

5 - Accès distant et sécurité

Publier Immich en HTTPS, intégrer Authentik et protéger les comptes et clés d'API.

- [5.1 - Reverse proxy Caddy](#)
- [5.2 - Cloudflare, DNS et accès distant](#)
- [5.3 - Authentification OIDC avec Authentik](#)
- [5.4 - Sécuriser les comptes, sessions et API](#)

5.1 - Reverse proxy Caddy

Immich doit être publié à la racine d'un domaine ou sous-domaine. Une publication sous `/immich` n'est pas prise en charge.

Exemple Caddy

Pour ton environnement :

```
immich.dreamsaphir.net {  
    reverse_proxy http://ADRESSE_TRUENAS:30041  
}
```

Après modification :

```
caddy validate --config /etc/caddy/Caddyfile  
sudo systemctl reload caddy  
sudo systemctl status caddy --no-pager
```

Si Caddy fonctionne en conteneur, l'adresse `127.0.0.1` désigne le conteneur Caddy lui-même. Utiliser une adresse ou un réseau Docker permettant d'atteindre TrueNAS.

En-têtes attendus

Le proxy doit transmettre :

```
Host  
X-Real-IP  
X-Forwarded-For  
X-Forwarded-Proto
```

Caddy gère normalement les en-têtes de proxy requis. Une configuration personnalisée ne doit pas les supprimer.

Gros fichiers et délais

Les vidéos volumineuses exigent des délais suffisants. Tester un vrai upload depuis l'extérieur, pas seulement l'ouverture de la page de connexion.

Contrôles

```
getent hosts immich.dreamsaphir.net
curl -I https://immich.dreamsaphir.net
curl -I http://ADRESSE_TRUENAS:30041
journalctl -u caddy -n 100 --no-pager
```

Tester également :

```
https://immich.dreamsaphir.net/.well-known/immich
```

Ce point de terminaison doit atteindre Immich, notamment pour éviter des problèmes avec l'application mobile.

Certificat interne

Si Caddy et Immich communiquent sur le réseau local en HTTP, le chiffrement public est terminé par Caddy. Restreindre le port 30041 au réseau interne et ne pas l'exposer directement sur Internet.

Après une migration

1. tester la nouvelle instance par IP locale ;
2. conserver l'ancienne instance arrêtée ou en lecture seule ;
3. modifier la cible Caddy ;
4. recharger Caddy ;
5. vérifier Web, mobile, OAuth et uploads ;
6. conserver un moyen de retour rapide vers l'ancienne cible.

Référence : <https://docs.immich.app/administration/reverse-proxy/>

5.2 - Cloudflare, DNS et accès distant

Cloudflare peut fournir le DNS, un proxy public et des certificats entre le client et son réseau. La configuration doit rester cohérente avec Caddy et Immich.

DNS

Créer un enregistrement pour :

immich.dreamsaphir.net

Deux modes sont possibles :

Mode	Effet
DNS only	le client rejoint directement l'adresse publiée
Proxied	le trafic passe par le proxy Cloudflare

Le mode proxied ajoute une couche de protection mais aussi des limites de taille, de délai et de comportement selon l'offre. Tester les vidéos les plus volumineuses. Si les envois échouent uniquement à travers Cloudflare, comparer avec un accès local et examiner les limites du compte.

TLS

Avec un certificat valide sur Caddy, utiliser un mode de chiffrement strict entre Cloudflare et l'origine. Éviter les modes qui acceptent un certificat invalide.

Ports et pare-feu

- exposer uniquement 80 et 443 vers Caddy si nécessaire ;
- ne pas publier directement 30041 sur Internet ;

- filtrer l'administration TrueNAS ;
- conserver WireGuard pour les accès d'administration ;
- limiter les règles NAT à la cible exacte.

En-têtes et adresse client

Le proxy Caddy doit transmettre l'adresse client et le protocole d'origine. Si plusieurs proxies se suivent, configurer les plages de confiance avec prudence afin d'éviter qu'un client forge `X-Forwarded-For`.

Diagnostic

```
dig +short immich.dreamsaphir.net
curl -vI https://immich.dreamsaphir.net
curl -I http://ADRESSE_TRUENAS:30041
```

Comparer :

1. accès local direct ;
2. accès local par le domaine ;
3. accès extérieur par le domaine ;
4. upload d'une petite photo ;
5. upload d'une grande vidéo.

Erreurs courantes

Symptôme	Piste
525	certificat ou TLS entre Cloudflare et Caddy
403	règle Cloudflare, authentification ou pare-feu
upload interrompu	taille ou délai du proxy
boucle OAuth	domaine ou URI de redirection incorrecte
mauvaise adresse client	chaîne d'en-têtes proxy incorrecte

La protection d'accès Cloudflare placée devant tout Immich peut interférer avec l'application mobile et OAuth. Tester avant de l'imposer.

Référence Immich : <https://docs.immich.app/administration/reverse-proxy/>

5.3 - Authentification OIDC avec Authentik

Immich prend en charge OpenID Connect. Ton fournisseur utilise le domaine `auth.dreamsaphir.net`.

Créer l'application Authentik

Dans Authentik :

1. ouvrir `Applications > Applications` ;
2. créer une application Immich ;
3. choisir un fournisseur `OAuth2/OpenID Connect` ;
4. utiliser un client confidentiel et le flux Authorization Code ;
5. noter le Client ID et le Client Secret ;
6. choisir une clé de signature.

URI de redirection

Ajouter exactement :

```
app.immich:///oauth-callback
https://immich.dreamsaphir.net/auth/login
https://immich.dreamsaphir.net/user-settings
```

La première URI est indispensable pour Android et iOS.

Pour Authentik 2026.5 et versions plus récentes, définir les URI comme `Strict` et `Authorization` selon le guide d'intégration. Les versions antérieures gèrent différemment le type d'URI.

Configurer Immich

Ouvrir :

Valeurs principales :

```
Enabled      : true
Issuer URL   : https://auth.dreamsaphir.net/application/o/immich/
Client ID    : valeur Authentik
Client Secret : valeur Authentik
Scope        : openid email profile
Button Text  : Connexion avec Authentik
Auto Register : selon la politique choisie
```

Adapter le slug `immich` si l'application Authentik en utilise un autre.

Vérifier la découverte OIDC

```
curl -fsS \
  https://auth.dreamsaphir.net/application/o/immich/.well-known/openid-configuration \
  | python3 -m json.tool
```

Tester sans se verrouiller

1. garder une session administrateur locale ouverte ;
2. utiliser une fenêtre privée pour le test OIDC ;
3. tester le Web ;
4. tester l'application mobile ;
5. vérifier la création ou liaison du compte ;
6. vérifier le retour après déconnexion.

Ne pas activer immédiatement `Auto Launch` ni désactiver le mot de passe local avant un test complet.

Récupération

Dans le conteneur serveur :

```
immich-admin enable-password-login  
immich-admin disable-oauth-login  
immich-admin reset-admin-password
```

Docker Compose :

```
docker exec -it immich_server immich-admin enable-password-login
```

Références :

- <https://docs.immich.app/administration/oauth/>
- <https://integrations.goauthentik.io/media/immich/>

5.4 - Sécuriser les comptes, sessions et API

Comptes

- utiliser un mot de passe unique pour le compte local de secours ;
- limiter le rôle administrateur ;
- désactiver ou supprimer les comptes inutiles après sauvegarde ;
- vérifier les sessions après une réinitialisation ;
- protéger Authentik par MFA ;
- conserver une procédure de récupération hors d'Immich.

Sessions

Après suspicion de compromission :

1. réinitialiser le mot de passe ;
2. invalider les sessions si l'option est proposée ;
3. révoquer les clés API ;
4. examiner les journaux du reverse proxy et d'Immich ;
5. vérifier les comptes administrateurs ;
6. changer les secrets OAuth si nécessaire.

Clés API

Les clés se créent dans les paramètres utilisateur. Limiter leurs permissions aux opérations nécessaires.

Ne jamais placer une clé directement dans :

- un script partagé ;
- BookStack ;
- l'historique du shell ;

- une URL ;
- un dépôt Git ;
- une capture d'écran.

Utiliser un fichier d'environnement protégé :

```
chmod 600 ~/.config/immich/cli.env
```

CLI Immich en conteneur

```
docker run --rm -it \  
  --env-file ~/.config/immich/cli.env \  
  -v "$PWD":/import:ro \  
  ghcr.io/immich-app/immich-cli:latest server-info
```

Exemple de fichier :

```
IMMICH_INSTANCE_URL=https://immich.dreamsaphir.net/api  
IMMICH_API_KEY=REPLACER
```

Exposition réseau

- publier uniquement le reverse proxy ;
- garder PostgreSQL et Redis non exposés ;
- restreindre le port TrueNAS 30041 au LAN ;
- utiliser WireGuard pour l'administration ;
- mettre à jour Immich, TrueNAS, Caddy et Authentik ;
- sauvegarder avant une mise à jour majeure.

Données sensibles

Les photos contiennent potentiellement visages, lieux et dates. Le partage partenaire peut exposer des métadonnées GPS. Vérifier les droits des albums, liens publics et partenaires.

Contrôle périodique

- liste des utilisateurs ;
- administrateurs ;
- clés API ;
- partages publics ;
- sauvegardes et tests de restauration ;
- certificats ;
- journaux d'authentification ;
- versions et correctifs.

Références :

- <https://docs.immich.app/administration/user-management/>
- <https://docs.immich.app/features/command-line-interface/>