Migrate Secure Access AD Connectors from Legacy Authentication to API Authentication

Contents

Issue

Organizations using Cisco Secure Access with Active Directory (AD) Connectors receive notifications indicating that API Authentication is recommended for Active Directory and Virtual Appliances, with legacy authentication set to expire on May 29, 2026. Users need configuration assistance to migrate from legacy authentication to API Authentication before the expiration date and want to understand the potential impact on AD and Virtual Appliance synchronization during the migration process. The primary concern is whether implementing this change during working hours could cause failures in AD and VA sync operations that can affect identity and policy-dependent operations.

Environment

- Cisco Secure Access (formerly Cisco Umbrella)
- Active Directory Connectors deployed
- Legacy authentication method currently in use
- API Authentication migration required before May 29, 2026
- AD-only environment (without Virtual Appliances in some cases)

Resolution

The migration from legacy authentication to API Authentication involves generating API keys in the Secure Access portal and configuring them properly. The process requires creating both Admin API keys and Client API keys for the AD Connectors and Virtual Appliances.

Step 1: Generate Admin API Key

Navigate to **Admin > API Keys** in the Secure Access portal and generate a new **Admin API Key** and

Admin Key Secret. Store these credentials securely as they are needed to generate the Client API key pair.

Step 2: Generate Client API Key Pair

Navigate to **Users and Groups > Configuration Management > Advanced Settings** and locate the API Authentication section. Enter the **Admin API Key** and **Admin Key Secret** generated in Step 1, then click **Generate Client API Key Pair**. This produces the Client API Key and Client Secret that is used by the AD Connectors and Virtual Appliances.

Step 3: Configure API Authentication in Advanced Settings

Copy the generated **Client API Key** and **Client Secret** into the API Authentication Advanced Settings section of the Secure Access portal. Save these credentials securely as they are required for all AD Connector and Virtual Appliance configurations.

Step 4: Update AD Connectors and Virtual Appliances

Apply the newly generated **Client API Key** and **Client Secret** to all deployed AD Connectors and Virtual Appliances. This ensures they can authenticate properly for registration and health checks using the new API authentication method.

Migration Impact and Best Practices

The generation of API keys in the Secure Access portal is typically not disruptive. However, operational impact occurs during the cutover moment when AD Connectors and Virtual Appliances are updated to use the new Client API Key and Secret.

Expected Impact During Cutover:

- Temporary sync and health-check failures can occur for components still using legacy authentication.
- AD/VA sync lag or failure during the transition window.
- Policy decisions relying on fresh identity/group data can be affected if sync fails.

Recommended Implementation Approach:

- Perform migration during off-working hours or maintenance windows when possible.
- For working hours implementation, use a controlled rolling update approach.
- Update one connector/VA at a time and verify healthy status before proceeding.
- Avoid updating all nodes simultaneously.
- Ensure adequate redundancy with multiple connectors/VAs for rolling updates.

Compatibility and Requirements:

- API Authentication works with AD-only deployments and does not require Virtual Appliances.
- Both legacy and API authentication methods remain active during the migration period.
- AD Connectors must be able to sync with Umbrella via api.opendns.com and transition to api.umbrella.com.

Cause

Cisco Secure Access is transitioning from legacy authentication methods to API Authentication as the standard authentication mechanism. The legacy authentication method has a scheduled deprecation date of May 29, 2026. API Authentication eventually becomes the only supported authentication method, and organizations must migrate before the legacy method expires to avoid service disruptions and potential AD/VA sync failures that could require full reinstallation to recover.

Related Content

- Cisco Secure Access API Authentication Documentation
- Cisco Secure Access Advanced Configuration
- Cisco Secure Access Configuration Management
- Cisco Technical Support & Downloads