CONNECTER VOTRE ANNUAIRE

Microsoft Entra ID

Désignez votre locataire Entra ID comme annuaire de votre espace REVIEWIT, avec une authentification forte exécutoire, ciblée sur les seules consoles d'administration.

VERSION	DURÉE	DIFFUSION
2.0 · Octobre 2026	**Vingt minutes, en trois étapes**	**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 compte de votre locataire qui peut créer une inscription d'application et accorder le consentement administrateur (rôle Administrateur d'application ou Administrateur général), et, pour la section 4, qui peut créer une stratégie d'accès conditionnel.

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 Microsoft Entra ID

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

Microsoft Entra ID est pris en charge nativement, par le type « Microsoft Entra ID » de l'assistant. L'authentification forte y est exécutoire : TrustGate demande un contexte d'authentification, l'accès conditionnel l'impose, et le jeton en rapporte la preuve.

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 Microsoft Entra ID

Un administrateur de votre locataire crée, dans le centre d'administration Microsoft Entra, une inscription d'application dédiée à REVIEWIT TrustGate. Elle ne sert à rien d'autre, et rien d'autre ne la partage.

01 **Identité › Applications › Inscriptions d'applications › Nouvelle inscription**

Nom : REVIEWIT TrustGate. Types de comptes pris en charge : comptes de cet annuaire d'organisation uniquement (locataire unique).

02 **Plateforme Web, avec les deux adresses de retour**

Dans « URI de redirection », choisissez Web et collez la première adresse de la section 2. Après la création, ouvrez Authentification › Ajouter un URI et collez la seconde. Les deux doivent y figurer, exactement.

03 **Configuration du jeton › Ajouter une revendication facultative**

Type de jeton ID : cochez auth_time et email. Acceptez, si Entra le propose, l'ajout de l'autorisation Microsoft Graph email qui va avec.

04 **Autorisations d'API › Accorder un consentement d'administrateur**

Les autorisations déléguées Microsoft Graph openid, profile et email suffisent. Le consentement administrateur évite à chaque utilisateur une demande de consentement à sa première connexion.

05 **Certificats et secrets › Nouveau secret client**

Copiez la valeur immédiatement : elle n'est plus jamais affichée. Notez sa date d'expiration. Elle ne doit être saisie que dans l'assistant (section 5) ; ne la transmettez à personne. Vous pourrez remplacer ce secret par un certificat renouvelé par REVIEWIT après l'activation (section 7).

06 **Vue d'ensemble : notez trois identifiants**

ID d'application (client), ID de l'annuaire (locataire) et ID d'objet. Les deux premiers servent à l'assistant ; le troisième servira au passage au certificat.

CE QUE VOUS SAISIREZ DANS L'ASSISTANT

CHAMP DE L'ASSISTANT	VALEUR
Annuaire	Microsoft Entra ID
Nom affiché à vos utilisateurs	Le nom de votre organisation, tel que vos utilisateurs le reconnaissent — « Contoso », pas « Entra ».
Autorité OIDC	`https://login.microsoftonline.com/<ID de l'annuaire (locataire)>/v2.0`
Identifiant client	L'ID d'application (client) de l'inscription.
Secret client	La valeur du secret créé à l'étape 05.

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 **Protection › Accès conditionnel › Contextes d'authentification › Nouveau contexte**

Nom affiché REVIEWIT MFA, identifiant c1 (ou celui de votre choix — vous le reporterez dans l'assistant), coché Publier dans les applications.

02 **Accès conditionnel › Nouvelle stratégie**

Utilisateurs : tous, ou le groupe de vos administrateurs REVIEWIT. Ressources cibles › Contexte d'authentification › c1. Accorder › Exiger une authentification multifacteur — ou Exiger une force d'authentification (par exemple « MFA résistante au hameçonnage ») si vos administrateurs disposent de clés FIDO2 ou de Windows Hello Entreprise. Activez la stratégie.

03 **Rien d'autre ne change chez vous**

La stratégie ne se déclenche que lorsqu'une connexion demande le contexte c1, et seul REVIEWIT le demande, au moment d'entrer dans une console d'administration. Vos autres applications ne sont pas concernées.

DANS L'ASSISTANT — RÉGLAGES MFA

Contexte d'authentification (acr)
c1 — la valeur de l'étape 01. Entra rapporte dans la revendication acrs les contextes effectivement satisfaits ; TrustGate n'accorde la session renforcée que s'il y lit c1.

Valeurs amr attestant le MFA
Laissez vide. Le défaut (mfa, ngcmfa) couvre Entra.

Valeurs amr attestant la résistance au hameçonnage
Laissez vide, sauf si vous imposez une force d'authentification résistante au hameçonnage et souhaitez que REVIEWIT la distingue.

SANS ENTRA ID P1

Les contextes d'authentification exigent une licence Microsoft Entra ID P1 (ou P2). Sans elle, laissez le champ « Contexte d'authentification » vide : TrustGate demande alors le second facteur par la revendication amr, et le jeton le rapporte si votre locataire impose le MFA à l'utilisateur (paramètres de sécurité par défaut, MFA par utilisateur). Cette demande n'est pas exécutoire : un locataire sans politique MFA peut l'ignorer, et la session renforcée est alors refusée — jamais accordée 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**
Microsoft Entra ID pour un locataire Microsoft 365. Avec un autre type, la connexion de preuve échoue à son dernier pas.

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
`oid`	L'identifiant stable de la personne dans votre locataire. C'est lui, avec l'émetteur, qui lie l'identité à son compte REVIEWIT — jamais l'adresse e-mail.
`preferred_username, email`	L'adresse de connexion (UPN en priorité), en minuscules. 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.
Passer du secret au certificat	Sur la carte « Comment REVIEWIT prouve son identité à votre annuaire », saisissez l'ID d'objet de l'application et cliquez « Préparer le certificat ». Téléchargez la partie publique et chargez-la dans Certificats et secrets › Certificats › Charger un certificat. REVIEWIT l'adopte seul dans les dix minutes, puis le renouvelle avant son échéance, sans geste de votre part : vous pouvez alors supprimer le secret client. Un secret, lui, expire à date fixe — et ce jour-là plus personne ne se connecte.
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
AADSTS50011 : l'URI de redirection ne correspond pas	Une des deux adresses de retour manque ou diffère d'un caractère.	Recopiez les deux adresses depuis l'assistant, sur la plateforme Web de l'inscription.
AADSTS65001 : l'utilisateur ou l'administrateur n'a pas consenti	Le consentement administrateur n'a pas été accordé.	Autorisations d'API › Accorder un consentement d'administrateur, puis refaites la preuve.
« Cette adresse ne répond pas comme fournisseur OpenID Connect »	L'autorité est incomplète ou porte un chemin en trop.	Saisissez exactement https://login.microsoftonline.com/<ID de locataire>/v2.0.
« Votre annuaire refuse cet identifiant et ce secret »	Secret mal copié ou expiré, ou ID d'objet saisi à la place de l'ID d'application.	Créez un nouveau secret et saisissez l'ID d'application (client).
La preuve réussit, mais la console d'administration demande encore une session renforcée	Le contexte c1 n'est pas publié, la stratégie n'est pas active, ou l'identifiant saisi diffère.	Vérifiez le contexte et la stratégie (section 4) ; refaites la preuve après correction.
AADSTS50105 : l'utilisateur n'est pas affecté	L'inscription exige une affectation (« Affectation requise »).	Affectez le groupe de vos utilisateurs dans Applications d'entreprise › REVIEWIT TrustGate › Utilisateurs et groupes.

Liste de contrôle avant d'ouvrir le lien

7 POINTS

- [ ] L'inscription REVIEWIT TrustGate existe, en locataire unique, plateforme Web.
- [ ] Les deux adresses de retour de l'assistant y sont enregistrées, exactement.
- [ ] Les revendications facultatives auth_time et email sont ajoutées au jeton ID.
- [ ] Le consentement administrateur est accordé sur openid, profile, email.
- [ ] Le secret client est copié, et sa date d'expiration notée.
- [ ] Le contexte d'authentification c1 est publié et sa stratégie d'accès conditionnel est active (Entra ID P1).
- [ ] Vous avez sous la main l'ID d'application (client) et l'ID de l'annuaire (locataire).

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.