STORMSHIELD

# STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

# RELEASE NOTES

Version 7

Document last updated: May 30, 2024

Reference: sns-en-vpn_client-exclusive-release_notes-v7.5

# 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.

# Change log

| Date | Description |
| --- | --- |
| May 30, 2024 | New document |

# New features and enhancements in version 7.5.007

## Enhancements

- For security reasons, PKCS#12 certificates encrypted with the RC2 algorithm can no longer be imported.

# Version 7.5.007 bug fixes

- Fixes an issue where the **Filtering Mode** could not be enabled at startup (IKESTART = 1),
- Fixes an issue where the Traffic Selectors list (*TSr*) was not properly handled when renegotiating Child SA,
- Fixes an issue where a tunnel configured with AES-CTR encryption could not be opened,
- Fixes an issue where method 14 was used instead of method 214 when a tunnel is configured with Brainpool,
- Fixes an issue where the GINA mode did not work with the **Connection Panel** once the product was activated.

# Compatibility

For more information, see the Product life cycle guide.

> **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 7.5.007 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.

# Limitations and explanations on usage

- 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,
- Mobile tunnels cannot be set up in standard mode (non-DR) with Brainpool 256-based certification authorities (CA) and certificates,
- If mobile tunnels are set up in DR mode without using *Config* mode (with the option **Request configuration from the gateway** unselected), the phase 2 renegotiation will fail,
- Tunnels cannot be set up in DR mode with Brainpool 256-based certificates in GINA mode (tunnel opened from the Windows connection page),
- If tunnels are set up in DR mode using a network group as the traffic selector (via *Config* mode), the phase 2 renegotiation will fail,
- The **Block Split Tunelling** and **All traffic through the tunnel** options are not compatible with OpenVPN tunnels transported over TCP,
- After waking up from sleep, the tunnel is no longer open, and it cannot be opened again. Either IKE failed to reset, or an interface error occurs after IKE reset,
- SSL tunnel creation wizards defaults to IKEv2 tunnel creation,
- The **Redundant Gateway** function should not be configured together with the **Fallback Tunnel** function. You should choose one or the other, failing which the VPN Client could have an undefined behavior,
- When migrating from an earlier version to a newer version, we recommend that you perform the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is particularly intended to avoid any issues with configuration format changes related to the automatic selection of certificates on smart cards and in the Windows store,
- A PIN code error may occur when automatic certificate selection is enabled.

# 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

Follow the steps below to download SN VPN Client Exclusive version 7.5.007.

1. Log in to your MyStormshield personal area.
2. Go to **Downloads** > **Downloads**.
3. Select **Stormshield Network Security** > **VPN CLIENT EXCLUSIVE** from the suggested categories.
4. Depending on the language chosen and the Windows version used, click on the SN VPN Client Exclusive installation program (*.msi* file). The download will begin automatically.
5. Enter one of the following commands to check the integrity of the retrieved binary files:
   - Linux operating systems: *sha256sum < filename>*
   - Windows operating systems:: *CertUtil -hashfile <filename> SHA256*

   Next, compare the result with the hash indicated in MyStormshield. To view it, click on **Show** in the **SHA256** column of the file in question.

**NOTE**
As a reminder, if you are upgrading from a previous version, the installer will automatically convert the previous configuration. Do not uninstall the previous version before you running the installer.

# 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.

| | | |
|---|---|---|
| 7.5.006 | New features | Bug fixes |
| 7.4.018 | New features | Bug fixes |
| 7.3.007 | New features | Bug fixes |
| 7.0.115 | New features | |

# New features and enhancements in version 7.5.006

## Main features

- The VPN Client now allows Active Directory (AD) to be used for Trusted Network Detection (TND),
- The VPN Client adapts the behavior of the **Connection Panel** and the **TrustedConnect Panel** according to the compliance level reported by the Secure Connection Agent (SCA), which determines whether an endpoint should be allowed to access the corporate network,
- The VPN Client is now able to forward audit traces to the Connection Management Center (CMC) when combined with the Secure Connection Agent add-on (SCA),
- Complies with ANSSI recommendations to ensure compatibility with gateways operating in "IPsec DR" (Restricted) mode, including use of SHA-2 hashing algorithm in the certificate request payload,
- The web browser to be used for Captive Portal Detection (CPD) can now be specified and a command line can be added, e.g. to disable the proxy in order to secure the connection,
- All OpenSSL-based components in the VPN Client have been migrated to version 3.0,
- The **TrustedConnect Panel** and the **Connection Panel** now manage endpoint compliance dynamically based on the SCA's status.

## Enhancements

- Greater granularity when configuring certificate selection: you can now specify the certificate's location (user store or machine store) at the tunnel level,
- Automated certificate selection regardless of medium, even when there are several tokens and smart cards,
- Added a dynamic parameter to enable the Online Certificate Status Protocol (OCSP),
- User certificates with a Brainpool curve using method 14 are supported by default and a dynamic parameter has been added to set method 214 as the default method when Restricted mode is required,
- ANSSI's new requirements relating to *Key Usage* and *Extended Key Usage* extensions have been applied,
- The SHA-1 or SHA-2 hash algorithm is now selected automatically for the certificate request payload (CERTREQ),
- Added a dynamic parameter to configure the size of the local virtual network,
- Added a Remediation checkbox to specify that the corresponding connection can be used for remediation,
- Better management of fragmented packets,
- **USB mode** has been removed to enhance product security.

# Version 7.5.006 bug fixes

- Fixes an issue where the TrustedConnect Panel allowed multiple tunnels to be opened simultaneously, including one in GINA mode,
- Fixes an issue that resulted in a system crash (BSOD) when the VPN Client was stopped and then restarted successively and repeatedly,
- Fixes an issue that resulted in a BSOD when receiving incorrect UDP packets,
- Fixes an issue where a smart card was not detected following a period of inactivity of the smart card manager,
- Fixes an issue where DNS entries for a physical interface were not restored,
- Fixes an issue where a temporary file created as a result of an abnormal termination of the program prevented the GINA mode from being started,
- Fixes an issue where entering an incorrect PIN code, when the Filtering Mode and Captive Portal Detection (CPD) are enabled, prevented a tunnel from being opened on any subsequent attempt to enter the correct PIN code,
- Fixes an issue where the IKE Auth message was incomplete,
- Fixes an issue where Trusted Network Detection (TND) was running in a loop in the TrustedConnect Panel when there was no valid certificate instead of generating an error,
- Fixes a buffer overflow issue when the syslog server name is too long,
- Fixes an issue where there was no more traffic when a tunnel was configured in IPv4 mode through an IPv6 connection,
- Fixes an issue where a single remote network was configured when renegotiating the Child SA phase for a tunnel with multiple remote networks,
- Fixes an issue where scripts were not run systematically when opening a tunnel,
- Fixes an issue where timestamps were not synchronized,
- Fixes an issue where the Filtering Mode configuration was ineffective,
- Addresses a traffic issue, when Windows automatically updates the VPN driver,
- Due to unsatisfactory algorithm suite proposals being generated, the Auto option has been removed from the algorithm selection drop-down lists,
- Fixes an issue where the SA payload formatting was incorrect in “Full IPsec Restricted” mode,
- Fixes an issue where configuring the EAP protocol was not possible.

# New features and enhancements in version 7.4.018

## Main features

- **TrustedConnect Panel** now handles multiple connections, including in GINA mode and with Filtering Mode active,
- TAS activation requests are spread out up to 90 days prior to end of subscription in order to prevent TAS server overload when a great number of licenses must be renewed on the same date,
- Supports automatic selection of user certificate from both token / smart card and Windows certificate store.

## Enhancements

- The **Console** window available from the **TrustedConnect Panel** now mirrors the behavior of the **Console** window available from the **Connection Panel**:
  - The menu item in the **TrustedConnect Panel**'s contextual menu can be enabled or disabled,
  - The same Ctrl+Alt+T keyboard shortcut to enable or disable logging is available,
  - A message in the **Console** window now specifies whether logging is enabled or disabled, and an icon to open the folder where logs are stored is shown when logging is enabled.
- Licenses can now be activated on TAS server after the trial period or the subscription has expired when *NoActivWin* and *AutoActiv* are enabled,
- Following ANSSI's changes to [RFC 7296] to specify IPsec DR compliance, the Certificate Request payload must now use SHA-2 instead of SHA-1 for releases running in IPsec DR mode (requires setting a dynamic parameter),
- Harmonizes behavior between SSL/OpenVPN and IKEv2 tunnels that use a client certificate with incorrect key usage or missing CA: a warning is displayed but tunnel can still be opened,
- Improves handling of OpenVPN tunnels with no certificate: SSL configuration can still be imported, no error is generated in the **Console**, and tunnel can still be opened,
- OpenSSL has been updated to version 1.1.1t,
- Warning messages and error codes are harmonized now between the **Connection Panel**, **TrustedConnect Panel**, and the panel displayed on the Windows logon screen when GINA mode is enabled,
- Tunnel now opens automatically when a redundant gateway is defined and main gateway sends a DELETE request followed by a CREATE request,
- Virtual network is forced to 32 when CP mode is not used.

# Version 7.4.018 bug fixes

- Fixes an issue where the generation of an authentication payload would fail when using a certificate automatically loaded into the Windows certificate store upon insertion of a smart card or token, but whose private key remains on the smart card or token,
- Fixes an issue where the **Certificate** tab would no longer be updated when inserting or removing a token or smart card,
- When using multiple smart cards, fixes an issue where a tunnel would be closed unexpectedly upon removing a smart card that is not used with the VPN Client,
- Fixes an issue where VPN Client installation would roll back on Windows 11,
- In the presence of a redundant gateway, the SPI size in the SA_INIT proposal is set to 8 instead of 0 when the VPN Client switches to the redundant gateway,
- Fixes an issue where the connection status indicator ring on the **TrustedConnect Panel** would remain grey during and after TND,
- Fixes an issue where a tunnel that does not use a token would be closed upon removal of a token,
- Fixes an issue where a tunnel would not close at the client end when a gateway sends DELETE requests and no longer responds,
- Fixes an issue where a tunnel would not open when the correct PIN code is entered after initially entering the wrong PIN code,
- Fixes an issue where the VPN Client would not explicitly ask for the PIN code when a smart card is removed and the reinserted,
- Fixes an issue where an IKE Reset would be triggered upon inserting a smart card when CPD is enabled,
- Fixes an issue where *path* and *ngpath* keys could be written or deleted,
- Fixes an issue where a long syslog server name would cause a buffer overflow,
- Fixes an issue with OpenVPN tunnels where gateway certificate validation was disabled by default,
- Fixes an issue where a TND beacon port change was not working,
- Fixes an issue where an “incompatible format” error occurred when retrieving a configuration from an older gateway model,
- Fixes an issue where the VPN Client would not accept a configuration file from a new gateway model that supports SHA-2 signature algorithms,
- Fixes an issue where the VPN Client would not accept a self-signed certificate or a certificate used by both the local and remote endpoints,
- SHA-1 hash algorithm has been reintroduced to support older equipment,
- Fixes an issue where the **Configuration Panel** remained accessible from the taskbar icon despite the option restricting access to the **Configuration Panel** to administrators being enabled,
- RSASSA-PKCS1-V1_5 signature scheme has been reverted as default to support older equipment.

# 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.

# 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.

STORMSHIELD