Microsoft Entra ID SSOを使用した試行のたびにCisco Secure Client SAML認証プロンプトが表示される

内容

お問い合わせ内容

SAML認証用のMicrosoft Entra IDと統合されたCisco Secure Client(AnyConnect)で、シングルサインオン(SSO)機能を中断する認証関連の問題が複数発生していました。

- ブラウザにアクティブなEntra IDセッションが存在する場合でも、VPN接続が試行されるたびにユーザに認証を求めるプロンプトが表示されていました
- 外部ブラウザの認証がSAMLに対して明示的に有効になっているにもかかわらず、クライアントは外部/システムブラウザではなく組み込みブラウザを起動していました
- ユーザで「Authentication error due to problem with redirecting to SSO URL」というエラーが頻繁に発生する
- SSOの動作は、ユーザが認証プロンプトなしでConnectをクリックするだけでVPNに接続できた以前の動作状態から変更されています

環境

- 製品：Cisco Secure Client(AnyConnect)
- テクノロジー：SAML認証によるセキュアアクセスVPN
- IDプロバイダー： Microsoft Entra ID (Azure AD)
- 認証方式：SAML SSO統合
- SAMLに対する外部ブラウザ認証の有効化

解決策

この問題の解決には、認証の問題を引き起こしていた、基盤となるAzure ADデバイスの参加状態とブラウザー構成の問題の解決が含まれていました：

手順1: Azure AD参加ステータスの診断

次のコマンドを実行して、影響を受けるデバイスの現在のAzure AD参加状態を確認します。

```
dsregcmd /status
```

出力を確認して、デバイスにAzureAdJoined = NOと表示されるかどうかを確認します。これは、Azure ADの参加状態が正しくないことを示します。

手順2: Azure ADの参加状態を修正する

dsregcmdコマンドを実行して、影響を受けるデバイスのAzure AD参加状態を修正します。適切なdsregcmd操作を実行した後、

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

デバイスのステータスに次のように表示されることを確認します。

```
AzureAdJoined = YES
```

この修正により、Cisco Secure Clientが各接続でクレデンシャルの入力を求める原因となっていた、基盤となる認証状態の問題が解決されます。

ステップ3：デフォルトのブラウザアプリケーションのリセット

外部ブラウザと組み込みブラウザの動作の問題に対処するには、次の手順を実行します。

デバイスのデフォルトアプリケーション設定をリセットして、Cisco Secure Clientが組み込みブラウザの代わりにSAML認証用の外部/システムブラウザを正しく起動するようにします。

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

ステップ4：検証

上記の変更を実装した後、次の動作を確認します。

- Cisco Secure Clientが各VPN接続でパスワードまたはWindows Hello認証のプロンプトを表示しなくなりました
- クライアントは、組み込みブラウザの代わりに、SAML認証用の外部ブラウザを適切に起動します
- SSO機能が復元され、アクティブなEntra IDセッションが存在する場合に、ユーザが認証プロンプトを繰り返さずに接続できるようになります
- 「Authentication error due to problem with redirecting to SSO URL」エラーが発生しなくなりました

原因

認証の問題は、影響を受けるデバイスでAzure ADの参加状態が正しくないことが原因です。デバイスでは、必須のAzureAdJoined = YESの状態ではなく、AzureAdJoined = NOと表示されていました。この不正な結合状態により、SSOトークンが正しく検証されず、接続が試行されるたびにCisco Secure Clientで認証を要求するように強制されました。

また、デバイスのデフォルトアプリケーション設定が誤って設定されているため、クライアント設定で外部ブラウザ設定が有効になっていても、Cisco Secure ClientがSAML認証用の外部ブラウザの代わりに組み込みブラウザを起動する原因となっていました。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。