STORMSHIELD

# STORMSHIELD NETWORK SECURITY

## STORMSHIELD IPSEC VPN CLIENT

# RELEASE NOTES

Version 1

Document last updated: April 22, 2026

Reference: sns-en-ipsec_vpn_client_release_notes-v1.0

# Table of contents



In the documentation, "Stormshield Network Security" is referred to in its short form "SNS".

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

# Change log

| Date | Description |
| --- | --- |
| April 22, 2026 | New document |

# Main features on the Stormshield IPsec VPN Client 1.0

The Stormshield IPsec VPN client allows users to connect securely to the corporate network. Depending on whether you have an Essential or Premium license, you gain access to additional advanced features that will improve your administrators' and users' experience.

## Compatibility and interoperability of the Stormshield IPsec VPN client with

- Operating systems: Windows 11, version 22H2 and upwards. We recommend using Windows 11 Professional or Windows 11 Enterprise.
- SNS firewalls: in versions 4.8 LTSB and 5, either in standard IPsec or IPsec DR mode. In IPsec DR (*Diffusion Restreinte*) restricted mode, SNS firewalls must comply with ANSSI recommendations (in French).

## Features included with the Essential license

### IPsec/IKEv2 profiles

The following algorithms and cryptographic functions are managed:

| Encryption | Key exchange (Diffie-Hellman) |
|---|---|
| • AES CBC (128, 192 or 256 bits)<br>• AES CTR (128, 192 or 256 bits)<br>• AES GCM-16 (128, 192 or 256 bits) | • Group 14 (2048-bit MODP)<br>• Group 15 (3072-bit MODP)<br>• Group 16 (4096-bit MODP)<br>• Group 17 (6144-bit MODP)<br>• Group 18 (8192-bit MODP)<br>• Group 19 (256-bit ECP)<br>• Group 20 (384-bit ECP)<br>• Group 21 (521-bit ECP)<br>• Group 28 (256-bit Brainpool ECP)<br>• Group 29 (384-bit Brainpool ECP)<br>• Group 30 (512-bit Brainpool ECP) |
| **Integrity** | |
| • 256-bit SHA2<br>• 384-bit SHA2<br>• 512-bit SHA2 | |
| **PRF (Pseudo-Random Function)** | |
| • 256-bit SHA<br>• 384-bit SHA<br>• 512-bit SHA | |

### Fragmentation

IKEv2 packet fragmentation is enabled by default, with a maximum size of 1280 bytes. It is possible to change fragment size or disable fragmentation in a VPN's configuration (**Fragmentation** setting).

### NAT-T (NAT-Traversal)

NAT-T is managed, with a port that can be configured for IKE and encapsulated ESP (UDP/4500 by default). NAT-T lets the IPsec protocol pass through a network that performs dynamic address translation.

### Authentication

The following authentication methods are managed:

- User authentication via X.509 v3 certificates stored in the Windows certificate store,
- User authentication via pre-shared keys, when IPsec/IKEv2 profiles are compatible.

### Certificate revocation list verification mechanism (OCSP)

The OCSP-based certificate revocation and verification mechanism can be enabled in a VPN's configuration (**Server Revocation Check** setting).

### Graphical interface

The Stormshield IPsec VPN client is equipped with a graphical interface with which settings can be configured locally.

### VPN configuration

- With an Essential license, a single VPN configuration can be added.
- A VPN configuration can be exported from or imported into the Stormshield IPsec VPN client. The supported format is JSON. Do note that VPN configuration secrets (PSK and certificates) are not exported.
- An automatic mode (also known as "*Configuration Payloads*" in IKEv2, RFC 7296) allows the network configuration (IP address, mask, DNS servers) to be retrieved from a remote server. This network configuration can also be manually edited.

### Connection mode

The VPN tunnel has to be manually set up by the user after they have opened their Windows session. Automatic tunnel setup will be available in a future version of the Stormshield IPsec VPN client. This will require a Premium license.

### Installation

The Stormshield IPsec VPN client can be installed and updated through an MSI package:

- Either locally on a workstation, by running the MSI package,
- Or using a method managed by an administrator, with a group policy (GPO, EMM or MDM) or in command line (CLI).

For more information, refer to the Stormshield IPsec VPN Client v1 Installation and user guide (available soon in English).

### Logs

Stormshield IPsec VPN client logs can be found in the Windows Event Viewer.

### License management (beta)

The management of Stormshield IPsec VPN client licenses, which enables and tracks the number of workstations that have been activated, is currently being conducted in a beta phase. When a valid license key is missing, a warning banner will appear, but does not block operations.

### Split tunneling mechanism

Split tunneling is managed, making it possible to determine which traffic has to pass through the VPN tunnel in order to reach remote networks that are defined by IP addresses or destination subnet masks.

# Features included with the Premium license

### Features in the Essential license

All features in the Essential license are included.

### IPsec DR (*Diffusion Restreinte*) profile

An IPsec DR (*Diffusion Restreinte*) profile is suggested when a VPN configuration is added. With this profile, a VPN can be configured in line with the ANSSI's IPsec DR guidelines (in French). The following cryptographic suites are suggested:

| Suite | Encryption | Integrity | Key exchange (Diffie-Hellman) | PRF |
|---|---|---|---|---|
| 1 | 256-bit AES GCM-16 | None* | Group 19 (256-bit ECP) | 256-bit SHA |
| 2 | 256-bit AES GCM-16 | None* | Group 28 (256-bit Brainpool ECP) | 256-bit SHA |
| 3 | 256-bit AES CTR | 256-bit SHA2 | Group 19 (256-bit ECP) | 256-bit SHA |
| 4 | 256-bit AES CTR | 256-bit SHA2 | Group 28 (256-bit Brainpool ECP) | 256-bit SHA |

(*) Integrity is natively guaranteed through the GCM encryption mode.

### Multi-tunnel VPN configuration

It is possible to configure multiple VPN tunnels with the Premium license. Do note that only one VPN tunnel can be set up at a time.

### ESN negotiation

ESN negotiation (Extended Sequence Number, RFC 4304) can be enabled in a VPN's configuration (**ESN** setting). Doing so will enable the use of 64-bit anti-replay counters in IKEv2 and CHILD_SA. ESN negotiation has been designed to manage high throughput and long sessions.

### Childless IKEv2

IKEv2 initiation without CHILD_SA (RFC 6023) can be enabled in a VPN's configuration (**Childless mode** setting). Enable this setting for advanced interoperability use cases.

### Administrator-managed configuration

A third-party centralized management server can be used to batch configure a pool of Stormshield IPsec VPN clients. Do note that users will not be able to edit the settings that were retrieved from the server in their Stormshield IPsec VPN client.

# Compatibility

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

# Known issues

The updated list of known issues relating to this version of Stormshield IPsec 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.

# 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 published by the TAC (Technical Assistance Center).

# Installing this version

To install or update the Stormshield IPsec VPN client, refer to the **Stormshield IPsec VPN Client v1 Installation and user guide** (available soon in English).

# 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