STORMSHIELD

GUIDE

STORMSHIELD NETWORK SSL VPN CLIENT

USER AND CONFIGURATION GUIDE

Version 5.1

Document last updated: October 22, 2025

Reference: sns-en-ssl_vpn_client_user_and_configuration_guide-v5.1

Table of contents

Change log

Date	Description
October 22, 2025	- Information regarding single sign-on added to the section "Creating a secure connection" - Information regarding the message "Probable security risk" added to the section "Creating 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	New document

Getting started with the Stormshield SSL VPN client

Welcome to the Stormshield Network SSL VPN Client version 5.1 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 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.

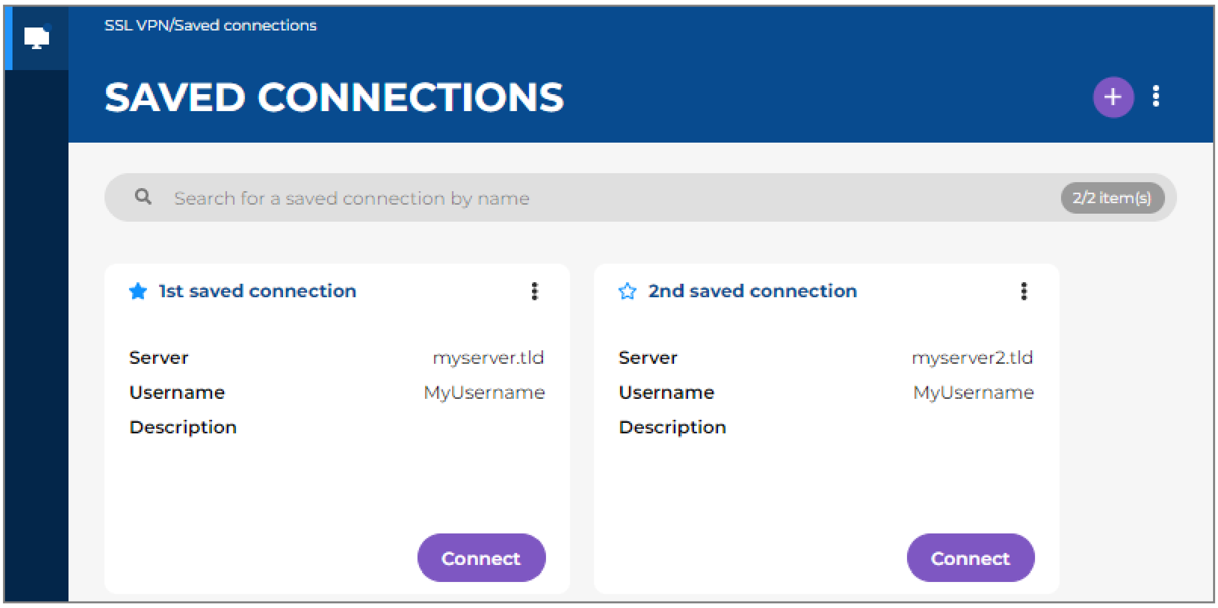
The graphical interface is available in French and English. The language used depends on the language that was selected in the user's session settings. If the chosen language is not supported, the Stormshield SSL VPN client will use English by default.

Overview of the graphical interface

To open the 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 general menu that can be accessed by scrolling over the icon in the shape of a monitor, and a main window containing information on the selected menu. The screen capture below shows the window of the **Saved connections** menu.



SSL VPN/Saved connections

SAVED CONNECTIONS

1st saved connection

Server myserver.tld
Username MyUsername
Description

2nd saved connection

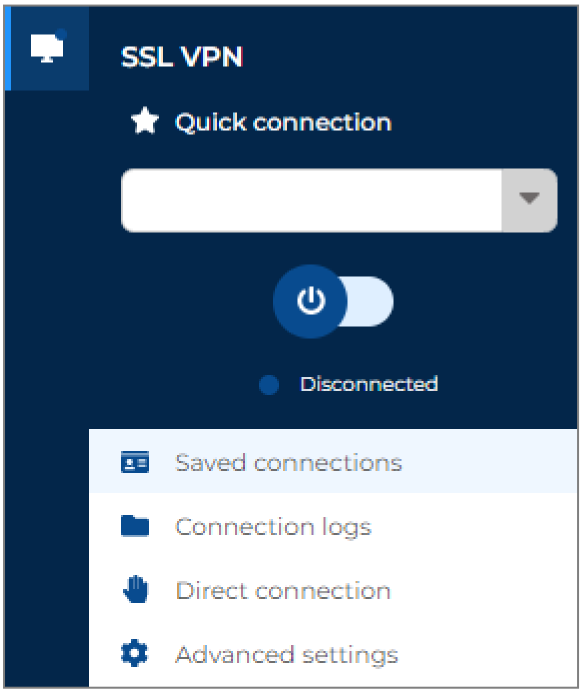
Server myserver2.tld
Username MyUsername
Description

Overview of the general menu

To open the general menu, scroll over the icon in the shape of a monitor on the left. In the general menu, you can access the following menus:

- **Quick connection**: the drop-down list makes it possible to select the last connection used, or a favorite connection, then set up the connection with the connection button. The current status of the established connection is also shown.
- **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.

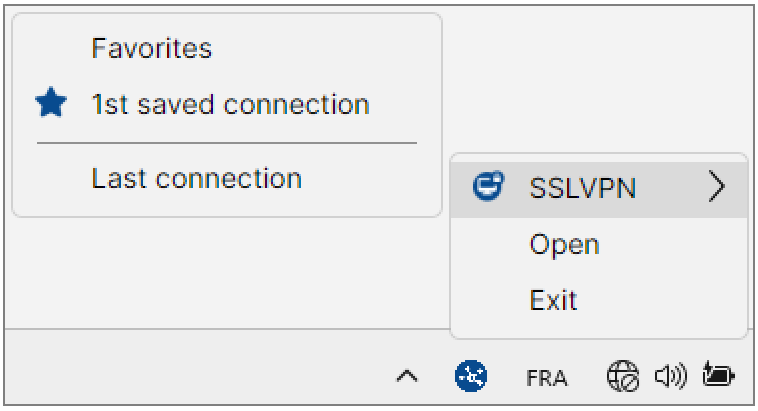


Overview of the pop-up menu

To open the pop-up menu, right-click on the icon of the Stormshield SSL VPN client in the system tray. In the pop-up menu, you can access the following menus:

- **SSLVPN**: makes it possible to log in to the last connection used, or a favorite connection. The user can also log out if a connection is currently set up.
- **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

> **NOTE**
> Only one connection can be set up at a time.

Setting up a saved connection

To set up a saved connection, information on the connection in question has to be saved in advance. For more information, refer to the section Managing saved connections.

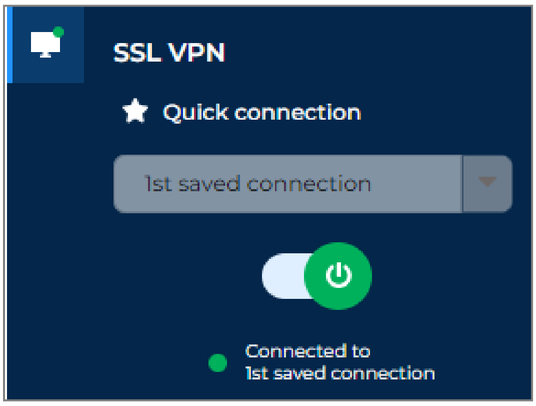
1. You can set up a saved connection in the following menus:
   - In the **Quick connection** menu: select a favorite connection from the drop-down list, or the last connection used, and click on the connection button .
   - In the **Saved connections** menu: in the section of the saved connection to which you wish to log in, click on **Connect**.
   - In the **pop-up menu** of the Stormshield SSL VPN client icon : select **SSLVPN**, then click on a favorite connection or the last connection used.
2. 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 is used, the expiry date of your authentication session appears. For more information, refer to the section Using single sign-on to set up a connection.

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

Quick connection menu



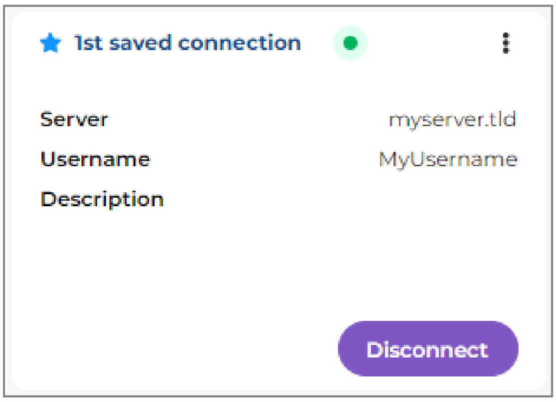
SSL VPN

★ Quick connection

1st saved connection

● Connected to
1st saved connection

Saved connections menu

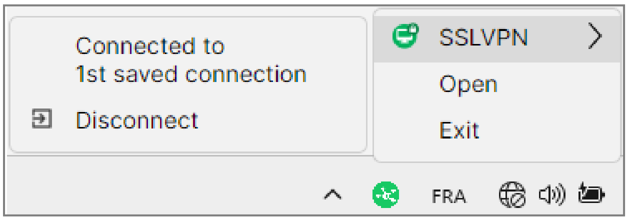


★ 1st saved connection ●

Server	myserver.tld
Username	MyUsername
Description	

Disconnect

Pop-up menu



Connected to
1st saved connection

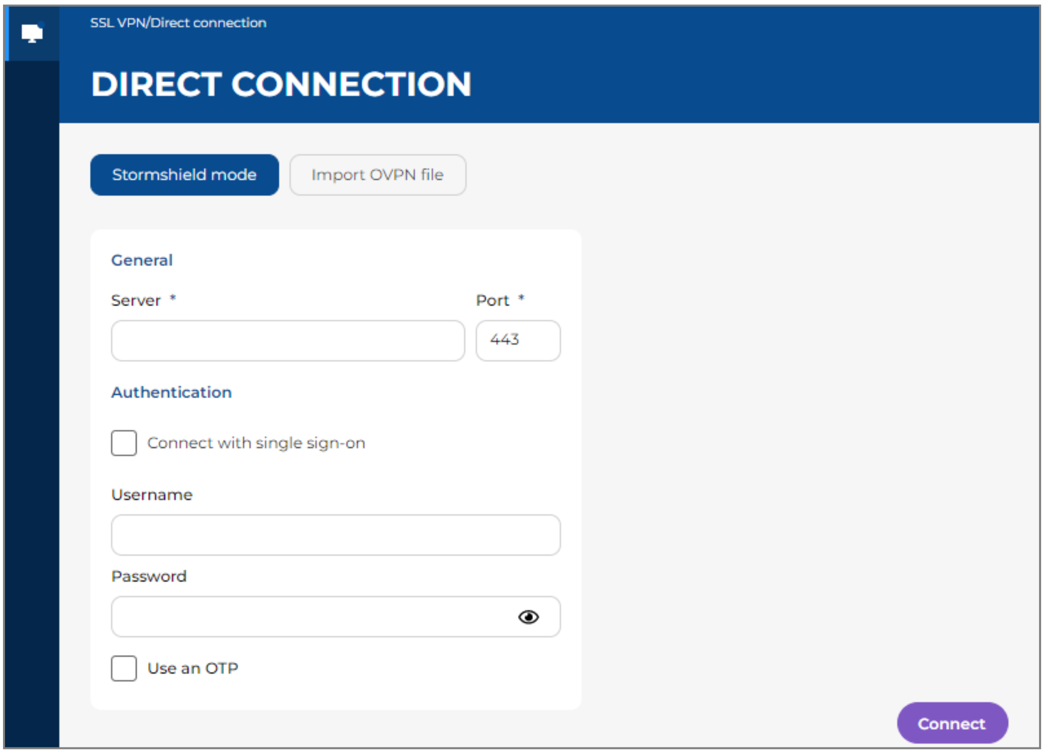
Disconnect

SSLVPN >
Open
Exit

FRA

Setting up a connection without saving information

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



2. Choose between **Stormshield mode** and **Import OVPN file** and fill in the fields.

> **NOTE**
> If you need help in choosing the right mode or filling in the fields, refer to the descriptions provided in the section Adding, editing or deleting saved connections. The modes and fields are similar in both menus, with a few exceptions mentioned in the descriptions.

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 is used, the expiry date of your authentication session appears. For more information, refer to the section Using single sign-on to set up a connection.

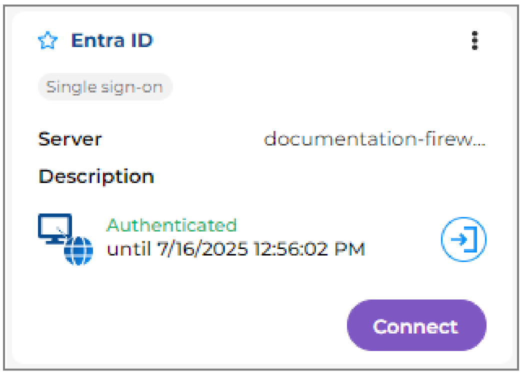
You can log out by clicking out on **Disconnect** or on the connection button.

Using single sign-on to set up a connection

If you are using single sign-on to set up a connection in the **Saved connections** or **Direct connection** menu, the expiry date of your authentication session will appear in the graphical interface once the connection is established,

As long as this date has not been reached, and your authentication session is still valid on the SNS firewall, you do not need to authenticate again to set up the connection.

Saved connections menu



Entra ID

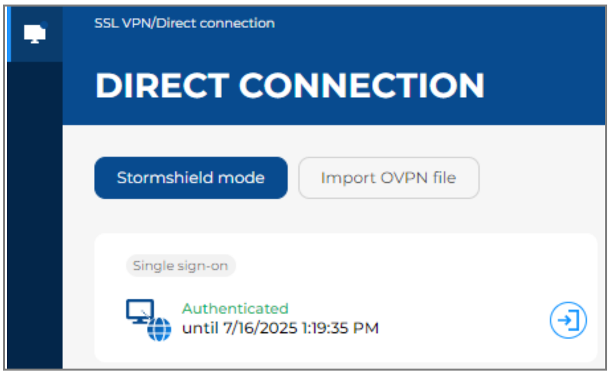
Single sign-on

Server documentation-firew...

Description

Authenticated until 7/16/2025 12:56:02 PM

Direct connection menu



SSL VPN/Direct connection

DIRECT CONNECTION

Single sign-on

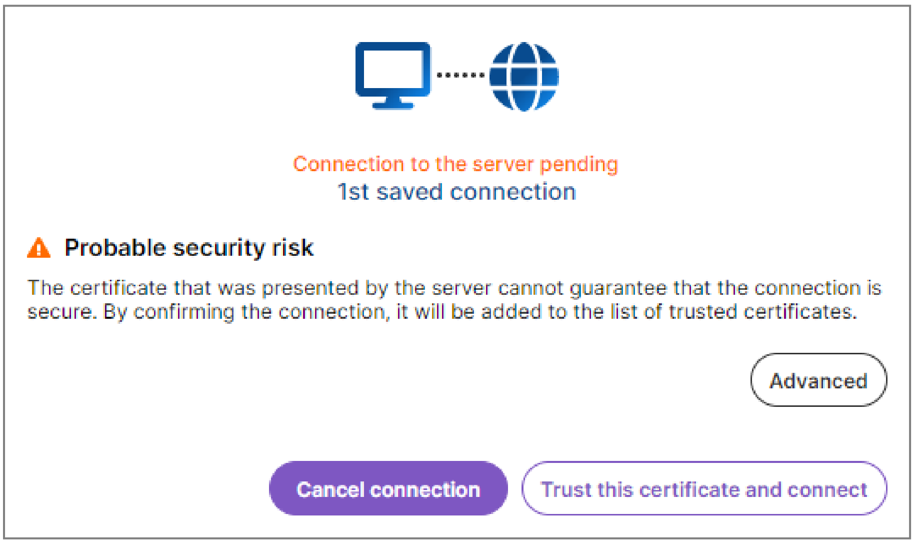
Authenticated until 7/16/2025 1:19:35 PM

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

- 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 information on the saved 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.
- 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.



Connection to the server pending
1st saved connection

⚠ Probable security risk

The certificate that was presented by the server cannot guarantee that the connection is secure. By confirming the connection, it will be added to the list of trusted certificates.

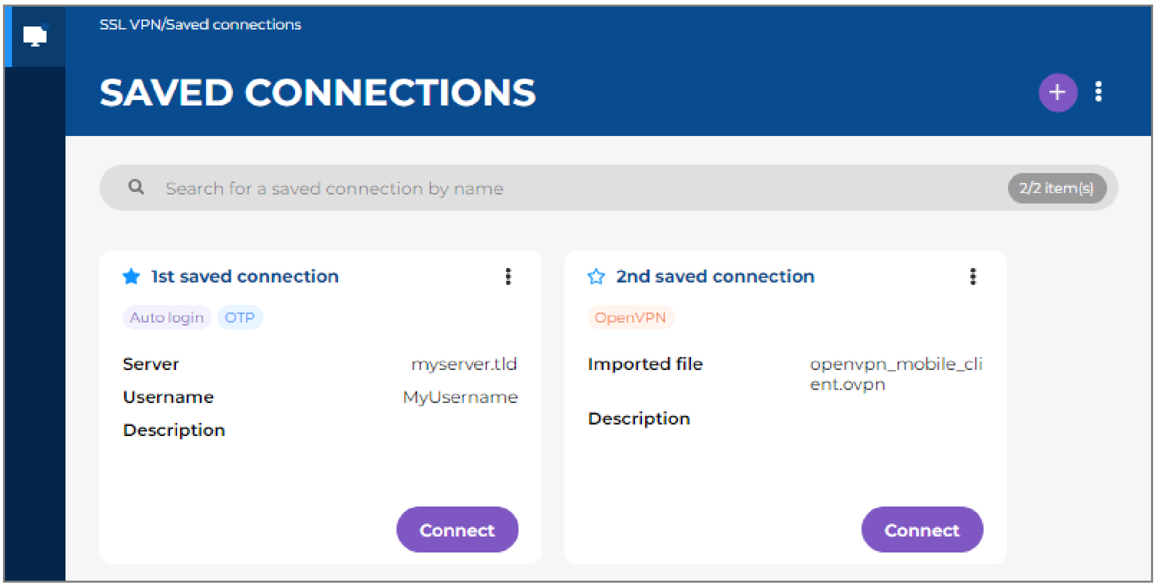
To do so, display information on the certificate and its trust chain by clicking on **Advanced** > **Show certificate** to check whether the connection is secure. If you are unable to decide, get in touch with an administrator from your organization.

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.

- 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.



SSL VPN/Saved connections

SAVED CONNECTIONS

1st saved connection

Server: myserver.tld
Username: MyUsername
Description

2nd saved connection

Imported file: openvpn_mobile_client.ovpn
Description

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 connection

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

Mode	Description
Stormshield mode	In this mode, the Stormshield SSL VPN client can: • Automatically retrieve the SSL VPN configuration, and check whether the configuration requires an update every time it connects. • Send to the SNS firewall information that enables the firewall to verify the client workstation's compliance (ZTNA) every time it connects.
Import OVPN file	This mode makes it possible to import an OpenVPN (OVPN) configuration file provided by the SNS firewall, and to connect to its OpenVPN gateway.

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

Stormshield mode

Field/checkbox	Description
Name	Name of the saved connection. This field does not appear in the **Direct connection** menu.
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 saved connection. This field does not appear in the **Direct connection** menu.
Connect with single sign-on	Select this checkbox to use single sign-on. To set up the connection, you will then need to authenticate on a portal, which automatically opens in your web browser. For more information, refer to the section Using single sign-on to set up a connection. If this option is selected, the **User name**, **Password** and **Use an OTP** fields will be hidden. **IMPORTANT** You will need an SNS firewall in version 5 in order to use single sign-on. You will not be able to set up any connections if the SNS firewall uses a version older than version 5.
Username	User name.
Password	User's password. If you are using multifactor authentication through a third-party application (push mode), leave this field empty.
Use an OTP	Select this checkbox if you are using a multifactor authentication solution, such as the Stormshield TOTP solution. To set up the connection, you will then need to enter an OTP (one-time password). If you are using multifactor authentication through a third-party application (push mode), select the checkbox but leave the **OTP** field unselected to set up a connection.
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. You will still need to manually log in to set up the connection in some cases (password-protected saved connections, or when an OTP or password has to be entered). For more information, refer to the section Enabling the auto login option.

Import OVPN file

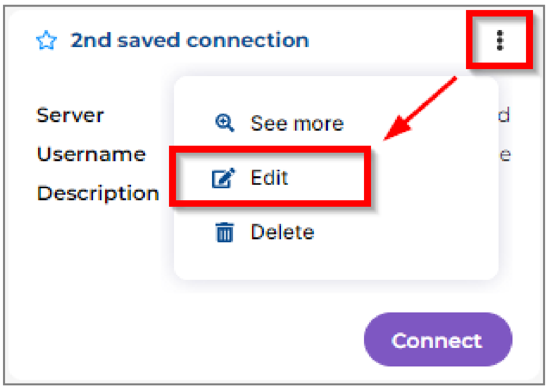
Field	Description
Drag & drop/Browse	OVPN file that you wish to import. To retrieve the OVPN file, refer to the section Appendix: Retrieving the SSL VPN configuration (OVPN file).

Field	Description
Name	Name of the saved connection. 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.
Password	User's password. If you are using multifactor authentication through a third-party application (push mode), leave this field empty.
Use an OTP	Select this checkbox if you are using a multifactor authentication solution, such as the Stormshield TOTP solution. To set up the connection, you will then need to enter an OTP (one-time password). If you are using multifactor authentication through a third-party application (push mode), select the checkbox but leave the **OTP** field unselected to set up a connection.
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. You will still need to manually log in to set up the connection in some cases (password-protected saved connections, or when an OTP or password has to be entered). For more information, refer to the section Enabling the auto login option.

4. Click on **Add**.

Editing a connection

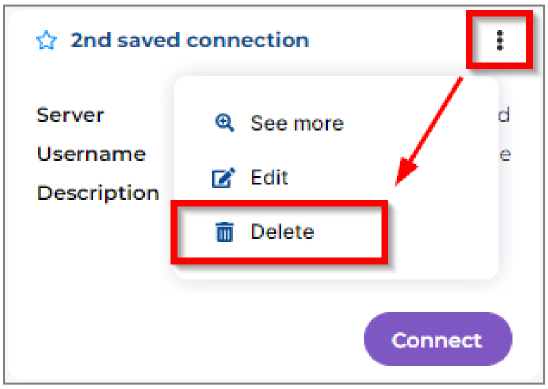
1. In **Saved connections**, in the section of the connection that you wish to edit, click on the ⋮ button, and on **Edit**.



2. Edit the connection information. 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**.

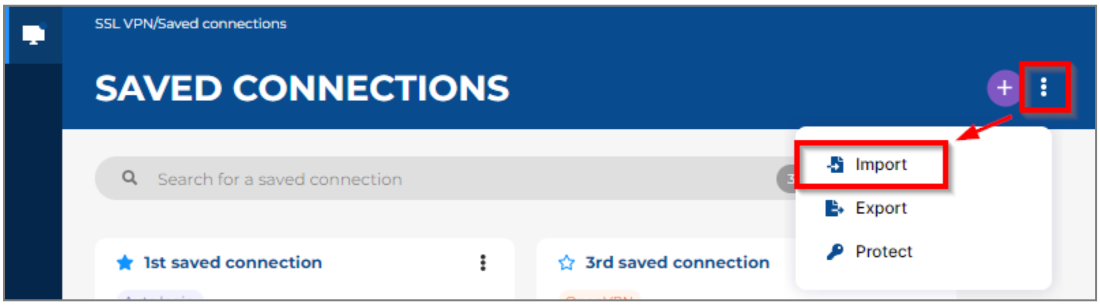


2. Click on **Delete** to confirm.

Importing saved connections

> **IMPORTANT**
> This operation **overwrites and replaces** 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, then click on **Import**.



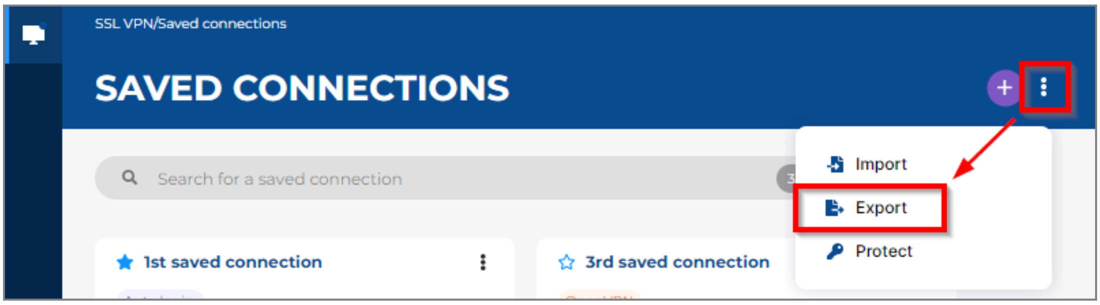
2. Select the .book file containing the saved connections that you wish to import, then click on **Open**.
3. If the .book file is password-protected, enter the password in the window that appears, then click on **Import**.

If you wish to protect imported saved connections, refer to section Protecting access to saved connections with a password.

> **NOTE**
> You can also import saved connections through 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.

Exporting saved connections

1. In **Saved connections**, click on the ⋮ button at the top to the right, then click on **Export**.



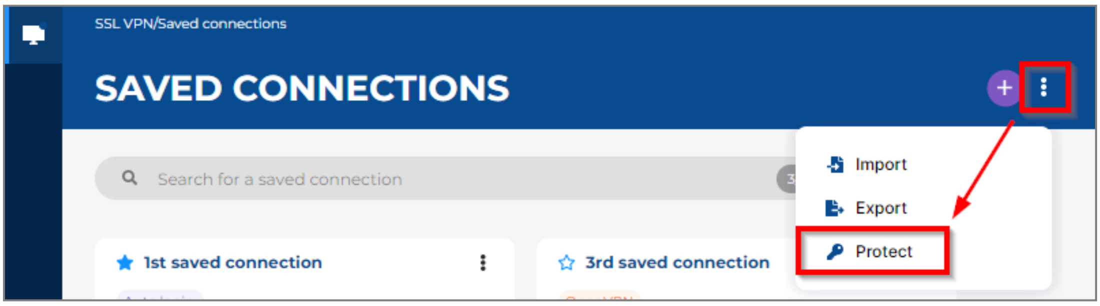
2. Select the location to save the .book file that contains exported saved connections, give it a name, and then click on **Save**.
3. If you wish to protect the .book file with a password, set a password in the window that appears. Leave the field empty if file protection is not required. This password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

Protecting access to saved connections with a password

Protecting access to saved connections

> **NOTE**
> If you protect access to saved connections with a password and the automatic login option is enabled on a connection, you must enter this password every time you open the Stormshield SSL VPN client to set up the automatic connection.

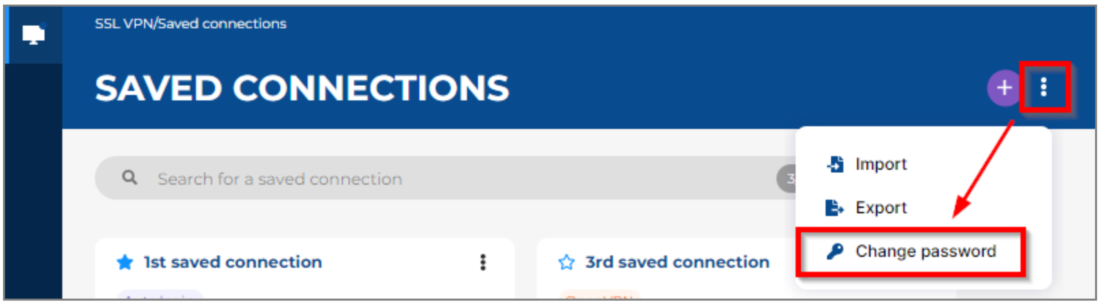
1. In **Saved connections**, click on the ⋮ button at the top to the right, then click on **Protect**.



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. For more information, refer to the section If you misplace your access password.
4. Click on **Change password.**

Changing the access password

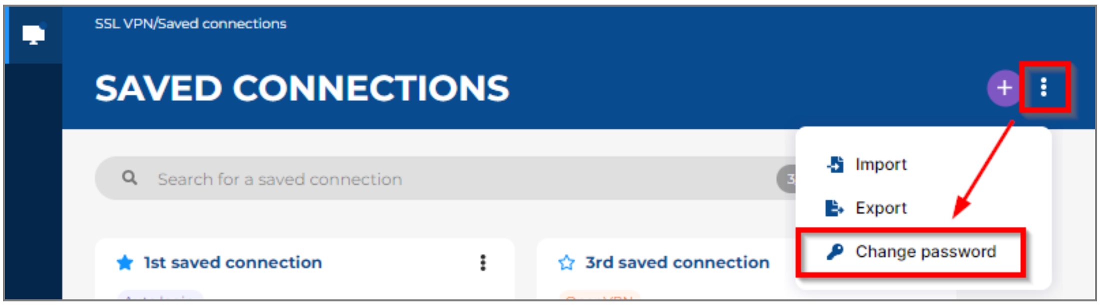
1. In **Saved connections**, click on the ⋮ button at the top to the right, then click on **Change password**.



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. For more information, refer to the section If you misplace your access password.
4. Click on **Change password.**

Removing protection

1. In **Saved connections**, 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 you misplace your access password

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 folder containing the file of saved connections, which will be permanently lost.

To access this folder and delete it, you must hold the required privileges on the workstation. If you need help for this operation, or do not hold the required privileges, get in touch with an administrator from your organization.

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/
  ```

It may contain several sub-folders. 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 Linux and macOS, 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.

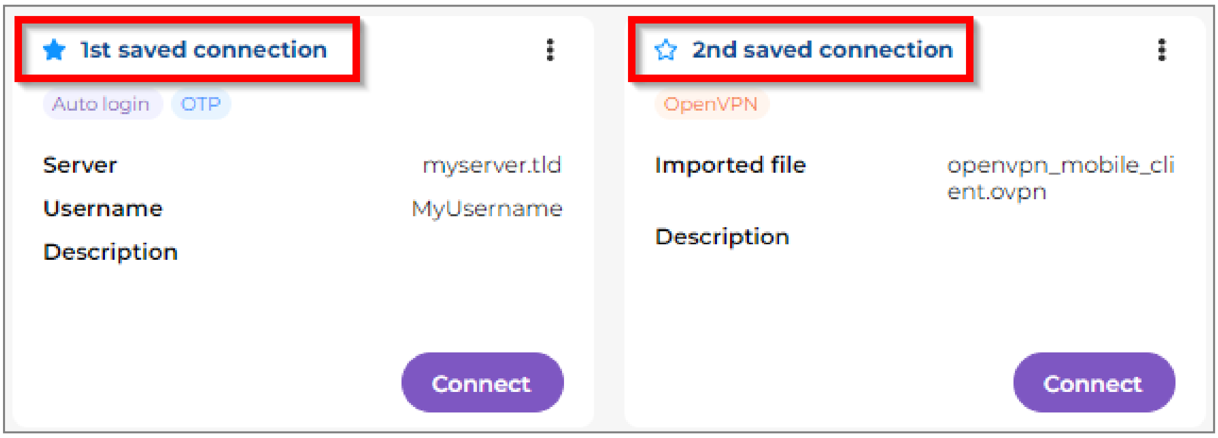
When you are ready, quit the Stormshield SSL VPN client, delete the sub-folder, and start the Stormshield SSL VPN client. The user can then add or import saved connections once again.

Managing the list of favorite connections

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

Icon	Description
☆	The connection is not in the list of favorite connections.
★	The connection is in the list of favorite connections.

Click on the icon to add or remove the connection from the list of favorite connections.



You can also find the list of favorite connections in the **Quick connection** menu and in the **pop-up menu** from the icon of the Stormshield SSL VPN client.

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.

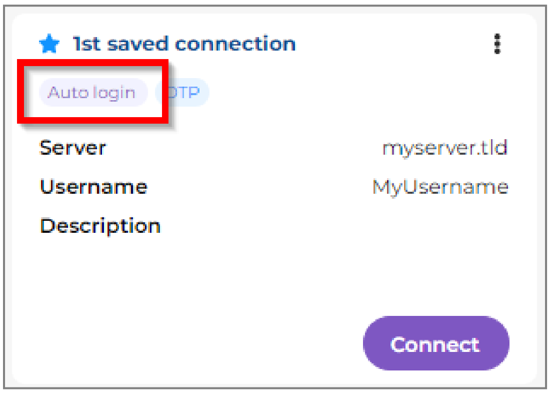
This option can only be enabled on a single saved connection.

NOTE
You will still need to manually log in if:

- Access to saved connections is protected - you have to enter the password every time the Stormshield SSL VPN client is opened, to unlock access to saved connections and set up auto login.
- You need to enter additional information to set up the connection, such as an OTP or the user's password.

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.



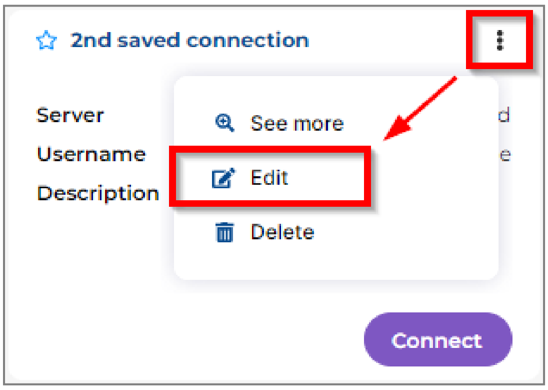
1st saved connection

Auto login OTP

Server myserver.tld
Username MyUsername
Description

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 ⋮ button, and on **Edit**.



2nd saved connection

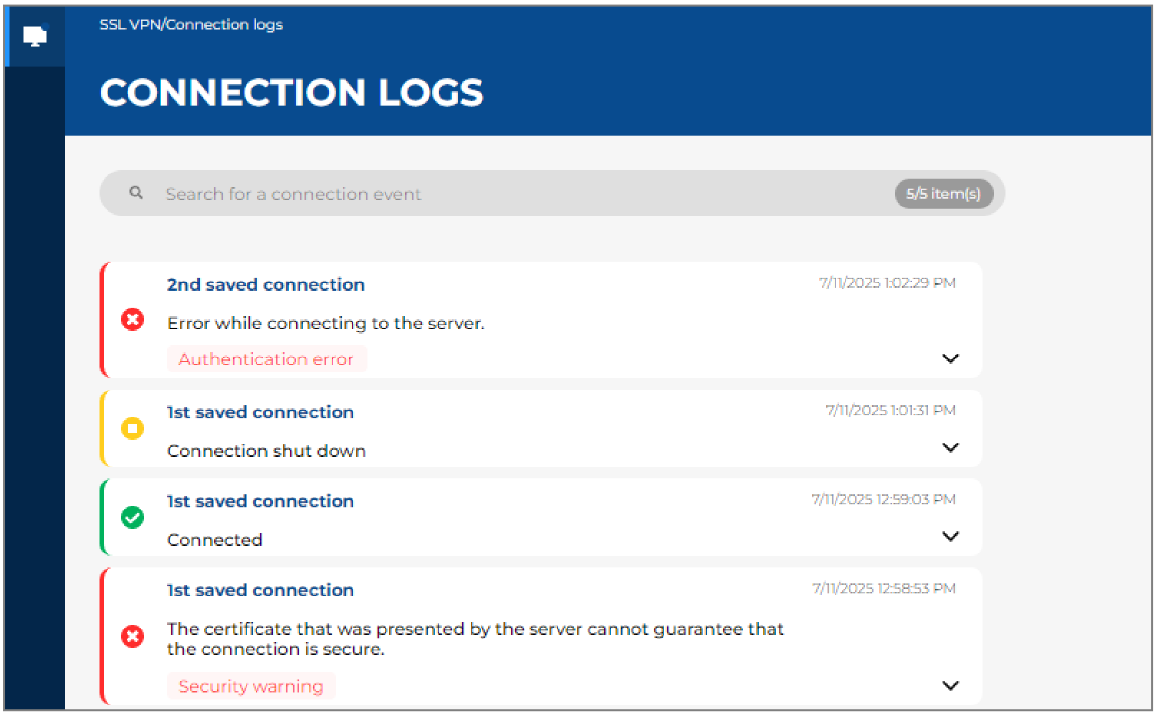
Server
Username
Description

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.



SSL VPN/Connection logs

CONNECTION LOGS

Search for a connection event 5/5 item(s)

2nd saved connection 7/11/2025 1:02:29 PM
Error while connecting to the server.
Authentication error

1st saved connection 7/11/2025 1:01:31 PM
Connection shut down

1st saved connection 7/11/2025 12:59:03 PM
Connected

1st saved connection 7/11/2025 12:58:53 PM
The certificate that was presented by the server cannot guarantee that the connection is secure.
Security warning

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 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 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

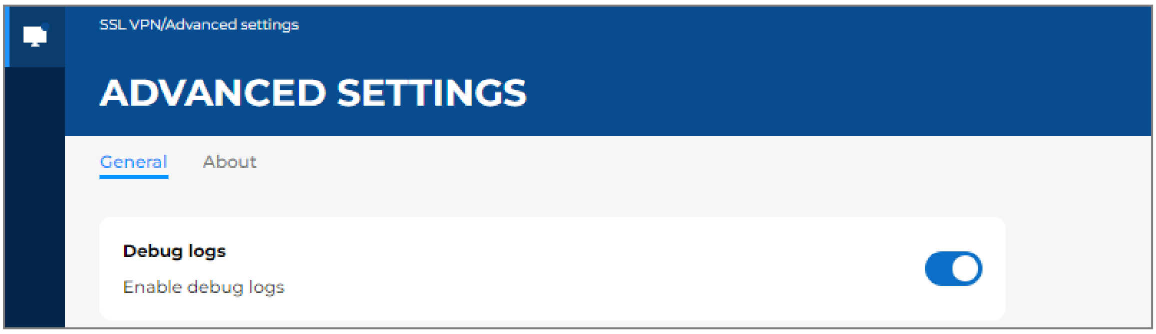
This section explains several advanced scenarios in the use and configuration of the Stormshield SSL VPN client.

Viewing debug logs (advanced settings)

An administrator from your organization may ask you to enable debug logs, which can be done in the **Advanced settings** menu.

Enabling debug logs

In **Advanced settings**, **General** tab, enable the setting **Enable debug logs** ●.



SSL VPN/Advanced settings

ADVANCED SETTINGS

General About

Debug logs

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 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/
    ```

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).

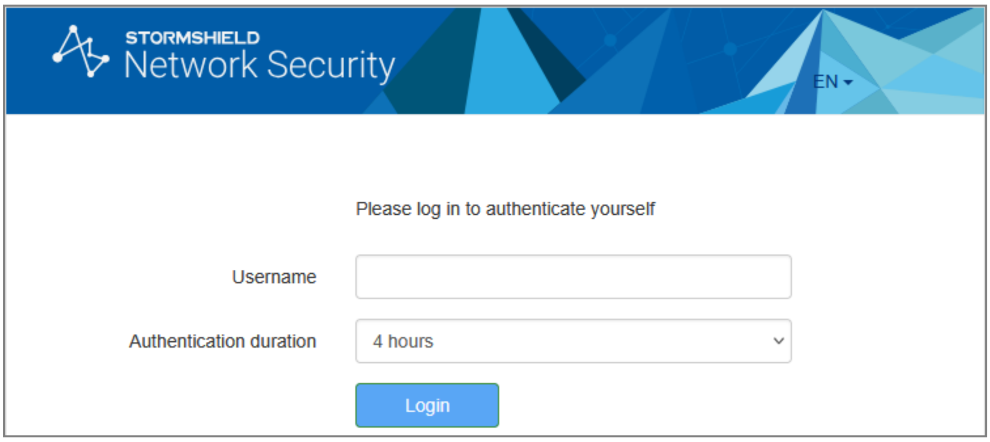
You will need this file if you intend to add connections from an imported OVPN file. An administrator from your organization may ask you to retrieve the OVPN file.

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.

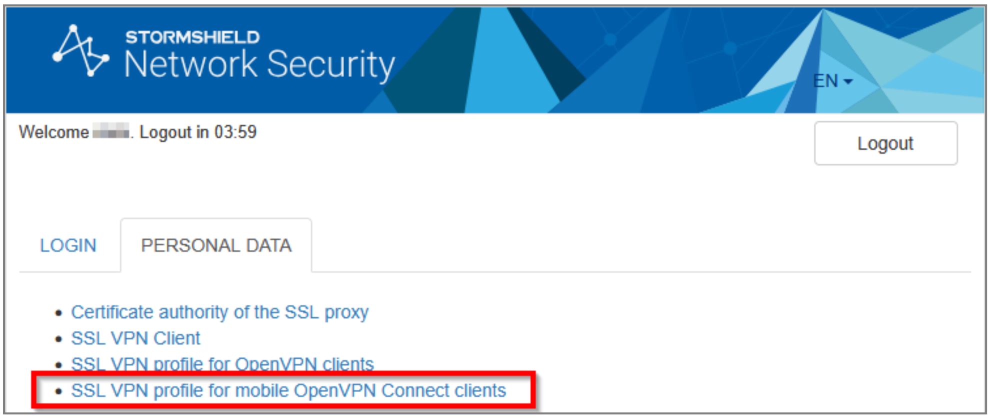


Please log in to authenticate yourself

Username

Authentication duration: 4 hours

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)**.



Welcome [redacted]. Logout in 03:59

- Certificate authority of the SSL proxy
- SSL VPN Client
- SSL VPN profile for OpenVPN clients
- SSL VPN profile for mobile OpenVPN Connect clients

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*.

documentation@stormshield.eu

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