Troubleshoot SWG SAML Authentication Cookie Surrogate Issue for Secure Access

Contents

Issue

Users accessing web applications through Cisco Secure Access experience authentication failures when applications perform cross-domain redirects or fetch resources from multiple related domains. The issue manifests as:

- Web applications failing to initialize properly after SAML authentication.
- Requests to cross-domain resources (CORS error) being blocked by default deny rules.
- Activity logs showing requests attributed to network or tunnel identity instead of authenticated user identity.
- CORS policy errors appearing in browser console for redirected requests.
- Applications working correctly on physical machines when using IP surrogate but failing on Citrix virtual desktop environments using Cookie surrogate.

The problem occurs specifically when cookie surrogate authentication is used in virtualized environments, where redirected requests lose the user-to-cookie mapping during cross-domain resource fetches.

Environment

- Cisco Secure Access with SAML authentication configured
- Cookie Surrogate authentication enabled for Citrix virtual desktop environments
- IP Surrogate authentication used for physical machines
- Web applications that perform cross-domain redirects (CORS error in Web developer tool console logs)
- Mixed environment with both physical and virtual desktop infrastructure

Resolution

The issue is resolved by implementing IP Surrogate bypass for the affected network ranges, allowing proper user identity attribution even during cross-domain redirects.

Step 1: Navigate to IP Surrogate Configuration

Access the Cisco Secure Access dashboard and navigate to **Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate**.

Step 2: Enable Internal Network Bypass

Add the affected network ranges to the Internal Network bypass configuration. This allows the system to maintain user identity attribution for requests originating from these networks.

Step 3: Test Application Access

After implementing the IP Surrogate, test the affected applications to verify that:

- Cross-domain resource requests are properly attributed to user identity
- Applications initialize successfully without CORS errors
- Activity logs show user identity instead of network or tunnel based identity for all requests

Step 5: Monitor Activity Reports

Use **Monitor > Activity Search** to verify that requests are now properly attributed to authenticated users rather than showing as network or tunnel based identity.

Cause

This behavior is expected due to the nature of SAML authentication combined with Cookie Surrogate in virtualized environments. When web applications perform cross-domain redirects or fetch resources from multiple related domains, the redirected requests possibly does not carry the surrogate cookie in a way that Cisco Secure Access can associate back to the authenticated user session.

The root cause occurs because:

- Cookie Surrogate relies on browser cookie propagation across redirects.
- Cross-domain security policies (CORS) can strip cookies during 307/redirect scenarios.
- Browser security measures prevent cookie sharing across different domains.
- Virtual desktop environments handle cookie propagation differently than physical machines.

Once the user-to-cookie mapping is lost, Secure Access cannot resolve the request to the authenticated user, causing the request to be attributed only to the registered network/different identity as source and subsequently blocked by default deny rules.

Related Content

- Cisco Technical Support & Downloads