

Falha na autenticação de RAVPN de acesso seguro com integração de SAML Duo

Contents

Problema

Ao tentar se conectar à Cisco Secure Access Remote Access VPN (RAVPN) usando Duo como o Identity Provider (IDP) com integração ao Ative Directory em segundo plano, os usuários experimentam falhas de autenticação apesar da autenticação bem-sucedida no nível do portal Duo.

Os sintomas específicos incluem:

- O portal Duo exibe uma mensagem de êxito para autenticação.
- O Cisco SecureClient exibe uma mensagem de erro "Authentication failed" imediatamente após o sucesso do Duo.
- Os registros Duo mostram o status "acesso concedido".
- Os registros do portal Cisco Secure Access mostram o status "AAA failure".

Isso cria uma desconexão em que o provedor de identidade externo confirma a autenticação bem-sucedida, mas o cliente VPN não pode estabelecer a conexão devido a falhas de validação de autenticação na infraestrutura de Acesso Seguro.

Ambiente

- Implantação do Cisco Secure Access RAVPN
- Segurança Duo como provedor de identidade SAML
- Integração do Ative Directory com o Duo

- Cisco SecureClient para conectividade VPN
- Fluxo de autenticação baseado em SAML

Resolução

A falha de autenticação foi resolvida corrigindo o mapeamento de atributos do usuário entre o Duo e o Cisco Secure Access. As etapas descritas nas próximas seções foram seguidas para identificar e resolver o problema.

Passo 1: Verificar Pesquisa de Atividade

- 1.- Faça login no Cisco Secure Access Dashboard. Clique em Monitor> Remote Access Logs.
- 2.- Procure o campo de nome de usuário nas mensagens de falha de verificação de autorização.
- 3.- Compare-o com o valor UPN em Connect > User and Groups.

O Cisco Secure Access examina o valor do Nome UPN para verificação de Autorização.

O nome UPN que está sendo passado do Duo não correspondeu ao valor do nome UPN para esse usuário em Usuário e Grupos.

O inquérito revelou:

- Endereço de email do usuário: user@gmail.com
- Nome UPN (nome de usuário principal)

Passo 2: Ajuste de configuração Duo

A resolução envolvia a modificação da configuração do SAML Duo para garantir o mapeamento adequado de atributos do usuário:

- Acesse o painel de administração do Duo.
- Navegue até a configuração do aplicativo SAML para o Cisco Secure Access.
- Modifique o mapeamento de atributos do usuário para enviar o endereço de email que deve corresponder ao valor do Nome UPN desse usuário em Usuário e Grupos.
- Salve as alterações de configuração.

Passo 4: Verificação

Depois de ajustar a configuração do Duo, o fluxo de autenticação foi testado e verificado com êxito. O usuário conseguiu se conectar usando a VPN de Acesso Remoto sem falhas de autenticação.

Causa

A causa raiz da falha de autenticação foi uma incompatibilidade de mapeamento de atributos do usuário entre as asserções do Duo SAML e as expectativas do Cisco Secure Access. O Duo foi configurado para enviar o nome de usuário sob o nome UPN em asserções SAML, enquanto o Cisco Secure Access foi configurado para esperar o endereço de e-mail do usuário. Essa incompatibilidade causou a falha da autenticação no nível de acesso seguro, apesar da autenticação bem-sucedida no nível IDP do Duo, resultando na "falha de AAA" registrada no acesso seguro, enquanto os registros do Duo mostraram "acesso concedido".

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.