CONNECTER VOTRE ANNUAIRE

Okta

Désignez votre organisation Okta comme annuaire de votre espace REVIEWIT : OpenID Connect standard, sans agent, sans modification de schéma, avec une authentification forte prouvée.

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 compte Okta Super Administrator ou Application Administrator, et, pour la section 4, le droit de modifier les stratégies d'authentification.

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 Okta

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

Okta est pris en charge par le type « OpenID Connect » de l'assistant. L'authentification forte y est prouvée : Okta rapporte les méthodes employées dans amr et, sur demande, la classe satisfaite dans acr.

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 Okta

Un administrateur Okta crée une intégration d'application dédiée à REVIEWIT TrustGate : une application Web OpenID Connect, à laquelle sont affectés les utilisateurs qui accèdent à REVIEWIT.

01 **Admin Console › Applications › Applications › Create App Integration**

Sign-in method : OIDC – OpenID Connect. Application type : Web Application.

02 **Paramètres généraux**

App integration name : REVIEWIT TrustGate. Grant type : Authorization Code seulement (ni Refresh Token, ni Implicit). Client authentication : Client secret.

03 **Sign-in redirect URIs : les deux adresses de retour**

Collez les deux adresses de la section 2, l'une après l'autre, exactement. Laissez « Sign-out redirect URIs » vide ; REVIEWIT gère sa propre déconnexion.

04 **Assignments**

Limit access to selected groups : les groupes de vos utilisateurs REVIEWIT — ou Allow everyone in your organization. Une personne non affectée est refusée par Okta avant même d'atteindre REVIEWIT.

05 **Notez le Client ID et le Client secret**

Le secret ne doit être saisi que dans l'assistant (section 5) ; ne le transmettez à personne.

06 **Choisissez l'autorité**

Le serveur d'autorisation de l'organisation convient : https://<votre-org>.okta.com. Un serveur d'autorisation personnalisé (https://<votre-org>.okta.com/oauth2/default) convient aussi, si ses règles d'accès laissent passer l'application REVIEWIT. L'autorité saisie doit être l'émetteur exact que publie /.well-known/openid-configuration.

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 « Okta ».
Autorité OIDC	`https://<votre-org>.okta.com (ou l'émetteur de votre serveur d'autorisation personnalisé)`
Identifiant client	Le Client ID de l'intégration.
Secret client	Le Client secret de l'intégration.
Réglages MFA	Voir 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 **Security › Authentication policies**

Créez une stratégie REVIEWIT (ou réutilisez votre stratégie MFA) : Password + Another factor, ou Any 2 factor types. Pour une authentification résistante au hameçonnage, exigez Possession › Phishing resistant (FIDO2 / WebAuthn, Okta FastPass).

02 **Appliquez-la à l'application**

Applications › REVIEWIT TrustGate › Sign On › Authentication policy : sélectionnez la stratégie. Vos utilisateurs doivent être inscrits à au moins un second facteur (Okta Verify, clé FIDO2).

03 **Laissez TrustGate demander l'élévation**

Au moment d'entrer dans une console d'administration, TrustGate envoie acr_values=urn:okta:loa:2fa:any : Okta exige alors le second facteur pour cette connexion-là, et rapporte acr dans le jeton. Sans ce réglage, seule la stratégie de l'étape 02 s'applique, à chaque connexion.

DANS L'ASSISTANT — RÉGLAGES MFA

Contexte d'authentification (acr)
urn:okta:loa:2fa:any. TrustGate le demande à l'élévation et n'accorde la session renforcée que s'il le relit dans acr.

Valeurs amr attestant le MFA
Laissez vide — Okta émet mfa quand deux facteurs ont été présentés, et c'est le défaut. Ajoutez otp, sms, swk, hwk si vous voulez compter chaque méthode même hors mfa.

Valeurs amr attestant la résistance au hameçonnage
hwk (clé matérielle FIDO2 / WebAuthn), si vous distinguez ce niveau.

SERVEUR D'AUTORISATION PERSONNALISÉ

Sur un serveur d'autorisation personnalisé, la revendication email n'est présente que si la portée email est autorisée par une règle d'accès, et amr n'y figure que pour les jetons d'identité. Si la connexion de preuve échoue sur « jeton sans email », vérifiez les règles d'accès du serveur — ou utilisez le serveur de l'organisation.

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 Okta — comme pour Google Workspace, 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 Okta. C'est lui, avec l'émetteur, qui lie l'identité à son compte REVIEWIT — jamais l'adresse e-mail.
`email, preferred_username`	L'adresse de connexion, 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.
Faire tourner le secret client	Okta permet de garder deux secrets actifs. Générez le nouveau dans l'intégration, déclarez l'annuaire à nouveau (même autorité, nouvelle référence de secret), prouvez-le, adoptez-le ; désactivez l'ancien secret chez Okta 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
400 Bad Request : redirect_uri non enregistré	Une des deux adresses de retour manque ou diffère d'un caractère.	Recopiez les deux adresses depuis l'assistant dans « Sign-in redirect URIs ».
User is not assigned to the client application	La personne n'est pas affectée à l'intégration.	Applications › REVIEWIT TrustGate › Assignments : ajoutez la personne ou son groupe.
401 : invalid_client	Secret mal copié, ou Client ID d'une autre intégration.	Vérifiez le couple Client ID + Client secret de l'intégration créée à la section 3.
« Cette adresse ne répond pas comme fournisseur OpenID Connect »	L'autorité ne correspond pas à l'émetteur publié.	Ouvrez https://<votre-org>.okta.com/.well-known/openid-configuration et saisissez la valeur exacte de issuer.
La preuve réussit, mais la console d'administration demande encore une session renforcée	acr ou amr absents ou sous un autre vocabulaire.	Renseignez urn:okta:loa:2fa:any en contexte (section 4) ; vérifiez la stratégie d'authentification ; refaites la preuve.
La connexion de preuve rend « jeton sans email »	Serveur d'autorisation personnalisé sans règle d'accès sur la portée email.	Autorisez les portées openid profile email dans une règle d'accès, ou utilisez le serveur de l'organisation.

Liste de contrôle avant d'ouvrir le lien

6 POINTS

- [ ] L'intégration REVIEWIT TrustGate (OIDC, Web Application, Authorization Code) existe.
- [ ] Les deux adresses de retour de l'assistant sont dans « Sign-in redirect URIs », exactement.
- [ ] Les utilisateurs (ou groupes) qui accèdent à REVIEWIT sont affectés à l'intégration.
- [ ] Le Client ID et le Client secret sont copiés.
- [ ] Une stratégie d'authentification à deux facteurs est appliquée à l'intégration.
- [ ] L'émetteur exact du serveur d'autorisation est sous la main.

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.