STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

RELEASE NOTES

Version 5

Document last updated: October 22, 2025

Reference: sns-en-ssl_vpn_client_release_notes-v5.1.2

Table of contents

In the documentation, Stormshield Network SSL VPN Client is named "Stormshield SSL VPN client". Stormshield Network Security is referred under the short form "SNS".

This document is not exhaustive and minor changes may have been included in this version.

Change log

Date	Description
October 22, 2025	New document

New Stormshield SSL VPN client behavior

This section lists the changes made to the automatic behavior of the Stormshield SSL VPN client when it is updated from the latest 4 version available to version 5.1.2.

Changes introduced in version 5.1.1 EA

Find out more

- Available languages - The Stormshield SSL VPN client is available in French and English. It is no longer available in German.
- Obsolete certificates - SHA-1 and MD5 are no longer supported on the Stormshield SSL VPN client. In the SSL VPN configuration on the SNS firewall, if you are using a certificate that was signed with an algorithm that is no longer supported, you will need to change it.

  This regards certificates for the SSL VPN service, and if you are using Stormshield SSL VPN clients that have been configured in **Stormshield mode** (formerly Automatic mode), this also concerns the captive portal's certificate. You can check the signature algorithm of your certificates in the SNS firewall web administration interface, in **Certificates and PKI**.

  If you need to change:

  - Certificates for the SSL VPN service, refer to the section Configuring the SSL VPN service in the *SSL VPN administration guide*. To update SSL VPN certificates that are generated by default on the SNS firewall, refer to the Stormshield knowledge base article How can I regenerate the sslvpn-full-default-authority?.
  - The certificate of the captive portal, refer to the section Customizing the captive portal certificate in the *SSL VPN administration guide*.
- Certificates - During the initial connection, some users will need to indicate once again that the SNS firewall certificate has to be trusted.
- Manual mode/Imported OVPN files - A new method of importing OVPN files is now available. During an update from version 4 or lower to version 5, older imported OVPN files will not be retrieved. You therefore need to import them again after the update is complete.
- Address book/Saved connections - The "**Address book**" is now named "**Saved connections**". During an update from version 4 or lower to version 5, address book entries are added to saved connections, either automatically, or by entering the address book password the first time that the Stormshield SSL VPN client starts up, if the address book is protected. The original address book is not modified, and will be kept at its original location.
- Update from a version lower than version 5 - The version 5 installation program no longer manages the uninstallation of version 3 and lower versions. During an update from one of these versions, you need to uninstall the original version in advance, before installing version 5.
- The Stormshield SSL VPN client's traffic is now initiated by a service account. If a hardened configuration is used on workstations (e.g., when a firewall is used), the Stormshield SSL VPN client must be able to contact the following ports to set up SSL VPN connections. As the listed ports are from a default configuration, adapt them if necessary.

Source	Destination	Protocol/Port (default)	Purpose of the connection
Client (SSLVPNService) **Stormshield mode only**	OpenVPN gateway on the SNS firewall	TCP/443 (captive portal)	Retrieve SSL VPN configuration and send information to the SNS firewall to verify the compliance of the client workstation (ZTNA).
Client (OpenVPN)	OpenVPN gateway on the SNS firewall	UDP/1194 (SSL VPN)	Set up the SSL VPN connection
Client (OpenVPN)	OpenVPN gateway on the SNS firewall	TCP/443 (SSL VPN)	Set up the SSL VPN connection (compatibility)

New features and enhancements in version 5.1.2

Connection

Using an OTP with OpenVPN connections

An OTP can now be used to set up an OpenVPN connection (imported OVPN file) in the **Saved connections** and **Direct connection** menus.

For more information on how to set up a connection with the Stormshield VPN SSL client, or to manage saved connections, refer to the Stormshield SSL VPN client v5 user and configuration guide.

Configuring the client in command line interface

Importing saved connections

Saved connections can now be imported into the Stormshield SSL VPN client, by using the new CLI command "*import-addressbook*".

For more information, refer to the section Configuring the Stormshield SSL VPN client through a command line interface in the *Stormshield SSL VPN client v5 user and configuration guide*.

Compatibility

New compatibility with macOS

The Stormshield SSL VPN client in version 5.1.2 can be installed in macOS Tahoe 26 (arm64) M1 and subsequent models.

To find out which operating systems are compatible, refer to the section SSL VPN Client in the *Network Security & Tools product life cycle* document, which is the reference page for compatibility with the Stormshield SSL VPN client.

Version 5.1.2 bug fixes

Migration of address book entries to saved connections

When an SNS firewall is updated from version 4 or lower to version 5.1.2, the custom port for address book entries (server:port) is now correctly converted in saved connections.

If there are still wrongly converted custom ports in saved connections after the update to version 5.1.1 EA, they will be automatically fixed during the update to version 5.1.2.

Communication with the SNS firewall

In some Windows environments, the Stormshield SSL VPN client in version 5.1.1 EA was unable to communicate with the SNS firewall, as its captive portal certificate had not been presented to the user. This issue has been fixed.

Multifactor authentication through a third-party application

Multifactor authentication through a third-party application that has been installed on a trusted device, and used with Trustbuilder (formerly inWebo) for example, now functions with version 5.1.2 of the Stormshield SSL VPN client. With this solution, users can now approve the setup of a connection by using a push notification on their devices, or by generating an OTP.

Compatibility

For more information, refer to the section SSL VPN Client in the *Network Security & Tools Product Life Cycle document*.

Known issues

The updated list of known issues relating to this version of SN SSL VPN Client can be found in the Stormshield Knowledge base. To log in to the Knowledge base, use the same credentials as for your MyStormshield client area.

Limitations and explanations on usage

This section lists the limitations and explanations on usage with the Stormshield SSL VPN client.

Installation

Installing version 5 in Windows when it is blocked by a previous version 3

When attempts to install version 5 of the Stormshield SSL VPN client are blocked due to a prior version 3, even if it has been uninstalled, you will need to use a script provided by Stormshield to clean up residual registry keys and files that were not correctly deleted by the version 3 uninstaller.

For more information, refer to the article **Unable to install SSL VPN Client v5 on Windows due to previous v3 installation** in the Stormshield knowledge base.

Multi-account installation under Linux and macOS

We recommend that individual users who share a Linux or macOS workstation with other users ensure that they shut down their SSL VPN connection after each use on the workstation.

Connection

Verifying Windows client workstations (ZTNA) - Firewall and antivirus

When client workstation verification (ZTNA) is enabled on the SNS firewall, and at least one of the criteria "**Client workstation antivirus enabled and up to date**" or "**Active firewall on the client workstation**" is selected, users have to wait for several minutes after opening their Windows sessions before they can set up a connection with the Stormshield VPN SSL client.

This is because the Windows service that checks the status of the antivirus and Windows firewall takes several minutes to start up after a session is opened. As long as this service has not started up, the Stormshield SSL VPN client will not be able to check the status of these criteria. The SNS firewall will then refuse to set up the connection because the workstation is considered non-compliant.

Certificates signed with SHA-1

When the OpenVPN gateway (e.g., the SNS firewall) presents a certificate that is signed with SHA-1, an error message appears in the Stormshield SSL VPN Client connection window, prompting you to check the credentials used to connect. Ignore the reason given in the message: the connection failed because SHA-1 is no longer supported on the Stormshield SSL VPN client.

Single sign-on - Minimum authentication duration allowed on the SNS firewall captive portal

When single sign-on is used to set up SSL VPN tunnels with the SNS firewall, we advise against configuring the allowed minimum authentication duration below 15 minutes (default value). This value can be configured in **Authentication > Captive portal profiles** on the SNS firewall.

If you choose to lower the duration anyway, indicate to users that they must not select a value lower than or equal to 5 minutes in the "**Authentication duration**" field on the captive portal, as the Stormshield SSL VPN client would need more time to set up the connection. The Stormshield

SSL VPN client cannot set up a connection if the authentication duration chosen by the user is lower than or equal to 5 minutes.

Usage

DCO feature on SNS v5 firewalls

The table below indicates whether Stormshield SSL VPN clients in Windows, Linux and macOS are eligible to benefit from enhancements to the DCO feature on SNS v5 firewalls.

Stormshield SSL VPN client in	DCO feature on SNS v5 firewalls
Windows	✅ Benefits from enhancements to the DCO feature
Linux	✅ Benefits from enhancements to the DCO feature, only if both of these conditions are met: • OpenVPN is in version 2.6.0 or higher, • The **openvpn-dco** package has been installed.
macOS	❌ Does not benefit from enhancements to the DCO feature

For more information on the DCO feature, refer to the section Configuring the SSL VPN service in the *SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients*.

Documentation resources

Technical documentation resources are available on the Stormshield technical documentation website. We recommend that you rely on these resources to get the best results from all features in this version.

Please refer to the Stormshield Knowledge base for specific technical information that the TAC (Technical Assistance Center) has created.

Installing this version

To install or update the Stormshield SSL VPN client, refer to the **Stormshield SSL VPN client v5 installation guide**.

Previous versions of SN SSL VPN Client v5

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of SN SSL VPN Client v5.

5.1.1 EA	New features

New features and enhancements in version 5.1.1 EA

New graphical user interface and enhanced user experience

The Stormshield VPN SSL client version 5 graphical interface has been redesigned, and user experience has been enhanced:

- "**Automatic mode**" is now known as "**Stormshield mode**". This mode allows the Stormshield SSL VPN client to automatically retrieve a connection's SSL VPN configuration over the SNS firewall, and to send information that enables the firewall to verify the client workstation's compliance (ZTNA).
- The "**Address book**" is now named "**Saved connections**".
  - You can save connections here, either by entering information of the SNS firewall in "**Stormshield Mode**", or by importing an OVPN file.
  - You can mark each connection as a favorite. The list of favorite connections is accessible via the Stormshield SSL VPN client graphical interface, and through the pop-up menu of the Stormshield SSL VPN client icon.
  - You can enable an option to automatically set up the SSL VPN connection of your choice each time the Stormshield SSL VPN Client is opened. However, a manual action is still required if the access to saved connections is password-protected, or if an OTP code must be entered.
- A new menu named "**Direct connection**" makes it possible to connect via SSL VPN without having to save a connection in the Stormshield SSL VPN client. In this menu, "**Stormshield mode**" and the OVPN file import feature can be used.
- A new menu named "**Connection logs**" makes it possible to look up connection events on the Stormshield SSL VPN client, such as "*Connection established*", "*Connection lost*", "*Server unreachable*", etc.
- The pop-up menu of the Stormshield SSL VPN client icon has been redesigned. In this menu, you can display the last connection used, or the list of favorite connections, and set up SSL VPN connections by clicking on the desired connection.

For more information, refer to the Stormshield SSL VPN client v5 user and configuration guide.

Extended compatibility

The Stormshield SSL VPN client in version 5.1.1 EA can be installed on the following operating systems:

- Windows: Windows 10 (x64) and Windows 11 (x64).
- Linux:
  - Ubuntu Desktop 22.04 LTS (amd64) and Ubuntu Desktop 24.04 LTS (amd64),
  - RHEL 8 (amd64) and RHEL 9 (amd64). The Stormshield SSL VPN client in RHEL 8 requires the installation of an OpenVPN package in at least version 2.5.
- macOS: macOS Sonoma 14 (arm64) M1 and later models, and macOS Sequoia 15 (arm64) M1 and later models.

This list may change over time, depending on the life cycle of the above operating systems, and the versions mentioned. Always refer to the SSL VPN Client section of the *Network Security*

& Tools product life cycle document, which is the reference page for compatibility with the Stormshield SSL VPN client.

Single sign-on support

Single sign-on is supported as of version 5 of the Stormshield SSL VPN client. This allows users to authenticate over an authentication portal, and allows them to set up SSL VPN connections with a compatible SNS firewall.

Users can authenticate:

- Either over the SNS firewall's captive portal, for example with their Active Directory identity and password,
- Or over the authentication portal of an identity-as-a-service (IDaaS) platform like Microsoft Entra ID solution.

For single sign-on to function:

- The Stormshield SSL VPN client must be configured to use this connection mode by selecting the **Connect with single sign-on** checkbox in a connection's settings or in the **Direct connection** menu. For more information, refer to the Stormshield SSL VPN client v5 user and configuration guide.
- The SNS firewall used for the connection must be version 5.0.1 or higher.
- For authentication using the OIDC/Microsoft Entra ID method, the method must be enabled and configured on the SNS firewall. For more information, refer to the technical note Configuring OIDC/Microsoft Entra ID authentication.

New organization of Stormshield SSL VPN client documentation

Stormshield SSL VPN client documentation is now split up into two guides:

- Stormshield SSL VPN client v5 installation guide,
- Stormshield SSL VPN client v5 user and configuration guide.

Previously, a single document explaining installation, configuration and the use of the Stormshield SSL VPN Client was available.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/

All requests to technical support must be submitted through the incident manager in the MyStormshield client area, under **Technical support** > **Manage cases**.

- +33 (0) 9 69 329 129

In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on MyStormshield.

STORMSHIELD