www.zyxel.com

ZYXEL

Zyxel

Software Release Note

SecuExtender IPSecVPN Windows

Release 3.8.204.61.32

Date: 2019.8.13

Author: Karena Lin

1 Design Limitation

The following ZyWALL/USG VPN Gateway rules configured cannot be provisioned to the SecuExtender IPSecVPN_Windows Client:

- Multiple Authentication not applicable
- Gina mode cannot function in occasions where VPN rules are moved to USB drive.
- VPN Client Address will be void in occasions where the Client and the Gateway are not unanimously both IPv4/IPv6, and users will be notified that "VPN Client Address is void so tunnels cannot be built with success".
- IPv4 rules with IKEv2 version
- IPv4 rules with User-based PSK authentication
- IPv6 rules

2 SecuExtender IPSec VPN Client Release Notes

This Release Note details the features, improvements and fixes of the release 6.60

New features summary :

Main features

- Implementation of administration and system logs, with ability to produce administration logs either locally, to the Windows Event Manager or to a Syslog Server.
- VPN Tunnel Fallback (for example: automatic fallback from an IPsec tunnel to an SSL tunnel when IPsec tunnel fails)
- Windows Store Certificate Roaming: Ability to select automatically the user certificate from the Windows Certificate Store, based on criteria (like for smartcards)
- Ability to select and store multiple CA (Certificate Authority) in the VPN Configuration

Cryptography

- Support of Elliptic curve Diffie-Hellman (Diffie-Hellman group 19, 20, 21) for IKEv2
- Support AES-GCM & AES CTR algorithms for IKEv2
- Support of PKCS8 Private Key format

GUI

- Redesign of the Configuration Panel interface, with a clearer organization of the configuration tabs between IKEv1, IKEv2 and TLS protocols.

2.1 TheGreenBow VPN Client 6.63 build 001

Features, improvements and fixes since release 6.62.003

- Bugfix: "Incorrect Password" when trying to update a previous installation with configuration panel acces lock by password.
- Bugfix: [Custo] Unable to access to the gui after setting a password.
- Known issue: when import wrong user certificate, the VPN Client will crash.

2.2 TheGreenBow VPN Client 6.62 build 003

Features, improvements and fixes since release 6.60.009

- Improvement: Implementation of a new software activation library.
- Bugfix: Opening an IKEv2 tunnel with 0.0.0.0 as a VPN Client address may causes routing issues.
- Bugfix: unable to set IPV6 Phase 2 for an IKEv1 Tunnel.

2.3 TheGreenBow VPN Client 6.60 build 009

Features, improvements and fixes since release 6.45.002

- Feature: Implementation of administration and system logs, with ability to produce administration logs either locally, to the Windows Event Manager or to a Syslog Server
- Feature: Re-integrate "Multiple Auth Support" checkbox , Zyxel GW now support RFC 4739.
- Feature: Ability to select and store multiple CA (Certificate Authority) in the VPN Configuration
- Feature: Support of Elliptic curve Diffie-Hellman (Diffie-Hellman group 19, 20, 21) for IKEv2, not support provisioning to Zyxel Gateway
- Feature: Option to disable DPD IKEv2
- Feature: Global redesign of the interface (Configuration Panel) with a clearer organization of the configuration tabs (new "advanced" tab, homogenization of the tabs between IKEv1, IKEv2 and TLS)
- Feature: Ability to configure wait time for gateway responses (timeout was previously set to 5 sec.)
- Feature: Support of Microsoft Signing for W10 drivers
- Feature: when rekeying, asking for X-Auth credentials is now configurable
- Feature: Handling of PKCS8 (in addition to PKCS1) Private Key format
- Improvement: Handling of uppercase/lowercase certificates "name" OID
- Improvement: Optimize VPN configuration loading and saving
- Improvement: Gina mode : Progress bar for IKEv2 and SSL enhanced
- Improvement: DPD, lifetime and IKE Ports are configurable for each tunnel
- Improvement: IKEv2 doesn't support PKCS#8 private key format, but only PKCS#1
- Improvement: Remote Sharing : RDP is not opened automatically from configuration panel
- Improvement: "vpnconf /stop"" doesn't work from another user session
- Bug: (Specific Partners) DH algo default is not set to "No"
- BugFix: IKEv2 Fragmentation issue: some fragment sizes lead to Auth Fail or Syntax Error
- BugFix: BSOD when receiving data in tunnel with a high rate

- BugFix: IKEv2 and TPM: Unable to import user certificate in internal store
- BugFix: DN pattern doesn't work properly for IKEv2
- BugFix: Remote ID mismatch on "DER ASN1 DN" with the same ASCII string
- BugFix: Virtual interface: bad handling of ARP table to add/remove gateway IP address
- BugFix: IKEv2: Sometimes tunnel doesn't open, IKE Initialization fails (error with "0")
- BugFix: IKEv2 : No traffic to remote network.VirtualItf error 1 - 209 - 5010
- BugFix: IKEv2 : Exporting a Single tunnel exports all Child SA
- BugFix: IKEv1: Tunnel is not deleted when XAuth fails during a Phase 1 renegotiation
- BugFix: Cannot open tunnel with a token inserted after the VPN Client starts
- BugFix: IKEv2 child SA is not removed when tunnel is closed for DPD timeout reason
- BugFix: IKEv2: no traffic when NATT port is changed for one tunnel, and UDP Encap enabled
- BugFix: IKEv2: IPV4 DNS not set properly when Gateway sends an IPV6 address
- BugFix: IKEv1 Traffic verification: 1st timer is not properly initialized

2.4 TheGreenBow IPsec VPN Client 6.45 build 002

Features, improvements and fixes of release 6.45.001

- Bugfix: IkeV2: Fragmentation IkeV2 and DH algo set to auto => fragmentation is not selected.
- Bugfix: InjectP12 command: new cert not update when closing the session.
- Bugfix: IkeV2 Fragmentation issue: some fragment sizes lead to Auth Fail or Syntax Error.
- Bugfix: IkeV2: Sometimes tunnel doesn't open, IKE Init fails (error with "0")
- Bugfix: IkeV1 Fragmentation: Cisco Vendor ID is not correctly sent.

2.5 TheGreenBow IPsec VPN Client 6.41 build 003

Features, improvements and fixes of release 6.43.002

- Feature:(Partner Specific) DH default algorithm is set to "No DH".
- Improvement: SSL VPN: Reception Socket buffer sizes are increased to accept traffic peaks.
- Bugfix: Remote ID mismatch on "DER ASN1 DN" with the same ASCII string.
- Bugfix: IKEv2: DPD handling: Tunnel was closing when one DPD message is lost.
- Bugfix: IKEv2 child SA is not removed when tunnel is closed for DPD timeout reason.
- Bugfix: Could not open tunnel with mixed SujectAltName containing an IP address.
- Bugfix: IKEv1: Traffic verification with pings doesn't work properly.
- Bugfix: No traffic when virtual IP address ends with .255.

- Bugfix: SSL VPN: When using TCP mode the tunnel may close unexpectedly.
- Bugfix: Silent install is not silent on Windows Seven.
- Bugfix: Bad renewal certificate used on the smart card.
- Bugfix: IKE SA renegotiation failed with a Fortigate gateway.
- Bugfix: IKE SA renegotiation failed in a CHILD SA.

2.6 TheGreenBow IPsec VPN Client 6.41 build 003

Features, improvements and fixes of release 6.41.002

- Feature: Add a notification to let users know GINA mode will not work when VPN rules in USB.
- Bugfix: Wrong pincode error occurs during Phase1 renewal in some case.

2.7 TheGreenBow IPsec VPN Client 6.41 build 002

Features, improvements and fixes of release 6.41.001

- Feature: When mounting several tunnels at the same time, PIN code is asked several times.
- Bugfix: PIN code is asked at each Phase1 renewal.

2.8 TheGreenBow IPsec VPN Client 6.41 build 001

Features, improvements and fixes of release 6.40.006

- Bugfix: Bad X-Auth password leads to a software error.
- Bugfix: Socket bind fails when executed too quickly after interface is up.
- Bugfix: Polish translation of the VPN Client.
- Bugfix: Correct default DPD values are set when importing a configuration without DPD.
- Bugfix: TgbIkeNg not stopped on fast shutdown on Windows 10.
- Feature: Re-branding Client customization.
- Feature: PIN code requests mutualising when building several tunnels.
- Feature: A warning is displayed when trying to build an IPv4/IPv6 tunnel with no virtual IP address. (OEM Partner specific).

2.9 TheGreenBow IPsec VPN Client 6.40 build 006

Features, improvements and fixes of release 6.40.005

- Bugfix: Font size fix in the Connection Panel (title and open button).
- Feature: New VPN Client customization.

2.10 TheGreenBow IPsec VPN Client 6.40 build 005

Features, improvements and fixes of release 6.40.004

- Improvement: All PKI options are now configurable in vpnsetup.ini (setup initialization) file and via the setup command line options. See the VPN Client Deployment Guide (VPN Premium only).
- Improvement: TLS tunnel: TlsAuth option worked only with SHA1 Authentication algorithm. TlsAuth is now possible with all authentication algorithms (SHA256, SHA 512, etc.).
- Improvement: TLS tunnel: TlsAuth option is also operational with key direction set to client or server.
- Improvement: All opened tunnels are properly closed when Windows shutdowns quickly.
- Bugfix: Windows 10: When the user session is locked, the VPN GINA is not displayed.
- Bugfix: Configuration with Virtual IP set to "::" doesn't work.
- Bugfix: No virtual interface when virtual IP is not specified and remote network is a range of address
- Bugfix: The Gateway Certificate CRL was checked despite this checking is disabled.
- Bugfix: Crash Ike on specific UNITY_DEF_DOMAIN values sent by the gateway (Mode config / Mode CP).

2.11 TheGreenBow IPsec VPN Client 6.40 build 004

Features, improvements and fixes of release 6.40.003

- Improvement: New parameters are backuped and restored during a software update.
- Bugfix: Configuration Panel and Connection Panel synchronization improvement.

2.12 TheGreenBow IPsec VPN Client 6.40 build 003

Features, improvements and fixes of release 6.30.005

- Feature: 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.
- A new browsing window is automatically displayed as the tunnel opens, to allow users using the GINA Mode to connect first to a WiFi captive portal before opening the VPN Connection.

- Using Some WiFi networks requires authentication (via a Captive Portal) => problem with Gina mode.
- Fonctionnalité : Nouveau design pour le panneau des connexions. Ce nouveau design améliore l'expérience utilisateur du Client VPN en simplifiant la gestion des connexions VPN. Le nouveau panneau des connexions est entièrement configurable via une nouvelle fenêtre de configuration qui permet de créer, renommer ou ordonner les connexions VPN.
- Feature: Add a verification of the gateway certificate subject (SSL)
- Feature: 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.
- Feature: New "/status" command line option allows to retrieve the status of a tunnel.
- Feature: Support of IKEv2 Fragmentation (RFC 7383)
- Feature: Always-on: automatically re-open tunnel when DPD timeout is detected (IKEv1 & IKEv2)
- Feature: New certificate selection criteria: It is possible to configure a pattern to be found in the certificate subject.
- Feature: Always-on: automatically re-open tunnel when remote network is no longer accessible (IKEv1 & IKEv2)
- Feature: "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.
- Feature: "No Split Tunneling": Ability to disable default route on physical interface for all in tunnel configurations
- Feature: New "/closeall" command line option (close all tunnels)
- Feature: New "/resetike" command line option
- Feature: Mode Config / Mode CP: Support of Virtual network size sent by the gateway (by default /24 when not specified)
- Feature: Option to check the gateway certificate CRL in addition to its signature.
- Feature: Copy / paste of IKEv2 and SSL configurations
- Improvement: In accordance with the development of the new Connection Panel, the system tray menu has been simplified
- Amélioration : Dans le cadre du nouveau panneau des connexions, le menu systray a été simplifié.
- Improvement: 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: Improvement when handling IKEv1 phase 1 renegotiations with Mode Config.

- Improvement: Improvement of the IKE Auth rekeying (IKEv2)
- Improvement: Enhancement of the management of IKEv2 gateway renegotiations
- Improvement: "Reset IKE" (from console window) starts IKE daemon if it's not already started
- Improvement: Various software startup enhancements
- Improvement: Improvements when handling a large list of remote networks for SSL connections
- Improvement: Various improvements of messages displayed in the console.
- Improvement: Systray icon is available after an explorer.exe restart
- Improvement: Support of the suffix domain name (Cisco extension: UNITY_DEF_DOMAIN/28674) when received through Mode Config / Mode CP
- Improvement: Various improvements in the subscription mode management (VPN Premium only)
- Improvement: The GINA Mode correctly handles the subscription mode (VPN Premium only)
- Improvement: Ability to open an IKEv2 VPN tunnel when the Mode CP is not enabled and the virtual IP address is not set.
- Improvement: Ability to uninstall the software when it is protected with a password
- Improvement: Improvement of the function "automatic tunnel opening on token insertion", with token owning several certificates with different subjects
- Improvement: Improvement of the IKE service stability
- Improvement: IKEv2 CP Mode: ability to specify a smaller remote network on client side
- Improvement: Detection traffic in Mode CP now supported with IKEv2
- Improvement: Various improvements in the GINA Mode
- Improvement: Improvement of the OpenVPN file importation
- Improvement: Improvement of the IPv6 management by IKEv2
- Improvement: Ability to open automatically a tunnel in GINA Mode
- Improvement: The PIN Code is required each time a tunnel is opened (or re-opened), even after a tunnel opening failure.
- Improvement: Improvement of the smartcard management (VPN Premium only)
- Improvement: Support of secondary Wins Server.
- Improvement: Enhancement of the Configuration Panel Control Access security
- Improvement: A VPN tunnel correctly closes if the physical interface disappears. (IKEv1)
- Improvement: Warning displayed in the Console when an outdated certificate is used in an IKEv2 configuration.
- Bugfix: Correct management of the virtual interface MTU
- Bugfix: The Configuration Panel and the Connection Panel might appear simultaneously.
- Bugfix: Correction of the font in the activation window

- Bugfix: Changing language led to address type duplication (in Child SA configuration)
- Bugfix: Deleting a ChildSA among N led to the alert: "An invalid argument was encountered"
- Feature: Support of UTF-8 character encoding for X-Auth password (requires a specific configuration)
- Bugfix: X-Auth Popup: Passwords containing ";" were not properly handled.
- Bugfix: A SA was closed too early when the lifetime is set in Kbytes from the Gateway
- Bugfix: Improvement of the certificate subject parsing
- Bugfix: IKEv2: When Mode CP is enabled, after tunnel is up, remote network is not properly displayed in VPNConf.
- Bugfix: Support of certificates containing multiple subjectaltnames (IKEv1)

2.13 TheGreenBow VPN Client 6.30 build 005

Features, improvements and fixes since release 6.30.004

- Feature: New customization of VPN Client
- Bugfix: Wrong word on popup message.

2.14 TheGreenBow VPN Client 6.30 build 004

Features, improvements and fixes since release 6.30.003

- Bug fixing: missing word "confirm" on IKE V2 settings.

2.15 TheGreenBow VPN Client 6.30 build 003

Features, improvements and fixes since release 6.30.002

- Improvement: update German

2.16 TheGreenBow VPN Client 6.30 build 002

Features, improvements and fixes since release 6.30.001

- Feature: Ability to hide the activation window which normally appears at the end of a subscription period
- Improvement: DPD mechanism improvement
- Improvement: Security of the tunnel opening is improved : when the gateway CA is unknown, the tunnel doesn't open.
- Bug fixing: IKEv1 erratic freeze fixed

2.17 TheGreenBow VPN Client 6.30 build 001

Features, improvements and fixes since release 6.21.002

- Feature: Windows 10 full compatibility
- Feature: New Token interoperability with Feitian epass2003 and gemalto/axalto .net
- Feature: Compatibility with Fortinet Fortigate IKEv2. TheGreenBow VPN Client is the only VPN Client which can be used to open an IKEv2 tunnel with a Fortigate gateway.
- Feature: New Ercom CryptoSmart Micro SD support for IKEv1 and IKEv2.
- Feature: New Xiring Pinpad support for IKEv2.
- Feature: After a 1st installation, a tip is displayed over the taskbar icon in order to show the user how to use the VPN Client.
- Feature: Logs can now be enabled from the Console.
- Improvement: IKEv1 - DPD mechanism improvement: tunnel correctly closes on DPD failure and gateway renegotiation, DPD keeps on on network disconnection, DPD timers management is tuned.
- Improvement: When a VPN Configuration is created with the Wizard, the default parameters are: DH Group = Auto and Aggressive Mode = TRUE (set)
- Improvement: smartcard management improvement
- Improvement: Debug/Trace mode can be activated from any window/panel of the VPN Client (Configuration panel, connection panel or Console).
- Bug fixing: Compatibility with 3rd party software such as firewall, anti-malware or antivirus
- Bug fixing: BSOD/Conflict with 3rd party software
- Bug fixing: log files names are correctly updated on date changing.
- Improvement: tunnel opening or closing process is stopped on IKE reset
- Bug fixing: 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.
- Bug fixing: For a 2-DNS tunnel, the management of the second DNS is fixed.
- Improvement: Compatibility between tunnel configured with VPN 5.5 and tunnel configured with VPN 6.2
- Improvement: Windows IKEEXT cohabitation is correctly managed on Windows 8 / Windows 6.1 upgrade.

2.18 TheGreenBow VPN Client 6.21 build 002

Features, improvements and fixes since release 6.21.001

- Bug fixing: the wizard works when Client use only one protocol.

2.19 TheGreenBow VPN Client 6.21 build 001

Features, improvements and fixes since release 6.20.007

- Improvement: IKE tunnel closes more quickly on network disconnection.
- Improvement: During a software update, the software activation can be processed within a VPN tunnel.
- Improvement: Possibility to create a VPN configuration with multiple Auth + EAP + Certificate.
- Improvement: (IKEv1) Phase1 closes (and can be re-open) as soon as the tunnel is closed by the gateway.
- Improvement: VPN Client can open tunnels even if the Internet connection appears after it starts.
- Improvement: (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.
- Bug fixing: Correct management of certificates containing an OID in the subject.
- Bug fixing: Tunnel opening on traffic detection might not work after a restart of the VPN Client software.
- Bug fixing: Cannot open an IKEv1 tunnel when switching from a network to another while VPN Client is running (on a workstation with two NICs)

2.20 TheGreenBow VPN Client 6.20 build 007

Features, improvements and fixes since release 6.20.005

- Feature: Default parameters (OEM Partner specific).
- Bug fixing: With Mode Config on IKEv1, Phase 2 establishment could fails.

2.21 TheGreenBow VPN Client 6.20 build 005

Features, improvements and fixes since release 6.20.001

- Feature: New Certificate's OIDs supported.
- Feature: Support of nested tunnels between different protocols
- Feature: New Configuration Wizards for IKEv2 tunnels
- Feature: Support of the Ingenico "Leo" Pinpad
- Feature: Possibility of certificate injection via a command line option (online certificate injection)
- Feature: Support of Freebox compatibility

- Feature: Automatic importation and translation mechanism for ~~OpenVPN (.ovpn) and~~ Cisco (.pcf) files
- Improvement: Dynamic display of Config Payload Mode informations for IKEV2/IPV6.
- Improvement: IKEv2: Support of several Child SA per Initial SA.
- Improvement: Improvement of token access speed.
- Improvement: IKEv1: When the PIN code entry is canceled, the tunnel opening process is aborted.
- Bug fixing: DPD still working when "split tunneling" is enabled.
- Bug fixing: IKEv1 "Automatic" mode works for Phase1 encryption when gateway reports AES.
- Bug fixing: Modification of IKE port and NAT port (IKEv1 parameters) is fixed.
- Bug fixing: Improvement of Token removal detection.

2.22 TheGreenBow VPN Client 6.20 build 001

Features, improvements and fixes since release 6.12.001

- Improvement: Allow to use a self-signed Root Certificate from Windows Certificate Store.
- Improvement: USB Mode Confirmation popup only appears when required.
- Feature: Smartcard roaming support for IKEv2.
- Feature: Handle IKEV2 multi-proposals in order to simplify tunnel setup.
- Feature: [IKEv2] Automatic switch to PKCS#11 when middleware doesn't work in CSP mode.
- Bug fixing: [IKEv2] Import certificate with "DC" RDN from Windows Store fixed.
- Bug fixing: [IKEv2] VPN tunnel properly opens when Certificate received from the VPN gateway is the same as the user Certificate.
- Bug fixing: [IKEv2] VPN tunnel properly opens even if no Remote Id has been specified in the VPN Client.
- Bug fixing: Windows firewall configuration correctly restored on uninstall.
- Bug fixing: [IKEv2] Gemalto PKCS#11 middleware now available.
- Bug fixing: VPNConf synchro issue when using USB Mode and autostart tunnel.
- Bug fixing: Autostart USB tunnel error "No thread found to handle IKE version 1 packet" fixed.
- Bug fixing: [DualToken] Fix on multiple partition token (automatic extraction detection)

2.23 TheGreenBow VPN Client 6.12 build 001

Features, improvements and fixes since release 6.11.003

- ~~Improvement: Support of TLS connection without user certificate.~~
- Improvement: Prevent broadcast transfers to remote network.

- Bug fixing: Import or export VPN Configuration to or from a mapped drive fails.
- Bug fixing: Packets with a payload smaller than 24 bytes are dropped in IPv6 VPN tunnel, causing issues for FTP.
- Bug fixing: Incoming packets ending with .255 on port 4500 are not handled properly.
- Bug fixing: 'TSocket message data type 0 could not be sent' error message preventing an IKEv1 VPN tunnel to open using an IPv6 IP address.
- Bug fixing: 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).

2.24 TheGreenBow VPN Client 6.11 build 003

Features, improvements and fixes since release 6.10.014

- Feature: Support of VPN Auto-Provisioning for IKEv2 VPN tunnels (OEM Partner specific).
- Improvement: Support of all 3 addressing modes i.e. host, subnet and IP address range with IKEv2 VPN tunnels.
- Improvement: Certificate Authority (CA) might or might not be specified when importing a P12 certificate within an IKEv2 VPN tunnel configuration.
- Improvement: 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.
- Improvement: New default Algorithms for Auto selections (OEM Partner specific).
- Bug fixing: Pre Shared Key can be saved with shortcut 'Crtl+S' without checking against the 'Confirm' field.

2.25 TheGreenBow VPN Client 6.10 build 014

Features, improvements and fixes since release 6.10.011

- Improvement: Various text strings and user interface improvements.
- Bug fixing: Error "disagreement on PFS" when configured with 'Auto' for PFS in IKEv1 Phase2 (gateway specific).

2.26 TheGreenBow VPN Client 6.10 build 011

Features, improvements and fixes since release 6.10.010

- Feature: Disable SHA-384 choice, IPsec IKEv2 VPN tunnel (OEM Partner specific).
- Improvement: Various user interface improvements.
- Improvement: VPN tunnel opens faster when using a certificate on a PKCS#11 Smartcard or Token.
- Bug fixing: The VPN Client might crash if import a VPN configuration file modified with wrong parameters for a VPN tunnel configured using IKEv1.

- Bug fixing: VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- Bug fixing: A new network interface is not detected when it becomes up.

Known issues:

- Known Issues: The VPN Client virtual network interface appears in 'Unidentified network' list in Windows Control Panel (Network).
- Known Issues: Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Known Issues: Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2).
- Known Issues: Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Known Issues: Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- Known Issues: The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- Known Issues: One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.
- Known Issues: Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- Known Issues: DPD continues after tunnel failure (IKEv1 only).

2.27 TheGreenBow VPN Client 6.10 build 010

Features, improvements and fixes since release 6.10.009

- Improvement: User interface improvements for IPsec IKEv2 VPN configuration (OEM partner specific):
- When selecting PSK or Certificate in VPN gateway (IKE Auth) while "Request config from gateway" is checked, a popup is displayed to the user requesting to uncheck it before pursuing.
- When checking "Request config from gateway" while PSK or Certificate is selected, a popup is displayed to the user suggesting to select EAP instead before pursuing.
- When creating a new VPN gateway (IKE Auth) the default User Authentication is PSK.
- When creating a new VPN connection (Child SA) "Request config from gateway" is unchecked by default.
- Improvement: User interface improvement for IPsec IKEv2 & IKEv1 VPN configuration:
- Root tree strings "IKE V1 Configuration" &"IKE V2 Configuration" might be truncated.

2.28 TheGreenBow VPN Client 6.10 build 009

Features, improvements and fixes since release 6.10.008

- Feature: IP address can change during renegotiation with VPN tunnel using IKEv2.
- Improvement: VPN tunnel IKEv2 and IPV6, replace mask with prefix length in the Child SA.
- Improvement: 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: VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv6 VPN tunnel is not opening properly.
- Bug fixing: VPN tunnel configured with IKEv2 and IPv6 toward a VPN gateway configured with IPv4 VPN tunnel is not opening properly.
- Bug fixing: 'View Certificate' button is not working properly with VPN tunnel using IKEv2, after saving the VPN configuration.
- Bug fixing: 'New Phase1' and 'Paste Phase1' menu from root tree not working properly.
- Bug fixing: VPN configuration with IKEv2 can be saved although Remote Gateway field is empty.
- Bug fixing: IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration.
- Bug fixing: VPN tunnel with IKEv2 CHILD SA negotiation in IKE AUTH exchange with Diffie-Hellman.
- Bug fixing: VPN tunnel with IKEv2, user must click twice on EAP button to have password enabled.
- Bug fixing: VPN tunnel with IKEv2, Pre Share Key is empty after saving the VPN Configuration.
- Bug fixing: VPN tunnel with IKEv2, the local/remote ID type of ID set to null is not working properly.
- Bug fixing: VPN tunnel with IKEv1, Auto for Phase 1 doesn't work.
- Bug fixing: VPN tunnel with IKEv1, X-Auth login/password popup is not working properly.
- Bug fixing: Change in configuration from IPv6 to IPv4 in VPN tunnel within IKEv2 Child SA is not detected.
- Bug fixing: 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.
- Bug fixing: VPN tunnel configured with IKEv2 and IPv4 toward a VPN gateway configured with IPv4, has no traffic if PFS=None.
- Bug fixing: New buttons in the Configuration Panel root IKEv1 and IKEv2 export all tunnels instead of particular branch tunnel.

- Bug fixing: Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- Bug fixing: Config Payload information in VPN tunnel configured with IKEv2 not displayed properly when tunnel opens or closes.
- Bug fixing: 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.
- Bug fixing: Word 'Static' appears in the Configuration Panel tree root IKEv1 and IKEv2.
- Bug fixing: Texts of protocol description displayed in the Configuration Panel tree for each protocol (i.e. IPsec IKEv1, IKEv2) are not corrects.
- Bug fixing: New buttons in the Configuration Panel root IKEv1 and IKEv2 export all tunnels instead of particular branch tunnel.

Known issues

- Known Issues: The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Known Issues: Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Known Issues: Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2).
- Known Issues: Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Known Issues: Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- Known Issues: The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- Known Issues: One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.
- Known Issues: VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- Known Issues: Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- Known Issues: DPD continues after tunnel failure (IKEv1 only).
- Known Issues: A new network interface is not detected when it becomes up. Workaround: quit and start the software.

2.29 TheGreenBow VPN Client 6.10 build 008

Features, improvements and fixes since release 6.10.006

- Bug fixing: VPN tunnel using IKEv2 opens only once when LocalId is not filled in with certificate subject.
- Bug fixing: The type IKEV2_ID_FQDN as remote ID Type is not yet supported.
- Bug fixing: Several text typos in Configuration Panel 'Child SA' or Phase2 tabs.
- Bug fixing: Phase renegotiation, on VPN tunnel with IKEv1, uses port 500 again instead of port 4500.
- Bug fixing: Shortcut Crtl+S doesn't save the remote sharing and Certificate store settings.
- Bug fixing: Feature blocking traffic outside VPN Tunnel (i.e. Split tunneling) with IKEv2 VPN tunnels is not yet available.
- Bug fixing: Notification FAILED_CP_REQUIRED with IKEv2 VPN tunnels received from the gateway closes the VPN tunnel unexpectedly.
- Bug fixing: The 'Initial Contact' mechanism is not yet supported with IKEv2 VPN tunnels.
- Bug fixing: VPN Configuration with IKEv2 is lost after transferring IPsec IKEv1 configuration to USB mode.
- Bug fixing: Remote ID ID_DER_ASN1_DN received from the gateway is not checked properly.
- Bug fixing: Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels.
- Bug fixing: SHA2 in 'Child SA' tab is not available yet with IKEv2 VPN tunnels.
- Bug fixing: DNS/WINS manual setup is not yet supported with IKEv2 VPN tunnels.

Known issues

- Known Issues: The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Known Issues: Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Known Issues: Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2).
- Known Issues: Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Known Issues: Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- Known Issues: The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- Known Issues: One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.

- Known Issues: VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- Known Issues: VPN tunnel with IKEv1 using SHA512 doesn't open properly.
- Known Issues: Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- Known Issues: DPD continues after tunnel failure (IKEv1 only).
- Known Issues: Texts of protocol description displayed in the Configuration Panel tree for each protocol (i.e. IPsec IKEv1, IKEv2) are not corrects.
- Known Issues: Word 'Static' appears in the Configuration Panel tree root IKEv1 and IKEv2.
- Known Issues: New buttons in the Configuration Panel root IKEv1 and IKEv2 export all tunnels instead of particular branch tunnel.

2.30 TheGreenBow VPN Client 6.10 build 006

Features, improvements and fixes since release 6.08.003

- Feature: TheGreenBow IPsec VPN Client becomes TheGreenBow VPN Client as it supports IPsec.
- Feature: 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) VPN tunnels.
- Ability to detect IPv4 or IPv6 network automatically for both IPsec VPN tunnels.
- Ability to send IPv4 and IPv6 within the same tunnel.
- 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, ..).
- Feature: 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.

- Feature: Supported OS: Windows Server 2003 32-bit, Server 2008 32/64-bit, Server 2012 32/64-bit, Vista 32/64-bit, Seven 32/64-bit, Windows 8/8.1 32/64-bit. TheGreenBow VPN Client 6.0 and further do not support Windows XP.
- Feature: Supported languages (25 languages). Arabic, Chinese simplified, Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai and Turkish.
- Improvement: All logs are now tagged by protocol (i.e. IPsec) with a new 'Facility' field.
- Improvement: Ability to select a specific network interface by its name (i.e. as displayed in 'Control Panel' > 'Network and Internet' > 'Network Connections') instead of an IP address.
- Improvement: All traces from console are now available in a text file with other logs when Trace/Debug mode is activated (i.e. Ctrl+Alt+D).
- Improvement: Several improvements on the reliability.
- Improvement: Names of virtual interface has been changed to be more meaningful (i.e. as displayed in the 'Control Panel' > 'Network and Internet' > 'Network Connections').
- Bug fixing: MiniPort driver uninstallation failure (i.e. error x023c) might occur when multiple upgrades from old releases.

Known issues

- Known Issues: The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Known Issues: Within VPN Configuration with two VPN Tunnels with the same virtual IP address, only the DNS/WINS server address of the first VPN tunnel is used. Workaround: use 2 different virtual IP addresses if DNS/WINS server addresses must be different for each VPN tunnel.
- Known Issues: DNS/WINS manual setup is not yet supported with IKEv2 VPN tunnels. Work around would be to enter IP address of the target machine or use Config Payload mode (i.e. equivalent to Config Mode in IKEv1).
- Known Issues: Traffic issues when having multiple tunnels opened toward the same remote network (single or multiple remote gateways) using different protocols (i.e. IKEv1 vs. IKEv2).
- Known Issues: Split tunneling can not be disabled with IKEv2 VPN tunnels. All internet traffic remains authorized. However, a work around would be forcing all traffic in the tunnel via a VPN config (i.e. 0.0.0.0 in remote network address).
- Known Issues: Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase2 (i.e. DH2, DH5).
- Known Issues: Multi-proposal with IKEv2 VPN tunnels is not yet supported.

- Known Issues: Both 'IKE SA' and 'Child SA' phases (equivalent to Phase1 and Phase2) renegotiation fails with IKEv2 VPN tunnels. Work around: set up a long time (e.g. 1 day) for 'IKE AUTH' and 'Child SA' Lifetime.
- Known Issues: IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration. Work around: Select your IP type for IDs (e.g. IP_IPv6_ADDR or IP_IPv4_ADDR) in 'IKE Advanced' tab > 'Identity' section and keep the value empty. For Config Payload mode, please proceed as follow in 'Child SA' tab:
- Uncheck 'Request configuration from gateway'
- Set VPN Client address to '0.0.0.0' (or '::' for IPv6)
- Set Remote LAN Address to '0.0.0.0' (or '::' for IPv6)
- Set Subnet Mask to '255.255.255.255' (or 'FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF' for IPv6)
- Check 'Request configuration from gateway'
- Known Issues: SHA2 in 'Child SA' tab is not available yet with IKEv2 VPN tunnels.
- Known Issues: The type IKEV2_ID_FQDN as remote ID Type is not yet supported.
- Known Issues: The 'Initial Contact' mechanism is not yet supported with IKEv2 VPN tunnels.
- Known Issues: The traffic indicator in the Connection Panel doesn't work properly with IKEv2 VPN tunnels.
- Known Issues: One Phase2 only can be created per Phase1 with IKEv2 VPN tunnels.

2.31 TheGreenBow IPsec VPN Client 6.08 build 003

Features, improvements and fixes since release 6.07.001

- Feature: OEM partner new branding.
- Bug fixing: Reception of fragmented packets in reverse order is not working properly.
- Bug fixing: Bad DPD handling when DPD reply from the gateway is lost, and the VPN Client resend a new DPD sequence.

2.32 TheGreenBow IPsec VPN Client 6.07 build 001

Features, improvements and fixes since release 6.05.001

- Bug fixing: A configuration with X-Auth and Mode Config (Push Mode) doesn't work properly when using Watchguard XTM 33W.
- Bug fixing: IKE process (TgbIke) might crash when the IP address is changing.
- Bug fixing: Packets with DF flag (i.e. Don't Fragment) are not handled properly in some specific circumstances.

2.33 TheGreenBow IPsec VPN Client 6.05 build 001

Features, improvements and fixes since release 6.04.001

- Feature: Support of Windows 8.1 32/64-bit.
- Bug fixing: The button 'Add WINS' server stays enabled after VPN tunnel opens in Mode-Config.
- Bug fixing: 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.
- Bug fixing: Wrong DNS server IP address format displayed after the VPN tunnel opens in Mode-Config.

2.34 TheGreenBow IPsec VPN Client 6.04 build 001

Features, improvements and fixes since release 6.02.001

- Feature: Ability to enter a machine name instead of an IP address when adding a Remote Sharing entry (i.e. 'Phase2' > 'Remote Sharing').
- Bug fixing: One of the log files is not created. This log file is used by our tech support for debug (OEM partners specific).
- Bug fixing: Config Mode tunnel fails with some Netgear routers (i.e. FVS318N, UTM25).
- Bug fixing: No connectivity to the DNS server when setting up an Alternative DNS in some very rare Windows configuration.
- Bug fixing: 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 (OEM partners specific).
- Bug fixing: License agreement is displayed in Spanish when choosing Italian during setup.

2.35 TheGreenBow IPsec VPN Client 6.02 build 001

Features, improvements and fixes since release 5.52.001

- Feature: Support of IPv4 and IPv6 protocols.
- Feature: Support of Diffie-Hellman Group 15 (3072-bit), Group 16 (4096-bit), Group 17 (6144-bit), Group 18 (8192-bit).
- Feature: Support of 2 new SHA2 algorithm: SHA2-384, SHA2-512. The IPsec VPN Client now supports SHA256-96, SHA256-128, SHA2-384, SHA2-512.
- Feature: Support of multiple DNS servers (2) per VPN Tunnel. They can be configured manually or, received from the VPN gateway in Mode Config.
- Feature: Ability to add a DNS suffix to DNS server addresses.

- Feature: 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.
- Feature: 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. Note: Windows XP is no longer supported, please download the previous release for Windows XP support.
- Feature: 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.
- Improvement: New IPv6 & IPv4 demo configuration file available here: www.thegreenbow.com/doc/tgbvpn_demo_ipv6.tgb.
- Improvement: 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.
- Improvement: More debug logs when user activates the Trace mode (Ctrl+Alt+D).
- Improvement: Ability to add a proxy to contact the Online Software Activation server via a new setup command line --proxy=http://thegreenbow.com:8080, --proxy=127.0.0.1.
- Improvement: 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'.
- Improvement: 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: IKE port and NAT ports not updated correctly upon VPN Configuration changes by user.
- Bug fixing: Unable to open tunnel (Phase 2 not completed) when forcing NAT-T in Transport Mode in the VPN Configuration.
- Bug fixing: DIR command (FTP protocol) doesn't work when trying to access a FTP server within a VPN tunnel, in some network circumstances.
- Bug fixing: No systray icon (taskbar) when Windows starts or after sleep mode, in some Windows configurations.
- Bug fixing: Multiple Phase1 with the same remote gateway addresses would not work properly.
- Bug fixing: 'Invalid Cookie' error message wrongfully displayed when SA expires during Phase1 renegotiation.

- Bug fixing: VPN tunnel may not re-open right after closing when the VPN Gateway is originating the closing (originator of the last DELETE payload).
- Bug fixing: Display of 'X-Auth warning' error message instead of 'Virtual Interface problem' when virtual interface issues detected.
- Bug fixing: VPN tunnel may not open properly when the VPN gateway rejects the request with a NO_PROPOSAL_CHOSEN error (e.g. possible reasons are encryption algorithm not supported, ..).
- Bug fixing: The icon 'tunnel opened' in the Configuration Panel tree might be displayed although VPN tunnel could not open in some cases where the computer opens the VPN tunnel really fast.
- Bug fixing: Old value for SHA2 header size for compatibility with some gateways.
- Bug fixing: Alternate DNS/WINS server addresses received via Mode Config are not immediately applied when opening tunnel in some circumstances.
- Bug fixing: The PKI Options parameter called KeyUsage is not taken into account by the Setup option.
- Bug fixing: Upgrade using silent install and setup installation options while the software is running might not complete properly.
- Bug fixing: Tunnel closes unexpectingly after wakeup from Windows sleep.
- Bug fixing: VPN tunnel does not open when Certificate received from the VPN Gateway contains a multi-valued subjectAltName field.
- Bug fixing: Selecting 'Any' interface (Configuration Panel > 'Phase1' > 'Interface') doesn't choose the correct network interface in some Windows configuration with other applications using network interfaces.
- Bug fixing: No VPN traffic when two Phase2 have the same IP address. Both VPN tunnel may have been configured this way or, when a VPN tunnel opens using Mode Config, then the VPN Client receives an IP address 10.10.10.100 (example) from the router while another VPN tunnel has been configured with the exact same IP address.
- Bug fixing: No VPN traffic when opening a VPN tunnel on a network interface with multiple IP addresses.
- Bug fixing: USB Token might not be detected if plugged in after the software started and the token was not used to create the VPN Configuration, even though the PKI option 'Use the first Token found on this computer' is checked.
- Bug fixing: VPN tunnel is not closing automatically when a Gemalto Dual .NET Token configured in the VPN Configuration is unplugged.
- Bug fixing: Crash when trying to import a localization file (i.e. strings in your language) if the file name is too long.

- Bug fixing: Unable to open tunnel when configuring 8 VPN tunnels with virtual IP address all set to 0.0.0.0.

Known issues

- Known Issues: The VPN Client virtual network interface appears in "Unidentified network" list in Windows Control Panel (Network).
- Known Issues: 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.