

# Dépannage de la synchronisation des identités utilisateur/groupe dans Cisco Secure Access avec diff IDP

## Table des matières

---

## Problème

Ce document décrit comment dépanner la synchronisation des identités des utilisateurs et des groupes dans Cisco Secure Access avec différents fournisseurs d'identité (IdP) tels qu'Okta, Microsoft Entra ID et IBM Cloud.

## Environnement

- Cisco Secure Access : intégration de la mise en service SCIM
- S'applique au connecteur IDp de SCIM 2.0 (Okta, Azure AD)

## Résolution

### Aperçu

Cisco Secure Access prend en charge l'approvisionnement des identités d'utilisateur et de groupe directement à partir d'Okta et de Microsoft Entra ID (anciennement Azure AD) à l'aide de la norme SCIM 2.0, ce qui élimine le besoin de déployer un connecteur Active Directory (AD) sur site pour les sources d'identité cloud uniquement. Cet article regroupe les hypothèses d'architecture, les modes de défaillance courants et les conseils de dépannage que les ingénieurs et les administrateurs sur site rencontrent le plus souvent lorsqu'ils déploient ou entretiennent cette

intégration.

Ce document est divisé en quatre sections :

- Configuration : où accéder aux instructions de configuration officielles
- Hypothèses d'architecture qui, en cas de violation, entraînent des défaillances silencieuses ou difficiles à diagnostiquer
- Problèmes spécifiques au fournisseur (Okta contre Entra ID)
- Problèmes de protocole SCIM générique qui s'appliquent quel que soit l'IdP

## Configuration

Cet article se concentre sur le dépannage et non sur la configuration initiale. Utilisez les notes techniques officielles de Cisco dans ce document pour une configuration pas à pas :

- Afin de configurer Cisco Secure Access avec Microsoft Entra ID (Azure AD), référez-vous à ce lien : Configurer les utilisateurs et les groupes pour sécuriser l'accès via un ID supplémentaire
- Afin de configurer Cisco Secure Access avec Okta, référez-vous à ce lien : Configuration des utilisateurs et des groupes pour un accès sécurisé via OKTA

Les deux documents traitent de la génération du jeton SCIM et de l'URL d'approvisionnement dans Secure Access, de la configuration de l'application correspondante dans le fournisseur d'identité et de l'exécution de la synchronisation d'approvisionnement initiale.

## Initiation à l'architecture

Avant de procéder au dépannage, vérifiez que le déploiement correspond à ces hypothèses de base. La plupart des échecs de synchronisation remontent à l'une de ces hypothèses.

Une source d'identité à la fois

L'approvisionnement simultané des mêmes utilisateurs ou groupes à partir d'un connecteur AD sur site et d'un ID de cloud (ID Okta ou Entra) n'est pas pris en charge et entraîne une application incohérente de la stratégie. Si vous migrez du connecteur AD vers un ID de cloud :

- Arrêtez le service AD Connector sur site.
- Vérifiez qu'aucune tâche de synchronisation résiduelle n'est en cours d'exécution avant d'activer le provisionnement IdP cloud.

Les appareils virtuels sont l'exception

Entra ID ou Okta ne peuvent pas fournir d'intégration d'identité pour les appareils virtuels (VA), car le fournisseur d'identité n'a aucune visibilité sur les mappages IP-utilisateur privés, ce que les VA requièrent. Les déploiements VA nécessitent toujours le connecteur AD sur site, quel que soit le composant utilisé pour les autres composants.

Attribuer/Diffuser

- Action : Affectation d'utilisateurs ou de groupes à l'application
  - Ce qu'il fait réellement : Met en service l'accès sécurisé pour les utilisateurs membres de ce groupe
- Action : Pousser un groupe (Okta)
  - Ce qu'il fait réellement : Met en service l'objet groupe lui-même (pour le ciblage de stratégie). Il ne synchronise aucun utilisateur.



Remarque : Ne diffusez pas un groupe qui est également affecté à l'application pour le provisionnement des utilisateurs. Cela peut créer un état de groupe en double ou conflictuel.

---

Limites de groupe et d'utilisateur

Il n'y a pas de limite stricte sur le nombre d'utilisateurs provisionnés à partir de l'un des IDp.

Les groupes sont limités. Historiquement, il s'agissait de 200 groupes par organisation, provenant

d'Okta ou d'Entra ID ; certains documents actuels montrent un plafond plus élevé (jusqu'à 1 000) pour Okta en particulier. Considérez le nombre exact comme dépendant de l'environnement et confirmez-le auprès du Centre d'assistance technique Cisco (TAC) ou de la documentation Cisco actuelle. Les groupes au-delà de la limite ne sont pas provisionnés en silence et aucune erreur n'est signalée.

Si vous avez besoin d'une couverture plus large, utilisez un groupe dynamique « Tous les utilisateurs » (Entra ID) ou « Tout le monde » (Okta) au lieu d'essayer de pousser chaque groupe individuellement.

## Cycle de vie des jetons SCIM

Dans Cisco Secure Access, les jetons sont générés lorsque vous choisissez Connect > Users, Groups and Endpoint Devices > Configuration Management > Integrate Directory. Le jeton n'est affiché qu'une seule fois lors de sa création.

Lorsque vous régénérez le jeton, il interrompt immédiatement le provisionnement côté fournisseur d'identité jusqu'à ce que le nouveau jeton soit entré dans la configuration de provisionnement de Microsoft Entra ID ou Okta. Il n'y a pas de délai de grâce et l'erreur côté IdP est souvent générique (échec d'authentification) plutôt qu'un message d'expiration de jeton.

Actualisez régulièrement le jeton pour des raisons d'hygiène et testez la connexion côté fournisseur d'identité immédiatement après la rotation.

## Problèmes spécifiques à Okta

- Symptôme : Les groupes n'apparaissent pas dans Secure Access
  - Cause première : La transmission d'un groupe ne provisionne que l'objet groupe ; il ne synchronise pas les membres.
  - Résolution : Assurez-vous que les membres du groupe concerné sont affectés séparément à l'application sous Affectations.
- Symptôme : Utilisateurs provisionnés mais attributs manquants ou incorrects
  - Cause première : Secure Access uniquement les surfaces Display Name et Username ; Les prénoms et les noms de famille ne sont pas répertoriés.

- Résolution : Confirmer que les attributs requis sont explicitement sélectionnés pour la synchronisation ; ne supposez pas que tous les champs de profil Okta se propagent.
- Symptôme : Le provisionnement ne fait rien
  - Cause première : Les options Créer des utilisateurs, Mettre à jour les attributs utilisateur ou Désactiver les utilisateurs ne sont pas activées.
  - Résolution : Vérifiez que les trois sont cochés sous Provisioning > To App dans la console de l'administrateur d'Okta.
- Symptôme : objectGUID ou attribut personnalisé non synchronisé
  - Cause première : L'attribut n'est pas ajouté et mappé via le mappage de profil utilisateur.
  - Résolution : Ajoutez l'attribut objectGUID et créez le mappage de profil correspondant si cet identificateur est requis.
- Symptôme : Synchronisation arrêtée après rotation du jeton
  - Cause première : Jeton SCIM ou API régénéré dans Secure Access mais pas mis à jour dans Okta.
  - Résolution : Entrez le nouveau jeton sous Provisioning > Configure API Integration et exécutez à nouveau Test API Credentials.
- Symptôme : Impossible de déterminer pourquoi un utilisateur ou un groupe spécifique a échoué
  - Cause première : Les journaux n'ont pas été vérifiés.
  - Résolution : Cochez Reports > System Log dans Okta, filtré vers l'application Cisco User Management Connector, avant que vous ne remontiez.
- Symptôme : Le nombre de groupes dépasse la limite, certains manquants sans erreur
  - Cause première : L'entreprise compte plus de groupes que ceux pris en charge par Secure Access.
  - Résolution : Réduisez la portée aux seuls groupes concernés par les politiques ou faites appel au TAC Cisco pour une assistance de groupe de niveau supérieur.

## Problèmes spécifiques à Microsoft Entra ID

- Symptôme : L'appartenance à un groupe dynamique ne se reflète pas dans Secure Access

- Cause première : La règle de groupe dynamique est mal configurée ou le groupe ne se trouve pas dans l'étendue provisionnée.
- Résolution : Validez la règle d'appartenance dynamique directement dans Entra ID avant de supposer un bogue de synchronisation Secure Access.
- Symptôme : SSO SAML attendu pour générer l'identité SWG
  - Cause première : AnyConnect Secure Web Gateway (SWG) ne prend pas en charge l'authentification SAML (Security Assertion Markup Language) avec l'ID supplémentaire ; il utilise le même mécanisme d'authentification passive que la fonction AD locale.
  - Résolution : Ne pas concevoir autour de l'identité SWG basée sur SAML pour Entra ID ; utilisez l'authentification passive comme documenté.
- Symptôme : L'utilisateur affiche incorrectement désactivé
  - Cause première : ID d'entrée envoyé actif : false car l'utilisateur est sorti d'une étendue de groupe attribuée ou un mappage d'attribut actif est mal configuré.
  - Résolution : Vérifier si l'utilisateur a été supprimé d'un groupe dont l'étendue est définie ; vérifiez le mappage actif (il doit généralement être évalué comme `Not([isSoftDeleted])`).
- Symptôme : Application mise en quarantaine, provisionnement interrompu
  - Cause première : L'application cible a renvoyé des réponses répétées non conformes à SCIM.
  - Résolution : Vérifiez l'état de mise en service de l'application d'entreprise pour un indicateur de quarantaine avant de supposer des défaillances d'utilisateur individuelles.
- Symptôme : Le cycle de provisionnement initial échoue complètement
  - Cause première : Échec transitoire de la synchronisation lors de la première exécution.
  - Résolution : Cliquez sur Restart Provisioning dans la page Overview pour forcer Entra ID à tenter à nouveau la synchronisation initiale.
- Symptôme : Les utilisateurs dupliqués fusionnent de manière inattendue
  - Cause première : Deux identités source partagent le même e-mail ou le même nom d'utilisateur principal (UPN).
  - Résolution : Veiller à l'unicité des e-mails et des UPN dans le répertoire source ; vérifiez que l'attribut mail provient d'un domaine vérifié.
- Symptôme : L'attribut cesse de se mettre à jour après une modification du schéma
  - Cause première : Le type d'attribut a changé du côté cible (par exemple, chaîne en

booléen), mais le mappage d'ID d'entrée n'a pas été mis à jour.

- Résolution : Corrigez manuellement le type dans Paramètres avancés sous Mappages d'attributs.
- Symptôme : La référence du manager ne remplit jamais
  - Cause première : Un utilisateur était dans le champ d'application avant que son responsable ne le soit ; le provisionnement n'effectue pas automatiquement de remblayage.
  - Résolution : Redémarrez le provisionnement pour forcer la réévaluation complète de tous les utilisateurs dans l'étendue.

## Vérification de la sécurité IBM - Problèmes spécifiques

- Symptôme : Les utilisateurs configurent mais les groupes n'apparaissent jamais dans Secure Access
  - Cause première : Vérifiez que le connecteur SCIM personnalisé émet uniquement des opérations utilisateur ; aucun appel POST /Groups n'est jamais envoyé (écart de capacité de provisionnement de compte, pas d'erreur de mappage).
  - Résolution : Capturez une trace de connecteur et vérifiez si des appels /Groups se produisent ; si aucun, provisionnez les groupes via le connecteur Cisco AD, l'importation CSV ou un script planifié sur le point d'extrémité SCIM d'accès sécurisé.
- Symptôme : La mise à jour des membres du groupe échoue avec 400 ou 404
  - Cause première : members[].value references Vérifiez les ID utilisateur internes au lieu de l'ID SCIM Secure Access renvoyé lors de la création de l'utilisateur.
  - Résolution : Corrigez le mappage des membres pour utiliser l'ID SCIM d'accès sécurisé et exécutez à nouveau une synchronisation complète.
- Symptôme : Les groupes apparaissent mais sont vides
  - Cause première : Groupe poussé avant que ses utilisateurs membres n'existent dans Secure Access ; Appartenance PATCH référencé utilisateurs inconnus.
  - Résolution : Exécuter à nouveau une synchronisation complète maintenant que les utilisateurs existent ; assurez-vous que la synchronisation crée des utilisateurs avant les groupes.
- Symptôme : Boucles de connexion SAML ou redirections répétées

- Cause première : Vérifiez que le point de terminaison IdP est mis en proxy ou déchiffré par le SWG, ce qui interrompt le flux d'authentification.
- Résolution : Ignorez l'URL de vérification du fournisseur d'ID de SAML pour le déchiffrement (liste de domaines externes ou déchiffrement sélectif).
- Symptôme : L'utilisateur s'authentifie via SAML mais aucune stratégie basée sur l'utilisateur ne correspond
  - Cause première : SAML NameID ne correspond pas à l'utilisateur configuré authName .
  - Résolution : Alignez le format NameID > dans l'application Verify SAML avec le mappage d'attribut authName (généralement email ou UPN) ; testez à nouveau.
- Symptôme : Le provisionnement cesse de fonctionner après des semaines ou des mois de stabilité
  - Cause première : Le jeton SCIM a été pivoté ou a expiré dans Secure Access mais n'a pas été mis à jour dans le connecteur de vérification.
  - Résolution : Actualisez le jeton dans Secure Access et mettez-le à jour dans l'application personnalisée Vérifier ; calendrier la cadence d'actualisation.
- Symptôme : Utilisateurs en double créés lors de la resynchronisation
  - Cause première : externalId mappé à un attribut muable ou non unique (par exemple, nom d'affichage, e-mail modifiable).
  - Résolution : Mapper externalId à un identificateur immuable (Vérifier l'ID utilisateur ou objectGUID); nettoyez les doublons et resynchronisez.
- Symptôme : Désactivé Vérifier que les utilisateurs restent actifs dans Secure Access
  - Cause première : L'action de suspension n'est pas mappée à active : false, ou l'opération de désactivation est désactivée dans le connecteur.
  - Résolution : Activez l'opération de désactivation et mappez la suspension à active:false ; vérifiez avec un utilisateur test.
- Symptôme : Les modifications d'attribut dans Vérifier ne sont pas propagées
  - Cause première : Utilisateur ou attribut hors de l'étendue de la stratégie d'approvisionnement ou opération de mise à jour désactivée.
  - Résolution : Examiner la politique ou les habilitations de mise en service des applications ; activer les mises à jour ; déclencher une synchronisation manuelle.
- Symptôme : Secure Access rejette les demandes avec des erreurs de schéma ou de type

- Cause première : Charge utile non conforme à la norme SCIM (tableau de schémas manquant, URN incorrect, opération non prise en charge).
- Résolution : Reproduire avec l'essai de bouclage de base ; corriger la charge utile ou le mappage ; Transférez à IBM si le connecteur émet la requête mal formée.
- Symptôme : Identité SWG manquante pour les utilisateurs itinérants malgré le fonctionnement de SAML
- Cause première : Le protocole SAML doit générer l'identité pour un mode de déploiement qui utilise l'identité passive ou basée sur l'agent.
- Résolution : Confirmer la méthode d'acquisition d'identité pour chaque mode de déploiement par rapport à la documentation Secure Access ; ne concevez pas SAML comme la seule source d'identité.

## Problèmes génériques du SCIM

Ils ne sont pas spécifiques à Cisco, mais apparaissent systématiquement dans les déploiements d'accès sécurisé, car le transport sous-jacent est la norme SCIM 2.0 :

- Les états de quarantaine masquent les erreurs individuelles : Si la synchronisation semble s'être entièrement arrêtée au lieu d'échouer par utilisateur, recherchez un état de quarantaine ou de suspension au niveau de l'application avant d'examiner les problèmes d'attributs individuels.
- 409 Conflit lors de la désactivation : Modèle courant dans lequel le fournisseur d'identité tente de désactiver un utilisateur et la cible génère un conflit. Il s'agit généralement d'un problème de mappage d'attribut actif ou d'étendue de groupe, et non d'une véritable erreur système.
- Les champs vides ou effacés ne se propagent pas toujours : Certaines implémentations de serveur SCIM conservent la dernière valeur non nulle ; lorsque vous effacez un champ dans le fournisseur d'identité, il peut vous être nécessaire de faire passer d'abord une valeur d'espace réservé.
- Les modifications d'URL ou de configuration invalident silencieusement l'authentification : Toute modification apportée à l'URL du point de terminaison SCIM nécessite généralement que vous fournissiez à nouveau le jeton porteur. Les erreurs apparaissent comme des URL non valides même lorsque le problème réel est un jeton périmé.
- Aucun webhook ou flux d'événements natif : L'automatisation qui attend des notifications push en temps réel sur les changements d'utilisateur ou de politique doit interroger l'API de reporting ou s'intégrer via Cisco XDR à la place. Secure Access n'émet pas de webhooks de

mise en service sortants.

Transférez au TAC Cisco les journaux de provisionnement du côté du fournisseur d'identité si les étapes précédentes ne résolvent pas le problème. Les journaux de provisionnement back-end côté accès sécurisé nécessitent généralement un accès TAC pour l'extraction.

## Motif

L'intégration de la mise en service SCIM n'a pas pu transmettre un ou plusieurs enregistrements en raison d'un jeton de support expiré, d'une non-correspondance de mappage d'attribut, d'un groupe cible manquant ou d'une portée de mise en service insuffisante.

## Autres informations utiles

- Cisco : [Configurer les utilisateurs et les groupes pour sécuriser l'accès via un ID supplémentaire](#)
- Cisco : [Configuration des utilisateurs et des groupes pour un accès sécurisé via OKTA](#)
- Microsoft Learn : Problèmes connus de conformité au protocole SCIM 2.0 - Microsoft Entra ID
- Microsoft Learn : Dépanner les erreurs de l'API SCIM Microsoft Entra ID
- Configurez SAML SSO dans le fournisseur d'identité : <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- Mise en service d'applications personnalisées (SCIM) : <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- Présentation du provisionnement et de la gouvernance (connecteur SCIM générique) : <https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- Pont de mise en service sur site (sources AD/LDAP) : <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.