TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING AND USING SSL VPN ON SNS FIREWALLS

Product concerned: SN SSL VPN Client 4, SNS 4 and SNS 5

Document last updated: May 22, 2025

Reference: sns-en-ssl_vpn_tunnels_technical_note

Table of contents

Change log

Date	Description
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 SNS firewall" has been enriched.
	• Addition of the implementation of zero trust network access (ZTNA).

Getting started

SSL VPN allows remote users to securely access a company's resources - internal or otherwise - via the SNS 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 SNS firewall. Communications between the SNS 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 SNS firewall. This solution therefore guarantees confidentiality, integrity and non-repudiation.

This technical note provides details on:

- Enabling and configuring the SSL VPN service on SNS firewalls in version 4.x,
- Implementing zero trust network access (ZTNA) with SNS 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, SN SSL VPN Client may be referred to as "Stormshield SSL VPN client".

NOTE
If you are using the Stormshield VPN SSL client in version 3.x, refer to the technical note Configuring and using the SSL VPN on SNS firewalls with the SSL VPN Client v3 (PDF only).

Requirements

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

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 SNS firewall. Compatible VPN clients are:

- **SN SSL VPN Client**: this technical note explains how to install, configure and use the client, including the setup of an SSL VPN tunnel, some of its specific characteristics (compatibility, connection modes, etc.) and access to its logs,
- **OpenVPN Connect**: for more information, refer to the section Appendix: installing, configuring and using OpenVPN Connect,
- **SN VPN Client Standard**: for further information, refer to the document SN VPN Client Standard User Guide,
- **SN VPN Client Exclusive**: for further information, refer to the SN VPN Client Exclusive Administration guide.

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.

An adapted SNS firewall

The maximum number of SSL VPN tunnels allowed on SNS 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 SNS firewall to a directory

The SNS 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 SNS 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 SNS version used*.

Permissions to access the SNS firewall's captive portal

The SNS 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 SNS 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 SNS 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 SNS version used.*

Multifactor authentication

When multifactor authentication is used for SSL VPN connections:

Multifactor authentication using the Stormshield TOTP solution

- The SNS 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 SNS 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 SNS 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.

The following sections in this technical note cover the configuration of these elements. Every one of the elements must be configured in order for zero trust network access (ZTNA) to be effectively implemented.

Specific characteristics of Stormshield SSL VPN clients

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

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 SNS 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 SNS firewall. It operates as follows:

During the initial connection:

- The Stormshield SSL VPN client will authenticate the first time on the SNS firewall:
  - The Stormshield SSL VPN client automatically retrieves its VPN configuration,
  - The SNS 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 SNS 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 SNS 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 SNS firewall's SSL VPN service. This operation is described in the section Scripts to run on the client.

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 SNS firewall

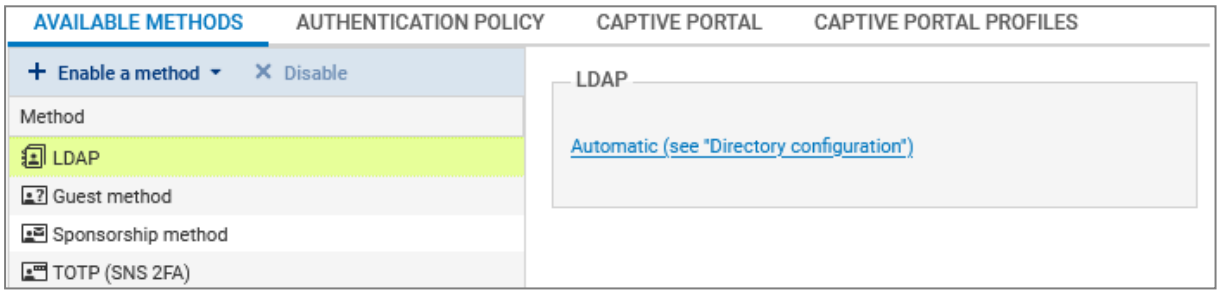
Before setting up SSL VPN tunnels, several modules must configured in the SNS firewall web administration interface.

Configuring authentication

Go to **Configuration > Users > Authentication**.

Multifactor authentication and zero trust network access (ZTNA)

You can see which methods have been enabled in the **Available methods** tab.



Multifactor authentication using the Stormshield TOTP solution

The TOTP method has to be enabled and 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 third-party multifactor authentication solution connected to your RADIUS server has to be configured in advance. The RADIUS method that makes it possible to connect the SNS firewall to your RADIUS server also has to be enabled and configured in advance. For more information, refer to the section on Authentication in the *user guide of the SNS version used*.

The default idle timeout allowed to connect to a RADIUS server is 3000 milliseconds (3 seconds). When a **Push mode** multifactor authentication method is used, you need to change this timeout to give users enough time to authenticate. For a 30-second timeout, for example, use the following CLI/serverd commands:

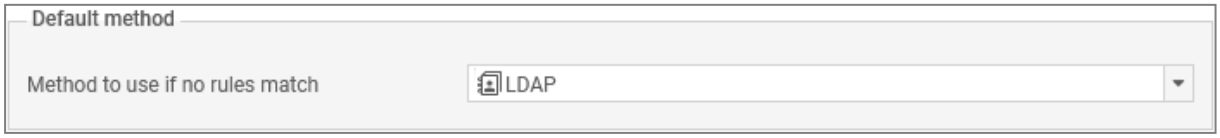
```
CONFIG AUTH RADIUS timeout=30000 btimeout=30000
CONFIG AUTH ACTIVATE
```

Zero trust network access (ZTNA)

A method enabling the verification of user identities through multifactor authentication has to be configured in advance. For more information, refer to the above examples.

Configuring the authentication policy

In the **Authentication policy** tab, you will see the **Method to use if no rules match**. Proceed accordingly.



The firewall uses the default LDAP method and I use only this method

The current configuration will suffice. Continue to Configuring the captive portal.

In all other cases

In all other cases (authentication restricted to only what is necessary, use of multifactor authentication, etc.), you need to add at least two rules by clicking on **New rule > Standard rule**.

For greater security, you can set specific rules for different user groups. Do note that during authentication, rules will be scanned in the order of their appearance in the list.

For the first rule:

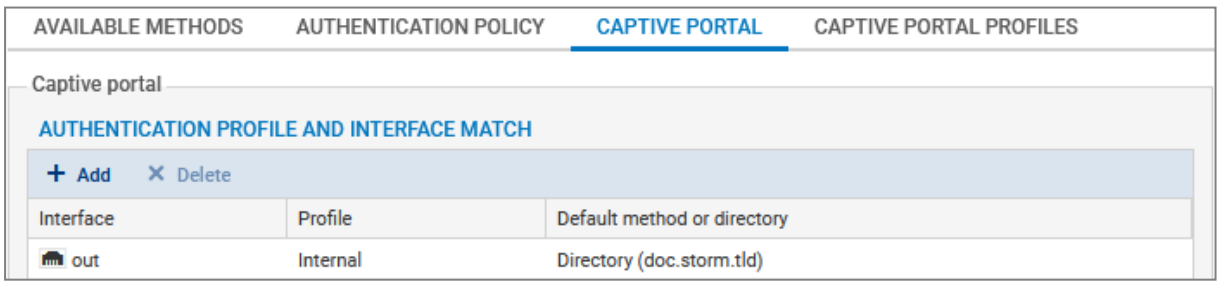
1. In the **User** tab, **User or group** field: select the relevant user group. *Any user@* applies to all users on the domain.
2. In the **Source** tab, add the external interface through which users authenticate (e.g. *out*).
3. in the **Authentication methods** tab, delete the *Default method* row and enable the method (*LDAP*, *RADIUS*, etc.) that makes it possible to connect to the firewall's captive portal and retrieve the VPN configuration. Set the selector to **ON** if the TOTP must be used.

For the second rule:

1. In the **User** tab, **User or group** field: select the relevant user group. *Any user@* applies to all users on the domain.
2. In the **Source** tab, add the *SSL VPN* interface.
3. In the **Authentication methods** tab, delete the *Default method* row and enable the method (*LDAP, RADIUS*) that makes it possible to set up SSL VPN tunnels, Set the selector to **ON** if the TOTP must be used.

Configuring the captive portal

The configuration of this portal can be found in the **Captive portal** tab.



Authentication profile and interface match

1. In the **Authentication profile and interface match** grid, click on **Add**.
2. In the **Interface** column, select the SSL VPN clients' source interface. If you are using a PPPoE or VLAN interface, select it instead of the physical parent interface.
3. In the **Default method or directory** column, if the directory entered corresponds to the directory of the users connecting to the SSL VPN, these users will be able to connect simply by entering their login in the connection window. Otherwise, they will need to enter their login and the domain in question (*login@domain.tld*).

You can edit the configuration so that these users no longer need to specify the relevant domain in addition to their login:

1. In the **Captive Portal** tab, select another profile (e.g. *default05*),
2. In the **Captive portal** profiles tab, select this other profile, choose the right directory from the **Default method or directory** field, and then enable the captive portal in the **Advanced properties** section.

SSL server - Captive portal certificate (private key)

You can select the certificate presented by the captive portal in the **Certificate (private key)** field. The icon indicates certificates with a TPM-protected private key.

If any one of these criteria applies to the selected certificate, a window will appear during each user's initial connection, to indicate that the certificate is not trusted:

- The certificate was not signed by a qualified certification authority,
- The certification authority has not been deployed on users' workstations,
- The certificate's **CN** does not match the firewall address that is used for connections to the SSL VPN.

Each user will then need to indicate that they trust the certificate order to log in. Although this message does not prevent users from proceeding, we recommend explaining to your users when they should or should not expect to see it. For example, this message will appear if you are using the self-signed certificate that was created when the SNS firewall was initialized, and which the firewall presents by default.

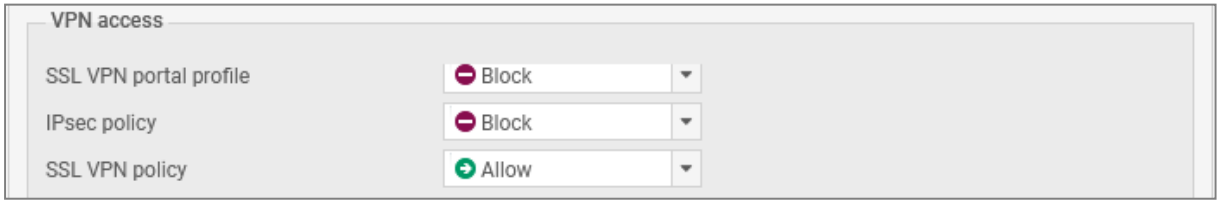
Assigning access privileges to the SSL VPN

Privileges have to be assigned to allow users to set up SSL VPN tunnels.

Go to **Configuration** > **Users** > **Access privileges**.

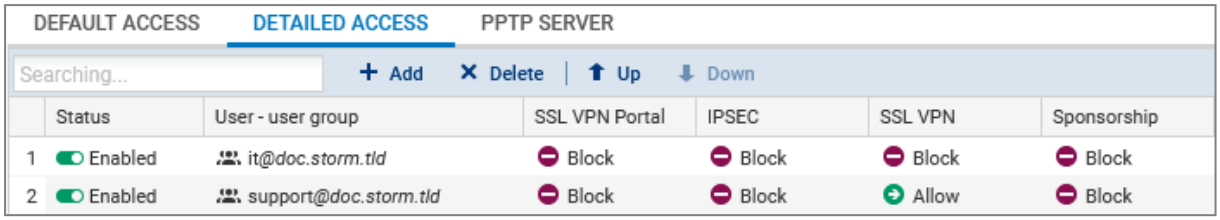
Allowing all users to set up SSL VPN tunnels

1. In the **Default access** tab, **SSL VPN policy** field, select **Allow**.



Allowing some users and user groups to set up SSL VPN tunnels

1. In the **Default access** tab, **SSL VPN policy** field, select **Block**.
2. In the **Detailed access** tab, click on **Add** to create a custom access rule.
3. Select the relevant user or user group.
4. In the **SSL VPN** column, select **Allow** as the action.
5. Enable the rule by double-clicking in the **Status** column in the relevant row.



Configuring the SSL VPN service

This section explains how to enable and configure the SSL VPN service.

Go to **Configuration > VPN > SSL VPN**.

NOTE
As of SNS version 4.8.5, if the LZ4 compression feature in the SSL VPN service is enabled, a warning message will automatically appear when the module opens, encouraging you to disable the feature. This scenario is described in the section Troubleshooting.

Enabling the SSL VPN service

Field	Description
Enable SSL VPN 	Set the selector to **ON** to enable the SSL VPN service.

Configuring the general settings of the SSL VPN service

On SNS in versions 4.8 and higher, these settings can be configured in the **General settings** tab.
On SNS 4.3 LTSB versions, there is no tab.

Field	Description
Enable client workstation verification (ZTNA) 	On SNS in version 5, set the selector to **ON** to enable the verification of client workstation compliance. When it is enabled: • Compatible SSL VPN clients can set up SSL VPN tunnels with the firewall **only if all** the criteria defined in the policy have been met, • Incompatible SSL VPN clients cannot set up SSL VPN tunnels with the firewall, **unless** permissive mode has been enabled. On SNS 4.8 versions, the verification can be enabled in the **Client workstation verification (ZTNA)** tab (see Configuring client workstation verification (ZTNA)). On SNS 4.3 LTSB versions, this feature is not available.

Network settings section

Field	Description
Public IP address (or FQDN) of the UTM used	Indicate the IP address that users must use to reach the SNS firewall in order to set up VPN tunnels. You can indicate either an IP address or FQDN. • For IP addresses: they must be public, and therefore accessible over the Internet, • For FQDNs: they must be declared on the DNS servers that the workstation uses when it is outside the corporate network. If you have a dynamic public IP address, you can use the services of a provider such as *DynDNS* or *No-IP* dynamic, and then configure this FQDN in the module **Configuration > Network > Dynamic DNS**.
Available networks or hosts	Select the object representing the networks or hosts that will be reached through the VPN tunnel. This object makes it possible to automatically set on the workstation the routes needed to reach resources that can be accessed via the VPN. You will need to set filter rules to more granularly allow or prohibit traffic between remote workstations and internal resources. You may also need to set static routes for access to the network assigned to VPN clients on corporate network devices located between the SNS firewall and the internal resources provided.
Network assigned to clients (UDP) **Network assigned to clients (TCP)**	Select the object corresponding to the network that has been assigned to VPN clients in UDP and TCP. The network mask must not be smaller than **/28**. If you assign two networks, VPN client will always choose the UDP network first to ensure better performance. Choosing the network or sub-networks: • The assigned network must not belong to any existing internal networks, or networks declared by a static route on the SNS firewall. Since the interface used for the SSL VPN is protected, the firewall would then detect an IP spoofing attempt and block the corresponding traffic. • To avoid routing conflicts, select less commonly used sub-networks (such as 10.**60.77**.0/24) as many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks already use the first few reserved address ranges. • On SNS in version 5, if you are using **TCP-based SSL VPN tunnels**, ensure that the DCO kernel acceleration feature is disabled in the *Advanced properties* section. Otherwise, the performance of such tunnels will be downgraded.
Maximum number of simultaneous tunnels allowed	The number appears automatically. This number corresponds to the lowest value, either the number of tunnels allowed on the SNS firewall (see Requirements), or the number of sub-networks available for VPN clients. For sub-networks: • On SNS in version 5: this shows the total number of IP addresses, minus 3. • On SNS in version 4.3 LTSB and 4.8: this represents 1/4 of the IP addresses, minus 2. An SSL VPN tunnel takes up 4 IP addresses and the server reserves 2 sub-networks for its own use.

DNS settings sent to client section

Field	Description
Domain name	Enter the domain name assigned to the SSL VPN clients so that they can resolve their host names.
Primary DNS server **Secondary DNS server**	Select the object representing the DNS server to be assigned.

Advanced properties section

Field	Description
Enable DCO kernel acceleration	On SNS in version 5, select the checkbox to enable the DCO (Data Channel Offload) kernel acceleration feature. This option is enabled by default in factory configuration. On SNS in version 4, this feature is not available. This feature transfers the encryption/decryption of data packets passing through SSL VPN tunnels to the operating system kernel. This increases the performance of **UDP-based tunnels** and enables the SSL VPN service to process the setup of many more UDP tunnels. However, this feature is not compatible with **TCP-based tunnels**, and **downgrades their performance**. Ensure that you disable it if you are using such tunnels. **NOTE** When the checkbox is selected, if the encryption suite used by the SSL VPN service is incompatible with the DCO kernel acceleration feature, a window appears, encouraging you to use the AES-256-GCM encryption suite. Accept the change to enable the feature.
Public IP address of the UTM for the SSL VPN (UDP)	In either of the following cases, you need to select the object representing the IP address used for setting up UDP SSL VPN tunnels: • The IP address used for setting up the SSL VPN tunnels (UDP) is not the main IP address of the external interface. • The IP address used for setting up the SSL VPN tunnels (UDP) belongs to an external interface that is not linked to the default gateway of the firewall.
Port (UDP) **Port (TCP)**	The listening ports of the SSL VPN service can be changed. Note: • Some ports are reserved for the SNS firewall's internal use only and cannot be selected, • Port 443 is the only port below 1024 that can be used, • If you change any of the default ports, the SSL VPN could become inaccessible from networks (hotels or public WiFi) on which Internet access is filtered.
Interval before key renegotiation (seconds)	You can change the length of time (14400 seconds by default, or 4 hours) after which the keys used by the encryption algorithms will be renegotiated. During this operation: • The SSL VPN tunnel will not respond for several seconds, • If multifactor authentication is used, the user will need to enter a new OTP, or approve the new connection on the third-party application (in push mode), in order to stay connected. It would be helpful to set an interval that corresponds to the average length of a workday, such as 28800 seconds (8 hours).
Use DNS servers provided by the firewall	You can instruct VPN clients to include the DNS servers retrieved via the SSL VPN in the workstation's (Windows only) network configuration. If DNS servers are already defined on the workstation, they may be queried.
Prohibit use of third-party DNS servers	You can instruct VPN clients to exclude the DNS servers that have already been defined in the workstation's (Windows only) configuration. Only DNS servers sent by the SNS firewall can be queried.

Scripts to run on the client

In Windows, the Stormshield SSL VPN client can run *.bat* scripts when an SSL VPN tunnel is opened or closed. In these scripts, you can use:

- Windows environment variables (**%USERDOMAIN%**, **%SystemRoot%**, etc.),
- Variables relating to the Stormshield SSL VPN client: **%NS_USERNAME%** (user name used for authentication) and **%NS_ADDRESS%** (IP address assigned to the SSL VPN client).

Field	Description
Script to run when connecting	Select the script to run when the VPN tunnel is opened. Example of a script that makes it possible to connect the Z: network drive to the shared network: `NET USE Z: \\myserver\myshare`
Script to run when disconnecting	Select the script to run when the VPN tunnel is closed. Example of a script that makes it possible to disconnect the Z: network drive from a shared network: `NET USE Z: /delete`

Certificates

Select the certificates that the SNS firewall's SSL VPN service and the Stormshield SSL VPN client must present to set up a tunnel. They must be issued from the same certification authority.

The default suggestions are the certification authority dedicated to the SSL VPN, and a server certificate and a client certificate created when the firewall was initialized.

Field	Description
Server certificate	Select the desired certificate. The icon indicates certificates with a TPM-protected private key. For more information, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.
Client certificate	Select the desired certificate. Client certificates with a TPM-protected private key cannot be selected as the private keys of such certificates must be available in plaintext (unencrypted) in the VPN configuration that is distributed to VPN clients.

Configuration

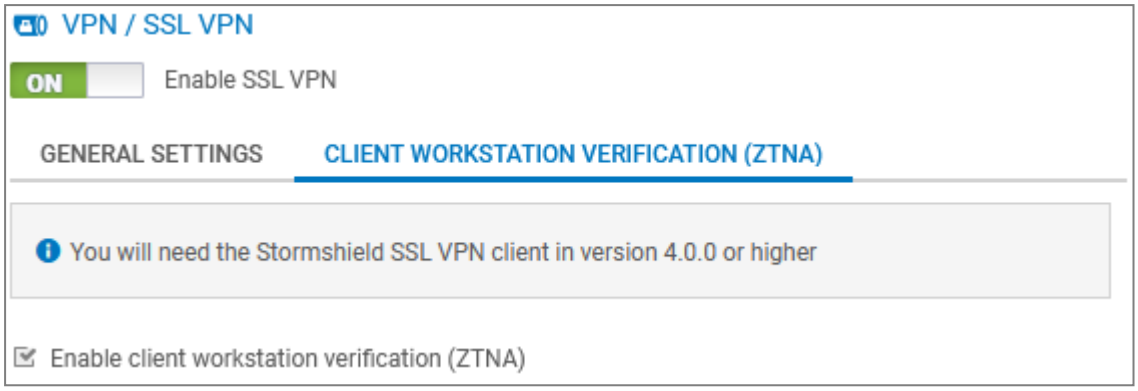
Field	Description
Export the configuration file	Click on this button to export the SSL VPN configuration in *.ovpn* format.

Configuring client workstation verification (ZTNA)

A policy can be set up to verify the compliance of client workstations (ZTNA) that set up SSL VPN tunnels with the SNS firewall. With this verification, workstations or users that do not comply with the criteria in the policy will not be able to set up SSL VPN tunnels with the SNS firewall.

This use case requires an SNS firewall in version 4.8 or higher, and the Stormshield SSL VPN client in version 4.0 or higher on each workstation in the corporate network.

Go to **Configuration > VPN** > **SSL VPN**. Continue according to the relevant SNS version.



On SNS firewalls in version 5

Settings for this version are configured in the **Client workstation verification (ZTNA)** and **Windows client workstation verification (ZTNA)** tabs.

Client workstation verification (ZTNA) tab

Stormshield SSL VPN client version

Select the checkbox to enable the settings section of the required versions.

Field	Description
Allow a version range (at least v4.0.0)	Select this option if you have a varied pool of Stormshield SSL VPN clients, and wish to allow several versions of the client to set up tunnels with the firewall. You must then enter the **Lowest version** of Stormshield SSL VPN clients that are allowed to set up tunnels. You can enter the **Highest version** or leave this field empty to allow all versions equal to or higher than the lowest specified version.
Allow only one version	Select this option to exclusively allow one Stormshield SSL VPN client version. You must then enter the exact version of Stormshield SSL VPN clients that are allowed to set up tunnels.

Allow tunnels to be set up for the following additional clients

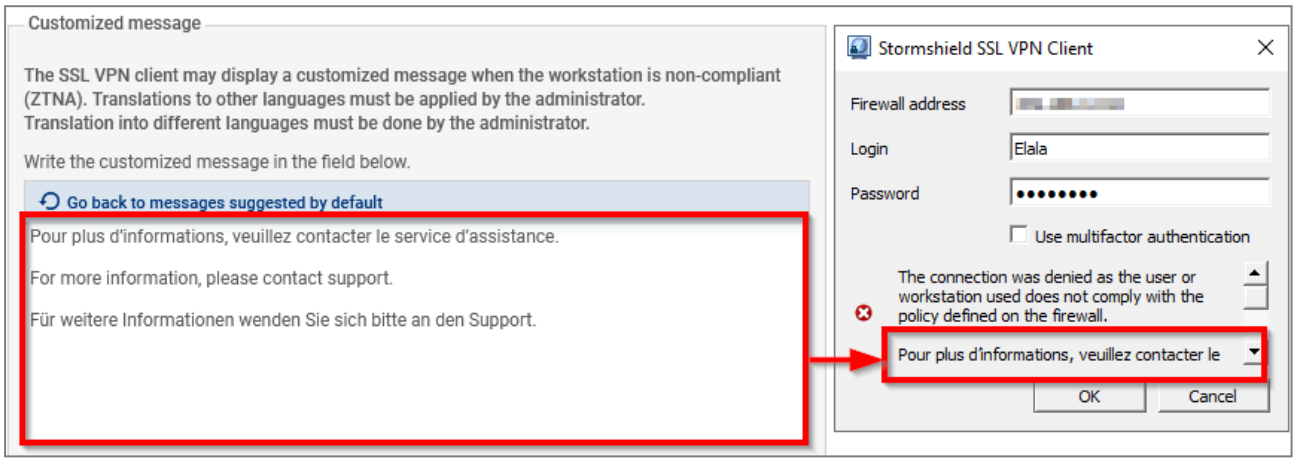
Field	Description
Stormshield SSL VPN clients for (Linux or macOS)	Select the option if you have client workstations with a Linux or Mac Stormshield SSL VPN client (available soon). By doing so, specific Windows criteria will not be applied to these workstations, and you will not need to adapt your criteria to them.
SSL VPN clients incompatible with ZTNA	Select the checkbox to enable permissive mode, which allows SSL VPN clients that are incompatible with the client workstation verification feature to set up tunnels with the SNS firewall. With this permissive mode, it is possible to: • Progressively update a pool of Stormshield SSL VPN clients to a compatible version, • Continue using third-party SSL VPN clients.

Customized message for incompatible workstations

If an SSL VPN tunnel fails to set up because the workstation or user is non-compliant, the Stormshield SSL VPN Client displays the default message "For more information, please contact support" in English, French and German.

In the text entry section, you can change the message, or delete it if you do not wish to display an additional message. Do note that as automatic translation mechanisms have not been set up: you will need to have the message translated with your own means.

You can reset the additional message that you have written by clicking on **Go back to messages suggested by default**.



Windows client workstation verification (ZTNA) tab

Windows client workstations are verified based on different criteria. Do note that if you select several criteria from those described below, the SSL VPN client has to meet all the defined criteria to be allowed to set up tunnels with the SNS firewall.

Field	Description
Client workstation antivirus enabled and up to date	The workstation must be equipped with an active antivirus program **with** the latest antivirus database updates. This information is based on the status of the antivirus recognized by the Windows Security center. Third-party antiviruses are therefore supported as long as the Windows Security center recognizes their status.
Active firewall on the client workstation	The Windows firewall must be running on the workstation, and the *domain network*, *private network* and *public network* profiles must be enabled. If a profile is disabled, the criterion will be considered non-compliant.
SES installed on the client workstation	In infrastructures that have deployed SES Evolution, the SES agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.
Prohibit users holding administration privileges on the client workstation	Users who hold administrator privileges on the workstation cannot set up tunnels with the SNS firewall.

Check the Windows 10/Windows 11 version (build number)

Select the checkbox to enable the settings section of the required Windows 10 and Windows 11 versions. Two tabs are available, depending on the Windows version in question.

Field	Description
Allow a version range (builds)	When this option is selected, you have to enter the **Lowest version** that the workstation must run (by default 10000 for Windows 10 and 20000 for Windows 11). You can enter the **Highest version** that the workstation must run, or leave this field empty to allow all versions equal to or higher than the lowest specified version.
Allow only one version	When this option is selected, you have to enter the exact Windows version of workstations that are allowed to set up tunnels.

Membership in a company domain

Field	Description
Ensure that the host is connected to a company domain	When this option is selected, you have to add to the grid the domains of the workstations that are allowed to set up tunnels. Do note that this criterion is not related to the configuration of directories on the firewall.
Ensure that the user belongs to a company domain	When this option is selected, you have to add to the grid the domains of users who are allowed to set up tunnels. With this criterion, the user's full name, including the domain, will be verified. As such, even if the workstation is connected to a domain, local users on the workstation will not be able to set up tunnels. Do note that this criterion is not related to the configuration of directories on the firewall.

On SNS firewalls in version 4.8

Settings are configured in the **Client workstation verification (ZTNA)** tab.

Field	Description
Enable client workstation verification (ZTNA)	Select the checkbox to enable verification of client workstation compliance. When it is enabled: • Compatible SSL VPN clients can set up SSL VPN tunnels with the firewall **only if all** the criteria defined in the policy have been met, • Incompatible SSL VPN clients cannot set up SSL VPN tunnels with the firewall, **unless** permissive mode has been enabled (see below).
Allow tunnels to be set up for Linux or Mac Stormshield SSL VPN clients	Select the option if you have client workstations with a Linux or Mac Stormshield SSL VPN client (available soon). By doing so, specific Windows criteria will not be applied to these workstations, and you will not need to adapt your criteria to them.
Allow tunnels to be set up for clients that are not compatible with ZTNA	Select the checkbox to enable permissive mode, which allows SSL VPN clients that are incompatible with the client workstation verification feature to set up SSL VPN tunnels with the SNS firewall. With this permissive mode, it is possible to: • Progressively update a pool of Stormshield SSL VPN clients to a compatible version, • Continue using third-party SSL VPN clients.

Client workstation verification (ZTNA) settings

Client workstations are verified based on different criteria. Do note that if you select several criteria from those described below, the SSL VPN client has to meet all the defined criteria to be

allowed to set up tunnels with the SNS firewall.

Field/Criterion	Description
Client workstation antivirus enabled and up to date	The workstation must be equipped with an active antivirus program **with** the latest antivirus database updates. This information is based on the status of the antivirus recognized by the Windows Security center. Third-party antiviruses are therefore supported as long as the Windows Security center recognizes their status.
Active firewall on the client workstation	The Windows firewall must be running on the workstation, and the *domain network*, *private network* and *public network* profiles must be enabled. If a profile is disabled, the criterion will be considered non-compliant.
SES installed on the client workstation	In infrastructures that have deployed SES Evolution, the SES agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.
Prohibit users holding administration privileges on the client workstation	Users who hold administrator privileges on the workstation cannot set up tunnels with the SNS firewall.
Check the Windows 10/Windows 11 versions (build number)	Select the checkbox to enable the settings section of the required Windows 10 and Windows 11 versions. Two tabs are available, depending on the Windows version in question. • **Allow a version range (builds)**: when this option is selected, you have to enter the **Lowest version** that the workstation must run (by default 10000 for Windows 10 and 20000 for Windows 11). You can enter the **Highest version** that the workstation must run, or leave this field empty to allow all versions equal to or higher than the lowest specified version. • **Allow only one version**: if this option is selected, you have to Fill the exact Windows version des workstation to set up tunnels.
Host connected to a domain tab	When you select **Connect the host to a company domain**, in the **List of Active Directory domains** grid, add the domains of the workstations that are allowed to set up tunnels. Do note that this criterion is not related to the configuration of directories on the firewall.
User connected to a domain tab	When you select **Connect the user to a company domain**, in the **List of Active Directory domains** grid, add the domains of the users that are allowed to set up tunnels. With this criterion, the user's full name, including the domain, will be verified. As such, even if the workstation is connected to a domain, local users on the workstation will not be able to set up SSL VPN tunnels with the firewall. Do note that this criterion is not related to the configuration of directories on the firewall.

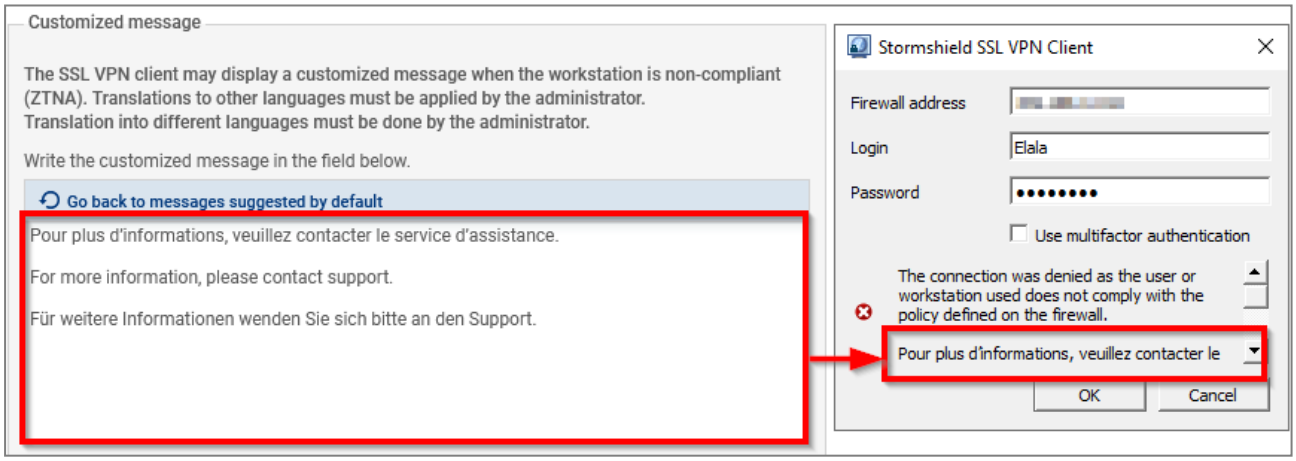
Field/Criterion	Description
Stormshield SSL VPN client version	Select **Check Stormshield SSL VPN client version** to enable the settings section of the required versions. • **Allow a version range (builds):** select this option if you have a varied pool of Stormshield SSL VPN clients, and wish to allow several versions of the client to set up tunnels with the firewall. You must then enter the **Lowest version** of Stormshield SSL VPN clients that are allowed to set up tunnels. The lowest version allowed is 4.0. 0. You can enter the **Highest version** or leave this field empty to allow all versions equal to or higher than the lowest specified version. • **Allow only one version**: select this option to exclusively allow one Stormshield SSL VPN client version. You must then enter the exact version of Stormshield SSL VPN clients that are allowed to set up tunnels.

Customized message

If an SSL VPN tunnel fails to set up because the workstation or user is non-compliant, the Stormshield SSL VPN Client displays the default message "For more information, please contact support" in English, French and German.

In the text entry section, you can change the message, or delete it if you do not wish to display an additional message. Do note that as automatic translation mechanisms have not been set up: you will need to have the message translated with your own means.

You can reset the additional message that you have written by clicking on **Go back to messages suggested by default**.



Creating filter and NAT rules

The SNS firewall's security policy has to be configured.

Go to **Configuration > Security policy > Filter - NAT**.

Configuring the filter policy

In the **Filtering** tab, set the rules that make it possible to grant or deny SSL VPN client access to the company's internal resources.

When ZTNA is used, you will need to set up granular filtering to restrict users' access to only what is necessary.

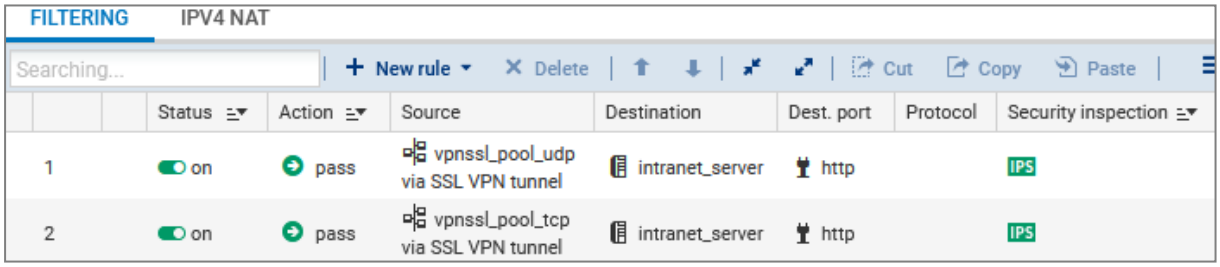
In the example below, we are adding two rules to allow all user connections from UDP and TCP SSL VPN clients to an HTTP intranet. For greater security, you can set specific rules for different user groups (**User** field).

Do note that rules will be scanned in the order of their appearance in the list. You can also use advanced filter functions (inspection profiles, application proxies, antivirus scans, etc.).

To add rules:

1. Click on **New rule** > **Single rule**, and double-click on the number of the rule to edit it; a new window will open.
2. In the **General** tab, **Status** field, select **On**.
3. In the **Action** tab, **Action** field, select *pass*.
4. In the **Source** tab:
   - In the **General** tab, **Source hosts** field, select the object that represents the IP addresses of UDP SSL VPN clients,
   - In the **Advanced properties** sub-tab, **Via** field, select *SSL VPN tunnel*.
5. In the **Destination** tab, **Destination hosts** field, select the object that represents the internal server or the intranet.
6. In the **Port - Protocol** tab, **Destination port** field, select *https*.
7. Click on **OK**.

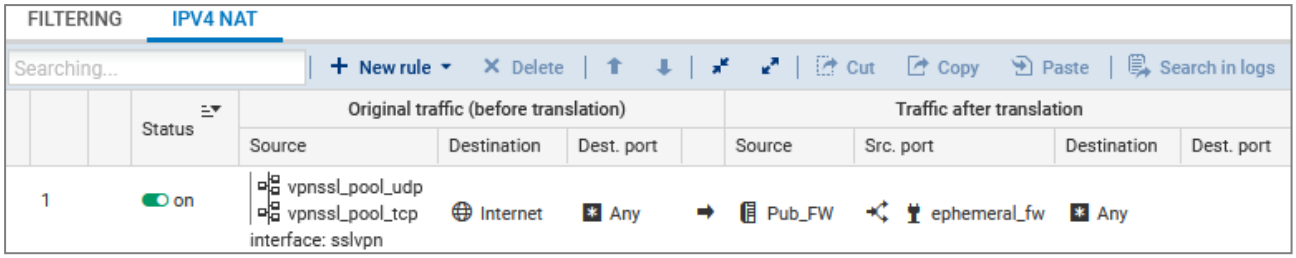
For the second rule, in the **Source** tab, **General** sub-tab, **Source hosts** field, select the object that represents the IP addresses of TCP SSL VPN clients.



Configuring the NAT policy

In the **NAT** or **IPv4 NAT** tab, if UDP and TCP SSL VPN clients must access the Internet, you will need to set up a network address translation (NAT) rule.

1. Click on **New rule** > **Source address sharing rule (masquerading)**, and double-click on the number of the rule to edit it; a new window will open.
2. In the **General** tab, **Status** field, select **On**.
3. In the **Original source** tab:
   - **Source hosts** field, select the objects that represent the IP addresses of UDP and TCP SSL VPN clients,
   - **Incoming interface** field, select *SSL VPN*.
4. In the **Original destination** tab, **Destination hosts** field, select *Internet*.
5. In the **Translated source** tab, **Translated source host** field, select the object that represents the public IP address.
6. In the **Translated source port** field, select the option **Choose random translated source port**.
7. Click on **OK**.


FILTERING
IPV4 NAT
Searching...
New rule
Delete
Cut
Copy
Paste
Search in logs
Status
Original traffic (before translation)
Traffic after translation
Source
Destination
Dest. port
Source
Src. port
Destination
Dest. port
1
on
vpnssl_pool_udp
vpnssl_pool_tcp
interface: sslvpn
Internet
Any
Pub_FW
ephemeral_fw
Any

Installing the Stormshield SSL VPN client

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

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

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:

- **The Stormshield SSL VPN website.**
  Log in to *https://vpn.stormshield.eu/* and follow the instructions given.
- **Your MyStormshield area.**
  Log in to your MyStormshield area and go to **Downloads > Downloads > Stormshield Network Security > SSL VPN**.
- **The captive portal of the SNS 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 client**.

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

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

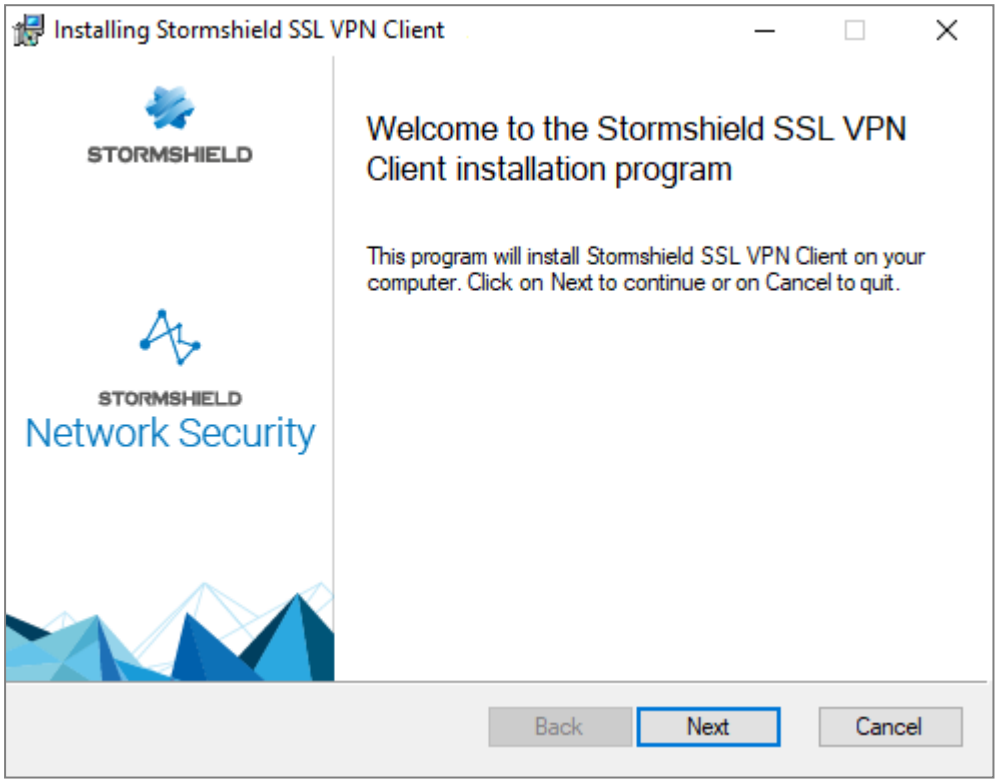
Compare the result obtained with the hash indicated on the Stormshield SSL VPN website or in your MyStormshield area under the **SHA256** column in the download table.

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

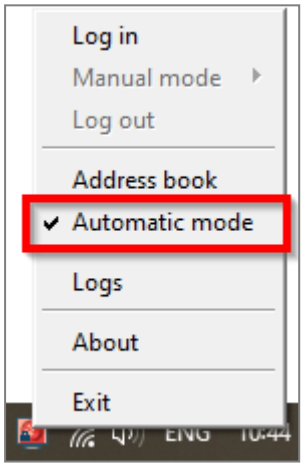
The Stormshield SSL VPN client has to be configured according to the desired connection mode. Refer to the section Connection mode compatibility table for the list of compatible features based on the connection mode used.

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.

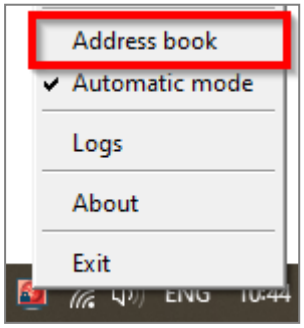


Configuring the address book (Automatic mode required)

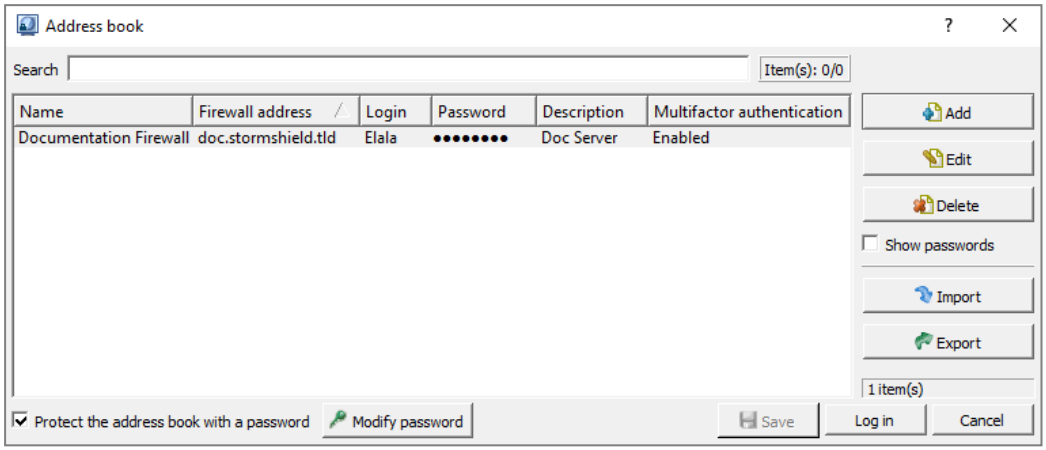
The Stormshield SSL VPN client has an address book that makes it possible to remember the login information to various firewalls: address to connect to the firewall (IPv4 address or FQDN), login, password and the use of multifactor authentication.

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**.

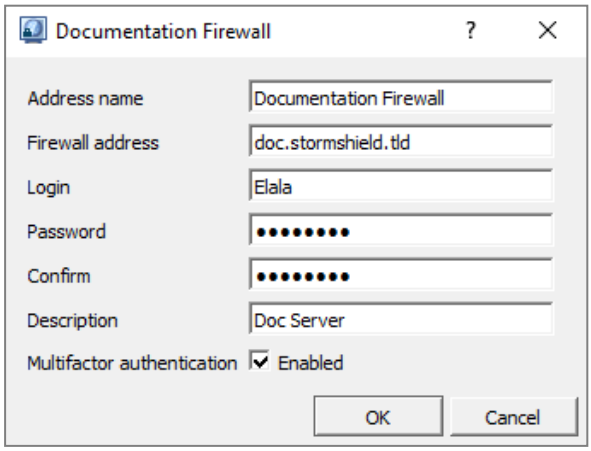


Adding or changing an address in the address book

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 SNS 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**.



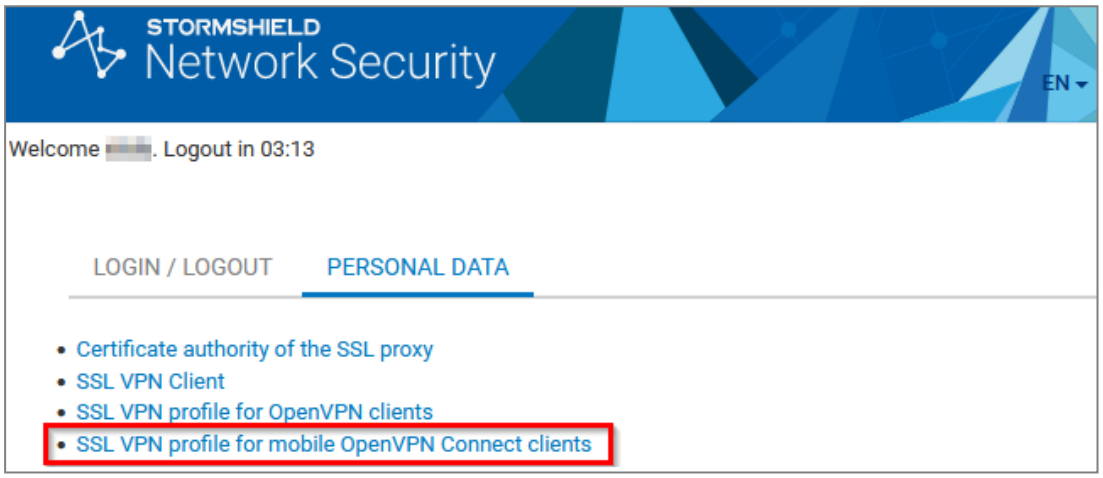
Configuring Manual mode

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:

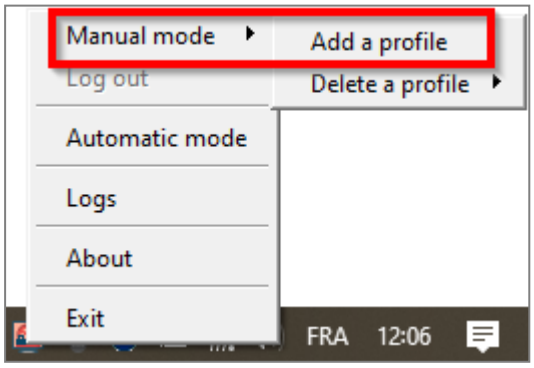
- **The captive portal of the SNS firewall that hosts the SSL VPN service.**
  Once you are connected to the corporate network, authenticate at *https://firewall_IPaddress/auth*, and in the **Personal data** tab, click on *SSL VPN profile for mobile OpenVPN Connect clients (single .ovpn file),*



- **The SNS 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.



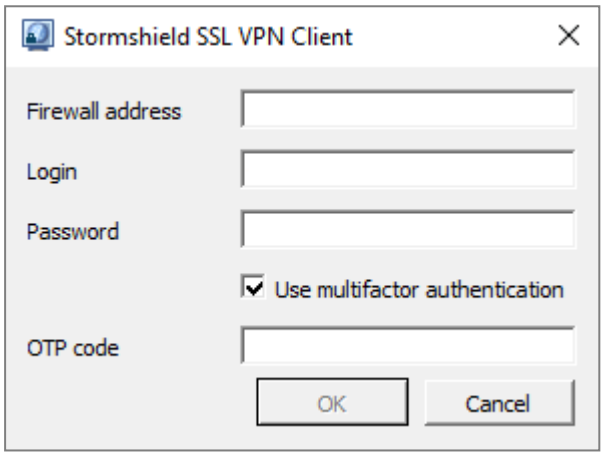
3. Select the *.ovpn* file.
4. Assign a name to the connection profile.
5. Click on **OK**.

Setting up a VPN tunnel with the Stormshield SSL VPN client

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

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 SNS 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.

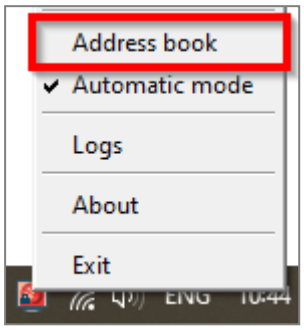
Authentication method	Password	Multifactor authentication	OTP
Standard	✅	❌	-
Password + OTP multifactor authentication	✅	✅	✅
OTP only multifactor authentication	❌	✅	✅
Push mode multifactor authentication	❌	✅	❌

5. Click on **OK**.

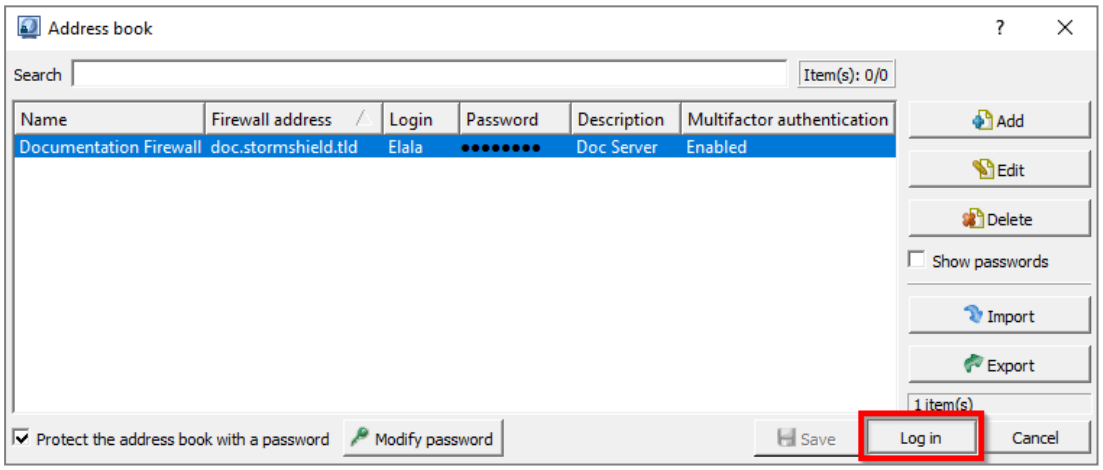
The Stormshield SSL VPN client will authenticate on the SNS firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

Setting up VPN tunnels by using the address book

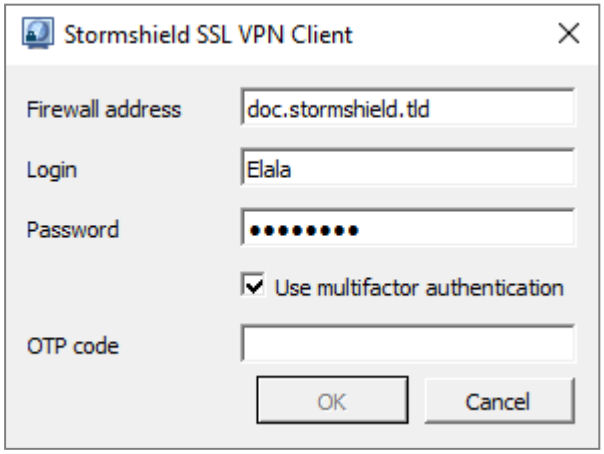
1. Right-click on the icon in the Windows system tray, then click on **Address book**. As a reminder, **Automatic mode** must be enabled.



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**.



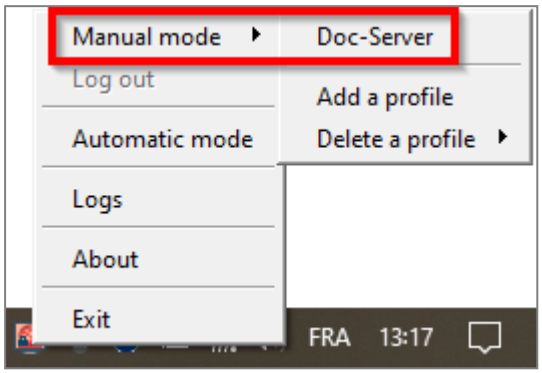
4. The connection window will appear.
   - In a standard authentication, the connection will automatically launch,
   - In a **Password + OTP** or **OTP only** multifactor authentication, enter an **OTP** (one-time password) and click on **OK**,
   - For **Push mode** multifactor authentication, click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



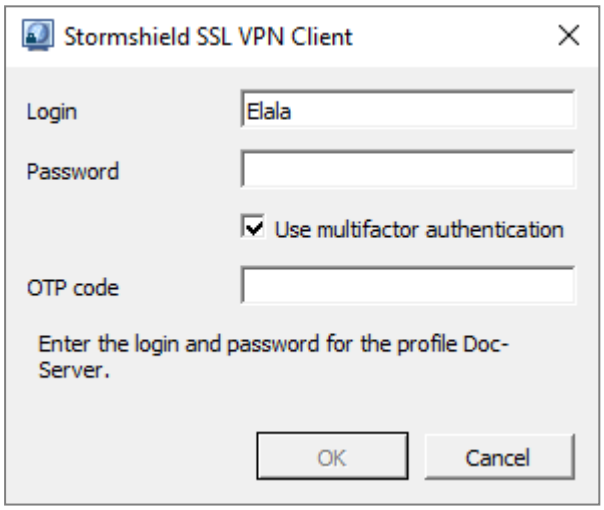
The Stormshield SSL VPN client will authenticate on the SNS firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

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 SNS firewall. If the authentication is unsuccessful, refer to the section When VPN tunnel fails to set up.

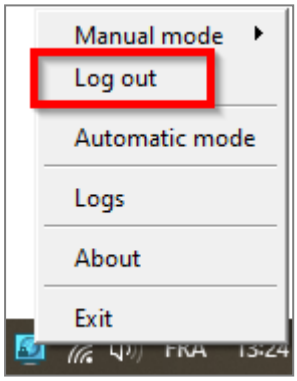
Showing the connection information of SSL VPN tunnels

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 SNS firewall, time at which the connection was set up with the SNS 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 SNS 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 Stormshield SSL VPN client's logs

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

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:

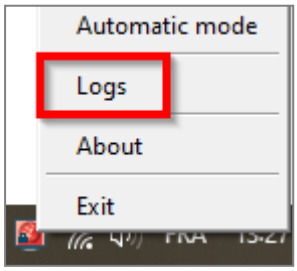
```
%programfiles%\Stormshield\Stormshield SSL VPN Client\install_logs
```

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

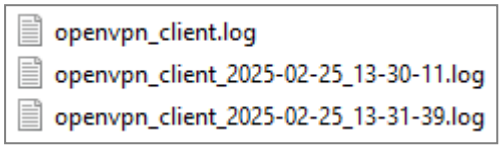
You can look up SSL VPN connection logs by right-clicking on the  icon in the Windows system tray, then on **Logs**, or in the Windows file explorer at this location:

```
%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 SNS firewall

In the SNS firewall's administration interface, you can track connected users or those connected to the SSL VPN. In the case of zero trust network access (ZTNA), this section also provides information on how to identify a client workstation's compliance status during a connection to the SSL VPN.

To ensure that images are easier to read, some columns in tables have been hidden. The default layout on your SNS firewall may differ slightly.

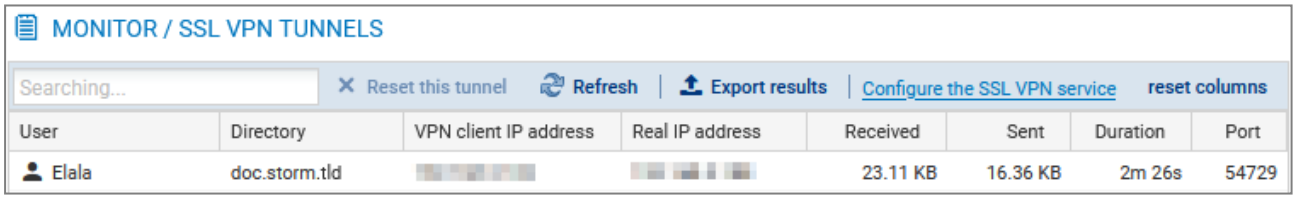
Information on access to private data

Some information can be accessed only if the user has been granted permissions to look up private data. If you hold this permission or a code to access private data, click on **Logs: restricted access**. For further information, refer to the technical note Complying with privacy regulations.

Displaying users currently connected to the SSL VPN

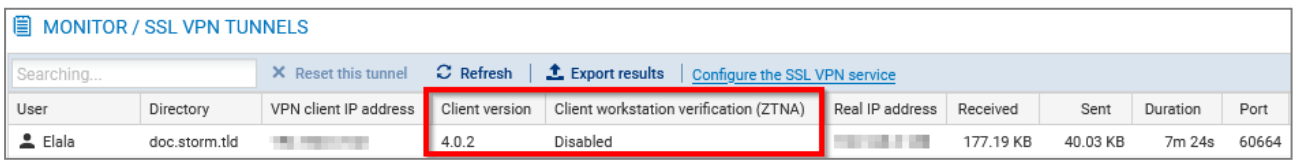
This view shows real-time information on the sessions of users connected to the SSL VPN.

Go to **Monitoring > Monitoring > SSL VPN tunnels.**



In SNS version 4.8 or higher:

- The "*Client version*" column shows the version of the Stormshield SSL VPN client used. The value indicated for a third-party or incompatible SN SSL VPN client is N/A.
- The "*Client workstation verification (ZTNA)*" column shows the client workstation's compliance status. There are several possible values:
  - **Disabled**: the client workstation verification policy has been not enabled,
  - **Not verified**: the SSL VPN client that was used to set up the tunnel is not compatible with the client workstation verification feature, but incompatible clients are explicitly allowed to set up tunnels (permissive mode),
  - **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy.

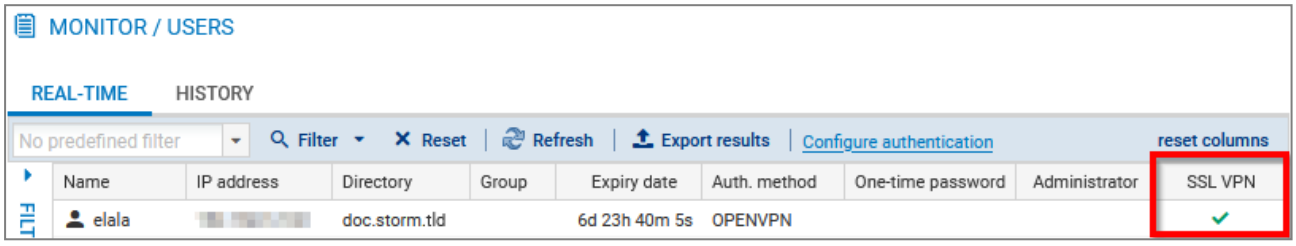


Displaying users currently authenticated on the SNS firewall

This view shows in real-time the users authenticated on the SNS firewall.

Go to **Monitoring > Monitoring > Users.**

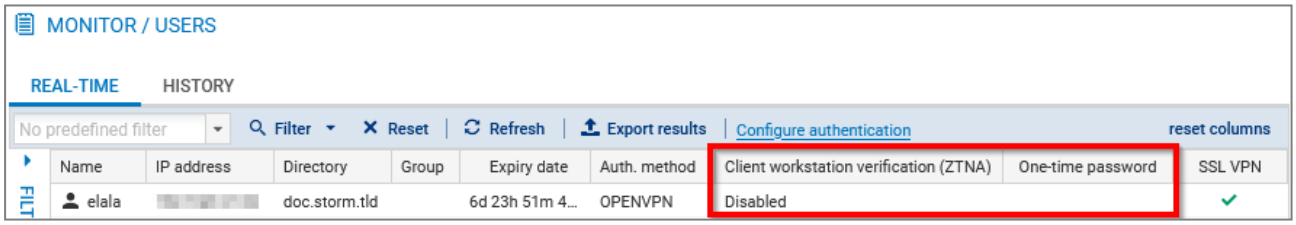
The *SSL VPN* column identifies users connected to the SSL VPN.



In SNS version 4.5 and higher, the *One-time password* column indicates whether a user has used a TOTP from the Stormshield TOTP solution to log in.

In SNS version 4.8 and higher, the *Client workstation verification (ZTNA)* column shows the client workstation's compliance status. There are several possible values:

- **Disabled**: the client workstation verification policy has been not enabled,
- **Not verified**: the SSL VPN client that was used to set up the tunnel is not compatible with the client workstation verification feature, but incompatible clients are explicitly allowed to set up tunnels (permissive mode),
- **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy.



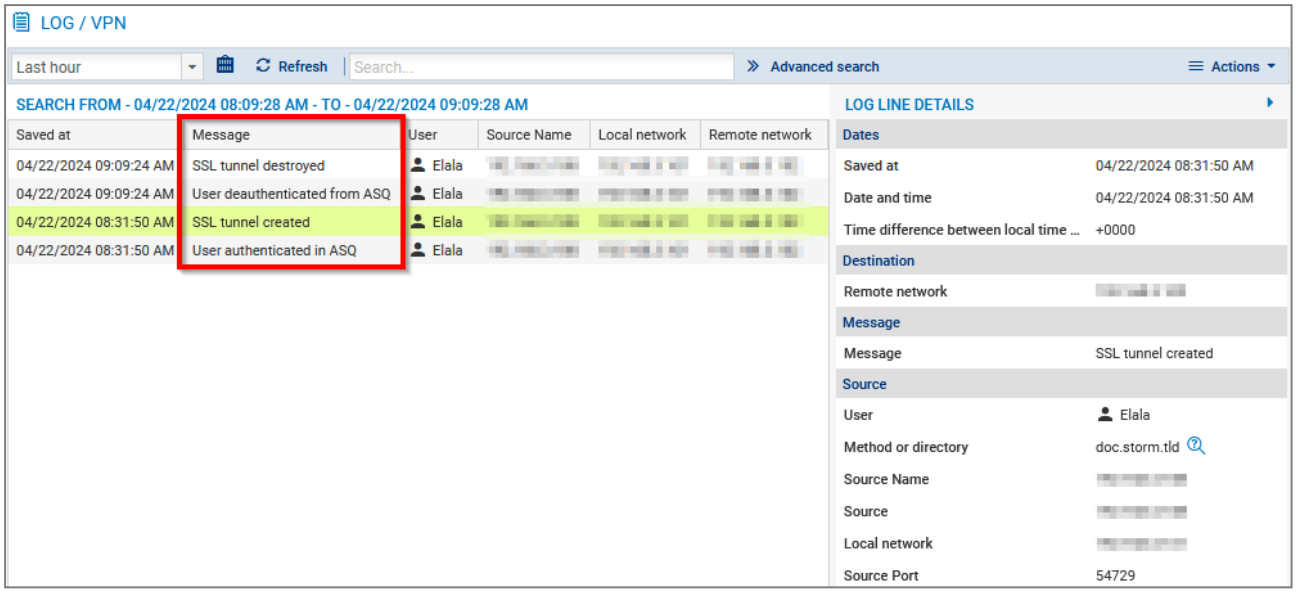
Displaying VPN logs (SSL and IPsec) and identifying the verification criteria that have not been met on a client workstation

This log shows events relating to the various types of tunnels (SSL or IPsec).

Go to **Monitoring > Logs - Audit logs > VPN.**

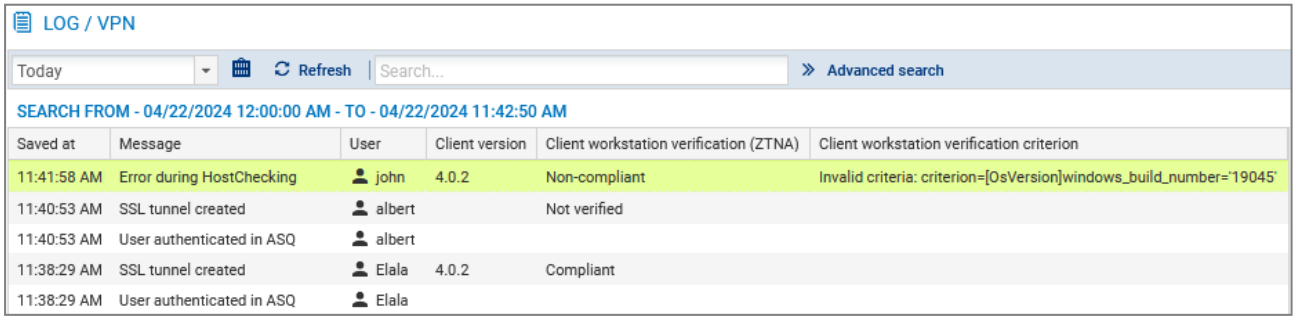
The *Message* and *User* columns show the user who generated the event and the event message (VPN tunnel connected or disconnected, user authentication in the firewall authentication engine, etc.).

You can view the details of an event in the panel on the right by clicking on it.



In SNS version 4.8 or higher:

- The *Message* column can contain messages relating to the verification of a client workstation's compliance (*HostChecking* feature):
  - "*Error during HostChecking*" with a "Non-compliant" client workstation: indicates that one or more criteria defined in the client workstation compliance verification policy are not compliant,
  - "*Error during authentication: HostChecking failed*" with a "*Not verified*" client: indicates that the SSL VPN client used is not compatible with the client workstation verification feature, and that the setup of tunnels for incompatible clients is not explicitly allowed (permissive mode),
- The "*Client workstation verification (ZTNA)*" column shows the client workstation's compliance status. There are several possible values:
  - **Disabled**: the client workstation verification policy has been not enabled,
  - **Not verified**: the workstation's compliance status has not been verified as the SSL VPN client used is not compatible with the client workstation verification feature. To find out whether the tunnel has been set up, refer to the *Message* column,
  - **Non-compliant**: the client workstation does not comply with the criteria defined in the client workstation verification policy,
  - **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy.
- The *Client workstation verification criterion* column shows non-compliant criteria when an SSL VPN tunnel fails to set up due to the non-compliance of the client workstation or user.



Troubleshooting

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

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 which criteria have not been met by referring to the section Displaying 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 by referring to the section Configuring the SSL VPN service.

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 SNS 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 SNS 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 SNS 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).

Appendix: installing, configuring and using OpenVPN Connect

This appendix explains the steps involved in installing, configuring and using OpenVPN Connect, and includes instructions on setting up SSL VPN tunnels and viewing the client's logs. This information can be supplemented by the information provided on the OpenVPN publisher website.

Installing OpenVPN Connect

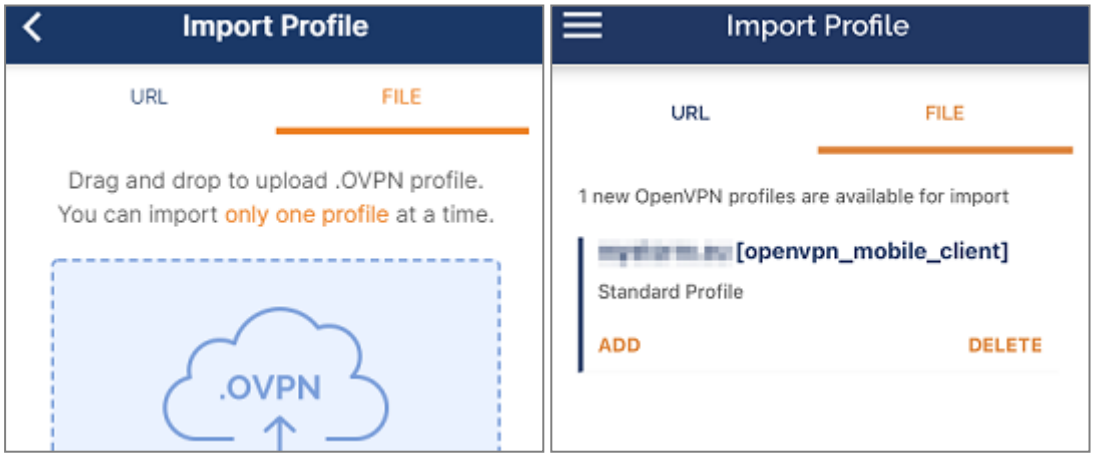
On a workstation: download the application from the OpenVPN website and install it.

On a mobile device: install the application from the *Google Play Store* or the *App Store*.

Configuring OpenVPN Connect

You will need to import the configuration components (CA, certificate, private key, etc.) that OpenVPN Connect must use, compiled in an *.ovpn* file.

1. Retrieve the *.ovpn* file. Follow the process described in the section Retrieving the SSL VPN configuration (.ovpn file).
2. Import the *.ovpn* file into OpenVPN Connect:
   - On a workstation: open the application and import the file via **Import Profile** > **File**,
   - On a mobile device: attempt to open the file, then from the choices given in the device, select OpenVPN Connect. The **Import Profile** > **File** window appears.



3. Next, follow the instructions given.

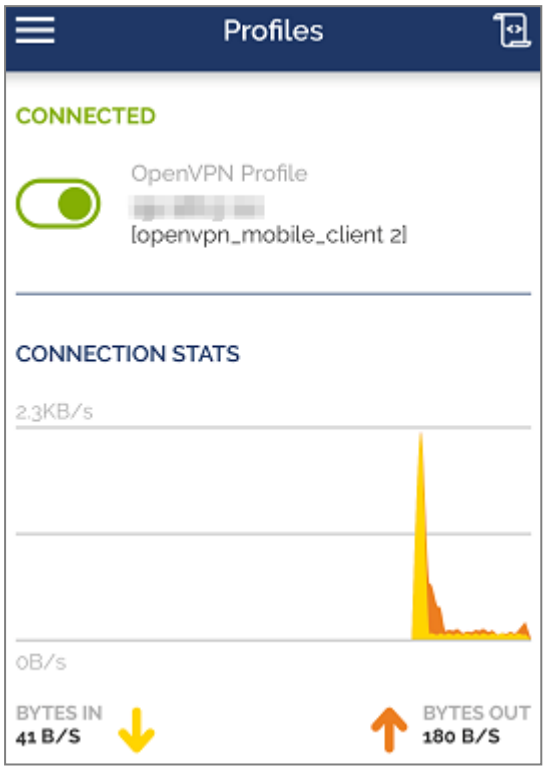
Perform this operation during the initial connection, and also when the SSL VPN configuration of the SNS firewall is modified, e.g., after a certificate is changed.

Setting up an SSL VPN tunnel with OpenVPN Connect

Connecting SSL VPN tunnels

1. Launch OpenVPN Connect.
2. For the desired profile, slide the connection cursor to the right or click on it.

3. If the user's password was not saved, enter it.
4. OpenVPN Connect authenticates on the SNS firewall. Once the connection is set up, information about the SSL VPN tunnel will appear.

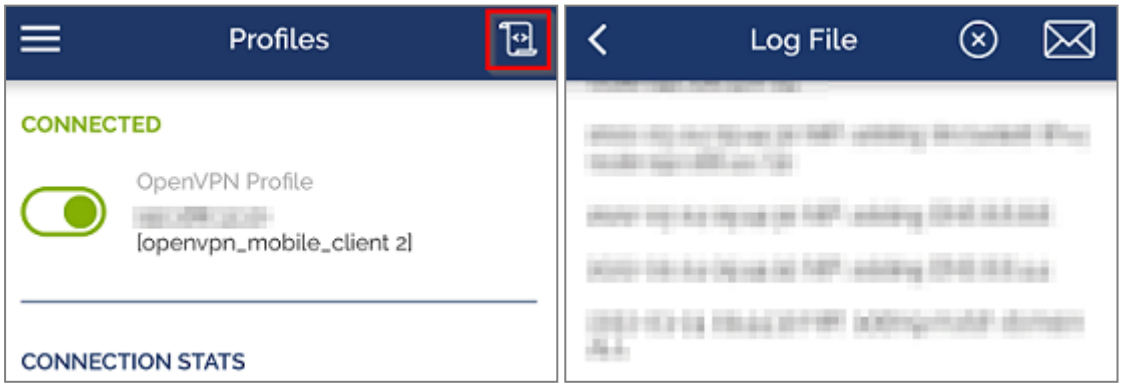


Disconnecting SSL VPN tunnels

Slide the connection cursor to the left or click on it.

Reading OpenVPN Connect logs

To read OpenVPN Connect logs, in the profile window, click on the icon in the shape of a newspaper on the right at the top.



STORMSHIELD

documentation@stormshield.eu