



STORMSHIELD



TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

CONFIGURING AND USING SSL VPN ON SNS FIREWALLS

Product concerned: SNS 3.x, SNS 4.x, SSL VPN Client 3.x

Document last updated: January 18, 2024

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



Table of contents

- Change log 4
- Getting started 5
- Requirements 6
- Operation and limitations 7
 - Compatible SSL VPN clients 7
 - Maximum number of SSL VPN tunnels allowed on SNS firewalls 7
 - Specific characteristics of Stormshield SSL VPN clients 7
 - Automatic connection mode 7
 - Running scripts 7
 - Multifactor authentication methods compatible with the SN SSL VPN Client 8
- Configuring the SNS firewall 9
 - Configuring authentication 9
 - Adding RADIUS as an authentication method (optional) 9
 - Configuring the authentication policy 9
 - Configuring the captive portal 10
 - Assigning access privileges to the SSL VPN 10
 - Enabling and configuring the SSL VPN service 11
 - Network settings section 11
 - DNS settings sent to client section 12
 - Advanced properties section 12
 - Creating filter and NAT rules 13
 - Configuring the filter policy 13
 - Configuring the NAT policy 14
- Installing and configuring the SSL VPN client 15
 - Installing and configuring the SN SSL VPN Client 15
 - Downloading the SN SSL VPN Client 15
 - Installing the SN SSL VPN Client 15
 - Configuring the SN SSL VPN Client 16
 - Installing and configuring OpenVPN Connect 18
 - Installing OpenVPN Connect 18
 - Configuring OpenVPN Connect 18
- Setting up an SSL VPN tunnel 19
 - Setting up SSL VPN tunnels with SN SSL VPN Client 19
 - Connecting SSL VPN tunnels in Automatic mode 19
 - Connecting SSL VPN tunnels by using the address book 19
 - Connecting SSL VPN tunnels in Manual mode 20
 - Showing the connection information of SSL VPN tunnels 21
 - Disconnecting SSL VPN tunnels 21
 - Setting up an SSL VPN tunnel with OpenVPN Connect 22
 - Connecting SSL VPN tunnels 22
 - Disconnecting SSL VPN tunnels 22
- Reading logs 23
 - In the SNS firewall's administration interface 23
 - On the SN SSL VPN Client 23



On OpenVPN Connect	23
Troubleshooting	25
Further reading	27



Change log

Date	Description
January 18, 2024	- Changes to section "Enabling and configuring the SSL VPN service" (information regarding TPM).
December 14, 2023	- Changes to section "Enabling and configuring the SSL VPN service".
July 20, 2023	- SN SSL VPN Client 3.2.3 release - Changes to sections "Operation and limitations", "Installing SN SSL VPN Client", "Setting up SSL VPN tunnels with SN SSL VPN Client" and "Troubleshooting".
May 25, 2023	- Changes to sections "Configuring authentication", "Installing SN SSL VPN Client" and "Troubleshooting"
February 21, 2023	- Changes to sections "Operation and limitations" and "Setting up SSL VPN tunnels"
February 02, 2023	- Changes to section "Configuring authentication"
January 26, 2023	- SN SSL VPN Client 3.2 release
January 10, 2023	- Compatibility with TOTP added - Changes to sections "Requirements", "Operation and limitations", "Configuring the SNS firewall" and "Setting up SSL VPN tunnels"
August 19, 2022	- Changes to section "Configuring authentication"
July 12, 2022	- Changes to sections "Requirements", "Configuring the SNS firewall", "Installing and configuring the SSL VPN client", "Setting up an SSL VPN tunnel" and "Reading logs"
May 12, 2022	- Compatibility with Windows 11 in 64 bits added
February 22, 2022	- SN SSL VPN Client 3.0 release - Changes to the "Requirements" section



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 an SSL 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 will only be set up if the server and client certificates presented are signed by a trusted certification authority (CA), thereby guaranteeing authentication, confidentiality, integrity and non-repudiation.



This technical note explains how to configure the SSL VPN service on the SNS firewall, and how to install and configure an SSL VPN client until an SSL VPN tunnel is set up.



Requirements

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

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. By doing so, the users and user groups allowed to set up SSL VPN tunnels can be determined during the configuration of the SSL VPN.

You can check this connection in the SNS firewall's administration interface in **Configuration > Users > Authentication > Available methods**. An **LDAP** line must appear in the grid. For more information, refer to the section on *Authentication* in the **v4** or **v3** 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. In particular, such access will allow them to retrieve the VPN configuration.

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, refer to the section on *Authentication* in the **v4** or **v3** user guide of the SNS version used.

Prior configuration of components involved in multifactor authentication (optional)

If you intend to use multifactor authentication for SSL VPN connections, the following components must already be configured:

- The selected multifactor authentication solution,
- The RADIUS server, with which the SNS firewall can be associated with the selected multifactor authentication solution.



Operation and limitations

Compatible SSL VPN clients

- **SN SSL VPN Client**, in its most recent 3.x version. SN SSL VPN Client is compatible with 64-bit Windows 8.1, 64-bit Windows 10 and 64-bit Windows 11,
- **OpenVPN Connect**, compatible with Windows, macOS, Linux, iOS and Android. Refer to the [OpenVPN website for more information](#),
- **SN VPN Client Standard**, in its most recent 6.x version. SN VPN Client Standard is compatible with Windows 10 and Windows 11 with a 64-bit Intel processor. For more information on how to configure and use this client, refer to the [SN VPN Client Standard User guide](#).

Maximum number of SSL VPN tunnels allowed on SNS firewalls

This number varies according to the SNS firewall model used. You can find this information on the [Stormshield website, under All our products > Network security](#).

Specific characteristics of Stormshield SSL VPN clients

Automatic connection mode

SN SSL VPN Client has an automatic connection mode in which it can securely retrieve its SSL VPN configuration. This mode operates as follows:

- **During the initial connection in Automatic mode:**
 - The SN SSL VPN Client authenticates the first time on the SNS firewall and automatically retrieves its SSL VPN configuration,
 - The SN SSL VPN Client authenticates a second time on the SNS firewall to set up the SSL VPN tunnel.
- **During subsequent connections:**
 - If there are no new SSL VPN configurations, the SN SSL VPN Client authenticates on the SNS firewall to set up the VPN tunnel,
 - If a new SSL VPN configuration is available, SN SSL VPN Client must authenticate again, in the same way as for an initial connection, to retrieve the new configuration.

SN SSL VPN Client also has a manual connection mode in which the SSL VPN configuration must be manually integrated. Do note that OpenVPN Connect has only one manual connection mode.

Running scripts

The SN SSL VPN Client can run scripts on the user's workstation (Windows only) every time an SSL VPN tunnel is opened or closed.



Multifactor authentication methods compatible with the SN SSL VPN Client

This table lists the compatible multifactor authentication methods according to the version installed on the SNS firewall and the connection mode that the SN SSL VPN Client uses.

SNS version	Connection mode used by the SN SSL VPN Client	Password + OTP	OTP only	Push mode	TOTP
4.5 or higher	All modes	✓	✓	✓	✓
4.3 and 4.4	All modes	✓	✓	✓	✗
3.x, 4.2 or below	Automatic mode	✗	✗	✗	✗
	Manual mode	✓	✓	✗	✗

The SN SSL VPN Client's connection modes are: Automatic mode (with or without address book) and manual mode.



Configuring the SNS firewall

Before setting up SSL VPN tunnels, several modules must be configured on the SNS firewall. Even though some have already been configured, ensure that the following components described in this chapter have been configured :

- [Configuring authentication](#),
- [Assigning access privileges to the SSL VPN](#),
- [Enabling and configuring the SSL VPN service](#),
- [Creating filter and NAT rules](#).

Perform the operations in this chapter in the SNS firewall's administration interface.

Configuring authentication

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

Adding RADIUS as an authentication method (optional)

If you are using multifactor authentication for SSL VPN connections, RADIUS makes it possible to connect the SNS firewall to your RADIUS server (configured beforehand), which itself is connected to your multifactor authentication solution (configured beforehand).

1. Go to the **Available methods** tab.
2. Click on **Add a method** or **Enable a method**, then click on **RADIUS**.
3. Follow the instructions. For more information on which fields to enter, refer to the section on Authentication in the **v4** or **v3** user guide of the SNS version used.
4. If you are using multifactor authentication in **Push mode**, you must change the RADIUS *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
CONFIG AUTH RADIUS btimeout=30000
CONFIG AUTH ACTIVATE
```

Configuring the authentication policy

1. Go to the **Authentication policy** tab.
2. In the **Default method** area, **Method to use if no rules match** field, identify the method specified. 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 (restricted only to authentication, the use of multifactor authentication, TOTP, etc.), you must add two rules. You can also set rules for specific user groups to strengthen security. Do note that during authentication, rules will be scanned in the order of their appearance in the list.

Add the first rule:



1. Click on **New rule > Standard rule**.
2. In the **User** tab, **User or group** field: select the relevant user group. *Any user@* applies to all users on the domain.
3. In the **Source** tab, click on **Add an interface** and select the external interface through which users authenticate (e.g. *out*).
4. In the **Authentication methods** tab in the grid, select the *Default method* row and click on **Delete**.
5. Click on **Authorize a method** and select the method (*LDAP, RADIUS*, etc.) that makes it possible to connect to the firewall's captive portal and retrieve the VPN configuration.

Add the second rule:

1. Click on **New rule > Standard rule**.
2. In the **User** tab, **User or group** field: select the relevant user group. *Any user@* applies to all users on the domain.
3. In the **Source** tab, click on **Add an interface** and select *SSL VPN*.
4. In the **Authentication methods** tab in the grid, select the *Default method* row and click on **Delete**.
5. Click on **Authorize a method** and select the method (*LDAP, RADIUS*, etc.) that makes it possible to set up SSL VPN tunnels.

Configuring the captive portal

1. Go to the **Captive portal** tab of the **Authentication profile and interface match** grid, and 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, check the directory entered: If it is the right directory, the profile selected be correctly pre-configured. Continue to [Assigning access privileges to the SSL VPN](#).
If it is not the right directory, select another profile, such as *default05*, and go to the **Captive portal profiles** tab. Select this other profile, choose the right directory from the **Default method or directory** field and enable the captive portal in the **Advanced properties** section.

Assigning access privileges to the SSL VPN

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.



Enabling and configuring the SSL VPN service

To enable the SSL VPN service on the SNS firewall:

1. Go to **Configuration > VPN > SSL VPN**.
2. Set the status cursor to **ON**.

Several sections are available for the configuration of the SNS firewall's SSL VPN service.

Network settings section

1. In the **UTM IP address (or FQDN) used** field, indicate the IP address that users must use to reach the SNS firewall to set up SSL VPN tunnels.
 - If you enter an IP address, it must be public, and therefore accessible over the Internet,
 - If you enter an FQDN (e.g., *ssl.company.tld*), it must be declared on the DNS servers that the client device 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*. In this case, configure this FQDN on the SNS firewall in **Configuration > Network > Dynamic DNS**.
2. In the **Available networks or hosts** field, 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 the client device 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 clients 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.
3. In **Network assigned to clients (UDP)** and **Network assigned to clients (TCP)**, select the object corresponding to the network that will be assigned to VPN clients. The network mask must not be smaller than /29 for SNS versions 3.x or 4.2 and below, or /28 for SNS versions 4.3 and above.

You can assign different networks to VPN clients in UDP and TCP. The VPN client will always choose the UDP network first for better performance.

As for the network or sub-networks:

 - Choose a network dedicated to SSL VPN clients that does not belong to any existing internal networks, or 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,
 - Choose seldom-used sub-networks (e.g., *10.60.77.0/24*) to prevent routing conflicts on client devices during the connection to the SSL VPN. Many filtered Internet access networks (public Wi-Fi, hotels, etc) or private local networks already use the first few reserved address ranges.
4. The maximum number of simultaneous tunnels allowed will appear automatically. This number corresponds to the minimum value between the maximum number of tunnels allowed on the SNS firewall (see [Operation and limitations](#)) and the number of sub-networks available for VPN clients. For the number of sub-networks, depending on the SNS version, this represents:
 - **3.x or 4.2 and higher** a quarter of the number of IP addresses, minus 1. An SSL VPN tunnel consumes 4 IP addresses, but the server reserves 1 sub-network for its own use.
 - **4.3 and higher** a quarter of the number of IP addresses, minus 2. An SSL VPN tunnel takes up 4 IP addresses, but the server reserves 2 sub-networks for its own use.



DNS settings sent to client section

1. In the **Domain name** field, enter the domain name assigned to the SSL VPN clients so that they can resolve their host names.
2. In the **Primary DNS server** and **Secondary DNS server** fields, select the object representing the DNS server to be assigned.

Advanced properties section

1. In the **UTM IP address for the SSL VPN (UDP)** field, especially in one of the following cases:
 - 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.

Select the object representing the IP address used for setting up SSL VPN tunnels (UDP). The SSL VPN service listens on all of the SNS firewall's IP addresses by default.

2. In the **Port (UDP)** and **Port (TCP)** fields, you can modify the listening ports of the SSL VPN service. Some ports are reserved for the SNS firewall's internal use only and cannot be selected. 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. On **4.3 versions and higher**, port 443 is the only port below 1024 that can be used.
3. In the **Interval before key renegotiation (seconds)** field, you can change the length of time after which the keys used by the encryption algorithms will be renegotiated. The default value is 4 hours (14400 seconds). This operation is transparent for the user - the active tunnel will not be disrupted during renegotiation.
4. When **Use DNS servers provided by the firewall** is selected, the SSL VPN client will save the DNS servers retrieved via the SSL VPN in the workstation's network configuration (Windows only). If DNS servers are already defined on the workstation, they may be queried.
5. When **Prohibit use of third-party DNS servers** is selected, the SSL VPN client will exclude DNS servers already defined in the workstation's configuration (Windows only). Only DNS servers sent by the SNS firewall can be queried.

Scripts to run on the client

On Windows workstations, SN SSL VPN Client can run *.bat* scripts when a VPN tunnel is opened or closed. In these scripts, you can use:

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

Example of a script to connect the Z: network drive to the \\myserver\myshare shared network:

```
NET USE Z: \\myserver\myshare
```

Example of a script to disconnect the Z: network drive from the \\myserver\myshare shared network:

```
NET USE Z: /delete
```

Certificates used


Select the certificates that the SNS firewall's SSL VPN service and the SSL VPN client must present to set up a tunnel. 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.

If you use your own certification authority, you must create a client identity and a server identity. If this CA is not the root authority, both peer certificates have to be issued from the same sub-authority.

On firewalls that are equipped with a TPM and are in SNS version 4.7 and higher:

- You can select a **server certificate** with a TPM-protected private key. The  icon indicates certificates with a TPM-protected private key,
- **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.

For more information ranging from TPM protection of private keys in the firewall's certificates, to the configuration of such certificates in the firewall's modules, refer to the technical note [Configuring the TPM and protecting private keys in SNS firewall certificates](#).

Configuration

The **Export the configuration file** button exports the SSL VPN configuration in *.ovpn* format.

Creating filter and NAT rules

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

Configuring the filter policy

Set the rules that allow or do not allow SSL VPN clients to access internal resources. In our example, we added two rules to allow connections from UDP and TCP SSL VPN clients to our intranet over HTTP.

For increased security, you can also create rules for specific user groups (**User** field) and use advanced filter functions (inspection profiles, application proxies, antivirus scans, etc.).

1. In the **Filtering** tab, click on **New rule > Single rule**.
2. 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, **General** sub-tab, **Source hosts** field, select the object that represents the IP addresses of UDP SSL VPN clients for the first rule. For the second rule, select the object that represents the IP addresses of TCP SSL VPN clients.
6. In the **Advanced properties** sub-tab, **Via** field, select *SSL VPN tunnel*.
7. In the **Destination** tab, **Destination hosts** field, select the object that represents the internal server or the intranet.
8. In the **Port - Protocol** tab, **Destination port** field, select *https*.
9. Click on **OK**.

Filter policy on an SNS firewall in version 4 (same in version 3).



FILTERING		IPV4 NAT						
Searching...								
+ New rule X Delete ↑ ↓ ↻ ✂ Cut 📄 Copy 📄 Paste								
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
1	on	pass	vpnssl_pool_udp via SSL VPN tunnel	intranet_server	http		IPS	
2	on	pass	vpnssl_pool_tcp via SSL VPN tunnel	intranet_server	http		IPS	

Configuring the NAT policy

Set up a network address translation (NAT) rule if UDP and TCP SSL VPN clients must access the Internet.

1. In the **NAT** or **IPv4 NAT** tab, click on **New rule** > **Single rule**.
2. Double-click on the number of the new rule to edit it; a new window will open.
3. In the **General** tab, **Status** field, select **On**.
4. In the **Original source** tab, **Source hosts** field, select the objects that represent the IP addresses of SSL VPN clients in UDP and TCP.
5. In the **Outgoing interface** field, select **SSL VPN**.
6. In the **Original destination** tab, **Destination hosts** field, select **Internet**.
7. In the **Translated source** tab, **Translated source host** field, select the object that represents the public IP address.
8. In the **Translated source port** field, select *ephemeral fw* and select the option **select a random translated source port**.
9. Click on **OK**.

NAT policy on an SNS firewall in version 4 (same in version 3).

FILTERING		IPV4 NAT							
Searching...									
+ New rule X 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	Internet	Any	Pub_FW	ephemeral_fw	Any		



Installing and configuring the SSL VPN client

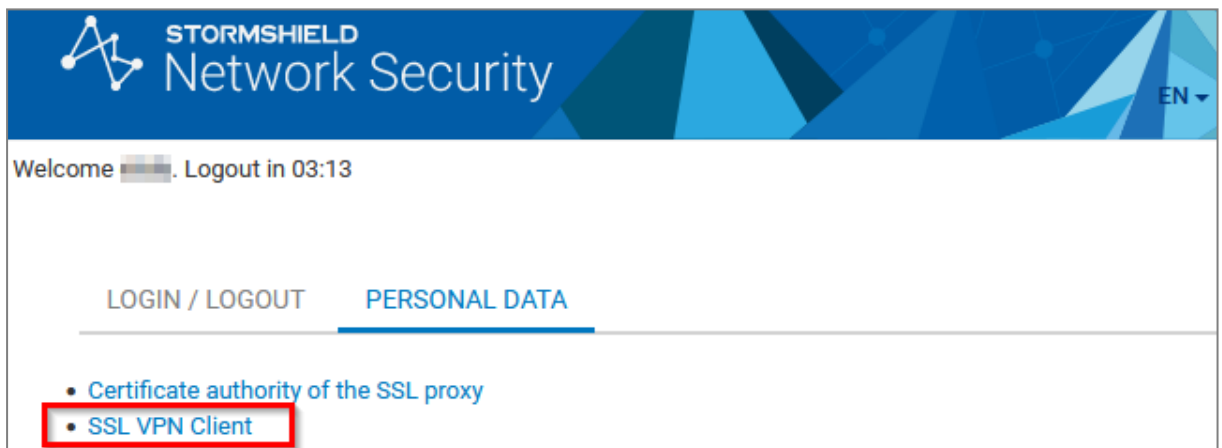
This chapter explains how to install and configure the [SN SSL VPN Client](#) and [OpenVPN Connect](#).

Installing and configuring the SN SSL VPN Client

Downloading the SN SSL VPN Client

- From the Stormshield SSL VPN website.
Log in to <https://vpn.stormshield.eu/> and follow the instructions given.
- From the MyStormshield personal area.
Log in to your [MyStormshield personal area](#) and go to **Downloads > Downloads > Stormshield Network Security > SSL VPN**.
- From the captive portal of the SNS firewall that hosts the SSL VPN service.
Authenticate on https://firewall_IPaddress/auth, and in the **Personal data** tab, click on **SSL VPN Client**.

Captive portal on an SNS firewall in version 4 (similar in version 3).



Installing the SN SSL VPN Client

The SN SSL VPN Client can only be used by a single Windows user profile, and must be installed on its end user's profile in one of the following ways. The installation requires local administrator privileges on the workstation or the user must enter the login and password of an administrator account.

Standard installation

1. Run the *msi* package downloaded earlier on the workstation.
2. Follow the steps in the installation wizard.

Deployment via a group policy (GPO)

By deploying the SN SSL VPN Client via a group policy (GPO), it will be automatically installed when the workstation connects to the company network. To set up this deployment, you must first retrieve the *msi* package.

Since the SN SSL VPN Client is not a multi-user application, you must set its installation policy in the User configuration tree of the domain controller: **Group Policy Management editor >**



Default Domain Policy > User configuration > Policies > Software settings > Software installation.


To make it easier for users to connect to the SSL VPN, you can fill in the **Firewall address** field in the connection window of the SN SSL VPN Client by changing the value of the registry key **HKEY_CURRENT_USER\Software\STORMSHIELD\SSL VPN Client\address**.

Configuring the SN SSL VPN Client

There are several connection modes that the SN SSL VPN Client can use. Refer to the section [Specific characteristics of Stormshield SSL VPN clients](#) to check the compatibility of the modes with multifactor authentication.

Configuring Automatic mode

In **Automatic mode**, the SN 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 SN SSL VPN Client  icon in the Windows system tray.
2. Click on **Automatic mode** to use this mode.

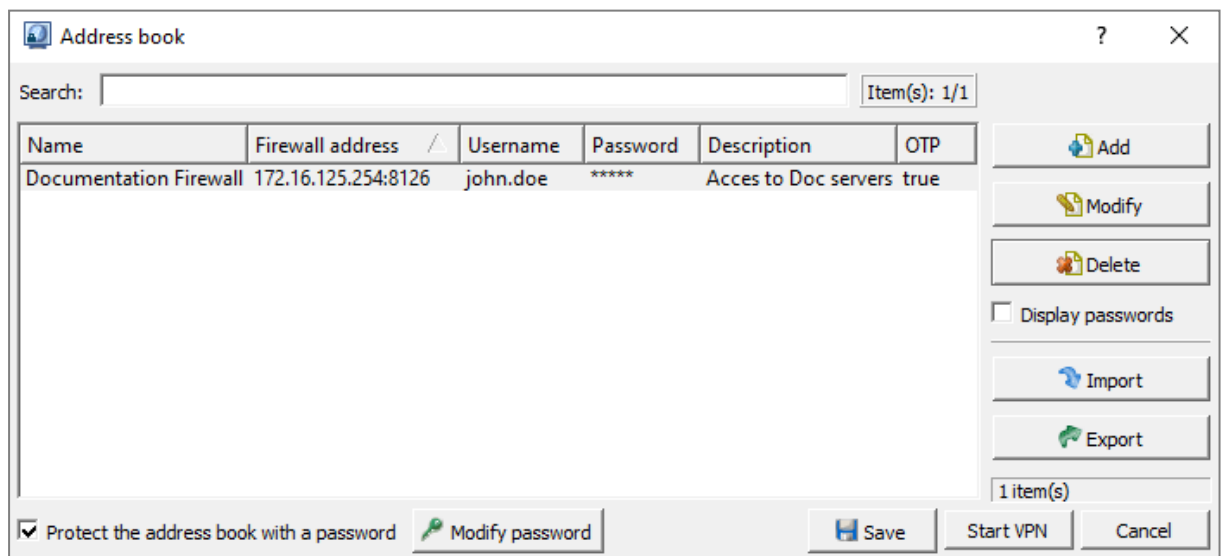
To enter connection information and set up SSL VPN tunnels, continue to the section [Setting up SSL VPN tunnels with SN SSL VPN Client](#). You can also enter connection information in the address book (see following section).

Configuring the address book (Automatic mode required)

The SN SSL VPN Client has an address book with which it memorizes addresses for the user profile (firewall address, login and password). **Automatic mode** must be enabled in order to use the address book.

Opening the address book

1. Right-click on the SN SSL VPN Client  icon in the Windows system tray.
2. Click on **Address book**.
3. If the address book is protected by a password, enter it to open the address book. If it is not, you can protect access to 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. In the **Name** field, assign a name to the address.
3. In the **Firewall address** field, indicate the IP address of the SNS firewall (IP or FQDN) to reach in order to set up the SSL 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],
4. In the **User name** field, enter the user's login.
5. In the **Password** and **Confirm** fields, enter the user's password. Leave these fields empty if an **OTP only** or **Push mode** multifactor authentication is used for the connection to the SSL VPN .
6. In the **Description** field, provide a description of the address if necessary.
7. Select **OTP** if a multifactor authentication method is used for the connection to the SSL VPN.
8. Click on **OK**.

The screenshot shows a dialog box titled "Documentation Firewall" with the following fields and values:


- Name: Documentation Firewall
- Firewall address: 172.16.125.254:8126
- Username: john.doe
- Password: [masked]
- Confirm: [masked]
- Description: Acces to Doc servers
- OTP: Enabled

Buttons for "OK" and "Cancel" are located at the bottom right of the dialog.

Once configuration is complete, go to [Setting up an SSL VPN tunnel with SN SSL VPN Client](#).

Configuring Manual mode

In manual mode, import the configuration components (CA, certificate, private key, etc.) that the SN SSL VPN Client must use, compiled in an *.ovpn* file. **Automatic mode** must be disabled order to use this mode.

1. To retrieve the *.ovpn* file:
 - **From the captive portal of the SNS firewall that hosts the SSL VPN service.**
Authenticate on `https://firewall_IPaddress/auth`, and in the **Personal data** tab, click on **SSL VPN profile for mobile OpenVPN Connect clients (single .ovpn file)**.
 - **From the SNS firewall's administration interface.**
Go to **Configuration > VPN > SSL VPN > Advanced configuration**, and click on **Export the configuration file**.
2. Right-click on the SN SSL VPN Client  icon in the Windows system tray and click on **Manual mode > Add a profile**.
3. Select the *.ovpn* file.
4. Assign a name to the connection profile.
5. Click on **OK**.

Once configuration is complete, go to [Setting up an SSL VPN tunnel with SN SSL VPN Client](#).



Installing and configuring OpenVPN Connect

Installing OpenVPN Connect

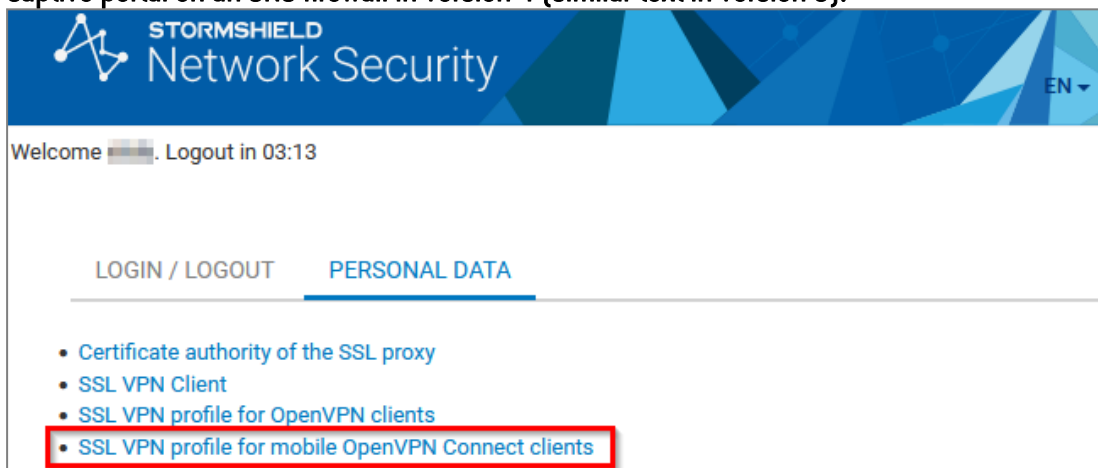
- On a workstation: download the application from the [OpenVPN website](#) and install it,
- On a mobile device: install the application from the *Google Play Store* or the *App Store*.

Configuring OpenVPN Connect

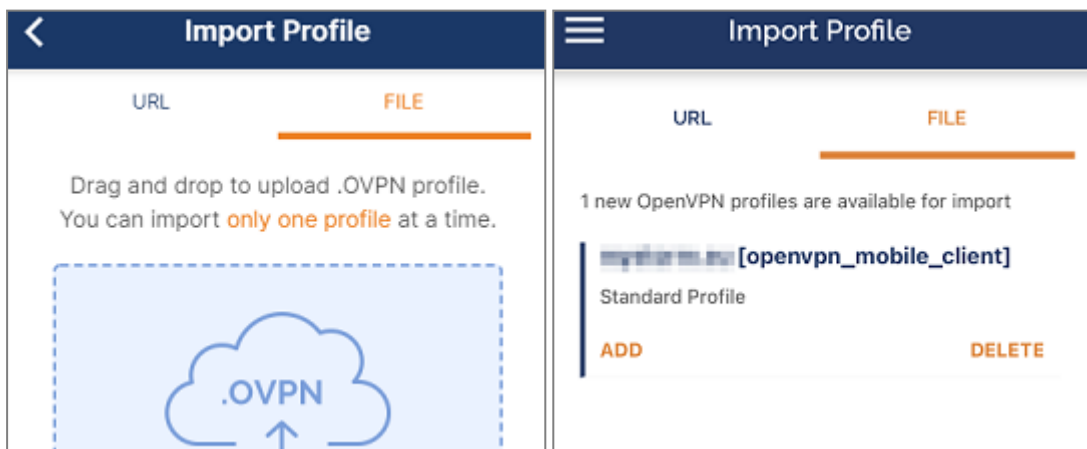
This operation must be performed during the initial connection, or when the SSL VPN configuration of the SNS firewall is modified, e.g., after a certificate is changed.

1. On your device, authenticate on https://firewall_IPAddress/auth, and in the **Personal data** a b, click on or press **SSL VPN profile for mobile OpenVPN Connect clients (single .ovpn file)**.

Captive portal on an SNS firewall in version 4 (similar text in version 3).



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. Refer to the [OpenVPN website](#) for help whenever necessary.

Once configuration is complete, go to [Setting up an SSL VPN tunnel with OpenVPN Connect](#).




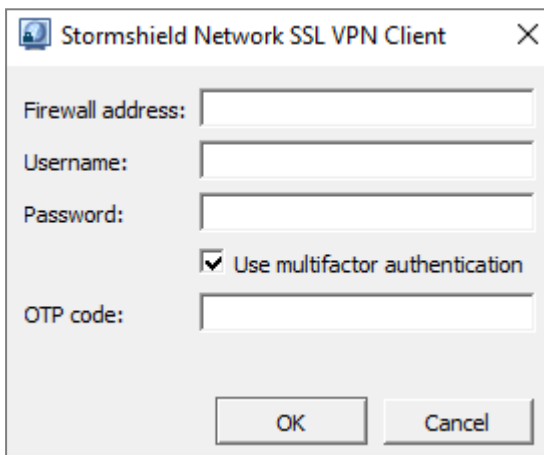
Setting up an SSL VPN tunnel

Now that the SNS firewall and SSL VPN client are configured, you can proceed to setting up an SSL VPN tunnel.

Setting up SSL VPN tunnels with SN SSL VPN Client


Connecting SSL VPN tunnels in Automatic mode

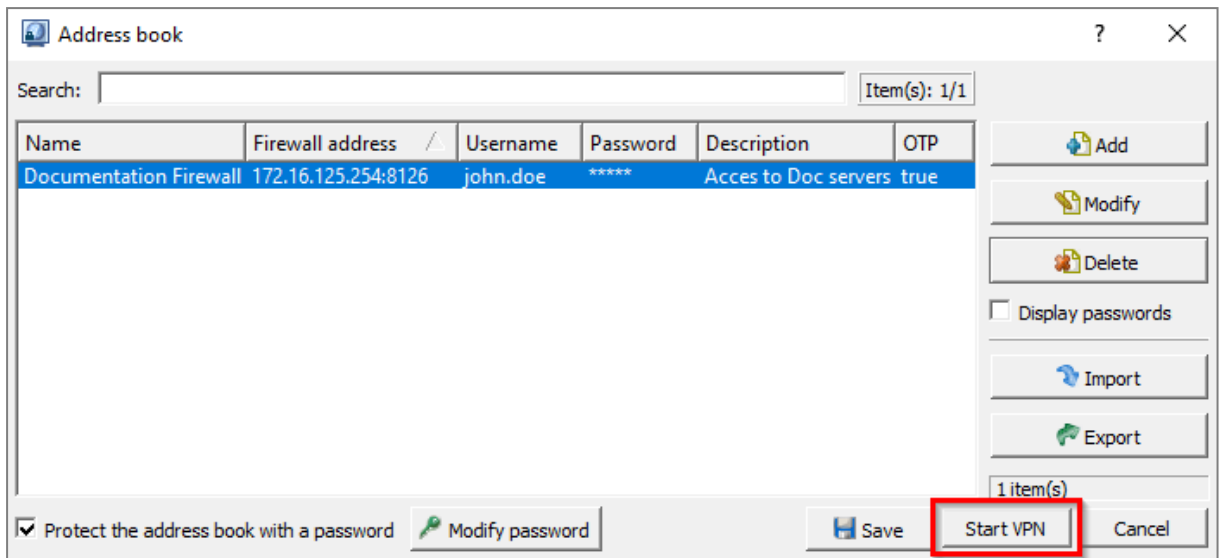
1. Double-click on the SN SSL VPN Client  icon in the Windows system tray to open the connection window.



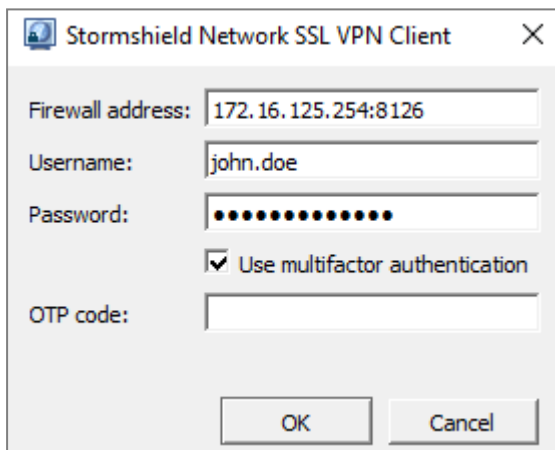
2. In the **Firewall address** field, indicate the IP address of the SNS firewall (IP or FQDN) to reach in order to set up the SSL VPN tunnel. If the port of the firewall's captive portal is different from the default port (TCP/443), enter the address and listening port separated by colons (address:port),
3. In the **User name** field, enter the user's login.
4. In the **Password** field, enter the user's password. Leave this field empty if an **OTP only** or **Push mode** multifactor authentication is used for the connection to the SSL VPN .
5. Select **Use multifactor authentication** if a multifactor authentication method is used for the connection to the SSL VPN .
6. In the **OTP code** field (which appears if **Use multifactor authentication** is selected), enter a one-time password, unless a Push mode multifactor authentication method has been used for the connection to the SSL VPN .
7. Click on **OK**. The SN SSL VPN Client authenticates on the SNS firewall. If the authentication is unsuccessful, check the connection information, or whether the OTP has expired (if entered).

Connecting SSL VPN tunnels by using the address book

1. Right-click on the SN SSL VPN Client  icon in the Windows system tray, then click on **Address book** to open it. **Automatic mode** must be enabled in order to use the address book.
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 **Connect**.




4. If a multifactor authentication method (OTP) is used for the connection to this address, enter a one-time password in the **OTP code** field. Leave this field empty if a **Push mode** method is used. Click on **OK**.



5. The SN SSL VPN Client authenticates on the SNS firewall. If the authentication is unsuccessful, check the address information, or whether the OTP has expired (if entered).

Connecting SSL VPN tunnels in Manual mode

1. Right-click on the SN SSL VPN Client  icon in the Windows system tray, click on **Manual mode** and on the profile on which you are connecting.








2. In the **User name** field, enter the user's login.
3. In the **Password** field, enter the user's password. Leave this field empty if an **OTP only** or **Push mode** multifactor authentication is used for the connection to the SSL VPN .
4. Select **Use multifactor authentication** if a multifactor authentication method is used for the connection to the SSL VPN .
5. In the **OTP code** field (which appears if **Use multifactor authentication** is selected), enter a one-time password, unless a Push mode multifactor authentication method has been used for the connection to the SSL VPN .
6. Click on **OK**. The SN SSL VPN Client authenticates on the SNS firewall based on the information entered in the connection window and the profile settings. If the authentication is unsuccessful, check the connection information, or whether the OTP has expired (if entered).

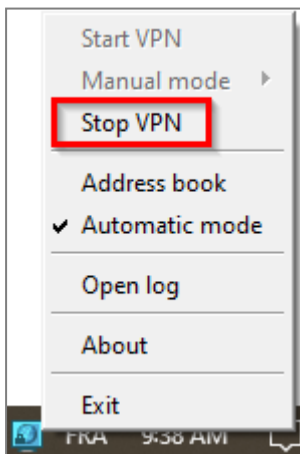
Showing the connection information of SSL VPN tunnels

The color of the icon representing the SN SSL VPN Client indicates its connection status.

	The SN SSL VPN 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 SN SSL VPN Client is in the process of connecting.
	The SN SSL VPN Client is not connected or a connection attempt failed.

Disconnecting SSL VPN tunnels

1. Right-click on the SN SSL VPN Client  icon in the Windows system tray.
2. Click on **Stop VPN**.

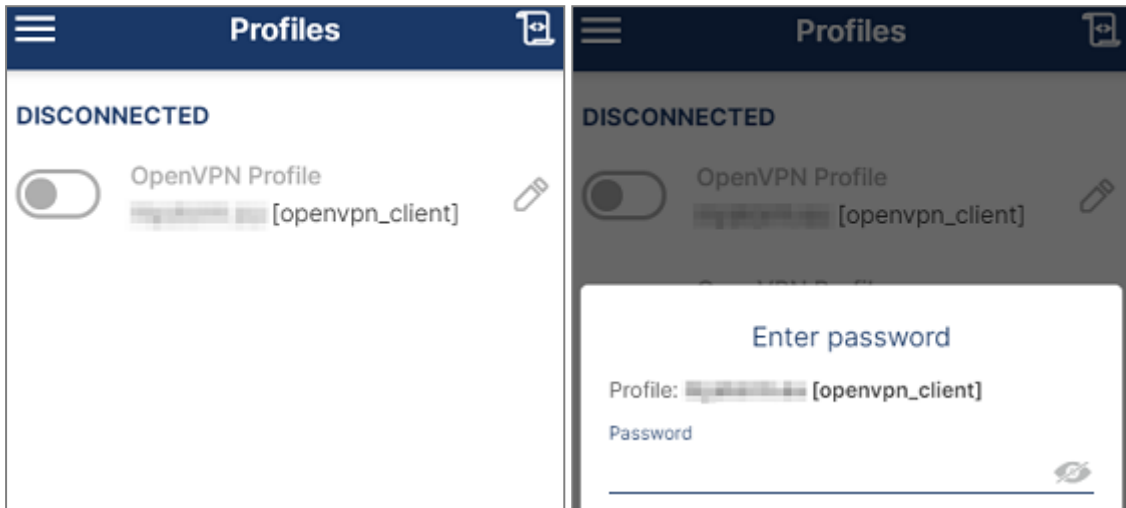




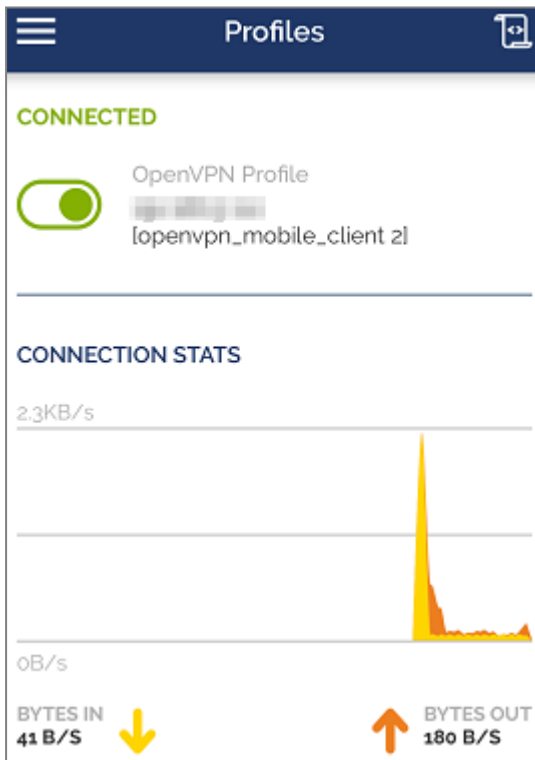
Setting up an SSL VPN tunnel with OpenVPN Connect

Connecting SSL VPN tunnels

1. Run the OpenVPN Connect program or application.
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 logs

In the SNS firewall's administration interface

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** in SNS version 4 or on **Restricted access to logs** in SNS version 3 in the upper banner. For further information, refer to the technical note [Complying with privacy regulations](#).

In SNSversion 4.x

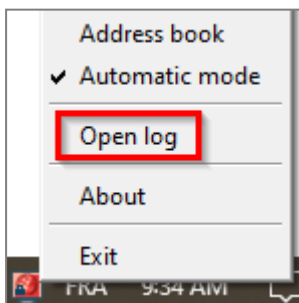
- In **Monitoring > Logs - Audit logs > VPN**, this log shows information relating to the various types of VPN tunnels (SSL or IPsec),
- In **Monitoring > Monitoring > Users**, this log shows events relating in particular to authentication via SSL VPN tunnels. You can filter the contents of logs by *Open VPN* authentication to display them,
- In **Monitoring > Monitoring > SSL VPN tunnels**, this log shows information regarding the sessions of users currently connected via SSL VPN tunnels.

In SNSversion 3.x

- In **Logs - Audit logs > Views > VPN**, this log shows information relating to the various types of VPN tunnels (SSL or IPsec),
- In **Audit logs > Logs > SSL VPN**, this log shows events, i.e., when users authenticate, or when SSL VPN tunnels are created and deleted,
- In **Monitoring > Users**, this log shows events relating in particular to authentication via SSL VPN tunnels. You can filter the contents of logs by *Open VPN* authentication to display them,
- In **Monitoring > SSL VPN tunnels**, this log shows information regarding the sessions of users currently connected via SSL VPN tunnels.

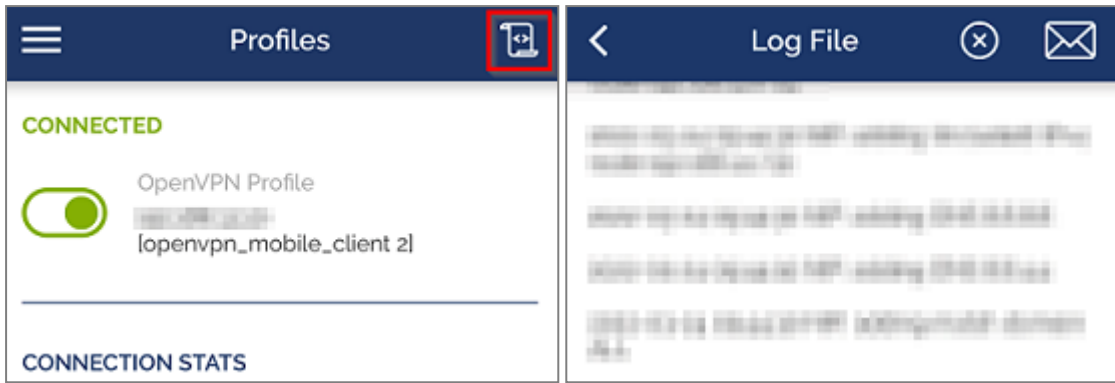
On the SN SSL VPN Client

1. Right-click on the SN SSL VPN Client  icon in the Windows system tray.
2. Click on **Logs**.



On OpenVPN Connect

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.





Troubleshooting

In this chapter, you will see some of the issues that occur most frequently when using the SN SSL VPN Client. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the [Stormshield knowledge base](#).

The tunnel won't set up and the message "Connecting to the local service, please wait" remains displayed.

- **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" persists.
- **Cause:** The connected user is not in the "OpenVPN Administrators" group on the workstation used.
- **Solutions:**
 - Update SN SSL VPN Client to version 3.2.3.
 - For versions lower than 3.2.3, ensure that the user belongs to the local "OpenVPN Administrators" group by executing the command `net localgroup "OpenVPN Administrators"` in the Windows command prompt. To manually add the user to the group, run `net localgroup "OpenVPN Administrators" "myuser" /add` [replace myuser with the relevant user].

The tunnel won't set up and 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 won't 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.

The tunnel won't set up and 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 tunnel won't set up and 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 VPN Service** is not running or is not working.
- **Solution:** Check that the Windows **Stormshield SSL VPN Service** has been started on the workstation. You can also try to restart the service.



The tunnel won't set up and 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, ensure that the filter rules enable access to the resource and that there is no record of any traffic being blocked in the logs (in **Monitoring > Logs - Audit logs > Filtering** for SNS 4.x versions or in **Audit logs > Logs > Filtering** for SNS 3.x versions),
 - Ensure that the requested resource is in fact physically available.
 - Clear the machine's ARP cache by typing 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.



Further reading

Additional information and responses to questions you may have about the SSL VPN 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 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.