

Linux
VPN Client 2.0
CentOS/RedHat

User Guide

Latest update: 28 April 2021

Table of Contents

1	Overview	3
1.1	Introduction	3
1.2	Secure	3
1.3	Ergonomic	3
1.4	Simple	3
1.5	Universal	3
1.6	Features	4
2	Downloading and verifying the software	5
2.1	Introduction	5
2.2	Verification procedure	5
2.3	Technical information	6
3	Installing the software	7
3.1	Introduction	7
3.2	Installation conditions	7
3.3	Dependencies	7
3.4	Package contents	7
3.5	Interactive installation	7
3.6	Installing from the command line	11
4	Activating the software	13
4.1	Introduction	13
4.2	Format and content of the vpnsetup.ini file	13
4.3	Activation procedure	13
4.4	Trial period	14
5	Uninstalling the software	15
6	Using the test tunnel	16
7	Command line	17
7.1	Introduction	17
7.2	Displaying help	17
7.3	Listing configured tunnels	17
7.4	Opening a tunnel	18
7.5	Closing a tunnel	18
7.6	Displaying the tunnel status	18
8	Configuring VPN tunnels	19
8.1	Introduction	19
8.2	Protecting the VPN security policy	19
8.3	Updating the VPN security policy	19
9	Logs	20
9.1	Introduction	20
9.2	Exporting in text format	20
10	Current limitations	21
11	Managing errors	22
11.1	User must belong to "tgb" group	22
11.2	Cannot get tunnel list	22
11.3	Tunnel opening failed	22
11.4	Non-root users must not be able to access the configuration file	23
11.5	Checking drivers	23
11.6	IKE daemon is unresponsive	23
12	Related reference documents	24

1 Overview

1.1 Introduction

Thank you for downloading our Linux VPN Client 2.0 software for CentOS and RedHat.

The Linux VPN Client has been thoughtfully designed to address the needs of major corporations, critical market operators, as well as civil and government bodies. It provides a high level of communication security and is also easy to deploy, integrate, and use.

Users of the Linux VPN Client also benefit from highly personal support that goes from customer-specific follow-up to the integration of customized developments.

It does not require the existing key management infrastructure (KMI) to be reconsidered and it is designed to be transparently integrated into the IKEv2 gateways that have been set up.

The Linux VPN Client is marketed on the basis of an annual subscription. The subscription includes customer-specific support and software maintenance.

1.2 Secure

Specifically designed for nomadic work practices, the Linux VPN Client is an IKEv2 IPsec VPN client software for Linux workstations that enables users to establish perfectly secure connections to the company's information system over the internet. It implements a broad range of encryption and hashing algorithms, as well as various strong authentication methods.

1.3 Ergonomic

Easy to install, easy to configure and deploy, perfectly transparent to the user, the Linux VPN Client is widely recognized today for its unparalleled ergonomics.

1.4 Simple

Our configuration guides make integration and deployment tasks painless by speeding up the implementation of an end-to-end VPN solution.

1.5 Universal

The Linux VPN Client runs on CentOS 8 and RedHat 8. The software is compatible with a great number of IPsec gateways available on the market. The constantly growing list of gateways that have been tested in our laboratory is available on our website.

1.6 Features

- IPsec network driver and IKE module developed by TheGreenBow
- IPsec module integrated in kernel mode
- Support for the IKEv2 protocol
- Interoperable with all IKEv2 compatible VPN routers
- Cryptography: AES CBC, AES CTR, AES GCM 128/192/256
- Hashing: SHA2 256/384/512
- DH groups: 14-21
- X.509 certificate management: PEM, PFX, PKCS #12
- Authentication: preshared key, certificates, EAP, two-factor authentication (certificate + EAP)
- Certificate authentication using:
 - Method 1: RSA Digital Signature [RFC7296]
 - Method 9: ECDSA with SHA-256 [RFC4754]
 - Method 14: Digital Signature Authentication RSA [RFC7427]
- IP fragmentation
- "All traffic through the VPN tunnel" mode
- Dead Peer Detection (DPD)
- Redundant gateway
- CP mode
- Automatic negotiation of algorithms with gateway
- IKE fragmentation
- Automatic NAT-Traversal mode
- Remote ID, Local ID
- Import VPN configurations generated using TheGreenBow Windows and macOS VPN clients
- Control from the command line
- Activation using a license key
- Support for syslog event log format and protocol
- Compiled for CentOS version 8 and RedHat version 8, 64-bit

2 Downloading and verifying the software

2.1 Introduction

The Linux VPN Client is available for download from our website: https://www.thegreenbow.fr/vpn_linux.html. You can download the software package after having filled in the form displayed when you click the **Download** link corresponding to the desired distribution on the **Download** tab.

Prior to installing the Linux VPN Client, it is essential to verify the authenticity of the software package downloaded from our website in order to confirm that it has indeed been signed by TheGreenBow and that it has not been altered in any way.

2.2 Verification procedure

To verify the authenticity of the package, follow the steps below:

1. Open a terminal window.
2. Run the following command to download the public key:

```
sudo gpg --keyserver keys.gnupg.net --recv-keys
EF44CB417249358E2A97894245038D5E2FE199A5
```

```
[tguser-fr@localhost ~]$ sudo gpg --keyserver keys.gnupg.net --recv-keys EF44CB417249358E2A97894245038D5E2FE199A5
[sudo] password for tguser-fr:
gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 45038D5E2FE199A5: public key "TGB Linux product manager <linux@thegreenbow.com>" imported
gpg: Total number processed: 1
gpg:      imported: 1
[tguser-fr@localhost ~]$
```

3. Run the following command to export the key to a temporary file:

```
sudo gpg --export -a
'EF44CB417249358E2A97894245038D5E2FE199A5' > /tmp/GPG-TGB-KEY
```

```
[tguser-fr@localhost ~]$ sudo gpg --export -a 'EF44CB417249358E2A97894245038D5E2FE199A5' > /tmp/GPG-TGB-KEY
[tguser-fr@localhost ~]$ █
```

4. Run the following command to import the key:

```
sudo rpm --import /tmp/GPG-TGB-KEY
```

```
[tguser-fr@localhost ~]$ sudo rpm --import /tmp/GPG-TGB-KEY
[tguser-fr@localhost ~]$
```

5. To check the software package, run the following command in the directory where the package is located (in this case Downloads, where the first x is the build number):

```
sudo rpm -K ~/Downloads/thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm
```

```
[tgbuser-fr@localhost ~]$ sudo rpm -K ~/Downloads/thegreenbow-vpn-client-2.0.1-5.el8.x86_64.rpm  
/home/tgbuser-fr/Downloads/thegreenbow-vpn-client-2.0.1-5.el8.x86_64.rpm: digests signatures OK  
[tgbuser-fr@localhost ~]$
```

6. Make sure the output data matches the following:

```
/home/[user_name]/Downloads/thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm: digests signatures OK
```

If this is not the case, contact customer support: <https://www.thegreenbow.com/form.html?lang=en>.

2.3 Technical information

The CentOS/RedHat package is signed with a 4096-bit RSA key. The corresponding public key is available here: <http://keys.gnupg.net/pks/lookup?op=get&search=0x45038D5E2FE199A5>.

Key ID: EF44 CB41 7249 358E 2A97 8942 4503 8D5E 2FE1 99A5.

Key fingerprint: 2FE199A5.

To delete the public key from the RPM database, follow the steps below:

1. Run the following command to retrieve the key's full identifier:

```
rpm -q gpg-pubkey --qf '%{NAME}-%{VERSION}-%  
%{RELEASE}\t%{SUMMARY}\n'
```

The output data should specify the key name as well as its version and release numbers:

```
gpg-pubkey-2fe199a5-[revision_number] gpg(TGB Linux product  
manager <linux@thegreenbow.com>)
```

2. Run the following command to delete the key, making sure to replace the release number with the number retrieved in the previous step:

```
sudo rpm --erase gpg-pubkey-2fe199a5-[release_number]
```

3 Installing the software

3.1 Introduction

After having downloaded the Linux VPN Client from the TheGreenBow website and having verified its authenticity (see section 2 Downloading and verifying the software), you can install the program by double-clicking its icon and then proceeding with the command line.

You can also install the product using the command line only, which allows you to create scripts to automate the process.

3.2 Installation conditions

To install the Linux VPN Client you must have superuser privileges (or root access) on the machine.

In addition, you will need to create a configuration file for the Linux workstation using the Windows or macOS VPN client.

3.3 Dependencies

When you install the Linux VPN Client, the following dependencies must also be installed:

- epel

3.4 Package contents

When you install the Linux VPN Client, the following directories and files will be added to the workstation:

- `/usr/bin/tgbctl`: command used to control the Linux VPN Client from the command line
- `/usr/sbin/tgbiked`: Linux VPN Client daemon running in the background
- `/lib/systemd/system/tgbiked.service`: daemon configuration file
- `/etc/tgb/conf.tgb`: configuration file for the VPN security policy, including a TheGreenBow test tunnel
- `/usr/share/doc/thegreenbow/CLUF_VPN_TheGreenBow_vFR3.51.pdf`: document containing TheGreenBow's End User License Agreement (currently only available in French)
- `/usr/src/tgbtun-1.0`: folder containing the source files for dynamic kernel module support (DKMS)

3.5 Interactive installation

To install the Linux VPN Client, proceed as follows:

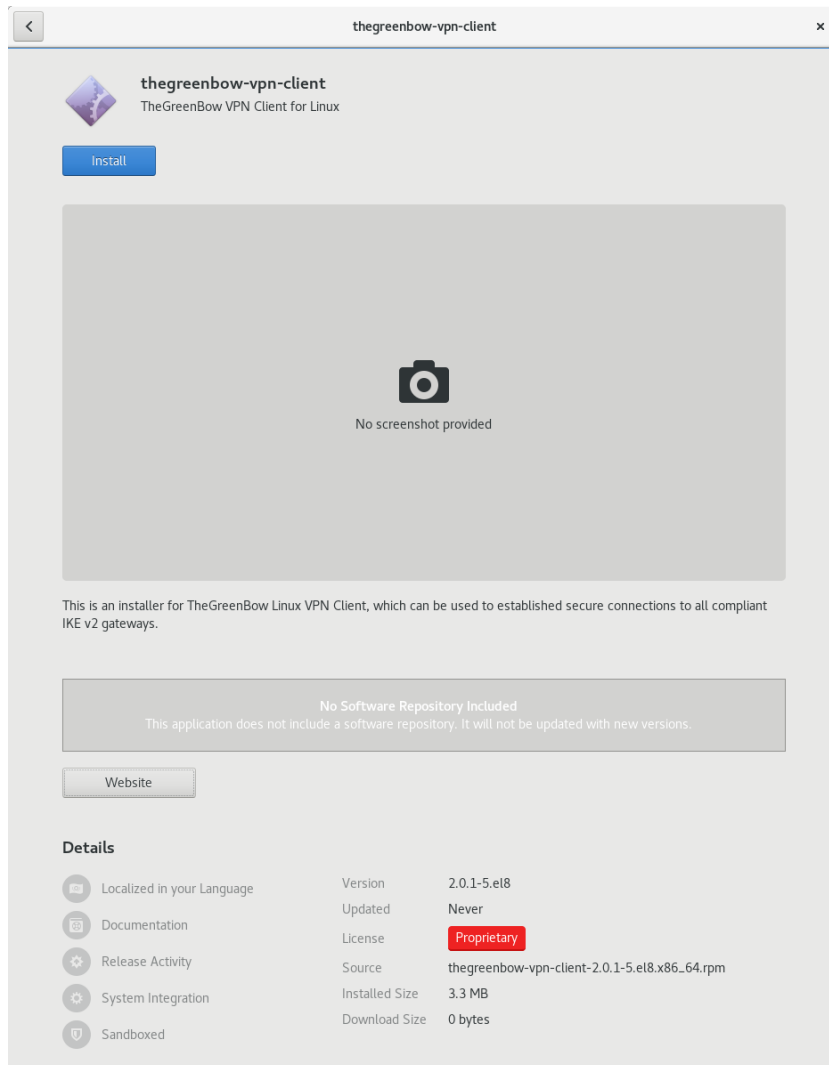
1. If you downloaded the software package on a machine other than the one on which the Linux VPN Client is to be installed, copy it to the destination machine.

2. Double-click the icon of the downloaded software package:

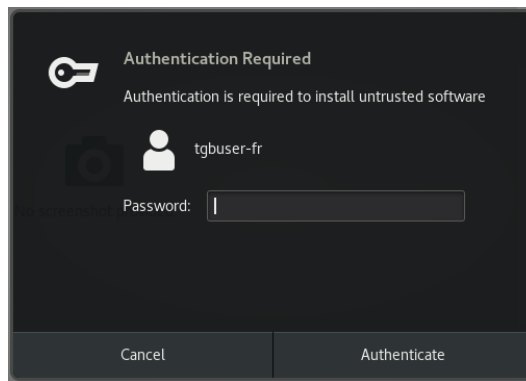


thegreenbow-vpn-client-2.0.1-5.el8.x86_64.rpm

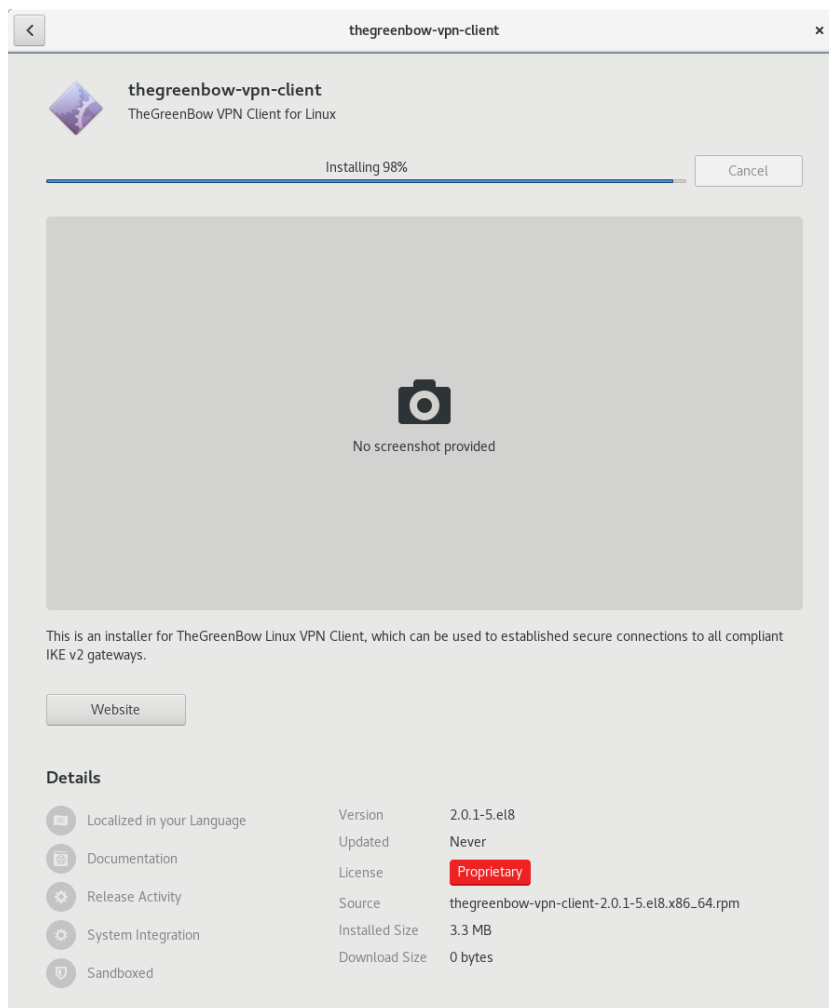
3. The installation of the program starts and the following window is displayed:



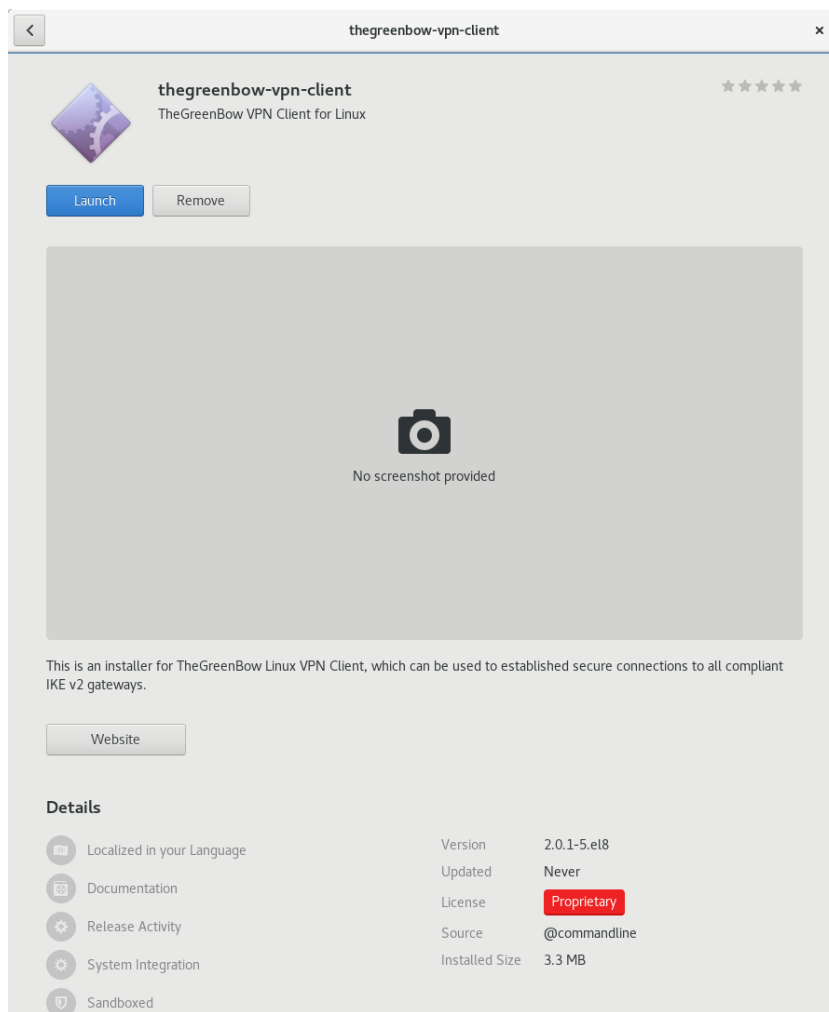
- Click **Install**. The installation program asks you to authenticate:



- Enter the password to authenticate. The actual installation of the software begins:



6. If the installation is successful, the following screen is displayed:



7. Open a terminal window.
8. Add the VPN users to the `tgb` group by running the following command:

```
sudo usermod -aG tgb [user_name]
```

```
[tgbuser-fr@localhost ~]$ sudo usermod -aG tgb tgbuser-fr
```

9. Enter the administrator's password and press Enter.

```
[tgbuser-fr@localhost ~]$ sudo usermod -aG tgb tgbuser-fr  
[sudo] password for tgbuser-fr:  
[tgbuser-fr@localhost ~]$
```

10. Activate the product (see section 4 Activating the software).

3.6 Installing from the command line

The Linux VPN Client can also be installed from the command line. To do this, proceed as follows:

1. If you downloaded the software package on a machine other than the one on which the Linux VPN Client is to be installed, copy it to the destination machine.
2. Open a terminal window.
3. Access the folder containing the `thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm` (where the first `x` is the build number of the software package).
4. Run the following command to update the package repositories:

```
sudo yum makecache
```

```
[tgbuger-fr@localhost ~]$ sudo yum makecache
CentOS Linux 8 - AppStream                289 B/s | 4.3 kB    00:15
CentOS Linux 8 - BaseOS                   374 B/s | 3.9 kB    00:10
CentOS Linux 8 - Extras                   147 B/s | 1.5 kB    00:10
Metadata cache created.
[tgbuger-fr@localhost ~]$ █
```

5. Run the following command to install the extra package for Enterprise Linux:

```
sudo yum install -y
https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
[tgbuger-en@localhost ~]$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
[sudo] password for tgbuger-en:
Last metadata expiration check: 0:18:59 ago on Wed 28 Apr 2021 12:27:15 AM CEST.
epel-release-latest-8.noarch.rpm                1.4 kB/s | 22 kB    00:15
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
  epel-release          noarch            8-10.el8         @commandline     22 k
Transaction Summary
=====
Install 1 Package

Total size: 22 k
Installed size: 32 k
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                :
  Installing                : epel-release-8-10.el8.noarch
  Running scriptlet: epel-release-8-10.el8.noarch
  Verifying                 : epel-release-8-10.el8.noarch
Installed products updated.

Installed:
  epel-release-8-10.el8.noarch

Complete!
```

6. Run the following command to install the Linux VPN Client software:

```
sudo yum install -y ~/Downloads/thegreenbow-vpn-client-2.0.1-x.el8.x86_64.rpm
```

```
[tguser-en@localhost ~]$ sudo yum install -y ~/Downloads/thegreenbow-vpn-client-2.0.1-6.el8.x86_64.rpm
Last metadata expiration check: 0:03:48 ago on Wed 28 Apr 2021 12:53:02 AM CEST.
Dependencies resolved.
=====
Package                                Architecture      Version           Repository        Size
=====
Installing:
thegreenbow-vpn-client                 x86_64           2.0.1-6.el8      @commandline     3.1 M
=====
Transaction Summary
=====
Install 1 Package

Total size: 3.1 M
Installed size: 9.1 M
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Running scriptlet: thegreenbow-vpn-client-2.0.1-6.el8.x86_64 1/1
  Preparing :                                                    1/1
  Running scriptlet: thegreenbow-vpn-client-2.0.1-6.el8.x86_64 1/1
  Installing : thegreenbow-vpn-client-2.0.1-6.el8.x86_64      1/1
  Running scriptlet: thegreenbow-vpn-client-2.0.1-6.el8.x86_64 1/1
Creating symlink /var/lib/dkms/tgbtun/1.0/source ->
/usr/src/tgbtun-1.0
DKMS: add completed.
```

7. Add the VPN users to the `tg` group by running the following command:

```
sudo usermod -aG tg [user_name]
```

8. Enter the administrator's password and press Enter.

```
[tguser-fr@localhost ~]$ sudo usermod -aG tg tguser-fr
[sudo] password for tguser-fr:
[tguser-fr@localhost ~]$ █
```

9. Activate the product (see section 4 Activating the software).

4 Activating the software

4.1 Introduction

You must activate the Linux VPN Client before being able to use it.

Licenses are available on a subscription basis. Visit the Linux VPN Client page on our website for further details: https://www.thegreenbow.fr/vpn_linux.html.

If you want to test the software before purchasing it, you can benefit from a trial version. Download the software from our website, install it and follow the trial license activation procedure described below in section 4.4 Trial period.

To activate the Linux VPN Client you must have superuser privileges (or root access) on the machine. You must also create a license file named `vpnsetup.ini` as described below.

4.2 Format and content of the `vpnsetup.ini` file

The data allowing you to activate the Linux VPN Client must be entered into a text file named `vpnsetup.ini` in ASCII format.

To do this, enter the license number you have received and the user's email address in an Activation section as follows:

```
[Activation]
License=123456-789012-345678-901234
Email=user@domain.com
```

4.3 Activation procedure

4.3.1 Activation steps

To activate the Linux VPN Client, follow the steps described below:

10. Move or copy the `vpnsetup.ini` file to the `/etc/tgb` folder.
11. Run the following command to restart the service:

```
sudo systemctl restart tgbiked.service
```

12. Run the following command to generate a log:

```
journalctl -r -t tgbiked
```

13. Check that the following message "Activation succeeded with license number 123456-789012-345678-901234" is in the log. For information on how to display the log, refer to section 9 Logs.

4.3.2 Activation errors

If the log contains the message “Activation failed: no activation parameters” and/or “Cancel starting UI Thread, product not activated”, activation has failed. The Linux VPN Client stops immediately.

```
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: Activation failed : no activation parameters
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: Cancel starting UI thread, product not activated
Apr 20 12:14:35 localhost.localdomain tgbiked[99681]: stopping ...
```

4.4 Trial period

You can use a fully functional version of the Linux VPN Client for free of charge during a 30-day trial period.

To do this, install the software normally and generate a `vpnsetup.ini` license file as described above (see section 4.2 Format and content of the `vpnsetup.ini` file) making sure to insert 000000-000000-000000-000000 (24 zeros) instead of the license number.

The license will expire at the end of the 30-day trial period, and you will no longer be able to use the software unless you purchase a license.

Our activation server stores your machine ID. You will only be eligible for a trial license once.

5 Uninstalling the software

When you no longer wish to use the Linux VPN Client, you can uninstall it from the command line as follows:

1. Open a terminal window.
2. Run the following command:

```
sudo yum remove thegreenbow-vpn-client.x86_64
```

This command deletes the files and dependent packages that were added during installation and which are no longer used. Configuration files added later, e. g. `config.tgb`, will not be deleted.

```
[tgbuger-en@localhost ~]$ sudo yum remove thegreenbow-vpn-client.x86_64
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Removing:
 thegreenbow-vpn-client  x86_64           2.0.1-6.el8      @commandline      9.1 M
Transaction Summary
=====
Remove 1 Package

Freed space: 9.1 M
Is this ok [y/N]: █
```

The Linux VPN Client has been uninstalled.

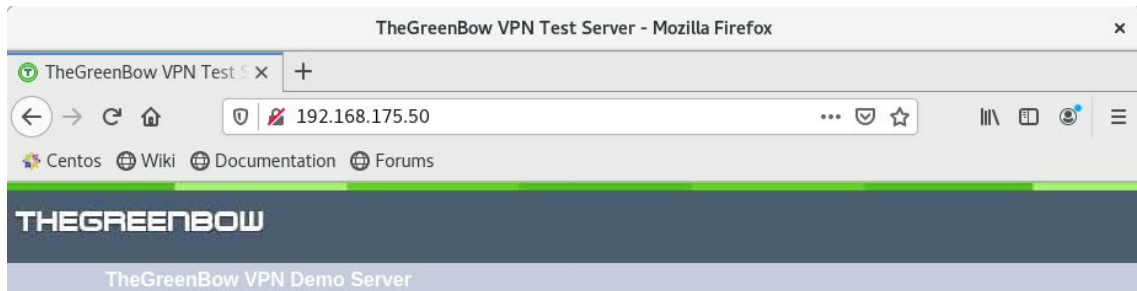
6 Using the test tunnel

A VPN security policy containing a test VPN tunnel called “TgbTest” is provided in the `conf.tgb` file located in the `/etc/tgb/` directory.

It is imported by default and allows you to test the Linux VPN Client by connecting to a test gateway.

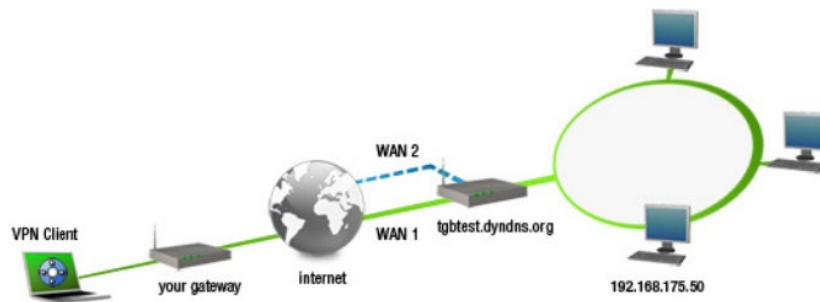
The test configuration can be used to check whether the Linux VPN Client is operational.

Once the tunnel is open, you should be able to send a ping request to IP address 192.168.175.50 or open the <http://192.168.175.50/> web page in your browser.



Congratulations, tunnel successfully opened.

Your machine's connectivity meets the requirements for IPSec VPN. This webpage is located on a webserver reachable through vpn only (extranet).



Examples of protocols that can be used with tunnelling:

Here is a **NetBios** link to our demo server. You can open Windows Explorer and try accessing the shared folder.

`\\192.168.175.50\share\`

RDP is enabled on the server. Feel free to connect to it with windows remote desktop tool.

We don't provide any login/password though, as this is for testing purpose only.

Thank you for using our software.

TheGreenBow Team.

7 Command line

7.1 Introduction

The Linux VPN Client provides a command line interface that enables you to carry out the following operations:

- Display help
- List configured tunnels
- Open a tunnel
- Close a tunnel
- Display the tunnel status

7.2 Displaying help

To display the help, open a terminal window and run the following command:

```
tgbctl help
```

```
[tgbuser-fr@localhost ~]$ tgbctl help
Usage : tgbctl COMMAND

Commands:
  help          produce this help message
  list          display available tunnel
  status <tunnel> display tunnel state
  up <tunnel>   open tunnel
  down <tunnel> close tunnel
[tgbuser-fr@localhost ~]$
```

7.3 Listing configured tunnels

To list configured tunnels, open a terminal window and run the following command:

```
tgbctl list
```

```
[tgbuser-fr@localhost ~]$ tgbctl list
TgbTest-TgbTest closed
[tgbuser-fr@localhost ~]$
```

7.4 Opening a tunnel

To open a tunnel, open a terminal window and run the following command:

```
tgbctl up [tunnel_name]
```

```
[tgbuser-fr@localhost ~]$ tgbctl up TgbTest-TgbTest
opening TgbTest-TgbTest...opened
[tgbuser-fr@localhost ~]$
```

7.5 Closing a tunnel

To close a tunnel, open a terminal window and run the following command:

```
tgbctl down [tunnel_name]
```

```
[tgbuser-fr@localhost ~]$ tgbctl down TgbTest-TgbTest
closing TgbTest-TgbTest...closed
[tgbuser-fr@localhost ~]$
```

7.6 Displaying the tunnel status

To display the status of a tunnel, open a terminal window and run the following command:

```
tgbctl status [tunnel_name]
```

```
[tgbuser-fr@localhost ~]$ tgbctl status TgbTest-TgbTest
open
[tgbuser-fr@localhost ~]$
```

8 Configuring VPN tunnels

8.1 Introduction

TheGreenBow VPN clients rely on a VPN security policy that defines the list of tunnels that the administrator makes available to the workstation user. This file is also called a configuration file and its extension is `.conf`.

The Linux VPN Client does not provide an HMI to build or modify the VPN configuration.

This feature is available in our Windows or macOS VPN Client products (see the corresponding Deployment Guide, you will find links to these documents in section 12 Related reference documents).

If you are an administrator, you must use one of these products to generate a VPN security policy as described in section 8.3 Updating the VPN security policy.

8.2 Protecting the VPN security policy

The Linux VPN Client relies on the Linux operating system to protect the configuration. The configuration file is only accessible to users with superuser privileges.

No other user can modify the configuration file or inject a new one, which guarantees its authenticity and integrity.

The VPN configuration file is stored in the `conf.tgb` file under the `/etc/tgb/` directory.

The rights to this file are `-rw-----`, owner `root`. A standard user therefore cannot gain read or write access to the VPN configuration.

8.3 Updating the VPN security policy

To modify the configuration of your Linux VPN Client, proceed as follows:

1. Generate the configuration in Windows or macOS.
2. Export the configuration in TGB format, without any password-protection, and name it `conf.tgb`.
3. Replace the `conf.tgb` file in the `/etc/tgb/` directory on the machine on which you want to import the configuration.

9 Logs

9.1 Introduction

The logs of the IKE daemon are stored using the log management provided by `systemd`.

To display the logs of the IKE daemon, run the following command in a terminal window:

```
journalctl -t tgbiked
```

9.2 Exporting in text format

To export the contents of the log in text format, run the following command in a terminal window:

```
journalctl -t tgbiked > [my_log_file.log]
```

Customer support is based on this file.

Should the support team ask you for the log file, make sure to also provide the following details in order for the support staff to have all the information it requires at hand:

- Version of the binary package used
- Version of the Linux distribution
- Version of the Linux kernel
- Version of the GNU C library (glibc)

To get information concerning the distribution and kernel, run the following command in a terminal window:

```
uname -a
```

To get information concerning the `glibc` library, run the following command in a terminal window:

```
ldd --version
```

10 Current limitations

The current version of the Linux VPN Client has the following limitations:

- No encrypted configurations can be imported.
- No smart cards or tokens can be used.
- Only a single VPN connection can be open at a time.
- The DH group 21 is not yet available.

11 Managing errors

11.1 User must belong to “tgb” group

If you have not added the current user to the `tgb` user group, the following error message is displayed when you run commands:

```
ERROR: User must belong to "tgb" group
```

To add the user to the `tgb` group, open a terminal window and run the following command:

```
sudo usermod -aG tgb [user_name]
```

You must log out and log back in for CentOS/RedHat to take into account this command. In some cases, you even need to restart the system. We recommend that you restart the system in all cases.

11.2 Cannot get tunnel list

When running the `tgbctl up [tunnel-name]` command, the following error may be displayed:

```
Error : Can't get tunnel list, check if tgbiked  
service is started  
can't be open: check status
```

To check whether the user has been added to the `tgb` group, open a terminal window and run the following command:

```
id
```

If the `tgb` group is not in the list, restart the machine in order for the group you've added to be taken into account.

11.3 Tunnel opening failed

When the Linux VPN Client fails to open a tunnel, the following error message is displayed:

```
Opening [tunnel_name] ..... failed
```

When opening a tunnel has failed, open a terminal window and run the following command:

```
journalctl -r -t tgbiked
```

You can analyze the log yourself (see section 9 Logs) or contact the support team:
<https://www.thegreenbow.com/form.html?subject=vpn&lang=en>.

11.4 Non-root users must not be able to access the configuration file

When the Linux VPN Client is unable to open a tunnel after having replaced the `/etc/tgb/conf.tgb` file with a new configuration, check the log to see whether it contains the following message: “Non-root users must not be able have access to file `/etc/tgb/conf.tgb`”. Users other than superusers should not be able to access the configuration file.

If this is the case, run the following command:

```
sudo chmod 600 /etc/tgb/conf.tgb
```

11.5 Checking drivers

Run the following command to check whether the driver is loaded:

```
lsmod | grep tgb
```

The command must return the following message:

```
tgbtun      [ID] 0
```

If this is not the case, please contact the support team to understand what happened:
<https://www.thegreenbow.com/form.html?subject=vpn&lang=en>.

11.6 IKE daemon is unresponsive

If the IKE daemon becomes unresponsive, which may happen after a network interface change or after disconnecting and reconnecting the network cable, run the following command to restart it:

```
sudo kill -9 $(pidof tgbiked)
```

12 Related reference documents

To find out how to generate the configuration file to be used with the Linux VPN Client, please refer to the following user guides:

- [Windows Enterprise VPN Client](#)
- [TheGreenBow macOS VPN Client](#)

You will find a list of compatible VPN routers and the corresponding configuration guides on our website:

https://www.thegreenbow.com/vpn_gateway.html.

You can download a demo configuration and open a test tunnel by following the instructions on our website:

https://www.thegreenbow.com/support_flow.html?page=122&product=vpn&lang=en.

You will find more information about TheGreenBow products on our website: <https://www.thegreenbow.com>.

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software