Cisco Secure Client SAML-Authentifizierungsaufforderung bei jedem Versuch mit Microsoft Entra ID SSO

Inhalt

Problem

Bei Cisco Secure Client (AnyConnect), der in Microsoft Entra ID für die SAML-Authentifizierung integriert war, traten mehrere authentifizierungsbezogene Probleme auf, die die Single Sign-On (SSO)-Funktion unterbrachen:

- Benutzer wurden bei jedem VPN-Verbindungsversuch zur Authentifizierung aufgefordert, selbst wenn im Browser eine aktive Entra-ID-Sitzung vorhanden war.
- Der Client startete den eingebetteten Browser anstelle des externen Browsers bzw. des System-Browsers, obwohl die externe Browser-Authentifizierung explizit für SAML aktiviert wurde.
- Benutzer haben häufig den folgenden Fehler festgestellt: "Authentifizierungsfehler aufgrund eines Problems mit der Umleitung zur SSO-URL"
- Das SSO-Verhalten hatte sich gegenüber dem vorherigen Arbeitsstatus, in dem Benutzer eine Verbindung mit VPN herstellen konnten, geändert, indem sie einfach auf Verbinden ohne Authentifizierungsaufforderungen klickten.

Umwelt

- Produkt: Cisco Secure Client (AnyConnect)
- Technologie: Secure Access VPN mit SAML-Authentifizierung
- Identitätsanbieter: Microsoft Entra ID (Azure AD)
- Authentifizierungsmethode: SAML SSO-Integration

- Authentifizierung über externen Browser für SAML aktiviert

Auflösung

Die Lösung umfasste die Behebung des zugrunde liegenden Azure AD-Geräte-Join-Zustands und der Browserkonfigurationsprobleme, die Authentifizierungsprobleme verursachten:

Schritt 1: Azure AD-Join-Status diagnostizieren

Führen Sie den folgenden Befehl aus, um den aktuellen Azure AD-Join-Status des betroffenen Geräts zu überprüfen:

```
dsregcmd /status
```

Überprüfen Sie die Ausgabe, um festzustellen, ob auf dem Gerät AzureAdJoined = NO angezeigt wird. Dies weist auf einen falschen Azure AD-Join-Status hin.

Phase 2: Azure AD-Beitrittsstatus korrigieren

Führen Sie den Befehl dsregcmd aus, um den Azure AD-Join-Status auf dem betroffenen Gerät zu korrigieren. Nach dem Ausführen der entsprechenden dsregcmd-Operationen

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

Überprüfen Sie, ob der Gerätestatus angezeigt wird:

```
AzureAdJoined = YES
```

Mit dieser Korrektur wird das zugrunde liegende Problem mit dem Authentifizierungsstatus behoben, das dazu geführt hat, dass der Cisco Secure Client bei jeder Verbindung nach Anmeldeinformationen gefragt hat.

Schritt 3: Standardbrowseranwendungen zurücksetzen

So beheben Sie das Problem mit dem Verhalten eines externen Browsers im Vergleich zum Verhalten eines eingebetteten Browsers:

Setzen Sie die Anwendungseinstellungen des Geräts zurück, um sicherzustellen, dass der Cisco Secure Client den externen Browser/Systembrowser für die SAML-Authentifizierung anstelle des eingebetteten Browsers ordnungsgemäß startet.

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

Schritt 4: Verifizierung

Überprüfen Sie nach dem Implementieren der oben genannten Änderungen das folgende Verhalten:

- Der Cisco Secure Client fordert nicht mehr bei jeder VPN-Verbindung zur Eingabe eines Kennworts oder zur Windows Hello-Authentifizierung auf
- Der Client startet den externen Browser zur SAML-Authentifizierung ordnungsgemäß, nicht den integrierten Browser
- Die SSO-Funktionalität wird wiederhergestellt, sodass Benutzer ohne wiederholte Authentifizierungsaufforderungen eine Verbindung herstellen können, wenn eine aktive Entra-ID-Sitzung vorhanden ist.
- Der Fehler "Authentication error due to problem with redirecting to SSO URL" (Authentifizierungsfehler aufgrund von Problemen mit der Umleitung zur SSO-URL) tritt nicht mehr auf.

Ursache

Die Authentifizierungsprobleme wurden durch einen falschen Azure AD-Join-Status auf dem betroffenen Gerät verursacht, wobei auf dem Gerät AzureAdJoined = NO anstelle des erforderlichen AzureAdJoined = YES-Status angezeigt wurde. Dieser falsche Join-Zustand verhinderte eine ordnungsgemäße Überprüfung des SSO-Tokens und zwang Cisco Secure Client, bei jedem Verbindungsversuch zur Authentifizierung aufzufordern.

Darüber hinaus waren die Standardanwendungseinstellungen des Geräts falsch konfiguriert, sodass der Cisco Secure Client den integrierten Browser anstelle des externen Browsers für die SAML-Authentifizierung startete, obwohl die externe Browsereinstellung in der Clientkonfiguration aktiviert war.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.