# Cisco Secure Access Identity Synchronization with Active Directory and Microsoft EntraID

## Contents

## Issue

Users experienced challenges when attempting to provision users and groups from two identity sources with the same domain name in Cisco Secure Access. The specific scenario involved synchronizing identities from both on-premises Active Directory and Microsoft EntraID (formerly Azure AD) where both sources used the same domain name (e.g., domain.com).

The primary concerns were:

- Understanding how identity ownership and group membership mapping behave when the same users and groups exist in both identity sources
- Ensuring consistent secure access policy enforcement for hybrid users accessing both on-premises and cloud resources
- Maintaining internal IP visibility for users in this hybrid identity configuration
- Determining if concurrent synchronization from both sources would cause issues in a production environment

Documentation indicated that "Concurrent synchronization of the same users and groups from the Cisco AD Connector and the Cisco User Management for Secure Access app is not supported and leads to inconsistent access rule enforcement."

## Environment

- Cisco Secure Access with AD Connector and EntraID integration
- On-premises Active Directory with domain name matching EntraID domain
- Microsoft EntraID (Azure AD) with same domain name as on-premises AD
- SAML SSO configuration for identity federation

- Secure Web Gateway (SWG) module for policy enforcement
- Hybrid environment requiring access to both on-premises and cloud resources

# Resolution

Following behavior was confirmed for concurrent synchronization from both Active Directory and EntraID sources:

## Group Synchronization Behavior

When synchronizing groups with the same name from both sources:

- Two separate group objects are created in Cisco Secure Access - one from each source
- Groups can be distinguished by their source prefix in access policies
- On-premises AD groups appear as: **AD-Domain/GroupName**
- EntraID groups appear as: **GroupName**

Lab verification showed successful synchronization with the message "Success. <<<< Synced" for groups from multiple EntraID domains.

## User Synchronization Behavior

When synchronizing users with the same user ID from both sources:

- The user identity gets overwritten during synchronization
- Only one unique user ID remains visible in Secure Access
- The final synchronization source determines the user's attributes and group memberships
- EntraID synchronization typically takes precedence over on-premises AD when both are configured

## Access Policy Configuration

Both group types can be utilized in access policies:

- Reference on-premises AD groups using the full path: **AD-Domain/GroupName**
- Reference EntraID groups using the simple name: **GroupName**
- Policies can differentiate between users based on their group membership source

**Following Set up works well for Many Customers**.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

# Cause

During our testing, we confirmed that whenever a user is synchronized from the On-Premises AD Connector, it effectively "claims" that identity in the Umbrella dashboard. If that same user already exists via the Azure AD sync, the On-Premises sync will overwrite the existing EntraID user data.

This behavior is a documented limitation. According to official Cisco technical documentation: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

> "Concurrent synchronization of the same user and group identities from the Umbrella AD Connector and the Cisco Umbrella Azure AD app is not supported and leads to inconsistent policy enforcement."

Conclusion: The desired setup (VA visibility for users existing in both Azure and On-Prem) is confirmed to be an **unsupported** configuration.The path forward requires using Roaming Clients to ensure consistent identity enforcement.

# Related Content

- Provision Identities from Azure AD - Cisco Umbrella Documentation
- Cisco Technical Support & Downloads