



Compass Hub

Installationsanleitung für die IT

Version 0.9.2 · Oktober 2026

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

Inhalt

1. [Was Sie installieren](#)
2. [Bevor Sie beginnen](#)
3. [Schritt 1 – Dateien und Ordner](#)
4. [Schritt 2 – hub.json und die Modelle](#)
5. [Schritt 3 – Geheimnisse](#)
6. [Schritt 4 – Der Windows-Dienst und die erste Anmeldung](#)
7. [Schritt 5 – HTTPS mit IIS \(URL Rewrite + ARR\)](#)
8. [Schritt 6 – Firmenanmeldung \(AD FS oder Entra ID\)](#)
9. [Schritt 7 – KI-Schlüssel, Jira, Confluence und die Teamrichtlinie](#)
10. [Schritt 8 – Die Arbeitsplätze \(Gruppenrichtlinien\)](#)
11. [Schritt 9 – Abnahmecheckliste](#)
12. [Betrieb: Update, Sicherung, Protokolle, Entfernen](#)
13. [Fehlerbehebung](#)
14. [Linux und Docker](#)

1. Was Sie installieren

Compass Hub ist der Teamdienst von Loonar Compass. Er besteht aus einem einzigen Programm, `compass-hub.exe`, ohne Installationsprogramm und ohne Enterprise Architect. Er läuft als Windows-Dienst und verwaltet:

- die EA-Modelle des Teams (nur lesend): `.qea` / `.qeax` -Dateien oder ein PostgreSQL-, SQL-Server-, MySQL- oder Oracle-Repository;
- die Teamrichtlinie, der die Compass-Anwendungen folgen: den minimalen Freigabemodus, den Webzugriff, KI nur über den Hub usw.;
- das Audit-Protokoll der Änderungen von allen Arbeitsplätzen, die Änderungssätze zur Prüfung und eine Weboberfläche für Personen ohne EA;
- das KI-Gateway: Die Claude-API-Schlüssel bleiben auf dem Server, mit einem Schlüssel und Limits pro Person oder Rolle;
- Jira und Confluence über ein einziges Dienstkonto, eine schreibgeschützte GraphQL-API, Tabellen für Power BI und einen MCP-Server.

Wo	Was	Netzwerk
Hub-Server	Dienst <code>CompassHub</code> (<code>compass-hub.exe</code>), lauscht nur auf <code>127.0.0.1:8730</code>	Nur lokal
Hub-Server	IIS-Site <code>https://hub.company.com</code> mit URL Rewrite + ARR vor dem Dienst	Eingehend 443 von den Arbeitsplätzen
Identitätsanbieter	AD FS oder Microsoft Entra ID: die Anwendung „Compass Hub“ (OpenID Connect)	Der Browser des Benutzers
Hub-Server → Internet	<code>api.anthropic.com</code> (KI-Gateway), die Atlassian-Site (Jira/Confluence)	Ausgehend 443, nur für die Teile, die Sie nutzen
Arbeitsplätze	Loonar Compass (Desktop und Add-in in EA), Einstellungen per Gruppenrichtlinie erzwungen	Ausgehend 443 zum Hub

Dies ist die Konfiguration, die durchgängig unter Windows Server 2022 mit AD, AD CS, AD FS und IIS getestet wurde. Jeder Schritt endet mit einer Prüfung, sodass ein Problem in dem Schritt sichtbar wird, der es verursacht hat.

2. Bevor Sie beginnen

✓	Punkt	Hinweise
☐	Windows Server 2019 oder 2022, x64	2 vCPU, 4 GB RAM und 2 GB Festplatte genügen für ein Team; mehr Speicherplatz für große Modelldateien. Kein Enterprise Architect.
☐	DNS-Name, z. B. <code>hub.company.com</code>	Von den Arbeitsplätzen auflösbar.
☐	TLS-Zertifikat für diesen Namen	Von der firmeneigenen CA oder einer öffentlichen CA. Die Arbeitsplätze müssen seinem Stammzertifikat vertrauen (Compass prüft es anhand des Windows-Zertifikatspeichers). Der Hub-Name muss im SAN des Zertifikats stehen; bei AD CS benötigt das Konto, das es anfordert, die Berechtigung „Registrieren“ (Enroll) für die Vorlage „Webserver“.
☐	IIS mit den Modulen URL Rewrite und Application Request Routing (ARR)	Download bei Microsoft (iis.net).
☐	AD FS (Windows Server) oder Microsoft Entra ID	Nur für die Firmenanmeldung, die empfohlen wird. Ohne sie hat der Hub eigene Benutzer und Kennwörter.
☐	AD-Gruppen: <code>Compass-Admins</code> , <code>Compass-Architects</code> , <code>Compass-Viewers</code>	Die Gruppe bestimmt die Rolle im Hub. Andere Namen sind möglich (Schritt 6).
☐	Die Modelle	.gea-Dateien, auf den Server kopiert, oder Lesezugriff auf die Datenbank des EA-Repositorys (ein schreibgeschütztes Konto genügt).
☐	Geheimnisse liegen bereit, bei der Person, die installiert	Claude-API-Schlüssel, Atlassian-API-Token, OIDC-Clientgeheimnis, DB-Kennwort. Sie werden nie in <code>hub.json</code> eingetragen.
☐	Ausgehendes HTTPS vom Server	<code>api.anthropic.com</code> (KI-Gateway), Ihre Atlassian-Site (Jira/Confluence). Über einen Proxy: Setzen Sie <code>HTTPS_PROXY</code> für den Dienst (Schritt 3).

Dateien aus dem Release: `CompassHub-0.9.0-windows-x64.zip` (mit `compass-hub.exe`, `hub.example.json`, `README.md`, den Lizenzen) und für die Arbeitsplätze `LoonarCompass-Setup-0.9.exe` sowie der Ordner `policies` (ADMX/ADML).

3. Schritt 1 – Dateien und Ordner

1. Vergleichen Sie den SHA-256-Wert des Downloads mit dem Wert, der mit dem Release veröffentlicht wurde:

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

2. Entpacken Sie die Datei nach `C:\CompassHub` und legen Sie die Unterordner `models` und `secrets` an.
3. Beschränken Sie den Ordner auf den Dienst und die Administratoren. Der Hub schreibt seine Daten hierher, und hier liegen die Geheimnisse:

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

Unter einem Windows in einer anderen Sprache verwenden Sie die SID `*S-1-5-32-544` statt des Namens der Gruppe Administratoren.

Prüfung: `C:\CompassHub\compass-hub.exe --version` gibt `0.9.0` aus.

4. Schritt 2 – hub.json und die Modelle

Kopieren Sie `hub.example.json` nach `C:\CompassHub\hub.json`. Ein minimaler Start:

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

- `listen` bleibt auf `127.0.0.1`: Nur IIS auf demselben Server spricht mit dem Hub.
- `sources`: ein Eintrag pro Modell. `id` ist kurz und stabil, weil die Benutzer und Power BI sie verwenden. `properties` ist relativ zu `hub.json`.
- Lassen Sie `users` weg: Der Hub legt dann das Konto `admin` an (Schritt 4) und schreibt die Benutzer selbst zurück, nur als Hashes.

Die Modelldatei, z. B. `C:\CompassHub\models\architecture.properties`:

```
# An EA project file (read only)
model.source=file
model.file=C:/CompassHub/models/Architecture.qea

# ... or a repository database (the password is the secret DB_PASSWORD):
# model.source=sqlserver          (or postgres, mysql, oracle)
# db.host=sql.company.com
# db.port=1433
# db.name=ea_repository
# db.user=compass_reader
# db.sslmode=verify-full
```

SQL Server, MySQL und Oracle werden über den 64-Bit-ODBC-Treiber des Herstellers gelesen, der auf dem Server installiert sein muss. Für SQL Server genügt „ODBC Driver 17 for SQL Server“ (wird mit SQL Server 2022 mitgeliefert) oder 18; die installierten Treiber: `Get-OdbcDriver -Name '*SQL Server*' -Platform 64-bit`. PostgreSQL und Dateien benötigen nichts weiter. Jeder Lesevorgang wird zurückgerollt, daher genügt ein schreibgeschütztes Datenbankkonto. SQL Server ohne das Geheimnis `DB_PASSWORD` verwendet die Windows-Authentifizierung: Der Hub-Dienst (LocalSystem) meldet sich als Computerkonto an (`DOMAIN\SERVER$`), das dann die Rolle `db_datareader` in der Modelldatenbank benötigt.

- **Benannte Instanz** (z. B. SQL Server Express): `db.host=SERVER\SQLEXPRESS` ohne Port, bei laufendem Dienst SQL Server Browser; oder ein fester TCP-Port (SQL Server Configuration Manager → TCP/IP → IPAll: TcpPort 1433, TcpDynamicPorts leer) und `db.host / db.port`.
- **Eigene Verbindungszeichenfolge**: `db.odbc=Driver={ODBC Driver 17 for SQL Server};Server=sql.company.com,1433;Database=ea_repository;Trusted_Connection=Yes` ersetzt Host, Port, Name und Benutzer (ohne Kennwort; `DB_PASSWORD` wird, falls gesetzt, ergänzt).
- **db.sslmode** für SQL Server: `prefer` = Verschlüsselung, wenn Server und Treiber sie verwenden (keine Zertifikatsprüfung); `require` = immer verschlüsselt, das Zertifikat wird nicht geprüft; `verify-full` = verschlüsselt, und das Zertifikat muss vertrauenswürdig sein und zum Servernamen passen (nicht mit einem selbstsignierten SQL-Server-Zertifikat).

Halten Sie die Modelldateien des Hubs getrennt von den Dateien, die in EA bearbeitet werden. Um ein Dateimodell zu aktualisieren, ersetzen Sie die Datei. Der Hub öffnet sie bei jeder Anfrage schreibgeschützt, daher ist kein Neustart nötig.

5. Schritt 3 – Geheimnisse

Jedes Geheimnis ist eine Textdatei in `C:\CompassHub\secrets`, die nur den Wert enthält. Den Pfad erfährt der Dienst aus einer Umgebungsvariablen `LOONAR_SECRET_<NAME>_FILE`. Die Person, die den Wert kennt, legt die Datei an, z. B. im Editor (Notepad) oder mit:

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

(`-AsPlainText` erfordert PowerShell 7; in Windows PowerShell 5.1 ist der Editor einfacher.)

Datei (Beispiel)	Variable für den Dienst	Benötigt für
claude_key_team	LOONAR_SECRET_CLAUDE_KEY_TEAM_FILE	Das KI-Gateway: eine Variable pro Schlüssel, der in hub.json genannt ist (Schritt 7)
claude_api_key	LOONAR_SECRET_CLAUDE_API_KEY_FILE	„Ask“ in der Weboberfläche
jira_token	LOONAR_SECRET_JIRA_TOKEN_FILE	Jira
confluence_token	LOONAR_SECRET_CONFLUENCE_TOKEN_FILE	Confluence
oidc_client_secret	LOONAR_SECRET_OIDC_CLIENT_SECRET_FILE	Firmenanmeldung
db_password	LOONAR_SECRET_DB_PASSWORD_FILE	Eine Modelldatenbank

Der Name in der Variablen ist der Name des Geheimnisses in Großbuchstaben, andere Zeichen werden zu `_`: Das Geheimnis `claude_key_anna` aus `hub.json` wird zu `LOONAR_SECRET_CLAUDE_KEY_ANNA_FILE`.

Die Variablen werden **nur für den Dienst** gesetzt, nicht für den ganzen Computer, und zwar nach der Installation des Dienstes (Schritt 4). Sie wirken beim nächsten Start des Dienstes, ohne Neustart des Rechners:

```
$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.company.com:8080'    only if the server goes out through a proxy
)
Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\CompassHub -Name Environment -Type
MultiString -Value $vars
Restart-Service CompassHub
```

Der Hub liest ein Geheimnis, wenn er es zum ersten Mal benötigt. Ein fehlendes Geheimnis wird dort gemeldet, wo es verwendet wird, z. B. „secret 'jira_token' is not set: give it as LOONAR_SECRET_JIRA_TOKEN (or a file named in LOONAR_SECRET_JIRA_TOKEN_FILE)“. Die Werte erscheinen nie in `hub.json`, in den Protokollen oder in der Weboberfläche. Eine Bytereihenfolgemarkierung (BOM) am Anfang sowie Leerzeichen oder ein Zeilenumbruch am Ende einer Geheimnisdatei (Editor) werden ignoriert.

6. Schritt 4 – Der Windows-Dienst und die erste Anmeldung

1. In PowerShell als Administrator:

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

Dies legt den Dienst `CompassHub` („Compass Hub (Loonar Compass team service)“) mit automatischem Start unter LocalSystem an und startet ihn.

2. Setzen Sie nun die Geheimnisse des Dienstes (Schritt 3) und führen Sie `Restart-Service CompassHub` aus.
3. Öffnen Sie auf dem Server `http://127.0.0.1:8730/` und melden Sie sich als `admin` / `password` (mit einer Null) an. Der Hub verlangt sofort ein neues Kennwort und erlaubt bis dahin nichts anderes. Das Kennwort muss mindestens 10 Zeichen lang sein. Erledigen Sie dies, **bevor** Schritt 5 den Hub erreichbar macht.

Prüfung:

- `Get-Service CompassHub` zeigt Running;
- `C:\CompassHub\hub.log` zeigt den Start und Ihre Anmeldung;
- die Weboberfläche listet das Modell aus Schritt 2 auf.

7. Schritt 5 – HTTPS mit IIS (URL Rewrite + ARR)

Der Hub spricht reines HTTP auf 127.0.0.1. IIS gibt ihm den Firmennamen und das Zertifikat.

1. Installieren Sie IIS mit URL Rewrite und ARR. Legen Sie eine Site an, z. B. **CompassHub**, mit einer Bindung für `https`, Port 443, dem Hostnamen `hub.company.com` und dem Zertifikat. Der physische Pfad ist ein leerer Ordner, z. B. `C:\inetpub\compasshub`.
2. Schalten Sie den Proxy ein und das Umschreiben des Hosts in Weiterleitungen aus. Dies ist **erforderlich**; andernfalls schreibt ARR die Weiterleitung zu AD FS auf die eigene Adresse des Hubs um, und die Firmenanmeldung schlägt fehl. Setzen Sie außerdem das Timeout für lange KI-Antworten:

```
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. Legen Sie diese `web.config` in den Ordner der Site. Sie leitet alles an den Hub weiter und erlaubt Anfragekörper bis 32 MB, weil Fragen mit Modelldiagrammen groß sind:

```
<?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. Firewall: Erlauben Sie nur eingehend 443. Port 8730 wird nie geöffnet, weil der Hub auf 127.0.0.1 lauscht.
5. AD FS auf demselben Server: AD FS verwendet ebenfalls Port 443 (HTTP.sys). Aktivieren Sie **Require Server Name Indication** an der IIS-Bindung (`New-WebBinding ... -SslFlags 1`), sonst behindern sich IIS und AD FS gegenseitig.
6. Der Hub benötigt weder `preserveHostHeader` noch `X-Forwarded-Proto` : Seine Adressen kommen aus `redirect_uri` in `hub.json`.

Der Hub vertraut `X-Forwarded-For` (das ARR hinzufügt) nur von einem Proxy auf demselben Computer. Das Audit-Protokoll und die Sperre bei falschen Tokens sehen dann die tatsächliche Clientadresse.

Prüfung: Von einem Arbeitsplatz aus zeigt `https://hub.company.com/` die Anmeldeseite ohne Zertifikatswarnung.

8. Schritt 6 – Firmenanmeldung (AD FS oder Entra ID)

AD FS

1. AD FS Management → Application Groups → Add, dann die Vorlage **Server application accessing a web API**, Name „Compass Hub“.
2. Server application:
 - notieren Sie die **Client-ID** (client identifier);
 - Umleitungs-URI: `https://hub.company.com/auth/callback`;
 - Anmeldeinformationen: **Generate a shared secret**. Speichern Sie es sofort in `C:\CompassHub\secrets\oidc_client_secret`; AD FS zeigt es nur einmal an.
3. Web API:
 - Bezeichner: die Client-ID aus dem vorherigen Schritt;
 - Zugriffssteuerungsrichtlinie: die Personen, die den Hub nutzen dürfen, z. B. „Permit everyone“ (die Rollen kommen weiterhin aus den Gruppen);
 - zulässige Bereiche (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`.

(Geben Sie die Namen der ausgehenden Claims genau so ein.)

In `hub.json` (der Hub fügt `allatclaims` für AD FS selbst hinzu, damit die Claims in das ID-Token gelangen):

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

Microsoft Entra ID

Die Konfiguration in Entra ID:

- **App-Registrierung:** Plattform *Web*, Umleitungs-URI `https://hub.company.com/auth/callback`, ein Clientgeheimnis (in die Geheimnisdatei) und das ID-Token mit den optionalen Claims `upn` und `email`.
- **Aussteller (Issuer):** `https://login.microsoftonline.com/<tenant-id>/v2.0`.
- **Gruppen:** Entra sendet sie standardmäßig als Objekt-IDs. Tragen Sie entweder diese IDs in `roles` ein, oder wählen Sie für aus AD synchronisierte Gruppen „SAMAccountName“ in der Tokenkonfiguration.

Regeln, die der Hub anwendet

- Die Rolle ergibt sich bei jeder Anmeldung aus den Gruppen, und die höchste gilt. Eine Person, die in keiner der Gruppen ist, erhält keinen Zugang.
- Ein Firmenkonto mit demselben Namen wie ein lokaler Hub-Benutzer wird abgelehnt, bis der lokale Benutzer umbenannt oder entfernt ist.
- Der Hub prüft das ID-Token selbst: die RS256-Signatur, Aussteller, Zielgruppe, Ablauf und Nonce, mit PKCE und einem einmaligen State.
- Wenn alles funktioniert, setzen Sie `"password_login": false`: Dann bleibt nur die Schaltfläche für die Firmenanmeldung. API-Tokens für MCP-Clients funktionieren weiterhin. Bewahren Sie ein lokales Admin-Kennwort in Ihrem Kennworttresor auf, für den Fall, dass der Identitätsanbieter ausfällt.

Prüfung: Nach `Restart-Service CompassHub` führt „Mit dem Firmenkonto anmelden“ zu AD FS und zurück. `hub.log` zeigt „... signed in with a company account as architect“, und die Registerkarte **Users** listet das Firmenkonto mit seiner Rolle auf.

9. Schritt 7 – KI-Schlüssel, Jira, Confluence und die Teamrichtlinie

Fügen Sie die Abschnitte in `hub.json` ein. Jedes hier genannte Geheimnis benötigt außerdem seine Variable `..._FILE` (Schritt 3). Führen Sie dann `Restart-Service CompassHub` aus; angemeldete Personen bleiben angemeldet.

```
"ai": {
  "keys": [ { "for": "role:architect", "secret": "claude_key_team" },
            { "for": "anna@company.com", "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://company.atlassian.net", "user": "svc-compass@company.com",
"project": "ARCH", "issue_type": "Task" },
  "confluence": { "url": "https://company.atlassian.net/wiki", "user": "svc-compass@company.com",
"space": "ARCH" }
},
"policy": {
  "min_approval": "ask",
  "ai_via_hub": true,
  "jira_via_hub": true,
  "confluence_via_hub": true,
  "web_access": false,
  "update_check": false
}
```

Einstellung	Bedeutung
<code>ai.keys</code>	Welchen Claude-Schlüssel eine Person verwendet. Reihenfolge: der Benutzername, dann <code>role:<role></code> , dann <code>*</code> . Ohne Treffer gibt es für diese Person keine KI.
<code>ai.limits</code>	Tokens pro Tag und pro Monat. Oberhalb des Limits lehnt der Hub mit einer klaren Meldung ab.
<code>ai.models</code>	Die erlaubten Modelle; andere Modelle werden abgelehnt.
<code>policy.ai_via_hub</code>	Compass fragt die KI nur über den Hub; kein API-Schlüssel auf den Arbeitsplätzen.
<code>policy.jira_via_hub</code> , <code>confluence_via_hub</code>	Jira/Confluence über das Dienstkonto des Hubs. Die Rolle viewer darf nur lesen; jede Änderung wird protokolliert.
<code>policy.min_approval</code>	Der schwächste Freigabemodus, der in Compass für Schreibvorgänge im Modell erlaubt ist (<code>ask</code> ist der strengste).
<code>policy.web_access</code> , <code>web_allowed_domains</code>	Ob der Assistent im Web suchen oder Seiten lesen darf, und von welchen Domänen.
<code>policy.update_check</code>	Ob Compass stündlich auf GitHub nach einer neuen Version sucht.

Administratoren ändern die Richtlinie später auf der Registerkarte **Team policy** der Weboberfläche, und die Nutzung pro Person steht unter **Users** → **AI usage**.

10. Schritt 8 – Die Arbeitsplätze (Gruppenrichtlinien)

1. **Dem Zertifikat vertrauen.** Wenn das Hub-Zertifikat von der firmeneigenen CA stammt, verteilen Sie deren Stammzertifikat an die Arbeitsplätze (GPO: Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Richtlinien für öffentliche Schlüssel → Vertrauenswürdige Stammzertifizierungsstellen). Ohne dieses meldet Compass ein nicht vertrauenswürdiges Zertifikat (UnknownIssuer).
2. **Vorlagen.** Kopieren Sie `LoonarCompass.admx` nach `\\<domain>\SYSVOL\<domain>\Policies\PolicyDefinitions` und `en-US\LoonarCompass.adml` (bei Bedarf auch `p1-PL`) in die Sprachunterordner. Ohne zentralen Speicher kopieren Sie sie nach `C:\Windows\PolicyDefinitions` auf dem Computer, auf dem Sie das GPO bearbeiten.
3. **GPO** für die OU der Arbeitsplätze: Computerkonfiguration → Administrative Vorlagen → Loonar → Loonar Compass.

Richtlinie	Registrierungswert (HKLM\SOFTWARE\Policies\Loonar\Compass)	Wirkung
Hub address	<code>HubUrl</code> (Text)	Die Hub-Adresse ist in Compass fest vorgegeben und kann nicht geändert werden.
Require the hub	<code>RequireHub</code> = 1	Der Assistent funktioniert nur, solange die Person beim Hub angemeldet ist.
Web access	<code>WebAccess</code> = 0	Keine Websuche und kein Lesen von Seiten; die Schaltfläche  ist deaktiviert.
Update check	<code>UpdateCheck</code> = 0	Keine tägliche Suche nach einer neuen Version.
Minimum approval mode	<code>MinApproval</code> = ask / plan / auto	Ein schwächerer Modus kann nicht gewählt werden.
Allowed AI providers	<code>AllowedProviders</code> , z. B. <code>anthropic</code>	Andere Anbieter (z. B. OpenAI) werden abgelehnt.

Ohne Domäne lassen sich dieselben Werte mit `LoonarCompass-company-policy.reg` importieren (und mit `LoonarCompass-remove-policy.reg` entfernen). Die Computerrichtlinie ist stärker als die Hub-Richtlinie und die Einstellungen des Benutzers; sie kann Compass nur strenger machen.

Compass installieren. `LoonarCompass-Setup-0.9.exe` installiert für den aktuellen Benutzer (`%LOCALAPPDATA%\Programs\Loonar Compass`) oder für alle Benutzer (`Program Files`) und registriert das Add-in in Enterprise Architect. Für Verteilungswerkzeuge (Intune, Configuration Manager, ein Startskript) installiert es ohne Fenster:

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

Option	Wirkung
<code>--quiet</code>	Kein Fenster und keine Rückfragen. Exitcode 0 = installiert, 1 = Fehler, 740 = <code>--all-users</code> ohne Administratorrechte. Das Ergebnis steht in <code>%TEMP%\LoonarCompass-Setup.log</code> (für SYSTEM: <code>C:\Windows\Temp</code>).
<code>--all-users</code>	Für alle: Program Files, das gemeinsame Startmenü, das Add-in in EA für alle Benutzer (HKLM). Als SYSTEM oder als Administrator ausführen.
<code>--dir <folder></code>	Ein anderer Programmordner.
<code>--lang en pl de fr</code>	Die Sprache der Lizenz- und Changelog-Dateien.
<code>--no-desktop, -- no-start-menu</code>	Ohne diese Verknüpfungen.
<code>--no-ea-addin</code>	Ohne das Add-in in Enterprise Architect.

Derselbe Befehl aktualisiert eine vorhandene Installation. Schließen Sie vorher Compass und EA auf dem Computer. Die Benutzereinstellungen bleiben unberührt; mit der Computerrichtlinie (Hub-Adresse, Hub erforderlich) muss niemand etwas konfigurieren. Stille Deinstallation: `"C:\Program Files\Loonar Compass\uninstall.exe" --uninstall --quiet`.

Die erste Anmeldung des Benutzers. Öffnen Sie in Compass Einstellungen → Team (Compass Hub) → **Mit dem Firmenkonto anmelden.** Der Browser öffnet AD FS und kehrt zu Compass zurück. Die Anmeldung gilt 12 Stunden und übersteht einen Neustart des Hubs.

11. Schritt 9 – Abnahmecheckliste

✓	Test	Erwartet
☐	<code>https://hub.company.com/</code> von einem Arbeitsplatz aus öffnen	Die Anmeldeseite, keine Zertifikatswarnung
☐	Firmenanmeldung als Mitglied von Compass-Architects	Rolle architect; hub.log „signed in with a company account as architect“
☐	Eine Person, die in keiner der Compass-Gruppen ist	Abgelehnt
☐	Compass mit dem GPO, vor der Anmeldung: eine Frage senden	„Ihre Organisation verlangt den Team-Hub: Melden Sie sich unter Einstellungen → Team (Compass Hub) ...“
☐	Dasselbe nach der Anmeldung	Eine Antwort, ohne API-Schlüssel auf dem Arbeitsplatz; eine Zeile in Users → AI usage
☐	Eine Person mit der Rolle viewer stellt eine Frage (kein Schlüssel für viewer)	„der Hub hat keinen KI-Schlüssel für Sie“
☐	Die Schaltfläche  in Compass	Deaktiviert: „Von Ihrer Organisation ausgeschaltet“
☐	Restart-Service CompassHub, dann erneut fragen	Funktioniert ohne erneute Anmeldung
☐	Hub gestoppt, fragen	Eine kurze Meldung, dass der Hub nicht antwortet; EA arbeitet weiter
☐	Jira: „Erstelle ein Jira-Issue: test“ (architect)	Das Issue im Projekt; ein Eintrag im Audit-Protokoll des Hubs mit dem Namen der Person

12. Betrieb: Update, Sicherung, Protokolle, Entfernen

Update

```
Stop-Service CompassHub
Copy-Item .\compass-hub.exe C:\CompassHub\compass-hub.exe -Force # from the new zip, after checking
its SHA-256
Start-Service CompassHub
```

hub.json, die Geheimnisse und die Anmeldungen bleiben unverändert. Angemeldete Personen bleiben angemeldet.

Was gesichert wird (C:\CompassHub)

Datei / Ordner	Inhalt
hub.json	Konfiguration, lokale Benutzer (nur Hashes von Kennwörtern und Tokens), Richtlinie
audit.jsonl	Das Audit-Protokoll der Änderungen und Anmeldungen
changes\, notes\	Änderungssätze zur Prüfung und die Teamnotizen
ai_usage.jsonl	KI-Nutzung pro Person (Grundlage der Limits)
company_accounts.json , sessions.json	Gesehene Firmenkonten und aktuelle Anmeldungen (Hashes); ihr Verlust ist unschädlich: Die Personen melden sich erneut an
secrets\	Nur wenn Ihre Sicherung verschlüsselt ist. Andernfalls bewahren Sie die Werte im Kennworttresor auf.
models\	Die Modelldateien, sofern sie nicht anderswo aufbewahrt werden

Protokolle

- hub.log : Start, Anmeldungen, abgelehnte Anfragen, Fehler. Zu einem „internal error (id ...)“, der einem Benutzer angezeigt wird, stehen die Details hier unter derselben ID.
- audit.jsonl und hub.log werden mit einem Datum umbenannt, wenn sie groß werden.

Entfernen

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

Entfernen Sie anschließend die IIS-Site, die AD-FS-Anwendungsgruppe und das GPO, und löschen Sie C:\CompassHub nach der Sicherung.

13. Fehlerbehebung

Symptom	Ursache und Abhilfe
Compass: Zertifikat nicht vertrauenswürdig / UnknownIssuer; der Browser zeigt „Nicht sicher“	Der Arbeitsplatz vertraut dem Stammzertifikat des Hub-Zertifikats nicht. Verteilen Sie die Stammzertifizierungsstelle (Schritt 8) und starten Sie dann Browser und Compass neu.
Die Firmenanmeldung endet bei <code>https://hub.company.com/adfs/...</code> oder mit 404	ARR schreibt die Weiterleitung um. Setzen Sie <code>reverseRewriteHostInResponseHeaders</code> = False (Schritt 5).
„<name> is not in any group of the hub (...): ask the administrator for access“	Die Person ist in keiner der Rollengruppen, oder der Claim <code>groups</code> fehlt. Prüfen Sie die Transformationsregel „Token-Groups - Unqualified Names → groups“ und den Bereich <code>allatclaims</code> .
„A local user of the hub has the same name“	Benennen Sie diesen lokalen Benutzer auf der Registerkarte Users um oder entfernen Sie ihn.
Compass: „Der Team-Hub oder der Server davor antwortet nicht richtig (502)“	Der Dienst ist gestoppt oder startet gerade: <code>Get-Service CompassHub</code> , dann <code>hub.log</code> .
Compass: „Ihre Anmeldung beim Team-Hub ist abgelaufen“	12 Stunden sind vergangen, oder <code>sessions.json</code> ging verloren. Melden Sie sich unter Einstellungen → Team erneut an.
„der Hub hat keinen KI-Schlüssel für Sie“	Kein Eintrag in <code>ai.keys</code> für die Person, ihre Rolle oder <code>*</code> .
„Ihr KI-Limit für heute ist aufgebraucht“	Erhöhen Sie <code>ai.limits</code> für die Person oder Rolle, oder warten Sie bis zum nächsten Tag.
„secret '...' is not set: give it as LOONAR_SECRET_...“	Die Variable <code>..._FILE</code> fehlt in <code>Environment</code> des Dienstes, oder die Datei ist leer oder für SYSTEM nicht lesbar.
hub.log: „<address>: 20 wrong tokens, refused for 10 minutes“	20 verschiedene falsche Tokens kamen von einer Adresse (ein wiederholtes altes Token zählt einmal). Gültige Tokens funktionieren weiterhin. Ermitteln Sie den Client in <code>hub.log</code> .
Große Fragen scheitern mit 413 oder 404.13	<code>maxAllowedContentLength</code> in <code>web.config</code> (Schritt 5).
Lange Antworten enden nach 2 Minuten mit 502.3	Das ARR- <code>timeout</code> (Schritt 5).
AD FS: MSIS7628 von <code>Grant-AdfsApplicationPermission</code> direkt nach der Installation von AD FS	Die Farm startet noch: Wiederholen Sie den Befehl einige Minuten später.
hub.log / AD FS: MSIS9622 „Client authentication failed“	Die Geheimnisdatei passt nicht zu AD FS. Erzeugen Sie ein neues Geheimnis: <code>Set-AdfsServerApplication -TargetIdentifier <client id> -ResetClientSecret</code> ,

	schreiben Sie es in die Datei, <code>Restart-Service CompassHub</code> .
Compass auf einem Windows Server (z. B. Remote Desktop Services): Der PDF-Export schlägt fehl, oder die erste Office-Anmeldung wird blockiert	Compass erstellt PDFs mit Word und PowerPoint auf dem Computer, auf dem es läuft. Unter Windows Server kann die verstärkte Sicherheitskonfiguration für IE die erste Office-Anmeldung blockieren (<code>odc.officeapps.live.com</code>): Fügen Sie die Office-Anmeldeseiten zu den vertrauenswürdigen Sites hinzu, oder schalten Sie die Einstellung für Benutzer im Server-Manager aus.

14. Linux und Docker

Derselbe Hub läuft in einem Container. Der Datenordner (hub.json mit `"listen": "0.0.0.0:8730"`, die Modelle und die Dateien des Hubs) wird als `/data` eingebunden und muss für den Benutzer 10001 beschreibbar sein. Die Geheimnisse kommen aus Variablen `LOONAR_SECRET_*` oder aus Docker Secrets über `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
```

Stellen Sie nginx oder einen anderen HTTPS-Proxy davor, wie in Schritt 5. Der Proxy muss den Header `Location` von Weiterleitungen unverändert lassen, `X-Forwarded-For` weitergeben sowie Anfragekörper von 32 MB und ein Timeout von 5 Minuten erlauben. Für Modelle in SQL Server, MySQL oder Oracle bauen Sie ein eigenes Image auf Basis dieses Images und fügen den Linux-ODBC-Treiber des Herstellers hinzu.