CONNECTER VOTRE ANNUAIRE

# AD FS

Désignez Active Directory Federation Services (2016 ou ultérieur) comme annuaire de votre espace REVIEWIT, en OpenID Connect natif, sans SAML.

VERSION
**2.0 · Octobre 2026**

DURÉE
**Vingt minutes, en trois étapes**

DIFFUSION
**Confidentiel · Clients REVIEWIT**

## CE QU'IL VOUS FAUT

01 **Le lien de configuration** reçu par e-mail de la part de REVIEWIT. Il est valable jusqu'à la date qu'il indique, et quiconque l'ouvre peut connecter un annuaire à votre espace : ne le transférez pas.

02 Un administrateur du serveur AD FS (console AD FS Management), et, pour la section 4, un fournisseur MFA configuré dans AD FS (Azure MFA, authentification par certificat ou adaptateur tiers).

03 **Vingt minutes**, dans l'ordre de ce guide : d'abord l'application chez votre annuaire, puis l'assistant REVIEWIT, en trois étapes.

## L'ASSISTANT, EN TROIS ÉTAPES

ÉTAPE 1

### Connecter l'annuaire

Votre annuaire se décrit, TrustGate le vérifie ; rien n'est enregistré avant sa réponse.

ÉTAPE 2

### Prouver que la porte s'ouvre

Une connexion réelle, sans session ni droit : la preuve que la porte s'ouvre, et pour qui.

ÉTAPE 3

### Activer l'espace

Vous devenez le premier administrateur ; le lien de configuration meurt.

## DANS CE GUIDE


1 Comment REVIEWIT se fédère à votre annuaire

2 Les deux adresses de retour à enregistrer

3 Créer l'application chez AD FS

4 Authentification forte (MFA)

5 L'assistant de configuration, en trois étapes

6 Ce que REVIEWIT reçoit, et ce qu'il ne reçoit jamais

7 Après l'activation

8 Dépannage et liste de contrôle

## 01 Comment REVIEWIT se fédère à votre annuaire

REVIEWIT ne stocke ni ne vérifie jamais les mots de passe de vos utilisateurs. L'authentification est déléguée à votre annuaire, à travers **REVIEWIT TrustGate**, l'autorité d'identité de REVIEWIT dans votre région d'hébergement. Votre annuaire reste la seule autorité sur qui sont vos utilisateurs et comment ils se connectent ; chaque application REVIEWIT se tient derrière cette frontière unique, auditable.




**PRINCIPE DIRECTEUR**

TrustGate demande ce qu'il peut demander à votre annuaire, et ne croit que ce qu'il peut vérifier. Une authentification forte demandée n'est jamais tenue pour acquise : seule la preuve rendue dans le jeton compte.

**PRISE EN CHARGE**

AD FS 2016 ou ultérieur est pris en charge par le type « OpenID Connect » de l'assistant, grâce à sa prise en charge native d'OpenID Connect. AD FS 2012 R2 (SAML / WS-Federation seulement) n'est pas pris en charge.

## 02 Les deux adresses de retour à enregistrer

Un annuaire refuse toute connexion dont il ne connaît pas l'adresse de retour. REVIEWIT en utilise deux pour votre espace : l'une sert à la connexion de preuve de l'assistant, l'autre à toutes les connexions qui suivront. Elles sont stables : vous les enregistrez une fois pour toutes, sur l'application que vous créez pour REVIEWIT.

| USAGE | ADRESSE DE RETOUR (REDIRECT URI) |
|---|---|
| **Connexion de preuve** | `https://auth.<région>.we-reviewit.com/federation/callback-candidate/<identifiant de votre espace>` |
| **Toutes les connexions suivantes** | `https://auth.<région>.we-reviewit.com/federation/callback/<identifiant de votre espace>` |

**OÙ LES TROUVER**

L'assistant les affiche prêtes à copier, à sa première étape, sous « Adresses de retour à enregistrer dans votre annuaire ». Ne les retapez pas : l'autorité qui sert votre espace et l'identifiant de l'espace n'existent que là. Vous pouvez ouvrir le lien, copier les deux adresses, et revenir à l'assistant plus tard : il reprend exactement où vous l'avez laissé.

# 03 Créer l'application chez AD FS

Un administrateur AD FS crée un groupe d'applications dédié à REVIEWIT TrustGate. Deux règles d'émission y ajoutent l'adresse e-mail et les méthodes d'authentification, que REVIEWIT lit dans le jeton.

01 **AD FS Management › Application Groups › Add Application Group**

Nom : REVIEWIT TrustGate. Modèle : Server application accessing a web API.

02 **Server application : les deux adresses de retour**

Notez le Client Identifier généré. Dans Redirect URI, ajoutez les deux adresses de la section 2, l'une après l'autre, exactement.

03 **Generate a shared secret**

Cochez la case et copiez le secret immédiatement : il n'est plus jamais affiché. Il ne doit être saisi que dans l'assistant (section 5) ; ne le transmettez à personne.

04 **Web API**

Identifier : collez le Client Identifier de l'étape 02. Access control policy : Permit everyone pour l'instant (la section 4 y ajoute le MFA). Permitted scopes : openid, profile, email, allatclaims.

05 **Issuance Transform Rules de la Web API : deux règles**

Send LDAP Attributes as Claims : attribut E-Mail-Addresses → type de revendication sortant email (ajoutez aussi User-Principal-Name → upn). Pass Through or Transform an Incoming Claim : revendication entrante Authentication Methods References → type sortant amr. Sans la première, la connexion de preuve échoue sur « jeton sans email » ; sans la seconde, aucune session renforcée n'est possible.

06 **Notez l'autorité**

https://<fs.votre-domaine>/adfs. Vérifiez qu'elle publie https://<fs.votre-domaine>/adfs/.well-known/openid-configuration et que son certificat TLS est émis par une autorité publique : l'autorité REVIEWIT, hébergée hors de votre réseau, doit pouvoir la joindre.

### CE QUE VOUS SAISIREZ DANS L'ASSISTANT

| CHAMP DE L'ASSISTANT | VALEUR |
|---|---|
| **Annuaire** | OpenID Connect |
| **Nom affiché à vos utilisateurs** | Le nom de votre organisation, tel que vos utilisateurs le reconnaissent — « Contoso », pas « AD FS ». |
| **Autorité OIDC** | `https://<fs.votre-domaine>/adfs` |
| **Identifiant client** | Le Client Identifier de la Server application. |
| **Secret client** | Le shared secret généré à l'étape 03. |
| **Valeurs amr attestant le MFA** | `http://schemas.microsoft.com/claims/multipleauthn (section 4)` |

# 04 Authentification forte (MFA)

Les consoles d'administration de REVIEWIT exigent une session renforcée : au moment voulu, TrustGate demande à votre annuaire une authentification à plusieurs facteurs, puis lit la preuve dans le jeton rendu. Deux revendications font foi : `amr` (les méthodes d'authentification employées) et `acr` (la classe d'authentification satisfaite). Par défaut, la valeur `mfa` dans amr atteste le second facteur ; tout autre vocabulaire se déclare dans l'assistant, sous « Réglages MFA ».

### 01 Un fournisseur MFA dans AD FS

AD FS Management › Service › Authentication Methods › Multi-factor Authentication Methods : activez Azure MFA, l'authentification par certificat, ou votre adaptateur tiers, et vérifiez que vos administrateurs y sont inscrits.

### 02 La stratégie de contrôle d'accès de la Web API

Application Groups › REVIEWIT TrustGate › Web API › Access Control Policy : Permit everyone and require MFA — ou Permit specific group and require MFA avec le groupe de vos administrateurs REVIEWIT, et une seconde règle « Permit everyone » pour les autres utilisateurs.

### 03 Ce que rapporte le jeton

Quand le MFA a été exigé, AD FS ajoute http://schemas.microsoft.com/claims/multipleauthn aux méthodes d'authentification, que la règle d'émission de la section 3 envoie dans amr. C'est cette valeur que TrustGate reconnaît, une fois déclarée dans l'assistant.

**DANS L'ASSISTANT — RÉGLAGES MFA**

**Valeurs amr attestant le MFA**
http://schemas.microsoft.com/claims/multipleauthn. Sans cette déclaration, TrustGate ne reconnaît que la valeur standard mfa, qu'AD FS n'émet pas.

**Valeurs amr attestant la résistance au hameçonnage**
Laissez vide, sauf si votre fournisseur MFA émet une méthode propre aux clés FIDO2 ou aux certificats que vous souhaitez distinguer.

**Contexte d'authentification (acr)**
Laissez vide. AD FS n'honore pas acr_values de façon générale ; l'exigence MFA vient de la stratégie de contrôle d'accès.

### UNE ÉLÉVATION À LA DEMANDE N'EXISTE PAS SUR AD FS

TrustGate demande le second facteur au moment d'entrer dans une console d'administration, mais AD FS applique sa stratégie à la connexion, pas sur demande. Si la stratégie exige le MFA de tous, chaque connexion REVIEWIT le porte ; si elle ne l'exige que d'un groupe, seuls ses membres obtiennent une session renforcée. Un administrateur hors de ce groupe se verra refuser la console, jamais accorder une session sur parole.

# 05 L'assistant de configuration, en trois étapes

Ouvrez le lien de configuration. Il vous dit à qui appartient l'espace, jusqu'à quand il est valable, et que personne ne peut s'y connecter tant que l'annuaire n'est pas connecté. Cliquez **Commencer**.

## ÉTAPE 1 Connecter votre annuaire

L'assistant affiche d'abord les deux adresses de retour (section 2), puis demande votre annuaire. Rien n'est enregistré tant que l'annuaire n'a pas répondu.

01 **Choisissez le type d'annuaire**
OpenID Connect pour AD FS — comme pour Google Workspace, Okta, Ping ou Keycloak. Le type « Microsoft Entra ID » est réservé à un locataire Microsoft 365.

02 **Renseignez le nom affiché, l'autorité OIDC, l'identifiant client et le secret client**
Le secret n'est jamais réaffiché ni écrit dans un journal : il n'est ouvert que par le composant qui connecte vos utilisateurs, et chaque ouverture laisse un reçu.

03 **Ajustez les réglages MFA si la section 4 vous l'a demandé**
Sinon, laissez-les vides : les défauts s'appliquent.

04 **Cliquez « Vérifier l'annuaire »**
TrustGate lit le document de découverte de votre annuaire et passe cinq contrôles, dans l'ordre : l'adresse répond ; c'est un document OpenID Connect lisible ; il annonce un émetteur, un point d'autorisation et un point de jeton ; il publie des clés de signature ; votre annuaire accepte l'identifiant et le secret. Un échec nomme le contrôle fautif.

05 **Cliquez « Enregistrer et continuer »**
L'annuaire est déclaré candidat : il ne sert encore personne.

## ÉTAPE 2 Prouver que la porte s'ouvre

Cliquez « Me connecter avec mon annuaire ». Vous êtes envoyé chez votre annuaire, vous vous y authentifiez (avec le second facteur si votre politique l'exige), et vous revenez dans l'assistant. Aucune session n'est ouverte et aucun droit n'est accordé : REVIEWIT enregistre seulement que la porte s'ouvre, pour qui, et avec quelle force d'authentification.

Si la connexion échoue, rien n'est adopté et rien n'a changé. « Modifier la configuration » vous ramène à l'étape 1 : le réglage le plus souvent corrigé à ce moment est celui de la section 4, quand l'annuaire annonce le second facteur sous un autre nom.

## ÉTAPE 3 Activer l'espace

L'assistant récapitule l'organisation, l'annuaire et l'identité qui vient de se connecter, puis énonce ce que l'activation change :

- cette identité devient le premier administrateur de l'espace ;
- toute connexion ultérieure passe par votre annuaire ;
- le lien de configuration cesse de fonctionner.

Cliquez « Activer mon espace ». Une confirmation est envoyée au contact désigné lors de la commande, et « Ouvrir mon espace » vous conduit à votre console, où vous vous connectez par votre annuaire.

## 06 Ce que REVIEWIT reçoit, et ce qu'il ne reçoit jamais

| REÇU DANS LE JETON | USAGE CHEZ REVIEWIT |
|---|---|
| `sub` | L'identifiant stable de la personne chez AD FS. C'est lui, avec l'émetteur, qui lie l'identité à son compte REVIEWIT — jamais l'adresse e-mail. |
| `email, upn` | L'adresse de connexion, en minuscules, émise par vos règles. Elle sert à l'affichage, aux habilitations et aux notifications ; elle n'a jamais valeur de lien. |
| `amr, acr / acrs` | La preuve de l'authentification forte (section 4). Lue, jamais supposée. |
| `auth_time` | L'instant de l'authentification réelle. Les gestes sensibles exigent une authentification récente : sans cette revendication, ils sont refusés. |
| `name` | Le nom affiché, à titre informatif. Il n'a jamais valeur d'identité. |

**JAMAIS REÇU, JAMAIS DEMANDÉ**

**Aucun mot de passe**
La saisie a lieu chez votre annuaire, sur sa page.

**Aucun accès à vos ressources**
TrustGate ne demande que les portées openid, profile et email. Rien n'autorise à lire votre messagerie, vos fichiers ou votre annuaire.

**Aucune liste de vos utilisateurs**
Un compte REVIEWIT naît à la première connexion d'une personne, et seulement s'il a été décidé de l'accorder ; ce compte ne porte aucun droit par lui-même.

**Aucun rapprochement par adresse e-mail**
L'identité est liée par le couple émetteur + identifiant stable. Une adresse réutilisée ne donne jamais accès au compte d'un autre.

## 07 Après l'activation

Votre annuaire s'administre depuis le Subscription Manager, sous **Paramètres › Fournisseur d'identité**. La page liste les annuaires déclarés, leur état, et porte le formulaire de déclaration — replié, parce que déclarer un annuaire est un acte rare. Chaque geste exige un motif, écrit tel quel dans la piste d'audit.

| | |
|---|---|
| **Changer d'annuaire sans jamais verrouiller personne** | Le nouvel annuaire est déclaré candidat, prouvé par une connexion réelle, puis adopté. Jusqu'à l'adoption, l'annuaire en service continue de servir. |

| | |
|---|---|
| **Désactiver un annuaire** | Refusé s'il ne resterait plus aucune porte : personne ne peut s'enfermer dehors. |
| **Faire tourner le secret partagé** | Générez un nouveau secret sur la Server application, déclarez l'annuaire à nouveau (même autorité, nouvelle référence de secret), prouvez-le, adoptez-le ; retirez l'ancien secret ensuite. Le support REVIEWIT dépose la valeur du nouveau secret dans le coffre de l'autorité sous la référence que vous avez déclarée. |
| **Révoquer une personne** | Désactivez-la chez votre annuaire, et sa prochaine connexion est refusée. Pour couper une session déjà ouverte, désactivez son compte dans REVIEWIT : les sessions sont revalidées toutes les cinq minutes. |

# 08 Dépannage

| CE QUE VOUS VOYEZ | CAUSE | CE QU'IL FAUT FAIRE |
|---|---|---|
| **MSIS9224 : redirect_uri invalide** | Une des deux adresses de retour manque ou diffère d'un caractère. | Recopiez les deux adresses depuis l'assistant dans la Server application. |
| **MSIS9605 : client non autorisé / secret refusé** | Secret mal copié ou expiré, ou Client Identifier d'un autre groupe. | Régénérez le secret partagé et vérifiez le Client Identifier. |
| **« Cette adresse ne répond pas comme fournisseur OpenID Connect »** | L'autorité n'est pas joignable depuis Internet, son certificat n'est pas public, ou le chemin diffère de /adfs. | Exposez https://<fs>/adfs/.well-known/openid-configuration avec un certificat public, et saisissez l'autorité sans chemin supplémentaire. |
| **La connexion de preuve rend « jeton sans email »** | La règle d'émission email manque sur la Web API, ou la portée allatclaims n'est pas accordée. | Ajoutez la règle LDAP E-Mail-Addresses → email et la portée allatclaims (section 3, étapes 04 et 05). |
| **La preuve réussit, mais la console d'administration demande encore une session renforcée** | La règle amr manque, ou la valeur multipleauthn n'est pas déclarée dans l'assistant, ou la stratégie n'exige pas le MFA. | Vérifiez la règle de la section 3, la déclaration de la section 4 et la stratégie de contrôle d'accès ; refaites la preuve. |
| **MSIS7012 : l'utilisateur est refusé par la stratégie** | La stratégie de contrôle d'accès exclut la personne. | Ajustez la stratégie de la Web API (section 4). |

## Liste de contrôle avant d'ouvrir le lien

7 POINTS

- [ ] Le groupe d'applications REVIEWIT TrustGate existe (Server application + Web API).
- [ ] Les deux adresses de retour de l'assistant sont dans la Server application, exactement.
- [ ] Le secret partagé est copié ; le Client Identifier est sous la main.
- [ ] La Web API autorise les portées openid, profile, email, allatclaims.
- [ ] Les règles d'émission email et amr sont en place sur la Web API.
- [ ] La stratégie de contrôle d'accès exige le MFA pour vos administrateurs REVIEWIT, au minimum.
- [ ] https://<fs>/adfs/.well-known/openid-configuration répond depuis Internet, avec un certificat public.

Ce guide est fourni aux clients REVIEWIT dans le cadre de l'ouverture de leur espace. Les chemins de menus sont ceux des consoles des éditeurs à la date de publication ; ils peuvent évoluer. En cas d'écart, le support REVIEWIT vous accompagne.