Troubleshoot Secure Access Browser-Based SAML Authentication Displaying Blank White Screen with EntraID

Contents

Issue

When configuring Cisco Secure Access to force browser-based SAML authentication on devices without Cisco Secure Client installed, the authentication process redirects to a blank white screen instead of displaying the EntraID authentication page. This issue occurs specifically in Microsoft Edge normal (non-InPrivate) mode and Google Chrome browsers. The authentication works correctly when using Edge InPrivate mode. The SAML authentication profile has both Decryption and SSO Authentication enabled.

The configured policy structure includes:

- Allow policy for post-authentication users. (source: any user, destination: any)
- Allow SAML authentication policy with SAML authentication profile. (source: endpoint IP, destination: 0.0.0.0 TCP 80,443)
- Allow SAML authentication helper policy with SAML authentication profile. (source: endpoint IP, destination: any)
- Block policy. (source: endpoint IP, destination: any)

Environment

- Cisco Secure Access (Internet Access module)
- EntraID as Identity Provider (IdP)
- Browser-based SAML authentication for devices without Cisco Secure Client
- SAML authentication profile with Decryption and SSO Authentication enabled
- Microsoft Edge and Google Chrome browsers

Resolution

The issue is resolved by adding specific EntraID-related domains to the decryption exclusion list in the SAML authentication profile configuration. This prevents the SSL/TLS decryption process from interfering with the EntraID authentication flow.

Step 1: Add EntraID Domains to Decryption Exclusion List

Configure these four EntraID domains in the decryption exclusion list for the SAML authentication profile:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Step 2: Apply Configuration to SAML Policies

Ensure the decryption exclusion settings are applied to both:

- The Allow SAML authentication policy. (source: endpoint IP, destination: 0.0.0.0 TCP 80,443)
- The Allow SAML authentication helper policy. (source: endpoint IP, destination: any)

Step 3: Verify Resolution

After applying the decryption exclusion configuration, test the authentication flow:

- Microsoft Edge (normal mode): Can successfully redirect to EntraID authentication page.
- Google Chrome: Can successfully redirect to EntraID authentication page.
- Both browsers can consistently display the EntraID authentication input screen.

Cause

The blank white screen occurs because the SSL/TLS decryption process in Cisco Secure Access interferes with the EntraID authentication flow when decryption is enabled for the SAML authentication profile. The decryption process breaks the secure communication between the browser and EntraID authentication servers, preventing the authentication page from loading properly. InPrivate mode works because it handles SSL/TLS sessions differently, bypassing the decryption interference. Adding the EntraID domains to the decryption exclusion list allows the authentication traffic to pass through without decryption, maintaining the integrity of the secure authentication flow.

Related Content

- Cisco Technical Support & Downloads