macOS VPN Client 2.5

Release Notes

Latest update: 25 September 2024
Document reference number: 20240925_RN_VPM_2.5_EN_1.0

www.thegreenbow.com

1 Preamble

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

2 TheGreenBow macOS VPN Client 2.5.003

Major changes, features, improvements, fixes, and limitations since release 2.4.010:

2.1 Major changes

- Provides full support for gateways configured in IPsec DR (Restricted) mode
- Support for RFC 4304 Extended Sequence Number (ESN) and RFC 6023 (Childless IKE Initiation) for enhanced security
- Support for Digital Signature Authentication RFC 4754 “ECDSA with SHA-2” (Method 9) and RFC 7427 “ECDSA with RSA” (Method 14) for strong authentication of certificates using elliptic curves
- Weaker algorithms (DES, 3DES, SHA, MD5, DH 1-2, DH 5) have been removed from the software for enhanced security
- The gateway certificate will be checked by default each time a tunnel is opened
- Adds automation features in a new **Automation** tab enabling script execution before tunnel opens and when tunnel is opened

2.2 Features

- Introduces new algorithm: Diffie-Hellman 28 (BrainpoolP256r1)
- Introduces certificate authentication method ECDSA BrainpoolP256r1 with SHA256
- Uses certificate authentication method 14 RSASSA-PSS by default with all RSA certificates
- Forces UDP encapsulation mode for IKEv2
- [Custom Version] Reintroduces support for cases where a DH group is absent from the IKE proposal

2.3 Improvements

- Configurations that contain CAs but do not include any user certificates are now accepted
- Code for customized versions is now properly set
- Packets sent from IPsec are now sent directly
- **More parameters** tab has been localized
- **IPv6** checkbox has been removed
- Legacy linker is now used following XCode update
- OpenSSL has been updated to version 3
- Apple API is now used instead of sockets
- Activation logging information has been enhanced

- Tunnel now remains connected if connection is dropped
- [Custom Version] External process is no longer called to get macOS version
- [Custom Version] Certificate is now accepted when key usage is not critical
- [Custom Version] Self-signed certificates are now accepted when configuration is retrieved from server
- [Custom Version] Provisions port for custom IPsec VPN Client
- [Custom Version] User agent for VPN configuration is now set to a custom value

2.4 Fixes

- Addresses minor spelling issues in **Compression** drop-down list
- Fixes an issue where a tunnel configuration would not open following VPN Client activation after fresh install
- SSL tunnel now closes when connection is dropped
- Fixes an issue where routes were not properly installed
- Fixes an issue where packets were not correctly reassembled for SSL tunnels over TCP
- Fixes a bandwidth limitation issue
- Addresses an issue where error codes from ECDSA signature verification were not handled properly or logged with sufficient detail
- [Custom Version] **More parameters** tab is now hidden
- [Custom Version] Debugging information has been removed from custom release profile

2.5 Limitations

- IPv6 is not supported
- Activation window is only displayed on initial startup
- Smart cards and tokens are not supported

3 Previous versions

3.1 TheGreenBow macOS VPN Client 2.4.010

Major changes, features, improvements, fixes, and limitations since release 2.0.019:

3.1.1 Major changes

- Support for RFC 4304 Extended Sequence Number (ESN) and RFC 6023 (Childless IKE Initiation) for enhanced security
- Support for Digital Signature Authentication RFC 4754 “ECDSA with SHA-2” (Method 9) and RFC 7427 “ECDSA with RSA” (Method 14) for strong authentication of certificates using elliptic curves
- Weaker algorithms (DES, 3DES, SHA, MD5, DH 1-2, DH 5) have been removed from the software for enhanced security
- The gateway certificate will be checked by default each time a tunnel is opened
- Activation and configuration files are stored in a different folder

3.1.2 Features

- Introduces new algorithm: Diffie-Hellman 28 (BrainpoolP256r1)
- Introduces certificate authentication method ECDSA BrainpoolP256r1 with SHA256
- Uses certificate authentication method 14 RSASSA-PSS by default with all RSA certificates
- Forces UDP encapsulation mode for IKEv2
- Adds the **Childless** checkbox on **IKE Auth** > **Protocol** tab
- Adds the **Extended Sequence Number** drop-down list on the **Child SA** > **Child SA** tab
- Adds the **Popup when tunnel opens** checkbox for SSL tunnels

3.1.3 Improvements

- OpenSSL has been updated to version 1.1.1s
- The “No Diffie-Hellman” option has been removed for Child SAs
- Greater stability of the IKE module
- Better performance of AES-GCM encryption
- Weak algorithms have been removed for SSL/OpenVPN: MD5, SHA1, TLS low security suite, BF-CBC
- 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

- KeyUsage extensions of user and gateway certificates are now checked in line with ANSSI rules

3.1.4 Fixes

- Activation and configuration data is no longer removed when the OS runs out of disk space
- Fixes an issue where the menu went missing near the end of the activation period
- Fixes a DPD issue after a retransmission
- Fixes an issue with IKEv2 fragmentation when using AES-GCM

3.1.5 Limitations

- IPv6 is not supported
- Activation window is only displayed on initial startup

3.2 TheGreenBow macOS VPN Client 2.0.019

Features, improvements, fixes, and limitations since release 2.0.004:

3.2.1 Features

- CA management is now included in the UI
- Now supports configuration files from the Windows VPN Client that include PKI checks
- **More Parameters** tab is now included in the UI

3.2.2 Improvements

- Improved logging and exception handling on startup
- OpenSSL library has been updated to version 1.1.1n

3.2.3 Fixes

- Virtual IP address is now correctly updated in CP mode (get configuration from gateway)
- English is now used as the default language
- Local ID is no longer lost when loading configuration file
- Fixes Child SA rekeying when DH mode is set to **Auto**
- DPD messages with old SPIs are now ignored
- Fixes issues with some certificates that use SHA-512

3.2.4 Limitations

- IPv6 is not supported
- Activation window is only displayed on initial startup

3.3 TheGreenBow macOS VPN Client 2.0.004

Features, improvements, and fixes since release 2.0.003:

3.3.1 Features

- The following languages have been added to the UI: Arabic, Czech, Danish, German, Greek, Spanish, Finnish, Hungarian, Hindi, Italian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Romanian, Slovenian, Bosnian, Thai, Turkish, Chinese, Farsi
- Configuration file is now encrypted; old configuration file will be encrypted when re-saved
- Accepts encrypted configuration files from TheGreenBow Windows Enterprise VPN Client 6.85
- VPN client now sets a default route for full tunnels (all traffic within tunnel)

3.3.2 Improvements

- OpenSSL library has been updated to version 1.1.1k
- UDP encapsulation is now enforced
- Traffic to remote network now allowed even if local and remote network are in same IP range
- All logs are now saved into files (simplifies sending logs to TheGreenBow's support team)
- **DNS servers** field in user interface is now disabled when **CP mode** is selected
- Deprecated algorithms (DES, 3DES, MD5, SHA1, DH1, DH2, DH5) have been removed
- Menus and menu items have been rearranged in the UI for better clarity
- EULA is now available in both French and English

3.3.3 Fixes

- DNS suffix is now correctly used when configured
- The keyboard shortcut for saving is now working again
- Fixes issue with Console not showing sometimes

3.4 TheGreenBow macOS VPN Client 2.0.003

Features, improvements, and fixes since release 2.0.000:

3.4.1 Features

- Gateway Certificate Authorities (CA) can now be imported into the VPN Client
- Ability to force the VPN Client to only open a tunnel when the gateway's CAs are valid
- Added "More Parameters" menu item, used to set bandwidth limitation

3.4.2 Improvements

- License activation can now be reset
- OpenSSL library has been updated to version 1.1.1j

3.4.3 Fixes

- "About..." window is now correctly displayed

3.5 TheGreenBow macOS VPN Client 2.0.000

Features, improvements, and fixes since release 1.2.007:

3.5.1 Features

- Adds ability to retrieve VPN configuration from gateway
- Adds 15-day grace period at end of subscription
- Bandwidth management
- EAP pop up for authentication

3.5.2 Improvements

- OpenSSL library has been updated to version 1.1.1.i
- Supports request for "mode-cfg type 3" to receive DNS from gateway
- General stability fixes

3.5.3 Fixes

- Corrects issues related to language translation

3.6 TheGreenBow macOS VPN Client 1.2.007

Features, improvements, and fixes since initial release:

3.6.1 Features

- App can now be downloaded directly from TheGreenBow web site
- App must now be activated with a license key from TheGreenBow
- App is now distributed as a DMG installer
- Support for OpenVPN (SSL tunnels)
- Adds AES-CTR and AES-GCM encryption methods
- Adds DH Groups 19-21 (Elliptic Curves)
- Adds Trace Mode
- Adds Dark Mode support
- French language is now supported

3.6.2 Fixes

- Fixes editing issue when clicking on the tunnel name
- Fixes crash when trying to open an empty IKEv2 tunnel
- Dead Peer Detection now correctly used to close tunnel when no traffic is detected
- All IKEv2 identity types are now correctly saved in configuration file

Protect your connections
in any situation

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com