STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

RELEASE NOTES

Version 7

Document last updated: February 21, 2023

Reference: sns-en-vpn_client-exclusive-release_notes-v7.3

Table of contents

In the documentation, Stormshield Network VPN Client Exclusive is referred to in its short form: SN VPN Client Exclusive and Stormshield Network Security under the short form SNS.

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

Compatibility

Stormshield Network Firewall

3.7, 3.11 and 4.x

Operating systems

Windows 10 - 64 bits
Windows 11 - 64 bits

NOTE
SN VPN Client Exclusive is not compatible with computers, smartphones and tablets equipped with ARM processors.

ANSSI *Diffusion Restreinte* (DR) mode on SNS firewalls

SN VPN Client Exclusive version 7.3.007 is compatible with ANSSI *Diffusion Restreinte* (DR) mode in SNS 4.3.12 versions upwards.

Compatibility of configuration files

VPN configuration files from previous versions of the software cannot be imported into this version once it is installed. If a previous version of the software is already present, this installer will automatically convert the previous configuration and import it into the new software.

When upgrading from a previous version, we therefore recommend that you do not uninstall the previous version before you launch the installer.

New features and enhancements in version 7.3.007

Main features

- Adds a **Console** window to the **TrustedConnect Panel**,
- Allows a tunnel to be opened in the **TrustedConnect Panel** even if a trusted network has been detected,
- The **TrustedConnect Panel** can now be restarted automatically when the application is quit or crashes,
- CRL can now be downloaded to a cache and an expiration time can be set for the cached CRL,
- Adds a feature to filter data flows combined with captive portal detection (CPD),
- Verification of the user certificate CRL has become optional.

Enhancements

- Increases the number of subnetworks supported to 16,
- Window height of the **Connection Panel** window can now be increased or decreased,
- Supports multiple source IP addresses on network interface,
- Number of rules for Filtering mode have been increased from 12 to 30,
- *Local ID* can now be filled automatically with DNS or e-mail in addition to certificate subject,
- Passwords for encrypting exported configurations must now follow ANSSI recommendations, i.e. at least 16 characters in length and use a 90-character alphabet, including at least one uppercase character, one lowercase character, and one special character,
- VPN Client now accepts `id-kp-ipsecIKE` in *Extended Key Usage* (EKU) for gateway certificate,
- Improved support for IPsec DR gateways:
  - Child SA rekey now asks for same TS as the one in the original SA that was established,
  - NONCE size is 16 bytes when *PRF_HMAC_SHA2_256* is used.
- Improved support for tokens/smart cards:
  - PIN code entry prompt now specifies which smart card/token it concerns,
  - PKCS#11 no longer causes VPN Client to crash with CNG readers,
  - Multiple smart card tunnel is now closed for other readers.
- Greater stability of the IKE module,
- Better performance of AES-GCM encryption,
- Weak algorithms have been removed for SSL/OpenVPN: MD5, SHA1, TLS low security suite, BF-CBC.

Version 7.3.007 bug fixes

- DSCP fields are now properly handled in ESP packets that are created,
- VPN Client no longer crashes when waking up form sleep,
- Activation module now reads all `tgbcode` files and uses the one with the latest renewal date,
- Fixes an issue where the **Console** no longer recorded logs when user left workstation or locked session,
- Fixes an issue where the activation server returned an undue error message,
- Fixes an issue where tunnel would stop and the error message "unsupported payload 53 for this exchange" was displayed,
- Fixes support for press and hold right-click to open the contextual menu for Windows in tablet mode,
- Various cosmetic and stability improvements.

Limitations and explanations on usage

- USB Mode: machine-specific configuration has been disabled in this version,
- Local identification type "**ID_DER_ASN1_DN**" cannot be used along with Pre-shared keys (PSK),
- PSK authentication : Preshared password cannot contain special characters,
- If opened right after command line installation, the about window may still display "*Evaluation Mode*" when activation was done correctly,
- Scroll bar sometimes disappears in **Automation** tab,
- In some screen resolutions, the status bar of the **Configuration Panel** is not displayed the first time it is launched,
- Language settings changed in the **Configuration Panel** are not applied to the **GINA** interface,
- Uninstalling by double clicking on the MSI package is not supported,
- In SSL VPN configuration, the cipher must not be set to "auto" but has to be specifically selected within the ciphers list which is proposed,
- Setting up a mobile tunnel in standard mode (not DR) with a Certification Authority (CA) and certificates based on the Brainpool 256 algorithm does not work,
- Setting up a mobile tunnel in DR mode without using the *Config* mode (**Request configuration from the gateway** option unselected) causes the renegotiation to fail in phase 2.

Documentation resources

The technical documentation resources are available in the documentation base on the Stormshield technical documentation. We suggest that you rely on these resources for a better application of all features in this version.

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

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 7.3.007 version of SN VPN Client Exclusive:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of SN VPN Client Exclusive binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
   - Linux operating system: `sha256sum filename`
   - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on MyStormshield personal area, section **Downloads**.

Previous versions of SN VPN Client Exclusive 7

In this section, you will find the new features, resolved vulnerabilities and fixes from previous versions of SN VPN Client Exclusive 7.

7.0.115	New features

Main features of SN VPN Client Exclusive 7.0

SN VPN Client Exclusive is a VPN client solution. When it is installed on a Windows workstation, VPN tunnels can be set up with a Stormshield Network Security firewall to secure communications between remote users and a network protected by an SNS firewall.

SN VPN Client Exclusive can be installed in the following environments:

- Windows 10 64-bit,
- Windows 11 64-bit.

For more information regarding SN VPN Client Exclusive 7.0, refer to the *Administrator's guide* on Stormshield's technical documentation website.

SN VPN Client Exclusive version 7.0 is equipped with the following main features:

High level of security

The SN VPN Client Exclusive client was developed according to the recommendations set out by the NIST and ANSSI (French National Cybersecurity Agency). It factors in the authentication features available on the information system, and includes the relevant mechanisms enabling integration with existing PKIs. All the protocols and algorithms implemented in the software make it a universal client that allows you to connect to all mainstream VPN gateways, regardless of whether they are hardware-based or software-based.

GINA mode

The GINA mode allows you to open VPN connections before the Windows logon. This function can, for example, create a secure connection to an access rights management server so that the user workstation access rights can be obtained before opening a user session.

TND (Trusted Network Detection)

This feature consists in detecting whether the workstation is connected to the corporate network (trusted network) or not. When the VPN Client detects that workstation is not on the corporate network, the predefined tunnel is opened automatically.

TrustedConnect uses two methods to detect whether the workstation is on a trusted network:

- It checks whether the DNS suffixes of the network interfaces available on the workstation are part of the list of trusted DNS suffixes (list configured in the software, see below),
- Automatically accesses a trusted web server in HTTPS mode and checks that its certificate is valid.

Always-On mode

The Always-On feature always ensures that the connection remains secure whenever the network interface changes.

The following network interfaces are supported:

- Virtual adapter (e.g. vmware),
- Wi-Fi,
- Ethernet,

- USB modem (i.e. smartphone),
- Bluetooth modem (i.e. smartphone),

The following network events trigger automatic tunnel reconnection (and, where appropriate, detection of the trusted network):

- Connection to a network (APIPA addresses ignored),
- Disconnection from a network,
- An adapter changes IP address or DHCP switches to static or vice versa,
- ipconfig /release,
- ipconfig /renew,
- Switch to airplane mode.

Microsoft Windows Installer (MSI)

Administrators can take advantage of the features found in the Windows installer (MSI) to deploy and administer the SN VPN Client Exclusive client using pool and user group management tools (GPO). Apart from the silent installation, scripts, customization options and pre-configuration options such as the customization of the user interface, or the configuration of PKI features, can be fully managed from a central location.

Certificate on a smart card or token

The SN VPN Client Exclusive client implements a mechanism to automatically detect smart card insertion. Tunnels that are associated with a certificate stored on a smart card will therefore be established automatically when the smart card is inserted. Likewise, removing the smart card will close all the corresponding tunnels.

Administrator logs, console, and traces

The SN VPN Client Exclusive client offers three types of logs:

- "Administrator" logs are specifically designed for software activity and usage reports. The following actions can be performed on collected logs either exclusively or simultaneously:
  - Store in a local file,
  - Record in the Windows Event Log,
  - Send in syslog format to a Syslog server.
- The "Console" provides detailed information on the tunnels as well as the related opening and closing steps. It essentially consists of the IKE messages and provides high-level information about the establishment of the VPN tunnel. It is intended for administrators to identify possible VPN connection issues.
- The "Trace" mode makes every component of the software write an activity log about its inner workings. This mode is intended for vendor support to diagnose software issues.

Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- https://mystormshield.eu/

All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support** > **Report an incident / Follow up on an incident**.

- +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 https://mystormshield.eu.

All images in this document are for representational purposes only, actual products may differ.