SSO を使って正しく (クレデンシャルが透過的に送信されるように) NTLM を設定するには、どうすればよいですか。

目次

質問：

症状： NTLM 認証の使用時に、ブラウザからクレデンシャルの入力を求められます。

環境： Cisco Web セキュリティ アプライアンス (WSA)、AsyncOS のすべてのバージョン

クライアントからクレデンシャルが自動的に送信されるか (SSO：シングル サインオン)、またはエンドユーザに対し各自のクレデンシャルを手動で入力するように求められるかどうかに影響する要因は多数あります。
SSO を使用して NTLM を実装するときに、次の項目を確認します。

WSA 認証設定：

NTLM Basic だけではなく、NTLMSSP を使用するように WSA が設定されていることを確認します。

この設定は、GUI の [Web Security Manager] > [Identities] ページにあります。 適切なアイデンティティを編集し、[Define Members by Authentication] > [Authentication Schemes] **設定を確認します。**

次のオプションのいずれかを選択します。

NTLMSSP により、クライアントがクレデンシャルをセキュアかつ透過的に Web プロキシに送信できるようになります。

NTLM Basic では、クライアントがクレデンシャルを求められたときに、ユーザ名とパスワードをプレーン テキストで送信できます。

クライアントは、[Use Basic or NTLMSSP] オプションが選択されている場合に使用できる最良の方式を選択します (推奨)。 クライアントで NTLMSSP がサポートされている場合、クライアントはこの方式を使用し、その他のすべてのブラウザは Basic を使用します。 これにより互換性を最大限に引き出すことができます。

クライアントの信頼：

クライアントは、WSA を信頼しない場合にはクレデンシャルを透過的に送信しません。 次に、クライアントが WSA を信頼しない環境をトラブルシューティングする際に役立つガイドラインを示します。

クライアントは認証リダイレクト URL を信頼しません（透過的な導入のみ）。

透過的な導入では、WSA は認証を実行するため、クライアントをそれ自体にリダイレクトする必要があります。 クライアントは、リダイレクト先のロケーションを信頼する場合もあれば、信頼しない場合もあります。

デフォルトでは、WSA は P1 の FQDN（プロキシ データに使用されている場合は M1 インターフェイス）にリダイレクトします。 これは FQDN であるため、Internet Explorer はこれをネットワーク外部のリソースと認識し、信頼しません。

Internet Explorer に WSA を信頼させる方法は、以下の 2 通りあります。