enertexbayern gmbh
simulation entwicklung consulting

Manual

ENA²

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

Notice

Table of Contents

Notes

- Installation and assembly of electrical equipment must be performed by qualified electricians.
- When connecting KNX interfaces skills are provided by KNX-Training.
- Ignoring the instructions may damage the device as well as causing fire or other hazards.
- This manual is part of the product and must remain with the end user.
- The manufacturer is not liable for any costs or damages incurred by the user or third parties through the use of this device, misuse or malfunction of the connection, malfunction of the device or the subscriber equipment.
- Opening the case or other authorized changes or modifications will void the warranty!
- The manufacturer is not liable for improper use.

Function

The ENA² combines four important functions in a single device:

- Remote maintenance with the integrated ETS IP tunnel.
- Remote access to network devices, e.g., to open a Web visualization on a smartphone.
- Record KNX telegrams to analyze them directly on the device or to export and store telegrams in an archive. The exported telegrams can be imported into the ETS group monitor.
- “Protected Network”: protect the network devices of your building automation of unwanted or fraudulent access and separate the building network from the private or company network.

With factory default settings active the device is configured to “Switch” mode and requests an IP address using DHCP.

Network interface mode

Switch mode

In Switch mode, both network interfaces LAN1 and LAN2 are connected to an internal switch. Data is forwarded between both interfaces. The ENA² has a single IP- and MAC address. In this configuration, you can connect one interface with the existing network and the other one with another IP device, e.g., a KNX IP interface. LAN1 and LAN2 are interchangeable in this configuration.

Warning: Communication between LAN1 and LAN2 is only possible if the ENA² is started and ready, otherwise the connection is interrupted, e.g., if the device is restarted.

All data is forwarded in this mode, and the ENA² cannot protect your devices. Use the Firewall mode to enable protection.

The integrated interface and VPN access is available in Switch and Firewall mode.

Firewall mode

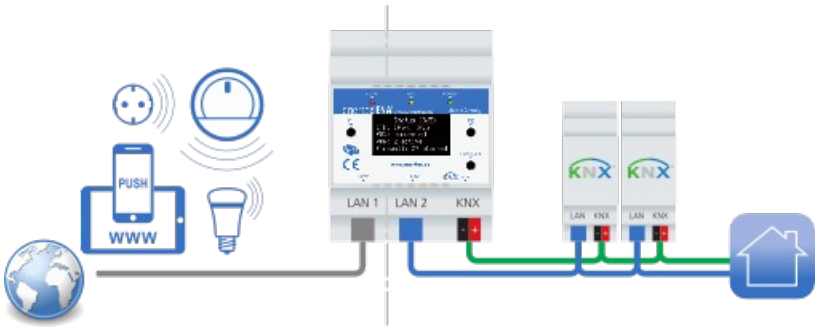


Figure 1: Firewall mode

Both Ethernet interfaces LAN1 and LAN2 are configured independently with different IP- and MAC addresses.

The IP address may not be part of the same network subnetwork!

For example, the interfaces may not be configured to receive an IP address from the same DHCP server. The IP addresses 192.168.1.1/netmask 255.255.0.0 and 192.168.2.1/netmask 255.255.0.0 also lie in the same subnetwork!

In this mode the Network is split into:

Home Network on LAN1

The existing home network with internet access, typically managed by an internet router. The

ENA² cannot restrict network access but is a regular network client.

“Protected Network” on LAN2

This network is managed by the ENA². Data between LAN1 and LAN2 can be filtered by the ENA². The ENA² can distribute IP addresses via DHCP and offers NTP and DNS services. Network access can be configured by intuitive filters rules.

E.g., you can allow internet access only for selected devices from the “Protected Network” or restrict access to the integrated KNX interface.

Features

The ENA² has the following functions:

- Overview:
- Secure remote access for your local network – Cloud-free End-to-end encrypted connection between mobile device and ENA²
- Forward remote access via Enertex relay server to connect to your local network, works with any internet provider (IPv4, IPv6, DS-Lite), no local router configuration required (optional)
- Guided browser-based configuration on device
- Easy-to-use user management
- Integrated free DynDNS service
- Integrated OpenVPN server
  - Restrict users access
  - Controllable via KNX group telegrams
  - Free client software for common operating systems (Windows, Linux, MacOS, Android, iOS)
  - VPN "on demand": automatically connect to your network (iOS-only)
- „Protected Network“
  - Separate physical Ethernet interfaces for your main and protected networks
  - Control forwarding and filtering
  - Firewall and DHCP server
- Recent security standards and well-known and trusted VPN software
- KNX Telegramlogger
  - Records all KNX telegrams in internal database (~ 100.000.000 tel., depends on data type)
  - Import ETS project for data type, topology and device information
  - Easy to query and analyze telegrams on ENA² web server
  - Show time-value charts, e.g. per hour, per day
  - Identify configuration errors, e.g., read requests without response

Interfaces and Controls

2 shows the device and its connection to network and KNX.

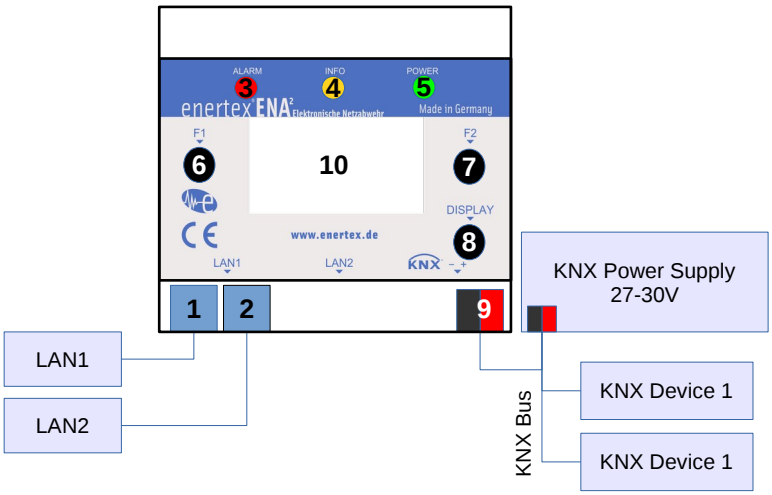


Figure 2: Connection of ENA²

Ethernet interfaces	LAN1 (1), LAN2 (2)
LEDs	Alarm red (3) Info orange (4) Power green (5)
Push buttons	F1 (6), F2 (7), Display (8)
Power supply and bus interface	KNX (9)
Status display	Display (10)

LEDs

1. Immediately after connecting the device with a power supply, the LEDs (3,4,5) are on with reduced brightness.
2. LED Power (5) is on during boot.
3. The device takes approx. 2 minutes to start. LED Power (5) flashes and Display is on.
4. LED Info (4) is on if a VPN connection is open.
5. The LED Alarm (3) and push buttons F1 (6) and F2 (7) are currently not used.

Display

The Display (10) stays on during boot. When ready, it show version information and the IP address. Press push button (8) to activate it for 5 minutes. Press push button (8) again to jump to the next page.

Commissioning

Prerequisites

- KNX power supply, 27-30V DC, with 3.2 Watt power available (110 mA at 29 V Bus voltage). The typical power consumption is 1.8 Watt.

We recommend our KNX power supplies Enertex® KNX PowerSupply 960³ and KNX Dual PowerSupply 1280.

- A computer with a recent web browser (Google Chrome, Firefox, Safari) for configura-

tion.

- Network with DHCP server. The device is initially set to “Switch mode” (see Switch mode, p. 4).

Connect the device to the KNX bus and your local network on LAN1. The device is ready after after approx. 2 minutes, and shows time and serial number. Press the push button Display (8) until you see the page LAN1. Read the IP address (e.g., 192.168.1.23) and navigate to it in your web browser.

Notes: If the IP address is 169.254..* the device did not receive an IP address from your DHCP server and uses „IP Automatic Configuration“.*

In your web browser you will get a security warning. Confirm to open the configuration.

You are now on the device configuration website. Click on the “Help”- icon in the top right corner for the manual.

The first-start wizard leads you through the basic configuration steps. You can select the network mode, create user for configuration and remote access, and import your ETS project.

The device generates the certificates at the end. This takes approx. 15 minutes and must not be interrupted. If an ETS project is selected for import, initialization may take significantly longer, depending on the project.

You can leave the web configuration or close the browser during initialization.

Once the device is initialized, log in using the user accounts from the wizard.

Configuration website

The device is configured only within the configuration website. You need to have network access for commissioning and for later changes. The device website is available in every zone (VPN, LAN1, LAN2).

You need a recent web browser to correctly show the configuration website. The configuration can also be controlled comfortably on mobile devices.

The following explains the basic concepts.

First-start wizard

If the device is not configured yet, either initially or after a factory reset, you will not see the login button but you can open the first-start wizard. After initialization, the wizard is not available. All settings of the wizard can be changed by the administrator.

Use the created user accounts to log in on the website. The device website contains two areas: user area and configuration.

User area

Every user has access to the user area. Depending on the individual permissions, you can open different pages, e.g., download the VPN profile, open the telegramlog or show the protocol.

Configuration

Only administrators may open the configuration to change device settings.

Configuration

User

The first-start wizard required to create the first set of user accounts. Every user has exactly one of the following roles:

- Owner (exactly one):
  - The physical owner of the device/the KNX installation.
  - Can issue a factory reset in the user area.
  - Is otherwise a regular user with the respective functions in the user area.
- Administrator (at least one):
  - Full access to the configuration
  - Has access to the respective functions in his user area.
- User (any number):
  - Has access to the respective functions in his user area.

On initialization, owner and a first administrator must be created.

Every user has a set of permissions, mostly independent from his role. You can create a user with access to the telegramlog only, but without being able to connect via VPN. Permissions can be changed by administrators at any time.

Every user can change his personal information (username, name, e-mail address, password) after log-in. The e-mail address is used to send mails to the user. The notifications a user wants to receive can be configured. For example, administrator and owner can be notified if a firmware update is available.

Network

Open the network settings to change the Network interface mode (S. 4).

Zones

The ENA² knows different subnetworks as zones. The firewall configuration allows or denied data transfer between zones. It depends on the Network interface mode, which zones are available.

KNX

This zone manages the integrated KNX interface. A device must have the permission to access the KNX zone to open a KNX tunnel connection.

LAN1

The existing home- or company network with internet access. In Switch mode both Ethernet interfaces LAN1 and LAN2 are equal and zone LAN1 refers to both interfaces.

LAN2

The “Protected Network” managed by the ENA² in Firewall mode, available on interface LAN2.

VPN

All connected clients receive an address within this zone. The ENA² forwards access to different zones if configured.

WAN

All networks outside of the local zones, which are reachable via the router of LAN1. This typically

includes the internet or other subnetworks within the company network.

Network Addresses

The options available depend on the network mode. Basically the device can request the IP address from a DHCP server or you can statically assign an address. The prerequisite of static addresses are that the device starts as usual even if the DHCP server is currently not available. Otherwise the device switches to “IP Automatic Configuration” and chooses an IP from the range 169.254.*.*

This allows the device to be directly connected to a PC or notebook for configuration.

In most cases a router provides access to the internet. If you assign a static IP address, it has be be outside of the DHCP range configured in the router settings.

The ENA² uses the notation of network address and prefix length to describe subnetworks. This is the default notation for IPv6 networks. For IPv4 the common notation used to give the netmask instead of the prefix length. The most common netmask for private networks is 255.255.255.0, which is equal to a prefix length of 24.

Routing

Every subnetwork must be disjoint. If a device from a different network is addressed, the routing information defines which gateway must be used to forward the request.

A gateway is a network device which takes requests for IP addresses different from its own address and forwards them according to its routing table, changing the source address to its own IP. The response is sent back to the original source.

Example: The internet router within a private network has IP 192.168.178.1, prefix length is 24. Connected devices can use IP addresses from the range 192.168.178.2 – 192.168.178.254. Other addresses (e.g., internet) are forwarded using the default route with the internet router being the gateway (default gateway).

Home network:

Netmask / prefix length	255.255.255.0 / 24
IP address Router	192.168.178.1
Valid device addresses	192.168.178.2 – 192.168.178.254
IP address ENA² (LAN1)	192.168.178.66

Routes of devices in home network:

192.168.178.0/24	direct
Default route	via gateway 192.168.178.1

With DHCP enabled, the router sends this information together with the client IP address. If the address is assigned statically, the router must be manually added as default gateway.

If the network consists of different subnetwork, information on how to route into these subnetworks is required as well. They can either be defined for every device individually or they are added to the default gateway, making them available to every device.

In Network interface mode “Switch” you need no additional routing information, because the ENA² does not manage a separate subnetwork. For “Protected Network”, this information is required for devices from LAN2 to address LAN1 devices (S. 4).

“Protected Network”:

Netmask / prefix length	255.255.255.0 / 24
IP address ENA² (LAN2)	192.168.177.1
Valid device addresses	192.168.177.2 – 192.168.177.254

Routes of ENA²:

192.168.178.0/24	direct via LAN1
192.168.177.0/24	direct via LAN2
Default route	via gateway 192.168.178.1

Routes of devices in “Protected Network”

192.168.177.0/24	direct
Default route	via ENA² 192.168.177.1The

The routes of the devices in home network must contain the “Protected Network” that can be reached via ENA². Ex explained, this information can either be configured in the gateway (the internet router) to be available to every connected device. Home-network-devices then send their requests to “Protected Network”-devices to the router, which forwards them to the ENA², again forwarding them to the respective device.

Routes of gateway with route to “Protected Network”:

192.168.178.0/24	direct
192.168.177.0/24	via ENA² 192.168.178.66 (LAN1)
Default route	via internet

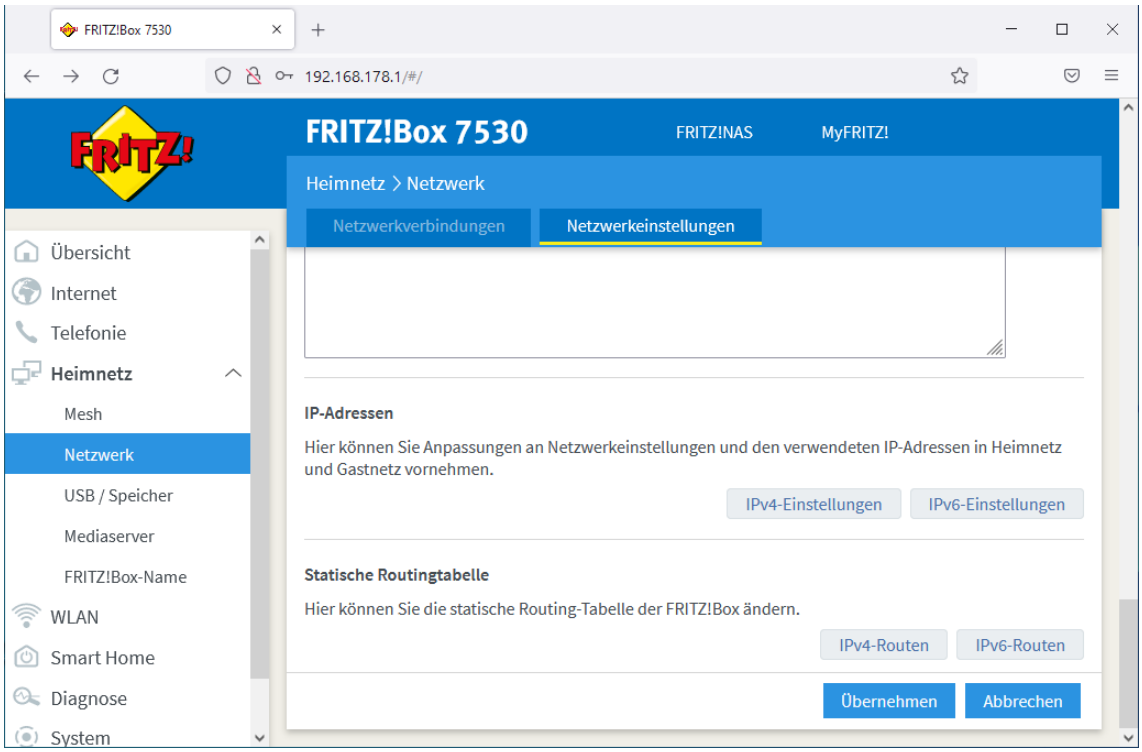
The other option is to add the route to every single device which should have access to “Protected Network”-devices. This eliminates the additional step to the router but every device sends its data for the “Protected Network” directly to the ENA².

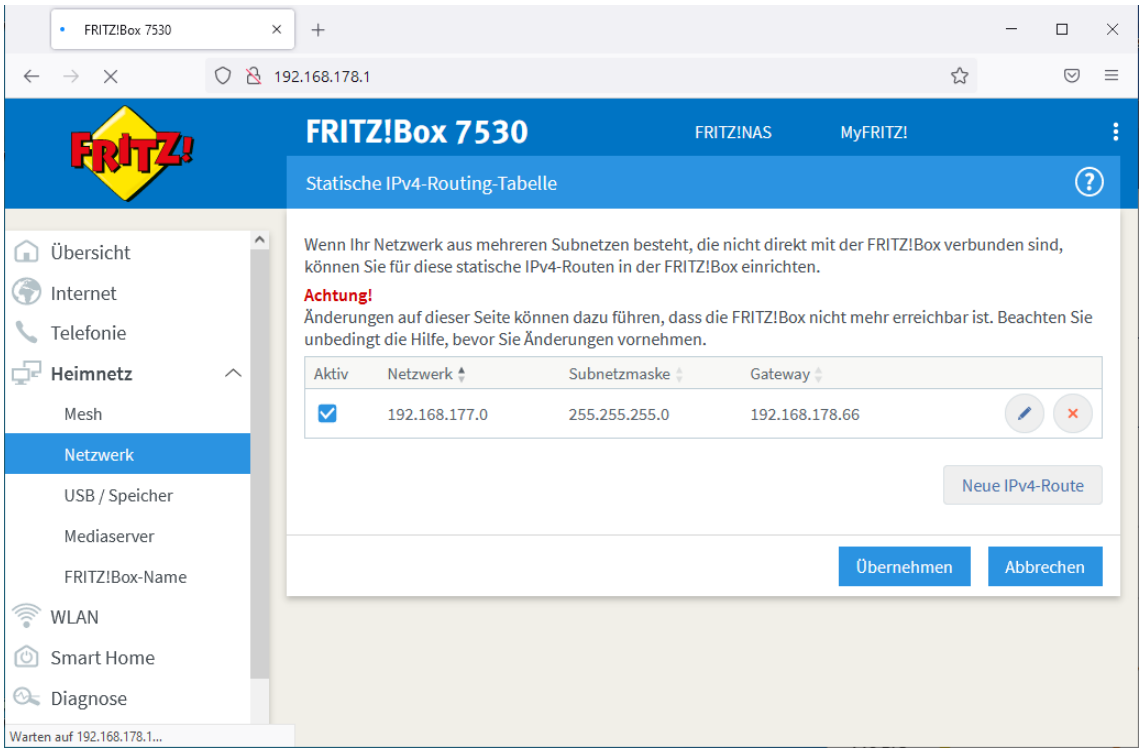
Alternative: Routes of the home network devices with route to “Protected Network”:

192.168.178.0/24	direct
192.168.177.0/24	via ENA² 192.168.178.66 (LAN1)
Default route	via gateway 192.168.178.1

Example: Fritz!Box, FRITZ!OS 07.28:

Open Home Network → Network → Network Settings → Additional Settings → IPv4 Routes. Enter the network address of the “Protected Network”. For example, if your ENA² has IP 192.168.177.1 with prefix length 24, the network address is 192.168.177.0 and netmask 255.255.255.0. The gateway is the IP address of your ENA² in your home network. If the address is assigned dynamically by the DHCP server of the Fritz!Box, it should be configured to always receive the same address.





VPN

The VPN server of the ENA² can be reached via UDP and TCP. Prefer to use UDP if possible, as it has advantages especially if the connection is slow or unreliable. The Relay server can only use TCP.

Port Forwarding

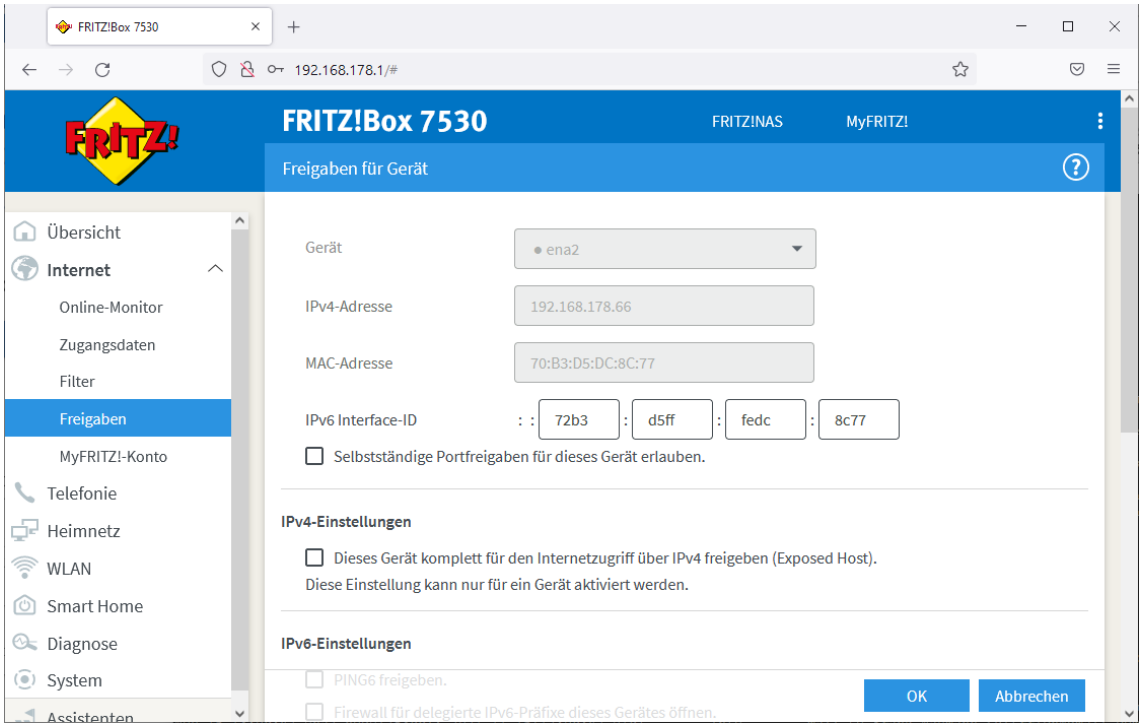
If your internet connection can be accessed from the internet, you can add the VPN server port (default 1194) to the list of forwarded ports in your internet router.

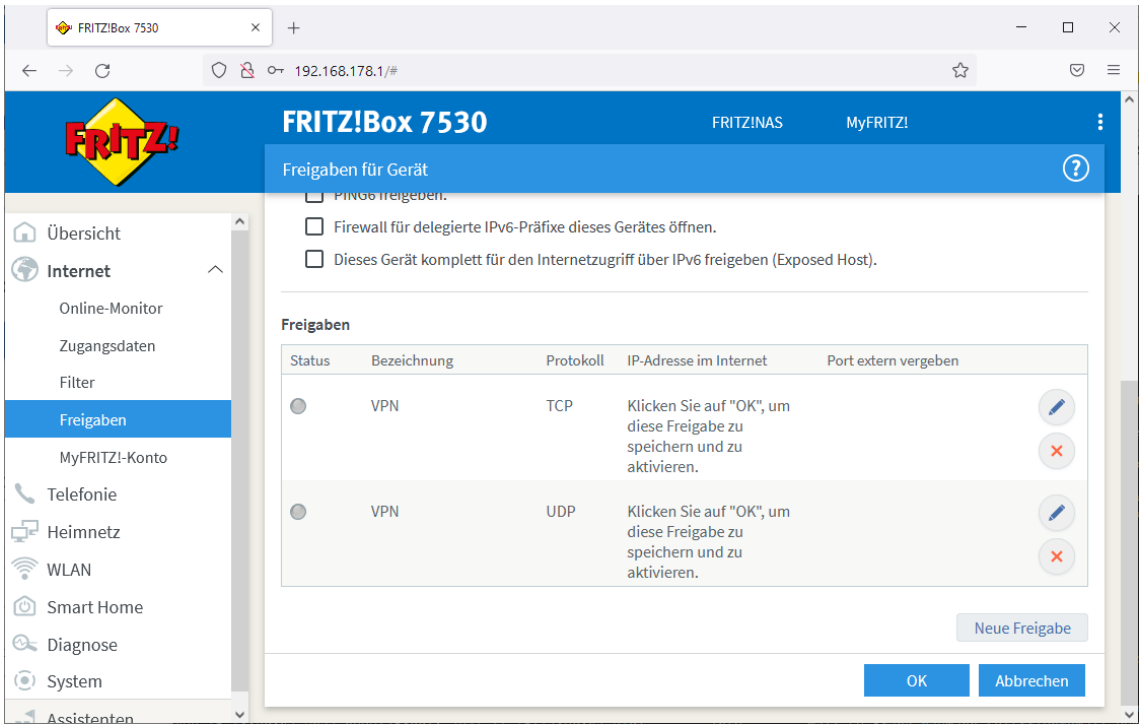
Disable the Relay server when you export a VPN profile to use the DDNS name and optionally configured additional hostnames as remote addresses in the profile. Use the configured VPN server port for internal and external port.

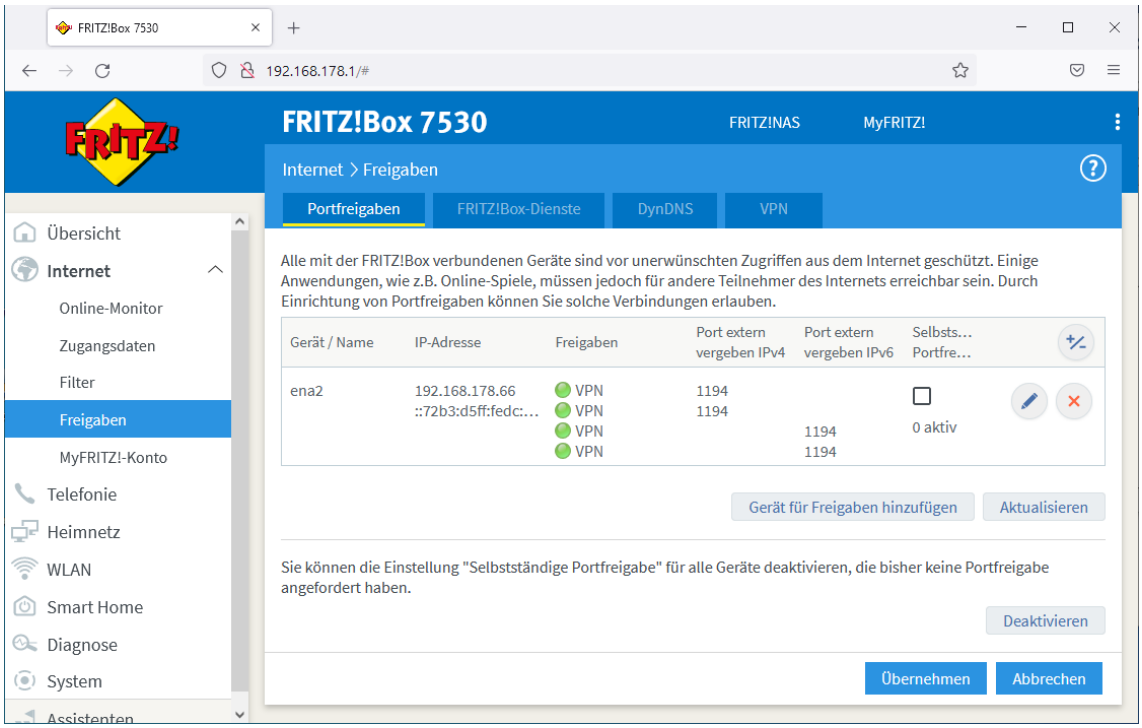
Warning: Do not forward the port of the ENA² configuration website. Always use a VPN connection for remote configuration!

Example: Fritz!Box, FRITZ!OS 07.28:

Port forwarding is called Port sharing in Fritz!OS. Navigate to Internet → Permit Access → Port Sharing and add a new device for sharing. Select the ENA² and insert the VPN port for UDP and/or TCP.







Addresses

The VPN server of the ENA² assigns IP addresses in separate subnetworks, similar to the “Protected Network”. Every connected client receives an address within these subnetworks, together with routing information to access the home network and the “Protected Network”.

These subnetworks must be unique and may not overlap with the home network or the “Protected Network”. The addresses of the VPN server are fixed and cannot be changed.

		Server address	VPN client addresses
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 (iOS only)

iOS devices can open a VPN connection if a specific hostname or a host within a specific domain is accessed. The domain must be set in the configuration. Either single hostnames or domains including wildcards, e.g. “*.domain” can be used. It is important that the hostname including domain can be resolved after opening the VPN connection.

VPN clients automatically receive all DNS servers the ENA² received from the DHCP server or which are configured statically, as well as the DNS server of the “Protected Network”.

You should add the SSIDs of you local WiFis to prevent the VPN connection to be opened at home.

Warning: VPN on demand settings only affect VPN profiles exported after changes have been made.

Example:

Add `*.protected` for the “Protected Network”. You can then use any of the DNS names of fixed DHCP clients of the ENA² to open a VPN connection.

If a Fritz!Box is used, add the domain `*.fritz.box`. If the connection however is to be used only for the ENA², add `ena2.fritz.box`.

Relay Server

All network devices, e.g., internet router, server, computer, connected to the internet or local, are addressed using their IP address. In addition to the common IPv4 protocol, IPv6 is available since several years. From a user’s perspective it makes no difference, as requests to servers on the internet most commonly use the DNS name instead of IP addresses. When the website http://www.enertex.de is opened, the name is resolved automatically, i.e. a responsible server is asked which IP address belongs to the DNS name www.enertex.de. The actual connection request is then sent to the IP address. Most services are accessible with IPv4 and IPv6, and internet providers translate accesses if required, so no access fails. Problems only arise if the connection is established “from outside” instead of “from inside”. If you want to open a connection to your local device from the Smartphone, it depends on the mobile and domestic internet providers.

Enertex Bayern GmbH offers a forwarding service – the Relay server. You do not need to configure your local internet router and any combination of IPv4/IPv6/DS-Lite offered by your providers works. The ENA² opens a connection to the Relay server and keeps it open. If a VPN clients wants to connect to the ENA², it also opens a connection to the Relay server instead. The Relay server simply forwards the encrypted VPN data between VPN client and ENA². You can use this service without having to worry about data security. Your data is still encrypted all the way between your ENA² and the VPN client software (E2EE/end-to-end encryption).

The Relay server requires no registration. You can select to use the Relay server separately for every VPN profile. Of course you still can open a direct connection to your ENA² is possible. To use the Relay server, activate it in the configuration and select “use Relay server” when exporting the VPN profile.

You can use the Relay server free of charge. Every ENA² has a data volume limit of 5 GB per month.

DynDNS

To simplify remote access for your domestic internet connection you can use the free DynDNS service of the ENA². No further configuration or registration is needed. Simply select your desired address and leave the rest to your ENA².

This service provides a fixed address for your connection. Most internet provider assign different IP address when opening the connection. The ENA² periodically sends its current IP address to the Enertex DynDNS service.

Please note: This is no remote access to any local device but only a symbolic name for your IP address. If you want to make other devices available for direct remote access, open respective ports in your internet router.

Only open ports to appropriately protected devices. Use a VPN connection where possible instead of exposing hosts directly by port forwarding.

The DnyDNS address is also used for your VPN connections if using the Relay server is disabled.

Open the protocol of your ENA² to verify that your local IP address is synchronized with your hostname:

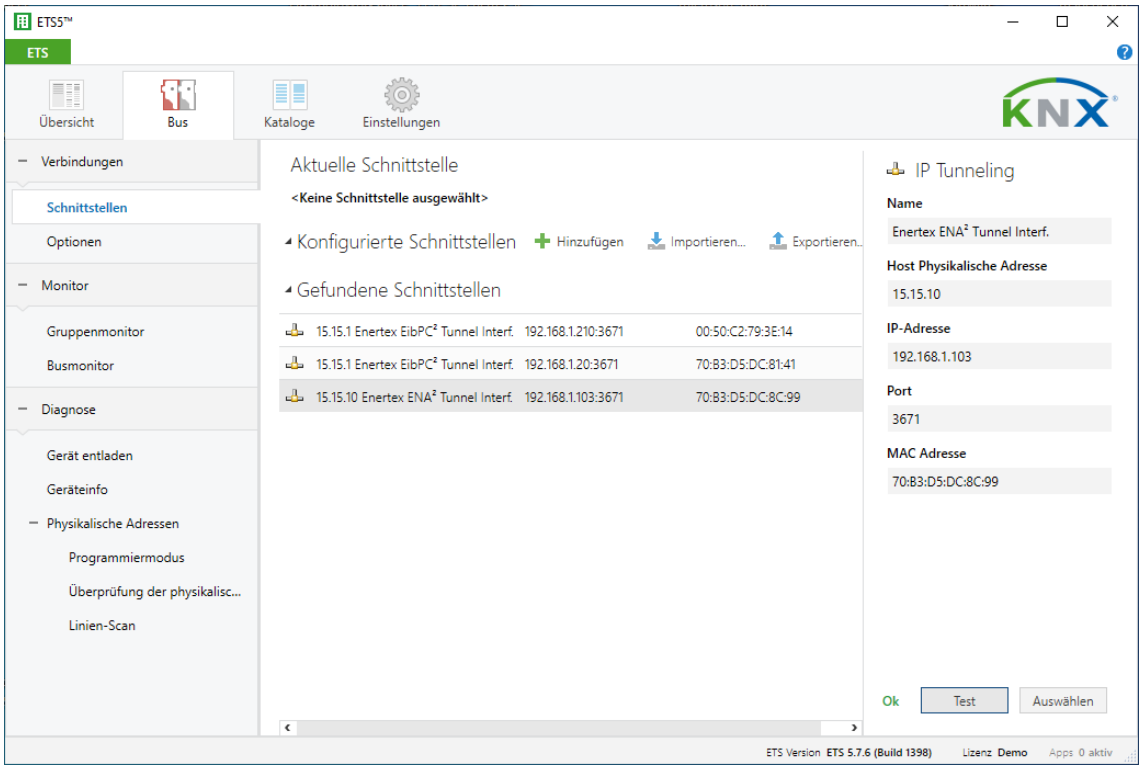
```
hostname meinedomain.ddns.enertex.de refreshed on 2021-11-23T09:20:43.175Z to
1.2.3.4, 1000:1:2:3:4:5:6:7, interval: 3600 s
```

KNX

Integrated Interface

The ENA² has an integrated KNX interface for Bus access and an additional KNX IP tunnel for the ETS. The ETS automatically lists the interface if the computer is in the same subnetwork (Home network or “Protected Network”) if access is permitted in firewall configuration.

The integrated interface is also available if a bus interface is selected for bus access of the ENA².



Control with KNX telegrams

The VPN server and selected user can be controlled using KNX telegrams. Enter the group addresses in KNX configuration. You do not need to import an ETS project first.

VPN Profiles

To open a VPN connection you need to export a VPN profile first. The profile contains all connection information (address, settings) as well as encryption keys. If the encryption parameters are invalid, e.g., because of a new certificate chain, the server ignores the request instead of rejecting it to increase security, so you do not get a specific error message but a timeout.

If the encryption is correct, the connection is terminated by the server if the respective user is not enabled.

Log in on the ENA² website using the user credentials. Select “VPN profile” in the user area. You can change profile-specific settings and export the profile. The settings only change the exported profile.

You need to provide a password on export. This is especially important when the profile is sent via e-mail, because the profile contains all encryption parameters for remote access but e-mails are not encrypted themselves.

Delete the exported profile after import to reduce the risk of losing it.

A description how to import the profile can be found on the VPN profile – website, so every user is able to export and import his profile.

Windows, Linux, Android, macOS

Export profile for OpenVPN Connect

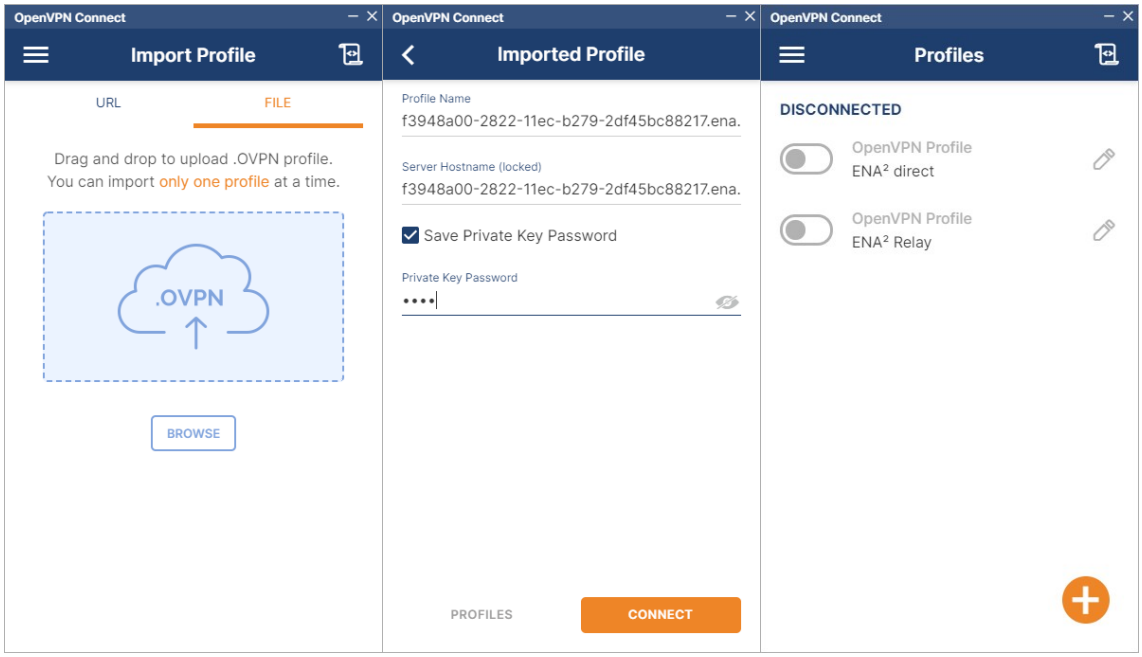
Download OpenVPN Connect:

- Windows 10: 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

Open OpenVPN Connect

Import profile

Enter the password used on export. You can rename the profile.



iOS 15

Export Mobileconfig for iOS

Download OpenVPN Connect for iOS:

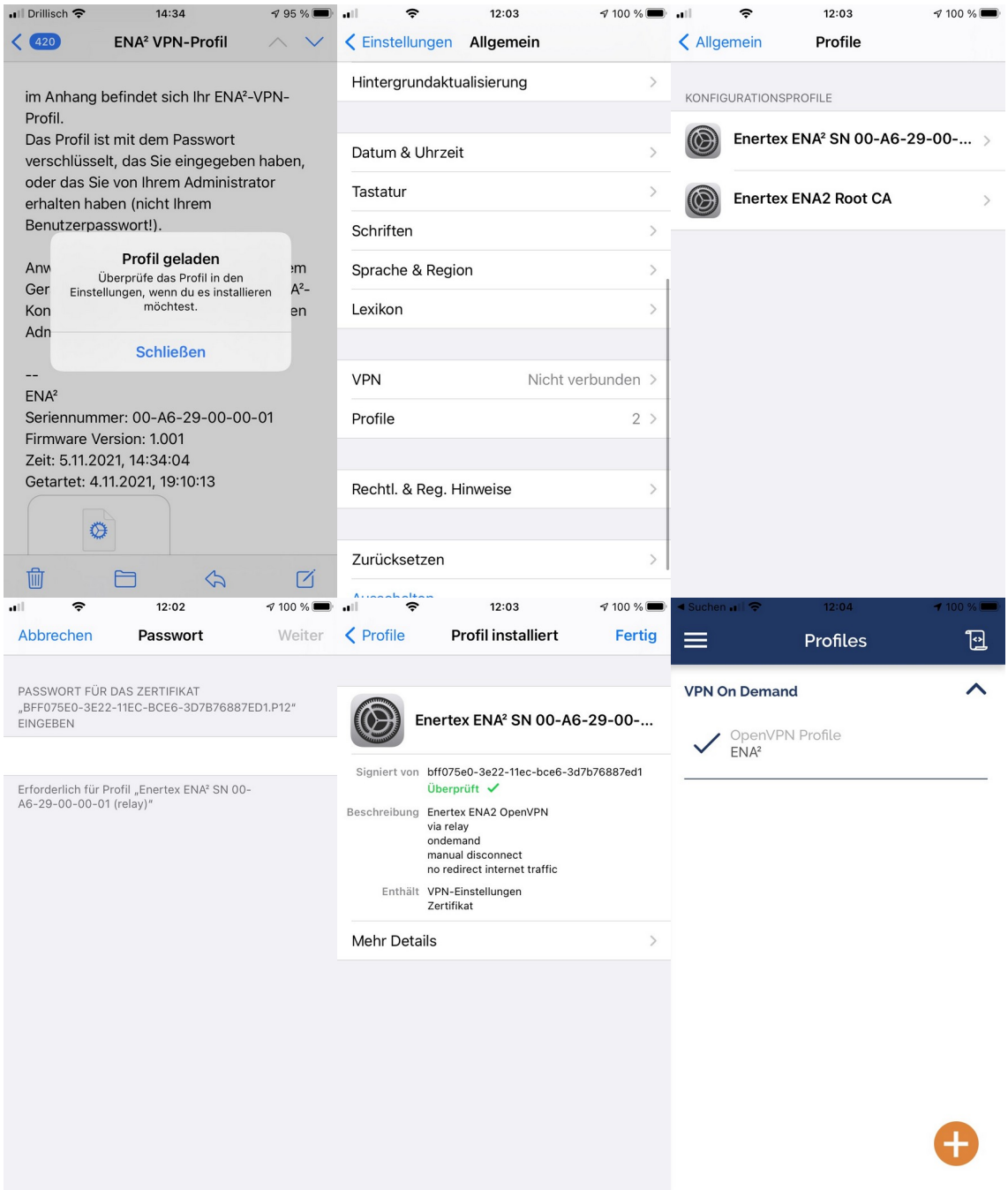
iPhone iOS: https://www.enertex.de/ena-openvpnclient-ios

Open the file .mobileconfig

Open Settings → General > Profiles and import the certificate

Open the profile and install it

OpenVPN Connect now shows the profile



Telegramlog

The ENA² records all telegrams either received on its integrated interface or the configured tunnel interface an internal database. Raw telegrams can be exported to be used in ETS.

If an ETS project is imported, telegrams are decoded and values are stored in the database. You Open the device website to show telegrams from the database. You can visualize values in a time-value chart.

The telegramlog provides predefined queries for analysis, e.g., to see all read requests without response telegram.

Certificates

Certificates are an integral part of internet security, mainly used for identification.

A certificate is similar to a passport. The authenticity depends on two assumptions:

1. You trust in the issuer to correctly validate the identity of the passport owner
2. You recognize that a passport is valid or has been copied

The photo helps to validate that the passport has been issued to your counterpart and not his neighbor.

In digital certification the “Certificate Authority” (CA) replaces the issuing administration. A CA is a company which guarantees to issue certificates only after having validated the identity. If the certificate is used by a server, the CA validates the internet address of the server (domain, hostname). If it is correct, the address is stored in the certificate (Subject), being the counterpart of the photo.

The CA signs the certificate as proof of correctness and its name is also stored in the server certificate.

If a client opens the website using https, the server presents its certificate. The browser compares the address of the website to the address stored in the certificate. If they match, the browser checks the signer of the server certificate. The certificate used to sign the server certificate may also be signed by another certificate, so this certificate is checked again. This check is performed recursively until a valid CA certificate is found. This is called certificate chain.

In contrast to a physical passport, data can be copied without being able to detect it. Anyone could intercept your request to the server, and present a copy of the server certificate instead. To detect this, every (public) certificate has a private key which must only be known by the owner. Even the signing CA does not know the private key. Only the owner of the private key can prove that the presented certificate is his own. An attacker can present a copy of the public certificate but your browser does not trust him anyway because of the invalid private key.

Every browser and operating system manage a list of trusted CS certificates.

ENA² Certificate Chain

The ENA² has no public domain, so a regular CA does not issue a certificate. Instead, the ENA² uses self-generated certificates. Every ENA² creates a unique certificate authority and separate certificates for user and services.

The services (VPN, Web) use the certificates to allow the client to validate the identity of the device. Every user in turn uses his certificate to be identified by the service of the ENA².

If the user adds the CA certificate to the list of trusted CAs, every certificate issued by the device is trustworthy. It is not required to import every single service certificate.

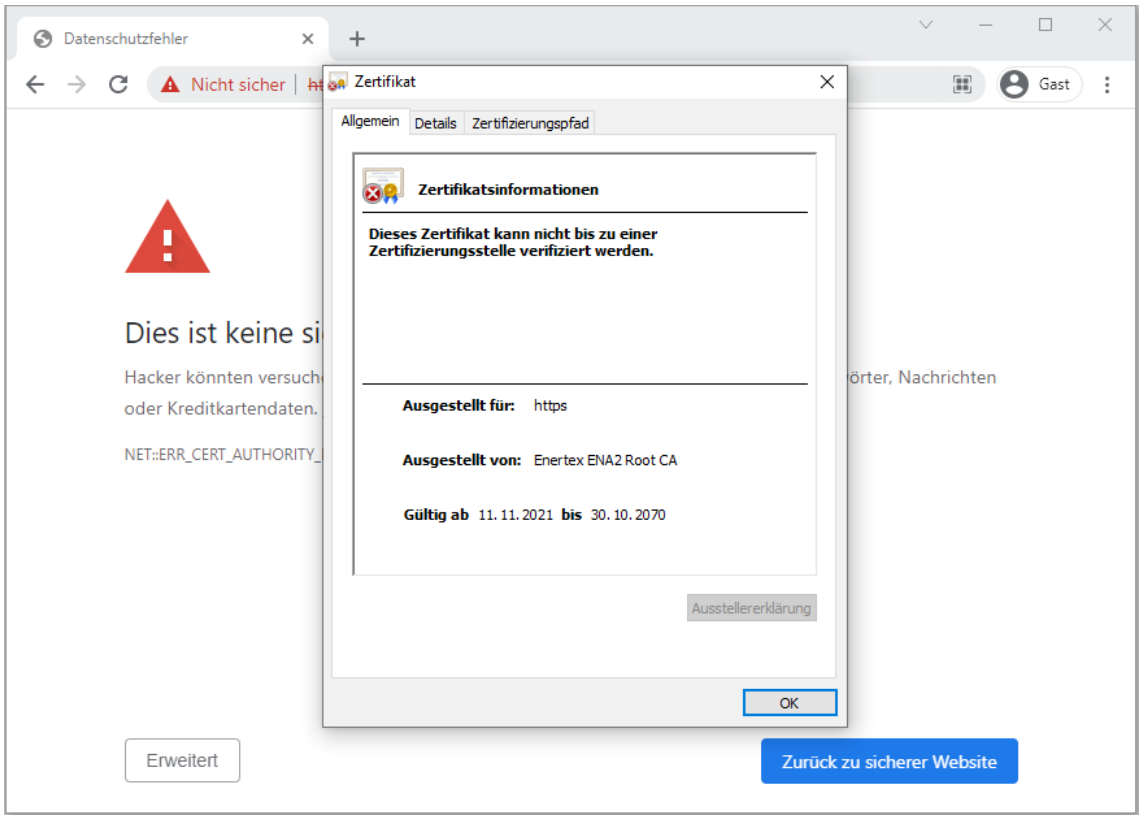
If the root certificate of the CA is changed, all issued certificates become invalid. It is typically not required to regenerate the CA and it is done automatically on factory reset.

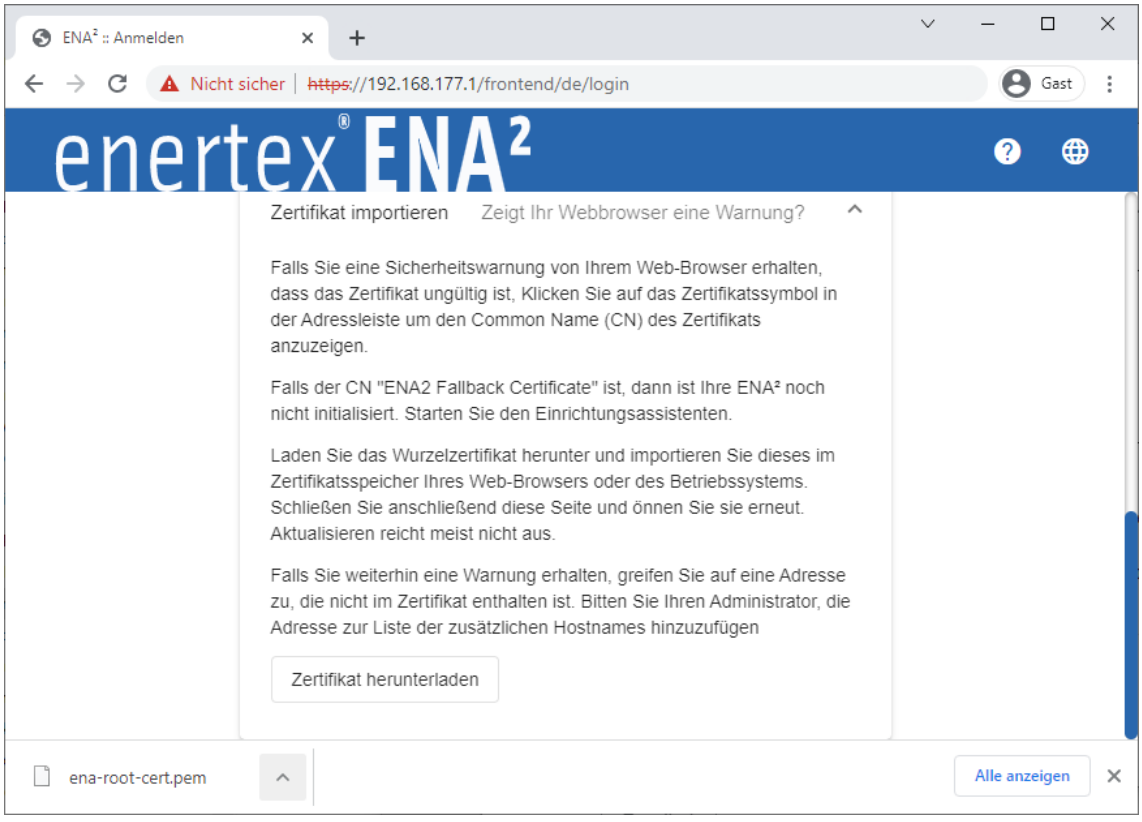
Import Root Certificate

Import the Root Certificate of the ENA² on any client device. The browser trusts the connection and the connection is secure. It is not required to import the server certificate once it is changed, e.g., because you changed the DynDNS address. This is only required after factory reset or if you manually generated a new certificate chain.

It depends on browser and operating system how to import the root certificate.

First download the root certificate to the respective device. You find a link to certificate on the login website of your ENA². The ENA² must be initialized, i.e., the first-start wizard must be completed.





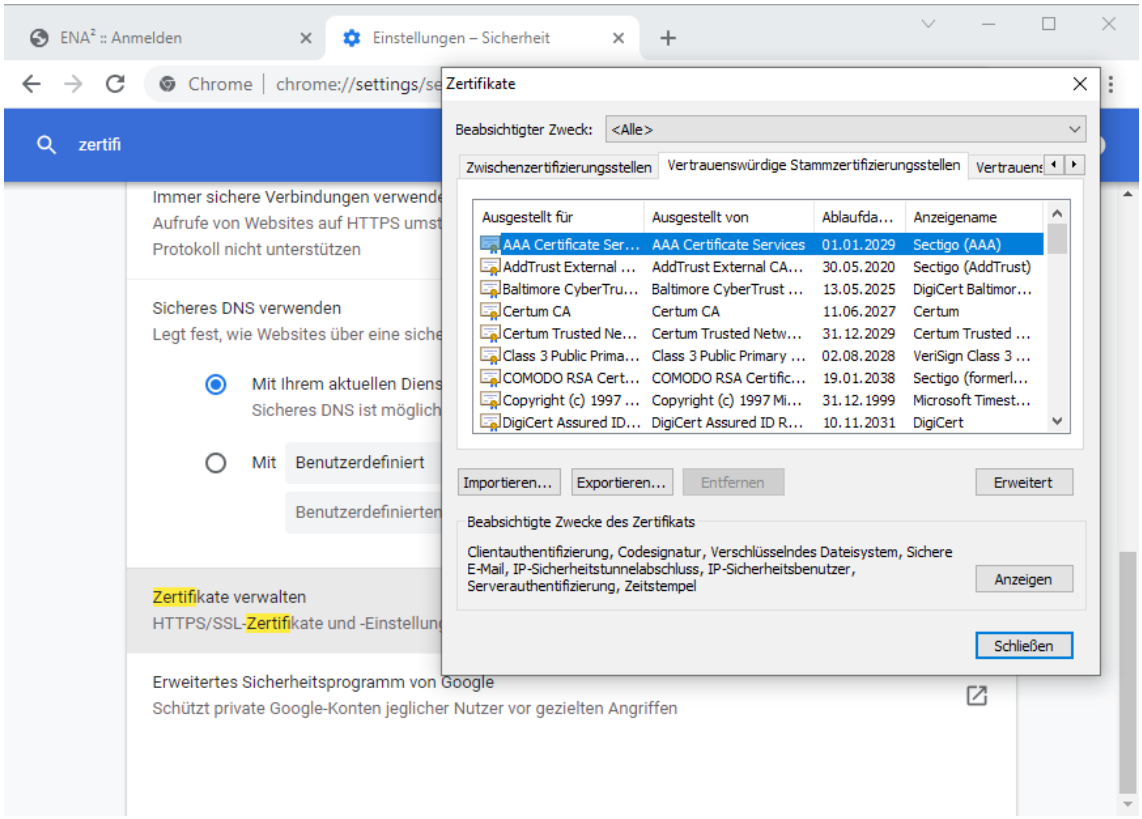
Windows 10

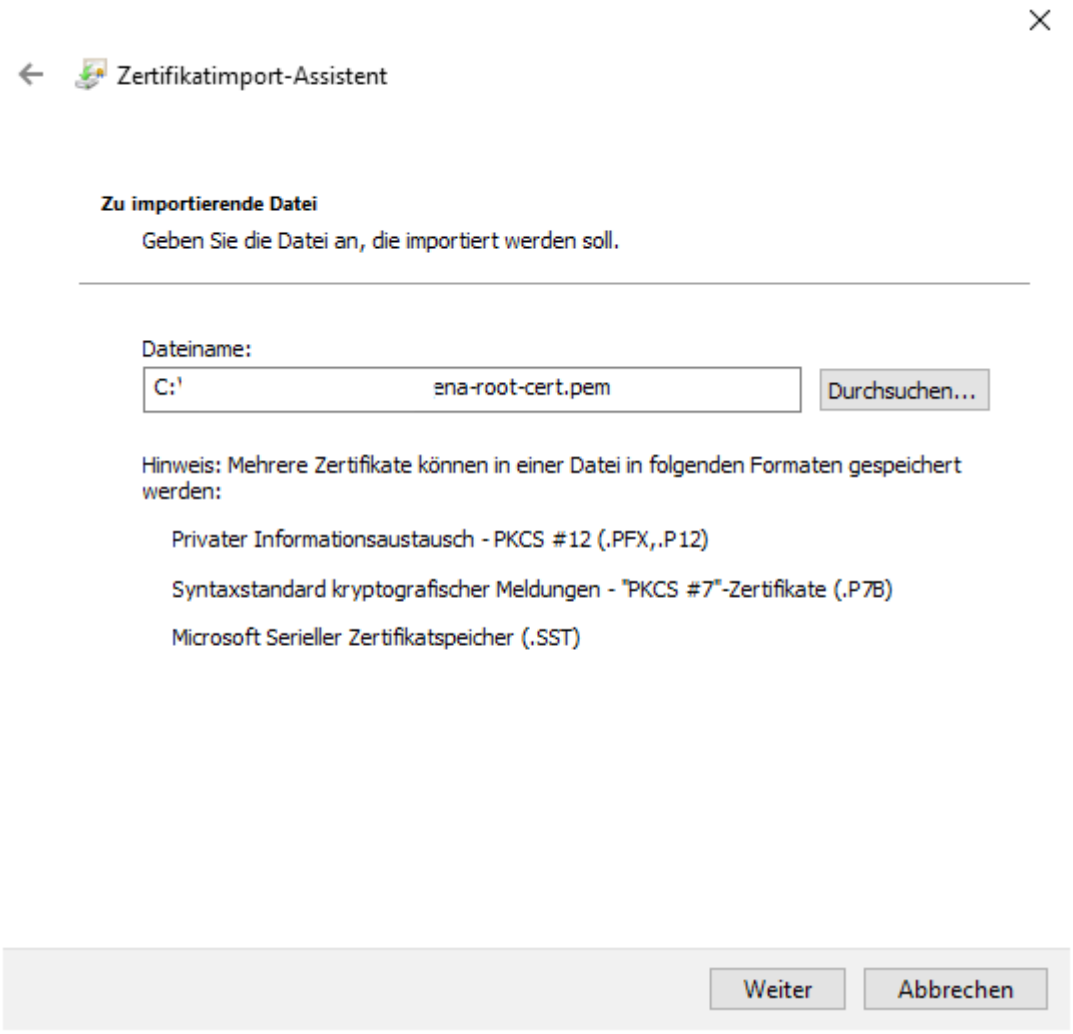
Google Chrome 95.0

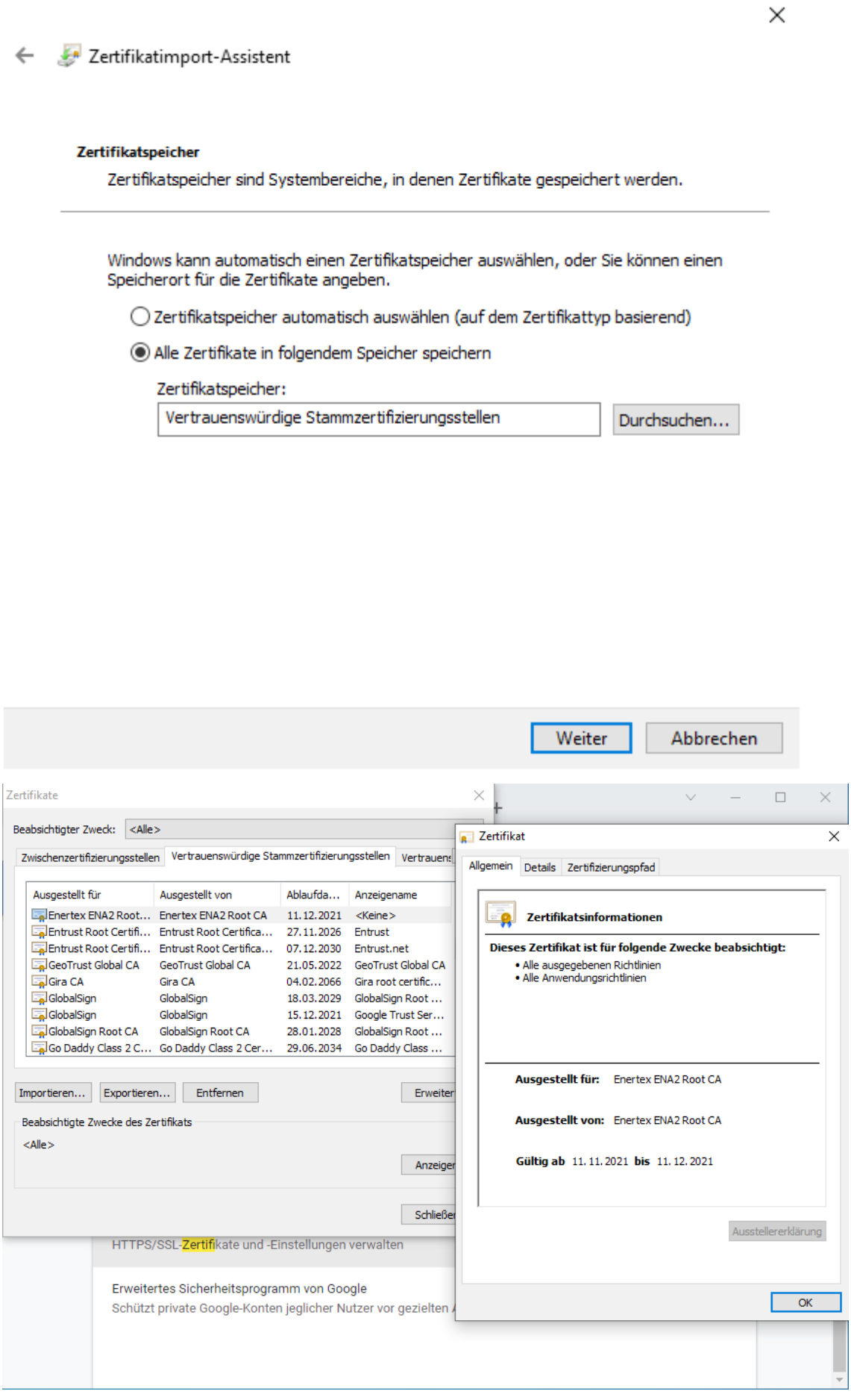
Open the browser settings and enter Certificate into the search bar. Open Privacy and security → Security → Advanced → Manage certificates.

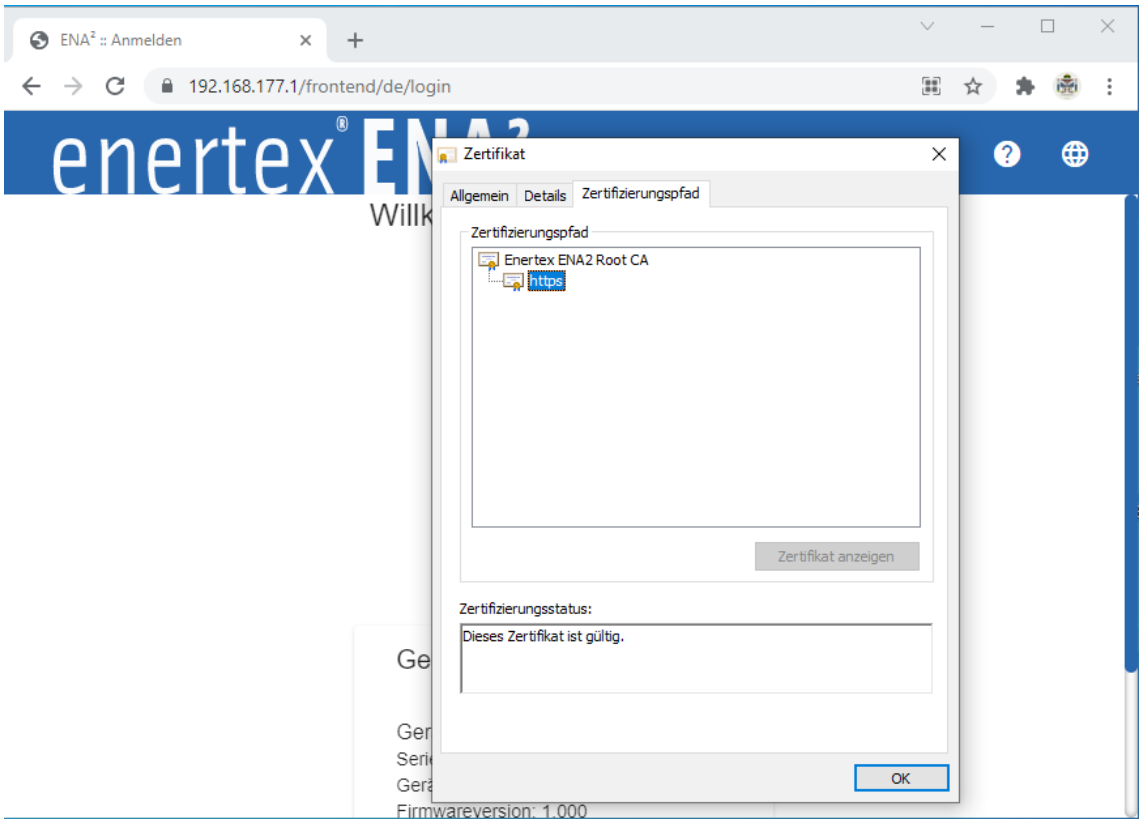
Open the tab Trusted Root Certification Authorities and import the root certificate. Close the

browser window and open the ENA² website again. The certificate is now accepted.



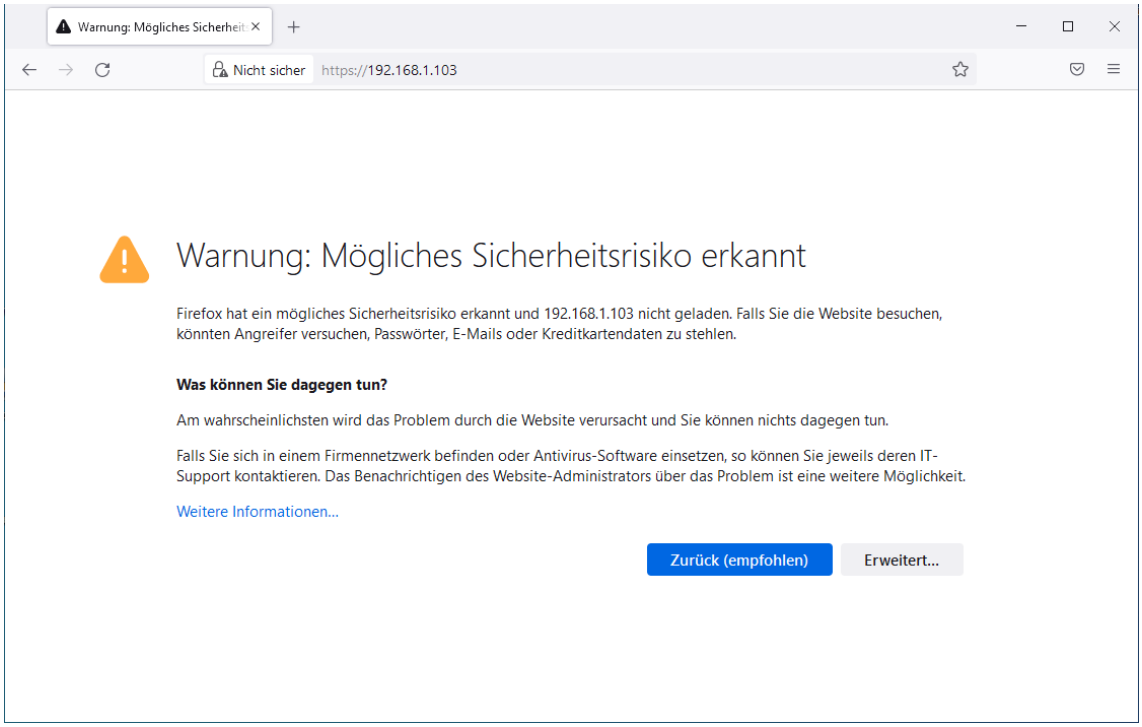

Zertifikatimport-Assistent
Zu importierende Datei
Geben Sie die Datei an, die importiert werden soll.
Dateiname:
C:\ ena-root-cert.pem
Durchsuchen...
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
Syntaxstandard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

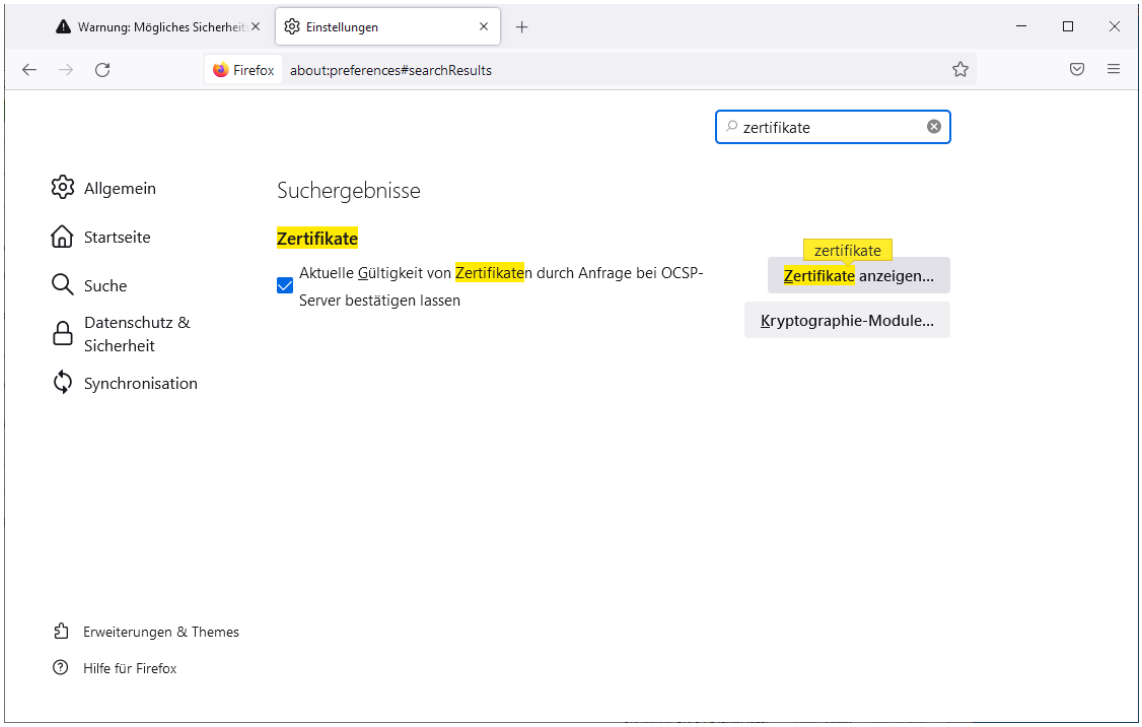

Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem 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

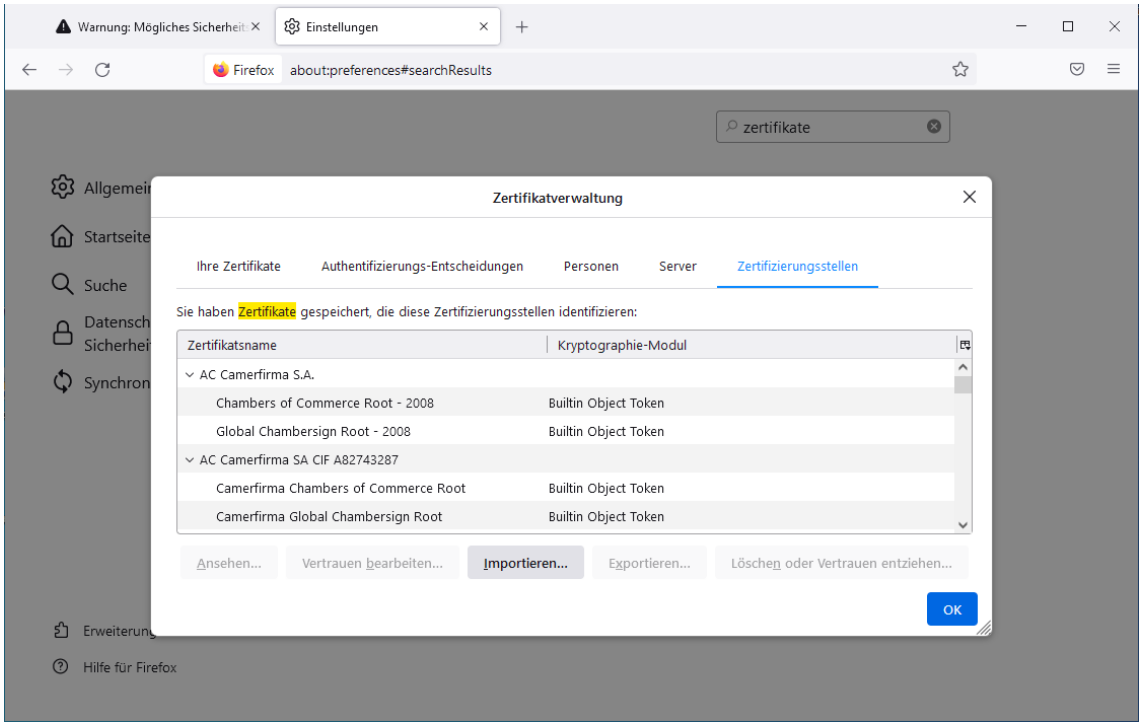


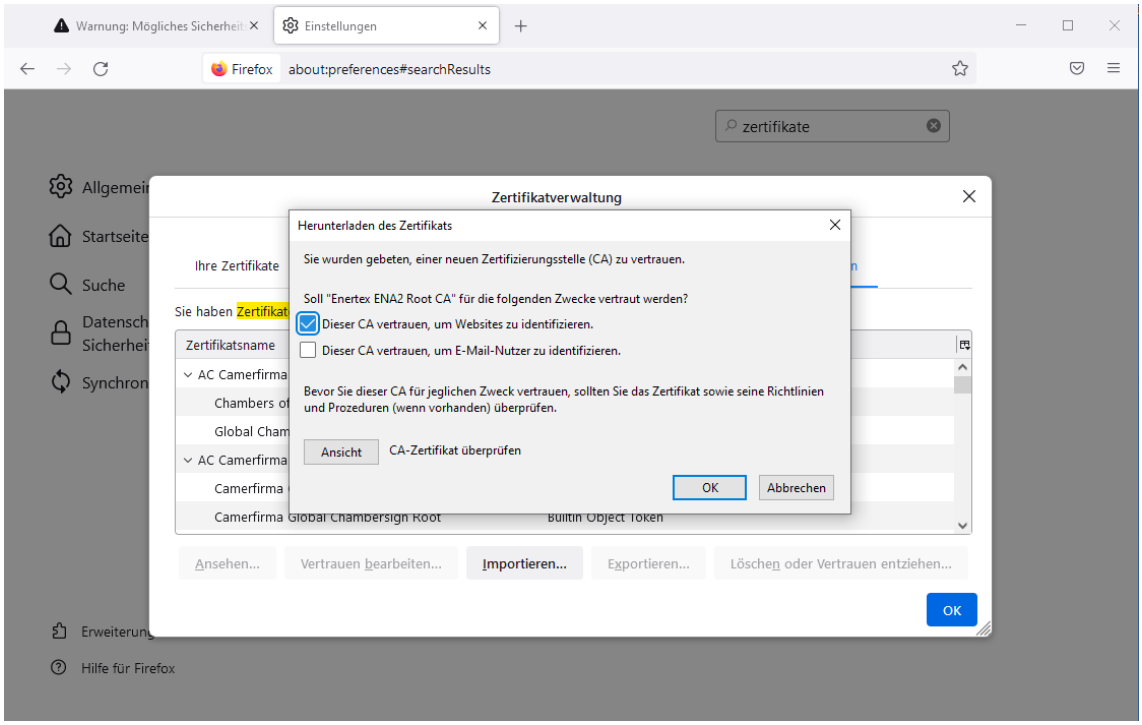
Firefox 94.0.1

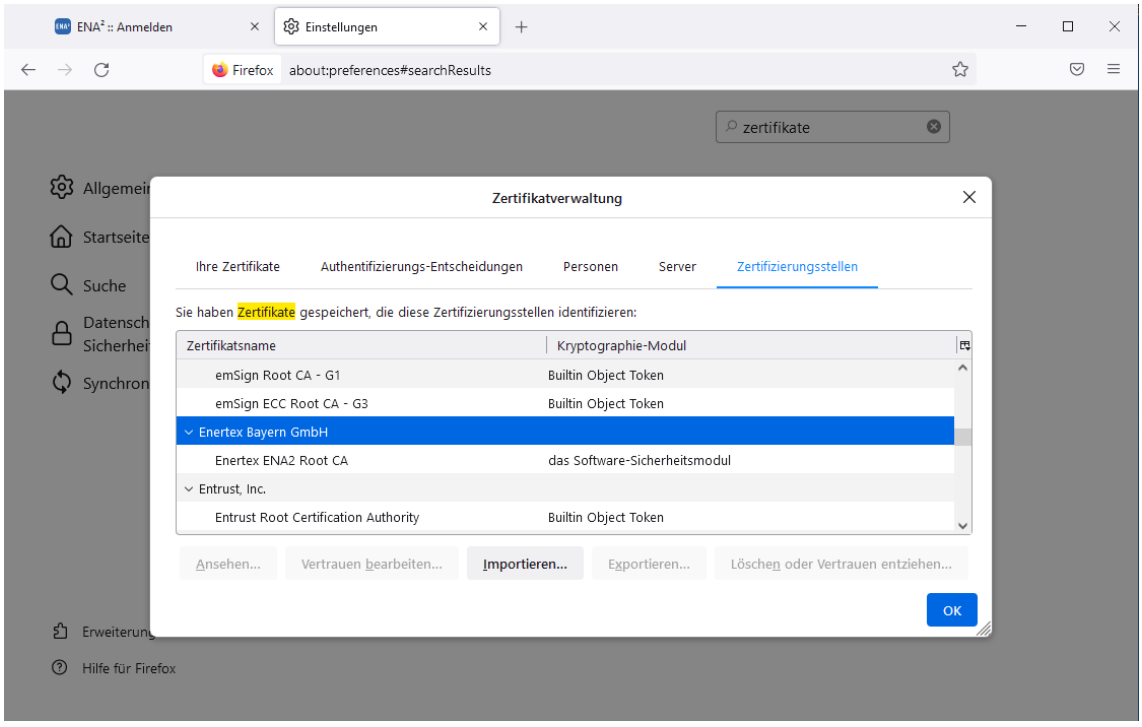
The process is similar to Google Chrome. Add the certificate to the list of certificate authorities. Close and open the ENA² website after import.

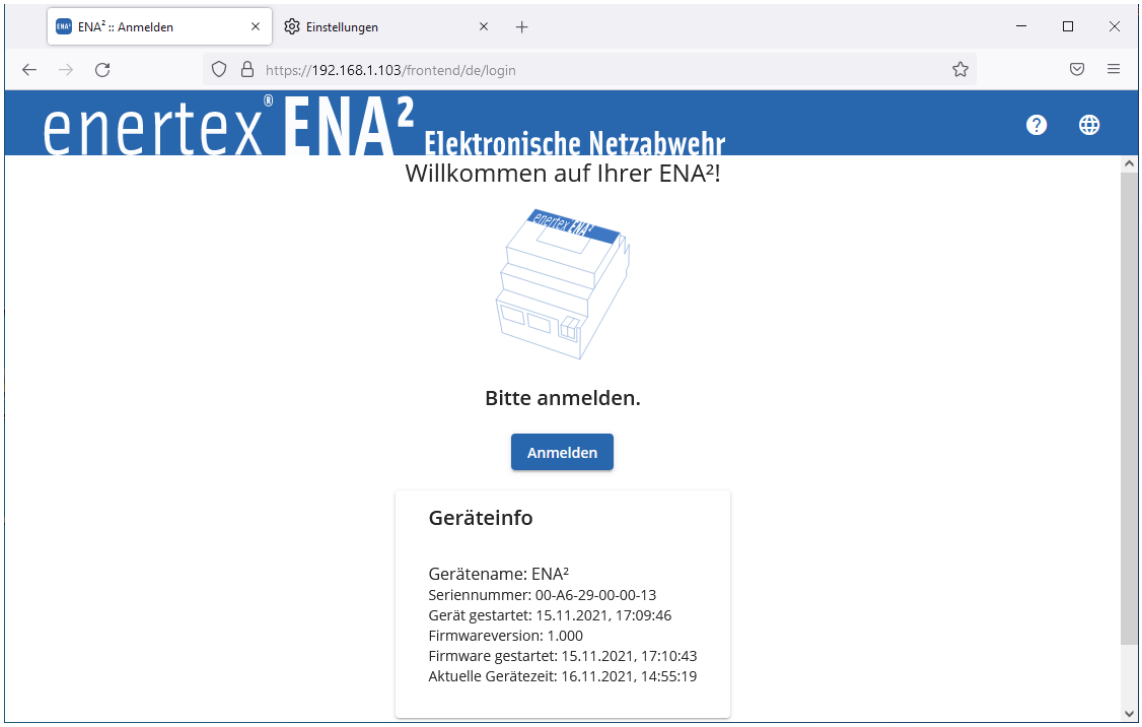



Warnung: Mögliches Sicherheit
Einstellungen
Firefox about:preferences#searchResults
zertifikate
Allgemein
Startseite
Suche
Datenschutz & Sicherheit
Synchronisation
Suchergebnisse
Zertifikate
Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen
zertifikate
Zertifikate anzeigen...
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
Allgemein
Startseite
Suche
Datensch
Sicherhei
Synchron
Erweiterun
Hilfe für Firefox
Zertifikatverwaltung
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
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


ENA² :: Anmelden
Einstellungen
Firefox about:preferences#searchResults
zertifikate
Allgemein
Startseite
Suche
Datensch
Sicherhei
Synchron
Erweiterun
Hilfe für Firefox
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



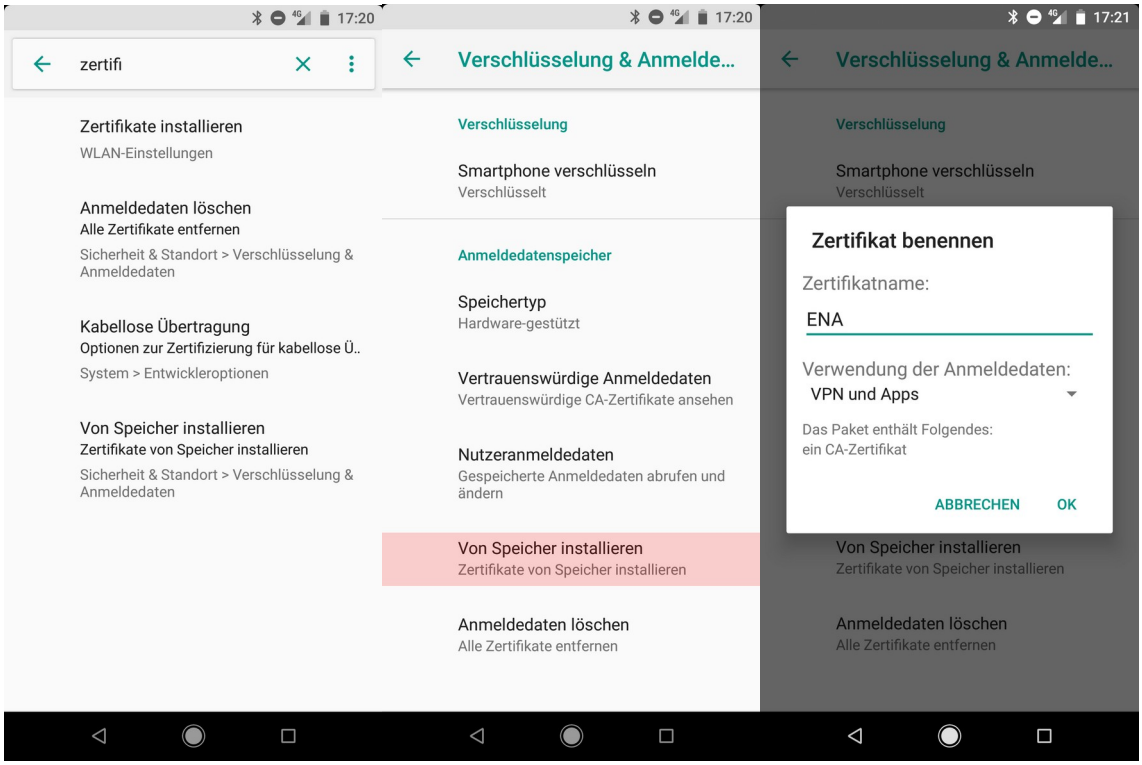
Android 8

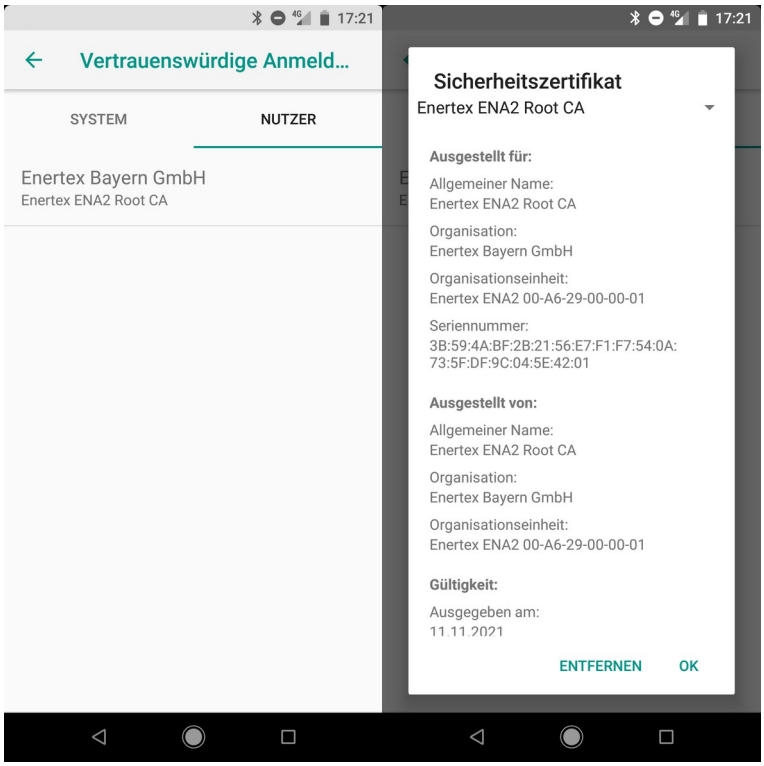
Google Chrome 95.0

The exact menu structure depends on Android version and device vendor but should be very similar.

Open the Settings → Security → Install from storage.

Install the downloaded root certificate. The certificate can now be found in the list of trusted CAs.





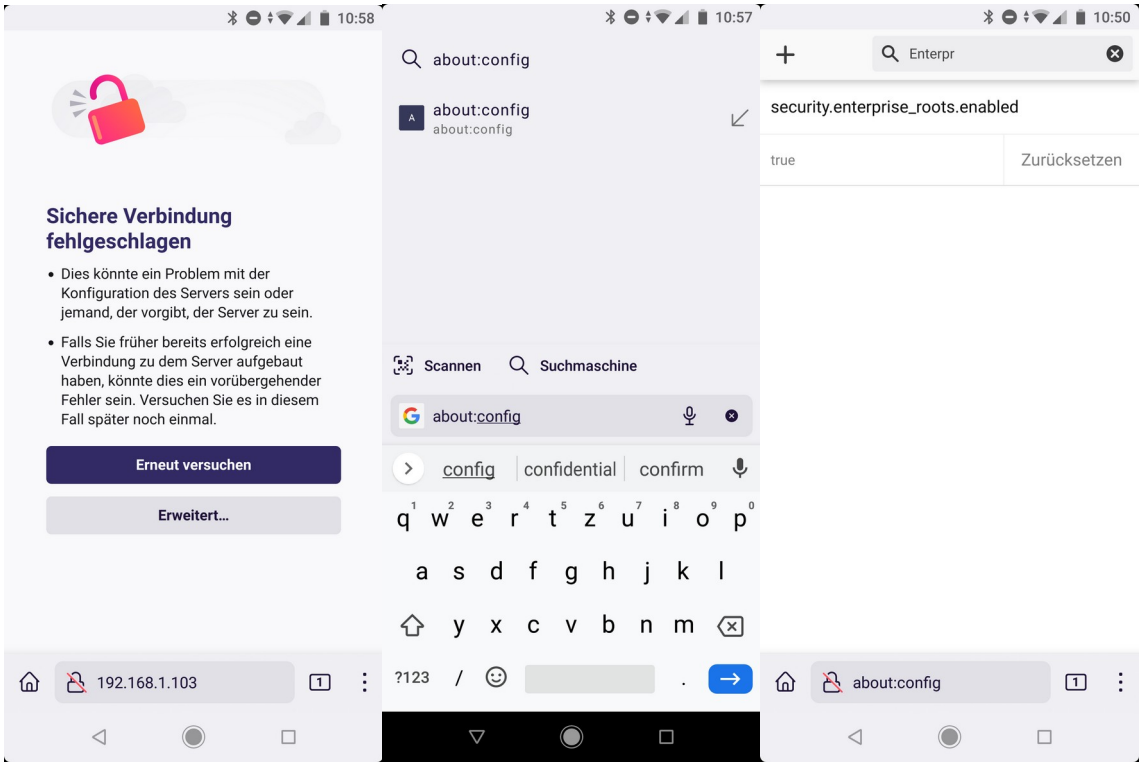
Firefox Beta 95.0

Firefox does not use the operating system certificate storage. This function has to be enabled first and is only available in Firefox Beta.

First import the root certificate as for Google Chrome 95.0.

Install Firefox Beta and navigate to “about:config”. Search for “enterprise_roots” and set the value to true.

Close the ENA² website and open it again. The certificate is now valid.



Problems

If the certificate is not accepted after import of the root certificate, verify that the server certificate is not the fallback certificate.

Open the certificate from the navigation bar and check that the subject is “https”. If not, the certificate chain is not initialized correctly or the device did not perform a restart after initialization.

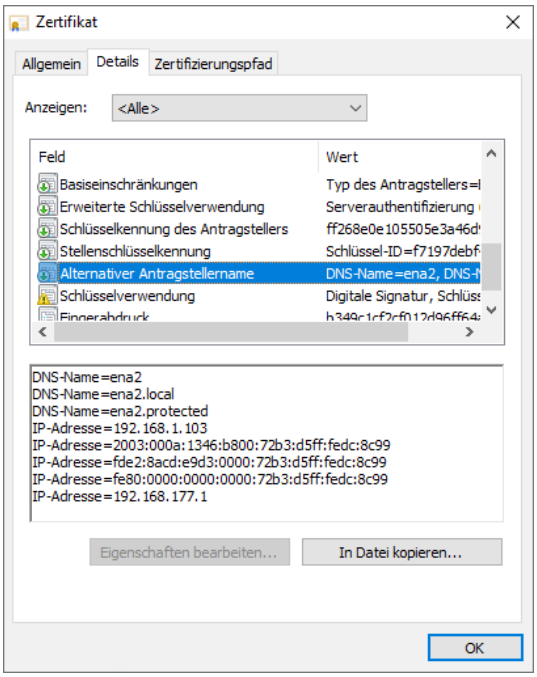
If the certificate is correct check the list of addresses stored in the certificate. The address used to open the website must be included. The list is generated as follows:

Network mode “Switch”:

- Static IP address if configured
- IP address received from DHCP at the time the device has been initialized. If the address changes, manually issue to regenerate the server certificates. Alternatively try one of the DNS names listed.

Network mode “Firewall”:

- Static IP address if configured
- If the DHCP server of the ENA² is enabled to manage the “Protected Network” you can use `ena2.protected` within the “Protected Network”.



Device certificate

Every device is produced with a unique device certificate, sent to the DDNS service and relay server for authentication. You do not need to change or refresh the device.

Factory reset

If you cannot reach your ENA² or if the owner- and administrator passwords are lost, you can reset the device ti factory defaults. All configuration is removed, the network mode is set back to “Switch mode” and the DHCP client is enabled. All telegrams and protocol entries are removed.

To issue a factory reset, the device must be in ready state, i.e., the power LED (5) flashes and the display is on. Press and hold the display button (10) for 5 seconds.

You see “Hold for reset“ on the display. Release the button (10) to cancel the factory reset.

Hold the button for another 5 seconds until you read “Factory reset” on the display.

The device reset is performed and automatically restarted.

Technical data

KNX (power supply)	Voltage: 27...30 V DC Current consumption < 110 mA at 29 V bus voltage.
Ethernet interface	2x RJ45 interface for 10M/100MBit Ethernet
Control and display elements	OLED Display LEDs: Power (green) Info (yellow), Alarm (red), Push buttons: F1, F2, Display
Casing	DIN rail housing for 35 mm mounting rails width: 4 SU Dimensions: 71,5 mm x 89,6 mm x 62,9 mm (L x B x H) Flammability class: UL94-V0 (casing) UL94-V2 (lid)
Additional	For indoor use only For operation in the control cabinet only Highest ambient temperature ta = 45 °C Lowest ambient temperature ta min = -5 °C Protection class III Protection class: IP20 Audits: Safety: IEC 63044-3 EMV: Certified IEC 63044-5-2 (Living area), IEC 63044-5-3 (Industrial area), Vicinity: Certificated DIN EN 50491-2

Changes

1: 20.12.2021, Dipl.-Inf. F. Naumann

- Initial version