Cisco Secure Access SSO Authentication with Duo IdP for Roaming Client SWG Traffic

Contents

Issue

When attempting to use SSO authentication with a Duo IdP for Secure Access SWG (Secure Web Gateway) traffic originating from a roaming client, users are not prompted for Duo SSO authentication and user identity is not populated in the Secure Access dashboard. Although the web traffic matches the intended SWG rule with authentication enabled and traffic is decrypted, the authentication flow does not initiate for roaming client traffic, preventing user-level identification of web activity.

Specifically, the following behavior was observed:

- SWG logging and activity showed the traffic matched the intended SWG rule and destination traffic was decrypted
- Logs and the Secure Access activity view showed only the PC identity and network identity; no Duo/SAML authentication challenge, SSO redirect, or interactive prompt was observed
- Policy entries showed roaming and origin information only; no user identity was present prior to AD join
- When the test VM was joined to Active Directory during troubleshooting, the user identity became visible in Secure Access Activity Search, but the Duo/SAML interactive prompt still did not occur

Environment

- Cisco Secure Access with SWG functionality
- Secure Client version 5.1.13.177
- Duo IdP configured for SSO authentication
- Organization subscription: Secure Access Essentials
- Re-authenticate web proxy interval set to Daily
- No PAC file or VPN in use during tests
- Test environment using roaming computer configuration

Resolution

After comprehensive analysis and testing, it was determined that SSO authentication using SAML is not supported for Secure Access roaming client traffic due to product design limitations. The following troubleshooting steps were performed to confirm this limitation:

Step 1: Live Troubleshooting and Behavior Reproduction

The testing confirmed that SWG policy matching and SSL decryption occurred correctly, but the authentication flow (interactive SAML/Duo SSO redirect and challenge) was not initiated for roaming client traffic.

Step 2: Rule and Source Modifications

The SWG rule source was changed from roaming computer name to a specific user identity during repro attempts. Secure Client services were restarted and policy propagation was observed. These modifications did not resolve the authentication flow issue.

Step 3: Active Directory Join Testing

The test VM was joined to Active Directory to determine the effect on user identity visibility. While this made the user identity visible in Secure Access Activity Search, the Duo/SAML interactive prompt still did not occur, confirming that the issue was not related to user identity visibility alone.

Step 4: DART Bundle Analysis

A DART bundle was collected and analyzed. The analysis confirmed SWG policy application but showed no authentication flow initiation for roaming client traffic, supporting the conclusion that this behavior is by design.

Step 5: Duo IdP Configuration Validation

Independent testing of the Duo IdP metadata and configuration was performed and completed successfully, confirming that the Duo configuration itself was not the source of the issue.

Step 6: Internal Validation

SSO authentication using SAML is not supported for Secure Access roaming client traffic as a product design limitation.

Conclusion: No misconfiguration was found in the setup. The lack of interactive SSO prompting was attributed to an explicit product support limitation rather than a fixable configuration issue.

Cause

The issue is caused by a product design limitation where SSO authentication using SAML (including Duo IdP integration) is not supported for Secure Access roaming client traffic. This is an inherent limitation of the current Secure Access platform architecture and is not related to configuration issues or software bugs.

Related Content

- Cisco Technical Support & Downloads