

TheGreenBow IPSec VPN Client

Benutzerhandbuch

Contact: support@thegreenbow.de

Website: www.thegreenbow.de

TheGreenBow IPSec VPN Client - Benutzerhandbuch

Property of TheGreenBow© - Sistech SA 2000-2005

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

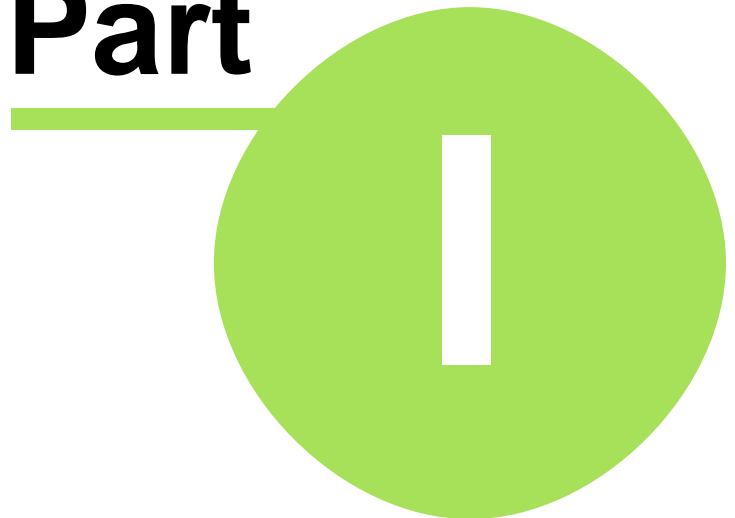
Printed: Oktober 2005 in (whereever you are located)

Table of Contents

Part I TheGreenBow VPN Client Version 3.0	4
1 TheGreenBow VPN Client Übersicht	4
2 Multi VPN Gateway Lösung	4
3 Linux IPSec Appliance Support	4
4 TheGreenBow VPN Client Features	5
5 OEM und Software Customisierung	5
Part II Installation des TheGreenBow VPN Client	7
1 Software Installation	7
2 Software Evaluierung	8
3 Aktivierungsassistent	8
Aktivierung in 2 Schritten	8
Schritt 1 von 2: Eintragen der Lizenznummer	8
Schritt 2 von 2: Online Aktivierung	9
Aktivierungsfehler	10
4 Software Deinstallation	11
Part III Benutzerinterface	13
1 Benutzerinterface - Übersicht	13
2 Taskleistensymbol	13
3 Hauptfenster	14
4 Hauptmenüleiste	15
5 Statusleiste	15
6 Fenster "Über"	16
7 Benutzerinterface verbergen	16
8 Assistenten	16
9 Präferenzen	17
Part IV VPN Konfiguration	19
1 Konfigurationsassistent	19
Konfiguration in 3 Schritten	19
Schritt 1 von 3: Remote Einstellungen	19
Schritt 2 von 3: VPN Tunnel Parameter	20
Schritt 3 von 3: Zusammenfassung	21
2 VPN Tunnel Konfiguration	21
VPN Tunnel einrichten	21
Mehrere Tunnel oder Phasen	22
Erweiterte Features	22
3 Authentifizierung oder Phase 1	22
Was ist die Phase 1	22
Phase 1 Grundeinstellungen	23
Phase1 Erweiterte Einstellungen	24
Erweiterte Einstellungen der Phase 1.....	24

4 IPsec Konfiguration oder Phase 2	26
Was ist Phase 2	26
Phase 2 Settings Description	26
Phase2 Erweiterte Einstellungen	27
Erweiterte Einstellungen der Phase 2.....	27
5 Globale Parameter	28
Globale Einstellungen	28
6 VPN Tunnel Übersicht	30
Übersicht der Tunnelverbindungen	30
7 USB Stick Modus	31
Was ist der USB Stick Modus	31
USB Stick Modus einrichten	31
Konfiguration übertragen	32
USB Stick Auto Tunnel	32
8 Verwaltung von Zertifikaten	33
Weiterführende Informationen	33
Konfiguration mit Zertifikaten	33
9 Konfigurationsmanagement	34
Import und Export der Konfigurationsdaten	34
10 Management Tools für Administratoren	35
Tool Übersicht	35
VPN Client stoppen	35
Konfiguration importieren	35
VPN Start Modus	36
VPN Hide Modus	36
11 Zusätzliche Supportdokumente	36
Part V Konsole und Protokollfunktionen	38
1 Die Konsole	38
2 Filter	39
Part VI Fehlerbehebung	41
Part VII Kontakt	43

Part



TheGreenBow VPN Client Version 3.0

1 TheGreenBow VPN Client Version 3.0

1.1 TheGreenBow VPN Client Übersicht

Speziell für mobile oder Telearbeitsplätze konzipiert, bietet der TheGreenBow® VPN Client eine softwarebasierte IPSec Lösung, welche sichere Verbindungen in Unternehmensnetzwerke über das Internet gewährleistet. Im Gegensatz zu hardwareabhängigen Lösungen ist der TheGreenBow® VPN Client kompatibel zu allen gängigen IPSec VPN Gateways.

Die TheGreenBow® Software bietet ein umfassendes Konfigurationsinterface. Das Einrichten eines Virtual Private Networks wird zum Kinderspiel...

1.2 Multi VPN Gateway Lösung

Unser Ziel ist, so viele IPSec VPN Router, Gateways und Appliances wie möglich zu unterstützen. Unsere IKE Implementierung basiert auf OpenBSD 3.1 (ISAKMPD), daher ist schon jetzt unser TheGreenBow® IPSec VPN Client eine der flexibelsten Lösungen am Markt. Hier eine [Liste der unterstützten VPN Gateways](#).

1.3 Linux IPSec Appliance Support

TheGreenBow® unterstützt verschiedene Linux IPSec VPN Implementierungen wie z.B. StrongS/WAN und FreeS/WAN. Daher ist unser VPN Client kompatibel zu den meisten IPSec Router / Appliances, welche auf diesen Implementierungen basieren. Hier eine vollständige [Liste der unterstützten Systeme](#).

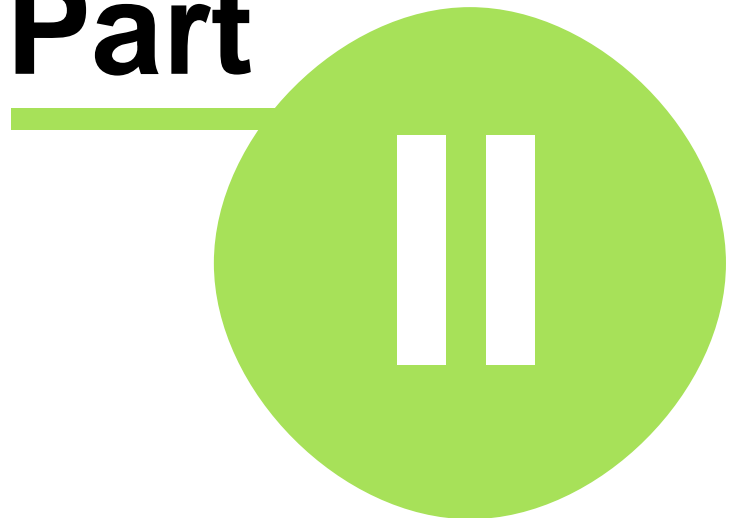
1.4 TheGreenBow VPN Client Features

Windows Versionen	Win98, Me, NT, Win2000, WinXP
Verbindungsarten	Peer-to-Peer VPN , "Point to multiple" Modus ohne Gateway oder Server. Alle Verbindungsarten wie z.B. DFÜ, Dial up, ISDN, DSL, Cable, GSM/GPRS und WiFi werden unterstützt.
Unterstützte Protokolle	Voller IKE Support: IKE Implementierung basierend auf OpenBSD 3.1 (ISAKMPD) Voller IPSec Support: <ul style="list-style-type: none"> • Main Mode and Aggressive Mode • MD5 und SHA Hash Algorithmen • IKE Port variabel
NAT Traversal	NAT Traversal Draft 1 (erweitert), Draft 2 und 3 (volle Implementierung) <ul style="list-style-type: none"> • Umfasst NAT_OA Support • Umfasst NAT Keepalive • Umfasst NAT T Aggressive Mode
Verschlüsselung	3DES, DES und AES 128/192/256 Bit Verschlüsselung. Erweiterte Features wie DH1536, DH2048 und RSA 2048 werden unterstützt.
Benutzer Authentifizierung	<ul style="list-style-type: none"> • X-AUTH Support • PreShared Keys und X509 Zertifikate. Kompatibel zu den meisten IPSec Gateways am Markt. • DH Gruppen 1, 2, 5 und 14 (z.B. 768, 1024, 1536 und 2048) • Flexible Zertifikatsunterstützung (PEM, PKCS12, ...)
Dead Peer Detection (DPD)	DPD ist eine Internet Key Exchange (IKE) Erweiterung (i.e. RFC3706) zur Erkennung von toten Verbindungen.
Redundant Gateway	Redundant Gateway bietet eine hoch skalierbare und ausfallsichere Verbindung in ein Remote Netzwerk. Das Redundant Gateway Feature erlaubt dem TheGreenBow VPN Client einen IPSec Tunnel zu einem alternativen Gateway (Fail Over) aufzubauen, wenn das primäre VPN Gateway ausgefallen ist oder nicht antwortet.
Mode Config	"Mode Config" ist eine Internet Key Exchange (IKE) Erweiterung welche es dem IPSec VPN Gateway ermöglicht, Konfigurationsinformationen des LAN an Remote User (z.B. an den IPSec VPN Client) weiterzuleiten.
USB Stick	VPN Konfigurations- und Sicherheitselemente (Zertifikate, Preshared Key,&) können auf einem USB Stick abgespeichert werden, um sensible Informationen physikalisch vom Rechner des Benutzers zu trennen.
Log Konsole	Alle Phasen und Aktionen der Tunnelverbindung können über die Konsole protokolliert werden.
Verborgenes User Interface	Silent Install und ein Verbergen der grafischen Benutzeroberfläche ermöglichen eine Implementierung ohne dass die Endbenutzer Konfigurationsdaten verändern können.
Live Update	Inkrementelle Patches erlauben Aktualisierungen ohne Systemreboot.

1.5 OEM und Software Customisierung

Für OEM Partner und Systemintegratoren / Hersteller bieten wir Lösungen wie z.B. Customisierung, Branding oder Lokalisierung rund um den TheGreenBow® VPN Client.

Part



Installation des TheGreenBow VPN Client

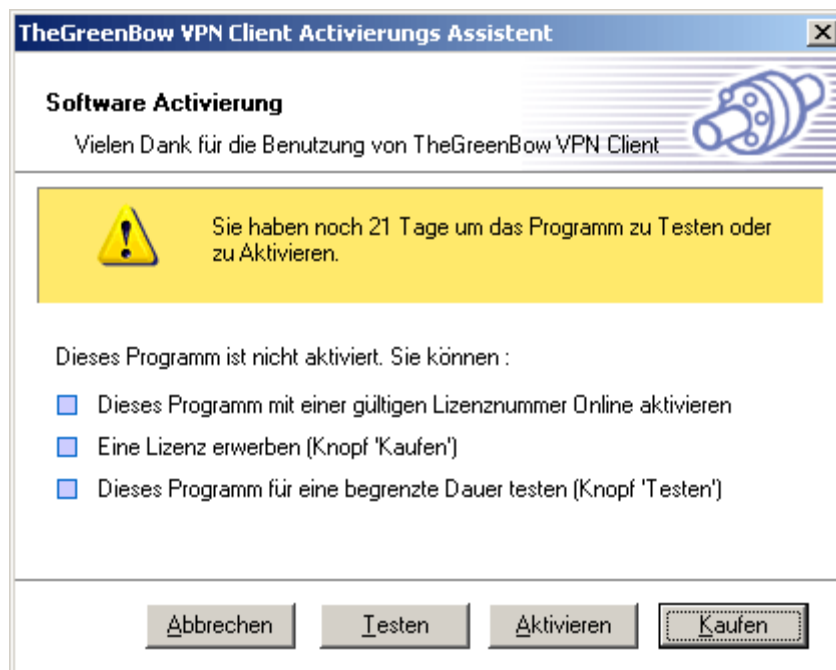
2 Installation des TheGreenBow VPN Client

2.1 Software Installation

Der TheGreenBow VPN Client verfügt über eine klassische Windows Installationsroutine. Sie können während der Installation den Installationspfad manuell auswählen. Nach erfolgreicher Installation ist ein Neustart der Rechners erforderlich.

Nach Neustart des Rechners und der Windows Anmeldung erscheint ein Fenster zur Auswahl verschiedener Optionen:

- "Abbrechen" schließt das Fenster und die Anwendung.
- "Testen" erlaubt die weitere Evaluierung der Applikation. Der verbleibende Testzeitraum wird in der gelben Box angezeigt.
- "Aktivieren" schaltet die Applikation über die Online Registrierung frei. Hierzu wird ein Lizenzschlüssel benötigt. Bei Klicken auf den "Aktivieren" Button, startet der Aktivierungsassistent.
- "Kaufen" führt Sie zu dem TheGreenBow Online Shop.



Achtung: Unter Windows NT, 2000 and XP sind Administratorrechte erforderlich. Sind Sie nicht als Administrator angemeldet stoppt die Installation nach der Auswahl der Sprache mit einer Fehlermeldung.

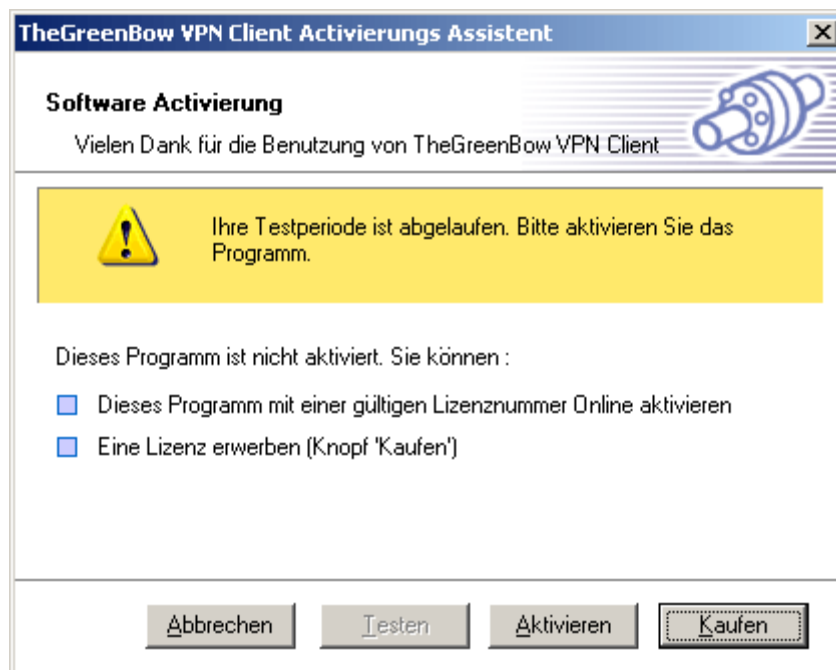
Shortcuts: Nach Installation der Software kann das VPN Konfigurationsinterface geöffnet werden:

- vom Desktop mit Doppelklick auf die TheGreenBow VPN Verknüpfung
- über das VPN Client Icon in der Taskleiste
- über Start > Programme > TheGreenBow > VPN > TheGreenBow VPN

2.2 Software Evaluierung

Sie können unseren voll funktionsfähigen VPN Client 30 Tage lang unverbindlich testen. Alle Features und Optionen stehen Ihnen in dieser Testversion uneingeschränkt zur Verfügung. Klicken Sie hierzu auf den Button 'Testen' nach Starten des VPN Clients. Im Demo Modus erscheint das Testversion-Fenster nach jedem Windows Start.

Ist der Testzeitraum abgelaufen, wird der Button "Testen" deaktiviert.



2.3 Aktivierungsassistent

2.3.1 Aktivierung in 2 Schritten

Der Aktivierungsassistent dient zur Aktivierung und Freischaltung der Software online. Die Aktivierung erfordert einen Lizenzschlüssel. Geben Sie Ihre Lizenznummer und Ihre eMail Adresse ein. Diese Angaben werden benötigt, um Ihnen die Aktivierungsinformationen zusenden zu können.

Der Aktivierungsassistent kann gestartet werden:

- Über einen Klick auf '?' und dann einen Klick auf "Activation Wizard...".
- Über einen Klick auf den 'Aktivieren' Button im Startfenster des VPN Client.

2.3.2 Schritt 1 von 2: Eintragen der Lizenznummer

Die Aktivierung erfordert einen Lizenzschlüssel. Geben Sie Ihre Lizenznummer und Ihre eMail Adresse ein. Diese Angaben werden benötigt, um den VPN Client freischalten zu können.

TheGreenBow VPN Client Aktivierungsassistent Schritt 1 von 2

Lizenz Nummer

Um dieses Programm zu aktivieren, bitte Lizenznummer und gültige eMail Adresse eingeben :

Lizenz Nummer - - - ▶ [Format](#)

eMail Adresse
(z.B. mail@company.com)

Die Bestätigung der Lizenzaktivierung wird an diese eMail Adresse geschickt. Bitte überprüfen Sie die Richtigkeit dieser Adresse.

< Zurück Weiter >

Ab der Version 3.0 des VPN Clients ist das Format der Lizenzschlüssel ein 24stelliger String, unterteilt in 4 Blöcke. Ältere Lizenzschlüssel haben ein 20stelliges Format. Klicken Sie auf "Format", wenn sie über einen älteren Lizenzschlüssel verfügen und die Software aktualisieren wollen.

TheGreenBow VPN Client Aktivierungsassistent Schritt 1 von 2

Lizenz Nummer

Um dieses Programm zu aktivieren, bitte Lizenznummer und gültige eMail Adresse eingeben :

Lizenz Nummer ▶ [Format](#)

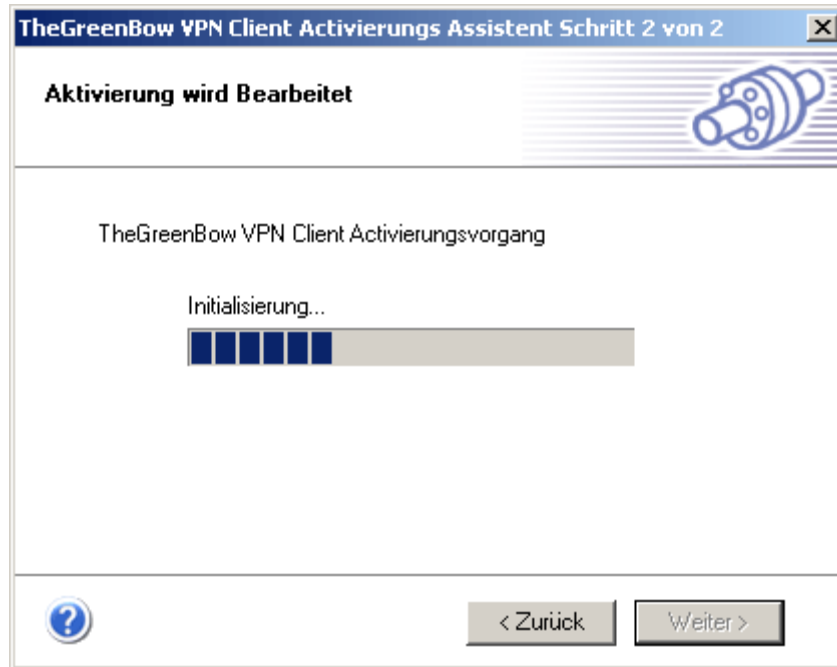
eMail Adresse
(z.B. mail@company.com)

Die Bestätigung der Lizenzaktivierung wird an diese eMail Adresse geschickt. Bitte überprüfen Sie die Richtigkeit dieser Adresse.

< Zurück Weiter >

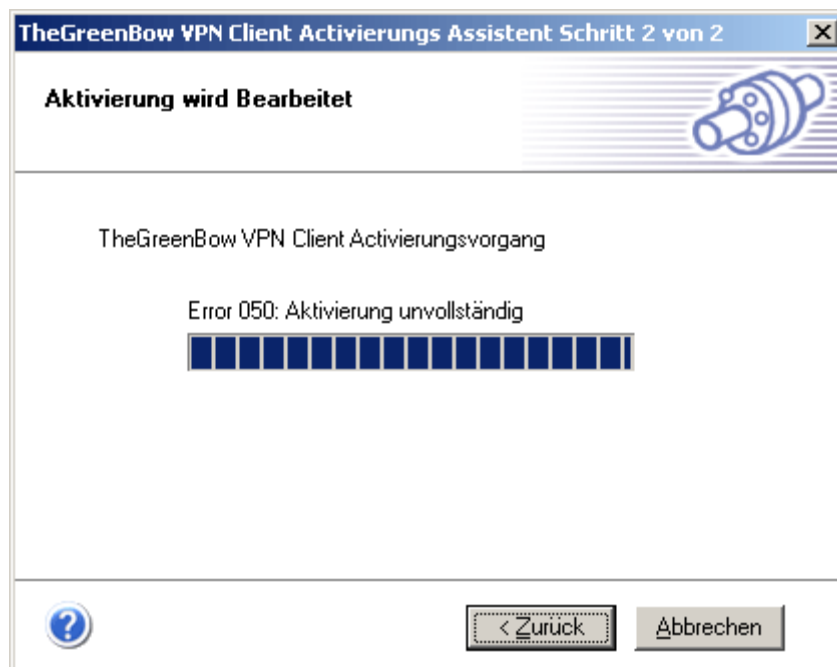
2.3.3 Schritt 2 von 2: Online Aktivierung

Der 'Aktivierungsassistent' konnektiert sich automatisch zu dem Online Aktivierungsserver und schaltet die Client Lizenz frei. Sie können diese Schritte beliebig wiederholen, um den Lizenzschlüssel zu ändern.



2.3.4 Aktivierungsfehler

Falls während der Registrierung und Freischaltung ein Fehler auftritt, meldet die Software einen Fehlercode zurück. Über den Button "Hilfe" erhalten Sie weitere Informationen über die Fehlerursache.



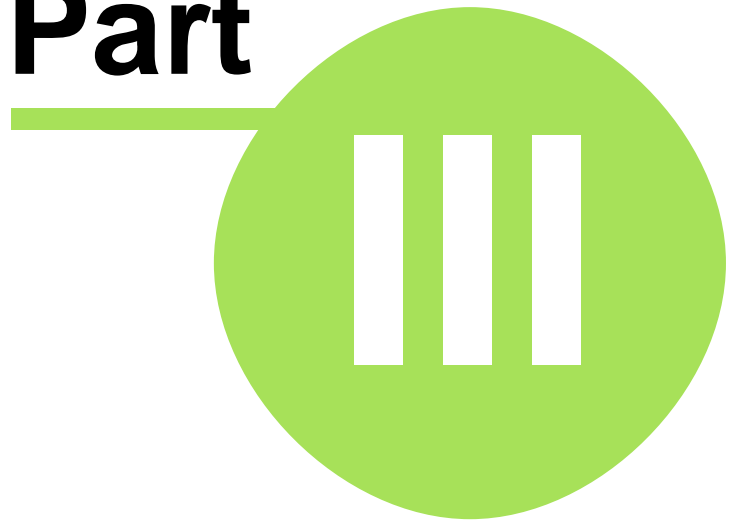
Fehlercode	Fehlermeldung	Erklärung
Error 001	License not found	License number doesn't exist in the activation server database. There must be an error in entering the license number. Also some old licenses are 20 digits only while new licenses are 24 digits.
Error 002	Reserved	Reserved
Error 003	Activation quota exceeded	Too many installations and activations have been processed for this specific license number. License numbers can not be used more than allowed by your IT department.
Error 004	Wrong product code	The License number you've entered is not allowed on this software product. This software product requires a specific license number that is provided by the distributor of this software.
Error 050	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation
Error 051	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation
Error 052	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation
Error 053	Cannot connect activation server	The activation server can't be contacted. Reasons can be broken Internet connection, activation server down, firewall and security policies.
Error 054	Cannot connect activation server	The activation server can't be contacted. Reasons can be broken Internet connection, activation server down, firewall and security policies.
Erreur 055	Activation code error	Activation code might have been modified after activation.

2.4 Software Deinstallation

Der TheGreenBow IPsec VPN Client kann wie folgt deinstalliert werden:

- über die Windows Systemsteuerung > Software > Neue Software hinzufügen
- über Start > Programme > TheGreenBow > VPN > VPN Client deinstallieren

Part



Benutzerinterface

3 Benutzerinterface

3.1 Benutzerinterface - Übersicht

Der TheGreenBow VPN Client kann völlig autonom agieren und kann ohne Benutzereingriffe IPSec Tunnel starten bzw. stoppen. Dies erfordert jedoch eine initiale Grundkonfiguration.

Die Konfiguration wird über eine Konfigurationsdatei eingelesen. Die Benutzeroberfläche erlaubt das Anlegen, Editieren, Speichern, Importieren und Exportieren der Konfigurationsdatei samt Sicherheitselemente (Preshared Key, Zertifikate, ...).

das Benutzerinterface besteht aus mehreren Elementen:

- [Icon in der Taskleiste \(Taskleistensymbol\)](#)
- [Hauptfenster](#)
- [Hauptmenüleiste](#)
- [Statusleiste](#)
- [Assistenten](#)
- [Präferenzen](#)

3.2 Taskleistensymbol

Die Benutzeroberfläche des TheGreenBow VPN Client kann via Doppelklick des Programmicons auf dem Desktop, über das Windows Startmenü oder über einen Klick auf das Icon in der Taskleiste gestartet werden. Ist der Client gestartet, zeigt das Icon durch seine Farbe an, ob ein Tunnel geöffnet ist.



Das Icon kann folgende Farbcodierung haben:

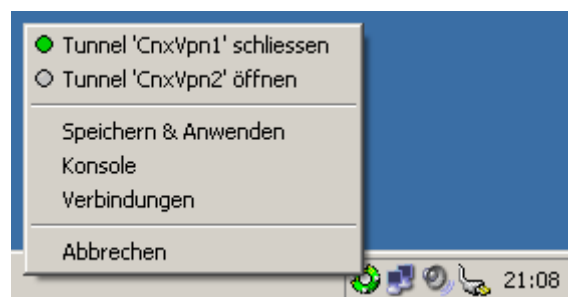


Blaues Icon: Kein Tunnel ist geöffnet



Grünes Icon: Mindestens ein Tunnel ist geöffnet

Ein Linksklick auf das Icon öffnet die Benutzeroberfläche.



Ein Rechtsklick auf das Icon öffnet ein Kontextmenü:

- Speichern & Anwenden schließt aktive VPN Tunnel, aktualisiert (reinitialisiert) vorgenommene Änderungen an der Konfiguration und startet vorhandene VPN Tunnel neu.

- Konsole führt zu erweiterten Funktionen wie z.B. Logfiles zur Fehlerbehebung / Analyse
- Verbindungen öffnet eine Liste der aktiven Verbindungen (geöffnete Tunnel).
- Abbrechen schließt alle aktiven VPN Tunnel und schließt ggfs. die Benutzeroberfläche.
- Eine Liste der konfigurierten Tunnel. Diese können hier geöffnet oder geschlossen werden.

Tooltips beim Überfahren des Icons mit der Maus zeigen den Status des VPN Tunnel:

- "Tunnel <Tunnel Name>" wenn mehr als ein Tunnel aktiv ist.
- "Wait VPN ready..." wenn der IKE Dienst reinitialisiert.
- "TheGreenBow VPN Client" wenn der Client bereit ist, aber keine VPN Tunnel geöffnet sind.

3.3 Hauptfenster

Das Hauptfenster besteht aus mehreren Elementen:

- Drei Buttons 'Konsole', 'Parameter' und 'Verbindungen' (linke Spalte)
- Ein Tree List Fenster (linke Spalte) mit den IKE und IPsec Konfigurationsdaten
- Ein Konfigurationsfenster (rechte Spalte) mit der in der linke Tree List zugeordneten Security Association (SA) für die Phasen 1 und 2).



3.4 Hauptmenüleiste

Im Hauptmenü finden sich folgende Optionen:

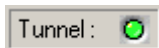
- 'Datei' - Importieren / Exportieren der Konfigurationsdatei. Über dieses Menü kann eine VPN Konfiguration von einem beliebigen Ort (Server, Festplatte, USB Stick...) importiert oder exportiert werden.
- 'Konfiguration' enthält alle den Zugriff auf die Security Associations (Phase 1 und 2).
- Über 'VPN Konfiguration' erhalten Sie ebenfalls Zugriff auf den Konfigurationsassistenten.
- Tools enthält Zugriff auf die Konsole und die Verbindungsauswahl.
- '?' enthält den Zugriff auf die Online Hilfe.

3.5 Statusleiste

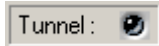
Die Statusleiste enthält mehrere Informationen:



- Die USB Token Box (links) zeigt an, ob der USB Stick Modus aktiviert ist. Erscheint hier 'USB', sind die Sicherheitselemente (Preshared Key, Zertifikate, ...) auf einem USB Stick physikalisch geschützt
- Die mittlere Box zeigt den aktuellen Status des VPN Clients an. Z.B. VPN Tunnel aktiv, VPN Konfiguration speichern, ...
- Das farbige Icon (rechts) zeigt den Status der Tunnel an:



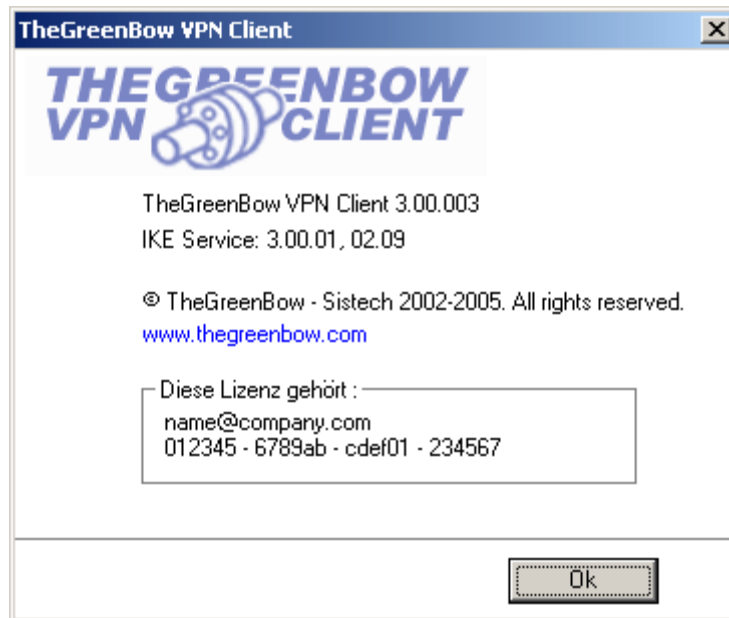
Grünes Icon: Mindestens ein Tunnel ist geöffnet und aktiv.



Graues Icon: Client aktiv, keine Tunnel geöffnet.

3.6 Fenster "Über"

Im Fenster 'Über' finden Sie Informationen zur Versions- und Revisionsnummer. Auch enthält es Angaben zu Ihrer Lizenz.

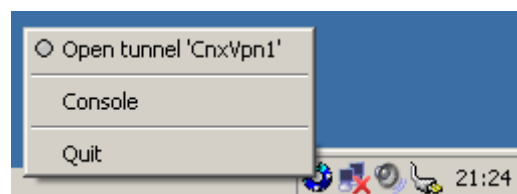


Die Versionsnummer hier in diesem Beispiel ist 3.00, die Revisionsnummer ist 003.

3.7 Benutzerinterface verbergen

Die grafische Benutzeroberfläche mit den Konfigurationsoptionen kann vor Endanwendern verborgen werden. Hierfür stellen wir ein Konfigurationstool VPNHide zur Verfügung. Dadurch können IT Manager oder Administratoren Änderungen an der Konfiguration durch Endanwender wirksam unterbinden.

Ist VPNHide aktiv, können die Konfigurationsoptionen durch den Anwender nicht aufgerufen oder verändert werden. Nur der Zugang zur Konsole, das Schließen des Clients und das Öffnen oder Beenden der Tunnels ist dann noch möglich.



3.8 Assistenten

Es stehen 2 Assistenten zur Verfügung:

- Der "VPN Konfigurationsassistent" kann über das Menü 'VPN Konfiguration' > 'Konfigurationsassistent' gestartet werden.

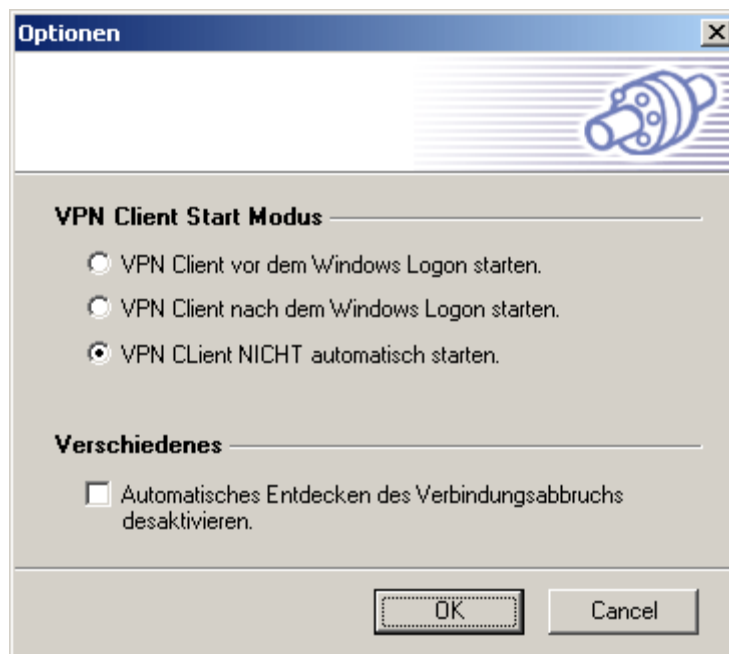
- Der "Aktivierungsassistent" kann über das Menü '?' > 'Aktivierungsassistent' gestartet werden.

3.9 Präferenzen

Das Fenster "Optionen" erlaubt folgende Einstellungen:

- Start Modus der Software
- Aktivieren bzw. Deaktivieren der Verbindungsabbruchserkennung

Die Präferenzen sind über das Menü 'Datei' -> 'Präferenzen' erreichbar.



VPN Client Start Modus

Über das Tool VPNStart.exe kann der Startmodus des TheGreenBow Clients bestimmt werden:

- Start vor der Windows® Anmeldung (Vor Logon).
- Start bei Windows® Anmeldung (Nach Logon).
- Manuell (Client wird nicht automatisch gestartet).

Verschiedenes

Ein automatisches Entdecken von Verbindungsabbrüchen deaktivieren erlaubt dem VPN Client, den Tunnel trotz Verbindungsabbrüchen geöffnet zu halten. Dies ist häufig bei instabilen Verbindungen wie z.B, Wifi, GPRS oder GSM hilfreich.

Part



VPN Konfiguration

4 VPN Konfiguration

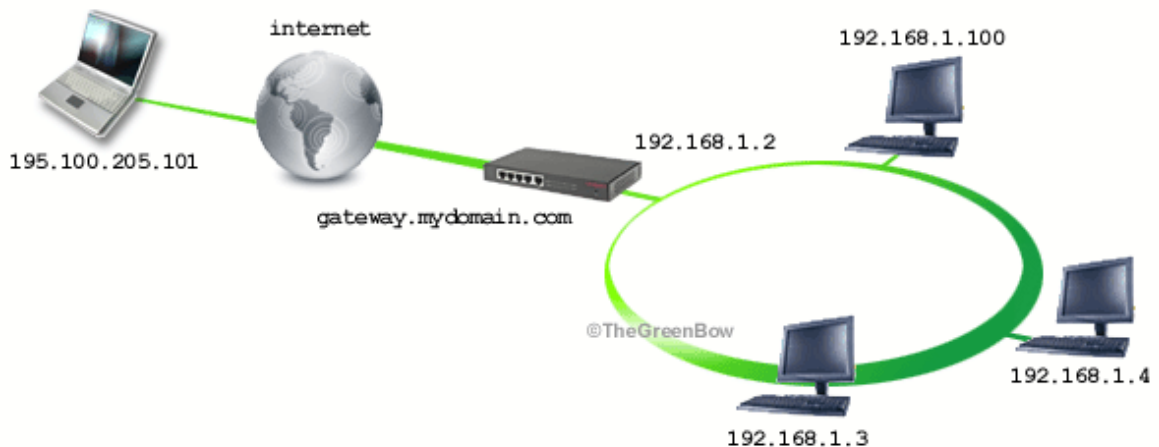
4.1 Konfigurationsassistent

4.1.1 Konfiguration in 3 Schritten

Der Konfigurationsassistent des TheGreenBow IPsec VPN Client ermöglicht die Konfiguration in 3 einfachen Schritten. Der Assistent unterstützt Sie bei der Einrichtung des Remote Computers, der sich über ein VPN Gateway in ein Firmennetzwerk (LAN) verbinden soll.

Hier ein Beispiel:

- Der Remote Computer (mit dem VPN Client) bezieht eine dynamische IP Adresse vom ISP.
- Der Remote Computer soll auf ein Firmennetzwerk hinter einem VPN Gateway (externe Adresse 'gateway.mydomain.com'.) zugreifen.
- Die IP Range des Firmennetzwerks ist 192.168.1.xxx, der Rechner auf welchen zugegriffen werden soll, hat beispielsweise die IP 192.168.1.100.



Zur Verbindungseinrichtung, öffnen Sie den Assistenten über das Menü 'VPN Konfiguration > Assistent'.

4.1.2 Schritt 1 von 3: Remote Einstellungen

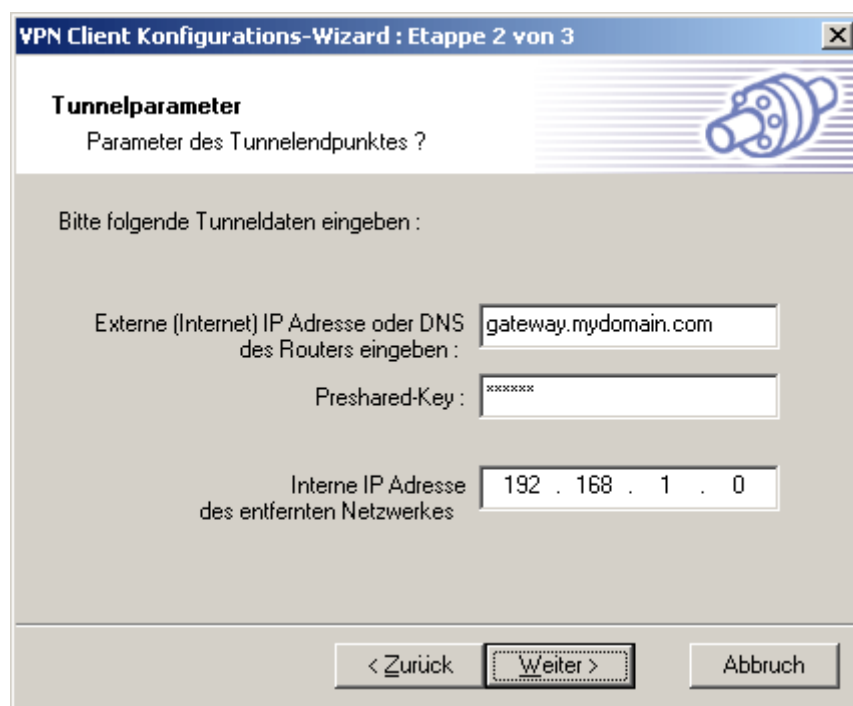
Hier wird der Typ des VPN Endpunktes angegeben.



4.1.3 Schritt 2 von 3: VPN Tunnel Parameter

Hier können Sie folgende Informationen hinterlegen:

- Die externe IP oder DNS Namen des zu erreichenden VPN Gateways
- Den Preshared Key für diese Tunnelverbindung (Der Preshared Key muss mit dem auf dem VPN Gateway hinterlegten Schlüssel übereinstimmen).
- Die interne IP Adresse des Netzwerks (LAN) hinter dem VPN Gateway (z.B. 192.168.1.0)



4.1.4 Schritt 3 von 3: Zusammenfassung

Im dritten Schritt sehen Sie eine Zusammenfassung der hinterlegten Einstellungen. Weitere Parameter wie z.B. Zertifikate, Verschlüsselung, virtuelle IP Adressen usw. können Sie über das Hauptfenster des VPN Client einstellen.

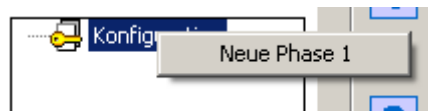


4.2 VPN Tunnel Konfiguration

4.2.1 VPN Tunnel einrichten

Um einen VPN Tunnel einzurichten gehen Sie bitte wie folgt vor:

Klicken Sie mit der rechten Maustaste auf den Eintrag "Konfiguration" und wählen Sie "Neue Phase 1"



Konfigurieren Sie die Authentisierung oder Phase 1 (**Phase 1**)
Klicken Sie mit der rechten Maustaste auf den Eintrag "Neue Phase 1" und wählen Sie "Neue Phase 2"



Konfigurieren Sie IPSec oder Phase 2 (**Phase 2**)
Nach einstellen der Parameter klicken Sie bitte auf "Regeln anwenden" um die neue Konfiguration zu aktivieren und den IKE Dienst neu zu starten.

Klicken Sie auf "Tunnel öffnen" um den IPSec VPN Tunnel zu öffnen.

Informationen zu den Parametern der [Phase 1](#) und [Phase 2](#)

4.2.2 Mehrere Tunnel oder Phasen

Sie können mit dem TheGreenBow IPSec VPN Client mehrere Tunnel verwalten.

Mehrere Authentisierungsphasen (Phase 1) können angelegt werden, sodass Sie Verbindungen zu verschiedenen VPN Gateways oder anderen Rechnern (Peer-to-Peer) aufbauen können. Ebenfalls können Sie mehrere IPSec Konfigurationen (Phase 2) innerhalb einer Authentisierungsphase (Phase 1) einrichten.

4.2.3 Erweiterte Features

Erweiterte Features können in den Phasen 1 und 2 definiert werden.

In Phase 1 (Einstellungen vererben ihre Gültigkeit zu der entspr. Phase 2):

- Aktivieren/Deaktivieren des [Config Mode](#)
- Aktivieren/Deaktivieren des [NAT-T Agressive Mode](#)
- Aktivieren/Deaktivieren des [Redundant Gateway](#) Features
- Einstellen des [IKE Port](#)
- [X-Auth Login/Password](#) mit PopUp Option einstellen

In Phase 2:

- [Tunnel automatisch starten](#)
- [Script/Application](#) Einstellungen
- Manuelle Einstellungen für [DNS/WINS](#) Server Adressen

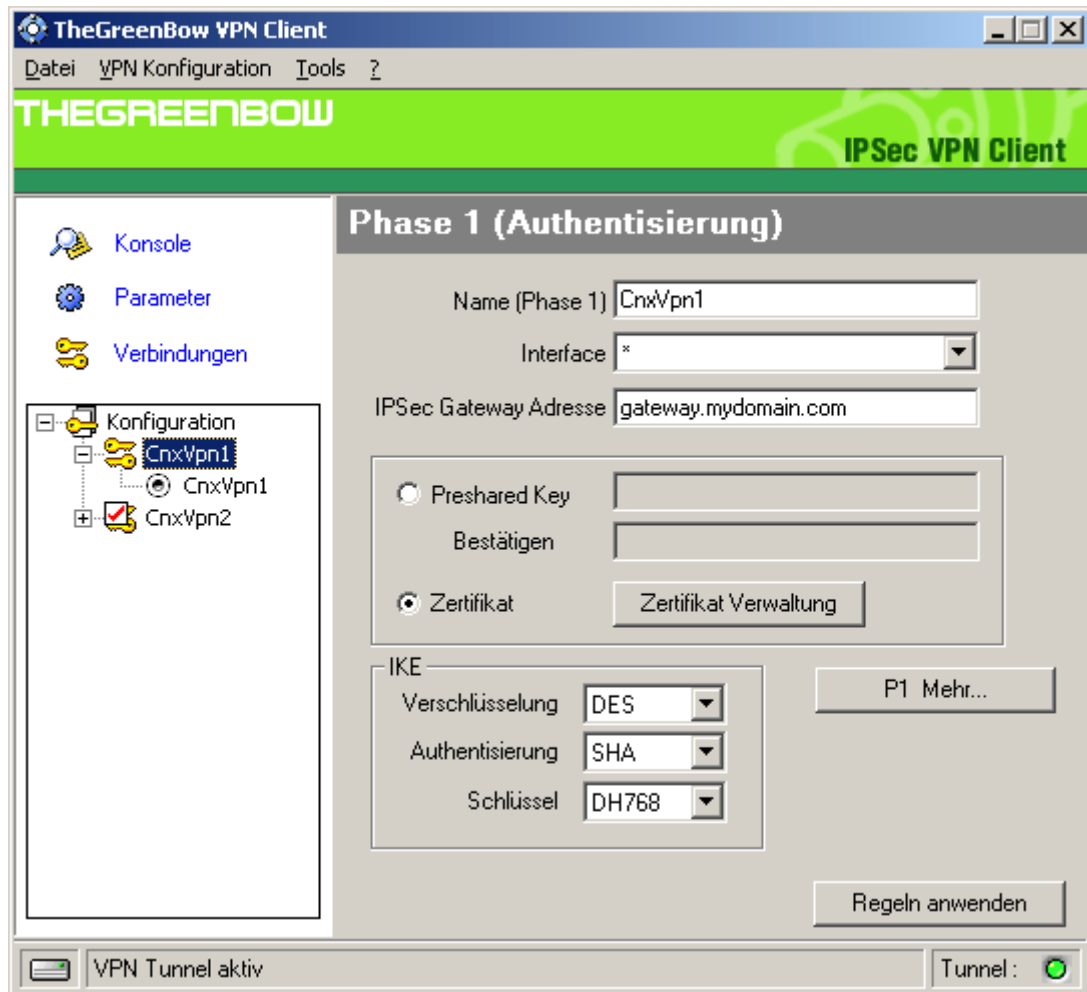
4.3 Authentifizierung oder Phase 1

4.3.1 Was ist die Phase 1

Das Authentisierung oder Phase 1 Fenster behandelt die Einstellungen zur Anmeldung an das VPN Gateway. Sie wird auch als IKE Negotiation bezeichnet.

In der Phase 1 werden die IKE (Internet Key Exchange) Richtlinien/Policies ausgehandelt, die Gegenstellen (Client und Gateway) identifiziert und ein sicherer Kanal zwischen beiden Parteien etabliert. Nun authentisieren sich Client und Gateway gegenseitig.

4.3.2 Phase 1 Grundeinstellungen



Name	Bezeichnung für die Authentisierung oder Phase 1. Dieser Wert hat beschreibenden Charakter und kann frei gewählt werden. Er dient nur zur Identifizierung der im linken Fenster in im VPN Client Hauptfenster.
Interface	IP Adresse des Rechners, auf welchem der VPN Client installiert ist. Dies kann je nach Netzwerkumgebung eine interne (LAN) Adresse, oder eine vom ISP dynamisch oder statisch vergebene externe IP (WAN). Wählen Sie "*", wenn Sie sich in einem lokalen Netzwerk hinter einem NAT Router mit IPsec Pass Through befinden, und/oder Sie eine dynamische IP über Ihren ISP beziehen..
IPsec Gateway Adresse	IP oder DNS Adresse des VPN Gateways (Remote Endpunkt)
Preshared Key	Passwort oder Preshared Key des VPN Gateways
Zertifikat	X509 Zertifikat des VPN Clients (siehe auch Verwaltung von Zertifikaten).
IKE Verschlüsselung	Verschlüsselungsalgorithmus während der Authentisierungsphase (3DES, AES, ...).
IKE Authentisierung	Authentisierungsalgorithmus während der Authentisierungsphase (MD5, SHA, ...).
IKE Schlüssel	Diffie-Hellman Schlüssellänge

Erweiterte Einstellungen zur Phase 1 sind über den Button '[P1 Mehr...](#)' erreichbar.

4.3.3 Phase1 Erweiterte Einstellungen

4.3.3.1 Erweiterte Einstellungen der Phase 1

Erweiterte Einstellungen zur Phase 1 sind über den Button '[P1 Mehr...](#)' erreichbar.

Phase1 Mehr

IKE Optionen

Config Mode IKE Port

Aggressive Mode Redund.GW

X-Auth

X-Auth Popup Login

 Password

Lokale und Entfernte ID

ID Typ auswählen : ID eintragen :

Lokale ID

Entfernte ID

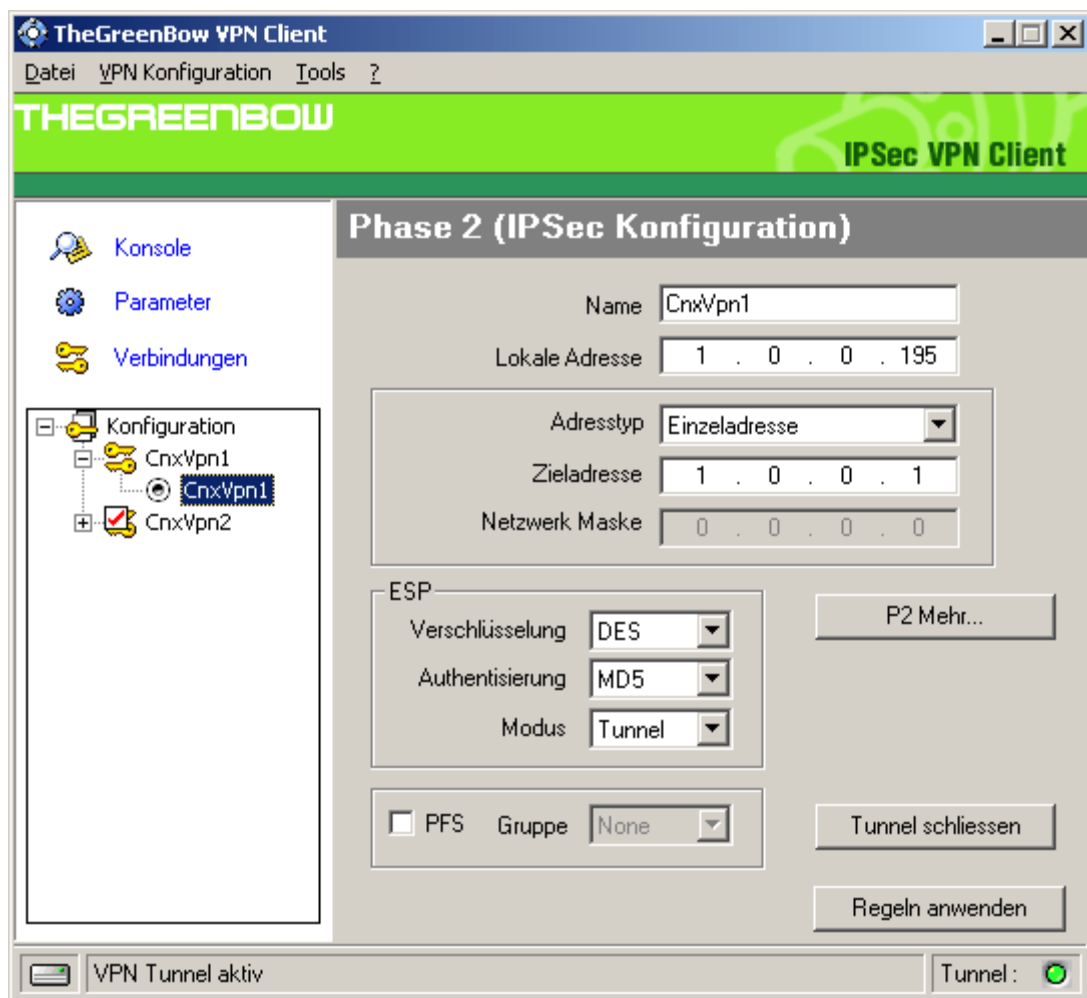
Config-Mode	Der Config Mode ermöglicht den VPN Client Informationen aus dem Zielnetz automatisch zu beziehen (z.B. DNS/WINS IP Adressen). Nicht alle VPN Gateways unterstützen den Config Mode, in der Phase 2 können jedoch DNS/WINS Server manuell eingegeben werden.
Aggressive Mode	Wenn aktiviert, nutzt der Client den Aggressive Modus um mit dem Remote Gateway zu kommunizieren.
Redundant GW	<p>Redundant Gateway Feature</p> <p>Diese Einstellung erlaubt, ein alternatives VPN Gateway zu definieren. Sie können hier IP oder DNS Namen eingeben.</p> <ul style="list-style-type: none">• Der TheGreenBow VPN Client kontaktiert das erste Hauptgateway um den Tunnel zu öffnen. Kann der Client nach 5 Versuchen das Hauptgateway nicht erreichen, wird der Tunnelaufbau über das Redundant Gateway versucht. Die Verzögerung zwischen den wiederholten Versuchen beträgt ca. 10 Sekunden.• Kann das Hauptgateway erreicht werden, jedoch der Tunnelaufbau gelingt z.B. durch Konfigurationsprobleme nicht, wird der Client keine Verbindung über das redundante Gateway versuchen. Hier arbeiten wir an einer Lösung für eine der nächsten Client Releases.• Ist ein Tunnel erfolgreich über das Hauptgateway aufgebaut, kann der VPN Client über das Dead Peer Detection Feature erkennen, wenn das Hauptgateway nicht mehr antwortet. In diesem Fall wird der Client sofort versuchen, eine Verbindung über das Redundant Gateway aufzubauen.• Dieses Verhalten gilt auch für das Redundant Gateway. Der VPN Client wechselt zwischen Haupt- und Redundant Gateway bis der User die Anwendung oder den Tunnel beendet.
IKE Port	UDP Port für IKE. Default Wert ist 500.
Local ID	<p>Über die lokale ID kann der VPN Client weitere Informationen zur Identifizierung an das VPN Gateway senden. Dies können folgende Werte sein:</p> <ul style="list-style-type: none">• Eine IP Adresse (Typ = IP Adresse), z.B. 195.100.205.101• Ein Domain Name (Typ = DNS), z.B. mydomain.com• Eine eMail Adresse (Typ = Email), z.B. support@thegreenbow.de• Eine numerische Zeichenkette (Typ = KEY ID), z.B. 123456• Ein Zertifikatsaussteller (Typ = DER ASN1 DN)• a certificate issuer (type=DER ASN1 DN) (siehe auch Verwaltung von Zertifikaten). Wird hier kein Wert eingetragen, wird die IP Adresse des VPN Clients verwendet.
Remote ID	<p>Die entfernte ID ist ein Wert, welche der VPN Client von VPN Gateway ur Identifizierung während der Phase 1 erwartet. Dies können folgende Werte sein:</p> <ul style="list-style-type: none">• Eine IP Adresse (Typ = IP Adresse), z.B. 195.100.205.101• Ein Domain Name (Typ = DNS), z.B. mydomain.com• Eine eMail Adresse (Typ = Email), z.B. support@thegreenbow.de• Eine numerische Zeichenkette (Typ = KEY ID), z.B. 123456• Ein Zertifikatsaussteller (Typ = DER ASN1 DN)• a certificate issuer (type=DER ASN1 DN) (siehe auch Verwaltung von Zertifikaten). Wird hier kein Wert eingetragen, wird die IP Adresse des VPN Gateways verwendet.
X-Auth	Aktiviert den X-Auth Verbindungsmodus. Wenn aktiviert fragt die X-Auth Funktion bei jedem Öffnen eines Tunnels nach Login und Passwort. Der Benutzer muss sich innerhalb 20 Sekunden anmelden, bevor die Anmeldung abbricht. Achtung: Nicht alle VPN Gateways unterstützen diese Funktion.

4.4 IPsec Konfiguration oder Phase 2

4.4.1 Was ist Phase 2

In der Phase 2 werden zwischen den Gegenstellen (VPN Client und Gateway) die IPsec Sicherheitselemente ausgetauscht. Ab hier wird nun die Kommunikation durch den Tunnel anhand der Sicherheitselemente verschlüsselt.

4.4.2 Phase 2 Settings Description



Name	Bezeichnung für die Authentifizierung oder Phase 1. Dieser Wert hat beschreibenden Charakter und kann frei gewählt werden. Er dient nur zur Identifizierung der im linken Fenster in im VPN Client Hauptfenster.
Lokale Adresse	Virtuelle IP Adresse, welche im Zielnetz (Remote Lan) verwendet wird. Wichtig: Diese Adresse darf nicht in der IP Range des Zielnetzes liegen (in Beispiel 192.168.1.10). Wählen Sie hier eine IP außerhalb des Zielnetzwerk, z.B. 192.168.123.123.
Adresstyp	Der Remote Endpunkt kann ein entferntes Netzwerk oder ein einzelner Computer. Möchten Sie einen Tunnel zu einem entfernten Netzwerk aufbauen, wählen Sie die Option "Subnet Adresse". Ist der Endpunkt ein einzelner Computer, wählen Sie hier "Einzeladresse".
Zieladresse	Abhängig von vom Adresstyp wird hier die Netzwerk IP des entfernten Netzes oder Einzeladresse des VPN Gateways eingetragen.
Netzwerk Maske	Die Subnetzmaske des entfernten Netzwerkes.
ESP Verschlüsselung	Verschlüsselungsalgorithmus der IPSec Phase (3DES, AES, ...)
ESP Authentisierung	Authentisierungsalgorithmus der IPSec Phase (MD5, SHA, ...)
ESP Modus	IPSec Encapsulation Modus : Tunnel oder Transport
PFS Gruppe	Diffie-Hellman Schlüssellänge.
Tunnel öffnen	Dieser Button öffnet den ausgewählten Tunnel direkt. Der Button ändert sich in "Tunnel schließen", sobald der Tunnel geöffnet ist.

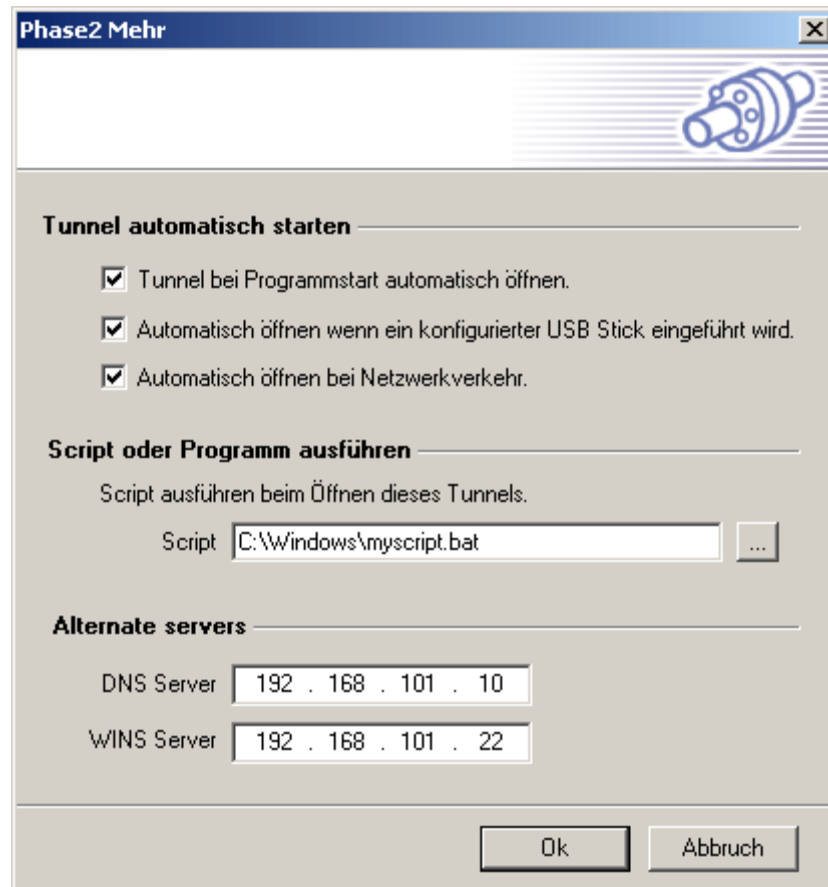
Erweiterte Einstellungen zur Phase 2 sind über den Button '[P2 Mehr...](#)' erreichbar.

Sind alle Parameter eingestellt, klicken Sie auf "Regeln anwenden" um die Konfiguration zu speichern und den IKE Dienst zu reinitialisieren. Auf unserer Webseite finden Sie [ausführliche Konfigurationsanleitungen zu vielen VPN Gateways](#).

4.4.3 Phase2 Erweiterte Einstellungen

4.4.3.1 Erweiterte Einstellungen der Phase 2

Erweiterte Einstellungen zur Phase 2 sind über den Button '[P2 Mehr...](#)' erreichbar.



Tunnel automatisch öffnen

- Der VPN Client kann automatisch den jeweiligen Tunnel öffnen (Phase2):
- Tunnel bei Programmstart öffnen
- Automatisch öffnen, wenn ein konfigurierter USB Stick eingeführt wird (siehe auch "[USB Modus](#)").
- Automatisch öffnen bei Netzwerkverkehr

Script oder Programm ausführen

Ein Script oder Programm (z.B. Outlook, CRM usw.) kann gestartet werden, wenn der Tunnel geöffnet ist.

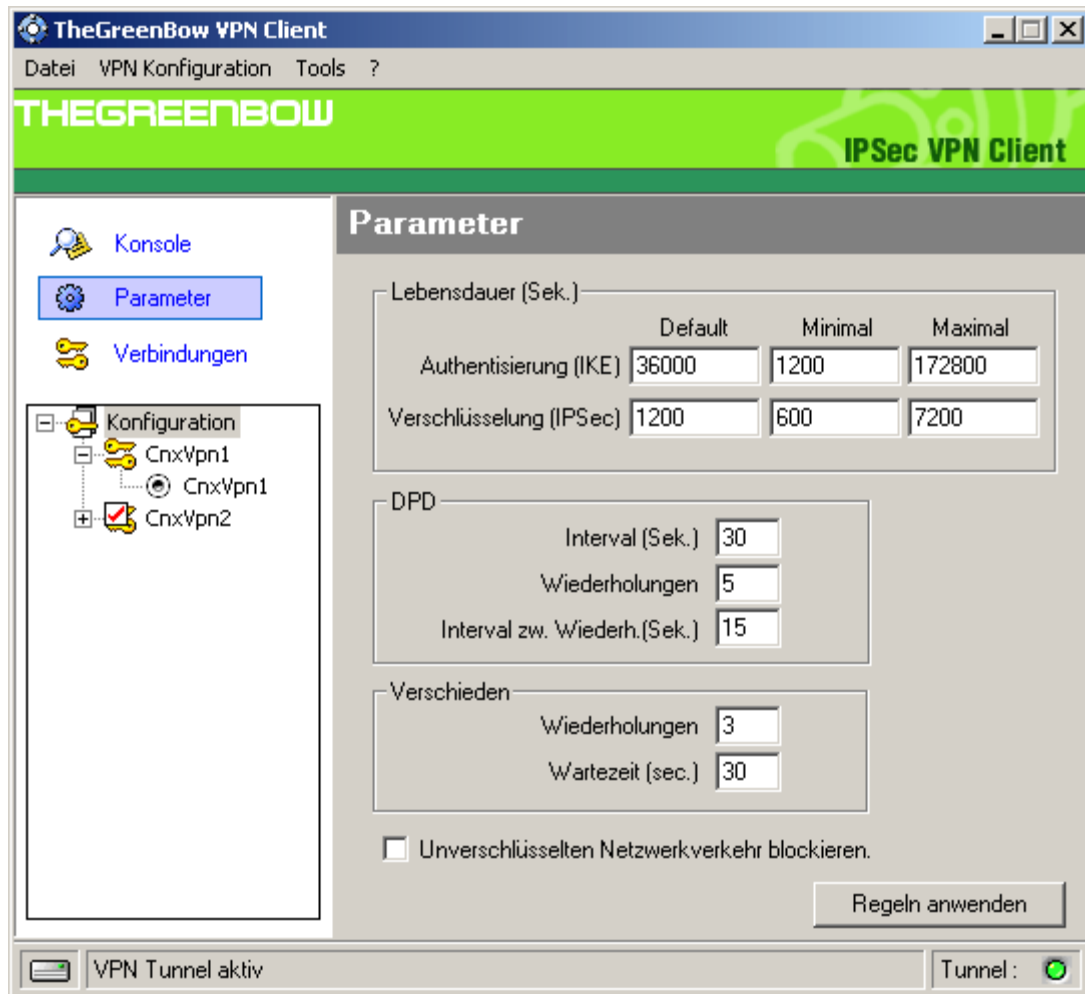
Alternate Servers

DNS und WINS Server IP Adressen des Remote Netzwerk können hier definiert werden.

4.5 Globale Parameter

4.5.1 Globale Einstellungen

Die globalen Einstellungen gelten für alle VPN Verbindungen und repräsentieren die üblichen Default Werte. Über den Button "Regeln anwenden" werden Änderungen übernommen.



- **Lebensdauer (Sec.)**
 - IKE Default lifetime** Zyklus bevor der IKE Schlüssel erneut ausgetauscht wird.
 - IKE Minimal lifetime** Minimaler Zyklus bevor der IKE Schlüssel erneut ausgetauscht wird.
 - IKE Maximal lifetime** Maximaler Zyklus bevor der IKE Schlüssel erneut ausgetauscht wird.
 - IPSec Default lifetime** Zyklus bevor der IPSec Schlüssel erneut ausgetauscht wird.
 - IPSec Minimal lifetime** Minimaler Zyklus bevor der IPSec Schlüssel erneut ausgetauscht wird.
 - IPSec Maximal lifetime** Maximaler Zyklus bevor der IPSec Schlüssel erneut ausgetauscht wird.
- **Dead Peer Detection (DPD)**
 - Interval (Sec.)** Intervall zwischen den DPD Nachrichten.
 - Wiederholungen** Anzahl der DPD Nachrichten (Sendewiederholung).
 - Intervall zw. Wiederholungen (Sec.)** Intervall zwischen den DPD Nachrichten wenn das Remote Gateway nicht antwortet.
- **Verschieden**
 - Wiederholungen** Anzahl der Versuche, bevor abgebrochen wird.
 - Wartezeit** Wartezeit, bevor die Schlüsselaushandlung abgebrochen wird.
 - Unverschlüsselten Netzwerkverkehr blockieren** Bei aktivierter Option wird nur verschlüsselter Netzwerkverkehr akzeptiert.

Dead Peer Detection (i.e. DPD) ist eine Internet Key Exchange (IKE) Erweiterung (i.e. RFC3706) um nicht reagierende oder tote Tunnel zu erkennen. Der TheGreenBow IPsec VPN Client verwendet DPD:

- um eine geöffnete SA zu löschen, wenn der Peer als "tot" erkannt wird oder nicht reagiert.
- um auf ein sog. "FallBack" oder Redundant Gateway auszuweichen, wenn diese Option in der Phase 1 aktiviert ist.

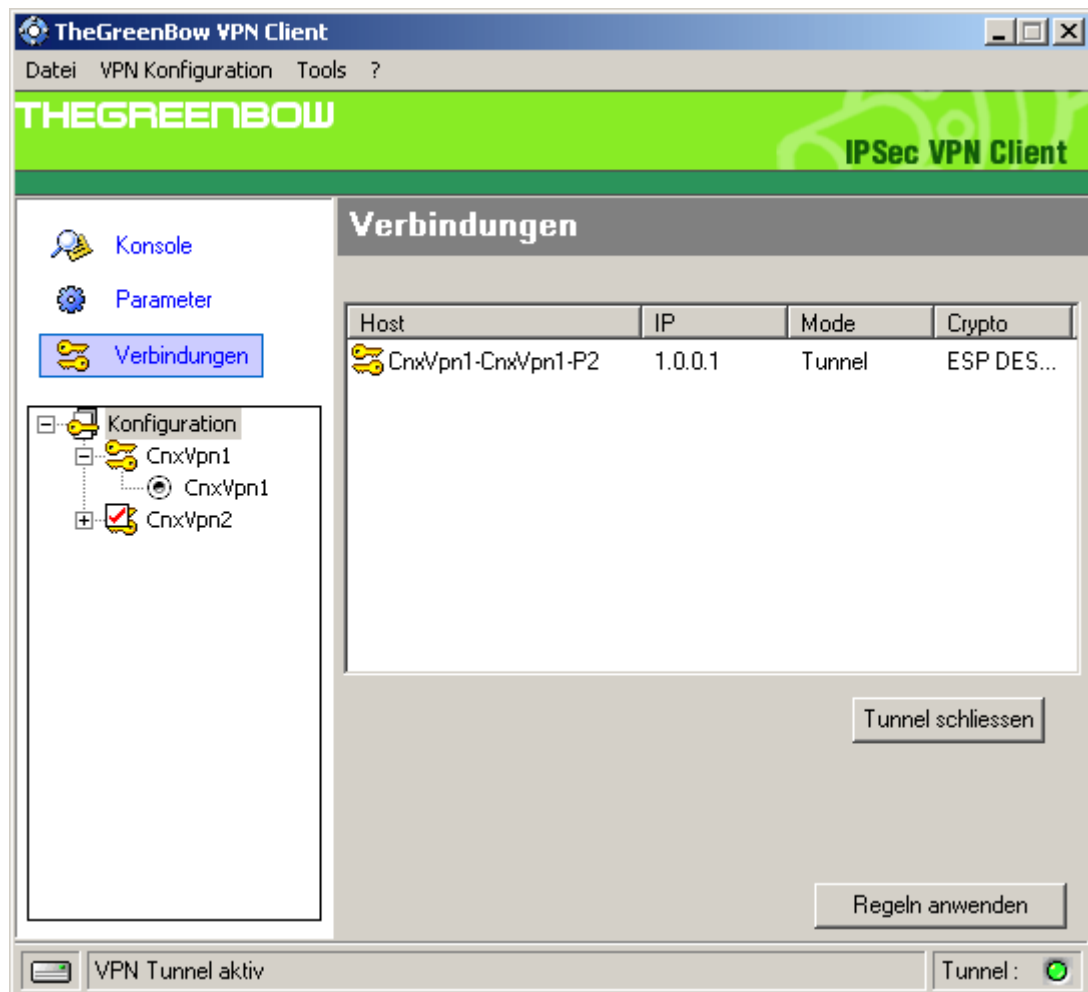
Über den Button "Regeln anwenden" werden Änderungen übernommen.

4.6 VPN Tunnel Übersicht

4.6.1 Übersicht der Tunnelverbindungen

Die Ansicht "Verbindungen" zeigt alle im Moment aktiven Verbindungen an. Um einen Tunnel zu schließen, markieren Sie diesen und klicken anschließend auf "Löschen".

Tunnels können ebenfalls über das Kontextmenü des Trayicons geschlossen oder geöffnet werden.



4.7 USB Stick Modus

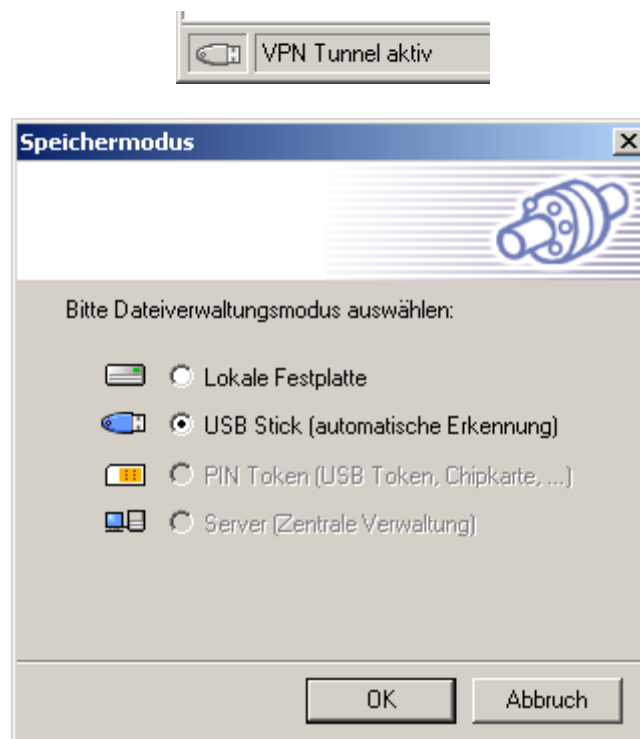
4.7.1 Was ist der USB Stick Modus

Der USB Stick Modus des erlaubt Benutzern unseres VPN Clients das Speichern und zusätzliche Verschlüsseln der Sicherheitselemente (Preshared Key, Zertifikate, Konfiguration) auf handelsüblichen Speichermedien.

Auf diese Weise können Tunnelverbindungen nicht ohne USB Stick geöffnet werden. Durch die zusätzliche Verschlüsselung der Sicherheitselemente kann der USB Stick nicht mit anderen Computern verwendet werden.

4.7.2 USB Stick Modus einrichten

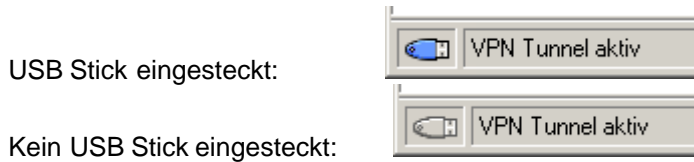
- Klicken Sie im Menü des VPN Clients auf Datei > USB Modus
- Wählen Sie die Option "USB Stick"
- Verzeichnis: Zeigt den Laufwerksbuchstaben des USB Stick, wenn dieser bereits eingesteckt ist.



Achtung: Ist bereits ein USB Stick, welcher VPN Konfigurationsdaten enthält eingesteckt, wird der zugeordnete Laufwerksbuchstabe angezeigt. Es ist nicht notwendig, während dieses Schrittes den USB Stick einzustecken. Ist kein USB Stick eingesteckt, erscheint folgendes Fenster:



Ist der USB Stick Modus aktiv, wird dies in der Statusleiste des VPN Clients angezeigt:



4.7.3 Konfiguration übertragen

Sie können Sicherheitselemente und die VPN Konfiguration auf einen USB Stick übertragen oder kopieren. Wird ein neuer USB Stick eingesteckt, wird der USB Speicher vom VPN Client erkannt.

- **Kopieren:**

VPN Konfiguration und Sicherheitselemente werden auf den USB Stick kopiert. Dabei verbleiben die ursprünglichen Sicherheitselemente und Konfigurationsdaten auf dem Rechner. Diese Funktion ist nützlich für Administratoren, um mit geringstem Zeitaufwand Konfigurationen zu verteilen.

- **Übertragen**

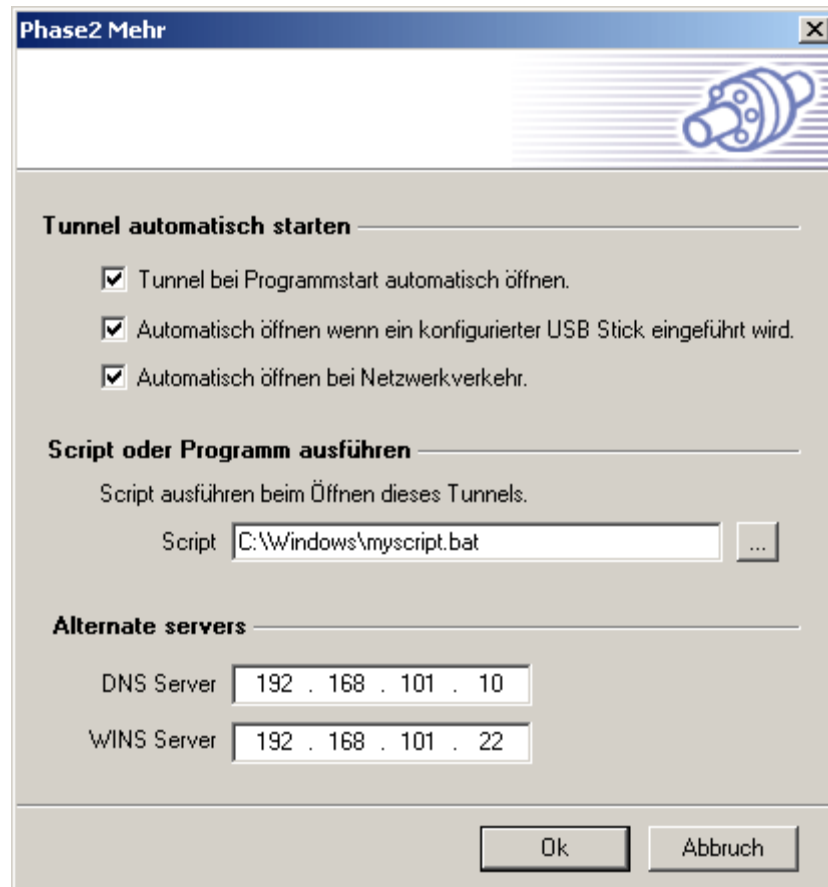
VPN Konfiguration und Sicherheitselemente werden auf den USB Stick übertragen. Dabei werden die ursprünglichen Sicherheitselemente und Konfigurationsdaten auf dem Rechner unwiderruflich gelöscht. Diese Methode wird verwendet, um Ihren VPN Zugang physikalisch zu schützen.



4.7.4 USB Stick Auto Tunnel

Jeder Tunnel muss individuell konfiguriert werden:

- Wählen Sie einen Tunnel über die IPSec Konfiguration (**Phase 2**) aus
- Aktivieren Sie die Option "Automatisch öffnen beim Einstecken des USB Stick"



4.8 Verwaltung von Zertifikaten

4.8.1 Weiterführende Informationen

Der TheGreenBow IPSec VPN Client unterstützt X509 Zertifikate im PEM Format. Diese Zertifikate werden mittels eines OpenSSL Toolkits generiert. (Der TheGreenBow VPN Client kann keine Zertifikate generieren).

[Weiterführende Dokumentation zur Umwandlung von Zertifikaten.](#)

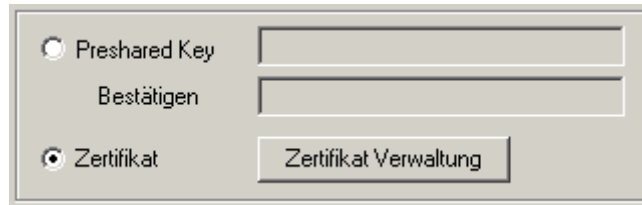
Um X509 Zertifikate zu benutzen, benötigen Sie folgende Elemente:

- Root Zertifikat
- Benutzer Zertifikat
- Private Key des Benutzer Zertifikats

Der Private Key darf nicht verschlüsselt werden. X509 Zertifikate werden in der **Phase 1** abgeglichen.

4.8.2 Konfiguration mit Zertifikaten

1. Aktivieren Sie die Option "Zertifikat" im Konfigurationsfenster der Phase 1 und klicken Sie den Button "Zertifikat Verwaltung".



2. Klicken Sie auf "Suchen..." um die entsprechenden Dateien auszuwählen.
- Root Zertifikat wird in das Verzeichnis " [install_path]\ca\" kopiert.
 - Benutzer Zertifikat wird in das Verzeichnis " [install_path]\cert\" kopiert.
 - Benutzer Private Key wird in das Verzeichnis " [install_path]\private\local.key" kopiert.



3. Klicken Sie nun auf "OK" und klicken Sie den Button "Mehr" im Hauptfenster der Phase 1. Tragen Sie hier im Feld "Lokale ID" ein:
- Typ = "DER_ASN1_DN".
 - Wert = subject user certificate ("Subject:") content like "C=FR, ST=Paris, L=Paris, O=TheGreenBow, OU=Internal OpenSSL CA, CN=exemple/Email=support@thegreenbow.com".

4.9 Konfigurationsmanagement

4.9.1 Import und Export der Konfigurationsdaten

Es ist möglich, die Konfigurationsdaten über das Hauptmenu des TheGreenBow VPN Clients zu importieren/exportieren. Mit diesem Feature können IT Administratoren Konfigurationsdaten schneller verwalten, implementieren und verteilen.

Import: Wählen Sie Datei > VPN Konfiguration laden.

Export: Wählen Sie Datei > VPN Konfiguration speichern.

Alle Konfigurationsdateien haben die Endung *.tgb und befinden sich im Programmverzeichnis (oder auf dem USB Stick - siehe USB Stick Modus) des TheGreenBow VPN Client.

Die *.tgb Konfigurationsdateien können mit einem beliebigen Texteditor, z.B. Windows® Notepad bearbeitet und reimportiert werden.

4.10 Management Tools für Administratoren

4.10.1 Tool Übersicht

Diverse Management Tools für Administratoren zur Steuerung des TheGreenBow VPN Client sind auf unserer [Webseite](#) verfügbar.

Hier Befehle für den VPN Client, die auf der Windows® Kommandozeile ausgeführt, oder über spezielle Tools ausgeführt werden können:

- IPsec VPN Client stoppen
- VPN Konfiguration importieren
- Startzeitpunkt des IPsec VPN Client festlegen
- IPsec VPN Client Benutzeroberfläche vor Anwendern verbergen

4.10.2 VPN Client stoppen

Der TheGreenBow VPN Client kann auf der Windows® Kommandozeile mit dem Befehl

" **[path]vpnconf.exe /stop** " gestoppt werden.

[path] ist das Programmverzeichnis des VPN Clients. Sind mehrere Tunnel aktiv, werden diese ohne Nachfrage geschlossen.

Diese Option eignet sich zur Skriptsteuerung des Clients.

4.10.3 Konfiguration importieren

Eine Konfigurationsdatei des TheGreenBow VPN Client kann über die Windows® Kommandozeile importiert werden:

" **[path]vpnconf.exe /import:[file.tgb]** "

[path] ist das Programmverzeichnis des VPN Client, die Datei [file.tgb] die Konfigurationsdatei.

" **/import:** " kann benutzt werden, wenn der Client gestartet oder geschlossen ist. Ist der Client gestartet, liest er die Konfigurationsdatei automatisch ein, wendet die Regeln an und reinitialisiert den IKE Dienst. Ist der Client geschlossen, startet dieser mit der neuen Konfiguration.

" **/importonce:** " kann benutzt werden, wenn der VPN Client geschlossen ist.

Dieser Befehl ist speziell für Installationsskripte gedacht: Es erlaubt Installation und Konfiguration des Clients im Hintergrund (Silent Install).

4.10.4 VPN Start Modus

Über das Tool VPNStart.exe kann der Startmodus des TheGreenBow® Clients bestimmt werden:

- Start vor Windows® Anmeldung (Boot)
- Start bei Windows® Anmeldung (Login)
- Manuell (Manual)

Die aktuelle Version ist auf unserer [Webseite](#) verfügbar.

4.10.5 VPN Hide Modus

VPNHide.exe erlaubt das Verbergen/Anzeigen der Client Konfiguration.

Endanwender können somit nicht auf die Konfiguration des VPN Clients zugreifen. Im sog. Hide Modus (Verbergen) verweist das Traybar Icon auf die Konsole, das Hauptfenster des Clients wird nicht angezeigt.

Die aktuelle Version ist auf unserer [Webseite](#) verfügbar.

4.11 Zusätzliche Supportdokumente

Zusätzliche Informationen, Konfigurationsanleitungen und Fehlerbeschreibungen finden Sie auf unserer [Webseite](#).

Part

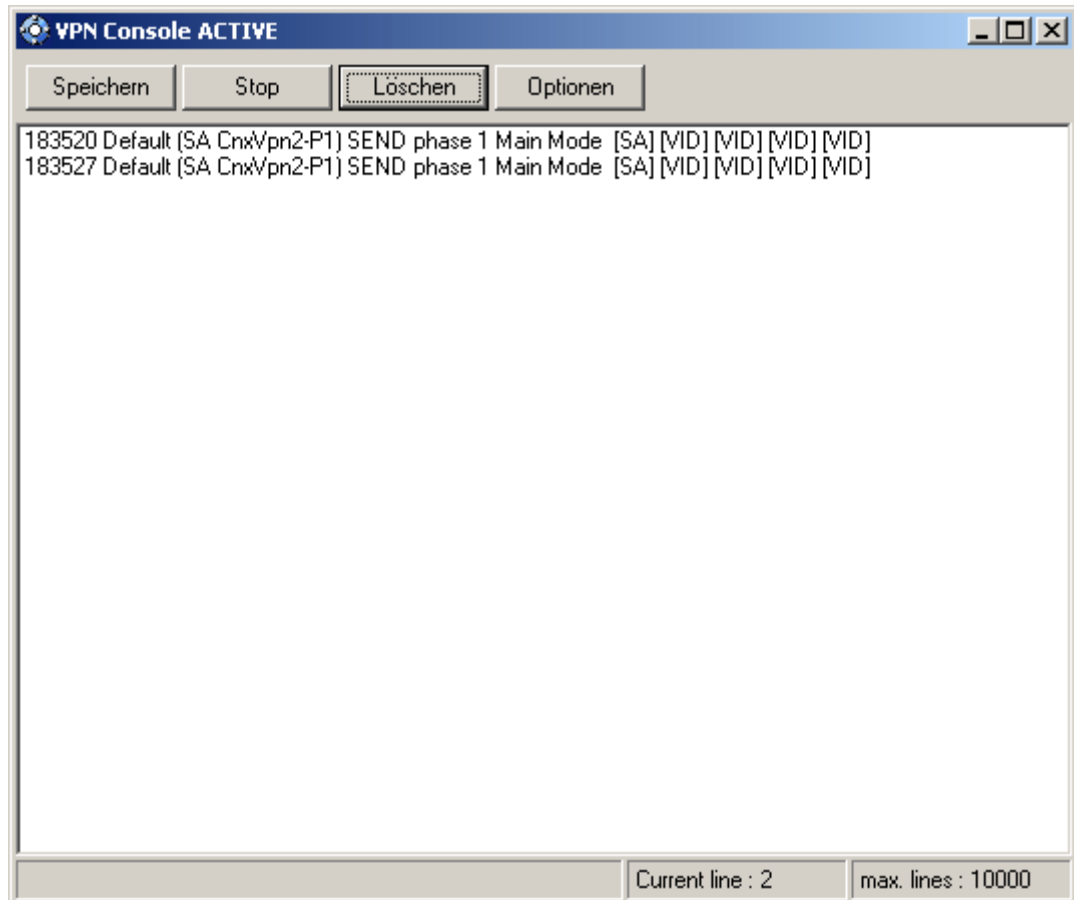


Konsole und Protokollfunktionen

5 Konsole und Protokollfunktionen

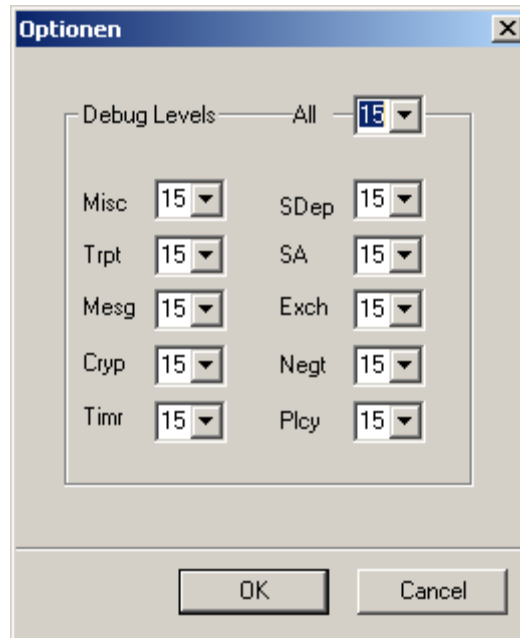
5.1 Die Konsole

Auf der Konsole kann über das Menü im Hauptfenster des TheGreenBow VPN Client oder über das Trayicon in der Taskleiste zugegriffen werden. Diese Funktion dient zur Anzeige und Aufzeichnung von Verbindungsprotokollen und Fehleranalyse. Alle Aktionen des Clients und die Rückmeldungen bei Aufbau einer VPN Verbindung werden hier angezeigt und ggfs. mitgeloggt.



Button	Beschreibung
Löschen	Löscht den Inhalt des Fensters
Speichern	Speichert das Logfile im Programmverzeichnis
Stop	Stoppt die Datenaufzeichnung
Optionen	Justiert die Detailtiefe der Logaufzeichnung

5.2 Filter



Bez.	Name	Beschreibung
Misc	Misc	log level for configuration reading or dump of low level
Trpt	Transport	log level for UDP transport mode
Mesg	Message	log level for IKE decode
Cryp	Crypto	log level and dump for crypto material exchanged
Timr	Timer	log level about timers
SDep	Sysdep	log level about IKE interface from/to IPSec
SA	SA	log level for SA management
Exch	Exchange	log level about IKE exchanges (very useful)
Negt	Negotiation	log level about phase 1 and phase 2 negotiation
Plcy	Policy	not used
All	All	Apply the same log level to all subsystems

Most of the time log level set to 0 is largely enough for resolving configuration issues.

Part



Fehlerbehebung

6 Fehlerbehebung

Auf unserer [Internetseite im Bereich Support](#) finden Sie detaillierte Hinweise zur Fehlerbehebung und Konfigurationsanleitungen zu diversen populären VPN Gateways.

Part



Kontakt

7 Kontakt

TheGreenBow Deutschland

Timm Richter - Internet Consulting

<http://www.thegreenbow.de>

Bahnstr. 7

66130 Saarbrücken

Germany

Tel: +49 (0)6898 - 50 47 03

Fax: +49 (0)6898 - 50 47 20

eMail: infos@thegreenbow.de