

# OpenVPN Modul für die Collax Plattform

OpenVPN-Einwahl auf Collax Server

Claus R. Wickinghoff  
Dipl.-Ing.

OpenVPN ist eine Software zum Aufbau eines Virtual Private Networks. Als Verschlüsselungsprotokoll kommt SSL/TLS zum Einsatz, welches weniger komplex als das von IPsec genutzte Verfahren ist. Dadurch funktioniert OpenVPN meist reibungslos in WLAN-Umgebungen in Hotels und anderen öffentlichen Bereichen.

Dieses Modul ist in die Collax-GUI integriert und realisiert die Server-Seite eines OpenVPN-Netzes. Client-Software für OpenVPN ist für die meisten Plattformen kostenlos verfügbar.

## **OpenVPN Modul für die Collax Plattform**

Version 02 vom 21. April 2016.

Copyright 2013-2016 linudata GmbH Ingenieurbüro, Essen  
<http://www.linudata.de/> – [info@linudata.de](mailto:info@linudata.de)

Alle in dieser Dokumentation enthaltenen Darstellungen und Informationen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht völlig auszuschließen. Die Autoren und die linudata GmbH übernehmen für die Inhalte keine Verantwortung und werden keine Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials oder Teilen davon oder durch Verletzungen der Rechte Dritter entsteht.

Die Wiedergabe von Warenbezeichnungen, Gebrauchsnamen, Handelsnamen und Ähnlichem in dieser Dokumentation berechtigt auch ohne deren besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne des Warenzeichen- und Markenschutzrechts frei seien und daher beliebig verwendet werden dürften. Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen Dritter.

Dieses Werk ist urheberrechtlich geschützt. Alle Rechte, insbesondere die Übersetzung in fremde Sprachen, sind vorbehalten. Kein Teil der Dokumentation darf ohne ausdrückliche Genehmigung der linudata GmbH fotokopiert oder in irgendeiner anderen Form reproduziert oder in eine von Maschinen verwendbare Form übertragen oder übersetzt werden.

Maschinenlesbare Fassungen dieser Dokumentation, insbesondere im HTML- oder PDF-Format, werden nur zum persönlichen Gebrauch zur Verfügung gestellt und dürfen ohne ausdrückliche Genehmigung der linudata GmbH nicht weiterverbreitet werden. Für Ausdrücke solcher Fassungen gelten dieselben Einschränkungen.

Autor: Dipl.-Ing. Claus R. Wickinghoff  
Gesetzt mit  $\LaTeX$  und KOMA-Script.

# Inhaltsverzeichnis

<b>1</b>	<b>Übersicht</b>	<b>2</b>
<b>2</b>	<b>Installation</b>	<b>3</b>
2.1	32- oder 64-Bit? . . . . .	3
2.2	Cabinet installieren . . . . .	3
2.3	Weitere Vorbereitungen . . . . .	3
<b>3</b>	<b>Konfiguration</b>	<b>5</b>
3.1	Einrichtung CA . . . . .	5
3.2	Anlegen des Server-Zertifikats . . . . .	7
3.3	Anlegen eines Benutzer-Zertifikats . . . . .	9
3.4	IP-Netzwerk für Client-Einwahl . . . . .	10
3.5	Konfiguration OpenVPN . . . . .	11
3.6	Setzen von Firewallregeln . . . . .	14
<b>4</b>	<b>Betrieb</b>	<b>16</b>
4.1	Export Client-Konfiguration . . . . .	16
4.2	Aktive Verbindungen . . . . .	17
4.3	Sperren von Clients . . . . .	18
4.4	Ablauf von Zertifikaten . . . . .	18
4.5	Verwenden eines anderen Ports . . . . .	20
<b>5</b>	<b>Fehlersuche</b>	<b>22</b>
5.1	Blick ins Logfile . . . . .	22
5.2	Verbindungstest zum OpenVPN Dienst . . . . .	24
5.3	Routing im Client . . . . .	24
<b>6</b>	<b>Unterstützte Geräte</b>	<b>26</b>
6.1	Windows . . . . .	26
6.2	Linux . . . . .	33
6.3	Mac OS X . . . . .	39
<b>7</b>	<b>Datensicherung</b>	<b>47</b>
<b>8</b>	<b>Support</b>	<b>47</b>

# 1 Übersicht

OpenVPN ist ein Protokoll zum Aufbau eines VPN<sup>1</sup>. Ein VPN verbindet Computersysteme durch eine verschlüsselte, sichere Verbindung über ein unsicheres Medium, meist das Internet.

Dies wird etwa zum Anbinden von Außenstellen an einen zentralen Standort oder zur Einwahl von mobilen Mitarbeitern in ein Unternehmensnetz genutzt. Bei der Einwahl von Mitarbeitern ist neben der verschlüsselten Übertragung auch der Aspekt der Authentifizierung wichtig, d.h. nur tatsächlich befugte Personen dürfen sich einwählen. Das Modul für den Collax Server ist für die Einwahl von mobilen Mitarbeitern gedacht.

OpenVPN nutzt für die Datenübertragung das OpenSSL-Protokoll, das auch bei Verwendung von HTTPS zum Einsatz kommt. Die Authentifizierung erfolgt über X.509-Zertifikate. Verläßt ein Mitarbeiter das Unternehmen oder wird ein Gerät mit installiertem Zertifikat entwendet oder verschrottet, kann das zugehörige Zertifikat gesperrt und ggf. neu erstellt werden.

Zum Aufbau eines VPN gibt es mehrere unterschiedliche Lösungen, OpenVPN ist nur eine der möglichen Lösungen. Vom Protokoll her ist OpenVPN vergleichsweise anspruchlos, da OpenSSL als Grundlage genutzt wird. So erfolgt die Datenübertragung entweder über UDP<sup>2</sup> oder TCP<sup>3</sup>-Pakete. Der Port ist per Konvention auf 1194 festgelegt, kann aber auch geändert werden.

UDP ist ein "zustandloses" Protokoll. D.h. hier werden Datenpakete verschickt, ohne daß das Protokoll die korrekte Zustellung sicherstellt. Dieses Verfahren ist sehr schnell und wird beispielsweise für DNS<sup>4</sup> und VoIP<sup>5</sup>-Verbindungen genutzt. TCP hingegen kennt den Zustand einer Verbindung und bietet somit eine einfache Fehlerkorrektur in Form des erneuten Versands verlorener Pakete. Aus diesem Grund wird TCP im Internet für sehr viele Dienste genutzt.

OpenVPN kann auf UDP- und TCP-Verbindungen gleichermaßen genutzt werden, da OpenVPN andere Datenverbindungen kapselt und eine über VPN abgewickelte TCP-Übertragung ihrerseits mit einem Verbindungszustand arbeitet. Üblicherweise kommt UDP zum Einsatz, wenn Stream-Übertragungen - etwa Telefonie - erfolgen oder die beteiligten Systeme geografisch weit voneinander entfernt sind. Andererseits ist es oft so, daß mobile Mitarbeiter in anderen Unternehmensnetzen, an Flughäfen oder in Hotels sitzen, wo UDP evt. geblockt wird. Dann kann der Einsatz von TCP überhaupt erst einen Verbindungsaufbau ermöglichen.

Die OpenVPN Projektseite finden Sie unter <http://openvpn.net>.

---

<sup>1</sup> VPN = Virtual Private Network

<sup>2</sup> UDP = User Datagram Protocol

<sup>3</sup> TCP = Transmission Control Protocol

<sup>4</sup> DNS = Domain Name Service

<sup>5</sup> VoIP = Voice over IP

## 2 Installation

Zur Installation des OpenVPN Moduls für die Collax Plattform benötigen Sie zunächst das passende Cabinet-File für Ihr System. Sie finden es auf den Webseiten der linudata GmbH im Bereich “Support & Service” (<http://www.linudata.de/service/>).

Um in den Downloadbereich zu gelangen, ist eine Registrierung notwendig. Nach Angabe einer E-Mail-Adresse erhalten Sie eine E-Mail mit einem Bestätigungslink. Sobald Sie diesen aufgerufen haben, wird Ihnen per E-Mail ein Passwort zugeschickt.

### 2.1 32- oder 64-Bit?

Das Modul ist als 32- und als 64-Bit Version verfügbar. Sie benötigen die jeweils zu Ihrem Collax System passende Version.

Wenn Sie in der Administrationsoberfläche Ihres Collax Systems angemeldet sind, sehen Sie in der Leiste links im Abschnitt **Systeminformation** die genaue Produktbezeichnung und Version Ihres Systems. 64-Bit Systeme sind an dem Zusatz **x86\_64** hinter der Versionsnummer erkennbar. Fehlt dieser, handelt es sich noch um eine 32-Bit Installation.

Collax Systeme, die mit Version 5.0.x oder älter installiert wurden, sind 32-Bit Systeme – auch wenn diese zwischenzeitlich auf 5.8.x aktualisiert wurden. Systeme, die neu mit Version 5.5.x oder neuer installiert wurden, sind 64-Bit Versionen.

### 2.2 Cabinet installieren

Wenn Sie das Cabinet-File auf Ihren Rechner heruntergeladen haben, können Sie es in der Collax Adminoberfläche über **Menü - Software - Anwendungen** über die Schaltfläche **Ein Anwendungs-Cabinet installieren** hinzufügen.

Abb. 1 zeigt das installierte Modul in der Admin-GUI.

Nach erfolgreicher Installation ist auf der obersten Menüebene im Abschnitt **System** ein neues Icon **linudata Erweiterungen** sichtbar. Hierüber sind die OpenVPN-Konfiguration, eine Statusübersicht und das Client-Paket erreichbar.

Eventuell ist ein Reload der Konfigurationsoberfläche nötig, damit die Icons sichtbar werden. Dies geschieht einfach durch Ab- und Anmelden an der Admin-GUI.

### 2.3 Weitere Vorbereitungen

Die Authentifizierung erfolgt bei OpenVPN mit Hilfe von Zertifikaten. Sie benötigen zur Verwendung von OpenVPN daher eine CA und entsprechende Zertifikate. Dies wird in den Abschnitten 3.1, 3.2 und 3.3 beschrieben.

Da Zertifikate nur in einem bestimmten Zeitraum gültig sind, ist eine korrekte Systemzeit nötig. Prüfen Sie daher unter **Menü - Dienste - Infrastruktur - Zeit** die Verwendung von NTP als **Synchronisationsquelle**.

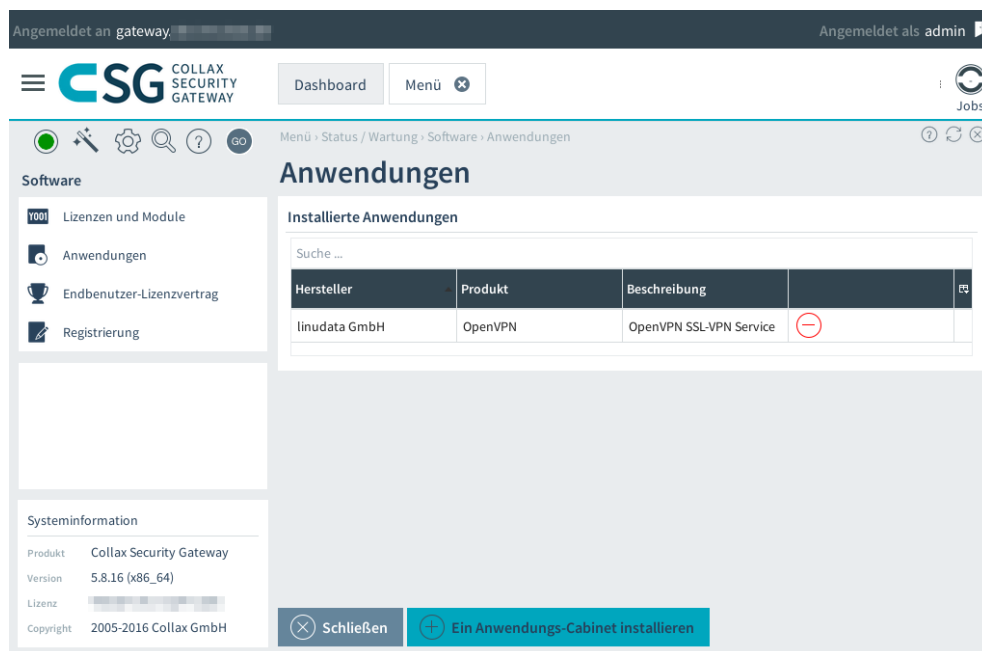


Abbildung 1: Installiertes Cabinet-File

Per OpenVPN verbundene Clients erhalten IP-Adressen aus einem eigenen Netzwerkbereich. Dies wird auch Roadwarrior-Netz genannt<sup>6</sup>. Die Konfiguration wird in Abschnitt 3.4 beschrieben.

<sup>6</sup> Roadwarrior bezeichnet einen Teilnehmer, der auf den "Straßen" des Internets unterwegs ist und sich ins Firmennetzwerk einwählt.

## 3 Konfiguration

Folgende Schritte sind zur Konfiguration des OpenVPN Dienstes auf einem Collax-System nötig. Sie werden in den folgenden Abschnitten jeweils ausführlich erläutert.

- Erstellen eines CA-Zertifikats (siehe Abschnitt 3.1 auf S. 5)
- Erstellen eines signierten Zertifikats für den Collax-Server (siehe Abschnitt 3.2 auf S. 7)
- Erstellen mindestens eines signierten Benutzer-Zertifikats (siehe Abschnitt 3.3 auf S. 9)
- Anlegen eines IP-Netzes für die ausgewählten Clients (Roadwarrior)
- Konfigurieren der Firewall-Regeln
- Konfiguration von OpenVPN selbst

### 3.1 Einrichtung CA

Die Authentifizierung der beteiligten Systeme untereinander erfolgt mit Hilfe von Zertifikaten. Dazu ist eine CA<sup>7</sup> nötig. Mit Hilfe dieses CA-Zertifikats werden später die Zertifikate für den Collax-Server und für jeden Client signiert.

Zertifikate werden in der GUI unter Menü - **Benutzungsrichtlinien** - **X.509-Zertifikate** verwaltet.

Hier sind evt. bereits ein durch Assistenten erstelltes CA-Zertifikat **ServerCA1** und ein Maschinenzertifikat **ServerCertificate1** aufgelistet. Diese können verwendet werden. Fehlen diese oder möchten Sie zur sauberen Trennung eine eigene CA für OpenVPN nutzen, können Sie über die Schaltfläche **Hinzufügen** ein CA-Zertifikat erzeugen.

Unter **Name** wird ein sinnvoller Name für das Zertifikat vergeben. Dieser Name läßt sich später nicht mehr anpassen.

Unter **Kommentar** kann ein erklärender Text hinzugefügt werden.

Die **Gültigkeit** wird in Tagen angegeben. Die Vorgabe des Systems sind **365 Tage**, also ein Jahr. Nach Ablauf des CA-Zertifikats selbst sind alle darüber erzeugten Zertifikate ebenfalls ungültig. Es ist daher sinnvoll, hier einen längeren Zeitraum zu wählen. In Abbildung 2 werden **5475 Tage** gewählt, entsprechend ca. 15 Jahre.

Der **Schlüssel** soll **generiert** werden.

Die **Schlüssellänge** soll laut BSI<sup>8</sup> "ausreichend" gewählt werden. Für das CA-Zertifikat selbst wählen wir daher die maximal möglichen **4096 Bit**.

Die **Verwendung** des Zertifikats ist vom Typ **CA**.

Bei **Signieren mit** wird nichts ausgewählt, da diese CA nur mit sich selbst signiert wird.

---

<sup>7</sup> CA = Certificate Authority, eine Art elektronischer Notar

<sup>8</sup> BSI = Bundesamt für Sicherheit in der Informationstechnik

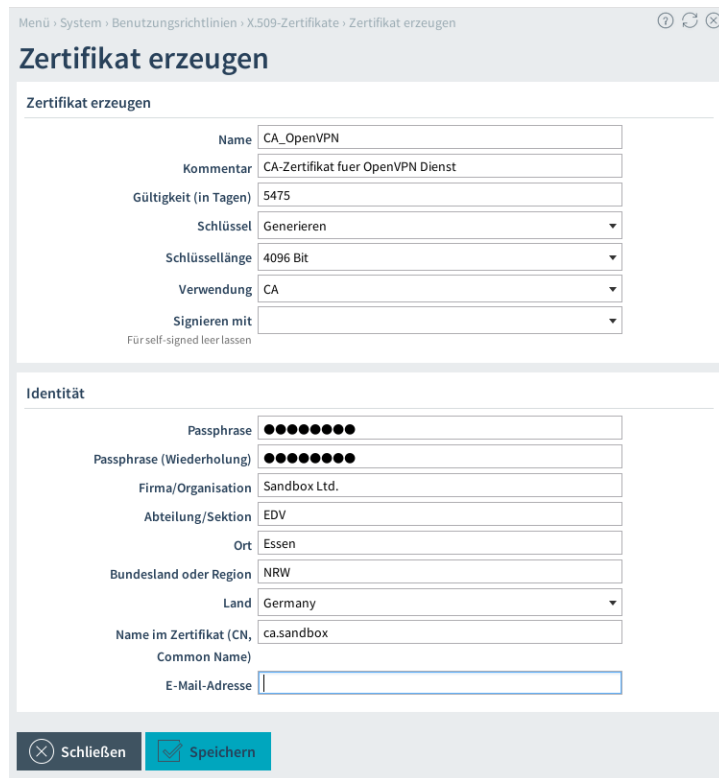


Abbildung 2: Erstellen eines CA-Zertifikats

Wichtig ist die **Passphrase**, die sicherheitshalber ein zweites Mal zur Kontrolle eingegeben werden muß. Diese Passphrase wird in Zukunft immer wieder benötigt, wenn mit der CA gearbeitet wird, um ein neues Zertifikat anzulegen oder um ein verlorenes (komprommittiertes) Zertifikat zu sperren.

In den Feldern **Firma/Organisation**, **Abteilung/Sektion**, **Ort**, **Bundesland** und **Land** werden die Daten des Unternehmens eingetragen, für das das Zertifikat ausgestellt wird. Diese Informationen werden in das Zertifikat übernommen und können dort wieder ausgelesen werden.

Als Vorgabe für diese Werte werden die Angaben unter **Menü - Benutzungsrichtlinien - Umgebung - Standort** genommen. Setzen Sie diese entsprechend, da Sie mindestens drei - vermutlich einige mehr - Zertifikate erstellen müssen.

Das Feld **Name im Zertifikat** ist wichtig. Hier wird der "Common Name" (CN) eingetragen. Der Common Name muß auf allen beteiligten Systemen verschieden sein. Es hat sich bewährt, diesen in Form eines Hostnamens mit dem Unternehmensnamen oder einem Kürzel als Domainanteil zu setzen.

Das Feld **E-Mail-Adresse** kann leer bleiben.

Durch Klick auf **Speichern** wird das Zertifikat erstellt. Wenn alles korrekt abläuft, ist in der Statusausgabe (siehe Bild 3) der Text `...writing new private key to...` zu lesen.

Mit **Schließen** wird die Maske geschlossen. In der Zertifikatsübersicht wird das neu erstellte CA-Zertifikat nun mit aufgelistet.





Abbildung 3: Erstelltes CA-Zertifikat

### 3.2 Anlegen des Server-Zertifikats

Sobald ein CA-Zertifikat vorhanden ist, können damit weitere Zertifikate signiert werden. Dabei wird eine Prüfsumme mit dem Schlüssel der CA erzeugt und dem Zertifikat hinzugefügt, um dessen Echtheit zu sichern. Alle von der selben CA signierten Zertifikate vertrauen einander.

Um den Collax-Server als Einwahl-Server nutzen zu können, muß über **Hinzufügen** ein Zertifikat erzeugt werden. Abbildung 4 zeigt die entsprechende Maske.



Abbildung 4: Erstellen des Server-Zertifikats

Unter **Name** wird ein sinnvoller Name für das Zertifikat vergeben. Unter **Kommentar** kann ein erklärender Text hinzugefügt werden. Beide Werte lassen sich später nicht mehr ändern.

Die **Gültigkeit** wird in Tagen angegeben. Hier sollte ein Termin vor Ablauf des CA-Zertifikats gewählt werden. Im vorhergehenden Abschnitt wurde das CA-Zertifikat mit 5475 Tagen (etwa 15 Jahre) erzeugt - ein sinnvoller Wert für das Server-Zertifikat wäre dann 5474 Tage.

Der **Schlüssel** soll **generiert** werden.

Die **Schlüssellänge** sollte hier auch auf **4096 Bit** gesetzt werden. Es mag speziellen Geräte geben (Smartcards, Mobile Devices o.ä.), die diese Schlüssellänge nicht unterstützen. Dann können auch **2048 Bit** Schlüssel erzeugt werden, kleinere Schlüssellängen sollten Sie nicht verwenden.

Die **Verwendung** des Zertifikats ist vom Typ **Lokaler Server**.

Bei **Signieren mit** wird das CA-Zertifikat ausgewählt. Dadurch ändert sich die Maske und erfordert die Eingabe der **CA-Passphrase**.

In den Feldern **Firma/Organisation**, **Abteilung/Sektion**, **Ort**, **Bundesland** und **Land** werden die Daten des Unternehmens eingetragen, für das das Zertifikat ausgestellt wird. Diese Informationen werden in das Zertifikat übernommen und können dort wieder ausgelesen werden.

Das Feld **Name im Zertifikat** ist wichtig. Hier wird der "Common Name" (CN) eingetragen. Der Common Name muß auf allen beteiligten Systemen verschieden sein.

Das Feld **Alias-Namen** kann leer bleiben.



Abbildung 5: Erstelltes Server-Zertifikat

Durch Klick auf **Speichern** wird das Zertifikat erstellt. Wenn alles korrekt abläuft, ist in der Statusausgabe (siehe Bild 5) der Text **Certificate created and signed** zu lesen.

Mit **Schließen** wird die Maske geschlossen. In der Zertifikatsübersicht wird das neu erstellte Zertifikat unterhalb der zugehörigen CA aufgelistet.

### 3.3 Anlegen eines Benutzer-Zertifikats

Für jeden Benutzer muß ein eigenes Zertifikat angelegt werden. Wichtig ist, daß hier der Name im Zertifikat unterschiedlich ist.

In der Zertifikatsübersicht wurde dazu mit Hinzufügen der Dialog zum Erstellen einen Zertifikats geöffnet.

Abbildung 6: Erstellen eines Benutzer-Zertifikats

Im Beispiel wird ein Zertifikat für den Nutzer Wilhelm Krause erstellt. Hierzu werden unter **Name** und **Kommentar** entsprechende Einträge gesetzt. Im Beispiel wird als Konvention jedem Nutzerzertifikat im Namen ein **ovpn\_** vorangestellt.

Bei der **Gültigkeit in Tagen** wird bei Nutzerzertifikaten üblicherweise ein kürzeres Intervall genutzt. Hier wird ein Zeitraum von **720 Tagen** (ca. 2 Jahre) gesetzt.

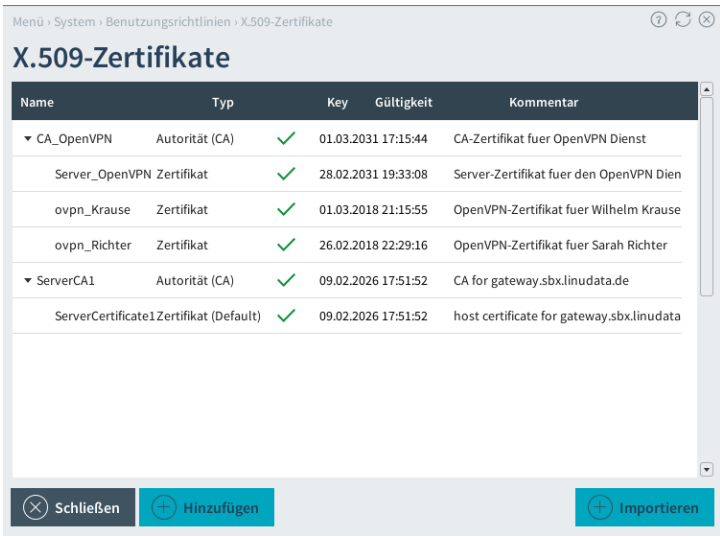
Der Schlüssel wird **generiert** und dabei eine **Schlüssellänge** von 4096 Bit verwendet.

Unter **Signieren mit** wird das CA-Zertifikat ausgewählt. Dabei muß auch die **CA-Passphrase** angegeben werden.

Im Abschnitt **Identität** werden wieder Angaben zur Organisation und zum Standort gesetzt. Wichtig ist wieder das Feld **Name im Zertifikat**, daß einen eindeutigen Namen enthalten muß.

Der Mail-Alias kann leer bleiben und wird für OpenVPN nicht benötigt.

Durch Klick auf **Speichern** wird das Zertifikat erstellt. Bei erfolgreichem Ablauf wird auch hier **Certificate created and signed** ausgegeben.



The screenshot shows a web interface titled "X.509-Zertifikate" with a breadcrumb trail "Menü > System > Benutzungsrichtlinien > X.509-Zertifikate". It displays a table of certificates with the following data:

Name	Typ	Key	Gültigkeit	Kommentar
CA_OpenVPN	Autorität (CA)	✓	01.03.2031 17:15:44	CA-Zertifikat fuer OpenVPN Dienst
Server_OpenVPN Zertifikat		✓	28.02.2031 19:33:08	Server-Zertifikat fuer den OpenVPN Dien
ovpn_Krause	Zertifikat	✓	01.03.2018 21:15:55	OpenVPN-Zertifikat fuer Wilhelm Krause
ovpn_Richter	Zertifikat	✓	26.02.2018 22:29:16	OpenVPN-Zertifikat fuer Sarah Richter
ServerCA1	Autorität (CA)	✓	09.02.2026 17:51:52	CA for gateway.sbx.linudata.de
ServerCertificate1Zertifikat (Default)		✓	09.02.2026 17:51:52	host certificate for gateway.sbx.linudata

At the bottom of the interface, there are three buttons: "Schließen" (Close), "Hinzufügen" (Add), and "Importieren" (Import).

Abbildung 7: Liste der erstellten Zerifikate

Abbildung 7 zeigt nochmals die Übersicht der erstellten Zertifikate: Das CA-Zertifikat, eines für den Collax-Server selbst und je eines pro Benutzer.

### 3.4 IP-Netzwerk für Client-Einwahl

Die per OpenVPN eingewählten Systeme erhalten eine IP-Adresse aus einem eigenen Netzwerkbereich zugewiesen. Dies muß ein IP-Netzwerk sein, daß bisher nicht genutzt wird (weder im LAN, noch zu einem Router oder an einem per VPN gekoppelten Standort).

Aus technischen Gründen nutzt OpenVPN pro aktivem Client vier IP-Adressen. D.h. wird für das Client-Netz ein Class-C-Netz (Netzmaske /24 bzw. 255.255.255.0) verwendet, können sich gleichzeitig ca. 63 Clients verbinden.

Netzwerke werden unter **Menü - System - Netzwerk - Netze** verwaltet. Über **Hinzufügen** wird ein neues Netzwerk angelegt.

**Bezeichnung** und **Kommentar** sollten weitgehend selbsterklärend gesetzt werden.

Unter **Netzwerkadresse** wird die Netzwerkadresse eingetragen und die **Netzmaske** muß passend gewählt werden.

Bei **Netzwerk verwenden für** reicht es aus, **Berechtigungen** und **Firewall-Matrix** auszuwählen. Die Auswahl von **Routing** ist nicht notwendig, da für OpenVPN kein Collax-typischer Link angelegt wird.

Bild 8 zeigt eine entsprechend ausgefüllte Maske. Mit **Speichern** wird das Netzwerk in die Konfiguration übernommen.

Menü > System > Netzwerk > Netze > Netzwerk bearbeiten

## Netzwerk bearbeiten

Grundeinstellungen Gruppenzugehörigkeit Optionen

**Grundeinstellungen**

Bezeichnung des Netzwerks: OpenVPN\_ClientNetz

Kommentar: IP-Netzwerk fuer OpenVPN Client Einwahl

Netzwerkadresse: 192.168.72.0

Netzmaske: 255.255.255.000 (24 bit)

Netz verwenden für: Berechtigungen und Firewall-Matrix

Schließen Speichern

Abbildung 8: Anlegen des Client-Netzwerks

### 3.5 Konfiguration OpenVPN

Die Konfiguration von OpenVPN erfolgt unter Menü - linudata Erweiterungen - OpenVPN - Grundeinstellungen. Zunächst muß OpenVPN aktiviert und ein Lizenzschlüssel eingegeben werden. Dadurch werden weitere Konfigurationsfelder und Reiter sichtbar (siehe Abb. 9 und 10).

Menü > System > linudata Erweiterungen > Openvpn: Grundeinstellungen

## Openvpn: Grundeinstellungen

Grundeinstellungen

**Status und Lizenz**

Aktiviert

Lizenzschlüssel

Formular speichern um Lizenz zu aktivieren

Schließen Speichern

Abbildung 9: Beginn der OpenVPN Konfiguration

Den Lizenzschlüssel erhalten Sie über Ihren Collax-Partner. Wird ein falscher Schlüssel eingegeben, wird in der GUI entsprechend **Lizenzschlüssel ungültig** ausgegeben.

Bei gültigem Lizenzschlüssel wird **Lizenz aktiviert** angezeigt und die Konfigurationsmaske wird sichtbar.

In den **Basiseinstellungen** muß zunächst festgelegt werden, ob als **Protokoll** TCP oder UDP genutzt werden soll. Üblicherweise bietet die Verwendung von UDP etwas bessere Performance. Es kann jedoch sein, daß Clients hinter Routern/Firewalls sitzen, die UDP sperren. Dann kann TCP die einzige Möglichkeit zur Datenübertragung sein.

Als Port wird immer 1194 genutzt. Hier muß evt. auf einem vorgeschalteten Router ein Portforward konfiguriert werden.

Unter **VPN Netzwerk** wird das in Abschnitt 3.4 beschriebene Netz ausgewählt, aus dem jedem Client bei Einwahl eine IP-Adresse zugewiesen wird.

Unter **Lokale Netzwerke** werden die Netze aktiviert, auf die per OpenVPN zugegriffen werden kann. Durch diese Auswahl werden Netzrouten an den Client übermittelt. Üblicherweise wird hier das lokale Netzwerk des Collax-Servers ausgewählt. Wenn es noch separate Netze für Server gibt (etwa eine DMZ), müssen diese ebenfalls aktiviert werden.

The screenshot shows the 'Openvpn: Grundeinstellungen' configuration page. It has three tabs: 'Grundeinstellungen', 'Berechtigungen', and 'Optionen'. The 'Grundeinstellungen' tab is active. Under 'Status und Lizenz', the 'Aktiviert' checkbox is checked, and the 'Lizenzaktiviert' status is shown. The 'Basiseinstellungen' section includes: 'Protokoll' set to 'TCP'; 'VPN Netzwerk' set to 'OpenVPN\_ClientNetz (192.168.72.0/24)'; 'Lokale Netzwerke' with checkboxes for 'Internet (0.0.0.0/0)', 'RouterNetz (83.223.68.0/24)', 'LocalNet (192.168.70.0/24)' (checked), and 'OpenVPN\_ClientNetz (192.168.72.0/24)'; 'CA Zertifikat' set to 'CA\_OpenVPN (CA-Zertifikat fuer OpenVPN Dienst)'; 'Server Zertifikat' set to 'Server\_OpenVPN (Server-Zertifikat fuer den OpenVPN Die...'; and 'DNS-Server bei Einwahl zuweisen' set to '192.168.70.1'. The 'Einstellungen für Client Config-Paket' section has 'Offizieller Hostname oder IP-Adresse des Einwahrservers' set to 'gateway.sandbox.dyndns.org'. At the bottom are 'Schließen' and 'Speichern' buttons.

Abbildung 10: OpenVPN Konfiguration

Unter **CA Zertifikat** wird das in Abschnitt 3.1 erzeugte Zertifikat der CA festgelegt. Alle Zertifikate, die von dieser CA signiert wurden und gültig sind, können sich per OpenVPN verbinden.

Analog wird unter **Server Zertifikat** das in Abschnitt 3.2 für den Collax-Server erzeugte Zertifikat ausgewählt.

Im Feld **DNS-Server bei Einwahl zuweisen** kann die IP-Adresse eines Nameservers angegeben werden, der bei Einwahl an den Client übermittelt wird. Dies kann

der Collax-Server selbst oder auch ein interner DNS (etwa ein Domaincontroller) sein. Dadurch ist es für den Client möglich, mit Hostnamen zu arbeiten, die nur im Firmennetz auflösbar sind.

In den **Einstellungen für Client Config-Paket** kann der Hostname oder die IP-Adresse angegeben werden, unter der der Collax-Server aus dem Internet erreichbar ist. Wenn Sie keine feste IP-Adresse auf Ihrer Internetleitung haben, sollten Sie einen Dyndns-Dienst nutzen und konfigurieren.

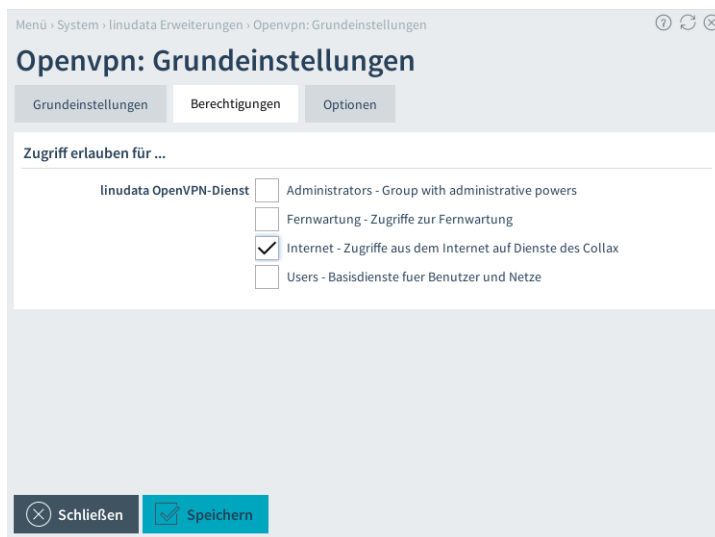


Abbildung 11: Berechtigung zur OpenVPN-Einwahl

Über den Reiter **Berechtigungen** wird eingestellt, aus welchen Netzen der OpenVPN-Dienst genutzt werden darf. Üblicherweise wird hier die Gruppe **Internet** ausgewählt (siehe Bild 11).

In bestimmten Fällen kann es erforderlich sein, die Einwahl nur aus bestimmten IP-Netzen zu erlauben. Dann sollte dazu in den **Benutzungsrichtlinien** eine eigene Gruppe angelegt werden, der dann die entsprechenden **Netzwerke** hinzugefügt werden. Diese Gruppe würde dann hier für die OpenVPN-Einwahl ausgewählt.

Über den Reiter **Optionen** können die Einstellungen für Logfiles und Auswertungen angepaßt werden, Abbildung 12 zeigt die entsprechende Maske.

Durch Aktivieren der Option **Daten für Statistiken erfassen** werden alle Verbindungen protokolliert. Beachten Sie dabei bitte, daß es sich um personenbezogene Daten handelt und diese entsprechend erfaßt und ausgewertet werden dürfen.

Über einen Logrotate-Mechanismus können die Logfiles **täglich** oder **wöchentlich neu angelegt** werden. Bei seltener Einwahl kann wöchentlich hier eine Option sein.

Über die **Anzahl archivierter Logfiles** wird festgelegt, wie lange die Loginformationen aufbewahrt werden. Tägliche Rotation und eine Haltezeit von 14 ergeben 14 Tage Loginformationen. Bei wöchentlicher Rotation und einer Haltezeit von 9 ergeben sich ca. 2 Monate Loginformationen.

Über **tägliche, wöchentliche bzw. monatliche Auswertung erstellen** wird ein Report aus den Loginformationen erzeugt, der pro Zertifikat (und damit pro ein-

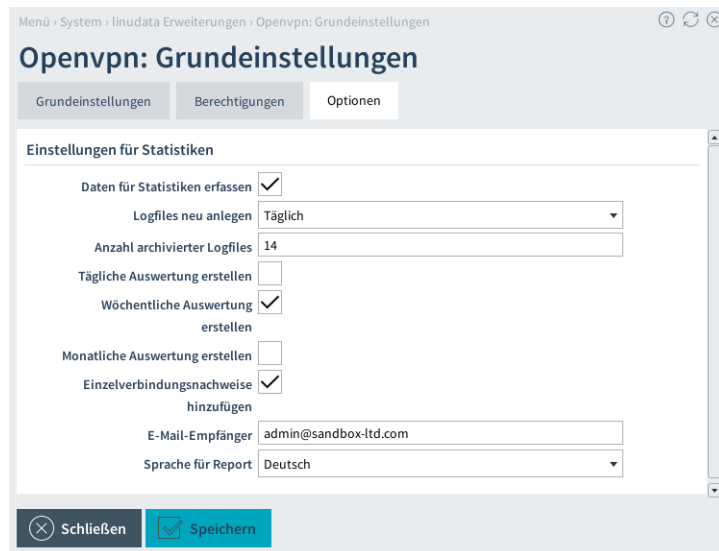


Abbildung 12: OpenVPN Auswertungen

gewählten Nutzer) eine Auswertung der Verbindungszeit und dem übertragenen Datenvolumen enzhält.

Durch Aktivieren der Option **Einzelverbindungsnaachweise hinzufügen** wird zusätzlich bei dem Nutzer die Verbindungszeit mit in den Report aufgenommen. So ist etwa eine Zeiterfassung von Heimarbeitsplätzen möglich.

Der fertige Report wird an die unter **E-Mail-Empfänger** hinterlegte Adresse geschickt. Die **Sprache für Report** kann auf **Deutsch** oder **Englisch** gesetzt werden.

Durch **Speichern** wird die eingestellte Konfiguration gesichert.

### 3.6 Setzen von Firewallregeln

Unter **System - Netzwerk - Firewall - Matrix** werden die Firewalleinstellungen für Zugriffe zwischen IP-Netzen konfiguriert. Abbildung 13 zeigt eine übliche Ansicht nach Anlegen des Client-Netzwerks für OpenVPN.

Hier ist die Default-Policy "Drop", also das Verwerfen aller Pakete (das Symbol mit dem schwarzen Loch). In der Zeile mit **OpenVPN\_ClientNetz** ist sichtbar, daß Zugriffe in alle übrigen Netze gesperrt sind.

Um eingewählten Clients den Zugriff auf Systeme im LAN zu erlauben, muß in der Matrix die entsprechende Verbindung erlaubt werden. Dies kann für einzelne **Dienste** geschehen oder auch für **Alle**, siehe Abb. 14.

Für Funktionstests ist es sinnvoll, wenn der Dienst **Ping** aus dem OpenVPN-Client-Netz in die benötigten Netze erlaubt wird.

Über Hostgruppen oder Subnetze kann in der Matrix auch der Zugriff auf einzelne Systeme beschränkt werden.



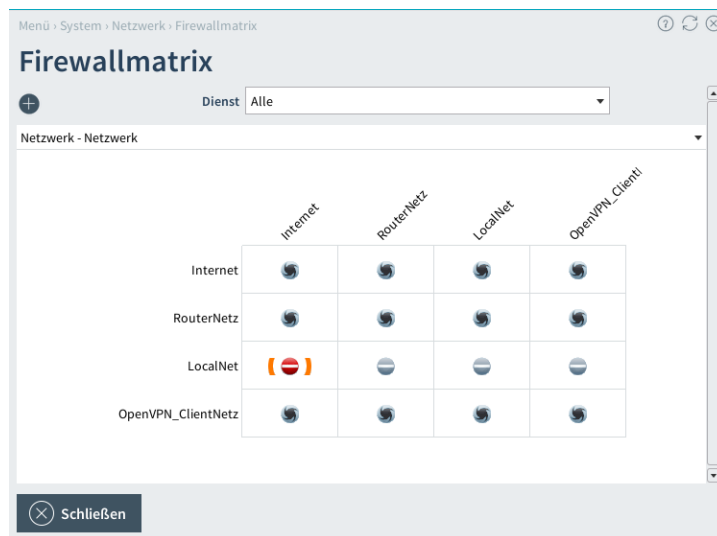


Abbildung 13: Firewall Matrix

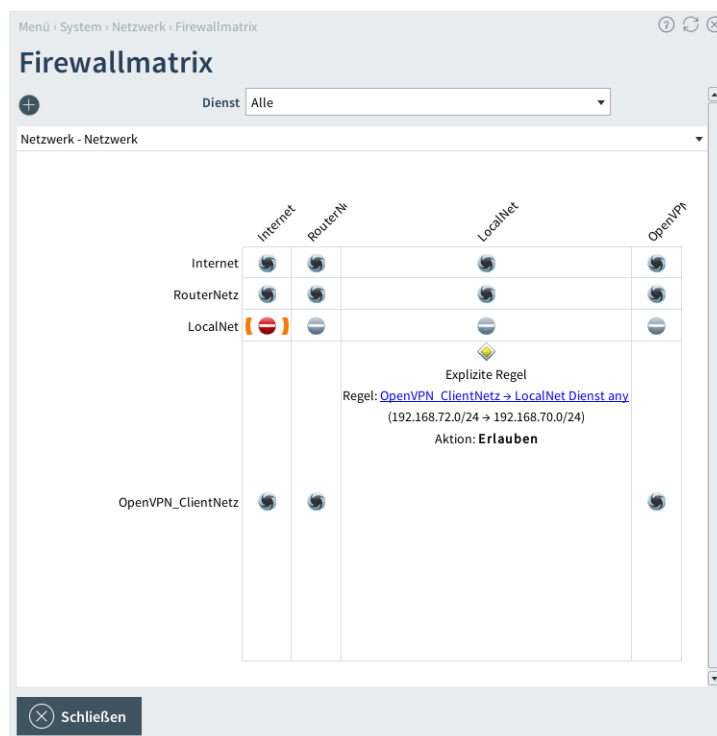


Abbildung 14: Vollzugriff ins LAN erlaubt

## 4 Betrieb

Nach Aktivieren der Collax-Konfiguration ist OpenVPN auf dem Server einsatzbereit.

### 4.1 Export Client-Konfiguration

Zur einfachen Einrichtung der Clients kann unter Menü - System - linudata Erweiterungen - OpenVPN - Client Paket für jeden Benutzer ein Paket mit allen nötigen Konfigurationsdateien erstellt werden.

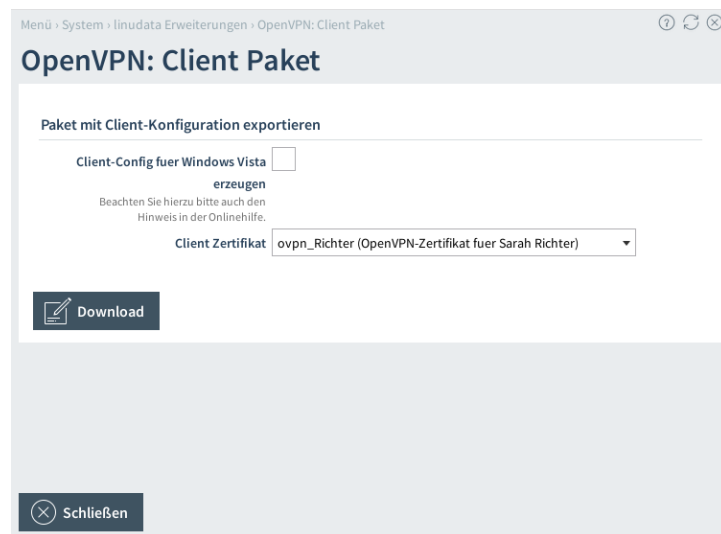


Abbildung 15: Erstellen des Client-Pakets

Über **Client-Config für Windows Vista erzeugen** werden spezielle Optionen in die Client-Config aufgenommen, die im Zusammenspiel OpenVPN 2.0 und Windows Vista notwendig sind.

Unter **Client Zertifikat** wird das Zertifikat des Benutzers ausgewählt, für den das Konfigurationspaket erzeugt wird. Dies Zertifikat wird mit in das Paket aufgenommen.

Wichtig: Das Zertifikat muß bereits erstellt und die Collax-Konfiguration aktiviert sein. Sonst kann es nicht in das Paket geladen werden.

Über **Download** wird das Paket erzeugt und kann über den Browser heruntergeladen werden. Das Client-Zertifikat sollte mit einer Passphrase geschützt sein (siehe dessen Erzeugung in Abschnitt 3.3). Nur mit Kenntnis dieser Passphrase kann der Tunnel aufgebaut werden.

Das erzeugte Paket ist ein einfaches ZIP-Archiv und enthält in einem Unterverzeichnis mehrere Dateien:

- Die Dateien **LIESMICH** und **README** enthalten kurze Informationen zur Installation der Client-Software.

- Die Datei `cbs.ovpn` ist die Konfigurationsdatei. Hier werden u.a. Port, Protokoll und Adresse des OpenVPN-Servers festgelegt. Es ist eine einfache Textdatei, die mit einem einfachen Editor (Wordpad o.ä.) bearbeitet werden kann.
- Drei Dateien mit der Endung `.pem` enthalten das CA-Zertifikat, das Client-Zertifikat sowie den Private Key des Clients (`*.key.pem`).
- Die Datei `ta.key` ist ein auf jedem Collax neu erzeugter statischer Pre-Shared Key, der auf allen beteiligten Clients und auf dem Collax-Server genutzt wird. Alle Datenpakete werden durch eine mit diesem Key erzeugte Prüfsumme gesichert. So ist eine zusätzliche Sicherheit zu den Zertifikaten gegeben, etwa gegen DDOS-Angriffsversuche.

## 4.2 Aktive Verbindungen

Unter Menü - linudata Erweiterungen - OpenVPN - VPN-Status werden alle aktuell verbundenen Clients aufgelistet (siehe Abb. 16).

The screenshot shows a web interface titled "OpenVPN: VPN Status". It includes a breadcrumb trail: "Menü > System > linudata Erweiterungen > OpenVPN: VPN Status". Below the title, it shows the last update time: "Letzte Aktualisierung: Thu Apr 14 17:13:15 2016".

The "Client Liste" section contains a search bar and a table with the following data:

Common Name	Öffentliche IP	Bytes empfangen	Bytes gesendet	Verbunden seit
sarah.richter.sandbox	94.110.29.241	261653	193958	Thu Apr 14 09:50:21 2016
wilhelm.krause.sandbox	83.101.62.57	8722	8804	Thu Apr 14 17:13:00 2016

The "Routing Tabelle" section also has a search bar and a table with the following data:

Common Name	Öffentliche IP-Adresse	Virtuelle IP-Adresse
sarah.richter.sandbox	94.110.29.241	192.168.72.6
wilhelm.krause.sandbox	83.101.62.57	192.168.72.10

At the bottom left, there is a "Schließen" button with a close icon.

Abbildung 16: Aktuell verbundene Clients

In der Tabelle **Client Liste** wird unter **Common Name** der aus dem Zertifikat entnommene Name gezeigt. Darüber sollte der Client (Benutzer) eindeutig identifizierbar sein. Die **Öffentliche IP** gibt die IP-Adresse an, von der die Verbindung aufgebaut wurde. In **Bytes empfangen** und **Bytes gesendet** wird das bisher in dieser Sitzung übertragene Datenvolumen aus Sicht des Collax Servers angezeigt. **Verbunden seit** zeigt, wie lange die aktuelle Sitzung bereits besteht.

In der **Routing-Tabelle** werden alle momentan verbundenen Clients mit Ihrem **Common Name**, der von ihnen genutzten **öffentlichen IP-Adresse** sowie der im OpenVPN-Tunnel genutzten **virtuellen IP-Adresse** aufgelistet.

### 4.3 Sperren von Clients

In bestimmten Situationen muß die Einwahl eines Benutzers deaktiviert werden, etwa bei Verlust des Geräts mit dem installierten Zertifikat oder falls der Benutzer aus dem Unternehmen ausscheidet.

Das Konzept einer CA sieht dafür das Zurückziehen des Zertifikats vor. Zurückgezogene Zertifikate werden in eine Liste gesperrter Zertifikate (die sog. Certificate Revocation List CRL) aufgenommen und damit ungültig.

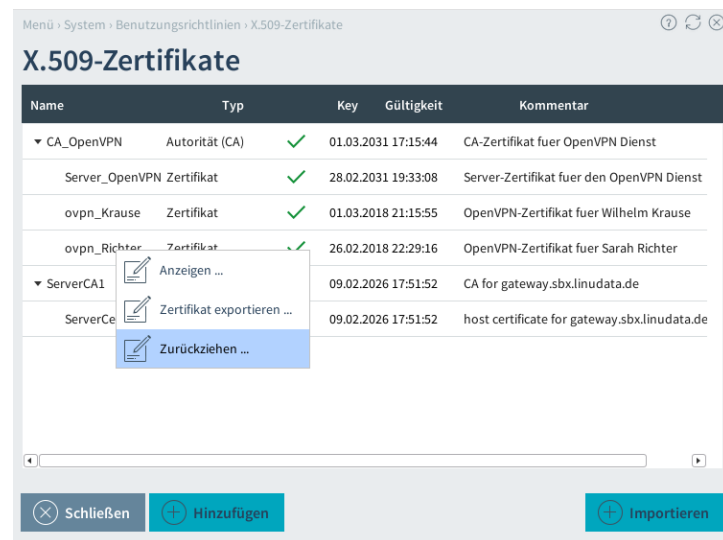


Abbildung 17: Sperren eines Zertifikats

Dazu wird die Zertifikatsübersicht unter **Menü - System - Benutzungsrichtlinien - X.509-Zertifikate** geöffnet. Auf dem betreffenden Zertifikat wird mit Rechtsklick das Kontextmenü geöffnet und die Aktion **Zurückziehen** ausgewählt.

In der folgenden Maske werden zur Sicherheit nochmals **Name** und **Kommentar** des Zertifikats angezeigt sowie das **CA-Passwort** abgefragt. Dieses wird benötigt, weil die CRL von der CA signiert wird, damit die beteiligten Systeme sicher sind, mit der korrekten CRL zu arbeiten (und keine "bereinigte" untergeschoben bekommen).

Der OpenVPN-Dienst auf dem Collax-Server nutzt die zu "seiner" CA gehörende CRL zur Überprüfung der einwählenden Zertifikate.

### 4.4 Ablauf von Zertifikaten

Das Collax System kann u.a. auch den Status der ausgestellten Zertifikate überwachen. Dazu muß die aktive Überwachung (Nagios) unter **Menü - System - Logging/Monitoring - Aktive Überwachung** aktiviert sein.

Im Dashboard der Admin-Oberfläche zeigt die Lampe links oben den aktuellen Nagios-Status an:

- rot (ALARM) - mindestens ein überwachtes Objekt ist ausgefallen.
- gelb (WARNING) - mindestens ein überwachtes Objekt liefert eine Warnung.

- grün (OK) - alle überwachten Objekte sind in Ordnung.

Ein Zertifikat, das in wenigen Tagen ausläuft, löst eine Warnung aus, siehe Abbildung 18.

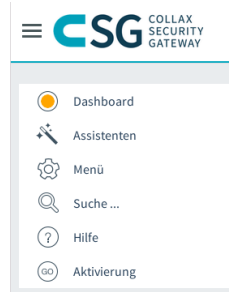


Abbildung 18: Collax zeigt eine Warnung

Ein Klick auf die Lampe öffnet das Dashboard. In dem Bereich **Überwachung** werden in Bild 19 ein Objekt mit einer Warnung und 29 Objekte aufgelistet, die "Ok" sind.

Ein Klick auf den Bereich **Überwachung** öffnet die Nagios-Konsole. Hier werden die problematischen Objekte angezeigt. In diesem Fall ein Zertifikat, das bald abläuft, siehe Abb. 20.

Abgelaufene Zertifikate werden entsprechend rot als Alarm dargestellt.

Ist das Collax System passend eingerichtet, werden die Nagios-Meldungen per E-Mail an den Admin geschickt, so daß hier vor Ablauf eines Zertifikats eine entsprechende Benachrichtigung erfolgt.

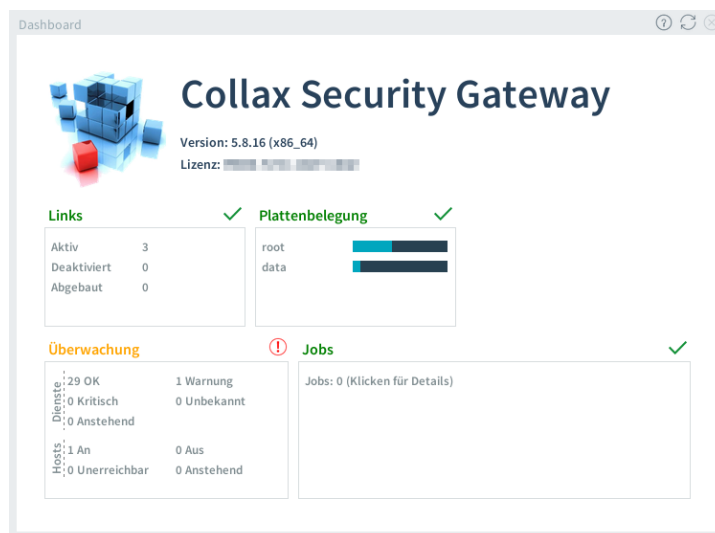


Abbildung 19: Dashboard

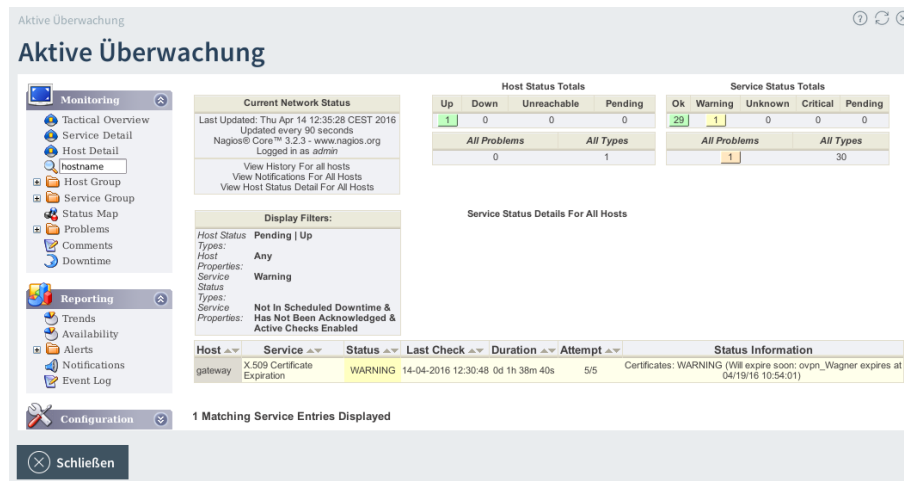


Abbildung 20: Nagios Zustandsübersicht

## 4.5 Verwenden eines anderen Ports

OpenVPN nutzt Port 1194 für den Verbindungsaufbau. Es kann vorkommen, daß sich ein Client in einem Netzwerk befindet, in dem Port 1194 ausgehend gesperrt wird. Es ist möglich, auf dem Collax Server weitere Ports zu konfigurieren, auf denen eine OpenVPN-Einwahl angenommen werden kann.

Eine mögliche Variante ist Port 443, auf dem regulär verschlüsselter Web-Traffic über HTTPS abgewickelt wird. Dieser Port ist in vielen Routern/Firewalls ausgehend offen.

Wenn Port 443 auf dem Collax für OpenVPN genutzt wird, ist die Benutzer-Webaccess-Oberfläche des Collax nicht mehr erreichbar. Als weitere Einschränkung gibt es zunehmend Firewall-Systeme, die auf HTTPS-Verbindungen eine Entschlüsselung durchführen, etwa um einen Virensan durchzuführen. Diese Systeme erwarten HTTP-Daten und werden OpenVPN-Daten verwerfen.

Auf dem Collax Server wird dazu für Port 443 eine Portweiterleitung konfiguriert. Es können mehrere unterschiedliche Ports umgeleitet werden und so unterschiedliche Adressen als Alternativen bereitgestellt werden, beispielsweise 443 und 8443.

Portumleitungen werden in der Admin-Oberfläche **Menü - System - Netzwerk - Portumleitung** verwaltet. Mit **Hinzufügen** wird ein neuer Portforward eingerichtet. **Bezeichnung** und **Kommentar** sollten entsprechend gesetzt werden. Unter **Dienst** wird ein vorhandener Dienst, hier HTTPS d.h. TCP Port 443, ausgewählt.

Abbildung 21 zeigt die entsprechend ausgefüllte Maske.

Dies soll nur auf der externen IP-Adresse des Collax greifen, dazu wird unter **auf diese Links einschränken** der Link mit der externen Adresse ausgewählt.

Unter **IP-Adresse des Ziels** wird die externe IP-Adresse des Collax angegeben. Die Angabe von 127.0.0.1 (Localhost) funktioniert nicht. Als **Zielport** wird 1194 gesetzt.

Menü > System > Netzwerk > Portumleitung > Portumleitung

## Portumleitung

**Portumleitung**

Bezeichnung der Portumleitung:

Kommentar:

Deaktivieren:

Dienst:

Umleitung auf diese Links einschränken:  LocalNetLink (ether) - IP 192.168.70.254 auf eth0  
 RouterLink (ether) - IP 83.223.68.51 auf eth1

Zugriff von Netzen und Hosts in folgenden Gruppen beschränken:  Administrators - Group with administrative powers  
 Fernwartung - Zugriffe zur Fernwartung  
 Internet - Zugriffe aus dem Internet auf Dienste des Collax  
 Users - Basisdienste fuer Benutzer und Netze

IP-Adresse des Ziels:

Zielport:

Protokollieren:

Abbildung 21: Anlegen des Portforwards

Beachten Sie, daß die Portumleitung und die OpenVPN-Konfiguration passen müssen. Sie können beispielsweise keine Portumleitung für TCP einrichten, wenn OpenVPN auf UDP konfiguriert ist.

Menü > System > Netzwerk > Portumleitung

## Portumleitung

Suche ...

Bezeichnung	Kommentar	Dienst	Ziel	Zielport	Aktiv
OpenVPN_443	OpenVPN alternati	https	83.223.68.51	1194	✓
					✓
					✓

Abbildung 22: Eingerichtete Portforwards

## 5 Fehlersuche

### 5.1 Blick ins Logfile

OpenVPN logt in den normalen Syslog. D.h. unter Menü - Status - System - System-Logdateien können die OpenVPN-Einträge abgefragt werden. Dazu wird unter Programm der Wert `openvpn` angegeben (siehe Abb. 23) und auf Anzeigen oder Download geklickt.

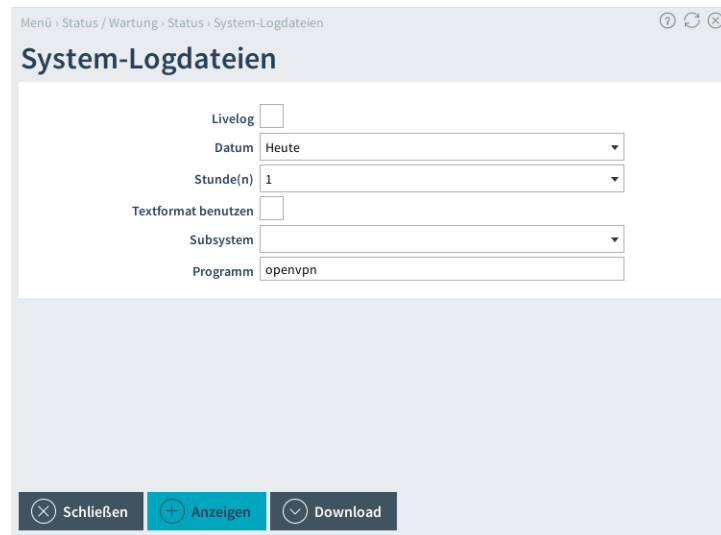


Abbildung 23: Test 1

Abbildung 24 zeigt den Ausschnitt einer erfolgreichen Einwahl im Syslog.

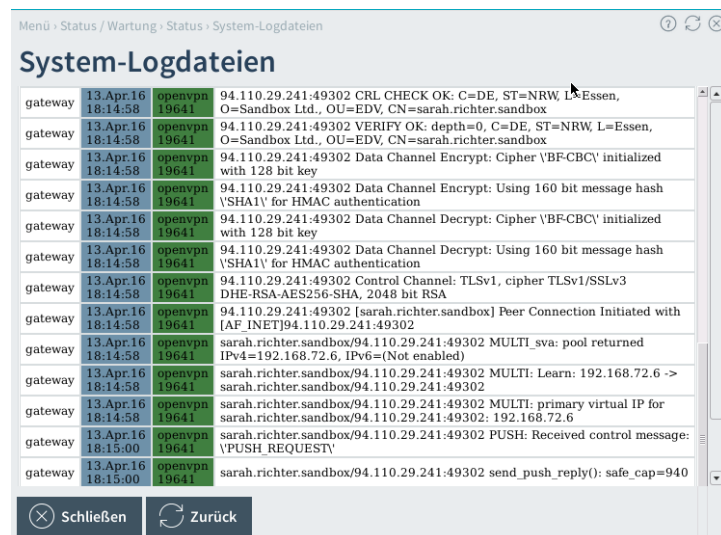


Abbildung 24: Test 2

Alternativ kann das Syslog auch über Kommandozeile mit dem Kommando `tail-sys` angeschaut werden. In Kombination mit `egrep` lassen sich auch nur OpenVPN-



Meldungen und Meldungen im Zusammenspiel mit dem OpenVPN-Client-Netzwerk herausfiltern:

```
admin@gateway:~$ tailsys | egrep "openvpn|192.168.72."

TCP connection established with [AF_INET]94.110.29.241:49304
94.110.29.241:49304 TLS: Initial packet from [AF_INET]94.110.29.241:49304,
  sid=45eb83c5 2bd837ef
94.110.29.241:49304 CRL CHECK OK: C=DE, ST=NRW, L=Essen, O=Sandbox Ltd.,
  OU=EDV, CN=ca.sandbox
94.110.29.241:49304 VERIFY OK: depth=1, C=DE, ST=NRW, L=Essen, O=Sandbox
  Ltd., OU=EDV, CN=ca.sandbox
94.110.29.241:49304 CRL CHECK OK: C=DE, ST=NRW, L=Essen, O=Sandbox Ltd.,
  OU=EDV, CN=sarah.richter.sandbox
94.110.29.241:49304 VERIFY OK: depth=0, C=DE, ST=NRW, L=Essen, O=Sandbox
  Ltd., OU=EDV, CN=sarah.richter.sandbox
94.110.29.241:49304 Data Channel Encrypt: Cipher '\BF-CBC\' initialized
  with 128 bit key
94.110.29.241:49304 Data Channel Encrypt: Using 160 bit message hash '\
  SHA1\' for HMAC authentication
94.110.29.241:49304 Data Channel Decrypt: Cipher '\BF-CBC\' initialized
  with 128 bit key
94.110.29.241:49304 Data Channel Decrypt: Using 160 bit message hash '\
  SHA1\' for HMAC authentication
94.110.29.241:49304 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-
  AES256-SHA, 2048 bit RSA
94.110.29.241:49304 [sarah.richter.sandbox] Peer Connection Initiated
  with [AF_INET]94.110.29.241:49304
sarah.richter.sandbox/94.110.29.241:49304 MULTI_sva: pool returned IPv4=
  192.168.72.6, IPv6=(Not enabled)
sarah.richter.sandbox/94.110.29.241:49304 MULTI: Learn: 192.168.72.6 ->
  sarah.richter.sandbox/94.110.29.241:49304
sarah.richter.sandbox/94.110.29.241:49304 MULTI: primary virtual IP for
  sarah.richter.sandbox/94.110.29.241:49304: 192.168.72.6
sarah.richter.sandbox/94.110.29.241:49304 PUSH: Received control message:
  '\PUSH_REQUEST\'
sarah.richter.sandbox/94.110.29.241:49304 send_push_reply(): safe_cap=940
sarah.richter.sandbox/94.110.29.241:49304 SENT CONTROL [sarah.richter.
  sandbox]: '\PUSH_REPLY,route 192.168.70.0 255.255.255.0,route
  192.168.72.1,topology net30,ping 10,ping-restart 60,ifconfig
  192.168.72.6 192.168.72.5\' (status=1)

fw: allow service any IN=tun0 OUT=eth0 MAC= SRC=192.168.72.6 DST=192.168.
  70.1 LEN=60 TOS=00 PREC=0x00 TTL=127 ID=262 PROTO=ICMP TYPE=8 CODE=0
  ID=1 SEQ=21

sarah.richter.sandbox/94.110.29.241:49304 Connection reset, restarting [-1]
sarah.richter.sandbox/94.110.29.241:49304 SIGUSR1[soft,connection-reset]
  received, client-instance restarting
^C
```

*Hinweis: Die Zeilen sind gekürzt und enthalten im Original immer noch Datum, Uhrzeit, den Hostnamen des Collax, den Prozeß (openvpn bzw. ulogd) und eine Prozess-ID.*

Dieser Ausschnitt zeigt oben den kompletten Einwahlvorgang eines Clients auf Collax-Seite. Danach einen Ping, der von der Firewall als zulässig durchgelassen wird (**allow service any** ist die passende Regel aus der Matrix) und abschließend das Trennen der Verbindung durch den Client.

## 5.2 Verbindungstest zum OpenVPN Dienst

Ist der OpenVPN-Server auf TCP konfiguriert, kann er von außen auch ohne Installation des Clients per **telnet** angesprochen werden. Da im OpenVPN auf Collax TLS aktiviert ist und wir über **telnet** nicht den passenden Schlüssel versenden wollen/können, wird OpenVPN auf eine **telnet**-Anfrage keine Antwort liefern.

Absetzen des Requests von einem möglichen Client-Rechner (Linux, MacOS oder Windows (ggf. **telnet** in der Systemsteuerung aktivieren):

```
C:\Users\richter> telnet gateway.sandbox.dyndns.org 1194
```

Der Request wird jedoch im Syslog erfaßt und liefert dort einen Eintrag:

```
2016 Apr 13 20:09:00 gateway openvpn[19641]: 94.110.29.241:49313
  TLS Error: TLS key negotiation failed to occur within 60 seconds
  (check your network connectivity)
```

D.h. das von dem Client aus der Server grundsätzlich erreichbar ist. Erscheint im Syslog kein Eintrag über den Verbindungsversuch, ist das Netzwerk dazwischen gestört, möglicherweise blockiert eine Firewall den Zugriff auf Port 1194.

Wird UDP genutzt, muß der OpenVPN-Client genutzt werden, um die Verbindung zu testen. Auch hier sollte der Syslog eine eingehende Verbindung protokollieren.

## 5.3 Routing im Client

Wenn der Verbindungsaufbau mittels OpenVPN funktioniert, der Zugriff aus Systeme im Netzwerk hinter dem Collax Server jedoch fehlschlägt, kann fehlendes Routing auf dem Client die Ursache sein.

Zum Setzen der notwendigen Routen sind unter Windows Admin-Berechtigungen notwendig. Daher sollte der OpenVPN Client auch mit entsprechenden Rechten ausgeführt werden.

Zur Kontrolle kann in einer Eingabeaufforderung mittels **route print -4** die aktuelle IPv4-Routingtabelle ausgegeben werden.

Abb. 25 zeigt die Routingtabelle bei einer korrekt funktionierenden OpenVPN Verbindung. Unter **Schnittstelle** ist deutlich zu sehen, daß mehrfach die dem Client zugewiesene IP-Adresse aus dem Client-Netzwerk auftaucht.

Unter **Netzwerkziel** ist eine Zeile zu finden, die den Eintrag für das Netzwerk hinter dem Collax (hier 192.168.70.0) enthält. Fehlt ein solcher Eintrag, wurde die Route nicht gesetzt. Prüfen Sie dazu das Logfile des Clients auf mögliche Hinweise. Ursache sind meist fehlende Berechtigungen.

```

C:\Windows\system32\cmd.exe

C:\Users\claus>route print -4
=====
Schnittstellenliste
14...00 ff 3e de 40 88 .....TAP-Windows Adapter V9
10...52 54 00 a2 0d bb .....Red Hat VirtIO Ethernet Adapter
1.....Software Loopback Interface 1
11...00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter
12...00 00 00 00 00 00 e0 Microsoft-6zu4-Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
15...00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #2
=====

IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel      Netzwerkmaste      Gateway      Schnittstelle      Metrik
  0.0.0.0           0.0.0.0           192.0.2.1    192.0.2.98         261
  127.0.0.0        255.0.0.0         Auf Verbindung  127.0.0.1         306
  127.0.0.1        255.255.255.255  Auf Verbindung  127.0.0.1         306
  127.255.255.255  255.255.255.255  Auf Verbindung  127.0.0.1         306
  192.0.2.0        255.255.255.0    Auf Verbindung  192.0.2.98        261
  192.0.2.98       255.255.255.255  Auf Verbindung  192.0.2.98        261
  192.0.2.255     255.255.255.255  Auf Verbindung  192.0.2.98        261
  192.168.70.0    255.255.255.0    192.168.72.5  192.168.72.6      30
  192.168.72.1    255.255.255.255  192.168.72.5  192.168.72.6      30
  192.168.72.4    255.255.255.252  Auf Verbindung  192.168.72.6      286
  192.168.72.6    255.255.255.255  Auf Verbindung  192.168.72.6      286
  192.168.72.7    255.255.255.255  Auf Verbindung  192.168.72.6      286
  224.0.0.0        240.0.0.0         Auf Verbindung  127.0.0.1         306
  224.0.0.0        240.0.0.0         Auf Verbindung  192.0.2.98        261
  224.0.0.0        240.0.0.0         Auf Verbindung  192.168.72.6      286
  255.255.255.255  255.255.255.255  Auf Verbindung  127.0.0.1         306
  255.255.255.255  255.255.255.255  Auf Verbindung  192.0.2.98        261
  255.255.255.255  255.255.255.255  Auf Verbindung  192.168.72.6      286
=====
Ständige Routen:
  Netzwerkadresse   Netzmaske   Gatewayadresse   Metrik
  0.0.0.0           0.0.0.0     192.0.2.1        Standard
=====
C:\Users\claus>

```

Abbildung 25: Auf dem Client gesetzte Routen

## 6 Unterstützte Geräte

### 6.1 Windows

#### 6.1.1 Installation

Laden Sie den OpenVPN-Client (OpenVPN 2.3.9 oder neuer) aus dem Internet herunter. Eine Anlaufstelle ist beispielsweise [www.heise.de/download](http://www.heise.de/download).

Den Client gibt es für 32- und 64-Bit Installationen. Wenn Sie nicht sicher sind, welche Sie benötigen, öffnen Sie das Startmenü und öffnen Sie das Kontextmenü von Computer durch Rechtsklick und klicken Sie dann auf **Eigenschaften**. Dort wird unter **Systemtyp** die Bitzahl angezeigt, siehe Abb. 26.

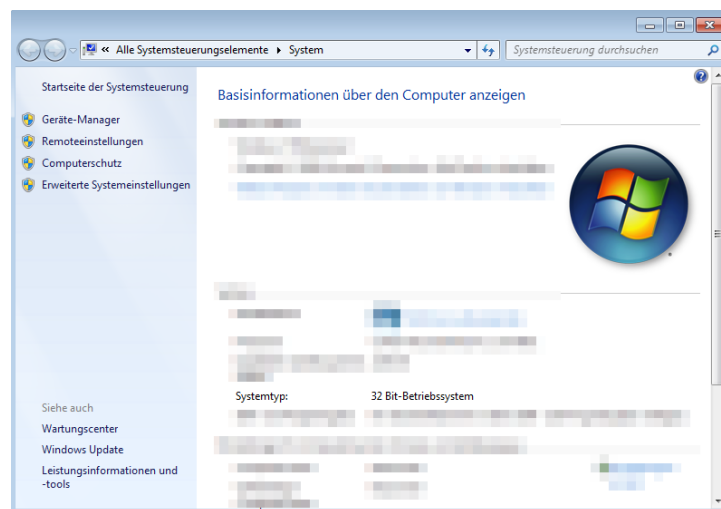


Abbildung 26: 32-Bit Client wird benötigt

Die Installation des Clients muß durch einen lokalen Benutzer mit administrativen Rechten durchgeführt werden. Dazu im Explorer auf der Datei im Kontextmenü (rechte Maustaste) den Punkt **Als Administrator ausführen** auswählen (siehe Abb. 27).

Die Installation selbst erfolgt wie bei Windows Programmen üblich durch Bestätigen von Lizenzhinweis und Installationspfad, siehe Bilder 28 bis 35.

Im ersten Schritt muß bestätigt werden, daß Sie wirklich das Programm ausführen wollen. Installieren Sie nur Softwarepakete aus seriösen Quellen.

Die Komponentenauswahl (Abb. 31) können Sie ohne Änderungen übernehmen.

Auch den Installationspfad (siehe Abb. 32) können Sie übernehmen. Bei einem deutschen Windows wird nach **C:\Programme** installiert.

Während der Installation wird noch ein TAP-Treiber installiert (zum Zugriff von OpenVPN auf das Netzwerkinterface), dies muß bestätigt werden (Abb. 33).

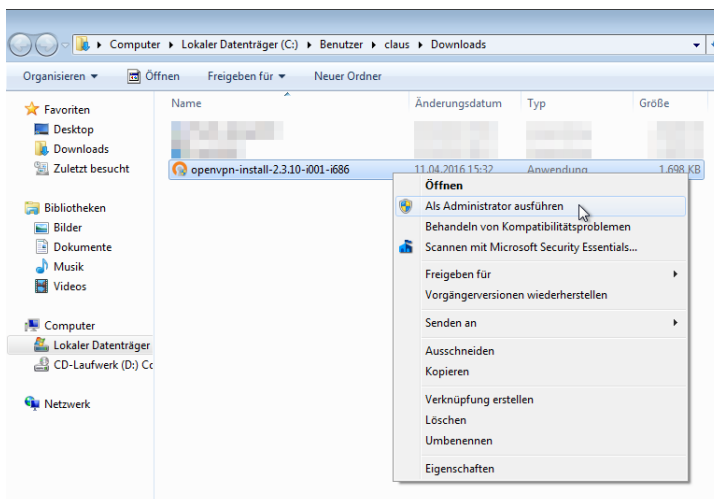


Abbildung 27: Installation mit Admin-Rechten

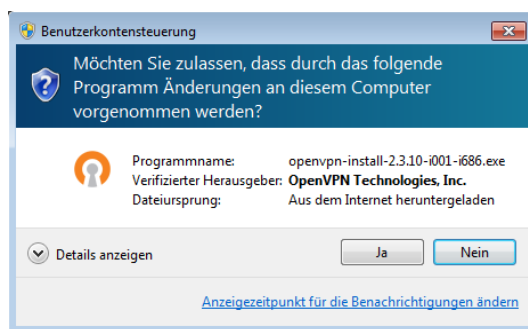


Abbildung 28: Bestätigen der Installation

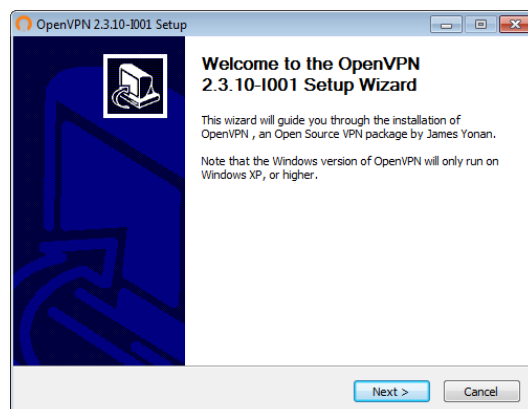


Abbildung 29: Beginn der Installation

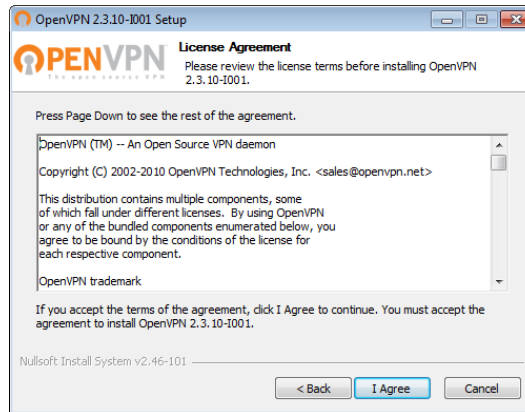


Abbildung 30: Lizenzvereinbarung

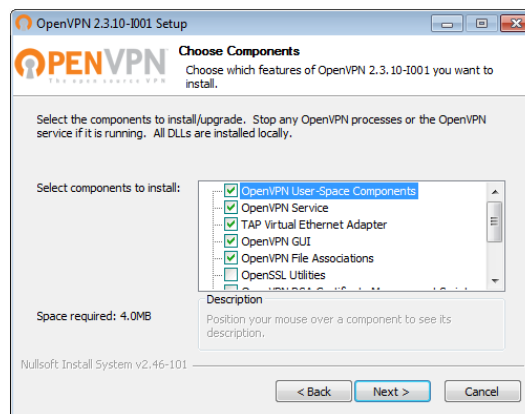


Abbildung 31: Komponentenauswahl

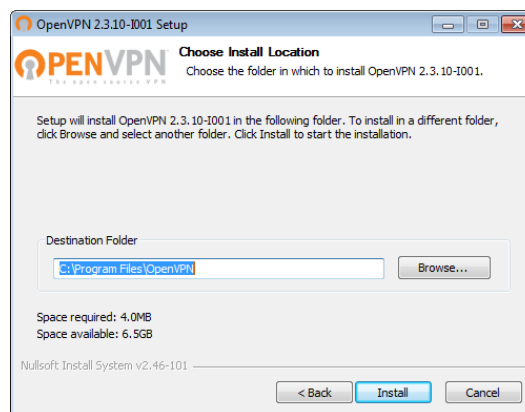


Abbildung 32: Installationspfad

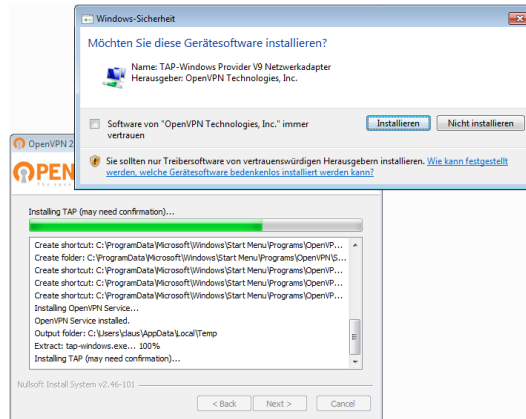


Abbildung 33: Installation des TAP-Treibers

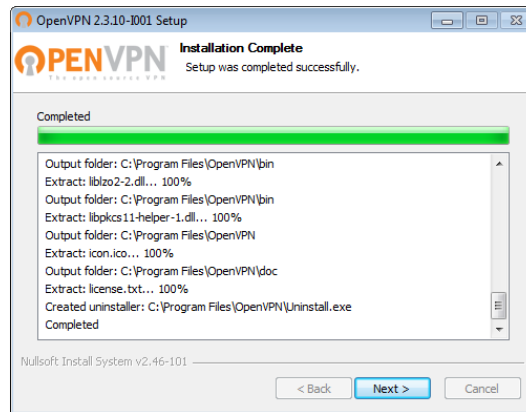


Abbildung 34: Installationsverlauf

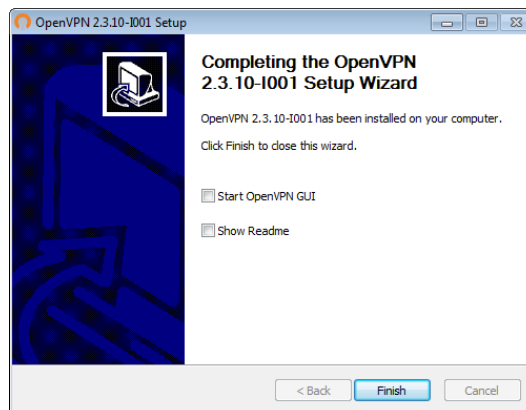


Abbildung 35: Installation abgeschlossen

Nach erfolgreicher Installation ist auf dem Desktop das Icon **OpenVPN GUI** installiert. Darüber wird der OpenVPN Client gestartet.

Da OpenVPN in die Netzwerkkonfiguration eingreifen muß, benötigt es Admin-Rechte. Bei einem beschränkten Nutzeraccount kann es entweder jeden Mal über **Als Administrator ausführen** gestartet werden oder es wird einmal entsprechend modifiziert.

Dazu wird auf dem Icon über die rechte Maustaste das Kontextmenü geöffnet und der Punkt **Eigenschaften** gewählt. Über den Reiter **Kompatibilität** läßt sich unten im Abschnitt **Berechtigungsstufe** die Option **Programm als Administrator ausführen** aktivieren (siehe Abb. 37).

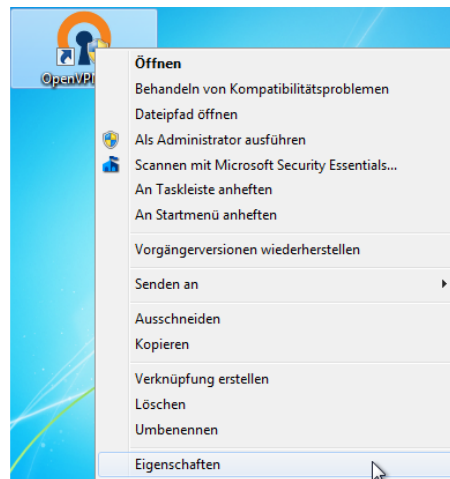


Abbildung 36: Kontextmenü des OpenVPU GUI Icons

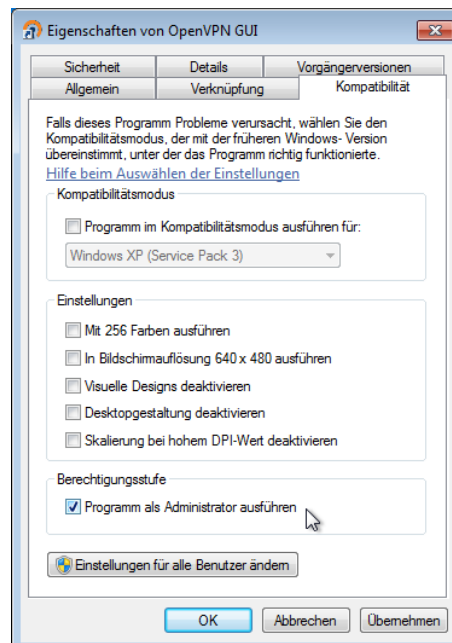


Abbildung 37: Dauerhafter Start mit Admin-Rechten



### 6.1.2 Konfiguration unter Windows

Der Benutzer erhält alle nötigen Konfigurationsdateien in einem ZIP-Archiv. Wird dies geöffnet, enthält es einen Ordner mit einer Anzahl Dateien.

Dieser Ordner wird nach `C:\Programme\OpenVPN\config` kopiert bzw. ausgepackt. Dazu sind evt. Administratorrechte nötig.

In diesem Ordner sind die vorbereitete Konfigurationsdatei sowie die nötigen Schlüsseldateien enthalten.

### 6.1.3 Betrieb unter Windows

Durch Doppelklick auf das OpenVPN GUI Icon auf dem Desktop wird der OpenVPN Client gestartet.

Der Client selbst bettet sich in die Symbolleiste rechts unten ein, siehe Abb. 38.



Abbildung 38: OpenVPN Client in der Symbolleiste

Auf diesem Symbol kann durch Rechtsklick das Kontextmenü geöffnet werden. Der oberste Punkt **Verbinden** startet den Verbindungsaufbau (siehe Abb. 39).

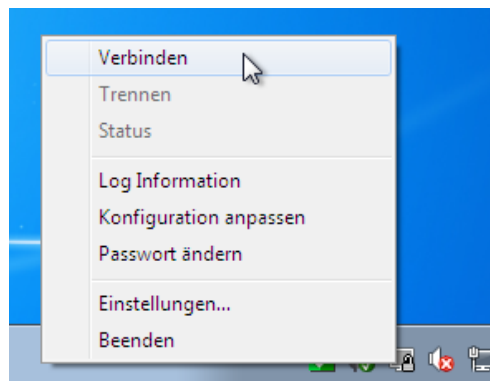


Abbildung 39: Verbindungsaufbau auslösen

Ein Fenster mit Logininformationen öffnet ein weiteres, in dem das **Passwort** für OpenVPN abgefragt wird. Hier muß die Passphrase angegeben werden, mit der der private Schlüssel des Benutzerzertifikats gesichert wurde, siehe Abschnitt 3.3 und Abb. 40.

Wird hier die falsche Passphrase eingegeben, wird bei den Logininformationen ein Eintrag `soft.private.key-password-failure` festgehalten und das **Passwort** wird erneut abgefragt.

Während der Aushandlung der Verbindung färbt sich das OpenVPN Symbol unten rechts gelb.

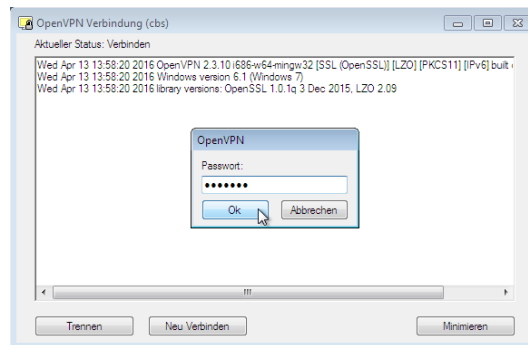


Abbildung 40: Verbindungsaufbau auslösen

Wird der Tunnel erfolgreich aufgebaut, schließt sich das Fenster mit den Logininformationen, das Symbol unten rechts wird grün und zeigt damit den aktiven Tunnel an. Zudem wird ein kleiner Hinweis über den erfolgreichen Verbindungsaufbau und die zugewiesene IP Adresse angezeigt, siehe auch Abb. 41.

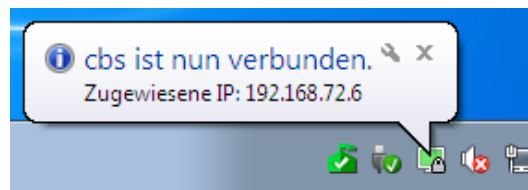


Abbildung 41: Verbindung hergestellt

#### 6.1.4 Funktionstest

Ein einfacher Funktionstest ist über Ping möglich. Dazu wird im Windows-System eine Eingabeaufforderung geöffnet (Start - Durchsuchen - cmd) und ping mit einer internen IP-Adresse im LAN aufgerufen. Funktioniert der Tunnel, sollten 3 Ping-Antworten erfolgreich zurückkommen (erkennbar an der Zeitangabe, siehe Abb. 42).

Funktioniert der Ping nicht, kommt die Meldung **Zielhost nicht erreichbar**. Dann ist zu prüfen, ob der angepingte Rechner überhaupt im LAN erreichbar ist und ob er den Collax als Gateway nutzt. Ggf. muß dann auf dem Rechner noch eine Netzroute für das OpenVPN-Client-Netz zum Collax gesetzt werden. In jedem Fall sollte der Collax-Server mit seiner internen IP-Adresse auf Ping antworten.

In der Collax Administrationsoberfläche werden unter Menü - linudata Erweiterungen - OpenVPN - VPN Status alle aktuell verbundenen Clients angezeigt, siehe auch Abschnitt 4.2 auf Seite 17).

```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\claus>ping 192.168.70.1

Ping wird ausgeführt für 192.168.70.1 mit 32 Bytes Daten:
Antwort von 192.168.70.1: Bytes=32 Zeit=43ms TTL=63
Antwort von 192.168.70.1: Bytes=32 Zeit=31ms TTL=63
Antwort von 192.168.70.1: Bytes=32 Zeit=31ms TTL=63
Antwort von 192.168.70.1: Bytes=32 Zeit=34ms TTL=63

Ping-Statistik für 192.168.70.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 31ms, Maximum = 43ms, Mittelwert = 34ms

C:\Users\claus>_

```

Abbildung 42: Pingtest auf einen Server im LAN

### 6.1.5 Anpassen der Konfiguration

In dem ausgepackten Verzeichnis mit den Zertifikaten liegt die Konfigurationsdatei `cbs.ovpn`. Dies ist eine einfache Textdatei, in der die nötigen Parameter festgelegt werden.

Wird diese in Windows durch Doppelklick mit dem **Editor** geöffnet, wird der Inhalt oft als eine einzige Endloszeile dargestellt. Mit **Wordpad** läßt sich die Datei jedoch einwandfrei bearbeiten. Beachten Sie dabei, daß **Wordpad** u.U. als Administrator ausgeführt werden muß, damit die Datei verändert und gespeichert werden kann.

In der Datei werden unter `remote` die Gegenstelle und der genutzte Port (Default 1194) und über `proto` das Protokoll TCP oder UDP festgelegt. Bei Änderungen auf dem Einwahlserver müssen diese Werte evt. angepaßt werden.

## 6.2 Linux

Stellvertretend für die vielen Linux Distributionen wird hier die Einrichtung des Clients unter Ubuntu 15.10 (Wily Werewolf) gezeigt.

### 6.2.1 Installation

Netzwerkverbindungen werden bei den meisten Linux Distributionen im **Network-Manager** verwaltet. Hier muß ggf. ein Plugin für OpenVPN nachinstalliert werden. Dies geschieht entweder im Software-Manager oder auf Kommandozeile in einem Terminal mittels

```
sudo apt-get install network-manager-openvpn-gnome
```

### 6.2.2 Konfiguration

Der Benutzer erhält alle nötigen Konfigurationsdateien in einem ZIP-Archiv. Wird dies geöffnet, enthält es einen Ordner mit einer Anzahl Dateien.

Dieser Ordner wird in das Homeverzeichnis des Benutzers ausgepackt. In diesem Ordner sind die vorbereitete Konfigurationsdatei sowie die nötigen Schlüsseldateien enthalten.

Der Network-Manager verbirgt sich (hier) hinter dem linken Logo in der Leiste ganz oben (das Icon mit den beiden Pfeilen rauf und runter). Klickt man es an, klappt ein Menü auf, daß beispielsweise die WLANs in der Nähe anzeigt und weiter unten den Punkt **Verbindungen bearbeiten** enthält (siehe Abb. 43).

Diesen Punkt klicken wir an. Das Menü verschwindet und ein Fenster mit den existierenden Netzwerkverbindungen öffnet sich (Abb. 44).

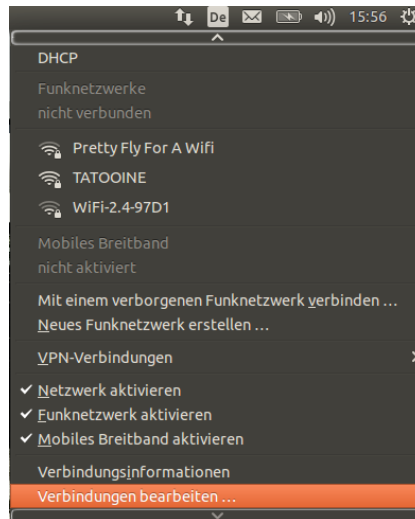


Abbildung 43: Verbindungs-Manager

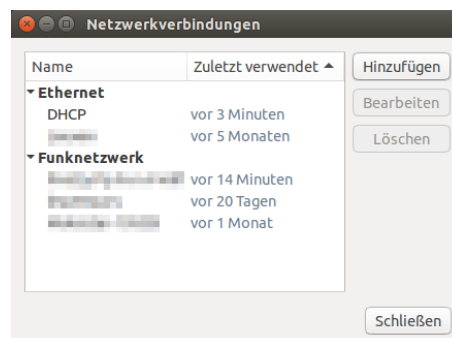


Abbildung 44: Vorhandene Verbindungen

Dort wird über **Hinzufügen** eine neue Verbindung angelegt. Als Typ muß **OpenVPN** ausgewählt werden. Fehlt in der Liste (siehe Abb. 45) diese Option, fehlt dem Network-Manager das Erweiterungsmodul für OpenVPN. Dies muß zuerst installiert werden.

Der **Verbindungsname** wird passend gesetzt. Unter diesem Namen ist die konfigurierte Verbindung nachher im Network-Manager zu finden.

Unter **Gateway** wird der Hostname oder die IP-Adresse des Collax Servers eingetragen.

Als **Art** der Legitimierung werden **Zertifikate** eingesetzt. Unter **Zertifikat des Benutzers**, **Zertifikat der Zertifizierungsstelle (CA)** und **Privater Schlüssel**

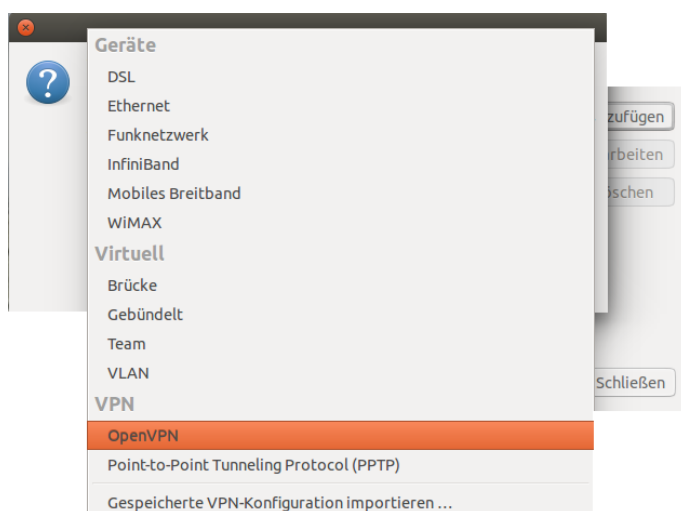


Abbildung 45: Auswahl der Verbindungsart

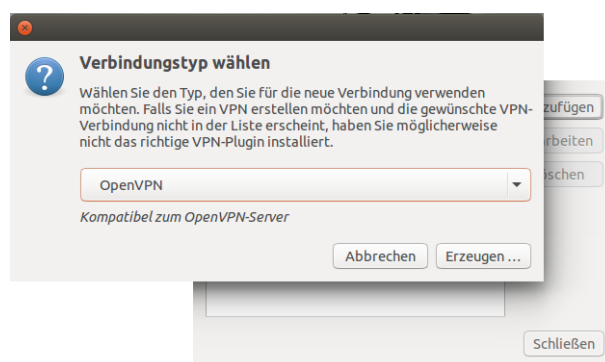


Abbildung 46: Verbindungstyp wird festgelegt

werden die im ausgepackten Client-Paket enthaltenen Files ausgewählt. Evt. muß das **Passwort für den privaten Schlüssel** gesetzt werden, damit die Konfiguration gespeichert werden kann.

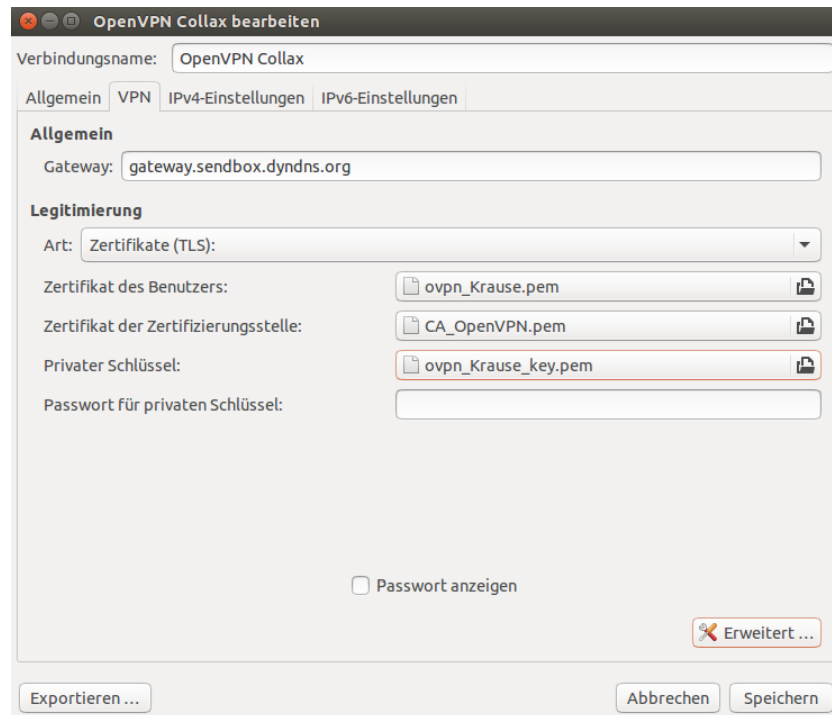


Abbildung 47: Konfiguration von Gateway und Zertifikaten

Über **Erweitert** wird ein weiteres Fenster geöffnet, in dem weitere Anpassungen vorgenommen werden.

Auf dem Reiter **Allgemein** werden die Optionen **LZO-Kompression verwenden** und **abhängig von der Einstellung im Collax System TCP-Verbindung verwenden** aktiviert (Abb. 48).

Auf dem Reiter **TLS-Legitimierung** wird die Option **Zusätzliche TLS-Legitimierung verwenden** aktiviert. Unter **Schlüsseldatei** wird die Datei **ta.key** aus dem Configpaket ausgewählt. Für die **Schlüsselrichtung** wird **1** gewählt.

Mit **OK** wird das Fenster geschlossen und mit **Speichern** die Verbindung gespeichert.

Sie wird dann in der **Übersicht** (Abb. 50) angezeigt und kann dort jederzeit mit **Bearbeiten** geändert werden.

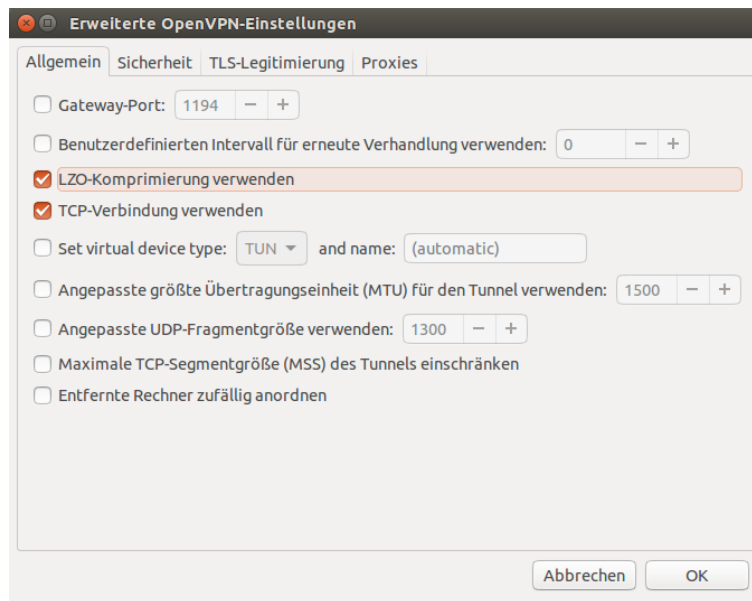


Abbildung 48: TCP oder UDP verwenden

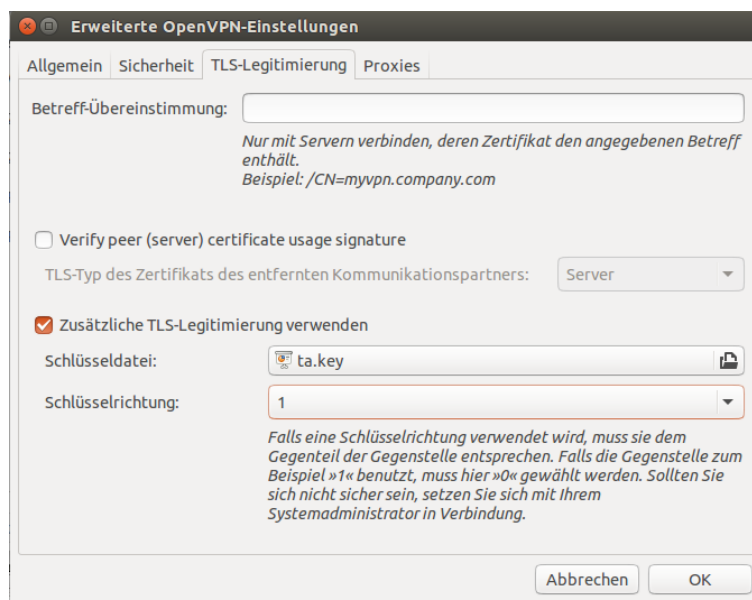


Abbildung 49: Verwendung von TLS aktivieren



Abbildung 50: Die neu angelegte Verbindung

### 6.2.3 Betrieb

Um den OpenVPN Tunnel aufzubauen, wird auf das Network-Manager Symbol in der Leiste oben angeklickt. In dem auflappenden Fenster kann über den Punkt **VPN-Verbindungen** ein weiteres Fenster geöffnet werden, in dem auch die neue OpenVPN Verbindung enthalten ist, siehe Abb. 51.

Linux versucht nun die Einwahl zum OpenVPN Server. Ist diese geglückt, wird das Symbol des Network-Managers um ein Schloss-Symbol erweitert und für kurze Zeit ein Texthinweis über die erfolgreiche Einwahl eingeblendet (ähnlich Abb. 52).

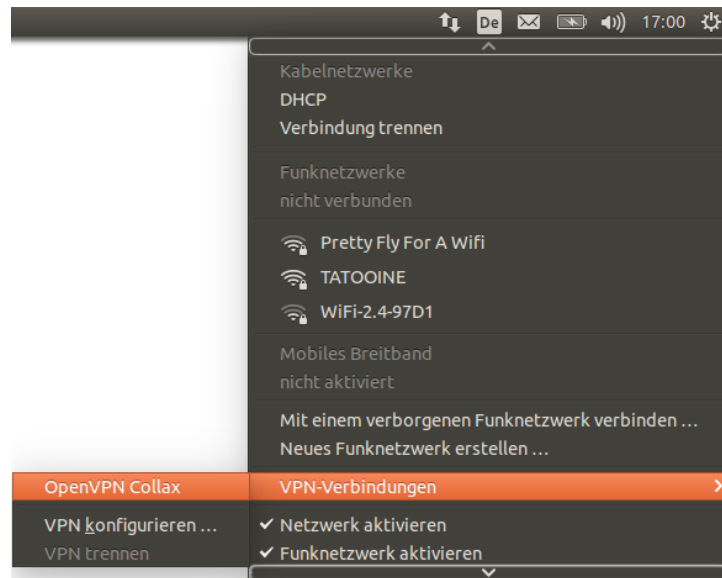


Abbildung 51: Ubuntu 9

Das Trennen der OpenVPN-Verbindung erfolgt ebenfalls über den Network-Manager. Durch Anklicken des Symbols in der Leiste oben öffnet sich die Übersicht, dort ist unterhalb der OpenVPN-Verbindung die Funktion **Verbindung trennen** zu finden.



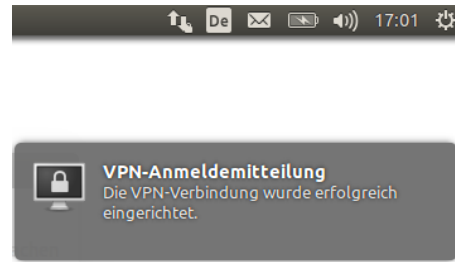


Abbildung 52: Ubuntu 10

#### 6.2.4 Funktionstest

Ein einfacher Funktionstest ist über Ping möglich. Dazu wird in einem Terminal das Kommando `ping` mit einer internen IP-Adresse im LAN aufgerufen. Funktioniert der Tunnel, werden kontinuierlich Ping-Antworten mit der jeweiligen Laufzeit ausgegeben. Dieser Ping kann mit `CTRL-C` beendet werden.

Funktioniert der Ping nicht, kommt die Meldung `Destination Host Unreachable`. Dann ist zu prüfen, ob der angepingte Rechner überhaupt im LAN erreichbar ist und ob er den Collax als Gateway nutzt. Ggf. muß dann auf dem Rechner noch eine Netzroute für das OpenVPN-Client-Netz zum Collax gesetzt werden. In jedem Fall sollte der Collax-Server mit seiner internen IP-Adresse auf Ping antworten.

### 6.3 Mac OS X

Für Mac OS X gibt es die OpenVPN-Client-Software `Tunnelblick`.

#### 6.3.1 Installation

Unter <http://tunnelblick.net> kann ein aktuelles Installationspaket für Mac OS X heruntergeladen werden. Per Doppelklick wird die Installation des Pakets gestartet.

Dieser öffnet ein Fenster, in dem ein Symbol `Tunnelblick` und ein Symbol zur Dokumentation angezeigt werden (siehe Abb. 53). Ein Doppelklick auf `Tunnelblick` führt zuerst zu einer Sicherheitsabfrage (Abb. 54) und dann zur Passwortabfrage des Benutzers, damit der Zugriff in das Programmverzeichnis gewährt wird (Abb. 55).

Nach erfolgreicher Installation startet `Tunnelblick` und fragt, ob es neue Konfiguration erstellen soll. Dies verneinen wir durch Anklicken von `Ich habe Konfigurationsdateien`, siehe Abb. 56.

`Tunnelblick` wird in der OS X Oberfläche bei den Programmen einsortiert. Das Icon kann in die Dockleiste unten gezogen werden und ist so schnell erreichbar (Abb. 57).



Abbildung 53: Starten der Installation

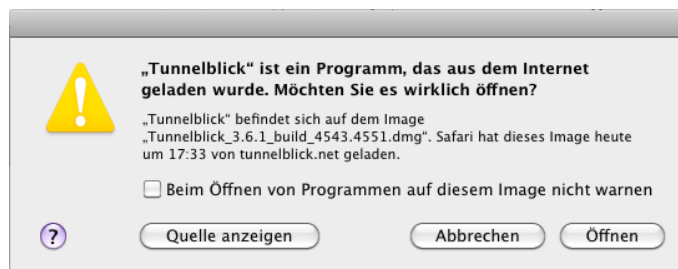


Abbildung 54: Sicherheitsabfrage

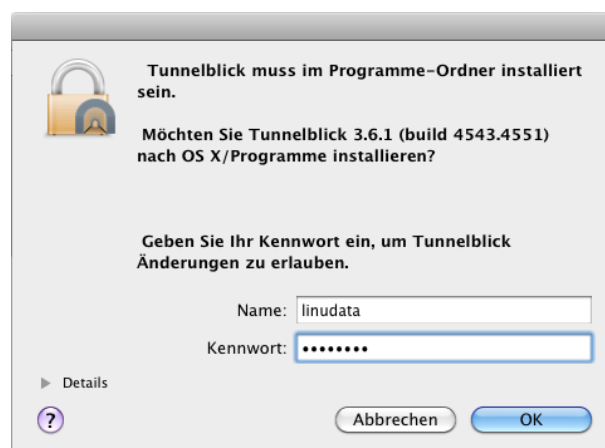


Abbildung 55: Berechtigung zur Installation

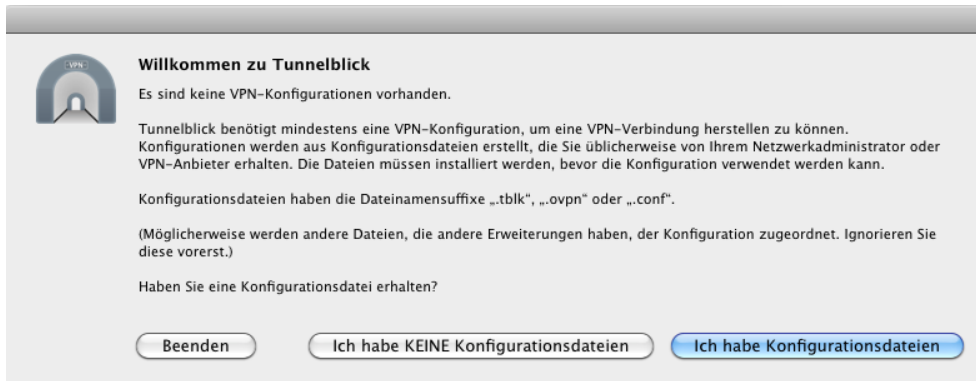


Abbildung 56: Installation abgeschlossen



Abbildung 57: Tunnelblick Icon ins Dock gezogen

### 6.3.2 Konfiguration

Der Benutzer erhält alle nötigen Konfigurationsdateien in einem ZIP-Archiv. Wird dies geöffnet, enthält es einen Ordner mit einer Anzahl Dateien.

Dieser Ordner wird in das Homeverzeichnis des Benutzers ausgepackt. In diesem Ordner sind die vorbereitete Konfigurationsdatei sowie die nötigen Schlüsseldateien enthalten.

Dieses Verzeichnis wird im **Finder** geöffnet. Dort liegt die Datei `cbs.ovpn` mit der Konfiguration. Diese Datei ist erkennbar am Icon bereits **Tunnelblick** zugeordnet und kann mittels Doppelklick importiert werden.

Ein Fenster öffnet sich und fragt, für welchen Benutzer die Konfiguration importiert werden soll. Üblicherweise ist dies nur der aktuelle Benutzer, siehe Abb. 58.

Auch hier erfolgt wieder eine Sicherheitsabfrage für Anpassungen am System (Abb. 59). Am Ende kommt eine Meldung zum erfolgreichen Import der Konfiguration, ähnlich Abb. 60.

### 6.3.3 Betrieb

Wenn die Konfiguration importiert ist, wird **Tunnelblick** gestartet und zeigt das Hauptfenster ähnlich Abbildung 61. In der Spalte links ist der Name der importierten Konfiguration zu sehen. Es ist auch möglich, mehrere Tunnel unter **Tunnelblick** zu verwalten. Dann muß der gewünschte in der linken Spalte jeweils ausgewählt werden.

Im rechten Teil gibt es zwei Reiter **Protokoll** und **Einstellungen**. Unter **Protokoll** sind Loginformationen über den Verbindungsaufbau zu finden. In den **Einstellun-**

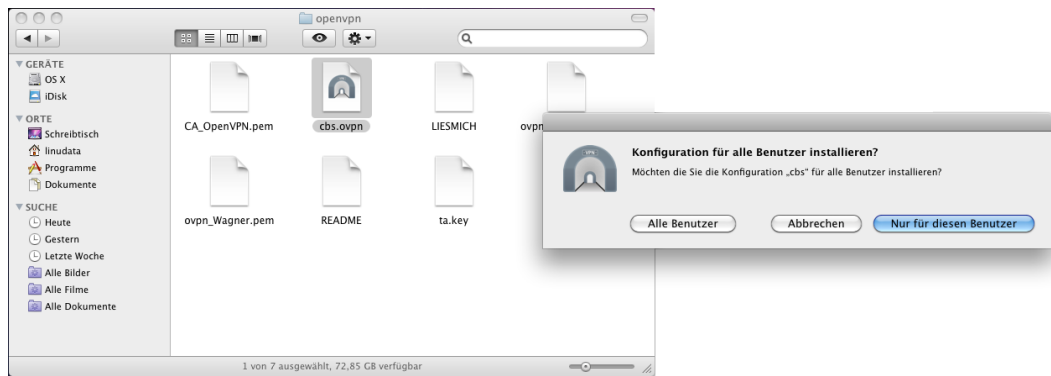


Abbildung 58: Konfigurationsverzeichnis im Finder

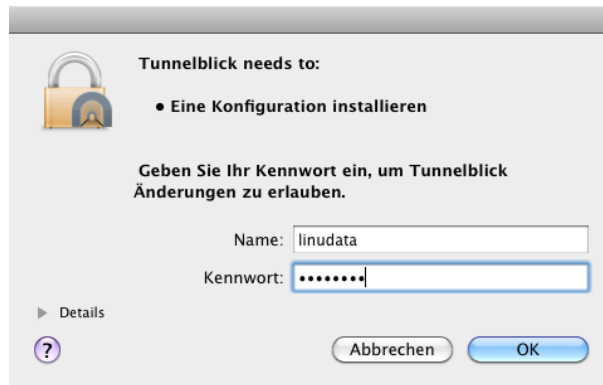


Abbildung 59: Berechtigungsanfrage

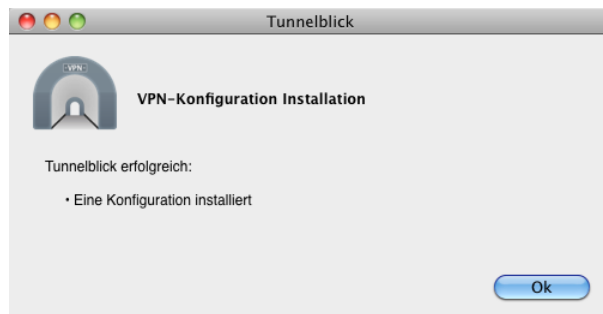


Abbildung 60: Konfiguration importiert

gen können noch Anpassungen vorgenommen werden, die aber mit der vorbereiteten Konfigurationsdatei nicht notwendig sind.

Der Tunnelaufbau wird über den Schalter **Verbinden** unten rechts gestartet. Da das Zertifikat zur Verschlüsselung mit einer Passphrase gesichert ist, wird diese in einem Fenster abgefragt, siehe Bild 62. Hier besteht die Möglichkeit, diese Passphrase im **Schlüsselbund** des Benutzers abzulegen.

Wird die falsche Passphrase eingegeben, erscheint eine Fehlermeldung ähnlich Abbildung 63.

Während des Verbindungsaufbaus erscheint ein Statusfenster, welches in der oberen rechten Ecke des Desktops Informationen liefert (Abb. 64).

Bei erfolgreichem Verbindungsaufbau zeigt das Hauptfenster von **Tunnelblick** in der Titelleiste oben **Verbunden** an. Gleichzeitig wird der Schalter **Verbinden** ausgegraut (siehe Abb. 65).



Abbildung 61: Hauptfenster

Zum Trennen einer aufgebauten Verbindung wird der Schalter **Trennen** geklickt. In der Titelleiste wird zunächst **Trennen der Verbindung** und dann **Getrennt** angezeigt. Nun ist der Schalter **Trennen** ausgegraut und der zum erneuten **Verbinden** wieder erreichbar (Abb. 66).

Schlägt der Verbindungsaufbau fehl, kann dies unterschiedliche Ursachen haben. Kapitel 5 auf Seite 22 liefert einige Hinweise zur Fehlersuche.

Auf Client-Seite kann das Logfile bereits Hinweise liefern. Abb. 67 zeigt beispielhaft die Meldung eines abgelaufenen Zertifikats. Über den Schalter **Diagnoseinformationen in die Zwischenablage kopieren** kann das Logfile in eine Textdatei eingefügt und weiter untersucht werden.

### 6.3.4 Funktionstest

Ein einfacher Funktionstest ist über Ping möglich. Dazu wird in einem **Terminal** das Kommando `ping` mit einer internen IP-Adresse im LAN aufgerufen. Funktioniert der

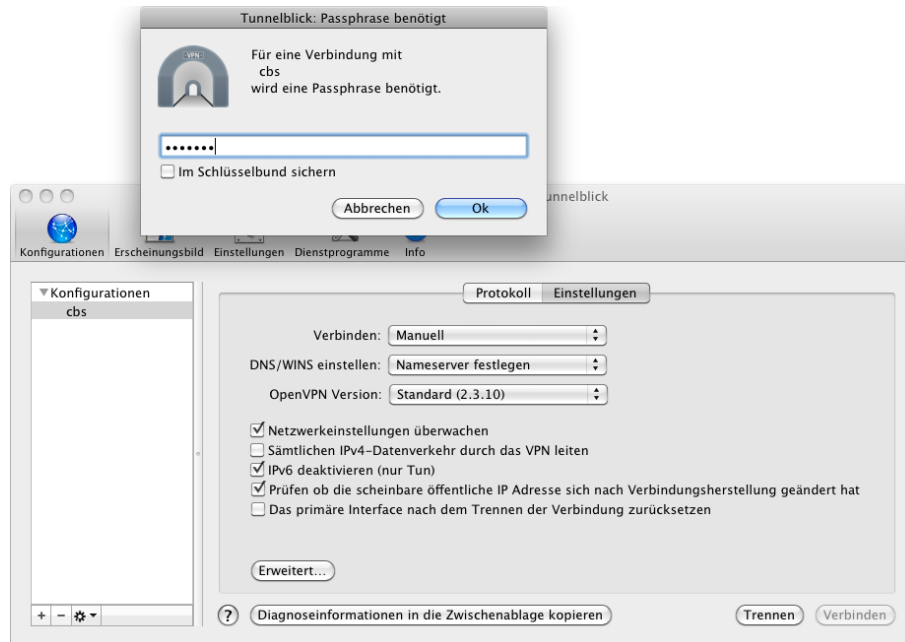


Abbildung 62: Abfrage der Passphrase



Abbildung 63: Passphrase ist nicht korrekt

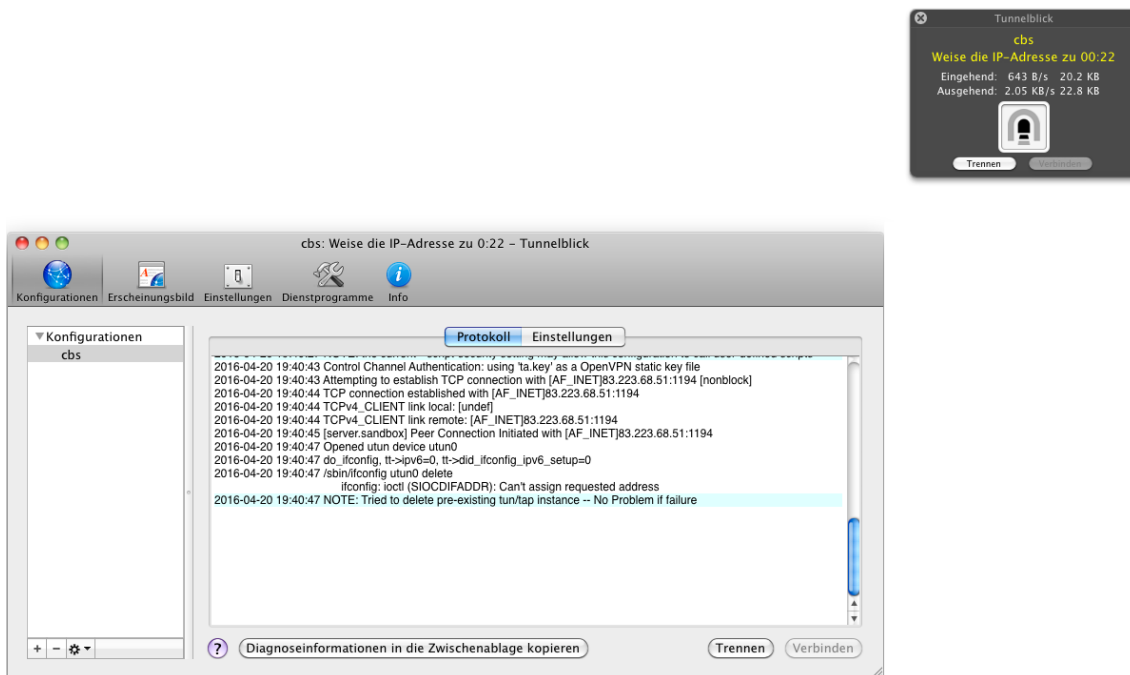


Abbildung 64: Hauptfenster und Status-Benachrichtigung

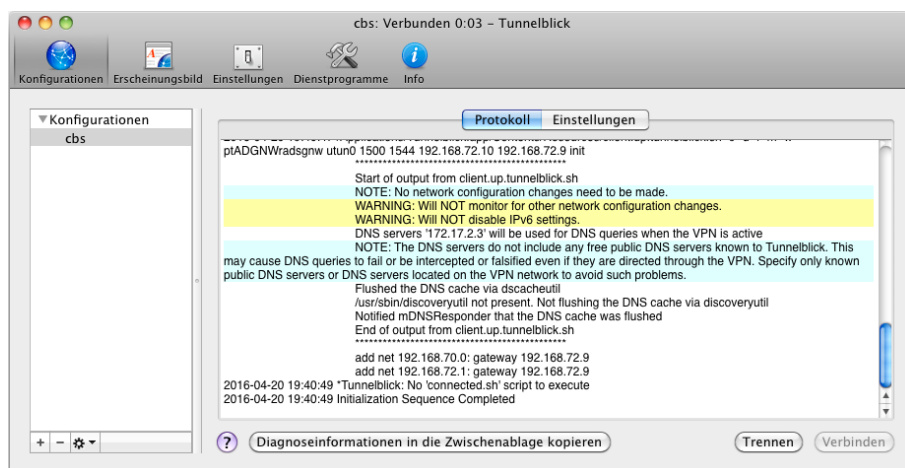


Abbildung 65: Verbindung erfolgreich aufgebaut

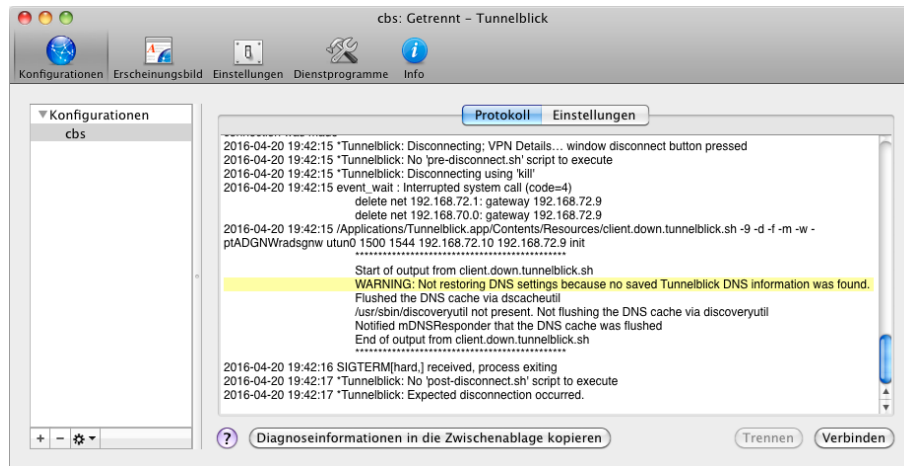


Abbildung 66: Verbindung getrennt

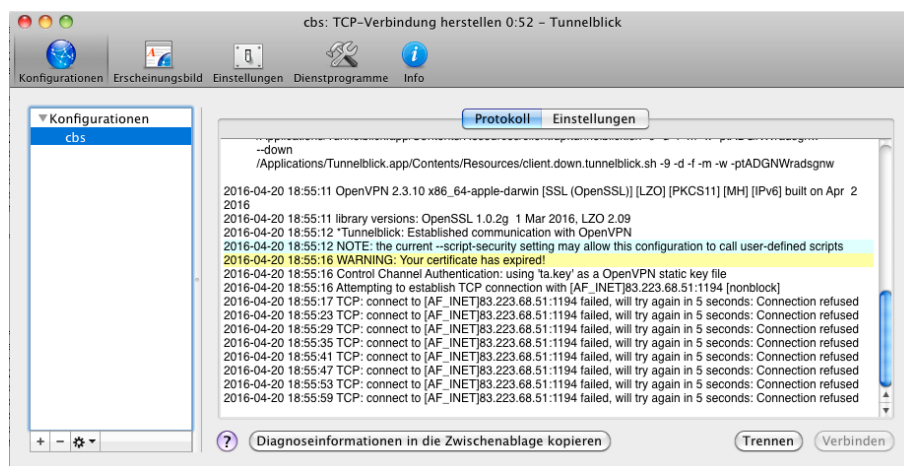


Abbildung 67: Fehlermeldung im Logfile



Tunnel, werden kontinuierlich Ping-Antworten mit der jeweiligen Laufzeit ausgegeben. Dieser Ping kann mit **CTRL-C** beendet werden.

Funktioniert der Ping nicht, kommt die Meldung **Destination Host Unreachable**. Dann ist zu prüfen, ob der angepingte Rechner überhaupt im LAN erreichbar ist und ob er den Collax als Gateway nutzt. Ggf. muß dann auf dem Rechner noch eine Netzroute für das OpenVPN-Client-Netz zum Collax gesetzt werden. In jedem Fall sollte der Collax-Server mit seiner internen IP-Adresse auf Ping antworten.

## 7 Datensicherung

Die Konfiguration von OpenVPN ist Teil der Gesamtkonfiguration des Collax Systems und kann mit der Konfiguration exportiert, importiert und gesichert werden.

Im Falle einer Neuinstallation des Collax-Systems muß das OpenVPN Cabinet manuell installiert werden, siehe Abschnitt "Cabinet installieren".

## 8 Support

Das beschriebene Erweiterungsmodul für die Collax Plattform wurde von der linudata GmbH erstellt.

Collax als Hersteller der genutzten Plattform kann für dieses Erweiterungspaket keinen Support übernehmen. Bitte beachten Sie, daß die Inanspruchnahme des Supports der Firma Collax möglicherweise mit Kosten verbunden ist.

Support für dieses Paket kann von der linudata GmbH bezogen werden. Dies kann sowohl im Bedarfsfall "on demand" als auch im Rahmen eines Supportvertrags mit festgelegten Reaktionszeiten erfolgen.

Eine Anfrage an [info@linudata.de](mailto:info@linudata.de) zur Abklärung des weiteren Vorgehens ist immer kostenfrei möglich. Fehler in diesem Erweiterungspaket werden durch die linudata GmbH ohne Zusicherung einer Reaktionszeit kostenlos beseitigt.