



STORMSHIELD

BETA – VPN SSL 5.1.0

BETA version presentation



Table of contents

1	Using the BETA version	3
2	Where to find the BETA version files?	3
3	What information should we report and how?	3
4	Main features of VPN SSL 5.1.0	4
4.1	Key features.....	4
4.2	Key points of the agent's operation	6
4.2.1	v4 address book recovery logic.....	6
4.2.2	Certificate validation (« Stormshield » mode, formerly « automatic » mode)	6
4.2.3	Other new features.....	6
5	Installation.....	7
5.1	Windows	7
5.2	Linux.....	7
5.3	MacOS.....	8
6	Known limitations and ongoing improvements	9
7	Vulnerabilities	9

Thank you for participating in this BETA program of VPN SSL version 5.1.0.

Your feedback will be invaluable in ensuring the release of an official version that meets the expectations of our users.

This document aims to guide you through this BETA program.



STORMSHIELD

1 Using the BETA version

This BETA version is NOT intended to be used in production.

The tests you carry out on this version should be done in conditions as realistic as possible, but not come in place of your production solution!

2 Where to find the BETA version files?

You will find the different VPN SSL client installation files in the Downloads section on [MyStormshield](#).

3 What information should we report and how?

We want to know the scope of your tests: please let us know which features you used, successfully or not.

Any abnormal or suspicious behavior must be reported to us. We are also open to any suggestions for improvement.

In any case, we ask you to specify as much as possible:

- your usage context (used OS, firewall model concerned, HA cluster...),
- the elements that can help us understand your feedback: screenshot, short video, logs...

For any operational issue, open a ticket with our technical support.

For any other feedback (improvement track, test scope feedback, graphic bug...), send a message to beta@stormshield.eu.



4 Main features of VPN SSL 5.1.0

This version of the VPN SSL client is an evolution of the Stormshield VPN SSL client with 3 major developments:

1. 1. An updated graphical interface,
2. 2. Compatibility with the 3 main laptop operating systems (Windows, MAC, Linux)
3. 3. Support for a new authentication mode via the web portal (which allows authentication via EntraID in particular). This new mode is available on SNS v5 versions (currently in BETA program on MyStormshield)

4.1 Key features

VPN SSL 5.1.0 is an evolution of the Stormshield VPN SSL client version 4.0, which is based on Open VPN while enriching this base with Stormshield-specific functions. In particular, here are the features that distinguish version 5.1.0:

- **SNS version compatibility**
 - Firmware version SNS 4.3.35 or higher
- **Multi-platform compatibility**
 - Windows 10 / 11
Note: installation is intentionally blocked on Windows server
 - Linux (x86-64)
 - Ubuntu 22.04 / 24.04
 - Red Hat RHEL 8 and RHEL 9
 - MacOS 14/15 ARM only
- Installation / lifecycle using **native tools for each environment** (.msi under Windows, .deb / .rpm for Linux, and .pkg for MacOS)
- **Command line interface** available to start / stop / monitor the status of a tunnel, as well as to import / export a list of registered connections
- Operation in **multi-user mode**:
 - A global "post" installation
 - Each user has their own configuration (see below, address book in particular)



STORMSHIELD

- Only the active user can establish a tunnel
 - ⚠ The concept of active user only exists under Windows
- The tunnel is automatically stopped if there is a change in the active user (Windows only)
- The tunnel is automatically stopped when the agent GUI is shut down

- **VPN SSL tunnel configuration**

- "OVPN" mode (manual mode in v4), by importing a .ovpn file
- "Stormshield" mode (automatic mode in v4)
 - Support for Hostcheck / ZTNA (from SNSv4.8)
 - ZTNA scope on Windows equivalent to that of the v4.0 agent
 - Minimal ZTNA scope under Linux / Mac (agent and OS version)
 - Automatic switching to "legacy" mode if the SNS does not support Hostcheck mode
 - Support for TOTP
 - Support for SNSv5 Web Portal Authentication mode

- **Address book**

- Entries of type "Stormshield", with all possible options for this mode (Portal authentication, TOTP, password provided or not, etc.)
 - Entries of type "OVPN"
 - Possibility to configure favorites
 - Possibility to select an entry to mount automatically at agent GUI startup
- Possibility to mount a tunnel in direct connection (without having to create an entry in the address book)



STORMSHIELD

4.2 Key points of the agent's operation

The v5 agent is designed to be used mainly through the systray quick menu, with the last used connection or a recorded and favorite connection.

4.2.1 v4 address book recovery logic

- When starting the v5 agent (frontend), if there is a v5 address book, it is used
- Otherwise, if there is a v4 (or v3) address book, its information is imported into the v5 address book
⚠ As a result, if your account has a v3/v4 address book, but it is password-protected, this password is requested during the first start of the v5 agent!
- The old address book is neither modified nor deleted during this process, nor during the subsequent use of the v5 agent.

4.2.2 Certificate validation (« Stormshield » mode, formerly « automatic » mode)

- When a certificate is accepted, the information (and the certificate fingerprint) is linked to the address book entry (the direct connection is viewed as an address book entry in this case), and is therefore specific to this entry.
- When a certificate is displayed for validation (or not), its complete certification chain is displayed

4.2.3 Other new features

Production events ("tunnel established", etc.) are now in the agent interface, in "event logs", instead of being reported through system events



5 Installation

5.1 Windows

The agent is supported on Windows 10 and Windows 11 systems, in x86_64 version.

Installation is done in a classic way, via the provided .msi file.

There are 2 versions of the .msi file: Fr and En. The language difference only affects the agent's installation screens.

5.2 Linux

The agent is supported on Ubuntu distributions (22.04 and 24.04) as well as on RedHat Enterprise Linux distributions (RHEL, latest v8 and latest v9).

In all cases, the x86_64 architecture is supported.

In both cases, a native package for the distribution is provided (a .deb for Ubuntu, a .rpm for RHEL), and is installed via the usual platform tools.

Note: the package has dependencies, so it is preferable, under Ubuntu, to install it via a method that will automatically manage these dependencies, for example:

```
$ sudo apt install ./stormshield-sslvpnagent-5.1.0.deb
```

Under RHEL, the dnf installation command provides dependency management:

```
$ sudo dnf install ./stormshield-sslvpnagent-5.1.0.rpm
```

Note: Both apt and dnf tools require providing a file path for the package (here "./", assuming the package is available in the current directory).

Under RHEL9, the "openvpn" dependency is not available by default. The simplest way to provide it is to enable the EPEL repository ("Extra Packages for Enterprise Linux"), via the following commands:

```
$ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
$ sudo dnf update -y
```

Depending on the desktop environment and its configuration, it may be necessary to add packages or enable options to have "systray" icon support.

For example, under RHEL in the default environment, you need to install and enable such a package, such as gnome-shell-extension-appindicator.

⚠ If your OpenVPN gateway provides a specific DNS configuration to use, it is not natively taken into account by OpenVPN in the Linux environment.



STORMSHIELD

It is then necessary to provide a local script that will perform the required manipulations, depending on the distribution and local DNS configuration (daemon and configuration used, etc.).

The connection / disconnection scripts are to be placed in the following locations:

```
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh
```

```
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

For example, under Ubuntu 22.04 / 24.04, which uses systemd-resolver in its default configuration, such a script is provided by the openvpn-systemd-resolved package, and is deployed to the location /etc/openvpn/update-systemd-resolved.

It can therefore be set up via the following commands:

```
$ sudo apt install openvpn-systemd-resolved
```

```
$ sudo ln -s /etc/openvpn/update-systemd-resolved  
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh
```

```
$ sudo ln -s /etc/openvpn/update-systemd-resolved  
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

5.3 MacOS

The installation is done via the .pkg file (stormshield-sslvpnclient-arm64-X.X.X.X.pkg).

The application is installed in the usual way under /Applications/Stormshield/SSL\ VPN\ Client.app/.

Uninstallation can be done by putting "SSL VPN Client.app" in the trash from the Finder's Applications menu.

No uninstaller is currently available: a traditional MacOS uninstallation will keep the files installed elsewhere than in the .app.

⚠ If your OpenVPN gateway provides a specific DNS configuration to use, it is not taken into account natively by OpenVPN in the MacOS environment (see for example <https://forums.openvpn.net/viewtopic.php?t=34612>)

It is then necessary to provide a local script that will perform the required manipulations, such as <https://github.com/andrewgdotcom/openvpn-mac-dns>.

The connection/disconnection scripts are to be placed in the following locations:

```
/Applications/Stormshield/SSL\ VPN\ Client.app/Contents/MacOS/Modules/ssl-  
vpn/etc/sslvpn_connect.sh
```

```
/Applications/Stormshield/SSL\ VPN\ Client.app/Contents/MacOS/Modules/ssl-  
vpn/etc/sslvpn_disconnect.sh
```




STORMSHIELD

6 Known limitations and ongoing improvements

The following points are currently being corrected/improved for a future version:

- No default values at agent installation (agent v4 feature)
However, it is possible to deploy an address book after agent installation via the cli command provided with the agent.
- Partial support for "push" / "inwebo" modes
- Does not work with an SNS version prior to 4.3.35
- Under Windows, agent deployment via GPO may fail or perform a non-functional installation in some cases.
- Under Windows, installation is currently not blocked on an unsupported version (version prior to Windows 10 or Windows Server version). However, proper functioning of the agent in these conditions is not guaranteed.
- Under Linux, the agent depends on an OpenVPN package provided by the environment. There is no official repository to provide this package in the required minimum version (2.5.0) on RHEL8.
- Portal Authentication mode support is currently disabled on the Mac version.
- A registered connection of type "OVPN" requires the registration of the identifier and password to be functional.
- If a tunnel was active when the computer went to sleep, the agent's behavior when exiting sleep mode is not always nominal.
- If the screen resolution is low, or if a global display ratio is applied, the location and size of the agent screens are not optimal.
- In rare cases, it may be necessary to stop and restart the tunnel manually (especially in TOTP mode).
- On Linux and Mac environments, it is necessary to stop the IHM manually before performing the update.

7 Vulnerabilities

As this is a BETA version, this version has not finalized quality and security testing and may contain vulnerabilities.

It should therefore not be used in production, and corrections of these possible vulnerabilities will not be declared in CVE.



STORMSHIELD

Thank you

www.stormshield.com