



**STORMSHIELD**



GUIDE

**STORMSHIELD NETWORK SSL VPN  
CLIENT**

# USER AND CONFIGURATION GUIDE

Version 5.1.1 EA

Document last updated: July 29, 2025

Reference: sns-en-ssl\_vpn\_client\_user\_and\_configuration\_guide-v5.1.1-EA



# Table of contents

Change log .....	3
Getting started with the Stormshield SSL VPN client .....	4
Presentation of the graphical interface and the menu bar .....	4
Presentation of the pop-up menu from the Stormshield SSL VPN client icon .....	5
Setting up an SSL VPN connection .....	6
Logging in to a connection with saved information .....	6
Logging in without saving connection information (Direct connection) .....	7
When an SSL VPN connection fails to set up .....	8
Managing saved connections .....	10
Adding, editing or deleting saved connections .....	10
Adding a connection .....	10
Editing a connection .....	12
Deleting a connection .....	12
Importing saved connections .....	12
Exporting saved connections .....	12
Protecting access to saved connections with a password .....	13
Protecting access to saved connections .....	13
Changing the access password .....	13
Removing protection .....	13
Managing the list of favorite connections .....	13
Enabling the auto login option .....	14
Checking whether the auto login option is enabled .....	14
Enabling the auto login option on a saved connection .....	15
Viewing connection logs .....	16
Advanced use and configuration of the Stormshield SSL VPN client .....	17
Advanced use case .....	17
SSL VPN connection - Manually validating the certificate presented by the server .....	17
Single sign-on - canceling authentication .....	17
Advanced configuration case .....	18
If you misplace your password to access saved connections .....	18
Enabling debug logs .....	19
Further reading .....	20



## Change log

---

Date	Description
July 29, 2025	New document



# Getting started with the Stormshield SSL VPN client

Welcome to the Stormshield Network SSL VPN Client version 5.1.1 EA user and configuration guide.



In this guide, Stormshield Network SSL VPN Client is named "Stormshield SSL VPN client".

SSL VPN allows remote users to securely access a organization's resources - internal or otherwise - via the SNS firewall.

The Stormshield SSL VPN client has a graphical interface that makes it possible to set up an SSL VPN connection, and to configure its settings. The client is available in French and English. The language used depends on the language that was selected in the user's session settings. If the chosen language is not supported, the Stormshield SSL VPN client will use English by default.

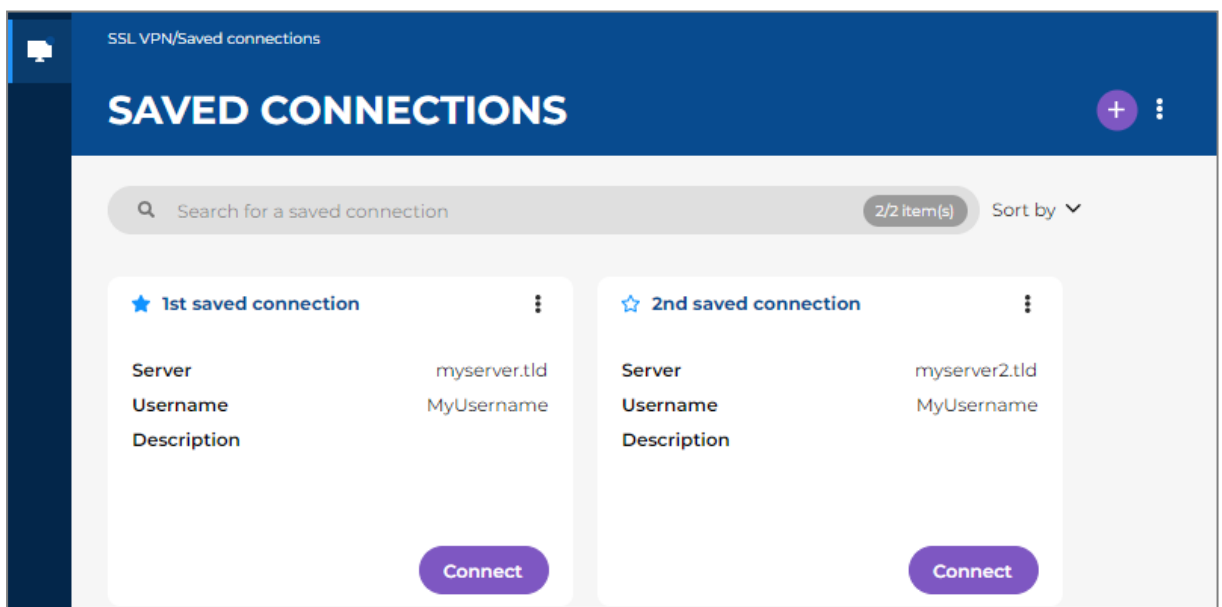
## Presentation of the graphical interface and the menu bar

To open the graphical interface:

- In Windows and some Linux environments: click on the  icon of the Stormshield SSL VPN client in the system tray.
- In macOS and some Linux environments: click on the  icon of the Stormshield SSL VPN client in the system tray, then click on **Open**.

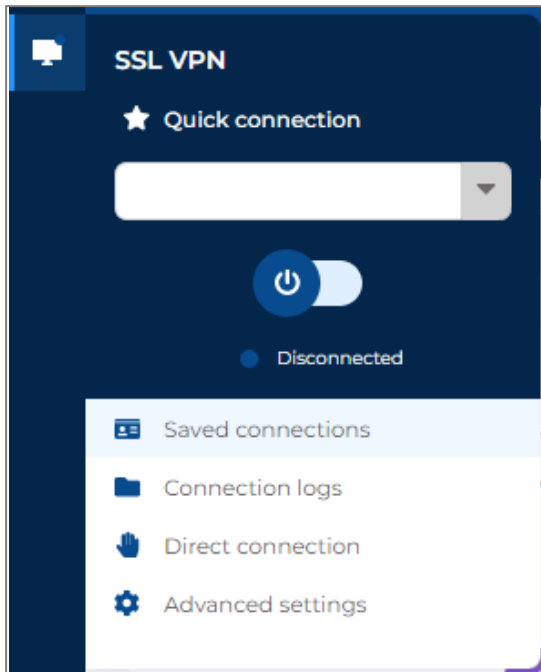
The graphical interface consists of:

- A menu bar on the left. By scrolling over the icon in the shape of a monitor, the Stormshield SSL VPN client general menu appears.
- A main window containing information on the selected menu. In the screen capture below, the window of saved connections appears.





The Stormshield SSL VPN client menu bar provides access to the following menus:



- **Quick connection:** the drop-down menu makes it possible to select the last connection used, or a favorite connection, then log in with the connection button.  
The current status of the connection appears.
- **Saved connections:** makes it possible to manage a list of saved connections, and to log in to a saved connection.
- **Connection logs:** makes it possible to display connection events on the Stormshield SSL VPN client.
- **Direct connection:** makes it possible to log in by manually entering connection information without saving it.
- **Advanced settings:** provides access to advanced parameters on the Stormshield SSL VPN client.

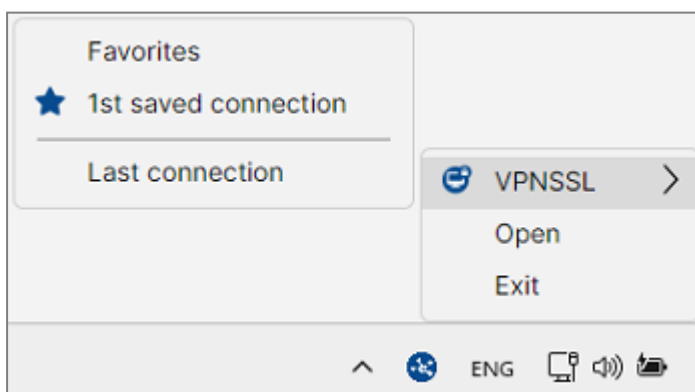
## Presentation of the pop-up menu from the Stormshield SSL VPN client icon

To open the pop-up menu, right-click on the  icon of the Stormshield SSL VPN client in the system tray.

The Stormshield SSL VPN client pop-up menu provides access to the following menus:

- **VPNSSL:** makes it possible to log in to the last connection used, or a favorite connection. The user can also log out if an SSL VPN is currently connected.
- **Open:** makes it possible to open the Stormshield SSL VPN client graphical interface.
- **Exit:** makes it possible to quit the application.

The screen capture below shows the pop-up menu of the Stormshield SSL VPN client in Windows. Visuals may vary according to the operating system used.





## Setting up an SSL VPN connection

### **i** NOTE

Only one SSL VPN connection can be set up at a time.

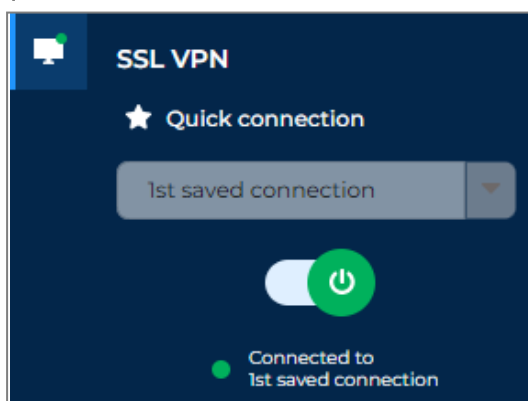
### Logging in to a connection with saved information

1. You can log in to a connection with saved information from the following menus:
  - From the drop-down list in the **Quick connection** menu, select the connection to which you wish to log in, then click on the connection button . You can select the last connection used or a **favorite connection**.
  - In the **Saved connections menu**, in the section of the saved connection to which you wish to log in, click on **Connect**.
  - In the **pop-up menu** of the Stormshield SSL VPN client icon , select **VPNSSL**, then click on the connection to which you wish to log in. You can select the last connection used or a **favorite connection**.
2. If additional information is required in order to log (such as an OTP), enter it. If single sign-on is used, authenticate on the portal, which will open automatically in your web browser, allowing you to connect.
3. Wait while the Stormshield SSL VPN client connects.

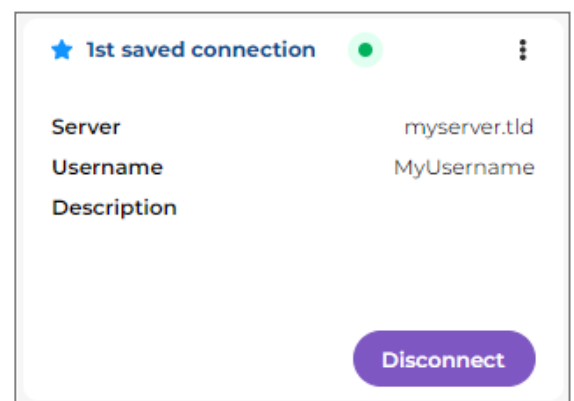
Once it is connected, the icon of the Stormshield SSL VPN client and the connection button in the **Quick connection** menu both turn green. If the connection is unsuccessful, refer to the section **When an SSL VPN connection fails to set up**.

You can log out by clicking out on **Disconnect** or on the connection button.

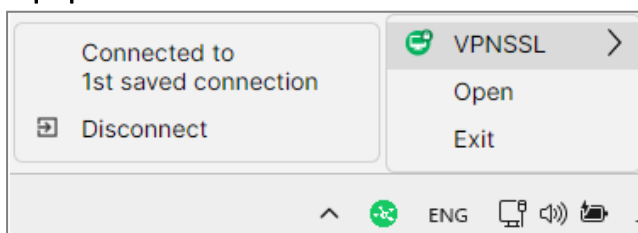
**Quick connection menu**



**Saved connections menu**



**Pop-up menu**





## Logging in without saving connection information (Direct connection)

You can log in through the **Direct connection** menu. Any information entered will not be saved.

### **i** NOTE

To save connection information, you need to create a saved connection. To do so, refer to the section [Adding, editing or deleting saved connections](#).

SSL VPN/Direct connection

## DIRECT CONNECTION

Stormshield mode Import OVPN file

**General**

Server \* Port \*

443

**Authentication**

☐ Connect with single sign-on

Username

Password

☐ Use an OTP

Connect

1. Choose from either of 2 available modes:

Connection mode	Description
Stormshield mode	This mode has to be used with an SNS firewall. In this mode, the Stormshield SSL VPN client automatically retrieves the SSL VPN configuration, and sends information that enables the SNS firewall to verify the client workstation's compliance [ZTNA].
Import OVPN file	This mode makes it possible to import an OpenVPN configuration file (OVPN format), and to connect to the OpenVPN gateway that provided the file.

2. Fill in the required fields based on the selected mode.





### Stormshield mode

Field/checkbox	Description
Server	IPv4 address or FQDN of the SNS firewall to contact in order to set up the connection.
Port	Server port [443 by default]. If the port of the SNS firewall's captive portal is different from the default port [TCP/443], enter the port used in this field.
Connect with single sign-on	Select this checkbox to connect with single sign-on. With single sign-on, after the connection has been initiated, authenticate on an authentication portal that opens in your web browser, for example the SNS firewall's captive portal or the portal of the Identity as a Service (IDaaS) platform chosen on the SNS firewall, such as Microsoft Entra ID. If this option is selected, the <b>User name</b> , <b>Password</b> and <b>Use an OTP</b> fields will be hidden.
Username	User name.
Password	User's password.
Use an OTP	Select the checkbox if you are using multifactor authentication (such as the Stormshield TOTP solution), and an OTP (one-time password) is required in order to connect. If this option is selected, the <b>OTP</b> field appears.
OTP	OTP to be entered in order to connect.

### Importing OVPN files

Field	Description
Drag & drop/Browse	OVPN file that you wish to import.
Username	User name.
Password	User's password.

3. Click on **Connect**.
4. If single sign-on is used, authenticate on the portal, which will open automatically in your web browser, allowing you to connect.
5. Wait while the Stormshield SSL VPN client connects.

Once it is connected, the  icon of the Stormshield SSL VPN client and the connection button  in the **Quick connection** menu both turn green. If the connection is unsuccessful, refer to the section [When an SSL VPN connection fails to set up](#).

You can log out by clicking out on **Disconnect** or on the connection button.

### When an SSL VPN connection fails to set up

- Read the error message that appears. If necessary, you can find it in the [Connection logs menu](#).
- Check the connection information that has been entered, either in the [Direct connection menu](#), or in the [settings of the saved connection](#).





- If the **Use an OTP** checkbox has been selected, check the validity of the OTP entered. The Stormshield SSL VPN client will make several attempts to connect if no response is received, but the OTP may expire in the meantime.
- If a warning message appears regarding a probable security risk, this means that the certificate presented to the Stormshield SSL VPN client cannot be automatically validated. For more information, refer to the section [SSL VPN connection - Manually validating the certificate presented by the server](#).



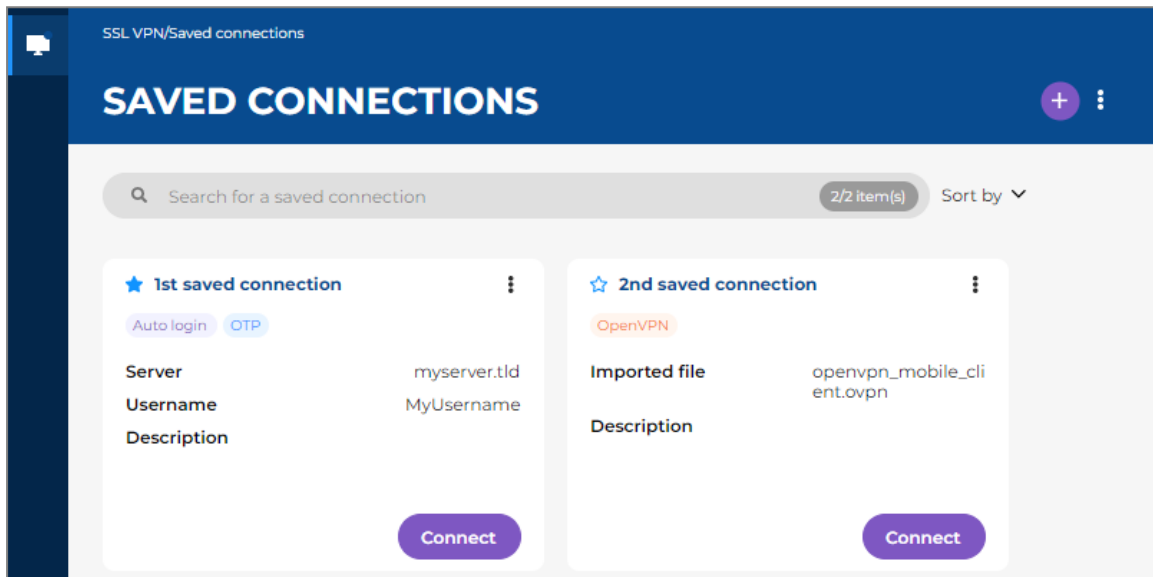
## Managing saved connections

This section explains how to manage saved connections on the Stormshield SSL VPN client.

In **Saved connections**, you can save information regarding your connections.

In the window, each section represents a saved connection. You will find the name of the connection in the window, as well as the server, labels identifying certain parameters (use of an OTP or single sign-on, auto login enabled, "OpenVPN" connection, etc.).

If there are no saved connections, you can add them.



### Adding, editing or deleting saved connections

#### Adding a connection

1. In **Saved connections**, click on the **+** button at the top to the right of the window. If there are no saved connections, you can also click on the **Add a connection** button in the middle.
2. Choose from either of 2 available modes:

Connection mode	Description
Stormshield mode	This mode has to be used with an SNS firewall. In this mode, the Stormshield SSL VPN client: <ul style="list-style-type: none"><li>• Automatically retrieves the SSL VPN configuration. The client will then check whether the configuration requires an update every time it connects.</li><li>• Sends information to the SNS firewall every time it connects, making it possible it to check the compliance of the client workstation (ZTNA).</li></ul>
Import OVPN file	This mode makes it possible to import an OpenVPN configuration file (OVPN format), and to connect to the OpenVPN gateway that provided the file.

3. Fill in the required fields based on the selected mode.



### Stormshield mode

Field/checkbox	Description
Name	Name of the connection.
Server	IPv4 address or FQDN of the SNS firewall to contact in order to set up the connection.
Port	Server port (443 by default). If the port of the SNS firewall's captive portal is different from the default port (TCP/443), enter the port used in this field.
Description	Description of the connection, if necessary.
Connect with single sign-on	Select this checkbox to connect with single sign-on. With single sign-on, after the connection has been initiated, authenticate on an authentication portal that opens in your web browser, for example the SNS firewall's captive portal or the portal of the Identity as a Service (IDaaS) platform chosen on the SNS firewall, such as Microsoft Entra ID. If this option is selected, the <b>User name</b> , <b>Password</b> and <b>Use an OTP</b> fields will be hidden.
Username	User name. If you do not fill in this field, you have to enter the user name every time you connect.
Password	User's password. If you do not fill in this field, you have to enter the password every time you connect.
Use an OTP	Select the checkbox if you are using multifactor authentication (such as the Stormshield TOTP solution), and an OTP (one-time password) is required in order to connect. If this option is selected, you will need to enter an OTP every time you wish to connect.
Connect automatically	Select this checkbox to log in automatically to this connection when the Stormshield SSL VPN client starts. This option can only be enabled on a single connection. Do note that you will need to manually log in if access to saved connections is password-protected, if an OTP is used for the connection, or if the user name and password have to be entered. For more information, refer to the section <a href="#">Enabling the auto login option</a> .

### Import OVPN file


Field	Description
Drag & drop/Browse	OVPN file that you wish to import.
Name	Name of the connection.
Description	Description of the connection, if necessary.
Username	User name.
Password	User's password.




Field	Description
Connect automatically	Select this checkbox to log in automatically to this connection when the Stormshield SSL VPN client starts. This option can only be enabled on a single connection.  Do note that you will need to manually log in if access to saved connections is password-protected, if an OTP is used for the connection, or if the user name and password have to be entered.  For more information, refer to the section <a href="#">Enabling the auto login option</a> .

4. Click on **Add**.

### Editing a connection

1. In **Saved connections**, in the section of the connection that you wish to edit, click on the  button, and on **Edit**.
2. Edit the connection settings. If necessary, refer to the descriptions of the fields above.
3. Click on **Edit** to save changes.


### Deleting a connection

1. In **Saved connections**, in the section of the connection that you wish to delete, click on the  button, and on **Delete**.
2. Click on **Delete** to confirm.


### Importing saved connections

#### IMPORTANT

When saved connections are imported, they **overwrite and replace** saved connections that are currently available with those contained in the imported .book file.

1. In **Saved connections**, click on the  button at the top to the right of the window, then click on **Import**.
2. Select the .book file containing the saved connections that you wish to import, then click on **Open**.
3. If the .book file is password-protected, enter the password in the window that appears, then click on **Import**.



### Exporting saved connections

1. In **Saved connections**, click on the  button at the top to the right of the window, then click on **Export**.
2. Select the location to save the .book file that contains exported saved connections, give it a name, and then click on **Save**.
3. If you wish to protect the .book file with a password, set a password in the window that appears. Leave the field empty if file protection is not required. This password has to be entered when the file is imported.  
Click on **Export** to export the file.



## Protecting access to saved connections with a password

### Protecting access to saved connections


1. In **Saved connections**, click on the  button at the top to the right of the window, then click on **Protect**.
2. Enable the parameter **Enable password protection** .
3. Set the access password, and confirm it. Keep the password in a safe and protected location. Stormshield will not be able to help you recover your password if you misplace it. For more information, refer to the section [If you misplace your password to access saved connections](#).
4. Click on **Change password**.

Access to saved connections is protected. The chosen password has to be entered when the Stormshield SSL VPN client is opened to allow access to saved connections.



#### NOTE

If the auto login option is enabled on a saved connection, the access password has to be entered so that the automatic connection can be set up.

### Changing the access password

1. In **Saved connections**, click on the  button at the top to the right of the window, then click on **Change password**.
2. Enter the current access password.
3. Set the new access password, and confirm it. Keep the password in a safe and protected location. Stormshield will not be able to help you recover your password if you misplace it. For more information, refer to the section [If you misplace your password to access saved connections](#).
4. Click on **Change password**.



### Removing protection

1. In **Saved connections**, click on the  button at the top to the right of the window, then click on **Change password**.
2. Disable the parameter **Enable password protection** .
3. Enter the access password.
4. Click on **Disable protection**.

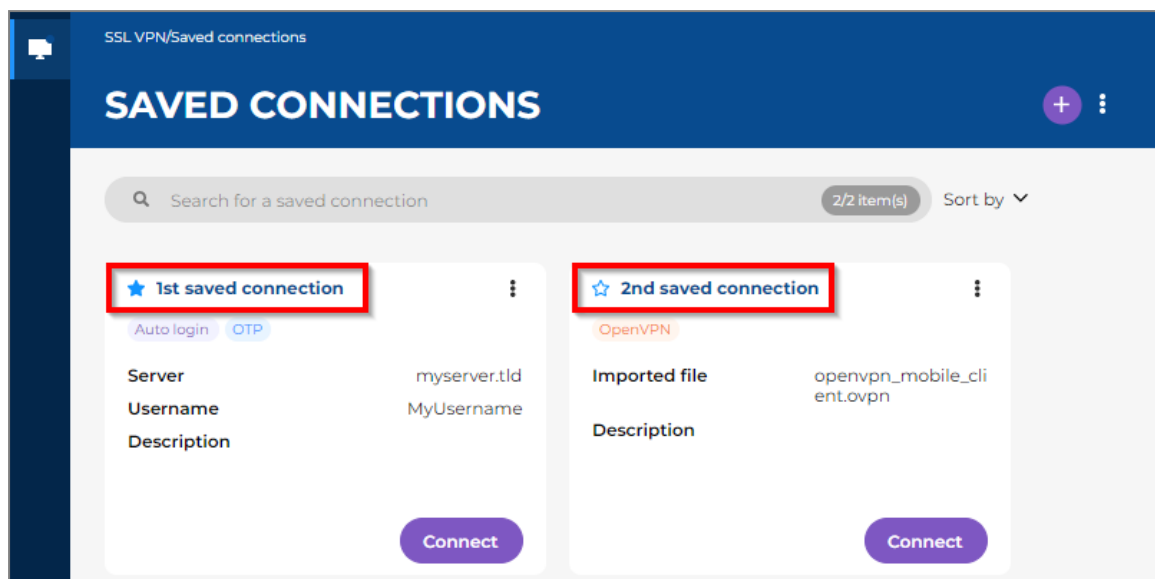
## Managing the list of favorite connections

Saved connections can be added to the list of favorite connections.


In the **Saved connections** menu, a star icon appears to the left of each saved connection.

- The  icon indicates a connection that is not in the list of favorite connections.
- The  icon indicates a favorite connection.

You can add or remove saved connections from the list of favorite connections by clicking on the star icon.



You can select a favorite connection to [set up an SSL VPN connection](#) in the following menus:

- The **Quick connection** menu,
- The **pop-up menu** of the Stormshield SSL VPN client icon .

## Enabling the auto login option

You can log in automatically to a saved connection when the Stormshield SSL VPN client starts. This option can only be enabled on a single connection.

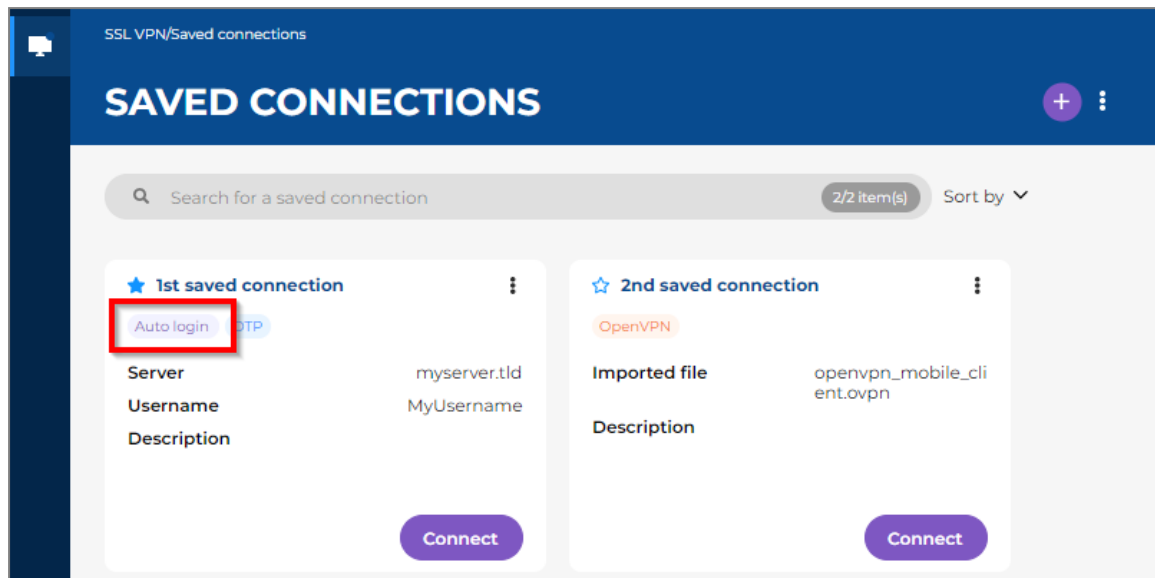
### NOTE

You will need to manually log in if access to saved connections is password-protected, if an OTP is used for the connection, or if the user name and password have to be entered.

## Checking whether the auto login option is enabled

In **Saved connections**, an "*Auto login*" label appears in the section of a saved connection if the **Connect automatically** option is enabled.

You can use the sort function to find saved connections that have this option.



### Enabling the auto login option on a saved connection

1. In **Saved connections**, in the section of the connection that you wish to edit, click on the **Edit** button, and on **Edit**.
2. Select the **Connect automatically** checkbox.
3. Click on **Edit** to save changes.
4. If the auto login option is already enabled on another saved connection, you need to indicate whether you wish to replace it with the connection currently being edited. Click on **Replace** to confirm the changes.



## Viewing connection logs

In **Connection logs**, you can view connection events on the Stormshield SSL VPN client.

You will find the following events in these logs:

Event	Description
Connected	The SSL VPN connection has been properly set up.
Connection shut down	The SSL VPN connection has been shut down, and the user has been logged out.
Connection lost	The SSL VPN connection with the server has been lost.
Server unreachable	The Stormshield SSL VPN client did not manage to reach the server to set up the SSL VPN connection.
Security warning	The certificate that was presented by the server did not guarantee that the connection was secure. For more information, refer to the section <a href="#">SSL VPN connection - Manually validating the certificate presented by the server</a> .
Authentication error	The name and password that were entered were not able to authenticate the user. There may be other reasons for this message appearing.

You can also search for an event by entering either the name of the saved connection or the server address in the search field.





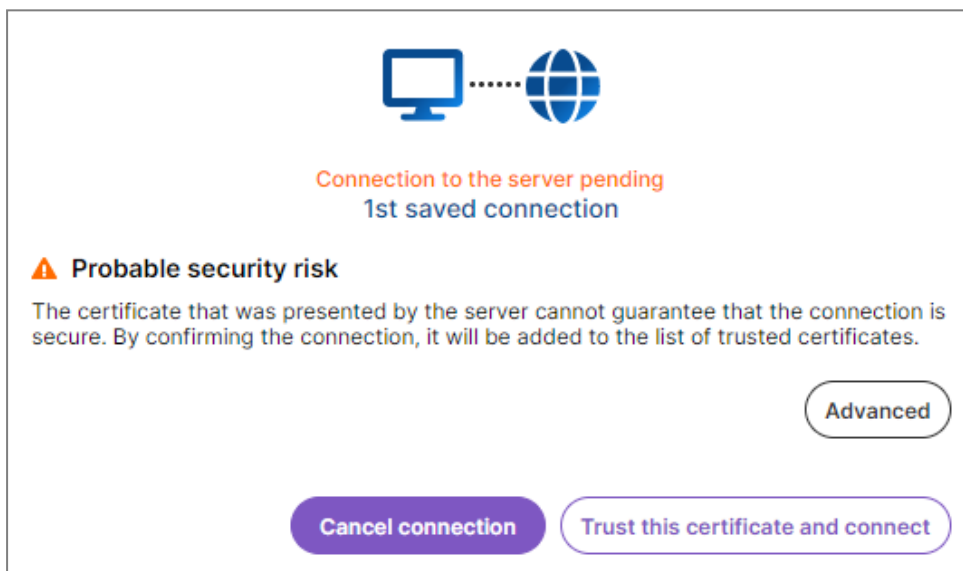
# Advanced use and configuration of the Stormshield SSL VPN client

This section explains several advanced scenarios in the use and configuration of the Stormshield SSL VPN client.

## Advanced use case

### SSL VPN connection - Manually validating the certificate presented by the server

When a certificate that is presented to the Stormshield SSL VPN client cannot be automatically validated, the message "Probable security risk" appears. You will then need to indicate whether to trust the certificate and connect, or cancel the connection.



To help you with the process, you can view information on the certificate and its trust chain by clicking on **Advanced**. > **Show certificate**.

When you choose to trust the certificate and connect, the information (certificate hash) is saved for the connection used. The choice to trust the certificate is specific to that connection, and not to the server to which you are connecting. This message will appear again if you are connecting to the same server over another connection (saved or from the **Direct connection** menu).

### Single sign-on - canceling authentication

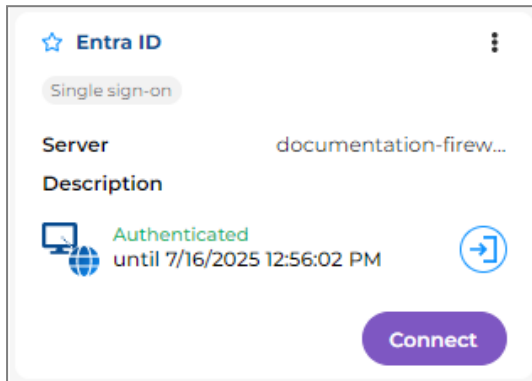
With single sign-on, after a connection has been initiated, authenticate on an authentication portal that opens in your web browser, for example the SNS firewall's captive portal or the portal of the Identity as a Service (IDaaS) platform chosen on the SNS firewall, such as Microsoft Entra ID.

Once the Stormshield SSL VPN client has authenticated over this portal, it can set up the SSL VPN connection.

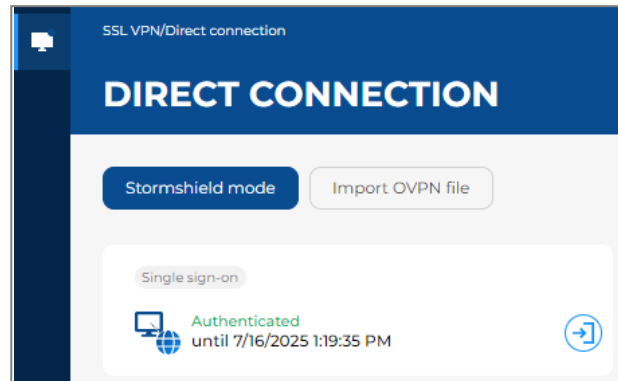


In the **Saved connections** and **Direct connection** menus, you will see the remaining time until your authentication expires. As long as the time has not run out, and you are still authenticated on the SNS firewall, you can set up SSL VPN connections.

Saved connections menu




Direct connection menu



You can manually cancel your authentication before it expires, by submitting a request to your organization's administrator. If an SSL VPN is currently connected, simply canceling authentication will not disconnect it.

To cancel authentication:

1. In **Saved connections**, click on the  button to the right of the remaining time before your authentication expires.
2. Click on **OK**.

## Advanced configuration case

### If you misplace your password to access saved connections

You will not be able to reset the access password, and Stormshield is not in a position to recover it. As a last resort, if you cannot remember the password, you will need to delete the folder containing the file of saved connections.

To access this folder and delete it, you must hold the required privileges on the workstation.

This folder can be found in the following locations:

- In Windows:

C:\ProgramData\Stormshield\SSL VPN Client\Addressbooks\

- In Linux:

/var/lib/stormshield/sslvpnclient/addressbooks/

- In macOS:


/Library/Application Support/Stormshield/SSL VPN Client/Addressbooks/

In this folder, each sub-folder corresponds to a user's saved connections. If only one sub-folder exists, this means that only one user has added saved connections. If there are several sub-folders, you need to identify the right sub-folder to delete, for example by checking when they were last modified.

When you are ready, quit the Stormshield SSL VPN client, delete the folder, and start the Stormshield SSL VPN client again.



## Enabling debug logs

1. Go to the **Advanced settings** menu in the graphical interface, **General** tab.
2. Enable the setting **Enable debug logs** .

These logs are found at the following locations. To access the service's logs, you must hold the required privileges on the workstation.

- In Windows:

- Service logs:

```
C:\ProgramData\Stormshield\SSL VPN Client\Logs\
```

- User logs:

```
C:\Users\<user>\AppData\Local\Stormshield\SSL VPN Client\Logs\
```

- In Linux:

- Service logs:

```
/var/log/stormshield/sslvpnclient/
```

- User logs:

```
$HOME/.local/share/stormshield/sslvpnclient/logs/
```

- In macOS:

- Service logs:

```
/Library/Application Support/Stormshield/SSL VPN Client/Logs/
```

- User logs:

```
/Users/<user>/Library/Application Support/Stormshield/SSL VPN Client/Logs/
```



## Further reading

---

For further information regarding the installation of the Stormshield SSL VPN client, refer to the [Stormshield SSL VPN client installation guide v5](#).

To configure the SSL VPN service on the SNS firewall, refer to the [SSL VPN](#) section of the *SNS user guide* in the relevant version.

Additional information and responses to questions you may have about the Stormshield SSL VPN client are available in the [Stormshield knowledge base](#) (authentication required).



# STORMSHIELD

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*