Windows Enterprise VPN Client 7.7

Release Notes

Latest update: 26 March 2026
Document reference number: 20260326_RN_VPE_7.7_EN_1.0

www.thegreenbow.com

Table of contents

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2026-03-26	All	Initial release	FBO, YLO, BBR

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 Client VPN Windows Enterprise 7.7 build 007

Features, improvements, fixes, and known issues since release 7.6.008:

3.1 Features

- This release introduces a new certificate selection method. It restricts selection to certificates issued by a known Certificate Authority (CA) and adds support for regular expression (regex) matching on certificate subject substrings.
- Adds the dynamic parameter `crl_download_timeout` to define the maximum wait time before retrying the download of a certificate revocation list (CRL).
- Adds the dynamic parameter `pincode_lifetime` to define the duration, in seconds, that a token or smart card PIN code remains in memory. This option allows the VPN Client to reconnect without requiring users to re-enter the PIN code after a Wi-Fi interruption.
- Adds the dynamic parameters `crl_cache_check_period` and `crl_cache_lifetime` to define how often the cached certificate revocation list (CRL) is checked and how long it remains valid. This option allows the VPN Client to reconnect without requiring users to reopen the tunnel after a Wi-Fi interruption.
- Adds the dynamic parameter `crl_download_retry` to define the maximum number of times the VPN Client attempts to download a certificate revocation list (CRL). This retry mechanism allows the VPN Client to reconnect without requiring users to reopen the tunnel after a Wi-Fi interruption.
- Adds the dynamic parameter `push_request_timer` to define the timeout for receiving a push reply from an external authentication method for an SSL/OpenVPN tunnel.

3.2 Improvements

- The VPN Client now correctly restores the original mode of the IKEEXT service on exit.
- OpenSSL has been updated to version 3.5.5.
- The messages associated with error 105 have been updated.
- Adds support for the Thales MultiApp 5.2 Premium PQC and SafeNet IDPrime 3930 FIDO smart card ATR.
- Improves handling of NDIS allocation and memory release in the driver.
- Updates the bundled LZ4 library to version 1.9.4.

3.3 Fixes

- Fixes an issue that caused the **TrustedConnect Panel** to enter an infinite loop of login attempts.
- Fixes a compatibility issue between sending an ECDSA certificate and receiving an RSA certificate in response.
- Fixes an issue where the VPN Client unexpectedly shut down when a specific captive portal was used.
- Fixes an issue where the Thales eToken Fusion security key could not be used unless it was configured in the `vpnconf.ici` file.
- Fixes an issue where closing the VPN Client set the IKEEXT service to Automatic, regardless of its previous configuration.
- Fixes socket binding errors that occurred when the IKEEXT service was activated.
- Fixes an issue that caused the **TrustedConnect Panel** to enter an endless loop when attempting to establish the tunnel.
- Fixes an issue where unexpected TND-related information was written to the logs.
- Fixes an issue where the CRL creation date was displayed incorrectly in the logs.
- Fixes log entry alignment issues caused by unnecessary leading whitespace.
- Fixes the **Child SA** and **TLS** context menus in the French version of the software, where the command **Ouvre Tunnel** was replaced with **Ouvrir le tunnel**.
- Fixes an issue where Trusted Network Detection (TND) incorrectly required administrators to configure a DNS suffix in AD, LDAP, or LDAPS mode.
- Fixes an issue where the **Connection Panel** opened instead of the **TrustedConnect Panel** when TrustedConnect was configured in GINA mode.
- Fixes an issue where authentication method 214 did not use the correct hash algorithm.
- [Customized version] Fixes an issue that caused the EAP dialog box to appear twice for tunnels configured with EAP authentication.

3.4 Known issues

- An activation error (54 or 31) occurs when the workstation clock is not synchronized with the activation server clock.
- An activation error (50, 54 or 70) occurs during an upgrade of the VPN Client from version 6.x to 7.x.
- An incorrect duration is recorded in the audit logs when tunnel opening fails.
- The **Block Split Tunelling** and **All traffic through the tunnel** options are not compatible with OpenVPN tunnels transported over TCP.
- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

- The **Redundant Gateway** function should not be configured together with the **Fallback Tunnel** function. You should choose one or the other, failing which the VPN Client could have an undefined behavior.
- When migrating from an earlier version to a newer version, we recommend that you perform the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is particularly intended to avoid any issues with configuration format changes related to the automatic selection of certificates on smart cards and in the Windows store.

4 Previous versions

4.1 Client VPN Windows Enterprise 7.6 build 008

Fixes and known issues since release 7.6.007:

4.1.1 Features

- Fixes an issue that caused the wrong binary to start (TgbLogonUI.exe instead of VpnDialer.exe) in TrustedConnect mode when GINA mode was configured.
- Fixes an issue where authentication method 214 incorrectly used the SHA-2 512-bit hash algorithm instead of the 256-bit version. This prevented tunnels from being established with gateways configured in IPsec DR mode.

4.1.2 Known issues

- An incorrect duration is recorded in the audit logs when tunnel opening fails.
- The **Block Split Tunelling** and **All traffic through the tunnel** options are not compatible with OpenVPN tunnels transported over TCP.
- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.
- The **Redundant Gateway** function should not be configured together with the **Fallback Tunnel** function. You should choose one or the other, failing which the VPN Client could have an undefined behavior.
- When migrating from an earlier version to a newer version, we recommend that you perform the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is particularly intended to avoid any issues with configuration format changes related to the automatic selection of certificates on smart cards and in the Windows store.

4.2 Client VPN Windows Enterprise 7.6 build 007

Features, improvements, fixes, and known issues since release 7.5.109:

4.2.1 Features

- System, syslog, and audit logs now comply with RFC 5424 and include structured data.
- TrustedConnect now generates audit logs.

- New ATRs added to simplify VPN configuration.
- ANSSI's Key Usage and Extended Key Usage requirements are now applied by default during automatic certificate selection.
- Adds a dynamic parameter, `redundant_retry`, which can be used to prevent switching from the main gateway to the redundant gateway after a defined number of retries.
- The list of traffic selectors used for rekeying is now compatible with certain gateways operating in IPsec DR mode.

4.2.2 Improvements

- The TrustedConnect icon turns yellow when a remediation tunnel is used.
- Introduces a retry mechanism to resolve TPM access issues encountered on some machines.
- The End User License Agreement (EULA) has been updated.
- OpenSSL has been updated to version 3.0.16.
- The status of the IKE service is now displayed in the TrustedConnect console when it is reset.
- The CRL download timeout has been extended to 60 seconds.
- For configurations using the "All through the tunnel" mode, the virtual interface metric is now set to 1 by default.
- Improved handling of network interface up events that should be ignored.
- Suppresses incorrect messages generated when the client certificate CA is stored on a token, smart card, or in the Windows certificate store.

4.2.3 Fixes

- Fixes an issue where the confirmation dialog box did not appear when selecting the **Reset** menu item.
- Fixes an issue that prevented the tunnel from initializing correctly when using a certificate stored in the certificate store in Remote Desktop (RDP) mode.
- Fixes a condition that prevented a tunnel from opening with a local token in Remote Desktop (RDP) mode.
- Corrects behavior where the tunnel was not closed when the workstation entered sleep mode and could no longer be opened after resuming.
- Fixes an issue where Trusted Network Detection (TND) was restarted and the tunnel was closed when the system redetected the primary network adapter after waking from sleep.
- Corrects behavior where TrustedConnect opened a tunnel without displaying an error when the driver was missing.

- Fixes an issue where the MSI installer displayed unresolved variables in a warning dialog box.
- Fixes an issue that prevented failover to the redundant gateway when Filtering Mode was enabled.
- Fixes an issue where IKE was reset after entering an incorrect PIN code in TrustedConnect mode with TND and CPD enabled.
- Corrects behavior where the visual cue for a direct connection to the trusted network was not shown when detection was performed via Active Directory (AD).
- Fixes an issue where the certificate request payload (CERTREQ) omitted hashe for all known CAs in the tunnel configuration.
- Fixes an issue where `IKE_AUTH` renegotiation could trigger error code 13 in combination with TrustedConnect.
- Fixes a defect in handling error codes generated during ECDSA signature verification.
- Fixes an issue prevented the tunnel from opening in TrustedConnect mode when used in combination with GINA mode, Filtering Mode, and the MSI property `IKESTART`.
- Corrects behavior where CHILD_SA phase renegotiation would fail when initiated by the gateway.
- [Custom version] Fixes an issue that prevented Filtering Mode from enabling at startup when both `IKESTART` and `NETPARAMS` MSI properties were enabled.

4.2.4 Known issues

- An incorrect duration is recorded in the audit logs when tunnel opening fails.
- The **Block Split Tunelling** and **All traffic through the tunnel** options are not compatible with OpenVPN tunnels transported over TCP.
- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.
- The **Redundant Gateway** function should not be configured together with the **Fallback Tunnel** function. You should choose one or the other, failing which the VPN Client could have an undefined behavior.
- When migrating from an earlier version to a newer version, we recommend that you perform the deployment with a configuration created using the version to be deployed rather than letting the VPN Client use the earlier configuration. This is particularly intended to avoid any issues with configuration format changes related to the automatic selection of certificates on smart cards and in the Windows store.

4.3 Windows Enterprise VPN Client 7.5 build 109

Features, improvements, fixes, and known issues since release 7.5.007:

4.3.1 Features

- [Custom Version] Reintroduces support for cases where a DH group is absent from the IKE proposal.

4.3.2 Improvements

- The error code logged when there are activation issues now provides more detailed information to help identify the root cause.
- The CRL download timeout has been increased from 30 seconds to 60 seconds to provide more time for mobile connections.
- [Custom Version] Access credentials can now be entered in the EAP popup window using Chinese characters.
- [Custom Version] The **Remeditation** checkbox has been removed, as it should not be included with this version.

4.3.3 Fixes

- Addresses an issue where error codes from ECDSA signature verification were not handled properly or logged with sufficient detail.
- Resolves an issue that prevented a tunnel from opening when TrustedConnect mode was used in combination with GINA mode, Filtering mode and the MSI property `IKESTART`.
- Fixes an issue where `IKE_AUTH` rekeying could result in error code 13 with TrustedConnect.
- Fixes an issue where `CHILD_SA` rekeying would fail if initiated by the gateway.

4.3.4 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.
- The SSL tunnel creation wizard 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

4.4 Windows Enterprise VPN Client 7.5 build 007

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

4.4.1 Features

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

4.4.2 Improvements

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

4.4.3 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.

4.4.4 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.
- The SSL tunnel creation wizard 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

4.5 Windows Enterprise VPN Client 7.5 build 006

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

4.5.1 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

4.5.2 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

4.5.3 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

4.5.4 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.
- The SSL tunnel creation wizard 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

4.6 Windows Enterprise VPN Client 7.4 build 018

Fixes, limitations, and known issues since release 7.4.016:

4.6.1 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

4.6.2 Limitations

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

4.6.3 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.7 Windows Enterprise VPN Client 7.4 build 016

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

4.7.1 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

4.7.2 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

4.7.3 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

4.7.4 Limitations

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

4.7.5 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.8 Windows Enterprise VPN Client 7.3 build 007

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

4.8.1 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

4.8.2 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

4.8.3 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

4.8.4 Limitations

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

4.8.5 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.9 Windows Enterprise VPN Client 7.2 build 008

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

4.9.1 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

4.9.2 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

4.9.3 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

4.9.4 Limitations

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

4.9.5 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.10 Windows Enterprise VPN Client 6.87 build 109

Fixes and known issues since release 6.87.108:

4.10.1 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

4.10.2 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.11 Windows Enterprise VPN Client 6.87 build 108

Improvements, fixes, and known issues since release 6.87.001:

4.11.1 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

4.11.2 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

4.11.3 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.12 Windows Enterprise VPN Client 6.87 build 001

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

4.12.1 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**

4.12.2 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)

4.12.3 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

4.12.4 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.13 Windows Enterprise VPN Client 6.86 build 015

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

4.13.1 Features

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

4.13.2 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

4.13.3 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

4.13.4 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.14 Windows Enterprise VPN Client 6.85 build 007

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

4.14.1 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

4.14.2 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

4.14.3 Fixes

- Tunnel now closes when smart card reader is pulled out

4.14.4 Known issues

- The SSL tunnel creation wizard defaults to IKEv2 tunnel creation.

4.15 TheGreenBow VPN Client 6.64 build 003

Fixes since release 6.64.002:

4.15.1 Fixes

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

4.16 TheGreenBow VPN Client 6.64 build 002

Fixes since release 6.64.001:

4.16.1 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.

4.17 TheGreenBow VPN Client 6.64 build 001

Features, improvements, and fixes since release 6.63.005:

4.17.1 Features

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

4.17.2 Improvements

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

4.17.3 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)

Secure your connections
in all circumstances

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com