GUIDE

STORMSHIELD SSL VPN CLIENT

USER AND CONFIGURATION GUIDE

Version 4

Document last updated: April 20, 2026

Reference: sns-en-ssl_vpn_client_user_and_configuration_guide-v4

Table of contents

Change log

Date	Description
April 20, 2026	• The technical note has been renamed "Stormshield SSL VPN Client v4 user and configuration Guide" • Minor changes.
May 22, 2025	• Addition of the setting "Enable DCO kernel acceleration", and information relating to networks assigned to VPN clients, as well as the maximum number of VPN tunnels allowed in the section "Configuring the SSL VPN service" for SNS in version 5. • The client workstation verification (ZTNA) configuration now occupies its own section in the document, and its contents have been modified. • Addition of a new issue on the display of a warning message regarding the LZ4 compression feature in the "Troubleshooting" section.
March 13, 2025	• Release of Stormshield SSL VPN client 4.0.10. • Explanations added regarding updates to a version lower than version 4 in the section "Specific characteristics of Stormshield SSL VPN clients". • Changes to information regarding SSL VPN connection logs in the section "Viewing the Stormshield SSL VPN client's logs". • Addition of two issues in the section "Troubleshooting".
February 06, 2025	• Addition of the field "Allow tunnels to be set up for Linux or Mac Stormshield SSL VPN clients" in the section "Configuring the SSL VPN service > Configuring the policy verifying the compliance of client workstations (in ZTNA)".
November 13, 2024	• Release of Stormshield SSL VPN client 4.0.9. • Addition of a paragraph “Limitations and explanations on usage” in the section “Specific characteristics of Stormshield SSL VPN clients” • Changes to information regarding the use of push mode: ◦ With the address book in the section "Configuring the Stormshield SSL VPN client", ◦ In the section "Setting up a VPN tunnel with the Stormshield SSL VPN client" • Removal of the note regarding users who share a Windows workstation with other users in the section "Setting up a VPN tunnel with the Stormshield SSL VPN client".
October 07, 2024	• Addition of explanations regarding the interval before key renegotiation in the section "Configuring the SSL VPN service". • Addition of explanations regarding the use of push mode: ◦ With the address book in the section "Configuring the Stormshield SSL VPN client", ◦ In the section "Setting up a VPN tunnel with the Stormshield SSL VPN client"

August 22, 2024	• Release of Stormshield SSL VPN client 4.0.
	• Content relating to OpenVPN Connect has been moved to an appendix, and content relating to the Stormshield SSL VPN client now contains its own sections.
	• Content on the Stormshield SSL VPN client has been enriched:
	  ◦ Addition of new specific characteristics,
	  ◦ Addition of *.exe* format for the installation program,
	  ◦ Addition of procedures for deployment via a group policy (GPO) and via a script,
	  ◦ Changes to the names of certain fields in the procedures,
	  ◦ Addition of information regarding available logs.
	• The content in the section "Tracking users connected to the SSL VPN on the Stormshield SSL VPN Client firewall" has been enriched.
	• Addition of the implementation of zero trust network access (ZTNA).

Getting started

Welcome to the Stormshield SSL VPN Client version 4 user and configuration guide.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

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

An SSL VPN client must be installed on the user's workstation or mobile device before a VPN tunnel can be set up with the Stormshield SSL VPN Client firewall. Communications between the Stormshield SSL VPN Client firewall and the user are then encapsulated and protected via an encrypted TLS tunnel.

This tunnel can only be set up if the user is authenticated over a TLS communication channel, and encrypted with shared client and server certificates that have been signed by a certification authority (CA) on the Stormshield SSL VPN Client firewall. This solution therefore guarantees confidentiality, integrity and non-repudiation.

This guide provides details on:

- Enabling and configuring the SSL VPN service on Stormshield SSL VPN Client firewalls in version 4.x,
- Implementing zero trust network access (ZTNA) with Stormshield SSL VPN Client firewalls in version 4.8 and higher, and Stormshield SSL VPN clients in version 4.0 or higher,
- Installing the Stormshield SSL VPN client in version 4.x, configuring and using the client, including the setup of an SSL VPN tunnel, some of its specific characteristics (compatibility, connection modes, etc.) and access to its logs,
- Tracking users who are connected to the SSL VPN,
- Some information regarding OpenVPN Connect.

In the rest of this document, Stormshield SSL VPN Client may be referred to as "Stormshield SSL VPN client".

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

Requirements

You will need the following to perform the operations described in this guide.

A compatible SSL VPN client

Every workstation or mobile device must have a compatible VPN client in order to set up SSL VPN tunnels with the Stormshield SSL VPN Client firewall. Compatible VPN clients are:

- **Stormshield SSL VPN Client** in version 4: this guide explains how to install, configure and use the client, including the setup of an SSL VPN tunnel, and some of its specific characteristics (compatibility, connection modes, etc.),
- **OpenVPN Connect**.

For further information on the versions and operating systems that are compatible with Stormshield software programs, refer to the Network Security & Tools life cycle guide.

> **NOTE**
> If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

An adapted SNS firewall

The maximum number of SSL VPN tunnels allowed on Stormshield SSL VPN Client firewalls varies according to the model used. Select a model that fits your requirements. You can find this information on the Stormshield website, under Product range (SNS), by selecting your model.

Prior connection of the Stormshield SSL VPN Client firewall to a directory

The Stormshield SSL VPN Client firewall must be connected to a directory so that it can display the lists of users and user groups in its modules. This will make it possible to define the users and user groups allowed to set up SSL VPN tunnels.

Check this connection in the Stormshield SSL VPN Client firewall's administration interface in **Configuration > Users > Authentication, Available methods** tab. An **LDAP** line must appear in the grid. For more information on how to configure directories, refer to the section Directory configuration in the *user guide of the Stormshield SSL VPN Client version used*.

Permissions to access the Stormshield SSL VPN Client firewall's captive portal

The Stormshield SSL VPN Client firewall's captive portal must be enabled and users who will connect via SSL VPN must be able to access it. With this access:

- Stormshield SSL VPN clients will be able to get their SSL VPN configuration,
- The Stormshield SSL VPN Client firewall and Stormshield SSL VPN clients will be able to apply the policy verifying the compliance of client workstations when zero trust network access is used.

You can check the configuration of the captive portal in the Stormshield SSL VPN Client firewall's administration interface in **Configuration > Users > Authentication, Captive portal** and **Captive**

portal profiles tabs. For more information on the configuration of the captive portal, refer to the section on Authentication in the *user guide of the Stormshield SSL VPN Client version used.*

Multifactor authentication

When multifactor authentication is used for SSL VPN connections:

Multifactor authentication using the Stormshield TOTP solution

- The Stormshield SSL VPN Client firewall must be in version 4.5 and higher,
- The TOTP solution must have been configured in advance. For more information, refer to the technical note Configuring and using the Stormshield TOTP solution.

Multifactor authentication using a third-party solution and a RADIUS server

- The selected multifactor authentication solution must have been configured in advance,
- The RADIUS server, with which the Stormshield SSL VPN Client firewall can be associated with the selected multifactor authentication solution, must have been configured in advance.

Implementing zero trust network access (ZTNA)

When zero trust network access is used:

- The Stormshield SSL VPN Client firewall must be in version 4.8 and higher,
- Every workstation has to use the Stormshield SSL VPN client in version 4.0 or higher,
- The Stormshield SSL VPN client has to be configured in automatic mode.

NOTE

Zero trust network access (ZTNA) consists of trusting users and devices only after they have been verified. Network access is considered "zero trust" when several elements come together:

- The compliance of the communication channel is guaranteed through TLS encryption of VPN tunnels.
- User identities are verified through multifactor authentication (e.g., with the Stormshield TOTP solution),
- A policy verifying the compliance of client workstations and users,
- Granular filtering to restrict users' access to only what is necessary.

Specific characteristics of Stormshield SSL VPN clients v4

This section presents some of the specific characteristics of Stormshield SSL VPN clients v4.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

Compatibility

Compatible versions and operating systems

For more information, refer to the Network Security & Tools life cycle guide.

Compatible multifactor authentication methods

- Password + OTP.
  This method is compatible with the Stormshield TOTP solution. The Stormshield SSL VPN Client firewall must be in version 4.5 and higher to use this solution,
- OTP only,
- Push mode (use of a third-party application to approve the connection).

Connection modes

Automatic mode

In this mode, the Stormshield SSL VPN client automatically and securely retrieves its SSL VPN configuration on the Stormshield SSL VPN Client firewall. It operates as follows:

During the initial connection:

- The Stormshield SSL VPN client will authenticate the first time on the Stormshield SSL VPN Client firewall:
  - The Stormshield SSL VPN client automatically retrieves its VPN configuration,
  - The Stormshield SSL VPN Client firewall and the Stormshield SSL VPN client apply the policy verifying the compliance of client workstations (ZTNA).
- If the first authentication is successful, the Stormshield SSL VPN client will authenticate a second time on the Stormshield SSL VPN Client firewall to set up the SSL VPN tunnel,

During subsequent connections:

- The Stormshield SSL VPN client checks whether a new VPN configuration is available:
  - If there are no new configurations, the Stormshield SSL VPN client will authenticate on the Stormshield SSL VPN Client firewall to set up the SSL VPN tunnel,
  - If a new configuration is available, the Stormshield SSL VPN client will authenticate twice, similarly to the initial connection.

Manual mode

In this mode, you have to import the VPN configuration into a connection profile.

You can retrieve the VPN configuration (*.ovpn* file) from the captive portal of the firewall hosting the SSL VPN service, or from the firewall's administration interface. This operation is described in the section Retrieving the SSL VPN configuration (.ovpn file).

Connection mode compatibility table

This table sums up the compatible features based on the connection mode used.

Feature	Automatic mode	Manual mode
Address book	✓	✗
Profile management	✗	✓
Client workstation compliance (ZTNA) verification *SNS version 4.8 and higher required*	✓	✗

Stormshield SSL VPN client features

Address book (Automatic mode required)

The Stormshield SSL VPN client has an address book that makes it possible to remember the login information to various firewalls: address to connect to the firewall (IPv4 address or FQDN), login, password and the use of multifactor authentication.

Running scripts

In Windows, the Stormshield SSL VPN client can automatically run scripts on the user's workstation every time an SSL VPN tunnel is opened or closed. To do so, you need to add in advance the scripts to run in the configuration of the Stormshield SSL VPN Client firewall's SSL VPN service.

Limitations and explanations on usage

Downgrading to a version lower than version 4

Downgrades to a version lower than version 4 of the Stormshield SSL VPN client are not supported.

When an address book from version 2 or 3 of the Stormshield SSL VPN client is opened in version 4, its format will be automatically updated, and it can no longer be used with its original version. If necessary, you can keep a copy of the address book file in version 2 or 3 before updating the Stormshield SSL VPN client to version 4.

Displaying the icon in the Windows 11 system tray

In Windows 11, ensure that the display of the Stormshield SSL VPN client icon has been enabled in the Windows system tray in **Taskbar settings > Other system tray icons > Hidden**

icon menu. If this is not the case, features of the Stormshield SSL VPN client will not be accessible, as they require access to the icon of the application in order to open its menu.

Configuring the Stormshield SSL VPN Client firewall

Before setting up SSL VPN tunnels, several modules must configured in the Stormshield SSL VPN Client firewall web administration interface. For more information, refer to the SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients.

Installing the Stormshield SSL VPN client v4

This section explains the standard installation process of the Stormshield SSL VPN client v4 with the installation program, either via a group policy (GPO) or via a script.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

NOTE
The Stormshield SSL VPN client cannot be downgraded to an earlier version. In addition, once the SSL VPN client is installed, ensure that it can access the notification zone in the Windows 11 system tray. For further information, refer to Limitations and explanations on usage.

Downloading the Stormshield SSL VPN client v4

The Stormshield SSL VPN client installation program exists in two formats:

Format	Description
.exe	A single executable file that groups all languages and Windows versions supported. For use in a standard installation or deployment via script.
.msi	Several *.msi* packages available depending on the languages and Windows versions supported. For use in a deployment via a group policy (GPO) or via a script.

The Stormshield SSL VPN client can be download in the desired format from:

- **Your MyStormshield area.**
  Log in to your MyStormshield area and go to **Downloads** > **Downloads** > **Stormshield Network Security** > **SSL VPN**.

Enter the following command to check the integrity of retrieved binary files:

```
CertUtil -hashfile <filename> SHA256
```

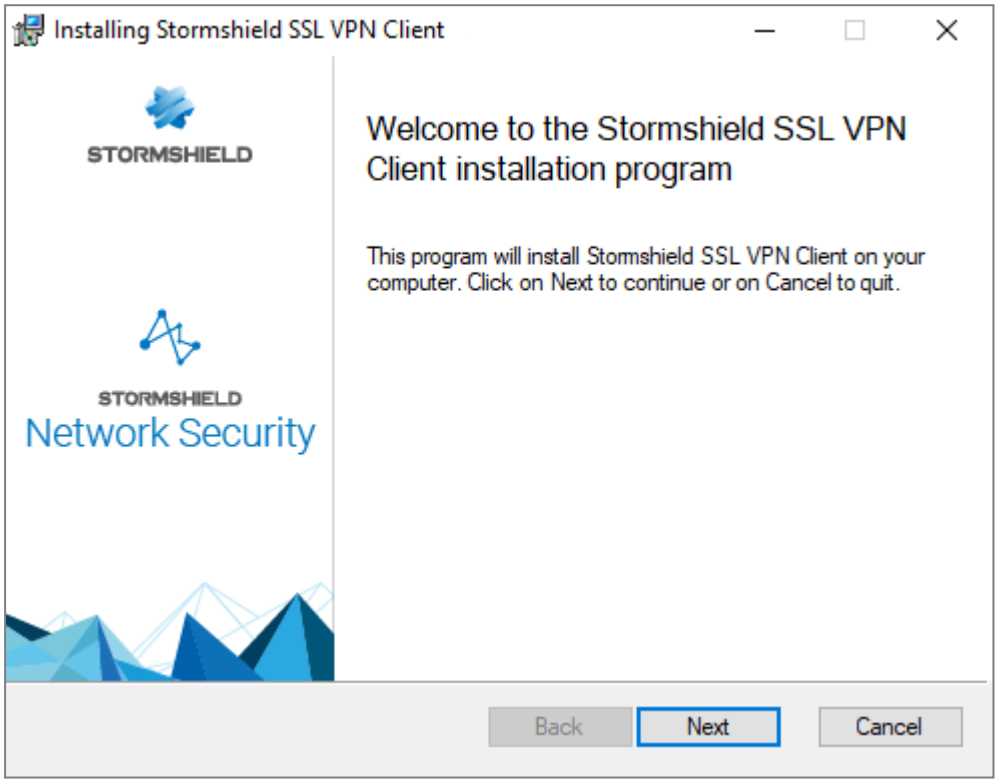
Compare the result obtained with the hash indicated in your MyStormshield area under the **SHA256** column in the download table.

Installing the Stormshield SSL VPN client with the *.exe* installation program

You must be the local workstation administrator or enter the login and password of an administrator account in order to install the Stormshield SSL VPN client.

1. Log in to the user session in which you wish to install the Stormshield SSL VPN client.
2. Run the installation program (*.exe* file) that was downloaded earlier.

3. Follow the steps in the installation wizard.
   You can customize default settings for connections to the VPN:
   - The IP address or FQDN of the firewall,
   - Whether the VPN configuration is to be retrieved in automatic mode,
   - Whether multifactor authentication is to be used,
   - Whether the Windows session user in question is to be used as the ID.



Deploying the Stormshield SSL VPN client via a group policy (GPO)

You can directly deploy the *.msi* package downloaded earlier, or edit it to make it easier for users to connect to the SSL VPN, by customizing certain settings.

Creating an .msi package to customize default settings for connections to the VPN

The following settings can be customized:

- The IP address or FQDN of the firewall,
- Whether the VPN configuration is to be retrieved in automatic mode,
- Whether multifactor authentication is to be used,
- Whether the Windows session user in question is to be used as the ID.

To create the *.mst* package:

1. On a workstation equipped with Microsoft Orca, go to the folder containing the Stormshield SSL VPN client's *.msi* package, right-click and select **Edit with Orca**.
2. Click on **Transform** > **New Transform**.
3. Select the **Property** table.

4. To ensure that the Windows user of the session in question is used as the login, set the **Value** of the *USE_DEFAULT_USERNAME* property to *1*.
5. To ensure that the SSL VPN client uses manual mode by default, set the **Value** of the *AUTOMATIC_MODE property to 0*,
6. To customize the IP address or on FQDN of the firewall:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *DEFAULT_ADDRESS*.
   3. In the **Value** field, enter the firewall's IP address or FQDN.
   4. Click on **OK**.
7. To indicate whether multifactor authentication has to be used:
   1. Right-click and choose **Add Row**.
   2. In the **Property** field, enter *ENABLE_OTP*.
   3. Set the **Value** field to *1* to use multifactor authentication, or to *0* to not use it.
   4. Click on **OK**.
8. Click on **Transform** > **Generate Transform**.
9. Save the *.mst* package in the same folder as the *.msi* package.

Configuring deployment via GPO

1. Run the server manager on the domain controller.
2. In the upper menu bar, click on **Tools** > **Group Policy Management**.
3. In the list on the left, right-click on the Microsoft Active Directory domain name and select **Create a GPO in this domain, and link it here...**
4. Name the GPO and click on **OK**.
5. In the list on the left, right-click on the name of the GPO that you have just created, and select **Edit**.
   The GPO editing window opens.
6. In the menu to the left of the GPO, expand the menu **Computer Configuration** > **Policies** > **Software Settings**.
7. Right-click on **Software installation**, select **New** > **Package**, then select the Stormshield SSL VPN client *.msi* installation package.
8. Select **Advanced** mode and click on **OK**.
   The GPO editing window opens.
9. If you wish to do so, you can rename this installation instance.
10. In the **Changes** tab, you can associate the *.mst* package created earlier with the Stormshield SSL VPN client's installation GPO. To do so, click on **Add**..., select the *.mst* package and click on *Open*.
11. Click on **OK**.

The installation will automatically run when a workstation connects to the company network.

Deploying the Stormshield SSL VPN client via a script

1. Open a command prompt as an administrator.
2. Go to the folder containing the *.exe* file or *.msi* package downloaded earlier.

3. Type the corresponding command:
   - For an *.exe* file:
     ```
     Stormshield_SSLVPN_Client_4.X.Y_x64.exe [PARAMETERS]
     ```
   - For an *.msi* package:
     ```
     msiexec /i Stormshield_SSLVPN_Client_4.X.Y_language_x64.msi
     [PARAMETERS] /qn
     ```

   You can facilitate users' connection to the SSL VPN by adding the following parameters to the command:
   - DEFAULT_ADDRESS=[IP address or FQDN of the firewall],
   - AUTOMATIC_MODE=[0 for manual mode, 1 for automatic mode],
   - USE_DEFAULT_USERNAME=[0 for the field to stay empty, 1 for the Windows user of the session in question to be used as the login],
   - ENABLE_OTP=[0 to not use multifactor authentication, 1 to use a method].
4. Run the command.

Example of a command enabling the deployment of the *.exe* file:

```
Stormshield_SSLVPN_Client_4.0.0_x64.exe DEFAULT_ADDRESS=vpn.company.tld
```

Example of a command enabling the deployment of an *.msi* package:

```
msiexec /i Stormshield_SSLVPN_Client_4.0.0_en_x64.msi DEFAULT_
ADDRESS=vpn.company.tld AUTOMATIC_MODE=1 ENABLE_OTP=0 /qn
```

The installation will automatically run when a workstation connects to the company network. A command prompt will appear on the desktop and a status bar indicates the progress of the installation.

Configuring the Stormshield SSL VPN client v4

The Stormshield SSL VPN client v4 has to be configured according to the desired connection mode. Refer to the section Connection mode compatibility table for the list of compatible features based on the connection mode used.

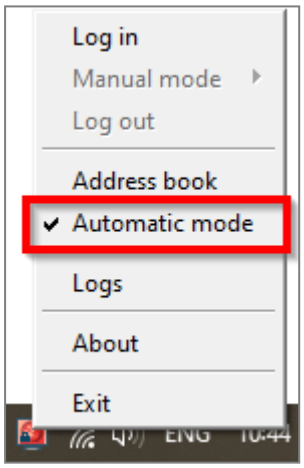
NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Enabling Automatic mode

In **Automatic mode**, the Stormshield SSL VPN client automatically retrieves the VPN configuration after authenticating the user and validating permission to use the SSL VPN.

1. Right-click on the icon in the Windows system tray.
2. Click on **Automatic mode**.

To log in, continue to the section Setting up VPN tunnels in Automatic mode.

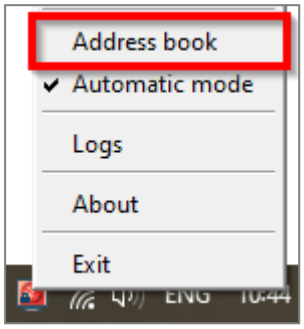


Configuring the address book (Automatic mode required)

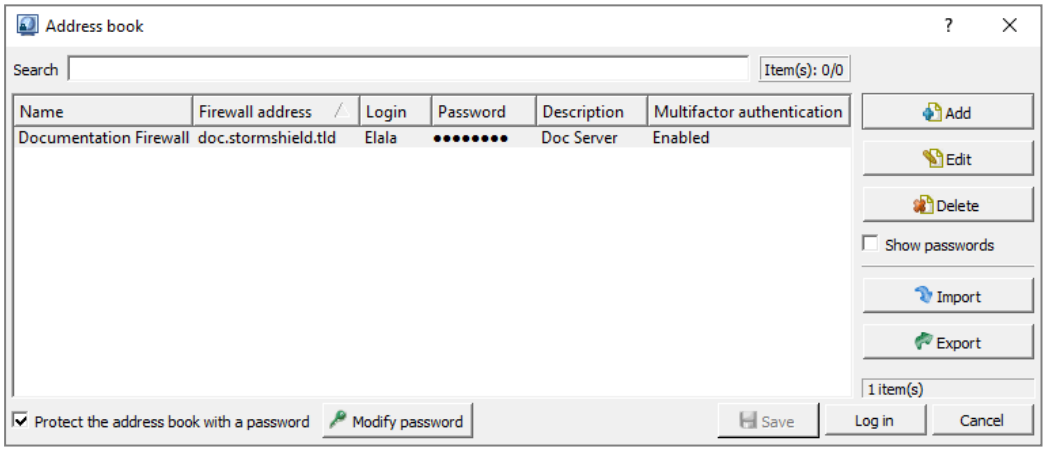
The Stormshield SSL VPN client has an address book that makes it possible to remember the login information to various firewalls: address to connect to the firewall (IPv4 address or FQDN), login, password and the use of multifactor authentication.

Opening the address book

1. Right-click on the icon in the Windows system tray.
2. Click on **Address book**. **Automatic mode** must be enabled.



3. If the address book is protected by a password, enter it to open the address book. You can protect the address book by using the options **Protect the address book with a password** and **Modify password**.

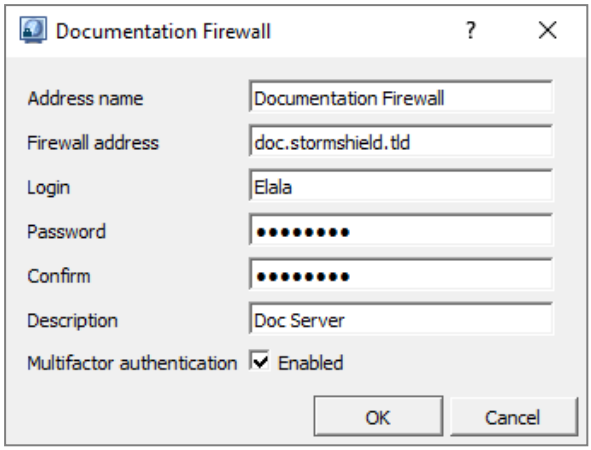


Adding or changing an address in the address book

1. Click on **Add** to add a new address. To change an existing address, select it and click on **Edit**.
2. Fill in the required fields.

Field/checkbox	Description
Address name	Name of the firewall address.
Firewall address	IPv4 address or FQDN of the Stormshield SSL VPN Client firewall to contact in order to set up the VPN tunnel. If the port of the firewall's captive portal is different from the default port (TCP/443), enter the address and listening port separated by colons (address:port).
Login	User Identifier.
Password **Confirm**	User's password. If **OTP only** or **Push mode** multifactor authentication is used, leave these fields empty.
Description	Description of the address, if necessary.
Multifactor authentication	If multifactor authentication is used (**Password + OTP, OTP only** or **Push mode**), select **Enabled**.

3. Click on **OK**, then on **Save**.



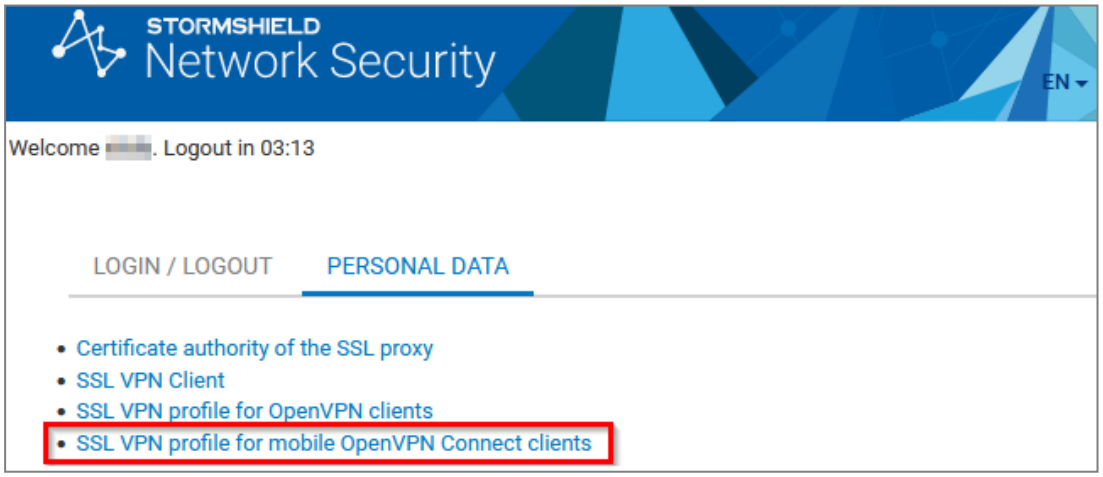
Configuring Manual mode

In **Manual mode**, import the configuration components (certification authority, certificate, private key, etc.) that the Stormshield SSL VPN client must use, compiled in an *.ovpn* file.

Retrieving the SSL VPN configuration (*.ovpn* file)

The configuration of the Stormshield SSL VPN can be retrieved from:

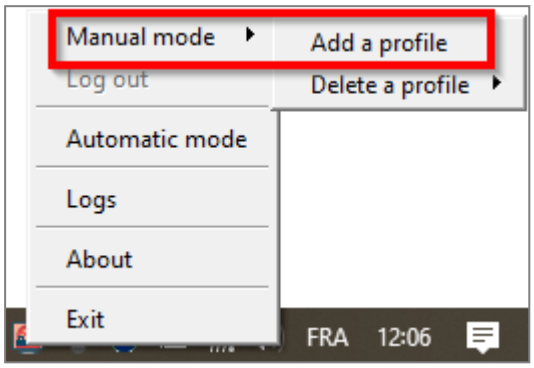
- **The captive portal of the Stormshield SSL VPN Client firewall that hosts the SSL VPN service.**
  Once you are connected to the corporate network, authenticate at *https://firewall_IPaddress/auth*, and in the **Personal data** tab, click on *SSL VPN profile for mobile OpenVPN Connect clients (single .ovpn file)*,



- **The Stormshield SSL VPN Client firewall's administration interface.**
  Go to **Configuration > VPN > SSL VPN** > **Advanced configuration**, and click on **Export the configuration file**.

Adding a connection profile

1. Right-click on the icon in the Windows system tray.
2. Click on **Manual mode** > **Add a profile**. **Automatic mode** must be disabled.



3. Select the *.ovpn* file.
4. Assign a name to the connection profile.
5. Click on **OK**.

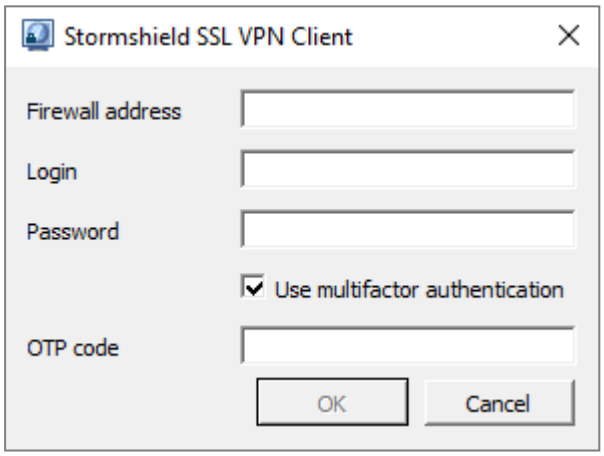
Setting up a VPN tunnel with the Stormshield SSL VPN client v4

Now that the Stormshield SSL VPN Client firewall and SSL VPN client v4 have been configured, you can proceed with setting up a VPN tunnel.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

Setting up VPN tunnels in Automatic mode

1. Double-click on the icon in the Windows system tray to open the connection window.



2. In the **Firewall address** field, indicate the IPv4 address or FQDN of the Stormshield SSL VPN Client firewall to reach in order to set up the VPN tunnel. If the port of the firewall's captive portal is different from the default port (TCP/443), enter the address and listening port separated by colons (address:port),
3. In the **User name** field, enter the user's login.
4. Fill in the remaining fields according to the authentication method used.
In the table, ✔ means that the fields are mandatory, ✘ means that they have to remain blank, and - means that they are not visible.

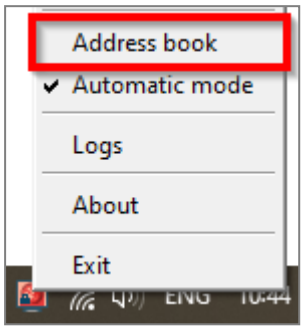
Authentication method	Password	Multifactor authentication	OTP
Standard	✔	✘	-
Password + OTP multifactor authentication	✔	✔	✔
OTP only multifactor authentication	✘	✔	✔
Push mode multifactor authentication	✘	✔	✘

5. Click on **OK**.

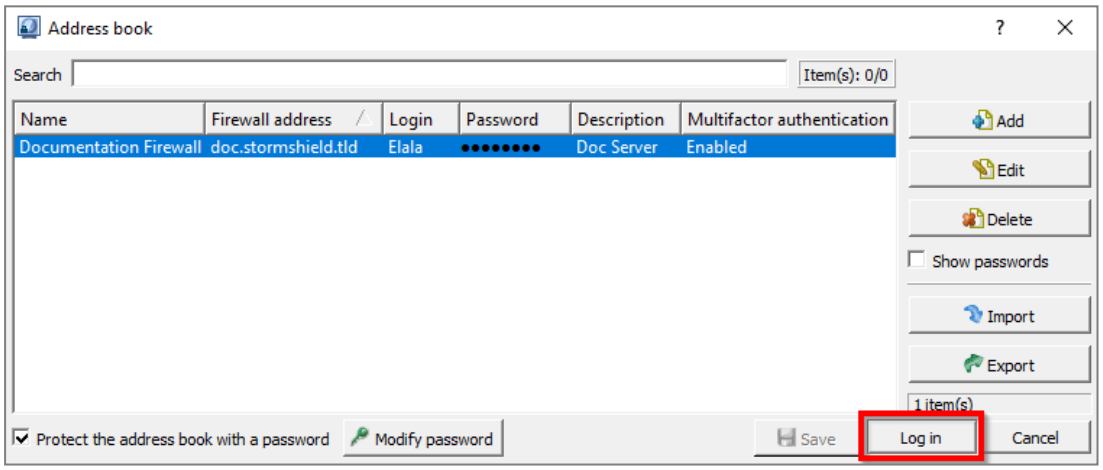
The Stormshield SSL VPN client will authenticate on the Stormshield SSL VPN Client firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

Setting up VPN tunnels by using the address book

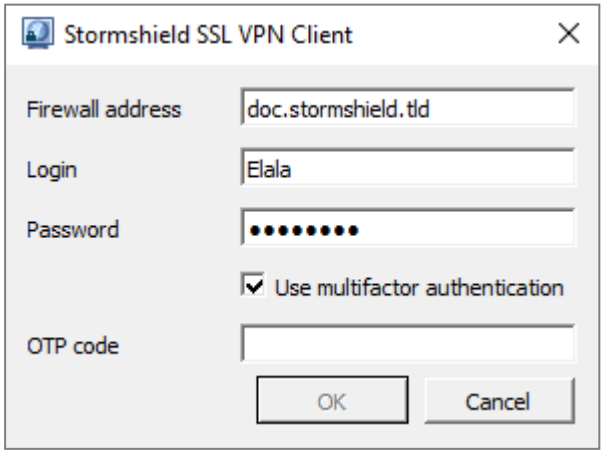
1. Right-click on the icon in the Windows system tray, then click on **Address book**. As a reminder, **Automatic mode** must be enabled.



2. If the address book is protected by a password, enter it to open the address book.
3. Select the address from which you are connecting and click on **Log in**.



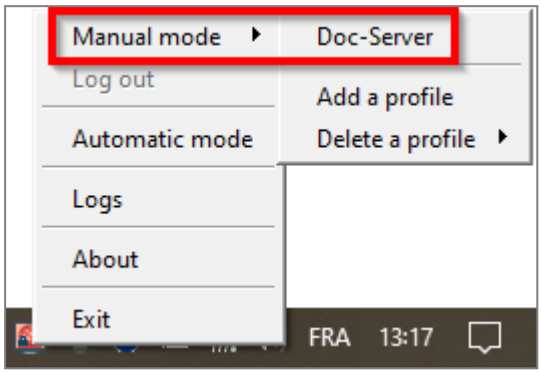
4. The connection window will appear.
   - In a standard authentication, the connection will automatically launch,
   - In a **Password + OTP** or **OTP only** multifactor authentication, enter an **OTP** (one-time password) and click on **OK**,
   - For **Push mode** multifactor authentication, click on **OK** and approve the connection to the third-party application.



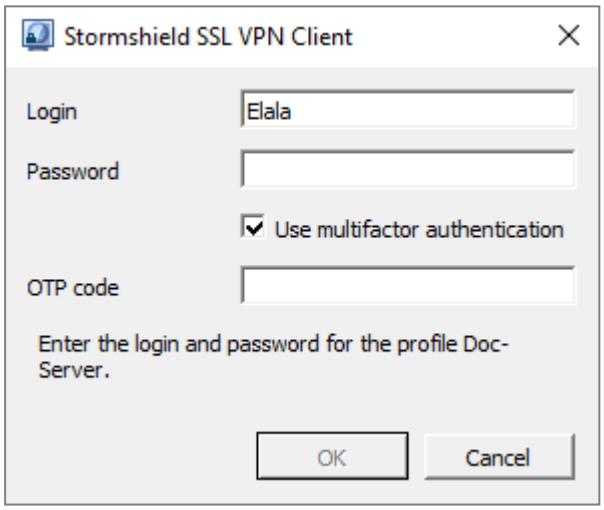
The Stormshield SSL VPN client will authenticate on the Stormshield SSL VPN Client firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

Setting up VPN tunnels in Manual mode

1. Right-click on the icon in the Windows system tray, then click on **Manual mode** and on the relevant profile.



The connection window will open.



2. In the **User name** field, enter the user's login.
3. Fill in the remaining fields according to the authentication method used.
In the table, ✅ means that the fields are mandatory, ❌ means that they have to remain blank, and - means that they are not visible.

Authentication method	Password	Multifactor authentication	OTP
Standard	✅	❌	-
Password + OTP multifactor authentication	✅	✅	✅
OTP only multifactor authentication	❌	✅	✅
Push mode multifactor authentication	❌	✅	❌

4. Click on **OK**.

The Stormshield SSL VPN client will authenticate on the Stormshield SSL VPN Client firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

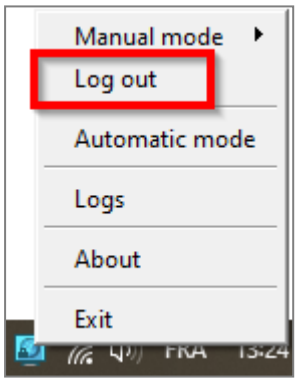
Showing the connection information of SSL VPN tunnels

The color of the Stormshield SSL VPN client icon in the Windows system tray indicates its connection status.

Icon	Description
	The Stormshield VPN SSL client is connected. Scroll over the icon to show information about the SSL VPN tunnel (user name and address of the Stormshield SSL VPN Client firewall, time at which the connection was set up with the Stormshield SSL VPN Client firewall, IP address of the workstation through the SSL VPN tunnel and number of bytes exchanged).
	The Stormshield SSL VPN client is connecting.
	The Stormshield SSL VPN client is not connected or a connection attempt failed.

Disconnecting SSL VPN tunnels

1. Right-click on the  icon in the Windows system tray.
2. Click on **Log out**.



When VPN tunnel fails to set up

When a VPN tunnel fails to set up, follow these recommendations:

- Read the error message that appears,
- Check the connection information in the connection window, and in the address book, if one is used,
- Check the validity of the OTP if it has been 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,
- Check the configuration of the imported connection profile (in Manual mode). For example, if the Stormshield SSL VPN Client firewall's SSL VPN configuration has been modified, it will be imported on the Stormshield SSL VPN client,
- Refer to the Troubleshooting section.

Viewing the logs of the Stormshield SSL VPN client v4

This section presents the logs available on the Stormshield SSL VPN client v4.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

Logs regarding installation errors, uninstallation or updates

Logs are generated whenever an error occurs while installing, uninstalling or updating the Stormshield SSL VPN client. You can find them at:

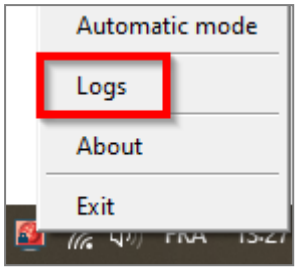
```
%programfiles%\Stormshield\Stormshield SSL VPN Client\install_logs
```

File name	Content
install_driver.log	Errors encountered while installing the OpenVPN driver
uninstall_driver.log	Errors encountered while deleting the OpenVPN driver
backward_update_sites.log	Errors encountered while copying connection profiles from the Stormshield SSL VPN client in version 3.2.3 or lower
generate_ovpn_auth.log	Errors encountered while generating the private key used to secure access to the OpenVPN management interface
tap_create.log	Errors encountered while installing the network interface for OpenVPN
tap_delete.log	Errors encountered while deleting the network interface for OpenVPN
update_ovpn_admin.log	Errors encountered while updating the *ovpn_admin_group* value in the *HKEY_LOCAL_MACHINE\SOFTWARE\StormshieldSSLVPN* key
clean_previous_version.log	Information regarding the uninstallation of version 3.2.3 or lower
install_certs.log	Errors encountered while installing the certificate
set_dacls.log	Errors encountered while updating privileges to access folders
service_update.log	Errors encountered while updating the SSL VPN service

SSL VPN connection logs

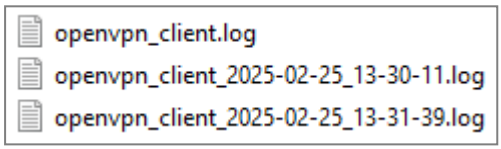
You can look up SSL VPN connection logs by right-clicking on the  icon in the Windows system tray, then on **Logs**, or in the Windows file explorer at this location:

```
%localappdata%\Stormshield\Stormshield SSL VPN Client\log\openvpn_
client.log
```



When setting up an SSL VPN tunnel:

- If the size of the *openvpn_client.log* file exceeds 1 MB, it will be renamed in the following format "*openvpn_client_yyyy-MM-dd_hh-mm-ss.log*" and a new file *openvpn_client.log* will be created,
- If the total size of the *.log* files exceeds 100 MB, the oldest files will be deleted.



Logs accessible in the Windows Event Viewer

Logs relating to the Stormshield SSL VPN client can be accessed through the Windows Event Viewer on user workstations.

By default, only error logs can be accessed through the Windows Event Viewer.

To access the Stormshield SSL VPN client's logs:

1. Open the Windows **Event Viewer**.
2. Select **Applications and services logs > Stormshield SSL VPN service**.

To change the logs accessible in the Windows Event Viewer:

1. Open the Windows **Registry editor**.
2. Change the *log_level* value of the following registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
StormshieldSSLVPNService\Parameters
```

   - 0: displays error logs. This is the default value,
   - 1: displays error and information logs,
   - 2: displays error, information and troubleshooting logs.

Tracking users connected to the SSL VPN on the Stormshield SSL VPN Client firewall

In the Stormshield SSL VPN Client firewall's administration interface, you can track connected users or those connected to the SSL VPN. For more information, refer to the SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients.

Troubleshooting

This chapter covers some of the issues that occur most frequently when using the Stormshield SSL VPN client v4. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the Stormshield knowledge base.

NOTE
If you are using the Stormshield VPN SSL client in version 5, refer to the Stormshield SSL VPN Client v5 documentation.

Users have to approve the certificate presented by the SNS firewall during an initial connection

- *Situation*: When the SSL VPN tunnel is being set up for the first time, users have to approve the certificate presented by the SNS firewall, even though the certification has been certified by a certification authority found in the users' certificate store.
- *Cause*: The root certificate authority is found only in users' certificate store, and is not in the certificate store on the workstation. By default, the certificate store on the workstation is used when the Stormshield SSL VPN client verifies the certificate.
- *Solution*: Change the **http_request_as_user** value to 1 in the registry base under the key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters
```

The SSL VPN tunnel failed to set up

A proxy configuration has been defined on the workstation and the Stormshield SSL VPN client is unable to reach the SNS firewall

- *Situation*: During an attempt to connect to the SSL VPN on a workstation that has a proxy connection, the tunnel failed to set up.
- *Cause*: Direct HTTPS access is not allowed without using the proxy on the workstation. By default, HTTPS requests to the SNS firewall, notably to download the VPN configuration, are directly submitted by the Stormshield SSL VPN client without going through the proxy.

  NOTE
  Up until version 4.0.9, version 4.0 of the Stormshield SSL VPN client used the proxy configuration that was defined on the workstation to contact the SNS firewalls in HTTPS. This behavior has been changed in version 4.0.10.

- *Solution*: Change the **http_use_default_proxy** value to 1 in the registry base under the key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters
```

The message "The connection was denied as the user or workstation used does not comply with the policy defined on the firewall" appears

- *Situation*: *During the attempt to connect to the SSL VPN, the tunnel would not set up and the message "The connection was denied as the user or workstation used does not comply with the policy defined on the firewall"* appears.
- *Cause*: The client workstation that was used does not comply with all the criteria defined in the policy verifying the compliance of client workstations and users (ZTNA).
- *Solutions*:
  - Check the VPN logs (SSL and IPsec) and identifying the verification criteria that have not been met on a client workstation, then rectify the configuration of the client workstation in question,
  - Check the configuration of the policy verifying the compliance of client workstations.

The message "*Could not connect to firewall: Failed to resolve UTM name*" appears

- *Situation*: During the attempt to connect to the SSL VPN, the tunnel will not set up and the message "*Could not connect to firewall: Failed to resolve UTM name*" appears.
- *Cause*: The address entered is incorrect or unreachable.
- *Solution*: Check that the firewall address entered is correct and can be reached.

The message "*Login or password incorrect*" appears

- *Situation*: During the attempt to connect to the SSL VPN, the tunnel won't set up and the message "*Could not connect to firewall: Failed to resolve UTM name*" appears.
- *Cause*: Either the user's password is incorrect or the user does not have sufficient privileges to authenticate on the SSL VPN.
- *Solutions*:
  - Check that the login and password are correct.
  - On the Stormshield SSL VPN Client firewall, check that the **SSL VPN policy** has been set to **Allow** in **Configuration > Users > Access privileges, Default access** tab, and that the user or user group in question is allowed to set up SSL VPN tunnels in **Configuration > Users > Access privileges, Detailed access** tab

The message "*Error while connecting to the service: Connection refused*" appears

- *Situation*: During the attempt to connect to the SSL VPN, the tunnel won't set up and the message "*Error while connecting to the service: Connection refused*" appears.
- *Cause*: The **Stormshield SSL OpenVPN Service** and **Stormshield SSL VPN Service** services are not running or are not working.
- *Solution*: Ensure that the Windows services have been started up on the workstation, or try to restart them.

Logs contain the message "*Route: Waiting for TUN/TAP interface to come up...*"

- *Situation*: During the attempt to connect to the SSL VPN, the tunnel won't set up and the message "*Error while connecting to the service: Connection refused*" appears in logs.

- *Cause*: An issue with the **TAP-Windows Adapter** interface prevents the VPN tunnel from setting up.
- *Solution*: In the **Windows Network and Sharing Center**, click on **Change adapter settings**, right-click on the **TAP-Windows Adapter** interface and click on **Diagnose**.

A corporate resource cannot be accessed over the VPN tunnel

- *Situation*: The tunnel has been set up, but a corporate resource cannot be accessed.
- *Cause*: Either the firewall's filter policy is blocking access to this resource or the resource is no longer accessible. There may also be other causes for this situation.
- *Solutions*:
  - On the Stormshield SSL VPN Client firewall, temporarily enable **Advanced** logging in the rule regarding the traffic in question to collect logs (in **Configuration > Security policy > Filter - NAT > Filtering**), then in the logs, check whether the rule applies to the traffic (in **Monitoring > Logs - Audit logs > Filtering**),
  - Ensure that the requested resource is in fact physically available.
  - Clear the workstation's ARP cache by running the command `arp -d *` in a console.

The VPN tunnel shuts down whenever very large files are sent

- *Situation*: Whenever a large file is sent, the VPN tunnel shuts down.
- *Cause*: The file sent is too large.
- *Solution*: Send the file over a protocol, such as FTP, that uses smaller blocks, or set up the tunnel over UDP.

A warning message indicates that LZ4 compression is obsolete

- *Situation*: In the web administration interface of an Stormshield SSL VPN Client firewall in version 4.8.5 or higher, if the LZ4 compression feature is enabled, a warning message automatically appears when the SSL VPN module opens.
- *Cause*: The LZ4 compression feature is obsolete, and we strongly recommend disabling it for security reasons.
- *Solution*: In the warning window, accept the suggestion to disable the feature. If you ignore this warning, a message will continue to be displayed as long as the feature is not disabled. You will then need to use these CLI/serverd commands to disable it:

```
CONFIG OPENVPN UPDATE compress=0
CONFIG OPENVPN ACTIVATE
```

Further reading

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

documentation@stormshield.eu