Compass Hub

Guide d'installation pour l'informatique

version 0.9.2 · octobre 2026

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

Sommaire

1. Ce que vous installez
2. Avant de commencer
3. Étape 1 – Fichiers et dossier
4. Étape 2 – hub.json et les modèles
5. Étape 3 – Secrets
6. Étape 4 – Le service Windows et la première connexion
7. Étape 5 – HTTPS avec IIS (URL Rewrite + ARR)
8. Étape 6 – Connexion d'entreprise (AD FS ou Entra ID)
9. Étape 7 – Clés d'IA, Jira, Confluence et la stratégie d'équipe
10. Étape 8 – Les postes de travail (stratégie de groupe)
11. Étape 9 – Liste de recette
12. Exploitation ┌ mise à jour, sauvegarde, journaux, suppression
13. Dépannage
14. Linux et Docker

1. Ce que vous installez

Compass Hub est le service d'équipe de Loonar Compass. Il s'agit d'un seul programme, `compass-hub.exe`, sans programme d'installation et sans Enterprise Architect. Il s'exécute comme service Windows et conserve ┌

- les modèles EA de l'équipe (en lecture seule) ┌ des fichiers `.qea` / `.qeax` ou un référentiel PostgreSQL, SQL Server, MySQL ou Oracle ┌
- la stratégie d'équipe, que les applications Compass appliquent ┌ le mode de validation minimal, l'accès au web, l'IA uniquement via le hub, etc. ┌
- le journal d'audit des modifications de tous les postes de travail, les ensembles de modifications à relire et une vue web pour les personnes sans EA ┌
- la passerelle d'IA ┌ les clés de l'API Claude restent sur le serveur, avec une clé et des limites par personne ou par rôle ┌
- Jira et Confluence via un seul compte de service, une API GraphQL en lecture seule, des tables pour Power BI et un serveur MCP.

Où	Quoi	Réseau
Serveur du hub	Service `CompassHub` (compass-hub.exe), à l'écoute uniquement sur `127.0.0.1:8730`	Local uniquement
Serveur du hub	Site IIS `https://hub.company.com` avec URL Rewrite + ARR devant le service	Entrant 443 depuis les postes de travail
Fournisseur d'identité	AD FS ou Microsoft Entra ID ┌ l'application « Compass Hub ┌ (OpenID Connect)	Le navigateur de l'utilisateur
Serveur du hub → internet	`api.anthropic.com` (passerelle d'IA), le site Atlassian (Jira/Confluence)	Sortant 443, uniquement pour les parties que vous utilisez
Postes de travail	Loonar Compass (application de bureau et complément dans EA), paramètres imposés par stratégie de groupe	Sortant 443 vers le hub

Il s'agit de la configuration testée de bout en bout sous Windows Server 2022 avec AD, AD CS, AD FS et IIS. Chaque étape se termine par une vérification, de sorte qu'un problème apparaît à l'étape qui l'a causé.

2. Avant de commencer

✓	Élément	Remarques
☐	Windows Server 2019 ou 2022, x64	2 vCPU, 4 Go de RAM et 2 Go de disque suffisent pour une équipe ; davantage de disque pour les gros fichiers de modèle. Pas d'Enterprise Architect.
☐	Nom DNS, par exemple `hub.company.com`	Résolvable depuis les postes de travail.
☐	Certificat TLS pour ce nom	Émis par l'autorité de certification de l'entreprise ou par une autorité publique. **Les postes de travail doivent faire confiance à sa racine** (Compass le vérifie dans le magasin de certificats Windows). Le nom du hub doit figurer dans le SAN du certificat ; avec AD CS, le compte qui le demande a besoin de l'autorisation Inscrire sur le modèle Serveur Web.
☐	IIS avec les modules URL Rewrite et Application Request Routing (ARR)	Téléchargements chez Microsoft (iis.net).
☐	AD FS (Windows Server) ou Microsoft Entra ID	Uniquement pour la connexion d'entreprise, qui est recommandée. Sans elle, le hub a ses propres utilisateurs et mots de passe.
☐	Groupes AD ; `Compass-Admins`, `Compass-Architects`, `Compass-Viewers`	Le groupe donne le rôle dans le hub. D'autres noms sont possibles (étape 6).
☐	Les modèles	Fichiers .qea copiés sur le serveur, ou accès en lecture à la base de données du référentiel EA (un compte en lecture seule suffit).
☐	Secrets prêts, détenus par la personne qui installe	Clé(s) de l'API Claude, jeton d'API Atlassian, secret client OIDC, mot de passe de la base de données. Ils ne sont jamais placés dans hub.json.
☐	HTTPS sortant depuis le serveur	`api.anthropic.com` (passerelle d'IA), votre site Atlassian (Jira/Confluence). Via un proxy ; définissez `HTTPS_PROXY` pour le service (étape 3).

Fichiers de la version ; `CompassHub-0.9.0-windows-x64.zip` (avec `compass-hub.exe`, `hub.example.json`, `README.md`, les licences), et pour les postes de travail `LoonarCompass-Setup-0.9.exe` ainsi que le dossier `policies` (ADMX/ADML).

3. Étape 1 – Fichiers et dossier

1. Comparez le SHA-256 du téléchargement avec la valeur publiée avec la version ┌

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

2. Décompressez-le dans `C:\CompassHub` et créez les sous-dossiers `models` et `secrets`.
3. Limitez l'accès au dossier au service et aux administrateurs. Le hub y écrit ses données, et les secrets s'y trouvent ┌

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

   Sur un Windows dans une autre langue, utilisez le SID `*S-1-5-32-544` au lieu du nom du groupe Administrateurs.

Vérification ┌ `C:\CompassHub\compass-hub.exe --version` affiche `0.9.0`.

4. Étape 2 – hub.json et les modèles

Copiez `hub.example.json` vers `C:\CompassHub\hub.json`. Un démarrage minimal ┌

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

- `listen` reste sur `127.0.0.1` ┌ seul IIS, sur le même serveur, communique avec le hub.
- `sources` ┌ une entrée par modèle. `id` est court et stable, car les utilisateurs et Power BI l'utilisent. `properties` est relatif à hub.json.
- Omettez `users` ┌ le hub crée alors le compte `admin` (étape 4) et réécrit lui-même les utilisateurs, uniquement sous forme de hachages.

Le fichier du modèle, par exemple `C:\CompassHub\models\architecture.properties` ┌

```
# Un fichier de projet EA (en lecture seule)
model.source=file
model.file=C:/CompassHub/models/Architecture.qea

# ... ou une base de données de référentiel (le mot de passe est le secret DB_PASSWORD) :
# model.source=sqlserver          (ou 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 et Oracle sont lus via le pilote ODBC 64 bits de l'éditeur, qui doit être installé sur le serveur. Pour SQL Server, « ODBC Driver 17 for SQL Server ┌ (fourni avec SQL Server 2022) ou 18 suffit ┌ les pilotes installés ┌ `Get-OdbcDriver -Name '*SQL Server*' -Platform 64-bit`. PostgreSQL et les fichiers ne nécessitent rien de plus. Chaque lecture est annulée (rollback), de sorte qu'un compte de base de données en lecture seule suffit. SQL Server sans le secret `DB_PASSWORD` utilise l'authentification Windows ┌ le service du hub (LocalSystem) se connecte avec le compte d'ordinateur (`DOMAIN\SERVER$`), qui a alors besoin du rôle `db_datareader` dans la base de données du modèle.

- **Instance nommée** (par exemple SQL Server Express) ┌ `db.host=SERVER\SQLEXPRESS` sans port, avec le service SQL Server Browser en cours d'exécution ┌ ou un port TCP fixe (Gestionnaire de configuration SQL Server → TCP/IP → IPAll ┌ TcpPort 1433, TcpDynamicPorts vide) et `db.host` / `db.port`.
- **Votre propre chaîne de connexion** ┌ `db.odbc=Driver={ODBC Driver 17 for SQL Server};Server=sql.company.com,1433;Database=ea_repository;Trusted_Connection=Yes` remplace l'hôte, le port, le nom et l'utilisateur (sans mot de passe ┌ `DB_PASSWORD`, s'il est défini, est ajouté).
- **db.sslmode** pour SQL Server ┌ `prefer` = chiffrement lorsque le serveur et le pilote l'utilisent (pas de vérification du certificat) ┌ `require` = toujours chiffré, le certificat n'est pas vérifié ┌ `verify-full` = chiffré, et le certificat doit être approuvé et correspondre au nom du serveur (pas avec un certificat SQL Server auto-signé).

> Séparez les fichiers de modèle du hub des fichiers que les personnes modifient dans EA. Pour actualiser un modèle sous forme de fichier, remplacez le fichier. Le hub l'ouvre en lecture seule à chaque requête, aucun redémarrage n'est donc nécessaire.

5. Étape 3 – Secrets

Chaque secret est un fichier texte dans `C:\CompassHub\secrets` qui ne contient que la valeur. Le service obtient le chemin par une variable d'environnement `LOONAR_SECRET_<NAME>_FILE`. La personne qui connaît la valeur crée le fichier, par exemple dans le Bloc-notes ou avec ┌

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

(`-AsPlainText` nécessite PowerShell 7 ┌ dans Windows PowerShell 5.1, le Bloc-notes est plus simple.)

Fichier (exemple)	Variable pour le service	Nécessaire pour
`claude_key_team`	`LOONAR_SECRET_CLAUDE_KEY_TEAM_FILE`	La passerelle d'IA ┌ une variable par clé nommée dans hub.json (étape 7)
`claude_api_key`	`LOONAR_SECRET_CLAUDE_API_KEY_FILE`	« Ask ┌ dans la vue web
`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`	Connexion d'entreprise
`db_password`	`LOONAR_SECRET_DB_PASSWORD_FILE`	Une base de données de modèle

Le nom dans la variable est le nom du secret en majuscules, les autres caractères étant remplacés par `_` ┌ le secret `claude_key_anna` de hub.json devient `LOONAR_SECRET_CLAUDE_KEY_ANNA_FILE`.

Les variables sont définies **uniquement sur le service**, et non pour tout l'ordinateur, une fois le service installé (étape 4). Elles prennent effet au prochain démarrage du service, sans redémarrage de l'ordinateur ┌

```
$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'   uniquement si le serveur sort par un proxy
)
Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\CompassHub -Name Environment -Type
MultiString -Value $vars
Restart-Service CompassHub
```

Le hub lit un secret la première fois qu'il en a besoin. Un secret manquant est signalé là où il est utilisé, par exemple « secret 'jira_token' is not set: give it as LOONAR_SECRET_JIRA_TOKEN (or a file named in LOONAR_SECRET_JIRA_TOKEN_FILE) ┌. Les valeurs n'apparaissent jamais dans hub.json, dans les journaux ni dans la vue web. Une marque d'ordre des octets (BOM) au début, ainsi que des espaces ou un saut de ligne à la fin d'un fichier de secret (Bloc-notes), sont ignorés.

6. Étape 4 – Le service Windows et la première connexion

1. Dans PowerShell en tant qu'administrateur ┌

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

   Cette commande crée le service `CompassHub` (« Compass Hub (Loonar Compass team service) ┌), avec démarrage automatique sous LocalSystem, et le démarre.
2. Définissez maintenant les secrets du service (étape 3) et exécutez `Restart-Service CompassHub`.
3. Sur le serveur, ouvrez `http://127.0.0.1:8730/` et connectez-vous en tant que `admin` / `passw0rd` (avec un zéro). Le hub demande immédiatement un nouveau mot de passe et n'autorise rien d'autre d'ici là. Le mot de passe doit comporter au moins 10 caractères. Faites-le **avant** que l'étape 5 ne rende le hub accessible.

Vérification ┌

- `Get-Service CompassHub` indique Running ┌
- `C:\CompassHub\hub.log` montre le démarrage et votre connexion ┌
- la vue web liste le modèle de l'étape 2.

7. Étape 5 – HTTPS avec IIS (URL Rewrite + ARR)

Le hub parle en HTTP simple sur 127.0.0.1. IIS lui donne le nom et le certificat de l'entreprise.

1. Installez IIS avec URL Rewrite et ARR. Créez un site, par exemple **CompassHub**, avec une liaison `https`, port 443, le nom d'hôte `hub.company.com` et le certificat. Le chemin physique est un dossier vide, par exemple `C:\inetpub\compasshub`.
2. Activez le proxy et désactivez la réécriture de l'hôte dans les redirections. C'est **obligatoire** ┌ sinon ARR réécrit la redirection vers AD FS en l'adresse propre du hub, et la connexion d'entreprise échoue. Définissez aussi le délai d'attente pour les longues réponses de l'IA ┌

   ```
   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. Placez ce `web.config` dans le dossier du site. Il transmet tout au hub et autorise des corps de requête jusqu'à 32 Mo, car les questions accompagnées de diagrammes du modèle sont volumineuses ┌

```
<?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. Pare-feu ┌ autorisez uniquement le port 443 en entrée. Le port 8730 n'est jamais ouvert, car le hub écoute sur 127.0.0.1.
5. AD FS sur le même serveur ┌ AD FS utilise lui aussi le port 443 (HTTP.sys). Cochez **Exiger l'indication du nom du serveur** sur la liaison IIS (`New-WebBinding … -SslFlags 1`), sinon IIS et AD FS se gênent mutuellement.
6. Le hub n'a pas besoin de `preserveHostHeader` ni de `X-Forwarded-Proto` ┌ ses adresses proviennent de `redirect_uri` dans hub.json.

Le hub ne fait confiance à `X-Forwarded-For` (qu'ARR ajoute) que s'il provient d'un proxy situé sur le même ordinateur. Le journal d'audit et le blocage des jetons erronés voient alors l'adresse réelle du client.

Vérification ┌ depuis un poste de travail, `https://hub.company.com/` affiche la page de connexion sans avertissement de certificat.

8. Étape 6 – Connexion d'entreprise (AD FS ou Entra ID)

AD FS

1. Gestion AD FS → Groupes d'applications → Ajouter, puis le modèle **Application serveur accédant à une API web**, nom « Compass Hub ┌.
2. Application serveur ┌
   - notez l'**identificateur client** ┌
   - URI de redirection ┌ `https://hub.company.com/auth/callback` ┌
   - informations d'identification ┌ **Générer un secret partagé**. Enregistrez-le immédiatement dans `C:\CompassHub\secrets\oidc_client_secret` ┌ AD FS ne l'affiche qu'une seule fois.
3. API web ┌
   - identificateur ┌ l'identificateur client de l'étape précédente ┌
   - stratégie de contrôle d'accès ┌ les personnes autorisées à utiliser le hub, par exemple « Autoriser tout le monde ┌ (les rôles proviennent toujours des groupes) ┌
   - étendues autorisées ┌ `openid`, `profile`, `email`, `allatclaims`.
4. API web → Règles de transformation d'émission → « Envoyer les attributs LDAP en tant que revendications ┌ (Active Directory) ┌
   - *User-Principal-Name* → `upn` ┌
   - *E-Mail-Addresses* → `email` ┌
   - *Display-Name* → `name` ┌
   - *Token-Groups - Unqualified Names* → `groups`.

   (Saisissez les noms des revendications sortantes exactement ainsi.)

Dans `hub.json` (le hub ajoute lui-même `allatclaims` pour AD FS, afin que les revendications parviennent au jeton d'ID) ┌

```
"oidc": {
  "issuer": "https://adfs.company.com/adfs",
  "client_id": "<identificateur client>",
  "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

La configuration dans Entra ID ┌

- **Inscription d'application** ┌ plateforme *Web*, URI de redirection `https://hub.company.com/auth/callback`, un secret client (dans le fichier de secret), et le jeton d'ID avec les revendications facultatives `upn` et `email`.
- **Émetteur** ┌ `https://login.microsoftonline.com/<tenant-id>/v2.0`.

- **Groupes** ┌ par défaut, Entra les envoie sous forme d'ID d'objet. Placez ces ID dans `roles` ou, pour les groupes synchronisés depuis AD, choisissez « sAMAccountName ┌ dans la configuration du jeton.

Règles appliquées par le hub

- Le rôle provient des groupes à chaque connexion, et le plus élevé l'emporte. Une personne qui n'appartient à aucun des groupes n'obtient aucun accès.
- Un compte d'entreprise portant le même nom qu'un utilisateur local du hub est refusé tant que l'utilisateur local n'a pas été renommé ou supprimé.
- Le hub vérifie lui-même le jeton d'ID ┌ la signature RS256, l'émetteur, l'audience, l'expiration et le nonce, avec PKCE et un state à usage unique.
- Lorsque tout fonctionne, définissez `"password_login": false` ┌ seul le bouton de l'entreprise subsiste. Les jetons d'API des clients MCP continuent de fonctionner. Conservez un mot de passe d'administrateur local dans votre coffre-fort, au cas où le fournisseur d'identité serait indisponible.

Vérification ┌ après `Restart-Service CompassHub`, « Sign in with your company account ┌ mène à AD FS et revient. hub.log indique « … signed in with a company account as architect ┌, et l'onglet **Users** liste le compte d'entreprise avec son rôle.

9. Étape 7 – Clés d'IA, Jira, Confluence et la stratégie d'équipe

Ajoutez les sections à `hub.json`. Chaque secret nommé ici a aussi besoin de sa variable `…_FILE` (étape 3). Exécutez ensuite `Restart-Service CompassHub` ┌ les personnes connectées le restent.

```
"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
}
```

Paramètre	Signification
`ai.keys`	Quelle clé Claude une personne utilise. Ordre ┌ le nom d'utilisateur, puis `role:<role>`, puis `*`. Aucune correspondance signifie pas d'IA pour cette personne.
`ai.limits`	Jetons par jour et par mois. Au-delà de la limite, le hub refuse avec un message clair.
`ai.models`	Les modèles autorisés ┌ les autres modèles sont refusés.
`policy.ai_via_hub`	Compass interroge l'IA uniquement via le hub ┌ aucune clé d'API sur les postes de travail.
`policy.jira_via_hub`, `confluence_via_hub`	Jira/Confluence via le compte de service du hub. Un lecteur (viewer) peut seulement lire ┌ chaque modification est auditée.
`policy.min_approval`	Le mode de validation le plus faible autorisé dans Compass pour les écritures dans le modèle (`ask` est le plus strict).
`policy.web_access`, `web_allowed_domains`	Si l'assistant peut effectuer des recherches sur le web ou lire des pages, et depuis quels domaines.
`policy.update_check`	Si Compass vérifie toutes les heures sur GitHub la présence d'une nouvelle version.

Les administrateurs modifient ensuite la stratégie dans l'onglet **Team policy** de la vue web, et la consommation par personne se trouve dans **Users** → **AI usage**.

10. Étape 8 – Les postes de travail (stratégie de groupe)

1. **Faire confiance au certificat.** Si le certificat du hub provient de l'autorité de certification de l'entreprise, déployez sa racine sur les postes de travail (GPO ┌ Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de clé publique → Autorités de certification racines de confiance). Sans cela, Compass signale un certificat non approuvé (UnknownIssuer).
2. **Modèles.** Copiez `LoonarCompass.admx` dans `\\<domain>\SYSVOL\<domain>\Policies\PolicyDefinitions`, et `en-US\LoonarCompass.adml` (et `pl-PL` si nécessaire) dans les sous-dossiers de langue. Sans magasin central, copiez-les dans `C:\Windows\PolicyDefinitions` sur l'ordinateur où vous modifiez la GPO.
3. **GPO** pour l'UO des postes de travail ┌ Configuration ordinateur → Modèles d'administration → Loonar → Loonar Compass.

Stratégie	Valeur de registre (HKLM\SOFTWARE\Policies\Loonar\Compass)	Effet
Hub address	`HubUrl` (texte)	L'adresse du hub est fixée dans Compass et ne peut pas être modifiée.
Require the hub	`RequireHub` = 1	L'assistant ne fonctionne que si la personne est connectée au hub.
Web access	`WebAccess` = 0	Pas de recherche sur le web ni de lecture de pages ┌ le bouton 🌐 est désactivé.
Update check	`UpdateCheck` = 0	Pas de vérification quotidienne d'une nouvelle version.
Minimum approval mode	`MinApproval` = ask / plan / auto	Un mode plus faible ne peut pas être choisi.
Allowed AI providers	`AllowedProviders`, par exemple `anthropic`	Les autres fournisseurs (par exemple OpenAI) sont refusés.

Sans domaine, les mêmes valeurs peuvent être importées avec `LoonarCompass-company-policy.reg` (et supprimées avec `LoonarCompass-remove-policy.reg`). La stratégie de l'ordinateur l'emporte sur la stratégie du hub et sur les paramètres de l'utilisateur ┌ elle ne peut que rendre Compass plus strict.

Installer Compass. `LoonarCompass-Setup-0.9.exe` installe pour l'utilisateur actuel (`%LOCALAPPDATA%\Programs\Loonar Compass`) ou pour tous les utilisateurs (`Program Files`), et enregistre le complément dans Enterprise Architect. Pour les outils de déploiement (Intune, Configuration Manager, un script de démarrage), il s'installe sans fenêtre ┌

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

Option	Effet
`--quiet`	Pas de fenêtre ni de questions. Code de sortie 0 = installé, 1 = erreur, 740 = `--all-users` sans droits d'administrateur. Le résultat se trouve dans `%TEMP%\LoonarCompass-Setup.log` (pour SYSTEM ┌ `C:\Windows\Temp`).
`--all-users`	Pour tout le monde ┌ Program Files, le menu Démarrer commun, le complément dans EA pour tous les utilisateurs (HKLM). Exécutez-le en tant que SYSTEM ou en tant qu'administrateur.
`--dir <dossier>`	Un autre dossier de programme.
`--lang en|pl|de|fr`	La langue des fichiers de licence et du journal des modifications.
`--no-desktop`, `--no-start-menu`	Sans ces raccourcis.
`--no-ea-addin`	Sans le complément dans Enterprise Architect.

La même commande met à jour une installation existante. Fermez d'abord Compass et EA sur l'ordinateur. Les paramètres de l'utilisateur ne sont pas modifiés ┌ avec la stratégie de l'ordinateur (adresse du hub, hub obligatoire), personne n'a rien à configurer. Désinstallation silencieuse ┌ `"C:\Program Files\Loonar Compass\uninstall.exe" --uninstall --quiet`.

La première connexion de l'utilisateur. Dans Compass, ouvrez Paramètres → Équipe (Compass Hub) → **Se connecter avec le compte d'entreprise**. Le navigateur ouvre AD FS et revient à Compass. La connexion dure 12 heures et survit à un redémarrage du hub.

11. Étape 9 – Liste de recette

✓	Test	Résultat attendu
☐	Ouvrir `https://hub.company.com/` depuis un poste de travail	La page de connexion, sans avertissement de certificat
☐	Connexion d'entreprise en tant que membre de Compass-Architects	Rôle architect ┌ hub.log « signed in with a company account as architect ┌
☐	Une personne n'appartenant à aucun des groupes Compass	Refusée
☐	Compass avec la GPO, avant la connexion ┌ envoyer une question	« Votre organisation exige le hub d'équipe ┌ connectez-vous dans Paramètres → Équipe (Compass Hub)… ┌
☐	La même chose après la connexion	Une réponse, sans clé d'API sur le poste de travail ┌ une ligne dans Users → AI usage
☐	Un lecteur (viewer) pose une question (pas de clé pour les lecteurs)	« le hub n'a pas de clé d'IA pour vous ┌
☐	Le bouton 🌐 dans Compass	Désactivé ┌ « Désactivé par votre organisation ┌
☐	`Restart-Service CompassHub`, puis poser une nouvelle question	Fonctionne sans nouvelle connexion
☐	Hub arrêté, poser une question	Un court message indiquant que le hub ne répond pas ┌ EA continue de fonctionner
☐	Jira ┌ « Create a Jira issue: test ┌ (architect)	Le ticket dans le projet ┌ une entrée dans le journal d'audit du hub avec le nom de la personne

12. Exploitation ┌ mise à jour, sauvegarde, journaux, suppression

Mise à jour

```
Stop-Service CompassHub
Copy-Item .\compass-hub.exe C:\CompassHub\compass-hub.exe -Force   # depuis le nouveau zip, après vérification de son SHA-256
Start-Service CompassHub
```

hub.json, les secrets et les connexions restent inchangés. Les personnes restent connectées.

Ce qu'il faut sauvegarder (C:\CompassHub)

Fichier / dossier	Contenu
`hub.json`	Configuration, utilisateurs locaux (uniquement les hachages des mots de passe et des jetons), stratégie
`audit.jsonl`	Le journal d'audit des modifications et des connexions
`changes\`, `notes\`	Ensembles de modifications à relire et notes de l'équipe
`ai_usage.jsonl`	Consommation d'IA par personne (la base des limites)
`company_accounts.json`, `sessions.json`	Comptes d'entreprise rencontrés et connexions en cours (hachages) ┌ leur perte est sans conséquence ┌ les personnes se reconnectent
`secrets\`	Uniquement si votre sauvegarde est chiffrée. Sinon, conservez les valeurs dans le coffre-fort de mots de passe.
`models\`	Les fichiers de modèle, s'ils ne sont pas conservés ailleurs

Journaux

- `hub.log` ┌ démarrage, connexions, requêtes refusées, erreurs. Une « internal error (id …) ┌ affichée à un utilisateur a ses détails ici sous le même id.
- `audit.jsonl` et `hub.log` sont renommés avec une date lorsqu'ils deviennent volumineux.

Suppression

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

Supprimez ensuite le site IIS, le groupe d'applications AD FS et la GPO, puis supprimez `C:\CompassHub` après la sauvegarde.

13. Dépannage

Symptôme	Cause et solution
Compass ┌ certificat non approuvé / UnknownIssuer ┌ le navigateur affiche « Non sécurisé ┌	Le poste de travail ne fait pas confiance à la racine du certificat du hub. Déployez l'autorité de certification racine (étape 8), puis redémarrez le navigateur et Compass.
La connexion d'entreprise aboutit à `https://hub.company.com/adfs/…` ou à une erreur 404	ARR réécrit la redirection. Définissez `reverseRewriteHostInResponseHeaders` = False (étape 5).
« <name> is not in any group of the hub (…): ask the administrator for access ┌	La personne n'appartient à aucun des groupes de rôles, ou la revendication `groups` est absente. Vérifiez la règle de transformation « Token-Groups - Unqualified Names → groups ┌ et l'étendue `allatclaims`.
« A local user of the hub has the same name ┌	Renommez ou supprimez cet utilisateur local dans l'onglet Users.
Compass ┌ « Le hub d'équipe ou le serveur placé devant lui ne répond pas correctement (502) ┌	Le service est arrêté ou en cours de démarrage ┌ `Get-Service CompassHub`, puis hub.log.
Compass ┌ « Votre connexion au hub d'équipe a expiré ┌	12 heures se sont écoulées, ou sessions.json a été perdu. Reconnectez-vous dans Paramètres → Équipe.
« le hub n'a pas de clé d'IA pour vous ┌	Aucune entrée `ai.keys` pour la personne, son rôle ou `*`.
« votre limite d'IA du jour est épuisée ┌	Augmentez `ai.limits` pour la personne ou le rôle, ou attendez le lendemain.
« secret '…' is not set: give it as LOONAR_SECRET_… ┌	La variable `…_FILE` manque dans la valeur `Environment` du service, ou le fichier est vide ou illisible pour SYSTEM.
hub.log ┌ « <address>: 20 wrong tokens, refused for 10 minutes ┌	20 jetons erronés **différents** sont venus d'une même adresse (un ancien jeton répété ne compte qu'une fois). Les jetons valides continuent de fonctionner. Identifiez le client dans hub.log.
Les grandes questions échouent avec 413 ou 404.13	`maxAllowedContentLength` dans web.config (étape 5).
Les longues réponses s'arrêtent avec 502.3 au bout de 2 minutes	Le `timeout` d'ARR (étape 5).
AD FS ┌ MSIS7628 de `Grant-AdfsApplicationPermission` juste après l'installation d'AD FS	La batterie est encore en cours de démarrage ┌ relancez la commande quelques minutes plus tard.
hub.log / AD FS ┌ MSIS9622 « Client authentication failed ┌	Le fichier de secret ne correspond pas à AD FS. Créez un nouveau secret ┌ `Set-AdfsServerApplication -`

	`TargetIdentifier <client id> -ResetClientSecret`, écrivez-le dans le fichier, `Restart-Service CompassHub`.
Compass sur un Windows Server (par exemple Services Bureau à distance) ┌ l'export PDF échoue, ou la première connexion à Office est bloquée	Compass produit les PDF avec Word et PowerPoint sur l'ordinateur où il s'exécute. Sous Windows Server, la configuration de sécurité renforcée d'Internet Explorer peut bloquer la première connexion à Office (`odc.officeapps.live.com`) ┌ ajoutez les sites de connexion d'Office aux sites de confiance, ou désactivez ce paramètre pour les utilisateurs dans le Gestionnaire de serveur.

14. Linux et Docker

Le même hub s'exécute dans un conteneur. Le dossier de données (hub.json avec `"listen": "0.0.0.0:8730"`, les modèles et les fichiers du hub) est monté en tant que `/data` et doit être accessible en écriture à l'utilisateur 10001. Les secrets proviennent des variables `LOONAR_SECRET_*` ou des secrets Docker via `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
```

Placez devant lui nginx ou un autre proxy HTTPS, comme à l'étape 5. Le proxy doit conserver inchangé l'en-tête `Location` des redirections, transmettre `X-Forwarded-For`, autoriser des corps de 32 Mo et un délai d'attente de 5 minutes. Pour les modèles SQL Server, MySQL ou Oracle, construisez votre propre image à partir de celle-ci et ajoutez le pilote ODBC Linux de l'éditeur.