CONNECTER VOTRE ANNUAIRE

Google Workspace

Désignez Google Workspace comme annuaire de votre espace REVIEWIT, par OpenID Connect, avec une règle claire sur l'authentification forte.

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 super-administrateur Google Workspace (pour la validation en deux étapes, section 4) et un compte pouvant créer un client OAuth dans un projet Google Cloud de votre organisation.

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 Google Workspace

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

Google Workspace est pris en charge par le type « OpenID Connect » de l'assistant : Google est un fournisseur OpenID Connect standard, et son émetteur est https://accounts.google.com. Une limite documentée : Google n'atteste pas le second facteur dans ses jetons. La section 4 explique comment REVIEWIT en tient compte, et ce que vous attestez à sa place.

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 Google Workspace

Un administrateur crée, dans la console Google Cloud, un client OAuth dédié à REVIEWIT TrustGate, dans un projet appartenant à votre organisation Workspace. L'écran de consentement est de type Interne : seuls les comptes de votre domaine peuvent se connecter.

01 **Console Google Cloud › choisissez un projet de votre organisation**

Créez-en un au besoin (par exemple reviewit-trustgate). Il doit appartenir à votre organisation Workspace, pas à un compte personnel.

02 **API et services › Écran de consentement OAuth (Google Auth Platform › Audience)**

Type d'utilisateur Interne. Nom de l'application : REVIEWIT. Adresse d'assistance : celle de votre équipe. Aucune portée sensible n'est à déclarer : openid, email et profile ne demandent aucune validation Google.

03 **Identifiants › Créer des identifiants › ID client OAuth**

Type Application Web. Nom : REVIEWIT TrustGate.

04 **URI de redirection autorisés : les deux adresses de retour**

Ajoutez les deux adresses de la section 2, l'une après l'autre, exactement. Aucune « origine JavaScript autorisée » n'est nécessaire.

05 **Notez l'ID client et le secret client**

L'ID client se termine par .apps.googleusercontent.com. Le secret ne doit être saisi que dans l'assistant (section 5) ; ne le transmettez à personne.

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 « Google ».
Autorité OIDC	`https://accounts.google.com`
Identifiant client	L'ID client (…apps.googleusercontent.com).
Secret client	Le secret du client OAuth.
Mon annuaire impose la validation en deux étapes…	Cochée, après l'étape 02 de la 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 **Console d'administration Google › Sécurité › Authentification › Validation en deux étapes**

Cochez Autoriser les utilisateurs à activer la validation en deux étapes, puis Application : Activée, pour l'ensemble de l'organisation ou au minimum pour l'unité organisationnelle de vos administrateurs REVIEWIT. Laissez un délai d'inscription raisonnable avant l'application.

02 **Choisissez la méthode**

Toutes, ou Clés de sécurité uniquement si vos administrateurs disposent de clés FIDO2 ou de clés d'accès : c'est la seule voie vers une authentification résistante au hameçonnage chez Google.

03 **Dans l'assistant, cochez la confiance déclarée**

« Mon annuaire impose la validation en deux étapes sur chaque compte ; compter ses connexions comme multifacteur ». Vous engagez votre organisation par cette déclaration : REVIEWIT comptera chaque connexion venue de Google comme une authentification à plusieurs facteurs, et la piste d'audit l'enregistrera comme déclarée, non prouvée.

DANS L'ASSISTANT — RÉGLAGES MFA

Valeurs amr / contexte acr
Laissez vides. Google ne les émet pas ; les renseigner ne changerait rien.

Confiance déclarée
Cochée. Sans elle, toute session Google vaut un seul facteur, et les consoles d'administration restent fermées à vos administrateurs.

POURQUOI UNE DÉCLARATION, ET PAS UNE PREUVE

Le jeton d'identité de Google ne porte ni amr ni acr : il ne dit pas comment la personne s'est authentifiée. TrustGate ne pouvant rien vérifier, il ne suppose rien — c'est vous qui attestez que l'annuaire impose le second facteur à tous ses comptes. Cette confiance n'élève la session qu'au niveau MFA, jamais au niveau résistant au hameçonnage, et chaque session ainsi élevée garde la trace de son origine (« declared_mfa »).

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 Google Workspace — comme pour 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 Google. C'est lui, avec l'émetteur, qui lie l'identité à son compte REVIEWIT — jamais l'adresse e-mail.
`email`	L'adresse Workspace, 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.
Renouveler le secret client	Un secret Google n'expire pas de lui-même, mais vous pouvez le faire tourner. Créez le nouveau secret dans la console Google Cloud, déclarez l'annuaire à nouveau (même autorité, nouvelle référence de secret), prouvez-le, adoptez-le ; supprimez l'ancien secret chez Google 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
Erreur 400 : redirect_uri_mismatch	Une des deux adresses de retour manque ou diffère d'un caractère.	Recopiez les deux adresses depuis l'assistant dans « URI de redirection autorisés ».
Erreur 403 : org_internal	La personne n'appartient pas à votre organisation Workspace. C'est la protection attendue.	Connectez-vous avec un compte de votre domaine.
Erreur 401 : invalid_client	Secret mal copié, ou ID client d'un autre projet.	Vérifiez le couple ID client + secret du client Application Web créé à la section 3.
« Cette adresse ne répond pas comme fournisseur OpenID Connect »	L'autorité porte un chemin en trop.	Saisissez exactement https://accounts.google.com.
La preuve réussit, mais la console d'administration demande encore une session renforcée	La confiance déclarée n'est pas cochée.	Cochez-la à l'étape 1 de l'assistant (après avoir appliqué la validation en deux étapes), puis refaites la preuve.
Google demande à l'utilisateur d'activer la validation en deux étapes	La période d'inscription est écoulée et le compte n'est pas inscrit.	C'est votre politique qui s'applique ; la personne s'inscrit, puis se reconnecte.

Liste de contrôle avant d'ouvrir le lien

6 POINTS

- [ ] Le client OAuth REVIEWIT TrustGate (type Application Web) existe dans un projet de votre organisation.
- [ ] L'écran de consentement est de type Interne.
- [ ] Les deux adresses de retour de l'assistant sont dans « URI de redirection autorisés », exactement.
- [ ] L'ID client et le secret client sont copiés.
- [ ] La validation en deux étapes est appliquée à vos administrateurs REVIEWIT, au minimum.
- [ ] Vous savez que vous cocherez la confiance déclarée dans l'assistant.

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.