TheGreenBow
VPN Client
for Android

User Guide
# Table of content

1 Introduction........................................................................................................................................................................... 3
   1.1 TheGreenBow VPN Client for Android..................................................................................................................... 3
   1.2 The universal VPN Client ........................................................................................................................................ 3
   1.3 Technical characteristics........................................................................................................................................ 4

2 Installation........................................................................................................................................................................... 5
   2.1 Installation................................................................................................................................................................. 5
   2.2 Evaluation period .................................................................................................................................................... 5

3 Activation........................................................................................................................................................................... 6
   3.1 Automatic activation ................................................................................................................................................ 6
   3.2 Manual activation ................................................................................................................................................... 6
   3.3 VPN License ........................................................................................................................................................... 7
   3.4 Activation error ....................................................................................................................................................... 7
   3.5 Subscription management .................................................................................................................................. 7

4 Application upgrade .......................................................................................................................................................... 8

5 Uninstallation .................................................................................................................................................................... 9

6 Quick use: Create and open a VPN Tunnel .................................................................................................................. 10

7 User Interface ............................................................................................................................................................... 12
   7.1 Application architecture ......................................................................................................................................... 12
   7.2 Main screen: VPN Connections .......................................................................................................................... 12

8 VPN Policy import........................................................................................................................................................... 14
   8.1 Create a VPN Policy .............................................................................................................................................. 14
   8.2 Import a VPN Policy ............................................................................................................................................. 14

9 Configure a VPN Tunnel ................................................................................................................................................ 16
   9.1 Configure an IKEv1 VPN Tunnel .......................................................................................................................... 16
   9.2 Configure an IKEv2 VPN Tunnel.......................................................................................................................... 18

10 Certificate management ................................................................................................................................................. 19
   10.1 IKEv1 Certificate management............................................................................................................................ 19
   10.2 IKEv2 Certificate management............................................................................................................................ 20

11 Logs ................................................................................................................................................................................ 21
   11.1 Console ................................................................................................................................................................. 21
   11.2 LogFiles ............................................................................................................................................................... 21
   11.3 LogFiles deletion ............................................................................................................................................... 22

12 Contact ............................................................................................................................................................................. 23
   12.1 Information .......................................................................................................................................................... 23
   12.2 Commercial ......................................................................................................................................................... 23
   12.3 Support ............................................................................................................................................................... 23

13 Appendices ...................................................................................................................................................................... 24
   13.1 Technical characteristics of TheGreenBow VPN Client for Android.............................................................. 24
1 Introduction

1.1 TheGreenBow VPN Client for Android

TheGreenBow VPN Client is the first VPN software for securing remote connections to a company’s Information System.

Available in 25 languages and used by more than 1.7 million connections all over the world, it allows to establish secure connections (VPN tunnels) with any VPN gateway.

TheGreenBow VPN Client is available on all platforms: Windows, Linux, Android, iOS and macOS.

1.2 The universal VPN Client

TheGreenBow VPN Client is the first universal VPN software for securing remote connections to a company’s information system.

VPN available for all hardware

TheGreenBow VPN Client is available on all platforms: Windows, Linux, Android, iOS and macOS. All versions of TheGreenBow VPN Client are available for free evaluation download on the www.thegreenbow.com website. This User Guide is about the Android version of TheGreenBow VPN Client.

Compatible with all VPN gateways

TheGreenBow VPN Client can create secure connections (VPN tunnels) with all VPN gateways on the market. TheGreenBow assesses the compatibility of new VPN gateways with the VPN Client software on a regular basis, and makes available to its users the list of certified gateways, alongside their configuration guides: www.thegreenbow.com/vpn_gateway.html

VPN on all network types

TheGreenBow VPN Client can secure and maintain communications on all network types: 3G, 4G, Wi-Fi, Ethernet, ADSL, Satellite, etc. It is designed and strengthened specifically to ensure performance on even the least reliable networks.
1.3 Technical characteristics

The GreenBow VPN Client for Android takes into account the characteristics required to ensure a maximum and reliable security of the connections:

- VPN tunnel on any medium: Wi-Fi, 3G/4G, etc.
- DPD
- "Disable Split Tunneling" mode
- "All through the tunnel" mode
- IKEv1, IKEv2
- IPsec
- IPv4
- X-Auth, Mode Config/CP Mode
- Preshared Key, Certificates X509 or PKCS12

See Appendix for more details on the technical characteristics of The GreenBow VPN Client.
2 Installation

2.1 Installation

Download the file "TheGreenBow_VPN_Android.apk" from TheGreenBow website on the target device. Via the device file explorer, launch the file TheGreenBow_VPN_Android.apk.

2.2 Evaluation period

When installed for the first time on a device, the software will enter an evaluation period of 30 days. During this evaluation period, the VPN Client is fully operational and all functions are unlocked.

During the evaluation period, the activation screen can be displayed from the upper-right "menu" icon of the main screen. This screen will display the number of remaining days in the evaluation period.

Once the evaluation period is expired, no VPN tunnel can be opened. Each time the user wants to open a tunnel, the following information screen will be displayed:
3 Activation

The GreenBow VPN Client must be activated in order to run after the end of the evaluation period.

The activation process can be run either manually (user mode) or automatically (deployment mode).

3.1 Automatic activation

The activation can be started and processed automatically. This feature is particularly useful when you want to activate the software automatically during a deployment.

To run an automatic activation:

1. Write the license number in a file called "license.txt", according to the following syntax:
   
   license = 123456-123546-123456-123456

2. Copy this file on the Device in the directory "vpnImport"

The license file will be read the next time the application starts, and the application will process the activation automatically.

Note: It is possible to check locally the result of the activation process in the menu "Activation".

3.2 Manual activation

To process a manual activation:

1. Open the upper-right menu of the main screen and select "Activation"

2. In the "Enter your license number" field, type in the license number you received by email. Note: The license number is only composed of the characters [0..9] and [A..F], sometimes in groups of 6 characters and separated by hyphens.

3. Click "Activate!" to run the online activation process.

Once the activation has been carried out successfully, the license number and the activation duration are displayed in the activation screen.
Note: The software activation is linked to the device on which the software has been installed. As a consequence, a license number allowing a single activation cannot be reused on another device once activated.

### 3.3 VPN License

In order to get the license number, click on "Buy" in the activation screen. This will open the VPN Store on TheGreenBow website.

### 3.4 Activation error

Software activation may fail for various reasons. The error is always displayed in the activation screen, together with a short explanation.

![Activation error screenshot]

On TheGreenBow website are listed all activation errors and procedures for solving activation issues. The most common activation errors are:

<table>
<thead>
<tr>
<th>#</th>
<th>Meaning</th>
<th>Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Wrong license number</td>
<td>Check license number</td>
</tr>
<tr>
<td>33</td>
<td>The license number is already activated on a different device</td>
<td>Uninstall the software on the device with the activated license or contact TheGreenBow’s Sales department</td>
</tr>
<tr>
<td>53</td>
<td>Communication with the activation server is impossible</td>
<td>Ensure that the device is connected to the internet. Check that communication is not blocked by a firewall or proxy. Configure the firewall to let the communication through or the proxy to reroute it properly.</td>
</tr>
</tbody>
</table>

### 3.5 Subscription management

TheGreenBow VPN Client for Android is licensed through a subscription mode.

During the month before the subscription period expires, a warning is displayed each time a VPN tunnel opens. It shows the number of days left before the subscription period expires.

The number of days left before the subscription period expires is also always displayed in the activation screen.

Note: To ease the process of subscription renewal, the software automatically tries to re-activate each time it starts.
4 Application upgrade

Download the upgrade "TheGreenBow_VPN_Android.apk" from TheGreenBow website on the target device.
Via the device file explorer, launch the file TheGreenBow_VPN_Android.apk

During an upgrade, the VPN configuration file and the activation parameters are kept.
5 Uninstallation

The procedure to uninstall the application is described below:

1. Open the Settings
2. select Application manager
3. select « TheGreenBow VPN »
4. press on UNINSTALL, and confirm the uninstallation
6 Quick use: Create and open a VPN Tunnel

To create a new VPN tunnel, follow the steps below:

1. In the main screen (VPN Connections screen), press the button "+" (Add) at the bottom of the screen
2. Choose a name for the new VPN tunnel
3. By default, the tunnel is an IKEv1 tunnel. Select IKEv2 to create an IKEv2 tunnel.

The new VPN tunnel is created: it is added to the list of VPN Connections.

This new VPN tunnel is configured with a set of default parameters which enable to open a VPN tunnel on TheGreenBow VPN test network.

Press the "OPEN" button.
In case of IKEv1 protocol, a pre-shared key is asked to open the tunnel. The default pre-shared key is "123456789".
In case of IKEv2 protocol, the tunnel opens automatically, no password is asked to the user.
In IKEv1 mode, the opening of the tunnel results in the display of a TheGreenBow VPN test web page:
7 User Interface

7.1 Application architecture

The GreenBow VPN Client for Android is organized around the following screens:

VPN Connections
IKEv1 Settings
IKEv2 Settings
Logs/Console
About
Activation

7.2 Main screen: VPN Connections
The VPN Client main screen provides an access to all the functionalities of the application.

**Upper-right menu button**

Clicking on the upper-right menu button enables access to the About screen and the Activation screen (Cf. chapter 3 "Activation" for details about the activation process)

**VPN Tunnel line**

Clicking on the "OPEN" button of a tunnel opens this tunnel. Clicking on the icon on the left of a tunnel name opens the settings of this tunnel.

**Bottom menu**

In the bottom menu, the "Logs" button opens the log/console screen. Note: The logs/console screen is only accessible if no tunnel is open. The "Restart" button enables to reinitialize the application (this includes a restart of the IKE daemon). The "Add" button enables to create a new VPN tunnel.

**Back and Home buttons of the device**

When the button "Back" of the device is pressed while the application is opened on the main screen (VPN Connections), a confirmation is asked to the user and the application exits. If a tunnel was opened, it is closed.

When the button "Home" of the device is pressed, the application goes in the background. If a tunnel is opened, it remains opened.
8 VPN Policy import

The VPN Client for Android is designed to use a VPN Policy created with the VPN Client for desktop (Windows).

8.1 Create a VPN Policy

A VPN Policy used by TheGreenBow VPN Client for Android must be created with TheGreenBow VPN Client for Windows. The following procedure describes the steps to generate a VPN Policy for the VPN Client for Android.

1. Download and install TheGreenBow VPN Client for Windows
2. In the main interface of the VPN Client for Windows, create the VPN Tunnel you want to open with the VPN Client for Android (check the tunnel is operational)
3. Export this VPN Tunnel (right click on the tunnel and select "export")

Note: Be careful to export only one VPN tunnel: the VPN Client for Android can handle several VPN Policies simultaneously, but only accepts VPN Policy which own a single VPN tunnel.

Note: If you are exporting an IKEv1 VPN tunnel, be careful to NOT protect the exported VPN Policy with a password (select "Don't protect the exported VPN Configuration" when exporting the VPN tunnel).
Conversely, if you are exporting an IKEv2 VPN tunnel, you can choose to protect or not the exported VPN Policy. If you protect the exported VPN Policy with a password, this password will be asked when the VPN Policy will be imported in the VPN Client for Android.

Note: The name of the exported VPN Policy will be used as the name of the VPN tunnel by the VPN Client for Android.

8.2 Import a VPN Policy

The following procedure describes the steps to import a VPN Policy in the VPN Client for Android.

1. Connect the Android device to the computer owning the VPN Policy to be imported via the USB port
2. Copy the VPN Policy in the device directory "TheGreenBow\tgbImport"
3. Run the VPN Client for Android: the VPN Policy is automatically added to the list of the available VPN tunnels.
Note: If the VPN Policy was protected with a password when it was exported from the VPN Client for Windows, this password is asked during the process of import.

Note: if the VPN Policy contains certificates, please refer to the chapter 10 "Certificate management".

Note: TheGreenBow VPN Client for Android can handle several VPN Policies. Thus, several VPN Policies can be imported successively. It is possible to copy several VPN Policies simultaneously, they will all be imported when the VPN Client for Android will start.
9 Configure a VPN Tunnel

The VPN Client for Android is designed to use a VPN Policy created with the VPN Client for desktop (Windows), Cf. chapter 8 "VPN Policy import".

Nevertheless, the VPN Client for Android interface enables to configure some VPN parameters. This VPN parameters are described below.

9.1 Configure an IKEv1 VPN Tunnel

Press the ">" button for the IKEv1 VPN tunnel you like to configure.
### Gateway
DNS or IP address of the remote VPN Gateway

### Mode
Main or aggressive mode

### Authentication Mode
Authentication mode: Certificate, Pre Shared Key or X-Auth

### Login (XAuth), Password (XAuth)
X-Auth login and password

### Certificate File Name
Name of the file containing the certificate (P12 or PFX) used by the VPN tunnel. See section "Certificate management".

### Mode Config
Enabled / Disabled. (This allows the VPN tunnel to automatically receive from the VPN gateway a set of parameters used to open the tunnel)

### Remote Network / Prefix length
Remote network address

### Virtual IP
Virtual IP address in the smartphone remote network.

### Interface
List of available interfaces

To save the VPN Policy, press the "Save" button.

### Password management
In IKEv1, it is not possible to store the password in the VPN configuration. Thus, the password is asked to the user each time the tunnel opens.

The password is different depending on the type of authentication:
- In PSK mode, the password is the Pre Shared Key.
- In X-Auth mode, the password is the X-Auth password

**Note:** in IKEv1 mode, the VPN Client for Android only allows an X-Auth authentication together with the PSK mode. Thus, when the X-Auth authentication is chosen, the PSK must be configured.
- In Certificate mode, the password is the password which protects the P12 certificate. Cf. chapter 10.1 "IKEv1 Certificate management".

Note: the latest used password is stored by the application. This enables to reopen the connection without having to re-enter the password.
9.2 Configure an IKEv2 VPN Tunnel

Press the ">" button for the IKEv2 VPN tunnel you like to configure.

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Tunnel Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>DNS or IP address of the remote VPN Gateway</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method: PSK, Certificate, EAP (Extended Authentication Protocol)</td>
</tr>
<tr>
<td>Login (EAP)</td>
<td>The EAP authentication enables the authentication of the user through a login/password which must be configured in the gateway. The EAP Login must be configured in the IKEv2 settings. The EAP password will be asked to the user each time the tunnel opens.</td>
</tr>
<tr>
<td>Preshared Key</td>
<td>Set a pre shared key if needed (only for EAP mode)</td>
</tr>
<tr>
<td>Confirm</td>
<td>Confirm the preshared key (only for EAP mode)</td>
</tr>
</tbody>
</table>

**Note:** Until release 5.10, it is not possible to use the interface (settings) to switch an IKEv2 VPN Configuration from a PSK or EAP mode to a Certificate mode. To switch to a certificate mode, it is required to import a new VPN configuration file that includes the certificate (Cf. chapter 8.2 "Import a VPN Policy")

To save the VPN Policy, press the "Save" button.

**Password management**

In IKEv2, the password is only asked to the user in EAP mode, each time the tunnel opens.
10 Certificate management

10.1 IKEv1 Certificate management

In IKEv1 mode, there are 2 possibilities to import certificates.

Solution 1: import a VPN configuration which contains a certificate.

When the VPN configuration is imported, the user is asked to enter a password in order to protect the certificate. This password will be asked to the user each time the tunnel opens.

Solution 2: import a certificate separately from the VPN configuration.

IKEv1 enables to import PKCS12 certificates, which are encrypted (P12 or PFX files). The password used to protect the P12 certificate will be asked to the user each time the tunnel opens.

To import a P12 certificate, follow the step below:

1. Copy the Certificate "P12" file into the following directory:
   ```
   TheGreenBow / TGBImport
   ```

2. Quit and restart the application.
3. The certificate is automatically imported into the application (and it is removed from the import directory). The certificate appears in the list of certificates that can be chosen for the selected VPN tunnel.
4. Open the configuration via the user interface (Press the ">") button for the VPN tunnel you like to configure).
5. Select the certificate in the dropdown for the "Certificate File Name" item.
6. Save using the "Save" button in the bottom of the app.
10.2 IKEv2 Certificate management

IKEv2 enables to use certificates which are stored in the VPN Configuration. It means, certificates can be used in an IKEv2 VPN tunnel as soon as they are stored in the VPN Configuration file that is imported (See chapter 8 for VPN import details).
11 Logs

TheGreenBow VPN Client Android implements two types of logs: logs displayed in the user interface (console) and logs available in log files.

11.1 Console

The "Console" gives detailed information on the tunnels as well as the related opening and closing steps. It is mostly made of the IKE messages and gives high-level information about the establishment of the VPN tunnel. It is intended for use by the administrator for identifying possible VPN connection incidents.

To display the console logs, click on the "Logs" button in the bottom of the main screen (VPN Connections screen).

The logs displayed in the console are those of the last VPN connection that was open.

Note: The Console cannot be opened/viewed if a tunnel is opened.

11.2 LogFiles

All log files are available in the directory "TheGreenBow / tgbExport" as soon as the log console is displayed. It means, they are produced continuously in the app directory and they are copied in the tgbExport directory when the log console is displayed.
Logfiles

tgblogYYYY-MM-DD.txt contains the IKEv1 logs which appear in the application console

ikelogYYYY-MM-DD.txt contains the detailed IKEv1 logs

ikev2ConsoleYYYY-MM-DD.txt contains the IKEv2 logs which appear in the application console

ikev2logYYYY-MM-DD.txt contains the detailed IKEv2 logs

where YYYY is the year, MM is the month, DD is the day.

11.3 LogFiles deletion

All logs files and all logs information are deleted as soon as the application is exited.
12 Contact

12.1 Information

All information about TheGreenBow products are available on the following website:
English: www.thegreenbow.com
French: www.thegreenbow.fr

12.2 Commercial

Phone contact: +33.1.43.12.39.30
Mail contact: sales@thegreenbow.com

12.3 Support

Technical information about the software support can be found on TheGreenBow website.

Support

English: http://www.thegreenbow.com/support.html
French: http://www.thegreenbow.fr/support.html

Online support


FAQ

English: http://www.thegreenbow.com/vpn_faq.html
French: http://www.thegreenbow.fr/vpn_faq.html

Contact

Technical support can be reached through the support forms available on TheGreenBow website, or directly through the support email: support@thegreenbow.com
13 Appendices

13.1 Technical characteristics of TheGreenBow VPN Client for Android

General

<table>
<thead>
<tr>
<th>Android version</th>
<th>Android 5.0 and further</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>English</td>
</tr>
</tbody>
</table>

Connection / Tunnel

<table>
<thead>
<tr>
<th>Connection mode</th>
<th>Peer-to-Gateway (see the list of certified gateways and their configuration guides)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>GSM/GPRS, Wi-Fi</td>
</tr>
<tr>
<td></td>
<td>Wireless LAN: 3G, 4G</td>
</tr>
<tr>
<td>Tunnelling Protocol</td>
<td>IPsec: complete support</td>
</tr>
<tr>
<td></td>
<td>IKEv1 or IKEv2 (IKE based on OpenBSD 3.1 (ISAKMPD))</td>
</tr>
<tr>
<td></td>
<td>Diffie-Hellman DH group 1 to 18</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>Main mode and Aggressive mode</td>
</tr>
<tr>
<td>Config mode</td>
<td>Obtaining automatically the network parameters from the VPN gateway</td>
</tr>
</tbody>
</table>

Cryptography

| Encryption            | Symmetric: DES, 3DES, AES 128/192/256bit                                           |
|                       | Asymmetric: RSA                                                                    |
|                       | Diffie-Hellman: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072),       |
|                       | DH16 (4096), DH17 (6144), DH18 (8192)                                               |
|                       | Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 (IKEv2 only)                        |
| Authentication        | Administrator: Protecting access to the VPN security policies                     |
|                       | User:                                                                             |
|                       | - Static or dynamic X-Auth (prompt for each tunnel opening)                        |
|                       | - Pre-shared key                                                                  |
|                       | - EAP (MSCHAP-V2)                                                                 |
|                       | - Multiple Auth                                                                   |
| PKI                   | - Support for X509-, PKCS12                                                       |
|                       | - Certificate criteria: validity date, cancellation, subject, key usage            |
|                       | - "Client" and "Gateway" certificate check                                         |

Misc

<p>| NAT/NAT-Traversal     | NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address       |
|                       | emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode,     |
|                       | NAT-T in forced, automatic or disabled mode                                         |
| DPD                   | RFC3706. Detection of inactive IKE endpoints.                                      |</p>
<table>
<thead>
<tr>
<th>Redundant Gateway</th>
<th>Redundant gateway management, automatically selected when DPD is triggered (inactive gateway)</th>
</tr>
</thead>
</table>

### Administration

| VPN policy management | Import and export options for VPN policies  
|                       | Securing import/export using passwords, encryption and integrity control |
| Log and traces        | IKE/IPsec log console  
|                       | Administrator log: local file. |
| License and activation| Flexibility when it comes to licenses (standard, temporary, limited duration, subscription), software activation (WAN, LAN) and deployment options (deployment of the activated softwares, silent activation, etc.) |
Secure, Strong, Simple
TheGreenBow Security Software