排除安全訪問瀏覽器型SAML身份驗證故障，顯示空白的白屏和EntraID

目錄

問題

當配置思科安全訪問以在未安裝思科安全客戶端的裝置上強制基於瀏覽器的SAML身份驗證時，身份驗證過程重定向到空白的白色螢幕，而不是顯示EntraID身份驗證頁面。此問題專門發生在Microsoft Edge常規（非InPrivate）模式和Google Chrome瀏覽器中。使用邊緣InPrivate模式時，身份驗證工作正常。SAML身份驗證配置檔案同時啟用解密和SSO身份驗證。

配置的策略結構包括：

- 允許身份驗證後使用者的策略。(來源：任何使用者，目標：any)
- 允許使用SAML身份驗證配置檔案的SAML身份驗證策略。(來源：終端IP，目標：0.0.0.0(TCP 80,443)
- 允許使用SAML身份驗證配置檔案的SAML身份驗證幫助程式策略。(來源：終端IP，目標：any)
- 阻止策略。(來源：終端IP，目標：any)

環境

- 思科安全存取（網際網路存取模組）
- EntraID as Identity Provider(IdP)
- 適用於沒有思科安全使用者端的裝置的基於瀏覽器的SAML驗證
- 已啟用解密和SSO身份驗證的SAML身份驗證配置檔案
- Microsoft Edge和Google Chrome瀏覽器

解析

通過將特定的EntraID相關域新增到SAML身份驗證配置檔案配置中的解密排除清單可以解決此問題。這可防止SSL/TLS解密過程干擾EntraID身份驗證流程。

步驟 1:將EntraID域新增到解密排除清單

在SAML身份驗證配置檔案的解密排除清單中配置以下四個EntraID域：

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

步驟 2:將配置應用於SAML策略

確保將解密排除設定應用於兩者：

- 允許SAML身份驗證策略。(來源：終端IP，目標：0.0.0.0(TCP 80,443)
- 允許SAML身份驗證幫助程式策略。(來源：終端IP，目標：any)

步驟 3:驗證解析度

應用解密排除配置後，測試身份驗證流程：

- Microsoft Edge（正常模式）：可以成功重定向到EntraID身份驗證頁面。
- Google Chrome:可以成功重定向到EntraID身份驗證頁面。
- 兩個瀏覽器都可以一致顯示EntraID身份驗證輸入螢幕。

原因

出現空白白屏的原因是，當為SAML身份驗證配置檔案啟用解密時，思科安全訪問中的SSL/TLS解密過程會干擾EntraID身份驗證流程。解密過程會中斷瀏覽器和EntraID身份驗證伺服器之間的安全通訊，從而阻止正確載入身份驗證頁面。InPrivate模式工作正常，因為它會以不同方式處理SSL/TLS會話，從而繞過解密干擾。將EntraID域新增到解密排除清單允許身份驗證流量在不解密的情況下通過，從而維護安全身份驗證流的完整性。

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）。