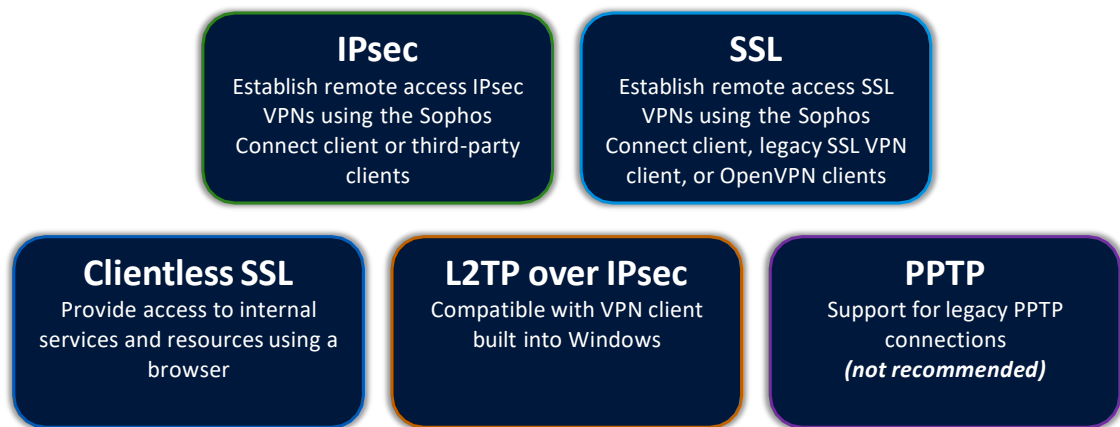




# Getting Started with Remote Access VPNs on Sophos Firewall

**Sophos Firewall**  
Version: 19.0v1

## Remote Access VPNs



SOPHOS

O Sophos Firewall suporta uma variedade de protocolos comuns para VPNs de acesso remoto.

Os mais utilizados são IPsec e SSL, por isso, neste capítulo, vamos nos concentrar nesses dois, mas é útil lembrar que o Sophos Firewall também suporta L2TP sobre IPsec, que é compatível com o cliente VPN interno do Windows, e PPTP, embora não recomendemos que você o use, pois é menos seguro.



## SSL and IPsec VPNs

### SSL Remote Access VPN

- Sophos Connect VPN Client for Windows and Mac OS X
- Compatible with OpenVPN clients on all platforms
- Support for multi-factor authentication
- Supports Synchronized Security
- Split tunnelling and tunnel all
- Guided configuration wizard

### IPsec Remote Access VPN

- Sophos Connect VPN Client for Windows and Mac OS X
- Compatible with third-party IPsec VPN clients
- Support for multi-factor authentication
- Supports Synchronized Security
- Split tunnelling and tunnel all

#### SOPHOS

A VPN de acesso remoto SSL do Sophos Firewall é baseada no OpenVPN, uma solução VPN completa. Os túneis criptografados entre dispositivos remotos e o Sophos Firewall usam certificados SSL e nome de usuário e senha para autenticar a conexão, e você também pode habilitar a autenticação multifator para segurança adicional.

A VPN de acesso remoto IPsec pode ser autenticada usando uma chave pré-compartilhada ou um certificado digital, com os usuários se autenticando com seu nome de usuário e senha e, opcionalmente, a autenticação multifator. Como uma VPN IPsec padrão, ela é compatível com clientes VPN de terceiros.

Para as VPNs de acesso remoto SSL e IPsec, fornecemos o cliente VPN Sophos Connect para Dispositivos Windows e Mac OS X.

Para VPNs de acesso remoto SSL, ainda oferecemos suporte ao cliente VPN SSL Sophos legado; no entanto, recomendamos atualizar para o Sophos Connect sempre que possível.

#### [Additional Information]

<https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/VPNSophosConnectClient.html>

# SSL VPN Assistant

The screenshot shows the Sophos Firewall web interface for configuring Remote access VPNs. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Remote access VPN' and includes tabs for 'IPsec', 'SSL VPN', 'L2TP', 'PPTP', 'Clientless SSL VPN policy', and 'IPsec (legacy)'. Under the 'SSL VPN' tab, there are links for 'SSL VPN global settings', 'Download client', and 'Logs'. A green box highlights the 'Assistant' button in the top right corner of the configuration area. Below this, a modal dialog box titled 'Remote access assistant (SSL VPN)' is open, showing 'Global settings' for the VPN connections. The settings include Protocol (TCP), Override hostname (192.168.0.242), Port (443), Assign IPv4 addresses (10.81.234.0), Subnet mask (255.255.255.0), and Lease mode (IPv4 only). The dialog also includes a 'Cancel' button and a 'Next' button.

**Global settings**  
These settings apply to all remote access SSL VPN connections.

Protocol	TCP
Override hostname	192.168.0.242
Port	443
Assign IPv4 addresses	10.81.234.0
Subnet mask	255.255.255.0
Lease mode	IPv4 only

You can change these settings on Remote access VPN > SSL VPN > SSL VPN global settings.

Cancel 1 of 9 Next

O Sophos Firewall tem um assistente para agilizar e simplificar a configuração de tudo o que é necessário para VPNs SSL de acesso remoto. O assistente inclui:

- Selecionando os usuários e grupos aos quais a política se aplicará

- Configurando os servidores de autenticação

- Selecionando os recursos que os usuários poderão acessar

- Escolhendo entre tunelamento dividido ou túnel todos

- Selecionando quais zonas podem acessar o portal do usuário para baixar o cliente e a configuração

- E selecionando de quais zonas os usuários podem estabelecer uma VPN SSL a partir de







Como parte do assistente, uma regra de firewall será criada para controlar o acesso a recursos internos de a VPN.

## Security Heartbeat over SSL VPN

Tunnel access \*

Use as default gateway ☒

Permitted network resources (IPv4)

SecurityHeartbeat_over_VPN	 
UK LAN	 
UK-Intranet01	 
Add new item	

Permitted network resources (IPv6)

Add new item

Split tunnel or tunnel all option

SOPHOS

Para habilitar o uso do Security Heartbeat sobre a VPN SSL, você precisa adicionar o objeto host 'SecurityHeartbeat\_over\_VPN' integrado. Isso contém o endereço IP público usado para o Security Heartbeat e garantirá que ele seja roteado pela VPN para o Sophos Firewall.

# SSL VPN Settings

**SOPHOS** Sophos Firewall

SSL VPN settings

protocol \* ☒ TCP ☐ UDP [Select UDP for better performance]

SSL server certificate \*

Override hostname

Port \*  [1-65535]

Assign IPv4 addresses \*  /24 [255.255.255.0]

Assign IPv6 addresses \*  /

Lease mode \*

IPv4 DNS

IPv4 WINS

Domain name

Disconnect dead peer after \*  Seconds [60 - 1800]

Disconnect idle peer after \*  Minutes [15 - 360]

Cryptographic settings

Encryption algorithm

Por padrão, o Sophos Firewall hospeda a VPN SSL na porta 8443, no entanto, isso pode ser alterado para uma porta disponível diferente nas configurações da VPN SSL. Observe que a VPN SSL pode compartilhar a porta 443 com outros serviços no Sophos Firewall, como o portal do usuário e as regras de firewall do aplicativo Web.

Você pode modificar o certificado SSL para a conexão e substituir o nome do host usado nos arquivos de configuração.

Você pode configurar o intervalo de concessão de IP, DNS, WININS e nome de domínio que serão usados para clientes que se conectam.

Além disso, existem várias configurações avançadas de conexão, como os algoritmos, o tamanho da chave, o tempo de vida da chave e as opções de compactação.

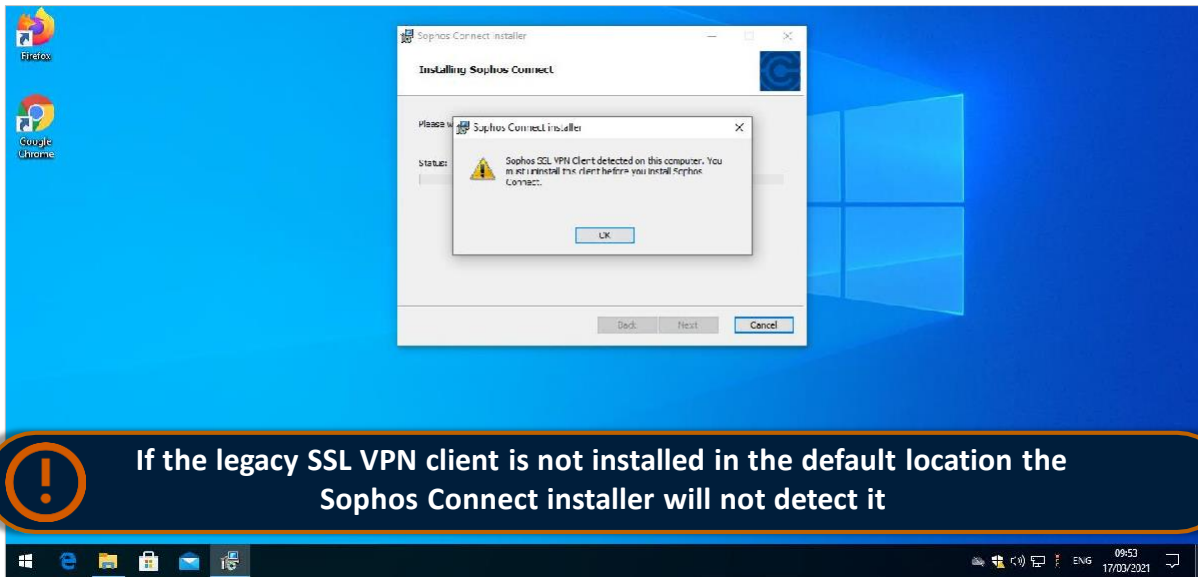
As configurações de VPN SSL são globais para VPNs SSL de acesso remoto e site a site; se você fizer alterações aqui, talvez seja necessário atualizar todas as VPNs SSL site a site que você configurou.

# SSL VPN Client

The screenshot shows the Sophos user portal interface. On the left is a dark blue sidebar with the 'SOPHOS' logo and navigation links: Home, Personal, Download client, VPN (highlighted in light blue), Internet usage, Email, and Logout. The main content area is titled 'User portal for jsmith@trainingdemo.xyz' and includes a help icon. It is divided into two sections: 'Sophos Connect client (IPsec and SSL VPN)' and 'SSL VPN client (legacy)'. The first section contains three download links: 'Download client for Windows', 'Download client for macOS', and 'Download connection for SSL VPN'. A green callout box points to this section. The second section contains four download links: 'Download client and configuration for Windows', 'Download configuration for Windows', 'Download configuration for other OSs', and 'Download configuration for Android/iOS'. An orange callout box points to this section.

Depois que um perfil VPN SSL for criado para um usuário, ele poderá baixar um cliente VPN SSL de seu Portal do Usuário. Para Windows e Mac OS X, recomendamos a utilização do cliente Sophos Connect. Há também um cliente VPN SSL herdado para Windows e download de configuração para todas as plataformas.

# Sophos Connect Client and Legacy SSL VPN Client



**If the legacy SSL VPN client is not installed in the default location the Sophos Connect installer will not detect it**

SOPHOS

O cliente VPN SSL herdado e o cliente Sophos Connect não podem ser instalados no mesmo computador, pois entrarão em conflito um com o outro. Para evitar isso, ao instalar o Sophos Connect, ele verificará a VPN herdada no caminho de instalação padrão e exibirá um erro, se encontrado.

Se o cliente VPN SSL herdado tiver sido instalado em um local não padrão, o instalador do Sophos Connect não o detectará. Isso pode tornar ambos os clientes VPN inoperantes devido ao conflito.

## [Additional Information]

O caminho de instalação padrão do cliente VPN SSL herdado é: C:\Arquivos de Programas (x86)\Sophos\Sophos VPN SSL)



## Simulation: Configure an SSL Remote Access VPN



In this simulation you will configure an SSL remote access VPN using the assistant. You will then review the configuration created and test your VPN using the Sophos Connect client.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/fw/simulation/SslUserVpn/1/start.html>

SOPHOS

Nesta simulação, você configurará uma VPN de acesso remoto SSL usando o assistente. Você então revise a configuração criada e teste sua VPN usando o cliente Sophos Connect.

### [Additional Information]

<https://training.sophos.com/fw/simulation/SslUserVpn/1/start.html>

# IPsec VPN Configuration

**SOPHOS** Firewall

Remote access VPN

Feedback How-to guides Log viewer Help admin@fw1.ad.trainingdemo.xyz Sophos

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced protection

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Monitors and services

IPsec

SSL VPN

L2TP

PPTP

Clientless SSL VPN policy

IPsec (legacy)

IPsec profiles Download client Logs

Quick links to IPsec profile, Sophos Connect client download, and logs

General settings

IPsec remote access ☒ Enable

Interface \* PortB - 192.168.0.242

IPsec profile \* DefaultRemoteAccess

Authentication type \* Preshared key

Preshared key \*

Local ID Select local ID

Remote ID Select remote ID

Allowed users and groups \* Training

Na parte superior da guia da VPN de acesso remoto IPsec estão os links rápidos que fornecem acesso ao Ipsec perfis, o download do cliente Sophos Connect e logs.

# IPsec VPN Profiles

**SOPHOS** FW  
Sophos Firewall

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Advanced protection

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

**Profiles**

Hosts and services

Profiles

Feedback How-to guides Log viewer Help admin@fw1.ad.trainingdemo.xyz Sophos

Schedule Access time Surfing quota Network traffic quota Decryption profiles **IPsec profiles** Device access

Show additional properties Add Delete

	Name	Keying method	Authentication mode	Compress	PFS	Encryption algorithm		Manage
						Phase1	Phase 2	
<input type="checkbox"/>	Default Profile	Automatic	Main mode	No	Enable	AES256 - SHA2 256	AES256 - SHA2 256	
<input type="checkbox"/>	DefaultBranchOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
<input type="checkbox"/>	DefaultHeadOffice	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 512 AES256 - SHA2 256 AES128 - SHA1	
<input type="checkbox"/>	DefaultL2TP	Automatic	Main mode	Yes	Disable	3DES - SHA1 3DES - MD5 AES128 - MD5	3DES - SHA1 3DES - MD5 AES128 - MD5	
<input type="checkbox"/>	DefaultRemoteAccess	Automatic	Main mode	No	Enable	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	AES256 - SHA2 256 AES256 - SHA1 AES128 - SHA1	
<input type="checkbox"/>	IKEv2	Automatic	Main mode	No	Enable	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	AES256 - SHA2 512 AES256 - SHA2 384 AES256 - SHA2 256	

Os perfis IPsec contêm a configuração de segurança para a conexão IPsec, como a criptografia algoritmos que serão suportados.

O Sophos Firewall fornece um perfil padrão para acesso remoto; no entanto, você pode clonar isso e criar o seu próprio para atender aos seus requisitos de segurança.

# IPsec VPN Configuration

**SOPHOS** Firewall

Remote access VPN

Feedback | How-to guides | Log viewer | Help | admin@fw1.ad.trainingdemo.xyz | Sophos

IPsec | SSL VPN | L2TP | PPTP | Clientless SSL VPN policy | IPsec (legacy)

IPsec profiles | Download client | Logs

General settings

IPsec remote access ☒ Enable

Interface \* PortB - 192.168.0.242

IPsec profile \* DefaultRemoteAccess

Authentication type \* Preshared key

Preshared key \*

Local ID Select local ID

Remote ID Select remote ID

Allowed users and groups \* Training

Select the IPsec profile

Pre-shared keys or digital certificate

Select the users and groups that can connect

Para configurar a VPN de acesso remoto IPsec, comece habilitando-a e selecionando qual interface ela irá ouça as conexões ligadas.

Selecione o perfil IPsec.

A VPN pode ser autenticada por chaves pré-compartilhadas ou com um certificado digital. Selecione os usuários e grupos que poderão se autenticar para usar a VPN.

# IPsec VPN Configuration

**SOPHOS** Firewall

Remote access VPN

Feedback How-to guides Log viewer Help admin@fw1.ad.trainingdemo.xyz Sophos

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced protection

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Maps and services

IPsec SSL VPN L2TP PPTP Clientless SSL VPN policy IPsec (legacy)

Client information

Name \* LondonVPN

Assign IP from \* 172.17.38.10 - 172.17.38.240

☐ Allow leasing IP address from RADIUS server for L2TP, PPTP and IPsec remote access

DNS server 1 172.16.16.10

DNS server 2 172.16.16.16

Idle time

Disconnect when tunnel is idle ☐ Enable

Idle session time interval (120-21600 seconds)

Advanced settings

Você precisa configurar o intervalo de IP que será usado para clientes que se conectam e, opcionalmente, você pode também atribua servidores DNS.

# IPsec VPN Configuration

The screenshot displays the Sophos Firewall web interface for Remote Access VPN configuration. The left sidebar shows the navigation menu with categories: MONITOR & ANALYZE, PROTECT, CONFIGURE, and SYSTEM. The 'Remote access VPN' option is selected under the CONFIGURE section. The main content area is titled 'Remote access VPN' and includes tabs for IPsec, SSL VPN, L2TP, PPTP, Clientless SSL VPN policy, and IPsec (legacy). The 'IPsec' tab is active, showing the 'Advanced settings' section. A note states: 'Adds these settings only to the .scx file used with Sophos Connect clients. To apply the changes, send the updated file to users for reimport into the client.' The settings include: 'Use as default gateway' (ON), 'Permitted network resources (IPv4) \*' (with an 'Add new item' button), and several checkboxes: 'Send Security Heartbeat through tunnel', 'Allow users to save username and password', 'Prompt users for 2FA token', 'Run AD logon script after connecting', and 'Connect tunnel automatically'. At the bottom right, there is a field for 'Hostname or DNS suffix to monitor' with a placeholder 'Enter a hostname or DNS suffix'.

**SOPHOS** Firewall

Remote access VPN

Feedback How-to guides Log viewer Help admin@fw1.ad.trainingdemo.xyz Sophos

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Advanced protection

CONFIGURE

- Remote access VPN**
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services

IPsec SSL VPN L2TP PPTP Clientless SSL VPN policy IPsec (legacy)

### Advanced settings

Adds these settings only to the .scx file used with Sophos Connect clients. To apply the changes, send the updated file to users for reimport into the client

Use as default gateway ☒

Permitted network resources (IPv4) \*

Add new item

- ☐ Send Security Heartbeat through tunnel
- ☐ Allow users to save username and password
- ☐ Prompt users for 2FA token
- ☐ Run AD logon script after connecting
- ☐ Connect tunnel automatically

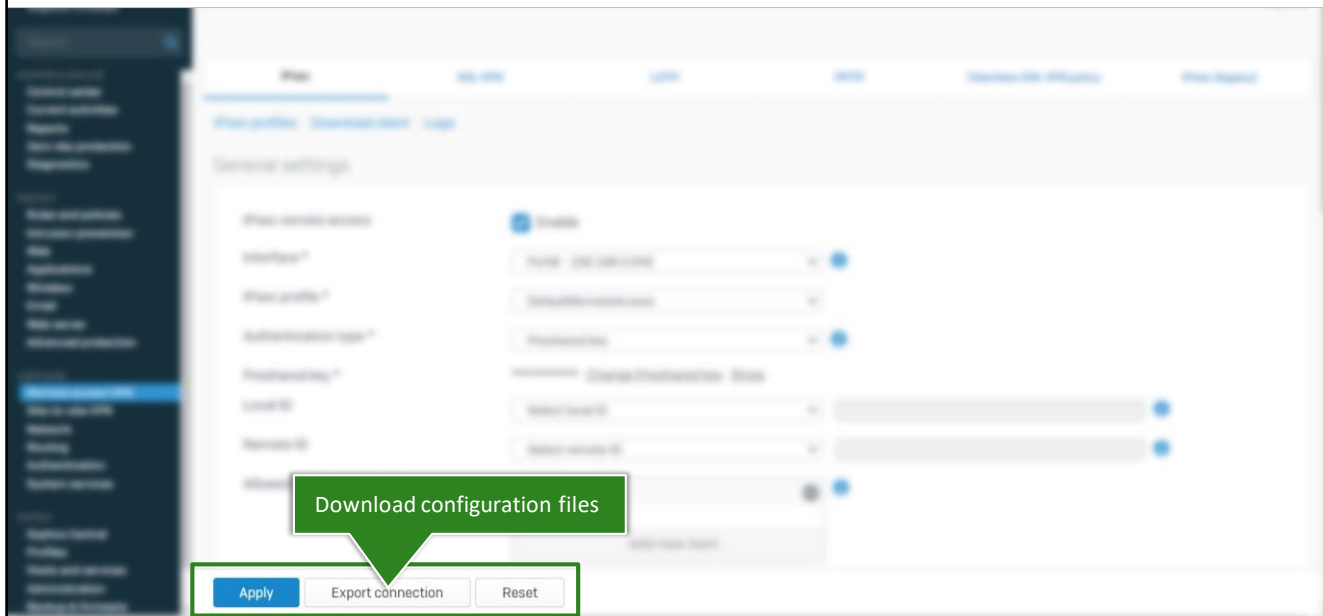
Hostname or DNS suffix to monitor

Enter a hostname or DNS suffix

DNS suffix

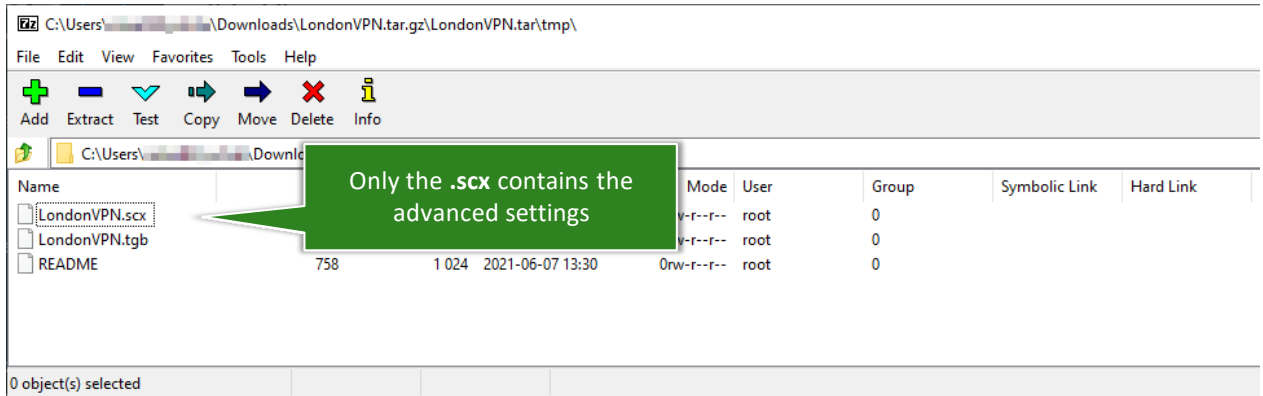
A configuração avançada pode ser encontrada na parte inferior da página e permite que você configure tunelamento dividido, autenticação de dois fatores, pulsação de segurança e outras configurações de conexão.

# IPsec VPN Configuration



Usando os botões na parte inferior da página, você pode exportar a configuração para a VPN.

# IPsec VPN Configuration



## SOPHOS

Quando você exporta a configuração do administrador da web, você baixará um arquivo com dois limas:

.scx – que inclui as configurações avançadas

.tgb – que contém apenas a configuração básica e encapsula todo o tráfego de volta para o Sophos Firewall



# IPsec VPN Client

SOPHOS

Home

Personal

Download client

VPN


Internet usage

Email


Logout

User portal for jsmith@trainingdemo.xyz


Sophos Connect client (IPsec and SSL VPN)



Download client for Windows




Download client for macOS




Download connection for SSL VPN

Sophos Connect client can be downloaded from the user portal


SSL VPN client (legacy)




Download client and configuration for Windows



Download configuration for Windows



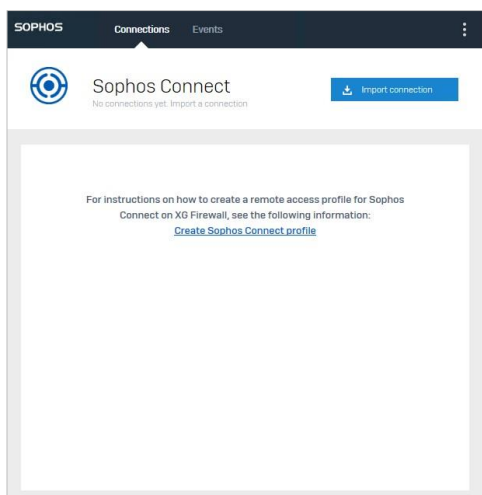
Download configuration for other OSs



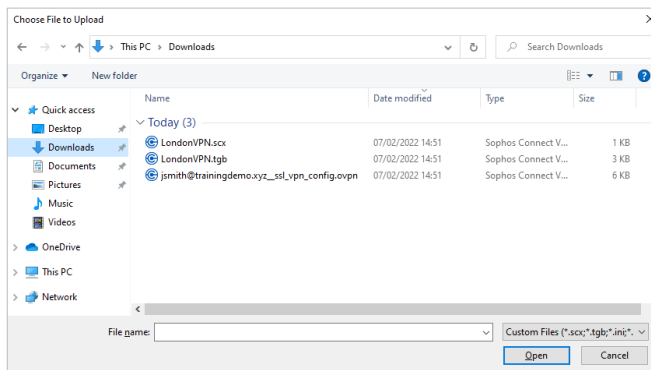
Download configuration for Android/iOS

O cliente Sophos Connect também pode ser baixado do portal do usuário; no entanto, o a configuração da VPN IPsec precisa ser fornecida pelo administrador.

# Sophos Connect Client



## Import the configuration file for either IPsec or SSL



SOPHOS

Para usar o cliente Sophos Connect, você precisa importar um arquivo de configuração. Isso pode ser tanto para o VPN IPsec ou SSL.

# Sophos Connect Client



## Connection Details

The image displays three sequential screenshots of the Sophos Connect Client interface, illustrating the connection process.

**First Screenshot (Left):** Shows the 'Connections' tab with a single entry for 'LondonVPN' with the status 'Never connected'. A 'Connect' button is visible.

**Second Screenshot (Middle):** Shows the 'Authenticate user' screen. It prompts the user to enter their username and password. The username field contains 'jsmith' and the password field is masked with dots. A 'Sign in' button is at the bottom.

**Third Screenshot (Right):** Shows the 'Monitor connection' screen. It displays the connection status as 'Connected' and provides details about the connection, including the connection name, gateway, remote and local IKE IDs, and the connection time.

Monitor connection	
Connection name	LondonVPN
Gateway	192.168.0.242
Remote IKE ID	192.168.0.242
Local IKE ID	10.16.16.20
Connected	Monday, Feb 7, 2022 @ 3:50:55 PM
VPN type	IPsec

Você pode então se conectar à VPN.

Quando o Cliente Sophos Connect entrar em contato com o firewall, você será solicitado a autenticar.

Uma vez conectado, os detalhes serão mostrados.

# Simulation: Configure an IPsec Remote Access VPN



In this simulation you will configure an IPsec remote access VPN. You will then test your VPN using the Sophos Connect client.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/fw/simulation/IpsecUserVpn/1/start.html>

SOPHOS

Nesta simulação, você configurará uma VPN de acesso remoto IPsec. Em seguida, você testará sua VPN usando o cliente Sophos Connect.

## [Additional Information]

<https://training.sophos.com/fw/simulation/IpsecUserVpn/1/start.html>

# Deploying Sophos Connect



Additional information in  
the notes



Deploy the Sophos Connect MSI via a GPO script



Push the configuration as a file in the Windows Settings GPO

## SOPHOS

O cliente Sophos Connect pode ser facilmente implantado usando a Diretiva de Grupo do Active Directory. Isso requer dois elementos a serem configurados.

Primeiro, você precisa adicionar o Sophos Connect MSI por meio de um script de GPO ou Objeto de diretiva de grupo.

Em segundo lugar, você precisa configurar um arquivo de configurações do Windows para enviar a configuração para os pontos de extremidade.

### [Additional Information]

Details on how to do this are covered in knowledgebase article **KB-000040793**.

<https://support.sophos.com/support/s/article/KB-000040793>