

Procedimento de Instalação SSLVPN Fortigate

OUTUBRO DE 2024

RESUMO

1	DOWNLOAD E INSTALAÇÃO DO CLIENTE SSLVPN	2
2	CONFIGURAÇÃO DO CLIENTE.....	2
3	CONFIGURAÇÃO DE SENHA E AUTENTICAÇÃO	4
4	PROBLEMAS CONHECIDOS.....	10

1 DOWNLOAD E INSTALAÇÃO DO CLIENTE SSLVPN

- Realizar o download do software FortiClient VPN para o sistema operacional desejado através do link abaixo. O fornecedor oferta diversas versões, gentileza realizar o download da versão **"FortiClient VPN"**.
 - Link para download: [FortiClient VPN - Download](#)

FortiClient VPN

A versão somente VPN do FortiClient oferece SSL VPN e IPsecVPN, mas não inclui nenhum suporte. Baixar do melhor software VPN para vários dispositivos.

Acesso remoto

- ✓ SSL VPN com MFA
- ✓ IPsec VPN com MFA



- Após o download realizar a instalação seguindo as telas de configuração, utilizar as opções padrões.

2 CONFIGURAÇÃO DO CLIENTE

- Após o término da instalação, execute o FortiClient VPN. Será apresentado a pagina abaixo, selecione a opção "Eu reconheço que esse software..." e clique em "Eu aceito".



- Na tela seguinte, clique em “**configurar a VPN**”.



- Configure os campos de acordo com a imagem abaixo.

Editar a Conexão de VPN

VPN	SSL-VPN VPN IPsec XML
Nome da Conexão	Engineering do Brasil
Descrição	
Gateway Remoto	sslvpn.br.engineering ✕ +Adicionar Gateway remoto
	☒ Porta customizada 4443
Single Sign On Settings	☒ Ativar logon único Single Sign On (SSO) para túnel VPN ☐ Use o navegador externo como agente de usuário para autenticação de usuário saml ☐ Enable auto-login with Azure Active Directory
Certificado do Cliente	Nenhum ▼ ☐ Habilite endereço IPv4/IPv6 Dual-stack
Cancelar Salvar	

- Gateway Remoto: sslvpn.br.engineering
- Porta Customizada: 4443

- OBS:** A opção para usar o navegador externo como agente de autenticação, permite você utilizar o seu navegador padrão para se conectar também de forma segura. Caso a autenticação já tenha sido realizada uma vez e foi armazenada em cache, ele irá dispensar a necessidade de inserir novamente o usuário e senha. O uso deste recurso é opcional.

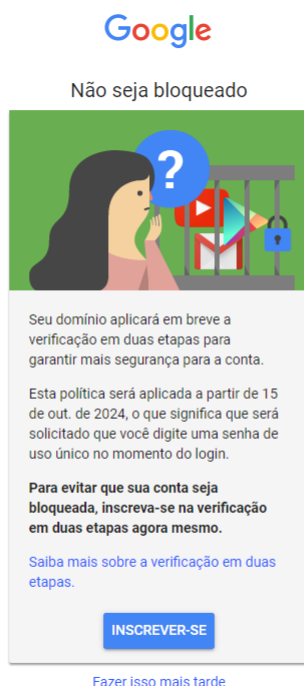
-



- Aceite a mensagem abaixo clicando em “Entendi”.



- Configure a autenticação em duas etapas clicando em “**INSCREVA-SE**”. Este passo é obrigatório seguindo as diretrizes de segurança da Eng.



[Fazer isso mais tarde](#)

- Clique em **"Adicionar app autenticador"**

← Verificação em duas etapas

Use uma camada extra de segurança para evitar que hackers acessem sua conta.

A menos que você faça login usando uma chave de acesso, será necessário concluir a segunda etapa mais segura disponível na sua conta. Você pode atualizar suas segundas etapas e opções de login nas configurações quando quiser. [Acesse as Configurações de segurança](#)



Segundas etapas

Mantenha essas informações atualizadas e adicione mais opções de login para que você possa sempre acessar sua Conta do Google

	Chaves de acesso e de segurança	 Adicionar uma chave de segurança	>
	Solicitação do Google		>
	Authenticator	 Adicionar app autenticador	>

- Clique em configurar autenticador.

← App Google Authenticator

Adicione mais opções de login para manter o acesso

 A verificação em duas etapas está ativada para esta conta. Evite a perda do acesso adicionando mais etapas de verificação na página do recurso agora mesmo.

[Adicionar opções](#)

Em vez de esperar mensagens de texto, receba códigos de verificação de um app autenticador. Essa opção funciona mesmo quando o smartphone está off-line.

Primeiro, baixe o Google Authenticator na [Google Play Store](#) ou na [App Store da Apple](#).



[+ Configurar o autenticador](#)

- Escaneie o QR Code com o app "Microsoft Authenticator" ou "Google Authenticator" e clique em avançar.

Configurar o app autenticador

- No app Google Authenticator, toque em +
- Selecione **Ler QR code**



[Não consegue ler o código?](#)

[Cancelar](#) [Avançar](#)

- Insira um código para concluir a configuração.

Configurar o app autenticador

Digite o código de seis dígitos mostrado no app

Digite o código

[Voltar](#) [Cancelar](#) [Verificar](#)

- Após configurar o autenticador, clique em **"Ativar a verificação em duas etapas"**.

Ativar a verificação em duas etapas

Use uma camada extra de segurança para evitar que hackers acessem sua conta.

A menos que você faça login usando uma chave de acesso, será necessário concluir a segunda etapa mais segura disponível na sua conta. Você pode atualizar suas segundas etapas e opções de login nas configurações quando quiser. [Acesse as Configurações de segurança](#) ➞



Ativar a verificação em duas etapas

- A configuração será concluída.

Agora você tem a proteção da verificação em duas etapas



Ao fazer login, será necessário concluir a segunda etapa mais segura. Portanto, estas informações precisam estar sempre atualizadas.



Authenticator



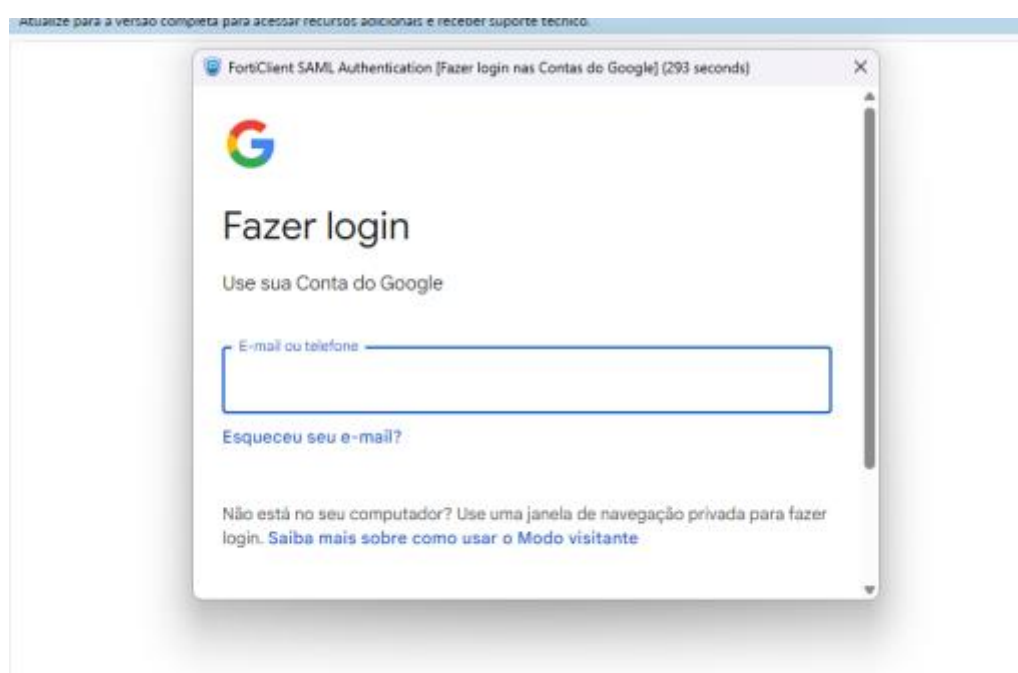
Adicionado em ontem

Concluído

- Após realizar o ajuste de senha, clicar em conectar.

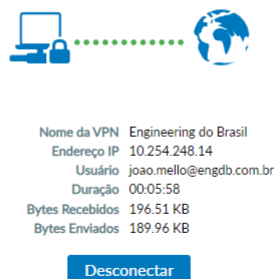


- Entrar com e-mail e senha Brasil na tela de login SAML exibida.



- Após a autenticação a conexão será estabelecida.

VPN Conectada



4 PROBLEMAS CONHECIDOS

- **Erro na autenticação SAML**

- Em algumas instalações do FortiClient, a página de autenticação SAML pode não ser exibida corretamente. Esse problema é causado pela ausência de um componente necessário no sistema operacional Windows.
- Para corrigir esse problema, é necessário instalar o seguinte pacote no sistema operacional: [Microsoft Visual C++ Redistributable](#)
- Este componente garante o funcionamento correto do FortiClient e a exibição adequada da página de autenticação SAML.

- **Erro de autenticação ao Google Workspace**

- Caso tenha feito login no console do google anteriormente e não tenha habilitado o MFA, o erro abaixo será exibido:



- Para solução deste problema, será necessário a abertura de um chamado através do portal <https://suporte-cloudlabs.engdb.com.br>. Com o chamado aberto a equipe de segurança vai gerar



novos códigos alternativos para que o login possa ser realizado, permitindo a configuração do MFA.