# 對安全訪問的SWG SAML身份驗證Cookie替代問題進行故障排除

## 目錄

## 問題

當應用程式執行跨域重定向或從多個相關域獲取資源時，通過Cisco Secure Access訪問Web應用程式的使用者會遇到身份驗證失敗。問題表現為：

- Web應用程式在SAML身份驗證後無法正確初始化。
- 對跨域資源的請求（CORS錯誤）被預設拒絕規則阻止。
- 顯示歸屬於網路或隧道標識而非經過身份驗證的使用者標識的請求的活動日誌。
- 瀏覽器控制檯中出現重定向請求的CORS策略錯誤。
- 使用IP代理時，應用程式在物理電腦上正常運行，但在使用Cookie代理的Citrix虛擬案頭環境中失敗。

當在虛擬環境中使用cookie替代身份驗證時，問題會特別出現，在虛擬環境中，重定向請求會在跨域資源讀取期間丟失使用者到cookie的對映。

## 環境

- 配置了SAML身份驗證的Cisco安全訪問
- 為Citrix虛擬案頭環境啟用了Cookie代理身份驗證
- 用於物理電腦的IP代理身份驗證
- 執行跨域重定向的Web應用程式（Web開發人員工具控制檯日誌中出現CORS錯誤）
- 具有物理和虛擬案頭基礎架構的混合環境

# 解析

通過為受影響的網路範圍實施IP代理旁路，從而在跨域重定向期間允許正確的使用者身份屬性來解決問題。

## 步驟 1:導覽至IP Surrogate Configuration

訪問Cisco Secure Access控制面板並導航至Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate。

## 步驟 2:啟用內部網路旁路

將受影響的網路範圍新增到內部網路旁路配置中。這允許系統維護來自這些網路的請求的使用者身份屬性。

## 步驟 3:測試應用程式訪問

實施IP代理後，測試受影響的應用程式以驗證：

- 跨域資源請求正確歸屬於使用者身份
- 應用程式成功初始化而沒有CORS錯誤
- 活動日誌顯示所有請求的使用者身份，而不是基於網路或隧道的身份

## 步驟 5:監控活動報告

使用Monitor > Activity Search驗證請求現在是否正確歸屬於經過身份驗證的使用者，而不是顯示為基於網路或隧道的標識。

# 原因

出現此行為的原因在於虛擬化環境中結合Cookie代理的SAML身份驗證的性質。當Web應用執行跨域重定向或從多個相關域獲取資源時，重定向請求可能沒有以思科安全訪問可以關聯回已驗證使用者會話的方式承載代理cookie。

出現根本原因的原因如下：

- Cookie替代依賴於瀏覽器在重定向間的cookie傳播。
- 跨域安全策略(CORS)可以在307/重定向場景期間剝離cookie。
- 瀏覽器安全措施可防止在不同域之間共用cookie。
- 虛擬案頭環境處理cookie傳播的方式與物理機不同。

一旦使用者到cookie的對映丟失，安全訪問便無法將請求解析為經過身份驗證的使用者，導致請求僅歸屬於註冊網路/作為源的不同身份，隨後被預設拒絕規則阻止。

# 相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。