

THEGREENBOW

TheGreenBow
Android
VPN Client

User Guide

Table of contents

1	Introduction.....	3
1.1	TheGreenBow VPN Clients.....	3
1.2	Features of TheGreenBow Android VPN Client.....	4
2	Installation.....	5
2.1	Installation Process.....	5
2.2	Evaluation Period.....	5
3	License Activation.....	6
3.1	Purchase a License.....	6
3.2	Automatic activation.....	6
3.3	Manual activation.....	6
3.4	Activation errors.....	7
4	Uninstalling.....	8
5	Testing the VPN Client.....	9
6	User Interface.....	11
6.1	Application wireframe.....	11
6.2	Main screen: VPN Connections.....	11
7	Importing VPN Policies.....	13
7.1	Creating a VPN Policy.....	13
7.2	Importing a VPN Policy.....	13
8	Configuring a VPN Tunnel.....	15
8.1	Configuring an IKEv1 VPN Tunnel.....	15
8.2	Configuring an IKEv2 VPN Tunnel.....	17
8.3	Configure an SSL VPN Tunnel.....	18
8.4	Configuring the network interface.....	19
9	Opening a VPN Tunnel.....	20
9.1	Opening an IKEv1 VPN Tunnel.....	20
9.2	Opening an IKEv2 VPN Tunnel.....	20
9.3	Opening an SSL VPN Tunnel.....	20
10	Logs.....	21
10.1	Console.....	21
10.2	Log files.....	21
11	Contact.....	23
11.1	Information.....	23
11.2	Commercial.....	23
11.3	Support.....	23
12	Technical features.....	24

1 Introduction

1.1 TheGreenBow VPN Clients

TheGreenBow VPN Clients are VPN Client software that can open IPsec and SSL tunnels, ensuring the upmost level of authentication, integrity and security for remote connections to a company's Information System.

Used by over 2 million people all over the world, TheGreenBow Windows and Linux VPN Clients have been certified Common Criteria EAL3+, which qualifies them to be used for critical communications at NATO and EU.

TheGreenBow VPN Clients are available for all platforms, compatible with all gateways and work on any kind of network.



Available for all platforms

TheGreenBow VPN Clients are available for the following platforms: Windows, Linux, Android, iOS and macOS. They can be downloaded from the www.thegreenbow.com website and used free of charge for an evaluation period of 30 days.

Compatible with all gateways

TheGreenBow VPN Clients can create secure connections with virtually all the VPN gateways in the market. TheGreenBow VPN Clients are tested for interoperability with a large list of VPN gateways. A list of guides for configuring VPN gateways and TheGreenBow VPN Clients is available here: www.thegreenbow.com/vpn_gateway.html.

Work on any kind of network

TheGreenBow VPN Clients can secure and maintain communications on any kind of network: 4G, 5G, Wi-Fi, Wired, Satellite, etc. It is designed and strengthened specifically to ensure great performance even on the least reliable networks.

1.2 Features of TheGreenBow Android VPN Client

TheGreenBow Android VPN Client is packed with the following features:

- Compatible with most IPsec and SSL compliant gateways
- Protocols: SSL, IPsec IKEv1 (not supported on Android 10 and higher) and IKEv2
- Strong Authentication: X-Auth, PSK, EAP
- Certificate management: PKCS#12, PFX, PEM
- NAT-T mode forced
- Mode Config / Configuration Payload
- Encryption: 3DES, AES 128, 192, 256
- SHA256, SHA384, SHA512
- DH Group 1, 2, 5, 14, 15, 16, 17, 18
- DPD (Dead Peer Detection)
- IKEv2 fragmentation
- Secure management of VPN policies (encryption and integrity)
- Intuitive GUI with full configuration capabilities
- Real time log display

See Appendix for more details on the [technical features of TheGreenBow Android VPN Client](#).

2 Installation

2.1 Installation Process

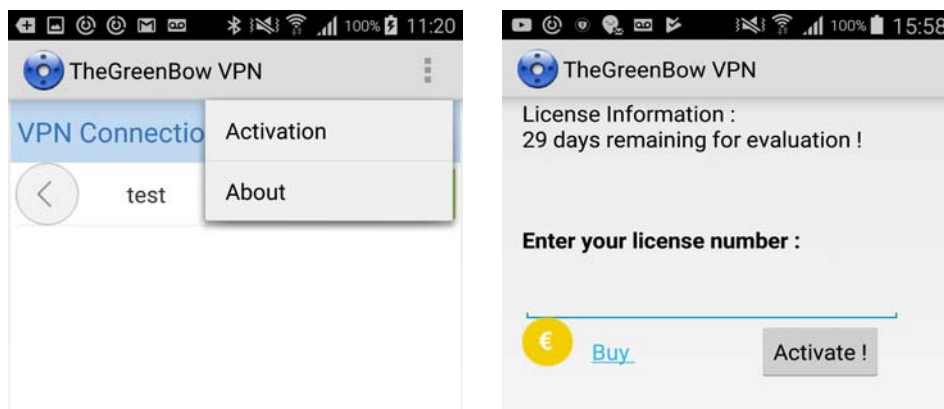
To install TheGreenBow Android VPN Client, download the file "TheGreenBow_VPN_Android.apk" from www.thegreenbow.com website and drop it into the target device, then launch the APK from the device's file explorer.

2.2 Evaluation Period

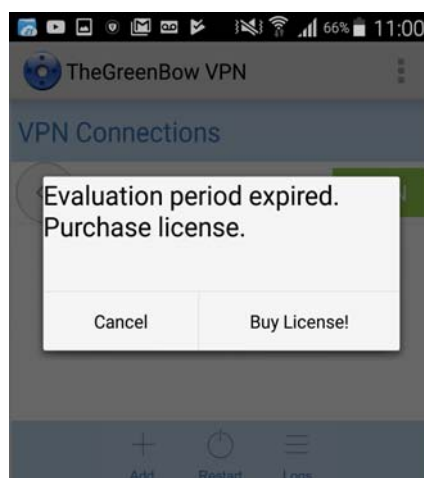
Once installed, the software can be used free of charge for an evaluation period of 30 days. During this evaluation period, the VPN Client is fully operational and all its functions are unlocked.

The activation screen can be displayed by clicking on the menu at the top right menu of the main screen and selecting the "Activation" menu item.

This screen will display the number of remaining days of the evaluation period.



Once the evaluation period is expired, VPN tunnels can no longer be opened. Instead, the following information screen will be displayed:



Note: When upgrading from a previous installation, the existing VPN configuration and activation files will be automatically used.

3 License Activation

After the end of the evaluation period, TheGreenBow VPN Client needs an active license to continue running. License activation can be done either automatically or manually.

3.1 Purchase a License

To obtain a license for using TheGreenBow Android VPN Client, click on the button "Buy" from the activation screen. This will open the VPN Store on the www.thegreenbow.com website.

An activate license allows you to use TheGreenBow Android VPN Client for a defined period of time, after which it will expire. 30 days before the expiration date, a warning will be displayed each time a VPN tunnel is opened. The number of remaining days before the license expires is also displayed. This information is also available on the activation screen.

To renew a license subscription, check the VPN Store on the www.thegreenbow.com website.

3.2 Automatic activation

License activation can be performed automatically by the application. This feature is particularly useful when you want to activate multiple Android VPN Client licenses at once.

For 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 the file in the "vpnImport" folder of the App. For Android up to version 9, the folder is called "TheGreenBow/". For Android 10 and higher, the folder is called "Android/data/com.thegreenbow.TheGreenBowVPN/files/".

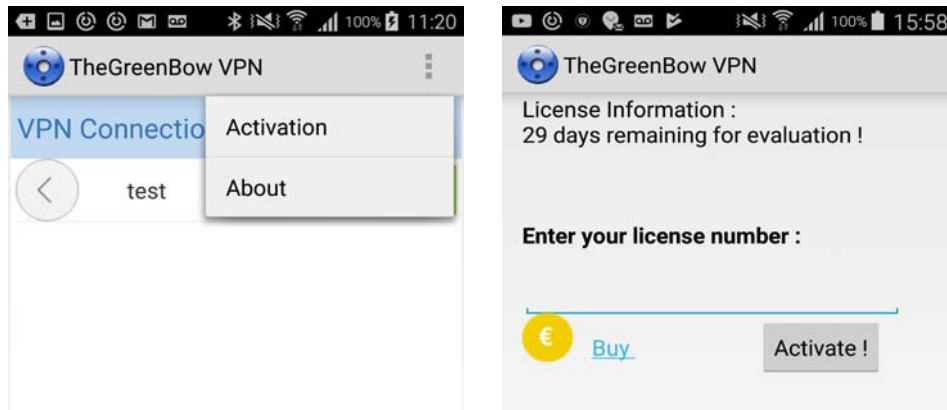
Next time the application starts, the license will be automatically activated.

Note: It is possible to check the result of the license activation from the "Activation" menu item.

3.3 Manual activation

For manual activation:

- 1 Open the menu on the top right of the main screen and select the "Activation" menu item.



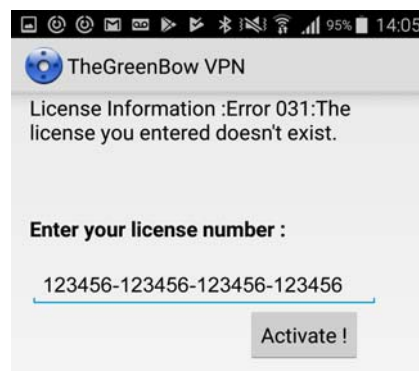
- 2 In the field "Enter your license number", write down the license number that you have received, e.g. by email. Note: The license number is only composed of the characters [0..9] and [A..F], in groups of 6 characters and separated by hyphens.
- 3 Click on the "Activate !" button to activate your license.

Once the activation is successful, the license number and the duration of the activation license can be displayed from the activation screen.

Note: The license is linked to the device on which the software was installed. As a consequence, once activated on one device, the license number cannot be reused on another device.

3.4 Activation errors

Software activation may fail for various reasons. If an error occurs, an error code will be displayed on the activation screen, followed by short error message:



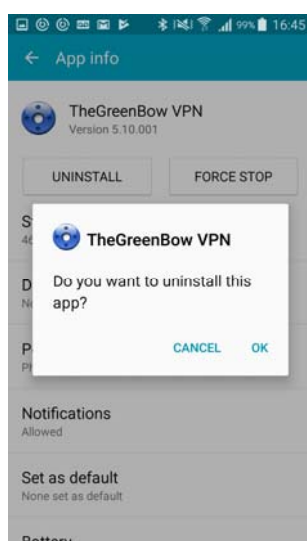
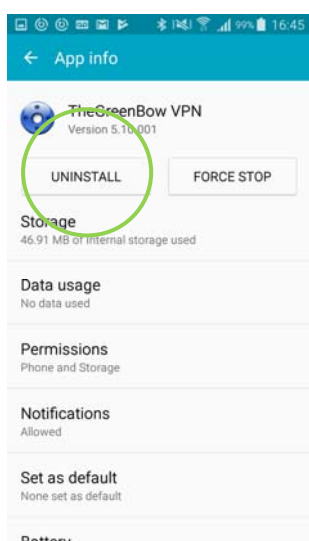
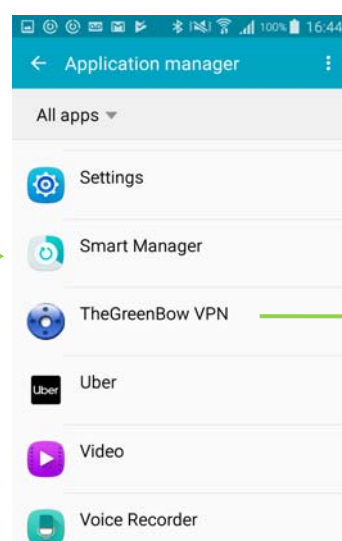
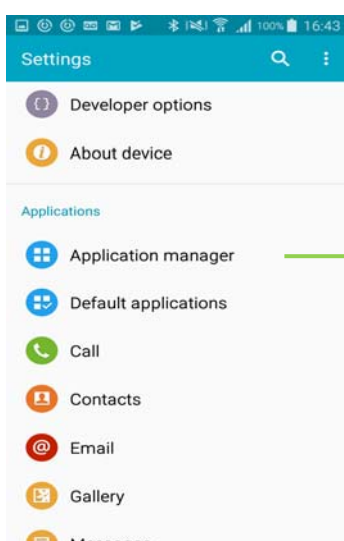
The most common activation error codes are the following:

#	Meaning	Troubleshooting
31	The license number does not exist	Check your license number and try again
33	The license number is already activated on a different device	Use a different license number
53/54	Communication with the activation server is impossible	Ensure that the device is connected to the internet Check that communications are not blocked by a firewall.

4 Uninstalling

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



5 Testing the VPN Client

This section shows you how to create and open a test VPN tunnel that will connect to TheGreenBow's test VPN network.

First, create a tunnel by following 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 Select the required VPN protocol "IKEv1", "IKEv2" or "SSL"



Note: IKEv1 is supported only on Android versions up to 9.

The new VPN tunnel is now created and added to the list of VPN Connections.

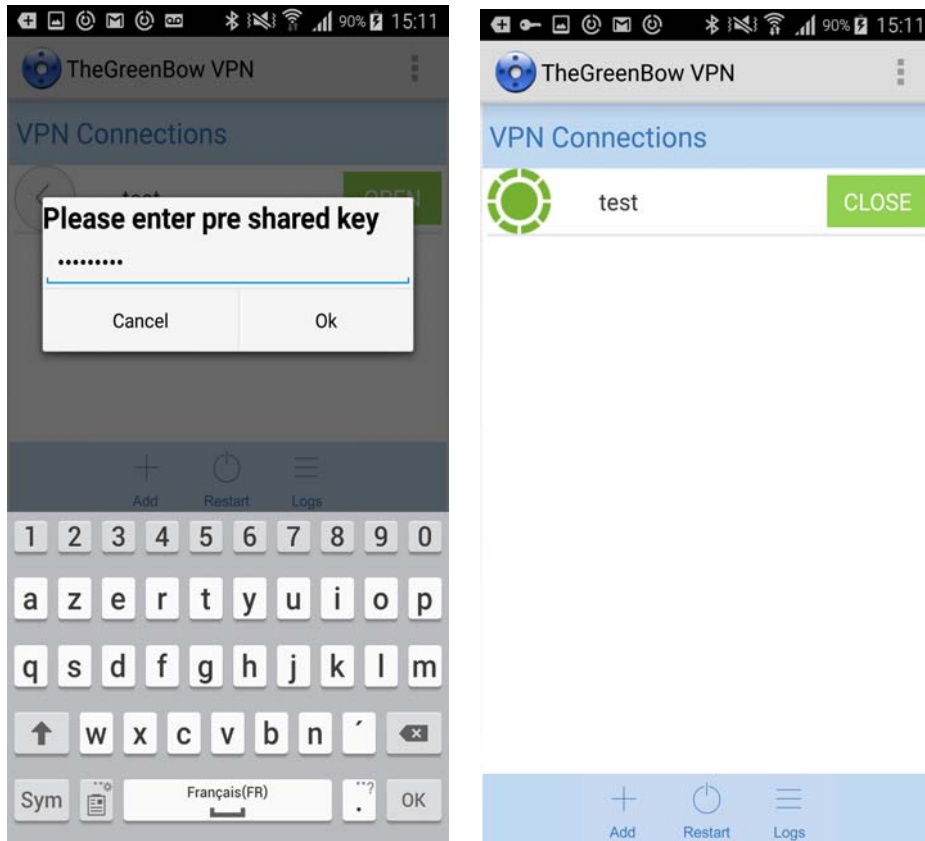
This new VPN tunnel is configured with a set of default parameters which enable to open a VPN tunnel on TheGreenBow's test VPN network.

Press the "OPEN" button.

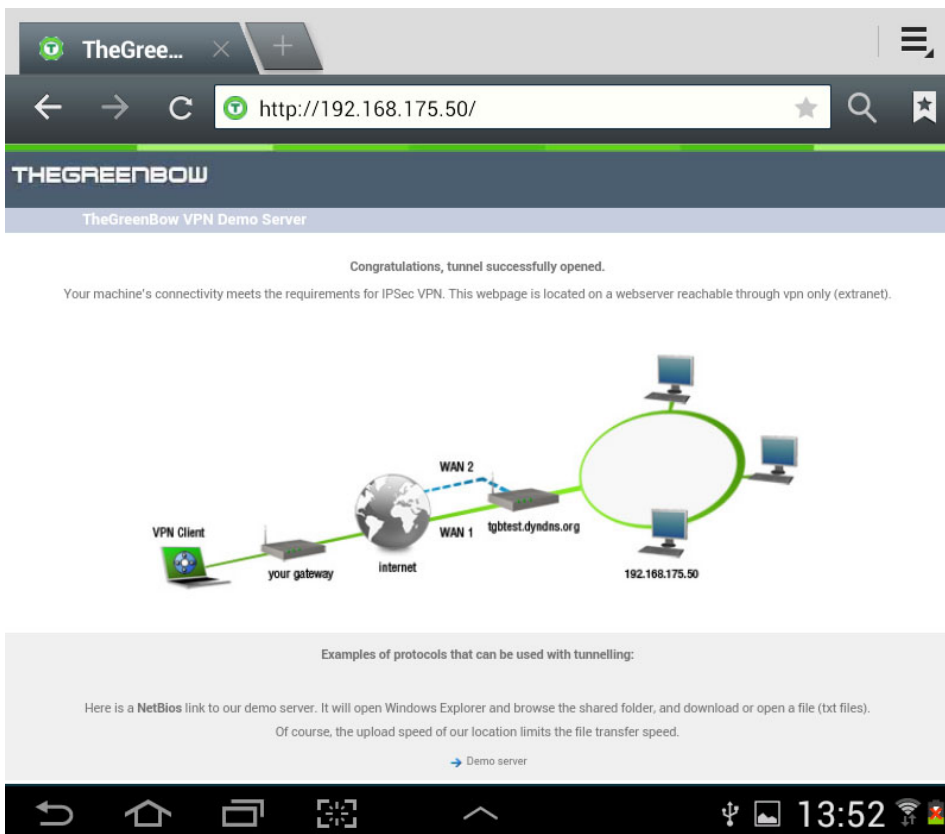
For the IKEv1 protocol, a pre-shared key is asked to open the tunnel. The default pre-shared key is "123456789".

For the IKEv2 protocol, the tunnel opens automatically, no password is asked to the user.

For the SSL protocol, a password is asked to the user. The default password is "tgbtest".



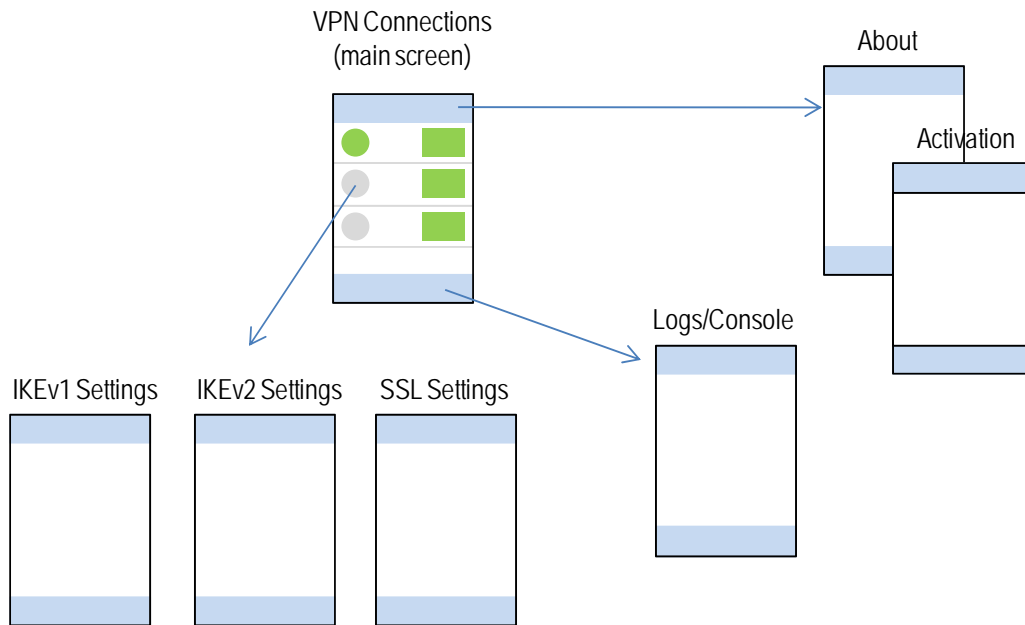
In IKEv1 mode, opening the tunnel results in the display of the following web page:



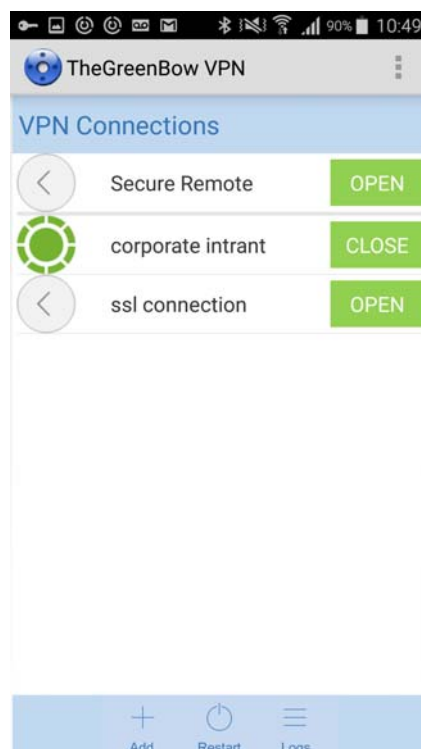
6 User Interface

6.1 Application wireframe

TheGreenBow Android VPN Client is organized around the following screens:



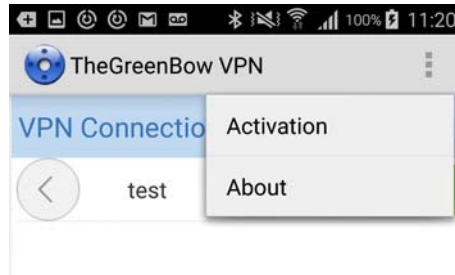
6.2 Main screen: VPN Connections



The Android VPN Client's main screen provides an access to all the features of the application.

Upper-right menu button

Clicking on the upper-right menu button opens a menu, where you can select the About menu item and the Activation menu item (Cf. chapter 3 "[License Activation](#)" for details about the activation process)



VPN Tunnel

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 allows you to create a new VPN tunnel.



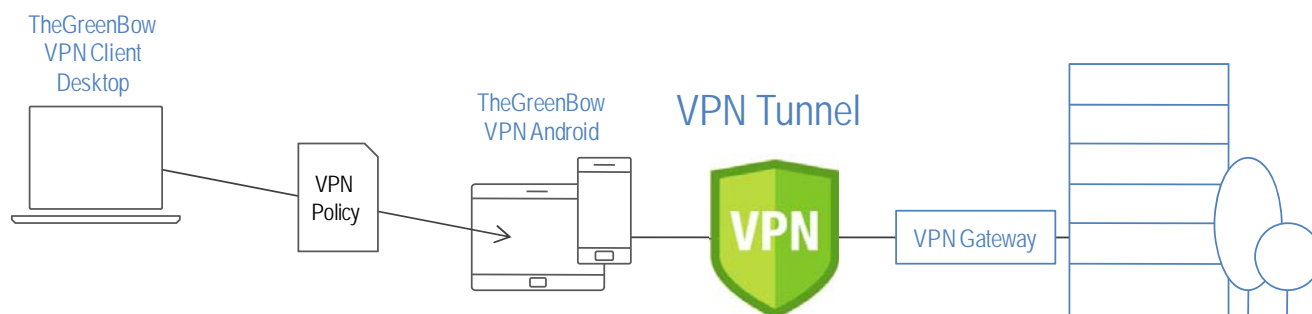
Back and Home buttons of the device

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.



7 Importing VPN Policies



To connect to your own remote network, TheGreenBow Android VPN Client must be configured with a VPN Policy created by TheGreenBow Windows VPN Client on a desktop or laptop computer.

7.1 Creating a VPN Policy

The following procedure describes the steps to create a VPN Policy from TheGreenBow Windows VPN Client:

- 1 Download and install TheGreenBow Windows VPN Client
- 2 Using the configuration manager of TheGreenBow Windows VPN Client, create a VPN tunnel with the parameters of your network
- 3 Export the configuration of the tunnel that you just created by right clicking on the created tunnel and selecting "export".

Note: Be careful to export only one policy in a VPN Policy file. The Android VPN Client can handle multiple VPN Policies, but only accepts VPN Policy files that contain a single policy.

Note: If you are exporting an IKEv1 VPN tunnel, make sure that you do NOT protect the exported VPN Policy with a password (select "Don't protect the exported VPN Configuration") when exporting the VPN tunnel. TheGreenBow Android VPN Client does not support importing VPN Policies protected with a password.

If you are exporting an IKEv2 VPN tunnel, you can choose to protect the exported VPN Policy with a password. If you protect the VPN Policy, the password will be asked when the VPN Policy is imported into the Android VPN Client.

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

7.2 Importing a VPN Policy

The following procedure describes the steps to import a VPN Policy into TheGreenBow Android VPN Client.

- 1 Connect the Android device via the USB port to the computer where the VPN Policy was exported
- 2 Copy the file in the "vpnImport" folder of the App. For Android up to version 9: copy the VPN Policy in the device directory "TheGreenBow\vpnImport". For Android 10 and over: copy the VPN Policy in the device directory "Android/data/com.thegreenbow.TheGreenBowVPN/files/vpnImport"

- 3 Launch the Android VPN Client: 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 Windows Client, enter the password during the import process.

Note: TheGreenBow Android VPN Client can handle several VPN Policies. They must be imported from multiple files, each containing a single VPN Policy. When the Android VPN Client is launched, all the imported VPN Policies will be added to the list of available tunnels.

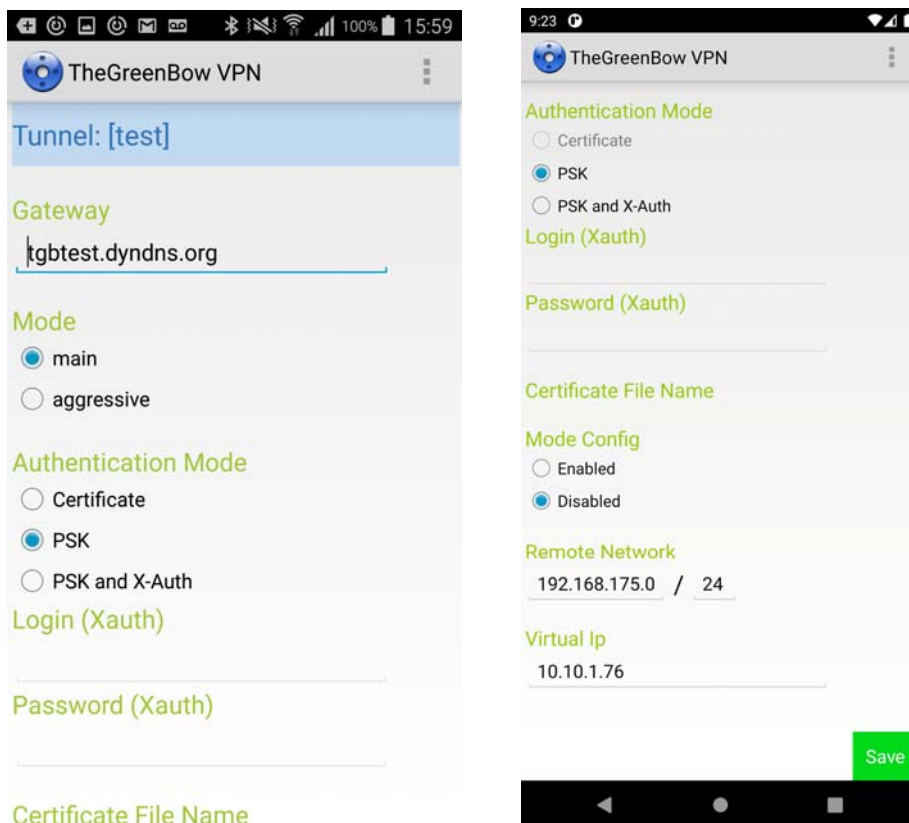
8 Configuring a VPN Tunnel

Even though the Android VPN Client is designed to be configured using VPN Policies created by TheGreenBow Windows VPN Client (see chapter 7 "[Importing VPN Policies](#)"), its user interface still allows you to modify the following VPN parameters.

8.1 Configuring an IKEv1 VPN Tunnel

Press the ">" button to configure one of the IKEv1 VPN tunnels in the list.

You will see the following screens that will allow you to make changes, as explained in the table that follows.



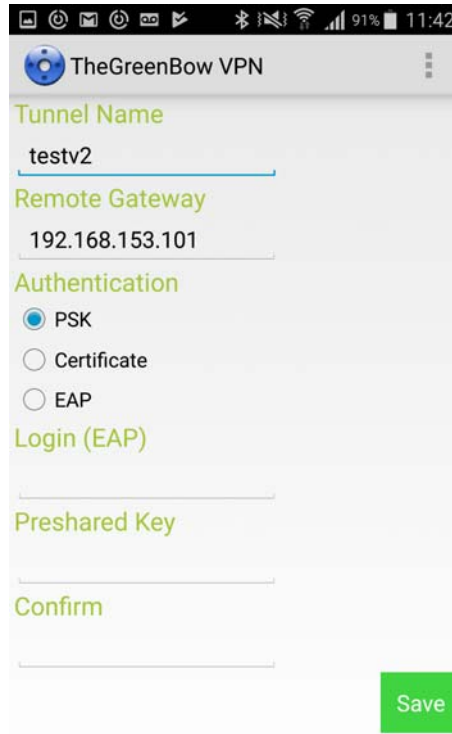
Gateway	DNS or IP address of the remote VPN Gateway
Mode	Main or aggressive mode
Authentication Mode	Authentication mode: Certificate, Pre-shared Key or X-Auth
Login (XAuth), Password (XAuth)	X-Auth login and password
Certificate File Name	This field is not available in the current version of the software
Mode Config	Enabled / Disabled (allows the Client to receive the following network parameters from the gateway)
Remote Network / Prefix length	Remote network address: enter a value only if Mode Config is disabled
Virtual IP	Virtual IP address of the Client: enter a value only if Mode Config is disabled

Once you have made your changes, press the "Save" button to save the updated VPN Policy on the Android device.

8.2 Configuring an IKEv2 VPN Tunnel

Press the ">" button to configure one of the IKEv2 VPN tunnels in the list.

You will see the following screen that will allow you to make changes, as explained in the table that follows.



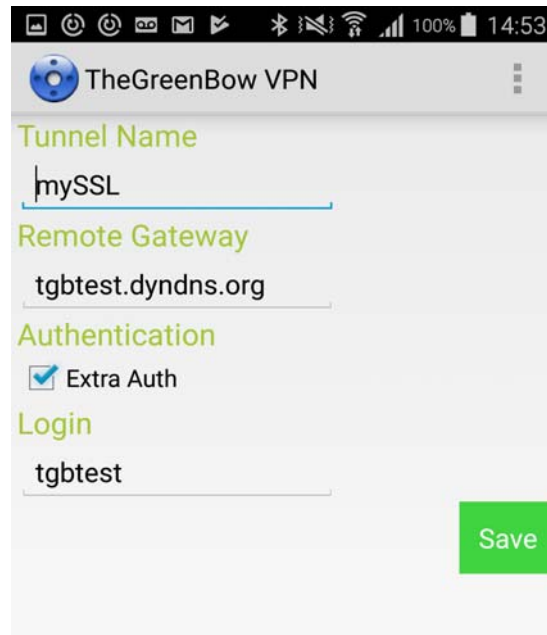
Tunnel Name	The name of the tunnel
Remote Gateway	IP address of the remote VPN Gateway
Authentication	Authentication method: PSK, Certificate, EAP (Extended Authentication Protocol)
Login (EAP)	The EAP authentication allows the authentication of the user with a login/password that must be configured in the gateway. The EAP login must be configured in the IKEv2 settings. The EAP password will be asked each time the tunnel is opened.
Pre-shared Key (PSK)	Set a pre-shared key if needed
Confirm	Confirm the pre-shared key

Note: Authentication with a certificate cannot be configured from the Android VPN Client interface. To use a certificate for authentication, you need to import a VPN Policy that embeds a certificate (Cf. chapter 7.2 "[Importing a VPN Policy](#)").

Once you have made your changes, press the "Save" button to save the updated VPN Policy on the Android device.

8.3 Configure an SSL VPN Tunnel

Press the ">" button to configure one of the SSL VPN tunnels in the list.

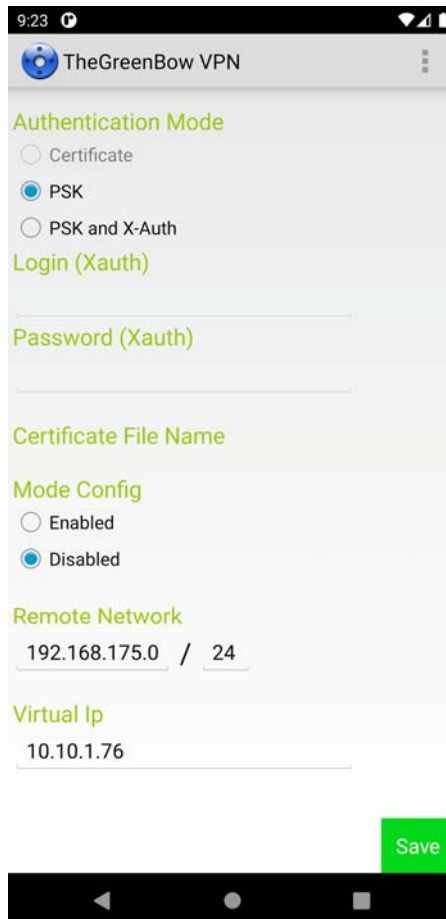


Tunnel Name	The name of the tunnel
Remote Gateway	IP address of the remote VPN gateway
Authentication	The "Extra Auth" authentication enables authentication of the user with a login/password that must be configured in the gateway. When "Extra Auth" is selected, the login must be configured.
Login	Login used for authentication when "Extra Auth" is selected. The login and password must be also configured in the gateway.

Once you have made your changes, press the "Save" button to save the updated VPN Policy on the Android device.

8.4 Configuring the network interface

Press the "About" button to set the network interface. The interface menu will list all the available network interfaces that can be used to open a tunnel, regardless of the protocol used (IKEv1, IKEv2 or SSL).



9 Opening a VPN Tunnel

9.1 Opening an IKEv1 VPN Tunnel

To open an IKEv1 tunnel, press on the OPEN button in the list of IKEv1 VPN tunnels.

A password will be required when an IKEv1 tunnel is first opened, depending on the configuration. If PSK is configured, enter the Pre-shared Key. If both PSK and X-Auth, only enter the X-Auth password.

9.2 Opening an IKEv2 VPN Tunnel

To open an IKEv2 tunnel, press on the OPEN button in the list of IKE v2 VPN tunnels.

A password will be required when an IKEv2 tunnel is first opened only when using EAP. In this case, enter the password associated to the configured login when prompted.

9.3 Opening an SSL VPN Tunnel

To open an IKEv2 tunnel, press on the OPEN button in the list of SSL VPN tunnels.

A password will be required when a tunnel is first opened only if Extra-Auth is configured. In this case, enter the Extra-Auth password when prompted.

10 Logs

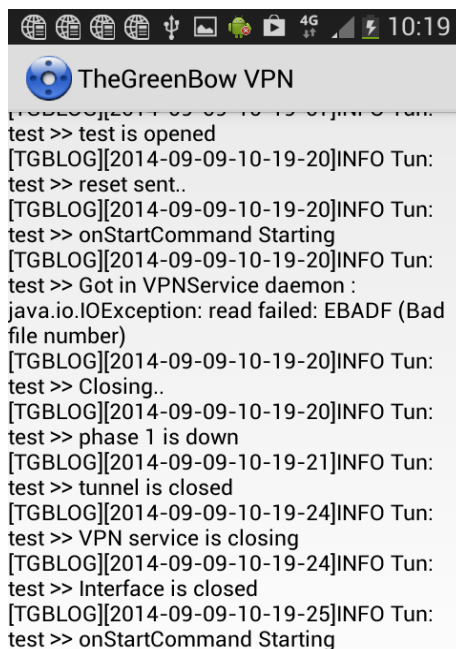
TheGreenBow Android VPN Client provides two types of logs: logs displayed in the user interface (Console) and log files.

10.1 Console

The Console gives detailed information on the opening and closing steps of VPN tunnels. They can be used by the administrator to identify possible connection incidents.

To display the Console, 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 opened VPN connection.

A screenshot of the TheGreenBow VPN application's console window. The window title is "TheGreenBow VPN". The log output shows a sequence of events: "test >> test is opened", "[TGBLOG][2014-09-09-10-19-20]INFO Tun:", "test >> reset sent..", "[TGBLOG][2014-09-09-10-19-20]INFO Tun:", "test >> onStartCommand Starting", "[TGBLOG][2014-09-09-10-19-20]INFO Tun:", "test >> Got in VPNService daemon :", "java.io.IOException: read failed: EBADF (Bad file number)", "[TGBLOG][2014-09-09-10-19-20]INFO Tun:", "test >> Closing..", "[TGBLOG][2014-09-09-10-19-20]INFO Tun:", "test >> phase 1 is down", "[TGBLOG][2014-09-09-10-19-21]INFO Tun:", "test >> tunnel is closed", "[TGBLOG][2014-09-09-10-19-24]INFO Tun:", "test >> VPN service is closing", "[TGBLOG][2014-09-09-10-19-24]INFO Tun:", "test >> Interface is closed", "[TGBLOG][2014-09-09-10-19-25]INFO Tun:", "test >> onStartCommand Starting". The screenshot also shows the Android status bar at the top with various icons and the time 10:19.

```
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> test is opened
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> reset sent..
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> onStartCommand Starting
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> Got in VPNService daemon :
java.io.IOException: read failed: EBADF (Bad
file number)
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> Closing..
[TGBLOG][2014-09-09-10-19-20]INFO Tun:
test >> phase 1 is down
[TGBLOG][2014-09-09-10-19-21]INFO Tun:
test >> tunnel is closed
[TGBLOG][2014-09-09-10-19-24]INFO Tun:
test >> VPN service is closing
[TGBLOG][2014-09-09-10-19-24]INFO Tun:
test >> Interface is closed
[TGBLOG][2014-09-09-10-19-25]INFO Tun:
test >> onStartCommand Starting
```

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

10.2 Log files

All log files are available in the "vpnExport" folder of the application's directory. For Android up to version 9, the directory is called "TheGreenBow/". For Android 10 and higher, the folder is called "Android/data/com.thegreenbow.TheGreenBowVPN/files/".

In this directory, you will find the following log files:

tgblogYYYY-MM-DD.txt	contains the IKEv1 logs which appear in the logs console
ikelogYYYY-MM-DD.txt	contains the detailed IKEv1 logs
ikev2ConsoleYYYY-MM-DD.txt	contains the IKEv2 logs which appear in the logs console
ikev2logYYYY-MM-DD.txt	contains the detailed IKEv2 and the detailed SSL logs

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

11 Contact

11.1 Information

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

11.2 Commercial

Phone contact: +33 1 43 12 39 30

Mail contact: sales@thegreenbow.com

11.3 Support

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

Support

<http://www.thegreenbow.com/support.html>

Online support

http://www.thegreenbow.com/support_flow.html

FAQ

http://www.thegreenbow.com/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

12 Technical features

General

OS version	Android 5.1 and higher
Languages	English

Tunnel

Connection mode	Peer-to-Gateway (see the list of certified gateways and their configuration guides)
Tunneling Protocol	SSL IPsec: IKEv1 (up to Android 9) or IKEv2
Tunnel mode	Main mode and Aggressive mode
Config mode / Configuration Payload	Automatically obtain network parameters from the VPN gateway

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: Protected access to the VPN security policies User: - X-Auth (SSL) - Pre-shared key - EAP (IKEv2) - Multiple Auth (IKEv2)
PKI	- Support of X509 certificates in the following formats: PKCS#12, PEM, PFX - Supported certificate criteria: validity date, cancellation, subject, key usage - Full validity check of both "Client" and "Gateway" certificates

Miscellaneous

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
Dead Peer Detection / Liveness	RFC3706. Detection of inactive IKE endpoints

Administration

VPN policy management	Import of encrypted VPN policies with integrity check
Log and traces	IKE/IPsec and SSL log console
License and activation	Software license activation over Internet

THEGREENBOW

Secure, Strong, Simple
TheGreenBow Security Software