



**STORMSHIELD NETWORK
SECURITY**
STORMSHIELD VPN CLIENT

RELEASE NOTES VERSION 6.40

English version

November 21, 2016



Version

This Release Note details the features, improvements and fixes of the Stormshield Network VPN Client.

6.40 build 004	Features	Improvements	Bug fixing	
6.30 build 002	Features	Improvements	Bug fixing	
6.21 build 001		Improvements	Bug fixing	
6.20 build 006	Features	Improvements	Bug fixing	
6.12 build 002	Features	Improvements	Bug fixing	
6.08 build 003	Features	Improvements	Bug fixing	Known issues



Compatibility

The following platforms are compatible with Stormshield VPN Client 6.40:

Stormshield Network Firewall	System requirements
Versions 1.x, 2.x and 3.x	Windows 10
	Windows 8.1
	Windows 8
	Windows 7
	Windows Vista
	Windows Server 2012
	Windows Server 2008

The IPSec VPN client is a service compatible with 32- and 64-bit operating systems.



Stormshield Network VPN Client 6.40 build 004

Features, improvements and fixes since release 6.30

Features

- New design for the Connection Panel. This new design improves VPN Client user experience by simplifying the management of VPN connections. The New Connection Panel is fully configurable via a dedicated management window which enables to create, rename and sort VPN connections.
- Add a verification of the gateway certificate subject (SSL).
- Using WiFi networks sometimes requires a local authentication (via a captive portal). For users using the GINA Mode (VPN Connection before Windows logon), the VPN Client implements a new browsing window which allows the authentication on the captive portal before opening the tunnel.
- New "/status" command line option allows to retrieve the status of a tunnel.
- Support of IKEv2 Fragmentation (RFC 7383).
- Always-on: automatically re-open tunnel when DPD timeout is detected (IKEv1 & IKEv2).
- New certificate selection criteria: It is possible to configure a pattern to be found in the certificate subject.
- Always-on: automatically re-open tunnel when remote network is no longer accessible (IKEv1 & IKEv2).
- "No Split DNS": Ability to force the physical DNS server address to the value of the Virtual DNS Server address. This function solves communication slowness and confidentiality problems.
- "No Split Tunneling": Ability to disable default route on physical interface for all in tunnel configurations.
- New "/closeall" command line option (close all tunnels).
- New "/resetike" command line option.
- Mode Config / Mode CP: Support of Virtual network size sent by the gateway (by default /24 when not specified).
- Option to check the gateway certificate CRL in addition to its signature.
- Copy / paste of IKEv2 and SSL configurations.
- New customization of VPN Client.

Improvements

- New parameters are backed up and restored during a software update.
- In accordance with the development of the new Connection Panel, the system tray menu has been simplified.
- Ability to disable the function "automatic close the tunnel on USB extraction". This option keeps the tunnel open even if the USB drive is removed from the computer.
- Improvement when handling IKEv1 phase 1 renegotiations with Mode Config.
- Improvement of the IKE Auth rekeying (IKEv2).
- Enhancement of the management of IKEv2 gateway renegotiations.



- "Reset IKE" (from console window) starts IKE daemon if it's not already started.
- Various software startup enhancements.
- Improvements when handling a large list of remote networks for SSL connections.
- Various improvements of messages displayed in the console.
- Systray icon is available after an explorer.exe restart.
- Ability to open an IKEv2 VPN tunnel when the Mode CP is not enabled and the virtual IP address is not set.
- Ability to uninstall the software when it is protected with a password.
- Improvement of the function "automatic tunnel opening on token insertion", with token owning several certificates with different subjects.
- Improvement of the IKE service stability.
- IKEv2 CP Mode: ability to specify a smaller remote network on client side.
- Detection traffic in Mode CP now supported with IKEv2.
- Various improvements in the GINA Mode.
- Improvement of the OpenVPN file importation.
- Improvement of the IPv6 management by IKEv2.
- Ability to open automatically a tunnel in GINA Mode.
- The PIN Code is required each time a tunnel is opened (or re-opened), even after a tunnel opening failure.
- Support of secondary Wins Server.
- Enhancement of the Configuration Panel Control Access security.
- A VPN tunnel correctly closes if the physical interface disappears. (IKEv1).
- Warning displayed in the Console when an outdated certificate is used in an IKEv2 configuration.
- Update German

Bug Fixing

- Configuration Panel and Connection Panel synchronization improvement.
- Correct management of the virtual interface MTU.
- The Configuration Panel and the Connection Panel might appear simultaneously.
- Correction of the font in the activation window.
- Changing language led to address type duplication (in Child SA configuration).
- Deleting a ChildSA among N led to the alert: "An invalid argument was encountered".
- Support of UTF-8 character encoding for X-Auth password (requires a specific configuration).
- X-Auth Popup: Passwords containing ";" were not properly handled.
- A SA was closed too early when the lifetime is set in Kbytes from the Gateway.
- Improvement of the certificate subject parsing.
- IKEv2: When Mode CP is enabled, after tunnel is up, remote network is not properly displayed in VPNConf.
- Support of certificates containing multiple subjectaltnames (IKEv1).



- Wrong word on popup message.
- Missing word "confirm" on IKE V2 settings.

Stormshield Network VPN Client 6.30 build 002

Features, improvements and fixes since release 6.21.

Features

- Ability to hide the activation window which normally appears at the end of a subscription period.
- Windows 10 full compatibility
- New Token interoperability with Feitian epass2003 and gemalto/axalto .net
- New Ecom CryptoSmart Micro SD support for IKEv1, IKEv2 and SSL
- New Xiring Pinpad support for IKEv2 and SSL.
- After a 1st installation, a tip is displayed over the taskbar icon in order to show the user how to use the VPN Client.
- Logs can now be enabled from the Console.

Improvements

- DPD mechanism improvement
- Ecom smartcard management improved with SSL
- Improvement of the .ovpn files conversion (OpenVPN configuration)
- Security of the tunnel opening is improved : when the gateway CA is unknown, the tunnel doesn't open.
- IKEv1 - DPD mechanism improvement: tunnel correctly closes on DPD failure and gateway renegotiation, DPD keeps on on network disconnection, DPD timers management is tuned.
- When a VPN Configuration is created with the Wizard, the default parameters are: DH Group = Auto and Aggressive Mode = TRUE (set)
- Smartcard management improvement
- Debug/Trace mode can be activated from any window/panel of the VPN Client (Configuration panel, connection panel or Console).
- Tunnel opening or closing process is stopped on IKE reset
- Compatibility between tunnel configured with VPN 5.5 and tunnel configured with VPN 6.2
- Integration of security update for OpenSSL (CVE-2015-0204, FREAK vulnerability fix)
- Windows IKEEXT cohabitation is correctly managed on Windows 8 / Windows 6.1 upgrade.

Bug Fixing

- SSL error "TLS handshake failure: No CA" fixed by improving the management of CA check.
- IKEv1 erratic freeze fixed.
- Systray popup message for SSL tunnel fixed.



- Compatibility with 3rd party software such as firewall, anti-malware or antivirus.
- BSOD/Conflict with 3rd party software.
- Log files names are correctly updated on date changing.
- Launched in silent mode, the setup ended with a crash if a password greater than 15 characters was set in the command line. This bug is fixed.
- For a 2-DNS tunnel, the management of the second DNS is fixed.
- The wizard works when Client use only one protocol.

Stormshield Network VPN Client 6.21 build 001

Improvements and fixes since release 6.20.

Improvements

- IKE tunnel closes more quickly on network disconnection.
- During a software update, the software activation can be processed within a VPN tunnel.
- Possibility to create a VPN configuration with multiple auth + EAP + certificate.
- (IKEv1) Phase1 closes (and can be re-open) as soon as the tunnel is closed by the gateway.
- VPN Client can open tunnels even if the Internet connection appears after it starts.
- (IKEv2) Local and Remote ID now display explicit "E-mail" instead "ID_RFC822_ADDRESS".

Bug Fixing

- (IKEv1) "Initial contact" is not sent anymore upon tunnel renegotiation.
- Correct management of certificates containing an OID in the subject.
- Tunnel opening on traffic detection might not work after a restart of the VPN Client software.
- Cannot open an IKEv1 tunnel when switching from a network to another while VPN Client is running (on a workstation with two NICs).
- With Mode Config on IKEv1, Phase 2 establishment could fail.

Stormshield Network VPN Client 6.20 build 006

Features, improvements and fixes since release 6.12

Features

- New Certificate's OIDs supported.
- Support of nested tunnels between different protocols.
- New Configuration Wizards for IKEv2 and SSL tunnels.
- Support of the Ingenico "Leo" Pinpad.
- Possibility of certificate injection via a command line option (online certificate injection).
- Smartcard roaming support for IKEv2.



- Handle IKEv2 multi-proposals in order to simplify tunnel setup.
- [SSL] Support of TCP mode for the transport.
- [IKEv2] Automatic switch to PKCS#11 when middleware doesn't work in CSP mode.

Improvements

- Dynamic display of Config Payload Mode informations for IKEv2/IPV6.
- Support of several Child SA per Initial SA.
- Improvement of token access speed.
- IKEv1: When the PIN code entry is canceled, the tunnel opening process is aborted.
- Allow to use a self-signed Root Certificate from Windows Certificate Store.
- USB Mode Confirmation popup only appears when required.

Bug fixing

- With Mode Config on IKEv1, Phase 2 establishment could fails.
- DPD still working when "split tunneling" is enabled.
- IKEv1 "Automatic" mode works for Phase1 encryption when gateway reports AES.
- Modification of IKE port and NAT port (IKEv1 parameters) is fixed.
- Improvement of Token removal detection.
- [IKEv2] Import certificate with "DC" RDN from Windows Store fixed.
- [IKEv2] VPN tunnel properly opens when Certificate received from the VPN gateway is the same as the user Certificate.
- [IKEv2] VPN tunnel properly opens even if no Remote Id has been specified in the VPN Client.
- Windows firewall configuration correctly restored on uninstall.
- [IKEv2] Gemalto PKCS#11 middleware now available.
- VPNConf synchro issue when using USB Mode and autostart tunnel.
- Autostart USB tunnel error "No thread found to handle IKE version 1 packet" fixed.
- [DualToken] Fix on multiple partition token (automatic extraction detection).



Stormshield Network VPN Client 6.12 build 002

Features, improvements and fixes since release 6.08

Features

- Disable SHA-384 choice, SSL and IPsec IKEv2 VPN tunnel.
- IP address can change during renegotiation with VPN tunnel using IKEv2.
- SSL disabled.
- Support of IPv4 and IPv6 simultaneously
 - Ability to handle heterogeneous IPv4 and IPv6 networks on the LAN and WAN sides, either on corporate or user home networks. The feature 'Auto' (for IPv4/IPv6) enables to support those complex environments with IPsec (IKEv1/v2) or SSL VPN tunnels.
 - Ability to detect IPv4 or IPv6 network automatically for both IPsec and SSL VPN tunnels.
 - Ability to send IPv4 and IPv6 within the same tunnel.
- Support of IPsec and SSL/TLS simultaneously
 - Ability to open multiple SSL VPN tunnels with any VPN gateways supporting OpenVPN.
 - Introduction of two new user authentication mechanisms specific to SSL i.e. Mode TLSAuth and Extra Login/Password.
 - Auto adaptive capabilities to adapt to the SSL gateway settings automatically, assuming the gateway support multi proposal mechanism. The IT manager can disable this feature and force his own settings.
 - Ability to define a redundant SSL gateway in case of unavailability of the primary SSL gateway.
 - Ability to open SSL VPN tunnel on detection of traffic to the remote network.
 - Ability to start automation via scripts before/after tunnel opens or closes.
 - Ability to start a desktop sharing session with a machine on remote network in one click.
 - Ability to add traffic compression.
 - Inherits all IPsec encryption and hash algorithms from TheGreenBow IPsec VPN client (e.g. SHA1, SHA2, ..).
- Support of IPsec with IKEv1 and IKEv2 simultaneously
 - Ability to open IKEv1 and IKEv2 VPN tunnels simultaneously.
 - Ability to define a redundant gateway in case of unavailability of the primary gateway.
 - IKEv2 introduces a new user authentication mechanism called EAP similar to X-Auth. The new user authentication mechanism EAP can be combined with Certificate (i.e. select multiple Auth support in your VPN tunnel configuration > 'IKEv2 Auth' > 'IKE SA' tab. EAP replaces X-Auth when using IKEv2 VPN tunnel.
 - Auto adaptive capabilities to adapt to the gateway settings automatically, assuming the gateway support multi proposal mechanism. The IT manager can disable this feature and force his own settings.



Improvements

- Support of TLS connection without user certificate.
- Prevent broadcast transfers to remote network.
- Support of all 3 addressing modes i.e. host, subnet and IP address range with IKEv2 VPN tunnels.
- Certificate Authority (CA) might or might not be specified when importing a P12 certificate within an IKEv2 VPN tunnel configuration.
- IKEv2 VPN tunnel supports an empty Remote ID and it is considered as 'Accept any ID from remote' as it does in IKEv1 VPN tunnels.
- New default Algorithms for Auto selections.
- Various text strings and user interface improvements.
- Various user interface improvements.
- VPN tunnel opens faster when using a certificate on a PKCS#11 Smartcard or Token.
- All settings in the 'Security' tab are set to 'Auto' mode when creating a new SSL VPN tunnel.
- User interface improvement for IPsec IKEv2 & IKEv1 VPN configuration:
 - Root tree strings "IKE V1 Configuration" & "IKE V2 Configuration" might be truncated.
- VPN tunnel IKEv2 and IPV6, replace mask with prefix length in the Child SA.
- New menu strings to create a Phase1 and Phase2 consistent between IKEv1 and IKEv2 now called 'New VPN Gateway' and 'New VPN Connection' accordingly.

Bug fixing

- Certificate could not be imported from Windows Certificate Store.
- Import or export VPN Configuration to or from a mapped drive fails.
- Packets with a payload smaller than 24 bytes are dropped in IPV6 VPN tunnel, causing issues for FTP.
- Incoming packets ending with .255 on port 4500 are not handled properly.
- 'Tsocket message data type 0 could not be sent' error message preventing an IKEv1 VPN tunnel to open using an IPV6 IP address.
- VPN tunnel fails to open due to unknown OID from the Certificate (i.e. Object Identifier). Need to add 'GN' label for OID (i.e. Given Name).
- Pre Shared Key can be saved with shortcut 'Ctrl+S' without checking against the 'Confirm' field.
- Error "disagreement on PFS" when configured with 'Auto' for PFS in IKEv1 Phase2 (gateway specific).
- The VPN Client might crash if import a VPN configuration file modified with wrong parameters for a VPN tunnel configured using IKEv1.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- A new network interface is not detected when it becomes up.
- VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv6 VPN tunnel is not opening properly.
- VPN tunnel configured with IKEv2 and IPv6 toward a VPN gateway configured with IPv4 VPN tunnel is not opening properly.



- 'View Certificate' button is not working properly with VPN tunnel using IKEv2, after saving the VPN configuration.
- 'New Phase1' and 'Paste Phase1' menu from root tree not working properly.
- VPN configuration with IKEv2 can be saved although Remote Gateway field is empty.
- IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration.
- VPN tunnel with IKEv2 CHILD SA negotiation in IKE AUTH exchange with Diffie-Hellman.
- VPN tunnel with IKEv2, user must click twice on EAP button to have password enabled.
- VPN tunnel with IKEv2, Pre Share Key is empty after saving the VPN Configuration.
- VPN tunnel with IKEv2, the local/remote ID type of ID set to null is not working properly.
- VPN tunnel with IKEv1, Auto for Phase 1 doesn't work.
- VPN tunnel with IKEv1, X-Auth login/password popup is not working properly.
- Change in configuration from IPv6 to IPv4 in VPN tunnel within IKEv2 Child SA is not detected.
- VPN tunnel configured with IKEv1 and IPv4 toward a VPN gateway configured with IPv4, has no traffic if PFS=None and without NAT-T in Phase 1.
- VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv4, has no traffic if PFS=None.
- New buttons in the Configuration Panel root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.
- Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- Config Payload information in VPN tunnel configured with IKEv2 not displayed properly when tunnel opens or closes.
- Timeout of 30sec to monitor VPN tunnel opening might too short in some circumstances like using USB Token with a certificate protected by PIN, or large number of packet rejections.
- Word 'Static' appears in the Configuration Panel tree root IKEv1, IKEv2 and SSL.
- Texts of protocol description displayed in the Configuration Panel tree for each protocol (i.e. SSL, IPsec IKEv1, IKEv2) are not corrects.
- New buttons in the Configuration Panel root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.
- VPN tunnel using IKEv2 opens only once when LocalId is not filled in with certificate subject.
- The type IKEV2_ID_FQDN as remote ID Type is not yet supported.
- Several text typos in Configuration Panel 'Child SA' or Phase2 tabs.
- Phase renegotiation, on VPN tunnel with IKEv1, uses port 500 again instead of port 4500.
- Shortcut Ctrl+S doesn't save the remote sharing and Certificate store settings.
- Feature blocking traffic outside VPN Tunnel (i.e. Split tunneling) with IKEv2 and SSL VPN tunnels is not yet available.
- Notification FAILED_CP_REQUIRED with IKEv2 VPN tunnels received from the gateway closes the VPN tunnel unexpectedly.
- The 'Initial Contact' mechanism is not yet supported with IKEv2 VPN tunnels.
- VPN Configuration with IKEv2 and SSL is lost after transferring IPsec IKEv1 configuration to USB mode.
- Remote ID ID_DER_ASN1_DN received from the gateway is not checked properly.



- Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- SHA2 in 'Child SA' tab is not available yet with IKEv2 VPN tunnels.
- DNS/WINS manual setup is not yet supported with IKEv2 VPN tunnels.



Stormshield Network VPN Client 6.08 build 003

Features

- Ability to enter a machine name instead of an IP address when adding a Remote Sharing entry (i.e. 'Phase2' > 'Remote Sharing').
- Support of IPv4 and IPv6 protocols.
- Support of Diffie-Hellman Group 15 (3072-bit), Group 16 (4096-bit), Group 17 (6144-bit), Group 18 (8192-bit).
- Support of 2 new SHA2 algorithm: SHA2-384, SHA2-512. The IPsec VPN Client now supports SHA256-96, SHA256-128, SHA2-384, SHA2-512.
- Support of multiple DNS servers (2) per VPN Tunnel. They can be configured manually or, received from the VPN gateway in Mode Config.
- Ability to add a DNS suffix to DNS server addresses.
- Ability to open a tunnel within another tunnel. This allows access your company network with a first gateway, and then access a second secured network within your company with a second gateway. Restriction: Mode Transport, and force all traffic in tunnel are not supported.
- Support of Windows Server 2008 32/64-bit, Windows Server 2012 32/64-bit, Windows Vista 32/64-bit, Windows Seven 32/64-bit, Windows 8 32/64-bit, Windows 8.1 32/64-bit. Note: Windows XP is no longer supported, please download the previous release for Windows XP support.
- Support of 25 languages including English, Arabic, Chinese simplified, Czech, Danish, Dutch, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, Turkish.

Improvements

- Log files generated when user activate the Trace mode (Ctrl+Alt+D) are now deleted automatically if older than 10 days. Those files could become fairly big fairly quickly.
- More debug logs when user activates the Trace mode (Ctrl+Alt+D).
- Remove both buttons 'Apply' and 'Save' from the Configuration Panel. Save can be found in the menu 'Configuration' > 'Save', or Ctrl+S. Apply is automatic when the user clicks on 'Open tunnel'.
- When trying to upgrade to the latest release without Update Option, or if Update Option has expired (i.e. license to update to the latest release), the upgrade was previously blocked.
- Now, the user can choose to proceed or not (knowing that software activation might fail right after installation).

Bug fixing

- Reception of fragmented packets in reverse order is not working properly.
- Bad DPD handling when DPD reply from the gateway is lost, and the VPN Client resend a new DPD sequence.
- IKE process (Tgblke) might crash when the IP address is changing.



- Packets with DF flag (i.e. Don't Fragment) are not handled properly in some specific circumstances.
- The button 'Add WINS' server stays enabled after VPN tunnel opens in Mode-Config.
- Alternate WINS server addresses are not applied to the Virtual Interface, and not showed in the VPN Client > 'Phase2 IPsec' > 'Advanced' tab after the VPN tunnel opens in Mode-Config.
- Wrong DNS server IP address format displayed after the VPN tunnel opens in Mode-Config.
- No connectivity to the DNS server when setting up an Alternative DNS in some very rare Windows configuration.
- Crash when using 'easyVPN' module in some circumstances. 'easyVPN' module allows to fetch a VPN Configuration on a VPN configuration server making VPN configuration update very easy for IT managers and users.
- License agreement is displayed in Spanish when choosing Italian during setup.
- IKE port and NAT ports not updated correctly upon VPN Configuration changes by user.
- Unable to open tunnel (Phase 2 not completed) when forcing NAT-T in Transport Mode in the VPN Configuration.
- DIR command (FTP protocol) doesn't work when trying to access a FTP server within a VPN tunnel, in some network circumstances.
- No systray icon (taskbar) when Windows starts or after sleep mode, in some Windows configurations.
- Multiple Phase1 with the same remote gateway addresses would not work properly.

Known issues

- The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- In VPN Configuration with two VPN Tunnels with the same virtual IP address, DNS/WINS server address of the first VPN tunnel only is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.



STORMSHIELD