THEGREENBOW

TheGreenBow VPN Client iOS

User Guide

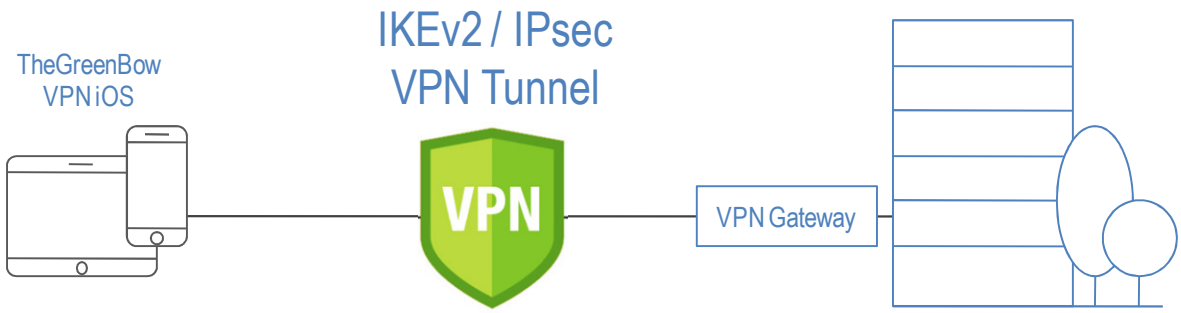
Table of Contents

1 Presentation

1.1 TheGreenBow VPN Client

TheGreenBow VPN Client iOS is a VPN Client software designed for iOS.It enables to establish secure connections between the user device and the Information System of the company.

TheGreenBow VPN Client iOS enables to open VPN connections with any VPN Gateway (see the list of qualified VPN gateways). TheGreenBow VPN Client implements IPsec, IKEV2 standards to be compatible with all VPN Gateways.



For most IKEv2 VPN gateways on the market, TheGreenBow provides a configuration guide. To configure your VPN gateway, see the list of configuration guides of VPN gateways.

1.2 TheGreenBow VPN Client main features

TheGreenBow VPN Client iOS provides the following features:

- Ability to create IPsec VPN tunnel using IKEv2
- "DPD" (Dead Peer Detection) features
- Mode CP (IKEv2) management
- Intuitive and powerful graphical interface

2 Installation

2.1 Installation and Updates

The VPN Client should be downloaded from Apple's App Store. As a consequence, all software updates will be handled by Apple's App Store as well. The application is free, but requires an In-App purchase to be fully functional (See also "Full Access" In App Purchase).

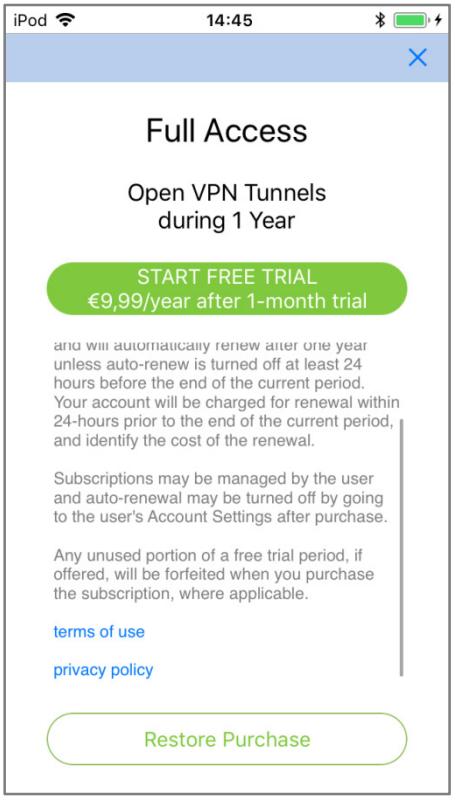
2.1.1 Installation requirements

The minimal iOS version required to run TheGreenBow VPN Client iOSis iOS 9.0.

2.2 "Full Access" In App Purchase

All management of VPN configurations can be done freely. However, to open a VPN tunnel, an In-App purchase is required. This "Full Access" In-App purchase is an auto-renewing subscription with a subscription period of 1 year. There is a 1 month trial after which you will be billed for the subscription, unless you decided to cancel the subscription explicitly.

The application will automatically check whether you have a valid subscription and show the subscription page if not so. If the subscription page is shown despite being subscribed, then use the restore button and log in with the correct Apple App Store account when asked to do so. The subscription page will not be shown anymore once a valid subscription is detected.



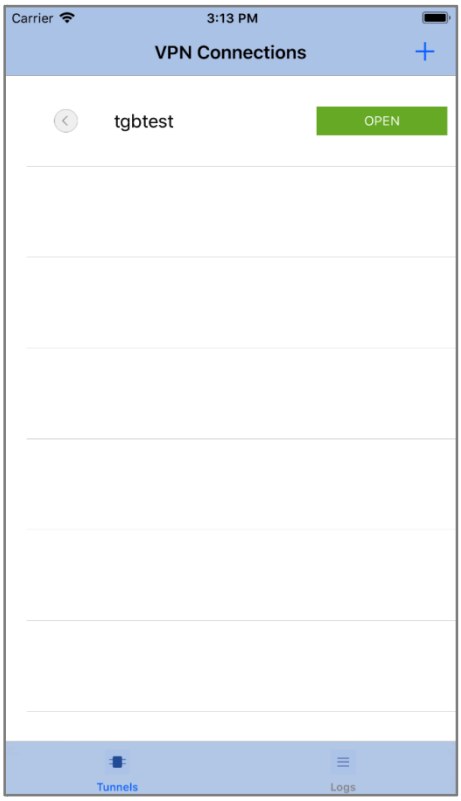
2.3 Uninstallation

The application can be uninstalled in the same way other iOS App Store apps can be uninstalled. One method is to tap and hold the VPN Client icon until all icons start to wiggle, then tap on the small X in the top left corner.

The app can always be reinstalled from the App Store if wanted.

2.4 Test Configuration

After the application is installed, a test VPN configuration is automatically added to the list of VPN configurations. This test configuration can be used to check that TheGreenBow VPN client is operational. After the tunnel is open you should be able to ping the machine at 192.168.175.50, or visit the webpage at http://192.168.175.50 in your web browser.



3 User Interface

3.1 Overview

After the VPN client is fully started and the splash screen disappeared, the main screen is visible. It is composed of the following elements:

- The title bar with the Add Tunnel icon (+)
- The VPN Tunnel Listwhich takes the main part of the screen
- A tab bar at the bottom with two items: “Tunnels” and “Logs”.

3.2 VPN Tunnel List

3.2.1 Introduction

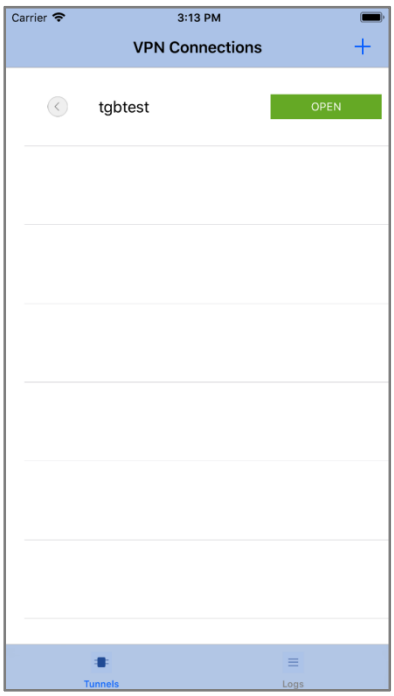
When the “Tunnels” tab is selected, the VPN Tunnel List is visible. Every item in the tunnel list represents a VPN security policy. The list can contain an unlimited number of VPN tunnels.

For IKE v2 tunnels, every item in the list correspond to the combination of exactly one IKE Auth and Child SA. The Open button opens (or closes when the tunnel is already open) the tunnel. The icon on the left for each item in the VPN Tunnel List gives extra info about the corresponding tunnel:

Closed tunnel. Tapping the “Open” button will open it if no other tunnel is opened. Tapping on the arrow will show the configuration of the tunnel.

Tunnel is opened. Tapping the “Close” button willclose the tunnel.

Tunnel is opening or closing



4 ImportVPN Security Policy

TheGreenBow VPN Client can import VPN security policies that are present on the device as files with file extension tgb. Tapping such a file (for example as an email attachment) will give the user the option to open it with TheGreenBow VPN Client iOS.

If the VPN security policy is password protected, then the password will be asked when importing the security policy.

Note: No check is done whether a tunnel with the same name exists already in the VPN Client and a duplicate name will not result in an error.

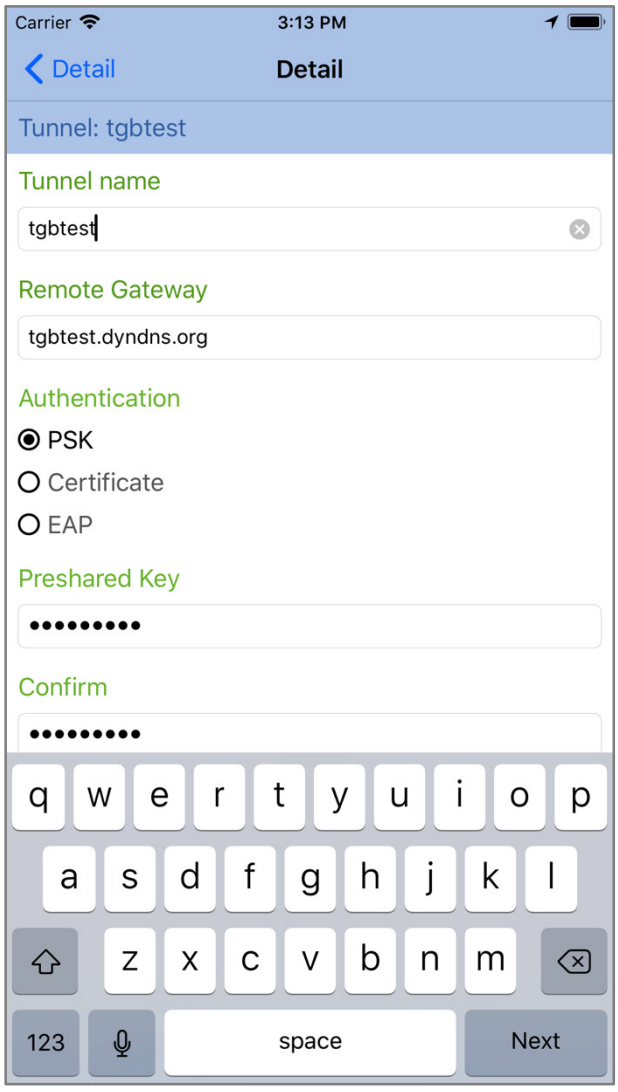
5 Configure a VPN tunnel

An IKE v2 security policy consists of two parts, the IKE Auth part which configures the IKE v2 authentication phase, and the Child SA part. There is no visible distinction between the IKE Auth and the Child SA part in the iOS app.

5.1 Configure an IKEv2 IPsec tunnel

To configure a tunnel, tap the  button for the VPN tunnel you like to configure
This symbol is only visible when the tunnel is closed.

The Detail screen will appear and show the specifics of the tunnel. To change to configuration, tap the “Edit” button at the bottom of the screen.



Remote Gateway

Remote Gateway	IP address or DNS address of the remote gateway (in our example: tgbtest.dyndns.org). This field is mandatory.

Authentication

Pre Shared Key	Password or key shared with the remote gateway. Note: The pre-shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates.
Certificate	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...).
EAP	EAP (i.e. Extensible Authentication Protocol) enables to authenticate the user through a login/password.
Multiple Auth Support	Multiple Auth Support enables the combination of both Certificate authentication then EAP (login/password) authentication. (1)

(1) The double authentication "Certificate then EAP" is supported by the VPN Client. The double authentication "EAP then Managing Certificates

In iOS, certificates cannot be set. This means that the Certificate option cannot be configured directly nor can Multiple Auth Support in the VPN Client. Certificate and Multiple Auth Support authentication is still possible through imported .tgb configurations with embedded certificates.

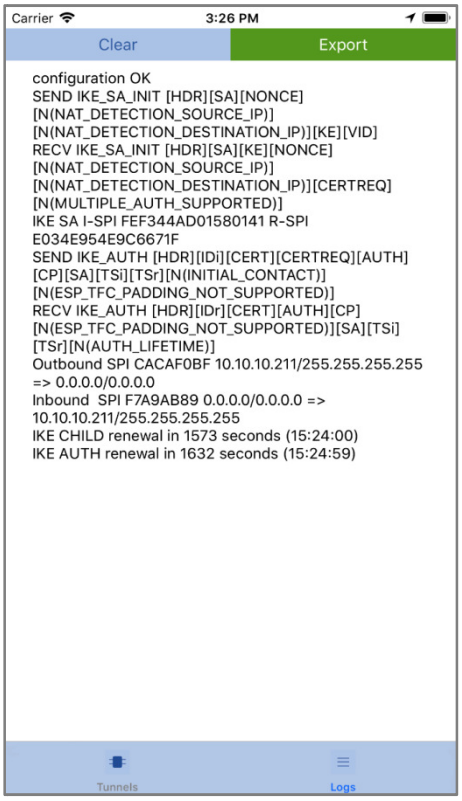
6 Console and Logs

TheGreenBow VPN Client offers two tools that generate logs:

1. The "Console" provides information aboutthe progression of the opening and closing of the tunnels (IKE messages for most of them)
2. A "Trace Mode" asks each software component to produce its activity's log.

Both tools are designed to help the network administrator to diagnose a problem during tunnels opening, or TheGreenBow support team in identifying software's incidents.

The Trace Mode's logs and the content of the Console window, can be exported from the Console window.



6.1 Console

The Console window can be displayed as follows by clicking on the Logs tab-bar item

The Console features include:

- Export: Save and export all traces displayed in the window and all log and .tgb files. The exported files will be stored in the app's Documents folder.
- Clear: Empty the content of the console window

7 Specifications

7.1 Main features

- Ability to create IPsec VPN tunnel using IKEv2
- "DPD" (Dead Peer Detection) features
- Mode CP (IKEv2) management
- Intuitive and powerful graphical interface

7.2 Languages

English

7.3 OS compatibility

The minimal iOS version required to run TheGreenBow VPN Client iOSis iOS 9.0.

7.4 Cryptography

Encryption	Symmetric: DES, 3DES, AES 128/192/256bit Asymmetric: RSA Diffie-Hellmann: 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
Authentication	User: - X-Auth static or dynamic (request at each tunnel's opening) - Hybrid Authentication - Pre-shared key - EAP

8 Contact

8.1 Information

All information about TheGreenBow products is available from: www.thegreenbow.com

8.2 Sales

Phone: +33.1.43.12.39.30
Email: sales@thegreenbow.com

8.3 Support

Different pages concerning the support are available on the TheGreenBow website:

Support

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

Online help

http://www.thegreenbow.com/support_flow.html?product=vpn&lang=en

FAQ

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

Contact

Technical support is available through the inline forms or directly at: support@thegreenbow.com

9 Credits and Licences

Credits and licences references.

```
/*
 * Copyright (c) 1998, 1999 Niels Provos.  All rights reserved.
 * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>.  All rights reserved.
 * Copyright (c) 1998, 1999, 2000, 2001 NiklasHallqvist.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson.  All rights reserved.
 * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */

/* ====================================================================
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
*     openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
```

```
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform withNetscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software