CONNECTER VOTRE ANNUAIRE

PingOne

Désignez votre environnement PingOne (Ping Identity) comme annuaire de votre espace REVIEWIT : OpenID Connect standard, second facteur PingID ou PingOne MFA, prouvé par la politique d'authentification que le jeton rapporte.

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 PingOne Environment Admin (ou Organization Admin) sur l'environnement de vos utilisateurs, et, pour la section 4, le droit de modifier les politiques d'authentification et les politiques MFA.

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 PingOne

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

PingOne est pris en charge par le type « OpenID Connect » de l'assistant. L'authentification forte y est prouvée par acr : PingOne rapporte dans le jeton le nom de la politique d'authentification accomplie, et TrustGate la demande par acr_values. La revendication amr de PingOne n'annonce que le mot de passe (pwd) : elle ne suffit pas, et c'est la politique qui fait foi.

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 PingOne

Un administrateur PingOne crée, dans l'environnement de vos utilisateurs, une application dédiée à REVIEWIT TrustGate : une application OIDC Web App, à laquelle sont rattachées vos politiques d'authentification.

01 **Applications › Applications › +**

Application Name : REVIEWIT TrustGate. Application Type : OIDC Web App. Enregistrez.

02 **Configuration › modifier : le protocole**

Response Type : Code. Grant Type : Authorization Code seulement (ni Implicit, ni Refresh Token). Token Endpoint Authentication Method : Client Secret Post (Client Secret Basic convient aussi). PKCE Enforcement : Optional.

03 **Redirect URIs : les deux adresses de retour**

Collez les deux adresses de la section 2, l'une après l'autre, exactement. Laissez « Signoff URLs » vide ; REVIEWIT gère sa propre déconnexion.

04 **Resources : les portées**

Onglet Resources › modifier : cochez openid, profile et email. Rien d'autre : TrustGate ne lit pas vos ressources.

05 **Activez l'application**

Le commutateur en haut du panneau de l'application doit être bleu. Si une population ou un groupe doit seul accéder à REVIEWIT, réglez-le dans vos politiques (section 4) : PingOne refuse alors les autres avant même d'atteindre REVIEWIT.

06 **Notez le Client ID et le Client Secret, puis l'émetteur**

Onglet Configuration : Environment ID, Client ID, Client Secret (« Generate New Secret » si besoin). L'autorité est https://auth.pingone.<région>/<Environment ID>/as — .eu, .com, .ca, .asia ou .com.au selon la région de votre environnement, ou votre domaine personnalisé suivi de /as. Vérifiez-la dans /.well-known/openid-configuration : c'est l'issuer exact qu'il faut saisir. 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 « PingOne ».
Autorité OIDC	`https://auth.pingone.<région>/<Environment ID>/as (ou https://<votre domaine>/as)`
Identifiant client	Le Client ID de l'application.
Secret client	Le Client Secret de l'application.
Contexte d'authentification (acr)	Le nom de votre politique à second facteur — Multi_Factor par défaut (section 4).

PINGFEDERATE, SUR SITE

Si vos utilisateurs s'authentifient sur PingFederate plutôt que sur PingOne, le parcours est le même : un client OAuth (Applications › OAuth › Clients ; Authorization Code, Client Secret, les deux adresses de retour, portées openid profile email, politique OpenID Connect qui émet sub, email et amr). L'autorité est l'adresse de base du serveur (https://sso.<votre-domaine>), qui publie /.well-known/openid-configuration et doit être jointe depuis Internet avec un certificat public. Le second facteur PingID est rapporté par l'adaptateur PingID dans amr, ou dans acr par un sélecteur de contexte demandé (Requested AuthN Context Selector) : déclarez dans l'assistant la valeur que votre politique émet.

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 **Authentication › MFA : une politique MFA**

Vérifiez la politique MFA de l'environnement (ou créez-en une) : les méthodes autorisées (application PingID ou PingOne MFA, FIDO2, TOTP, SMS) et l'inscription de vos administrateurs. Elle ne s'applique qu'à travers une étape MFA d'une politique d'authentification.

02 **Authentication › Authentication : une politique à second facteur**

Créez une politique Multi_Factor (le nom existe déjà dans beaucoup d'environnements) avec deux étapes : Login (mot de passe), puis Multi-Factor Authentication — ou PingID Authentication pour un environnement Workforce — liée à la politique MFA de l'étape 01. Dans « None or incompatible methods », choisissez Block : une personne sans second facteur inscrit est refusée, jamais admise sur parole.

03 **Rattachez les politiques à l'application**

Applications › REVIEWIT TrustGate › onglet Policies › modifier : sélectionnez votre politique à un facteur (Single_Factor) et Multi_Factor. La première de la liste s'applique par défaut ; TrustGate demande Multi_Factor par acr_values au moment d'entrer dans une console d'administration, et PingOne la rapporte dans acr. Une politique non rattachée à l'application ne peut pas être demandée.

DANS L'ASSISTANT — RÉGLAGES MFA

Contexte d'authentification (acr)
Multi_Factor — ou le nom exact de votre politique à second facteur. TrustGate le demande à l'élévation et n'accorde la session renforcée que s'il relit ce nom dans acr. Sans cette ligne, chaque entrée en console d'administration est refusée.

Valeurs amr attestant le MFA
Laissez vide. PingOne n'annonce que pwd dans amr ; la preuve vient de acr.

Valeurs amr attestant la résistance au hameçonnage
Laissez vide. PingOne ne distingue pas la méthode dans le jeton.

POLITIQUES DAVINCI

Si votre environnement utilise des politiques DaVinci au lieu des politiques PingOne, le contexte à déclarer est l'identifiant de la flow policy (32 caractères hexadécimaux), pas son nom, et acr le rapporte tel quel. Une application ne peut rattacher qu'un seul type de politiques.

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 PingOne — comme pour Google Workspace, Okta 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 PingOne (son identifiant d'utilisateur). 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	Dans Applications › REVIEWIT TrustGate › Configuration, cliquez Generate New Secret ; PingOne garde l'ancien secret valide le temps que vous choisissez. Déclarez l'annuaire à nouveau (même autorité, nouvelle référence de secret), prouvez-le, adoptez-le ; révoquez l'ancien secret ensuite (« Revoke Previous Client Secret »). 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
Redirect URI mismatch	Une des deux adresses de retour manque ou diffère d'un caractère.	Recopiez les deux adresses depuis l'assistant dans « Redirect URIs ».
invalid_client : « Votre annuaire refuse cet identifiant et ce secret »	Secret mal copié ou révoqué, ou méthode d'authentification du point de jeton réglée sur None ou Private Key JWT.	Vérifiez le couple Client ID + Client Secret, et réglez « Token Endpoint Authentication Method » sur Client Secret Post.
« Cette adresse ne répond pas comme fournisseur OpenID Connect »	L'autorité ne correspond pas à l'émetteur publié : mauvaise région, /as manquant, ou Environment ID d'un autre environnement.	Ouvrez https://auth.pingone.<région>/<Environment ID>/as/.well-known/openid-configuration et saisissez la valeur exacte de issuer.
PingOne refuse la connexion avant d'atteindre REVIEWIT	L'application n'est pas activée, ou la personne est refusée par la politique (population, groupe, second facteur non inscrit).	Activez l'application (section 3, étape 05) ; vérifiez la politique et l'inscription MFA de la personne.
La preuve réussit, mais la console d'administration demande encore une session renforcée	Le contexte n'est pas déclaré, son nom diffère de celui de la politique, ou la politique n'est pas rattachée à l'application.	Déclarez le nom exact (section 4) ; rattachez la politique dans l'onglet Policies ; refaites la preuve.
La connexion de preuve rend « jeton sans email »	La portée email n'est pas cochée dans Resources, ou la personne n'a pas d'adresse e-mail dans PingOne.	Cochez openid, profile et email (section 3, étape 04) ; renseignez l'adresse de la personne.

Liste de contrôle avant d'ouvrir le lien

6 POINTS

- [ ] L'application REVIEWIT TrustGate (OIDC Web App, Authorization Code, Client Secret Post) existe et est activée.
- [ ] Les deux adresses de retour de l'assistant sont dans « Redirect URIs », exactement.
- [ ] Les portées openid, profile, email sont cochées dans Resources.
- [ ] Le Client ID et le Client Secret sont copiés ; l'Environment ID et la région sont sous la main.
- [ ] Une politique d'authentification à second facteur (Multi_Factor) existe, bloque sans méthode inscrite, et est rattachée à l'application.
- [ ] L'émetteur exact (…/as) publié par /.well-known/openid-configuration 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.