enertexbayern gmbh
simulation entwicklung consulting

Handbuch und Konfiguration

ENA²

Hinweis

Inhalt

Hinweise

- Einbau und Montage elektrischer Geräte darf nur durch Elektrofachkräfte erfolgen.
- Beim Anschluss von KNX-Schnittstellen werden Fachkenntnisse durch KNX-Schulungen vorausgesetzt.
- Bei Nichtbeachtung der Anleitung können Schäden am Gerät, sowie ein 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.

Funktion

Die ENA² vereint vier wichtige Funktionen in einem Gerät:

- (Fern-)Wartung der KNX-Installation durch den integrierten IP-Tunnel für die ETS.
- Fernzugang zum Netzwerk, um beispielsweise vom Mobiltelefon aus auf die Web-Visualisierung des Enertex EibPC² zuzugreifen.
- Aufzeichnung von KNX-Telegrammen zur Auswertung direkt auf dem Gerät oder zum Export und Archivierung. Die exportierten Telegramme können im Gruppenmonitor der ETS geladen werden.
- „Sicheres Gebäudenetzwerk“: Schutz der netzwerkbasierten Komponenten der Gebäudeautomatisierung vor ungewolltem Zugriff und klare Trennung des Gebäude-Netzwerkes vom privaten oder Firmennetz.

In der Werkseinstellung befinden sich die Netzwerkschnittstellen im „Switch-Modus“ und erwartet die Zuteilung einer IP-Adresse von einem DHCP-Server.

Netzwerkmodus

Switch-Modus

Im Switch-Modus sind die beiden Netzwerkschnittstellen LAN1 und LAN2 über einen internen Switch verbunden. Dieser leitet alle Daten zwischen den Ports weiter. Die ENA² selbst besitzt nur eine IP- und MAC-Adresse. Sie können damit das Gerät mit der einen Netzwerkschnittstelle mit dem vorhandenen Netzwerk verbinden und an der anderen Schnittstelle beispielsweise einen KNX IP-Router anstecken. Dabei spielt es keine Rolle, welche Netzwerkschnittstelle Sie jeweils verwenden.

Achtung: Kommunikation zwischen LAN1 und LAN2 ist nur möglich, wenn die ENA² gestartet und betriebsbereit ist. Anderenfalls ist keine Kommunikation zwischen LAN1 und LAN2 möglich. Dies ist auch der Fall, wenn das Gerät neu gestartet wird.

Da alle Daten direkt weitergeleitet werden, kann die ENA² die angeschlossenen Geräte jedoch nicht vor ungewollten Zugriffen schützen. Verwenden Sie dazu den „Firewall-Modus“.

Zugriff auf die integrierte Schnittstelle und Fernzugang stehen selbstverständlich uneingeschränkt zur Verfügung.

Firewall-Modus

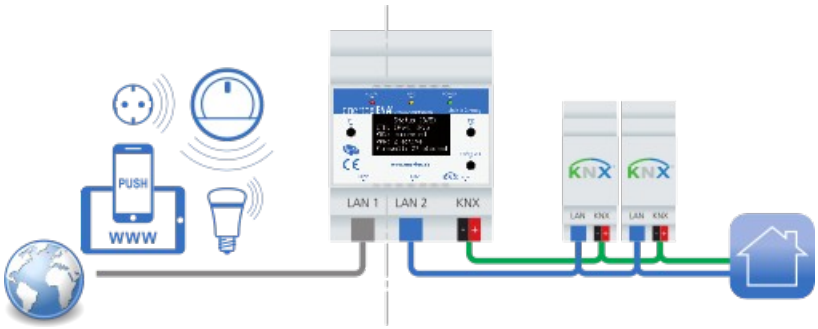


Abbildung 1: Firewall-Modus

In diesem Modus werden die beiden Netzwerkschnittstellen LAN1 und LAN2 getrennt behandelt. Sie besitzen eigene IP- und MAC-Adressen.

Die IP-Adressen dürfen nicht im selben Netz liegen!

Sie dürfen also beispielsweise nicht beide auf DHCP konfiguriert sein und mit dem gleichen DHCP-Server verbunden sein oder die IP-Adresse 192.168.1.1/Netzmaske 255.255.0.0 und 192.168.2.1/Netzmaske 255.255.0.0 besitzen!

Das Netzwerk ist in diesem Modus aufgeteilt:

Heimnetz an LAN1:

Das bestehende Heimnetz mit Zugang zum Internet, typischerweise über einen Router des Internet-Providers. Die ENA² kann Zugriffe innerhalb des Netzes oder nach außen nicht einschränken, sie ist ein regulärer Teilnehmer des Netzes.

„Sicheres Gebäudenetzwerk“ an LAN2:

Dieses Netz wird von der ENA² verwaltetet. Die Daten zwischen LAN1 und LAN2 können von der ENA² kontrolliert werden. Die ENA² vergibt bei Bedarf IP-Adressen per DHCP und stellt NTP und DNS für dieses Netz bereit. Über einfach zu konfigurierende Filter-Regeln kann der Zugriff zwischen den Netzen eingeschränkt werden.

So kann z.B. Internet-Zugriff nur für bestimmte Geräte im „Sicheren Gebäudenetzwerk“ aktiviert werden, oder der Zugriff auf den ETS-Programmiertunnel der integrierten IP-Schnittstelle darf nur von bestimmten Geräten im Heimnetz erfolgen.

Kurzbeschreibung

Die Funktionen im Überblick:

- Sicherer Fernzugang zum lokalen Netzwerk – ohne Cloud, Ende-zu-Ende-verschlüsselt zwischen mobilem Gerät und ENA²
- Optionale Vermittlung des Fernzugangs über Enertex Relais-Server, dadurch unabhängig von der Art des Internetanschlusses (IPv4, IPv6, DS-Lite) und keine Portweiterleitung nötig
- Geführte Konfiguration direkt auf dem Gerät mit einem Webbrowser
- Einfache Benutzerverwaltung
- Integrierter kostenloser DynDNS-Dienst
- OpenVPN-Server auf dem Gerät
  - Zugriff kann auf einzelne Benutzer eingeschränkt werden
  - Steuerbar über KNX Gruppenkommunikation
  - Kostenloses Client-Programm für alle üblichen Betriebssysteme verfügbar: Windows, Linux, MacOS, Android, iOS
  - VPN „on demand“: Automatischer Verbindungsaufbau auf iOS-Geräten
- „Sicheres Gebäudenetzwerk“
  - Physikalisch getrennte Netzwerk-Schnittstellen für Heimnetz und durch die ENA² verwaltetes und geschütztes Netzwerk
  - Komfortable Freigabe und Filterung von Geräten
- Verwendung von aktuellen Sicherheitsstandards und etablierter VPN-Software
- KNX-Telegrammlogger
  - Datenbankgestütztes Speichern des Busverkehrs (~ 100.000.000 Telegramme, datentypabhängig)
  - ETS-Projektimport für Datentypen, Topologie und Geräteadressinformationen
  - Einfache Abfrage und Analyse über Webserver der ENA²
  - Grafische Anzeige von Zeit-Wertverläufen, z.B. stundenweise, tageweise
  - Fehleranalyse, z.B. Leseanfragen ohne Antworttelegramm

Anschlüsse und Bedienelemente

Abbildung 2 stellt das Gerät mit seinen Anschlüssen schematisch dar.

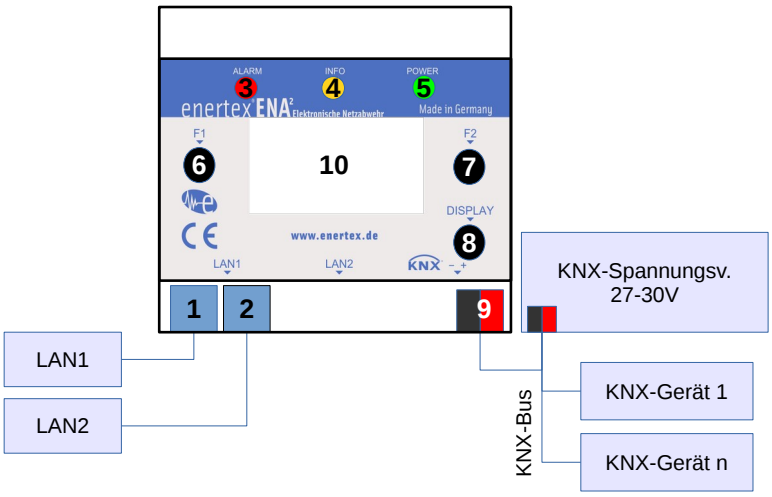


Abbildung 2: Anschluss der Enertex® ENA²

Netzwerkschnittellen	LAN1 (1), LAN2 (2)
LEDs	Alarm-LED rot (3) Info-LED orange (4) Power-LED grün (5)
Tasten	F1-Taste (6), F2-Taste (7), Display-Taste (8)
Spannungsversorgung und Bus-Zugriff	KNX (9)
Anzeige	Display (10)

Bedeutung der LEDs

1. Unmittelbar nach Verbinden des Gerätes mit der Spannungsversorgung leuchten alle drei LEDs (3,4,5) halb-hell.
2. Während des Startvorgangs leuchtet die Power-LED (5) durchgängig.
3. Nach etwa 2 Minuten ist der Startvorgang abgeschlossen. Die Power-LED (5) blinkt durchgängig und das Display ist aktiv.

Die Info-LED (4) leuchtet, sobald eine aktive VPN-Verbindung besteht.

Die Alarm-LED (3) sowie die Tasten F1 (6) und F2 (7) sind für künftige Funktionen vorgesehen.

Anzeige

Die Anzeige (10) bleibt während des Starts ausgeschaltet. Danach werden Versionsinformationen und die zugewiesene IP angezeigt. Durch Drücken der Taste (8) wird die Anzeige für 5 Minuten aktiviert.

Wird innerhalb dieser Zeit die Taste (8) erneut betätigt, wechselt die Anzeige auf die nächste Seite.

Inbetriebnahme

Voraussetzungen:

- KNX-Spannungsversorgung, 27-30V DC, sowie eine verfügbare Leistung von max. 3,2 Watt (110 mA bei 29 V Busspannung). Die typische Leistungsaufnahme liegt bei 1,8 Watt.

Wir empfehlen unsere KNX-Spannungsversorgungen Enertex® KNX PowerSupply 960³ und KNX Dual PowerSupply 1280.

- Für die Konfiguration einen Computer mit einem aktuellen Web-Browser (Google Chrome, Firefox, Safari)
- Netzwerk mit DHCP-Server. Im Auslieferungszustand arbeitet das Gerät im „Switch-Modus“ (siehe Switch-Modus S. 5).

Schließen Sie das Gerät wie in Abbildung 2 gezeigt am KNX-Bus und LAN1 am Netzwerk an. Nach etwa 2 Minuten ist das Gerät bereit und Uhrzeit und Seriennummer werden angezeigt. Drücken Sie die Display-Taste (8), bis die Anzeige für LAN1 erscheint. Lesen Sie die IP-Adresse ab, z.B. IP:192.168.1.23. Öffnen Sie diese Adresse im Web-Browser.

Hinweis: Erscheint als IP-Adresse 169.254..*, hat das Gerät keine Adresse vom DHCP-Server erhalten und verwendet die „IP Automatic Configuration“.*

Es wird eine Sicherheitswarnung vom Browser angezeigt. Bestätigen Sie, dass die Seite trotzdem geöffnet werden soll.

Sie befinden sich nun auf der ENA²-Konfigurationsseite. Oben rechts finden Sie das Handbuch für weitere Hilfe.

Der Assistent führt Sie durch die Einrichtung. Dabei haben Sie u.a. die Möglichkeit, den Netzwerkmodus zu wählen, Benutzer für Konfiguration und Fernzugriff anzulegen, und ein ETS-Projekt zu importieren.

Am Ende werden die Zertifikate generiert. Dieser Schritt dauert etwa 15 Minuten und darf nicht unterbrochen werden. Bei Import eines ETS-Projekts verlängert sich dieser anhängig vom Projekt.

Sie können währenddessen die Seite verlassen oder den Browser schließen.

Nach der Einrichtung können Sie sich mit den eingegebenen Benutzerinformationen am Gerät anmelden.

Gerätewebseite

Die gesamte Bedienung der ENA² erfolgt ausschließlich direkt auf dem Gerät. Sowohl für die Inbetriebnahme als auch für spätere Änderungen muss Netzwerkzugriff auf das Gerät bestehen. Die Gerätewebseite ist dabei von jedem Netz aus erreichbar (VPN, Heimnetz, „Sicheres Gebäudenetz“).

Für den Zugriff auf die Gerätewebseite benötigen Sie einen aktuellen Browser. Auch auf mobilen Geräten ist die Konfiguration komfortabel zu bedienen.

Im folgenden werden die grundlegenden Konzepte im Umgang mit der ENA² beschrieben.

Einrichtungsassistent

Ist das Gerät noch nicht eingerichtet oder wurde auf Werkseinstellungen zurückgesetzt, steht statt dem Login der Einrichtungsassistent zur Verfügung. Ist das Gerät fertig eingerichtet, kann dieser nicht mehr aufgerufen werden. Alle Einstellungen des Assistenten können vom Administrator in der Konfiguration angepasst werden.

Nach der Einrichtung müssen die erstellen Benutzer zur Anmeldung an der Webseite verwendet werden. Die Gerätewebseite gliedert sich grob in zwei Bereiche: den Benutzerbereich und die Konfiguration.

Benutzerbereich

Der Benutzerbereich steht jedem Benutzer nach dem Anmelden zur Verfügung. Je nach Berechtigung können verschiedene Seiten aufgerufen werden, z.B. um das eigene VPN-Profil herunterzuladen, den Telegrammlogger abzufragen, oder das Geräteprotokoll auszulesen.

Konfiguration

Nur Administratoren haben zudem Zugriff auf die Konfiguration, um Geräteeinstellungen zu verändern. Die einzelnen Konfigurationsbereiche werden im folgenden Kapitel genauer beschrieben.

Konfiguration

Benutzer

Bei der Einrichtung des Gerätes müssen bereits die ersten Benutzer angelegt werden. Es gibt drei Rollen, von denen jeder Benutzer genau eine besitzt:

- Besitzer (genau einer):
  - Der physische Besitzer des Gerätes, bzw. der KNX-Anlage.
  - Kann im Benutzerbereich das Gerät auf Werkseinstellungen zurücksetzten.
  - Ist ansonsten ein normaler Benutzer mit entsprechenden Funktionen im Benutzerbereich.
- Administrator (einer oder mehrere):
  - Besitzt Vollzugriff auf die Web-Konfiguration.
  - Hat im Benutzerbereich Zugriff auf die Funktionen, zu denen er die Berechtigung besitzt.
- Benutzer (beliebig viele):
  - Hat im Benutzerbereich Zugriff auf die Funktionen, zu denen er die Berechtigung besitzt

Bei der Initialisierung müssen der Besitzer und ein erster Administrator angelegt werden.

Jedem Benutzer sind Berechtigungen zugeordnet, größtenteils unabhängig von der Rolle. So kann beispielsweise ein Benutzer angelegt werden, der nur Zugriff auf die Telegrammaufzeichnung besitzt, sich aber nicht per VPN verbinden kann. Berechtigungen können von einem Administrator jederzeit geändert werden.

Jeder Benutzer kann seine persönlichen Informationen wie Benutzername, Name, E-Mail-Adresse, Passwort nach dem Anmelden selbst ändern. Die E-Mail-Adresse wird verwendet, um dem Benutzer E-Mails zu senden. Dazu können verschiedene Benachrichtigungen gewählt werden. So kann beispielsweise dem Administrator und dem Besitzer eine E-Mail gesendet werden, sobald ein Firmware-Update vorliegt.

Netzwerk

In den Netzwerkeinstellungen können Sie den verwendeten Netzwerkmodus (S. 5) ändern.

Zonen

Die ENA² unterscheidet verschiedene Subnetze. Diese werden als Zonen bezeichnet. In den Firewall-Einstellungen kann festgelegt werden, zwischen welchen Zonen Daten ausgetauscht werden dürfen. Abhängig vom Netzwerkmodus sind nicht alle Zonen vorhanden.

KNX

Diese Zone verwaltet die integrierte KNX Tunnelschnittstelle. Zum Öffnen einer KNX Tunnelverbindung ist es nötig, dass das entsprechende Gerät Zugriff auf diese Zone besitzt.

LAN1

Das bestehende Heim- oder Firmennetzwerk mit Zugang zum Internet. Im Switch-Modus wird nicht zwischen den Netzwerkschnittstellen LAN1 und LAN2 unterschieden und die Zone LAN1 bezieht sich auf beide Schnittstellen.

LAN2

Im Firewall-Modus verwaltet die ENA² an der Netzwerkschnittstelle LAN2 das „Sichere Gebäudenetzwerk“.

VPN

Alle verbundenen VPN-Clients erhalten eine Adresse in dieser Zone. Die ENA² leitet Anfragen in die anderen Zonen bei Bedarf weiter.

WAN

Alle Netze außerhalb der lokalen Zonen, typischerweise das Internet oder weitere Firmennetze, die über den Router von LAN1 erreichbar sind.

Adressvergabe

Je nach gewähltem Netzwerkmodus stehen verschiedene Konfigurationsmöglichkeiten zur Verfügung. Grundsätzlich kann das Gerät deine Adressen von einem DHCP-Server beziehen, oder sie werden statisch vergeben. Der Vorteil einer statischen Konfiguration ist, dass das Gerät auch wie gewohnt startet, falls der DHCP-Server nicht erreichbar sein sollte. Anderenfalls wechselt das Gerät auf „IP Automatic Configuration“ und vergibt sich selbst eine Adresse im Bereich 169.254.*.*

Dies erlaubt es, das Gerät z.B. direkt an einem PC oder Notebook anzustecken und konfigurieren zu können.

In den meisten Fällten ist die ENA² über einen Router mit dem Internet verbunden. Falls Sie eine statische IP-Adresse verwenden möchten, beachten Sie, dass diese außerhalb des dynamischen Bereichs liegen muss, der im Router konfiguriert ist.

> *Die ENA² verwendet zur Angabe von Netzen einheitlich die Angabe der Netzadresse und Präfixlänge. Dies ist die Standardschreibweise für IPv6. Bei IPv4 war bisher die Angabe einer Netzmaske üblich. Die in privaten Netzen am häufigsten verwendete Netzmaske 255.255.255.0 entspricht dabei einer Präfixlänge von 24.*

Routing

Für alle Netzbereiche gilt, dass diese eindeutig sein müssen. Werden Geräte eines anderen Bereichs adressiert, bestimmt die Route, über welches Gateway die Anfrage gesendet wird.

Ein Gateway ist ein Gerät im Netzwerk, das Anfragen für andere IP-Adressen als die eigene entgegennimmt und diese in seinem Namen, also mit seiner Absenderadresse, über seine Route weiterleitet. Die erhaltene Antwort wird dann wieder an den Anfragenden gesendet.

Beispiel: In einem privaten Netz mit einem Internet-Router besitzt dieser die IP-Adresse 192.168.178.1, die Präfixlänge ist 24. Verbundene Geräte können damit IP-Adressen aus dem Bereich 192.168.178.2 bis 192.168.178.254 verwenden. Adressen außerhalb des Bereichs (z.B. Adressen im Internet) werden über die Standardroute mit dem Internet-Router als Gateway erreicht (Standardgateway).

Heimnetz:

Netzmaske / entspricht Präfix	255.255.255.0 / 24

IP-Adresse Router	192.168.178.1
Gültige Geräteadressen	192.168.178.2 – 192.168.178.254
IP-Adresse ENA² (LAN1)	192.168.178.66

Routen der Heimnetzgeräte:

192.168.178.0/24	direkt
Standardroute	über Gateway 192.168.178.1

Wird DHCP verwendet, sendet der Router diese Information zusammen mit der IP-Adresse. Bei statischer Konfiguration muss der Router als Gateway selbst angegeben werden.

Besteht das Netzwerk aus weiteren Bereichen, müssen dafür ebenfalls Routing-Informationen vorhanden sein. Diese können entweder in jedem einzelnen Gerät konfiguriert werden, das auf die entsprechenden Netze zugreifen soll, oder sie werden direkt im Standard-Gateway für alle angeschlossenen Geräte konfiguriert.

Im Netzwerkmodus „Switch“ ist dies nicht nötig, da hier die ENA² kein eigenes Netz betreibt. Für das „Sichere Gebäudenetzwerk“ müssen diese Routing-Informationen jedoch vorhanden sein, falls aus der Zone „LAN1“ auf die Zone „LAN2“ (S. 6) zugegriffen werden soll.

„Sicheres Gebäudenetzwerk“:

Netzmaske / entspricht Präfix	255.255.255.0 / 24
IP-Adresse ENA² (LAN2)	192.168.177.1
Gültige Geräteadressen	192.168.177.2 – 192.168.177.254

Routen der ENA²:

192.168.178.0/24	direkt über LAN1
192.168.177.0/24	direkt über LAN2
Standardroute	über Gateway 192.168.178.1

Routen der Geräte im „Sicheren Gebäudenetzwerk“

192.168.177.0/24	direkt
Standardroute	über ENA² 192.168.177.1

Die Routen der Heimnetzgeräte müssen das „Sichere Gebäudenetzwerk“ enthalten, das über die ENA² zu erreichen ist. Wie beschrieben, kann diese Information direkt im Gateway (dem Internet-Router) hinterlegt werden, um für alle angeschlossenen Geräte zu gelten. Dadurch senden die Heimnetz-Geräte Daten für Geräte im „Sichere Gebäudenetzwerk“ an den Router, der diese an die ENA² weiterleitet, die die Daten dann wiederum an das entsprechende Gerät sendet.

Routen im Gateway mit Route zum „Sichere Gebäudenetzwerk“:

192.168.178.0/24	direkt
192.168.177.0/24	über ENA² 192.168.178.66 (LAN1)
Standardroute	über Internetanschluss

Alternativ wird die Route über die ENA² auf jedem Gerät einzeln gesetzt, das Zugriff auf das „Sicheren Gebäudenetzwerk“ besitzen soll. Der Weg über den Router entfällt dadurch, jedes entsprechend konfigurierte Gerät im Heimnetz sendet direkt über die ENA².

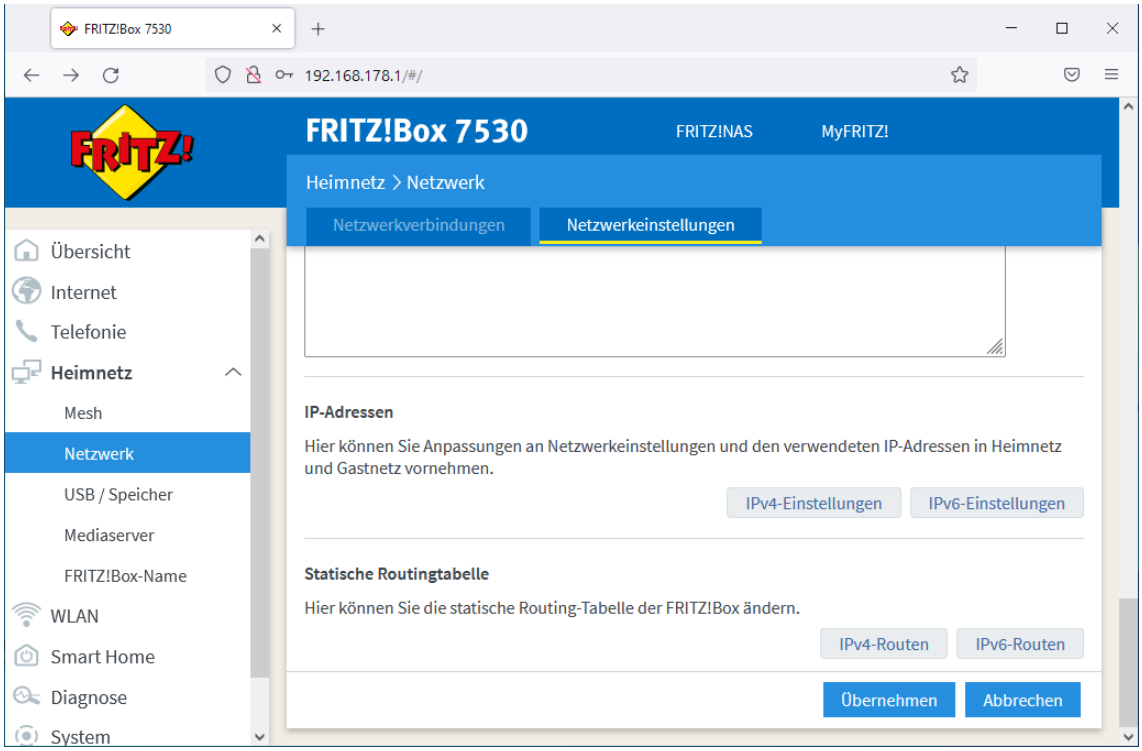
Alternativ: Routen der Heimnetzgeräte mit Route zum „Sichere Gebäudenetzwerk“:

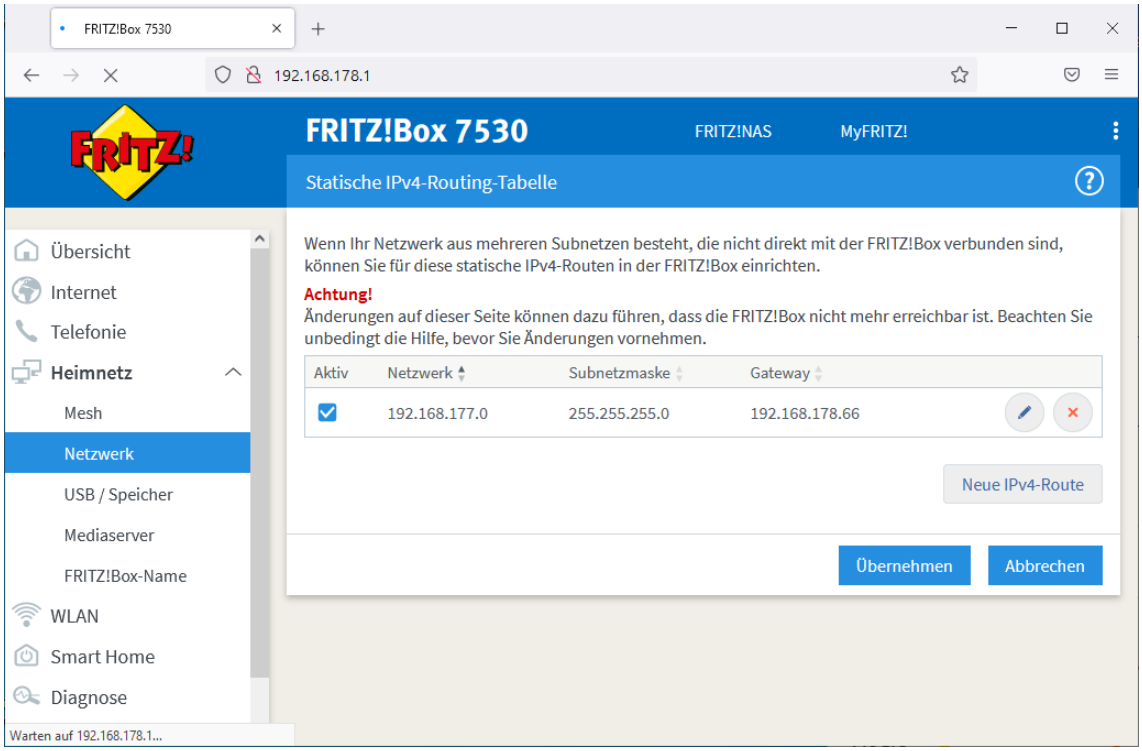
192.168.178.0/24	direkt

192.168.177.0/24	über ENA² 192.168.178.66 (LAN1)
Standardroute	über Gateway 192.168.178.1

Beispiel: Fritz!Box, FRITZ!OS 07.28:

Öffnen Sie Netzwerk → Netzwerkeinstellungen → Statische Routingtabelle → IPv4-Routen und tragen Sie die Netzwerk-Adresse des „Sicheren Gebäudenetzwerks“ ein. Hat die ENA² beispielsweise die IP-Adresse 192.168.177.1 mit Präfixlänge 24, ist die Netzwerkadresse 192.168.177.0 und die Netzmaske 255.255.255.0. Das Gateway ist die IP-Adresse der ENA² im Heimnetz. Diese sollten Sie im DHCP-Server der Fritz!Box fest zuweisen, falls Sie DHCP verwenden.





VPN

Der VPN-Server der ENA² kann sowohl per UDP als auch per TCP erreicht werden. Falls möglich, ist UDP zu bevorzugen. Insbesondere bei schlechten oder langsamen Verbindungen ist die Stabilität der Verbindung besser als bei TCP. Der Relais-Server verwendet aus technischen Gründen immer TCP als Übertragungsprotokoll.

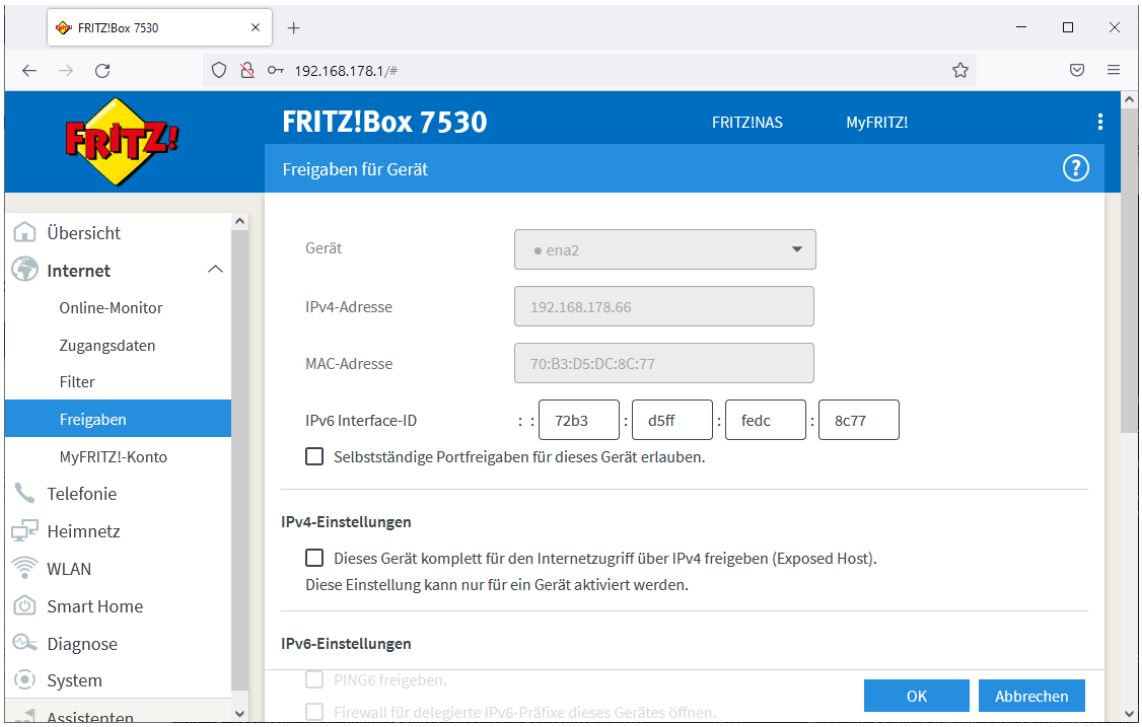
Portfreigabe

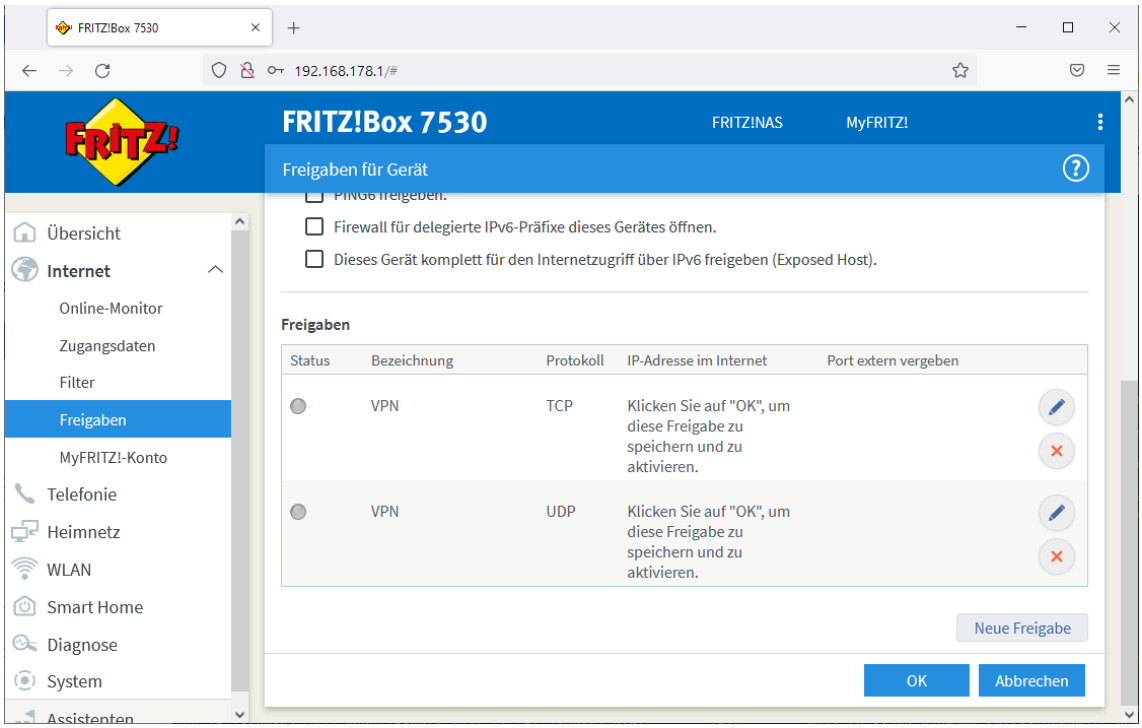
Falls Ihr Anschluss von außen erreichbar ist, können Sie den konfigurierten VPN-Server-Port (Standard: 1194) in der Liste der Port-Weiterleitungen Ihres Internet-Routers eintragen. Deaktivieren Sie beim Exportieren des VPN-Profils die Verwendung des Relais-Servers. Es wird dann der konfigurierte DDNS-Name und die zusätzlichen Hostnamen als Zieladresse im VPN-Profil hinterlegt. Als externer und interner Port der Freigabe muss der konfigurierte VPN-Server-Port angegeben werden.

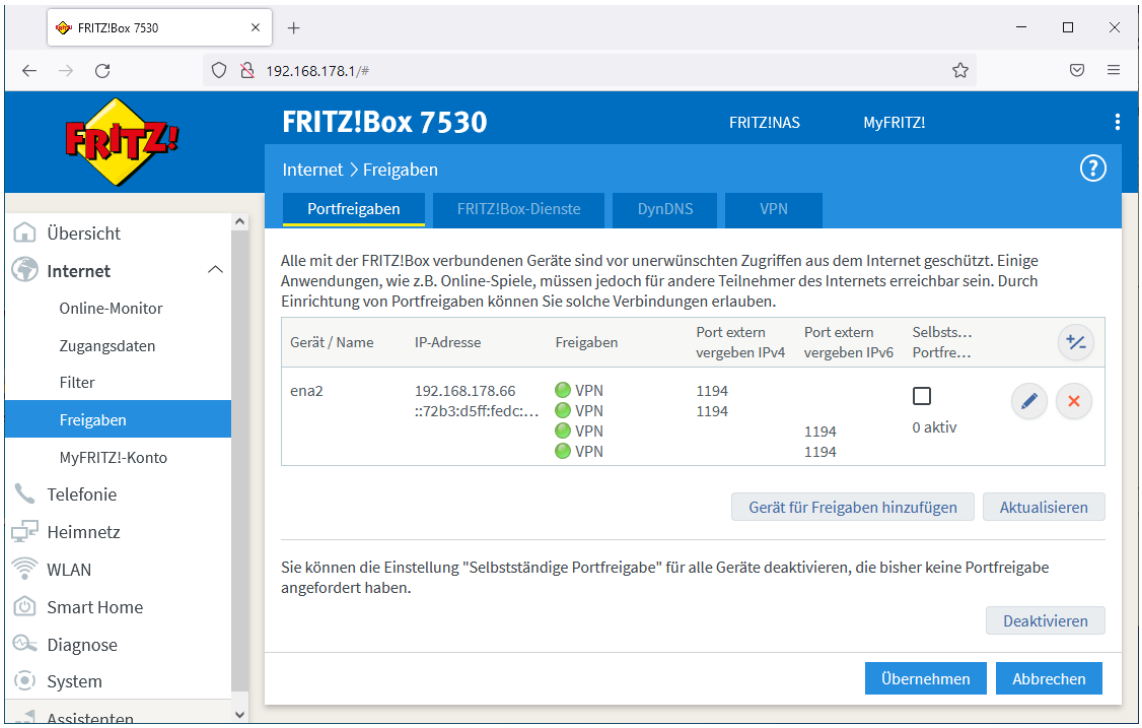
Achtung: Richten Sie keine Port-Weiterleitung für die Gerätewebseite ein. Verwenden Sie statt dessen immer eine VPN-Verbindung, um von außen auf die Konfiguration zuzugreifen!

Beispiel: Fritz!Box, FRITZ!OS 07.28:

Öffnen Sie Internet → Freigaben → Portfreigaben und fügen Sie ein neues Gerät für Freigaben hinzu. Wählen Sie die ENA² und tragen Sie den Port für UDP und/oder TCP ein.







Adressen

Der VPN-Server der ENA² erstellt, ähnlich wie das „Sichere Gebäudenetzwerk“, eigene Netze. Jedem verbundenen VPN-Client wird automatisch eine IP-Adresse innerhalb dieses Netzes zugewiesen. Er erhält zudem Routing-Informationen, um auf das Heimnetz und ggf. das „Sichere Gebäudenetzwerk“ zuzugreifen. Entsprechende Pakete werden von der ENA² weitergeleitet.

Voraussetzung ist auch hier, dass die IP-Bereiche eindeutig sind. Die Bereiche des Heimnetzes und des „Sicheren Gebäudenetzwerks“ dürfen sich also nicht mit den unten stehenden Bereichen überschneiden.

Die Adresse der VPN-Server sind fest vorgegeben.

		Serveradresse	VPN-Clientadressen
TCP	IPv4	10.23.1.1/24	10.23.1.2 – 10.23.1.254
	IPv6	fd60:dc0:ffee:600d:1::1/64	fd60:0dc0:ffee:600d:0000:0000:0000:0000 – fd60:0dc0:ffee:600d:ffff:ffff:ffff:ffff
UDP	IPv4	10.23.2.1/24	10.23.2.2 – 10.23.2.254
	IPv6	fd60:dc0:ffee:600d:2::1/64	fd60:0dc0:ffee:600d:0000:0000:0000:0000 – fd60:0dc0:ffee:600d:ffff:ffff:ffff:ffff

VPN on demand (nur iOS)

Auf iOS-Geräten ist es möglich, die VPN-Verbindung automatisch im Hintergrund aufzubauen, sobald auf einen bestimmten DNS-Namen zugegriffen wird. VPN on demand kann sowohl im Switch- als auch im Firewall-Modus verwendet werden.

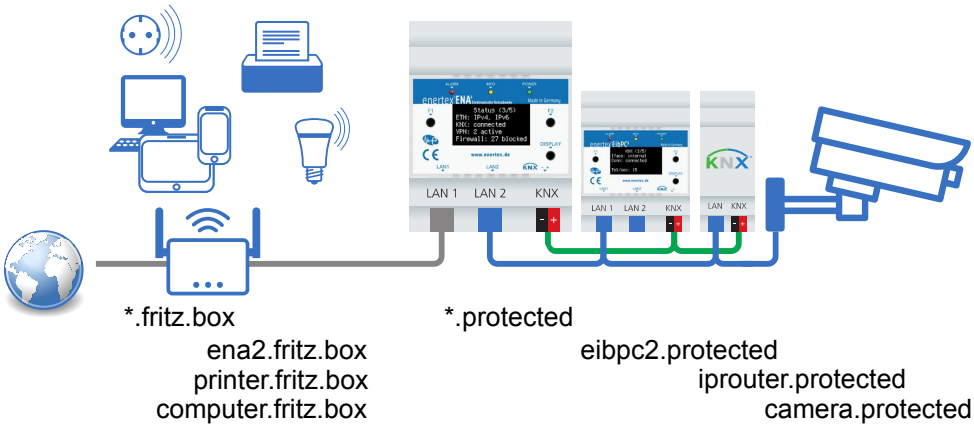


Abbildung 3: Namensauflösung bei VPN on demand

Im folgenden Beispiel ist die ENA² im Heimnetzwerk eingebunden. Sie befindet sich im Firewall-Modus und verwaltet das Sichere Gebäudenetzwerk, in dem sich weitere Geräte befinden (vgl. Abbildung 3).

Das Heimnetzwerk wird meist von einem Router mit integriertem DNS-Server verwaltet. Dieser weist den Geräten einen Namen in einer lokalen Domäne zu. Das bedeutet, dass die Namenszuteilung nur im angeschlossenen Netzwerk („hinter dem Router“) gültig ist, aber nicht außerhalb (z.B. im Internet).

Die Fritz!Box im Beispiel verwendet als Domäne `.fritz.box`, die ENA² ist im Heimnetzwerk mit dem DNS-Namen `ena2.fritz.box` erreichbar. So kann im Webbrowser die Gerätewebseite unter der Adresse `https://ena2.fritz.box/` erreicht werden. Die Domäne kann bei den meisten Routern auch weggelassen werden, so dass ein Aufruf von `https://ena2/` ebenso möglich ist.

Im Firewall-Modus betreibt die ENA² ebenfalls einen DNS-Server zur Verwaltung der lokalen Domäne `.protected`. Im Beispiel in Abbildung 3 besitzen die Geräte im Sicheren Gebäudenetzwerk die DNS-Namen `eibpc2.protected`, `iprouter.protected` und `camera.protected`. Die Web-Visualisierung des EibPC² ist innerhalb des Sicheren Gebäudenetzwerks z.B. unter der Adresse `http://eibpc2.protected` zu erreichen. Für den Zugriff aus dem Heimnetzwerk siehe Routing (S. 10).

Durch VPN on demand kann die VPN-Verbindung in obigem Beispiel automatisch aufgebaut werden, sobald auf `eibpc2.protected` zugegriffen wird. Dies ist nur möglich, falls von einem iOS Gerät (Apple) aus die Seite aufgerufen wird. Der Komfortgewinn ist dabei spürbar, da nicht extra die OpenVPN Connect-App geöffnet werden muss. Statt einzelner DNS-Namen kann der Platzhalter `*` verwendet werden. Dadurch wird die VPN-Verbindung beim Zugriff auf beliebige Adressen innerhalb der nachfolgenden Domain aufgebaut.

In Abbildung 4 ist dies beispielhaft für das gesamte Heimnetzwerk (`*.fritz.box`) sowie das gesamte Sichere Gebäudenetzwerk (`*.protected`) konfiguriert.

Achtung: Die Einstellungen zu VPN on demand betreffen nur neu exportierte VPN-Profile.

Durch die Konfiguration von VPN on demand besteht nicht automatisch Zugriff auf die entsprechenden Geräte. Es kann zwar der Name eines Gerätes für VPN on demand konfiguriert werden, der Zugriff aber durch die Firewall-Regeln verhindert werden. Dadurch hat es in der Regel keinen Nachteil, jeweils die gesamte lokale Domäne einzutragen.

Um zu verhindern, dass innerhalb des eigenen Netzes beim Zugriff auf den DNS-Namen die VPN-Verbindung aufgebaut wird, sollte die SSID des WLANs hinterlegt werden.

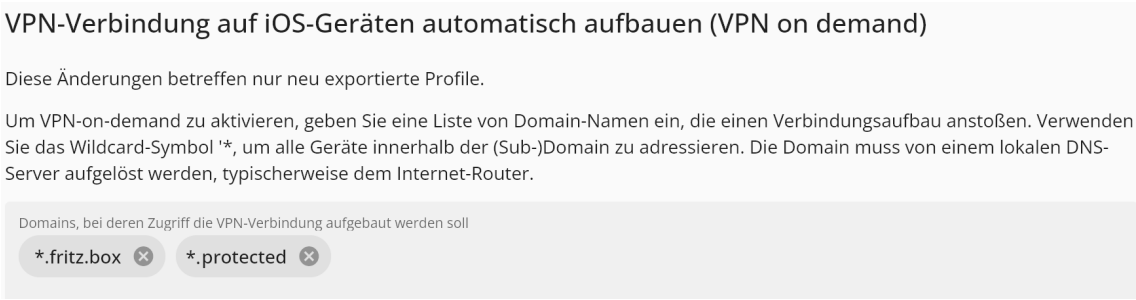


Abbildung 4: VPN Einstellungen für VPN on demand

Relais-Server

Alle Netzwerkgeräte, also Internet-Router, Server, Rechner werden im Internet und in privaten Netzen über ihre IP-Adresse angesprochen. Seit Jahren gibt es neben parallel zum klassischen IPv4 den Nachfolger IPv6. Als Anwender spielt das selten eine Rolle, da Zugriffe z.B. auf Web-Seiten meist anhand ihrer DNS-Namen erfolgen. Beim Zugriff auf http://www.enertex.de wird deshalb im Hintergrund eine Namensauflösung durchgeführt, also eine Abfrage, welche IP-Adresse zum DNS-Eintrag www.enertex.de gehört. Die eigentliche Verbindung wird dann zur zurückgegebenen IP-Adresse aufgebaut. Da nahezu alle Dienste über IPv4 und IPv6 erreichbar sind und sich der Internetprovider um eine Übersetzung kümmert, ist der Zugriff immer erfolgreich, unabhängig vom der Art des eigenen Internet-Anschlusses. Problematischer ist der Zugriff „von außen“ statt „von innen“. Soll also eine Verbindung vom Smartphone zum eigenen Internetanschluss aufgebaut werden, hängt es vom Mobilfunk- und dem Internetprovider des Anschlusses ab, ob der Zugriff möglich ist.

Enertex Bayern GmbH bietet für den Fernzugriff einen Weiterleitungsdienst – den Relais-Server. Sie benötigen dadurch in der Regel keine Konfiguration des Internet-Routers, und sind unabhängig von IPv4/IPv6/DS-Lite des Internet- und Mobilfunkanbieters. Dazu baut die ENA² eine Verbindung zum Relais-Server auf und hält sie offen. Möchte sich ein VPN-Benutzer mit der ENA² verbinden, baut dieser ebenfalls eine Verbindung zum Relais-Server auf, statt sich direkt zu verbinden. Der Relais-Server leitet nun die verschlüsselten Daten zwischen VPN-Client und ENA² weiter. Sie können diesen Dienst verwenden, ohne sich Sorgen um die Sicherheit Ihrer Daten machen zu müssen. Ihre Daten sind durchgängig verschlüsselt und können nur von Ihrer ENA² und Ihrem VPN-Clientprogramm entschlüsselt werden (E2EE/Ende-zu-Ende-Verschlüsselung).

Es ist keine Registrierung notwendig. Für jedes VPN-Profil kann die Verwendung des Relais-Servers gewählt werden. Eine direkte Verbindung ist selbstverständlich ebenfalls möglich.

Um den Relais-Server zu verwenden, aktivieren Sie diesen in den VPN-Einstellungen und aktivieren Sie „Relais-Server verwenden“ beim Exportieren eines VPN-Profils. Außerdem muss die ENA² Internetzugriff besitzen. Die Verbindung mit dem Relais-Server erfolgt mit folgender Zieladresse:

```
ena.enertex.de:2301 TCP
```

Die Verwendung des Relais-Servers ist kostenlos. Die Datenmenge pro ENA² ist auf 5 GB pro Monat beschränkt.

DynDNS

Zur einfachen Adressierung des Internet-Anschlusses kann der kostenlose DynDNS-Dienst der ENA² genutzt werden. Es ist keine weitere Konfiguration oder Registrierung bei einem anderen Anbieter nötig. Wählen Sie einfach die gewünschte Adresse, um den Rest kümmert sich die ENA².

Der Dienst sorgt dafür, dass Sie immer eine feste Adresse für Ihren Internetanschluss haben. Die meisten Provider vergeben beim Einwählen immer unterschiedliche IP-Adressen. Die ENA² meldet sich dazu regelmäßig am Enertex DynDNS-Dienst an. Dieser prüft, ob sich die Adresse geändert hat, und aktualisiert ggf. den DNS-Eintrag.

Hinweis: Dies ist nicht mit einem Fernzugang gleichzusetzen, sondern lediglich ein Verweis auf Ihre aktuelle Adresse. Falls Sie andere Geräte unter dieser Adresse erreichen möchten, müssen Sie im Internet-Router die entsprechenden Ports zu den Geräten weiterleiten.

Richten Sie nur Weiterleitungen zu ausreichend gesicherten Geräten ein! Verwenden Sie nach Möglichkeit stets eine VPN-Verbindung, um auf Geräte in Ihrem Netzwerk zuzugreifen, statt Ports einzelner Geräte direkt freizugeben.

Mit Hilfe der DynDNS-Adresse können Sie Ihren Anschluss per VPN auch erreichen, falls Sie den Relais-Server nicht verwenden. Die DynDNS-Adresse wird dann automatisch für exportierte VPN-Profile verwendet.

Dass die Aktualisierung der Adresse funktioniert können Sie auch anhand der Einträge im Protokoll nachvollziehen:

```
hostname meinedomain.ddns.enertex.de refreshed on 2021-11-23T09:20:43.175Z to
1.2.3.4, 1000:1:2:3:4:5:6:7, interval: 3600 s
```

KNX

Integrierte Schnittstelle

Das Gerät besitzt eine integrierte KNX-Schnittstelle, die zur Bus-Kommunikation genutzt werden kann, und zusätzlich einen IP-Tunnel für die ETS bereitstellt. Die ETS findet die Schnittstelle automatisch, sofern sich der Rechner im gleichen Netz (Heimnetz oder „Sicheres Gebäudenetzwerk“). Voraussetzung ist jeweils, dass der Zugriff in den Firewall-Regeln erlaubt wurde.

Die integrierte Schnittstelle steht immer zur Verfügung, auch wenn für den Bus-Zugriff eine andere Schnittstelle gewählt wurde.

Physikalische Adressen

Die physikalischen Adressen der ENA² (Geräteadresse) sowie der beiden KNX-IP-Tunnel können angepasst werden. Passen Sie die Adressen entsprechend Ihrer KNX-Konfiguration an. Befindet sich die ENA² physikalisch beispielsweise auf Linie 1.1, so sollten sich die Adressen ebenfalls auf dieser Linie befinden, beispielsweise

- Geräteadresse 1.1.250
- ENA²-Tunnel 1.1.251
- ETS-Tunnel 1.1.252

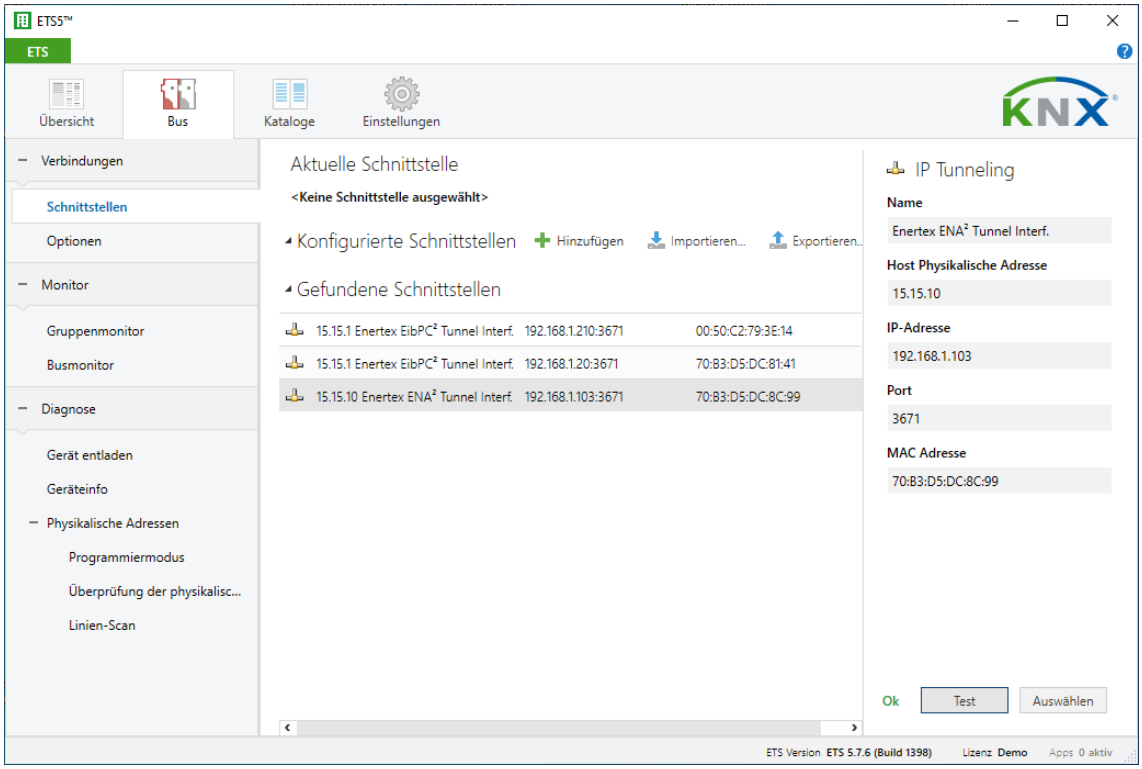
Damit vermeiden Sie die Warnung der ETS, dass sich die Schnittstellenadresse außerhalb des konfigurierten Bereichs befindet.

Zugriff über VPN

Die IP-Schnittstelle kann von allen Zonen aus genutzt werden, sofern der KNX-Zugriff in den Firewall-Regeln der Zone aktiviert wurde. Über VPN werden Multicast-Pakete nicht weitergeleitet, weshalb die automatische Suche der ETS die Schnittstelle nicht auflistet. Fügen Sie deshalb die Schnittstelle manuell hinzu. Dabei können Sie die folgenden IP-Adressen verwenden:

- 10.23.1.1 bei Verwendung des Relais-Servers bzw. OpenVPN mit Portfreigabe über TCP

- 10.23.1.2 bei Verwendung von OpenVPN mit Portfreigabe über UDP
- die konfigurierte ENA²-IP im Heimnetz
- die konfigurierte ENA²-IP im „Sicheren Gebäudenetzwerk“



Problembehebung

Falls die ETS beim Zugriff auf die Tunnelschnittstelle meldet, dass keine weiteren Verbindungen mehr verfügbar sind, starten Sie die KNX-Schnittstelle der ENA² über den entsprechenden Knopf in der KNX-Konfiguration der ENA² neu.

Steuerung über KNX-Telegramme

Der VPN-Server und einzelne Benutzer können über Gruppenadress-Telegramme gesteuert werden. Tragen Sie dazu die gewünschten Gruppenadressen ein. Ein ETS-Projektimport ist dazu nicht notwendig.

VPN-Verbindung

Um eine VPN-Verbindung aufzubauen, wird ein VPN-Profil benötigt. Dies enthält alle angaben zur Verbindung (Adresse, Einstellungen), sowie die Schlüsselinformationen. Sind die Schlüssel falsch, z.B. weil die Zertifikatskette neu erstellt wurde, wird der Verbindungsaufbau aus Sicherheitsgründen vom VPN-Server ignoriert. Es wird also keine Fehlermeldung „Schlüssel falsch“ generiert.

Sind die Schlüsselinformationen korrekt, der Benutzer ist aber aktuell nicht per KNX freigeschaltet, wird die Verbindung vom Server wieder getrennt.

Melden Sie sich mit dem VPN-Benutzer an der ENA² an, der für den Fernzugriff verwendet werden soll. Im Benutzerbereich finden Sie die Seite „VPN-Profil“. Dort können profilspezifische Einstellungen gesetzt und das Profil exportiert werden. Diese Einstellungen wirken sich nur auf das exportierte Profil aus.

Beim Export muss ein Passwort vergeben werden. Insbesondere beim Versand per E-Mail ist dies wichtig, da die E-Mail selbst nicht verschlüsselt ist, das Profil aber alle Schlüsselinformationen beinhaltet, die zum Aufbau der VPN-Verbindung notwendig sind.

Nach dem Import auf dem Gerät sollten Sie das Profil wieder löschen.

Die Vorgehensweise zum Importieren eines Profils befindet sich auch auf der „VPN-Profil“-Seite der ENA², so dass jeder Nutzer selbst sein Profil herunterladen und importieren kann.

Windows, Linux, Android, macOS

Profil für OpenVPN Connect exportieren

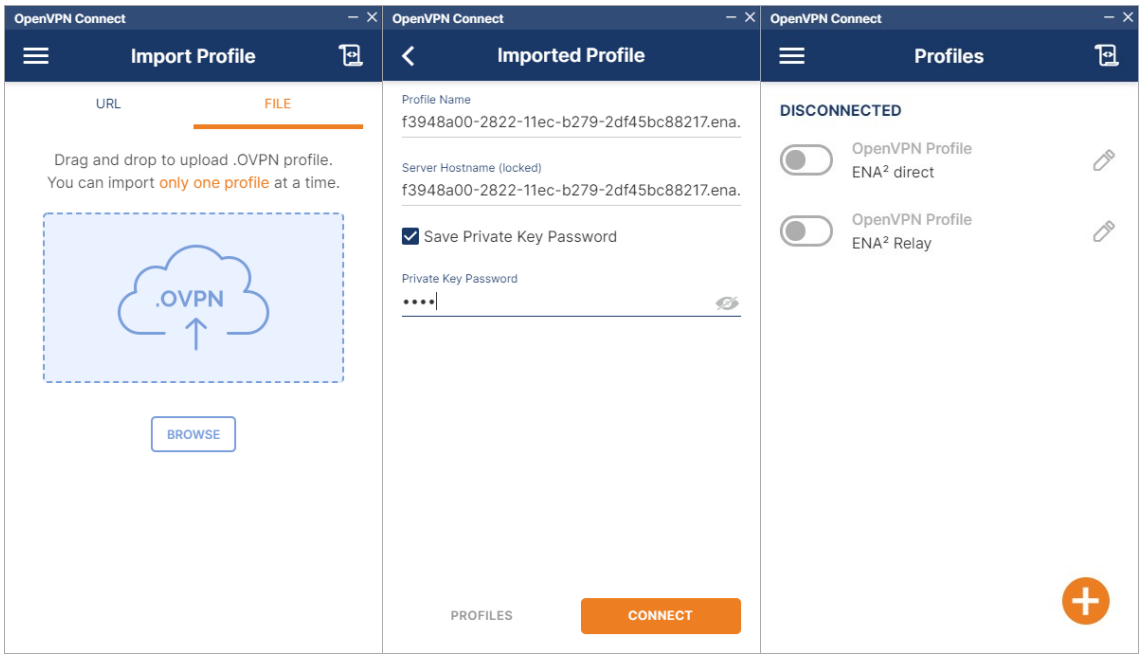
OpenVPN Connect herunterladen:

- Windows 10, Windows 11: https://www.enertex.de/ena-openvpnclient-win
- Android: https://www.enertex.de/ena-openvpnclient-android
- Linux: https://www.enertex.de/ena-openvpnclient-linux
- macOS: https://www.enertex.de/ena-openvpnclient-osx

OpenVPN Connect öffnen

Profil importieren

Geben Sie das Passwort ein, das beim Exportieren gewählt wurde. Sie können das Profil umbenennen.



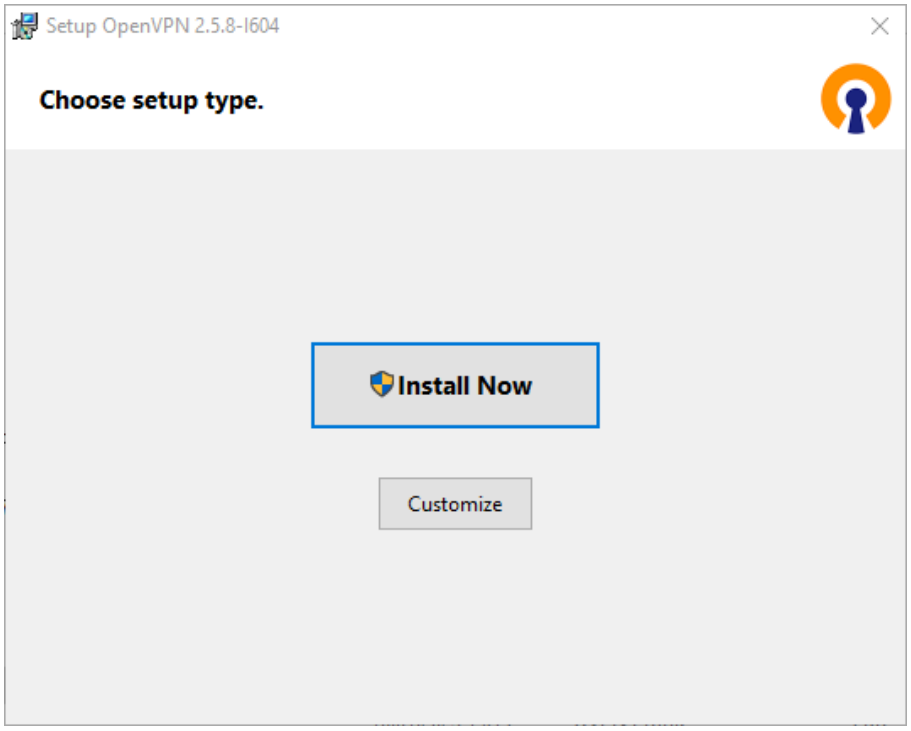
OpenVPN-GUI

Alternativ zu OpenVPN Connect kann unter Windows der Open-Source-Client OpenVPN-GUI verwendet werden, falls es Probleme beim Verbindungsaufbau gibt.

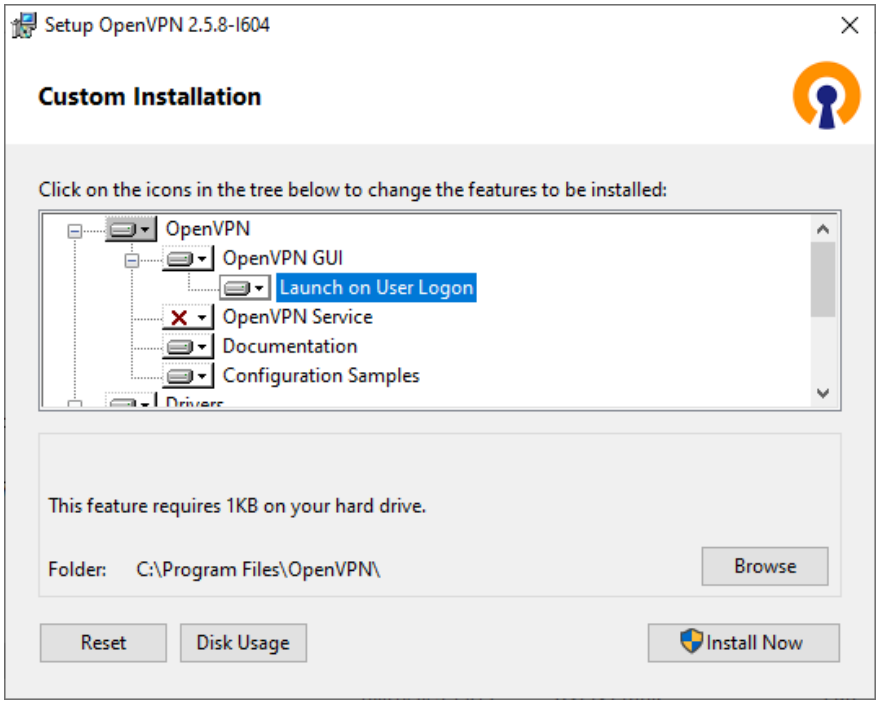
https://www.enertex.de/ena-openvpngui-win

Laden Sie sich die aktuelle (nicht Beta-)Version von OpenVPN herunter und starten Sie die Installation. Verwenden Sie entweder `Windows 64-bit MSI installer` oder `Windows 32-bit MSI installer`.

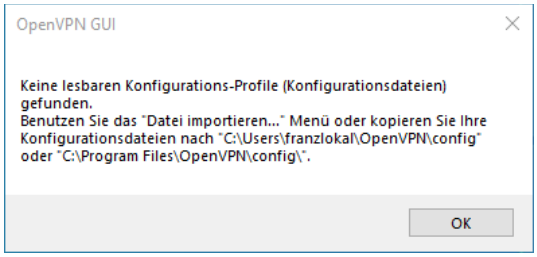
Wählen Sie „Customize“.



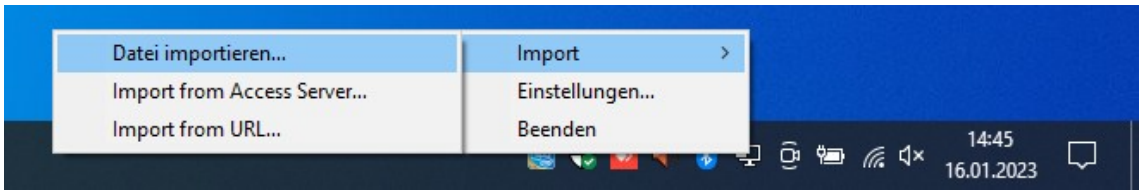
Die OpenVPN Service-Komponente wird nicht benötigt.



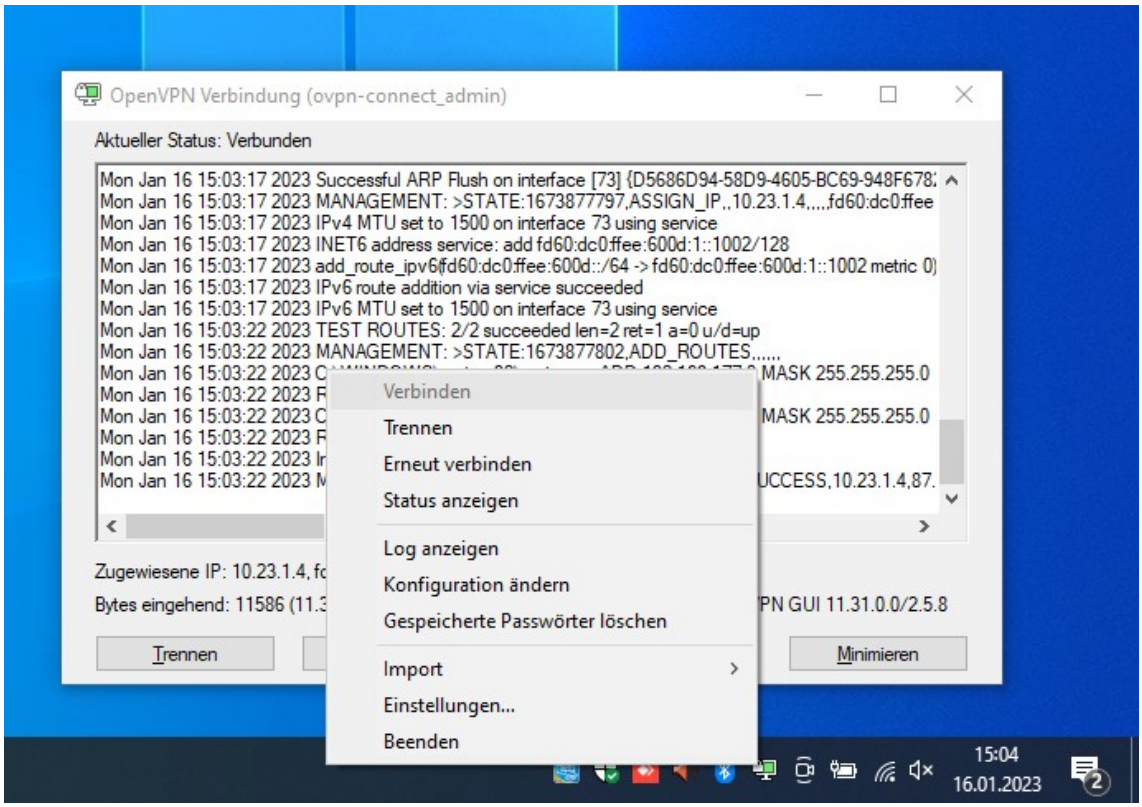
Beim ersten Start wird der Hinweis angezeigt, dass noch kein Profil importiert wurde.



Klicken Sie mit der rechten Maustaste auf das neue Icon in der Taskleiste und importieren Sie ein Profil.



Anschließend können Sie „Verbinden“ wählen, um die VPN-Verbindung aufzubauen.



iOS 15

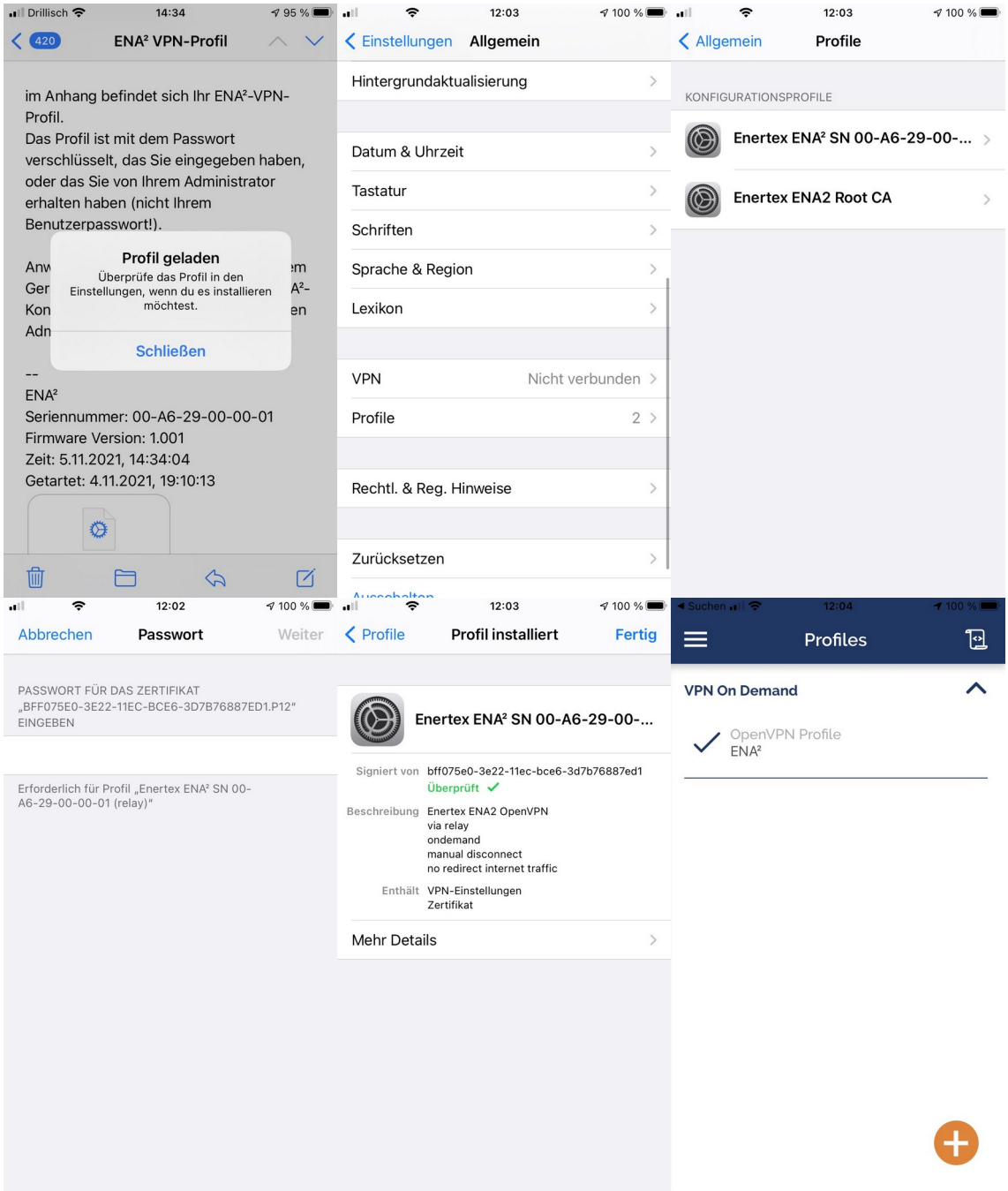
Mobileconfig für iOS erstellen

OpenVPN Connect für iOS herunterladen:

iPhone iOS: https://www.enertex.de/ena-openvpnclient-ios

Öffnen Sie die Datei .mobileconfig.

Öffnen Sie Einstellungen → Allgemein → Profile & Geräteverwaltung und importieren Sie das Zertifikat. Öffnen Sie das Profil und installieren Sie es. Das Profil wird nun in der OpenVPN-Connect App angezeigt.



Telegrammaufzeichnung

Die ENA² zeichnet automatisch alle empfangenen KNX-Telegramme der integrierten Schnittstelle oder einer konfigurierten IP-Schnittstelle auf. Rohtelegramme können in einem ETS-kompatiblen Format exportiert werden.

Ist ein ETS-Projekt importiert, werden die Telegramme decodiert und die empfangenen Werte abgespeichert. Diese können Sie auf der Geräte-Webseite abfragen und auswerten. So lässt sich z.B. der Temperaturverlauf als Zeit-Wert-Diagramm darstellen.

Zusätzlich bietet der Telegrammlogger vorbereitete Analysefunktionen, um z.B. alle Leseanfragen ohne Antworttelegramm abzufragen.

Zertifikate

Zertifikate sind ein zentraler Bestandteil der Sicherheit im Internet. Sie werden hauptsächlich verwendet, um sich seinem Gegenüber auszuweisen.

Ein Zertifikat ist vergleichbar mit dem Personalausweis. Der Ausweis selbst erhält seine Glaubwürdigkeit durch zwei Annahmen:

1. Sie vertrauen darauf, dass die ausgebende Stelle die Identität überprüft hat.
2. Der Ausweis kann nicht nachgemacht werden, ohne dass es Ihnen auffällt.

Ob der Ausweis Ihrem Gegenüber oder seinem Nachbarn gehört, können Sie selbst anhand des Passfotos überprüfen.

Bei digitalen Zertifikaten tritt eine Zertifizierungsstelle, die sog. „Certificate Authority“ (CA) an die Stelle des ausgebenden Behörde. Dies ist eine Firma, die garantiert, Zertifikate nur nach erfolgreicher Identitätsprüfung auszustellen. Soll das Zertifikat genutzt werden, um die Identität eines Servers zu beweisen, überprüft die CA die Internet-Adresse (Domain, ggf. Hostname) des Servers. Ist die Prüfung erfolgreich, wird diese Adresse im Zertifikat gespeichert (Subject). Die Adresse tritt hier an die Stelle des Passfotos.

Die Zertifizierungsstelle signiert als Beweis der Überprüfung das Server-Zertifikat. Das Zertifikat, das zur Signatur verwendet wurde, wird im Server-Zertifikat ebenfalls vermerkt.

Öffnet man eine Webseite per https, präsentiert der Server das Zertifikat. Der Browser überprüft, ob die Adresse im Zertifikat mit der aufgerufenen Adresse übereinstimmt. Ist dies der Fall, wird das Zertifikat überprüft, das zur Signatur genutzt wurde. Dies wird wiederholt, bis der Browser am Anfang angekommen ist oder auf ein ihm bekanntes Zertifikat einer Zertifizierungsstelle gestoßen ist. Der Verweis auf die jeweilige Zertifizierungsstelle nennt sich Zertifikatskette.

Da aber Daten im Gegensatz zu einem physischen Ausweis spurlos kopierbar sind, genügt allein die Adresse im Zertifikat nicht. Jeder könnte das Zertifikat des Servers kopieren und seinen Platz einnehmen. Deshalb gehört zu jedem (öffentlichen) Zertifikat ein privater Schlüssel, der nur seinem rechtmäßigen Besitzer bekannt sein darf. Auch die Zertifizierungsstelle (CA) kennt diesen nicht. Anhand dieses privaten Schlüssels kann der Server beweisen, dass das von Ihm präsentierte Zertifikat auch tatsächlich ihm gehört. Ein Angreifer kann sich somit nicht als der korrekte Server ausgeben und der Browser kann sicher sein, dass er tatsächlich mit dem richtigen Server kommuniziert.

Jeder Browser und jedes Betriebssystem beinhaltet allgemein bekannte und vertrauenswürdige CA-Zertifikate.

Zertifikatskette der ENA²

Da die ENA² in der Regel keine feste Domain besitzt, für die ein Zertifikat von einer offiziellen Zertifizierungsstelle ausgestellt wird, verwendet die ENA² eigene Zertifikate. Dazu wird eine eigene Zertifizierungsstelle auf dem Gerät erzeugt, die Zertifikate für Benutzer und Server ausstellt.

Die Serverdienste (VPN, Web) verwenden die Zertifikate, um sich dem Benutzer gegenüber als die erwarteten Dienste auszuweisen. Ebenso verwenden die Benutzer ihr Zertifikat, um sich dem Server gegenüber auszuweisen.

Vertraut der Benutzer der ENA²-Zertifizierungsstelle, kann diese einzelne Zertifikate erneuern, und der Benutzer vertraut diesen Zertifikaten automatisch. Dies ist wichtig, falls z.B. Zertifikat des Web-Servers geändert wird. Anderenfalls müsste das neue Web-Server-Zertifikat auf allen Geräten neu importiert werden.

Wird jedoch das Wurzelzertifikat, also das der ENA²-Zertifizierungsstelle geändert, werden alle anderen Zertifikate ungültig. Somit müssen alle VPN-Profile neu erzeugt und importiert werden, da diese die jeweiligen Benutzerzertifikate und das erwartete Wurzelzertifikat beinhalten.

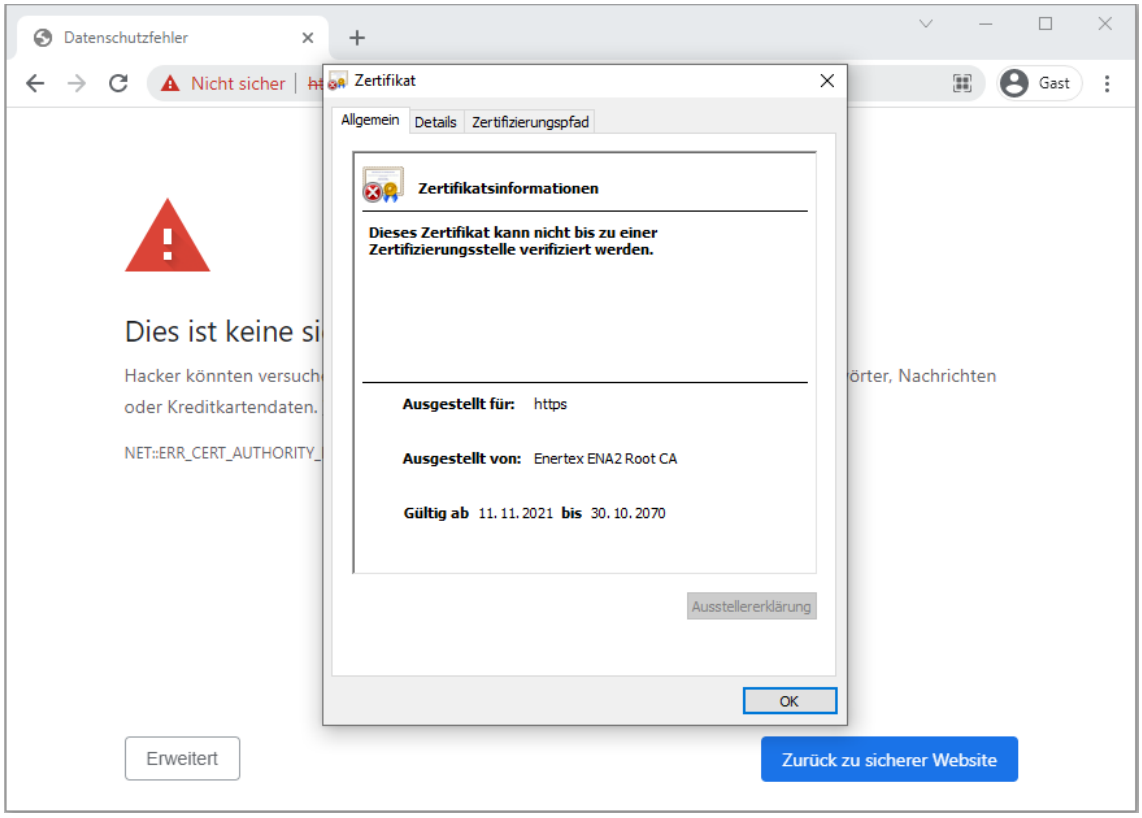
Dies ist in der Regel nicht nötig und geschieht automatisch beim Zurücksetzen auf Werkseinstellungen.

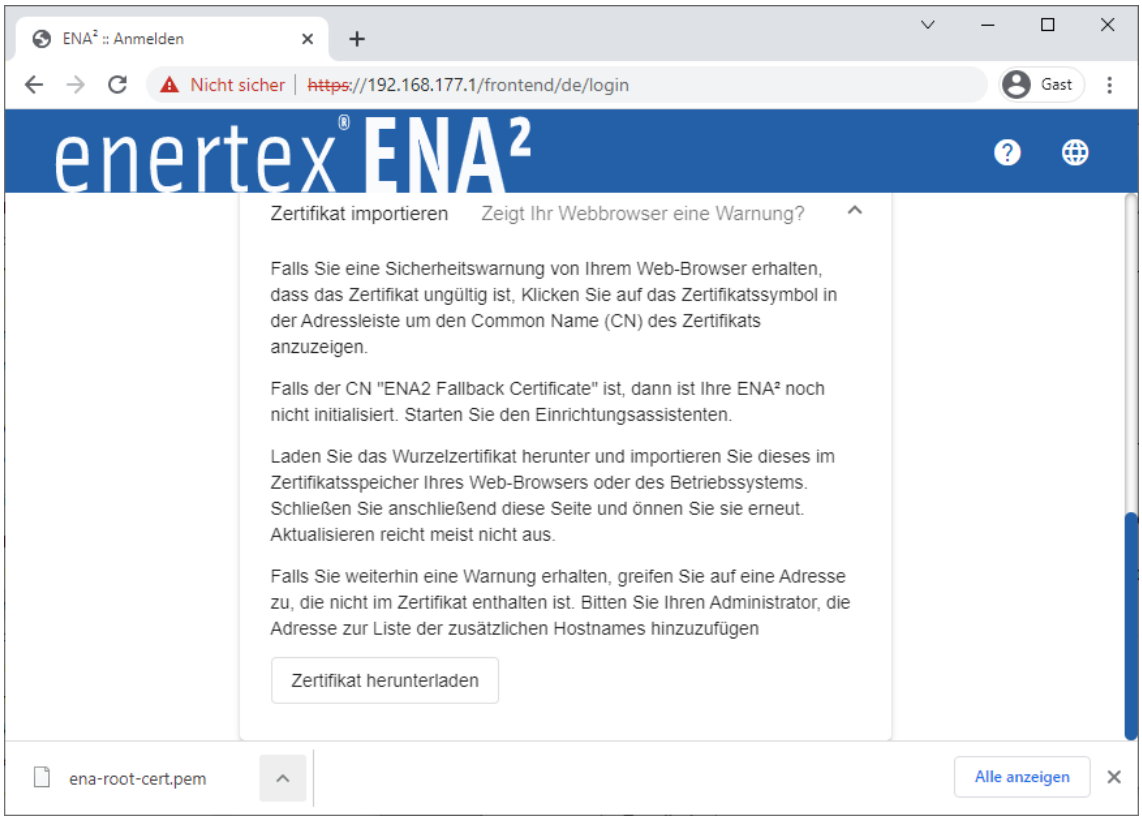
Import des Wurzelzertifikats

Sie sollten das erzeugte Wurzelzertifikat der ENA² in jedem Gerät importieren. Dadurch erkennt der Browser die Konfigurationsseite als vertrauenswürdig an, und die Kommunikation ist sicher. Es ist nicht nötig, das Wurzelzertifikat neu zu importieren, falls sich Server- oder Benutzerzertifikate geändert haben. Dies ist nur nach dem Zurücksetzen auf Werkseinstellungen nötig, oder falls die PKI in der Konfiguration neu initialisiert wurde.

Der Vorgang unterscheidet sich, je nach verwendetem Browser und Betriebssystem.

Laden Sie zunächst das Wurzelzertifikat auf das entsprechende Gerät. Dies finden Sie direkt auf der Login-Seite der ENA². Die ENA² muss dazu eingerichtet sein, d.h. der Einrichtungsassistent muss abgeschlossen worden sein.



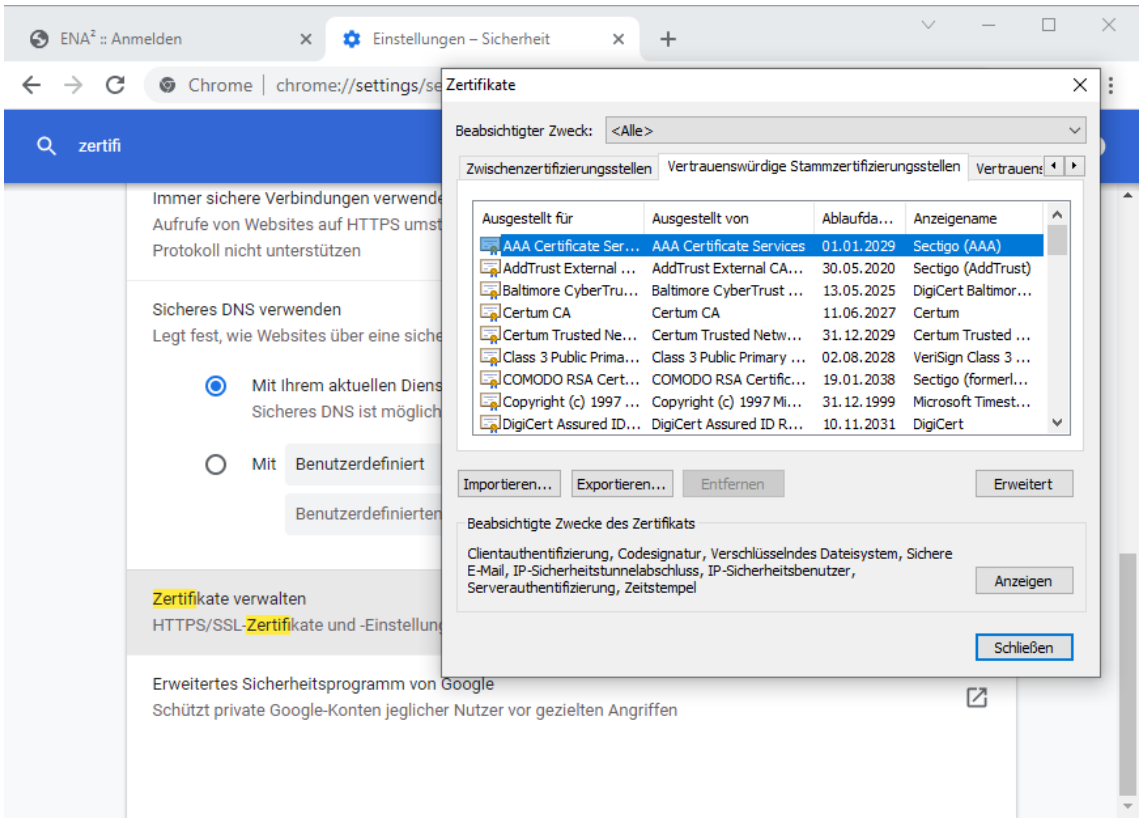


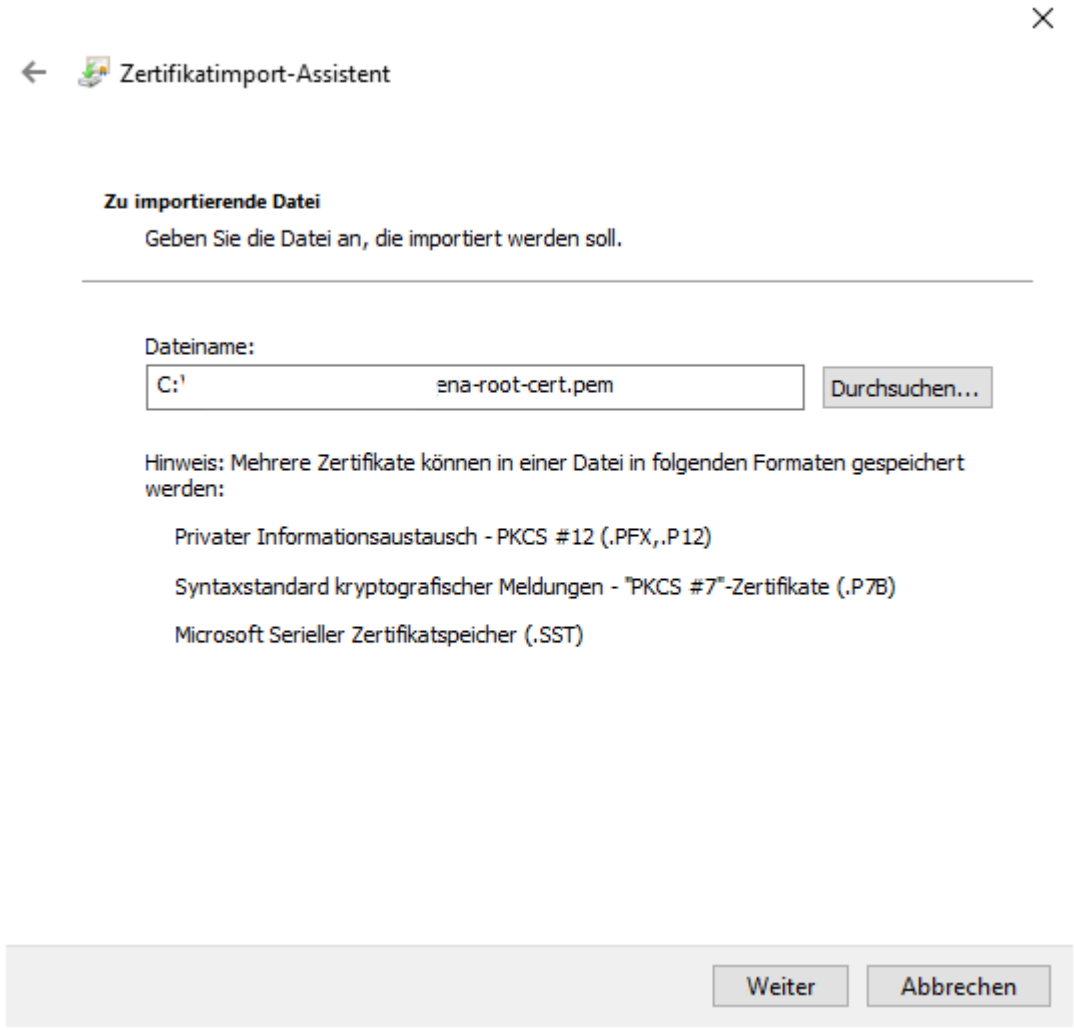
Windows 10

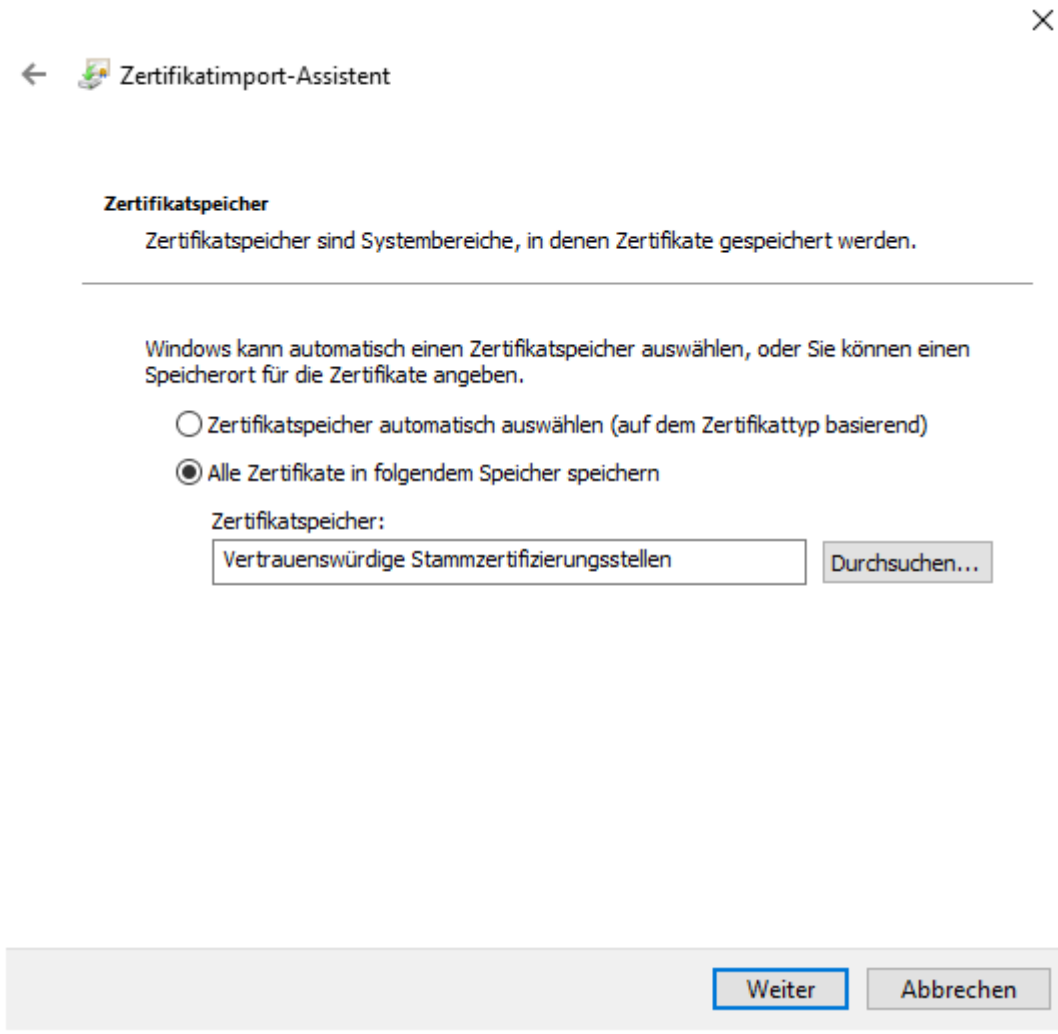
Google Chrome 95.0

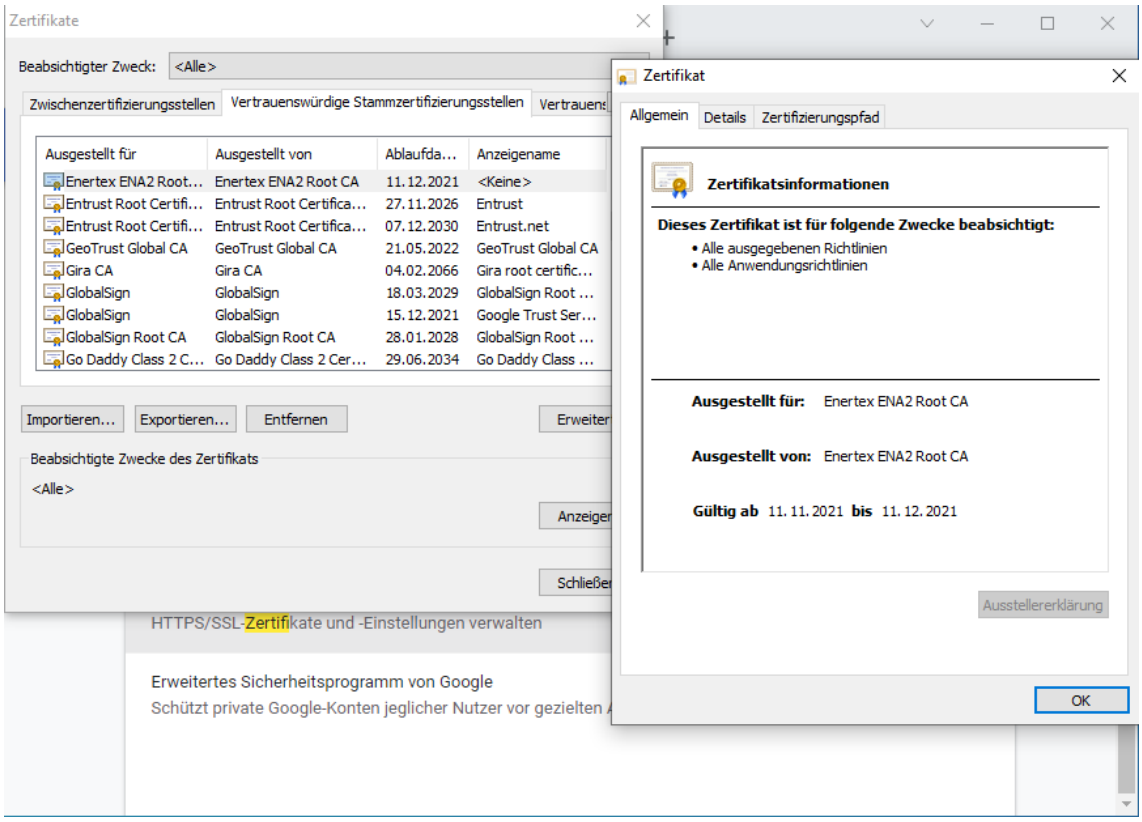
Öffnen Sie die Browser-Einstellungen und suchen Sie nach Zertifikat. Die Liste der Zertifikate befindet sich in den Einstellungen in der Kategorie „Datenschutz und Sicherheit“ → „Sicherheit“ → Erweitert → Zertifikate verwalten.

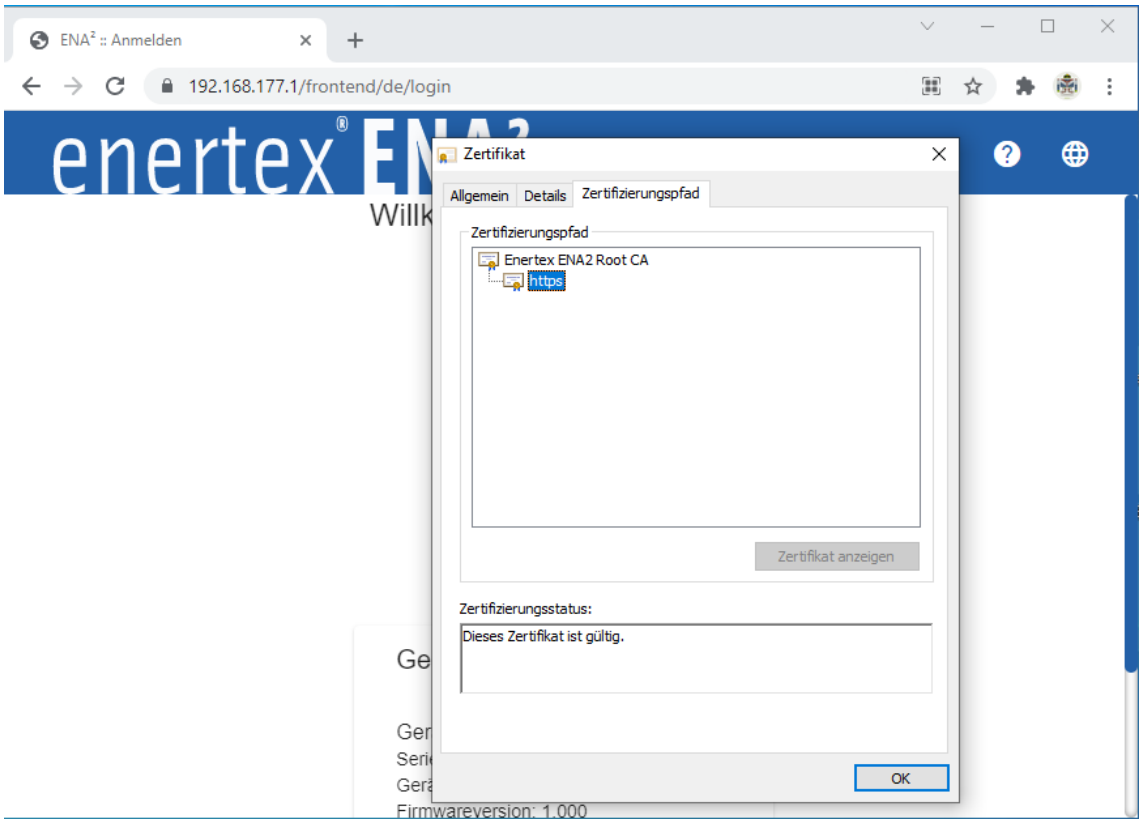
Öffnen Sie den Reiter „Vertrauenswürdige Stammzertifizierungsstellen“ und importieren Sie das Wurzelzertifikat.
Schließen Sie das Browserfenster und öffnen Sie die Webseite der ENA² neu. Das Zertifikat sollte nun als vertrauenswürdig markiert sein.


ENA² :: Anmelden
Einstellungen – Sicherheit
Chrome | chrome://settings/se
zertifi
Immer sichere Verbindungen verwende
Aufrufe von Websites auf HTTPS umst
Protokoll nicht unterstützen
Sicheres DNS verwenden
Legt fest, wie Websites über eine siche
Mit Ihrem aktuellen Diens
Sicheres DNS ist möglich
Mit Benutzerdefiniert
Benutzerdefinierten
Zertifikate verwalten
HTTPS/SSL-Zertifikate und -Einstellun
Erweitertes Sicherheitsprogramm von Google
Schützt private Google-Konten jeglicher Nutzer vor gezielten Angriffen
Zertifikate
Beabsichtigter Zweck: <Alle>
Zwischenzertifizierungsstellen
Vertrauenswürdige Stammzertifizierungsstellen
Vertrauens
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigename
AAA Certificate Ser... AAA Certificate Services 01.01.2029 Sectigo (AAA)
AddTrust External ... AddTrust External CA... 30.05.2020 Sectigo (AddTrust)
Baltimore CyberTru... Baltimore CyberTrust ... 13.05.2025 DigiCert Baltimor...
Certum CA Certum CA 11.06.2027 Certum
Certum Trusted Ne... Certum Trusted Netw... 31.12.2029 Certum Trusted ...
Class 3 Public Prima... Class 3 Public Primary ... 02.08.2028 VeriSign Class 3 ...
COMODO RSA Cert... COMODO RSA Certific... 19.01.2038 Sectigo (formerl...
Copyright (c) 1997 ... Copyright (c) 1997 Mi... 31.12.1999 Microsoft Timest...
DigiCert Assured ID... DigiCert Assured ID R... 10.11.2031 DigiCert
Importieren...
Exportieren...
Entfernen
Erweitert
Beabsichtigte Zwecke des Zertifikats
Clientauthentifizierung, Codesignatur, Verschlüsselndes Dateisystem, Sichere E-Mail, IP-Sicherheitstunnelabschluss, IP-Sicherheitsbenutzer, Serverauthentifizierung, Zeitstempel
Anzeigen
Schließen


Zertifikatimport-Assistent
Zu importierende Datei
Geben Sie die Datei an, die importiert werden soll.
Dateiname:
C:' ena-root-cert.pem
Durchsuchen...
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Microsoft Serieller Zertifikatspeicher (.SST)
Weiter
Abbrechen

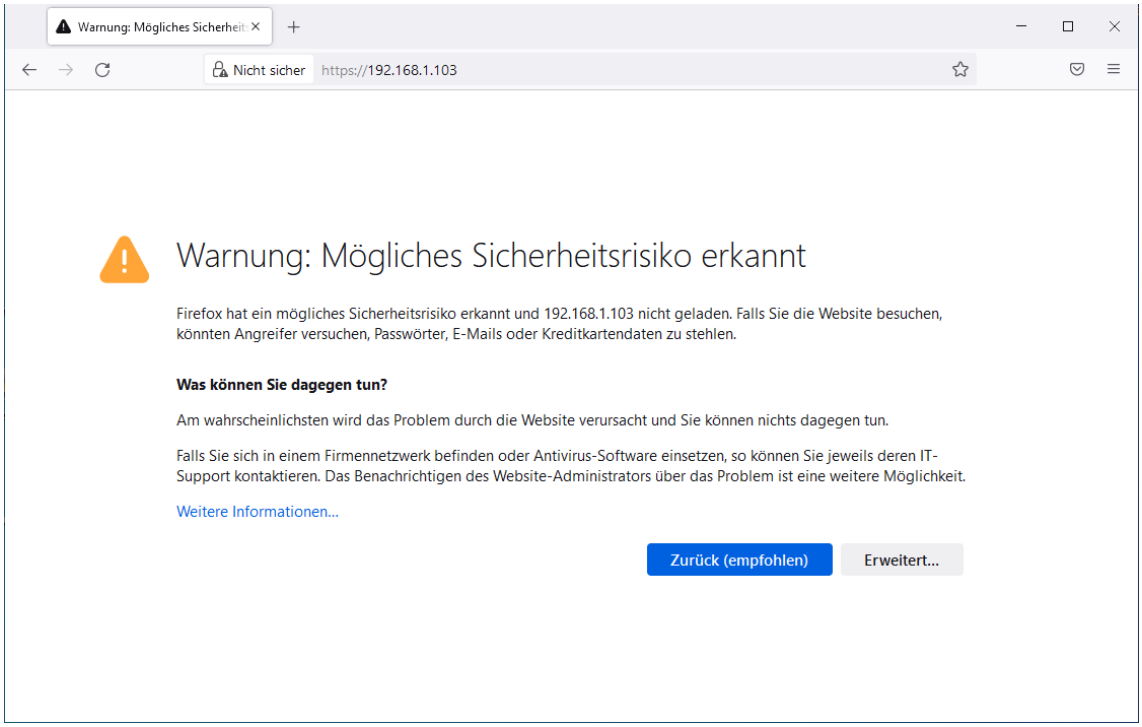

Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Vertrauenswürdige Stammzertifizierungsstellen
Durchsuchen...
Weiter
Abbrechen

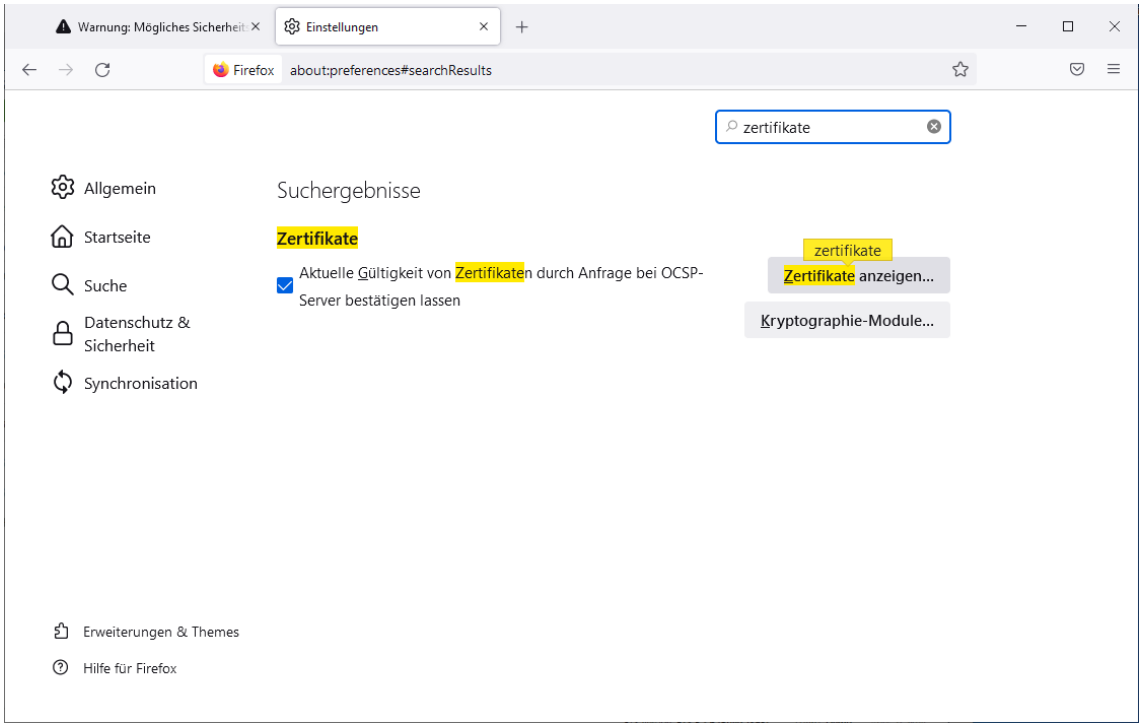

Zertifikate
Beabsichtigter Zweck: <Alle>
Zwischenzertifizierungsstellen
Vertrauenswürdige Stammzertifizierungsstellen
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigename
Enertex ENA2 Root... Enertex ENA2 Root CA 11.12.2021 <Keine>
Entrust Root Certifi... Entrust Root Certifica... 27.11.2026 Entrust
Entrust Root Certifi... Entrust Root Certifica... 07.12.2030 Entrust.net
GeoTrust Global CA GeoTrust Global CA 21.05.2022 GeoTrust Global CA
Gira CA Gira CA 04.02.2066 Gira root certific...
GlobalSign GlobalSign 18.03.2029 GlobalSign Root ...
GlobalSign GlobalSign 15.12.2021 Google Trust Ser...
GlobalSign Root CA GlobalSign Root CA 28.01.2028 GlobalSign Root ...
Go Daddy Class 2 C... Go Daddy Class 2 Cer... 29.06.2034 Go Daddy Class ...
Importieren...
Exportieren...
Entfernen
Beabsichtigte Zwecke des Zertifikats
<Alle>
Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifikatsinformationen
Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
• Alle ausgegebenen Richtlinien
• Alle Anwendungsrichtlinien
Ausgestellt für: Enertex ENA2 Root CA
Ausgestellt von: Enertex ENA2 Root CA
Gültig ab 11.11.2021 bis 11.12.2021
Ausstellererklärung
OK
HTTPS/SSL-Zertifikate und -Einstellungen verwalten
Erweitertes Sicherheitsprogramm von Google
Schützt private Google-Konten jeglicher Nutzer vor gezielten

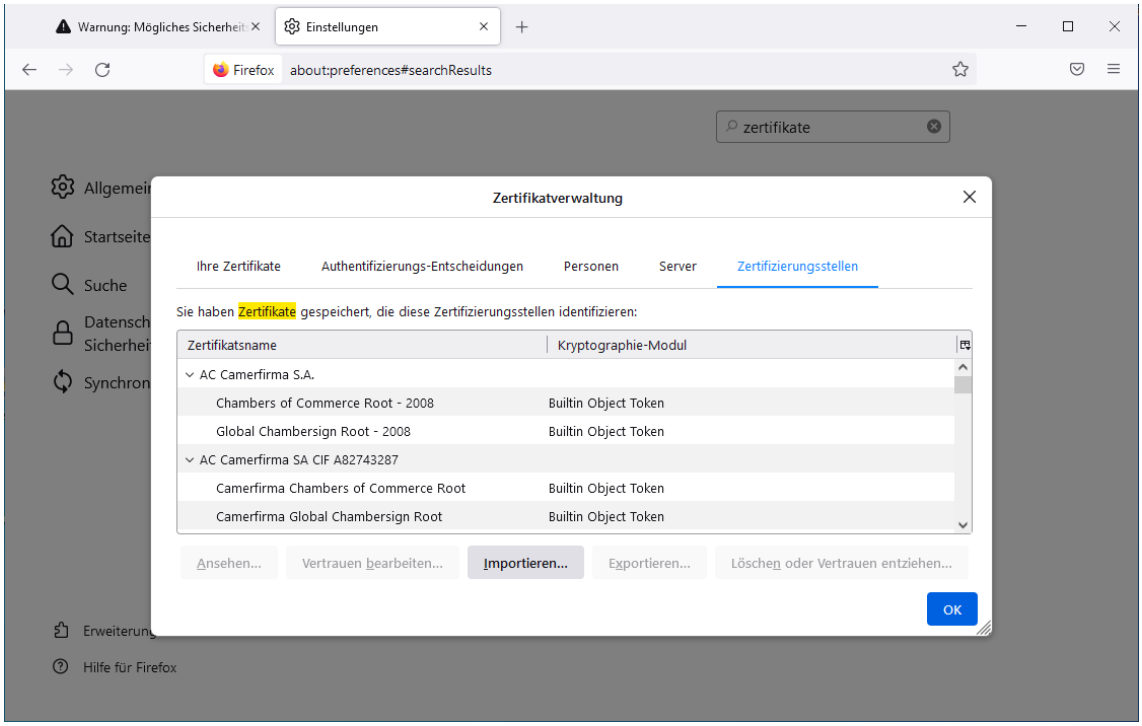


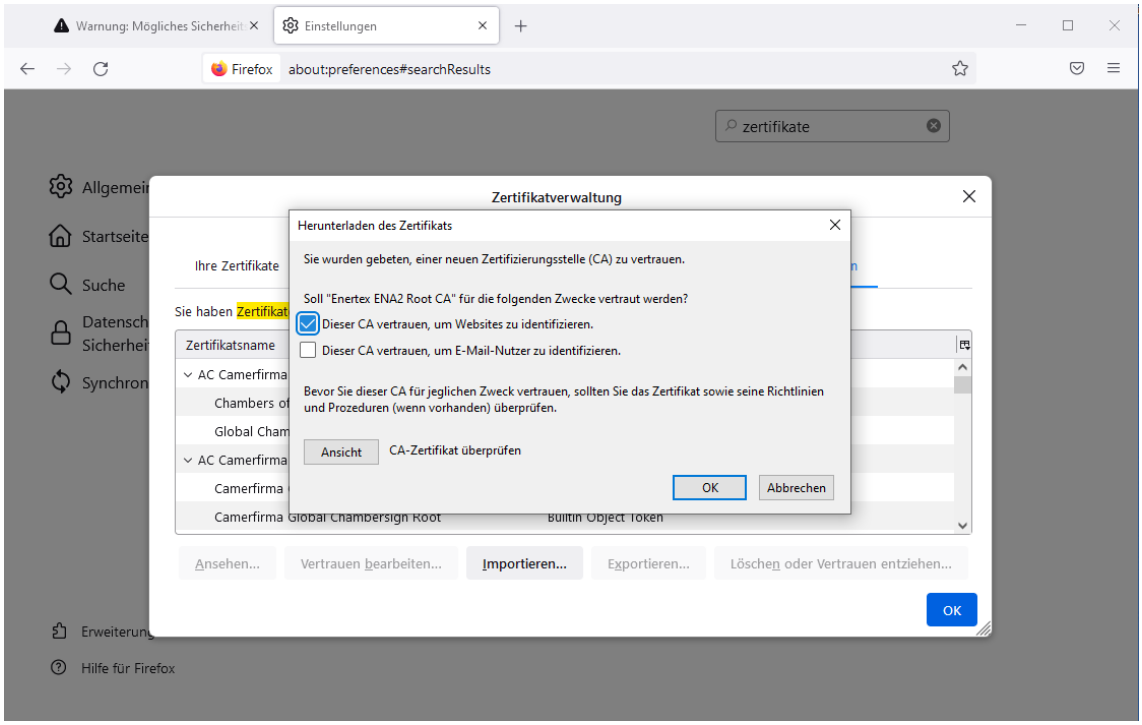
Firefox 94.0.1

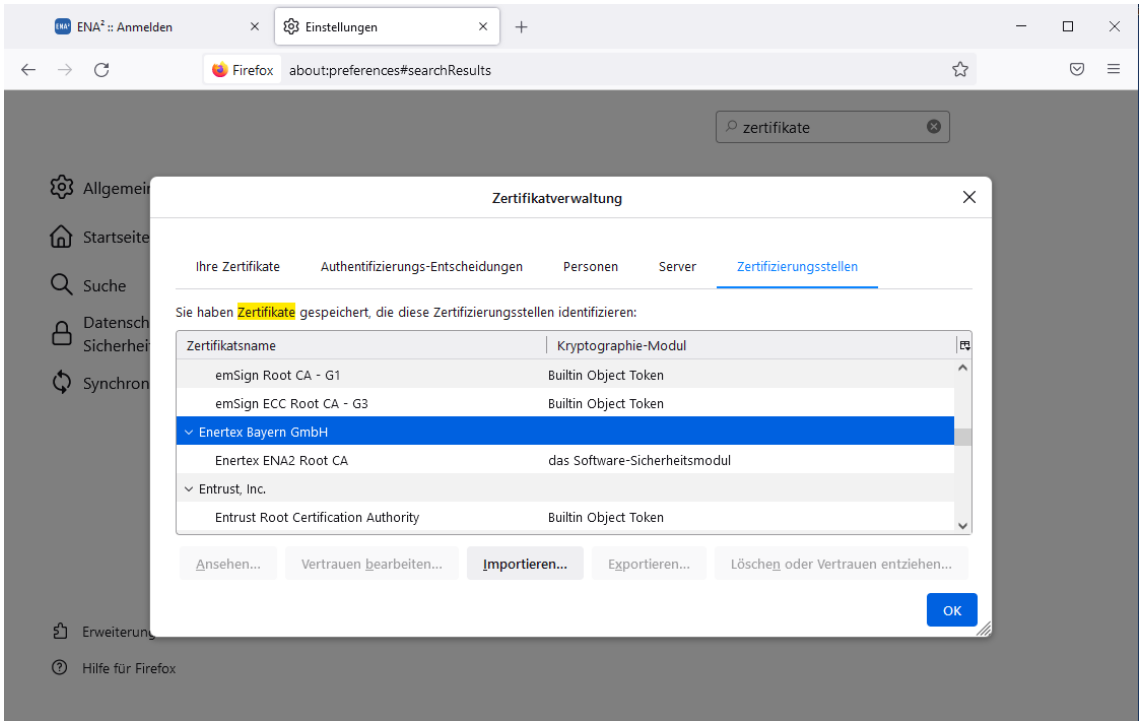
Das Vorgehen in Firefox erfolgt analog zu Google Chrome. Das Wurzelzertifikat wird der Liste der Zertifizierungsstellen hinzugefügt, um Webseiten zu identifizieren. Nach dem Hinzufügen muss die Zertifikatsliste ggf. geschlossen und neu geöffnet werden, dass das ENA²-Wurzelzertifikat angezeigt wird. Ebenso muss das Browserfenster der ENA² geschlossen und neu geöffnet werden.

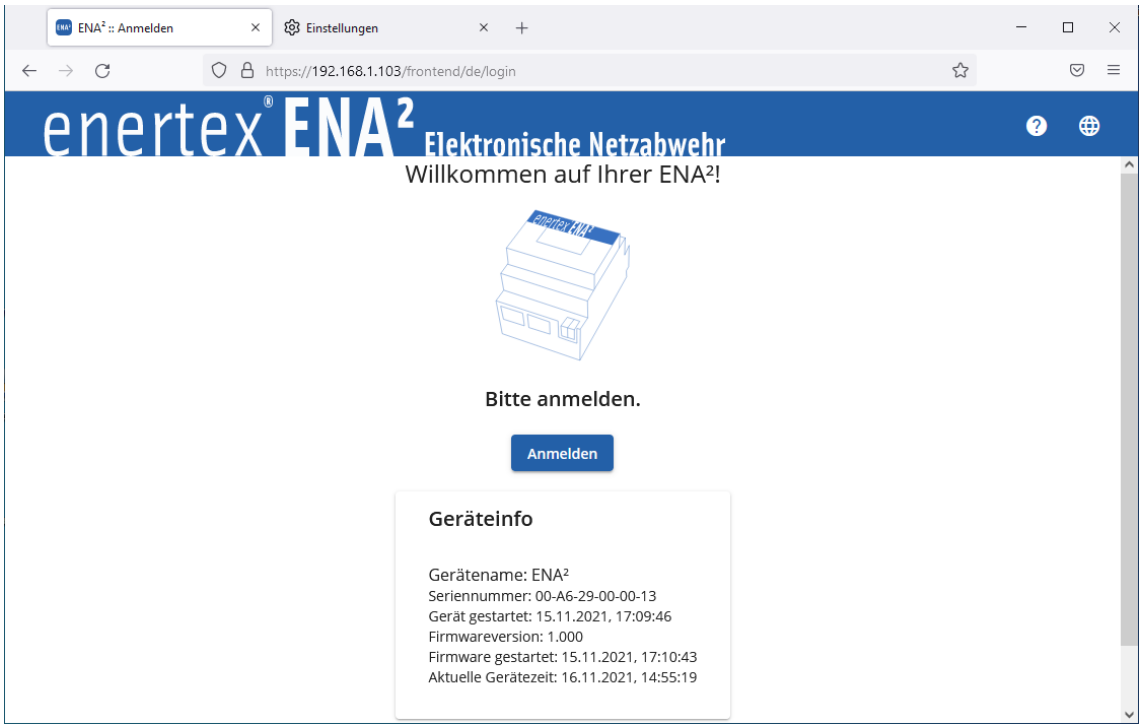



Warnung: Mögliches Sicherheit
Einstellungen
Firefox
about:preferences#searchResults
zertifikate
Allgemein
Startseite
Suche
Datenschutz & Sicherheit
Synchronisation
Suchergebnisse
Zertifikate
Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen
zertifikate
Zertifikate anzeigen...
Kryptographie-Module...
Erweiterungen & Themes
Hilfe für Firefox


Warnung: Mögliches Sicherheit
Einstellungen
Firefox
about:preferences#searchResults
zertifikate
Zertifikatverwaltung
Ihre Zertifikate
Authentifizierungs-Entscheidungen
Personen
Server
Zertifizierungsstellen
Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:
Zertifikatsname
Kryptographie-Modul
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce Root
Builtin Object Token
Camerfirma Global Chambersign Root
Builtin Object Token
Ansehen...
Vertrauen bearbeiten...
Importieren...
Exportieren...
Löschen oder Vertrauen entziehen...
OK
Hilfe für Firefox


Warnung: Mögliches Sicherheit
Einstellungen
Firefox about:preferences#searchResults
zertifikate
Allgemei
Startseite
Suche
Datensch
Sicherhei
Synchron
Zertifikatverwaltung
Ihre Zertifikate
Sie haben Zertifikat
Zertifikatsname
AC Camerfirma
Chambers of
Global Cham
AC Camerfirma
Camerfirma
Camerfirma Global Chambersign Root
Builtin Object Token
Ansehen...
Vertrauen bearbeiten...
Importieren...
Exportieren...
Löschen oder Vertrauen entziehen...
OK
Herunterladen des Zertifikats
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.
Soll "Enertex ENA2 Root CA" für die folgenden Zwecke vertraut werden?
Dieser CA vertrauen, um Websites zu identifizieren.
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.
Ansicht
CA-Zertifikat überprüfen
OK
Abbrechen
Erweiterun
Hilfe für Firefox


ENA² :: Anmelden
Einstellungen
Firefox about:preferences#searchResults
zertifikate
Allgemei
Startseite
Suche
Datensch
Sicherhei
Synchron
Zertifikatverwaltung
Ihre Zertifikate
Authentifizierungs-Entscheidungen
Personen
Server
Zertifizierungsstellen
Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:
Zertifikatsname
Kryptographie-Modul
emSign Root CA - G1
Builtin Object Token
emSign ECC Root CA - G3
Builtin Object Token
Enertex Bayern GmbH
Enertex ENA2 Root CA
das Software-Sicherheitsmodul
Entrust, Inc.
Entrust Root Certification Authority
Builtin Object Token
Ansehen...
Vertrauen bearbeiten...
Importieren...
Exportieren...
Löschen oder Vertrauen entziehen...
OK
Erweiterun
Hilfe für Firefox

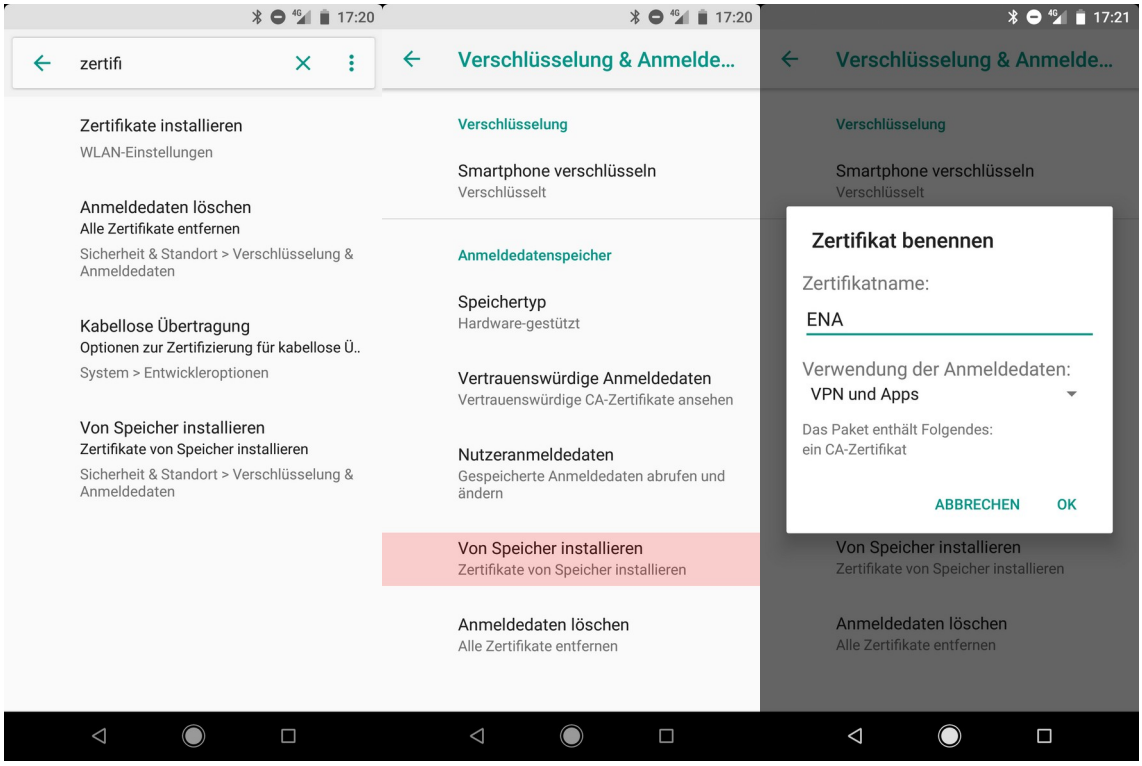


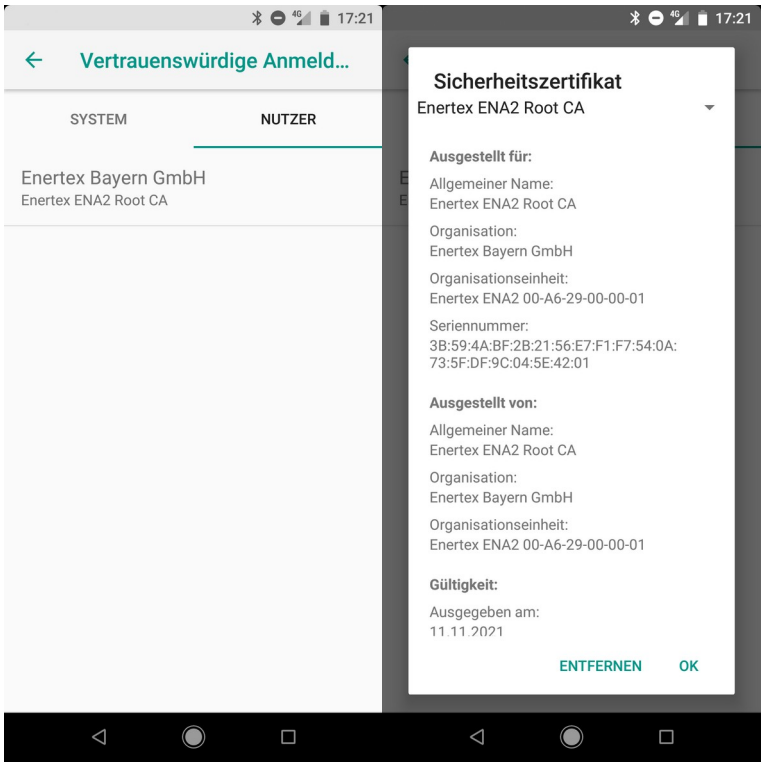
Android 8

Google Chrome 95.0

Je nach Hersteller und Android-Version unterscheidet sich die Menüstruktur. Das Vorgehen ist jedoch prinzipiell identisch.

Öffnen Sie die Einstellungen. Unter dem Menüpunkt „Sicherheit & Standort“ → “Verschlüsselung & Anmeldedaten“ finden Sie die Liste der vertrauenswürdigen Wurzelzertifikate (CA-Zertifikate) sowie die Option, um ein neues Zertifikat hinzuzufügen. Installieren Sie das heruntergeladene Zertifikat. Das Zertifikat ist nun in der Liste der Vertrauenswürdigen Zertifikate gespeichert.





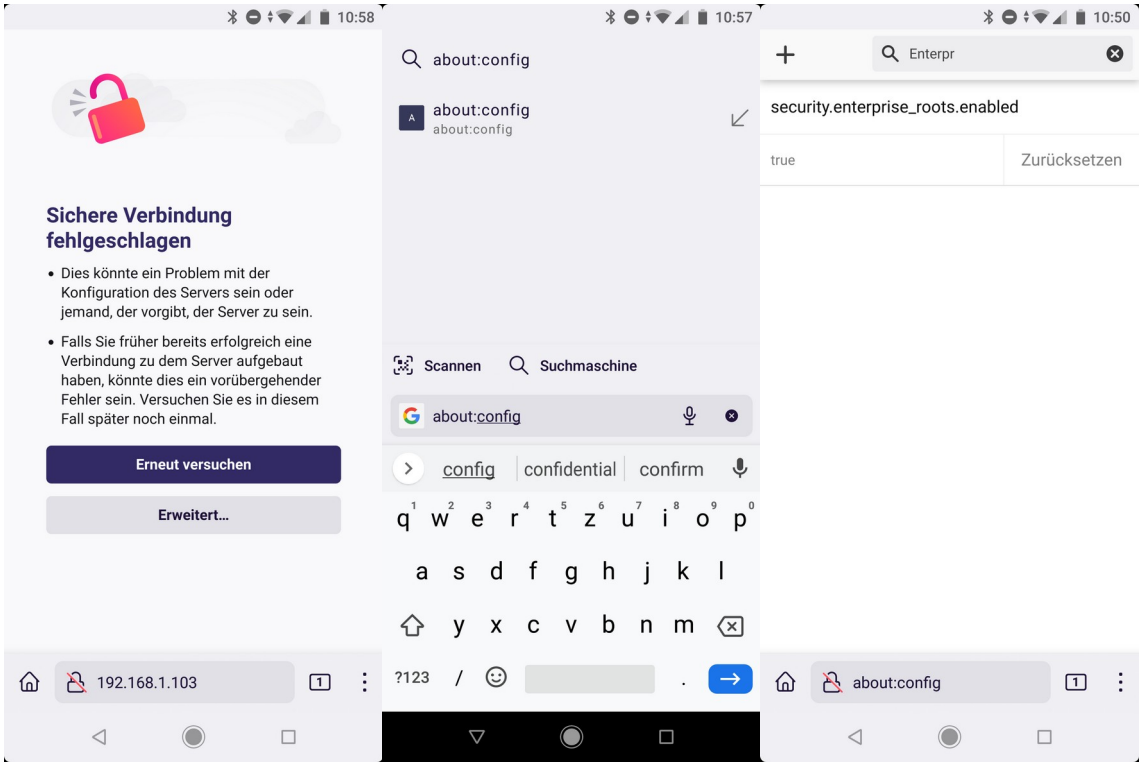
Firefox Beta 95.0

Firefox verwendet nicht den Betriebssystem-Zertifikatsspeicher. Dies muss erst aktiviert werden und funktioniert nur in der Firefox Beta-App. In der Firefox App (nicht Beta oder Nightly) ist der Zugriff auf die erweiterte Konfiguration deaktiviert.

Importieren Sie zunächst das Wurzelzertifikat wie unter Google Chrome 95.0 gezeigt.

Installieren und öffnen Sie Firefox Beta und navigieren Sie zur Seite „about:config“, um die Konfiguration zu öffnen. Suchen Sie nach „enterprise_roots“ und ändern Sie den Eintrag auf „true“.

Schließen Sie die ENA²-Webseite und öffnen Sie sie neu. Das Zertifikat wird nun akzeptiert.



Problembehandlung

Wird das Zertifikat auch nach dem Import als nicht gültig angezeigt, prüfen Sie zunächst, dass das ausgelieferte Zertifikat nicht das Fallback-Zertifikat ist.

Öffnen Sie dazu das Zertifikat und prüfen Sie, dass im Feld „Ausgestellt für“ „https“ eingetragen ist. Ist dies nicht der Fall, ist die Zertifikatskette nicht korrekt initialisiert oder das Gerät hat nach der Initialisierung nicht neu gestartet.

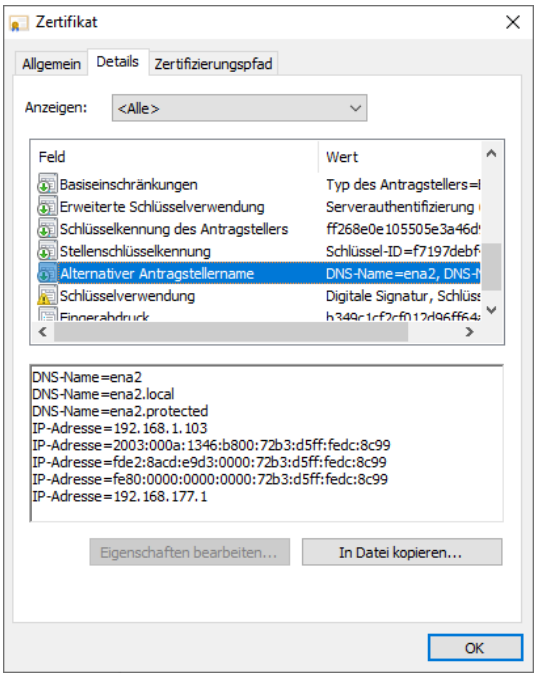
Wird ein korrektes Zertifikat ausgeliefert, prüfen Sie die Liste der gültigen Adressen, die im Zertifikat gespeichert ist. Diese muss die Adresse beinhalten, über die die Webseite der ENA² aufgerufen wird. Die Liste wird automatisch erstellt:

Netzwerkmodus „Switch“:

- Bei statischer Adressvergabe wird diese Adresse eingetragen.
- Bei DHCP wird die aktuelle IP-Adresse eingetragen. Ändert sich diese, muss das Zertifikat manuell neu erzeugt werden. Statt dessen können Sie auch die Konfigurationsseite über den DNS-Namen aufrufen, falls der DHCP-Server dies unterstützt.

Netzwerkmodus „Firewall“:

- Bei statischer Adressvergabe wird diese Adresse eingetragen.
- Ist der DHCP-Server der ENA² für „Sichere Gebäudenetzwerk“ aktiv, verwenden Sie den DNS-Namen `ena2.protected` im „Sichere Gebäudenetzwerk“.



SSL-Fehler

Falls Firefox nach dem Einrichtungsassistent den Zugriff auf die Gerätewebseite mit der Fehlermeldung `SEC_ERROR_REUSED_ISSUER_AND_SERIAL` verbietet, öffnen Sie die Seite `about:support` und klicken Sie neben Profilverzeichnis auf `Ordner öffnen`. Schließen Sie alle Browserfenster und löschen Sie die Dateien *cert9.db* und *key4.db* im Profilverzeichnis.

Gerätezertifikat

Jedes Gerät erhält bei der Produktion ein anonymes Gerätezertifikat, das an den DDNS-Dienst und den Relais-Server zur Anmeldung gesendet wird, um Zugang zu den Diensten zu erhalten. Das Zertifikat muss nicht geändert oder erneuert werden.

Werkseinstellungen

Sollte die ENA² nicht mehr erreichbar sein, oder das Besitzer- und Administratorpasswort unbekannt sein, können Sie das Gerät auf Werkseinstellungen zurücksetzen. Dabei wird die gesamte Konfiguration gelöscht, der Netzwerkmodus wieder auf „Switch“ gesetzt und der DHCP-Client aktiviert. Alle gespeicherten Telegramme und Logdateien werden gelöscht.

Zum Zurücksetzten muss das Gerät bereit sein, d.h. die Power-LED (5) blinkt und die Anzeige ist aktiv. Halten Sie die Display-Taste (10) für 5 Sekunden.

Es wird „Hold for reset“ angezeigt. Das Zurücksetzten kann durch Loslassen der Taste (10) noch abgebrochen werden.

Halten Sie die Taste weitere 5 Sekunden, bis „Factory reset“ angezeigt wird.

Das Gerät wird nun zurückgesetzt und startet anschließend automatisch neu.

Technische Daten

KNX (Versorgung)	DC 27 ... 30 V SELV Stromaufnahme < 110 mA bei 29 V Busspannung.
Ethernet-Schnittstelle	2x RJ45-Buchse für 10M/100MBit Ethernet
Bedien- und Anzeige-elemente	Grafisches OLED LEDs: Spannungs-LED (grün) Info-LED (gelb), Alarm-LED (rot), RJ45-Buchsen: Netzwerklink (grün), Netzwerkaktivität (gelb) Taster: F1, F2, Display
Gehäuse	DIN Hutschienengehäuse für 35 mm Tragschiene Breite: 4 TE 71,5 mm x 89,6 mm x 62,9 mm (L x B x H)
Weiteres	Nur zur Verwendung in Innenräumen Nur für den Betrieb im Schaltschrank Höchste Umgebungstemperatur ta = 45 °C Niedrigste Umgebungstemperatur ta min = -5 °C Schutzklasse III Schutzart: IP20 Prüfungen: Sicherheit: IEC 63044-3 EMV: Geprüft nach IEC 63044-5-2 (Wohnbereich), IEC 63044-5-3 (Industriebereich) Umgebung: Geprüft nach DIN EN 50491-2