



Compass Hub

Instrukcja instalacji dla działu IT

wersja 0.9.2 · październik 2026

Loonar Mariusz Głowacki
ul. Gombrowicza 12, 73-110 Stargard
loonar.eu · mariusz@loonar.eu

Spis treści

1. [Co instalujesz](#)
2. [Zanim zaczniesz](#)
3. [Krok 1 – Pliki i folder](#)
4. [Krok 2 – hub,json i modele](#)
5. [Krok 3 – Sekrety](#)
6. [Krok 4 – Usługa Windows i pierwsze logowanie](#)
7. [Krok 5 – HTTPS przez IIS \(URL Rewrite + ARR\)](#)
8. [Krok 6 – Logowanie kontem firmowym \(AD FS lub Entra ID\)](#)
9. [Krok 7 – Klucze AI, Jira, Confluence i polityka zespołu](#)
10. [Krok 8 – Stacje robocze \(zasady grupy\)](#)
11. [Krok 9 – Lista odbiorcza](#)
12. [Eksploatacja: aktualizacja, kopia zapasowa, logi, usunięcie](#)
13. [Rozwiązywanie problemów](#)
14. [Linux i Docker](#)

1. Co instalujesz

Compass Hub to usługa zespołowa Loonar Compass. Jest to jeden program, `compass-hub.exe`, bez instalatora i bez Enterprise Architect. Działa jako usługa Windows i przechowuje:

- modele EA zespołu (tylko do odczytu): pliki `.qea` / `.qeax` albo repozytorium PostgreSQL, SQL Server, MySQL lub Oracle;
- politykę zespołu, którą stosują aplikacje Compass: minimalny tryb zatwierdzania, dostęp do internetu, AI tylko przez hub itd.;
- dziennik audytu zmian ze wszystkich stacji, zestawy zmian do przeglądu i widok webowy dla osób bez EA;
- bramkę AI: klucze Claude API zostają na serwerze, z kluczem i limitami na osobę lub rolę;
- Jirę i Confluence przez jedno konto serwisowe, API GraphQL tylko do odczytu, tabele dla Power BI i serwer MCP.

Gdzie	Co	Sieć
Serwer huba	Usługa <code>CompassHub</code> (<code>compass-hub.exe</code>), nasłuchuje tylko na <code>127.0.0.1:8730</code>	Tylko lokalnie
Serwer huba	Witryna IIS <code>https://hub.firma.pl</code> z URL Rewrite + ARR przed usługą	Ruch przychodzący 443 ze stacji
Dostawca tożsamości	AD FS albo Microsoft Entra ID: aplikacja „Compass Hub” (OpenID Connect)	Przeglądarka użytkownika
Serwer huba → internet	<code>api.anthropic.com</code> (bramka AI), witryna Atlassian (Jira/Confluence)	Ruch wychodzący 443, tylko dla używanych części
Stacje robocze	Loonar Compass (aplikacja i dodatek w EA), ustawienia wymuszone zasadami grupy	Ruch wychodzący 443 do huba

To jest konfiguracja przetestowana od początku do końca na Windows Server 2022 z AD, AD CS, AD FS i IIS. Każdy krok kończy się sprawdzeniem, więc problem wychodzi w kroku, który go spowodował.

2. Zanim zaczniesz

✓	Element	Uwagi
☐	Windows Server 2019 lub 2022, x64	2 vCPU, 4 GB RAM i 2 GB dysku wystarczą dla zespołu; więcej dysku na duże pliki modeli. Bez Enterprise Architect.
☐	Nazwa DNS, np. <code>hub.firma.pl</code>	Rozwiązywalna ze stacji roboczych.
☐	Certyfikat TLS dla tej nazwy	Z firmowego CA albo publicznego. Stacje muszą ufać jego głównemu urzędowi (Compass sprawdza go w magazynie certyfikatów Windows). Nazwa huba musi być w SAN certyfikatu; z AD CS konto, które o niego prosi, potrzebuje prawa Enroll do szablonu Web Server.
☐	IIS z modułami URL Rewrite i Application Request Routing (ARR)	Do pobrania od Microsoft (iis.net).
☐	AD FS (Windows Server) albo Microsoft Entra ID	Tylko do logowania kontem firmowym, które jest zalecane. Bez niego hub ma własnych użytkowników i hasła.
☐	Grupy AD: <code>Compass-Admins</code> , <code>Compass-Architects</code> , <code>Compass-Viewers</code>	Grupa daje rolę w hubie. Możliwe inne nazwy (krok 6).
☐	Modele	Pliki .qea skopiowane na serwer albo dostęp do bazy repozytorium EA (wystarczy konto tylko do odczytu).
☐	Sekrety u osoby, która instaluje	Klucz(e) Claude API, token API Atlassian, sekret klienta OIDC, hasło do bazy. Nigdy nie trafiają do hub.json.
☐	Wychodzące HTTPS z serwera	<code>api.anthropic.com</code> (bramka AI), Twoja witryna Atlassian (Jira/Confluence). Przez proxy: ustaw <code>HTTPS_PROXY</code> dla usługi (krok 3).

Pliki z wydania: `CompassHub-0.9.0-windows-x64.zip` (z `compass-hub.exe`, `hub.example.json`, `README.md` i licencjami), a dla stacji `LoonarCompass-Setup-0.9.exe` oraz folder `policies` (ADMX/ADML).

3. Krok 1 – Pliki i folder

1. Sprawdź SHA-256 pobranego pliku z wartością opublikowaną przy wydaniu:

```
Get-FileHash .\CompassHub-0.9.0-windows-x64.zip -Algorithm SHA256
```

2. Rozpakuj go do `C:\CompassHub` i utwórz podfoldery `models` i `secrets`.
3. Ogranicz dostęp do folderu do usługi i administratorów. Hub zapisuje tu swoje dane, a tu leżą sekrety:

```
icacls C:\CompassHub /inheritance:r /grant:r "SYSTEM:(OI)(CI)F" "BUILTIN\Administrators:(OI)(CI)F"
```

W polskim Windows grupa nazywa się `BUILTIN\Administratorzy`; zamiast nazwy można podać SID `*S-1-5-32-544`.

Sprawdzenie: `C:\CompassHub\compass-hub.exe --version` wypisuje `0.9.0`.

4. Krok 2 – hub.json i modele

Skopiuj `hub.example.json` do `C:\CompassHub\hub.json`. Minimalny start:

```
{
  "listen": "127.0.0.1:8730",
  "sources": [
    { "id": "architecture", "name": "Architektura korporacyjna", "properties":
"models/architecture.properties" }
  ],
  "policy": { "min_approval": "ask" }
}
```

- `listen` zostaje na `127.0.0.1`: z hubem rozmawia tylko IIS na tym samym serwerze.
- `sources`: jeden wpis na model. `id` ma być krótkie i stałe, bo używają go użytkownicy i Power BI. `properties` jest względne wobec `hub.json`.
- Pomiń `users`: hub utworzy wtedy konto `admin` (krok 4) i sam zapisze użytkowników, tylko jako skróty.

Plik modelu, np. `C:\CompassHub\models\architecture.properties`:

```
# Plik projektu EA (tylko odczyt)
model.source=file
model.file=C:/CompassHub/models/Architecture.qea

# ... albo baza repozytorium (hasło to sekret DB_PASSWORD):
# model.source=sqlserver          (albo postgres, mysql, oracle)
# db.host=sql.firma.pl
# db.port=1433
# db.name=ea_repository
# db.user=compass_reader
# db.sslmode=verify-full
```

SQL Server, MySQL i Oracle są czytane przez 64-bitowy sterownik ODBC producenta, który musi być zainstalowany na serwerze. Dla SQL Server wystarczy „ODBC Driver 17 for SQL Server” (instaluje się z SQL

Server 2022) albo 18; zainstalowane sterowniki: `Get-OdbcDriver -Name '*SQL Server*' -Platform 64-bit`. PostgreSQL i pliki nie potrzebują niczego więcej. Każdy odczyt jest wycofywany, więc wystarczy konto bazy tylko do odczytu. SQL Server bez sekretu `DB_PASSWORD` używa uwierzytelniania Windows: usługa huba (LocalSystem) loguje się kontem komputera (`DOMENA\SERWER$`), które potrzebuje roli `db_datareader` w bazie modelu.

- **Instancja nazwana** (np. SQL Server Express): `db.host=SERWER\SQLEXPRESS` bez portu, przy działającej usłudze SQL Server Browser; albo stały port TCP (SQL Server Configuration Manager → TCP/IP → IPAll: TcpPort 1433, TcpDynamicPorts puste) i `db.host / db.port`.
- **Własny ciąg połączenia:** `db.odbc=Driver={ODBC Driver 17 for SQL Server};Server=sql.firma.pl,1433;Database=ea_repository;Trusted_Connection=Yes` zastępuje host, port, nazwę i użytkownika (bez hasła; `DB_PASSWORD`, jeśli jest, zostaje dodane).
- **db.sslmode** dla SQL Server: `prefer` = szyfrowanie, gdy serwer i sterownik go używają (bez sprawdzania certyfikatu); `require` = zawsze szyfrowane, certyfikat nie jest sprawdzany; `verify-full` = szyfrowane, a certyfikat musi być zaufany i zgodny z nazwą serwera (nie z certyfikatem samopodpisanym SQL Server).

Trzymaj pliki modeli huba osobno od plików, które ludzie edytują w EA. Aby odświeżyć model plikowy, podmień plik. Hub otwiera go tylko do odczytu przy każdym zapytaniu, więc restart nie jest potrzebny.

5. Krok 3 – Sekrety

Każdy sekret to plik tekstowy w `C:\CompassHub\secrets`, który zawiera tylko wartość. Usługa poznaje ścieżkę ze zmiennej środowiskowej `LOONAR_SECRET_<NAZWA>_FILE`. Plik tworzy osoba, która zna wartość, np. w Notatniku albo poleceniem:

```
Read-Host -AsSecureString "Wartość" | ConvertFrom-SecureString -AsPlainText | Set-Content
C:\CompassHub\secrets\claude_key_team -NoNewline
```

(`-AsPlainText` wymaga PowerShell 7; w Windows PowerShell 5.1 prościej użyć Notatnika.)

Plik (przykład)	Zmienna dla usługi	Potrzebny do
<code>claude_key_team</code>	<code>LOONAR_SECRET_CLAUDE_KEY_TEAM_FILE</code>	Bramka AI: jedna zmienna na każdy klucz wskazany w hub.json (krok 7)
<code>claude_api_key</code>	<code>LOONAR_SECRET_CLAUDE_API_KEY_FILE</code>	„Zapytaj” w widoku webowym
<code>jira_token</code>	<code>LOONAR_SECRET_JIRA_TOKEN_FILE</code>	Jira
<code>confluence_token</code>	<code>LOONAR_SECRET_CONFLUENCE_TOKEN_FILE</code>	Confluence
<code>oidc_client_secret</code>	<code>LOONAR_SECRET_OIDC_CLIENT_SECRET_FILE</code>	Logowanie kontem firmowym
<code>db_password</code>	<code>LOONAR_SECRET_DB_PASSWORD_FILE</code>	Baza modelu

Nazwa w zmiennej to nazwa sekretu wielkimi literami, z innymi znakami zamienionymi na `_`: sekret `claude_key_anna` z hub.json to `LOONAR_SECRET_CLAUDE_KEY_ANNA_FILE`.

Zmienne ustawia się **tylko dla usługi**, nie dla całego komputera, po zainstalowaniu usługi (krok 4). Działa to od następnego startu usługi, bez restartu serwera:

```
$vars = @(
  'LOONAR_SECRET_CLAUDE_KEY_TEAM_FILE=C:\CompassHub\secrets\claude_key_team',
  'LOONAR_SECRET_JIRA_TOKEN_FILE=C:\CompassHub\secrets\jira_token',
  'LOONAR_SECRET_CONFLUENCE_TOKEN_FILE=C:\CompassHub\secrets\confluence_token',
  'LOONAR_SECRET_OIDC_CLIENT_SECRET_FILE=C:\CompassHub\secrets\oidc_client_secret'
  # 'HTTPS_PROXY=http://proxy.firma.pl:8080'    tylko gdy serwer wychodzi przez proxy
)
Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\CompassHub -Name Environment -Type
MultiString -Value $vars
Restart-Service CompassHub
```

Hub czyta sekret, gdy pierwszy raz go potrzebuje. Brakujący jest zgłaszany tam, gdzie jest używany, np. „secret 'jira_token' is not set: give it as LOONAR_SECRET_JIRA_TOKEN (or a file named in LOONAR_SECRET_JIRA_TOKEN_FILE)”. Wartości nigdy nie pojawiają się w hub.json, w logach ani w widoku webowym. Znacznik BOM na początku oraz spacje i znak nowej linii na końcu pliku sekretu (Notatnik) są pomijane.

6. Krok 4 – Usługa Windows i pierwsze logowanie

1. W PowerShell jako administrator:

```
C:\CompassHub\compass-hub.exe --service-install C:\CompassHub\hub.json
```

Polecenie tworzy usługę `CompassHub` („Compass Hub (Loonar Compass team service)”) z automatycznym startem na koncie LocalSystem i ją uruchamia.

2. Teraz ustaw sekrety usługi (krok 3) i wykonaj `Restart-Service CompassHub`.
3. Na serwerze otwórz `http://127.0.0.1:8730/` i zaloguj się jako `admin` / `password` (z zerem). Hub od razu żąda nowego hasła i do tego czasu nie pozwala na nic innego. Hasło ma co najmniej 10 znaków. Zrób to **przed** krokiem 5, który udostępni hub w sieci.

Sprawdzenie:

- `Get-Service CompassHub` pokazuje Running;
- `C:\CompassHub\hub.log` pokazuje start i Twoje logowanie;
- widok webowy pokazuje model z kroku 2.

7. Krok 5 – HTTPS przez IIS (URL Rewrite + ARR)

Hub mówi zwykłym HTTP na 127.0.0.1. IIS daje mu firmową nazwę i certyfikat.

1. Zainstaluj IIS z URL Rewrite i ARR. Utwórz witrynę, np. **CompassHub**, z powiązaniem `https`, port 443, nazwą hosta `hub.firma.pl` i certyfikatem. Ścieżka fizyczna to pusty folder, np.

```
C:\inetpub\compasshub
```

2. Włącz proxy i wyłącz przepisywanie hosta w przekierowaniach. To jest **konieczne**; inaczej ARR przepisze przekierowanie do AD FS na adres huba i logowanie firmowe się nie uda. Ustaw też limit czasu dla długich odpowiedzi AI:

```
Import-Module WebAdministration
$p = 'MACHINE/WEBROOT/APPHOST'
Set-WebConfigurationProperty -PSPath $p -Filter system.webServer/proxy -Name enabled -Value True
Set-WebConfigurationProperty -PSPath $p -Filter system.webServer/proxy -Name
reverseRewriteHostInResponseHeaders -Value False
Set-WebConfigurationProperty -PSPath $p -Filter system.webServer/proxy -Name timeout -Value
'00:05:00'
```

3. Wstaw ten `web.config` do folderu witryny. Przekazuje on wszystko do huba i pozwala na zapytania do 32 MB, bo pytania z diagramami modelu są duże:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="CompassHub" stopProcessing="true">
          <match url="(.*)" />
          <action type="Rewrite" url="http://127.0.0.1:8730/{R:1}" />
        </rule>
      </rules>
    </rewrite>
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="33554432" />
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

4. Zapora: wpuść tylko ruch przychodzący 443. Portu 8730 nie otwiera się nigdy, bo hub nasłuchuje na 127.0.0.1.
5. AD FS na tym samym serwerze: AD FS też używa portu 443 (HTTP.sys). Zaznacz **Wymagaj oznaczania nazwy serwera (SNI)** w powiązaniu IIS (`New-WebBinding ... -SslFlags 1`), inaczej IIS i AD FS sobie przeszkadzają.
6. Hub nie potrzebuje `preserveHostHeader` ani `X-Forwarded-Proto` : jego adresy wynikają z `redirect_uri` w `hub.json`.

Hub ufa nagłówkowi `X-Forwarded-For` (dodawanemu przez ARR) tylko od proxy na tym samym komputerze. Dziennik audytu i blokada błędnych tokenów widzą wtedy prawdziwy adres klienta.

Sprawdzenie: ze stacji roboczej `https://hub.firma.pl/` pokazuje stronę logowania bez ostrzeżenia o certyfikacie.

8. Krok 6 – Logowanie kontem firmowym (AD FS lub Entra ID)

AD FS

1. AD FS Management → Application Groups → Add, potem szablon **Server application accessing a web API**, nazwa „Compass Hub”.
2. Server application:
 - zanotuj **client identifier**;
 - redirect URI: `https://hub.firma.pl/auth/callback`;
 - credentials: **Generate a shared secret**. Zapisz go od razu do `C:\CompassHub\secrets\oidc_client_secret`; AD FS pokazuje go tylko raz.
3. Web API:
 - identifier: client identifier z poprzedniego kroku;
 - access control policy: osoby, które mogą używać huba, np. „Permit everyone” (role i tak wynikają z grup);
 - permitted scopes: `openid`, `profile`, `email`, `allatclaims`.
4. Web API → Issuance Transform Rules → „Send LDAP Attributes as Claims” (Active Directory):
 - *User-Principal-Name* → `upn`;
 - *E-Mail-Addresses* → `email`;
 - *Display-Name* → `name`;
 - *Token-Groups - Unqualified Names* → `groups`.

(Nazwy oświadczeń wyjściowych wpisz dokładnie tak.)

W `hub.json` (hub sam dodaje `allatclaims` dla AD FS, żeby oświadczenia trafiły do ID tokenu):

```
"oidc": {
  "issuer": "https://adfs.firma.pl/adfs",
  "client_id": "<client identifier>",
  "redirect_uri": "https://hub.firma.pl/auth/callback",
  "groups_claim": "groups",
  "roles": { "admin": ["Compass-Admins"], "architect": ["Compass-Architects"], "viewer": ["Compass-Viewers"] },
  "password_login": true
}
```

Microsoft Entra ID

Konfiguracja w Entra ID:

- **App registration:** platforma *Web*, redirect URI `https://hub.firma.pl/auth/callback`, client secret (do pliku sekretu) i ID token z opcjonalnymi oświadczeniami `upn` i `email`.
- **Issuer:** `https://login.microsoftonline.com/<tenant-id>/v2.0`.
- **Grupy:** Entra domyślnie wysyła ich identyfikatory obiektów. Wpisz te identyfikatory w `roles` albo, dla grup synchronizowanych z AD, wybierz „SAMAccountName” w konfiguracji tokenu.

Zasady, które stosuje hub

- Rola wynika z grup przy każdym logowaniu i wygrywa najwyższa. Osoba spoza wszystkich grup nie dostaje dostępu.
- Konto firmowe o tej samej nazwie co lokalny użytkownik huba jest odrzucane, dopóki lokalny użytkownik nie zostanie przemianowany lub usunięty.
- Hub sam sprawdza ID token: podpis RS256, wystawcę, odbiorcę, ważność i nonce, z PKCE i jednorazowym state.
- Gdy wszystko działa, ustaw `"password_login": false` : zostaje tylko przycisk konta firmowego. Tokeny API dla klientów MCP dalej działają. Zachowaj w sejfie hasło jedno lokalne hasło admina na wypadek awarii dostawcy tożsamości.

Sprawdzenie: po `Restart-Service CompassHub` przycisk „Sign in with your company account” prowadzi do AD FS i z powrotem. `hub.log` pokazuje „... signed in with a company account as architect”, a zakładka **Users** pokazuje konto firmowe z rolą.

9. Krok 7 – Klucze AI, Jira, Confluence i polityka zespołu

Dodaj sekcje do `hub.json`. Każdy wskazany tu sekret potrzebuje też swojej zmiennej `..._FILE` (krok 3). Potem wykonaj `Restart-Service CompassHub`; zalogowane osoby pozostają zalogowane.

```
"ai": {
  "keys": [ { "for": "role:architect", "secret": "claude_key_team" },
            { "for": "anna@firma.pl", "secret": "claude_key_anna" } ],
  "limits": [ { "for": "*", "tokens_per_day": 2000000, "tokens_per_month": 30000000 } ],
  "models": [ "claude-haiku-5-5", "claude-sonnet-5-5" ]
},
"integrations": {
  "jira": { "url": "https://firma.atlassian.net", "user": "svc-compass@firma.pl", "project":
"ARCH", "issue_type": "Task" },
  "confluence": { "url": "https://firma.atlassian.net/wiki", "user": "svc-compass@firma.pl", "space":
"ARCH" }
},
"policy": {
  "min_approval": "ask",
  "ai_via_hub": true,
  "jira_via_hub": true,
  "confluence_via_hub": true,
  "web_access": false,
  "update_check": false
}
```

Ustawienie	Znaczenie
<code>ai.keys</code>	Którego klucza Claude używa osoba. Kolejność: nazwa użytkownika, potem <code>role:<rola></code> , potem <code>*</code> . Brak dopasowania oznacza brak AI dla tej osoby.
<code>ai.limits</code>	Tokens na dzień i na miesiąc. Po przekroczeniu hub odmawia z czytelnym komunikatem.
<code>ai.models</code>	Dozwolone modele; inne są odrzucane.
<code>policy.ai_via_hub</code>	Compass pyta AI tylko przez hub: na stacjach nie ma klucza API.
<code>policy.jira_via_hub</code> , <code>confluence_via_hub</code>	Jira/Confluence przez konto serwisowe huba. Viewer może tylko czytać; każda zmiana jest w audycie.
<code>policy.min_approval</code>	Najsłabszy dozwolony w Compass tryb zatwierdzania zapisów do modelu (<code>ask</code> jest najostrzejszy).
<code>policy.web_access</code> , <code>web_allowed_domains</code>	Czy asystent może szukać w internecie i czytać strony, i z jakich domen.
<code>policy.update_check</code>	Czy Compass co godzinę sprawdza na GitHubie nową wersję.

Administratorzy zmieniają później politykę w zakładce **Team policy** widoku webowego, a zużycie na osobę jest w **Users** → **AI usage**.

10. Krok 8 – Stacje robocze (zasady grupy)

- Zaufanie do certyfikatu.** Jeśli certyfikat huba pochodzi z firmowego CA, rozdaj jego główny urząd na stacje (GPO: Konfiguracja komputera → Zasady → Ustawienia systemu Windows → Ustawienia zabezpieczeń → Zasady kluczy publicznych → Zaufane główne urzędy certyfikacji). Bez tego Compass zgłasza niezauwany certyfikat (UnknownIssuer).
- Szablony.** Skopiuj `LoonarCompass.admx` do `\\<domena>\SYSVOL\<domena>\Policies\PolicyDefinitions`, a `pl-PL\LoonarCompass.adml` (i `en-US`) do podfolderów językowych. Bez magazynu centralnego skopiuj je do `C:\Windows\PolicyDefinitions` na komputerze, na którym edytujesz GPO.
- GPO dla OU stacji:** Konfiguracja komputera → Szablony administracyjne → Loonar → Loonar Compass.

Zasada	Wartość rejestru (HKLM\SOFTWARE\Policies\Loonar\Compass)	Działanie
Adres huba	<code>HubUrl</code> (tekst)	Adres huba jest ustalony w Compass i nie można go zmienić.
Wymagaj huba	<code>RequireHub</code> = 1	Asystent działa tylko wtedy, gdy osoba jest zalogowana do huba.
Dostęp do internetu	<code>WebAccess</code> = 0	Bez wyszukiwania i czytania stron; przycisk  jest wyłączony.
Sprawdzanie aktualizacji	<code>UpdateCheck</code> = 0	Bez codziennego sprawdzania nowej wersji.
Minimalny tryb zatwierdzania	<code>MinApproval</code> = ask / plan / auto	Nie można wybrać słabszego trybu.
Dozwoleni dostawcy AI	<code>AllowedProviders</code> , np. <code>anthropic</code>	Inni dostawcy (np. OpenAI) są odrzucani.

Bez domeny te same wartości można zaimportować plikiem `LoonarCompass-company-policy.reg` (i usunąć plikiem `LoonarCompass-remove-policy.reg`). Zasady komputera są silniejsze niż polityka huba i ustawienia użytkownika; mogą Compass tylko zaostrzyć.

Instalacja Compass. `LoonarCompass-Setup-0.9.exe` instaluje dla bieżącego użytkownika (`%LOCALAPPDATA%\Programs\Loonar Compass`) albo dla wszystkich (`Program Files`) i rejestruje dodatek w Enterprise Architect. Dla narzędzi wdrożeniowych (Intune, Configuration Manager, skrypt startowy) instaluje bez okna:

```
LoonarCompass-Setup-0.9.exe --quiet --all-users
```

Opcja	Działanie
<code>--quiet</code>	Bez okna i bez pytań. Kod wyjścia 0 = zainstalowano, 1 = błąd, 740 = <code>--all-users</code> bez uprawnień administratora. Wynik jest w <code>%TEMP%\LoonarCompass-Setup.log</code> (dla SYSTEM: <code>C:\Windows\Temp</code>).
<code>--all-users</code>	Dla wszystkich: Program Files, wspólne menu Start, dodatek w EA dla wszystkich użytkowników (HKLM). Uruchamiaj jako SYSTEM albo administrator.
<code>--dir <folder></code>	Inny folder programu.
<code>--lang en pl de fr</code>	Język plików licencji i listy zmian.
<code>--no-desktop, -- no-start-menu</code>	Bez tych skrótów.
<code>--no-ea-addin</code>	Bez dodatku w Enterprise Architect.

To samo polecenie aktualizuje istniejącą instalację. Najpierw zamknij Compass i EA na komputerze. Ustawienia użytkownika nie są zmieniane; przy zasadach komputera (adres huba, wymagany hub) nikt nie musi niczego konfigurować. Ciche usunięcie: `"C:\Program Files\Loonar Compass\uninstall.exe" --uninstall --quiet`.

Pierwsze logowanie użytkownika. W Compass: Ustawienia → Zespół (Compass Hub) → **Zaloguj się kontem firmowym**. Przeglądarka otwiera AD FS i wraca do Compass. Logowanie trwa 12 godzin i przetrwa restart huba.

11. Krok 9 – Lista odbiorcza

✓	Test	Oczekiwane
☐	Otwórz <code>https://hub.firma.pl/</code> ze stacji	Strona logowania, bez ostrzeżenia o certyfikacie
☐	Logowanie firmowe członka Compass-Architects	Rola architect; hub.log „signed in with a company account as architect”
☐	Osoba spoza grup Compass	Odmowa
☐	Compass z GPO, przed zalogowaniem: wyślij pytanie	„Twoja organizacja wymaga huba zespołu: zaloguj się w Ustawienia → Zespół (Compass Hub)...”
☐	To samo po zalogowaniu	Odpowiedź, bez klucza API na stacji; wiersz w Users → AI usage
☐	Viewer zadaje pytanie (brak klucza dla viewerów)	„the hub has no AI key for you”
☐	Przycisk  w Compass	Wyłączony: „wyłączyła Twoja organizacja”
☐	<code>Restart-Service CompassHub</code> , potem pytanie	Działa bez ponownego logowania
☐	Hub zatrzymany, pytanie	Krótki komunikat, że hub nie odpowiada; EA działa dalej
☐	Jira: „Utwórz w Jirze zadanie: test” (architect)	Zadanie w projekcie; wpis w audycie huba z nazwą osoby

12. Eksploatacja: aktualizacja, kopia zapasowa, logi, usunięcie

Aktualizacja

```
Stop-Service CompassHub
Copy-Item .\compass-hub.exe C:\CompassHub\compass-hub.exe -Force # z nowego zipa, po sprawdzeniu SHA-256
Start-Service CompassHub
```

hub.json, sekrety i logowania zostają bez zmian. Ludzie pozostają zalogowani.

Co archiwizować (C:\CompassHub)

Plik / folder	Zawartość
hub.json	Konfiguracja, lokalni użytkownicy (tylko skróty haseł i tokenów), polityka
audit.jsonl	Dziennik audytu zmian i logowań
changes\, notes\	Zestawy zmian do przeglądu i notatki zespołu
ai_usage.jsonl	Zużycie AI na osobę (podstawa limitów)
company_accounts.json , sessions.json	Widziane konta firmowe i bieżące logowania (skrót); ich utrata nie szkodzi, ludzie zalogują się ponownie
secrets\	Tylko jeśli kopia jest szyfrowana. W przeciwnym razie trzymaj wartości w sejfie haseł.
models\	Pliki modeli, jeśli nie są przechowywane gdzie indziej

Logi

- hub.log : start, logowania, odrzucone zapytania, błędy. „Internal error (id ...)” pokazany użytkownikowi ma tu szczegóły pod tym samym id.
- audit.jsonl i hub.log dostają datę w nazwie, gdy urosną.

Usunięcie

```
C:\CompassHub\compass-hub.exe --service-uninstall
```

Potem usuń witrynę IIS, grupę aplikacji AD FS i GPO, a po archiwizacji usuń C:\CompassHub .

13. Rozwiązywanie problemów

Objaw	Przyczyna i rozwiązanie
Compass: certyfikat niezaufany / UnknownIssuer; przeglądarka pokazuje „Niezabezpieczona”	Stacja nie ufa głównemu urzędowi certyfikatu huba. Rozdaj główny urząd CA (krok 8), potem uruchom ponownie przeglądarkę i Compass.
Logowanie firmowe kończy się na <code>https://hub.firma.pl/adfs/...</code> albo błędem 404	ARR przepisuje przekierowanie. Ustaw <code>reverseRewriteHostInResponseHeaders = False</code> (krok 5).
„<nazwa> is not in any group of the hub (...): ask the administrator for access”	Osoba nie należy do żadnej grupy ról albo brakuje oświadczenia <code>groups</code> . Sprawdź regułę „Token-Groups - Unqualified Names → groups” i zakres <code>allatclaims</code> .
„A local user of the hub has the same name”	Zmień nazwę lub usuń tego lokalnego użytkownika w zakładce Users.
Compass: „Hub zespołu albo serwer przed nim nie odpowiada poprawnie (502)”	Usługa jest zatrzymana albo się uruchamia: <code>Get-Service CompassHub</code> , potem <code>hub.log</code> .
Compass: „Logowanie do huba zespołu wygasło”	Minęło 12 godzin albo zginął <code>sessions.json</code> . Zaloguj się ponownie w Ustawienia → Zespół.
„the hub has no AI key for you”	Brak wpisu <code>ai.keys</code> dla osoby, jej roli albo <code>*</code> .
„your AI limit for today is used up”	Podnieś <code>ai.limits</code> dla osoby lub roli albo poczekaj do następnego dnia.
„secret '...' is not set: give it as LOONAR_SECRET_...”	Brak zmiennej <code>..._FILE</code> w <code>Environment</code> usługi albo plik jest pusty lub nieczytelny dla SYSTEM.
hub.log: „<adres>: 20 wrong tokens, refused for 10 minutes”	Z jednego adresu przyszło 20 różnych błędnych tokenów (ten sam stary token liczy się raz). Prawidłowe tokeny dalej działają. Znajdź klienta w <code>hub.log</code> .
Duże pytania kończą się błędem 413 albo 404.13	<code>maxAllowedContentLength</code> w <code>web.config</code> (krok 5).
Długie odpowiedzi kończą się 502.3 po 2 minutach	<code>timeout</code> ARR (krok 5).
AD FS: MSIS7628 z <code>Grant-AdfsApplicationPermission</code> zaraz po instalacji AD FS	Farma jeszcze się uruchamia: powtórz polecenie po kilku minutach.
hub.log / AD FS: MSIS9622 „Client authentication failed”	Plik sekretu nie zgadza się z AD FS. Wygeneruj nowy sekret: <code>Set-AdfsServerApplication -TargetIdentifier <client id> -ResetClientSecret</code> , zapisz go do pliku, <code>Restart-Service CompassHub</code> .

Compass na Windows Server (np. Usługi pulpitu zdalnego): eksport do PDF nie działa albo pierwsze logowanie do Office jest blokowane

Compass tworzy PDF-y Wordem i PowerPointem na komputerze, na którym działa. Na Windows Server pierwsze logowanie do Office może blokować Konfiguracja zwiększonych zabezpieczeń programu IE (odc.officeapps.live.com): dodaj strony logowania Office do zaufanych albo wyłącz to ustawienie dla użytkowników w Menedżerze serwera.

14. Linux i Docker

Ten sam hub działa w kontenerze. Folder danych (hub.json z `"listen": "0.0.0.0:8730"`, modele i pliki huba) jest montowany jako `/data` i musi być zapisywalny dla użytkownika 10001. Sekrety pochodzą ze zmiennych `LOONAR_SECRET_*` albo z sekretów Dockera przez `LOONAR_SECRET*_FILE`:

```
docker run -d --name compass-hub -p 127.0.0.1:8730:8730 -v /srv/compass-hub:/data \
-e LOONAR_SECRET_CLAUDE_KEY_TEAM_FILE=/run/secrets/claude_key_team \
ghcr.io/loonar-eu/compass-hub:0.9.0
```

Przed nim postaw nginx albo inne proxy HTTPS, jak w kroku 5. Proxy ma nie zmieniać nagłówka `Location` przekierowań, przekazywać `X-Forwarded-For`, przyjmować zapytania do 32 MB i mieć limit czasu 5 minut. Dla modeli w SQL Server, MySQL lub Oracle zbuduj własny obraz na bazie tego i dodaj linuksowy sterownik ODBC producenta.