每次嘗試使用Microsoft Entra ID SSO時出現Cisco安全客戶端SAML身份驗證提示

目錄

問題

與用於SAML身份驗證的Microsoft Entra ID整合的Cisco Secure Client(AnyConnect)遇到多個身份驗證相關問題，導致單點登入(SSO)功能中斷：

- 每次VPN連線嘗試都會提示使用者進行身份驗證，即使瀏覽器中存在活動的Entra ID會話也是如此
- 儘管已為SAML顯式啟用外部瀏覽器身份驗證，但客戶端正在啟動嵌入式瀏覽器，而不是外部/系統瀏覽器
- 使用者經常遇到錯誤："由於重定向到SSO URL時出現問題導致的身份驗證錯誤"
- SSO行為與先前的工作狀態不同，使用者只需按一下Connect即可連線到VPN，而無需身份驗證提示

環境

- 產品:思科安全使用者端(AnyConnect)
- 技術：採用SAML驗證的安全存取VPN
- 身份提供程式：Microsoft Entra ID(Azure AD)
- 身份驗證方法：SAML SSO整合
- 為SAML啟用的外部瀏覽器身份驗證

解析

解決方案涉及解決導致身份驗證問題的基礎Azure AD裝置加入狀態和瀏覽器配置問題：

步驟 1:診斷Azure AD加入狀態

執行以下命令檢查受影響裝置的當前Azure AD加入狀態：

```
dsregcmd /status
```

檢視輸出以確定裝置是否顯示AzureAdJoined = NO，這表示Azure AD加入狀態不正確。

步驟 2:正確的Azure AD加入狀態

運行dsregcmd命令以更正受影響裝置上的Azure AD加入狀態。執行適當的dsregcmd操作後，

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

驗證裝置狀態是否顯示：

```
AzureAdJoined = YES
```

此更正解決了導致Cisco安全客戶端在每個連線上提示輸入憑據的基本身份驗證狀態問題。

步驟 3:重置預設瀏覽器應用程式

要解決外部瀏覽器與嵌入式瀏覽器的行為問題：

重置裝置的預設應用設定，以確保Cisco安全客戶端正確啟動外部/系統瀏覽器進行SAML身份驗證

，而不是嵌入式瀏覽器。

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

步驟 4:驗證

實施上述更改後，驗證以下行為：

- Cisco Secure Client不再在每個VPN連線上提示密碼或Windows Hello身份驗證
- 客戶端正確啟動用於SAML身份驗證的外部瀏覽器，而不是嵌入式瀏覽器
- 恢復了SSO功能，允許使用者在存在活動Entra ID會話時進行連線，而無需重複身份驗證提示
- 不再出現「Authentication error due to problem to SSO URL（由於重定向到SSO URL時出現問題導致的身份驗證錯誤）」錯誤

原因

身份驗證問題是由受影響裝置上的Azure AD加入狀態不正確引起的，其中裝置顯示AzureAdJoined = NO而不是所需的AzureAdJoined = YES狀態。這種不正確的連線狀態阻止了正確的SSO令牌驗證，並強制思科安全客戶端在每次連線嘗試時提示進行身份驗證。

此外，裝置的預設應用設定配置錯誤，導致Cisco安全客戶端啟動嵌入式瀏覽器而不是外部瀏覽器進行SAML身份驗證，儘管客戶端配置中啟用了外部瀏覽器設定。

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）。