STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD IPSEC VPN CLIENT

RELEASE NOTES

Version 1

Document last updated: September 14, 2026

Reference: sns-en-ipsec_vpn_client_release_notes-v1.1.1

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
September 14, 2026	New document

Version 1.1.1

This section lists the latest enhancements to version 1.1.1 of the Stormshield IPsec VPN client.

Latest enhancements to Essential and Premium licenses

Network
An anomaly would occasionally prevent IPsec tunnels from being set up. This anomaly has been fixed.

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**.

Previous versions of Stormshield IPsec VPN client v1

In this section, you will find new features, resolved vulnerabilities and fixes from previous versions of Stormshield IPsec VPN client v1.

1.1.1	Open
1.0.1	Open
1.0	Open

Version 1.1

This section lists the latest enhancements to version 1.1 of the Stormshield IPsec VPN client.

Introduction of Essential and Premium licenses

Two licenses are now available for the Stormshield IPsec VPN client. 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.

List of features	Essential License	Premium License
IPsec/IKEv2 VPN		
Standard IPsec profiles	✓	✓
ANSSI IPsec DR (*Diffusion Restreinte*) Profile		✓
Multi-tunnel VPN configuration		✓
IKE fragmentation, NAT-T	✓	✓
Config mode	✓	✓
ESN negotiation	✓	✓
Childless IKEv2		✓
Certificate authentication and management		
Pre-shared key (PSK)	✓	✓
Certificate in the Windows Certificate Store	✓	✓
Certificate in a smart card or token		✓
Certificate verification and revocation (OCSP)	✓	✓
VPN tunnel launch mode		
Manual	✓	✓
Advanced network features		
Dead Peer Detection (DPD)	✓	✓
Deploying and configuring the VPN client		
Local or managed installation	✓	✓
Local configuration	✓	✓
Managed configuration (EMM/GPO)		✓
Windows event logs	✓	✓
License management		
SaaS mode with automatic release	✓	✓

Latest Essential license enhancements

License management

It is now possible to import and activate a license key from the user interface of the Stormshield IPsec VPN client or via a configuration file. License activation is done on a remote server hosted in the cloud. The user interface displays the subscribed license type (Essential or Premium) and its expiration date.

For more information, refer to the License section of the *Stormshield IPsec VPN Client v1 Installation and User Guide*.

Latest Premium license enhancements

All the latest enhancements in the Essential license are included.

User authentication by certificate

User authentication by X.509 v3 certificate stored in a smart card is now supported. For more information on the smart card references tested, refer to the Appendix section of the *Stormshield IPsec VPN Client v1 Installation and User Guide*.

Managed configuration – Select certificate

The administrator can now simplify the selection of the user certificate by filtering on one or more criteria defined in the *.json* configuration file. For more information, refer to the Setting up a secure connection section in the *Stormshield IPsec VPN Client v1 Installation and User Guide*.

Version 1.0.1

This section lists the latest enhancements to version 1.0.1 of the Stormshield IPsec VPN client.

Using the VPN client

Network
VPN tunnels now automatically reconnect when they resume after an extended standby.

VPN configuration
Excess spaces in text fields in the configuration of the Stormshield IPsec VPN client are now better managed.

Graphical interface
Dark mode on the Stormshield IPsec VPN client has been enhanced.

VPN tunnel management

The IKE reauthentication and key renegotiation (*rekey*) processes have been enhanced in **Automatic** and **Manual** network configuration modes.

Security

Some internal components of the Stormshield IPsec VPN client have been upgraded.

Main features on the Stormshield IPsec VPN Client 1.0

The Stormshield IPsec VPN client allows users to connect securely to the corporate network. It includes the following features.

Compatibility and interoperability of the Stormshield IPsec VPN client with

- Operating systems: Windows 11, version 22H2 and higher. We recommend using Windows 11 Professional or Windows 11 Enterprise.
- SNS firewalls: versions 4.8 LTSB and 5, either in standard IPsec or IPsec DR (*Diffusion Restreinte*).

IPsec/IKEv2 VPN

Standard IPsec profiles

The following algorithms and cryptographic functions are managed:

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

ANSSI IPsec DR (*Diffusion Restreinte*) Profile

An IPsec DR 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

The Stormshield IPsec VPN client makes it possible to add several VPN configurations. Do note that only one VPN tunnel can be set up at a time.

IKE 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 supported 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.

Config mode

In automatic mode (also known as “Config Mode” or "*Configuration Payloads*" in IKEv2, RFC 7296) makes it possible to retrieve the network configuration (IP address, mask, DNS servers) from the remote server. This network configuration can also be manually edited.

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.

Certificate authentication and management

Pre-shared key (PSK)

User authentication by pre-shared key is supported.

Certificate stored in the Windows certificate store

User authentication via X.509 v3 certificates stored in the Windows certificate store is supported.

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).

VPN tunnel launch mode

Manual

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.

Deploying and configuring the VPN client

Local or managed installation

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.

Local or managed configuration

- Stormshield IPsec VPN client can be configured locally on a workstation by adding VPN configurations via the GUI.
- VPN configurations 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.
- A pool of Stormshield IPsec VPN clients can be configured in a managed manner with a group policy (GPO, EMM or MDM). Note that users will not be able to edit the settings that were retrieved from the server in their Stormshield IPsec VPN client.

Logs

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

Advanced network features

Split tunneling mechanism

The *split tunneling* mechanism is supported. It makes 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.

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