Pierwsza konfiguracja: panel admina, organizacja i zaproszenia

Poziom: podstawy **Dotyczy: Vaultwarden 1.37** **Czas: ~25 min**

Po instalacji kontenera Vaultwarden umie tylko przyjmować nowe konta. Ta strona prowadzi przez panel administracyjny, założenie organizacji „Zielona" z kolekcjami per dział, zaproszenie pierwszych osób i podłączenie klientów, żeby sejf zaczął realnie zastępować plik `hasla.xlsx`.

Skróty użyte na tej stronie (5)

Skrót	Co znaczy
2FA	Two Factor Authentication, dwuetapowe logowanie: drugi składnik logowania obok hasła głównego, na przykład kod z aplikacji uwierzytelniającej albo klucz sprzętowy
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
TOTP	Time based One Time Password: jednorazowy kod zmieniający się co chwilę, generowany przez aplikację uwierzytelniającą jako jedna z metod dwuetapowego logowania

Fiszka

TYLKO ODCZYT

Otwarcie panelu administracyjnego: adres w przeglądarce

```
https://hasla.zielona.example/admin
```

Panel prosi o hasło ustawione przy generowaniu `ADMIN_TOKEN` na stronie Instalacja Vaultwardena w Dockerze. Stąd zarządzamy całą instancją: listą kont, ustawieniami SMTP, diagnostyką i konfiguracją serwera bez edycji `compose.yaml` dla części ustawień.

SMTP = Simple Mail Transfer Protocol: protokół wysyłania poczty

TYLKO ODCZYT

Założenie pierwszego konta i organizacji: interfejs Vaultwardena

```
https://hasla.zielona.example
```

Pierwsze konto zakładamy tak samo jak każde kolejne, przez formularz rejestracji, zanim jeszcze wyłączymy go ustawieniem `SIGNUPS_ALLOWED=false`. To konto, w Zielonej konto Oli, zakłada później organizację i zaprasza resztę zespołu.

KLIKAMY W INTERFEJSIE

Sprawdzenie listy kont z panelu administracyjnego: Users

```
/admin → Users
```

Pokazuje każde konto, datę utworzenia, datę ostatniego logowania i to, czy ma włączone dwuetapowe logowanie. Stąd też, jednym kliknięciem, dezaktywujemy konto osoby, która odeszła z firmy.

Z życia wzięte

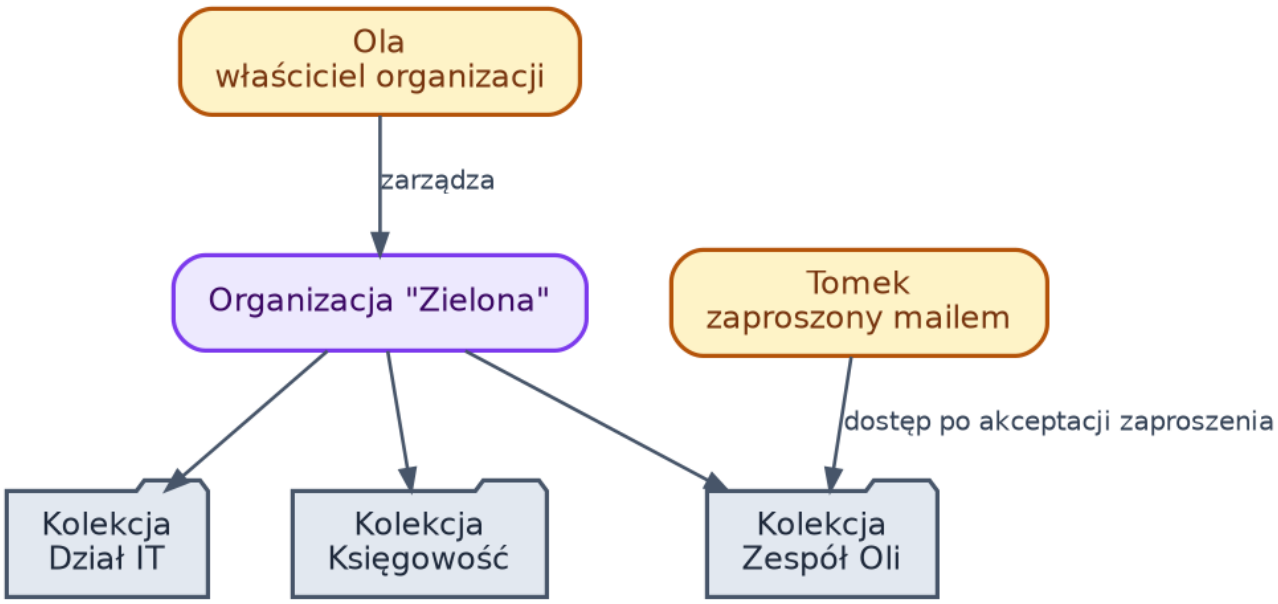
Z ŻYCIA WZIĘTE

Tomek dostaje polecenie zainstalowania rozszerzenia Vaultwarden w przeglądarce. Wchodzi na stronę Bitwardena, instaluje rozszerzenie ze sklepu i loguje się mailem służbowym. Rozszerzenie łączy się z chmurą oficjalnego Bitwardena, a nie z serwerem Zielonej, więc konto nie istnieje i logowanie kończy się błędem, mimo że konto w Vaultwardenie od dawna działa.

Organizacja i kolekcje

Pojęcie: organizacja. Kontener na wspólne hasła w Vaultwardenie, oddzielony od osobistego sejfu każdej osoby. Ola zakłada organizację „Zielona" jednym kreatorem w interfejsie, a każde kolejne konto dołącza do niej przez zaproszenie, nie przez założenie własnej.

Pojęcie: kolekcja. Podzbiór haseł wewnątrz organizacji, z osobnymi uprawnieniami dostępu. W Zielonej kolekcje pokrywają się z działami: `Dział IT`, `Księgowość`, `Zespół Oli`, każda widoczna tylko dla osób dodanych do niej wprost albo przez grupę.



Organizacja Zielona z kolekcjami per dział i dostępem po zaproszeniu (kliknięcie otwiera pełny rozmiar)

Zakładanie kolekcji i dodawanie do nich osób odbywa się wyłącznie przez interfejs webowy, nie przez CLI ani API wywoływane ręcznie: Vaultwarden, tak jak oficjalny Bitwarden, szyfruje nazwy i zawartość kolekcji kluczem organizacji po stronie klienta, więc utworzenie kolekcji „z linii poleceń" po stronie serwera nie miałoby jak wygenerować poprawnego szyfrowania.

```
Organizations → Zielona → Collections → New collection
```

Zaproszenia mailem

```
Organizations → Zielona → Members → Invite member
```

Zaproszenie trafia na adres e-mail przez MailCow, skonfigurowany na stronie instalacji. Osoba zaproszona klika link, zakłada hasło główne, jeśli jeszcze nie ma konta, i od razu widzi kolekcje, do których organizacja ją przypisała.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Organizations → Zielona → Members z widocznym wierszem zaproszonej osoby ze statusem „Invited" i przyciskiem „Resend invitation".

Polityki organizacji

> **Pojęcie: polityka organizacji.** Reguła wymuszana na wszystkich członkach organizacji, ustawiana raz przez właściciela, bez możliwości obejścia przez samego użytkownika. Vaultwarden nie wspiera całego zestawu polityk znanego z płatnych planów oficjalnego Bitwardena, ale kilka kluczowych działa i jest potwierdzone w dokumentacji projektu.

Polityka	Co robi w Zielonej
Single organization	blokuje należenie do więcej niż jednej organizacji naraz, przydatne, gdy chcemy mieć pewność, że nikt nie trzyma firmowych haseł też w prywatnej organizacji
Two factor authentication	wymusza dwuetapowe logowanie na każdym koncie organizacji, zanim zdąży ono cokolwiek zapisać w kolekcji
Account recovery administration	pozwala administratorowi zresetować hasło główne osobie, która je zapomniała, bez utraty dostępu do jej haseł w organizacji

Reszty polityk znanych z dokumentacji oficjalnego Bitwardena, na przykład wymuszania konkretnej siły hasła głównego, w danej wersji Vaultwardena sprawdzamy osobno w panelu `/admin`, zanim zaczniemy na nich polegać.

Dwuetapowe logowanie

> **Pojęcie: dwuetapowe logowanie.** Drugi składnik logowania obok hasła głównego: kod z aplikacji uwierzytelniającej, kod wysłany mailem albo klucz sprzętowy. W Vaultwardenie każde konto ma dostęp do wszystkich tych metod bez ograniczeń znanych z darmowego planu chmury oficjalnego Bitwardena.

Włączamy je z poziomu własnego konta, nie z panelu administratora, bo klucze drugiego składnika są częścią zaszyfrowanego profilu użytkownika:

```
Ustawienia konta → Security → Two-step Login
```

> W Zielonej zalecamy aplikację uwierzytelniającą (kod TOTP) jako podstawową metodę i klucz sprzętowy jako zapasową dla kont z dostępem do kolekcji `Dział IT`. Kod wysyłany mailem chroni słabiej: przejęta skrzynka pocztowa daje dostęp do obu składników logowania naraz.

Klienci: rozszerzenie i aplikacja

Każdy klient Bitwardena, rozszerzenie przeglądarki, aplikacja na komputer i aplikacja na telefon, domyślnie łączy się z chmurą oficjalnego Bitwardena. Zanim zalogujemy się kontem z Zielonej, wskazujemy własny serwer w ustawieniach klienta, dokładnie tym samym ekranem we wszystkich wersjach.

```
Ekran logowania → Ustawienia (ikona koła zębatego) → Self-hosted → Server URL:
https://hasla.zielona.example
```

Bez tego kroku klient próbuje zalogować konto, którego po prostu nie ma na serwerach Bitwardena, i zgłasza błąd logowania nieoddający prawdziwej przyczyny, dokładnie tak jak w scence z Tomkiem wyżej.

Częste błędy

Objaw	Przyczyna	Co robimy
Logowanie w rozszerzeniu kończy się błędem mimo poprawnego hasła	klient wskazuje domyślnie chmurę Bitwardena zamiast własnego serwera	ustawiamy `Self-hosted → Server URL` na `https://hasla.zielona.example` przed logowaniem

Objaw	Przyczyna	Co robimy
Zaproszona osoba nie dostaje maila	zła konfiguracja SMTP z instalacji albo mail w spamie	sprawdzamy `docker compose logs vaultwarden \

Objaw	Przyczyna	Co robimy
Nowa osoba widzi puste kolekcje po zaakceptowaniu zaproszenia	administrator nie przypisał jeszcze konta do żadnej kolekcji	`Organizations → Zielona → Members`, edytujemy dostęp do kolekcji przy koncie
Rejestracja wciąż działa mimo `SIGNUPS_ALLOWED=false`	zmienna nieprzeładowana po zmianie `.env`	`docker compose up -d` ponownie wczytuje zmienne środowiskowe

□□ Ćwiczenia

1. Wyjaśniamy, dlaczego kolekcję dla nowego działu zakładamy przez interfejs webowy, a nie komendą w kontenerze, tak jak konto administratora w Gitei.

Odpowiedź

Nazwa i zawartość kolekcji są szyfrowane po stronie klienta kluczem organizacji, który serwer nigdy nie widzi w postaci jawnej. Utworzenie kolekcji z linii poleceń po stronie serwera nie miałoby jak wygenerować poprawnego szyfrowania, więc Vaultwarden, tak jak oficjalny Bitwarden, zostawia tę operację wyłącznie klientom.

1. Nowa osoba w zespole zgłasza, że rozszerzenie przeglądarki każe jej logować się kontem Google albo Microsoft, którego nie ma w Zielonej. Wskazujemy pierwszy krok naprawy.

Odpowiedź

Sprawdzamy ustawienie `Self-hosted → Server URL` w rozszerzeniu: bez wskazania `https://hasla.zielona.example` klient domyślnie próbuje zalogować konto w chmurze oficjalnego Bitwardena, gdzie żadne konto z Zielonej nie istnieje.

Powiązane: Instalacja Vaultwardena w Dockerze · Konta z Active Directory: Directory Connector i SSO · MailCow

Źródła: github.com/dani-garcia/vaultwarden, wiki „Enabling admin page" · bitwarden.com/help/policies · vaultwarden.discourse.group, wątek „Manage 2FA methods"

Revision #23
Created 2026-09-28 16:58:02 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:28 UTC by Tomasz Konieczny