CONNECTER VOTRE SOLUTION

Google Workspace

Raccordez votre organisation Google Workspace à REVIEWIT : un compte de service Google Cloud, délégué à l'échelle du domaine, agissant au nom d'un administrateur, en lecture seule.

VERSION
1.0 · Novembre 2026

DURÉE
Quarante minutes, en quatre étapes

DIFFUSION
Confidentiel · Clients REVIEWIT

CE QU'IL VOUS FAUT

01 **Un super-administrateur Google Workspace** (console `admin.google.com`) et un **propriétaire d'un projet Google Cloud** — souvent la même personne.

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 Google Workspace, 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 Google Workspace dans le catalogue de votre souscription.	Cochez ce que REVIEWIT doit collecter ; l'assistant en déduit les droits à accorder.	Saisissez ce que Google Workspace 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 Google Workspace
2 Ce que REVIEWIT lira, et les droits que cela demande
3 Créer l'identifiant chez Google Workspace
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 Google Workspace

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 Google Workspace, 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
Google Workspace
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 Google Workspace.

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

Toutes les éditions Google Workspace. Les portées d'administration et de rapports exigent un **super-administrateur** à usurper ; Google Chat, Keep et les rapports Marketplace demandent en plus que ces services soient activés dans votre organisation.

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
`admin.directory.user.readonly` · `admin.directory.orgunit.readonly`	Utilisateurs, unités organisationnelles, invités ; base de Drive, Gmail, Calendar, Sites, Keep
`admin.directory.group.readonly` · `apps.groups.settings`	Groupes Google, membres et paramètres des groupes
`drive.readonly`	Google Drive, Drives partagés et leurs membres, liens partagés, Sites, déploiements Apps Script
`calendar.readonly` · `calendar.acls.readonly` · `admin.directory.resource.calendar.readonly`	Agendas, partages d'agenda, ressources (salles)
`gmail.settings.basic`	Délégués, règles de transfert, adresses d'envoi des boîtes
`chat.admin.spaces.readonly` · `chat.admin.memberships.readonly`	Espaces Google Chat et leurs membres
`admin.directory.rolemanagement.readonly`	Rôles privilégiés et attributions de rôles
`admin.directory.user.security` · `admin.reports.audit.readonly`	Autorisations OAuth accordées, applications Marketplace
`cloud-identity.userinvitations.readonly` · `admin.directory.device.*.readonly`	Invitations en attente, appareils Chrome et mobiles
`script.projects.readonly` · `script.deployments.readonly` · `keep.readonly`	Projets et déploiements Apps Script, Google Keep

03 Créer l'identifiant chez Google Workspace

Un administrateur crée, dans la console Google Cloud, **un compte de service dédié à REVIEWIT**, puis l'autorise dans la console d'administration Google Workspace à agir au nom d'un administrateur, pour les seules portées de lecture du plan. Aucun utilisateur ne se connecte ; aucun mot de passe n'est partagé.

01 **Dans `console.cloud.google.com`, créez (ou choisissez) un projet dédié, par exemple « REVIEWIT Collector »**

Un projet à part isole la clé et ses journaux ; il n'a besoin d'aucune facturation.

02 **Activez les API du plan dans API et services › Bibliothèque**

Admin SDK API, Google Drive API, Google Calendar API, Gmail API, Groups Settings API, Google Chat API, Google Keep API, Apps Script API, Cloud Identity API. Une API non activée rend une erreur 403 à la collecte, jamais à la vérification.

03 **Créez le compte de service : IAM et administration › Comptes de service › Créer**

Nom libre ; aucun rôle IAM n'est nécessaire sur le projet. Relevez son **identifiant client unique** (OAuth 2 Client ID, une suite de chiffres) sur sa fiche.

04 **Créez une clé : onglet Clés › Ajouter une clé › Créer une clé › JSON**

Le fichier JSON se télécharge une seule fois : c'est lui que l'assistant REVIEWIT demande. Ne le conservez pas ailleurs après la saisie.

05 **Dans `admin.google.com`, ouvrez Sécurité › Contrôle des accès et des données › Commandes des API › Gérer la délégation au niveau du domaine**

Cliquez **Ajouter**, collez l'identifiant client du compte de service, puis la liste des portées **copiée depuis l'assistant REVIEWIT** (étape Préparer › « Copier le plan »), et autorisez.

06 **Relevez l'ID client de votre organisation : Compte › Paramètres du compte › Profil**

Une chaîne de la forme `C0xxxxxxx`. C'est le champ « Customer ID » de l'assistant.

07 **Choisissez l'administrateur à usurper**

L'adresse d'un **super-administrateur** actif : l'Admin SDK n'accepte d'agir qu'au nom d'un administrateur du domaine. Préférez un compte d'administration dédié, sans boîte personnelle.

PORTÉES : NE LES DEVINEZ PAS

La délégation au niveau du domaine refuse toute portée absente de sa liste, et la liste doit correspondre exactement à ce que REVIEWIT demandera. Copiez le plan depuis l'assistant ; si vous ajoutez des ressources plus tard, l'assistant vous rendra les portées manquantes, à compléter dans la même délégation.

04 Ce que vous saisirez dans l'assistant

L'étape **Identifiant** n'affiche que les champs que Google Workspace 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 « Google Workspace · <votre domaine> ».
Customer ID	L'ID client de l'organisation (`C0xxxxxxx`), relevé à l'étape 6. C'est l'identifiant externe de la connexion.
Service account key (JSON)	Le contenu du fichier JSON téléchargé à l'étape 4, collé tel quel. REVIEWIT vérifie qu'il est lisible avant de l'enregistrer.
Admin to impersonate	L'adresse du super-administrateur choisie à l'étape 7.

UNE CLÉ JSON EST UN SECRET

Elle porte la clé privée du compte de service. Saisie une fois, elle est rangée au coffre et désignée par référence ; aucun écran ne la montre à nouveau. Un fichier JSON invalide bloque l'enregistrement : il écraserait la clé déjà stockée par un texte illisible.

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 Google Workspace.

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 Google Workspace, 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 Google Workspace ; **Enregistrer sans vérifier** garde la connexion inactive, à vérifier plus tard.

Google saisit son identité (le Customer ID) : « Enregistrer sans vérifier » est ouvert dès que le nom et le Customer ID sont renseignés, la clé pouvant être ajoutée plus tard.

ÉTAPE 4 Vérification

Google Workspace 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.

La vérification demande un jeton à Google au nom de l'administrateur, puis lit l'organisation : un refus `unauthorized_client` désigne une délégation absente ou incomplète (section 8).

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

REÇU DE GOOGLE WORKSPACE	USAGE CHEZ REVIEWIT
`Customer ID · nom de l'organisation`	L'identité de la connexion et son nom d'affichage.
`Admin SDK Directory`	Utilisateurs, groupes, membres, unités organisationnelles, rôles : qui existe et qui détient quoi.
`Drive · Sites · Calendar · Chat · Keep`	Les objets, leurs propriétaires, leurs membres et leurs permissions — jamais leur contenu.
`Paramètres Gmail`	Délégués, règles de transfert et adresses d'envoi des boîtes — jamais un courriel.
`Permissions de type « domaine » · liens « toute l'organisation »`	Le signal **Partage trop large** : un Drive partagé ou un site ouvert au domaine, un Mon Drive riche en liens d'organisation, comptés et datés, jamais nommés.

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 Google Workspace, puis « Vérifier les droits ».
Renouveler le secret	Créez une **nouvelle clé JSON** sur le compte de service (IAM › Comptes de service › Clés), saisissez-la dans « Connexions › Ajouter un identifiant », vérifiez, puis supprimez l'ancienne clé côté Google. La délégation au niveau du domaine porte sur l'identifiant client du compte de service : elle ne change pas.
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 Google Workspace. Les plans de collecte qui s'appuyaient dessus s'arrêtent.

08 Dépannage

CE QUE VOUS VOYEZ	CAUSE	CE QU'IL FAUT FAIRE
`unauthorized_client` à la vérification	La délégation au niveau du domaine n'autorise pas ce compte de service, ou pas toutes les portées demandées.	Dans « Gérer la délégation au niveau du domaine », vérifiez l'identifiant client et recollez le plan complet des portées.
`invalid_grant` / « Invalid email or User ID »	L'administrateur à usurper n'existe pas, est suspendu, ou n'est pas administrateur.	Saisissez l'adresse d'un super-administrateur actif.
Une ressource rend 403 « Not Authorized to access this resource/api »	L'API correspondante n'est pas activée sur le projet, ou le service est désactivé dans l'organisation.	Activez l'API dans la bibliothèque du projet ; vérifiez que le service (Chat, Keep…) est activé pour les utilisateurs.
« Le JSON n'est pas lisible »	Fichier tronqué, ou copie d'un autre type de clé (P12, clé publique).	Recréez une clé JSON et collez le fichier entier, accolades comprises.
Le Customer ID est refusé	Il ne correspond pas à l'organisation que la clé sert.	Relevez-le dans `admin.google.com › Compte › Paramètres du compte`, sur la même organisation que l'administrateur usurpé.

LISTE DE CONTRÔLE AVANT D'OUVRIR L'ASSISTANT — 6 points

- [ ] Je dispose d'un super-administrateur Google Workspace et d'un projet Google Cloud dédié.
- [ ] Les API du plan sont activées sur le projet.
- [ ] Le compte de service existe ; sa clé JSON est téléchargée et prête à être collée.
- [ ] La délégation au niveau du domaine porte **l'identifiant client du compte de service** et **les portées copiées depuis l'assistant**.
- [ ] Je connais l'ID client de l'organisation (`C0xxxxxxx`) et l'adresse de l'administrateur à usurper.
- [ ] J'ouvre le Subscription Manager avec un compte 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.