enertexbayern gmbh
simulation entwicklung consulting

Handbuch und Konfiguration

ENA - elektronische Netzabwehr

Enertex® Bayern GmbH – Ebermannstädter Straße 8 - 91301 Forchheim - Deutschland - mail@enertex.de

Inhalt

Hinweise

- Einbau und Montage elektrischer Geräte dürfen nur durch Elektrofachkräfte erfolgen.
- Beim Anschluss von KNX/EIB-Schnittstellen werden Fachkenntnisse durch KNX™-Schulungen vorausgesetzt.
- Bei Nichtbeachtung der Anleitung können Schäden am Gerät, sowie Brand oder andere Gefahren entstehen.
- Diese Anleitung ist Bestandteil des Produkts und muss beim Endanwender verbleiben.
- Der Hersteller haftet nicht für Kosten oder Schäden, die dem Benutzer oder Dritten durch den Einsatz dieses Gerätes, Missbrauch oder Störungen des Anschlusses, Störungen des Gerätes oder der Teilnehmergeräte entstehen.
- Das Öffnen des Gehäuses, andere eigenmächtige Veränderungen und oder Umbauten am Gerät führen zum Erlöschen der Gewährleistung!
- Für nicht bestimmungsgemäße Verwendung haftet der Hersteller nicht.

Funktionsbeschreibung

Im Smarthome verbinden sich KNX und IT immer enger miteinander. Dadurch erreicht der Aspekt der Sicherheit vor Angriffen Dritter eine neue Dimension. Oft wird dieser Aspekt vernachlässigt, weil der Elektriker das komplette System warten muss und die Sicherheitsfunktionalität den Komfort bei der Bedienung z.B. durch umständliche Passworteingaben erheblich reduziert.

Die Lösung: Die elektronische Netzabwehr - ENA - der Enertex® Bayern GmbH.

Fernwartung

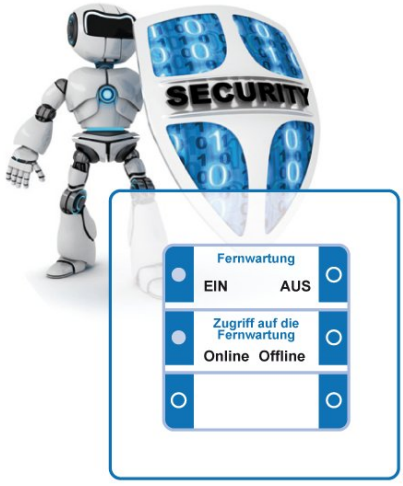


Abbildung 1: Fernwartung

Eine Fernwartung des Systems ohne Sicherheitsfunktionalität öffnet IT-spezialisierten Kriminellen jegliche Möglichkeit, elektrische Schlösser zu öffnen und Türen zu entriegeln etc.. Durch gezielte Angriffe kann u.U. sogar das IT Netz der gesamten Familie gehackt werden. Mit der ENA kann diese sonst umfangreich zu konfigurierende Sicherheitsfunktion dem Anwender einfach über die Visualisierung oder einen KNX Taster schaltbar gemacht werden. Wenn Sie es möchten, wird der gesicherte Fernwartungszugang geöffnet oder ganz abgeschaltet. Und Sie erkennen, wenn dieser genutzt wird. Einfach an Ihren KNX Schaltern.

Sichere Verbindung nach Hause

Befindet man sich im Heimnetz, so ist die Bedienung der Visualisierung, LAN-Geräte über eine spezifische APP bequem aufrufbar.

Abbildung 2: Sichere Verbindung nach Hause

Der gleiche Komfort sollte natürlich auch von unterwegs aus gegeben sein, was aber ohne sichere Verbindung nicht möglich ist. Mit der elektronischen Netzabwehr, kurz ENA wird dieser Sicherheitsaspekt gewährleistet, ohne auf den Anwenderkomfort verzichten zu müssen.

On Demand (nur iOS)

Die Enertex ENA ermöglicht sicheren Zugriff vom Internet auf Ihr Heimnetzwerk. Mit der „on demand“ Technologie ist optimaler Schutz gewährleistet, ohne umständliche Eingabe von Passwörtern. Sie klicken einfach auf Ihre App. Den Rest erledigen ENA und Ihr iPhone (getestet mit iOS 8 und 9).

Gesicherte Internetverbindung

Abbildung 3: Gesicherte Internetverbindung

Mit ENA machen Sie auch Ihre Internetverbindung unterwegs sicherer: Sie wählen sich über einen öffentlichen Internetzugang in Ihr Hausnetzwerk ein und surfen dann ausschließlich und sicher über Ihren privaten Anschluss.

Übersicht

Die Enertex ENA ermöglicht sicheren Zugriff vom Internet auf Ihr Heimnetzwerk.

Die Einrichtung des Gerätes ist in wenigen Schritten auf einfachste Weise möglich:

- Einfache Konfiguration über einen Webbrowser
  - Basiskonfiguration
  - Einspielen von Sicherheitspatches
  - Sichern/Wiederherstellen der Konfiguration
- Verwaltung von Dynamischen DNS (DDNS) bei folgenden Anbietern:
  - Dyn.com
  - FreeDNS
  - Gira DNS
  - No IP
- HTTPS Reverse Proxy mit vier Weiterleitungen (2048-Bit Schlüssel)
- OpenVPN-Server
  - Benutzerverwaltung
  - Benutzerauthentifizierung mittels verschlüsselter PKCS#12-Datei
  - Verschlüsselte Datenübertragung auf höchstem Niveau (AES-256)
- Erstellung der OpenVPN-Konfigurationsdateien für
  - iOS
  - Android
  - PC-Systeme (Windows/OSX/Linux)
- Optionale Integration ins KNX-System (KNXnet/IP-Schnittstelle oder Router notwendig):
  - Öffnen und Schließen der Zugangsberechtigung eines Benutzers über KNX-1-Bit Gruppenadresse

- Anzeige des Verbindungsstatus über KNX-1-Bit-Gruppenadresse d.h. Anzeige, ob ein Benutzer wirklich die OpenVPN-Verbindung nutzt
- An/Abschalten des OpenVPN-Servers über KNX-1-Bit-Gruppenadresse

- OpenVPN Experten Optionen - auf einfache Weise konfigurierbar
  - OpenVPN „on demand“ für Apple iOS
  - Externe Internetverbindung über das eigene Heimnetzwerk via VPN leiten, wenn man z.B. in einem öffentlichen WLAN angemeldet ist

Technisch Daten

Hardware	
Abmessungen	Hutschiene, 6 TE
Spannungsversorgung	20 ... 30 V DC
Leistungsaufnahme	1,2 – 1,7 W (abhängig von LAN Aktivität)
Schnittstellen	Ethernet 10/100 Mbit/s
Software	
Betriebssystem	Linux
OpenVPN	Beliebige Benutzeranzahl 4 Benutzer per KNX überwachbar 2048-Bit RSA Schlüssel Übertragungsverschlüsselung AES-256 Perfect Forward Secrecy
HTTPS Reverse Proxy	4 Weiterleitungen 2048-Bit RSA Schlüssel Übertragungsverschlüsselung AES-256 Perfect Forward Secrecy
Dynamisches DNS	Verwaltung von 4 Domains

Hinweis

Einige der Verschlüsselungsmethoden sind abhängig von den Fähigkeiten der verwendeten Verbindungspartners (Browser, OpenVPN Client, Betriebssystem).

KNX

Eine zum Betrieb am EIB/KNX-System erforderliche Schnittstelle ist nicht im Lieferumfang enthalten und muss ggf. getrennt beschafft werden.

Wir empfehlen:

- Enertex® KNXNet/IP Router
- Enertex® KNXNet/IP Schnittstelle

Montage und Anschluss

Für den Betrieb der Enertex® ENA wird benötigt:

- Eine Stromversorgung mit mindestens 2 Watt Ausgangsleistung: Sicherheitskleinspannung 20 bis 30 VDC (Gleichspannung)
- Eine 10/100 Mbit kompatible Ethernetverbindung
- Eine Internetverbindung für den Fernzugriff und Port-Weiterleitungen im Router und Zugriff auf DNS-Server und NTP-Server

Bitte beachten:

Die externe Sicherheitskleinspannung wird durch das Gerät mit dem Erdpotential des LAN verbunden. Damit besteht keine Isolation mehr zur Erde, wenn der LAN-Schirm geerdet wird. Um eine Trennung herzustellen, wird empfohlen eine externe Kleinspannungsversorgung nur für die Enertex® ENA zu verwenden.

Inbetriebnahme

Die Bootzeit beim Einschalten beträgt ca. 60 Sekunden. Voreinstellung für das Netzwerk ist DHCP.

Sobald die grüne LED anfängt zu blinken, kann auf die ENA zugegriffen werden. Sie müssen mittels des Routers die IP-Adresse des Geräts ermitteln. Alternativ kann das Netzwerk via Smartphone nach Geräten gescannt werden. Dazu empfehlen wir die App "Fing" (Android/iOS). Die MAC-Adresse der ENA beginnt mit 00:50:C2:79.

Die IP-Adresse geben Sie in einem Webbrowser ein und gelangen so auf die Weboberfläche der ENA.

Hinweis

Beim ersten Systemstart generiert die ENA Sicherheitszertifikate. Währenddessen sind nicht alle Einstellungen auf der Weboberfläche verfügbar.

Schnellanleitung

1. Mit dem Browser auf der ENA Weboberfläche anmelden: Benutzer admin, Passwort admin
2. Netzwerk: IP-Adressen konfigurieren. Sicherstellen, dass die ENA Zugriff auf einen DNS-Server und einen NTP-Server hat.
3. Dynamisches DNS: DDNS-Verwaltung aktivieren, DDNS-Provider wählen, Zugangsdaten und Domainnamen angeben und anwenden. Abwarten, bis PKI-Subsystem beendet wurde.
4. Public-Key-Infrastruktur: CA Zertifikat herunterladen und im Browser (Firefox, Chrome) oder Betriebssystem (Android/iOS) importieren.
5. HTTPS Reverse Proxy: Benutzername und Passwort anlegen, die externen DDNS-Domains mit HTTP-Hosts im LAN verknüpfen. Port 443 (TCP) auf die ENA weiterleiten.
6. OpenVPN: Benutzer hinzufügen und warten bis PKI-Subsystem beendet wurde. Passende Konfig. auf Endgerät herunterladen. Port 1194 (UDP) auf ENA weiterleiten.
7. IP-Adresse des KNXnet/IP Interfaces angeben. Gruppenadressen, jeweils zum Starten/Stoppen und Status des OpenVPN-Servers angeben, gleiches gilt für einzelnen OpenVPN-Benutzer.

Weboberfläche

Die Weboberfläche der ENA ist zugriffsgeschützt.

Der Standard Login ist:

Benutzer: admin

Passwort: admin

Netzwerk

Hier können die Netzwerkeinstellungen der ENA vorgenommen werden. Die ENA unterstützt die automatische Konfiguration über DHCP oder die statische Vergabe der Netzwerkeinstellungen.

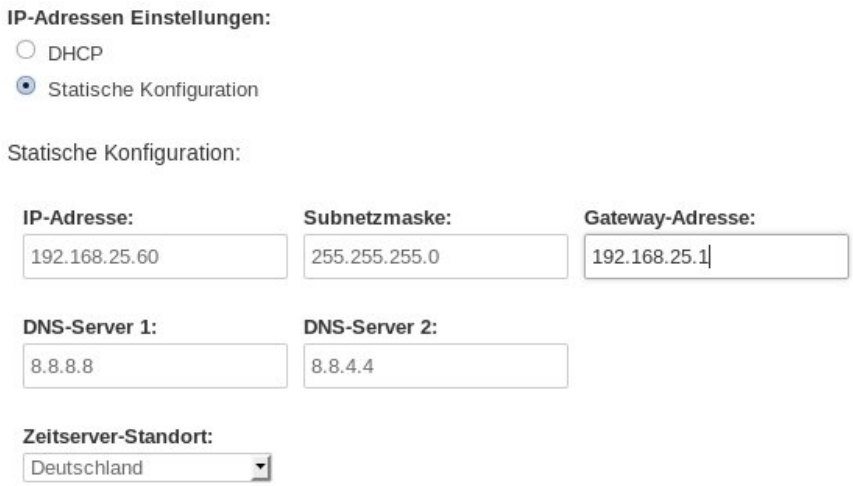


Abbildung 4: Netzwerkeinstellungen

Hinweis

Für den OpenVPN-Betrieb ist es zwingend notwendig, dass sich die ENA als OpenVPN-Server in einem Subnetz mit anderer Netzadresse befindet als die zugreifenden OpenVPN-Clients. Es wird daher empfohlen, dass sich die ENA nicht in einem Subnetz mit den weit verbreiteten Netzadressen 192.168.0.0, 192.168.1.0 oder 192.168.2.0 befindet. Für iOS VPN on demand wird ein DNS-Server im lokalen Netzwerk benötigt. Geben Sie diesen als DNS-Server 1 an.

Zeitserver

Die ENA synchronisiert ihre Uhrzeit mit einem Zeitserver. Welche Zeitserver benutzt werden sollen, kann entweder über eine vorgegebene Standortliste gewählt (Synchronisation über das Internet) oder manuell festgelegt werden.

Dynamisches DNS

Dynamisches DNS oder DDNS ist eine Technik, um Domains im Domain Name System dynamisch zu aktualisieren. Der Zweck ist, dass ein Rechner nach dem Wechsel seiner IP-Adresse automatisch den dazugehörigen Domaineintrag ändert. So ist der Rechner immer unter demselben Domainnamen erreichbar, auch wenn die aktuelle IP-Adresse für den Nutzer unbekannt ist.

Die ENA kann bis zu vier DDNS-Domainnamen selbst verwalten und aktualisieren. Aktivieren Sie hierzu die DDNS-Verwaltung und wählen einen DDNS-Provider aus der Liste aus.

Abbildung 5: DDNS-Verwaltung aktiviert

Die ENA überprüft dann zyklisch die eigene, öffentliche IP-Adresse und aktualisiert DNS-Einträge für alle angegebenen DDNS-Domains beim DDNS-Provider.

Alternativ kann auch ein anderes Gerät (z.B. der Internetrouter) die DNS-Einträge aktualisieren, bzw. per fester IP-Adresse auf die ENA zugegriffen werden. In diesem Fall müssen der ENA nur die Domains bzw. die IP-Adresse bekannt gemacht werden, unter der sie aus dem Internet erreichbar ist.

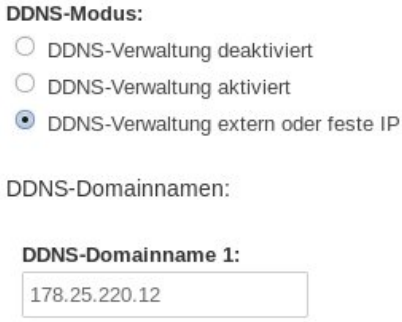


Abbildung 6: Zugriff über feste IP-Adresse

Experten-Optionen

Wenn die DDNS-Verwaltung aktiviert ist, kann in den Experten-Optionen festgelegt werden, in welchem Intervall die eigene, öffentliche IP-Adresse überprüft und bei Änderung an den DDNS-Provider übermittelt wird.

Außerdem ist es möglich eine eigene Website anzugeben, mit der die öffentliche IP-Adresse ermittelt wird. Die Ausgabe der Website muss die IP-Adresse im HTML-Format enthalten. Vergleichen Sie hierzu die Seite myip.enertex.de.

Public-Key-Infrastruktur

Public-Key-Infrastruktur (PKI) bezeichnet in der Kryptologie ein System, das digitale Zertifikate erstellen, verteilen und prüfen kann. Es basiert in der ENA auf einer Zertifizierungsstelle (CA), die Zertifikate für HTTPS- und OpenVPN-Server erstellt und signiert. Die Zertifizierungsstelle muss dafür auf der ENA initialisiert (dies geschieht automatisch) und das zugehörige Zertifikat im Browser oder Betriebssystem importiert werden.

Funktionsweise

Das PKI-System funktioniert stark vereinfacht wie folgt:

- Die Zertifizierungsstelle (CA) erstellt und signiert Zertifikate für den HTTPS-Reverse Proxy, den OpenVPN-Server und den iOS-Profilgenerator.
- Die Zertifikate sind nicht geheim. Beim Verbindungsaufbau (HTTPS/OpenVPN) wird das jeweilige Server-Zertifikat an den Client gesendet. Der Server weist sich damit gegenüber dem Client aus.
- Ist dem Client die Zertifizierungsstelle (CA) bekannt, kann er damit die Echtheit der Signatur in den Serverzertifikaten überprüfen und somit sicherstellen, dass er sich nicht mit einem Angreifer unterhält.

Import

Die Vorteile des Imports des CA Zertifikats (ca.crt) im Browser (oder Betriebssystem) sind:

- Verbindungen zum HTTPS Reverse Proxy können als sicher erkannt werden und es müssen keine Ausnahmeregeln hinzugefügt werden. So wird sichergestellt, dass man auch wirklich eine Verbindung zur ENA und nicht zu einem potentiellen Angreifer aufbaut (siehe Abbildung 7).

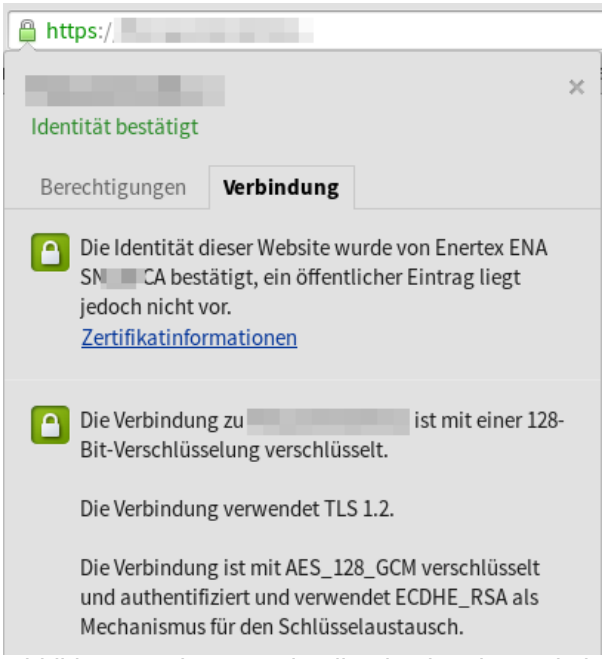


Abbildung 7: Chrome zeigt die Identität der Website als bestätigt

- Beim OpenVPN-Profilimport in iOS kann die Herkunft des Profils überprüft werden (siehe Abbildung 8).

Abbildung 8: iOS Profil: Herkunft überprüft

Chrome

In Chrome (Version 39) kann das CA Zertifikat folgendermaßen importiert werden: „Einstellungen → Erweiterte Einstellungen anzeigen → HTTPS/SSL → Zertifikate verwalten... → Zertifizierungsstellen → Importieren...“. Dann ca.crt auswählen. Bei der Frage, ob der Zertifizierungsstelle vertraut werden soll, muss „Diesem Zertifikat zur Identifizierung von Websites vertrauen“ ausgewählt werden.

Firefox

In Firefox (Version 35) kann das CA Zertifikat folgendermaßen importiert werden: „Einstellungen → Erweitert → Zertifikate → Zertifikate anzeigen → Zertifizierungsstellen → Importieren“. Dann ca.crt auswählen. Bei der Frage für welche Zwecke der Zertifizierungsstelle vertraut werden soll, muss „CA vertrauen, um Websites zu identifizieren“ ausgewählt werden.

iOS

Bei iOS (Version 8 und 9) kann das Zertifikat direkt mit Safari heruntergeladen werden, der Importdialog startet dann automatisch.

Experten-Optionen

In den Experten-Optionen kann die Zertifizierungsstelle neu initialisiert werden. Dabei werden alle bisher erstellten Zertifikate und OpenVPN-Zugänge ungültig! Alle bestehenden OpenVPN-Verbindungen werden getrennt!

HTTPS Reverse Proxy

Über den Reverse Proxy kann von außen mittels Domainnamen auf einen Host im lokalen Netz zugegriffen werden. Aus Nutzersicht ist dies vergleichbar mit dem Port-Forwarding einer Firewall. Der Reverse Proxy verschlüsselt allerdings die Verbindung. Und der Zugriff ist passwortgeschützt. Es kann im lokalen Netz nur auf HTTP/HTTPS-Dienste zugegriffen werden.

Hinweis

Für den HTTPS Reverse Proxy muss im Internetrouter ein Port von außen an den ENA-Zielport 443 (TCP) weitergeleitet werden.

Benutzerverwaltung

Hier werden die Zugangsdaten für den Zugriff auf den HTTPS Reverse Proxy festgelegt.

Domainnamen verknüpfen

Für den Zugriff auf einen Host im lokalen Netzwerk muss jeweils ein bereits konfigurierter DDNS-Domainnamen verknüpft werden, es können also nicht mehr Reverse Proxys als vorhandene DDNS-Domainnamen genutzt werden (siehe Abbildung 9).

Abbildung 9: Beispiel einer HTTPS Reverse Proxy Verknüpfung zu einer Synology Diskstation

OpenVPN

OpenVPN ist ein Programm, das ein Virtuelles Privates Netzwerk (VPN) über eine verschlüsselte TLS-Verbindung aufbauen kann. Zur Verschlüsselung wird die OpenSSL-Bibliothek benutzt.

Hinweis

Für OpenVPN muss im Internetrouter ein Port von außen an den ENA-Zielport 1194 (UDP) weitergeleitet werden.

Benutzerverwaltung

Die ENA kann beliebig viele OpenVPN-Benutzer verwalten, es können sich aber maximal zehn Benutzer gleichzeitig verbinden.

Wenn ein OpenVPN-Benutzer hinzugefügt wird, wird vom PKI-Subsystem eine PKCS#12-Datei erzeugt und zusammen mit einer Konfigurationsdatei für den OpenVPN-Client zum Donwload angeboten. Die PKCS#12-Datei wird mit dem angegebenen Passwort verschlüsselt und mit ihrer Hilfe kann sich der Client gegenüber dem Server authentifizieren. Das Erstellen der PKCS#12-Datei dauert bis zu zwei Minuten.

Konfigurationsdateien herunterladen

Um die Konfigurationsdateien für die OpenVPN-Clients herunterzuladen, muss folgendermaßen vorgegangen werden:

- Den gewünschten **Benutzer** aus dem Drop-Down-Menü auswählen
- **Nicht trennen:** Wird diese Option aktiviert, bleibt die OpenVPN-Verbindung des Clients auf unbestimmte Zeit bestehen. Dies kann für stationäre Clients (PCs) gewünscht sein. Lässt man diese Option dagegen deaktiviert, so wird die OpenVPN-Verbindung nach einem Timeout automatisch beendet. Dies ist in der Regel für mobile Clients (Android/iOS) gewünscht, da die OpenVPN-Verbindung auf Dauer die Akkulaufzeit negativ beeinflussen kann.
- **Internet:** Wird diese Option aktiviert, so versucht der OpenVPN-Client den gesamten Internetverkehr über das VPN umzuleiten. Dies ist z.B. sinnvoll, wenn man sich in einem öffentlichen WLAN befindet und verhindern möchte, dass der Besitzer des WLANs oder Dritte den Internetverkehr überwachen können. Hinweis: Bricht die Internetverbindung der ENA ab, kann es - je nach Client-Betriebsystem - vorkommen, dass das Internet ohne VPN über die normale Verbindung fortgesetzt wird.
- Den **Knopf** für die gewünschte Konfigurationsdatei drücken.

  Folgende Dateien sind verfügbar:

  - **Client-Konfig.:** Die Konfigurationsdatei kann für die Standard-Clients auf den gängigen Betriebssystemen (Windows/Mac OS/Linux/Android) benutzt werden.
  - **IOS-Konfig.:** Mit der iOS-Mobileconfig. kann in iOS sehr einfach ein VPN-Profil importiert werden. Hinweis: Importieren Sie zunächst das CA Zertifikat in iOS und installieren Sie die App "OpenVPN Connect"!

- **PKCS12:** Die PKCS12-Datei beinhaltet lediglich das Zertifikat, mit dem sich der Benutzer gegenüber dem VPN-Server ausweist. Diese Datei ist für manche Clients zusätzlich nötig.

iOS VPN "on demand"

Mit Apple iOS ist es möglich, die VPN-Verbindung bei Bedarf automatisch aufzubauen. Dies geschieht, sobald auf die konfigurierten Zieladressen zugegriffen wird (siehe Abbildung 10). Die Zieladressen müssen Domainnamen sein, es dürfen keine IP-Adressen benutzt werden. Sie müssen im lokalen Netzwerk von einem DNS-Server (z.B. Fritzbox) aufgelöst werden und dürfen als Präfix den Wildcard * enthalten (z.B. *.fritz.box).

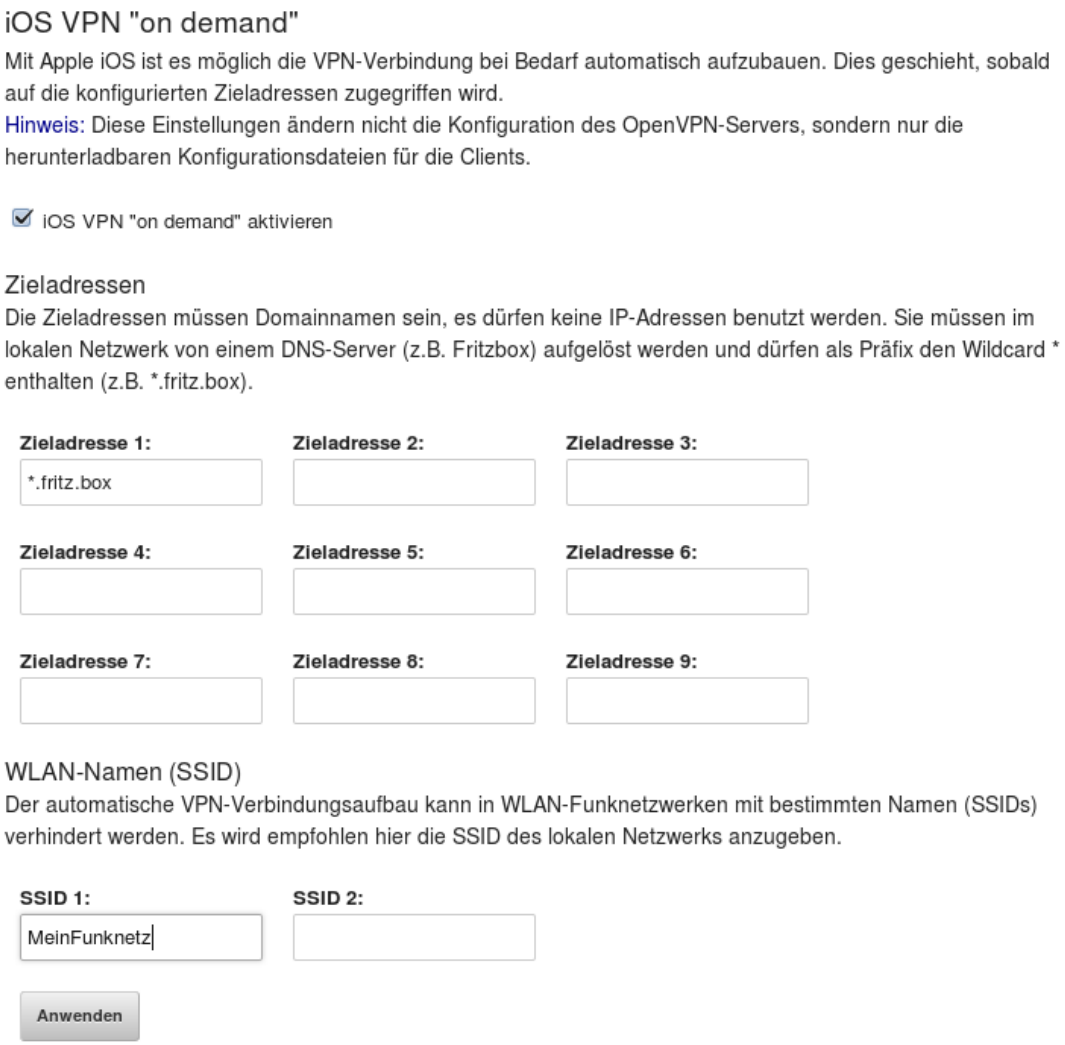


Abbildung 10: Adressen, bei deren Zugriff das VPN automatisch aufgebaut werden soll

Außerdem kann der automatische VPN-Verbindungsaufbau in WLAN-Funknetzwerken mit bestimmten Namen (SSIDs) verhindert werden. Es wird empfohlen hier die SSID des lokalen Netzwerks anzugeben, damit die VPN-Verbindung getrennt wird, wenn sie nach Hause kommen.

Hinweis

Diese Einstellungen ändern nicht die Konfiguration des OpenVPN-Servers, sondern nur die herunterladbaren Konfigurationsdateien für die Clients. Wird hier also etwas geändert, muss die Konfigurationsdatei im Client neu importiert werden.

Experten-Optionen

Verbindungs-Einstellungen

Wird beim Port Forwarding im Internet-Router ein anderer öffentlicher Port als der Standardport weitergeleitet, so muss der Port hier angegeben werden. Als OpenVPN-Serveradresse wird automatisch die erste DDNS-Domain benutzt.

Verbindung automatisch trennen

Die Verbindung automatisch trennen, wenn in einer bestimmten Zeit (in Sekunden) nicht mehr als ein bestimmtes Datenvolumen (in kByte) übertragen wurde.

Einrichtung der OpenVPN-Clients

iOS 8.3

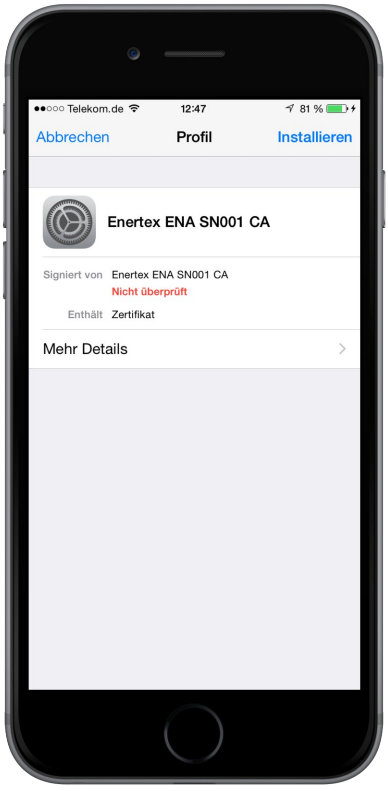
Je nach iOS-Version kann die Vorgehensweise von der Anleitung abweichen.

Installieren Sie zunächst die App „OpenVPN Connect“ aus dem Apple Appstore.

Öffnen Sie die ENA-Weboberfläche mit dem Safari-Browser (keine alternativen Browser benutzen!).

Auf der Seite „Public-Key-Infrastruktur“ den Knopf „CA Zertifikat herunterladen“ drücken.

Es öffnet sich automatisch ein Dialog zum Installieren des Zertifikats. Die Installation muss mit dem Telefon-Code bestätigt werden. Folgen Sie den weiteren Anweisungen:

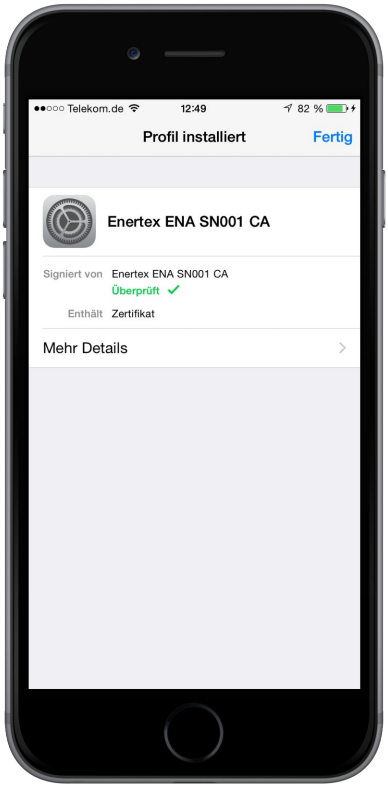


Sie werden aufgefordert das Zertifikat zu installieren.

Geben Sie dazu Ihren Telefoncode ein.

Drücken Sie bei diesem Hinweistext „Installieren“.

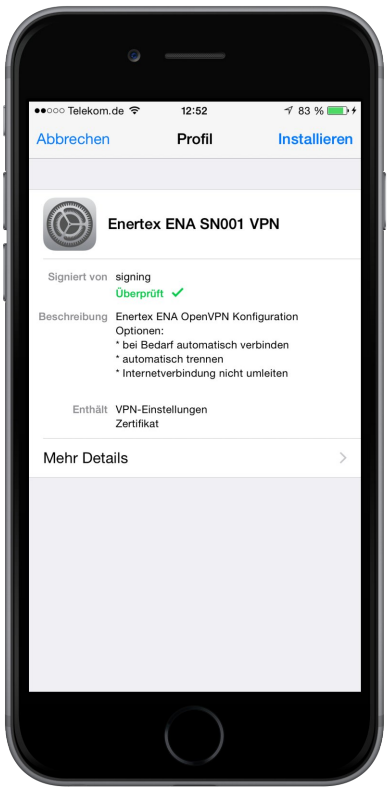
Bestätigen Sie erneut mit „Installieren“.



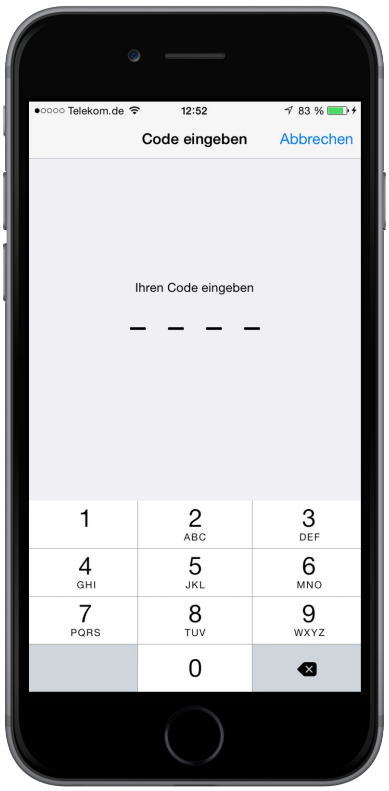
Das Zertifikat wurde installiert. Drücken Sie „Fertig“.

Auf der Seite „OpenVPN“ den gewünschten Nutzer auswählen und den Knopf „iOS-Konfig“ drücken:

Es öffnet sich automatisch ein Dialog zum Installieren der Konfiguration. Die Installation muss mit dem Telefon-Code bestätigt werden. Folgen Sie den weiteren Anweisungen. Sie müssen außerdem das Passwort angeben, mit dem der Nutzer auf der ENA angelegt wurde:



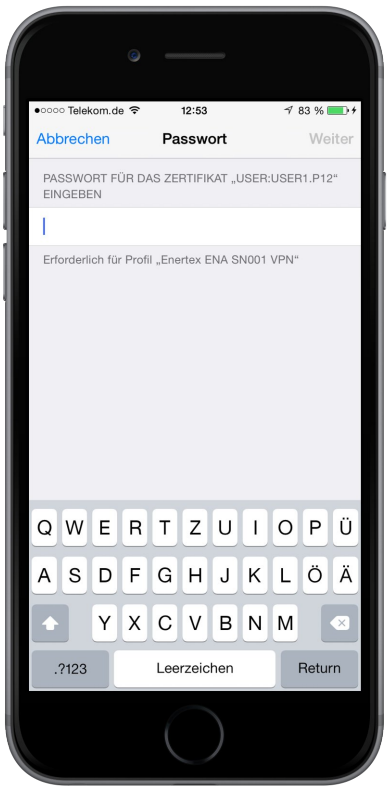
Schritt 1: Sie werden aufgefordert, das VPN-Profil zu installieren. Es wird als „Überprüft“ angezeigt.



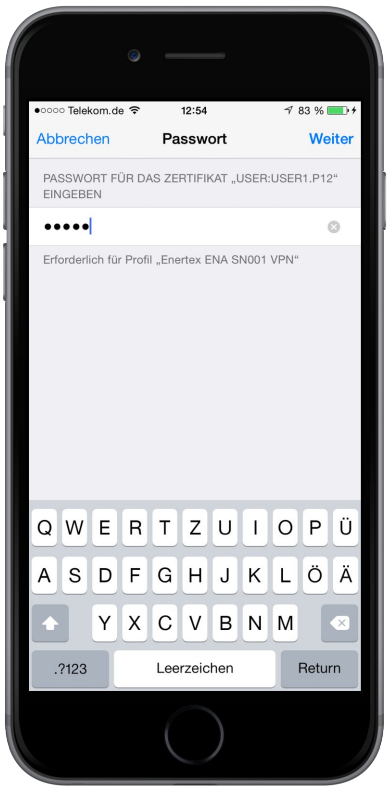
Geben Sie Ihren Telefoncode ein.

Schritt 2: Dieser Hinweis gibt an, dass der Netzwerkverkehr über die ENA geleitet wird. Drücken Sie „Installieren“ und...

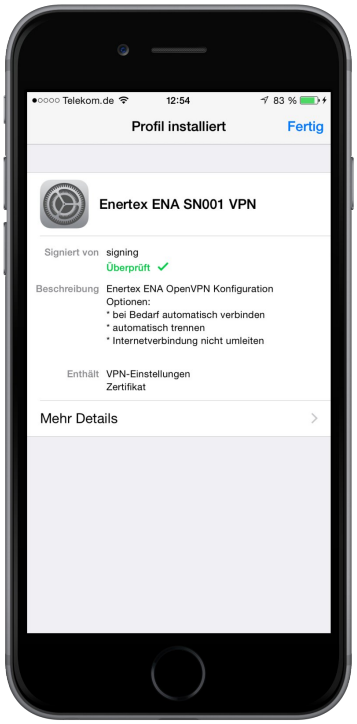
… bestätigen Sie erneut mit „Installieren“.



Schritt 3: Das Passwort, das beim Anlegen des VPN-Benutzers in der ENA vergeben wurde, eingeben...

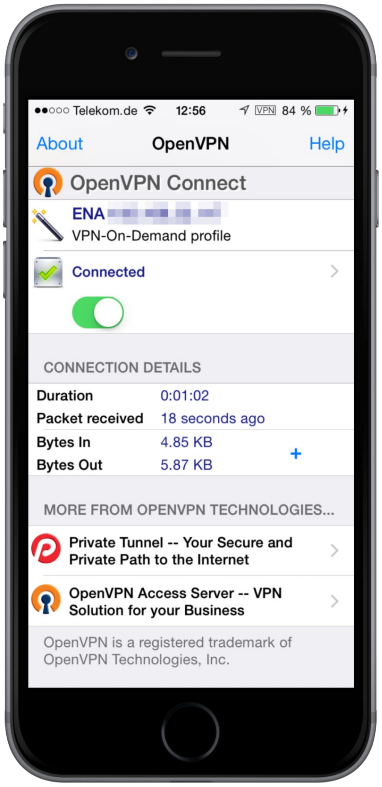


… und „Weiter“ drücken.



Das VPN-Profil wurde installiert. Drücken Sie „Fertig“.

Testen Sie den Verbindungsaufbau in den iPhone-Einstellungen unter „Allgemein → VPN“ (nicht unter „VPN“ im Hauptmenü!).



Sobald das VPN verbunden ist, können Sie in der „OpenVPN Connect“ App die Verbindungsdetails betrachten.

Android 5.1

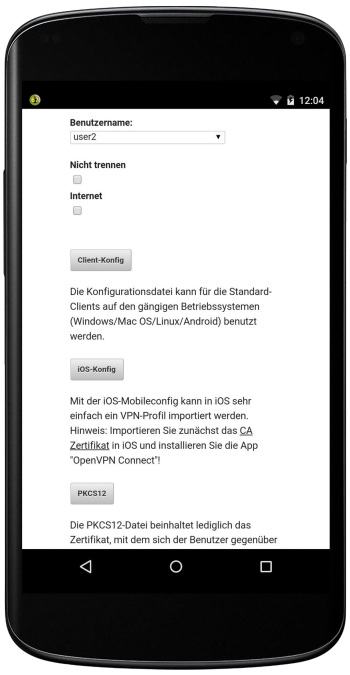
Je nach Android-Version und Gerätehersteller kann die Vorgehensweise von der Anleitung abweichen.

Als erstes muss in den Einstellungen des Android-Geräts unter „Sicherheit“ die Displaysperre aktiviert werden.

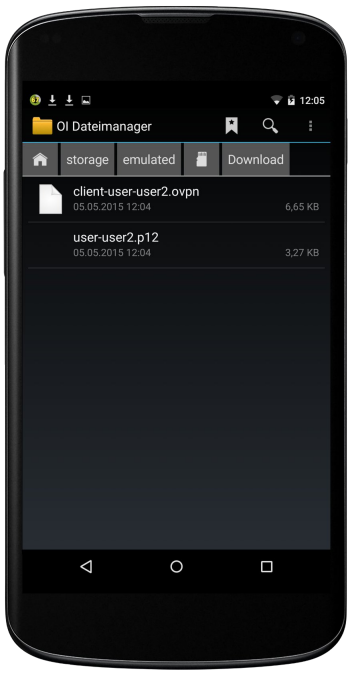
Installieren Sie nun zunächst die App „OpenVPN Connect“ aus dem Google Playstore

Öffnen Sie die ENA-Weboberfläche mit dem Chrome-Browser

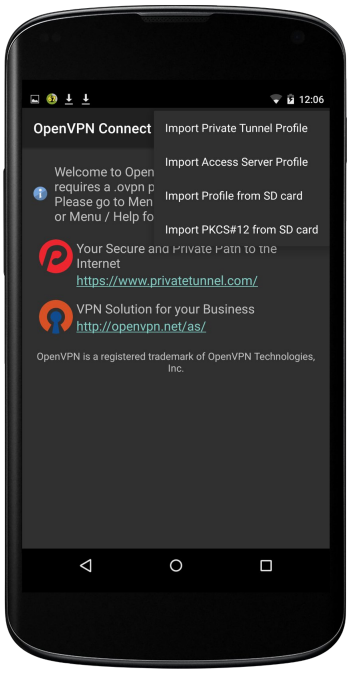
Auf der Seite „OpenVPN“ den gewünschten Nutzer auswählen und zuerst den Knopf „Client-Konfig“ drücken, um die entsprechende Datei herunterzuladen. Wenn der Download vollständig ist, den Knopf „PKCS12“ drücken, um auch diese Datei herunterzuladen. Die beiden Dateien müssen anschließend in die „OpenVPN Connect“ App importiert werden:



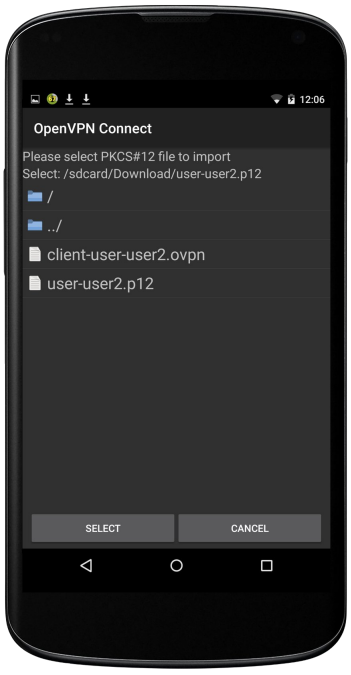
Schritt 1: ENA-Weboberfläche im Chrome Browser aufrufen.



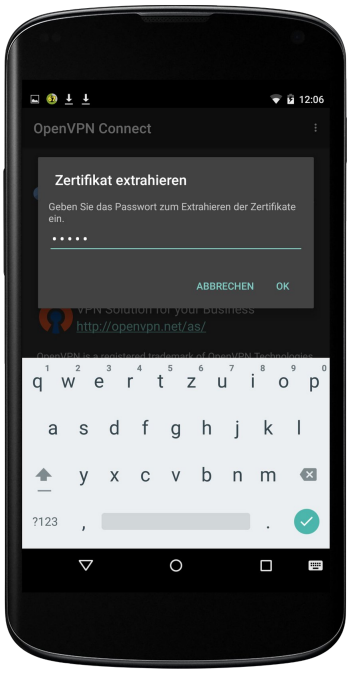
Die beiden heruntergeladenen Dateien befinden sich dann im Ordner „Download“.



Schritt 2: Die „OpenVPN Connect“ App öffnen und im Menü „Import → Import PKCS#12 from SD card“ aufrufen. Damit wird das Nutzerzertifikat, in den Android-Keystore übernommen.

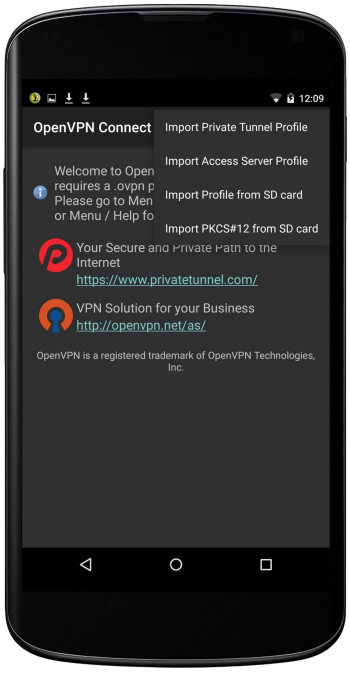


Schritt 3: Die zuvor heruntergeladene Zertifikat mit dem Dateinamen „user-Nutzername.p12“ im Download-Ordner auswählen und „Select“ drücken.

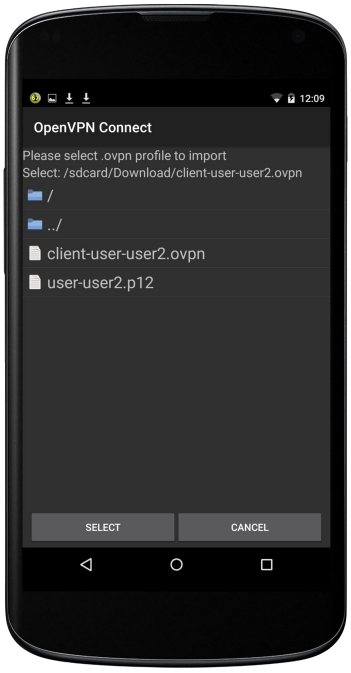


Schritt 4: Das Passwort, das beim Anlegen des VPN-Benutzers in der ENA vergeben wurde, eingeben.

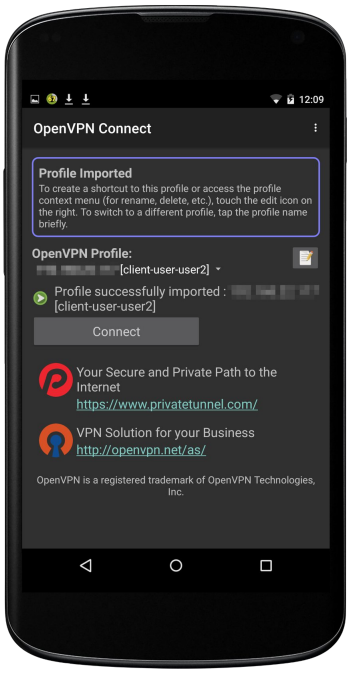
Schritt 5: Dem Nutzerzertifikat einen beliebigen Namen geben. Über den Namen kann es später aus dem Android-Keystore ausgewählt werden.



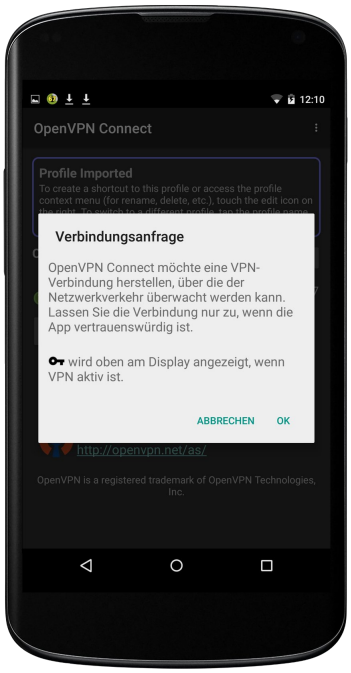
Schritt 6: Im Menü „Import → Import Profile from SD card“ aufrufen. Dabei wird die eigentliche OpenVPN-Konfiguration importiert.



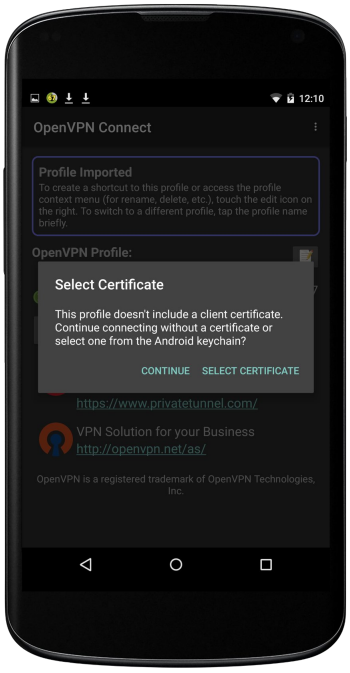
Schritt 7: Die zuvor heruntergeladene Konfig-Datei mit dem Dateinamen „client-user-Nutzername.ovpn“ im Download-Ordner auswählen und „Select“ drücken.



Schritt 8: Nachdem das Profil erfolgreich importiert wurde, kann die Verbindung das erste mal gestartet werden.

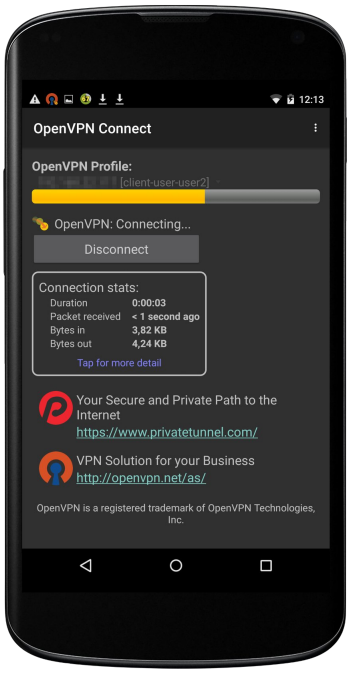


Schritt 9: Android gibt einen Hinweis, dass eine VPN-Verbindung aufgebaut wird. Dies mit „OK“ bestätigen.

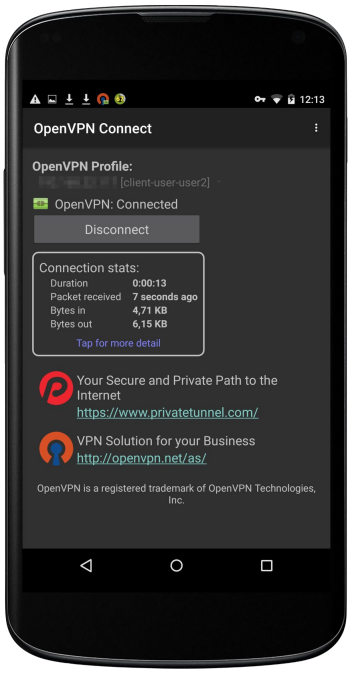


Schritt 10: Beim ersten Verbindungsaufbau muss der Verbindung ein Nutzerzertifikat zugewiesen werden. Dazu „Select Certificate“ drücken...

… und das zuvor importierte Zertifikat auswählen. Mit „Zulassen“ bestätigen.

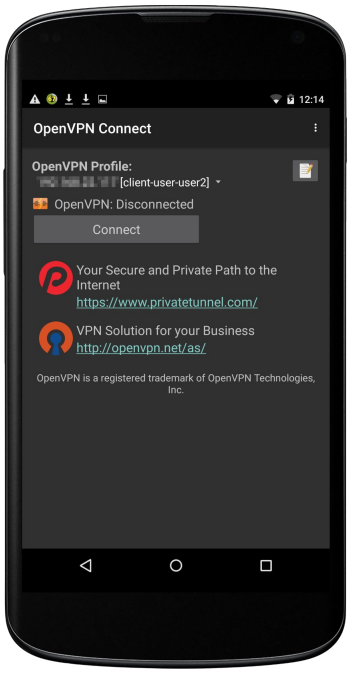


Die Verbindung wird aufgebaut...

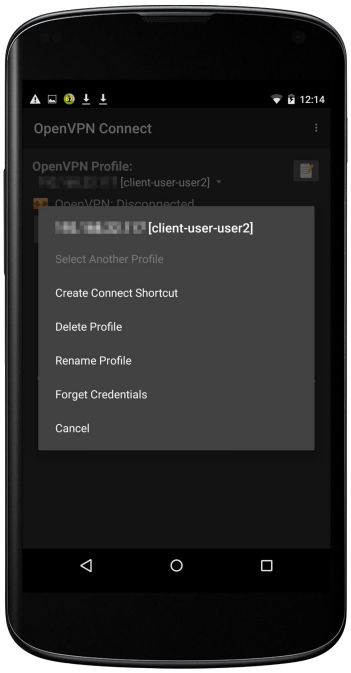


… und ist nun verbunden. In der Statusleiste wird dazu ein Schlüsselsymbol angezeigt. Sie können nun beliebige Apps nutzen, um auf ihr Netzwerk zuzugreifen. Mit der Schaltfläche „Disconnect“ kann die Verbindung getrennt werden.

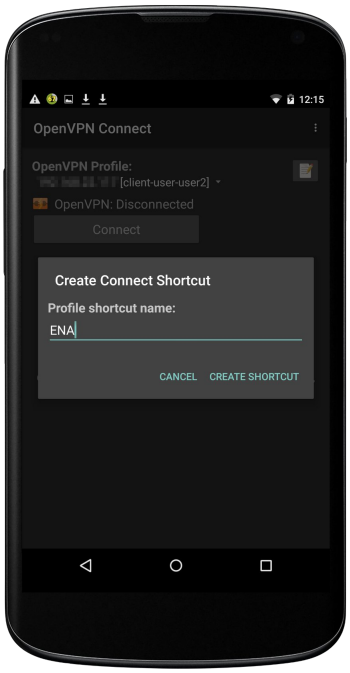
Optional kann ein Widget zum schnellen Verbindungsaufbau auf den Android-Homescreen gelegt werden:



Schritt 1: bei getrennter VPN-Verbindung den Knopf zum Bearbeiten der Verbindung (mit dem Textblock) drücken...



… und „Create Connect Shortcut“ auswählen.



Schritt 2: einen Namen für das Widget vergeben.

Das Widget wurde auf dem Homescreen abgelegt. Durch drücken des Symbols wird die Verbindung aufgebaut.

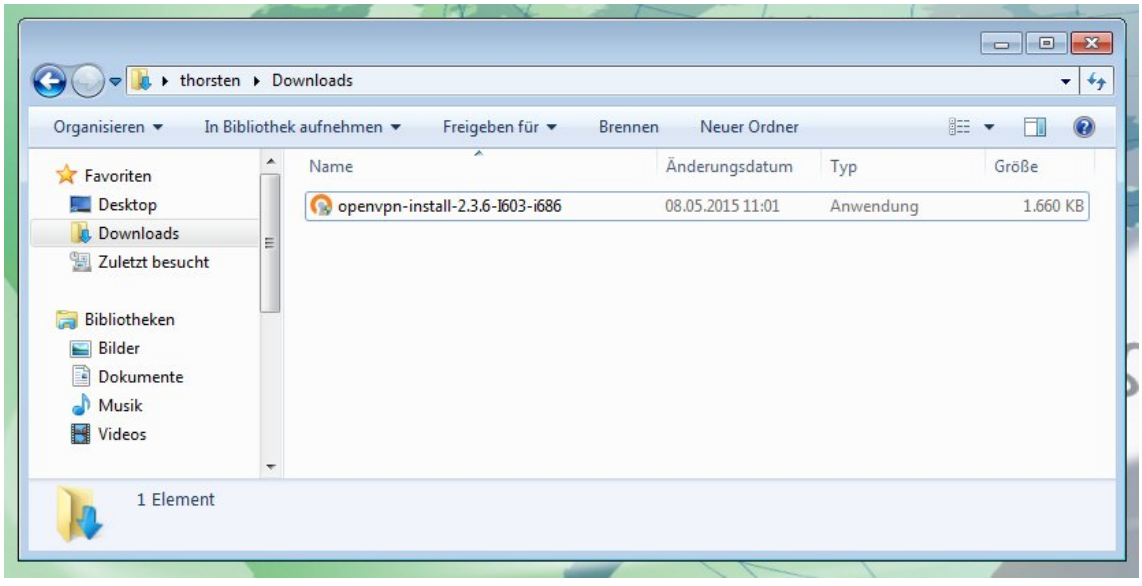
Hinweis

Nachdem ein Nutzerzertifikat in den Android-Keystore importiert wurde, zeigt Android nach jedem Neustart den Hinweis: „Das Netzwerk wird möglicherweise überwacht“. Dies lässt sich leider nicht abstellen, da von Google so gewollt.

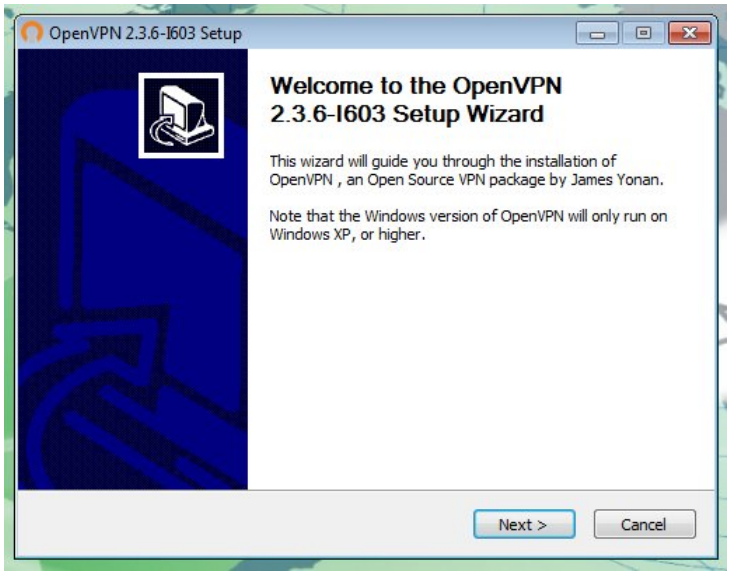
Windows 7

Laden Sie sich zunächst den Installer der Anwendung „OpenVPN GUI“ von der OpenVPN-Webseite (https://openvpn.net/index.php/open-source/downloads.html) herunter:

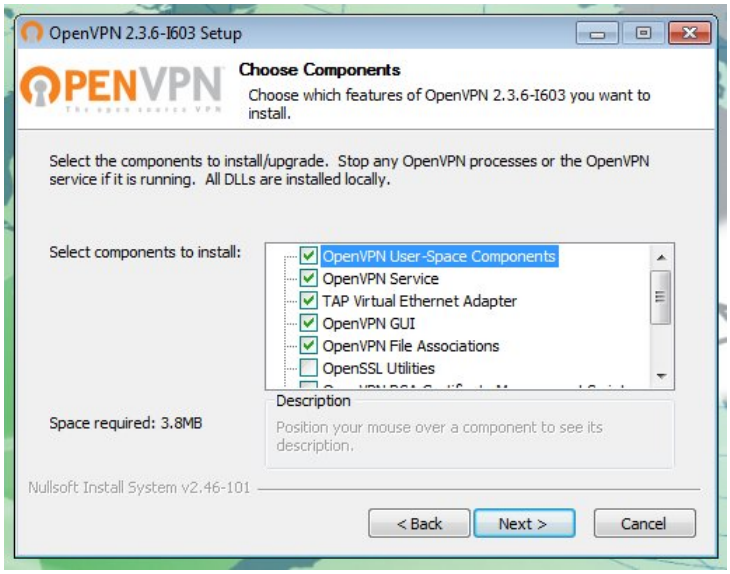
Der Installer liegt im Download-Ordner:

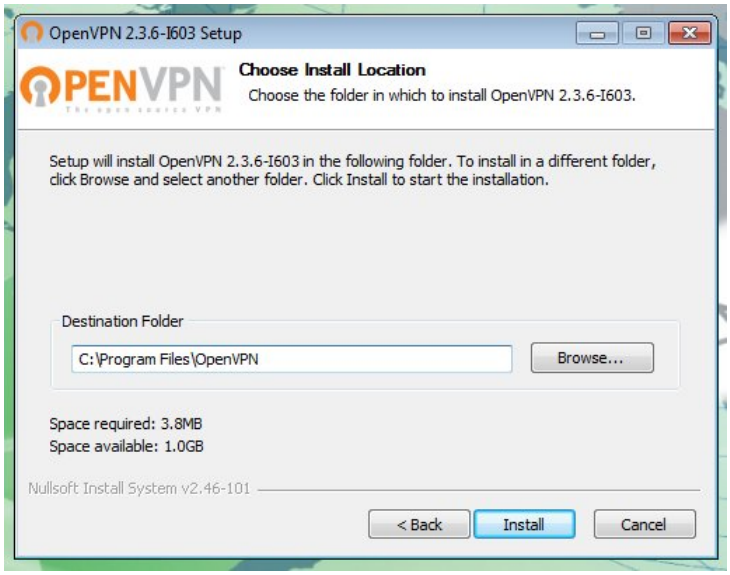


Installieren Sie die Anwendung:



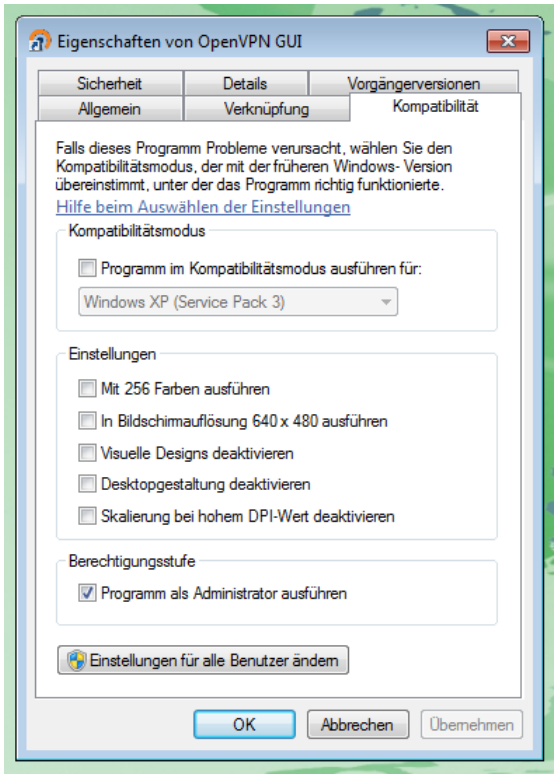
Sie können OpenVPN GUI mit den Standardeinstellungen installieren:



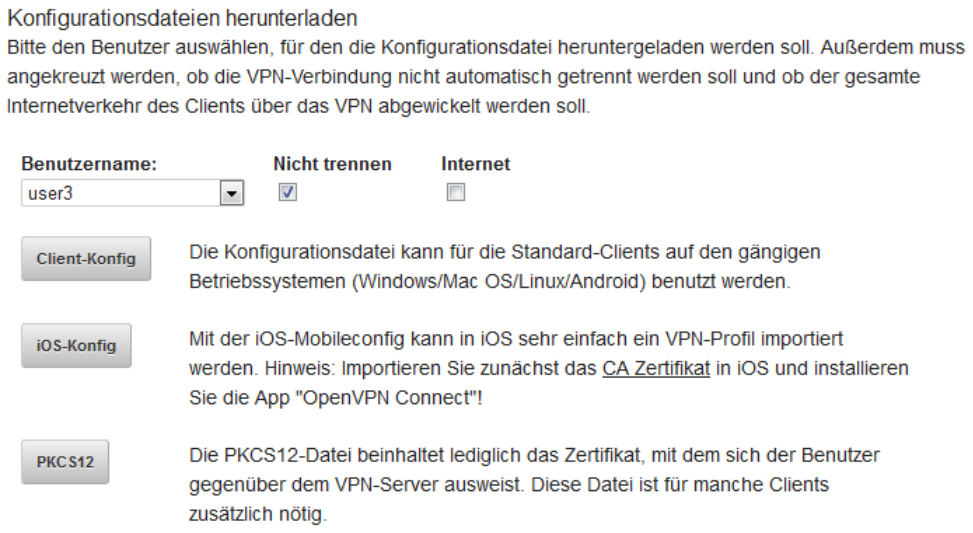


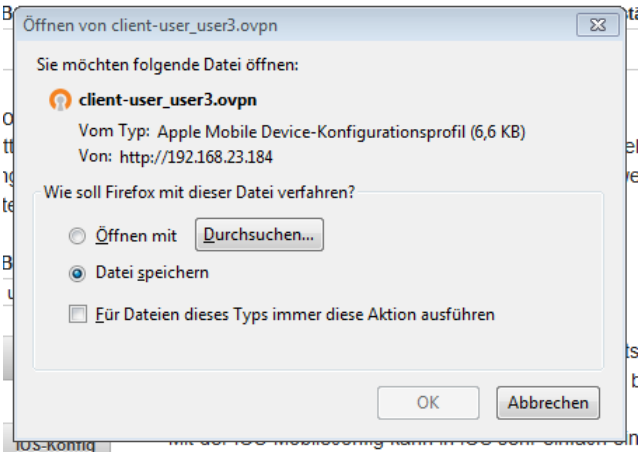
Nach der Installation finden Sie das Programmsymbol auf dem Desktop:

Stellen Sie sicher, dass das Programm als Administrator ausgeführt wird. Rufen Sie dazu mit der rechten Maustaste die Eigenschaften des Programms auf und setzen Sie den entsprechenden Haken:

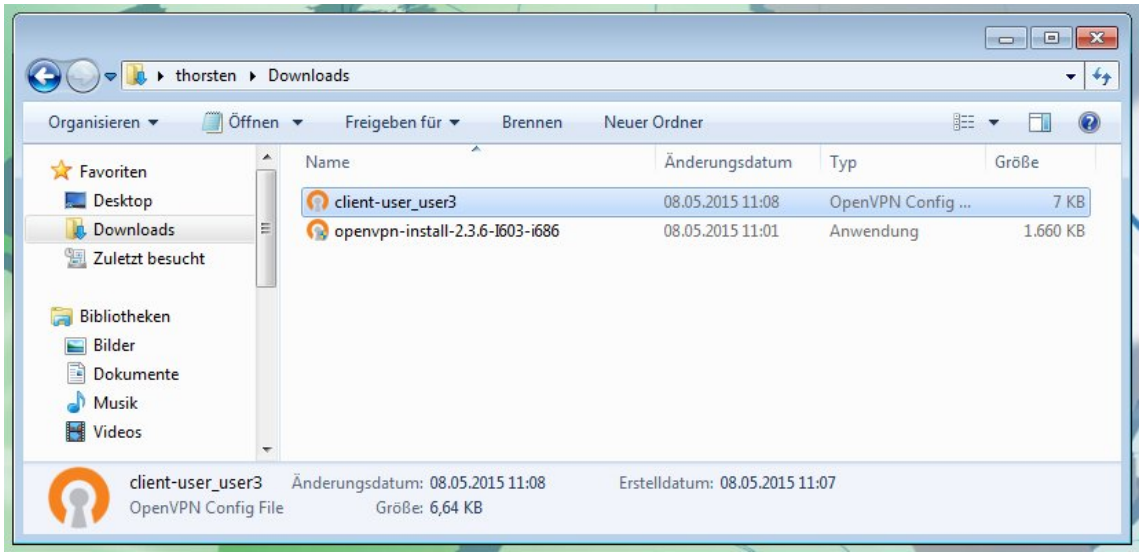


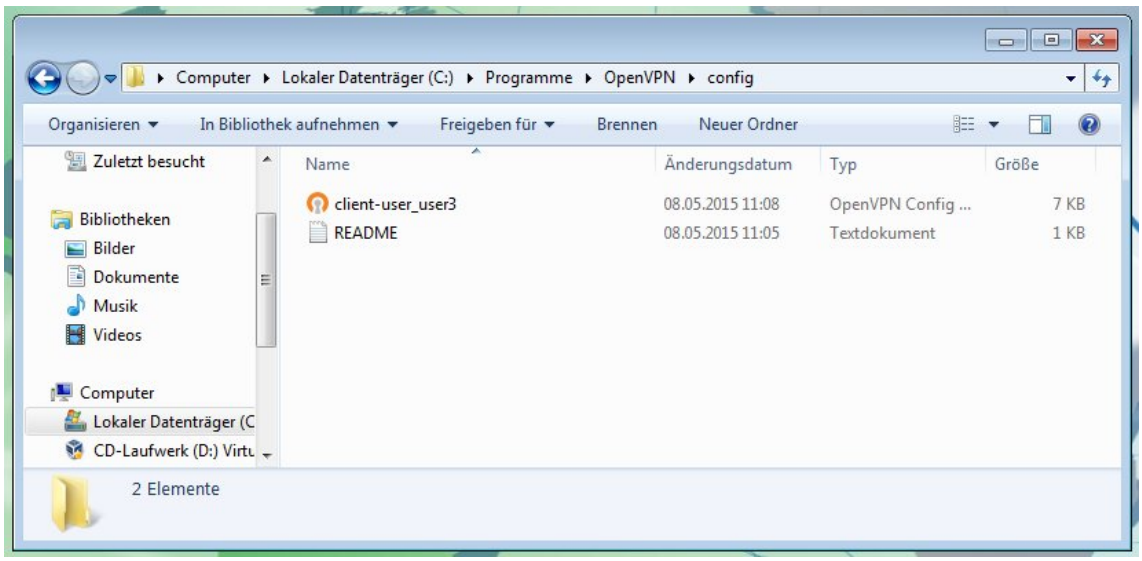
Öffnen Sie die ENA-Weboberfläche mit einem Browser. Auf der Seite „OpenVPN“ wählen Sie den gewünschten Nutzer aus. Falls die Verbindung nicht automatisch getrennt werden soll, setzen Sie den Haken bei „Nicht trennen“, anschließend den Knopf „Client-Konfig“ drücken, um die entsprechende Datei herunterzuladen:



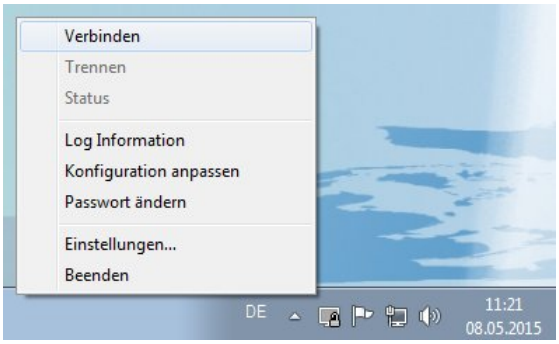


Kopieren Sie die heruntergeladene Datei aus dem Download-Ordner in den Ordner „C:\Programme\OpenVPN\config“:

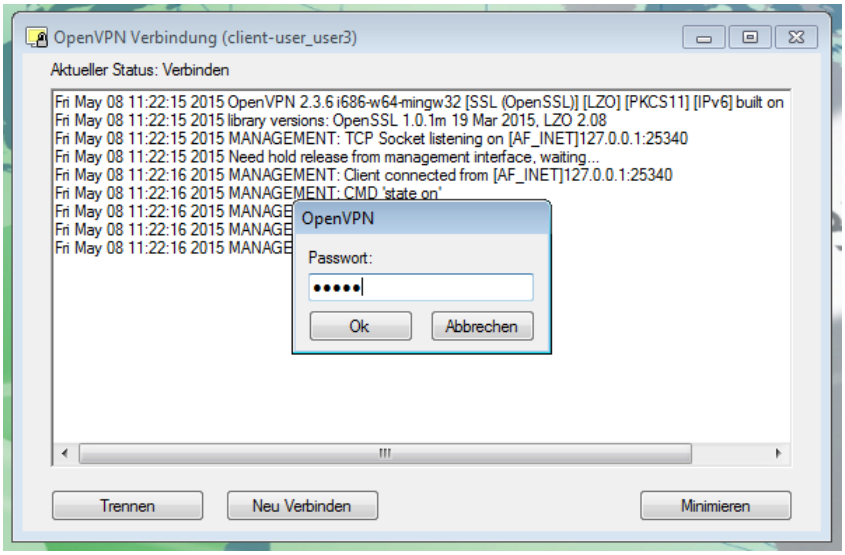




Nun können Sie sich mit dem VPN verbinden. Klicken Sie dazu mit der rechten Maustaste auf das OpenVPN GUI Symbol unten rechts im Bildschirm und wählen Sie „Verbinden“:



Sie werden dabei aufgefordert, das Passwort einzugeben, das beim Anlegen des VPN-Benutzers in der ENA vergeben wurde:



Danach sind Sie verbunden:

KNX-Anbindung

Über KNX-Gruppenadressen können bestimmte Funktionen getriggert werden, z.B. der OpenVPN-Server gestartet oder gestoppt werden. Dazu muss zuerst die IP-Adresse einer KNXnet/IP-Schnittstelle oder eines KNXnet/IP-Routers konfiguriert werden, damit eine Tunneling-Verbindung zum KNX-Bus aufgebaut werden kann.

KNXnet/IP-Verbindung

Hier muss die IP-Adresse der KNXnet/IP-Schnittstelle oder des KNXnet/IP-Routers angegeben werden (siehe Abbildung 11).

Abbildung 11: KNXnet/IP-Tunneling-Verbindung

OpenVPN-KNX-Anbindung

Der OpenVPN-Server kann über eine 1-Bit KNX-Gruppenadresse gestartet bzw. gestoppt werden. Über eine weitere kann der aktuelle Status ausgegeben werden (siehe Abbildung 12).

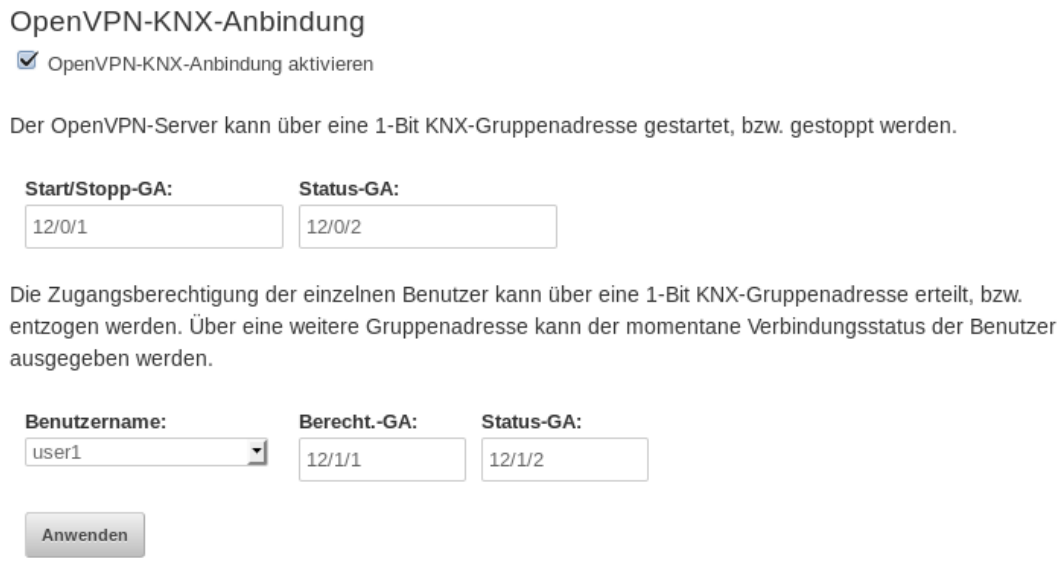


Abbildung 12: OpenVPN-KNX-Anbindung

Die Zugangsberechtigung für bis zu 16 Benutzer kann über eine 1-Bit KNX-Gruppenadressen erteilt bzw. entzogen werden. Über eine weitere Gruppenadresse kann der momentane Verbindungsstatus der Benutzer ausgegeben werden.

Hinweis

Wird die Zugangsberechtigung eines Benutzers entzogen, wird die Verbindung des Benutzers nicht getrennt, falls er gerade eingeloggt ist. Die Aktualisierung des Verbindungsstatus der Benutzer verzögert sich bis zu zwei Minuten.

Administration

Zugangsdaten zur Webadmin-Oberfläche ändern

Hier können die Zugangsdaten zur administrativen Weboberfläche der ENA geändert werden.

Neustart

Das Gerät wird neu gestartet. Der Vorgang dauert etwa eine Minute.

Werkseinstellungen wiederherstellen

Die Werkseinstellungen werden wiederhergestellt und das Gerät wird neu gestartet. Der Vorgang dauert etwa zwei Minuten.

Hinweis

Falls das Webinterface nicht mehr erreichbar ist, können die Werkseinstellungen wie folgt wiederhergestellt werden: Während des Betriebs (LED blinkt im Sekundentakt) den Resettaster mindestens 10 Sekunden lang drücken. Sobald die LED schneller blinkt, kann der Taster losgelassen werden. Die ENA führt dann einen Neustart aus und stellt die Werkseinstellungen wieder her.

Firmware aktualisieren

Firmwareupgrade-Datei auswählen und hochladen. Nach dem Upgrade startet das Gerät neu. Der Vorgang dauert etwa zwei Minuten.

Konfiguration sichern

Die aktuelle Konfiguration kann in einer Datei abgespeichert und heruntergeladen werden. Sie kann dann jederzeit wiederhergestellt werden.

Hinweis

In der Sicherung sind weder Zertifikate noch OpenVPN-Benutzer enthalten.

Konfiguration wiederherstellen

Eine zuvor gesicherte Konfiguration wiederherstellen.

Änderungsverzeichnis

1: 28.1.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- Initialversion

2: 25.2.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- Anpassungen für Firmwareversion 1.000

3: 23.3.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- Funktionsbeschreibung erweitert

4: 4.5.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- OpenVPN-Einrichtung auf Clients erweitert

5: 8.5.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- OpenVPN-Einrichtung auf Clients erweitert

6: 1.6.2015 , C. Sykosch

- Sprachliche Korrekturen

7: 2.6.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- Korrekturen

8: 7.10.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- Korrekturen
- OpenVPN on demand Kapitel aktualisiert.