

# Falha de Conexão VPN do Cisco Secure Client com Erros de Autenticação SAML e Dicionário de Bencode

## Contents

---

---

## Problema

As conexões VPN que usam o Cisco Secure Client não são estabelecidas ao usar a autenticação SAML com o Google IdP. Embora a autenticação SAML seja bem-sucedida no lado do IdP, o cliente falha durante o processamento de pós-autenticação e faz a transição para um estado desconectado, impedindo que o túnel VPN seja criado.

## Ambiente

- Cisco Secure Client versão 5.1.13.177
- Autenticação SAML configurada com o Google IdP
- Acesso seguro - Acesso remoto seguro do cliente (VPN, postura, recurso privado)
- Os logs de autenticação do Google IdP mostram a autenticação SAML bem-sucedida

## Resolução

O problema foi resolvido com a reinstalação do Cisco Secure Client. A seguinte abordagem de solução de problemas foi documentada:

### Etapas do diagnóstico inicial

Passo 1: Coletar registros DART do endpoint afetado -

<https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html>

Extract Dart Bundle > Cisco Secure client > Anyconnect VPN > Logs > Under VPN Folder > AnyConnectVPN.txt - mostra os seguintes erros ao ler as configurações internas, com os seguintes erros aparecendo continuamente:

- Falha na internalização do dicionário de código de desempenho
- Não foi possível criar o dicionário de código de desempenho.
- PHONEHOMEVPN\_ERROR\_UNEXPECTED
- GLOBAL\_ERROR\_UNEXPECTED

Passo 2: Verificar o status da autenticação SAML no lado do IdP

Confirme se os logs do Google IdP mostram uma autenticação SAML bem-sucedida para isolar o problema para o processamento de pós-autenticação do lado do cliente.

## Implementação da resolução

Passo 1: Reinstale o Cisco Secure Client

Desinstale a instalação existente do Cisco Secure Client e execute uma reinstalação limpa do software cliente.

Passo 2: Verificar a restauração da conectividade da VPN

Após a reinstalação, teste a conexão VPN com a autenticação SAML para confirmar se a conexão foi estabelecida com êxito e se o túnel foi criado corretamente.

A reinstalação do Cisco Secure Client restaurou a funcionalidade da VPN, permitindo a autenticação SAML bem-sucedida e o estabelecimento de túnel.

## Causa

A causa raiz parece estar relacionada a dados de configuração internos corrompidos dentro da instalação do Cisco Secure Client, afetando especificamente a capacidade do componente CPhoneHomeVpn/PhoneHomeAgent de processar dados do dicionário Bencode durante o processamento de pós-autenticação. Os repetidos erros "Bencode dictionary internalize failed" e "Failed to create Bencode dictionary" indicam que o cliente não conseguiu analisar ou processar corretamente os dados de configuração interna necessários para estabelecer o túnel VPN após a autenticação SAML bem-sucedida.

O problema foi resolvido através da reinstalação do cliente, sugerindo que o problema estava relacionado a dados corrompidos do lado do cliente, em vez de problemas de configuração do lado do servidor ou de integração de IdP.

## 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.