

# Linux VPN Client 3.4

## Release Notes

---

# 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 Linux VPN Client.



## 2 TheGreenBow Linux VPN Client 3.4.3 build 001

Features, improvements, and fixes since release 3.4.2 build 002:

### 2.1 Features

- This version is compatible with RedHat 9.4 and Ubuntu 22.04 (kernel 5.15).

### 2.2 Improvements

- TheGreenBow driver's compatibility with the kernel is now verified at startup before the `tgbliked` service starts. The supported kernel can be configured.
- TheGreenBow driver is no longer stored in `initramfs`, ensuring it does not start after the VPN Client has been uninstalled.

### 2.3 Fixes

- Addresses an issue where error codes from ECDSA signature verification were not handled properly or logged with sufficient detail.

## 3 Previous versions

### 3.1 TheGreenBow Linux VPN Client 3.4.2 build 002

Major changes, features, improvements, and fixes since release 2.1.2 build 003:

#### 3.1.1 Major changes

- Provides full support for gateways configured in IPsec DR (Restricted) mode
- This version is compatible with RedHat 9.3 and Ubuntu 22.04 (kernel 5.15)
- 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

#### 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
- Support for Yubikey tokens
- A PIN code option has been added to the command line interface to set smart card PIN code
- A reset option has been added to the command line interface to allow users to reload a tunnel without needing administrator rights, except in the event of a configuration change

#### 3.1.3 Improvements

- Installation of EPEL package has been made optional
- The **Disconnect all** menu item has been removed from the system menu icon’s contextual menu, since there can only be one connection at a time

- The installed configuration is now properly backed up when upgrading the VPN Client
- The system menu icon now displays spinning arrows when the VPN Client is opening a tunnel and turns orange when there is an error
- Several error messages have been added to give clear indications regarding any issues when opening a tunnel
- A message now clearly indicates failure to connect to the activation server or failure to activate
- The system menu icon can now be restarted even if the VPN Client daemon is not running or if the system menu icon has crashed

### 3.1.4 Fixes

- Fixes an issue where the VPN Client's version number was not displayed correctly in the system menu icon's contextual menu
- Fixes an issue where the PIN code entry pop-up window would open in the background
- Fixes an issue where the system menu icon would remain green when a tunnel is disconnected
- Fixes an issue where the time in logs was based on GMT rather than the workstation's local time

## 3.2 TheGreenBow Linux VPN Client 2.1.2 build 003

Features, improvements, and fixes since release 2.0.1 build 007:

### 3.2.1 Features

- Systray icon now works on CentOS and Red Hat 8 when installed with XFCE or KDE (but not GNOME). See <https://www.linuxtricks.fr/wiki/centos-installer-centos-8-avec-xfce> for instructions on how to install CentOS 8 with XFCE.
- The validity of the firewall's certificates is checked before opening a tunnel
- Support for PKCS#11 smart cards and tokens
- Support for Diffie-Hellman Groups 21 and 28 (elliptic curves)
- The Linux VPN Client is now compatible with TheGreenBow Activation Server (TAS)

### 3.2.2 Improvements

- Bandwidth performance improvement
- New JSON license format
- Support for multiple DNS servers

- User is now informed of license expiry date
- A generic package for Ubuntu now works for both 20.04 and 18.04 versions
- Upgrade to OpenSSL 1.1.1.k
- The Linux VPN Client now offers a 30-day free trial period after installation
- Network interface state changes are detected and correctly managed
- Manual activation is now supported

### 3.2.3 Fixes

- ESN mode now works correctly
- Fixed various freezes
- Fixed activation issue when adding a new license after old one expired
- Supports certificates with elliptic curves in Android certificate store
- SHA-1 has algorithm has been removed entirely from the software

## 3.3 TheGreenBow Linux VPN Client 2.0.1 build 007

Features and fixes since release 2.0.1 build 006:

### 3.3.1 Features

- Now also available for Ubuntu 18.04 64-bit with GCC version 9

### 3.3.2 Fixes

- server DNS and DNS suffix parameters returned by the gateway (in Configuration Payload mode) are now taken into account

## 3.4 TheGreenBow Linux VPN Client 2.0.1 build 006

Features and fixes since release 2.0.1 build 005:

### 3.4.1 Features

- Now also available for CentOS/Red Hat 8 64-bit

### 3.4.2 Fixes

- All Windows, Mac, and Linux style new line characters (CR/LF) are now supported in vpnsetup.ini for license activation

## 3.5 TheGreenBow Linux VPN Client 2.0.1 build 005

Features of the first Linux 2.0 release:

### 3.5.1 Features

- IPsec network driver and IKE module developed by TheGreenBow
- IPsec driver integrated in kernel mode
- Support for the IKEv2 protocol
- Full implementation of the IPsec IKE v2 protocol
- Encryption: AES CBC, AES CTR, AES GCM 128/192/256
- Hash: SHA2 256/384/512
- Diffie-Hellman Group : 14-20
- Support for X.509 certificates: PEM, PFX, PKCS #12
- Authentication : pre-shares key, certificates, EAP, double authentication (certificate + EAP)
- Certificate authentication:
  - Method 1: RSA Digital Signature [RFC7296]
  - Method 9: ECDSA with SHA-256 [RFC4754]
  - Method 14: Digital Signature Authentication RSA [RFC74]
- IP Fragmentation
- All traffic within the tunnel
- Dead Peer Detection (DPD)
- Redundant gateway
- Mode CP
- Automatic negotiation of algorithms with the gateway
- IKE Fragmentation
- Automatic NAT-Traversal
- Remote ID, Local ID
- Import of VPN security policies from the Windows and macOS TheGreenBow VPN Clients
- Silent install
- Command-line and user interface (systray)
- License activation
- Support of syslog protocol and format
- Available for Ubuntu 20.04 64 bits
- Ubuntu only: Integration in the Ubuntu system menu (systray)

**Protect your connections**  
in any situation

28, rue Caumartin  
75009 Paris - France  
[sales@thegreenbow.com](mailto:sales@thegreenbow.com)

[www.thegreenbow.com](http://www.thegreenbow.com)