Migration von AD-Connectors für sicheren Zugriff von Legacy-Authentifizierung zu API-Authentifizierung

Inhalt

Problem

Organisationen, die Cisco Secure Access mit Active Directory (AD)-Connectors verwenden, erhalten Benachrichtigungen, dass die API-Authentifizierung für Active Directory und virtuelle Appliances empfohlen wird. Die Legacy-Authentifizierung läuft am 29. Mai 2026 aus. Benutzer benötigen Konfigurationsunterstützung, um vor dem Ablaufdatum von der Legacy-Authentifizierung zur API-Authentifizierung zu migrieren, und möchten die möglichen Auswirkungen auf die AD- und Virtual Appliance-Synchronisierung während des Migrationsprozesses kennen. Das Hauptproblem besteht darin, ob die Implementierung dieser Änderung während der Arbeitszeit zu Fehlern bei AD- und VA-Synchronisierungsvorgängen führen kann, die identitäts- und richtlinienabhängige Vorgänge beeinflussen können.

Umwelt

- Cisco Secure Access (ehemals Cisco Umbrella)
- Active Directory-Connectors bereitgestellt
- Derzeit verwendete Legacy-Authentifizierungsmethode
- API-Authentifizierungsmigration vor dem 29. Mai 2026 erforderlich
- AD-Umgebung (in einigen Fällen ohne virtuelle Appliances)

Auflösung

Bei der Migration von der Legacy-Authentifizierung zur API-Authentifizierung werden API-Schlüssel im Secure Access-Portal generiert und richtig konfiguriert. Für diesen Prozess müssen sowohl Admin-API-Schlüssel als auch Client-API-Schlüssel für die AD Connectors und virtuellen

Appliances erstellt werden.

Schritt 1: Admin-API-Schlüssel generieren

Navigieren Sie zu Admin > API Keys im Secure Access-Portal, und generieren Sie einen neuen Admin API Key und einen Admin Key Secret. Speichern Sie diese Anmeldeinformationen sicher, da sie für die Generierung des Client-API-Schlüsselpaars erforderlich sind.

Phase 2: Schlüsselpaar der Client-API generieren

Navigieren Sie zu Benutzer und Gruppen > Konfigurationsverwaltung > Erweiterte Einstellungen, und suchen Sie den Abschnitt API-Authentifizierung. Geben Sie den in Schritt 1 generierten Admin-API-Schlüssel und Admin-Schlüssel-Schlüssel ein, und klicken Sie dann auf Client-API-Schlüsselpaar generieren. Dadurch werden der Client-API-Schlüssel und der Client-Schlüssel erstellt, die von den AD Connectors und virtuellen Appliances verwendet werden.

Schritt 3: Konfigurieren der API-Authentifizierung in den erweiterten Einstellungen

Kopieren Sie den generierten Client-API-Schlüssel und den Client-Schlüssel in den Abschnitt "Erweiterte Einstellungen für die API-Authentifizierung" des Portals für sicheren Zugriff. Speichern Sie diese Anmeldeinformationen sicher, da sie für alle AD Connector- und Virtual Appliance-Konfigurationen erforderlich sind.

Schritt 4: AD Connectors und virtuelle Appliances aktualisieren

Wenden Sie den neu generierten Client-API-Schlüssel und Client-Schlüssel auf alle bereitgestellten AD Connectors und virtuellen Appliances an. So wird sichergestellt, dass sie sich mit der neuen API-Authentifizierungsmethode für Registrierungs- und Integritätsprüfungen ordnungsgemäß authentifizieren können.

Auswirkungen und Best Practices auf die Migration

Die Generierung von API-Schlüsseln im Secure Access-Portal erfolgt in der Regel unterbrechungsfrei. Die Betriebsabläufe werden jedoch während der Umstellung beeinträchtigt, wenn AD Connectors und virtuelle Appliances aktualisiert werden, um den neuen Schlüssel und Schlüssel für die Client-API zu verwenden.

Erwartete Auswirkungen während der Umstellung:

- Temporäre Synchronisierungs- und Integritätsprüfungsfehler können für Komponenten auftreten, die noch die Legacy-Authentifizierung verwenden.
- AD/VA-Synchronisierungsverzögerung oder -fehler während des Übergangsfensters.
- Wenn die Synchronisierung fehlschlägt, können Richtlinienentscheidungen beeinflusst werden, die auf neuen Identitäts-/Gruppendaten basieren.

Empfohlener Implementierungsansatz:

- Führen Sie die Migration außerhalb der Arbeitszeiten oder, wenn möglich, während Wartungsfenstern durch.
- Verwenden Sie für die Implementierung während der Arbeitszeit einen kontrollierten, fortlaufenden Aktualisierungsansatz.
- Aktualisieren Sie jeweils einen Connector/VA, und prüfen Sie den Status "fehlerfrei", bevor Sie fortfahren.
- Vermeiden Sie die gleichzeitige Aktualisierung aller Knoten.
- Gewährleistung einer angemessenen Redundanz mit mehreren Connectors/VAs für fortlaufende Updates

Kompatibilität und Anforderungen:

- Die API-Authentifizierung funktioniert mit reinen AD-Bereitstellungen und erfordert keine virtuellen Appliances.
- Sowohl die Legacy- als auch die API-Authentifizierungsmethoden bleiben während des Migrationszeitraums aktiv.
- AD Connectors müssen mit Umbrella über api.opendns.com synchronisiert werden können und auf api.umbrella.com umgestellt werden.

Ursache

Cisco Secure Access wird von älteren Authentifizierungsmethoden auf API-Authentifizierung als Standardauthentifizierungsmechanismus umgestellt. Die Legacy-Authentifizierungsmethode hat das geplante Datum für die Außerbetriebnahme am 29. Mai 2026. Die API-Authentifizierung wird letztendlich zur einzigen unterstützten Authentifizierungsmethode, und Organisationen müssen migrieren, bevor die Legacy-Methode abläuft, um Serviceunterbrechungen und potenzielle AD/VA-Synchronisierungsfehler zu vermeiden, die eine vollständige Neuinstallation erforderlich machen könnten, um sich zu erholen.

Verwandte Inhalte

- Authentifizierungsdokumentation für die Cisco Secure Access API
- Erweiterte Konfiguration von Cisco Secure Access
- Konfigurationsmanagement für Cisco Secure Access
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.