



STORMSHIELD



GUIDE

STORMSHIELD SSL VPN CLIENT

USER AND CONFIGURATION GUIDE

Version 5.1

Document last updated: April 20, 2026

Reference: [sns-en-ssl_vpn_client_user_and_configuration_guide-v5.1](#)



Table of contents

Change log	4
Getting started with the Stormshield SSL VPN client	5
Overview of the graphical interface and menus of the Stormshield SSL VPN client	6
Available languages	6
Overview of the graphical interface	6
Overview of the general menu	6
Overview of the pop-up menu	7
Setting up a secure connection	8
Setting up a saved connection	8
Setting up a direct connection (without saving information)	9
Setting up a connection using single sign-on	9
When a connection error occurs	10
First things to check	10
Error messages	10
Other errors	11
Managing saved connections	12
Adding, editing or deleting saved connections	12
Adding a saved connection	12
Editing a saved connection	13
Description of connection modes and available fields	13
Deleting a saved connection	15
Exporting saved connections	16
Importing saved connections	16
Protecting access to saved connections with a password	17
Protecting access to saved connections	17
Changing the access password	17
Removing protection	18
If the access password is misplaced	18
Managing the list of favorite connections	19
Enabling the auto login option	19
Checking whether the auto login option is enabled	19
Enabling the auto login option on a saved connection	20
Viewing connection logs	21
Advanced use and configuration of the Stormshield SSL VPN client	22
Viewing debug logs	22
Enabling debug logs	22
Accessing debug logs	22
Configuring the Stormshield SSL VPN client through a command line interface	23
Using the command line interface	23
List of commands	23
Further reading	24
Appendix: Retrieving the SSL VPN configuration (OVPN file)	25
Retrieving the OVPN file from the SNS firewall captive portal	25



Retrieving the OVPN file from the SNS firewall's web administration interface 26



Change log

Date	Description
April 20, 2026	<ul style="list-style-type: none">- Name of "Import OVPN file" mode changed to "OpenVPN mode" in the sections "Setting up a secure connection" and "Adding, editing or deleting saved connections"
December 16, 2025	<ul style="list-style-type: none">- Information regarding single sign-on added to the section "Setting up a secure connection"- Information regarding the use of the Stormshield SSL VPN client with an OpenVPN gateway, other than the one used on SNS firewalls, added to the sections "Setting up a secure connection" and "Adding, editing or deleting saved connections"- Information regarding the message "<i>The VPN configuration has been updated.</i>" added to the section "Setting up a secure connection"- Information regarding multifactor authentication (OTP) added to the section "Adding, editing or deleting saved connections"- Information regarding access to saved connections added to the section "Protecting access to saved connections with a password"- Link to the procedure "Deploying saved connections through a group policy (GPO)" added to the section "Importing saved connections"
October 22, 2025	<ul style="list-style-type: none">- Information regarding single sign-on added to the section "Setting up a secure connection"- Information regarding the message "<i>Probable security risk</i>" added to the section "Setting up a secure connection"- Information regarding fields in a connection added to the section "Adding, editing or deleting saved connections"- Information on how to retrieve a misplaced access password added to the section "Protecting access to saved connections with a password"- Information regarding the use of the auto login option added to the section "Enabling the auto login option"- New section "Appendix: Retrieving the SSL VPN configuration (OVPN file)" added- New section "Configuring the Stormshield SSL VPN client through a command line interface" added- Link to the Stormshield SSL VPN client v5 administration guide added
July 29, 2025	<ul style="list-style-type: none">- New document



Getting started with the Stormshield SSL VPN client

Welcome to the Stormshield SSL VPN Client version 5.1 user and configuration guide.

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

This guide explains:

- The graphical interface and menus of the Stormshield SSL VPN client,
- How to use the Stormshield SSL VPN client, particularly the process of setting up secure connections,
- The configuration of the Stormshield SSL VPN client, particularly managing saved connections.





Overview of the graphical interface and menus of the Stormshield SSL VPN client

The Stormshield SSL VPN client has a graphical interface that makes it possible to set up secure connections, and to configure its settings.


Available languages

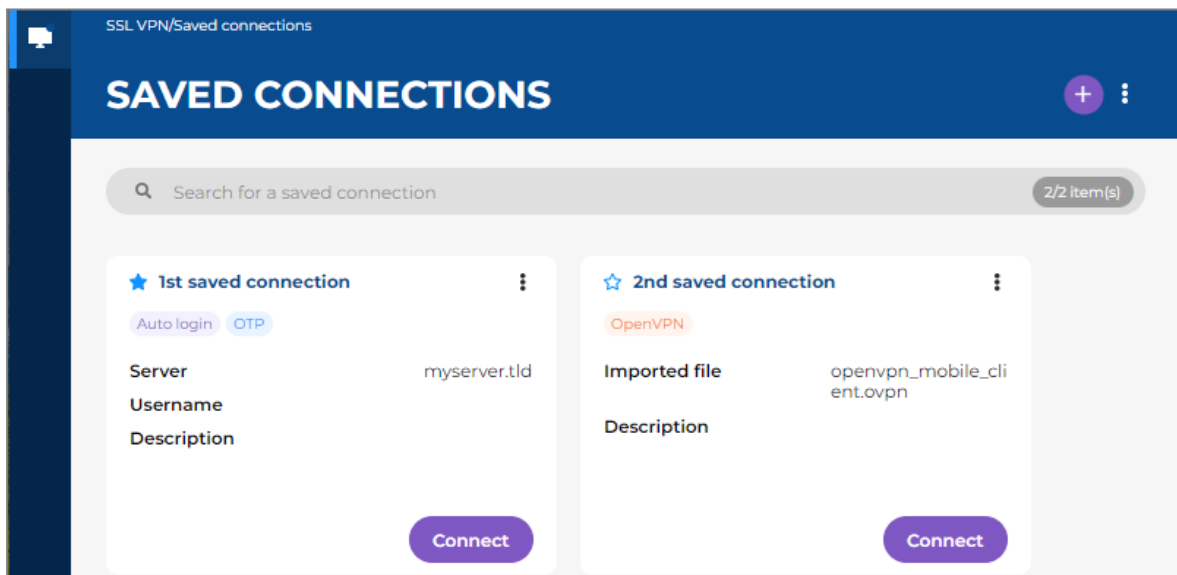
The Stormshield SSL VPN client is available in French and English. The language used depends on the language that was selected in the user's session settings. If the chosen language is not supported, the Stormshield SSL VPN client will use English by default.

Overview of the graphical interface



To open the Stormshield SSL VPN client graphical interface, click on the icon  in the system tray. In macOS and some Linux environments: click on the  icon, and on **Open**.

The Stormshield SSL VPN client's graphical interface consists of:



- A general menu that can be accessed by scrolling over the  icon in the shape of a monitor on the left,
- A main window containing information on the selected menu.



Overview of the general menu

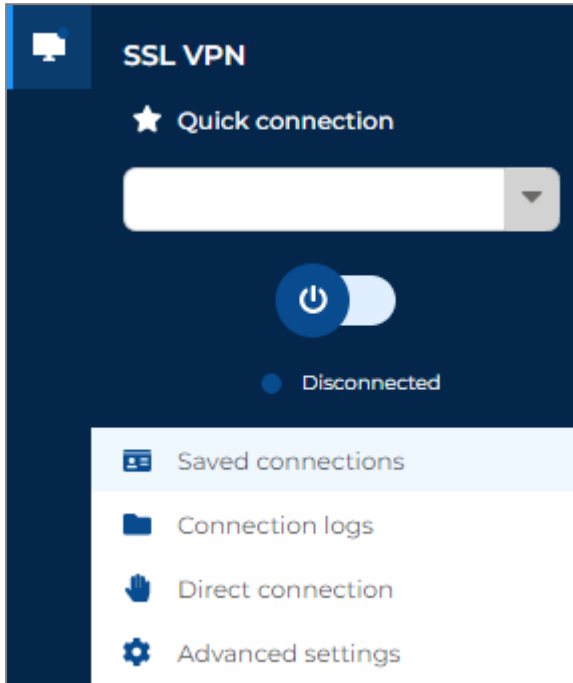
To open the general menu of the graphical interface, scroll over the  icon in the shape of a monitor on the left. When there is an open connection, a green dot appears in the icon .

In the general menu, you can access the following menus:



- **Quick connection:** makes it possible to set up a connection. To connect, select a **favorite connection** or the last connection used from the drop-down list, and click on the button . To disconnect, click on the button .



- **Saved connections:** makes it possible to save connections and set up a saved connection,
- **Connection logs:** makes it possible to display connection events,
- **Direct connection:** makes it possible to set up a connection without saving information,
- **Advanced settings:** provides access to advanced parameters.



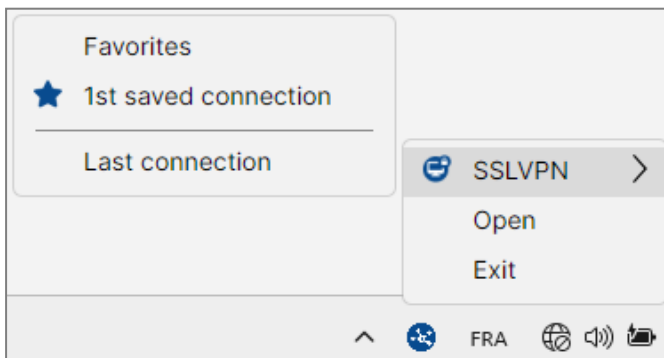
Overview of the pop-up menu

To open the Stormshield SSL VPN client pop-up menu, right-click on the icon  in the system tray. When there is an open connection, the  icon will be green.

In the pop-up menu, you can access the following menus:

- **SSLVPN:** makes it possible to set up a connection. To connect, click on a **favorite connection** or the last connection used. To disconnect, click on **Disconnect**.
- **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 in Windows. Visuals may vary according to the operating system used.





Setting up a secure connection

i NOTE
Only one connection can be set up at a time. In addition, shared workstations allow only one connection at a time.

Setting up a saved connection

A connection has to be saved in advance in the **Saved connections** menu.

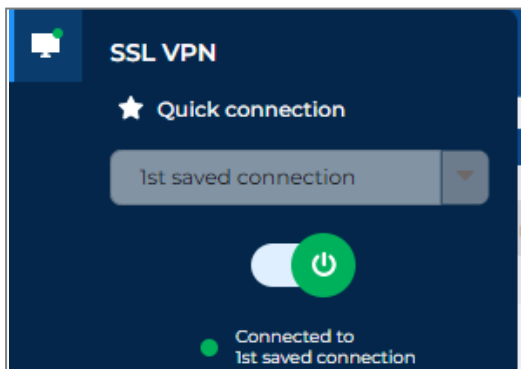
- To set up a saved connection:
 - In the **Quick connection** menu, select a **favorite connection** or the last connection used from the drop-down list, and click on the button
 - In the **Saved connections** menu, click on **Connect** in the section of a saved connection,
 - In the **pop-up menu** (click on the icon in the system tray), select **SSLVPN** and click on the last connection used or a **favorite connection**.
- If additional information is required to set up the connection, such as an OTP, enter it. If single sign-on is used, authenticate on the portal, which opens automatically in your web browser, to set up the connection.

Once you are logged in, the icon of the Stormshield SSL VPN client and the connection button both turn green. If an error occurs, refer to the section **When a connection error occurs**.

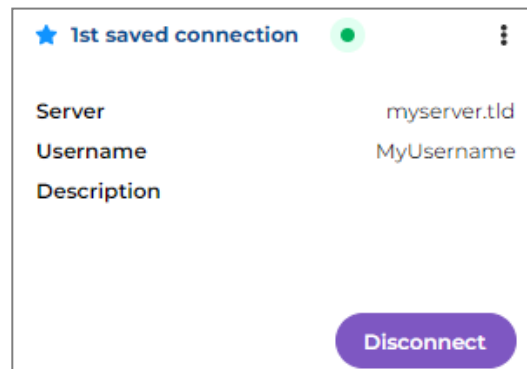
If single sign-on was used to set up the connection, the expiry date of your authentication session appears. For more information, see the section **Setting up a connection using single sign-on**.

Log out by clicking on **Disconnect** or on the connection button .

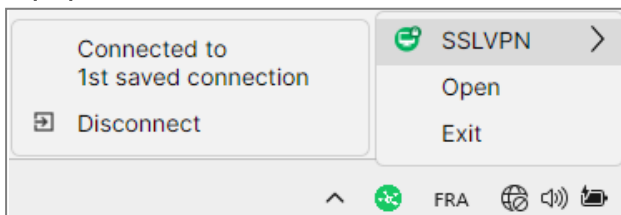
Quick connection menu



Saved connections menu



Pop-up menu





Setting up a direct connection (without saving information)

1. Go to the **Direct connection** menu.



The screenshot shows the 'DIRECT CONNECTION' configuration interface. At the top, there are two mode selection buttons: 'Stormshield mode' (highlighted in blue) and 'OpenVPN mode'. Below this, the 'General' section contains a 'Server *' text input field and a 'Port *' dropdown menu set to '443'. The 'Authentication' section includes a checkbox for 'Connect with single sign-on', a 'Username' text input field, a 'Password' text input field with a visibility toggle (eye icon), and a checkbox for 'Use an OTP'. A purple 'Connect' button is located at the bottom right of the form.

2. Choose between **Stormshield mode** and **OpenVPN mode**, and fill in the fields. If necessary, refer to the section [Description of connection modes and available fields](#).


i NOTE

The Stormshield SSL VPN client has been designed to connect to SNS firewalls in version 4 or 5. Methods that involve connecting to another OpenVPN gateway, or importing an OVPN file generated by another OpenVPN gateway, are not officially supported, and may not be guaranteed to function normally.

3. Click on **Connect**.
4. If single sign-on is used, authenticate on the portal, which opens automatically in your web browser, to set up the connection.

Once you are logged in, the  icon of the Stormshield SSL VPN client and the connection button  both turn green. If an error occurs, refer to the section [When a connection error occurs](#).

If single sign-on was used to set up the connection, the expiry date of your authentication session appears. For more information, see the section [Setting up a connection using single sign-on](#).

Log out by clicking on **Disconnect** or on the connection button .

Setting up a connection using single sign-on

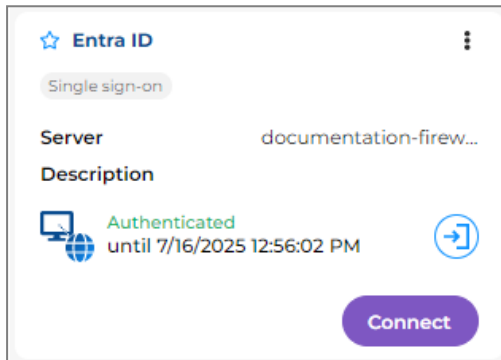
To set up a connection using single sign-on, you must first select **Stormshield mode** and the checkbox **Connect with single sign-on** in the details of the connection.



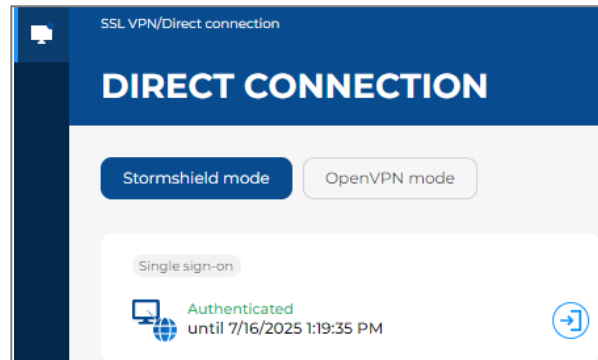
1. Set up the [saved connection](#) or [direct connection](#).
2. On the authentication portal that automatically opens in your web browser, follow the steps in the authentication process.
3. Once you are successfully authenticated, wait while the Stormshield SSL VPN client sets up the connection.

Once you are connected, the expiry date of your authentication session appears. As long as the expiry date remains in the future, you can set up the connection without having to authenticate again.


Saved connections menu



Direct connection menu



When requested by an administrator from your organization, you can cancel your authentication before it expires:

1. Click on the  button to the right of the date on which your authentication session expires.
2. Click on **OK**. This operation will not disconnect the connection that is currently set up.

When a connection error occurs

First things to check

- Read the error message that appears, as it may provide clues to the issue that has occurred. If necessary, you can find it in the [Connection logs](#) menu.
- Check the information that has been entered for the [saved connection](#) or [direct connection](#).
- If an OTP was used, check whether it is still valid. The Stormshield SSL VPN client will make several attempts to connect if no response is received, but the OTP may expire in the meantime.

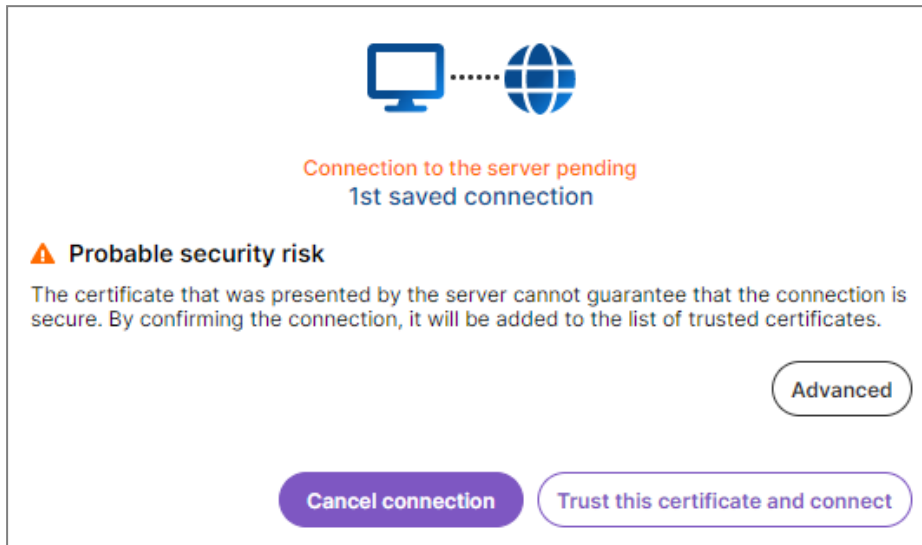
Error messages

- If the message *"The VPN configuration has been updated. Enter a new OTP to connect."* appears, this means that the Stormshield SSL VPN client has just retrieved a VPN configuration update from the SNS firewall.

The OTP (one-time password) that you entered made it possible to retrieve the new VPN configuration. As it is generated for a single use, this OTP can no longer be used. Wait for a new OTP to be generated in your OTP generator, then connect.



- If the warning message "*Probable security risk*" appears, this means that the certificate presented to the Stormshield SSL VPN client cannot be automatically validated. You will then need to indicate whether to trust the certificate and connect, or cancel the connection.



To do so, you need check whether the connection is secure. Click on **Advanced > Show certificate**, and verify the details of the certificate and its trust chain; if you are unable to decide, get in touch with an administrator from your organization.

If you choose to trust the certificate and connect, this decision will be saved for the connection used. The message will appear again if you use another saved connection or a connection from the **Direct connection** menu.

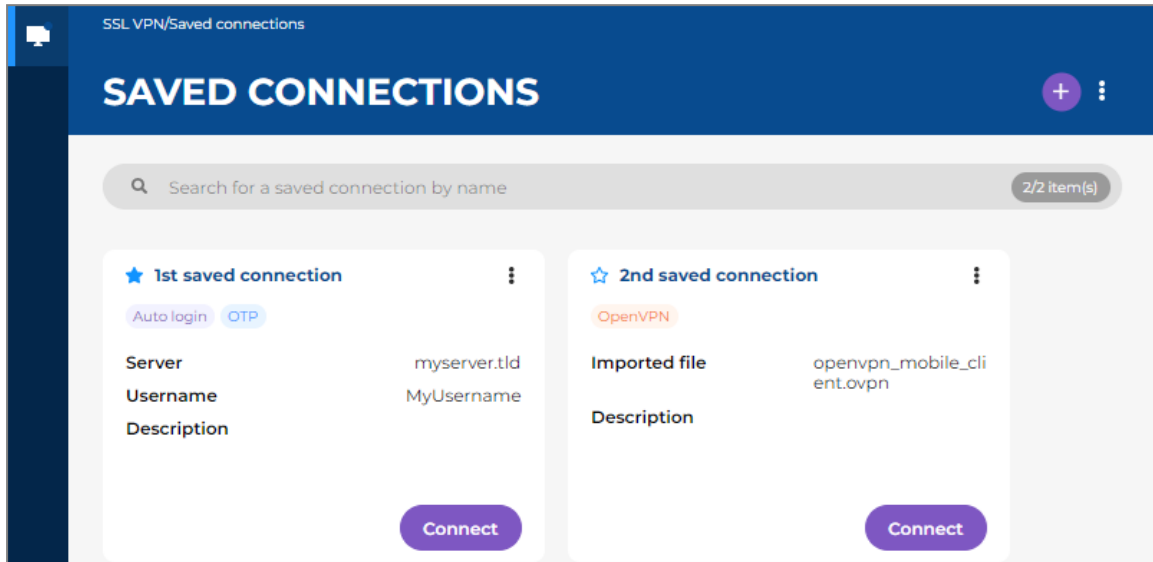
Other errors

- Ensure that the Stormshield SSL VPN client can reach the SNS firewall (this can be done by an administrator from your organization):
 - Check the configuration of the SSL VPN service and associated elements by referring to the [SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients](#).
 - If a hardened configuration is used on the organization's workstations (use of a firewall, for example), the Stormshield SSL VPN client may be unable to connect if some ports are unreachable. For further information on ports and protocols, refer to the [Stormshield SSL VPN client v5 installation guide](#).



Managing saved connections

Connections can be saved and managed in the **Saved connections** menu.



In the window, each section represents a saved connection. You will find the name of the connection, its server, as well as labels.

Label	Description
OTP	The use of OTPs is enabled on the connection.
Auto login	The auto login option is enabled on the connection.
Single sign-on	The use of single sign-on is enabled on the connection.
OpenVPN	OpenVPN connection (OVPN file import).

Adding, editing or deleting saved connections

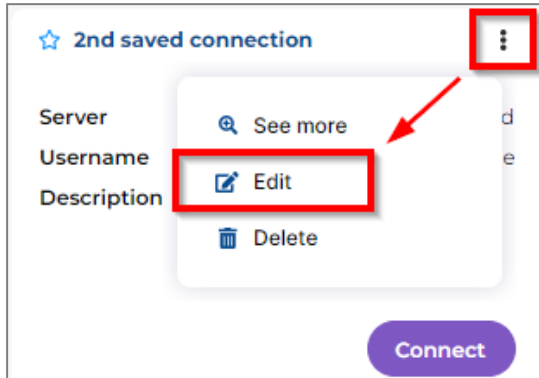
Adding a saved connection

1. Click on the **+** button at the top to the right, or on the button **Add a connection** at the center if there are no existing saved connections.
2. Choose between **Stormshield mode** and **OpenVPN mode**, and fill in the fields. If necessary, refer to the section [Description of connection modes and available fields](#).
3. Click on **Add**.



Editing a saved connection

1. For the saved connection in question, click on the button, and on **Edit**.



2. Edit the information. If necessary, refer to the section [Description of connection modes and available fields](#).
3. Click on **Edit** to save changes.

Description of connection modes and available fields

Connection modes

Mode	Description
Stormshield mode	In this mode, the Stormshield SSL VPN client can: <ul style="list-style-type: none"> • Connect and automatically retrieve the VPN configuration from the SNS firewall. Every time the connection is set up, the Stormshield SSL VPN client will check whether the VPN configuration needs to be updated. • Send the SNS firewall information on the client workstation to verify its compliance (ZTNA) every time the connection is set up.
OpenVPN mode	This mode makes it possible to import an OpenVPN (OVPN) configuration file provided by the SNS firewall, and to connect to its OpenVPN gateway.

NOTE

The Stormshield SSL VPN client has been designed to connect to SNS firewalls in version 4 or 5. Methods that involve connecting to another OpenVPN gateway, or importing an OVPN file generated by another OpenVPN gateway, are not officially supported, and may not be guaranteed to function normally.

Available fields with Stormshield mode

Field/checkbox	Description
Name	Name of the saved connection. This field does not appear in the Direct connection menu.
Server	FQDN or IPv4 address 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.



Field/checkbox	Description
Description	Description of the saved connection. This field does not appear in the Direct connection menu.
Connect with single sign-on	Select this checkbox to set up the connection using single sign-on. You will then need to authenticate on a portal, which automatically opens in your web browser to set up the connection. For more information, see the section Setting up a connection using single sign-on . If this option is selected, the User name , Password and Use an OTP fields will be hidden. ! IMPORTANT Select this checkbox only if the SNS firewall is in version 5.
Username	User name.
Save password	Select the checkbox to save the connection password. When a connection is being modified, if a password has already been saved, unselect the checkbox to stop saving it.
Password	User's password. Leave this field empty if you are not saving the password, or if you are using an authentication method that does not require a password (e.g., a solution using an application that has been installed on a trusted device, which makes it possible to generate OTPs or approve connection setups).
Use an OTP	Select the checkbox to set up the connection by using an OTP (one-time password), as with the Stormshield TOTP solution. In this case, you will need to enter the OTP in the OTP field.
OTP	This field appears when you are setting up a connection and the Use an OTP checkbox is selected. This field does not appear in the window to add or modify a saved connection. Enter an OTP, or leave the field empty if you are using a solution that approves the setup of a connection (push notification) in an application that is installed on a trusted device.
Connect automatically	Select the checkbox to automatically set up the saved connection when the Stormshield SSL VPN client starts. This option can only be enabled on a single saved connection. It does not appear in the Direct connection menu. Auto login may require a manual operation in some cases. For more information, refer to the section Enabling the auto login option .

Available fields with OpenVPN mode

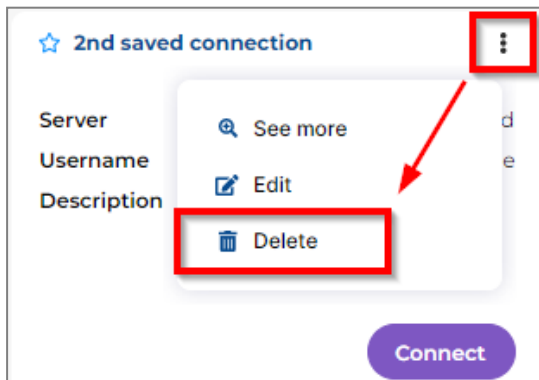
Field	Description
Drag & drop/Browse	OVPN file that you wish to import. To retrieve the OVPN file from the SNS firewall's SSL VPN service, refer to the section Appendix: Retrieving the SSL VPN configuration (OVPN file) .



Field	Description
Name	Name of the saved connection. Special characters cannot be entered when the connection is being added. However, they can be added when the connection is being edited. This field does not appear in the Direct connection menu.
Description	Description of the saved connection. This field does not appear in the Direct connection menu.
Username	User name.
Save password	Select the checkbox to save the connection password. When a connection is being modified, if a password has already been saved, unselect the checkbox to stop saving it.
Password	User's password. Leave this field empty if you are not saving the password, or if you are using an authentication method that does not require a password (e.g., a solution using an application that has been installed on a trusted device, which makes it possible to generate OTPs or approve connection setups).
Use an OTP	Select the checkbox to set up the connection by using an OTP, as with the Stormshield TOTP solution. In this case, you will need to enter the OTP in the OTP field.
OTP	This field appears when you are setting up a connection and the Use an OTP checkbox is selected. This field does not appear in the window to add or modify a saved connection. Enter an OTP, or leave the field empty if you are using a solution that approves the setup of a connection (push notification) in an application that is installed on a trusted device.
Connect automatically	Select the checkbox to automatically set up the saved connection when the Stormshield SSL VPN client starts. This option can only be enabled on a single saved connection. It does not appear in the Direct connection menu. Auto login may require a manual operation in some cases. For more information, refer to the section Enabling the auto login option .

Deleting a saved connection


1. For the saved connection in question, click on the **⋮** button, and on **Delete**.

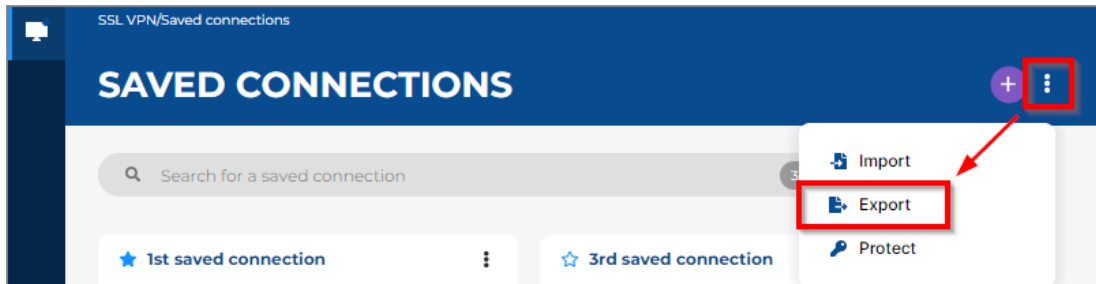


2. Click on **Delete** to confirm.



Exporting saved connections

1. Click on the  button at the top right, then click on **Export**.



2. Select the location to save the .book file, give it a name, and then click on **Save**.
3. If you wish to protect the .book file with a password, enter the password in the window that appears. Leave the field empty if the .book file does not need to be protected.

NOTE


Protected .book files can only be imported after the protection password is entered. Only the Stormshield SSL VPN client graphical interface allows .book files to be **imported**. Other methods, such as the CLI command `import-addressbook`, do not allow protected .book files to be imported.

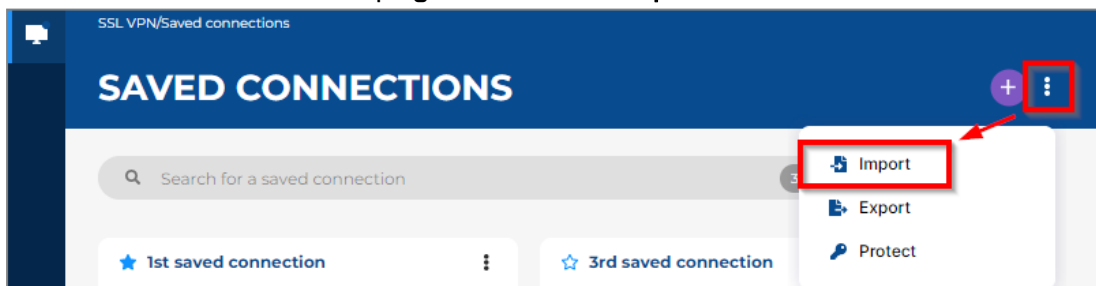
4. Click on **Export** to export the file.

Importing saved connections

IMPORTANT

This operation **overwrites and replaces** saved connections that are currently available with those contained in the imported .book file.

1. Click on the  button at the top right, 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 protected by a password, enter it in the **Password** field.
4. Click on **Import**.

Once the saved connections are imported, you can [Protecting access to saved connections with a password](#) if you wish to do so.

NOTE

Administrators can also import saved connections:




- On a workstation with the Stormshield SSL VPN client command line interface. For more information, refer to the section [Configuring the Stormshield SSL VPN client through a command line interface](#).
- On a pool of Windows workstations, through a script in a GPO. For more information, refer to the section [Deploying saved connections through a group policy \(GPO\)](#) in the *Stormshield SSL VPN client v5 installation guide*.

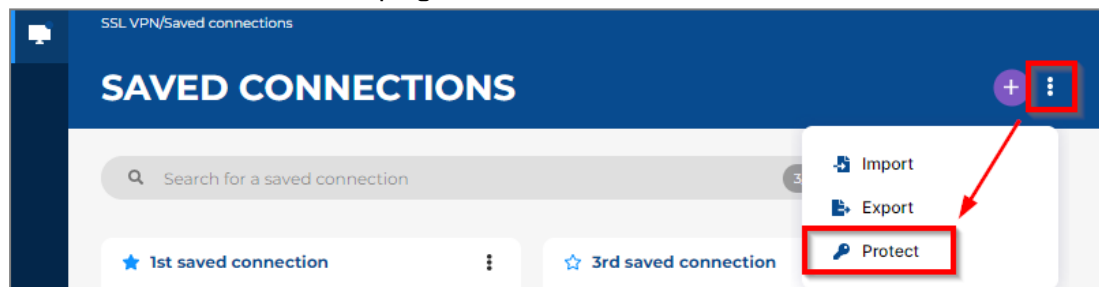
Protecting access to saved connections with a password

You can protect access to saved connections with a password.

Protecting access to saved connections


If you are protecting access to saved connections, you must enter the access password the first time that the Stormshield SSL VPN client accesses these connections after startup (when saved connections are displayed, or when a saved connection is being set up with the auto login option enabled).

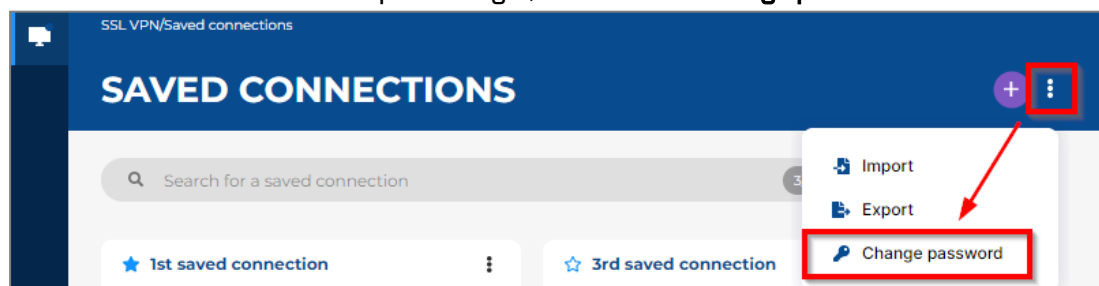
1. Click on the  button at the top right, then click on **Protect**.



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.
4. Click on **Change password**.

Changing the access password


1. Click on the  button at the top to the right, then click on **Change password**.

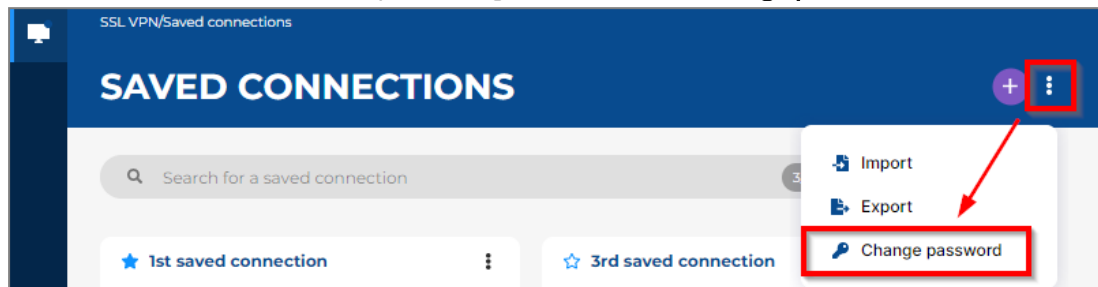



2. Enter the current access password.
3. Set the new access password, and confirm it. Keep the password in a safe and protected location. Stormshield will not be able to help you recover your password if you misplace it.
4. Click on **Change password**.



Removing protection

1. Click on the  button at the top to the right, then click on **Change password**.



2. Disable the parameter **Enable password protection** .
3. Enter the access password.
4. Click on **Disable protection**.

If the access password is misplaced

You will not be able to reset the access password, and Stormshield is not in a position to recover it. As a last resort, you need to delete the file containing the saved connections, which can be found in a folder at the following location:

- In Windows:

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

- In macOS:

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

- In Linux:

```
/var/lib/stormshield/sslvpnclient/addressbooks/
```

You must already hold the required permissions on the workstation to access the folder. If you need assistance, get in touch with an administrator from your organization.

In this folder, if only one sub-folder exists, this means that only one user on the workstation has added saved connections. If there are several sub-folders, you need to identify the sub-folder of the user in question:

- In macOS and Linux, the name of each sub-folder corresponds to the ID of a user on the workstation.
- In Windows, the name of each sub-folder corresponds to an internal Windows ID that does not contain any information identifying the user. You can use the dates of the last modification to find the user in question.

When you are ready, quit the Stormshield SSL VPN client, delete the sub-folder, and start the Stormshield SSL VPN client. The user can then **add** or **import saved connections** once again.

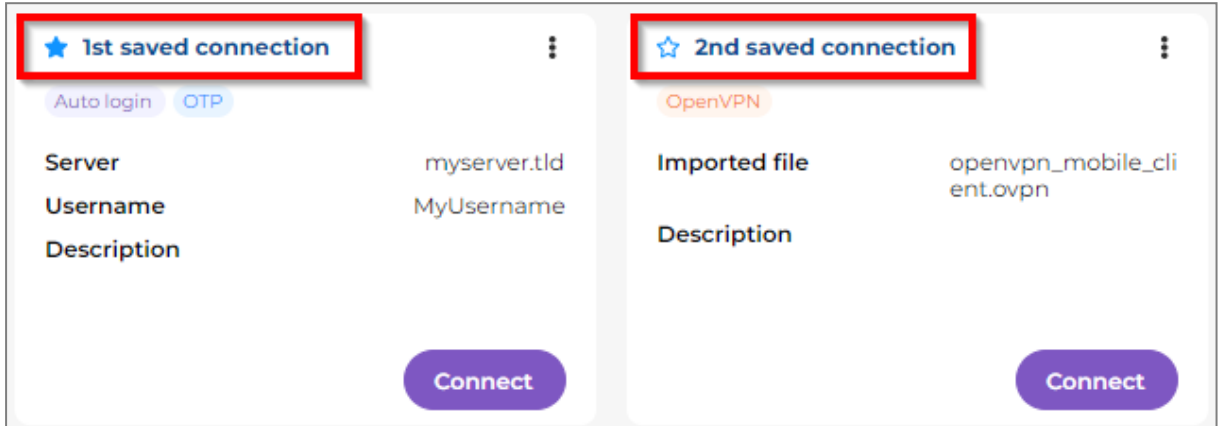


Managing the list of favorite connections

A star icon appears to the left of each saved connection. Click on the icon to add or remove the connection from the list of favorite connections.

★ Favorite connection

☆ Connection that is not in the list of favorite connections



Enabling the auto login option

The auto login option can be enabled on saved connections. This will automatically set up the connection when the Stormshield SSL VPN client starts.

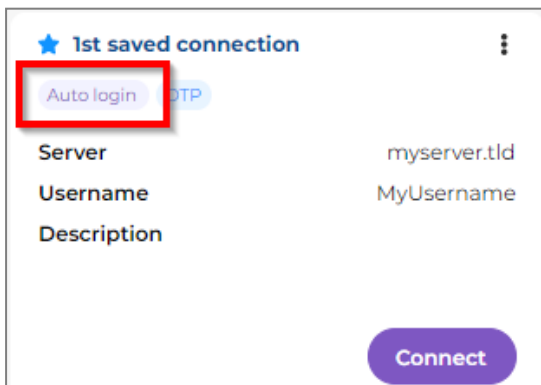
NOTE

Auto login requires a manual operation in the following cases:

- If **access to saved connections is protected**, you have to enter the access password to unlock access to saved connections.
- If additional information is required, such as an OTP or a password, you will need to enter it.

Checking whether the auto login option is enabled

An "Auto login" label appears in the section of a saved connection if the **Connect automatically** option is enabled.

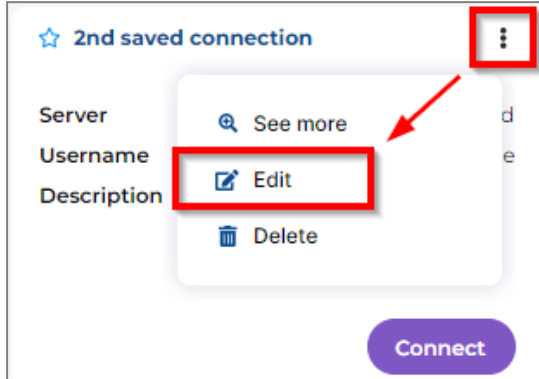




Enabling the auto login option on a saved connection

This option can only be enabled on a single saved connection.

1. For the saved connection in question, click on the  button, and on **Edit**.

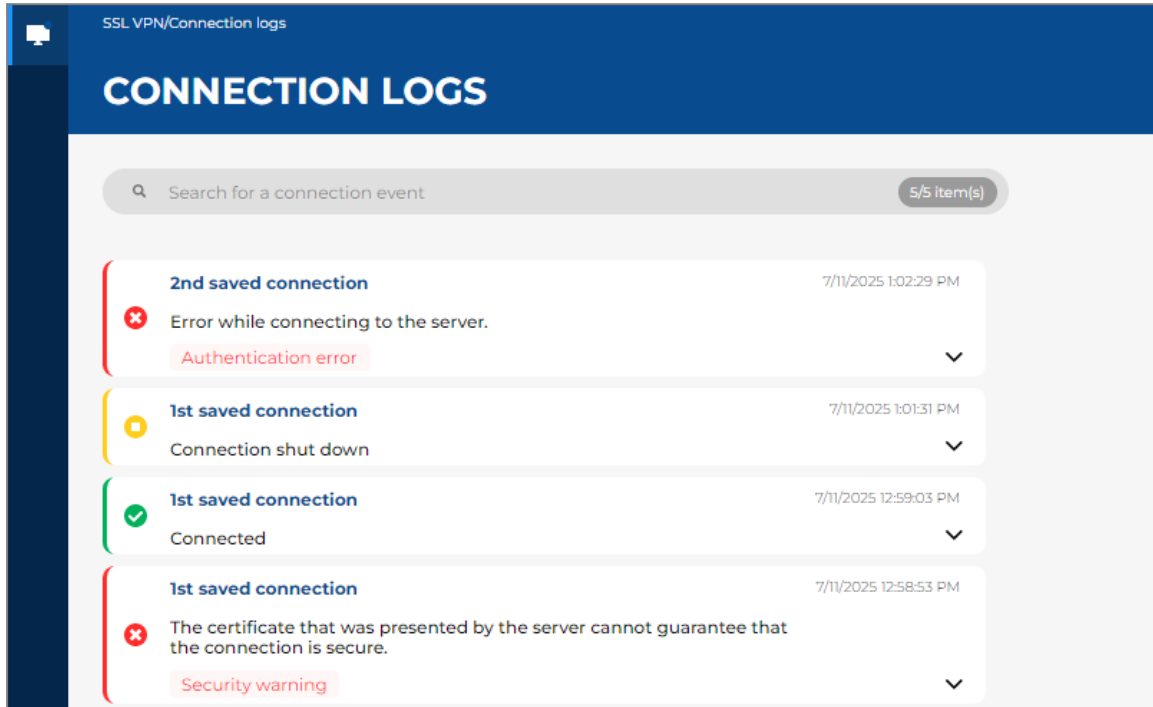


2. Select the **Connect automatically** checkbox.
3. Click on **Edit** to save changes.
4. If the auto login option is already enabled on another saved connection, you need to indicate whether you wish to replace it with the connection currently being edited. Click on **Replace** to confirm the changes.



Viewing connection logs

You can view connection events on the Stormshield SSL VPN client in the **Connection logs** menu.



You will find the following events in these logs:

Event	Description
Connected	The connection was properly set up.
Connection shut down	The connection was shut down, and the user has been logged out.
Connection lost	The connection with the server was lost.
Server unreachable	The Stormshield SSL VPN client did not manage to reach the server to set up the connection.
Security warning	The certificate that was presented by the server did not guarantee that the connection was secure (probable security risk). For more information, refer to the section When a connection error occurs .
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

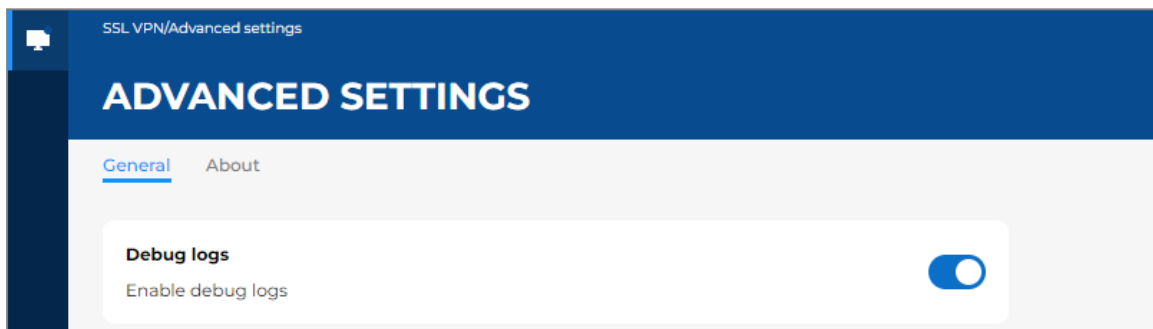
This section explains several advanced scenarios in the use and configuration of the Stormshield SSL VPN client.

Viewing debug logs

An administrator from your organization may ask you to enable debug logs.

Enabling debug logs

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



Accessing 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 macOS:
 - Service logs:
`/Library/Application Support/Stormshield/SSL VPN Client/Logs/`
 - User logs:
`/Users/<user>/Library/Application Support/Stormshield/SSL VPN Client/Logs/`
- In Linux:
 - Service logs:
`/var/log/stormshield/sslvpnclient/`
 - User logs:
`$HOME/.local/share/stormshield/sslvpnclient/logs/`



Configuring the Stormshield SSL VPN client through a command line interface

This section explains how to configure the Stormshield SSL VPN client through a command line interface.

Using the command line interface

Commands are run locally on the workstation.

- In the Windows command prompt:

```
sslvpn-cli.exe [command] [options]
```

- In Linux and macOS on a terminal:

```
sslvpn-cli [command] [options]
```

If the command is not detected by default, you can find the program at the following location:

- In Windows:

```
C:\Program Files\Stormshield\SSL VPN Client\Modules\ssl-vpn\Services\sslvpn-cli.exe
```

- In Linux:

```
/usr/bin/sslvpn-cli
```

- In macOS:

```
/Applications/Stormshield/SSL VPN Client.app/Contents/MacOS/Modules/ssl-vpn/sslvpn-cli
```

List of commands

import-addressbook

History

Added in version 5.1.2

Description

Imports a .book file containing saved connections. The file must not be password-protected.

Usage

- Windows:

```
sslvpn-cli.exe import-addressbook --file <path\file.book>
```

- Linux:

```
sslvpn-cli import-addressbook --file <path/file.book>
```

- macOS:

```
sslvpn-cli import-addressbook --file <path/file.book>
```

Replace *<path/file.book>* with the file's full access path.



Further reading

For further information on installing, updating and uninstalling the Stormshield SSL VPN client, refer to the [Stormshield SSL VPN client v5 installation guide](#).

To configure the SSL VPN service on SNS firewalls and monitor connected users, refer to the [SSL VPN administration guide for SNS firewalls and Stormshield SSL VPN clients](#).

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



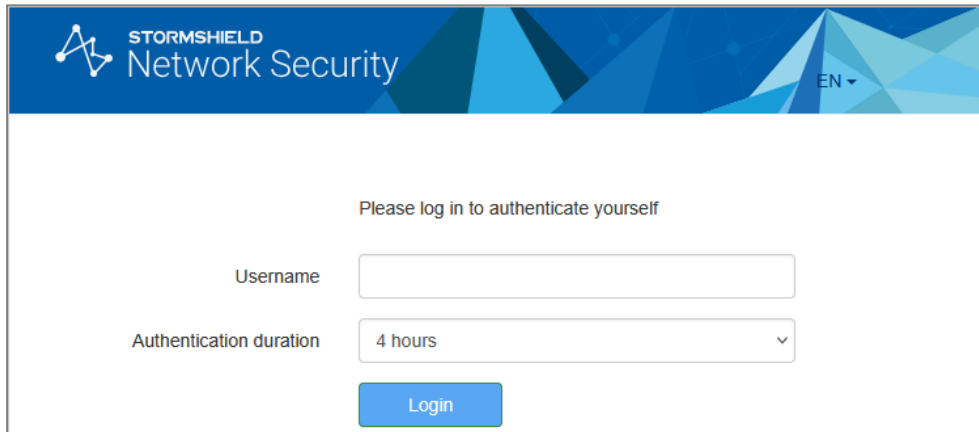
Appendix: Retrieving the SSL VPN configuration (OVPN file)

This appendix explains how to retrieve the SSL VPN configuration file (OVPN file).

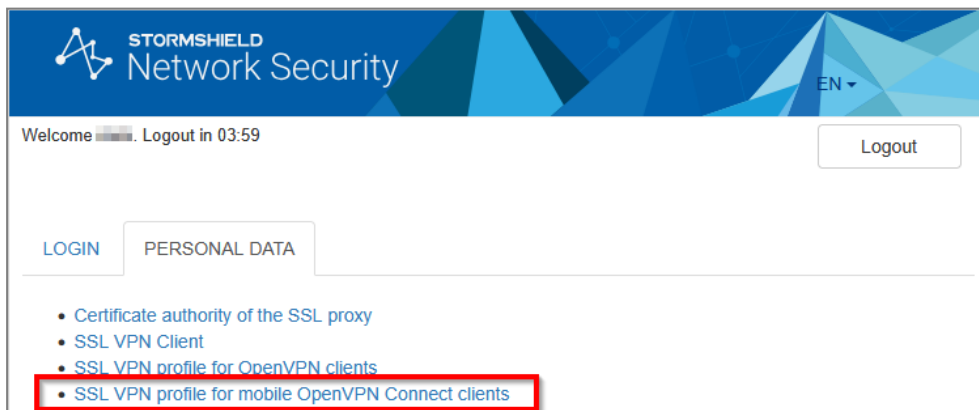
You will need this file if you are connecting in **OpenVPN mode**. An administrator from your organization may ask you to retrieve the OVPN file.

Retrieving the OVPN file from the SNS firewall captive portal

1. Ensure that you are logged in to your organization's network.
2. Open a web browser and go to the address of the SNS firewall captive portal.
An administrator in your organization would have provided you with this address, which is generally in this format: *mycompany.tld/auth* or *gateway.mycompany.tld/auth*.
The image below shows the default captive portal login page. Do note that this page can be customized to reflect your organization's visual identity.



3. Authenticate on the login page by entering the requested information.
4. Once you are authenticated, go to the **Personal data** tab, and click on **SSL VPN profile for mobile OpenVPN Connect clients (single .ovpn file)**.



5. Agree to download the OVPN file by accepting.

If you are unable to download the OVPN file, get in touch with an administrator from your organization.



Retrieving the OVPN file from the SNS firewall's web administration interface

An SNS firewall administrator can retrieve the OVPN file from the SNS firewall's web administration interface. For more information, refer to the section [Configuring the SSL VPN service](#) in the *SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients*.



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.