Jak zalogowa? si? do Arcane (przewodnik dla adminów)

Jak zalogowa? si? do Arcane (przewodnik dla adminów)

Adres Arcane: https://arcane.t-pizza.pl **Adres Authentika (SSO):** https://id.t-pizza.pl

Masz **dwa sposoby** logowania:

1. **Logowanie lokalne** (login + hasło bezpośrednio w Arcane) — działa zawsze, niezależnie od Authentika
2. **Logowanie przez Authentik (SSO/OIDC)** — wygodniejsze, jedno konto dla wielu usług w przyszłości

Strona logowania pokazuje **oba przyciski jednocześnie**: zwykły formularz login/password + przycisk „Sign in with Authentik".

Scenariusz A: Istniej?cy admin (Twój login ju? jest w Arcane)

Dotyczy: `admin-combo@t-pizza.pl`, `kamil.lendlewicz@telepizza.pl`, `matzxp84@gmail.com` — kontá utworzone przed wdrożeniem SSO.

Wariant A1 — najprostszy: zaloguj si? jak dawniej (lokalne has?o)

1. Otwórz https://arcane.t-pizza.pl
2. Wpisz **swój login** (email) + **lokalne hasło Arcane**
3. Kliknij **Sign in**
4. Gotowe — żaden Authentik nie jest potrzebny

To samo, co przed wdrożeniem SSO. Twoje hasło ani konto nie zostało zmienione.

Wariant A2 — przejd? na SSO (zalecane na przysz?o??)

Wymaga: konta w Authentiku z **tym samym emailem** co konto w Arcane.

Krok 1 — admin Authentika (m.fleis) utworzy ci konto:

- Otwiera https://id.t-pizza.pl/if/admin/ → Directory → Users → Create
- Username: `kamil.lendlewicz` (część przed `@`)
- Email: `kamil.lendlewicz@telepizza.pl` ← **MUSI być identyczny** z emailem w Arcane (bez tego konta się nie skleją)
- Name: imię i nazwisko
- Path: `users`
- Klika **Create**
- Następnie w detalach usera klika **Set Password** lub **Email password reset link**
- Dodaje cię do grupy `arcane-admin` (Directory → Groups → arcane-admin → Members → Add)

Krok 2 — Ty się logujesz:

1. Otwierasz https://arcane.t-pizza.pl
2. Klikasz **Sign in with Authentik**
3. Authentik prosi o login/hasło → wpisujesz swoje dane z Authentika
4. (Jeśli pierwszy raz logujesz się do Arcane przez SSO) Authentik pokaże ekran „Authorize" — kliknij **Authorize**
5. Wracasz do Arcane jako zalogowany admin

Co się stało pod spodem: Arcane dostał z Authentika twój email `kamil.lendlewicz@telepizza.pl`. Sprawdził lokalną bazę → znalazł istniejące konto z tym emailem → skleił konta (`oidcMergeAccounts=true`). Od tego momentu możesz logować się oboma sposobami — to ten sam user.

Co je?li zapomnia?em lokalnego has?a Arcane?

Arcane nie ma self-service password reset. Inny admin musi zresetować:

- Inny admin loguje się do Arcane → Settings → Users → znajdź usera → **Reset password**
- Albo: wszyscy adminowie z dostępem do VPS-a mogą zresetować via API (technical procedure dla zaufanych)

Alternatywa: jeśli admin Authentika utworzy ci konto z tym samym emailem, możesz zalogować się przez SSO (nie potrzebując lokalnego hasła) — następnie w Arcane → Profile → Set password

ustaw nowe lokalne hasło.

Scenariusz B: Nowy admin (nikt go nie ma w Arcane)

Dotyczy: ktoś nowy w organizacji, kto nie ma jeszcze konta w Arcane.

Wymagania

- Konto w Authentik (zakłada admin Authentika, m.fleis)
- Członkostwo w grupie `arcane-admin` w Authentik (claim który Arcane mapuje na rolę admin)

Procedura dla admina Authentika

1. Otwórz https://id.t-pizza.pl/if/admin/ → **Directory → Users → Create**
2. Wypełnij:
   - **Username:** np. `j.kowalski` (część przed `@`)
   - **Email:** `j.kowalski@telepizza.pl` (pełny email)
   - **Name:** Jan Kowalski
   - **Path:** `users`
3. Kliknij **Create**
4. W detalach świeżo utworzonego usera kliknij ⋮ → **Set password** (wpisz tymczasowe hasło i przekaż userowi przez bezpieczny kanał) **LUB** ⋮ → **Email password reset link** (system wyśle link na email — wymaga SMTP, mamy skonfigurowany)
5. **Directory → Groups →** `arcane-admin` **→ Users → Add existing user** → wybierz `j.kowalski` → Add

Procedura dla nowego admina (Jan Kowalski)

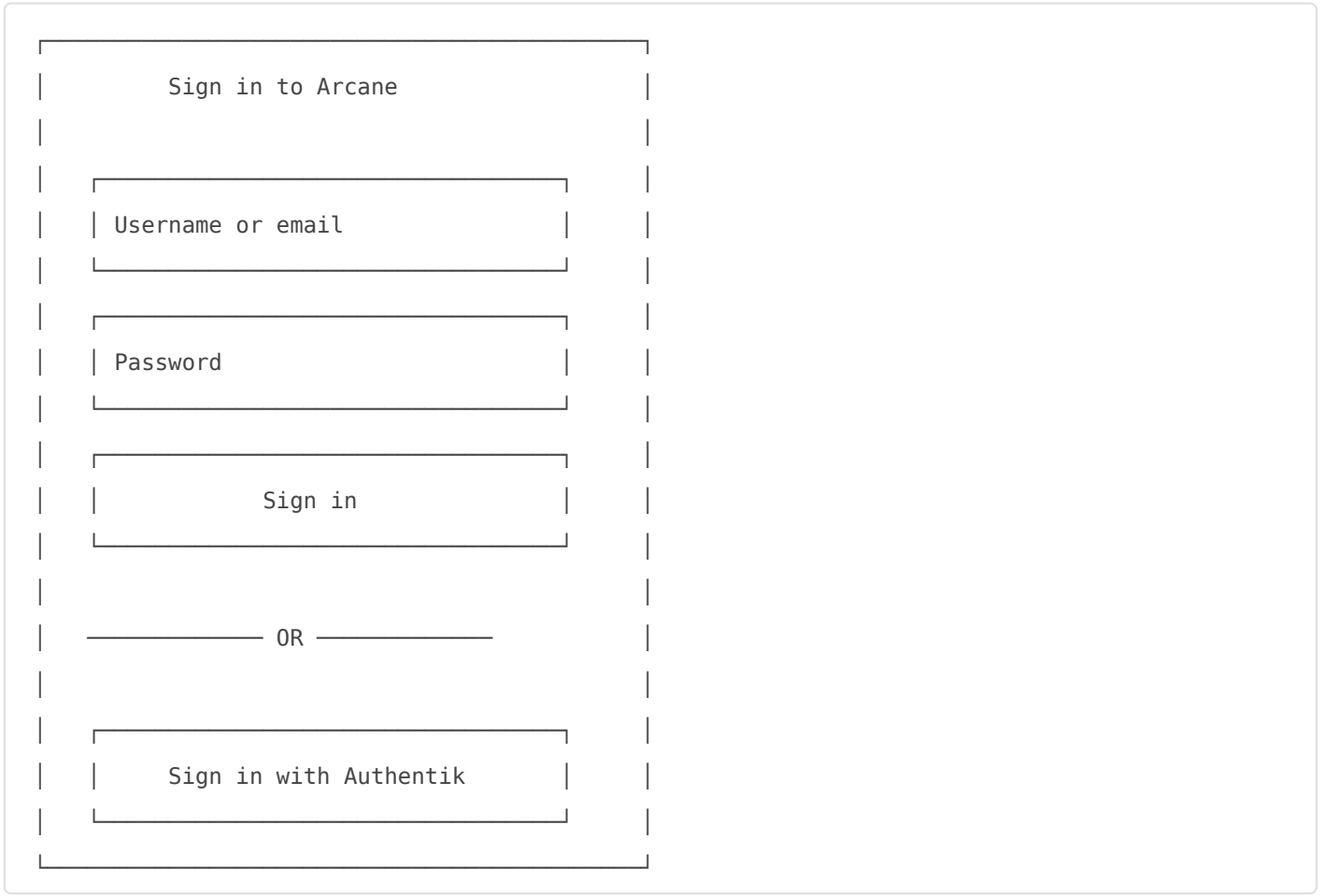
1. Sprawdź skrzynkę `j.kowalski@telepizza.pl` — jeśli admin Authentika wysłał link resetu hasła, kliknij go i ustaw swoje hasło
2. Otwórz https://arcane.t-pizza.pl
3. Kliknij **Sign in with Authentik**
4. Authentik prosi o login/hasło → wpisz `j.kowalski` (lub `j.kowalski@telepizza.pl`) + hasło ustawione w kroku 1
5. (Pierwszy raz) Kliknij **Authorize** na ekranie consent
6. Wracasz do Arcane — **konto zostało utworzone automatycznie** (Arcane nie miał takiego usera, więc go utworzył przy pierwszym SSO login)

7. Sprawdź: w prawym górnym rogu Arcane powinieneś widzieć swój email + ikonkę admin

Od teraz logujesz się tylko przez SSO. Twoje hasło w Arcane nie istnieje (chyba że je sobie wyklikasz w Profile → Set password — to dodatkowe lokalne hasło dla scenariusza break-glass).

Co wida? na stronie logowania

Strona `https://arcane.t-pizza.pl` (gdy nie jesteś zalogowany) wygląda tak:



- **Górna część** — logowanie lokalne (login/hasło bezpośrednio w Arcane). Działa dla `admin-combo`, `kamil.lendlewicz`, `matzxp84`.
- **Dolny przycisk** — przekierowanie do Authentika. Po loginie w Authentiku wracasz tu zalogowany.

Mapowanie ról i dost?p do aplikacji

W Authentiku jest **policy binding** na aplikacji `Arcane`: tylko członkowie grupy **`arcane-admin`** widzą i mogą używać aplikacji. Jeśli ktoś zaloguje się do Authentika ale nie jest w `arcane-admin`, na ekranie

consent dostanie błąd "permission denied" / "Application is not accessible to this user".

Wewnątrz Arcane: claim `groups` z ID tokenu mapuje się na rolę:

Twoja grupa w Authentik	Co widzisz w Arcane (po SSO)
`arcane-admin`	**admin** (pełne uprawnienia, widzisz aplikację, możesz zarządzać kontenerami)
inna / żadna	**dostęp odrzucony przez policy** — nie zobaczysz aplikacji w Authentiku

Wniosek: żeby ktoś mógł zalogować się do Arcane przez SSO, **musi być w grupie** `arcane-admin` **w Authentiku**. Nie ma „zwykłego usera SSO" — albo admin, albo nie wpuszczamy.

Dla istniejących adminów lokalnych (`admin-combo`, `kamil.lendlewicz`, `matzxp84`): ich rola admin jest zapisana lokalnie w Arcane — działa niezależnie od Authentika. Po sklejeniu kont (mergeAccounts) zachowują rolę admin.

FAQ

P: Co jeśli Authentik padnie / nie odpowiada? O: Strona logowania Arcane nadal pokazuje formularz lokalny — możesz zalogować się hasłem bezpośrednio w Arcane (jeśli masz lokalne konto). Authentik jest opcjonalną drogą, nie obowiązkową.

P: Mogę zalogować się raz przez SSO, a innym razem lokalnym hasłem? O: Tak, jeśli masz oba: konto w Authentiku **i** lokalne hasło w Arcane. Konta są sklejone, więc to ten sam user — ale możesz wybrać sposób logowania za każdym razem.

P: Czy SSO obejmuje też combo.t-pizza.pl? O: Nie, na razie tylko Arcane. Combo-raport-app ma własny system użytkowników (lokalny). W przyszłości można dodać OIDC client do `combo-raport-app` i wpiąć tę samą aplikację w Authentiku.

P: Jak zmienić swoje hasło w Authentiku? O: https://id.t-pizza.pl/if/user/ → User settings (ikona w prawym górnym rogu) → Change password.

P: Jak zmienić swoje hasło lokalne w Arcane? O: Po zalogowaniu w Arcane → Profile (prawy górny róg) → Set/Change password. Tylko lokalnie — nie wpływa na Authentika.

P: Co znaczy „mergeAccounts" w praktyce? O: Authentik wysyła email do Arcane. Arcane szuka usera z tym emailem:

- **Znalazł** lokalnego → ten sam user, dodaje połączenie z OIDC (od teraz oba sposoby logowania).

- **Nie znalazł** → tworzy nowego usera (tylko OIDC, bez lokalnego hasła do czasu aż user sam je ustawi).

P: Jak admin Authentika może zobaczyć kto się zalogował? O: https://id.t-pizza.pl/if/admin/ → Events → wszystkie eventy login/logout/authorize.

P: Czy hasło z Authentika jest takie samo jak z Arcane? O: **Nie.** To dwa oddzielne hasła (chyba że celowo ustawisz takie same). Authentik trzyma swoje hasło w swojej bazie; Arcane trzyma swoje lokalne hasło osobno. SSO oznacza tylko że Arcane *ufa* Authentikowi że potwierdził tożsamość — nie wymienia haseł.

Lista obecnych userów (stan na 2026-05-28)

W Arcane (lokalni adminowie)

Email	Username	Rola	Konto w Authentik?
`admin-combo@t-pizza.pl`	admin-combo@t-pizza.pl	admin	**tak** (utworzone 2026-05-28, gotowe do SSO)
`kamil.lendlewicz@telepizza.pl`	kamil.lendlewicz@telepizza.pl	admin	**tak** (utworzone 2026-05-28, gotowe do SSO)
`matzxp84@gmail.com`	matzxp84	admin	**tak** (utworzone 2026-05-28, gotowe do SSO)
`m.fleis@czcyber.pl`	akadmin	admin	**tak** (zlane z Authentik akadmin, super-admin Authentika)

W Authentik (wszyscy w grupie `arcane-admin`)

Username	Email	Grupy	Hasło startowe
`akadmin`	m.fleis@czcyber.pl	authentik Admins, arcane-admin	ustawione wcześniej
`admin-combo`	admin-combo@t-pizza.pl	arcane-admin	wygenerowane, zapisane w `~/.secrets/authentik-users.env`
`kamil.lendlewicz`	kamil.lendlewicz@telepizza.pl	arcane-admin	wygenerowane, zapisane w `~/.secrets/authentik-users.env`

Username	Email	Grupy	Hasło startowe
`matzxp84`	matzxp84@gmail.com	arcane-admin	wygenerowane, zapisane w `~/.secrets/authentik-users.env`

Przy pierwszym logowaniu SSO: user wpisuje swoje hasło startowe w Authentiku → Arcane mergeAccounts wykrywa pasujący email → konto w Arcane staje się dostępne także przez SSO (lokalne hasło Arcane dalej działa równolegle).

Zalecane: każdy user po pierwszym loginie powinien zmienić hasło: https://id.t-pizza.pl/if/user/ → User settings → Change password.

Policy binding (kto widzi aplikacj? Arcane)

Aplikacja `Arcane` w Authentiku ma policy binding (pk=`4a4d46af-...`, enabled, order=0): wymaga członkostwa w grupie `arcane-admin`. Jeśli ktoś spoza tej grupy zaloguje się do Authentika i kliknie aplikację Arcane → dostanie błąd "permission denied".

To znaczy: żeby kogoś dopuścić do Arcane przez SSO, **wystarczy dodać go do grupy `arcane-admin`** w Authentiku (Directory → Groups → arcane-admin → Users → Add existing user). Nie trzeba nic robić po stronie Arcane — wszystko dzieje się przez claim `groups` w ID tokenie.

Dla adminów Authentika — quick reference

Utwórz usera: Directory → Users → Create **Dodaj do grupy:** Directory → Groups → `arcane-admin` → Users → Add existing **Reset hasła:** Directory → Users → wybierz usera → ⋮ → Set password / Email password reset link **Wyłącz usera:** Directory → Users → wybierz usera → ⋮ → Set inactive (zostaje w bazie, ale nie może się logować) **Usuń usera:** Directory → Users → wybierz usera → ⋮ → Delete (UWAGA: nieodwracalne) **Eventy login:** Events → Logs (filtruj po username) **Sesje aktywne:** Directory → Users → wybierz usera → tab "Sessions" → Revoke

Break-glass (jeśli `akadmin` zgubi hasło):

```
ssh root@212.132.103.157
docker exec authentik-worker ak shell -c "
from authentik.core.models import User
u = User.objects.get(username='akadmin')
u.set_password('NOWE-HASLO-TUTAJ')
u.save()
print('OK')
```

"

Revision #4
Created 2026-05-28 04:00:58 CEST by matzxp84
Updated 2026-05-28 04:34:04 CEST by matzxp84