

THEGREENBOW

TheGreenBow
iOS
VPN Client

User Guide

Table of Contents

1	Introduction.....	3
1.1	TheGreenBow VPN Clients	3
1.2	Features of TheGreenBow iOS VPN Client.....	4
2	Installation	5
2.1	Installation and Updates.....	5
2.2	“Full Access” In-App Purchase	5
2.3	Uninstallation.....	6
2.4	Test Configuration	6
3	User Interface	7
3.1	Overview	7
3.2	VPN Tunnel List.....	7
4	Importing a VPN Security Policy	9
5	Adding a VPN Security Policy.....	10
6	Configuring a VPN tunnel	11
6.1	Configuring an IKEv2 IPsec tunnel	11
6.2	Configuring an SSL tunnel	18
7	Redundant Gateway.....	23
8	Console and Logs	24
8.1	Console	24
8.2	Export.....	24
9	Specifications.....	25
9.1	Tunnels.....	25
9.2	Network	25
9.3	Cryptography	25
9.4	Languages	25
9.5	OS compatibility.....	25
10	Contact	26
10.1	Information	26
10.2	Sales	26
10.3	Support	26
11	Third-party licenses	27

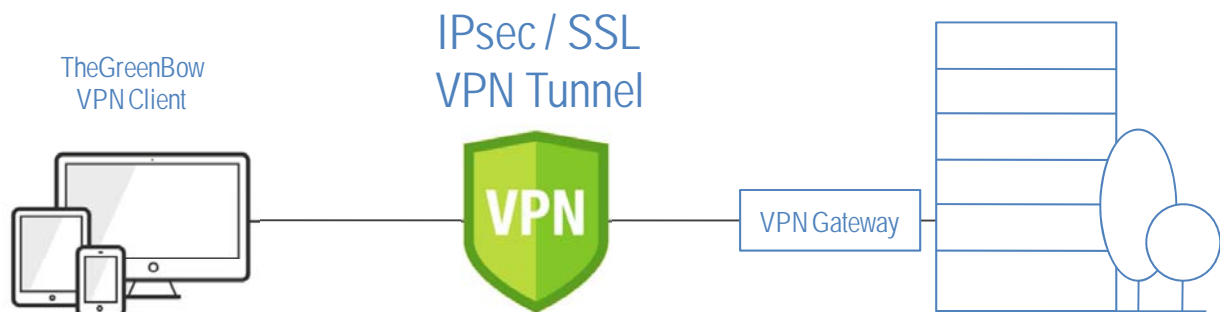
1 Introduction

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 iOS VPN Client

TheGreenBow iOS VPN Client is packed with the following features:

- Compatible with most IPsec and SSL compliant gateways
- Protocols: SSL, IPsec IKEv2
- Authentication: PSK, EAP, Certificate, Multiple Auth
- Certificate management: PKCS#12, PFX, PEM
- IKE fragmentation
- NAT-T support
- Configuration Payload
- Encryption: 3DES, AES 128, 192, 256
- Authentication: SHA2-256, SHA2-384, SHA2-512
- DH Group 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
- DPD (Dead Peer Detection)
- Redundant gateway
- IKEv2 fragmentation
- Secure management of VPN security policies (encryption and integrity)
- Intuitive GUI with full configuration capabilities
- Real time log display

2 Installation

2.1 Installation and Updates

The VPN Client should be downloaded from the [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).

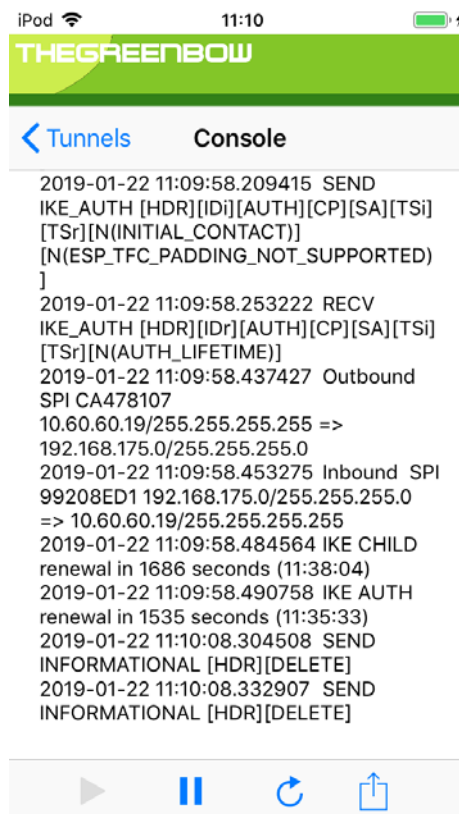
TheGreenBow iOS VPN Client currently supports iOS version 13.0 and higher.

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.

After your purchase the subscription, you will benefit from a 1-month trial, after which you will be billed for the subscription, unless you explicitly cancel the subscription.

The App will automatically check whether you have a valid subscription and show the subscription page if it's not the case. If the subscription page is shown despite having subscribed, 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 iOSapps 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 of TheGreenBow iOS VPN Client icon.

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

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 iOS VPN client is operational. After the tunnel is opened, you should be able to ping the machine at 192.168.175.50 or visit our test webpage at <http://192.168.175.50> from your web browser.

3 User Interface

3.1 Overview

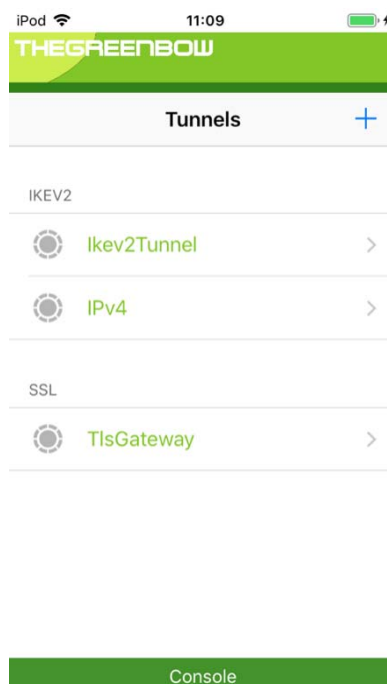
After the VPN client is fully started and the splash screen disappeared, the main screen is visible. It is composed of the following elements:

- The title bar with the Add Tunnel icon (+)
- The VPN Tunnel list which takes the main part of the screen
- A button at the bottom to launch the "Console".

3.2 VPN Tunnel List

3.2.1 Introduction

When not in Console mode, 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, each item in the list corresponds to the combination of exactly one IKE Auth and Child SA. The icon on the left of each item in the VPN Tunnel List provides live information on the corresponding tunnel:



Tunnel is closed



Tunnel is open



Tunnel is opening


3.2.2 Opening a tunnel

To open a tunnel in the list, tap on the line of the tunnel of your choice, then tap on the green “Connect” Button. The button will turn grey and display the text: “Connecting”.

If the tunnel is successfully opened, the button turns Red and displays the text “Disconnect”. If not, then the button turns green again and displays the text “Connect” once again.

Note: you can open only one tunnel at a given time. If you try to open a tunnel while another one is already opened, the “Connect” button will be grey and display the text: “Another tunnel is connected”.

3.2.3 Closing a tunnel

To close an open tunnel, select the tunnel from the list that has the “Tunnel is open”  green icon, and tap the “Disconnect” button.

4 Importing a VPN Security Policy

TheGreenBow iOS 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 iOS VPN Client. Another option is to transfer the file by Apple’s AirDrop service which is builtin iOS and macOS devices.

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 already exists. Duplicate names do not result in any error.

5 Adding a VPN Security Policy

To add an IKEv2 or SSL VPN tunnel, tap on the + button in the navigation bar of the Tunnels View. A menu appears that asks whether to add an IKEv2 or SSL tunnel. An IKEv2 tunnel automatically creates an IKE Auth and Child SA pair.

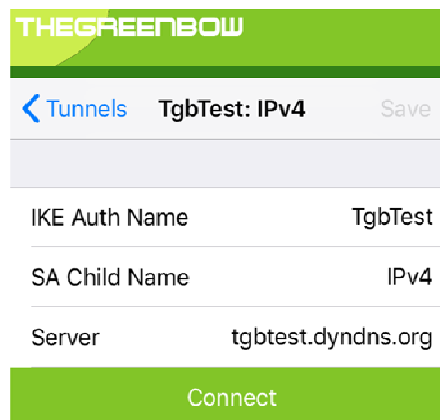
Look at [Configure](#) the next section to see how to configure security policies.

6 Configuring a VPN tunnel

6.1 Configuring an IKEv2 IPsec 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.

To names of either the IKE Auth as well as the SA Child item can be changed easily in the detail view. Also, the Gateway can be entered there.



The screenshot shows the THEGREENBOW app interface. At the top, there's a green header with the app name. Below it, a navigation bar shows a back arrow, the word 'Tunnels', the current tunnel name 'TgbTest: IPv4', and a 'Save' button. The main area contains three rows of configuration fields: 'IKE Auth Name' with the value 'TgbTest', 'SA Child Name' with the value 'IPv4', and 'Server' with the value 'tgbtest.dyndns.org'. At the bottom, there is a large green 'Connect' button.

IKE Auth Name	The name of the IKE Auth item
SA Child Name	The name of the Child SA item. This name will be shown in the VPN Tunnel List
Server	IP address (note IPv6 is not supported) or name of the remote gateway (in our example: tgbtest.dyndns.org). This field is mandatory.

6.1.1 Configure IKE Auth

A VPN tunnel IKE Auth is the Authentication Phase in IKEv2.

IKE Auth purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of IKE Auth, each end-system must identify and authenticate itself to the other.

To configure an IKE Auth item, select it in the VPN Tunnel list and tap on the IKE Auth item in the segment control.

IKE Auth

Child SA

Select whether you would like to see or alter the IKE AUTH or the Child SA phase.

AUTHENTICATION

Authentication Type **Preshared Key** >

Preshared Key ●●●●●●●●

CRYPTOGRAPHY

Encryption **Auto** >

Authentication **Auto** >

Key Group **Auto** >

IDENTITY

Local Identity Type >

Remote Identity Type >

ADVANCED FEATURES

Fragmentation ☐

IKE port **500**

NAT port **4500**

DEAD PEAR DETECTION (DPD)

Check Interval [s] **0**

Max. number retries **0**

Delay between retries **0**

LIFETIME

Lifetime [s] **1800**

GATEWAY RELATED PARAMETERS

Redundant Gateway

Retransmission **3**

Gateway Timeout [s] **0**

Authentication

Authentication Type	<p>The type of authentication that is chosen. The types available are:</p> <p><i>Pre-shared Key</i> 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 security than using a certificate.</p> <p><i>Certificate</i> Use a certificate for the authentication of the VPN connection. Note: Using a certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...).</p> <p><i>EAP</i> EAP (i.e. Extensible Authentication Protocol) enables to authenticate the user using a login/password. The login and password must be explicitly saved in the configuration.</p>
Multiple AUTH support	Multiple Auth Support enables the combination of both Certificate authentication then EAP (login/password) authentication.

Certificates cannot be added to configurations in TheGreenBow iOS VPN Client. In order to create a Certificate or EAP with Multiple AUTH support configuration, create it on a desktop client and import it in the TheGreenBow iOS VPN client.

Cryptography

Encryption	<p>Encryption algorithm used during Authentication phase: Auto (1), DES, 3DES and AES, AES-CTR and AES-GCM with 128, 192 and 256-bit key sizes.</p>
Authentication	<p>Authentication algorithm used during Authentication phase: Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512. This parameter is ignored when AES-GCM is chosen as encryption.</p>
Key Group	<p>Diffie-Hellman key length: Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), DH19 (ECP 256), DH20 (ECP 384), DH21(ECP 512)</p>

⁽¹⁾ Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When "Auto" is selected, all implemented algorithms are proposed to the VPN gateway. Note: gateways that require that AES-GCM algorithms are put in a different proposal are not supported.

Identity

Local Identity Type	<p>"Local ID" is the identifier of the authentication phase (IEK Auth), sent by the VPN Client to the VPN Gateway.</p> <p>Depending on the selected type, the identifier can be:</p> <ul style="list-style-type: none"> – IP address (type = IP address), e.g. 195.100.10.101.
---------------------	---

- (IPv4 since IPv6 is not supported in the current version)
- A domain name (type = FQDN), e.g. gw.mydomain.net
- Address (type = USER FQDN), e.g. support@thegreenbow.com
- A string (type = KEY ID), e.g. 123456
- The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)).
This happens when the tunnel is associated with a user certificate.

If this parameter is not set, the IP address of the VPN Client is used by default.

Remote Identity Type	<p>"Remote ID" is the identifier the VPN Client expects from the VPN gateway.</p> <p>Depending on the type selected, this identifier can be:</p> <ul style="list-style-type: none"> - IP address (type = IP address), e.g. 80.2.3.4. (IPv4 since IPv6 is not supported in the current version) - A domain name (type = FQDN), e.g. routeur.mydomain.com - Address (type = USER FQDN), e.g. admin@mydomain.com - A string (type = KEY ID), e.g. 123456 - The subject of a certificate (type = DER ASN1 DN) <p>When this parameter is not set, the VPN Client will accept any identifier sent by the VPN gateway without checking.</p>
----------------------	---

Advanced Features

Fragmentation	<p>Enables the fragmentation of IKEv2 packets, in accordance to RFC 7383. Use this function to prevent IKEv2 packets from being fragmented by the IP network. The value of "Fragment size" should be less or equal than the IP network's fragment size (typically 1500).</p>
IKE Port	<p>IKE Auth phase exchanges (Authentication) are performed on the UDP protocol using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to pass through these filtering devices.</p> <p><u>Note:</u> The remote VPN gateway must also be capable of performing the IKE Auth Phase exchanges on a different port than 500.</p>
NAT Port	<p>Child SA phase exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the NAT port to a different value allows passing through these filtering devices.</p> <p><u>Note:</u> The remote VPN gateway must also be capable of performing the Child SA phase exchange on a different port than 4500.</p>

Dead Peer Detection (DPD)

Check interval	Period between 2 DPD verification messages. Dead Peer Detection (DPD) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive.
Max. number of retries	Number of consecutive unsuccessful attempts before declaring the remote

gateway unreachable.

Delay between retries

Interval between DPD messages when no response is received from the VPN gateway.

Lifetime

Lifetime

Lifetimes of IKE Authentication phase. Expressed in seconds.
Lifetimes are not negotiated during IKEv2 exchanges

Gateway Related Parameters

Redundant Gateway

This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the URL of the Redundant Gateway (e.g. router2.dyndns.com).
See section "[Managing Redundant Gateway](#)" below.

Retransmissions

Number of IKE protocol message retransmissions before failure

Gateway Timeout

Delay in seconds between two retransmissions

6.1.2 Configure Child SA

The purpose of Child SA is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during IKE Auth.

To configure a Child SA, select the item in Configuration Panel Tunnel List and select Child SA in the segmented control.

IKE AuthChild SA

Select whether you would like to see or alter the IKE AUTH or the Child SA phase.

TRAFFIC SELECTORS

Request configuration from t...

CRYPTOGRAPHY

EncryptionAuto >

AuthenticationAuto >

Key GroupNo Diffie-Hellman >

LIFETIME

Child SA Lifetime [s]1800

ALTERNATE SERVERS

DNS suffix

Alternate DNS server

Alternate DNS server

Traffic Selectors

Request configuration from the gateway	When this option is selected (also known as "Configuration Payload" or "CP"), all information (VPN Client address, Remote LAN address, Subnet mask and DNS addresses) is sent by the VPN gateway. When selected, the corresponding fields are hidden from the user interface, as they can't be edited. They will be received from the VPN gateway during the opening of the VPN tunnel.
VPN Client address	This is the "virtual" IP address of the computer, as it will be seen on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel.
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below

Cryptography

Encryption	Encryption algorithm negotiated during IPsec phase: Auto ⁽¹⁾ , DES, 3DES and AES, AES-CTR and AES-GCM with 128, 192 and 256-bit key sizes.
Integrity	Authentication algorithm negotiated during IPsec phase: Auto ⁽¹⁾ , MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512.
Diffie-Hellman	Diffie-Hellman key length: Auto ⁽¹⁾ , DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), DH19 (ECP 256), DH20 (ECP 384), DH21(ECP 512), No Diffie-Hellman

⁽¹⁾ Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When "Auto" is selected, all implemented algorithms are proposed to the VPN gateway. Note: gateways that require that AES-GCM algorithms are put in a different proposal are not supported.

Lifetime

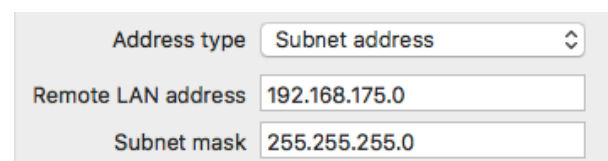
Child SA lifetime	Child SA time in seconds before re-negotiation. <u>Note</u> : Unlike IKEv1, the lifetimes are not negotiated in IKEv2, between the VPN Client and the VPN Gateway. The Lifetimes used for the tunnel are the lifetimes set in the VPN Client configuration.
-------------------	--

Alternate servers

DNS Suffix	Domain suffix to be added to any machine, e.g. "mozart.dev.thegreenbow". This parameter is optional: The VPN Client will first try to translate the machine address without adding a DNS suffix. If the translation fails, the VPN Client will add the DNS suffix and try to translate the address again.
Alternate servers	Table of the IP addresses of DNS servers (2 maximum) and WINS servers (2 maximum) available on the remote network. The IP addresses to be entered will be either IPv4 or IPv6 depending on the network type selected in the "Child SA" tab. Note: If CP Mode is enabled (see "Request configuration from the gateway" in the "Child SA" tab), these fields are disabled (they cannot be entered). They will be actually automatically filled by the gateway when the tunnel is opened.

6.1.2.1 Address type configuration

If the end of the tunnel is a network, choose the "Subnet Address" and then set the address and mask of the remote network:



The screenshot shows a configuration window with a title bar. Inside, there's a section titled 'Address type' with a dropdown menu currently showing 'Subnet address'. Below this, there are two input fields: 'Remote LAN address' containing the text '192.168.175.0' and 'Subnet mask' containing the text '255.255.255.0'.

Or choose "Range Address" and set the start address and the end address:

Address type

Start address

End address

If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:

Address type

Remote host address

Note: If the IP address of the VPN Client is part of the IP address range of the remote network (e.g. @IP computer = 192.168.10.2 and @remote network = 192.168.10.x), the opening of the tunnel prevents the device to contact its local network. All communications will be routed into the VPN tunnel.

Configuring "all traffic through the VPN tunnel":

It is possible to configure the VPN Client to force all outgoing traffic to go through the VPN tunnel. To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

Reminder: Many configuration guides with different VPN Client VPN gateways are available on TheGreenBow website: http://www.thegreenbow.com/vpn_gateway.html.

6.2 Configuring an SSL tunnel

SSL tunnels established by TheGreenBow iOS VPN Client are compatible with OpenVPN and can establish secure connections with all gateways implementing this protocol.

It is not possible in the current version to change or add the certificate used for authentication. As a consequence, VPN security policies for SSL tunnels using a certificate need to be created on a desktop client, saved, and then imported into TheGreenBow iOS VPN Client.

iPod 11:25

THEGREENBOW

[←](#) **TLS Gateway: TlsGateway** [Save](#)

Name TlsGateway

Gateway remotehost

Connect

REMOTE GATEWAY

Redundant Gateway

AUTHENTICATION

Common Name

Issuer

Expiration Date

EXTRA AUTHENTICATION

Enabled ☒

Login

Password

INITIAL AUTHENTICATION (TLS)

Security Suite Auto >

TRAFFIC SECURITY SUITE

Authentication SHA1 >

Encryption BF-CBC-128 >

Compression Auto >

EXTRA HMAC (TLS_AUTH)

Extra HMAC



Key Direction

BiDir >

Key

DEAD PEAR DETECTION (DPD)

Ping Gateway [s]

0

Detect Gateway [s]

0

On Dead Pear Detection Close T... >

KEY RENEGOTIATION

Bytes [KB]

0

Packets

0

Lifetime [s]

3600

TUNNEL OPTIONS

Physic.If MTU

0

Tunnel MTU

0

TUNNEL ESTABLISHMENT OPTIONS

Port

1194

Retransmissions

2

Authentication Timeout

15

Traffic Setup Timeout

10

Name	Name of the tunnel
Gateway	IP address (IPv4 because this version does not support IPv6) or name of the remote gateway (in our example: tgbtest.dyndns.org). This field is mandatory.

Remote Gateway

Redundant Gateway	Defines the address of an alternate VPN gateway that the VPN Client will switch to when the initial gateway is down or inactive. The redundant VPN gateway's address can be either an IP or DNS address. See section " Managing Redundant Gateway " below.
-------------------	--

Initial Authentication (TLS)

Security Suite	<p>This parameter is used for configuring the security level of the authentication phase during the SSL exchange.</p> <ul style="list-style-type: none">- Automatic: all cypher suites (except null) are presented to the gateway, which will use the best fit.- Low: only weak cypher suites are presented to the gateway. In the current version, these are suites using 64- or 56-bit encryption algorithms.- Normal: only "medium" cypher suites are presented to the gateway. In the current version, these are suites using 128-bit encryption algorithms- High: only strong cypher suites are presented to the gateway. In the current version, these are suites using 128-bit or higher encryption algorithms.
----------------	---

Traffic Security Suite

Authentication	<p>Authentication algorithm negotiated for traffic: Automatic (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512.</p> <p><u>Note:</u> If the "Extra HMAC" option is activated (see below), the authentication algorithm cannot be set to "Automatic". It will have to be explicitly configured and identical to the one chosen at the gateway endpoint.</p>
Encryption	<p>Traffic encryption algorithm: Automatic (1), BF-CBC-128, AES128-CBC, AES192-CBC, AES256-CBC.</p>
Compression	<p>Traffic compression: Automatic (1), enabled (yes) or disabled (no).</p>

(1) In Automatic mode, the VPN Client will automatically adapt to the gateway's parameters.

Extra HMAC (TLS-Auth)

Enabled	<p>This option adds an authentication layer to the packets exchanged between the VPN Client and the VPN gateway. For this option to be fully operational, it must also be configured for the gateway (on gateways, this option is often referred to as "TLS-Auth").</p>
---------	---

If this option is activated, a key must be typed in the field below the ticked box. The same key must also be typed in the gateway. It consists of a string of hexadecimal characters, in the following format:

```
-----BEGIN Static key-----
362722d4fbff4075853fbe6991689c36
b371f99aa7df0852ec70352122aee7be
...
515354236503e382937d1b59618e5a4a
cb488b5dd8ce9733055a3bdc17fb3d2d
-----END Static key-----
```

“Key direction” must also be defined

Key Direction	<ul style="list-style-type: none"> - BiDir: The specified key is used both ways (default mode) - Client: The gateway’s key direction must be defined as “Server” - Server: The gateway’s key direction must be defined as “Client”
---------------	---

Dead Peer Detection (DPD)

The DPD (Dead Peer Detection) function enables both endpoints of the tunnel to mutually make sure the other one is there.

The DPD function is activated once the tunnel is open. When linked to a redundant gateway, DPD allows the VPN Client to switch automatically between gateways when one of them is unavailable.

Ping Gateway	Period, expressed in seconds, between two “pings” sent by the VPN Client to the gateway. By this, the VPN Client confirms to the gateway that it is still active.
Detect Gateway	Time, expressed in seconds, after which the gateway is considered down if no “ping” has been received.
On Dead Peer Detection	When the gateway is detected as down (i.e. after the “gateway detection” time is up), the tunnel can be closed, or the VPN Client may try and reopen it.

Key Renegotiation

Bytes, Packets, Lifetime	<p>Keys can be renegotiated when any of three criteria (which can be combined) expire:</p> <ul style="list-style-type: none"> - Traffic volume, expressed in Ko - Quantity of packets, expressed in number of packets - Lifetime, expressed in seconds <p>If more than one criterion is set, keys will be renegotiated when the first of these expires.</p>
--------------------------	--

Tunnel Options

Physic. If MTU	<p>Maximum size of OpenVPN packets.</p> <p>Gives the possibility to set a packet size so that OpenVPN frames are not fragmented on the network level.</p> <p>The default value for MTU is 0, meaning that the software will use the physical interface’s MTU value.</p>
----------------	---

Tunnel MTU	<p>Virtual interface MTU.</p> <p>When the values are set, it is recommended that the tunnel's MTU value be lower than the one of the physical interface's MTU.</p> <p>The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface minus a fixed delta value.</p>
Tunnel IPv4	<p>Defines the VPN Client's behavior when receiving an IPv4 configuration from the gateway:</p> <ul style="list-style-type: none">- Automatic: Accepts the information sent by the gateway- Yes: Checks whether the information sent by the gateway matches the configured behavior. If not, a warning message is displayed on the console and the tunnel is not established.- No: Ignore

Tunnel Establishment Options

Port	<p>Port number used for establishing the tunnel. The default port value is 1194.</p> <p>The tunnel will use UDP.</p>
Retransmissions	<p>Number of protocol message resends.</p> <p>If no answer is received before this number is reached, the tunnel is closed.</p>
Authentication timeout	<p>Time allowed for establishing the authentication phase, at the end of which it will be assumed that the tunnel won't open. When this timeout is reached, the tunnel is closed.</p>
Traffic setup timeout	<p>Tunnel establishment phase: time after which the tunnel is closed if any of the steps hasn't been completed.</p>

7 Redundant Gateway

TheGreenBow iOS VPN Client allows you to configure a redundant VPN gateway.

The use of a redundant gateway can be coupled with the implementation of DPD. When the DPD feature of the VPN Client detects that the original gateway is unavailable, it will automatically switch to the redundant gateway.

Note: It is possible to configure the same gateway for the main gateway and the redundant gateway in order to benefit from the automatic re-open function with only one gateway.

The redundant gateway algorithm is the following:

1. The VPN Client contacts the original gateway to open the VPN tunnel.
2. If no tunnel can be opened after N retries (number of retries for the DPD function), then the VPN Client contacts the redundant gateway.

The same algorithm applies to the Redundant gateway: If the redundant gateway is unavailable, the VPN Client attempts to open the VPN tunnel towards the original gateway.

Note: The VPN Client does not try to contact the redundant gateway if the original gateway is available but there is an issue when opening the tunnel.

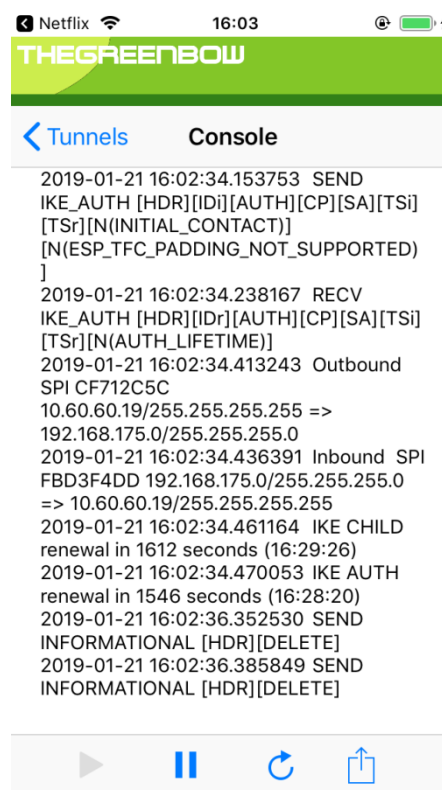
8 Console and Logs

TheGreenBow iOS VPN Client offers three types of logs:

1. The console log which provides information and steps about the opening and closing of tunnels (mostly IKE messages)
2. Trace mode logs that contain detailed information
3. System logs which logs general events like opening or closing tunnels

These logs are designed to help the network administrator to diagnose problems, or to help identify incidents by TheGreenBow support team.

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



8.1 Console

The Console window can be displayed as follows by clicking on the Console button at the bottom of the VPN Tunnel Tree.

The console logging can be paused and restarted with the corresponding buttons. The view can be refreshed, and the console log can be shared. When sharing, all other logs and the configuration (the set of all tunnels) will be exported.

8.2 Export

All logs and the tunnels can be exported using the share button in the Console view.

9 Specifications

9.1 Tunnels

- IPsec IKEv2
- SSL

9.2 Network

- Dead Peer Detection (DPD)
- Redundant gateway
- Configuration Payload: retrieve network configuration from gateway
- NAT-T support
- IKE Fragmentation

9.3 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), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (521) Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
Authentication	Pre-shared key Certificate EAP Multiple Auth

9.4 Languages

English

9.5 OS compatibility

The minimal version required to run TheGreenBow iOS VPN Client is iOS 13.0.

10Contact

10.1 Information

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

10.2 Sales

Phone: +33.1.43.12.39.30

Email: sales@thegreenbow.com

10.3 Support

Different pages concerning support are available on the TheGreenBow website:

Support

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

Online help

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

FAQ

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

Contact

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

11 Third-party licenses

```
/*
 * 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 with Netscapes 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 routines 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 publicly 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.]
*/
```

Secure, Strong, Simple
TheGreenBow Security Software