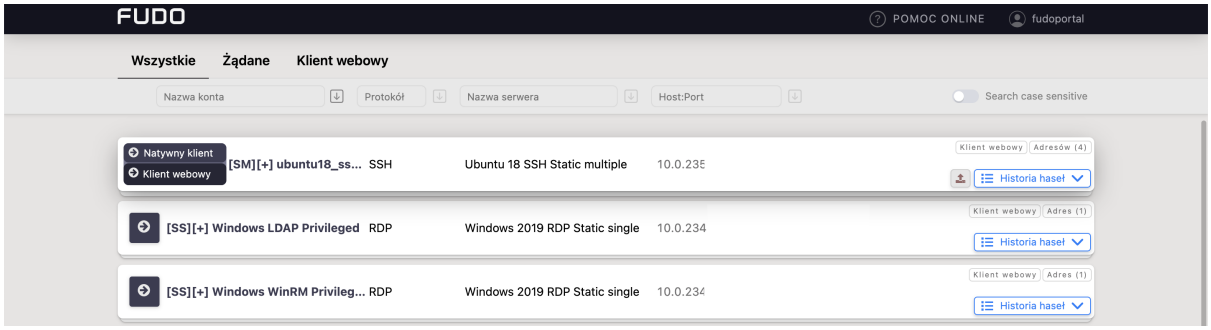
   `https://winscp.net/download/putty-0.75-installer.msi`

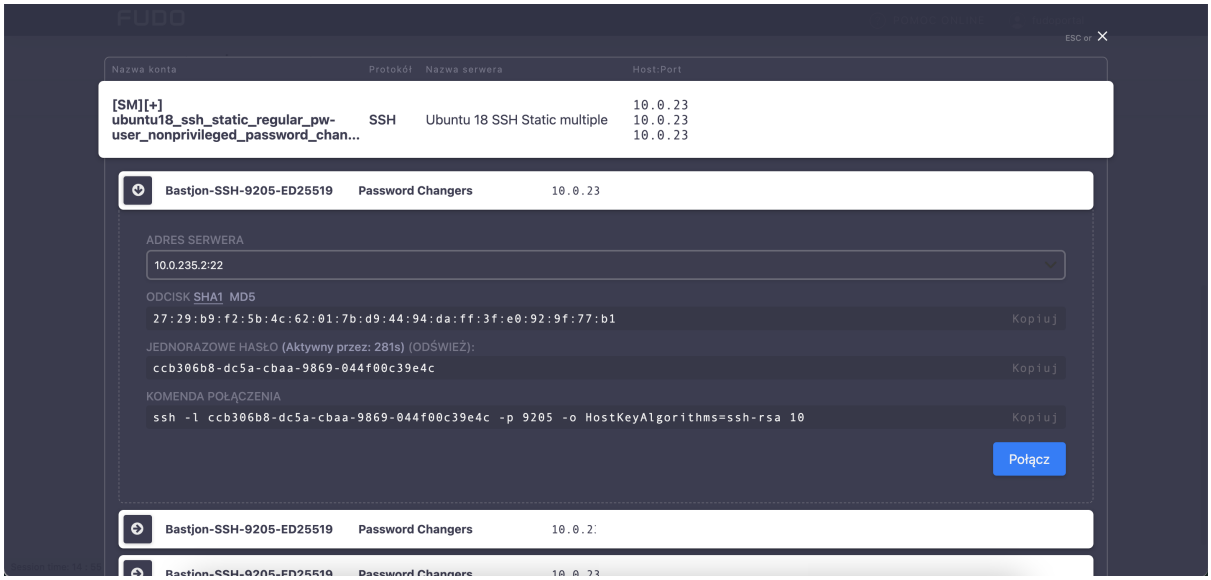
Uwaga

- Zainstaluj program w domyślnej ścieżce instalacyjnej: `C:\Program Files (x86)\PuTTY\`.
- Podczas instalacji, wybierz domyślny zestaw funkcjonalności.

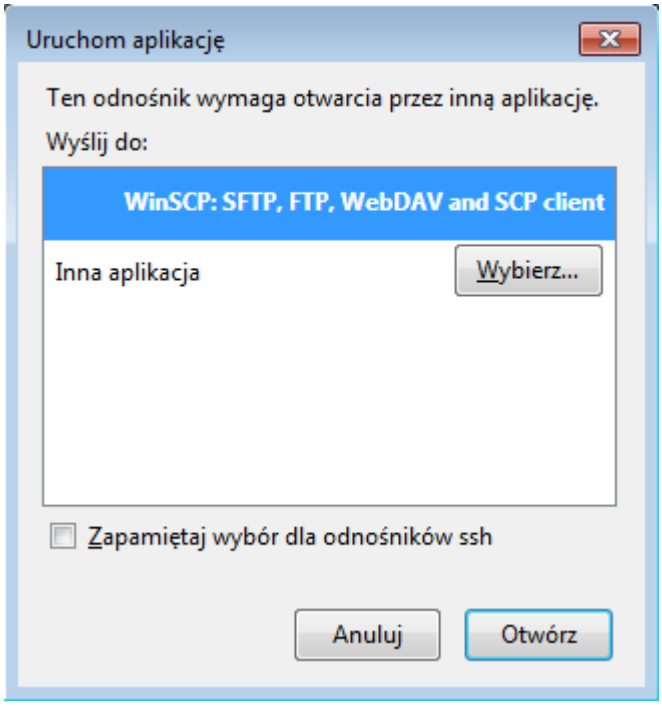


3. Znajdź konto i serwer, z którym chcesz się połączyć.
4. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
5. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.

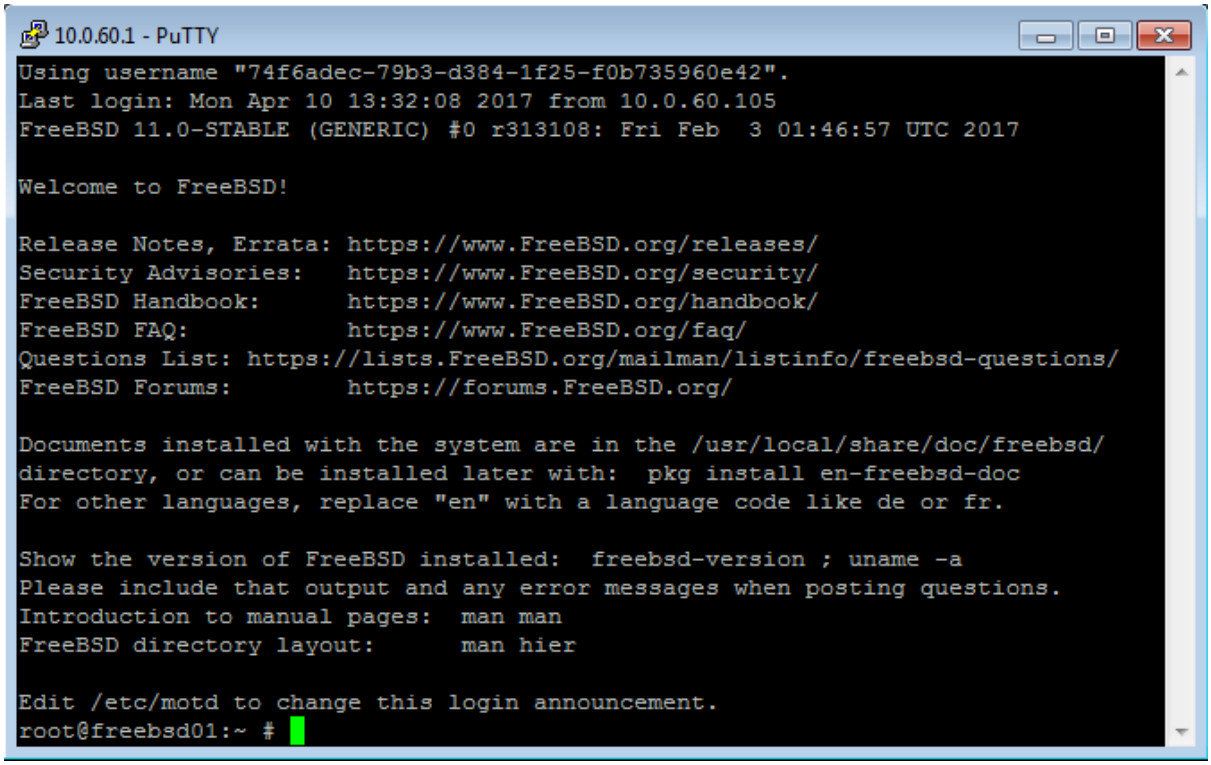




6. Kliknij *Połącz*.
7. W oknie *Uruchom aplikację* wybierz *WinSCP:SFTP,FTP,WebDAV and SCP* i kliknij *Otwórz*.



8. Połączenie zostało zainicjowane.

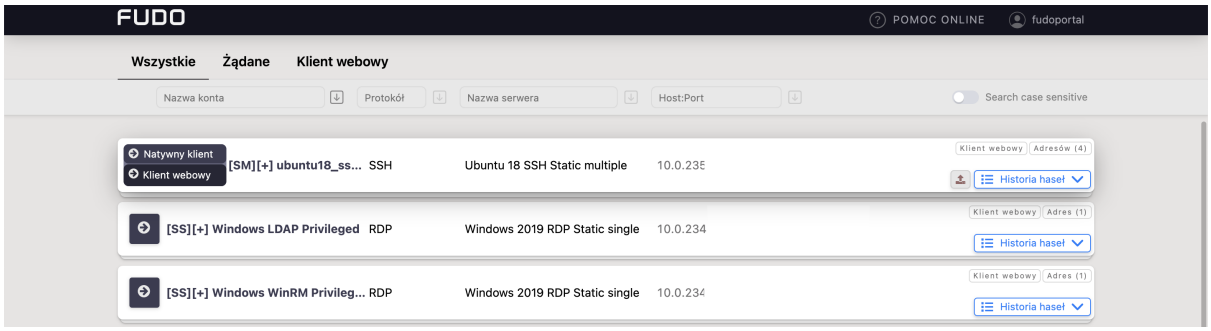


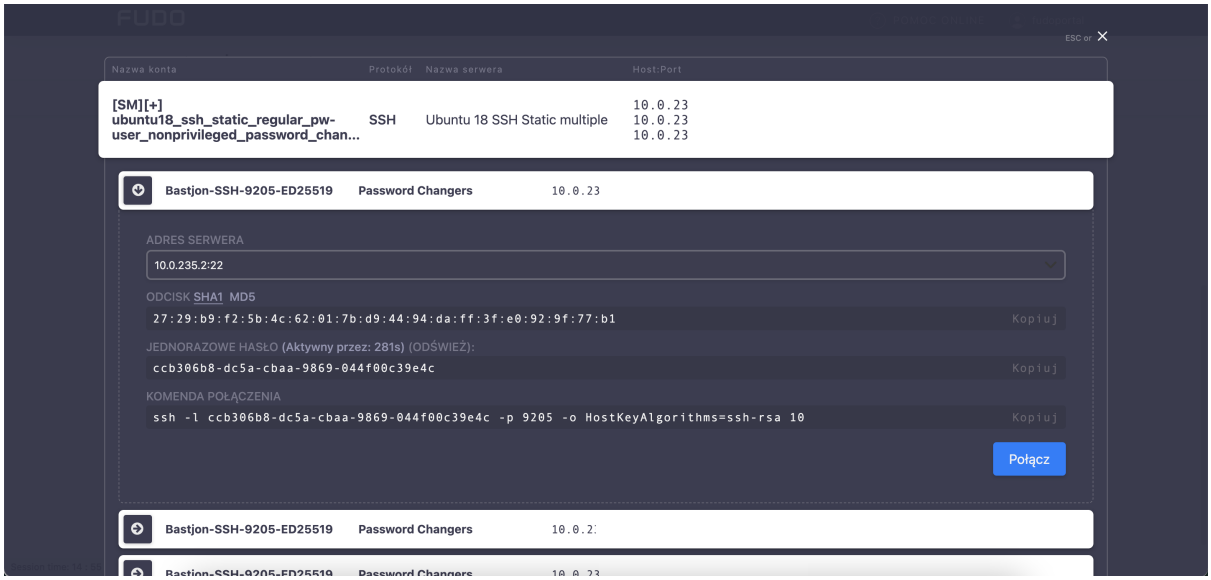
Tematy pokrewne:

- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Ubuntu*

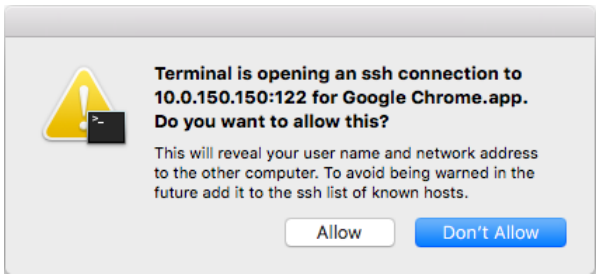
1.9.7 SSH na systemie operacyjnym Mac OS

1. Zaloguj się do Portalu Użytkownika.
2. Znajdź konto i serwer, z którym chcesz się połączyć.
3. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
4. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.





5. Kliknij *Połącz*.
6. Kliknij *Zezwól*, aby otworzyć terminal i zainicjować połączenie.



7. Połączenie zostało nawiązane.

Tematy pokrewne:

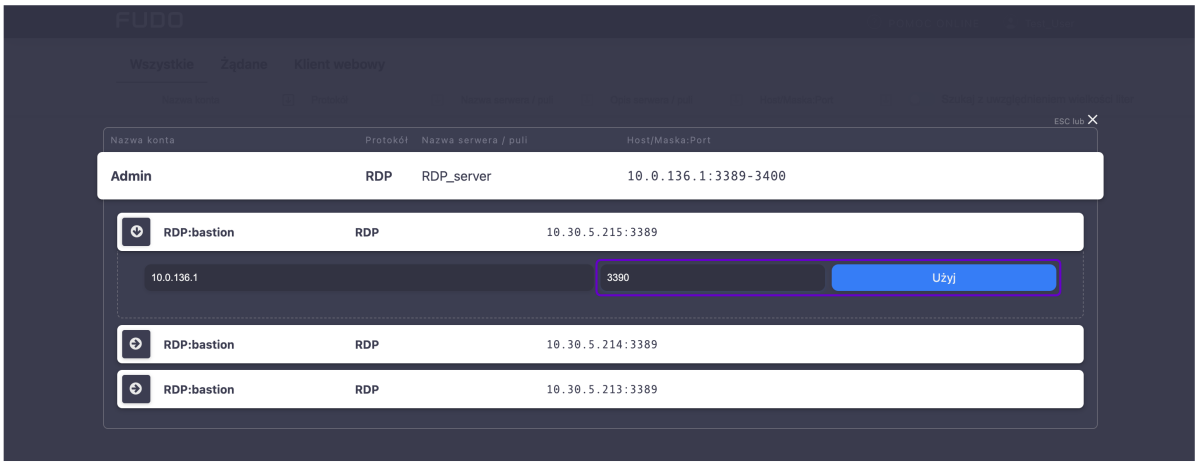
- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Ubuntu*
- *SSH na systemie operacyjnym Microsoft Windows 7/10*

1.9.8 Nawiązywanie połączenia z serwerem z zakresem portów

Klient natywny

Po najechaniu kursorem na konto, którego chcemy użyć do połączenia i wybraniu Natywny klient należy:

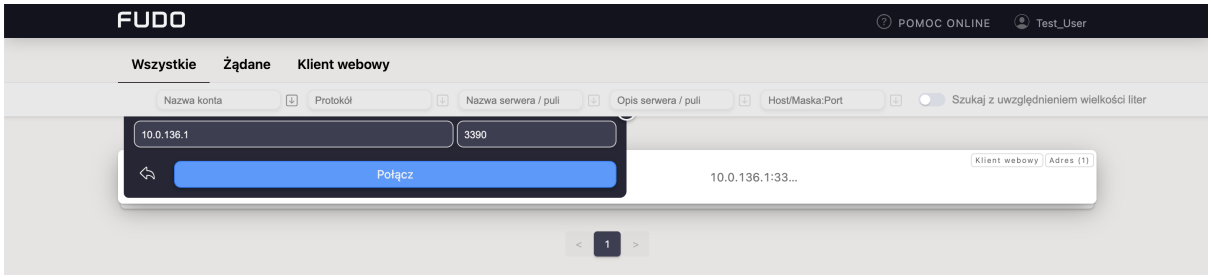
1. Wybrać z listy rozwijanej adres serwera z zakresem portów z którym chcemy nawiązać połączenie (w przypadku puli serwerów),
2. W polu **Port** wpisać port wybrany z zakresu podanego podczas konfiguracji danego serwera,
3. Wcisnąć przycisk **Użyj**.
4. Wcisnąć przycisk **Połącz** aby pobrać/uzyskać dane do nawiązania połączenia w odpowiednim dla serwera protokole.



Klient webowy

Po najechaniu kursorem na konto, którego chcemy użyć do połączenia i wybraniu Klient webowy należy:

1. Wybrać z listy rozwijanej adres serwera z zakresem portów z którym chcemy nawiązać połączenie (w przypadku puli serwerów).
2. W polu **Port** wpisać port wybrany z zakresu podanego podczas konfiguracji danego serwera.
3. Wcisnąć przycisk **Połącz** aby nawiązać połączenie w przeglądarce.

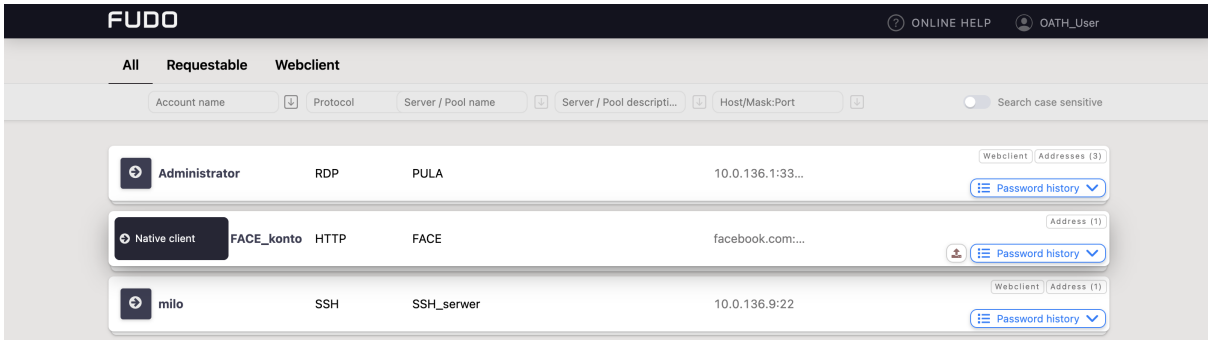


Tematy pokrewne:

- *Funkcjonalności Webclienta*
- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*
- *RDP na systemie operacyjnym Ubuntu*

1.9.9 Nawiązywanie połączenia HTTP

1. Zaloguj się do Portalu Użytkownika.
2. Znajdź konto i serwer, z którym chcesz się połączyć.
3. Najedź na to konto myszką, aby zobaczyć dostępne opcje.
4. Kliknij przycisk *Natywny klient* obok wybranego konta w celu połączenia się z serwerem docelowym.



5. Kliknij *Połącz*.

6. Połączenie zostanie nawiązane i zostaniesz przekierowany do nowego okna przeglądarki.

Tryby dostępu przeglądarki w renderowanych sesjach HTTP

Renderowane sesje HTTP mogą być otwierane w jednym z następujących trybów dostępu przeglądarki. Dostępny tryb zależy od ustawień sejfu skonfigurowanych przez administratora.

Tryb kiosku z pojedynczą zakładką

W trybie kiosku z pojedynczą zakładką renderowana sesja HTTP jest wyświetlana w zablokowanym widoku przeglądarki. Interfejs przeglądarki jest ukryty, w tym pasek adresu i elementy sterowania nawigacją przeglądarki.

W tym trybie:

- Dostępna jest tylko jedna zakładka przeglądarki.
- Pasek adresu nie jest wyświetlany.
- Elementy sterowania nawigacją przeglądarki, takie jak wstecz, dalej i odśwież, nie są wyświetlane.
- Menu kontekstowe otwierane prawym przyciskiem myszy jest wyłączone.
- Okna wyskakujące są przekierowywane na bieżącą stronę i zastępują jej zawartość.

Pełny dostęp do przeglądarki

W trybie pełnego dostępu do przeglądarki renderowana sesja HTTP jest wyświetlana z widocznym interfejsem przeglądarki.

W tym trybie:

- Dostępnych jest wiele zakładek przeglądarki.
- Pasek adresu jest wyświetlany.
- Elementy sterowania nawigacją przeglądarki, takie jak wstecz, dalej i odśwież, są dostępne.
- Możesz otwierać i przełączać się między zakładkami przeglądarki.
- Nie ma limitu zakładek.
- Dostęp do ograniczonych narzędzi przeglądarki, takich jak narzędzia deweloperskie i ustawienia przeglądarki, pozostaje zablokowany.

Zachowanie okien wyskakujących

W renderowanych sesjach HTTP zachowanie okien wyskakujących zależy od trybu dostępu przeglądarki i ustawień sejfu.

- W trybie kiosku z pojedynczą zakładką okna wyskakujące są przekierowywane na bieżącą stronę i zastępują jej zawartość.
- W trybie pełnego dostępu do przeglądarki okna wyskakujące mogą być konwertowane na zakładki przeglądarki, w zależności od ustawień sejfu.
- Jeśli konwersja okien wyskakujących na zakładki przeglądarki jest wyłączona, okna wyskakujące mogą otwierać się poza widokiem przeglądarki i zakrywać zawartość sesji.

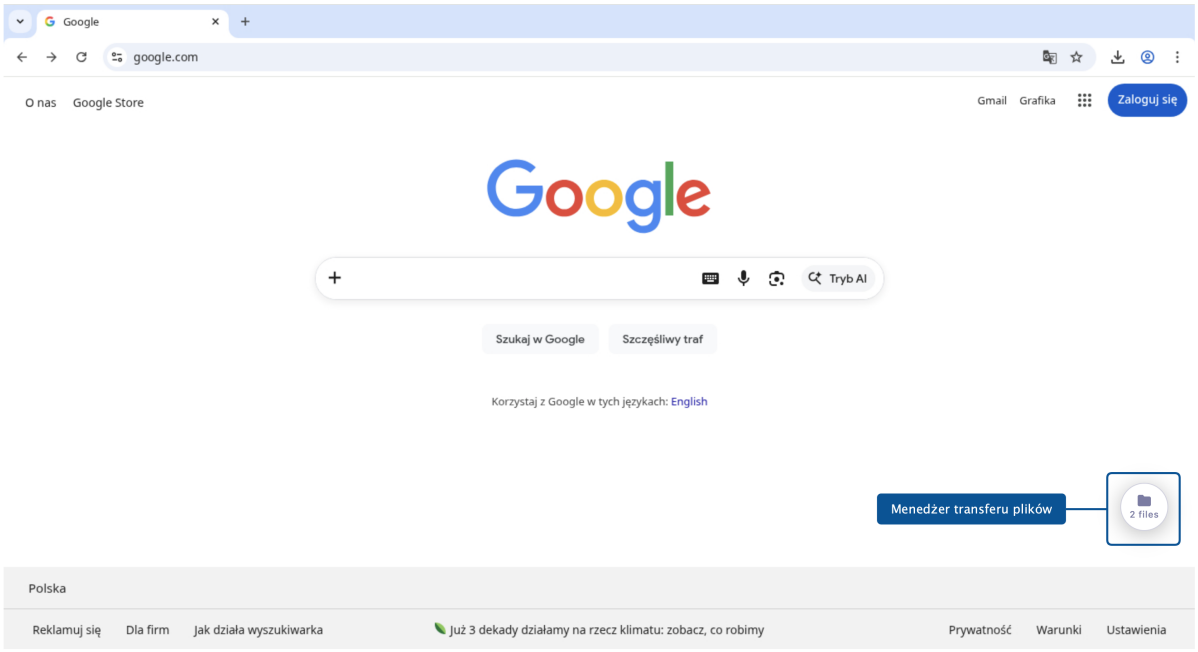
Jeśli przekierowana strona nie załaduje się poprawnie, spróbuj odświeżyć ją za pomocą skrótu klawiaturowego **Ctrl** + **R**.

Jeśli okno wyskakujące zastępuje bieżącą stronę, możesz wrócić do poprzedniej strony po przekierowaniu. Skróty klawiaturowe służące do cofania zależą od przeglądarki i systemu operacyjnego, na przykład:

- **Windows / Linux**: Left Alt + Strzałka w lewo
- **macOS (Chrome)**: Right Option + Strzałka w lewo
- **macOS (Edge / Safari)**: Right Option + Strzałka w lewo

Transfer plików w renderowanych sesjach HTTP

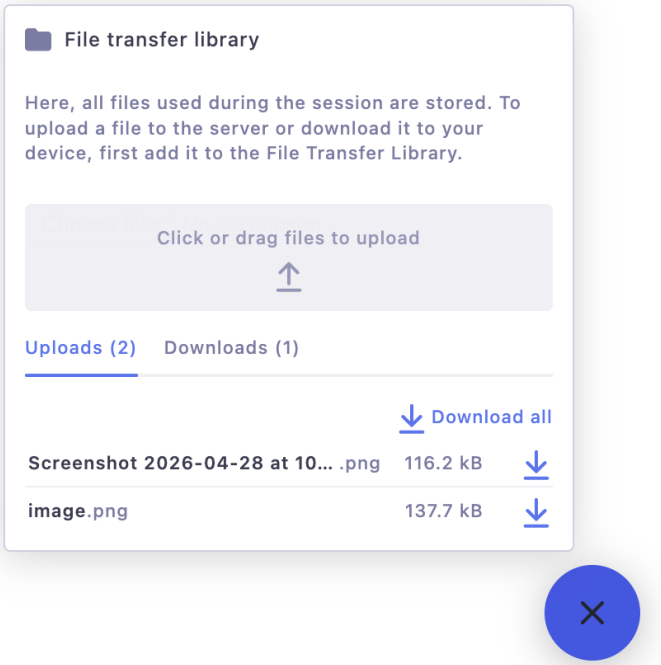
Jeśli przesyłanie lub pobieranie plików jest dozwolone dla sejfu, na ekranie sesji wyświetlany jest pływający przycisk menedżera transferu plików.



Możesz przenieść przycisk menedżera transferu plików w inne miejsce na ekranie. Domyślnie jest on zwykle wyświetlany w prawym dolnym rogu okna sesji.

Kliknij przycisk menedżera transferu plików, aby otworzyć okno modalne z następującymi zakładkami:

- **Przesyłanie** - umożliwia przesyłanie plików z urządzenia lokalnego do renderowanej sesji HTTP.
- **Pobieranie** - wyświetla pliki pobrane w przeglądarce podczas renderowanej sesji HTTP.



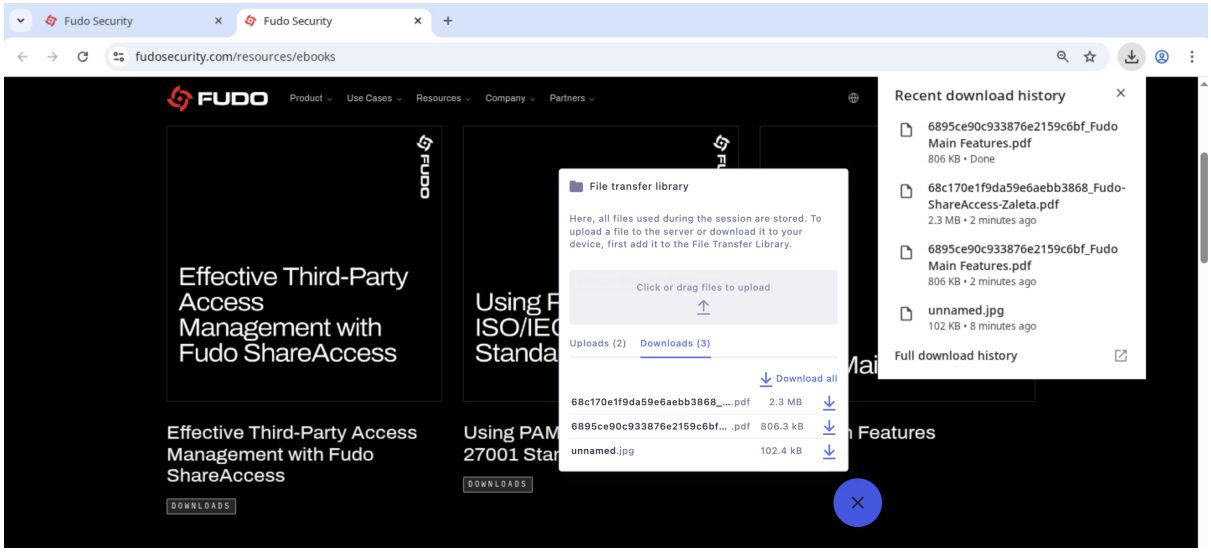
Przesyłanie plików

Aby przesłać plik do sesji, otwórz zakładkę **Przesyłanie** i wykonaj jedną z następujących czynności:

- Kliknij pole **Kliknij lub przeciągnij, aby przesłać** i wybierz plik z przeglądarki plików.
- Przeciągnij i upuść plik do pola **Kliknij lub przeciągnij, aby przesłać**.

Pobieranie plików

Pliki pobrane w przeglądarce są wyświetlane w zakładce **Pobieranie**.



Uwaga

- Uprawnienia do przesyłania i pobierania plików są kontrolowane oddzielnie przez admi-

nistratora w ustawieniach sejfu. W zależności od konfiguracji sejfu w renderowanej sesji HTTP może być dostępne tylko przesyłanie, tylko pobieranie, obie czynności lub żadna z nich.

- Łączny limit miejsca na pliki przesyłane i pobierane w sesji wynosi maksymalnie 5120 MB.

Tematy pokrewne:

- *Funkcjonalności Webclienta*
- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*
- *RDP na systemie operacyjnym Ubuntu*

1.10 Funkcjonalności Webclienta

Uwaga

Dostępność elementów paska narzędzi zależy od protokołu nawiązanej sesji.

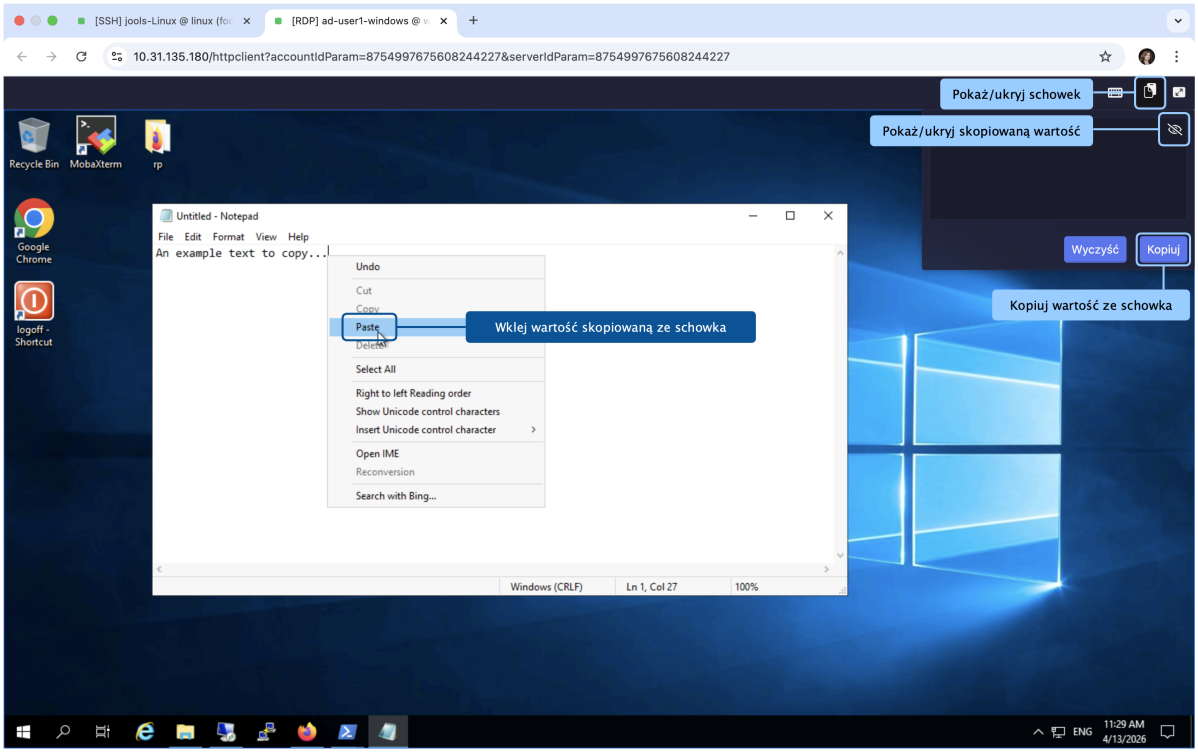
Dostępne funkcje Webclienta:

- Zakładki przeglądarki pokazujące typ protokołu, nazwę serwera i konta użytego do nawiązania sesji oraz status połączenia:
  - połączenie jest nawiązywane,
  - sesja jest połączona,
  - sesja jest rozłączona.

Uwaga

Pełny podgląd informacji o sesji jest dostępny po najechaniu myszki na kartę zakładkę.

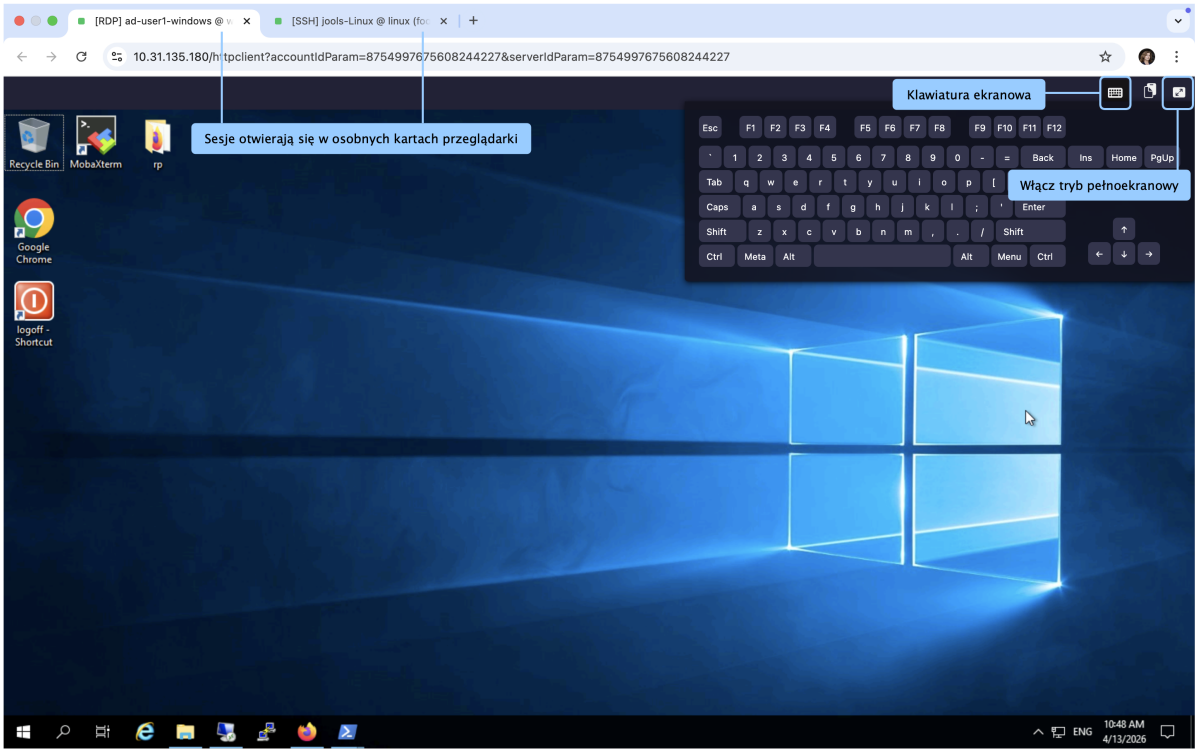
- Przycisk *Schowek* umożliwiający skopiowanie fragmentu tekstu do schowka systemowego po stronie serwera sesji. Wystarczy wkleić tekst do okna schowka i wcisnąć *Kopiuj*.
- Zawartość wrażliwa w schowku Webclienta może zostać ukryta za pomocą ikony oka, dzięki czemu skopiowane wartości, takie jak hasła, mogą być maskowane zamiast wyświetlane w postaci jawnego tekstu.



- Przycisk *Klawiatura ekranowa*.
- Przycisk *Tryb pełnoekranowy*, który pozwala ukryć pasek narzędzi Webclienta i uzyskać czystszy widok sesji.

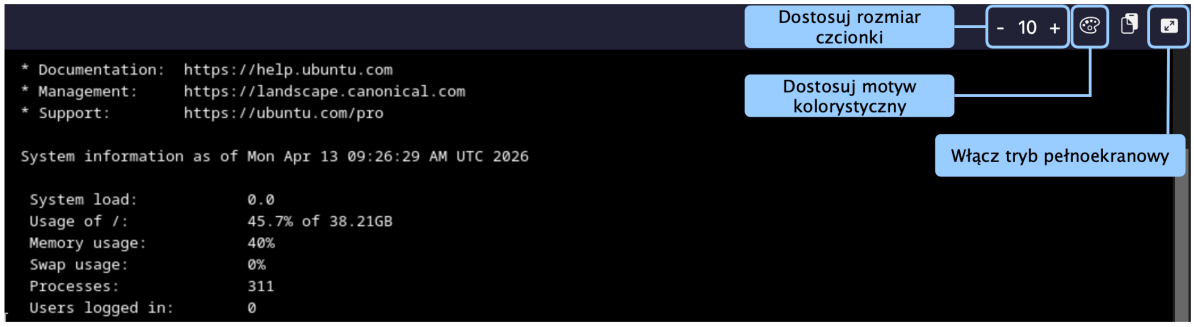
Uwaga

Od wersji 6.0 sesje Webclienta otwierają się w osobnych kartach przeglądarki, co zapewnia więcej miejsca na aktywną sesję.



Dodatkowo, dla połączeń nawiązanych przy użyciu protokołu SSH istnieje opcja modyfikacji widoku sesji poprzez dostosowanie rozmiaru czcionki oraz kolorystyki terminala. Dostępne są następujące motywy kolorystyczne połączeń SSH:

- czarno-biały (czarne litery na białym tle) - domyślny,
- szaro-czarny (szare litery na czarnym tle),
- zielono-czarny (zielone litery na czarnym tle),
- biało-czarny (białe litery na czarnym tle).



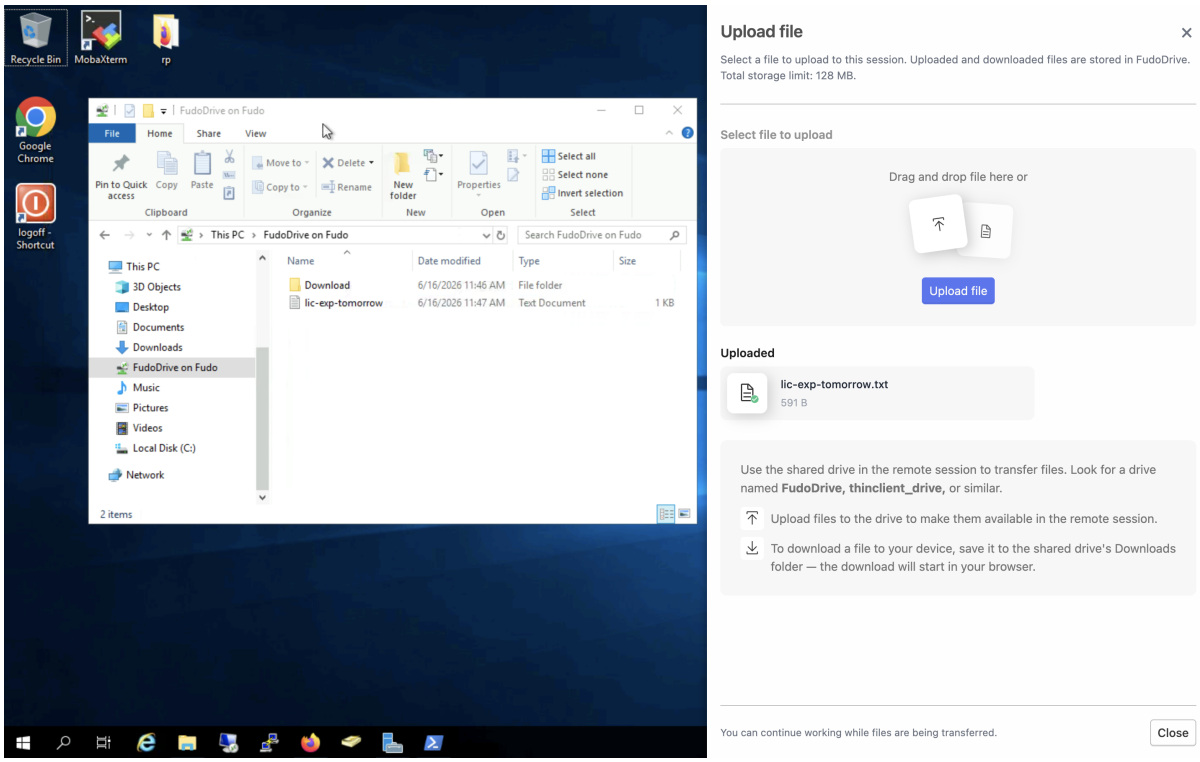
Transfer plików w sesjach RDP

Sesje RDP w Kliencie webowym umożliwiają wgrywanie i pobieranie plików. Pliki są przechowywane na dysku współdzielonym danej sesji, z łącznym limitem **128 MB** (wgrywanie i pobieranie razem); można przesyłać wyłącznie pojedyncze pliki (wgrywanie folderów nie jest obsługiwane).

Uwaga

Ikony wgrywania i pobierania są widoczne na pasku bocznym tylko wtedy, gdy dla sejfu

włączono opcję **Przekierowanie urządzeń**.



Aby wgrać plik:

1. Na pasku bocznym sesji kliknij ikonę wgrywania, aby otworzyć panel transferu plików.
2. Kliknij *Wgraj plik*, wybierz plik z urządzenia i kliknij *Otwórz*. Możesz też przeciągnąć i upuścić plik w panelu transferu.

Uwaga

Plik zostaje umieszczony na **współdzielonym dysku sesji** i staje się dostępny w sesji zdalnej:

- W środowiskach Windows dysk jest dostępny jako **FudoDrive** i widoczny w Eksploratorze plików w sekcji **Przekierowane dyski i foldery**.
- W środowiskach Ubuntu jest wyświetlany jako **thinclient_drive**.

Aby pobrać plik:

1. W sesji zdalnej zapisz plik w folderze *Downloads* na dysku współdzielonym.
2. Pobieranie rozpocznie się automatycznie w przeglądarce.

Ważne

Podczas przesyłania plików możesz kontynuować pracę w sesji. Po **zakończeniu sesji** dysk współdzielony i wszystkie jego **pliki są trwale usuwane**, a **historia** transferu plików jest **czyszczona**, więc ponowne połączenie rozpoczyna się z pustym dyskiem.

Tematy pokrewne:

- *RDP, VNC oraz SSH na połączeniu w przeglądarce*
- *RDP na systemie operacyjnym Mac OS*
- *RDP na systemie operacyjnym Microsoft Windows 7 i 10*
- *RDP na systemie operacyjnym Ubuntu*

1.11 Udostępnianie własnej sesji

Możesz udostępnić innej osobie sesję, którą prowadzisz, bez pomocy administratora. Przydaje się to, gdy potrzebujesz drugiej pary oczu przy wykonywanej pracy albo gdy część zadań ma przejąć współpracownik.

Uwaga

Opcja jest dostępna tylko wtedy, gdy administrator włączył udostępnianie sesji dla sejfu, do którego należy sesja. Jeśli nie widzisz ikony *Share session*, skontaktuj się z administratorem.

Tworzony link zawsze:

- wymaga od odbiorcy **zalogowania** do Fudo Enterprise, aby mógł zobaczyć sesję,
- pozwala odbiorcy **działać** w sesji, nie tylko ją obserwować,
- przestaje działać w chwili zakończenia Twojej sesji.

Ważne

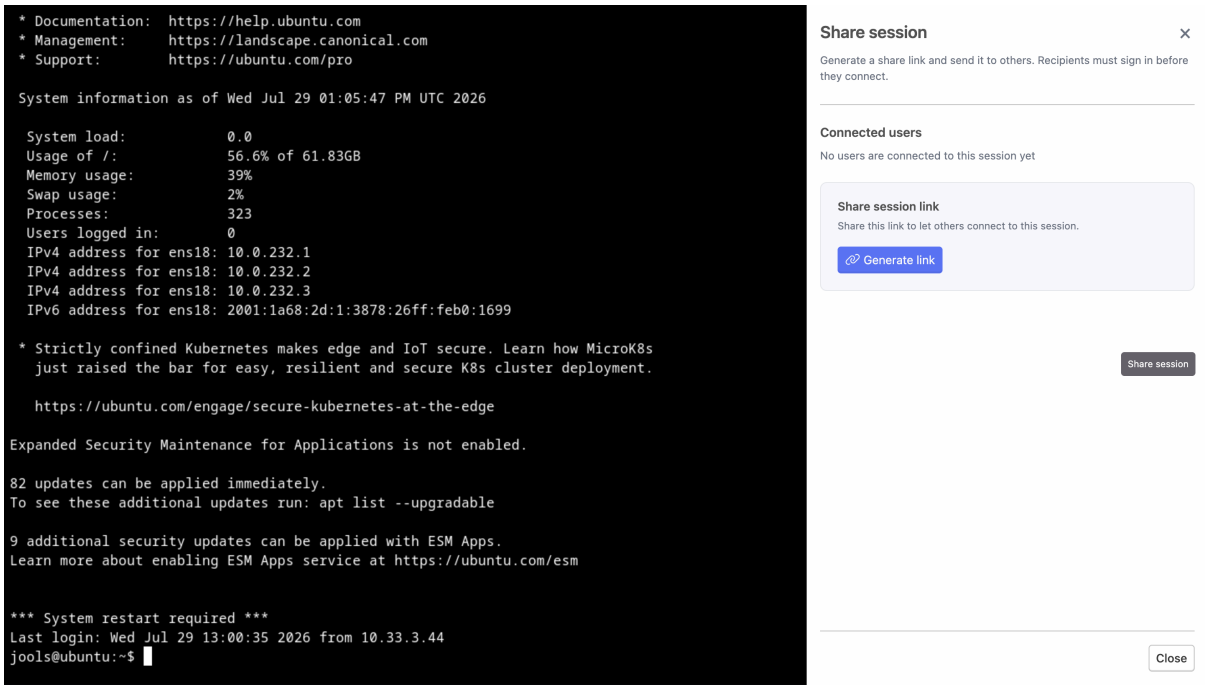
Do sesji może dołączyć każdy, kto zaloguje się do Fudo Enterprise i posiada Twój link. Wysyłaj link tylko do osób, które powinny widzieć, co się w niej dzieje.

Udostępnianie trwającej sesji

Aby udostępnić sesję, którą aktualnie prowadzisz, wykonaj następujące kroki.

1. W sesji klienta webowego kliknij *Share session* na pasku bocznym.

2. Kliknij *Generate link*.



3. Skopiuj link i wyślij go osobie, która ma dołączyć do sesji.

Lista *Connected users* w tym samym panelu pokazuje, kto jest aktualnie połączony z Twoją sesją. Dopóki nikt nie dołączył, wyświetlany jest komunikat *No users are connected to this session yet*.

Zakończenie udostępniania

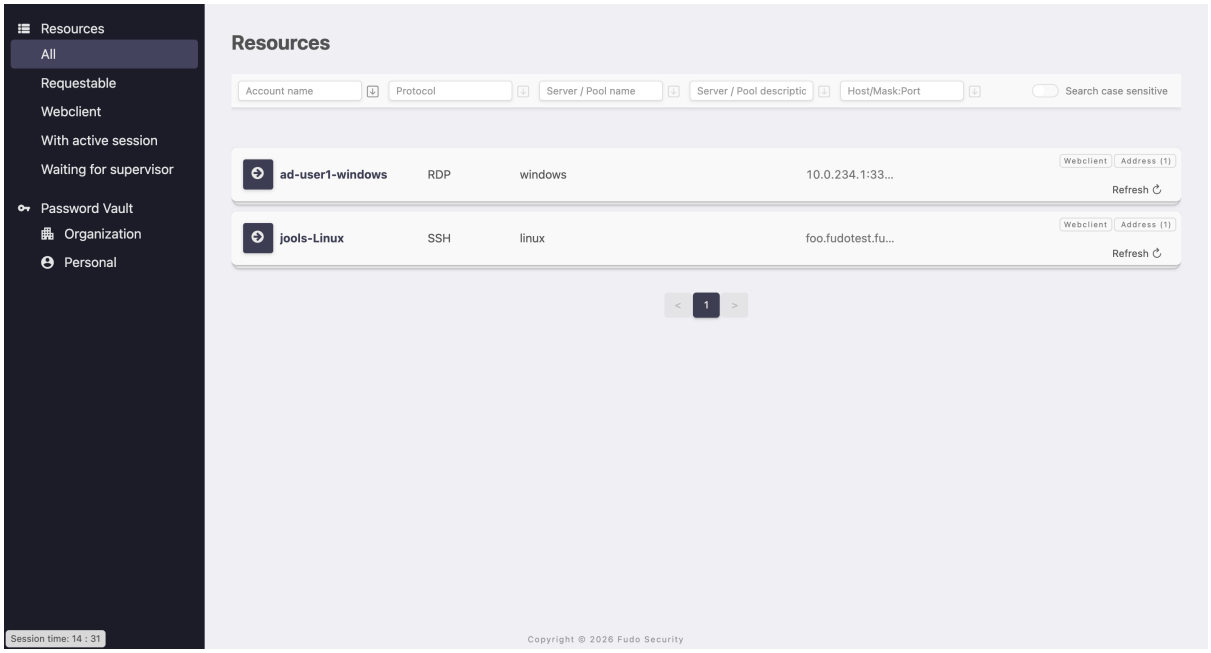
Aby przestać udostępniać sesję, kliknij *Deactivate* w panelu *Share session*. Link natychmiast przestaje działać, a osoby połączone za jego pomocą zostają odłączone.

Link przestaje też działać samoczynnie w chwili zakończenia sesji, więc nie musisz go dezaktywować przed rozłączeniem.

Wyszukiwanie udostępnionych sesji

Lista *Zasoby* udostępnia dwa filtry pomocne przy sesjach związanych z udostępnianiem:

- **With active session** - zasoby, na których masz aktualnie trwającą sesję,
- **Waiting for supervisor** - sesje, które nie mogą się rozpocząć, dopóki nie obserwuje ich wymagana liczba nadzorców.



Tematy pokrewne:

- *Funkcjonalności Webclienta*
- *RDP, VNC oraz SSH na połączeniu w przeglądarce*

1.12 Rozwiązywanie problemów

Problem	Objawy i opis rozwiązania
Nie można zalogować się do Portalu Użytkownika	**Objawy:** • Użytkownik nie może się zalogować.
	Rozwiązanie: • Upewnij się, że wprowadzasz prawidłowe dane logowania. • Skontaktuj się z administratorem, w celu zweryfikowania praw dostępu do Portalu Użytkownika. • Skontaktuj się z administratorem, w celu zweryfikowania polityki czasowej dostępu do Portalu Użytkownika.

Problem	Objawy i opis rozwiązania
Na liście gniazd nasłuchiwania brakuje obiektów.	**Przyczyna:** • Skontaktuj się z administratorem, w celu potwierdzenia przypisania do odpowiedniego sejfu.
	Objawy: • Nie można nawiązać połączenia z wybranym serwerem.
	Przyczyna: połączenie ma miejsce poza godzinami zdefiniowanymi w polityce czasowej dostępu do sejfu obsługującego wybrane połączenie.
	Rozwiązanie: skontaktuj się z administratorem w celu w celu zweryfikowania ustawień polityki czasowej.

Problem	Objawy i opis rozwiązania
Sekcja jest wyszarzona i nie da się jej otworzyć.	**Objawy:** • Sekcja *Zasoby* albo *Skarbiec haseł* jest wyszarzona i nie reaguje na kliknięcia. • Po wskazaniu sekcji kursorem wyświetlany jest komunikat informujący, że moduł został wyłączony dla tego konta. • Wpisanie adresu sekcji bezpośrednio w przeglądarce również jej nie otwiera.
	Przyczyna: odpowiedni moduł — PSM albo Skarbiec haseł — został wyłączony dla Twojego konta przez administratora.
	Rozwiązanie: skontaktuj się z administratorem w celu przywrócenia dostępu do modułu.