

Android VPN Client 6.4

User's Guide

TheGreenBow is a registered trademark.

Microsoft and Windows 10 are either registered trademarks or brand names owned by Microsoft Corp. in the U.S.A. and/or in other countries.

Apple, the Apple logo, iPhone, iOS, Mac, and macOS are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

Android, Google Chrome, Google Play and the Google Play logo are trademarks or registered trademarks of Google LLC.

Any other third-party trademarks mentioned in this document are the property of their respective owners.

All reproduction rights are reserved, including for iconographic or photographic representations. No part of this document may be copied and/or published by any means whatsoever without our express written consent.

All the information provided is subject to modifications at any time and without notice.

Despite our utmost care and attention in producing this document and its regular updates, errors may have been introduced in the information provided. If you notice any issues, please feel free to contact us and let us know. We will make the necessary changes.

Table of contents

1	Overview	1
1.1	Introduction	1
1.2	Security	1
1.3	Ergonomic.....	1
1.4	Simple.....	2
1.5	Features	2
1.6	What's new in release 6	2
1.7	Cryptography and authentication.....	2
1.7.1	Cryptography	2
1.7.2	IKEv1 and vulnerable algorithms have been deprecated.....	3
1.7.3	SSL/OpenVPN	3
1.7.4	Certificate authentication and revocation.....	3
1.8	Current limitations.....	4
2	Installing the app.....	5
2.1	Installation procedure	5
2.2	Minimum requirements	6
2.3	Trial period	7
2.4	Update procedure.....	8
3	Activating the app.....	9
3.1	Introduction	9
3.2	Online activation.....	9
3.3	Offline manual activation	10
3.4	Advantages of using TAS	14
3.4.1	Format and content of the vpnsetup.json file	14
3.4.2	Activating within a tunnel connected to a TAS server	15
3.4.3	Activating on the local network where the TAS server is located.....	18
3.5	Renewing the license	20
3.5.1	Interactive mode.....	20
3.5.2	Always-on mode	20
3.6	Activation errors	21



4	Uninstalling the app.....	23
5	Testing the VPN Client.....	24
6	Getting started with the app	27
6.1	Introduction	27
6.2	Main screen.....	27
6.2.1	Overview.....	27
6.2.2	Managing connections	27
6.3	Main menu with three vertical dots	28
6.3.1	Configuration submenu	29
6.3.2	Activation submenu	29
6.3.3	Tools submenu	30
6.3.4	About submenu.....	30
6.4	Notifications.....	32
6.5	Status icons	33
7	Using certificates stored in the certificate store.....	35
7.1	Introduction	35
7.2	Importing a certificate into the mobile device's certificate store	35
7.3	Referencing a certificate in the Android VPN Client.....	37
8	Configuring VPN connections.....	40
8.1	Introduction	40
8.2	Importing a VPN configuration file	40
8.3	Changing the configuration of a VPN connection	40
8.4	Importing a certificate into the configuration of a VPN connection.....	42
8.5	Exporting the configuration of a VPN connection.....	44
8.6	Deleting a VPN connection	46
9	Opening a VPN connection.....	49
9.1	Introduction	49
9.2	Opening an IKEv2 VPN connection.....	49
9.3	Opening an SSL VPN connection	49
9.4	Enabling the Always-on VPN function	49
9.5	Disabling the Always-on VPN function.....	52

10	Logging	53
10.1	Displaying logs.....	53
10.2	Sharing logs.....	56
10.3	Clearing logs.....	58
11	Troubleshooting	60
11.1	Resetting the app.....	60
11.2	Deleting app data.....	60
12	Technical data	63
12.1	General.....	63
12.2	Connection/Tunnel	63
12.3	Cryptography and authentication.....	63
13	Contact	65
13.1	Information.....	65
13.2	Sales.....	65
13.3	Support	65



Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2023-07-26	All	Initial draft	FB, BB

1 Overview

1.1 Introduction

Thank you for downloading our Android VPN Client 6.4 software. Once it is installed on your mobile device, the app is named TheGreenBow VPN.

The Android VPN Client secures data exchanges to and from smartphones and tablets. While it is particularly suitable for managing industrial systems (maintenance, diagnostics, logistics, etc.), it also meets the requirements for protecting critical communications of public and private security services.

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

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

This guide is intended for users of the Android VPN Client.

It contains all the information required to implement and configure the software so that secure VPN tunnels can be opened.

1.2 Security

The Android VPN Client has been developed according to recommendations from NIST and ANSSI. The protocols in the current version meet the ANSSI's IPsec DR profile for restricted communications. The software is thus compatible with gateways available on the market that implement this profile (e.g. Stormshield SNS, Thales Mistral, and Atos Trustway).

The many protocols and algorithms implemented in the software make it a universal client allowing your users to connect to any OpenVPN or IPsec VPN firewall/gateway on the market, regardless of whether it is software or hardware-based.

1.3 Ergonomic

Installation on any terminal running Android 10 or higher is entirely transparent for users. The software supports a variety of protocols, settings, and options that enable interoperability with your gateway/firewall and your PKI.



1.4 Simple

The Android VPN Client makes it easy to use a VPN, owing to its user-friendly interface that helps your users establish secure connections to your information system. Users get a direct view of the status of their VPN connections to ensure that their communications are properly protected.

1.5 Features

- Interoperable with all IKEv2 and OpenVPN compatible firewalls/gateways
- Cryptography: AES CBC/CTR/GCM (128/192/256 bits)
- Hashing: SHA-2 (256/384/512 bits)
- DH groups: 14-21, 28
- X.509 certificate management: PFX, PKCS #12¹
- Authentication: preshared key, certificates, EAP, two-factor authentication (certificate + EAP)

1.6 What's new in release 6

- Use certificates stored in the mobile device's certificate store, including elliptic curve certificates
- Keep VPN always on, even when the application is not running
- Biometric authentication
- Activate licenses using TAS (manually or within a tunnel)
- Check gateway CAs
- End of support for the IKEv1 protocol
- Improved logs
- Receive notifications about application events
- Enhanced graphics

1.7 Cryptography and authentication

1.7.1 Cryptography

- Support for Diffie-Hellman key group DH 28 (BrainpoolP256r1) [RFC 5639]

¹ Configuration to be performed using the Windows Enterprise VPN Client.

1.7.2 IKEv1 and vulnerable algorithms have been deprecated

The security of our software has been enhanced with the end of support for the following:

- Vulnerable IPsec/IKEv1 protocol, which has been deprecated by the IETF in September 2019
- Vulnerable algorithms DES, 3DES, SHA-1, DH 1, DH 2, DH 5 in IPsec/IKEv2 (even in “auto” mode)

1.7.3 SSL/OpenVPN

- OpenSSL has been updated to version 1.1.1s for enhanced security
- End of support for vulnerable algorithms in SSL/OpenVPN: MD5, SHA-1, BF-CBC, TLS 1.1, LOW security suite for TLS V1.2
- Compression is no longer enabled by default

1.7.4 Certificate authentication and revocation

Due to increased security requirements, deprecation of certain algorithms, and stricter rules for using certificates, version 6 of the Android VPN Client comes with certain restrictions on certificates.

- Support for the following certificate authentication methods:
 - Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
 - Method 9: ECDSA on the secp256r1 curve with SHA-2 (256 bits) [RFC 4754]
 - Method 10: ECDSA on the secp384r1 curve with SHA-2 (384 bits) [RFC 4754]
 - Method 11: ECDSA on the secp521r1 curve with SHA-2 (512 bits) [RFC 4754]
 - Method 14: Digital Signature Authentication RSASSA-PSS with SHA-2 (256/384/512 bits) [RFC 7427]
 - Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) (only available for gateways that support this method)
- Certificate authentication method 14, which is based on the RSASSA-PSS signature algorithm, is used by default for all RSA certificates
- UDP encapsulation mode is forced for the IKEv2 protocol
- End of support for Method 1: RSA Digital Signature with SHA-1 [RFC 7296]
- RSA certificates with less than 2048-bit key length are rejected
- ECDSA certificates with less than 256-bit key length are rejected
- Key Usage and Extended Key Usage of certificates is verified



1.8 Current limitations

- The software does not currently support certificates with validity dates set too far in the future (only on ARMv7 phones).
- The Android VPN Client's license cannot be renewed when the application is in Always-on mode. To update the license, you must return to the interactive VPN mode, renew the subscription, and then enable Always-on again.

2 Installing the app

2.1 Installation procedure

To install the Android VPN Client, proceed as follows:

1. Download the Android package `TheGreenBow_VPN_Android.apk` from our online store at store.thegreenbow.com.
2. If you downloaded the Android package from a workstation, transfer it to the target device.
3. Run the APK from the file explorer on the device and follow the on-screen instructions.



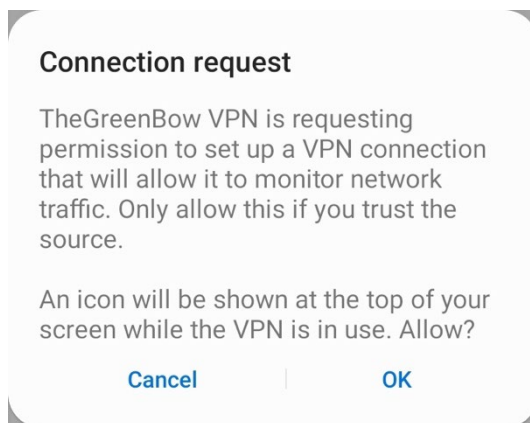
If you have never installed an APK from a file on your mobile device, a message is displayed requesting you to allow installation of unknown apps from this source. Tap **Settings**, and then then toggle the **Allow from this source** option to authorize installation of apps from the file explorer.

4. The first time you run the app, a certain number of dialog boxes will be shown prompting you to authorize the use of a feature in the app or in the mobile device's operating system.

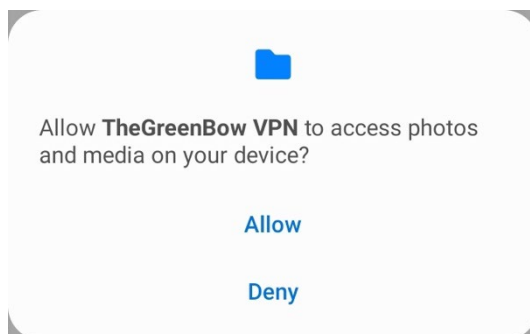


The order in which these authorization prompts are displayed may vary according to your interaction with the device.

5. The first message shown asks you to unlock the app. Enter the same PIN code you use to unlock the mobile device or use facial recognition or your fingerprint, if this feature is available and enabled on your device.
6. Tap **Continue**.
7. If this is the first time that you are installing a VPN application, a dialog box will be shown asking for your permission to configure a VPN connection.



8. Tap **OK**.
9. When the system prompts you to access photos and media on your device, we recommend that you authorize this so that you will be able to import and export configuration files, log files, and manual activation files.



The TheGreenBow VPN app is installed, and you can start using it.



To add a test VPN connection, refer to chapter 5 Testing the VPN Client.



To learn how to use the application, refer to chapter 6 Getting started with the app.



For more information on activating the app, refer to chapter 3 Activating the app.

2.2 Minimum requirements

Minimum Android version: 10

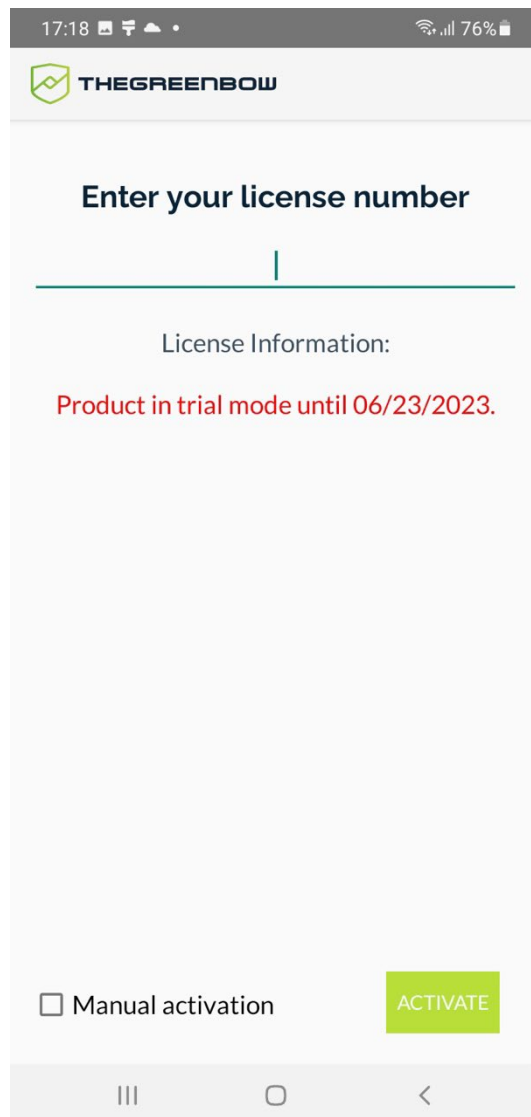
Available internal storage space: 40 MB

2.3 Trial period

Once it is installed, the application can be used for free for a 30-day trial period. During this trial period, the Android VPN Client is fully operational, and all functions are unlocked.

To display the activation screen, tap the menu at the top right of the main screen (three vertical dots), select **Activation**, and then **Enter license number**.

This screen shows the number of days remaining in the trial period.



For more information on activating the app, refer to chapter 3 Activating the app.

2.4 Update procedure

To update the Android VPN Client on your mobile device, simply install the new version of the app over the current one, by following the steps described in section 2.1 Installation procedure.



If you are performing an update from version 5.11 or earlier, you must uninstall the software before installing the new version.

Any existing VPN configuration and activation files will be kept and automatically reused.

This allows you to continue using the Android VPN Client as before, while benefiting from the new features and fixes.



Due to a signature change, which prevents the conversion of old configuration files to the new `.tgb` file format, configuration files from versions 5.11 and earlier are not compatible with version 6.0 or higher. You must re-export the configuration from a Windows VPN Client version 6.87 or higher.

3 Activating the app

3.1 Introduction

The Android VPN Client can be activated in several different ways:

- Online, directly from the app (see section 3.2 Online activation)
- Offline, from another workstation connected to the internet (see section 3.3 Offline manual activation)
- Using TheGreenBow activation server (TAS)
 - Within a tunnel connected to a TAS server (see section 3.4.2 Activating within a tunnel connected to a TAS server)
 - On the local network where the TAS server is located (see section 3.4.3 Activating on the local network where the TAS server is located)

The corresponding procedures are described in the subsections below.



For more information on TAS, refer to the following page on our website:

<https://www.thegreenbow.com/en/products/secure-connection-management/>.

3.2 Online activation

To purchase a license for the Android VPN Client and activate it directly from the mobile device, proceed as follows:

1. From the **Activation** menu, select **Enter license number**.
2. On the screen that appears, tap **Buy**.

TheGreenBow online store opens in a browser window.

3. Select the **Android VPN Client**, then the **Delivery Method**, the length of **Engagement** and the **Number of licenses**.
4. Add the product to the cart, then complete your purchase.

You will receive the license in an activation e-mail.

5. Return to TheGreenBow VPN app and enter the license number in the corresponding field, then tap **Activate**.



You can also access the online store from a workstation and then enter the license number delivered in the activation e-mail.



To find out what the activation error codes mean, refer to section 3.6 Activation errors.



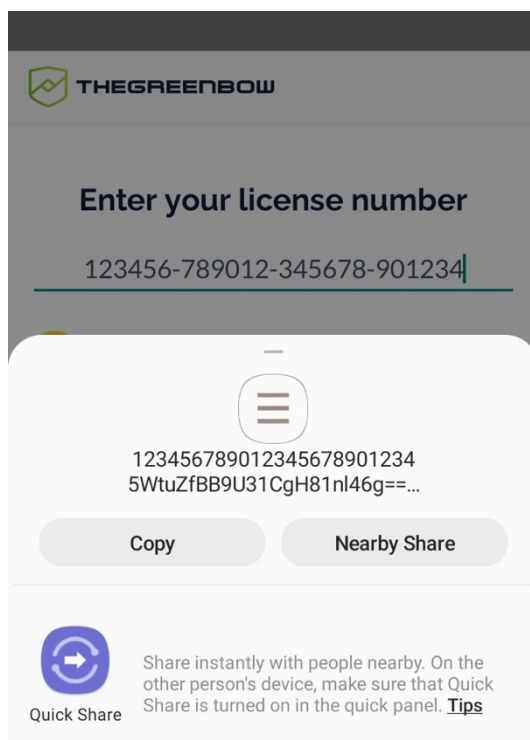
To find out how to renew a license that has been activated online, refer to section 3.5 Renewing the license.

3.3 Offline manual activation

In some cases, access to the internet may be restricted on a mobile device for security reasons. You then need to activate the license offline from another workstation that is connected to the internet.

To manually activate the license from another workstation that is connected to the internet, follow the steps below:

1. Open the menu at the top right of the main screen (three vertical dots), select **Activation**, and then **Enter license number**.
2. Enter the license number that you received in the activation e-mail in the corresponding field.
3. Check the **Manual Activation** box.
4. Tap **Activate**. The share sheet is displayed:

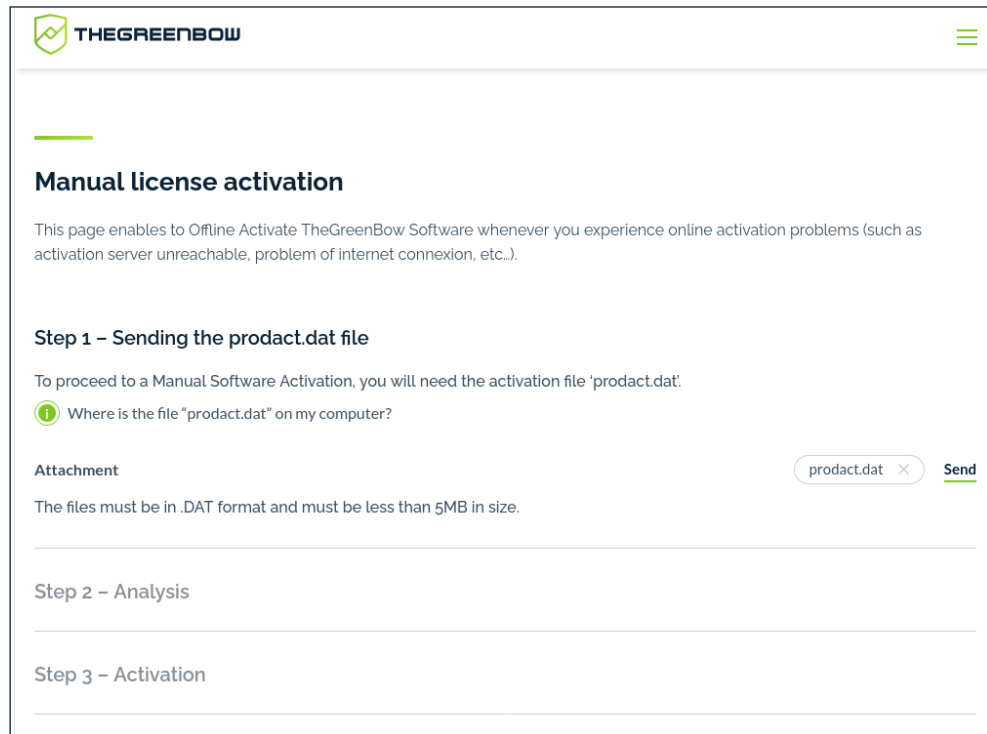


The technical information corresponding to the contents of the `product.dat` activation file is copied to the clipboard. You can send it via e-mail or save it to a text file named `product.dat` directly on the mobile device.

5. Transfer the `product.dat` file to a workstation that is connected to the internet or create it on the workstation using the data shared from

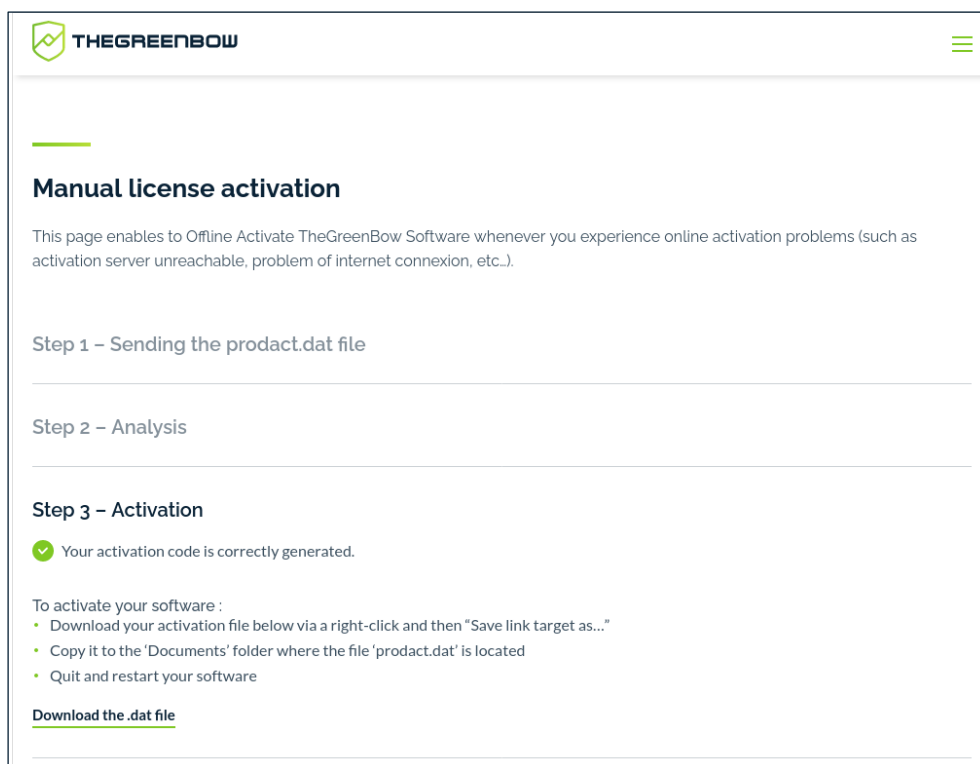
the mobile device. The `product.dat` file must be a text file in UTF-8 format.

6. Open a browser and access TheGreenBow activation server available at <https://www.thegreenbow.com/en/support/license-management/manual-license-activation/>.



The screenshot shows the 'Manual license activation' page of TheGreenBow. The page has a header with the TheGreenBow logo and a hamburger menu icon. Below the header, there is a section titled 'Manual license activation' with a sub-header 'Step 1 – Sending the product.dat file'. The text explains that this page enables offline activation. A message states: 'To proceed to a Manual Software Activation, you will need the activation file 'product.dat'.' Below this, there is a green information icon and the text 'Where is the file "product.dat" on my computer?'. There is an 'Attachment' section with a file input field containing 'product.dat' and a 'Send' button. A note states: 'The files must be in .DAT format and must be less than 5MB in size.' Below this, there are sections for 'Step 2 – Analysis' and 'Step 3 – Activation', each with a horizontal line for content.

7. Click **Add a file** and select the `product.dat` file created for the terminal that you want to activate.
8. Click **Send**. The activation server will check the validity of the information contained in the `product.dat` file.
9. Click **Submit**. The activation server will provide a link to download a file containing the activation code for the mobile device to be activated.



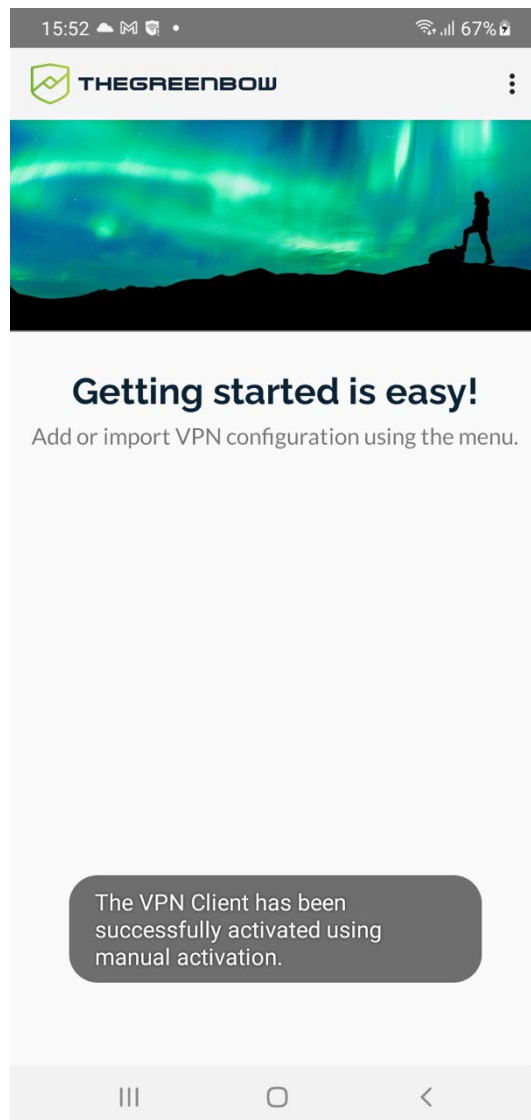
The file name has the following format:

tgbbcode_[date]_[code].dat (e.g.
tgbbcode__20230415_1029.dat).

10. Transfer the tgbbcode_[date]_[code].dat file to the mobile device you want to activate.
11. In the TheGreenBow VPN app on the mobile device, open the menu at the top right of the main screen (three vertical dots), select **Activation**, and then **Import activation code**.

The file manager opens, allowing you to select the file to import.

12. An information message is displayed to confirm that the file has been imported correctly and that the manual activation was successful:



When activation is successful, the license number and validity period of the license are displayed on the activation screen.



The message displayed on screen after importing a file does not specify whether the import was successful. When you import any file or if you cancel the import, the same message confirming that manual activation has been performed is still displayed.



To find out what the activation error codes mean, refer to section 3.6 Activation errors.



To find out how to renew a license that has been activated manually, refer to section 3.5 Renewing the license.

3.4 Advantages of using TAS

If you use a TAS server to manage your licenses, you can import an activation file containing the license number and the address of the TAS with which the Android VPN Client must communicate to perform the activation.

You can also activate the license on the local network if your TAS is located on this network or open a tunnel and connect to the TAS within a tunnel to activate the license.



To perform an activation using the TAS server, you must first create a `vpnsetup.json` activation file, refer to section 3.4.1 Format and content of the `vpnsetup.json` file to find out how.



To perform an activation within a tunnel connected to a TAS server, refer to section 3.4.2 Activating within a tunnel connected to a TAS server.



To perform an activation on the local network on which the TAS server is located, refer to section 3.4.3 Activating on the local network where the TAS server is located.



For more information on how to use TheGreenBow Activation Server (TAS), refer to the corresponding documentation on our website:
<https://www.thegreenbow.com/en/support/product-documentation/>.

3.4.1 Format and content of the `vpnsetup.json` file

When you perform the activation using a TAS server, regardless of whether you do so within a tunnel or on the local network, the data used to activate the Android VPN Client must be entered into a text file named `vpnsetup.json` in ASCII format.



You can choose any name for the file, but the `.json` extension is required.

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

```
{
  "license" : "123456789012345678901234",
  "email" : "username@company.com"
  "osaur1" : "192.168.217.102/osace_activation.php"
  "osaport" : "80"
  "osacert" : "MIICGjCCAYOgAwIBAgIBADANBg [.....]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
}
```

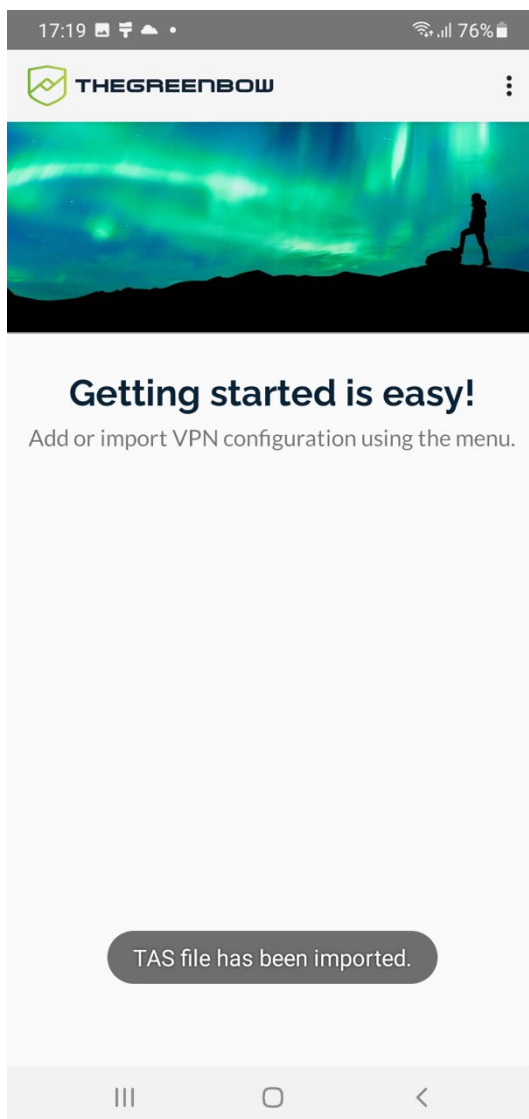


If the URL in the `osaur1` parameter contains `https`, the protocol used will be the secure protocol `https`. Otherwise, the protocol used will be `http`.

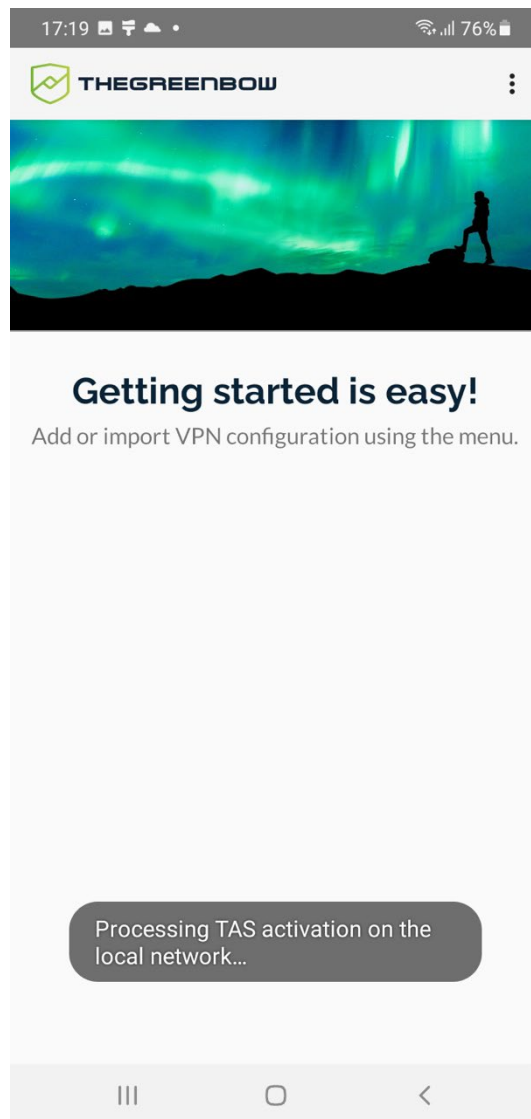
3.4.2 Activating within a tunnel connected to a TAS server

To perform an activation within a tunnel connected to a TAS server, follow the steps below:

1. Create the `vpnsetup.json` activation file (see section 3.4.1 Format and content of the `vpnsetup.json` file above).
2. Transfer the `vpnsetup.json` TAS activation file to the mobile device.
3. Open the menu at the top right of the main screen (three vertical dots), select **Activation**, and then **Import TAS configuration file**. The file manager opens, allowing you to select the file to import.
4. Select the file to import. The TAS file is imported. A message is displayed to confirm that import was successful.



5. A message is displayed indicating that the Android VPN Client tried to connect to the TAS server on the local network, but could not find it.



6. Import a configuration containing a connection to a network on which the TAS server is located (see chapter 8 Configuring VPN connections to find out how to create it).
7. Open the tunnel of the connection you just created. If the tunnel remains open and no error message is displayed, activation was successful. You can open the **About** window to conform it (see section 6.3.4 About submenu to find out how to display it).

The Android VPN Client has been activated.



To prevent any undesired changes to the license number from being made, when the license has been imported from a TAS file, the **Activation > Enter license number** menu option is grayed.



To find out what the activation error codes mean, refer to section 3.6 Activation errors.

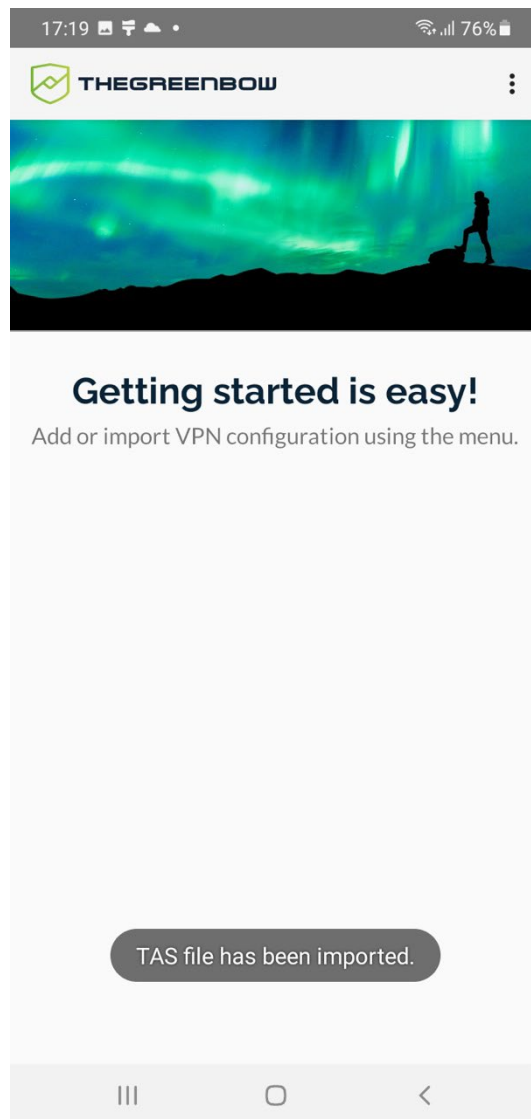


To find out how to renew a license that is managed by a TAS server, refer to section 3.5 Renewing the license.

3.4.3 **Activating on the local network where the TAS server is located**

To perform an activation on the local network where the TAS server is located, proceed as follows:

1. Create the `vpnsetup.json` activation file (see section 3.4.1 Format and content of the `vpnsetup.json` file above).
2. Transfer the `vpnsetup.json` file you created to the mobile device you want to activate.
3. Make sure the mobile device is connected to the local network on which the TAS server is located.
4. Open the menu at the top right of the main screen (three vertical dots), select **Activation**, and then **Import TAS configuration file**. The file manager opens, allowing you to select the file to import.
5. Select the file to import. The TAS file is imported. A message is displayed to confirm that import was successful.



6. The Android VPN Client connects to TAS on the local network. If no error message is displayed, activation was successful. You can open the **About** window to confirm it (see section 6.3.4 About submenu to find out how to display it).

The Android VPN Client has been activated.



To prevent any undesired changes to the license number from being made, when the license has been imported from a TAS file, the **Activation > Enter license number** menu option is grayed.



If the Android VPN Client does not find the TAS server on the local network, a corresponding message is displayed. In this case, you must specify the TAS server's address in the `vpnsetup.json` activation file and proceed with an activation within the tunnel (see section 3.4.2 Activating within a tunnel connected to a TAS server).



To find out what the activation error codes mean, refer to section 3.6 Activation errors.



To find out how to renew a license that is managed by a TAS server, refer to section 3.5 Renewing the license.

3.5 Renewing the license

When the license is about to expire, a message is displayed in the Android VPN Client seven days before the expiration date to remind you that it's time to renew it.

The behavior of the Android VPN Client will differ depending on whether you use it in interactive or always-on mode.

3.5.1 Interactive mode

When you use the Android VPN Client in interactive mode, i.e. you manually open and close the tunnel(s) configured in the connections list, the app will behave as described below starting from seven days before the license expires.

When you open a tunnel, an activation query is run within the tunnel and the following will take place depending on the situation:

- If there are less than 6 days left before the license expires and you have not renewed, activation fails, but the tunnel remains open
- If there are less than 6 days left before the license expires and you have renewed it, the VPN Client's activation is updated with the new date
- If the license has expired, the tunnel is closed and a message is displayed indicating that the license has expired

3.5.2 Always-on mode

When you use the Android VPN Client in always-on mode, i.e. the configured tunnel is always on (see section 9.4 Enabling the Always-on VPN function), the app will behave as described below starting from 7 days before the license expires.

An activation query is run within the tunnel and the following will take place depending on the situation:

- If there are less than 6 days left before the license expires and you have not renewed, the tunnel remains open and a message indicating the number of days left before the license expires is displayed

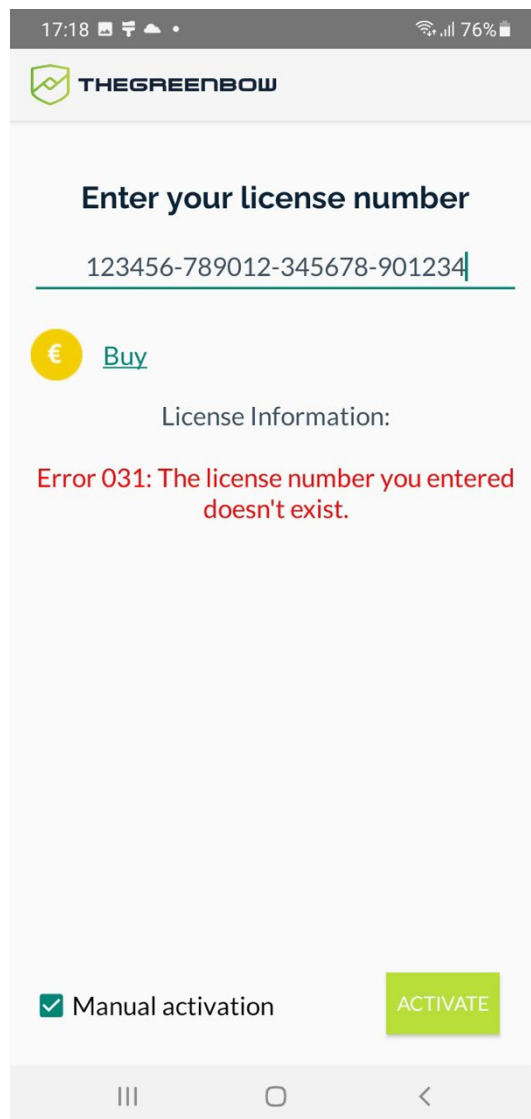
- If the license has expired, the tunnel is closed, a message is displayed indicating that the license has expired, and the key-shaped icon in the status bar moves back to the left side



You must disable the always-on mode and return to interactive mode to renew the license (see section 9.4 Enabling the Always-on VPN function).

3.6 Activation errors

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



TheGreenBow lists all activation errors and [procedures for solving activation issues](#) on its website.

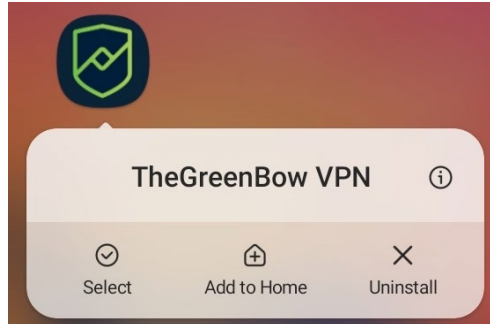
The following are the most common activation errors:

No.	Meaning	Troubleshooting
31	Wrong license number	Check license number.
33	The license number is already activated on another device	Uninstall the app on the mobile device with the activated license or contact TheGreenBow's Sales department.
53, 54	Communication with the activation server is impossible	Ensure that the mobile device is connected to the internet. Check that communication is not blocked by a firewall or proxy.

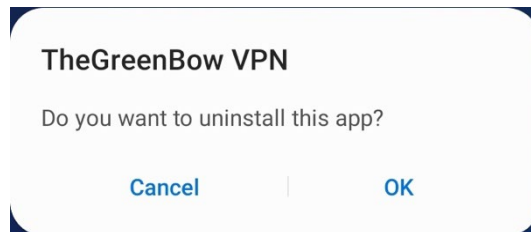
4 Uninstalling the app

The procedure to uninstall the application is described below:

1. Tap and hold the **TheGreenBow VPN** app icon.



2. Select **Uninstall** in the contextual menu.



3. Tap **OK** to confirm.

5 Testing the VPN Client

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

To create a test VPN connection, proceed as follows:

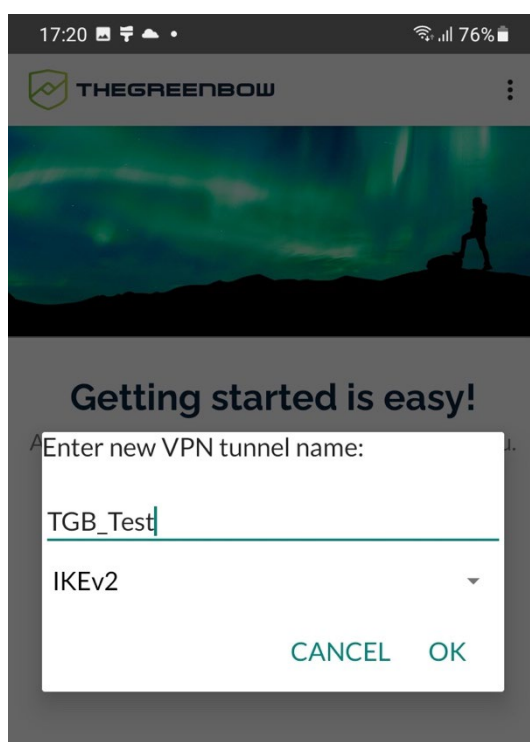
1. Open the menu at the top right of the main screen (three vertical dots), select **Configuration**, and then **Add a test configuration**.

Configuration

Add a test configuration

Import a configuration file

A dialog is displayed:



2. Enter a name for the new tunnel, e.g. TGB_Test. The only protocol available is IKEv2.



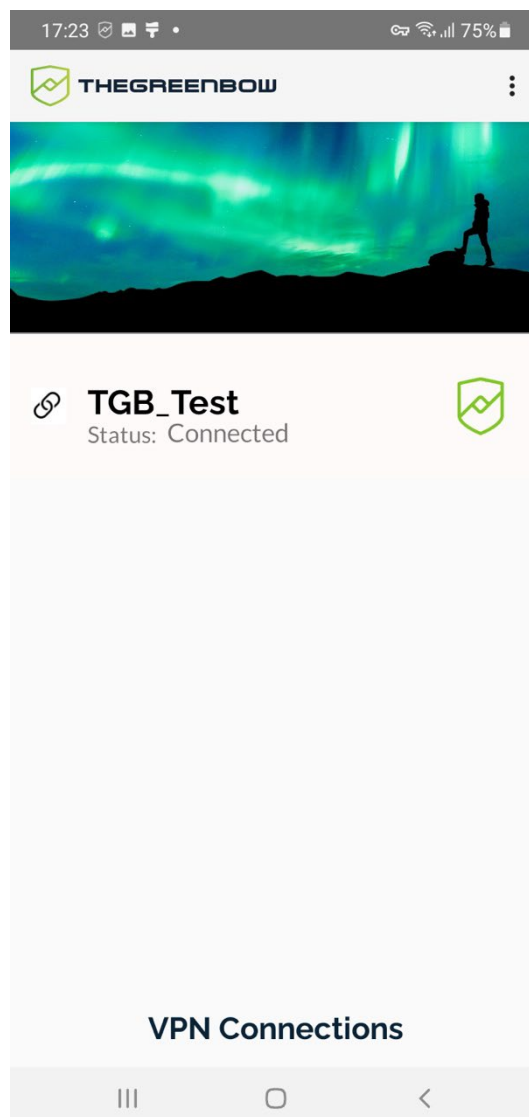
Connection names may not contain any blank spaces. You can insert an underscore to separate two words.

3. Tap **OK**. The new test VPN connection is added to the main screen. The settings to connect to TheGreenBow's test VPN network are filled in automatically.
4. Tap the name of the test connection you just created. The Android VPN Client will initiate the connection.



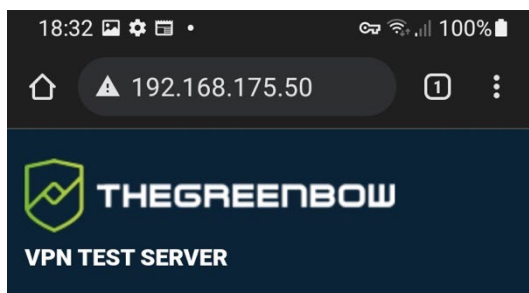
The first time you open a tunnel, a message is displayed requesting your permission to set up a VPN connection. Tap **OK** to allow this.

When the connection is successful, the TheGreenBow logo next to the connection name turns green and the connection status indicates that the tunnel is **Connected**.



Once the tunnel is open, you should be able to open the following web page in your browser: <http://192.168.175.50/>.

If you successfully opened the test tunnel, you should see the following page in your web browser:



Congratulations! You've successfully opened a VPN tunnel.

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



If opening the test tunnel does not work, open a browser on the mobile terminal to check your internet connection.

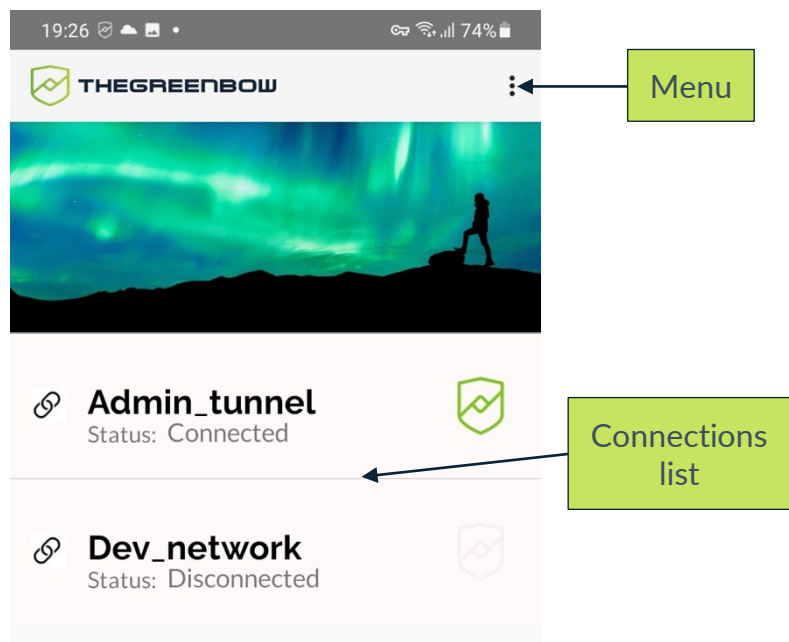
6 Getting started with the app

6.1 Introduction

The interface of the Android VPN Client is simple and intuitive. It consists of a main screen with the list of VPN connections and a menu.

6.2 Main screen

6.2.1 Overview



The first time you start the app, the connections list is empty.



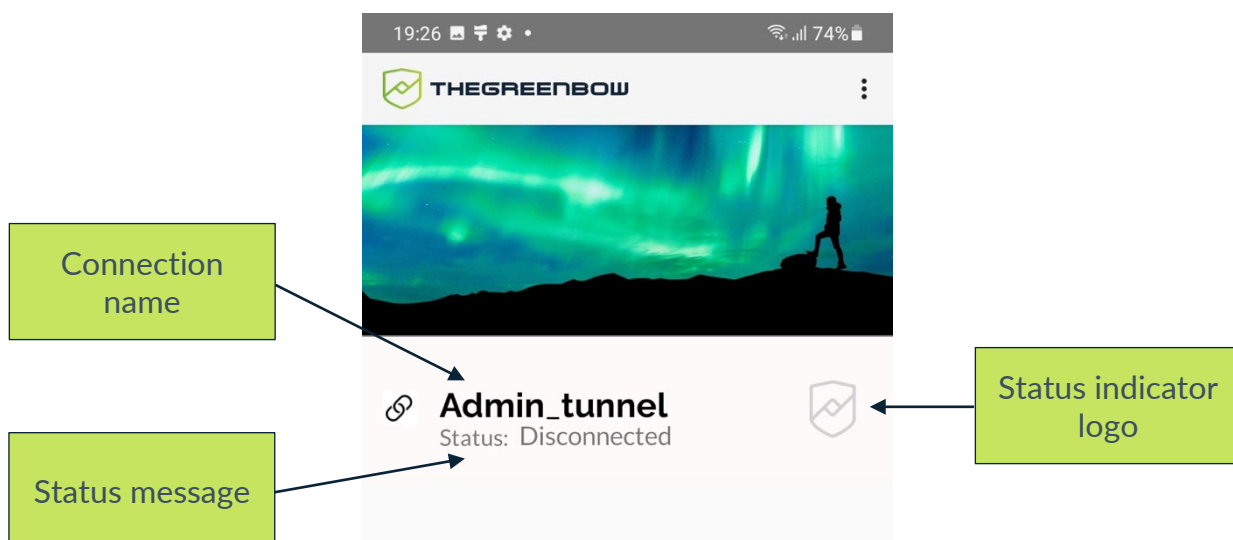
To add a test VPN connection, refer to chapter 5 Testing the VPN Client.



To import a configuration file, refer to section 8.2 Importing a VPN configuration file.

6.2.2 Managing connections

As soon as you add a VPN connection, it is displayed in the connections list.



Each connection includes the following items in the corresponding banner:

- A name
- A status message
- A TheGreenBow logo indicating the connection status

Tapping the connection name initiates the establishment of a connection.

A long press on the connection name opens the connection configuration window.



To find out more about how to configure a VPN connection, refer to chapter 8 Configuring VPN connections.

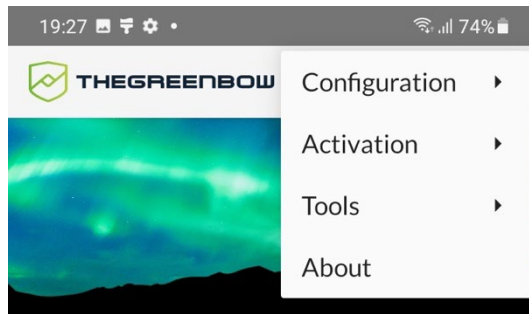


To learn how to open a VPN connection, refer to chapter 9 Opening a VPN connection.

6.3 Main menu with three vertical dots

The menu with three vertical dots at the top right of the screen includes the following entries:

- Configuration
- Activation
- Tools
- About

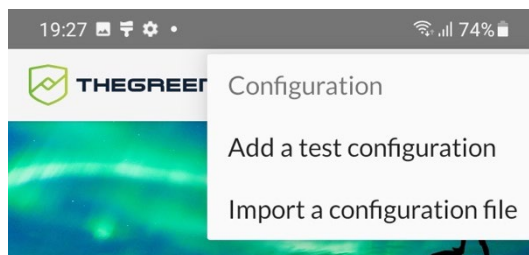


For more information about each of these submenus, refer to the corresponding sections below.

6.3.1 Configuration submenu

The **Configuration** submenu includes the following entries:

- Add a test configuration
- Import a configuration file



To add a test VPN connection, refer to chapter 5 Testing the VPN Client.

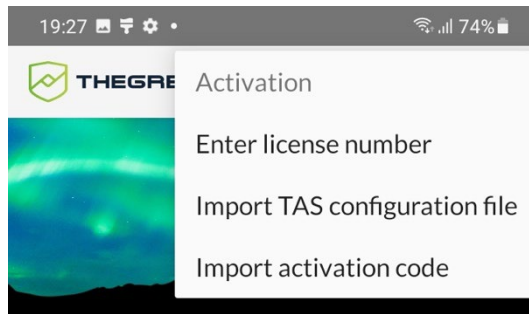


To import a configuration file, refer to section 8.2 Importing a VPN configuration file.

6.3.2 Activation submenu

The **Activation** submenu includes the following entries:

- Enter license number
- Import TAS configuration file
- Import activation code

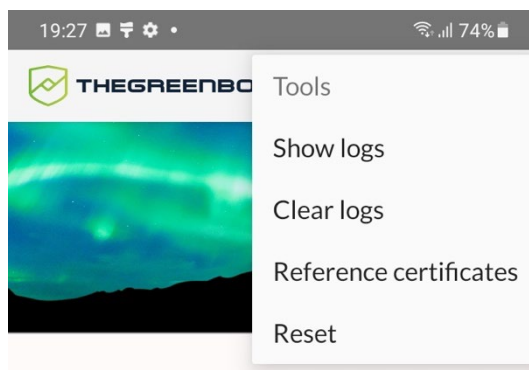


For more information on activating the app, refer to chapter 3 Activating the app.

6.3.3 Tools submenu

The **Tools** submenu includes the following entries:

- Show logs
- Share logs
- Clear logs
- Reference certificates
- Reset



For more information about logs, refer to chapter 10 Logging.



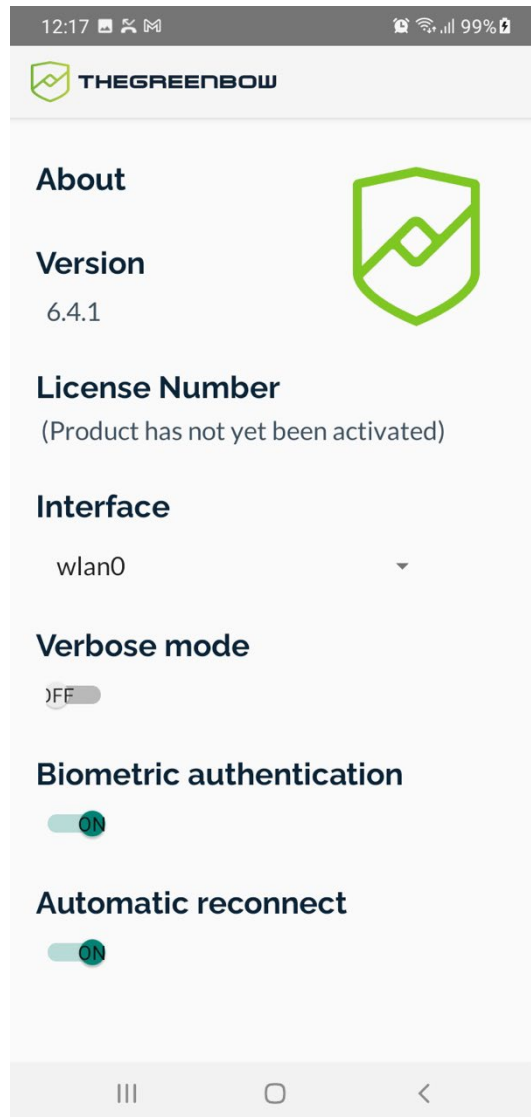
For more information about how to reference certificates, refer to chapter 7 Using certificates stored in the certificate store.



For more information about resetting the app and resolving problems, refer to chapter 11 Troubleshooting.

6.3.4 About submenu

The **About** submenu directly displays the **About** window.



It contains information about the version of the app and the license number when it has been entered.

It also includes an **Interface** drop-down list, allowing you to select the network interface to be used, and the following three toggle buttons:

- **Verbose mode**, used to enable or disable the verbose logging mode



As of version 6.2 of the Android VPN Client, the verbose mode is slightly less extensive than in previous versions.

- **Biometric authentication**, used to enable or disable biometric authentication when the VPN Client is started and after a certain period of inactivity
- **Automatic reconnect**, used to automatically reestablish the connection after a disconnection or interruption following a network interface change (e.g. when switching from Wi-Fi to 5G)



Automatic reconnect stops after three unsuccessful attempts.

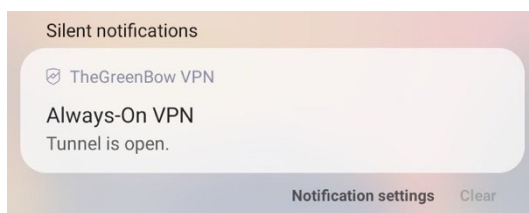


For more information about the verbose logging mode and logs, refer to chapter 10 Logging.

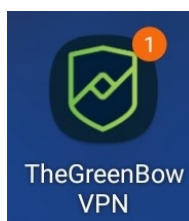
6.4 Notifications

As of version 6.3 of the Android VPN Client, the app sends silent notifications about the VPN's states and errors to the notification drawer. These may concern the following:

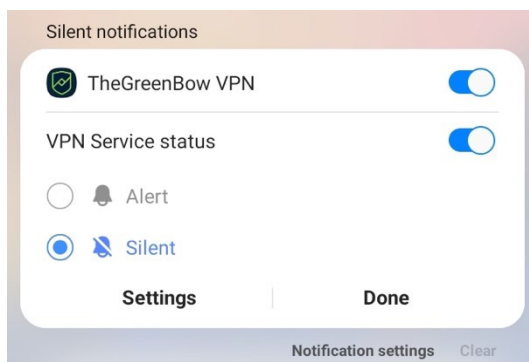
- Tunnel state, i.e. whether it is open or closed
- License expiration
- Network issues
- Errors that were displayed on the Always-on VPN screen in the previous version of the app



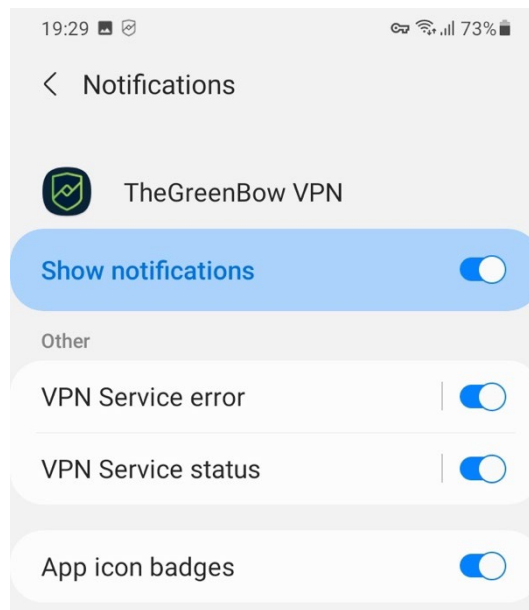
A notification badge is also displayed on the app icon when new notifications have been received.




You can change the notification settings in the app settings. To do this, tap and hold a notification, and then make the desired changes.

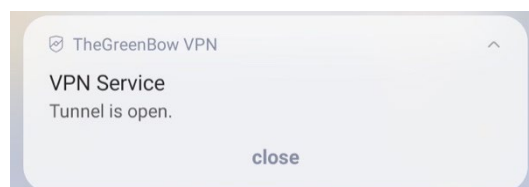


Tap **Settings** to access the app's notification settings in the system settings.



Depending on the type of notification, you can perform different actions from the notification. For example, when a tunnel is open and the app is closed, simply tap the notification to open the app.

To expand a notification, tap the down arrow . You will then be able to perform an action directly from the notification.






For example, if you have opened a tunnel in interactive mode, you can tap **close** to close it.

Notifications provide many other facilities that we cannot describe exhaustively here. They are usually intuitive enough to be self-explanatory.



6.5 Status icons

As of version 6.3 of the Android VPN Client, the VPN's state is shown by a TheGreenBow icon in addition to the key-shaped VPN icon provided by the operating system.

This icon appears in the left part of the status bar. It can appear as follows:

Icon	Meaning
	A tunnel is opening.
	The tunnel is mounted.
	The VPN encountered an issue.

The key icon appears in the right part of the mobile device's status bar. It indicates the tunnel and traffic status as follows:

Icon	Meaning
	Hollow icon on the right: a tunnel is mounted and encrypted traffic is passing through.
	Full icon on the left: there is a tunnel failure and no encrypted traffic is passing through.

7 Using certificates stored in the certificate store

7.1 Introduction

As of version 6.2 of the Android VPN Client, you can manage certificates in several different ways. You can store them in either of the following ways:

- In the configuration of a VPN connection
- In the mobile device's certificate store

You can also import a certificate into an existing configuration from a certificate file stored in the mobile device (see section 8.4 Importing a certificate into the configuration of a VPN connection).



If the certificate is included in the connection's configuration, you cannot use the configuration with any of the certificates stored in the mobile device's certificate store.

Using certificates stored in the mobile device's certificate store is more secure than loading a certificate from a file.



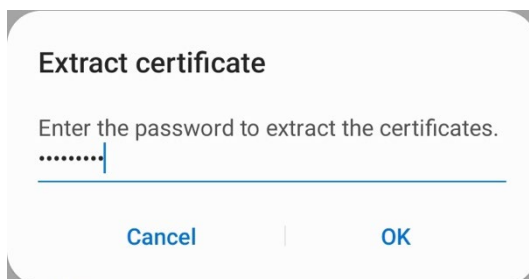
We recommend that you delete the certificate file once you have imported the certificate.

To use a certificate stored in the certificate store on the mobile device, you must first import the certificate into the mobile device's certificate store prior to referencing it in the Android VPN Client's certificate list. You will then be able to import a configuration that uses this certificate. It will then be automatically associated with this configuration. These steps are explained in detail in the sections below.

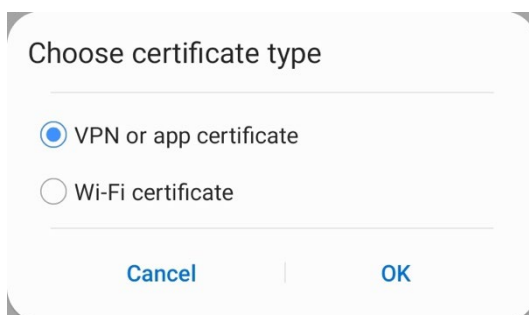
7.2 Importing a certificate into the mobile device's certificate store

To import a certificate into the certificate store on the mobile device, proceed as follows:

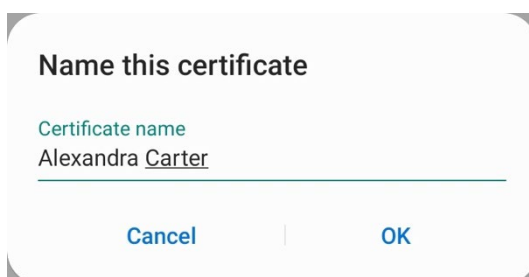
1. Transfer the certificate in P12 or PFX format to the mobile device.
2. In the file manager on the mobile device, navigate to the location to which you transferred the certificate.
3. Tap the certificate file. A dialog box is displayed asking you to enter a password to extract the certificate.



4. Enter the password associated with the certificate and tap **OK**. Another dialog box is displayed asking you to choose the certificate type.

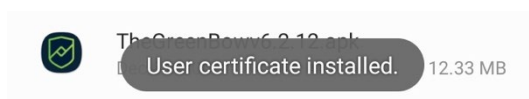


5. Select the type **VPN or app certificate**, then tap **OK**. Yet another dialog box is displayed asking you to assign a name to the certificate. You can keep the default name contained in the certificate or assign another name.



You can import a given certificate as many times as you wish and assign a different name to it each time.

6. A message is briefly displayed to confirm that the certificate has been imported successfully.



You can view the user certificates imported in the certificate store on the mobile device. To do this, open the mobile device's **Settings**. Then, depending

on the Android version and manufacturer's custom interface, select the following options to access the list of user certificates: **Biometrics and security** > **Other security settings** > **User certificates**.

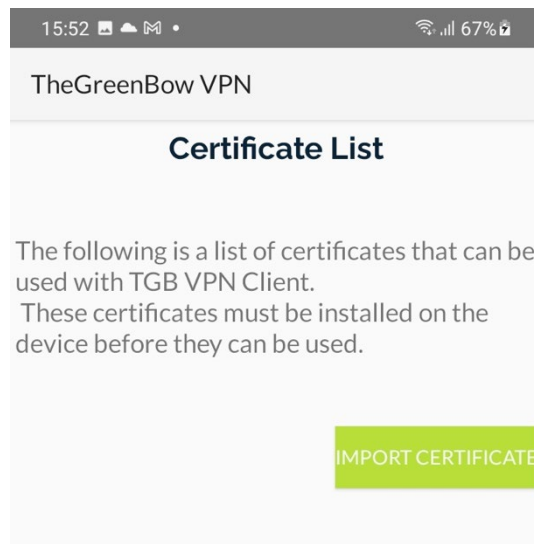


You can also search for “certificate” in the mobile device's settings to display all the certificate-related settings.

7.3 Referencing a certificate in the Android VPN Client

Once you have imported one or several certificates into the mobile device's certificate store, you can reference them in the Android VPN Client's certificate list. To do this, proceed as follows:

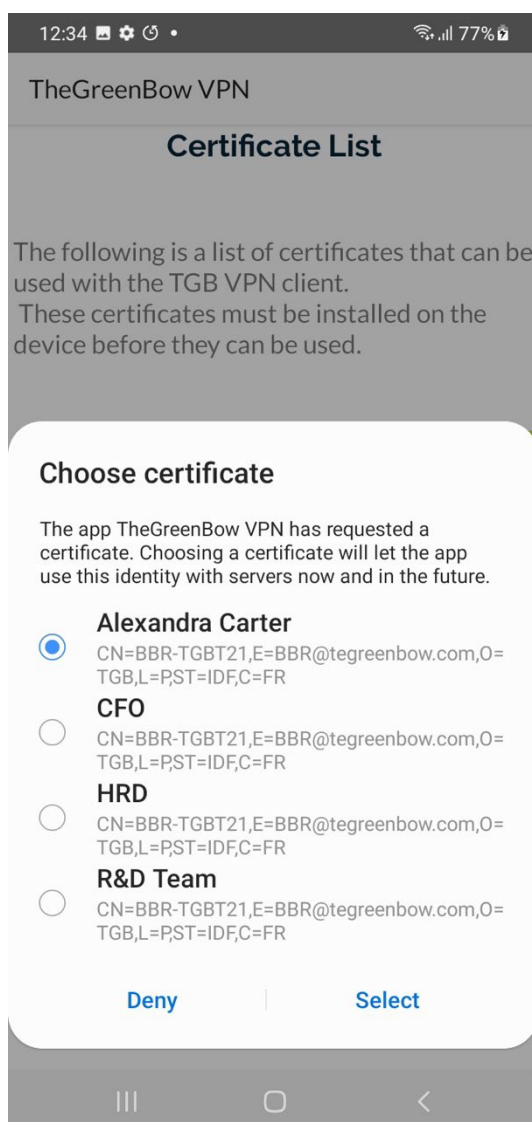
1. Open the menu at the top right of the main screen (three vertical dots), select **Tools**, then **Reference certificates**.



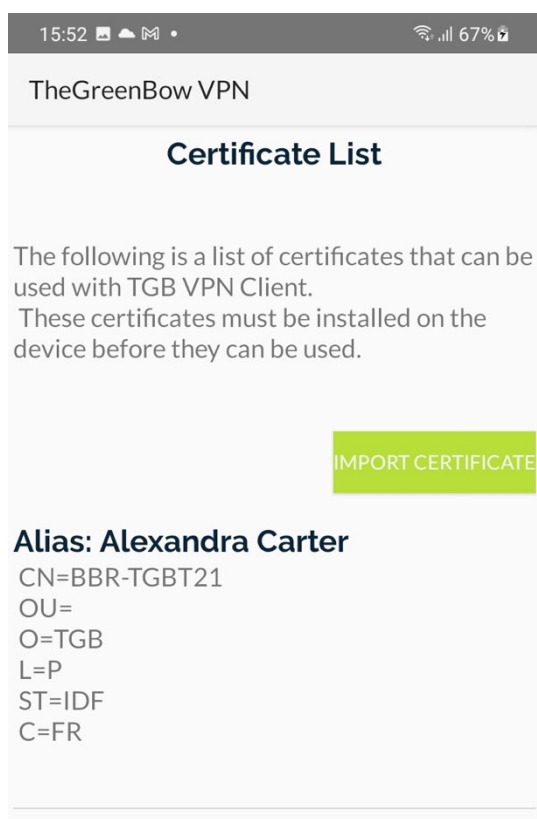
2. Tap **IMPORT CERTIFICATE**. A dialog box is displayed prompting you to choose a certificate from the list of certificates stored in the certificate store on the mobile device.



In this context, import simply means that the certificate is referenced in the VPN Client from the Android certificate store. The certificate must first have been imported into the store (see section 7.2 Importing a certificate into the mobile device's certificate store).



3. Choose the desired certificate, then tap **Select**. The certificate is added to the Android VPN Client's certificate list. You can now import a configuration that uses this certificate.





8 Configuring VPN connections

8.1 Introduction

To connect to your own remote network, you must create a VPN configuration using TheGreenBow's Windows VPN Client on a desktop or laptop computer and import it to the Android VPN Client.



To learn how to create a VPN configuration file, refer to the Administrator's Guide of your Windows VPN Client.

Once you have created a VPN configuration and exported it to a VPN configuration file, you must import it to the Android VPN Client.

You can also edit, export, or delete an existing VPN configuration.

8.2 Importing a VPN configuration file

To import a VPN configuration that you created using one of TheGreenBow's Windows VPN Clients on a workstation, proceed as follows:

1. Transfer the VPN configuration file from the computer to the mobile device.
2. Open the menu at the top right of the main screen (three vertical dots), select **Configuration**, and then **Import a configuration file**.
3. Select the file to import in the file explorer that is displayed.

The new VPN connection will be added to the connections list.



To learn how to create a VPN configuration file, refer to the Administrator's Guide of your Windows VPN Client.



If an error occurs during the import, it is likely that the configuration file has not been set up correctly. For example, the Android VPN Client does not support the IKEv1 protocol. In this case, you need to correct the settings in the VPN configuration file using the Windows VPN Client and import it again.

8.3 Changing the configuration of a VPN connection

Once you have imported a VPN configuration, you can edit it from the VPN connections list. To do this:

1. From the VPN connections list, press and hold the VPN connection whose configuration you want to edit.

The configuration of the VPN connection is displayed:

The screenshot shows the configuration interface of the Android VPN Client. At the top, the status bar displays the time 23:06, signal strength, and 96% battery. The main form has the following sections:

- Tunnel Name:** A text field containing "Dev_network".
- Remote Gateway:** A text field containing "tgbtest.dyndns.org".
- Authentication:** Three radio button options:
 - ☒ PSK
 - ☐ Certificate
 - ☐ EAP
 To the right of these options is a green button labeled "IMPORT CERTIFICATE".
- Preshared Key:** A text field with masked characters ".....".
- Confirm:** A text field with masked characters ".....".

At the bottom of the form is a green bar containing three buttons: "SAVE", "EXPORT", and "DELETE". The very bottom of the screen shows the standard Android navigation bar with icons for the app drawer, home, and back.

You can edit the following items:

- Tunnel name
- Remote router address
- Authentication type
- Preshared key

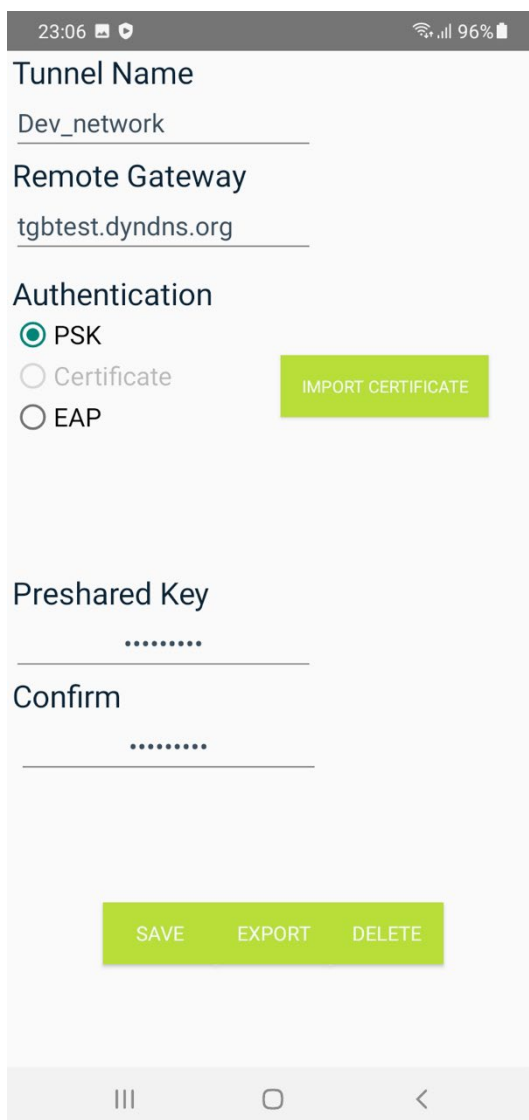
You can also import a certificate in P12 or PFX format (see section 8.4 Importing a certificate into the configuration of a VPN connection below).

2. Tap **SAVE** to save your changes.

8.4 Importing a certificate into the configuration of a VPN connection

You can import a certificate into the configuration of a VPN connection using a certificate file on the mobile device. To do this, follow the steps below:

1. Tap and hold a connection to open it in edit mode. The configuration editing screen is displayed.



23:06 96%

Tunnel Name
Dev_network

Remote Gateway
tgbtest.dyndns.org

Authentication
☒ PSK
☐ Certificate
☐ EAP

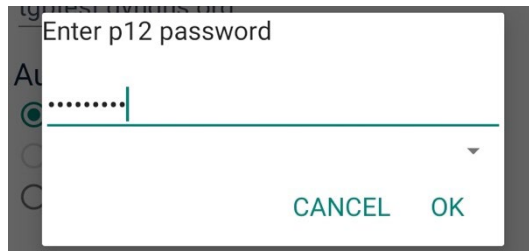
IMPORT CERTIFICATE

Preshared Key
.....

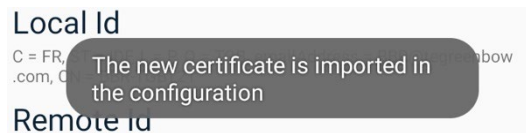
Confirm
.....

SAVE EXPORT DELETE

2. Tap **IMPORT CERTIFICATE**. A file manager window is displayed, allowing you to select the certificate file to import.
3. Select the desired file. A dialog box is displayed, asking you to enter the password associated with the certificate.



4. Enter the password. A message is displayed to confirm that the certificate has been imported successfully.



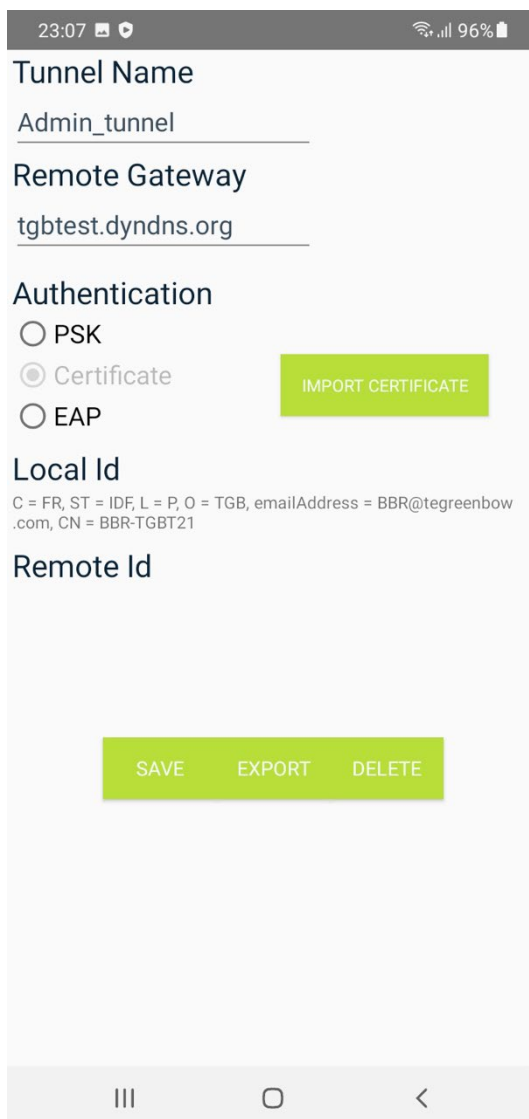
5. The **Certificate** authentication mode is selected and grayed. The certificate's characteristics are shown under **Local ID** and/or **Remote ID**.



Local ID is the identifier that the VPN Client sends to the remote VPN gateway during the authentication phase. **Remote ID** is the identifier of the authentication phase that the VPN Client expects to receive from the VPN gateway. Refer to the Administrator's Guide of the Windows Enterprise VPN Client for more details.



The **Local ID** on the router is the **Remote ID** on the VPN Client and vice versa!



23:07 96%

Tunnel Name
Admin_tunnel

Remote Gateway
tgbtest.dyndns.org

Authentication
☐ PSK
☒ Certificate **IMPORT CERTIFICATE**
☐ EAP

Local Id
C = FR, ST = IDF, L = P, O = TGB, emailAddress = BBR@tegreenbow.com, CN = BBR-TGBT21

Remote Id

SAVE EXPORT DELETE

8.5 Exporting the configuration of a VPN connection

To export a VPN configuration, proceed as follows:

1. From the VPN connections list, press and hold the VPN connection whose configuration you want to export.

The configuration of the VPN connection is displayed:

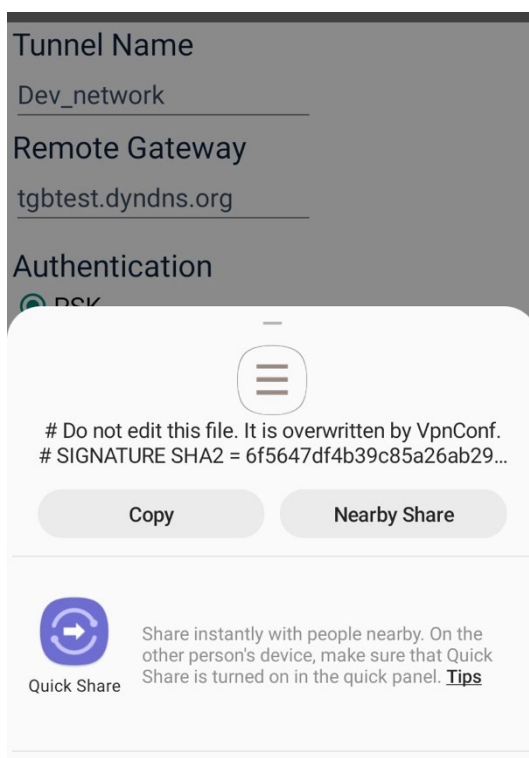
The screenshot displays the configuration interface for a VPN connection on an Android device. The status bar at the top shows the time as 23:06 and a battery level of 96%. The configuration fields are as follows:

- Tunnel Name:** Dev_network
- Remote Gateway:** tgbtest.dyndns.org
- Authentication:** PSK (selected), Certificate, and EAP are listed with radio buttons. An **IMPORT CERTIFICATE** button is located to the right of the Certificate option.
- Preshared Key:** A text field containing seven dots.
- Confirm:** A text field containing seven dots.

At the bottom of the screen, there is a green bar with three buttons: **SAVE**, **EXPORT**, and **DELETE**. The Android navigation bar is visible at the very bottom.

2. Tap the **EXPORT** button at the bottom of the screen.

The **Share** sheet of your mobile device is displayed:



3. You can copy the configuration and paste it into a document or send it directly by e-mail or using other messaging applications available in the **Share** sheet.

8.6 Deleting a VPN connection

To delete a VPN connection, proceed as follows:

1. From the VPN connections list, press and hold the VPN connection that you want to delete.

The configuration of the VPN connection is displayed:

The screenshot shows the configuration screen for a VPN connection. At the top, the status bar displays the time 23:06, signal strength, and 96% battery. The main screen has a light gray background. The 'Tunnel Name' is 'Dev_network'. The 'Remote Gateway' is 'tgbtest.dyndns.org'. Under 'Authentication', 'PSK' is selected with a green radio button, while 'Certificate' and 'EAP' are unselected. A green button labeled 'IMPORT CERTIFICATE' is to the right of the authentication options. Below this, there are two password fields: 'Preshared Key' and 'Confirm', both masked with dots. At the bottom, there is a green bar with three buttons: 'SAVE', 'EXPORT', and 'DELETE'. The bottom of the screen shows the standard Android navigation bar with three icons: a square, a circle, and a triangle.

23:06 96%

Tunnel Name
Dev_network

Remote Gateway
tgbtest.dyndns.org

Authentication
☒ PSK
☐ Certificate
☐ EAP

IMPORT CERTIFICATE

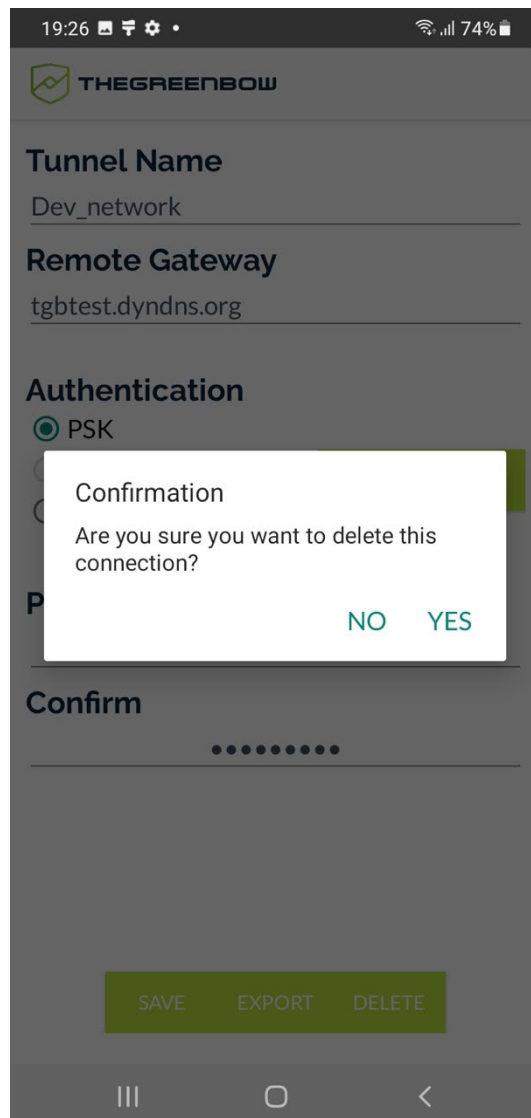
Preshared Key
.....

Confirm
.....

SAVE EXPORT DELETE

2. Tap the **DELETE** button at the bottom of the screen.

A pop-up dialog is displayed prompting you to confirm deletion:



3. Tap **YES** to confirm deletion. The configuration is deleted, and the connection is removed from the connections list.

9 Opening a VPN connection

9.1 Introduction

Once you have configured one or several VPN connections, simply tap the connection name to open it.

By default, the Android VPN Client works in interactive mode. As of version 6.2 of the software, you can enable the **Always-on VPN** function. If you do, the VPN will remain on even if you quit the app or restart the mobile device.

9.2 Opening an IKEv2 VPN connection

To open an IKEv2 connection, tap the name of the connection that you want to open in the list of VPN connections.

The first time you open an IKEv2 connection, a password will only be required if **EAP** has been configured. In this case, enter the password matching the configured login name when prompted.

9.3 Opening an SSL VPN connection

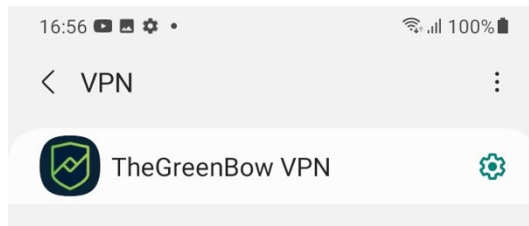
To open an SSL connection, tap the name of the connection in the list of VPN connections.

The first time you open an SSL connection, a password will only be required if **Extra Auth** has been configured. In this case, enter the Extra Auth password when prompted.

9.4 Enabling the Always-on VPN function

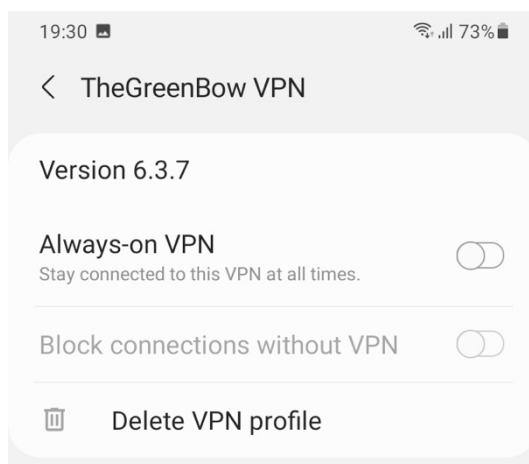
As of version 6.2 of the Android VPN Client, you can enable the VPN permanently so that it remains always on even if you quit the app or restart the mobile device. To do this, follow the steps below:

1. Make sure that no connection is open in the Android VPN Client and that the connection you want to keep always on is at the top of the connection list.
2. Access the mobile device's **Settings**, depending on the version of Android and of the manufacturer's interface, select **Connections**, then **More connection settings**, and then **VPN**. A list of VPN applications available on the mobile device is shown.



You can also open the mobile device's **Settings** and then search for “VPN” to display all the settings related to VPNs.

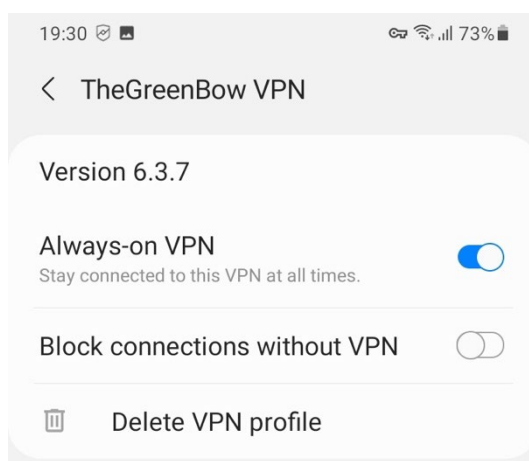
3. In the list, search for the TheGreenBow VPN app and tap the gear to the right of the name. The VPN profile options are shown.



4. In TheGreenBow VPN app settings, enable the **Always-on VPN** option.



The various options may have different names in other Android versions.



The **Always-on VPN** has now been enabled.

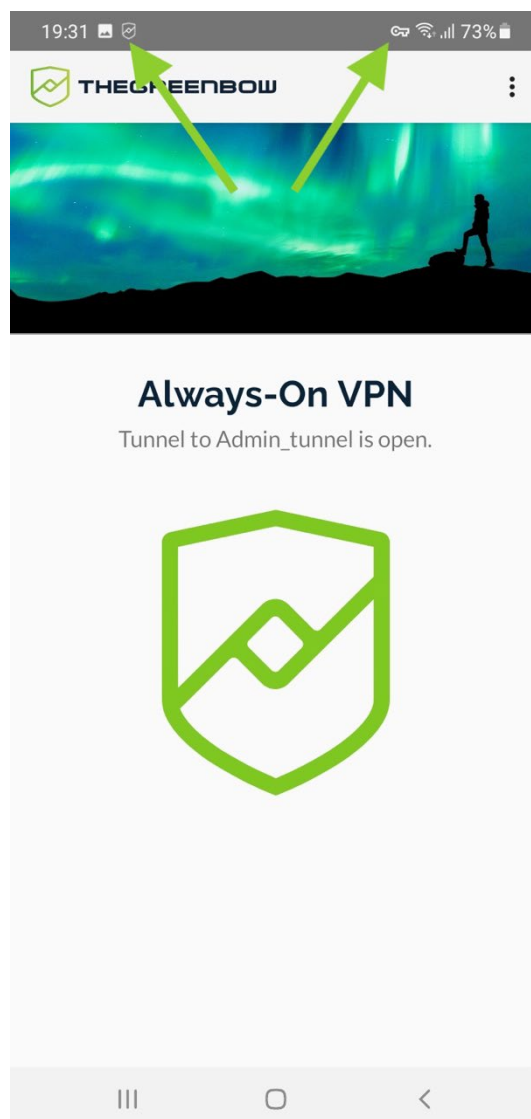


If you enable the **Always-on VPN** option in the system settings while a connection is open in the Android VPN Client, this may lead to improper operation of the app.



You can also enable the **Block connections without VPN** option. In this case, no connection other than the one that uses the VPN can be established.

When you open the TheGreenBow VPN app, instead of the connection list, you will see a message indicating that the **Always-on VPN** function is enabled as well as the name of the open connection.



Moreover, two icons appear in the mobile device's status bar.



For further details on the icons shown in the status bar, refer to section 6.5 Status icons.



When you enable the **Always-on VPN** function and there are several connections in the connection list, the Android VPN Client will select the first connection in the list. Make sure that this connection is the one that you want to keep always on.

9.5 Disabling the Always-on VPN function

To disable the function follow the steps below:

1. Access the mobile device's **Settings**, depending on the version of Android and of the manufacturer's interface, select **Connections**, then **More connection settings**, and then **VPN**. A list of VPN applications available on the mobile device is shown.
2. In the list, search for the **TheGreenBow VPN** app and tap the gear to the right of the name. The VPN profile options are shown.
3. In TheGreenBow VPN app settings, disable the **Always-on VPN** option.

The connection is closed. The TheGreenBow and key icons disappear from the status bar. You can use the Android VPN Client in interactive VPN mode.

10 Logging

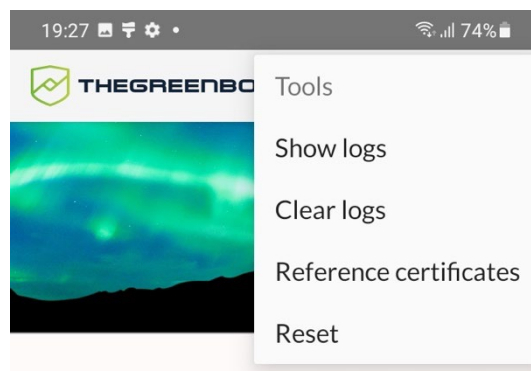
The Android VPN Client provides a logging facility that allows you to perform the following tasks:

- Display log entries in the user interface
- Share log entries with other users
- Clear the current log entries

10.1 Displaying logs

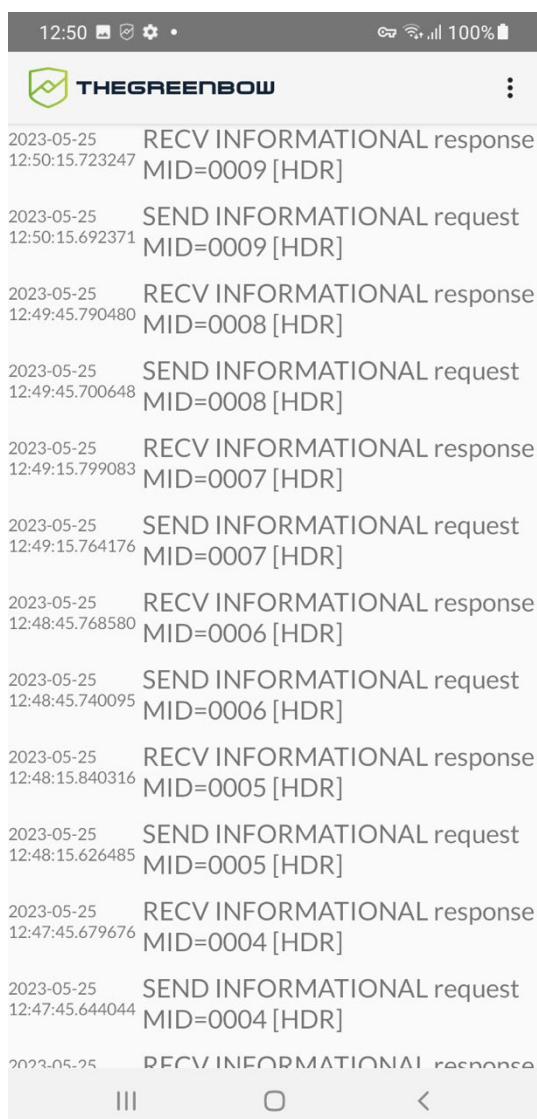
The logging facility provides detailed information on the various steps performed when opening and closing VPN tunnels. Administrators can use this information to identify potential connection issues.

To display the log entries, open the menu at the top right of the main screen (three vertical dots), select **Tools**, and then **Show logs**.



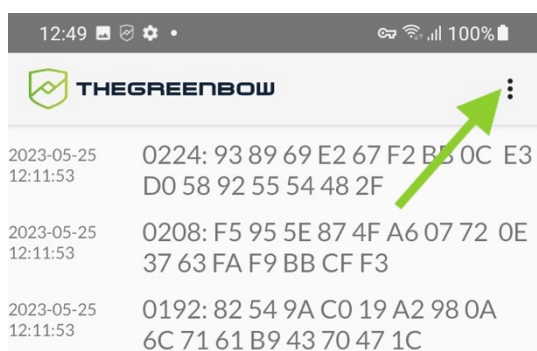
You can enable a verbose mode to get more detailed logs. To do this, in the logs window, select the **Verbose mode** option from the contextual menu (see below) or enable the corresponding toggle button in the **About** window (see section 6.3.4 About submenu).

The log entries are shown on the screen:



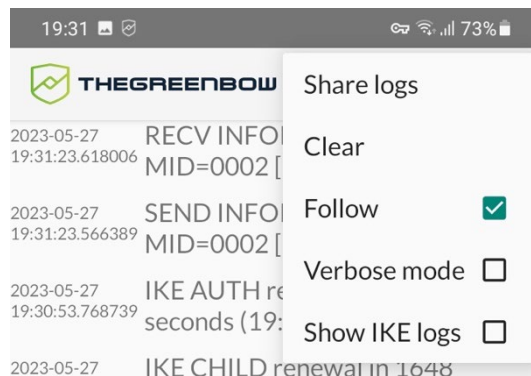
The log entries displayed are the ones corresponding to the last VPN connection that you opened.

As of version 6.3 of the Android VPN Client, a contextual menu is displayed in place of the menu with three vertical dots in the logs window.

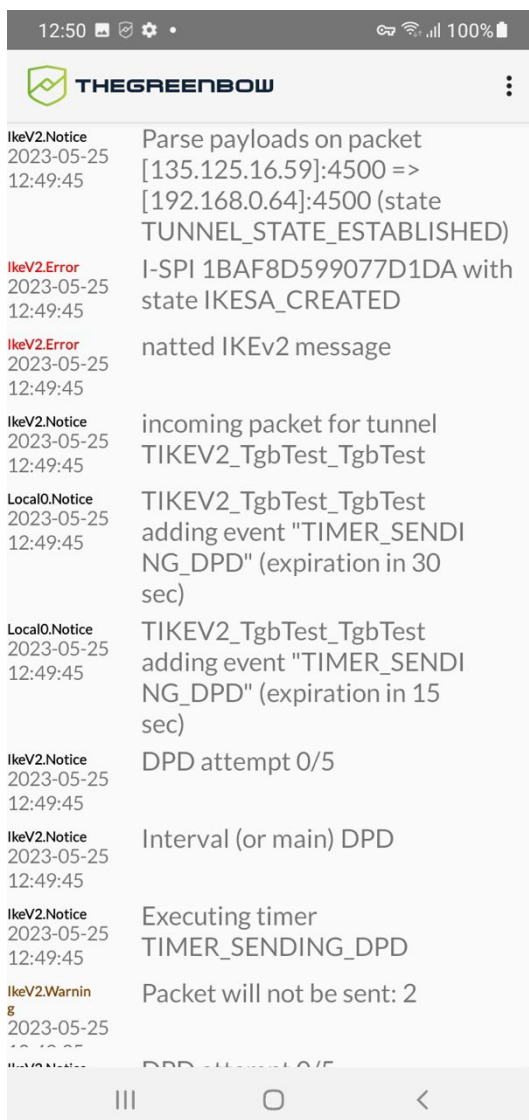


This menu contains the following options:

- **Share logs**, see section 10.2 Sharing logs below
- **Clear**, see section 10.3 Clearing logs below
- **Follow**, stops or restarts scrolling log entries
- **Verbose mode**, used to enable or disable the verbose mode (this option is also available in the **About** window)
- **Show IKE logs**, displays the IKE log entries



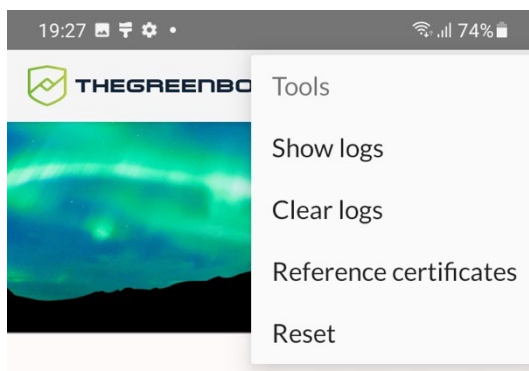
When the **Show IKE logs** option is enabled, the log entries appear as follows in the window:



10.2 Sharing logs

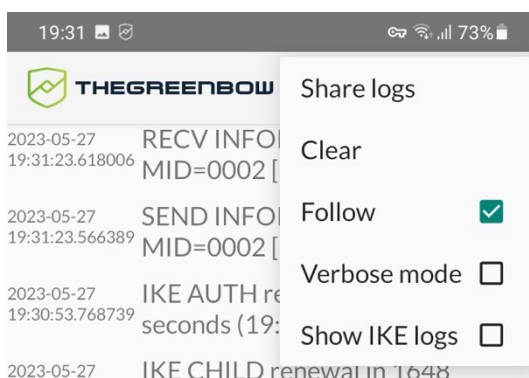
To export the log entries and share them with other users (e.g. technical support), proceed as follows:

1. Open the menu at the top right of the main screen (three vertical dots), select **Tools**, and then **Show logs**.



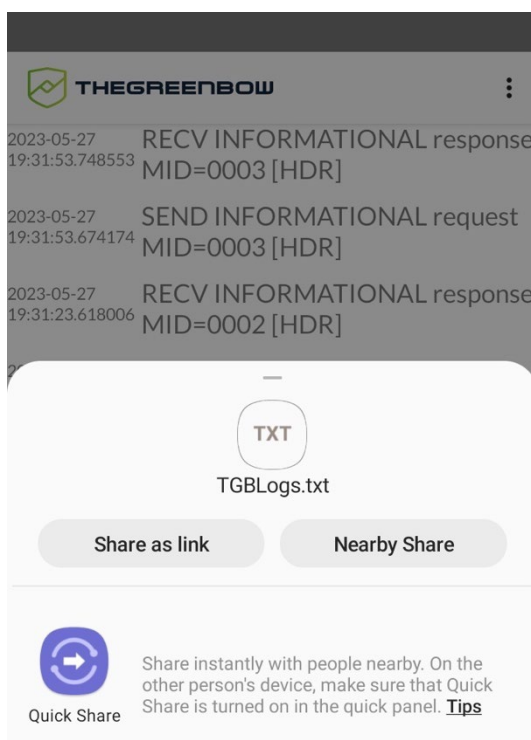
The logs window is displayed.

2. Open the menu at the top right (three vertical dots). The contextual menu is displayed.



3. Select **Share logs**.

The **Share** sheet of your mobile device is displayed:

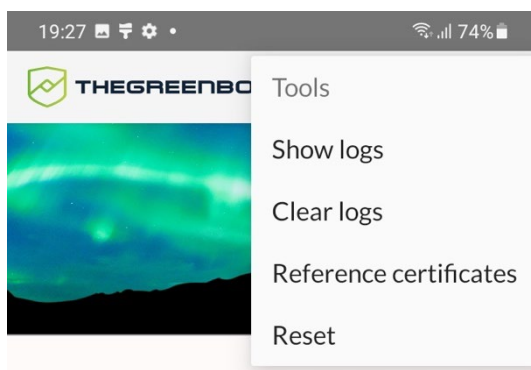


4. The log entries are recorded in a log file named `TGBLogs.txt` that you can share using any of the facilities available in the **Share** sheet.

10.3 Clearing logs

To clear the log entries currently loaded in the user interface, proceed as follows:

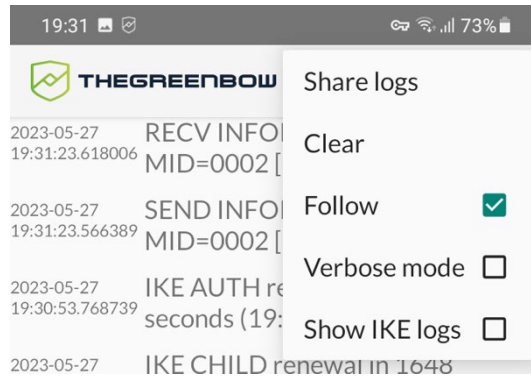
1. Open the menu at the top right of the main screen (three vertical dots), select **Tools**, and then **Clear logs**.



The log entries are cleared. If you display the logs window, the screen will be empty. As soon as you start a new connection, any new log entries that are generated will be shown.

You can also clear the log entries from the contextual menu in the logs window. To do this, proceed as follows:

1. Open the menu at the top right (three vertical dots). The contextual menu is displayed.



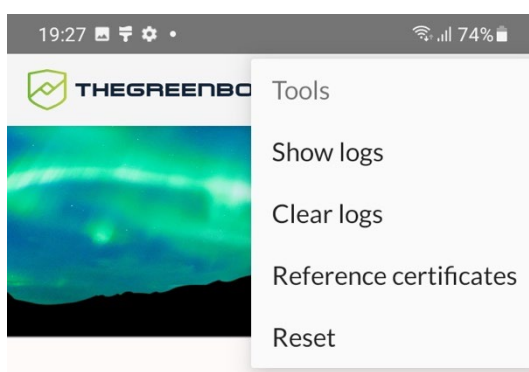
2. Select **Clear**.

11 Troubleshooting

11.1 Resetting the app

If you are unable to close a tunnel, if a tunnel is in an unstable state neither open nor closed, or when the VPN Client is no longer responding, you can reset the app. The processes that are running in the background will be restored to their initial state. Processes will be forced to quit in order to start from fresh.

To do this, open the menu at the top right of the main screen (three vertical dots), select **Tools**, and then **Reset**.



The app is reset, and the main screen is displayed.

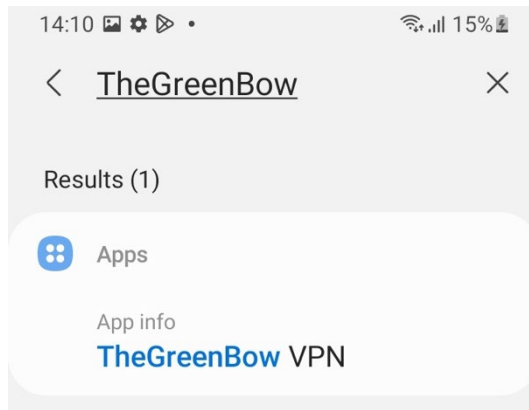
11.2 Deleting app data

In some cases, such as when you encounter activation issues, technical support may ask you to delete the app data.

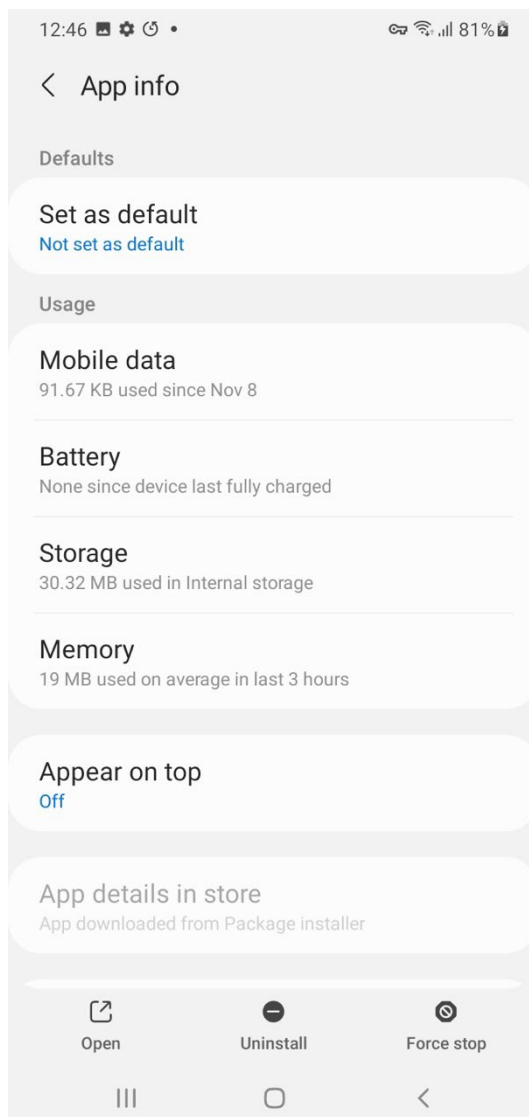
All the data that you have configured in the app, i.e. connections, activation data, and log files, will be deleted from the mobile device. The app will then behave as if it had been installed for the first time.

To delete app data, proceed as follows:

1. Search for the TheGreenBow VPN app in the device's settings.

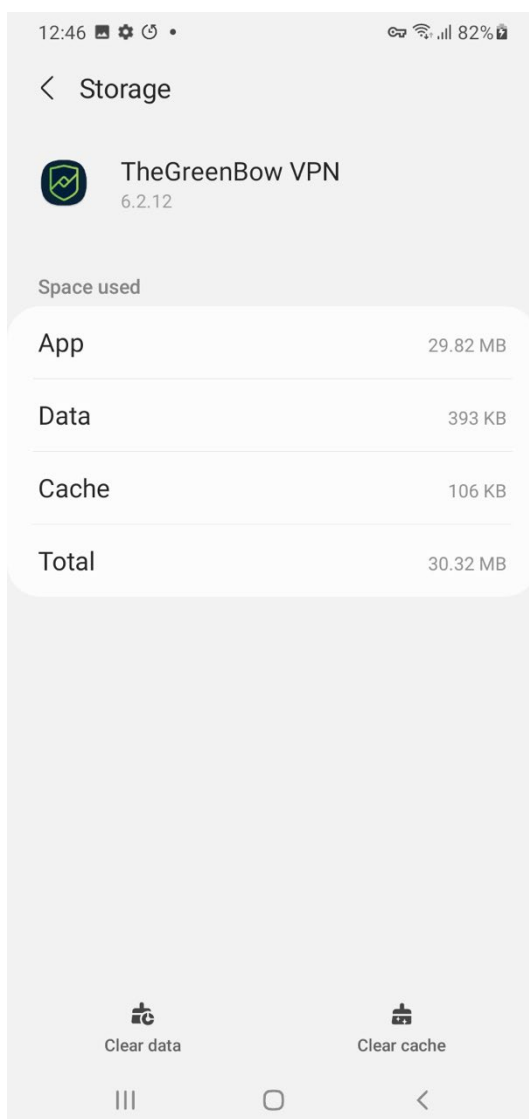


2. Tap **TheGreenBow VPN** in the search results.



3. Select **Storage**.

The storage information is shown:



4. Tap **Clear data**, and then tap **OK** to confirm the warning message that is displayed.

All app data is deleted.

12 Technical data

12.1 General

OS version	Android 10 or higher
Languages	English, French

12.2 Connection/Tunnel

Connection mode	Peer-to-Gateway (see the list of certified gateways and corresponding configuration guides)
Protocols	SSL: OpenVPN IPsec: IKEv2
Configuration Payload (CP) mode	Automatically retrieve network settings from the VPN gateway

12.3 Cryptography and authentication

Encryption, Key group, Hashing (IKEv2)	<ul style="list-style-type: none">Symmetric: AES CBC/CTR/GCM 128/192/256 bitsDiffie-Hellman groups: DH 14 (MODP 2048), DH 15 (MODP 3072), DH 16 (MODP 4096), DH 17 (MODP 6144), DH 18 (MODP 8192), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (ECP 521), DH 28 (BrainpoolP256r1)Hashing algorithm: SHA-2 (256/384/512 bits, IKEv2 only)
Encryption, Hashing (OpenVPN)	Symmetric: AES-128-CBC, AES-192-CBC, AES-256-CBC Hashing: SHA-2 (224/256/384/512 bits)

	<p>TLS 1.2—Medium</p> <p>TLS 1.2—High</p> <p>TLS 1.3:</p>
TLS security suites (OpenVPN)	<ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Authentication	<ul style="list-style-type: none"> • IKEv2: X.509 certificates, EAP-MSCHAPv2, shared key, Multiple Auth (certificate + EAP) • SSL: X509 certificates, Extra-Auth (certificate + username and password)
Certificate authentication methods (IKEv2)	<ul style="list-style-type: none"> • Method 1: RSA digital signature with SHA-2 [RFC 7296] • Method 9: ECDSA “secp256r1” on the P-256 curve with SHA-2 (256 bits) [RFC 4754] • Method 10: ECDSA “secp384r1” on the P-384 curve with SHA-2 (384 bits) [RFC 4754] • Method 11: ECDSA “secp521r1” on the P-521 curve with SHA-2 (512 bits) [RFC 4754] • Method 14: RSASSA-PSS and RSASSA-PKCS1-v1_5 digital signature [RFC 7427] • Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits)
PKI	<ul style="list-style-type: none"> • Support for certificates in X509 format • Importing PKCS#12, PFX certificates • Multiple media: Android Certificate Store, configuration file • Complete check of the “user” and “gateway” certificate chain (with root CA in configuration)

13 Contact

13.1 Information

All the information on TheGreenBow products is available on our website:
<https://thegreenbow.com/>.

13.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

13.3 Support

There are several pages related to the software's technical support on our website:

Online help

<https://www.thegreenbow.com/en/support/online-support/>

FAQ

<https://www.thegreenbow.com/en/frequently-asked-questions/>

Contact form

Technical support can be reached using the form on our website at the following address: <https://www.thegreenbow.com/en/support/online-support/technical-support/>.

Protect your connections
in any situation