

# SOPHOS

Cybersecurity  
made  
simple.

Sophos Connect  
help

# Contents

About Sophos Connect.....	1
Installing Sophos Connect.....	1
Uninstalling Sophos Connect.....	1
Connections.....	3
Import connection.....	3
Establish connection.....	5
Connection options.....	9
Events.....	10
Troubleshooting events.....	11
General troubleshooting.....	15
Technical support.....	17
Legal notices.....	18

# 1 About Sophos Connect

Sophos Connect is a VPN client that can be installed on Windows and Macs. It allows you to connect to networks behind the Sophos XG Firewall from a remote location, for instance, your company network. Your Sophos XG Firewall administrator will configure connection details on the Sophos XG Firewall and provide you with the installation package and the connection configuration files.

This guide provides information about how to use Sophos Connect:

- For instructions on how to install and uninstall Sophos Connect, see [Installing Sophos Connect](#) (page 1) and [Uninstalling Sophos Connect](#) (page 1).
- For instructions on importing connection files and managing connections, see [Connections](#) (page 3).
- For information on events, and how to troubleshoot event errors, see [Events](#) (page 10).
- To troubleshoot issues that do not appear in the **Events** section, see [General troubleshooting](#) (page 15).

## 1.1 Installing Sophos Connect

### Install Sophos Connect on Windows

- Open the installer.
- Accept the license agreement and click **Install**.
- Once the installation is complete, click **Finish**. You can choose to launch Sophos Connect after closing the installer.

### Install Sophos Connect on Mac

- Open the installer.
- Choose the installation destination. Make sure you have enough free space in the destination you have chosen, for example, System Drive.
- Click **Install**.
- Once the installation is complete, click **Finish**.

## 1.2 Uninstalling Sophos Connect

### Uninstall Sophos Connect from Windows

- Go to **Control Panel** and under **Programs** click **Uninstall a program**.
- Right-click **Sophos Connect**, and select **Uninstall**.

## Uninstall Sophos Connect from Mac

- Open **Terminal**.
- Elevate permission to root and run the uninstall script from the location Sophos Connect is installed on:

```
sudo /Library/Sophos Connect/uninstall.sh
```

You will get the following message if the uninstallation was successful:

```
Sophos Connect has been uninstalled
```

## 2 Connections

For information on importing connections, establishing a connection, and viewing and editing connections, see:

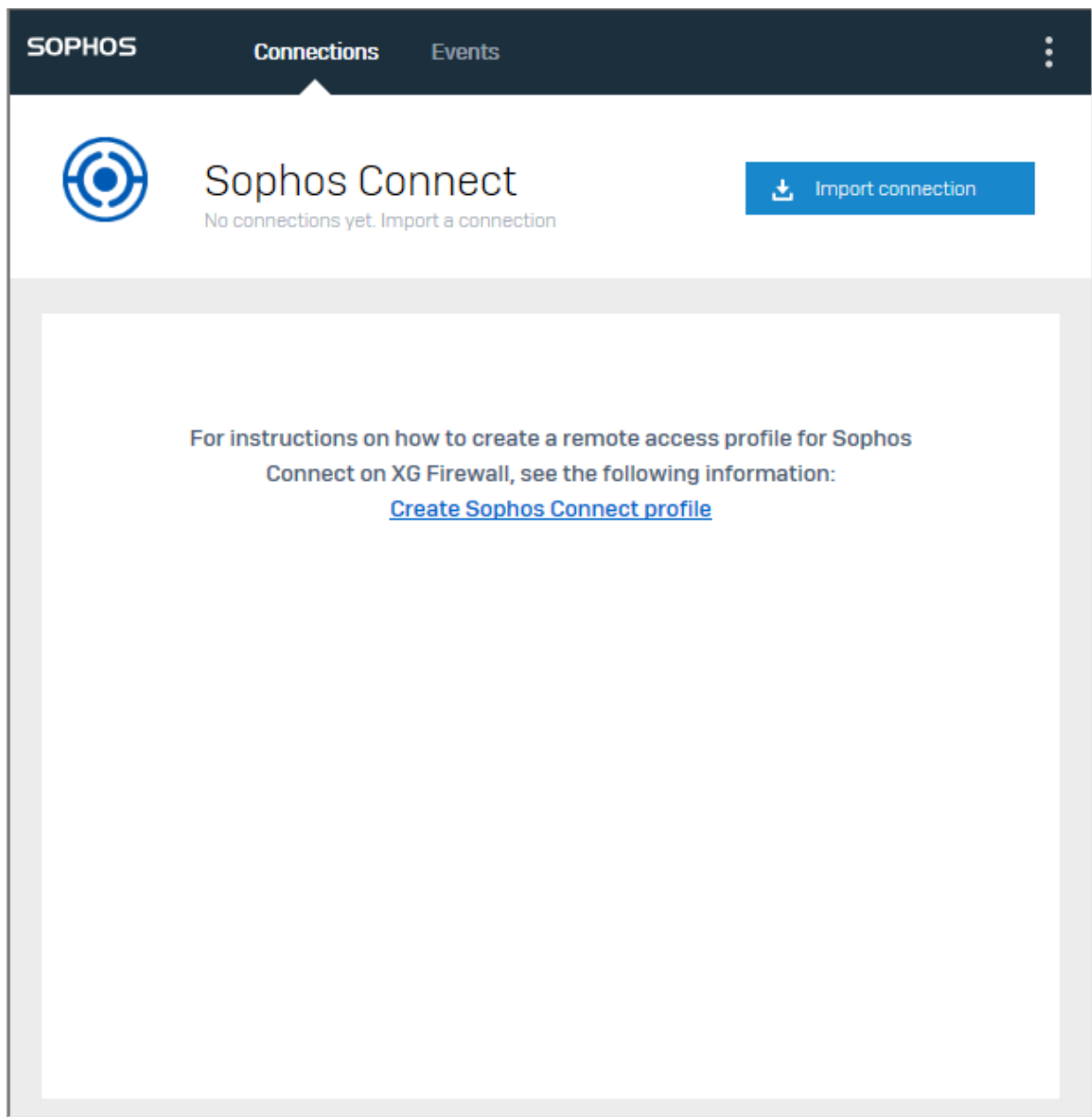
- [Import connection](#) (page 3)
- [Establish connection](#) (page 5)
- [Connection options](#) (page 9)

### 2.1 Import connection

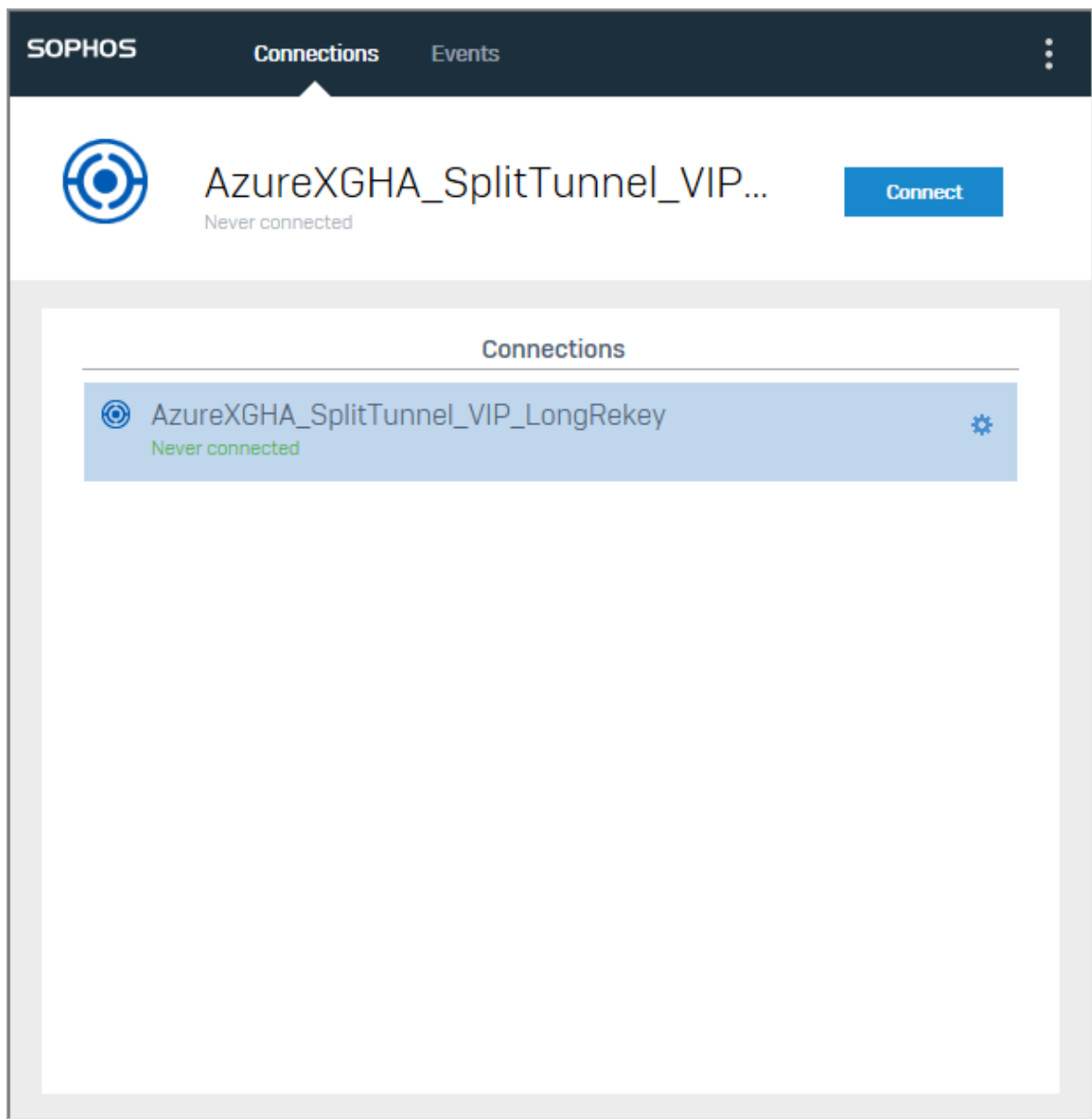
A connection file has been provided to you by your Sophos XG Firewall administrator. It has the extension `tgb`, for example `Company_connection.tgb`.

To import a connection:

1. Click **Import connection** on the **Connections** page.



2. Browse for the `tgb` file and open it.  
The connection will be displayed under **Connections**.



You can now establish the connection.

**Note**

You can import multiple connections.

## 2.2 Establish connection

Make sure there is at least one imported connection available and you have been given the required credentials.

To establish a connection:

1. Select a connection on the **Connections** page.
2. Double-click the connection.

You can also click **Connect**.

The sign in screen will appear.

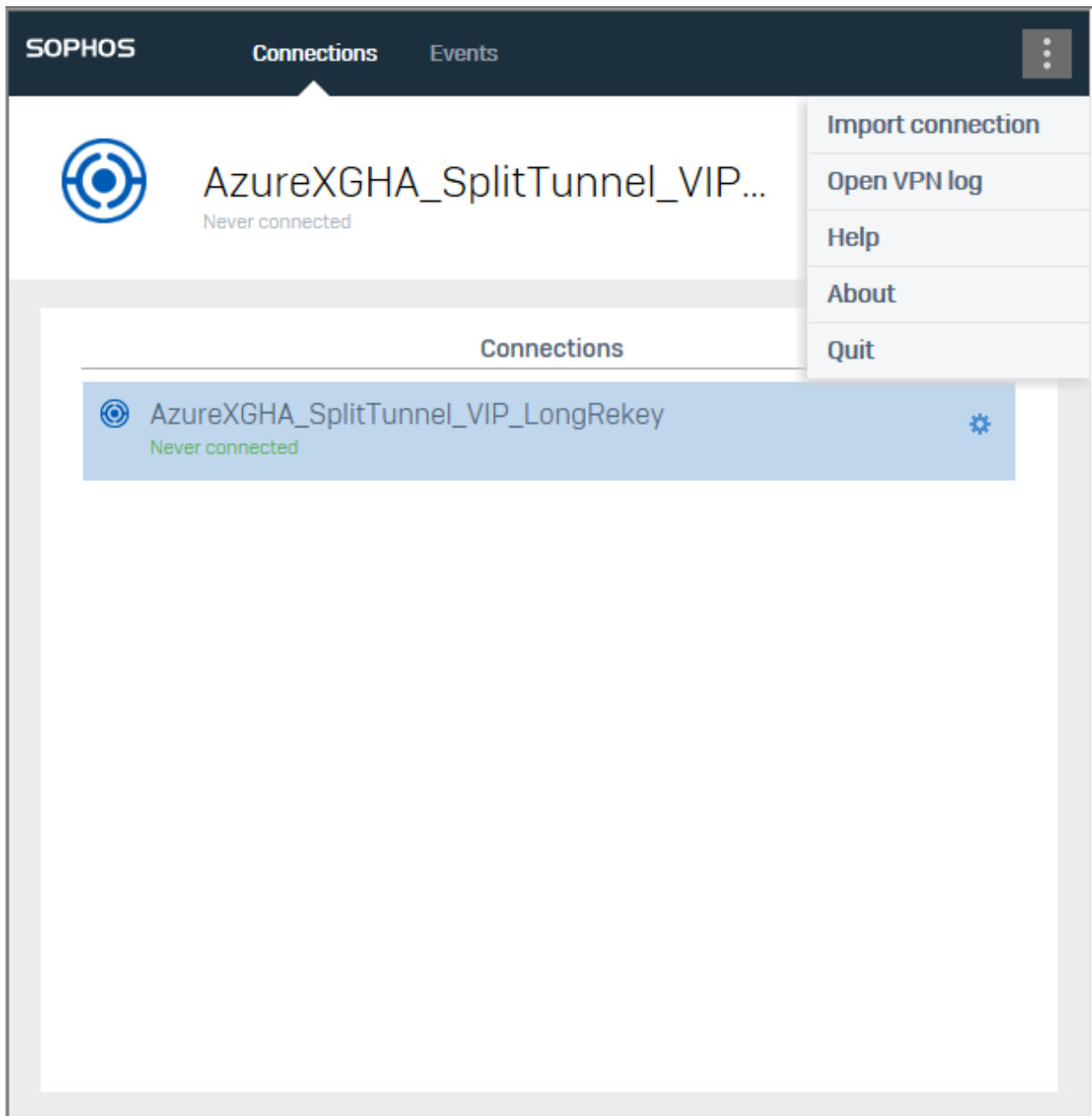
The screenshot shows the Sophos Connect interface. At the top, there is a dark blue header with the 'SOPHOS' logo on the left, and 'Connections' and 'Events' tabs in the center. A menu icon (three vertical dots) is on the right. Below the header, the main content area has a white background. On the left is the Sophos logo. To its right, the connection name 'AzureXGHA\_SplitTunnel\_VIP...' is displayed in a large font, with the subtitle 'Please enter user credentials' below it. A blue 'Cancel' button is positioned to the right of the connection name. The central part of the screen is a white box with a light gray border, titled 'Authenticate user'. Below the title, it says 'To connect, enter your user name and password and click Sign in.' There are two input fields: the first is for the username, and the second is for the password, with the label 'Password' inside the field. Below the password field is a checkbox labeled 'Save user name and password'. At the bottom of the box is a blue 'Sign in' button.

3. Enter your user name and password and click **Sign in**.  
Sophos Connect attempts to establish the connection and authenticate you.

**Note**

If you are facing connection issues, have a look at the **Events** page and contact your IT. You can also check the VPN logs by selecting **Open VPN log** from the menu icon.





The connection to the remote server is established.

The screenshot shows the Sophos Connect web interface. At the top, there is a dark blue header with the 'SOPHOS' logo on the left, and 'Connections' and 'Events' tabs in the center. On the right side of the header, there are three vertical dots representing a menu. Below the header, the main content area features a large green checkmark icon on the left. To its right, the connection name 'AzureXGHA\_SplitTunnel\_VIP...' is displayed in a large font, with the status 'Connected today March 27, 2019 @ 10:38:25 AM' in a smaller font below it. A blue 'Disconnect' button is positioned to the right of the connection name. Below this information, there is a section titled 'Monitor connection' with a sub-header containing icons for a computer, a double-headed arrow, and a lock. The details are presented in a table-like format:

Connection name	AzureXGHA_SplitTunnel_VIP_LongRekey
Gateway	xgha.eastus.cloudapp.azure.com
Remote IKE ID	sophos.azure.com
Local IKE ID	192.168.1.236
Connected	March 27, 2019 @ 10:38:25 AM

If the connection is successful, you will see this icon on the taskbar:



If the connection is unsuccessful, you will see this icon on the taskbar:

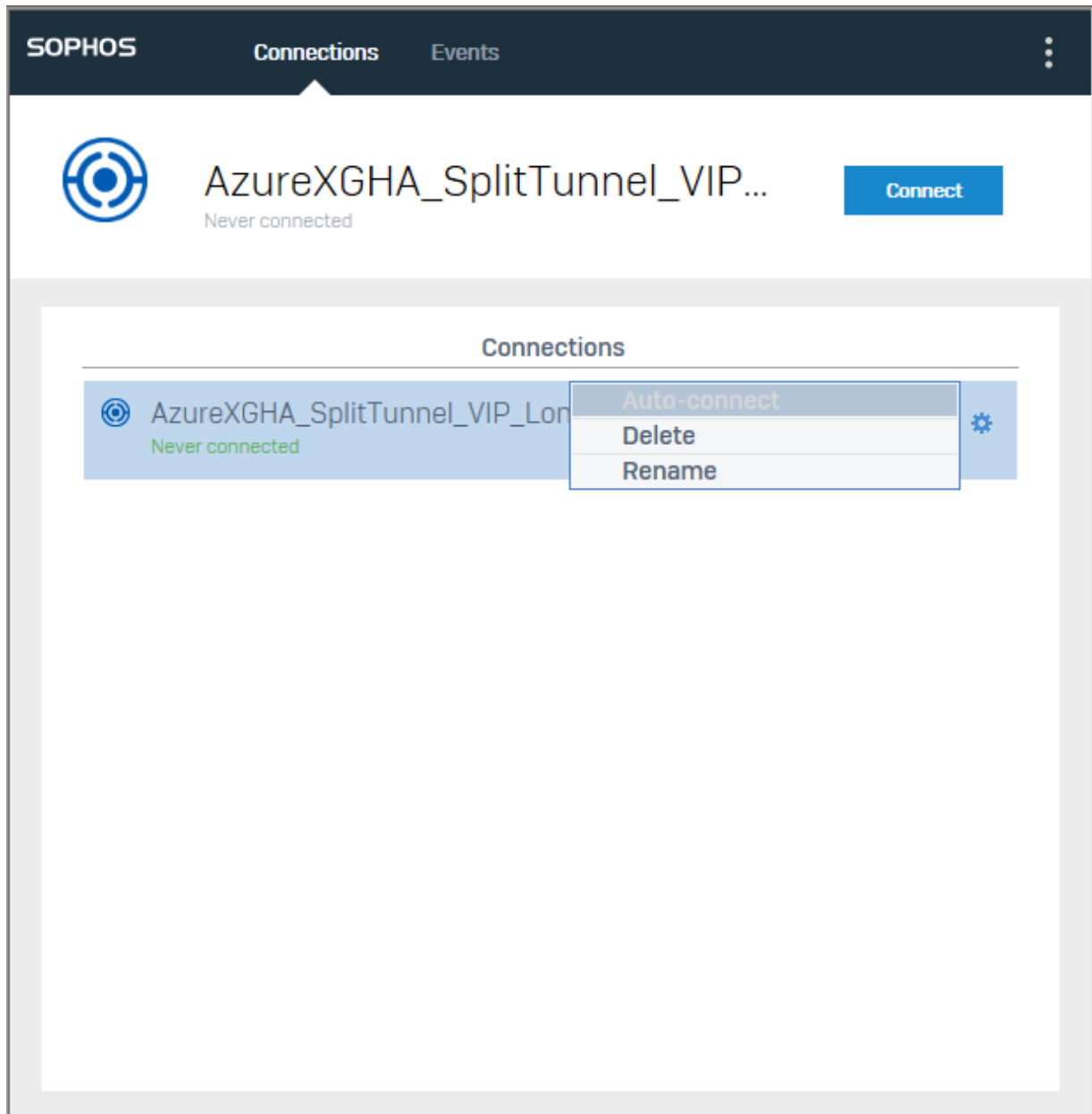


**Note**

If you have renamed the connection, the original name as provided by your Sophos XG Firewall administrator will still show in connection details. For instructions on how to rename it see [Connection options](#) (page 9).

## 2.3 Connection options

You can make various changes to the connections in Sophos Connect by clicking the settings icon.

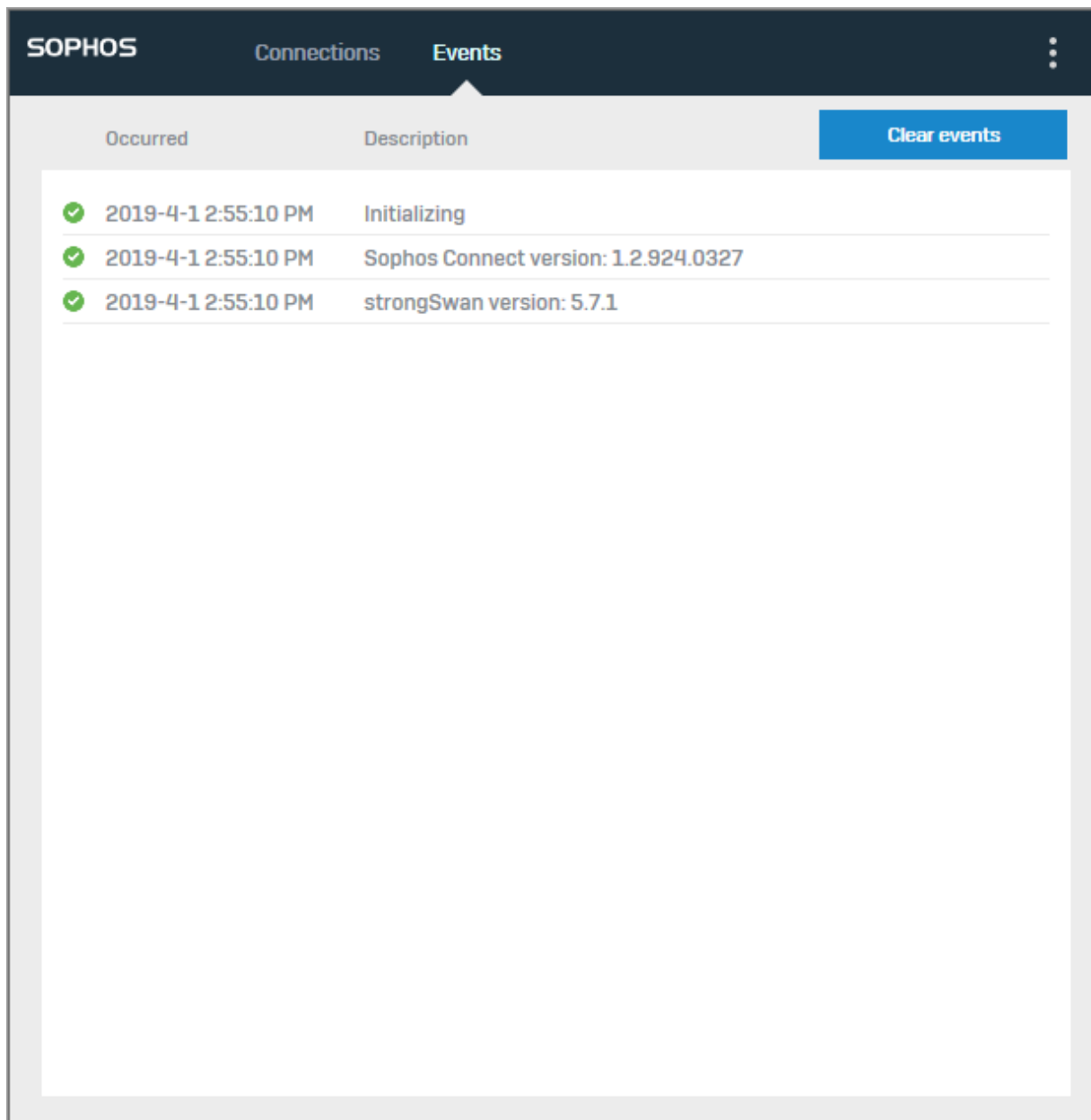


1. **Auto-connect** attempts a connection when Sophos Connect is started up.
2. **Delete** deletes the connection. If you want to re-establish the connection you will need to import it again.
3. **Rename** gives you the option to rename your connection.

## 3 Events

On the **Events** page, you can see all the actions and their results within Sophos Connect. This includes failures resulting from user actions as well as IKE negotiation failures. To troubleshoot event errors, see [Troubleshooting events](#) (page 11).

- If verbose errors are required to troubleshoot a problem, click **Open VPN log**.
- To remove events from the list, click **Clear events**.



The screenshot shows the Sophos Connect interface with the 'Events' tab selected. The table contains three rows of event data, each with a green checkmark icon in the 'Occurred' column. A blue 'Clear events' button is located in the top right corner of the table area.

Occurred	Description
2019-4-1 2:55:10 PM	Initializing
2019-4-1 2:55:10 PM	Sophos Connect version: 1.2.924.0327
2019-4-1 2:55:10 PM	strongSwan version: 5.7.1

## 3.1 Troubleshooting events

If you have issues connecting, click on **Events**, look at the timestamp from when you attempted a connection, and find the relevant error. In this section you will see the error messages, possible causes for the errors, and information on what to do next. If you experience any issues that are not listed below, please contact [Sophos Support](#)

### No internet connection available

**Cause:** The client is unable to get a response to an ICMP request from a public address on the internet.

**What to do:** Check that you have a valid IP address, and that your existing network connection is working.

### DNS resolution failed for gateway: <gateway>

**Cause:** The client is not able to resolve the gateway host name.

**What to do:** Check if a DNS server is assigned to the network interface. Do an `nslookup` for a public host, for example [www.sophos.com](http://www.sophos.com) and verify that it resolves to an IP address. If it does not resolve, contact your ISP.

### The IKE UDP port seems to be blocked

**Cause:** The Sophos XG Firewall or the router is blocking UDP ports 500 and 4500.

**What to do:** Check your local Sophos XG Firewall or router configuration and allow traffic on these ports. If you do not have access to the Sophos XG Firewall or router, for example if you are in a hotel, connect through your mobile hotspot and try to connect again.

### No response from gateway: <gateway FQDN or IP specified in connection>

**Cause:** The gateway is not responding to IKE negotiation messages. This may be because:

- The remote gateway (Sophos XG Firewall or router) has been shut down.
- The WAN address on the remote gateway is not connected directly to the internet.

**What to do:** Contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.

### Received NO\_PROPOSAL\_CHOSEN notification from gateway

**Cause:** The remote gateway responded back to IKE negotiations from Sophos Connect with this error notification. This may be because:

- The Sophos Connect policy is not defined or activated on the Sophos XG Firewall .

- The Sophos XG Firewall administrator changed the IKE Phase 1 proposals used for the Sophos Connect policy on the Sophos XG Firewall and the new configuration was not exported and uploaded to the client.

**What to do:** Contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.

### ID mismatch. Expected %%1%% but got %%2%%

**Cause:** The local ID type or value configured in the Sophos Connect policy on the Sophos XG Firewall is different than the value used for this connection. This may be because the Sophos XG Firewall administrator changed the local ID on the Sophos XG Firewall and the new configuration file was not imported to Sophos Connect.

**What to do:** Contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.

### Incorrect PSK

**Cause:** The pre-shared key on the Sophos XG Firewall does not match the one used for this connection. This may be because the Sophos XG Firewall administrator changed it on the Sophos XG Firewall and the new configuration file has not been uploaded to Sophos Connect.

**What to do:** Contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.

### User authentication failed. Please try again

**Cause:** The username or password did not match.

**What to do:** Retry to see if it was a due to a user input error. If you retry multiple times and get the same error, the password may have changed or been disabled on the Sophos XG Firewall . In this case, contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.

### Failure to add route [network/mask] prevented Phase 2 completion

#### Note

The troubleshooting steps below are for Windows only.

**Cause:** After the Phase 2 SA (Security Association) is established, `route add` to the remote network failed. This may be because the strongSwan service crashed while the tunnel was active.

**What to do:** Disable and enable the TAP adapter. Open the command prompt as an administrator and type the following commands:

```
net stop scvpn
net start scvpn
```

## The connection data could not be added. Connection <connection name> already exists

A connection with this name already exists. If you continue, the existing connection will be overwritten. Continue?

**Cause:** A connection with the same name has already been imported.

**What to do:** Either delete the connection before you import or click OK to overwrite the existing connection with the same name.

## The connection could not be added - invalid configuration, The connection could not be parsed - unknown format, The connection could not be added - invalid format

**Cause:** Failed to import the connection file because the connection file (tgb or ini or scx) was manually modified with incorrect settings or invalid attributes or missing attributes.

**What to do:** Export a new connection file from Sophos XG Firewall, Sophos UTM or Sophos Connect Admin and then import it again.

## VPN service has been stopped

### Note

The troubleshooting steps below are for Windows only.

**Cause:** The Sophos Connect service (scvpn) is not running.

**What to do:** Open the command prompt as an administrator and type the following command:

```
net start scvpn
```

## Failed to load connection info

### Note

The troubleshooting steps below are for Windows only.

**Cause:** The strongSwan service is not running (Service Name: charon-svc.exe).

**What to do:** Open the command prompt as an administrator and type the following command:

```
net start strongswan
```

## Connection has been disabled by the gateway: <gateway>

**Cause:** The gateway sent an IKE delete request then the tunnel was deleted. This may be because:

- The Sophos XG Firewall administrator changed the policy on the Sophos XG Firewall . This sends an IKE delete request to all the active SAs (Security Associations) on the Sophos XG Firewall .

## Sophos Connect

- The Sophos XG Firewall administrator manually deleted all of the IPsec connections for this user on the Sophos XG Firewall .

**What to do:** Try to reconnect again. If it still does not work then contact your Sophos XG Firewall administrator and report the problem to troubleshoot further.



## 4 General troubleshooting

This section covers troubleshooting issues that do not appear on the **Events** page.

### Traffic stops going through the VPN tunnel

**Cause:** If you are running a firmware version prior to v17.5, it is possible that the client received a new virtual IP after the phase 1 rekey.

**What to do:** You will have to disconnect and reconnect. The permanent solution is to upgrade to v17.5.

### Sophos Connect dashboard will not open

**Cause:** If the Sophos Connect dashboard does not open, or it does not respond when you click on the tray icon, this means that the Sophos Connect GUI is stuck in an infinite loop and cannot respond to external input.

**What to do (Windows):** Open task manager and select the Details tab. Find scgui.exe and then right click to end task. Restart the application from the desktop shortcut.

**What to do (Mac):** Open Activity Monitor and find the Sophos Connect process. Open this process and select Force Quit. Restart the application from LaunchPad.

### Sophos Connect GUI displays "Service unavailable"

#### Note

This is more common on Macs.

**Cause:** When a tunnel disconnect is initiated, the strongSwan IPsec daemon gets stuck in an infinite loop. This will result in the GUI not getting a response for disconnect and ultimately timeout and show the error as "Service unavailable".

#### What to do:

1. Open the Activity Monitor and quit the Sophos Connect GUI process.
2. Open the Terminal and run the following commands:

```
sudo /bin/launchctl unload -w /Library/LaunchDaemons/
com.sophos.connect.scvpn.plist
```

```
sudo /bin/launchctl load -w /Library/LaunchDaemons/
com.sophos.connect.scvpn.plist
```

### Sophos Connect can't establish a tunnel

**Cause:** You probably installed the Sophos Connect client first and then installed the Sophos SSL VPN client.

**What to do:** Uninstall both clients then re-install the Sophos SSL VPN client and then the Sophos Connect client.

**Note**

They must be installed in that order.

## 5 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at [community.sophos.com/](https://community.sophos.com/) and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at [www.sophos.com/en-us/support.aspx](https://www.sophos.com/en-us/support.aspx).
- Download the product documentation at [www.sophos.com/en-us/support/documentation.aspx](https://www.sophos.com/en-us/support/documentation.aspx).
- Open a ticket with our support team at <https://secure2.sophos.com/support/contact-support/support-query.aspx>.

## 6 Legal notices

Copyright © 2019 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.