



STORMSHIELD



GUIDE

STORMSHIELD SSL VPN CLIENT

SSL VPN ADMINISTRATION GUIDE FOR STORMSHIELD SNS FIREWALLS AND SSL VPN CLIENTS

Document last updated: April 20, 2026

Reference: [sns-en-ssl_vpn_administration_guide](#)



Table of contents

- Change log 4
- Getting started 5
- Requirements 6
 - An appropriately scaled SNS firewall 6
 - A compatible SSL VPN client 6
 - Prior connection of the SNS firewall to a directory 6
- Configuring the authentication policy 7
- Configuring the captive portal 9
 - Configuring authentication profile and interface match 9
 - Checking whether the captive portal is enabled 9
 - Customizing the captive portal's certificate 10
- Configuring strong authentication: TOTP, SSL certificates or OIDC 11
 - Configuring one-time password (OTP) authentication 11
 - General information on OTP authentication 11
 - Configuring the selected OTP authentication solution 11
 - Setting up SSL VPN tunnels using OTP authentication 12
 - Configuring authentication with a user certificate 13
 - Requirements 13
 - Setting up an SSL VPN tunnel by authenticating with a user certificate 14
 - Known limitations 17
 - Using OIDC authentication 17
 - Introduction 17
 - Requirements 17
 - Setting up SSL VPN tunnels using OIDC authentication 17
- Configuring privileges to access the SSL VPN 21
 - Allowing all users to set up SSL VPN tunnels 21
 - Allowing some users and user groups to set up SSL VPN tunnels 21
- Configure the SSL VPN service 22
 - Enabling the SSL VPN service 22
 - Configuring the general settings of the SSL VPN service 22
 - Network settings section 23
 - DNS settings sent to client section 23
 - Advanced properties section 24
- Configuring client workstation verification (ZTNA) 27
 - General information on zero trust network access (ZTNA) 27
 - How client workstation verification (ZTNA) works 27
 - Requirements 27
 - Configuring client workstation verification 27
 - Client workstation verification (ZTNA) tab 28
 - Windows client workstation verification (ZTNA) tab 29
- Configuring the filter and NAT policy 31
 - Configuring the filter policy 31



- Configuring the NAT policy 31
- Tracking connected users 33
 - Information on access to private data 33
 - Displaying users currently connected to the SNS firewall through the SSL VPN 33
 - In SSL VPN tunnel monitoring 33
 - In user monitoring 34
 - Viewing logs on VPN tunnel events 34
- Troubleshooting 36
 - A user is unable to log in and the message "Client workstation compliance verification failed" appears 36
 - An internal resource cannot be accessed over the SSL VPN tunnel 36
 - A warning message indicates that LZ4 compression is obsolete 36
- Further reading 37



Change log

Date	Description
April 20, 2026	- Contents of the "Configuring strong authentication: TOTP, SSL certificates or OIDC" section enriched
December 29, 2025	- Contents of the "Configuring multifactor authentication (TOTP)" section enriched - New section "Using OIDC authentication" added - Contents of the section "Configuring client workstation verification (ZTNA)" enriched
October 22, 2025	- New document



Getting started

Welcome to the SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients.

In this guide, Stormshield Network Security is referred to as "SNS firewall".

SSL VPN allows remote users to securely access an organization's resources - internal or otherwise - via the SNS firewall. An SSL VPN client must be installed on the user's workstation and/or mobile device before they can set up SSL VPN tunnels with the SNS firewall.

Once the SSL VPN tunnel has been set up, communications between the user and the SNS firewall are encapsulated and protected through an encrypted TLS tunnel, referred to in this guide as an "SSL VPN tunnel".



This guide explains:

- The configuration to apply in the **Authentication, Access privileges** and **Filter - NAT** modules on the SNS firewall in order to deploy SSL VPN tunnels,
- How to enable and configure the SSL VPN service on the SNS firewall,
- How to configure the client workstation verification feature when zero trust network access (ZTNA) is used,
- How to track users who are connected to the SNS firewall through an SSL VPN.



Requirements

This section describes the requirements for deploying SSL VPN tunnels with an SNS firewall and compatible SSL VPN clients.

An appropriately scaled SNS firewall

The maximum number of SSL VPN tunnels allowed on SNS firewalls varies according to the model used. You must have a model that fits your requirements.

You can find this information on the [Stormshield website, under Product range \(SNS\)](#), by selecting your model.

A compatible SSL VPN client

Each user must have a compatible SSL VPN client on their workstation and/or mobile device to set up SSL VPN tunnels with the SNS firewall.

Compatible SSL VPN clients:

- The **Stormshield SSL VPN client**. For further information on installing the client, refer to the [Stormshield SSL VPN client v5 installation guide](#). To find out which versions are currently supported, refer to the [Network Security & Tools life cycle guide](#).
- The **OpenVPN Connect** client. This SSL VPN client does not have a mode in which the SNS firewall's SSL VPN configuration can be automatically retrieved, and is not compatible with the SNS firewall's client workstation verification feature.

i NOTE

To test the configuration before deploying SSL VPN across users, install a compatible SSL VPN client on some of your devices now.

Prior connection of the SNS firewall to a directory

The SNS firewall must be connected to a directory. Check this connection in the SNS firewall's web administration interface in **Configuration > Users > Authentication, Available methods** tab. An LDAP line must appear in the grid.

For more information, refer to the section **Directory configuration** in the [v4 user guide](#) or [v5 user guide](#), depending on the SNS version used.



Configuring the authentication policy

This section explains how to configure the authentication policy in order to allow users or user groups to authenticate on the SNS firewall and set up SSL VPN tunnels.

1. Go to **Configuration > Users > Authentication, Authentication policy** tab.
2. Identify the **Method to use if no rules match**.

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL CAPTIVE PORTAL PROFILES

Search by user... + New rule X Delete ↑ Up ↓ Down Cut Copy Paste

	Status	Action	Source	Methods (assess by order)	One-time password	Comment
1	Enabled	Allow	finance@storm.doc out	1 LDAP	<input checked="" type="checkbox"/>	
2	Enabled	Allow	finance@storm.doc sslvpn	1 LDAP	<input checked="" type="checkbox"/>	
3	Enabled	Allow	hr@storm.doc out	1 LDAP	<input checked="" type="checkbox"/>	
4	Enabled	Allow	hr@storm.doc sslvpn	1 LDAP	<input checked="" type="checkbox"/>	

Default action

Default action to apply: Allow

Default method

Method to use if no rules match: LDAP

Proceed accordingly.

Case 1: The "LDAP" method is selected and only this method is used on the SNS firewall

The current configuration of the authentication policy will suffice. Continue to [Configuring the captive portal](#).

Case 2: In all other cases

In all other cases (restricted only to authentication on the SNS firewall, use of multifactor authentication, etc.), you need to add at least two rules to the authentication policy to allow users to authenticate with the Stormshield SSL VPN client and set up SSL VPN tunnels.

For stronger security, we recommend creating these two rules for each user group that is setting up SSL VPN tunnels with the SNS firewall. However, you can also choose to create only two rules for all users, with no particular distinction.

The first rule allows users and Stormshield SSL VPN clients that are configured in Stormshield mode to connect to the SNS firewall's captive portal. Stormshield SSL VPN clients can then automatically retrieve the SSL VPN configuration, and send information that enables the SNS firewall to verify the client workstation's compliance [ZTNA].



1. Click on **New rule > Standard rule**.
2. In the **User** tab, select a user or user group from an SNS firewall directory (such as *finance@domain.tld*). If you wish to do so, select all the users in a directory by setting *Any user@domain.tld*. On SNS in version 5, you can also select all users from all SNS firewall directories by selected **All users (any)**.
3. In the **Source** tab, add the source interface of SSL VPN connections (e.g. *out*).
4. In the **Authentication methods** tab:
 - a. Delete the *Default method* row.
 - b. Enable the method allowing users and Stormshield SSL VPN clients to connect to the SNS firewall's captive portal, e.g., *LDAP* or *RADIUS*.
 - c. If a multifactor authentication method is used (authentication with a one-time password), set the **One-time password** selector to **ON**
5. Click on **OK**.

The **second rule** allows users to set up SSL VPN tunnels from their SSL VPN clients to the SNS firewall.

1. Click on **New rule > Standard rule**.
2. In the **User** tab, select the same user or user group as the one in the first rule.
3. In the **Source** tab, add the *SSL VPN* interface.
4. In the **Authentication methods** tab:
 - a. Delete the *Default method* row.
 - b. Enable the method allowing users to set up SSL VPN tunnels from their SSL VPN clients to the SNS firewall, e.g., *LDAP* or *RADIUS*.
 - c. If a multifactor authentication method is used (authentication with a one-time password), set the **One-time password** selector to **ON**
5. Click on **OK**.

i NOTE
During an authentication on the SNS firewall, rules in the authentication policy are scanned in order of their appearance in the list.

1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Allow	finance @storm.doc out	1	LDAP	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Allow	finance @storm.doc sslvpn	1	LDAP	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Allow	hr @storm.doc out	1	LDAP	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Allow	hr @storm.doc sslvpn	1	LDAP	<input checked="" type="checkbox"/>



Configuring the captive portal

This section explains how to configure the captive portal to allow Stormshield SSL VPN clients, and users or user groups, to set up SSL VPN tunnels.

Configuring authentication profile and interface match

1. Go to **Configuration > Users > Authentication, Captive portal** tab.
2. In the **Authentication profile and interface match** grid, click on **Add**.
3. In the **Interface** column, select the source interface of SSL VPN connections (e.g., *out*). If you are using a PPPoE or VLAN interface, select it instead of the physical parent interface.
4. In the **Default method or directory** column, if the directory entered matches the directory of the users who are setting up SSL VPN tunnels with the SNS firewall, the value of the **Profile** column does not need to be changed. This configuration allows users to simply enter their user name in their SSL VPN client to set up the SSL VPN tunnel.

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY **CAPTIVE PORTAL** CAPTIVE PORTAL PROFILES

Captive portal

AUTHENTICATION PROFILE AND INTERFACE MATCH

+ Add X Delete

Interface	Profile	Default method or directory
out	Internal	Directory (storm.doc)

Otherwise, users will need to enter their user name with the directory authentication domain (*identifiant@domain.tld*) in their SSL VPN client to set up the SSL VPN tunnel. If you want users to simply enter their user name, adapt the configuration:

- a. In the **Profile** column, select another profile (e.g., *default05*).
- b. In the **Captive portal profiles** tab, select this other profile and choose the right directory in the **Default method or directory** field.

USERS / AUTHENTICATION

AVAILABLE METHODS AUTHENTICATION POLICY CAPTIVE PORTAL **CAPTIVE PORTAL PROFILES**

default05 | Rename | i

Authentication

Default method or directory: Directory (storm.doc) | i

Enable sponsorship

Checking whether the captive portal is enabled

1. Go to **Configuration > Users > Authentication, Captive portal profiles** tab.
2. Select the profile used for the SSL VPN connections.



3. In the **Advanced properties** section, ensure that the **Enable the captive portal** checkbox has been selected.

Customizing the captive portal's certificate

You can customize the certificate presented by the SNS firewall when accessing the captive portal. If this certificate is not customized, the SNS firewall will present a default certificate:

- On SNS in version 4, this will be a certificate corresponding to the SNS firewall serial number,
- On SNS in version 5, this will be a self-generated certificate for this access.

To customize the captive portal's certificate:

1. Go to **Configuration > Users > Authentication, Captive portal** tab.
2. In the **Certificate (private key)** field, select the new certificate. If necessary, you can add a new certificate (server identity) in **Configuration > Objects > Certificates and PKI**.

The screenshot shows the configuration page for the captive portal. The breadcrumb is 'USERS / AUTHENTICATION'. There are four tabs: 'AVAILABLE METHODS', 'AUTHENTICATION POLICY', 'CAPTIVE PORTAL' (which is active), and 'CAPTIVE PORTAL PROFILES'. Below the tabs, there is a section for 'SSL server' configuration. The 'Certificate (private key)' field is a dropdown menu with the text 'Select a certificate' and a close button (x).

If any of the following criteria applies to the selected certificate:

- The certificate was not signed by a trusted certification authority,
- The certification authority has not been deployed on users' workstations,
- The certificate's **CN** does not match the SNS firewall address that is used for connections to the SSL VPN. This is the case, for example, with the default certificate presented by the SNS firewall.

The certificate cannot be automatically validated by the Stormshield SSL VPN client or web browser, and a window indicating a probable security risk will appear. Each user must then ensure that the connection is secure by checking the certificate information, and then indicate that they trust the certificate presented by the SNS firewall to set up the SSL VPN tunnel. Although this message does not prevent users from proceeding, we recommend explaining it to your users.



Configuring strong authentication: TOTP, SSL certificates or OIDC

This section explains how to configure strong authentication, using authentication methods such as TOTP, SSL certificates or OIDC on the SNS firewall.

If you do not wish to use a strong authentication method, proceed to the next section.

Configuring one-time password (OTP) authentication

This section explains how to configure a one-time password authentication method (OTP or TOTP) to set up SSL VPN tunnels with the SNS firewall.

General information on OTP authentication

OTP authentication strengthens the authentication of users who set up SSL VPN tunnels with a second authentication factor.

The second factor is a one-time password, known as an OTP or TOTP, which the user must enter in addition to their password to set up the SSL VPN tunnel. Stormshield has its own OTP authentication solution.

A third-party solution can also be used with a RADIUS server. For example, the Trustbuilder solution (formerly inWebo) is compatible and allows users to generate OTPs or approve setting up connections (push notifications) in an application that is installed on a trusted device.

Configuring the selected OTP authentication solution

Stormshield TOTP solution

Refer to the technical note [Configuring and using the Stormshield TOTP solution](#), which explains how to configure and manage the TOTP solution on the SNS firewall, and presents the enrollment procedure for TOTP solution users.

Third-party OTP solution with a RADIUS server

The chosen third-party OTP authentication solution has to be configured and connected to your RADIUS server. If you need help with this configuration, refer to the documentation for your chosen solution.

On the SNS firewall:

- Enable and configure the RADIUS method to connect your SNS firewall to your RADIUS server. To do so, go to **Configuration > Users > Authentication, Available methods** tab. For more information, refer to the section **Authentication > Available methods** tab > **RADIUS** in the [v4 user guide](#) or [v5 user guide](#), depending on the SNS version used.
- Increase the maximum response time for RADIUS requests if the selected solution requires users to approve the setup of their SSL VPN tunnels in an application. The default maximum response time is 3 seconds. To increase it to 30 seconds, for example, use the following CLI/serverd commands:

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



Setting up SSL VPN tunnels using OTP authentication

In the Saved connections menu

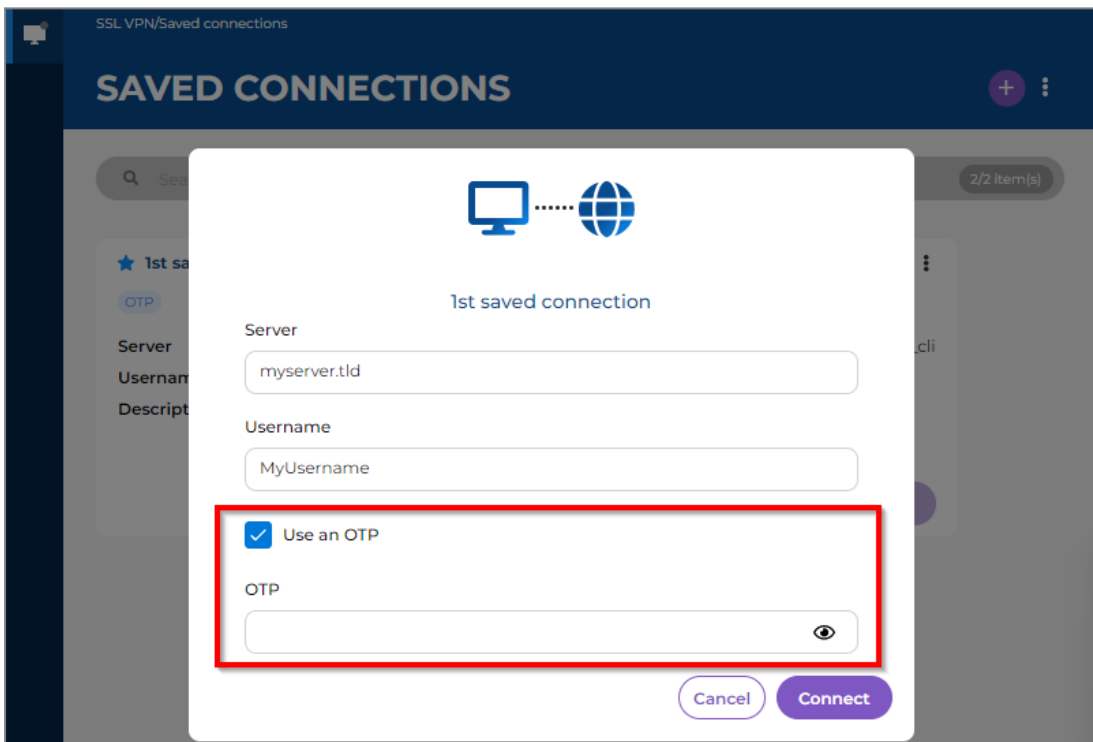
The **Use an OTP** checkbox must be selected in advance in the details of the saved connection.

1. Click on **Connect** in the section of the connection in question.
2. Fill in the **Password** and **OTP** fields, depending on whether your authentication solution requires a password and/or OTP.

The following combinations are possible:

Password field	OTP field
✔ Value entered (*)	✔ Value entered
✘ Empty field	✔ Value entered
✘ Empty field	✘ Empty field

(*) The **Password** field does not appear if it was saved in the details about the saved connection.



3. Click on **Connect**.
4. If your authentication solution requires approval of the SSL VPN tunnel setup in an application (with the **Password** and **OTP** fields left empty), a push notification will be sent to your trusted device. Open your application and approve the setup of the SSL VPN tunnel.
5. Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

In the Direct connection menu

1. Select the connection mode. If necessary, refer to the section [Description of connection modes and available fields](#) in the *Stormshield SSL VPN client user and configuration guide*.
2. Select the **Use an OTP** checkbox.



- Fill in the **Password** and **OTP** fields, depending on whether your authentication solution requires a password and/or OTP.

The following combinations are possible:

Password field	OTP field
✔ Value entered	✔ Value entered
✘ Empty field	✔ Value entered
✘ Empty field	✘ Empty field

The screenshot shows the 'DIRECT CONNECTION' configuration page. Under the 'Authentication' section, the 'Password' field is empty, the 'Use an OTP' checkbox is checked, and the 'OTP' field is empty. A red box highlights these three elements. The 'Connect' button is visible at the bottom right.

- Click on **Connect**.
- If your authentication solution requires approval of the SSL VPN tunnel setup in an application (with the **Password** and **OTP** fields left empty), a push notification will be sent to your trusted device. Open your application and approve the setup of the SSL VPN tunnel.
- Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

Configuring authentication with a user certificate

This section explains how to configure authentication with a user certificate to set up SSL VPN tunnels with the SNS firewall.

Requirements

- An SNS firewall in version 5.0.1 or higher.
- Stormshield SSL VPN clients in version 5.1.1 or higher. Do note that third-party SSL VPN clients, such as OpenVPN Connect, are not compatible.



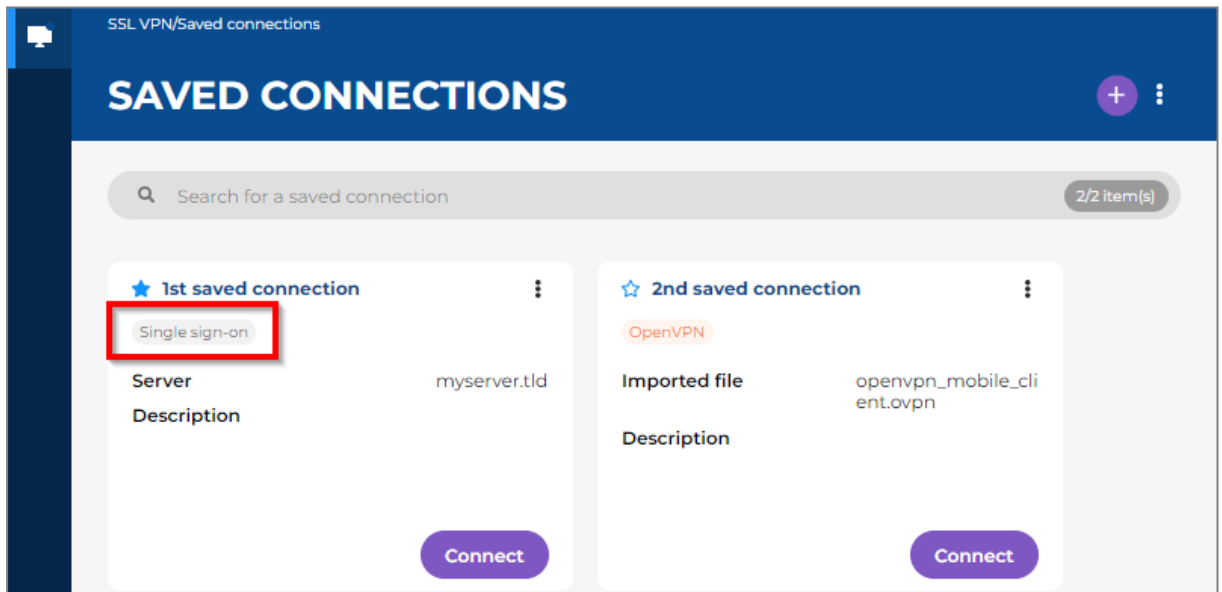
- SSL VPN service configured in the **SSL VPN** module on the SNS firewall. This configuration is described in the following sections.
- **SSL certificate** method configured in **Authentication > Available Methods** on the SNS firewall. For more information, refer to the section **Authentication > Available methods** tab > **Certificate (SSL)** in the [v4 user guide](#) or [v5 user guide](#), depending on the SNS version used.
- Rules created, allowing users to authenticate through the **SSL Certificate** method in the **Authentication > Authentication Policy** module on the SNS firewall. Adapt the information in the section [Configuring the authentication policy](#) in this case.
- User certificates installed on the workstations of the users in question. You can download the user identity of the certificate in P12 format in the **Objects > Certificates and PKI** module on the SNS firewall.

Setting up an SSL VPN tunnel by authenticating with a user certificate

In the Saved connections menu

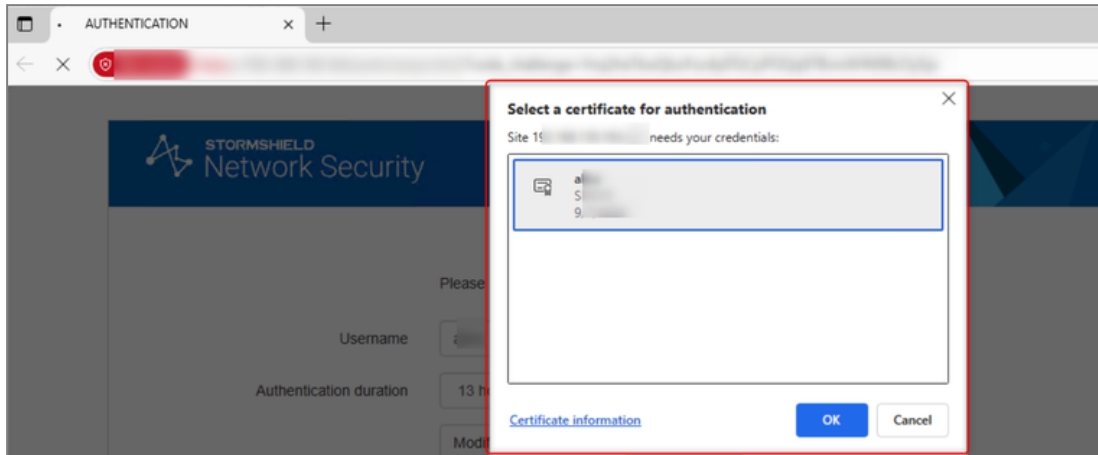
You must first select **Stormshield mode** and the checkbox **Connect with single sign-on** in the details of the saved connection.

In a saved connection, the label "*Single sign-on*" is an indication that the checkbox **Connect with single sign-on** was selected.



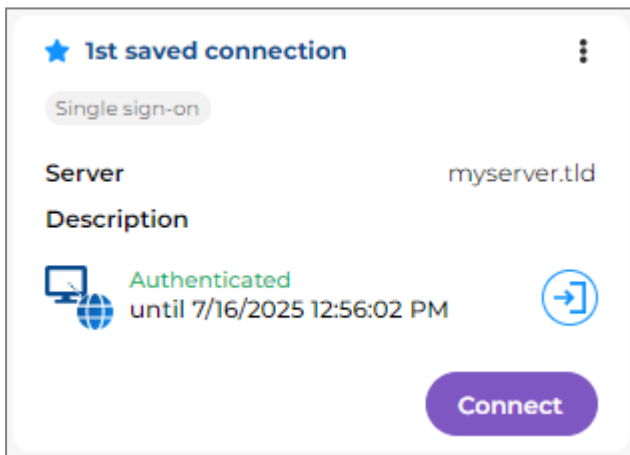


1. Click on **Connect** in the section of the saved connection in question.
2. On the authentication portal that automatically opens in your web browser, follow the steps in the authentication process.



3. Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

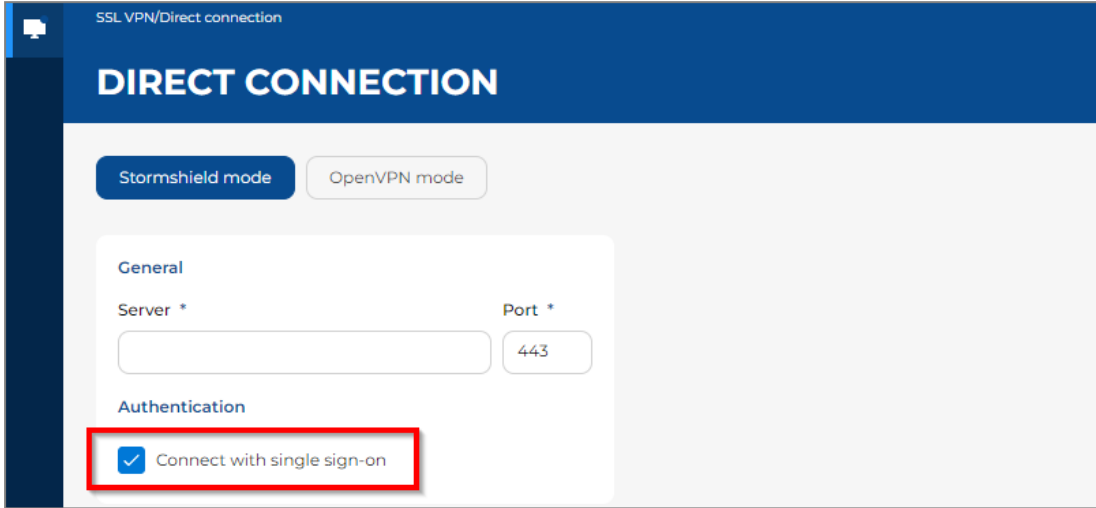
Once the SSL VPN tunnel has been set up, the expiry date of your authentication session appears. As long as the expiry date remains in the future, you can set up the SSL VPN tunnel without having to authenticate again.



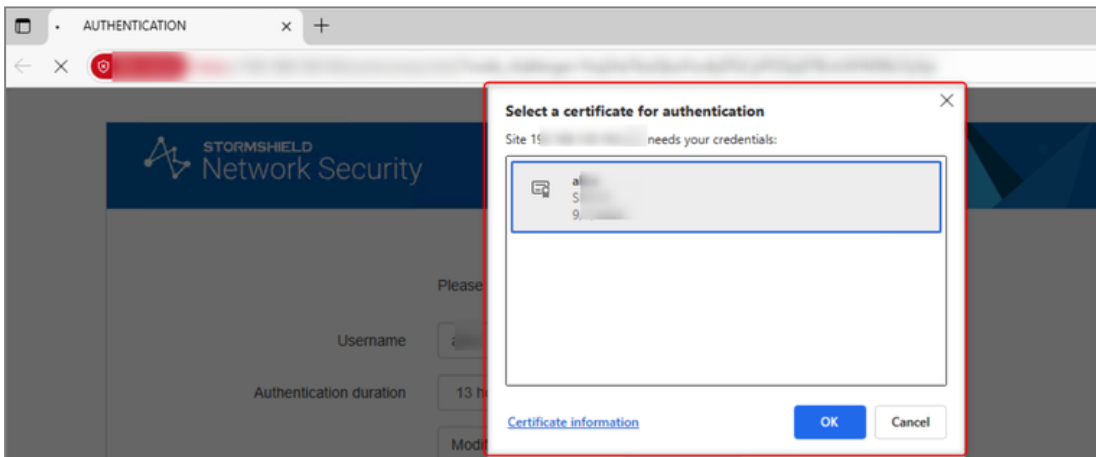


In the Direct connection menu

1. Select **Stormshield mode**.
2. Select the checkbox **Connect with single sign-on**.

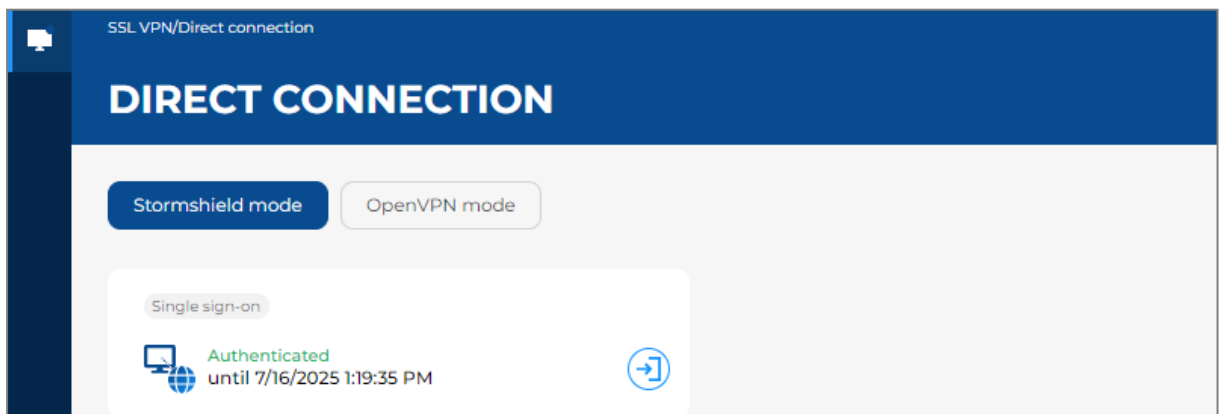


3. Click on **Connect**.
4. On the authentication portal that automatically opens in your web browser, follow the steps in the authentication process.



5. Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

Once the SSL VPN tunnel has been set up, the expiry date of your authentication session appears. As long as the expiry date remains in the future, you can set up the SSL VPN tunnel without having to authenticate again.





Known limitations

TLS 1.3 incompatibility

With SNS version 5.0.2, authentication with user certificates is not supported over TLS 1.3. This limitation will be fixed in a future version of SNS.

Workarounds are available, depending on your users' web browser:

- On Firefox, enable the following setting in the Firefox configuration:

```
security.tls.enable_post_handshake_auth
```

- For other browsers such as Chrome or Edge, you need to force the SNS firewall's captive portal to use TLS 1.2. To do so, run the following SSH commands on the SNS firewall:

```
setconf /usr/Firewall/ConfigFiles/auth Config TLSv13 0  
ensl
```

Entering the user name during authentication

Users currently have to enter their user names on the captive portal before they can select the certificate to be used for authentication. This limitation will be improved in a future version of SNS.

Using OIDC authentication

This section explains how to configure OIDC authentication, which is based on the OpenID Connect (OIDC) authorization protocol, to set up SSL VPN tunnels with the SNS firewall.

Introduction

With OIDC authentication, you can connect your SNS firewall to an identity provider (IdP), such as Microsoft Entra ID. This will enable your users to authenticate using their accounts with your IdP, which will notably allow them to set up SSL VPN tunnels.

Requirements

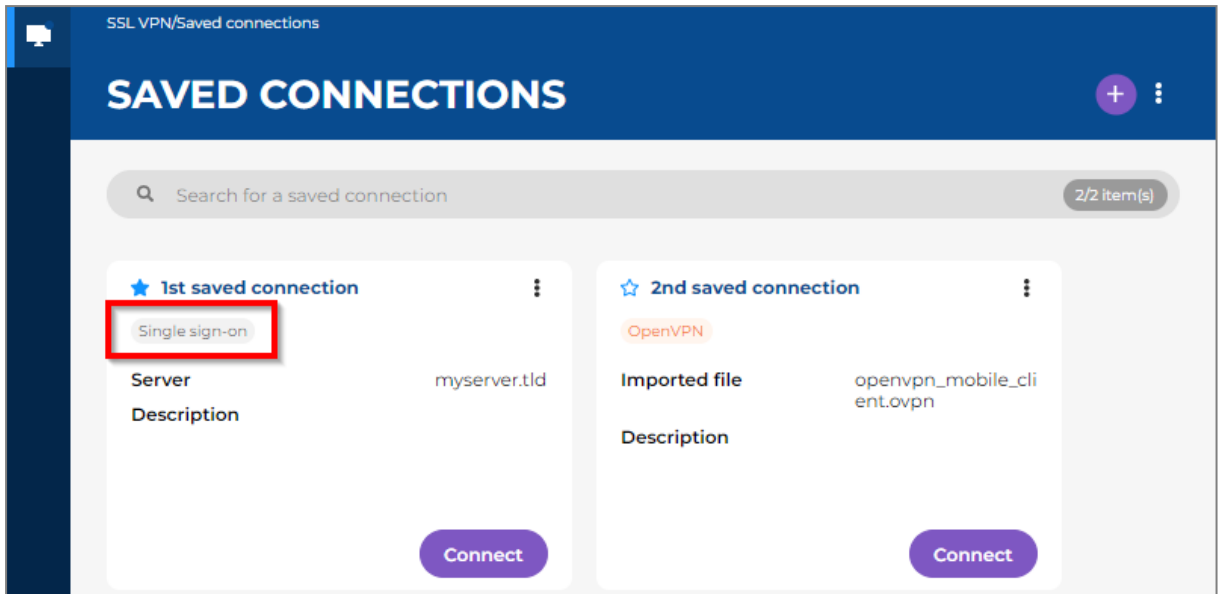
- An SNS firewall in version 5.0.1 or higher.
- Stormshield SSL VPN clients in version 5.1.1 or higher. Do note that third-party SSL VPN clients, such as OpenVPN Connect, are not compatible.
- **OIDC** method configured in **Authentication > Available methods** on the SNS firewall, and your IdP configured. For more information, refer to the technical note [Configuring OIDC/Microsoft Entra ID authentication](#).

Setting up SSL VPN tunnels using OIDC authentication

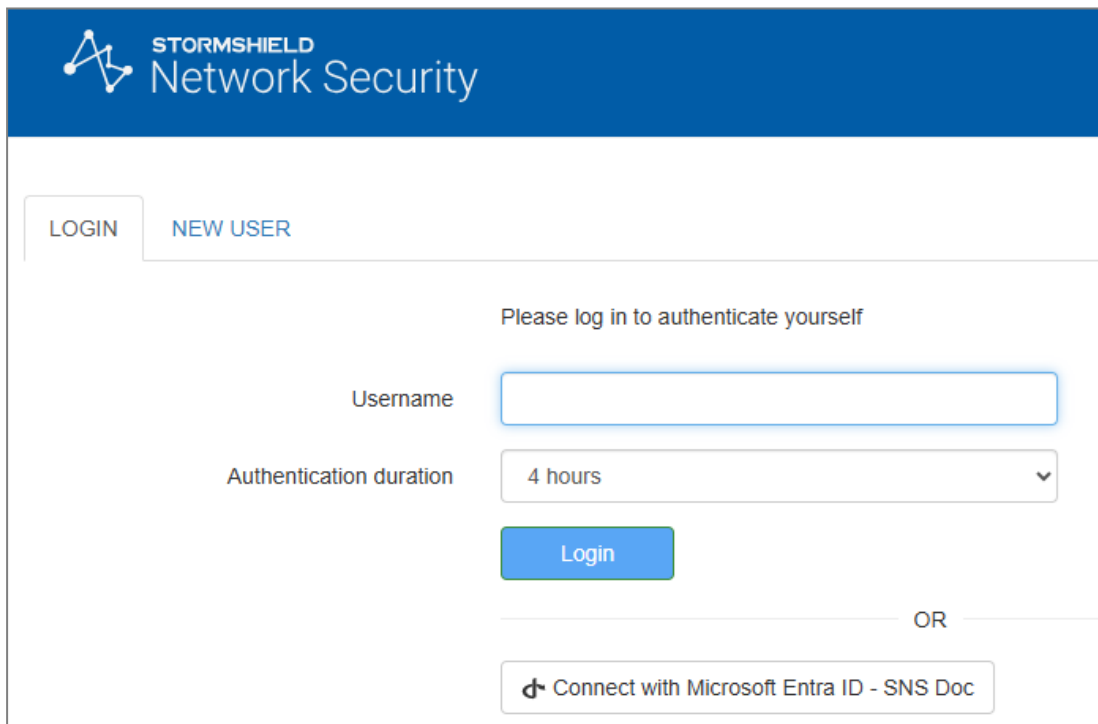
In the Saved connections menu

You must first select **Stormshield mode** and the checkbox **Connect with single sign-on** in the details of the saved connection.

In a saved connection, the label "*Single sign-on*" is an indication that the checkbox **Connect with single sign-on** was selected.

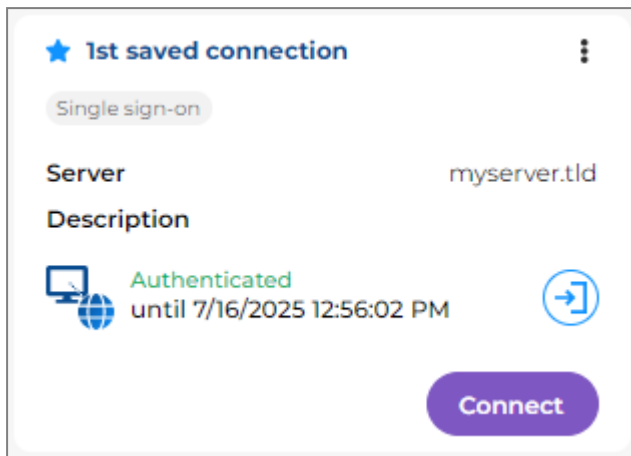


1. Click on **Connect** in the section of the connection in question.
A page will open automatically in your web browser. Depending on the configuration of your SNS firewall, this page may be:
 - Your IdP's authentication portal, or
 - The SNS firewall's captive portal. If this is the case, click on the button corresponding to your IdP to be redirected to its authentication portal.



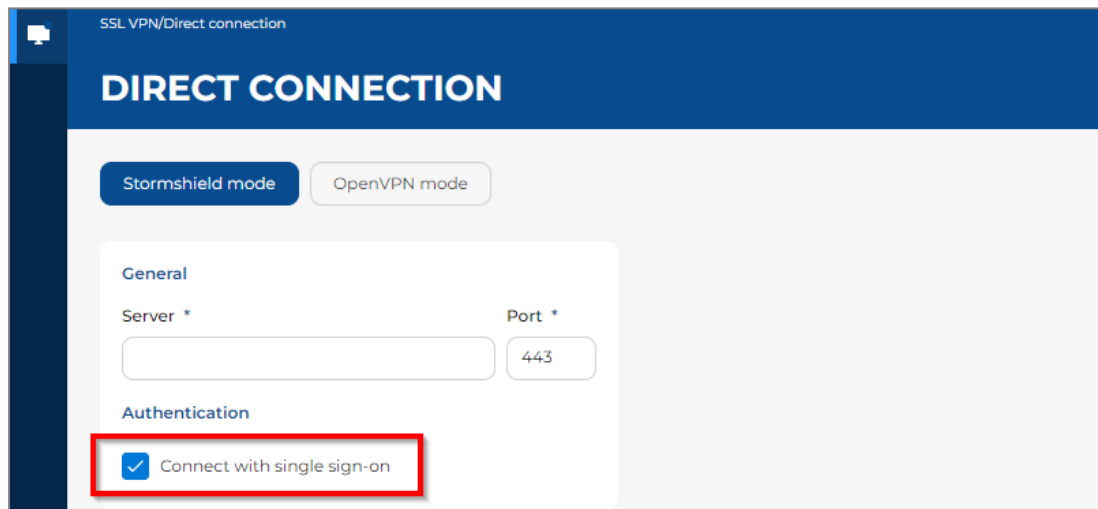
2. On your IdP's authentication portal, follow the steps in the authentication process.
3. Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

Once the SSL VPN tunnel has been set up, the expiry date of your authentication session appears. As long as the expiry date remains in the future, you can set up the SSL VPN tunnel without having to authenticate again.



In the Direct connection menu

1. Select **Stormshield mode**.
2. Select the checkbox **Connect with single sign-on**.

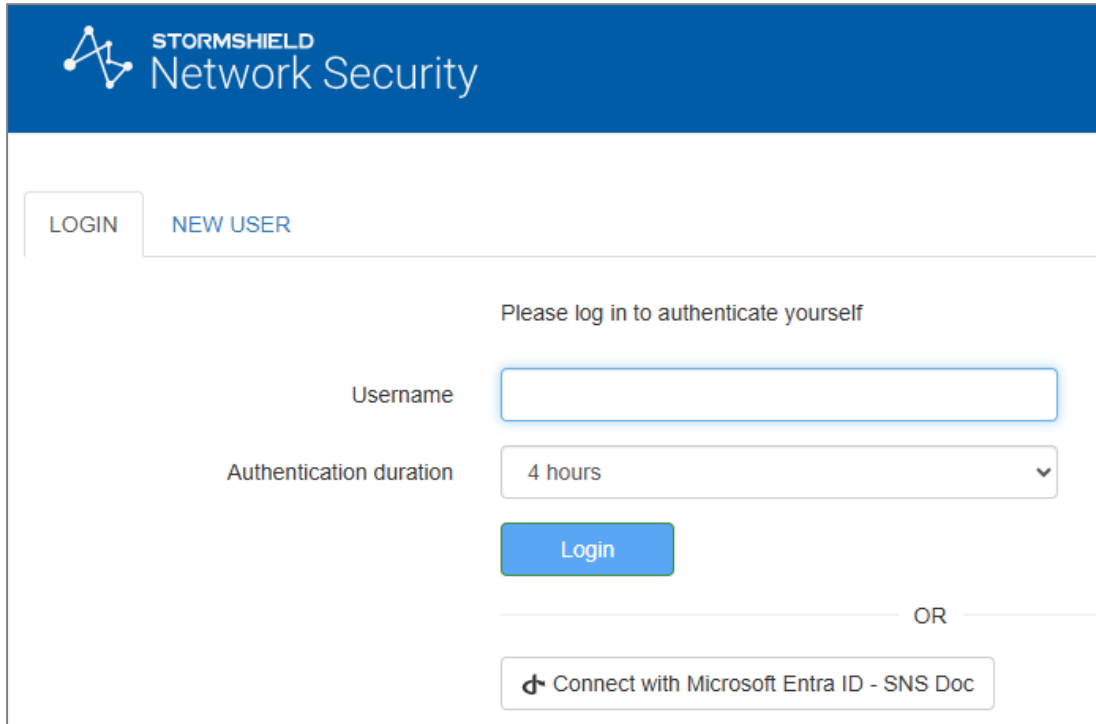




3. Click on **Connect**.

A page will open automatically in your web browser. Depending on the configuration of your SNS firewall, this page may be:

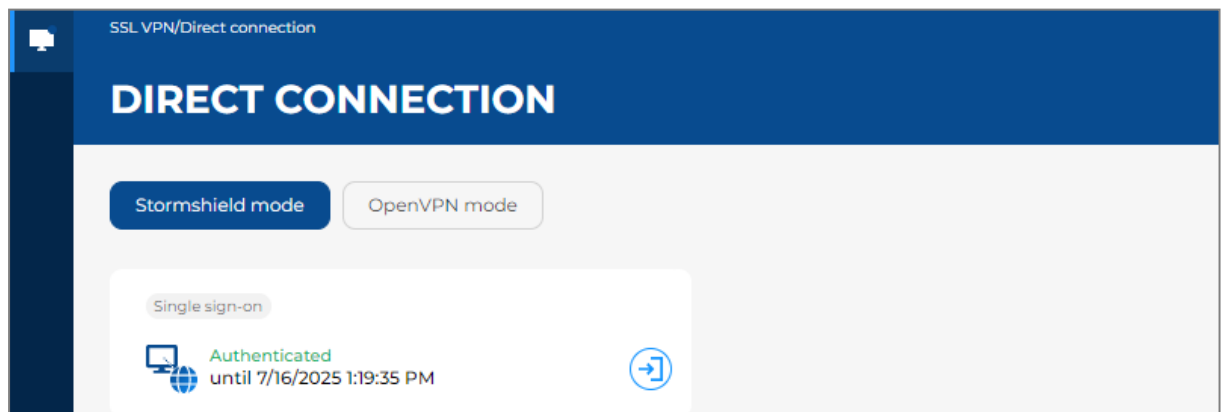
- Your IdP's authentication portal, or
- The SNS firewall's captive portal. If this is the case, click on the button corresponding to your IdP to be redirected to its authentication portal.



4. On your IdP's authentication portal, follow the steps in the authentication process.

5. Wait while the Stormshield SSL VPN client sets up the SSL VPN tunnel.

Once the SSL VPN tunnel has been set up, the expiry date of your authentication session appears. As long as the expiry date remains in the future, you can set up the SSL VPN tunnel without having to authenticate again.





Configuring privileges to access the SSL VPN

This section explains how to grant users the privilege to set up SSL VPN tunnels. This privilege can be assigned to all users, or to certain users and user groups.

Allowing all users to set up SSL VPN tunnels

1. Go to **Configuration > Users > Access privileges, Default access** tab.
2. In the **SSL VPN policy** field, select **Allow**.

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS DETAILED ACCESS

When no access rules have been defined for the user

VPN access

IPsec policy

SSL VPN policy

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

1. Go to **Configuration > Users > Access privileges, Default access** tab.
2. In the **SSL VPN policy** field, select **Block**.
3. Go to the **Detailed access** tab.
4. Click on **Add** to create a custom access rule.
5. In the window that appears, select a user or user group from an SNS firewall directory (such as *finance@domain.tld*). If you wish to do so, select all the users in a directory by setting *Any user@domain.tld*. Click on **Apply** or **OK**, depending on the SNS version used.
A new row will appear in the grid.
6. In the **SSL VPN** column of the new row, select **Allow** as the action.
7. Enable the rule by double-clicking in the **Status** cell of the relevant row.

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS **DETAILED ACCESS**

Searching... + Add X Delete ↑ Up ↓ Down

	Status	User - user group	IPSEC	SSL VPN	Sponsorship	Description
1	<input checked="" type="checkbox"/> Enabled	it@storm.doc	<input type="button" value="Block"/>	<input type="button" value="Block"/>	<input type="button" value="Block"/>	
2	<input checked="" type="checkbox"/> Enabled	finance@storm.doc	<input type="button" value="Block"/>	<input type="button" value="Allow"/>	<input type="button" value="Block"/>	
3	<input checked="" type="checkbox"/> Enabled	hr@storm.doc	<input type="button" value="Block"/>	<input type="button" value="Allow"/>	<input type="button" value="Block"/>	



Configure the SSL VPN service

This section explains how to enable and configure the SSL VPN service on the SNS firewall.
Go to **Configuration > VPN > SSL VPN**.

Enabling the SSL VPN service

Field	Description
Enable SSL VPN <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	Set the selector to ON to enable the SSL VPN service.

VPN / SSL VPN

ON Enable SSL VPN

GENERAL SETTINGS CLIENT WORKSTATION VERIFICATION (ZTNA) (DISABLED) WINDOWS CLIENT WORKSTATION VERIFICATION (ZTNA)

OFF Enable client workstation verification (ZTNA)

Network settings

Public IP address (or FQDN) of the UTM used

Configuring the general settings of the SSL VPN service

On SNS in versions SNS 4.8 LTSB and 5, these settings can be configured in the **General settings** tab. On SNS in version 4.3 LTSB version, there is no tab.

i NOTE
 As of SNS version 4.8.5, a warning will prompt you to disable the LZ4 compression feature if it is enabled. This scenario is described in the section [Troubleshooting](#).

Field	Description
Enable client workstation verification (ZTNA) <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	<p>This field appears in this tab on SNS in version 5. On SNS in version 4.8 LTSB, the feature can be enabled in the Client workstation verification (ZTNA) tab.</p> <p>Set the selector to ON to enable the verification of client workstation compliance. If you have not yet set the criteria for client workstation verification, define them before enabling verification. For more information, refer to the section Configuring client workstation verification (ZTNA).</p>



Network settings section

Field	Description
Public IP address (or FQDN) of the UTM used	<p>Indicate the IP address that users must use in their SSL VPN client to reach the SNS firewall and set up SSL VPN tunnels. You can specify an FQDN or IP address.</p> <ul style="list-style-type: none"> For an FQDN: it must be declared in the DNS servers used by the user's device. If you have a dynamic public IP address, you can use the services of a provider such as <i>DynDNS</i> or <i>No-IP</i>. Next, configure this FQDN in Configuration > Network > Dynamic DNS. For IP addresses: they must be public, and therefore accessible over the Internet.
Available networks or hosts	<p>Select the object representing the networks or hosts that will be reached through the SSL VPN tunnel. This object makes it possible to automatically set on your organization's devices the routes needed to reach resources that can be accessed through the SSL VPN tunnel.</p> <p>To more granularly allow or prohibit traffic between your users' devices and internal resources, you need to define filter rules (see Configuring the filter and NAT policy).</p> <p>If other devices in your organization are located between the SNS firewall and accessible internal resources, you must set static routes on these devices for access to the network assigned to SSL VPN clients.</p>
Network assigned to clients (UDP) Network assigned to clients (TCP)	<p>Select the object corresponding to the TCP and UDP networks assigned to SSL VPN clients. Select the network or sub-networks according to the following criteria:</p> <ul style="list-style-type: none"> The network mask must not be smaller than /28. If you assign two networks, the SSL VPN client will always use the UDP-based SSL VPN tunnel first to ensure better performance. This order is defined in the SSL VPN (OpenVPN) configuration that the SNS firewall provides to SSL VPN clients. 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 SNS firewall would then detect an IP spoofing attempt and block the corresponding traffic. To avoid routing conflicts, select sub-networks that are usually seldom used, and which follow the recommendations given in RFC 1918, such as 10.60.77.0/24. Many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks already use the first few reserved address ranges.
Maximum number of simultaneous tunnels allowed	<p>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 SSL VPN clients. For sub-networks:</p> <ul style="list-style-type: none"> On SNS in version 5: this shows the total number of IP addresses, minus 3. On SNS in version SNS 4.3 LTSB and 4.8 LTSB: 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.



Field	Description
Primary DNS server	Select the object representing the DNS server to be assigned.
Secondary DNS server	

! IMPORTANT

With Stormshield SSL VPN clients in macOS and Linux, scripts must be used to accommodate a specific DNS configuration when OpenVPN does not manage it natively. For further information on the use of these scripts, refer to the [Stormshield SSL VPN client installation guide](#).

Advanced properties section

Field	Description
Enable DCO kernel acceleration	<p>On SNS in version 5 in factory configuration, the DCO (<i>Data Channel Offload</i>) kernel acceleration feature is enabled by default. Select or unselect the checkbox to enable or disable this feature. On SNS in version 4, this feature is not available.</p> <p>This feature improves the performance of UDP-based SSL VPN tunnels. It is not compatible with TCP-based SSL VPN tunnels.</p> <p>The SSL VPN client used must be compatible with the DCO feature to benefit from enhancements. As for the Stormshield SSL VPN client:</p> <ul style="list-style-type: none"> • The Windows version benefits from enhancements. • The Linux version benefits from enhancements only if OpenVPN is in version 2.6.0 or higher, and the openvpn-dco package has been installed. • The macOS version does not benefit from enhancements. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>i NOTE When you enable the DCO feature, a message may appear, prompting you to change the encryption suite if the one you are using is incompatible. Accept the change to enable the feature.</p> </div>
Public IP address of the UTM for the SSL VPN (UDP)	<p>In the following cases, you need to select the object representing the IP address to reach in order to set up UDP SSL VPN tunnels:</p> <ul style="list-style-type: none"> • The IP address to reach is not the main IP address of the external interface, • The IP address to reach belongs to an external interface that is not linked to the default gateway of the SNS firewall.
Port (UDP) Port (TCP)	<p>The listening ports of the SSL VPN service can be changed. Note:</p> <ul style="list-style-type: none"> • 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.



Field	Description
Interval before key renegotiation (seconds)	You can change the length of time after which the keys used by the encryption algorithms will be renegotiated. By default, it is set to 14400 seconds, or 4 hours. During this operation: <ul style="list-style-type: none"> 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 order to stay connected. In this use case, we advise increasing the interval before key renegotiation so that it aligns with the average length of a workday, such as 28800 seconds, or 8 hours.
Use DNS servers provided by the firewall	You can instruct SSL 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 SSL 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 (Windows only)

The Windows Stormshield SSL VPN client can automatically run scripts on the user's workstation every time an SSL VPN connection is opened or closed.

SNS firewall provides these *.bat* scripts to the Stormshield SSL VPN client. They have to be selected in the following fields:

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

In these *.bat* 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).

Certificates

Select the certificates that the SNS firewall's SSL VPN service and SSL VPN clients must present to set up SSL VPN tunnels. These certificates must be issued from the same certification authority.

By default, a server certificate and a client certificate, issued by the same certification authority dedicated to the SSL VPN, are suggested. These certificates and the certification authority were created when the SNS firewall was initialized.

Field	Description
Server certificate	Select the desired certificate.



Field	Description
Client certificate	Select the desired certificate. Client certificates with a TPM-protected private key (🔒 icon) cannot be selected as the private keys of such certificates must be available in plaintext (unencrypted) in the SSL VPN configuration that is distributed to SSL VPN clients.

Configuration

Field	Description
Export the configuration file	Click on this button to export the SSL VPN configuration in OVPN format. You can then import this file into your organization's SSL VPN clients to add a new connection. As for the Stormshield SSL VPN client v5, this configuration is automatically retrieved for connections that are set up in Stormshield mode (or Automatic mode in v4). For OpenVPN connections (imported OVPN file), the file must be imported to set up or save the connection. For more information, refer to the Stormshield SSL VPN client v5 user and configuration guide .



Configuring client workstation verification (ZTNA)

This section explains how to configure a policy to verify the compliance of client workstations that set up SSL VPN tunnels with the SNS firewall.

General information on zero trust network access (ZTNA)

ZTNA consists of trusting users and devices only after they have been verified. To do so, ZTNA can rely on the following components:

- Guaranteed compliance of the communication channel through TLS encryption of SSL VPN tunnels.
- User verification, for example through multifactor authentication, such as the Stormshield TOTP solution (see [Configuring one-time password \(OTP\) authentication](#)).
- A policy verifying the compliance of client workstations and users. This configuration is covered in the section below.
- Granular filtering to restrict users' access to only what is necessary (see [Configuring the filter and NAT policy](#)).

How client workstation verification (ZTNA) works

When client workstation verification is enabled:

- SSL VPN clients that are compatible with this feature can set up SSL VPN tunnels with the SNS firewall only if they are compliant (**all** the criteria defined in the policy have been met),
- SSL VPN clients that are not compatible with this feature cannot set up SSL VPN tunnels with the SNS firewall, **unless** they are explicitly allowed to do so by enabling the **SSL VPN clients incompatible with ZTNA** setting.

Requirements

- An SNS firewall in version 4.8 LTSB or 5.
- SSL VPN clients that are compatible with client workstation verification:
 - The Stormshield SSL VPN client in version 4.0 and higher is compatible. It must be set to **Stormshield mode** for versions 5 or **Automatic mode** for versions 4.
 - Third-party SSL VPN clients, such as OpenVPN Connect, are not compatible.

Configuring client workstation verification

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

The order of the fields described below corresponds to the order on SNS in version 5. While there are differences with SNS in version 4.8 LTSB, the titles should allow you to identify the fields.



Client workstation verification (ZTNA) tab

Field	Description
Enable client workstation verification (ZTNA)	This field appears in this tab on SNS in version 4.8 LTSB. On SNS in version 5, this feature can be enabled in the General settings tab. Select the checkbox to enable verification of client workstation compliance. If you have not yet set the criteria for client workstation verification, define them before enabling verification.

Version of the Stormshield SSL VPN client / Checking the 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 to allow multiple versions of the Stormshield SSL VPN client to set up SSL VPN tunnels (when there is a pool of varied Stormshield SSL VPN clients). By selecting this option: <ul style="list-style-type: none"> You must enter the Lowest version of Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall, You can enter the Highest version, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall.
Allow only one version	Select this option to exclusively allow one Stormshield SSL VPN client version. You must then enter the exact version of the Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall.

Allow tunnels to be set up for the following additional clients

Field	Description
Stormshield SSL VPN clients (Linux or macOS)	Select the checkbox if your organization's pool of Stormshield SSL VPN clients includes Stormshield SSL VPN clients running in Linux and/or macOS. By doing so, specific Windows criteria will not be applied to these workstations.
SSL VPN clients incompatible with ZTNA	Select the checkbox to allow SSL VPN clients that are not compatible with the client workstation verification feature to set up SSL VPN tunnels with the SNS firewall, e.g., for use with mobile devices.

Customized message for non-compliant workstations

If an SSL VPN tunnel fails to set up because it does not comply with the policy, the Stormshield SSL VPN Client displays the default message *"For more information, please contact support"* in English, French and German.

If you prefer a different message, you can customize it by editing it in the text entry section. You can also delete the message so that it will no longer be shown. 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 revert to the default message by clicking on **Go back to messages suggested by default**.



Customized message for incompatible workstations

Write the customized message below, which will be displayed by the SSL VPN client when ZTNA criteria are not met.

[Go back to messages suggested by default](#)

Pour plus d'informations, veuillez contacter le service d'assistance.
For more information, please contact support.
Für weitere Informationen wenden Sie sich bitte an den Support.

182 characters (maximum 1000)

Could not connect to the server. Client workstation compliance verification failed..

Pour plus d'informations, veuillez contacter le service d'assistance.
For more information, please contact support.
Für weitere Informationen wenden Sie sich bitte an den Support.

Server

Windows client workstation verification (ZTNA) tab

On SNS in version 4.8 LTSB, this tab does not exist. The fields that are described below are found in the **Client workstation verification (ZTNA)** tab.

! IMPORTANT
If you select multiple criteria below, they must **all** be met to allow the SSL VPN client to set up SSL VPN tunnels with the SNS firewall.

Field	Description
Client workstation antivirus enabled and up to date	<p>When this checkbox is selected, 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, which means that third-party antivirus modules can be supported as long as their status is recognized.</p> <p>i NOTE The Windows service that checks the status of the antivirus takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.</p>
Active firewall on the client workstation	<p>If this checkbox is selected, the workstation's Windows firewall must be running, and the <i>Domain network</i>, <i>Private network</i> and <i>Public network</i> profiles must be enabled. If a profile is inactive, this criterion will be considered non-compliant.</p> <p>i NOTE The Windows service that checks the status of the Windows firewall takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.</p>
SES installed on the client workstation	<p>If this checkbox is selected, the SES Evolution agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.</p>



Field	Description
Prohibit users holding administration privileges on the client workstation	When this checkbox is selected, users who hold administrator privileges on the workstation cannot set up SSL VPN tunnels with the firewall SNS.

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. Settings are configured in the tab corresponding to the version in question.

Field	Description
Allow a version range (builds)	Select this option to allow multiple versions of Windows (when there is a pool of varied Windows workstations). By selecting this option: <ul style="list-style-type: none"> You must enter the Lowest version that the workstation must run, so that it can set up SSL VPN tunnels with the SNS firewall. The default versions are: 10000 for Windows 10 and 20000 for Windows 11. You can enter the Highest version, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall.
Allow only one version	Select this option to exclusively allow one single Windows version. You must then enter the exact Windows version of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall.

Membership in a company domain

On SNS in version 4.8 LTSB, the visible field changes, depending on whether the **Host connected to a domain** or **User connected to a domain** tab has been selected.

Field	Description
Ensure that the host is connected to a company domain (SNS v5)	When this option is selected, you have to add to the grid the domains of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall. Do note that this criterion is not related to the configuration of directories on the SNS firewall.
Connect the host to a company domain (SNS v4.8 LTSB)	
Ensure that the user belongs to a company domain (SNS v5)	When this option is selected, you have to add to the grid the domains of users who are allowed to set up SSL VPN tunnels with the SNS firewall. 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. Do note that this criterion is not related to the configuration of directories on the SNS firewall.
The user is connected to a company domain (SNS v4.8 LTSB)	



Configuring the filter and NAT policy

This section explains how to configure the filter and NAT policy to be implemented in order to deploy SSL VPN tunnels. You can click on **Apply** at any time to save your changes.

Configuring the filter policy

You need to define rules to grant or deny SSL VPN clients access to your organization's internal resources. In the example below, we are adding a rule to allow all user connections from UDP and TCP SSL VPN clients to an HTTP intranet.

To increase security, you can set up granular filtering to restrict users' access to only what is necessary. To do so, create rules for each user group that is setting up SSL VPN tunnels with the SNS firewall (in the rule editing window: **User** tab on SNS in version 5 or **Source** tab, **User** field on SNS in version 4).

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

i NOTE

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.).

FILTERING		IPV4 NAT									
Searching...		+ New rule		X Delete		↑ ↓		Cut Copy Paste		Search in logs	
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection				
1	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> pass	vpnsnl_pool_udp vpnsnl_pool_tcp via SSL VPN tunnel	intranet_server	http		IPS				

Configuring the NAT policy

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



1. Go to **Configuration > Security policy > Filter - NAT, NAT** tab.
2. 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.
3. In the **General** tab, **Status** field, select **On**.
4. In the **Original source** tab:
 - a. **Source hosts** field, select the objects that represent the IP addresses of UDP and TCP SSL VPN clients,
 - b. **Incoming interface** field, select **SSL VPN**.
5. In the **Original destination** tab, **Destination hosts** field, select **Internet**.
6. In the **Translated source** tab, **Translated source host** field, select the object that represents the public IP address.
7. In the **Translated source port** field, select the option **Choose random translated source port**.
8. Click on **OK**.

FILTERING		IPV4 NAT							
		Original traffic (before translation)				Traffic after translation			
	Status	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		




Tracking connected users

This section explains how to track currently connected users, or those that are connected through the SSL VPN, from the SNS firewall web administration interface.

To improve the readability of images, some columns in tables have been hidden. As such, what you see on your SNS firewall may be slightly different. Not all of the available columns are described in this section. For more information, refer to the in the [v4 user guide](#) or [v5 user guide](#), depending on the SNS version used.

Information on access to private data

Some information can be accessed if the user has been granted permissions to look up private data. If you hold this permission or a code to access private data:

- On SNS in version 5: click on the icon representing a user  in the upper banner, then click on **Obtain personal data access**. If an access code is required, enter it and click on **Obtain**.
- On SNS in version 4: click on **Logs: restricted access** in the upper banner. If an access code is required, enter it and click on **Obtain**.

For further information, refer to the Technical note [Complying with privacy regulations](#).

Displaying users currently connected to the SNS firewall through the SSL VPN

In SSL VPN tunnel monitoring

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

This view shows which users are connected to the SNS firewall through the SSL VPN in real time, and includes session details (IP addresses, number of bytes sent and received, etc.).

Column	Description
User	Indicates the name of the user currently connected to the SNS firewall through the SSL VPN.
Client version	Indicates the version of the Stormshield SSL VPN client that was used to connect. In order for the version to be displayed, the Stormshield SSL VPN client has to be in version 4.0 and higher, and it must be set to Stormshield mode in version 5 or Automatic mode in version 4. This column is available only on SNS versions 4.8 LTSB and 5.
Client workstation verification (ZTNA)	Indicates the client workstation's compliance status. There are several possible values: <ul style="list-style-type: none"> • Disabled: the client workstation verification feature has been not enabled. • Not verified: the SSL VPN client that was used to set up the SSL VPN tunnel is not compatible with client workstation verification, but SSL VPN tunnels can be set up for incompatible clients. • Compliant: the client workstation complies with the criteria defined in the client workstation verification policy. This column is available only on SNS versions 4.8 LTSB and 5.



MONITOR / SSL VPN TUNNELS									
Searching...									
Reset this tunnel Refresh Export results Configure the SSL VPN service reset columns									
User	Directory	VPN client IP address	Client version	Client workstation verification (ZTNA)	Real IP address	Received	Sent	Duration	Port
Elala	storm.doc		5.1.1	Disabled		27.63 KB	20.8 KB	3m 33s	64892

In user monitoring

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

This view provides a real-time view of the users connected on the SNS firewall.

Column	Description
User	Indicates the name of the user currently connected on the SNS firewall. To find out whether the user is connected to the SNS firewall through the SSL VPN, check the "SSL VPN" column.
Client workstation verification (ZTNA)	Indicates the client workstation's compliance status. There are several possible values: <ul style="list-style-type: none"> Disabled: the client workstation verification feature has been not enabled. Not verified: the SSL VPN client that was used to set up the SSL VPN tunnel is not compatible with client workstation verification, but SSL VPN tunnels can be set up for incompatible clients. Compliant: the client workstation complies with the criteria defined in the client workstation verification policy. This column is available only on SNS versions 4.8 LTSB and 5.
One-time password	Indicates whether a user has logged in using a TOTP from the Stormshield TOTP solution. This column is available only on SNS versions 4.8 LTSB and 5.
SSL VPN	Identifies users connected on the SNS firewall through the SSL VPN.

MONITOR / USERS									
REAL-TIME HISTORY									
No predefined filter									
Filter Reset Refresh Export results Configure authentication reset columns									
Name	IP address	Directory	Group	Expiry date	Auth. method	Client workstation verification (ZTNA)	One-time password	SSL VPN	
elala		storm.doc	finance	6d 23h 54m 42s	OPENVPN	Disabled			✓

Viewing logs on VPN tunnel events

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

This log shows events relating to SSL VPN and IPsec VPN tunnels.

By default, events from the last hour are displayed. You can change the time range by selecting another value in the toolbar above the grid.

Column	Description
Saved at	Indicates the date and time of the event.



Column	Description
Message	<p>Indicates the nature of the event: VPN tunnel connected or disconnected, user authentication in the firewall authentication engine, etc.</p> <p>On SNS versions 4.8 LTSB and 5, messages relating to the client workstation verification feature (<i>HostChecking</i> in the logs) may appear:</p> <ul style="list-style-type: none"> Error during authentication: HostChecking failed with a value of "Unverified" in the "Client workstation verification (ZTNA)" column: the connection was not set up because the SSL VPN client used is not compatible with client workstation verification, and the policy does not allow SSL VPN tunnels to be set up for incompatible clients. "Error during HostChecking" with a value of "Non-compliant" in the "Client workstation verification (ZTNA)" column: the connection was not set up because the client workstation does not comply with the criteria defined in the client workstation verification policy.
User	Indicates the user that is associated with the event.
Client workstation verification (ZTNA)	<p>Indicates the client workstation's compliance status. There are several possible values:</p> <ul style="list-style-type: none"> Disabled: the client workstation verification feature 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 client workstation verification. To find out whether the SSL VPN 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. <p>This column is available only on SNS versions 4.8 LTSB and 5.</p>
Client workstation verification criterion	<p>Shows non-compliant criteria when an SSL VPN tunnel fails to set up due to the non-compliance of the client workstation or user.</p> <p>This column is available only on SNS versions 4.8 LTSB and 5.</p>

LOG / VPN								
Last hour Refresh No predefined filter Save Delete Simple search Actions								
SEARCH FROM - 09/11/2025 10:28:03 AM - TO - 09/11/2025 11:28:03 AM								
Saved at	Message	User	Source Name	Local network	Remote network	Client version	Client workstation verification (ZTNA)	Client workstation verification criterion
11:24:30 AM	SSL tunnel destroyed	elala						
11:24:30 AM	User deauthenticated from ASQ	elala						
10:56:21 AM	SSL tunnel created	elala				5.1.1	Disabled	
10:56:21 AM	User authenticated in ASQ	elala						
10:55:56 AM	Error during HostChecking	Elala				5.1.1	Non-compliant	ClientVersion



Troubleshooting

This section lists several issues that are frequently encountered when the SSL VPN is used. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the [Stormshield knowledge base](#) (authentication required).

A user is unable to log in and the message "*Client workstation compliance verification failed*" appears

- **Situation:** When a user attempts to connect, the SSL VPN tunnel fails to set up and the message "*Client workstation compliance verification failed*" appears on the user's Stormshield SSL VPN client.
- **Cause:** The client workstation that was used does not comply with all the criteria defined in the client workstation verification policy (ZTNA).
- **Solutions:**
 - Check for non-compliant criteria by referring to [Viewing logs on VPN tunnel events](#), then rectify the compliance of the client workstation.
 - Check the configuration of the client workstation verification policy by referring to the section [Configuring client workstation verification \(ZTNA\)](#).

An internal resource cannot be accessed over the SSL VPN tunnel

- **Situation:** The SSL VPN tunnel has been set up, but an internal 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.

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 in the SSL VPN module.
- **Cause:** The LZ4 compression feature is obsolete, and we recommend disabling it
- **Solution:** In the warning window, accept the suggestion to disable the feature. If you have ignored this warning, a message will continue to be displayed until this feature is disabled. To disable it, use the following CLI serverd commands:

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



Further reading

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

To configure and use the Stormshield SSL VPN client, refer to the [Stormshield SSL VPN client v5 user and configuration guide](#).

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



STORMSHIELD

documentation@stormshield.eu

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

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