

Troubleshoot User/Group Identity Sync in Cisco Secure Access with diff IDP

Contents

Issue

This document describes how to troubleshoot user and group identity synchronization in Cisco Secure Access with different Identity Providers (IdPs) such as Okta, Microsoft Entra ID, and IBM Cloud.

Environment

- Cisco Secure Access — SCIM provisioning integration
- Applies to SCIM 2.0 IdP connector (Okta, Azure AD)

Resolution

Overview

Cisco Secure Access supports provisioning user and group identities directly from Okta and Microsoft Entra ID (formerly Azure AD) using the SCIM 2.0 standard, which removes the need in order to deploy an on-premises Active Directory (AD) Connector for cloud-only identity sources. This article consolidates the architecture assumptions, common failure modes, and troubleshooting guidance that field engineers and admins encounter most often when they deploy or maintain this integration.

This document is organized into four sections:

- Configuration — where to go for official setup instructions
- Architecture assumptions that, if violated, cause silent or hard-to-diagnose failures

- Provider-specific issues (Okta versus Entra ID)
- Generic SCIM protocol issues that apply regardless of IdP

Configuration

This article focuses on troubleshooting, not initial setup. Use the official Cisco TechNotes in this document for step-by-step configuration:

- In order to configure Cisco Secure Access with Microsoft Entra ID (Azure AD), refer to this link: [Provision Users and Groups to Secure Access via Entra ID](#)
- In order to configure Cisco Secure Access with Okta, refer to this link: [Provision Users and Groups to Secure Access via OKTA](#)

Both documents cover generating the SCIM token and provisioning URL in Secure Access, configuring the corresponding application in the IdP, and running the initial provisioning synchronization.

Architecture Primer

Before you troubleshoot, confirm the deployment matches these core assumptions. The majority of synchronization failures trace back to one of these assumptions.

One Identity Source at a Time

Concurrent provisioning of the same users or groups from an on-premises AD Connector and a cloud IdP (Okta or Entra ID) is not supported and leads to inconsistent policy enforcement. If you migrate from the AD Connector to a cloud IdP:

- Stop the on-premises AD Connector service.
- Confirm no residual synchronization jobs are running before you enable cloud IdP provisioning.

Virtual Appliances Are the Exception

Entra ID or Okta cannot provide identity integration for Virtual Appliances (VAs), because the IdP has no visibility into private IP-to-user mappings, which VAs require. VA deployments still need the on-premises AD Connector regardless of what is used for other components.

Assign Versus Push

- **Action:** Assigning users or groups to the application
 - What it actually does: Provisions the member users of that group to Secure Access
- **Action:** Pushing a group (Okta)
 - What it actually does: Provisions the group object itself (for policy targeting). It does not synchronize any users.



Note: Do not push a group that is also assigned to the application for user provisioning. This can create duplicate or conflicting group state.

Group and User Limits

There is no hard limit on the number of users provisioned from either IdP.

Groups are capped. Historically, this was 200 groups per organization from either Okta or Entra ID; some current documentation shows a higher ceiling (up to 1,000) for Okta specifically. Treat the exact number as environment-dependent and confirm with the Cisco Technical Assistance Center (TAC) or current Cisco documentation. Groups beyond the cap are silently not provisioned, and no error is surfaced.

If you need broader coverage, use a dynamic "All Users" (Entra ID) or "Everyone" (Okta) group instead of an attempt to push every group individually.

SCIM Token Lifecycle

In Cisco Secure Access, tokens are generated when you choose **Connect > Users, Groups and Endpoint Devices > Configuration Management > Integrate Directory**. The token is shown only once at creation.

When you regenerate the token, it immediately breaks provisioning on the IdP side until the new token is entered in the provisioning configuration of Microsoft Entra ID or Okta. There is no grace period, and the IdP-side error is often generic (authentication failure) rather than a token expired message.

Refresh the token periodically for security hygiene and test the connection on the IdP side immediately after rotation.

Okta-Specific Issues

- **Symptom:** Groups **do not** appear in Secure Access
 - **Root Cause:** Pushing a group only provisions the group object; it does not synchronize members.
 - **Resolution:** Ensure the relevant group members are separately assigned to the application under Assignments.
- **Symptom:** Users provisioned but attributes missing **or** wrong
 - **Root Cause:** Secure Access only surfaces Display Name and Username; Given and Family names are not listed.
 - **Resolution:** Confirm required attributes are explicitly selected for synchronization; do not assume all Okta profile fields propagate.
- **Symptom:** Provisioning silently does nothing
 - **Root Cause:** Create Users, Update User Attributes, or Deactivate Users toggles are not enabled.
 - **Resolution:** Verify all three are checked under **Provisioning > To App** in the Okta administrator console.
- **Symptom:** **objectGUID** **or** custom attribute not synchronizing
 - **Root Cause:** Attribute **is** not added and mapped via User Profile Mapping.
 - **Resolution:** Add the **objectGUID** attribute and create the corresponding profile mapping if this identifier is required.
- **Symptom:** **Synchronization** stopped after token rotation
 - **Root Cause:** SCIM **or** API token regenerated in Secure Access but not updated in Okta.
 - **Resolution:** Enter the new token under **Provisioning > Configure API Integration** and run **Test API Credentials again**.
- **Symptom:** **Cannot determine** why a specific user **or** group failed
 - **Root Cause:** Logs were not checked first.
 - **Resolution:** Check **Reports > System Log** in Okta, filtered to the Cisco User Management Connector application, before you escalate.
- **Symptom:** Group count exceeds cap, some missing with no error
 - **Root Cause:** **Organization** has more groups scoped than Secure Access supports.

- **Resolution:** Reduce scope to policy-relevant groups only, or engage Cisco TAC for higher-tier group support.

Microsoft Entra ID Specific Issues

- **Symptom:** Dynamic group membership does not reflect in Secure Access
 - **Root Cause:** Dynamic group rule is misconfigured, or the group is not in the provisioned scope.
 - **Resolution:** Validate the dynamic membership rule directly in Entra ID before you assume a Secure Access synchronization bug.
- **Symptom:** SAML SSO expected to drive SWG identity
 - **Root Cause:** AnyConnect **Secure Web Gateway (SWG)** does not support **Security Assertion Markup Language (SAML) authentication** against Entra ID; it uses the same passive authentication mechanism as on-premises AD.
 - **Resolution:** **Do not** design around SAML-driven SWG identity for Entra ID; use passive authentication as documented.
- **Symptom:** User incorrectly shows deactivated
 - **Root Cause:** Entra ID sent **active: false** because the user fell out of an assigned group scope, or an active attribute mapping is misconfigured.
 - **Resolution:** Check whether the user was removed from a scoped group; verify the active mapping (commonly must evaluate as **Not([isSoftDeleted])**).
- **Symptom:** **Application** quarantined, all provisioning halted
 - **Root Cause:** Target **application** returned repeated non-SCIM-compliant responses.
 - **Resolution:** Check the Enterprise **Application** provisioning status for a quarantine flag before you assume individual user failures.
- **Symptom:** Initial provisioning cycle fails outright
 - **Root Cause:** Transient synchronization failure on the first run.
 - **Resolution:** Click **Restart Provisioning** from the Overview page to force Entra ID to attempt the initial synchronization again.
- **Symptom:** Duplicate users merge unexpectedly
 - **Root Cause:** Two source identities share the same email or User Principal Name (UPN).
 - **Resolution:** Ensure email and UPN uniqueness in the source directory; verify the mail attribute comes from a verified domain.
- **Symptom:** Attribute stops updating after a schema change

- **Root Cause:** Attribute type changed on the target side (for example, string to boolean) but the Entra ID mapping was not updated.
- **Resolution:** Manually correct the type in **Advanced Settings** under **Attribute Mappings**.
- **Symptom:** Manager reference never populates
 - **Root Cause:** A user was in scope before their manager was; provisioning does not automatically backfill.
 - **Resolution:** Restart provisioning to force full re-evaluation of all users in scope.

IBM Security Verify Specific Issues

- **Symptom:** Users provision but groups never appear in Secure Access
 - **Root Cause:** Verify custom SCIM connector is issuing User operations only; no **POST /Groups** calls are ever sent (account-provisioning capability gap, not a mapping error).
 - **Resolution:** Capture a connector trace and confirm whether any **/Groups** calls occur; if none, provision groups via the Cisco AD Connector, CSV import, or a scheduled script against the **Secure Access** SCIM endpoint.
- **Symptom:** Group membership update fails with 400 or 404
 - **Root Cause:** **members[].value** references Verify internal user IDs instead of the SCIM **ID** **Secure Access** returned at user creation.
 - **Resolution:** Correct the members mapping to use the **Secure Access** SCIM ID and run a full synchronization again.
- **Symptom:** Groups appear but are empty
 - **Root Cause:** Group pushed before its member users existed in **Secure Access**; membership **PATCH** referenced unknown users.
 - **Resolution:** Run a full synchronization again now that users exist; ensure synchronization ordering creates users before groups.
- **Symptom:** SAML login loops or repeated redirects
 - **Root Cause:** Verify IdP endpoint is proxied or decrypted by the SWG, which breaks the authentication flow.
 - **Resolution:** Bypass the Verify IdP URL from **SAML or decryption** (external domains list or selective decryption).
- **Symptom:** User authenticates via SAML but no user-based policy matches
 - **Root Cause:** SAML **NameID** does not match the provisioned user **authName**.
 - **Resolution:** Align the **NameID** > format in the Verify SAML application with the **authName**.

attribute mapping (typically email or UPN); test again.

- **Symptom:** Provisioning stops working after weeks or months of stability
 - **Root Cause:** SCIM token was rotated **or** expired in Secure Access but not updated in the Verify connector.
 - **Resolution:** Refresh the token in **Secure Access** and update it in the Verify custom **application**; calendar the refresh cadence.
- **Symptom:** Duplicate users created on **re-synchronization**
 - **Root Cause:** **externalId** mapped to a mutable or non-unique attribute (**for example**, display name, changeable email).
 - **Resolution:** Map **externalId** to an immutable identifier (Verify user ID or **objectGUID**); clean up duplicates and synchronize again.
- **Symptom:** Deactivated Verify users remain active in **Secure Access**
 - **Root Cause:** Suspend action not mapped to **active:false**, or deactivate operation disabled in the connector.
 - **Resolution:** Enable the deactivate operation and map suspend to **active:false**; verify with a test user.
- **Symptom:** Attribute changes in Verify **do not** propagate
 - **Root Cause:** User or attribute out of provisioning policy scope, or update operation disabled.
 - **Resolution:** Review the application provisioning policy or entitlements; enable updates; trigger a manual synchronization.
- **Symptom:** **Secure Access** rejects requests with schema **or** 501-style errors
 - **Root Cause:** Non-SCIM-compliant payload (missing schemas array, wrong URN, unsupported operation).
 - **Resolution:** Reproduce with the baseline **curl** test; correct the payload **or** mapping; escalate to IBM if the connector emits the malformed request.
- **Symptom:** SWG identity missing for roaming users despite SAML working
 - **Root Cause:** Expecting SAML to drive identity for a deployment mode that uses passive **or** agent-based identity.
 - **Resolution:** Confirm the identity acquisition method for each deployment mode against Secure Access documentation; do not design SAML as the sole identity source.

Generic SCIM Issues

These are not Cisco-specific but consistently appear in Secure Access deployments because the underlying transport is standard SCIM 2.0:

- **Quarantine states mask individual errors:** If synchronization appears to have stopped entirely rather than failing per-user, check for an application-level quarantine or suspension state before you investigate individual attribute issues.
- **409 Conflict on deactivation:** A common pattern where the IdP attempts to deactivate a user and the target throws a conflict. This is usually an active attribute mapping or group-scope issue, not a true system error.
- **Blank or cleared fields do not always propagate:** Some SCIM server implementations retain the last non-null value; when you clear a field in the IdP, it can require you to push a placeholder value through first.
- **URL or configuration changes silently invalidate authentication:** Any change to the SCIM endpoint URL typically requires you to supply the bearer token again. Errors surface as invalid URL even when the real issue is a stale token.
- **No native webhook or event stream:** Automation that expects real-time push notifications on user or policy changes must poll the Reporting API or integrate via Cisco XDR instead. Secure Access does not emit outbound provisioning webhooks.

Escalate to Cisco TAC with provisioning logs from the IdP side if the previous steps do not resolve the issue. Backend provisioning logs on the Secure Access side generally require TAC access to pull.

Cause

The SCIM provisioning integration failed to push one or more records due to an expired bearer token, attribute mapping mismatch, missing target group, or insufficient provisioning scope.

Related Content

- Cisco: [Provision Users and Groups to Secure Access via Entra ID](#)
- Cisco: [Provision Users and Groups to Secure Access via OKTA](#)
- Microsoft Learn: *Known issues with SCIM 2.0 protocol compliance – Microsoft Entra ID*
- Microsoft Learn: *Troubleshoot Microsoft Entra ID SCIM API errors*
- Configure SAML SSO in the identity provider: <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>

- Provisioning for custom (SCIM) applications: <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- Provisioning and governance overview (generic SCIM connector): <https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- On-premises provisioning bridge (AD/LDAP sources): <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>