CONNECTER VOTRE SOLUTION

Microsoft 365 et Azure

Raccordez votre locataire Microsoft Entra ID à REVIEWIT, pour Microsoft 365 comme pour Azure : une inscription d'application dédiée, des permissions d'application en lecture seule, un secret ou un certificat.

VERSION
1.0 · Novembre 2026

DURÉE
Quarante-cinq minutes, en quatre étapes

DIFFUSION
Confidentiel · Clients REVIEWIT

CE QU'IL VOUS FAUT

01 **Un administrateur général ou un administrateur d'application cloud** du locataire Entra ID, pouvant créer une inscription d'application et **accorder le consentement d'administrateur** ; pour Azure, un **propriétaire** des abonnements à revoir.

02 **Un compte REVIEWIT** avec le rôle d'administrateur de la souscription, pour ouvrir le Subscription Manager.

03 **Le temps indiqué**, dans l'ordre de ce guide : d'abord l'identifiant chez Microsoft 365 et Azure, puis l'assistant REVIEWIT, en quatre étapes.

L'ASSISTANT, EN QUATRE ÉTAPES

ÉTAPE 1	ÉTAPE 2	ÉTAPE 3	ÉTAPE 4
Solution	**Préparer**	**Identifiant**	**Vérification**
Choisissez Microsoft 365 et Azure dans le catalogue de votre souscription.	Cochez ce que REVIEWIT doit collecter ; l'assistant en déduit les droits à accorder.	Saisissez ce que Microsoft 365 et Azure vous a remis ; REVIEWIT le vérifie avant d'enregistrer.	Un verdict par ressource : ce qui est couvert, ce qui reste à accorder.

DANS CE GUIDE

1 Comment REVIEWIT se connecte à Microsoft 365 et Azure

2 Ce que REVIEWIT lira, et les droits que cela demande

3 Créer l'identifiant chez Microsoft 365 et Azure

4 Ce que vous saisirez dans l'assistant

5 L'assistant de connexion, en quatre étapes

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

7 Après la connexion

8 Dépannage et liste de contrôle

01 Comment REVIEWIT se connecte à Microsoft 365 et Azure

REVIEWIT revoit des **accès** : qui peut atteindre quoi, et si c'est encore justifié. Pour cela il lit, en **lecture seule**, l'inventaire de vos ressources et de leurs droits chez Microsoft 365 et Azure, depuis votre région d'hébergement. Il n'écrit jamais chez vous, ne lit aucun contenu, et conserve l'identifiant que vous lui remettez dans un coffre dont seul le collecteur ouvre la porte.

CHEZ VOUS
Microsoft 365 et Azure
Vous créez un identifiant technique, limité aux droits de lecture que l'assistant vous indique.

→

VOTRE RÉGION
Collecteur REVIEWIT
Vérifie l'identifiant par un appel réel, puis lit l'inventaire aux fréquences de vos plans de collecte.

→

VOS CONSOLES
Workspace Manager
Campagnes, revues et rapports : jamais un appel direct à Microsoft 365 et Azure.

PRINCIPE DIRECTEUR

REVIEWIT ne croit que ce qu'il a constaté par appel : un droit accordé mais non vérifié reste « non vérifié » jusqu'à la passe de santé suivante. Ce qu'une connexion ne peut pas collecter se dit **ressource par ressource** ; une ressource non collectable reste importable sous forme de rapport.

PRISE EN CHARGE

Microsoft 365 et Azure d'un même locataire Entra ID : une connexion par solution, qui peuvent partager la même inscription d'application. Azure lit les abonnements où le rôle **Lecteur** est accordé à l'application ; Exchange et Power BI exigent chacun un geste d'administration propre (section 2).

02 Ce que REVIEWIT lira, et les droits que cela demande

L'assistant calcule la liste exacte des droits à partir des ressources que vous cochez à l'étape **Préparer**, et vous la remet prête à copier (« Copier le plan »). Le tableau ci-dessous donne les droits des ressources les plus souvent retenues ; votre plan peut en comporter moins.

DROIT OU GESTE	RESSOURCES QU'IL OUVRE
`Directory.Read.All`	Utilisateurs, groupes, rôles, sites SharePoint, équipes, canaux, communautés : la base de tout
`Sites.Read.All` · `Sites.FullControl.All`	Sites SharePoint et OneDrive, leurs permissions et leurs liens de partage (FullControl n'est demandé que pour lire les attributions de rôles des sites)
`Reports.Read.All`	Rapports d'usage : dernière activité des sites, OneDrive, équipes, communautés et boîtes partagées
`ReportSettings.Read.All (facultative)`	Lire le réglage de masquage des rapports d'usage : la collecte dit s'il cache les noms. Sans elle, rien n'est bloqué
`Channel.ReadBasic.All` · `ChannelMember.Read.All`	Canaux Teams et leurs membres
`Community.Read.All`	Communautés Viva Engage
`Exchange.ManageAsApp (Office 365 Exchange Online)`	Boîtes partagées et dossiers publics, avec le geste Exchange ci-dessous
`Global Reader (rôle d'annuaire)`	Catalogues de packages d'accès, inscriptions d'applications (Azure)

DROIT OU GESTE	RESSOURCES QU'IL OUVRE
Accorder le consentement d'administrateur	Toutes les permissions d'application ci-dessus : sans lui, chaque appel rend 403.
Attribuer un rôle d'administration Exchange à l'application	Boîtes partagées, dossiers publics — rôle **Global Reader** ou « View-Only Organization Management » sur le principal de service.
Ouvrir l'API d'administration Power BI en lecture seule à un groupe contenant l'application	Espaces de travail Power BI — Portail d'administration › Paramètres du locataire › « Autoriser les principaux de service à utiliser les API d'administration en lecture seule ».
Afficher les vrais noms dans les rapports d'usage	Centre d'administration Microsoft 365 › Paramètres › Paramètres de l'organisation › Services › Rapports : décochez « Afficher des noms d'utilisateur, de groupe et de site masqués ». Tant que la case est cochée, aucune date d'activité n'est posée.
Attribuer le rôle Lecteur sur au moins un abonnement Azure	Attributions de rôles, rôles personnalisés, machines virtuelles, App Service, disques, adresses IP, comptes de stockage, étendues et ressources.

03 Créer l'identifiant chez Microsoft 365 et Azure

Un administrateur du locataire crée, dans le centre d'administration Microsoft Entra, **une inscription d'application dédiée à REVIEWIT**, lui accorde des **permissions d'application** (pas déléguées) en lecture, consent pour l'organisation, puis lui remet un secret ou un certificat. Les gestes Exchange, Power BI et Azure complètent le plan selon les ressources retenues.

01 **Dans `entra.microsoft.com`, ouvrez Identité › Applications › Inscriptions d'applications › Nouvelle inscription**

Nom « REVIEWIT Collector », comptes **de cet annuaire d'organisation uniquement**, aucune URI de redirection : l'application n'ouvre aucune session.

02 **Relevez l'ID de l'application (client) et l'ID de l'annuaire (locataire) sur la page Vue d'ensemble**

Deux GUID : ce sont les deux premiers champs de l'assistant.

03 **API autorisées › Ajouter une autorisation › Microsoft Graph › Autorisations d'application**

Cochez les permissions du plan copié depuis l'assistant (Directory.Read.All, Sites.Read.All, Reports.Read.All, Channel.ReadBasic.All, ChannelMember.Read.All, Community.Read.All, ReportSettings.Read.All, facultative, et Sites.FullControl.All si vous revoyez les permissions SharePoint). Ajoutez **Office 365 Exchange Online › Exchange.ManageAsApp** pour les boîtes partagées et dossiers publics.

04 **Cliquez Accorder un consentement d'administrateur pour <votre organisation>**

Chaque ligne passe à « Accordé ». Une permission non consentie rend 403 à la collecte : l'assistant la nommera.

05 **Certificats et secrets : créez un secret client (durée 12 à 24 mois) et relevez sa valeur et sa date d'expiration**

La valeur ne se réaffiche jamais dans Entra. Ou bien chargez le **certificat public (.cer)** de votre paire de clés : le `.pfx` ira dans REVIEWIT.

06 **Exchange, si vous revoyez les boîtes partagées ou les dossiers publics**

Identité › Rôles et administrateurs › Global Reader (ou « View-Only Organization Management » dans l'EAC) › Ajouter une attribution › choisissez l'application « REVIEWIT Collector ».

07 **Power BI, si vous revoyez ses espaces de travail**

Créez un groupe de sécurité contenant l'application ; dans le **portail d'administration Power BI › Paramètres du locataire**, activez « Autoriser les principaux de service à utiliser les API d'administration Power BI en lecture seule » pour ce groupe.

08 **Azure, pour la solution Microsoft AZURE**

Sur chaque **abonnement** à revoir : **Contrôle d'accès (IAM)** › **Ajouter une attribution de rôle** › **Lecteur** › l'application « REVIEWIT Collector ». Le rôle d'annuaire **Global Reader** couvre les catalogues et les inscriptions d'applications.

UNE INSCRIPTION, DEUX CONNEXIONS

Microsoft 365 et Microsoft AZURE sont deux solutions dans REVIEWIT, chacune avec sa connexion et son plan de droits. Elles peuvent partager la même inscription d'application et le même secret : le plan de l'une s'ajoute à celui de l'autre dans Entra.

04 Ce que vous saisirez dans l'assistant

L'étape **Identifiant** n'affiche que les champs que Microsoft 365 et Azure déclare à REVIEWIT. Le nom de la connexion est celui que vous lirez dans les tableaux et les alertes.

CHAMP DE L'ASSISTANT	VALEUR
Nom de la connexion	Libre — par exemple « Microsoft 365 · <votre locataire> ».
Méthode d'authentification	**Secret client** ou **Certificat** : une méthode par identifiant, jamais les deux.
Tenant ID	L'ID de l'annuaire (locataire) relevé à l'étape 2 — l'identifiant externe de la connexion.
Application (client) ID	L'ID de l'application relevé à l'étape 2.
Client secret · Expires on	La valeur du secret, saisie une fois, et sa date d'expiration : Entra ne la rend pas à la vérification, relevez-la dans le portail. REVIEWIT vous préviendra avant l'échéance.
Certificate (.pfx) · Certificate password	La **paire de clés**, pas le certificat public : le `.cer` est dans Entra, le `.pfx` vient ici. Mot de passe vide si le fichier n'en porte pas.

LE SECRET NE REVIENT JAMAIS À L'ÉCRAN

Saisi une fois pour la vérification, il est rangé au coffre et désigné par référence. Pour en changer : « Ajouter un identifiant », jamais une réécriture.

05 L'assistant de connexion, en quatre étapes

Dans le Subscription Manager, ouvrez **Sources de données** › **Connexions**, puis **Connecter une solution** (ou **Connecter une instance** sur la tuile de la solution si elle est déjà présente). Rien n'est enregistré avant la réponse de Microsoft 365 et Azure.

ÉTAPE 1 Solution

Le catalogue ne liste que ce qui n'est pas encore connecté. Une solution « sonde disponible » se vérifie par un appel réel ; une solution « déclarable » s'enregistre sur votre parole, au niveau que vous choisissez.

ÉTAPE 2 Préparer

Cochez les ressources à collecter : la liste des droits à accorder suit. Copiez le plan, accordez-le chez Microsoft 365 et Azure, puis revenez. L'assistant n'applique jamais ce plan lui-même.

ÉTAPE 3 Identifiant

Nommez la connexion et saisissez les champs. **Vérifier la connexion** appelle Microsoft 365 et Azure ; **Enregistrer sans vérifier** garde la connexion inactive, à vérifier plus tard.

Microsoft saisit son identité (le Tenant ID) : « Enregistrer sans vérifier » est ouvert dès que les champs non secrets sont remplis ; la vérification demande un jeton à Entra et lit le locataire.

ÉTAPE 4 Vérification

Microsoft 365 et Azure a répondu : l'assistant affiche l'identité lue et, ressource par ressource, un verdict. **Enregistrer et activer** met la connexion en service ; **Enregistrer inactive** la garde pour plus tard.

Le verdict par ressource dit exactement quelle permission ou quel geste manque : Graph, Exchange, Power BI ou Azure. Accordez, puis « Vérifier les droits » : rien n'est à ressaisir.

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

REÇU DE MICROSOFT 365 ET AZURE	USAGE CHEZ REVIEWIT
`Tenant ID · nom du locataire`	L'identité de la connexion et son nom d'affichage.
`Microsoft Graph`	Utilisateurs, groupes, rôles, sites, équipes, canaux, communautés, applications : les objets, leurs propriétaires, leurs membres et leurs permissions — jamais leur contenu.
`Rapports d'usage`	La dernière activité des sites, OneDrive, équipes et boîtes : une date par objet, jamais un document.
`Journal d'activité Power BI`	Le dernier geste d'une personne sur chaque espace de travail, sur les 28 jours que Power BI garde : une date, jamais un rapport ni une requête.
`Exchange Online (cmdlets Get-*)`	Boîtes partagées, dossiers publics, délégations : des listes, jamais un courriel.
`Azure Resource Manager (lecture)`	Abonnements, groupes de ressources, ressources et attributions de rôles — jamais une clé, un secret ou une donnée stockée.
`Permissions « Tout le monde » · liens « Personnes de votre organisation »`	Le signal **Partage trop large** : audience, groupes larges, liens d'organisation comptés et datés.

JAMAIS REÇU, JAMAIS DEMANDÉ

Aucun mot de passe d'utilisateur
L'identifiant est technique, créé pour REVIEWIT ; aucun compte de personne n'est utilisé.

Aucun contenu
Ni message, ni fichier, ni courriel : REVIEWIT lit des listes d'objets et de droits, jamais ce qu'ils contiennent.

Aucune écriture
Les droits demandés sont en lecture ; la remédiation, quand elle existe, est un module à part, activé séparément.

Aucun secret réaffiché
Le secret est saisi une fois, rangé au coffre et désigné par référence ; aucun écran ni journal ne le montre à nouveau.

07 Après la connexion

La connexion se gère depuis **Sources de données** › **Connexions**. Une passe de santé rejoue la vérification **toutes les 24 heures** ; « Vérifier toutes les connexions » la relance à la demande. Chaque tuile dit combien de ressources sont prêtes, à configurer ou non vérifiées.

Un droit manque	La ressource reste « non vérifiée » et l'assistant dit lequel. Accordez-le chez Microsoft 365 et Azure, puis « Vérifier les droits ».
Renouveler le secret	Créez un **nouveau secret** dans Entra (Certificats et secrets), relevez sa date d'expiration, saisissez-le dans « Connexions › Ajouter un identifiant » avec la date, vérifiez, puis supprimez l'ancien secret. Pour ne plus renouveler : passez au **certificat** — le `.cer` dans Entra, le `.pfx` dans REVIEWIT ; la politique de certains locataires l'impose.
Une ressource non collectable	Importez son rapport depuis **Sources de données** › **Collecter** › **Choisir un rapport** : le contrat CSV exact se télécharge dans le tiroir.
Déconnecter	Désactivez la connexion ; révoquez ensuite l'identifiant chez Microsoft 365 et Azure. Les plans de collecte qui s'appuyaient dessus s'arrêtent.

08 Dépannage

CE QUE VOUS VOYEZ	CAUSE	CE QU'IL FAUT FAIRE
`AADSTS7000215` « **Invalid client secret** »	Secret mal copié, ou copie de l'identifiant du secret au lieu de sa valeur.	Créez un nouveau secret et copiez sa **valeur** au moment de la saisie.
`AADSTS700016` « **Application not found in the directory** »	Le Tenant ID ou l'ID d'application est celui d'un autre locataire.	Relevez les deux GUID sur la page Vue d'ensemble de l'inscription, dans le bon locataire.
`AADSTS7000222` « **The provided client secret keys are expired** »	Le secret est arrivé à échéance.	Nouveau secret dans Entra, « Ajouter un identifiant » dans REVIEWIT avec sa date.
Une ressource rend 403 `Authorization_RequestDenied`	Permission d'application absente ou non consentie.	Ajoutez-la, accordez le consentement d'administrateur, puis « Vérifier les droits ».
Boîtes partagées ou dossiers publics « non vérifiés »	Exchange.ManageAsApp consentie mais aucun rôle d'administration Exchange attribué à l'application.	Attribuez Global Reader (ou View-Only Organization Management) à l'application.
Espaces Power BI « non vérifiés »	L'API d'administration en lecture seule n'est pas ouverte au groupe de l'application.	Paramètres du locataire Power BI : activez l'option pour un groupe de sécurité contenant l'application.
Avis « le tenant masque les noms dans les rapports d'usage »	Le réglage de masquage est actif : les rapports remplacent les noms par des empreintes et rien ne s'apparie.	Décochez la case dans le centre d'administration Microsoft 365 (Paramètres de l'organisation › Services › Rapports) ; la collecte suivante date les objets.
Avis « réglage de masquage des rapports illisible »	ReportSettings.Read.All n'est pas consentie.	Ajoutez-la et accordez le consentement. Elle est facultative : sans elle, la collecte continue.
Azure : « aucun abonnement » ou ressources absentes	Le rôle Lecteur n'est pas attribué sur l'abonnement, ou l'est sur un seul groupe de ressources.	Attribuez **Lecteur** au niveau de chaque abonnement à revoir.

LISTE DE CONTRÔLE AVANT D'OUVRIR L'ASSISTANT

6 points

- [ ] Je peux créer une inscription d'application et accorder le consentement d'administrateur dans le locataire.
- [ ] L'inscription « REVIEWIT Collector » existe : comptes de cet annuaire uniquement, aucune redirection.
- [ ] Les permissions **d'application** du plan sont ajoutées et **consenties** pour l'organisation.
- [ ] Je dispose d'un secret (valeur et date d'expiration) ou d'une paire de clés `.pfx` dont le `.cer` est chargé dans Entra.
- [ ] Exchange, Power BI et Azure : les gestes correspondant aux ressources retenues sont faits.
- [ ] J'ai relevé le Tenant ID et l'Application (client) ID, et j'ouvre le Subscription Manager en administrateur de la souscription.

Ce guide est fourni aux clients REVIEWIT pour raccorder leurs solutions. Les chemins de menus sont ceux des consoles des éditeurs à la date de publication ; ils peuvent changer. En cas d'écart, l'assistant REVIEWIT fait foi : il affiche le plan exact calculé pour votre souscription.