Solução de problemas de autenticação SAML baseada em navegador de acesso seguro exibindo tela branca em branco com EntraID

Contents

Problema

Ao configurar o Cisco Secure Access para forçar a autenticação SAML baseada em navegador em dispositivos sem o Cisco Secure Client instalado, o processo de autenticação é redirecionado para uma tela branca em vez de exibir a página de autenticação EntraID. Esse problema ocorre especificamente no modo normal (não InPrivate) do Microsoft Edge e nos navegadores Google Chrome. A autenticação funciona corretamente ao usar o modo Edge InPrivate. O perfil de autenticação SAML tem a Descriptografia e a Autenticação SSO habilitadas.

A estrutura de política configurada inclui:

- Permitir política para usuários de pós-autenticação. (fonte: qualquer usuário, destino: qualquer um)
- Permitir política de autenticação SAML com perfil de autenticação SAML. (fonte: IP do endpoint, destino: 0.0.0.0 (TCP 80.443)
- Permitir política auxiliar de autenticação SAML com perfil de autenticação SAML. (fonte: IP do endpoint, destino: qualquer um)
- Bloquear política. (fonte: IP do endpoint, destino: qualquer um)

Ambiente

- Cisco Secure Access (módulo de acesso à Internet)
- EntraID como Provedor de Identidade (IdP)
- Autenticação SAML baseada em navegador para dispositivos sem Cisco Secure Client

- Perfil de autenticação SAML com Descriptografia e Autenticação SSO habilitadas
- Navegadores Microsoft Edge e Google Chrome

Resolução

O problema é resolvido adicionando domínios específicos relacionados a EntraID à lista de exclusão de descriptografia na configuração do perfil de autenticação SAML. Isso evita que o processo de descriptografia SSL/TLS interfira no fluxo de autenticação do EntraID.

Passo 1: Adicionar domínios EntraID à lista de exclusão de descriptografia

Configure estes quatro domínios EntraID na lista de exclusão de descriptografia para o perfil de autenticação SAML:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Passo 2: Aplicar configuração a políticas SAML

Verifique se as configurações de exclusão de descriptografia estão aplicadas a:

- A política Permitir autenticação SAML. (fonte: IP do endpoint, destino: 0.0.0.0 (TCP 80.443)
- A política do auxiliar Permitir autenticação SAML. (fonte: IP do endpoint, destino: qualquer um)

Passo 3: Verificar resolução

Após aplicar a configuração de exclusão de descriptografia, teste o fluxo de autenticação:

- Microsoft Edge (modo normal): Pode redirecionar com êxito para a página de autenticação do EntraID.
- Google Chrome: Pode redirecionar com êxito para a página de autenticação do EntraID.
- Ambos os navegadores podem exibir consistentemente a tela de entrada de autenticação do EntraID.

Causa

A tela branca em branco ocorre porque o processo de descriptografia SSL/TLS no Cisco Secure Access interfere no fluxo de autenticação do EntraID quando a descriptografia é ativada para o perfil de autenticação SAML. O processo de descriptografia interrompe a comunicação segura entre o navegador e os servidores de autenticação EntraID, impedindo que a página de autenticação seja carregada corretamente. O modo InPrivate funciona porque trata as sessões SSL/TLS de forma diferente, ignorando a interferência de descriptografia. Adicionar os domínios EntraID à lista de exclusão de descriptografia permite que o tráfego de autenticação passe sem descriptografia, mantendo a integridade do fluxo de autenticação seguro.

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.