

如何使用SSO (以透明方式傳送憑證) 正確設定NTLM?

目錄

問題：

症狀:使用NTLM身份驗證時，瀏覽器會提示輸入憑據。

環境:思科網路安全裝置(WSA),AsyncOS的所有版本

有幾個因素會影響客戶端是否自動傳送其憑據 (SSO — 單點登入) ，或提示終端使用者手動輸入其憑據。

嘗試使用SSO實施NTLM時，請驗證以下各項：

WSA身份驗證配置：

驗證WSA是否設定為使用NTLMSSP，而不是僅使用NTLM Basic

在GUI的Web Security Manager > Identities頁面下可以找到此設定。編輯適當的身份，然後選中Define Members by Authentication > Authentication Schemes設定。

選擇以下選項之一：

NTLMSSP使客戶端能夠安全透明地將憑證傳送到Web代理。

NTLM Basic允許客戶端在提示輸入憑證時以純文字檔案格式傳送使用者名稱和密碼。

選擇使用基本或NTLMSSP選項 (推薦) 時，客戶端會選擇最佳可用方法。如果客戶端支援NTLMSSP，它將使用此方法，並且所有其他瀏覽器都將使用「基本」。這允許最大程度的相容性。

客戶端信任：

如果客戶端不信任WSA，它將不會透明地傳送其憑據。以下是幫助排除客戶端不信任WSA環境的指導原則。

客戶端不信任身份驗證重定向URL (僅透明部署)

在透明部署中，WSA必須將客戶端重定向到自身才能執行身份驗證。客戶端可能信任也可能不信任此重定向位置。

預設情況下，WSA重定向到P1的FQDN (或者M1介面，如果用於代理資料)。由於這是一個FQDN，Internet Explorer不會信任它，因為它認為這是一個網路之外的資源。

有兩種方法可以使Internet Explorer信任WSA: