Windows Enterprise VPN Client 7.5

Release Notes

Latest update: 23 May 2024
Document reference number: 20240523_RN_VPE_7.5_EN_1.2

www.thegreenbow.com

Table of contents

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2024-01-22	All	Initial release	FB, FG, BB
1.1	2024-02-02	3.1 & 3.3	Rephrased for greater clarity	JK, BB
1.2	2024-05-23	3	Updated for build 007	BB

1 Preamble

The following release notes provide a detailed description of the features, improvements, fixes, known issues and limitations in the various releases of the Windows Enterprise VPN Client.

The product name has changed on several occasions over the years. Previous names include:

- TheGreenBow VPN Client
- TheGreenBow IPsec VPN Client

2 Major changes in version 7

2.1 Support for Windows 11

The 64-bit version of Windows 11 is now supported on x86-64 processors.

2.2 End of support for Windows 7 32/64-bit, Windows 8 32/64-bit, and Windows 10 32-bit

This version of the software is compatible with Windows 10 & 11 64-bit on x86-64 processors only. Should you need a VPN Client for Windows 7 32/64-bit, Windows 8 32/64-bit or Windows 10 32-bit, please use version 6.64 of the software.

2.3 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.

2.4 Gateway certificate check

By default, the gateway certificate will be checked each time a tunnel is opened. It may be necessary to import the complete chain of certification authorities (CAs) to authenticate the gateway, either into the Windows store or into the VPN configuration file.

You can change this default behavior, though we do not recommend doing so (**Options** menu -> **PKI Options**).

2.5 End of support for “weak” algorithms

For security reasons, this version no longer supports the following algorithms: DES, 3DES, MD-5, SHA-1, DH 1-2, DH 5. If a previous configuration contains one of these algorithms, the installer will convert them to “auto” (automatic negotiation with the gateway).

If the gateway only supports this type of algorithm, you will not be able to establish a connection with this version of the software.

3 Windows Enterprise VPN Client 7.5 build 007

Features, improvements, fixes, and known issues since release 7.5.006:

3.1 Features

- [Custom Version] The logo of a custom version has been updated to match the new graphic charter.

3.2 Improvements

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

3.3 Fixes

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

3.4 Known issues

- 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. One or the other should be chosen, failing which the VPN Client could have an undefined behavior.
- When migrating from an earlier version to a newer version, we recommend performing the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is 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

4 Previous versions

4.1 Windows Enterprise VPN Client 7.5 build 006

Features, improvements, fixes, and known issues since release 7.4.018:

4.1.1 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 logs 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 were migrated to version 3.0
- The **TrustedConnect Panel** and the **Connection Panel** now manage endpoint compliance dynamically based on the SCA’s status

4.1.2 Improvements

- 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

4.1.3 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 when the VPN Client was stopped and then restarted successively and repeatedly
- Fixes an issue that resulted in a system crash 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 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 longer any 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 not functioning
- Addresses a traffic issue, when Windows automatically updates the VPN driver
- [Custom version] Due to unsatisfactory algorithm suite proposals being generated, the **Auto** option has been removed from the algorithm selection drop-down lists

- [Custom Version] Fixes an issue where the SA payload formatting was incorrect in “Full IPsec Restricted” mode
- [Custom Version] Fixes an issue where configuring the EAP protocol was not possible

4.1.4 Known issues

- 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. One or the other should be chosen, failing which the VPN Client could have an undefined behavior.
- When migrating from an earlier version to a newer version, we recommend performing the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is 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

4.2 Windows Enterprise VPN Client 7.4 build 018

Fixes, limitations, and known issues since release 7.4.016:

4.2.1 Fixes

- 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

4.2.2 Limitations

- USB Mode: machine-specific configuration has been disabled in this version
- IPv4 within an IPv6 connection does not work with all configurations

4.2.3 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.3 Windows Enterprise VPN Client 7.4 build 016

Features, improvements, fixes, and known issues since release 7.3.007:

4.3.1 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

4.3.2 Improvements

- 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 customized 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

- [Customized version] Tunnel now opens automatically when a redundant gateway is defined and main gateway sends a DELETE request followed by a CREATE request
- [Customized version] Virtual network is forced to 32 when CP mode is not used

4.3.3 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 using an exploitation tool
- Fixes an issue where a long syslog server name would cause a buffer overflow
- [Customized version] Fixes an issue where an “incompatible format” error occurred when retrieving a configuration from an older gateway model
- [Customized version] Fixes an issue where the VPN Client would not accept a configuration file from a new gateway model that supports SHA-2 signature algorithms
- [Customized version] 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

- [Customized version] SHA-1 hash algorithm has been reintroduced to support older equipment
- [Customized version] 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
- [Customized version] RSASSA-PKCS1-V1_5 signature scheme has been reverted as default to support older equipment

4.3.4 Limitations

- USB Mode: machine-specific configuration has been disabled in this version
- IPv4 within an IPv6 connection does not work with all configurations

4.3.5 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.4 Windows Enterprise VPN Client 7.3 build 007

Features, improvements, fixes, and known issues since release 7.2.008:

4.4.1 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

4.4.2 Improvements

- 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

4.4.3 Fixes

- DSCP fields are now properly handled in ESP packets that are created
- VPN Client no longer crashes when waking up from 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

4.4.4 Limitations

- USB Mode: machine-specific configuration has been disabled in this version

4.4.5 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.5 Windows Enterprise VPN Client 7.2 build 008

Features, improvements, fixes, and known issues since release 6.87.109:

4.5.1 Features

- Implements Zero Trust Network Access (ZTNA) principles for better workstation protection
- Adds a feature to filter data flows combined with captive portal detection (CPD)
- Introduces new algorithm: Diffie-Hellman 28 (BrainpoolP256r1)
- Introduces certificate authentication method ECDSA BrainpoolP256r1 with SHA-2 (256 bits)
- Uses certificate authentication method 14 RSASSA-PSS by default with all RSA certificates
- Verification of the user certificate CRL has become optional
- Forces UDP encapsulation mode for IKEv2
- User interface now allows adding more than 3 CAs
- Increases the number of subnetworks supported to 16
- Window height of the **Connection Panel** window can now be increased or decreased

4.5.2 Improvements

- Greater stability of the IKE module
- Better performance of AES-GCM encryption
- User interface color scheme and bitmaps have been updated to match the new graphical charter
- Weak algorithms have been removed for SSL/OpenVPN: MD5, SHA1, TLS low security suite, BF-CBC
- Weak algorithms have been removed for IKEv2: DES, 3DES, MD5/PRF_HMAC_MD, SHA1/PRF_HMAC_SHA1, SHA2/PRF_HMAC_SHA2_224, DH 1 (modp768), DH 2 (modp1024), DH 5 (modp1536)
- IKEv1 has been removed
- RSA certificates with a key size smaller than 2048 bits are now rejected
- ECDSA certificates with a key size smaller than 256 bits are now rejected
- Software version information has been added to MSI properties
- OpenSSL has been updated to version 1.1.1l
- New Gemalto Safenet smart cards are now detected automatically
- Systray fade-out pop-up is now deactivated by default
- LZ4 library has been updated to version 1.9.3 for OpenVPN
- User interface now only allows adding CAs in the **CA Management** dialog box

- KeyUsage extensions of user and gateway certificates are now checked in line with ANSSI rules
- All CAs of a P12 file are now imported into the VPN configuration
- Uses HMAC 256 instead of SHA-2 (256 bits) hash for VPN configuration file signature
- Passwords for encrypting exported configurations must now be at least 16 characters in length

4.5.3 Fixes

- Fixes freezes when selecting Arabic or Greek language
- Fixes rare issues with how the TrustedConnect status is displayed
- Users can now refuse to use a fallback tunnel even when no message is displayed
- Fixes some issues with the Filtering Mode
- Fixes issue with IKEv2 fragmentation when using AES-GCM
- Various cosmetic and stability improvements

4.5.4 Limitations

- USB Mode: machine-specific configuration has been disabled in this version

4.5.5 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.6 Windows Enterprise VPN Client 6.87 build 109

Fixes and known issues since release 6.87.108:

4.6.1 Fixes

- Fixes various TrustedConnect stability issues
- 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 TrustedConnect Filtering Mode issues when switching to a USB-C network adapter

4.6.2 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.7 Windows Enterprise VPN Client 6.87 build 108

Improvements, fixes, and known issues since release 6.87.001:

4.7.1 Improvements

- Support for multiple smart cards/tokens with CNG
- Updates OpenSSL to version 1.1.1n to increase security level
- **Connection Panel** is now displayed automatically upon startup

4.7.2 Fixes

- Fixes an issue that prevented VPN Client from quitting in rare cases
- PIN caching now works when logging back in after locking session
- Fixes an issue with RSA/SHA512 certificates
- Fixes a rare crash in **Connection Panel** when quitting
- Fixes a DPD issue after a retransmission
- Fixes an issue that occurred when a DELETE is not followed by a RECV and causes an error in TrustedConnect mode
- CA no longer disappears after unchecking EAP pop-up
- Fixes a Trusted Network Detection issue
- Fixes a Local ID issue during authentication
- Fixes activation issues during update
- Activation now works in https
- Includes a security fix to prevent buffer overflow on response from activation server
- DNS modifications on physical interface are now applied after virtual IP change during SA Auth Rekey
- Always-On now automatically reconnects to a Wi-Fi network with a different SSID
- Default driver registry keys are now set during update
- Fixes an issue with Yubikey 5 NFC
- Fixes license backup incompatibility during upgrade
- Fixes unexpected error “Code 103: DNS Error”
- Fixes VPNLogPurge option

4.7.3 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.8 Windows Enterprise VPN Client 6.87 build 001

Features, improvements, fixes, and known issues since release 6.86.015:

4.8.1 Features

- Each tunnel can now independently use automatic user certificate selection
- MSI property `TOKENOUTHANDLE` (originally for TrustedConnect) can now be used for the **Connection Panel**

4.8.2 Improvements

- Added an MSI property to avoid scanning entire `ProgramData` directory
- Added a dynamic parameter for choosing the virtual network interface type (public or private)

4.8.3 Fixes

- Fixes invalid syntax when sending cipher proposals in OpenVPN automatic mode
- Fixes a disconnection issue over Wi-Fi with TrustedConnect
- Fixes PIN caching issues with SafeNet tokens and smart cards
- Fixes an issue when using MSI property `SIGNFILE=1`
- MSI properties `CERT` and `OSACERT` can now be used interchangeably to specify a certificate for TAS
- Fixes an issue where TrustedConnect failed to authenticate remote endpoint
- Fixes an IKEv2 fragmentation issue when using AES-GCM
- Fixes an IKEv2 fragmentation issue when resending lost packets
- Fixes an issue in the **Connection Panel** that only closed the tunnel the first time a token is removed
- All `tgbcode*.dat` and `tgbparam*.dat` files are now copied during an upgrade
- Fixes `OSACheck` issue and disabled `OSACheck` upon uninstall
- Fixes an issue that deleted license file when upgrading from 6.6x to 6.86 with a new license
- Fixes an issue where TrustedConnect remained stuck in “Connecting” status
- Fixes an issue that prevented a license from being freed up on TAS when uninstalling the VPN Client
- Cisco configuration files (.pcf) are no longer supported and are no longer suggested in the configuration file explorer window

- Fixes an issue when reading the subject of a certificate encoded in BMPString

4.8.4 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.9 Windows Enterprise VPN Client 6.86 build 015

Features, improvements, fixes, and known issues since release 6.85.007:

4.9.1 Features

- Admin can now disable “blue vs green” info identifying direct connections to the trusted network

4.9.2 Improvements

- OpenSSL has been updated to version 1.1.1l
- Configuration files from OpenVPN version 2.4.7 and higher are now supported
- Silent activation can now be performed even when trial period has expired

4.9.3 Fixes

- TrustedConnect: Corrects an issue that potentially allowed disabling Filtering Mode during a connection error
- TrustedConnect: Corrects an issue that sometimes showed the tunnel as closed, even though it was open
- TrustedConnect: Corrects an issue that displayed Code 9 (no response from gateway) after key renewal, even though traffic is still flowing
- TrustedConnect: The panel now quits properly when the “About” window is open
- Corrects an issue in which a socket was sometimes created on port 500/4500 when not required
- ACL of activation data is now correctly restored during an upgrade from older versions
- Fixes special character encoding issues during an upgrade from older versions
- Fixes an issue in which older versions of the software could not be reinstalled if MSI installation failed
- License activation is now correctly reset after uninstalling

- Fixes a rare issue in which the Activation Windows popped up after silent activation
- Existing licenses are now correctly taken into account during an upgrade from older versions
- MSI property `VPNLOGPURGE` is now correctly taken into account
- PKCS#11 middleware configuration for smart card readers/tokens are now correctly set during an upgrade from older versions
- Tunnel now closes when smart card reader/token is pulled out
- Fixes an issue with the silent upgrade when `%TEMP%\vpncfg.bak` file was present
- MSI properties `NOPINCODE`, `SIGNFILE`, and `TOKENOUTHANDLE` are now correctly managed
- Adds some missing translations
- **Disable Split tunneling** option is unchecked by default for IKEv1 (as for IKEv2)
- `VpnConf.ini` file is now kept during upgrade

4.9.4 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.10 Windows Enterprise VPN Client 6.85 build 007

Features, improvements, fixes, and known issues since release 6.64.003:

4.10.1 Features

- New MSI installer
- New TrustedConnect user interface
- Silent software update from previously installed editions, including recovery of license, VPN security policy and installation parameters
- Configurable Always-On mode
- Configurable Trusted Network Detect mode
- Adds support for Microsoft CNG API
- Adds support for RFC 4304 Extended Sequence Number (ESN)
- Adds support for RFC 6023 (Childless IKE Initiation)
- Adds support for certificate authentication using SHA-2 (Method 9) [RFC 4754]
- Adds support for certificate authentication using RSA (Method 14) [RFC 7427]
- Imports PKCS#12 formatted certificates from the command line
- VPN security policy access restricted to Windows administrator (specific password no longer needed)
- Adds support for Lz4 compression for OpenVPN/SSL

4.10.2 Improvements

- Updated SSL library to version 1.1.1.i
- Explicit request for DNS (for compatibility with Fortinet gateways)
- Compiled for Windows 10 64-bit
- Encrypts VPN security policies using SHA-2
- Removed weaker algorithms (DES, 3DES, SHA, MD5, DH 1-2, DH 5)
- After connecting to a redundant gateway, the next time the tunnel is opened, the VPN Client tries to switch back to the main gateway
- Auto reconnect when getting back from sleep mode

4.10.3 Fixes

- Tunnel now closes when smart card reader is pulled out

4.10.4 Known issues

- SSL tunnel creation wizards defaults to IKEv2 tunnel creation

4.11 TheGreenBow VPN Client 6.64 build 003

Fixes since release 6.64.002:

4.11.1 Fixes

- [Partner Specific] Activation wizard: the **Buy a license** link is dead

4.12 TheGreenBow VPN Client 6.64 build 002

Fixes since release 6.64.001:

4.12.1 Fixes

- Multiple networks on several tunnels is not working properly on single virtual IP.
- DistVPN should handle several PKCS11 DLL providers.
- No traffic with AESGCM for particular packet sizes.

4.13 TheGreenBow VPN Client 6.64 build 001

Features, improvements, and fixes since release 6.63.005:

4.13.1 Features

- Disable script execution (partner specific).
- Update OpenSSL to 1.1.1.
- IKEv2 Multiple Phase 2.

4.13.2 Improvements

- Possibility to modify the coordinates of the GINA window, and also the “foreground” mode

4.13.3 Fixes

- Winstore roaming with keyusage and dnpattern doesn’t work properly
- EAP Multiple Auth tunnel opens without certificate
- “No socket” error after resume from standby/hibernation
- TgbLogonUI: When renegotiating IKEV2 Auth tunnel displayed state is not correct
- Certificate not taken into account when importing the configuration (partner specific)

4.14 TheGreenBow VPN Client 6.63 build 005

Fixes since release 6.63.001:

4.14.1 Fixes

- When GINA mode is enabled, the **Configuration Panel** may sometimes be empty (no VPN tunnel) after windows restart.
- Crash when receiving a gateway certificate which contains a specific `SubjectAltName`.

4.15 TheGreenBow VPN Client 6.63 build 001

Fixes since release 6.62.003:

4.15.1 Fixes

- “Incorrect Password” when trying to update a previous installation with **Configuration Panel** access locked by password.
- Command line password doesn’t work.
- [Customized version] Unable to access to the GUI after setting a password.

4.16 TheGreenBow VPN Client 6.62 build 003

Improvements and fixes since release 6.62.002:

4.16.1 Improvements

- Implemented a new software activation library.

4.16.2 Fixes

- Opening an IKEv2 tunnel with 0.0.0.0 as a VPN Client address may cause routing issues.
- Unable to set IPV6 Phase 2 for an IKEv1 Tunnel.

4.17 TheGreenBow VPN Client 6.62 build 002

Features, vulnerabilities, and fixes since release 6.60.009:

4.17.1 Features

- Displays “No CRL” instead of “No CA” in console where appropriate.
- New URL for customized release.

4.17.2 Vulnerabilities

- Fixes an issue in which a man-in-the-middle attack was possible using a CA stored in the Windows certificate store.
- Disables the ability to start a browser for captive portal authentication.
- Fixes an issue in which the certificate date validity could be bypassed using the GeneralizedTime format.

- Resolves a DOS vulnerability when a malformed certificate was received.
- Resolves a DOS vulnerability while the software is in trace mode, with a UDP packet flood.
- Fixes an issue in which some padding bytes of the VPN configuration file signature could be patched.
- Addresses an issue which could lead the software to crash upon receiving a malformed SA.
- Resolves an issue in which listen port 1194 was open even if not required.
- Improves CA handling in Windows Certificate Store

4.17.3 Fixes

- BSOD: Crash in `ForwardIPPacket` when using `FwpsQueryPacketInjectionState0`
- BSOD after VPN up
- Smart card roaming with different readers (`smartcardroaming=5`) doesn't work for IKEv1
- Unable to enter a lifetime in the main interface
- Display of a French button
- Error upon certificate selection with `keyusage = 3`
- With some specific PKI configurations, tunnel opens only once

4.18 TheGreenBow VPN Client 6.60 build 009

Features, improvements, and fixes since release 6.45.002:

4.18.1 Features

- VPN Tunnel Fallback (for example: automatic fallback from an IPsec tunnel to an SSL tunnel when IPsec tunnel fails)
- Implemented administration and system logs, with ability to produce administration logs either locally, to the Windows Event Manager or to a Syslog Server
- Re-integrated “Multiple Auth Support” checkbox, Zyxel GW now supports RFC 4739.
- Windows Store Certificate Roaming: Ability to automatically select the user certificate from the Windows Certificate Store, based on criteria (like for smart cards)
- Ability to select and store multiple CA (Certificate Authority) in the VPN Configuration
- Adds support for Elliptic curve Diffie-Hellman (Diffie-Hellman group 19, 20, 21) for IKEv2
- Adds support for AES-GCM & AES CTR algorithms for IKEv2

- Update OpenSSL library version
- SSL: Add a way to change the receive socket buffer size (SO_RCVBUF)
- SSL: Support for multiple remote networks
- Option to disable DPD IKEv2
- IKEv2: Support for multiple networks in the same remote TS, in CP mode
- 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)
- Ability to configure wait time for gateway responses (timeout was previously set to 5 sec.)
- Adds support for IAS smart card
- Adds support for ID Prime MD smart card
- Adds support for Gemalto MD smart card ATR
- Set ERRORLEVEL on /add, /replace, /importonce commands
- Adds support for Microsoft Signing for W10 drivers
- Prevent tunnels to work when several users are logged simultaneously
- when rekeying, asking for X-Auth credentials is now configurable
- Time-out on token PIN Code popup
- Handling of PKCS8 (in addition to PKCS1) Private Key format

4.18.2 Improvements

- Handling of uppercase/lowercase certificates “name” OID
- IKE Port change is supported for more gateway configurations
- Optimize VPN configuration loading and saving
- Gina mode: Progress bar for IKEv2 and SSL enhanced
- DPD, lifetime and IKE Ports are configurable for each tunnel
- IKEv2 doesn't support PKCS#8 private key format, but only PKCS#1
- Remote Sharing: RDP is not opened automatically from **Configuration Panel**
- `vpnconf /stop` doesn't work from another user session
- PIN code is no more asked when the Phase 1 is already up

4.18.3 Fixes

- (Specific Partners) DH algo default is not set to “No”
- IKEv2 Fragmentation issue: some fragment sizes lead to Auth Fail or Syntax Error
- BSOD when receiving data in tunnel with a high rate
- IKEv2 and TPM: Unable to import user certificate in internal store
- DN pattern doesn't work properly for IKEv2
- IKE SA renegotiation fails with a Fortigate Gateway
- Remote ID mismatch on “DER ASN1 DN” with the same ASCII string
- Virtual interface: bad handling of ARP table to add/remove gateway IP address

- TLS Connection: renewal from gateway is not implemented, and tunnel closes after a while
- Error with 6.4x VPN Configuration using certificates with accents on smart cards
- Conversion tools: Ovpn2Tgb: verify-x509-name is not properly handled
- IKEv2: Sometimes tunnel doesn't open, IKE Initialization fails (error with “0”)
- IKEv2: No traffic to remote network.VirtualItf error 1 - 209 - 5010
- IKEv2: Exporting a Single tunnel exports all Child SA
- IKEv1: Tunnel is not deleted when XAuth fails during a Phase 1 renegotiation
- Cannot open tunnel with a token inserted after the VPN Client starts
- IKEv2 child SA is not removed when tunnel is closed for DPD timeout reason
- IKEv2: no traffic when NATT port is changed for one tunnel, and UDP Encap enabled
- IKEv2: IPV4 DNS not set properly when Gateway sends an IPV6 address
- IKEv1 Traffic verification: 1st timer is not properly initialized

4.19 TheGreenBow IPsec VPN Client 6.45 build 002

Fixes since release 6.45.001:

4.19.1 Fixes

- IKEv2: Fragmentation IKEv2 and DH algo set to auto => fragmentation is not selected.
- InjectP12 command: new cert not updated when closing the session.
- IKEv2 Fragmentation issue: some fragment sizes lead to Auth Fail or Syntax Error.
- IKEv2: Sometimes tunnel doesn't open, IKE Init fails (error with “0”)
- IKEv1 Fragmentation: Cisco Vendor ID is not correctly sent.

4.20 TheGreenBow IPsec VPN Client 6.45 build 001

Features and fixes since release 6.44.004:

4.20.1 Features

- Fragmentation of IKEv1 based on MS-IKE doc.

4.20.2 Fixes

- Traffic issue when physical IP Address ends with .255 and virtual IP address = Physical IP address.

4.21 TheGreenBow VPN Client 6.44 build 004

Improvements since release 6.44.003:

4.21.1 Improvements

- [Partner Specific] New URL on client VPN.

4.22 TheGreenBow VPN Client 6.44 build 003

Features, improvements, and fixes since release 6.43.002:

4.22.1 Features

- (Partner Specific) DH default algorithm is set to “No DH”.

4.22.2 Improvements

- SSL VPN: Reception Socket buffer sizes are increased to accept traffic peaks.

4.22.3 Fixes

- Remote ID mismatch on “DER ASN1 DN” with the same ASCII string.
- IKEv2: DPD handling: Tunnel was closing when one DPD message is lost.
- IKEv2 child SA is not removed when tunnel is closed for DPD timeout reason.
- Could not open tunnel with mixed SubjectAltName containing an IP address.
- IKEv1: Traffic verification with pings doesn't work properly.
- No traffic when virtual IP address ends with .255.
- SSL VPN: When using TCP mode the tunnel may close unexpectedly.
- Silent install is not silent on Windows Seven.
- Bad renewal certificate used on the smart card.
- IKE SA renegotiation failed with a Fortigate gateway.
- IKE SA renegotiation failed in a CHILD SA.

4.23 TheGreenBow VPN Client 6.43 build 002

Features, improvements, and fixes since release 6.43.001:

4.23.1 Features

- Adds support for Microsoft Signing for W10 drivers.

4.23.2 Improvements

- Improved automatic software activation when subscription is about to expire.
- Improved software activation mechanism if activation errors occur.

4.23.3 Fixes

- Error message “driver not signed” when installing VPN Client on Windows 10 with UEFI BIOS option Secure Boot Enabled.
- IKEv2 EAP MultipleAuth tunnel closed after key renewal.
- IKEv2 Multiple Auth: When changing an option in IKE SA Tab, certificate vanishes.

4.24 TheGreenBow VPN Client 6.43 build 001

Features and fixes since release 6.41.003:

4.24.1 Features

- Re-integrated “Multiple Auth Support” checkbox and vendor ID for specific partner.

4.24.2 Fixes

- With EAP and Multiple Auth, tunnel closed after key renewal in some case.

4.25 TheGreenBow VPN Client 6.41 build 003

Features and fixes since release 6.41.002:

4.25.1 Features

- Added a notification to let users know GINA mode will not work when VPN rules in USB.

4.25.2 Fixes

- Wrong PIN code error occurs during Phase 1 renewal in some case.

4.26 TheGreenBow VPN Client 6.41 build 002

Features and fixes since release 6.41.001:

4.26.1 Features

- When mounting several tunnels at the same time, PIN code is asked several times.

4.26.2 Fixes

- PIN code is asked at each Phase 1 renewal.

4.27 TheGreenBow VPN Client 6.41 build 001

Features and fixes since release 6.40.006:

4.27.1 Features

- Re-branding Client customization.
- PIN code requests mutualizing when building several tunnels.
- A warning is displayed when trying to build an IPv4/IPv6 tunnel with no virtual IP address (OEM Partner specific).

4.27.2 Fixes

- Bad X-Auth password leads to a software error.
- Socket bind fails when executed too quickly after interface is up.
- Polish translation of the VPN Client.
- Correct default DPD values are set when importing a configuration without DPD.
- TgbIkeNg daemon not stopped on fast shutdown on Windows 10.

4.28 TheGreenBow VPN Client 6.40 build 006

Features and fixes since release 6.40.005:

4.28.1 Features

- New VPN Client customization.

4.28.2 Fixes

- Font size fixed in **Connection Panel** (title and open button).

4.29 TheGreenBow VPN Client 6.40 build 005

Improvements and fixes since release 6.40.004:

4.29.1 Improvements

- 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).
- TLS tunnel: TlsAuth option worked only with SHA1 Authentication algorithm. TlsAuth is now possible with all authentication algorithms (SHA256, SHA 512, etc.).
- TLS tunnel: TlsAuth option is also operational with key direction set to client or server.
- All opened tunnels are properly closed when Windows shutdowns quickly.

4.29.2 Fixes

- Windows 10: When the user session is locked, the VPN GINA is not displayed.
- Configuration with Virtual IP set to “::” doesn't work.
- No virtual interface when virtual IP is not specified, and remote network is a range of address
- The Gateway Certificate CRL was checked despite this checking is disabled.
- Crash IKE on specific UNITY_DEF_DOMAIN values sent by the gateway (Mode config / Mode CP).

4.30 TheGreenBow VPN Client 6.40 build 004

Improvements and fixes since release 6.40.003:

4.30.1 Improvements

- New parameters are backed up and restored during a software update.

4.30.2 Fixes

- **Configuration Panel** and **Connection Panel** synchronization improvement.

4.31 TheGreenBow VPN Client 6.40 build 003

Features, improvements, and fixes since release 6.30.005:

4.31.1 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 Wi-Fi 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.
- Adds support for 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: Adds support for 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
- Adds support for UTF-8 character encoding for X-Auth password (requires a specific configuration)

4.31.2 Improvements

- In accordance with the development of the new **Connection Panel**, the system tray menu has been simplified
- Ability to disable the function **Automatically 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 IKEv1phase 1 renegotiation 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
- Adds support for the suffix domain name (Cisco extension: UNITY_DEF_DOMAIN/28674) when received through Mode Config/ Mode CP
- Various improvements in the subscription mode management (VPN Premium only)

- The GINA Mode correctly handles the subscription mode (VPN Premium only)
- 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 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 automatically open 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.
- Improvement of the smart card management (VPN Premium only)
- Adds support for 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.

4.31.3 Fixes

- Correct management of the virtual interface MTU
- The **Configuration Panel** and the **Connection Panel** might appear simultaneously.
- Corrected font in Activation window
- Changing language led to address type duplication (in Child SA configuration)
- Deleting a Child SA among N led to the alert: “An invalid argument was encountered”
- 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.
- Adds support for certificates containing multiple subjectaltnames (IKEv1)

4.32 TheGreenBow VPN Client 6.30 build 005

Features and fixes since release 6.30.004:

4.32.1 Features

- New customization of VPN Client

4.32.2 Fixes

- Wrong word on popup message

4.33 TheGreenBow VPN Client 6.30 build 004

Fixes since release 6.30.003:

4.33.1 Fixes

- Missing word “confirm” in IKE V2 settings.

4.34 TheGreenBow VPN Client 6.30 build 003

Improvements since release 6.30.002:

4.34.1 Improvements

- Updated German

4.35 TheGreenBow VPN Client 6.30 build 002

Features, improvements, and fixes since release 6.30.001:

4.35.1 Features

- Ability to hide the activation window which normally appears at the end of a subscription period

4.35.2 Improvements

- DPD mechanism improvement
- Ercom smart card 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.

4.35.3 Fixes

- 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

4.36 TheGreenBow VPN Client 6.30 build 001

Features, improvements, and fixes since release 6.21.002:

4.36.1 Features

- Windows 10 full compatibility
- New Token interoperability with Feitian epass2003 and Gemalto/Axalto .net
- Compatibility with Fortinet FortigateIKEv2. TheGreenBow VPN Client is the only VPN Client which can be used to open an IKEv2 tunnel with a Fortigate gateway.
- New ErcomCryptoSmart Micro SD support for IKEv1, IKEv2 and SSL
- New XiringPinpad 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.

4.36.2 Improvements

- IKEv1 – DPD mechanism tunnel correctly closes on DPD failure and gateway renegotiation, DPD stays on upon network disconnection, DPD timer management is tuned.
- When a VPN Configuration is created with the Wizard, the default parameters are DH Group = Auto and Aggressive Mode = TRUE (set)
- smart card management improvement
- Debug/Trace mode can be activated from any window/panel of the VPN Client (**Configuration Panel**, **Connection Panel**, or **Console**).

- 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.

4.36.3 Fixes

- 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.
- tunnel opening or closing process is stopped on IKE reset
- 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.

4.37 TheGreenBow VPN Client 6.21 build 002

Fixes since release 6.21.001:

4.37.1 Fixes

- The wizard works when Client only uses one protocol.

4.38 TheGreenBow VPN Client 6.21 build 001

Improvements and fixes since release 6.20.007:

4.38.1 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) Phase 1 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”.

4.38.2 Fixes

- (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)

4.39 TheGreenBow VPN Client 6.20 build 007

Features and fixes since release 6.20.005:

4.39.1 Features

- Default parameters (OEM Partner specific).

4.39.2 Fixes

- With Mode Config on IKEv1, Phase 2 establishment could fail.

4.40 TheGreenBow VPN Client 6.20 build 005

Features, improvements, and fixes since release 6.20.001:

4.40.1 Features

- New Certificate's OIDs supported.
- Adds support for nested tunnels between different protocols
- New Configuration Wizards for IKEv2 and SSL tunnels
- Adds support for the Ingenico “Leo” Pinpad
- Possibility of certificate injection via a command line option (online certificate injection)
- Adds support for Freebox compatibility
- Automatic importation and translation mechanism for OpenVPN (.ovpn) and Cisco (.pcf) files

4.40.2 Improvements

- Dynamic display of Config Payload Mode information for IKEv2/IPV6.
- IKEv2: Adds support for 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.

4.40.3 Fixes

- DPD still working when “split tunneling” is enabled.
- IKEv1 “Automatic” mode works for Phase 1 encryption when gateway reports AES.
- Modification of IKE port and NAT port (IKEv1 parameters) is fixed.
- Improvement of Token removal detection.

4.41 TheGreenBow VPN Client 6.20 build 001

Features, improvements, and fixes since release 6.12.001:

4.41.1 Features

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

4.41.2 Improvements

- Allow to use a self-signed Root Certificate from Windows Certificate Store.
- USB Mode Confirmation popup only appears when required.

4.41.3 Fixes

- [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)

4.42 TheGreenBow VPN Client 6.12 build 001

Improvements and fixes since release 6.11.003:

4.42.1 Improvements

- Adds support for TLS connection without user certificate.
- Prevent broadcast transfers to remote network.

4.42.2 Fixes

- 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).

4.43 TheGreenBow VPN Client 6.11 build 003

Features, improvements, and fixes since release 6.10.014:

4.43.1 Features

- Adds support for VPN Auto-Provisioning for IKEv2 VPN tunnels (OEM Partner specific).

4.43.2 Improvements

- Adds support for 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 (OEM Partner specific).

4.43.3 Fixes

- Pre-shared Key can be saved with shortcut “Crtl+S” without checking against the “Confirm” field.

4.44 TheGreenBow VPN Client 6.10 build 014

Improvements and fixes since release 6.10.011:

4.44.1 Improvements

- Various text strings and user interface improvements.

4.44.2 Fixes

- Error “disagreement on PFS” when configured with “Auto” for PFS in IKEv1 Phase 2 (gateway specific).

4.45 TheGreenBow VPN Client 6.10 build 011

Features, improvements, fixes, and known issues since release 6.10.010:

4.45.1 Features

- Disable SHA-384 choice, SSL and IPsec IKEv2 VPN tunnel (OEM Partner specific).

4.45.2 Improvements

- Various user interface improvements.
- VPN tunnel opens faster when using a certificate on a PKCS#11 smart card or token.
- All settings in the “Security” tab are set to “Auto” mode when creating a new SSL VPN tunnel.

4.45.3 Fixes

- 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.

4.45.4 Known issues

- The VPN Client virtual network interface appears in “Unidentified network” list in Windows Control Panel (Network).
- 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.
- 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 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase 2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the **Connection Panel** doesn't work properly with IKEv2 VPN tunnels.
- One Phase 2 only can be created per Phase 1 with IKEv2 VPN tunnels.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- DPD continues after tunnel failure (IKEv1 only).

4.46 TheGreenBow VPN Client 6.10 build 010

Improvements since release 6.10.009:

4.46.1 Improvements

- 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.
- User interface improvement for IPsec IKEv2 & IKEv1 VPN configuration:
  - Root tree strings “IKE V1 Configuration” & “IKE V2 Configuration” might be truncated.

4.47 TheGreenBow VPN Client 6.10 build 009

Features, improvements, fixes, and known issues since release 6.10.008:

4.47.1 Features

- IP address can change during renegotiation with VPN tunnel using IKEv2.
- SSL disabled (OEM partner specific).

4.47.2 Improvements

- VPN tunnel IKEv2 and IPV6, replace mask with prefix length in the Child SA.
- New menu strings to create a Phase 1 and Phase 2 consistent between IKEv1 and IKEv2 now called “New VPN Gateway” and “New VPN Connection” accordingly.

4.47.3 Fixes

- 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 Phase 1” and “Paste Phase 1” 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, Preshared 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 Phase 1 and Phase 2) 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 30 s 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.

4.47.4 Known issues

- The VPN Client virtual network interface appears in “Unidentified network” list in Windows Control Panel (Network).
- 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.
- 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 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase 2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the **Connection Panel** doesn't work properly with IKEv2 VPN tunnels.
- One Phase 2 only can be created per Phase 1 with IKEv2 VPN tunnels.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- DPD continues after tunnel failure (IKEv1 only).
- A new network interface is not detected when it becomes up. Workaround: quit and start the software.

4.48 TheGreenBow VPN Client 6.10 build 008

Fixes and known issues since release 6.10.006:

4.48.1 Fixes

- VPN tunnel using IKEv2 opens only once when Local ID 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 Phase 2 tabs.
- Phase renegotiation, on VPN tunnel with IKEv1, uses port 500 again instead of port 4500.
- Shortcut Crtl+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 Phase 1 and Phase 2) 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.

4.48.2 Known issues

- The VPN Client virtual network interface appears in “Unidentified network” list in Windows Control Panel (Network).
- 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.
- 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 vs. SSL).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase 2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- The traffic indicator in the **Connection Panel** doesn't work properly with IKEv2 VPN tunnels.
- One Phase 2 only can be created per Phase 1 with IKEv2 VPN tunnels.
- VPN tunnel imported which uses a port that no other tunnel is using, doesn't open properly.
- VPN tunnel with IKEv1 using SHA512 doesn't open properly.
- Traffic detection is not working properly with Config Payload mode enabled (i.e. equivalent to Config Mode in IKEv1).
- DPD continues after tunnel failure (IKEv1 only).
- Texts of protocol description displayed in the **Configuration Panel** tree for each protocol (i.e. SSL, IPsec IKEv1, IKEv2) are not corrects.
- Word “Static” appears in the **Configuration Panel** tree root IKEv1, IKEv2 and SSL.
- New buttons in the **Configuration Panel** root IKEv1, IKEv2 and SSL export all tunnels instead of particular branch tunnel.

4.49 TheGreenBow VPN Client 6.10 build 006

Features, improvements, fixes, and known issues since release 6.08.003:

4.49.1 Features

- TheGreenBow IPsec VPN Client becomes TheGreenBow VPN Client as it supports IPsec and SSL.
- Adds support for 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.
- Adds support for 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 TLS-Auth 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, etc.).
- Adds support for 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.
- 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.
- 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.

4.49.2 Improvements

- All logs are now tagged by protocol (i.e. IPsec vs SSL) with a new “Facility” field.
- 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.
- 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).
- Several improvements on the reliability.
- Names of virtual interface has been changed to be more meaningful (i.e. as displayed in the “Control Panel” > “Network and Internet” > “Network Connections”).

4.49.3 Fixes

- MiniPort driver uninstallation failure (i.e. error x023c) might occur when multiple upgrades from old releases.

4.49.4 Known issues

- The VPN Client virtual network interface appears in “Unidentified network” list in Windows Control Panel (Network).
- 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.
- 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).

- 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 vs. SSL).
- Split tunneling cannot be disabled with IKEv2 and SSL 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).
- Multi-proposal with IKEv1 VPN tunnels is limited to 2 choices only for Key Group within Phase 2 (i.e. DH2, DH5).
- Multi-proposal with IKEv2 VPN tunnels is not yet supported.
- Both “IKE SA” and “Child SA” phases (equivalent to Phase 1 and Phase 2) renegotiation fails with IKEv2 VPN tunnels. Work around: set up a long time (e.g. 1 day) for “IKE AUTH” and “Child SA” Lifetime.
- IKEv2 default parameters (IDs and Config Payload) are not properly setup when creating a new configuration. Workaround:
  - 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”
- SHA2 in “Child SA” tab is not available yet with IKEv2 VPN tunnels.
- The type IKEv2_ID_FQDN as remote ID Type is not yet supported.
- The “Initial Contact” mechanism is not yet supported with IKEv2 VPN tunnels.
- The traffic indicator in the **Connection Panel** doesn't work properly with IKEv2 VPN tunnels.
- One Phase 2 only can be created per Phase 1 with IKEv2 VPN tunnels.

4.50 TheGreenBow IPsec VPN Client 6.08 build 003

Features and fixes since release 6.07.001:

4.50.1 Features

- OEM partner new branding.

4.50.2 Fixes

- 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.

4.51 TheGreenBow IPsec VPN Client 6.07 build 001

Fixes since release 6.05.001:

4.51.1 Fixes

- A configuration with X-Auth and Mode Config (Push Mode) doesn't work properly when using Watchguard XTM 33W.
- IKE process (TgbIke) 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.

4.52 TheGreenBow IPsec VPN Client 6.05 build 001

Features and fixes since release 6.04.001:

4.52.1 Features

- Adds support for Windows 8.1 32/64-bit.

4.52.2 Fixes

- 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 > “Phase 2 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.

4.53 TheGreenBow IPsec VPN Client 6.04 build 001

Features and fixes since release 6.02.001:

4.53.1 Features

- Ability to enter a machine name instead of an IP address when adding a Remote Sharing entry (i.e. “Phase 2” > “Remote Sharing”).

4.53.2 Fixes

- One of the log files is not created. This log file is used by our tech support for debug (OEM partners specific).
- Config Mode tunnel fails with some Netgear routers (i.e. FVS318N, UTM25).
- 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 (OEM partners specific).
- License agreement is displayed in Spanish when choosing Italian during setup.

4.54 TheGreenBow IPsec VPN Client 6.02 build 001

Features, improvements, fixes, and known issues since release 5.22.005:

4.54.1 Features

- Adds support for IPv4 and IPv6 protocols.
- Adds support for Diffie-Hellman Group 15 (3072-bit), Group 16 (4096-bit), Group 17 (6144-bit), Group 18 (8192-bit).
- Adds support for 2 new SHA2 algorithm: SHA2-384, SHA2-512. The IPsec VPN Client now supports SHA256-96, SHA256-128, SHA2-384, SHA2-512.
- Adds support for 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.
- Adds support for 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.
- Adds support for 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.

4.54.2 Improvements

- New IPv6 & IPv4 demo configuration file available here: www.thegreenbow.com/doc/tgbvpn_demo_ipv6.tgb.
- 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).
- 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.
- 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).

4.54.3 Fixes

- 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 an 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 Phase 1 with the same remote gateway addresses would not work properly.
- “Invalid Cookie” error message wrongfully displayed when SA expires during Phase 1 renegotiation.

- VPN tunnel may not re-open right after closing when the VPN Gateway is originating the closing (originator of the last DELETE payload).
- Display of “X-Auth warning” error message instead of “Virtual Interface problem” when virtual interface issues detected.
- 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, etc.).
- 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.
- Old value for SHA2 header size for compatibility with some gateways.
- Alternate DNS/WINS server addresses received via Mode Config are not immediately applied when opening tunnel in some circumstances.
- The PKI Options parameter called KeyUsage is not taken into account by the Setup option.
- Upgrade using silent install and setup installation options while the software is running might not complete properly.
- Tunnel closes unexpectedly after wakeup from Windows sleep.
- VPN tunnel does not open when Certificate received from the VPN Gateway contains a multi-valued subjectAltName field.
- Selecting “Any” interface (**Configuration Panel** > “Phase 1” > “Interface”) doesn't choose the correct network interface in some Windows configuration with other applications using network interfaces.
- No VPN traffic when two Phase 2 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.
- No VPN traffic when opening a VPN tunnel on a network interface with multiple IP addresses.
- 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.
- VPN tunnel is not closing automatically when a Gemalto Dual .NET Token configured in the VPN Configuration is unplugged.
- Crash when trying to import a localization file (i.e. strings in your language) if the file name is too long.
- Unable to open tunnel when configuring 8 VPN tunnels with virtual IP address all set to 0.0.0.0.

4.54.4 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.

4.55 TheGreenBow IPsec VPN Client 5.22 build 527 (VPN Certified)

Internal versioning: 5.27 build 001

Improvements since release5.26.001:

4.55.1 Improvements

- Create a specific route to the gateway for all traffic in tunnel configuration.
- Ability to disable default route on physical interface for all in tunnel configuration.
- Increase timeout for getting CRL in CryptRetrieveObjectByUrl.
- Ability to let local traffic outside the tunnel.
- Certificate selection based on Key usage.
- Reset tunneling timeout to 30 sec on receipt of “SEND phase 1”

4.56 TheGreenBow IPsec VPN Client 5.22 build 526 (VPN Certified)

Internal versioning: 5.26 build 001

Improvements and fixes since release 5.25.001:

4.56.1 Improvements

- CPU usage (6% to 20%) during idle mode fixed.

4.56.2 Fixes

- TgbIke crashed after submitting the PIN code when the token is inserted after the client starts.

4.57 TheGreenBow IPsec VPN Client 5.22 build 525 (VPN Certified)

Internal versioning: 5.25 build 001

Features and fixes since release 5.24.001:

4.57.1 Features

- Configurable timeout on pincode popup which automatically close the popup window if no activity.
- Ability to select a certificate based on a pattern to be retrieved in the certificate subject.
- Implementation of the DNS suffix retrieval from the Cisco Mode Config extension
- Ability to manage 2 DNS servers with Config Mode.

4.57.2 Fixes

- Tunnel didn't close on ActivIdentity token removal
- Tunnel didn't open when the VPN Client starts if a token is inserted.
- The PIN code is correctly re-asked when the previous VPN Connection was closed by the Gateway

4.58 TheGreenBow IPsec VPN Client 5.22 build 524 (VPN Certified)

Internal versioning: 5.24 build 001

Improvements and fixes since release 5.23.003:

4.58.1 Improvements

- “Cisco Mode Config” feature implemented for interoperation with ASA Cisco gateway.
- Full compatibility with Windows 8 and Windows 10.

4.58.2 Fixes

- The expiration of the subscription doesn't lead to a software lock.
- The GINA module correctly takes into account the software activation.
- USB mode didn't exit if the PIN code is cancelled, and the token is extracted.
- Tunnel doesn't close on Neowave Token extraction without USB Mode

4.59 TheGreenBow IPsec VPN Client 5.22 build 523 (VPN Certified)

Internal versioning: 5.23 build 003

Features and fixes since release 5.22.005:

4.59.1 Features

- Adds support for the XIRING pinpad (alias Pinpad Leo Ingenico)
- Adds a way to specify the MTU of the virtual interface

4.59.2 Fixes

- Problem of unknown OID in the certificate
- [DualToken] When the token is removed on second drive, tunnel and conf doesn't reset.
- Tunnel remains on Token-Extraction for Neowave Dual-Token.
- USB Configuration move cause a signature issue.
- English strings remaining in French version

Protect your connections
in any situation

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com