Prompt de Autenticação SAML do Cisco Secure Client em todas as tentativas com a ID do Microsoft Entra SSO

Contents

Problema

O Cisco Secure Client (AnyConnect) integrado ao Microsoft Entra ID para autenticação SAML estava passando por vários problemas relacionados à autenticação que interromperam a funcionalidade Single Sign-On (SSO):

- Os usuários estavam sendo solicitados para autenticação em cada tentativa de conexão VPN, mesmo quando uma sessão Entra ID ativa existia no navegador
- O cliente estava iniciando o navegador incorporado em vez do navegador externo/do sistema, apesar da autenticação do navegador externo estar explicitamente habilitada para SAML
- Os usuários frequentemente encontraram o erro: "Erro de autenticação devido a problema com o redirecionamento para a URL do SSO"
- O comportamento do SSO mudou do estado de trabalho anterior, em que os usuários podiam se conectar à VPN simplesmente clicando em Connect sem avisos de autenticação

Ambiente

- Produto: Cisco Secure Client (AnyConnect)
- Tecnologia: VPN de acesso seguro com autenticação SAML
- Provedor de identidade: ID do Microsoft Entra (Azure AD)
- método de autenticação: Integração de SAML SSO
- Autenticação do Navegador Externo habilitada para SAML

Resolução

A resolução envolveu o endereçamento do estado de ingresso do dispositivo Azure AD subjacente e problemas de configuração do navegador que estavam causando os problemas de autenticação:

Passo 1: Diagnosticar Status de Ingresso do Azure AD

Execute o seguinte comando para verificar o status atual de ingresso do Azure AD do dispositivo afetado:

```
dsregcmd /status
```

Revise a saída para identificar se o dispositivo mostra AzureAdJoined = NO, que indica um estado de junção incorreto do Azure AD.

Passo 2: Estado de Ingresso no Azure AD Correto

Execute o comando dsregcmd para corrigir o status de associação do Azure AD no dispositivo afetado. Depois de executar as operações dsregcmd apropriadas,

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

Verifique se o status do dispositivo mostra:

```
AzureAdJoined = YES
```

Essa correção resolve o problema de estado de autenticação subjacente que estava fazendo com que o Cisco Secure Client solicitasse credenciais em cada conexão.

Passo 3: Redefinir Aplicativos de Navegador Padrão

Para solucionar o problema de comportamento do navegador externo versus navegador incorporado:

Redefina as configurações padrão dos aplicativos do dispositivo para garantir que o Cisco Secure Client inicie corretamente o navegador externo/do sistema para a autenticação SAML em vez do navegador incorporado.

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

Passo 4: Verificação

Após implementar as alterações acima, verifique os seguintes comportamentos:

- O Cisco Secure Client não solicita mais a senha ou a autenticação do Windows Hello em cada conexão VPN
- O cliente inicia corretamente o navegador externo para a autenticação SAML em vez do navegador incorporado
- A funcionalidade SSO é restaurada, permitindo que os usuários se conectem sem repetidos avisos de autenticação quando uma sessão Entra ID ativa existir
- O erro "Authentication error due to problem with redirecting to SSO URL" (Erro de autenticação devido a problema no redirecionamento para a URL do SSO) não ocorre mais

Causa

Os problemas de autenticação foram causados por um estado de junção incorreto do Azure AD no dispositivo afetado, onde o dispositivo estava mostrando AzureAdJoined = NO em vez do status necessário AzureAdJoined = YES. Esse estado de junção incorreto impediu a validação adequada do token SSO e forçou o Cisco Secure Client a solicitar autenticação em cada tentativa de conexão.

Além disso, as configurações de aplicativo padrão do dispositivo foram configuradas incorretamente, fazendo com que o Cisco Secure Client iniciasse o navegador incorporado em vez do navegador externo para autenticação SAML, apesar da configuração do navegador externo estar habilitada na configuração do cliente.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.