Migration des connecteurs AD d'accès sécurisé de l'authentification héritée vers l'authentification API

Table des matières

Problème

Les entreprises utilisant les connecteurs Cisco Secure Access avec Active Directory (AD) reçoivent des notifications indiquant que l'authentification API est recommandée pour Active Directory et les appareils virtuels, l'authentification héritée devant expirer le 29 mai 2026. Les utilisateurs ont besoin d'une assistance à la configuration pour migrer de l'authentification héritée vers l'authentification API avant la date d'expiration et souhaitent comprendre l'impact potentiel sur la synchronisation d'AD et d'appliance virtuelle pendant le processus de migration. La principale préoccupation est de savoir si la mise en oeuvre de ce changement pendant les heures de travail peut entraîner des pannes dans les opérations de synchronisation des services AD et VA, qui peuvent affecter les opérations dépendantes des politiques et des identités.

Environnement

- Cisco Secure Access (anciennement Cisco Umbrella)
- Connecteurs Active Directory déployés
- Méthode d'authentification existante actuellement utilisée
- Migration de l'authentification API requise avant le 29 mai 2026
- Environnement AD uniquement (sans appareils virtuels dans certains cas)

Résolution

La migration de l'authentification héritée vers l'authentification API implique la génération de clés API dans le portail d'accès sécurisé et leur configuration correcte. Le processus nécessite la création de clés d'API Admin et de clés d'API Client pour les connecteurs AD et les appliances

virtuelles.

Étape 1: Générer une clé API Admin

Accédez à Admin > API Keys dans le portail Secure Access et générez une nouvelle clé d'API d'administration et un nouveau secret de clé d'administration. Stockez ces informations d'identification en toute sécurité, car elles sont nécessaires à la génération de la paire de clés API client.

Étape 2: Générer une paire de clés API client

Accédez à Users and Groups > Configuration Management > Advanced Settings et localisez la section API Authentication. Entrez la clé d'API d'administration et le secret de clé d'administration générés à l'étape 1, puis cliquez sur Générer la paire de clés d'API client. Ceci produit la clé d'API client et le secret client utilisés par les connecteurs AD et les appareils virtuels.

Étape 3: Configuration de l'authentification API dans les paramètres avancés

Copiez la clé API client et le secret client générés dans la section API Authentication Advanced Settings du portail Secure Access. Enregistrez ces informations d'identification en toute sécurité, car elles sont requises pour toutes les configurations du connecteur AD et de l'appliance virtuelle.

Étape 4: Mettre à jour les connecteurs AD et les appareils virtuels

Appliquez la clé d'API client et le secret client nouvellement générés à tous les connecteurs AD et appliances virtuels déployés. Cela garantit qu'ils peuvent s'authentifier correctement pour l'enregistrement et les contrôles d'intégrité en utilisant la nouvelle méthode d'authentification API.

Impact de la migration et bonnes pratiques

La génération de clés d'API dans le portail d'accès sécurisé n'est généralement pas gênante. Cependant, l'impact opérationnel se produit pendant le moment de basculement lorsque les connecteurs AD et les appareils virtuels sont mis à jour pour utiliser la nouvelle clé et le nouveau secret de l'API client.

Impact attendu pendant la transition :

- Des échecs temporaires de synchronisation et de vérification de l'intégrité peuvent se produire pour les composants qui utilisent encore l'authentification héritée.
- Retard ou échec de synchronisation AD/VA pendant la fenêtre de transition.
- Les décisions de stratégie reposant sur de nouvelles données d'identité/de groupe peuvent être affectées si la synchronisation échoue.

Approche de mise en oeuvre recommandée :

- Effectuez la migration pendant les heures de fermeture ou pendant les périodes de maintenance lorsque cela est possible.
- Pour la mise en oeuvre des heures de travail, utilisez une approche de mise à jour continue contrôlée.
- Mettez à jour un connecteur/une carte VA à la fois et vérifiez l'état d'intégrité avant de continuer.
- Évitez de mettre à jour tous les noeuds simultanément.
- Garantissez une redondance adéquate avec plusieurs connecteurs/cartes d'accès pour les mises à jour progressives.

Compatibilité et exigences :

- L'authentification API fonctionne avec les déploiements AD uniquement et ne nécessite pas d'appliances virtuelles.
- Les méthodes d'authentification héritées et API restent actives pendant la période de migration.
- Les connecteurs AD doivent pouvoir se synchroniser avec Umbrella via api.opendns.com et passer à api.umbrella.com.

Motif

Cisco Secure Access est en train de passer des méthodes d'authentification traditionnelles à l'authentification API en tant que mécanisme d'authentification standard. La méthode d'authentification héritée a une date d'annulation planifiée du 29 mai 2026. L'authentification de l'API devient finalement la seule méthode d'authentification prise en charge, et les entreprises doivent migrer avant l'expiration de la méthode existante pour éviter les interruptions de service et les échecs de synchronisation AD/VA potentiels qui pourraient nécessiter une réinstallation complète pour récupérer.

Autres informations utiles

- Documentation d'authentification de Cisco Secure Access API
- Configuration avancée de Cisco Secure Access
- Gestion de la configuration Cisco Secure Access
- Assistance technique de Cisco et téléchargements

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.