Cisco Secure Client SAML Authentication Prompt on every attempt with Microsoft Entra ID SSO

Contents

Issue

Cisco Secure Client (AnyConnect) integrated with Microsoft Entra ID for SAML authentication was experiencing multiple authentication-related issues that disrupted the Single Sign-On (SSO) functionality:

- Users were being prompted for authentication on every VPN connection attempt, even when an active Entra ID session existed in the browser
- The client was launching the embedded browser instead of the external/system browser, despite external browser authentication being explicitly enabled for SAML
- Users frequently encountered the error: "Authentication error due to problem with redirecting to SSO URL"
- SSO behavior had changed from the previous working state where users could connect to VPN by simply clicking Connect without authentication prompts

Environment

- Product: Cisco Secure Client (AnyConnect)
- Technology: Secure Access VPN with SAML authentication
- Identity Provider: Microsoft Entra ID (Azure AD)
- Authentication Method: SAML SSO integration
- External Browser authentication enabled for SAML

Resolution

The resolution involved addressing the underlying Azure AD device join state and browser configuration issues that were causing the authentication problems:

Step 1: Diagnose Azure AD Join Status

Execute the following command to check the current Azure AD join status of the affected device:

```
dsregcmd /status
```

Review the output to identify if the device shows AzureAdJoined = NO, which indicates an incorrect Azure AD join state.

Step 2: Correct Azure AD Join State

Run the dsregcmd command to correct the Azure AD join status on the affected device. After executing the appropriate dsregcmd operations,

```
dsregcmd /status
dsregcmd /leave
dsregcmd /join`
```

Verify that the device status shows:

```
AzureAdJoined = YES
```

This correction resolves the underlying authentication state issue that was causing Cisco Secure Client to prompt for credentials on each connection.

Step 3: Reset Default Browser Applications

To address the external browser vs embedded browser behavior issue:

Reset the device's default applications settings to ensure that Cisco Secure Client properly launches the external/system browser for SAML authentication instead of the embedded browser.

```
Settings → Apps → Default apps → Reset
```

Step 4: Verification

After implementing the above changes, verify the following behaviors:

- Cisco Secure Client no longer prompts for password or Windows Hello authentication on each VPN connection
- The client properly launches the external browser for SAML authentication instead of the embedded browser
- SSO functionality is restored, allowing users to connect without repeated authentication prompts when an active Entra ID session exists
- The "Authentication error due to problem with redirecting to SSO URL" error no longer occurs

Cause

The authentication issues were caused by an incorrect Azure AD join state on the affected device, where the device was showing AzureAdJoined = NO instead of the required AzureAdJoined = YES status. This incorrect join state prevented proper SSO token validation and forced Cisco Secure Client to prompt for authentication on each connection attempt.

Additionally, the device's default application settings were misconfigured, causing Cisco Secure Client to launch the embedded browser instead of the external browser for SAML authentication, despite the external browser setting being enabled in the client configuration.

Related Content

- Cisco Technical Support & Downloads