每次尝试使用Microsoft Entra ID SSO时出现Cisco安全客户端SAML身份验证提示

目录

问题

与Microsoft Entra ID集成的Cisco Secure Client(AnyConnect)进行SAML身份验证时遇到了多个身份验证相关问题，导致单点登录(SSO)功能中断：

- 每次VPN连接尝试都会提示用户进行身份验证，即使浏览器中存在活动的Entra ID会话也是如此
- 客户端正在启动嵌入式浏览器，而不是外部/系统浏览器，尽管已明确为SAML启用外部浏览器身份验证
- 用户经常遇到错误："由于重定向到SSO URL时出现问题导致的身份验证错误"
- SSO行为与之前的工作状态不同，在之前的工作状态下，用户只需点击Connect即可连接到VPN，无需身份验证提示

环境

- 产品:思科安全客户端(AnyConnect)
- 技术：采用SAML身份验证的安全访问VPN
- 身份提供程序：Microsoft Entra ID(Azure AD)
- 认证方法:SAML SSO集成
- 为SAML启用的外部浏览器身份验证

分辨率

解决方案涉及解决导致身份验证问题的基础Azure AD设备加入状态和浏览器配置问题：

步骤 1：诊断Azure AD加入状态

执行以下命令检查受影响设备的当前Azure AD加入状态：

```
dsregcmd /status
```

查看输出以确定设备是否显示AzureAdJoined = NO，这表示不正确的Azure AD加入状态。

步骤 2：正确的Azure AD加入状态

运行dsregcmd命令以更正受影响设备上的Azure AD加入状态。执行相应的dsregcmd操作后，

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

验证设备状态显示：

```
AzureAdJoined = YES
```

此更正解决了导致Cisco安全客户端在每个连接上提示输入凭据的基本身份验证状态问题。

步骤 3：重置默认浏览器应用

要解决外部浏览器与嵌入式浏览器的行为问题，请执行以下操作：

重置设备的默认应用设置，确保Cisco安全客户端正确启动外部/系统浏览器进行SAML身份验证，而

不是嵌入式浏览器。

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

步骤 4：确认

实施上述更改后，请确认以下行为：

- Cisco安全客户端不再在每个VPN连接上提示输入密码或Windows Hello身份验证
- 客户端正确启动外部浏览器进行SAML身份验证，而不是嵌入式浏览器
- 恢复了SSO功能，当存在活动的Entra ID会话时，允许用户在没有重复身份验证提示的情况下进行连接
- 不再出现“Authentication error due to problem with redirecting to SSO URL”错误

原因

身份验证问题是由受影响设备上的Azure AD加入状态不正确引起的，其中设备显示AzureAdJoined = NO而不是所需的AzureAdJoined = YES状态。这种不正确的加入状态阻止了正确的SSO令牌验证，并强制思科安全客户端在每次连接尝试时提示进行身份验证。

此外，设备的默认应用设置配置错误，导致Cisco安全客户端启动嵌入式浏览器而不是外部浏览器进行SAML身份验证，尽管客户端配置中启用了外部浏览器设置。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。