CONNECTER VOTRE SOLUTION

Okta

Raccordez votre organisation Okta à REVIEWIT : une application de service dédiée, authentifiée par une paire de clés, limitée à des portées de lecture.

VERSION
1.1 · Novembre 2026

DURÉE
Trente minutes, en quatre étapes

DIFFUSION
Confidentiel · Clients REVIEWIT

CE QU'IL VOUS FAUT

01 **Un super-administrateur Okta** : lui seul peut accorder des portées de l'API Okta et affecter des rôles d'administrateur à une application.

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

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 Okta, 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
Okta
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 Okta.

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 organisations Okta, sur les domaines `okta.com`, `oktapreview.com` et `okta-emea.com`. L'application de service n'appartient à aucune personne : elle survit aux départs. Les propriétaires de groupes dépendent d'une fonctionnalité d'Okta : là où elle manque, le passage le signale et les groupes sont rapportés sans propriétaire. La lecture des portées accordées aux applications dépend de droits qu'Okta ne délègue pas en lecture seule ; quand elle est refusée, le passage le signale et rapporte quand même les consentements des personnes.

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
`okta.users.read`	Comptes, comptes fermés, comptes jamais activés ; base des affectations d'applications, des rôles d'administrateur et des consentements OAuth
`okta.groups.read`	Groupes et leurs propriétaires, membres des groupes, règles de groupe, affectations de groupes aux applications ; rôles d'administrateur portés par des groupes
`okta.apps.read`	Applications, affectations des personnes et des groupes ; rôles d'administrateur portés par des applications de service
`okta.roles.read`	Affectations de rôles d'administrateur — des personnes, des groupes et des applications de service —, rôles d'administrateur personnalisés
`okta.apiTokens.read`	Jetons d'API et leur titulaire
`okta.appGrants.read`	Consentements OAuth

DROIT OU GESTE	RESSOURCES QU'IL OUVRE
Rôle « Administrateur en lecture seule »	Toutes les ressources : sans rôle d'administrateur, Okta délivre le jeton mais refuse chaque lecture
Rôle personnalisé « Voir les rôles, les ressources et les affectations d'administrateur »	Affectations de rôles d'administrateur, rôles personnalisés

03 Créer l'identifiant chez Okta

Un super-administrateur crée, dans la console d'administration Okta, **une application de service dédiée à REVIEWIT**. Elle s'authentifie par une paire de clés : Okta garde la clé publique, REVIEWIT reçoit la clé privée. Aucun utilisateur ne se connecte ; aucun mot de passe ni jeton personnel n'est partagé.

01 **Ouvrez Applications › Applications › Créer une intégration d'application, choisissez Services d'API**

Nommez-la, par exemple « REVIEWIT Collect », et gardez un ID client généré par Okta.

02 **Onglet Général › Informations d'identification client › Modifier : choisissez Clé publique / Clé privée, puis enregistrez**

Par défaut l'application attend un secret client, qu'Okta refuse pour les portées de son API. Tant que ce choix n'est pas enregistré, la vérification échoue en `invalid_client`.

03 **Section Clés publiques › Modifier › Ajouter une clé › Générer une nouvelle clé**

Copiez la **clé privée au format PEM** dans un fichier `.pem` : Okta ne l'affiche qu'une fois. Terminez, puis enregistrez la section ; la clé doit apparaître « Active ».

04 **Section Paramètres généraux › Modifier : décochez Exiger l'en-tête Demonstrating Proof of Possession (DPoP)**

La case est cochée par défaut. REVIEWIT n'envoie pas cette preuve : laissée cochée, la vérification le dit et s'arrête.

05 **Onglet Portées de l'API Okta : accordez les portées du plan**

Les six portées de lecture ci-dessus, et aucune autre. L'assistant REVIEWIT les liste à l'étape Préparer.

06 **Onglet Rôles d'administrateur › Modifier les affectations : affectez Administrateur en lecture seule**

Okta demande une authentification renforcée à l'enregistrement.

07 **Pour les rôles d'administrateur : créez un rôle personnalisé et son ensemble de ressources, puis affectez-les**

Sécurité › **Administrateurs** › **Rôles** › **Créer un rôle** avec la seule permission « Voir les rôles, les ressources et les affectations d'administrateur » ; **Ressources** › **Créer un ensemble de ressources** sur « Gestion des identités et des accès », toutes les ressources. Dans l'affectation, choisissez l'ensemble de ressources avant le rôle.

08 **Relevez le Client ID de l'application et le domaine de l'organisation**

Le Client ID commence par `0oa`. Le domaine est celui de l'organisation, sans le suffixe `-admin` de la console.

LECTURE SEULE, ET VÉRIFIABLE

L'application ne reçoit que des portées `…read` : REVIEWIT ne peut rien modifier dans Okta. À chaque échange de jeton, Okta nomme les portées qu'il accorde ; c'est cette liste, constatée, que l'assistant affiche.

04 Ce que vous saisirez dans l'assistant

L'étape **Identifiant** n'affiche que les champs que Okta 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 « Okta · <votre organisation> ».
Authentication method	**API service app.** Le jeton d'API ne sert qu'à l'annuaire des personnes : aucune collecte ne l'admet.
Okta org domain	L'hôte de l'organisation, sans `https://` — par exemple `acme.okta.com`. C'est l'identifiant externe de la connexion.
Client ID	Celui de l'application de service, relevé à l'étape 8.
Private key (.pem)	Le fichier `.pem` enregistré à l'étape 3.

UNE CLÉ PRIVÉE EST UN SECRET

Déposée une fois, elle est rangée au coffre et désignée par référence ; aucun écran ne la montre à nouveau. Supprimez le fichier `.pem` de votre poste après la vérification.

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 Okta.

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

Okta saisit son identité (le domaine de l'organisation) : elle est verrouillée après la création de la connexion.

ÉTAPE 4 Vérification

Okta 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 Okta, relève les portées accordées, puis lit un groupe : un refus à cette lecture désigne un rôle d'administrateur manquant (section 8).

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

REÇU DE OKTA	USAGE CHEZ REVIEWIT
`Domaine de l'organisation`	L'identité de la connexion.
`Comptes · groupes · membres · règles`	Qui existe, dans quel état, et qui appartient à quoi.
`Applications · affectations`	Quelle personne et quel groupe accèdent à quelle application.
`Propriétaires des groupes`	Qui répond de chaque groupe, quand votre organisation les déclare.
`Rôles d'administrateur · rôles personnalisés`	Qui administre Okta — personne, groupe ou application de service — et avec quelles permissions.
`Jetons d'API · consentements OAuth`	Les identifiants techniques et leur titulaire, les consentements donnés — jamais la valeur d'un jeton.

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 Okta, puis « Vérifier les droits ».

Renouveler le secret	Ajoutez une **nouvelle clé** sur l'application de service (Général › Clés publiques › Ajouter une clé), déposez sa clé privée dans « Connexions › Ajouter un identifiant », vérifiez, puis désactivez l'ancienne clé côté Okta. Le Client ID, les portées et les rôles ne changent 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 Okta. Les plans de collecte qui s'appuyaient dessus s'arrêtent.

08 Dépannage

CE QUE VOUS VOYEZ	CAUSE	CE QU'IL FAUT FAIRE
`invalid_client` à la vérification	L'application attend encore un secret client, ou la clé déposée n'est pas celle enregistrée sur l'application.	Enregistrez « Clé publique / Clé privée » dans les informations d'identification client ; vérifiez le Client ID ; au besoin générez une nouvelle clé.
« The API service app requires proof of possession (DPoP) »	La case DPoP est restée cochée.	Décochez-la dans Général › Paramètres généraux, puis vérifiez à nouveau.
`E0000006` « You do not have permission »	Les portées sont accordées mais l'application ne porte aucun rôle d'administrateur.	Affectez « Administrateur en lecture seule » dans l'onglet Rôles d'administrateur.
Les rôles d'administrateur restent non lisibles	Le rôle en lecture seule ne lit pas les rôles.	Affectez le rôle personnalisé de l'étape 7, sur son ensemble de ressources.
Avis « portées d'application non lisibles »	Okta refuse cette lecture à une application en lecture seule.	Aucun geste : les consentements des personnes sont rapportés ; l'avis reste au rapport du passage.
Avis « propriétaires de groupes non disponibles »	Votre organisation Okta n'a pas la fonctionnalité des propriétaires de groupes (la fiche d'un groupe n'a pas d'onglet Propriétaires).	Aucun geste côté REVIEWIT : les groupes sont rapportés sans propriétaire. Activez la fonctionnalité chez Okta pour les voir apparaître au passage suivant.
Le domaine est refusé	Il porte `https://`, un chemin, ou le suffixe `-admin` de la console.	Saisissez l'hôte nu de l'organisation, par exemple `acme.okta.com`.

LISTE DE CONTRÔLE AVANT D'OUVRIR L'ASSISTANT

6 points

- [ ] Je dispose d'un super-administrateur Okta.
- [ ] L'application de service existe, en « Clé publique / Clé privée », avec une clé **Active**.
- [ ] La case DPoP est décochée.
- [ ] Les six portées de lecture sont accordées, et elles seules.
- [ ] L'application porte « Administrateur en lecture seule », et le rôle personnalisé si je collecte les rôles d'administrateur.
- [ ] J'ai le fichier `.pem`, le Client ID et le domaine de l'organisation, 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.