enertexbayern gmbh
simulation entwicklung consulting

Manual and Configuration
ENA (Electronic Network Defense)

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

Inhalt

Note

- Installation and assembly of electrical equipment must be carried out by qualified electricians.
- Connecting KNX/EIB interfaces requires specialized knowledge by KNX™ trainings.
- Non-observance of the instruction can entail damange to the implement, fire or other hazards.
- This instruction is component of the product and has to remain at the end user.
- The producer takes no responsibility for charge or damage which are accured by using this device to the user or third person, misusing or disturbance of the connection, disturbance of the device or devices of participants.
- The opening of the case other unauthorised changes and or rebuilding of the device leads to the expiration of the warranty!
- The producer is not in charge for not designated use!

Function Description

KNX and IT are connected more closely in Smarthome. Thereby the aspect of security of attacks by third parties reaches a new dimension. Often this aspect is neglected because the electrician has to maintain the complete system and the functionality of security reduces substantially the comfort of operating unit e.g. by cumbersome password entries.

The solution: The electronic network defense – ENA - of Enertex® Bayern GmbH.

Remote Maintenance

A remote maintenance of the system without functionality of security entitles IT-specialised criminals each posibility to open electric pivots and doors et cetera. Via targeted attacks the entire IT network of the whole family can be hacked.

With the ENA the otherwise extensively configurating function of security can be made easily switchable for the user via the visualisation or via the KNX button. If you want to the remote maintenance access can be opened or can be turned off. And you recognise if this is used – simply at your KNX switches.

Abbildung 1: Remote mainteance

Secure Connection to your Home

When you are in your home network the operation of visualisation, LAN devices are comfortable accessible via a specific APP.

The same comfort should be ensured too if you are on move, but what is not possible without a secure connection.

With the ENA the secure aspect is guaranteed without resigning the user comfort.

Abbildung 2: Secure connection to your home

On Demand (nur iOS)

The Enertex ENA offers secure access via internet to your home network. With the „on demand“ - technology optimal secure is guaranteed, without cumbersome password entries.

Just click on your APP. ENA and your iPhone deal the rest (tested with iOS 8 and 9).

Secure Internet Connection

With ENA you make your Internet connection safer in transit: You dial in via a public internet access in your home network and than you surf exclusively and securely via your private connenction.

Abbildung 3: Secure internet connection

General view

The Enertex ENA offers secure access via Internet to your home network.

The setup of the equipment is possible in a few steps in the simplest way:

- Easy configuration via a Web browser
  - Basic configuration
  - Applying security patches
  - Backup / restore of configuration
- Management of dynamic DNS (DDNS) about following suppliers:
  - Dyn.com
  - FreeDNS
  - Gira DNS
  - No IP
- HTTPS reverse proxy with four redirects (2048 bite key)
- OpenVPN-Server
  - User management
  - User authentication using an encrypted PKCS#12 file
  - Encrypted data transfer at the highest level (AES-256)
- Creating the OpenVPN configuration files for:
  - iOS
  - Android
  - PC systems (Windows/OSX/Linux)
- Optional integration into the KNX system (KNXnet/IP interface or router required):
  - Opening and closing of the access authorisation of a user via KNX 1 bit group address i.e. Display whether a user actually uses the OpenVPN connection.

- Display of connection status via KNX 1 bite group address i.e. Display whether a user actually uses the OpenVPN connection.
- Turn on/off of the OpenVPN server cia KNX 1 bite group address

- OpenVPN experten options – configurable easily
  - OpenVPN „on demand“ for Apple iOS
  - Lead external Internet connection via your own home network via VPN, if you e.g. registered in a public WLAN.

Specifications

Hardware	
Dimensions	Rail, 6 TE
Power supply	20 ... 30 V DC
Performance input	1,2 – 1,7 W (depends on LAN activity)
Interface	Ethernet 10/100 Mbit/s
Software	
Operating system	Linux
OpenVPN	Any number of users 16 users controllable via KNX 2048 bite RSA key Transmission encryption AES-256 Perfect Forward Secrecy
HTTPS Reverse Proxy	4 forwarders 2048-Bit RSA key Transmission encryption AES-256 Perfect Forward Secrecy
Dynamic DNS	Administration of 4 Domains

Note

Some of the encryption methods depend on the capabilities of the used link partners (browser, OpenVPN Client, operating system).

KNX

An interface which is required to operate on the EIB/KNX system is not included in the delivery, and may need to be procured separately.

We recommend:

- Enertex® KNXNet/IP Router
- Enertex® KNXNet/IP Interface

Installation and Connection

For the operation of the Enertex® ENA is required:

- A power supply with at least 2W output power: Safety extra-low voltage 20 to 30 VDC (direct current)
- A 10/100 Mbyte compatible Ethernet connection
- An Internet connection for the remote control and port transmission in the router and access to DNS server and NTP server

Please note:

The external safety extra-low voltage is connected via the device to the earth potential of the LAN. For this reason exists any isolation to earth, if the LAN shield is grounded. To establish a separation we advise to use an external low voltage power supply only for the Enertex® ENA.

Commissioning

The boot time when engaging amounts to ca 60 seconds. The preadjustment for the network is DHCP.

As soon as the green LED starts flashing, you can access ENA. You have to determine the IP address of the device by using the router. Alternatively, the network can be scanned for devices by smartphone. Thereto we recommend the APP „Fing“ (Android/iOS). The MAC address set to work on 00:50:C2:79.

You enter the IP address in a Web browser and get that way to the Web interface of the ENA.

Note

At the first startup ENA generates security certificates. Meanwhile there are not all settings available in the Web interface.

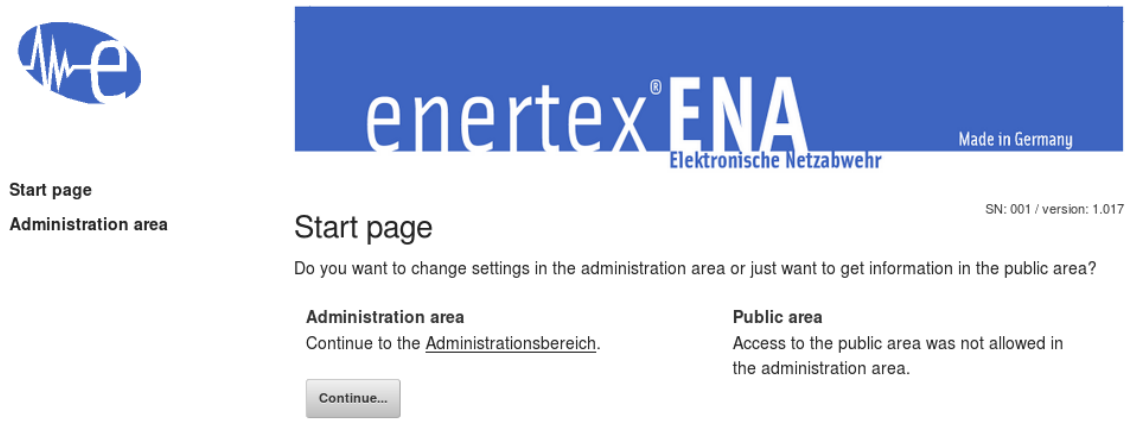
Quick Guide

1. Log on with the browser of the ENA Web interface: User admin, Password admin
2. Network: Configured IP addresses. Ensure ENA access to a DNS server an a NTP server.
3. Dynamic DNS: Activate DDNS administration, choose DDNS provider, specify and apply data of access and domain names. Wait and see till the PKI subsystem has finished.
4. Public Key Infrastructur: Download the CA certificate and import it in browser (Firefox, Chrome) or operating system (Android/iOS).
5. HTTPS Reverse Proxy: Apply user name und password, connect the external DDNS domains with HTTP hosts in LAN. Send Port 443 (TCP) on ENA.
6. OpenVPN: Add user and wait till PKI subsystem has ended. Download the matching configuration on your terminal device. Send Port 1194 (UDP) on ENA.
7. Specify IP address of KNXnet/IP interfaces. Specify group addresses respectively for start/stop and status of OpenVPN server. The same for each OpenVPN user.

Web Interface

Start page

On the start page you can chose between the admin area (webadmin) and public area. Public area is disabled by default.



Webadmin

The admin area of the web interface of ENA is access protected. The standard login is:

User: admin

Password: admin

Network

The network settings of ENA can be made here.The ENA supports the automatic configuration via DHCP or the static allocation of the network settings.

Picture 4: Network Settings

Note

For the OpenVPN operation it is obligatory necessary, that ENA as an OpenVPN server is located in a subsystem with another network address, as the accessed OpenVPN clients. Therefore it is recommended, that ENA is not located in a subnet with widely-used network addresses 192.168.0.0 or 192.168.1.0 or 192.168.2.0. For iOS VPN on demand a DNS server in the local network is required. Add it as DNS server 1.

Time Server

The ENA synchronises its time with a time server. Which time server should be used, can either be choosed via a specified location list (synchronisation via Internet) or can be defined manual.

Dynamic DNS

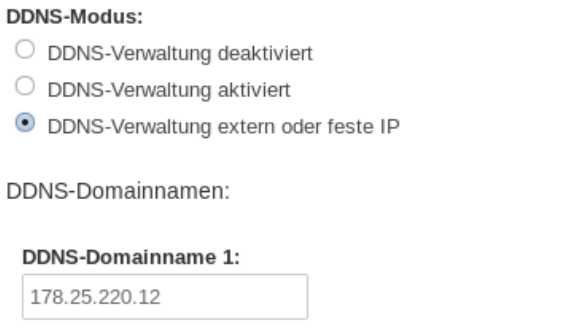
Dynamic DNS or DDNS is a technic to refresh dynamically domains in the Domain Name System. The purpose is that a computer is changing automatically the depending domain entry after the change of its IP address. So the computer is always accessible under the same domain name, even if the actual IP address is unknown for the user.

The ENA is able to self administrate and to refresh up to four DDNS domain names. Activate for this the DDNS administration and choose one DDNS provider out of the list.

Picture 5: DDNS Administration activated

The ENA checks cyclically the own public IP address and refreshes the DNS entries for all specified DDNS domains at DDNS provider.

Alternative another device (e.g. Internet router) can refresh the DNS entries respectively can be accessed via fixed IP address to the ENA. In this case the domains respectively the IP address has to be publicised to the ENA under which it is accessible from the Internet.



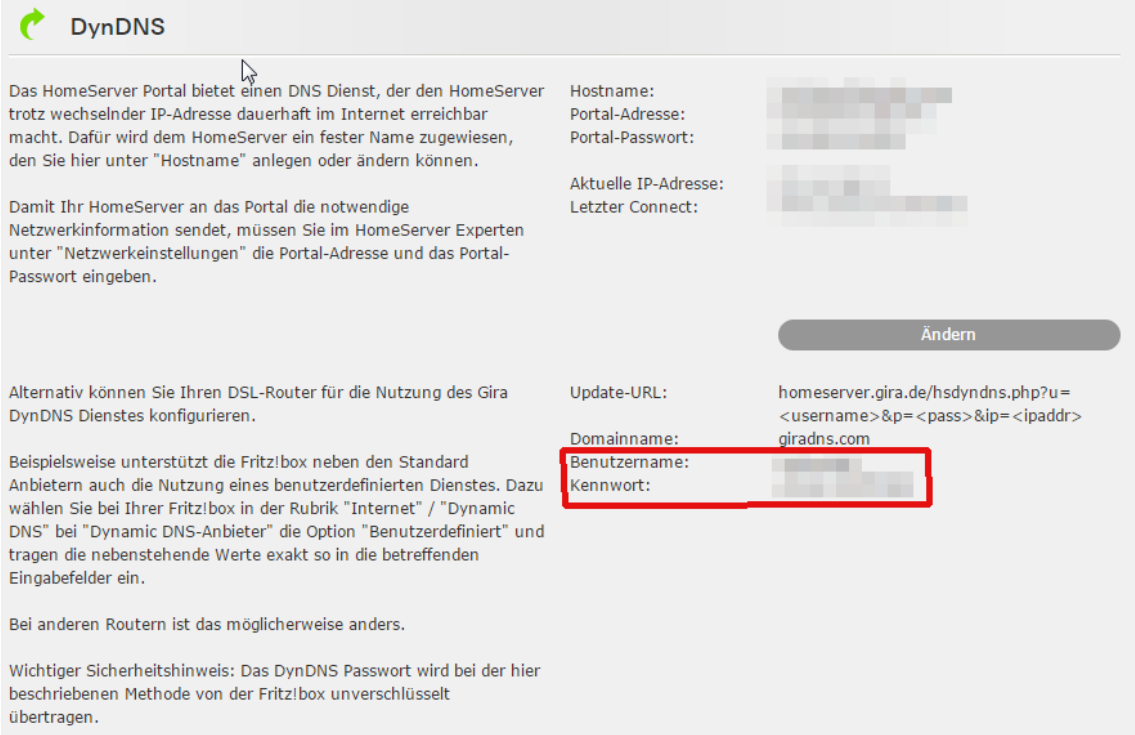
Picture 6: Access via fixed IP address

Experts Options

If the DDNS administration is refreshed, in the expert options can be fixed in which term the own, public IP address can be checked and if changing it can be transferred to the DDNS provider. Furthermore it is possible to specify an own webside with which the public IP address will be identified. The output of the webside has to contain the IP address in the HTML format.

Please compare page myip.enertex.de.

Note



Picture 7: Gira DynDNS credentials

For GiraDNS you have to use username/password as DDNS credentials, that are marked in the screenshot!

Public-Key-Infrastructure

Public-Key-Infrastructure (PKI) named a system in the cryptology. This system can construct, give out, check digital certificates. It is based on a certification authority (CA) in the ENA. CA creats and signs certificates for HTTPS and OpenVPN server. The certification authority has to be initialized on the ENA (this happens automatically) and the associated certificate has to be imported in the browser or operating system.

Operating Mode

The PKI system works as follows (simplistically):

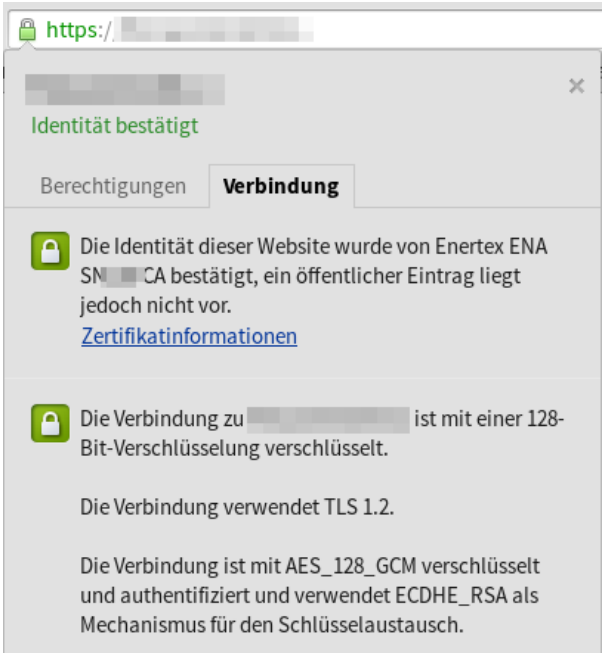
- The certification authority (CA) creats and signs certificates for the HTTPS Reverse Proxy and the OpenVPN server and the iOS Profile Generator.
- The certificates are not secret. The respective server certificate is sended to the client while connecting (HTTPS/OpenVPN). Therewith the server is identifying itself to the client.
- If the client knows the certification authority (CA), he is able to check the realness of the signature from the server certificates and therefore to ensure that he is not talking to an attacker.

Import

The pros of the import of the CA certificates (ca.crt) in the browser (or operating system) are:

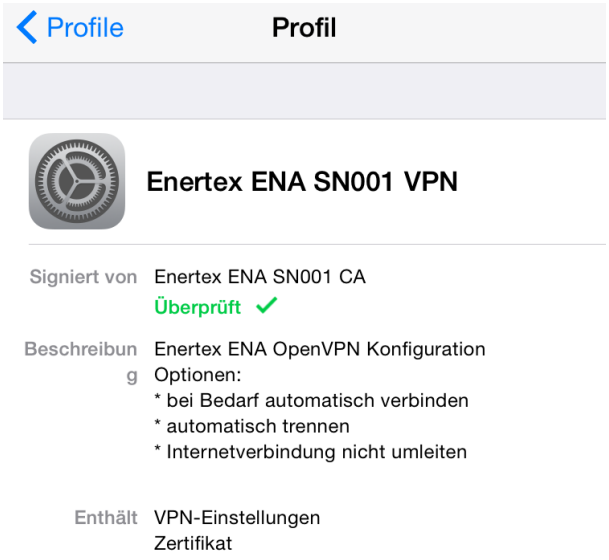
- The connection to the HTTPS Reverse Proxy can be known as safe and there is no need for adding exception rules. So it is ensured, that a real connection to ENA is assembled and not to potential attacker.

(Picture 8).



Picture 8: Chrome shows the identity of webside as confirmed

- The origin of the profile can be checked while importing to OpenVPN profile via iOS. (Picutre 9)



Picture 9: iOS Profile: Origin checked

Chrome

The CA certificate can be imported via Chrome (version 39) as follows: „Settings → Show additional settings → HTTPS/SSL → Manage certificates → Certification authorities → Import...“. Then choose ca.crt. With the question if you can trust the certification authority you have to choose „Trust this certificate of identification of websides“.

Firefox

The CA certificate can be imported via Firefox (version 35) as follows: „Settings → Extended → Certificate → Show certificate → Certification authorities → Import“. Then choose ca.crt. With

the question for what purpose the certification authority should be trusted you have to choose „Trust CA for identifying websides“.

iOS

With iOS (version 8 and 9) the certificate can be downloaded directly with Safari, the dialog of import starts automatically.

Expert-Options

In the expert options the certification authority can be new initialised. Thereby all former created certificates and OpenVPN entries are invalid! All existing OpenVPN connections will be unlinked!

HTTPS Reverse Proxy

Via the Reverse Proxy you can access to a host in the local net from outside using a domain name. From the user's view is this comparable with the port forwarding of a firewall. The Reverse Proxy encrypts however the connection and the access is password controlled. You can only access the HTTP/HTTPS services via the local net.

Note

In the Internet router a port from outside has to be transferred to the ENA final port 443 (TCP) for using the HTTPS Reverse Proxy.

User Administration

The login details are here fixed for the access of the HTTPS Reverse Proxy.

Connecting Domain Name

For the access of a host in the local network an already configurated DDNS domain name has to be connected. Not more Reverse Proxys than existing DDNS domain name can be used.

(Picture 10).

Picture 10: Example of a HTTPS Reverse Proxy connection to a synology diskstation

OpenVPN

OpenVPN is a program which can assemble a virtual private network (VPN) via an encrypted TLS connection. For the encryption the OpenSSL library is used.

Note

In the internet router a port from outside has to be transferred to ENA final port 1194 (UDP) for using the OpenVPN.

User Administration

The ENA can administrate a lot of optional OpenVPN user. But only ten users can be connected at the same time. If a OpenVPN user is added, the PKI subsystem creates a PKCS#12 data and together with a configuration data for OpenVPN client offered to download. The PKCS#12 data file is encrypted with a specified password and therewith the client is able authenticate to the server. The creation of the PKCS#12 data file takes upto two minutes.

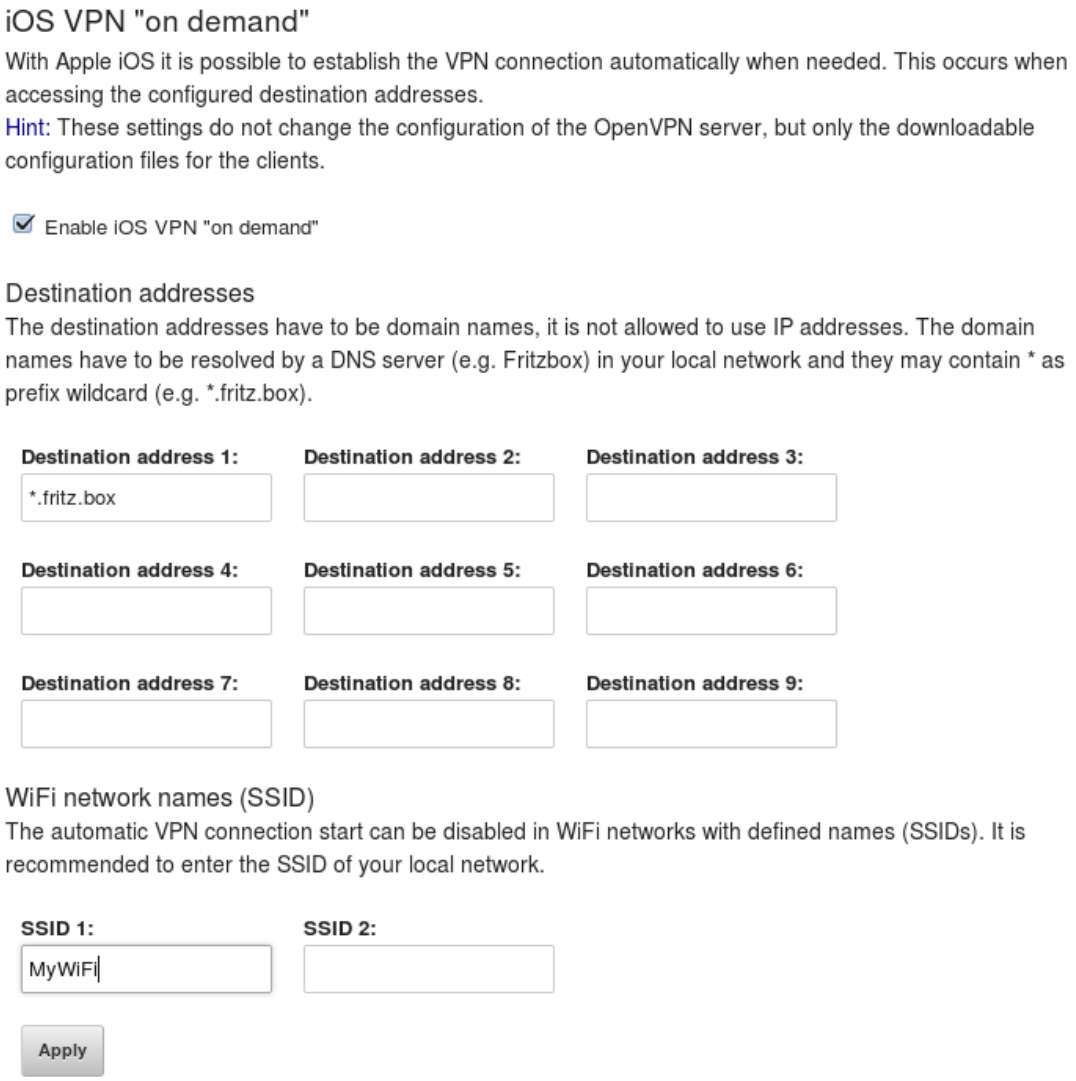
Download of Configuration Data Files

In order to download the configuration data files for the OpenVPN clients you have to act as follows:

- Choose the favoured **user** from Drop Down Menue
- **Do not unlink:** If this option is activated, the OpenVPN connection of the client persists indefinitely. This could be an option for stationary clients (PCs). If you do not activate this option the OpenVPN connection is finished automatically after a timeout. Generally is this desired for mobile Clients (Android/iOS) because the battery life is negatively influenced by the OpenVPN connection in perpetuity.
- **Internet:** Is this option activated, the OpenVPN client tries to detour the whole internet traffic via the VPN. This is e.g. reasonable, if you are locked in a public WLAN and you might prevent that the user of the WLAN or a third person can observe the internet traffic. Note: If the internet connection to the ENA is interrupted, it could happen that the internet without VPN is continued via the normal connection.
- Push the button for the favourite configuration data file. The following data files are available:
  - **Client Config.:** The configuration data file can be used to current operating systems (Windows/Mac OS/Linux/Android) for the standard clients.
  - **IOS Config.:** A VPN profile can be imported very easily in iOS via iOS mobile config. Note: At first import the CA certification in iOS and install the App „OpenVPN connect“!
  - **PKCS12:** The PKCS12 data file contains only the certification with which the user can be identified towards the VPN server. This data file is additionally necessary for some clients.

iOS VPN "on demand"

With Apple iOS it is possible the start the VPN connection automatically as needed. This happens as soon as you access the configured destination addresses (Picture 11). The destination addresses have to be domain names, it is not allowed to use IP addresses. The domain names have to be resolved by a DNS server (e.g. Fritzbox) in your local network and they may contain * as prefix wildcard (e.g. *.fritz.box). When using the wildcard the VPN is started for all addresses in the destination network, e.g. eibpc.fritz.box., nas.fritz.box or homeserver.fritz.box.



Picture 11: The VPN is automatically connected on access to these addresses

Furthermore the automatic VPN connection start can be disabled in WiFi networks with defined names (SSIDs). It is recommended to enter the SSID of your local network, so VPN is disabled when you are coming home.

Note

These settings do not change the configuration of the OpenVPN server but only the downloadable configuration data files for the clients. If here something is changed the configuration data file has to be re-imported to the client.

Experts Options

Connection Settings

If another public port than the standard port is sent while port forwarding in the internet router so the port has to be indicated. As OpenVPN server address the first DDNS domain is automatically used.

Automatically Unlink Connection

The connection is automatically unlinked if in a certain time (in seconds) not more than a certain data volume (kBytes) was transferred.

OpenVPN Client Setup

iOS 8.3

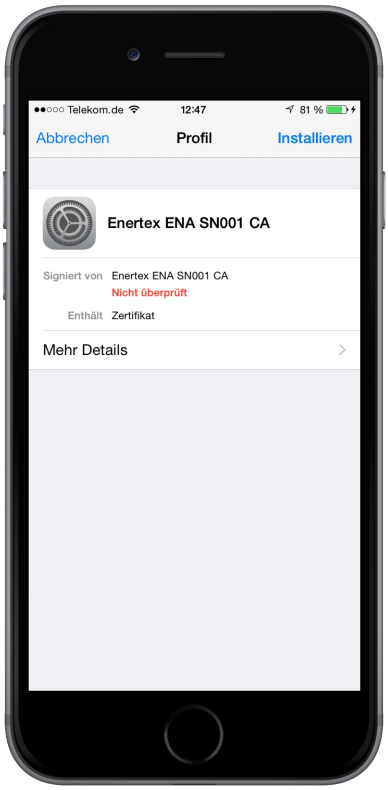
Depending on iOS version the procedure can differ from the manual.

First install the app „OpenVPN Connect“ from Apple app store.

Open the ENA web interface with the Safari browser (don't use alternative browsers!).

On the page „Public Key Infrastructure“ press the button „Download CA certificate“.

A dialog to install the certificate is opened automatically. The installation has to be confirmed with the telephone code. Follow the instructions:

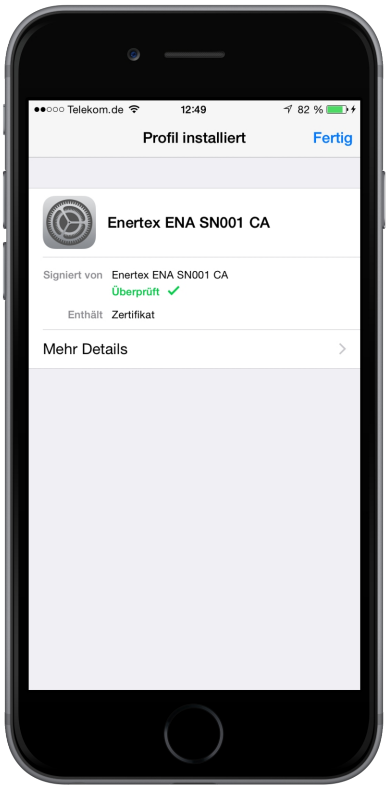


You are prompted to install the certificate.

Enter the phone code.

Press „Install“

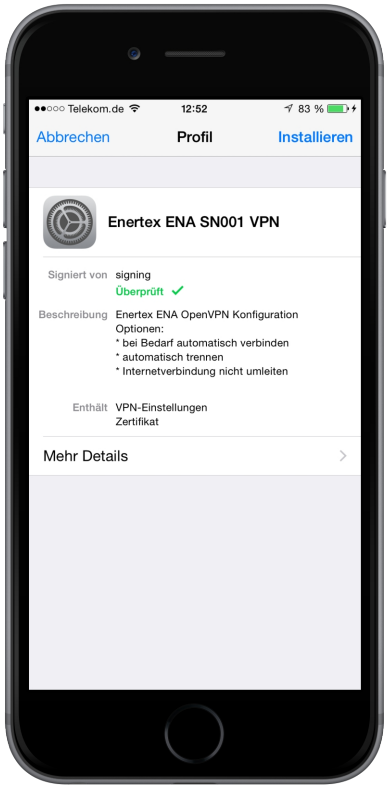
Again confirm with „Install“



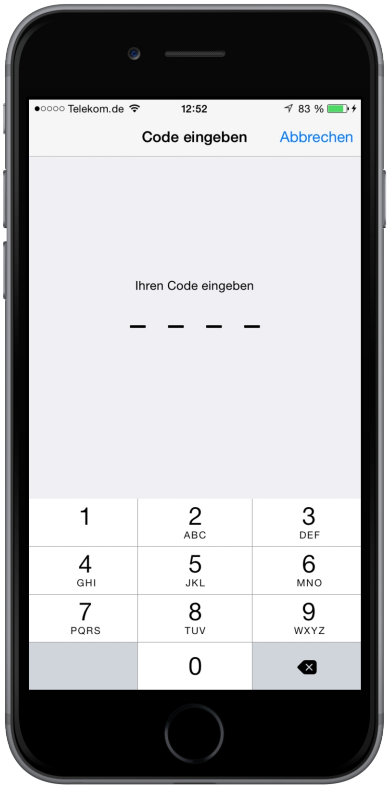
The certificate has been installed. Press „Done“

Go to the page „OpenVPN, chose the desired user and press the button „iOS config“:

It automatically opens a dialog to install the configuration. The installation must be confirmed with the phone code. Follow the instructions. You must also specify the password with which the user has been created on the ENA:



Step 1: You will be prompted to install the VPN profile. It is displayed as "Trusted".



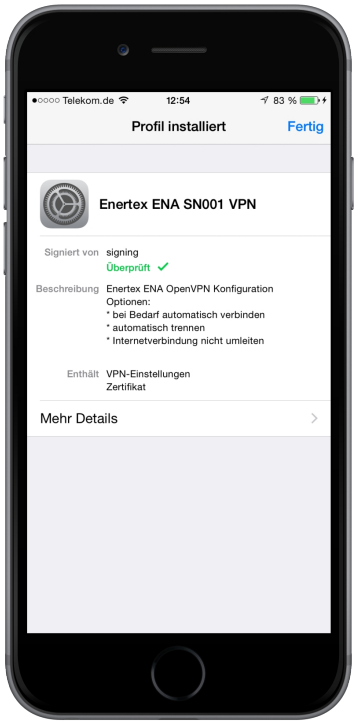
Enter your phone code

Step 2: This note specifies that the network traffic is passed through the ENA . Press "Install" and ...

… confirm again with „Install“.

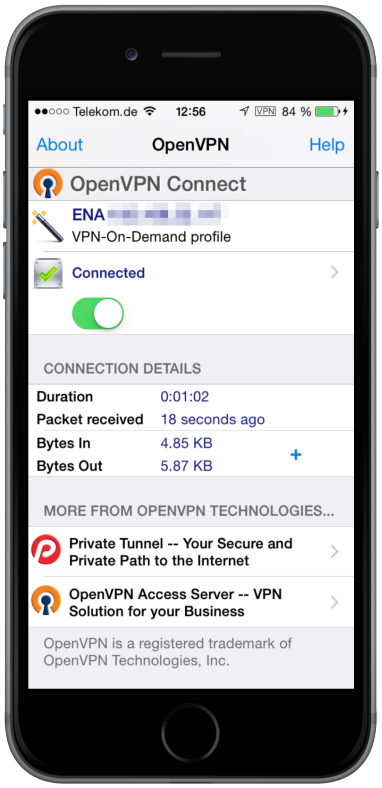
Step 3: Enter the password that was assigned when creating the VPN user in the ENA...

… and press „Next“.



The VPN profile has been installed. Press „Done“.

Test the connection in the iPhone settings at „General → VPN“ (not at „VPN“ in the main menu!).



As soon as the VPN is connected, you can check the connection details in the „OpenVPN Connect“ app.

Android 5.1

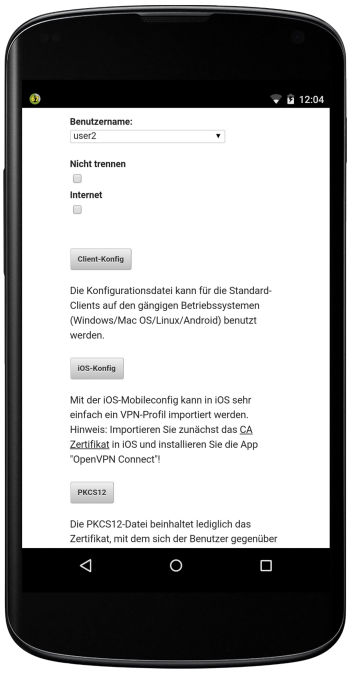
Depending on Android version and device manufacturer the procedure can differ from the manual.

At first you have to enable the display lock in the Android settings at „Security“.

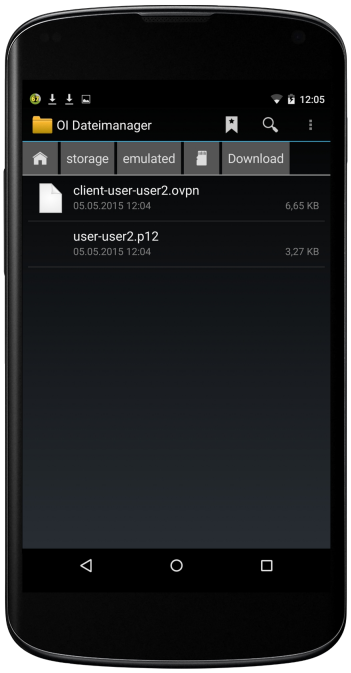
Then install the app „OpenVPN Connect“ from the Google Playstore.

Open the ENA web interface with the Chrome browser.

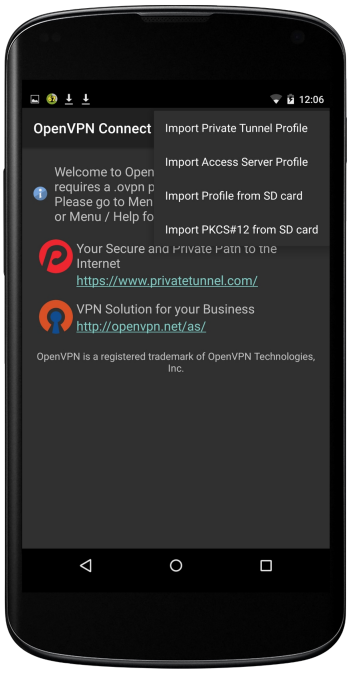
Go to the page „OpenVPN“, chose the desired user and press the button „Client config“ to download the respective file. After the download has finished press the button „PKCS12“ to also downlaod this file. Both files have to be imported in the „OpenVPN Connect“ app afterwards:



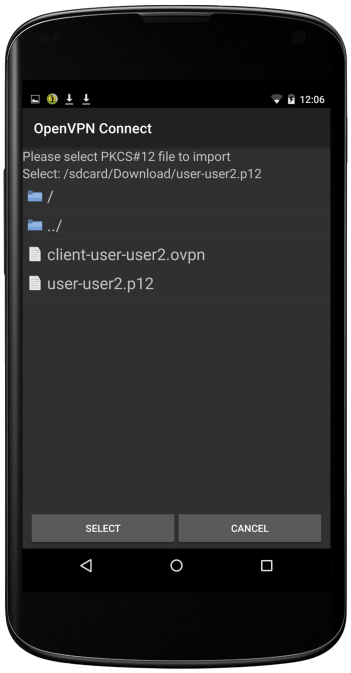
Step 1: Open ENA web interface in Chrome browser.



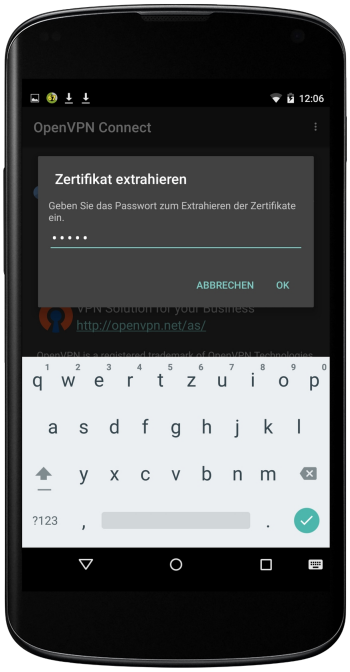
Both downloaded files are in the „Download“ folder now.



Step 2: Open the „OpenVPN Connect“ app and chose „Import → Import PKCS#12 from SD card“ from the menu. This way the user certificate will be imported to the Android Keystore.

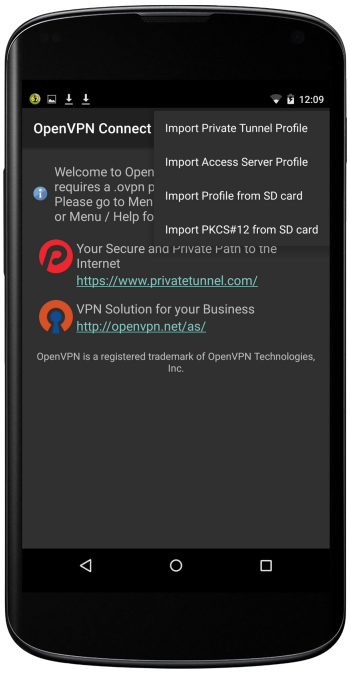


Step 3: Chose the previously downloaded certificate with the file name „user-username.p12“ in the Download folder and press „Select“.

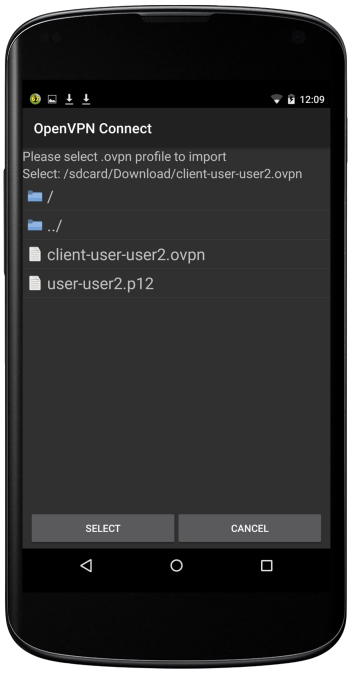


Step 4: Enter the password that was assigned when creating the VPN user in the ENA.

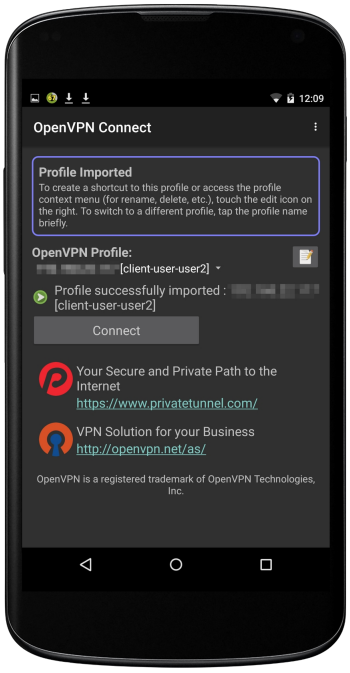
Step 5: Give any desired name to the user certificate. Later it can be selected by this name in the Android Keystore.



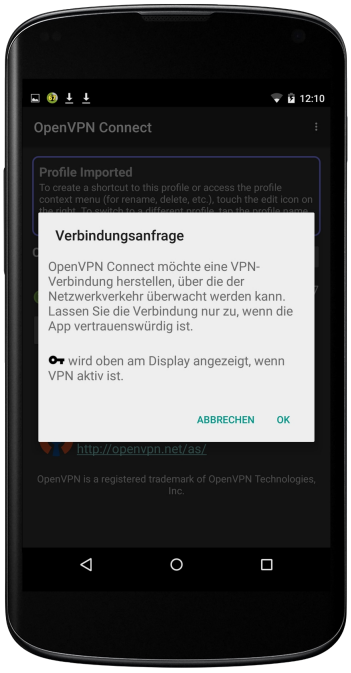
Step 6: Chose „Import → Import Profile from SD card“ from the menu. This way the OpenVPN settings are imported.



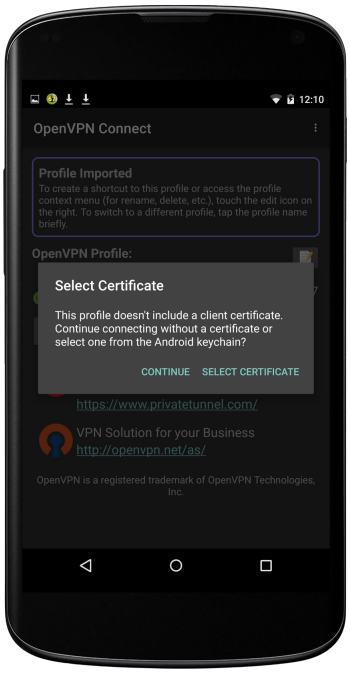
Step 7: Chose the previously downloaded config file with the file name „client-user-username.ovpn“ from the „Download“ folder and press „Select“.



Step 8: After the successful import of the profile, the connection can be started the first time.

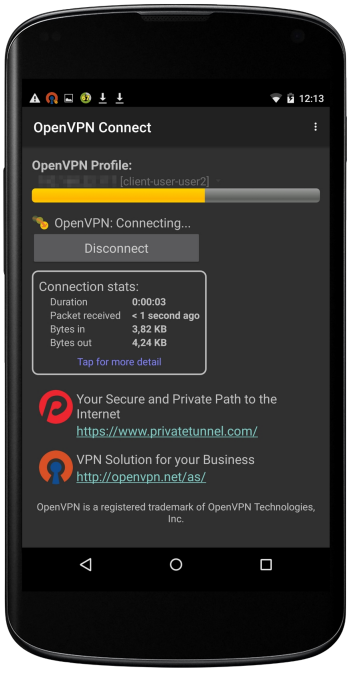


Step 9: Android shows a note, that a VPN connection will be started. Confirm with „OK“.

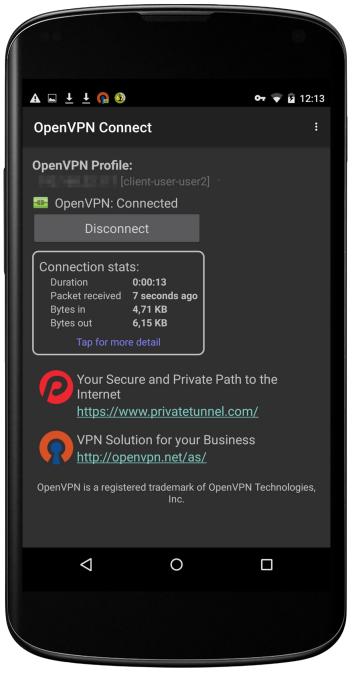


Step 10: At first connection attempt a user certificate must be chosen for the connection. Therefore press „Select Certificate“...

… and chose the previously installed certificate. Confirm with „Allow“.

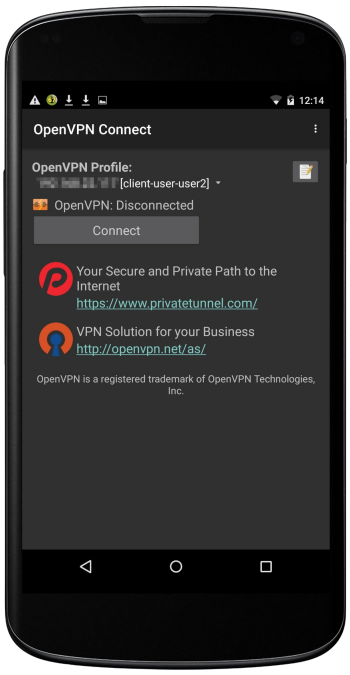


The connection is started...

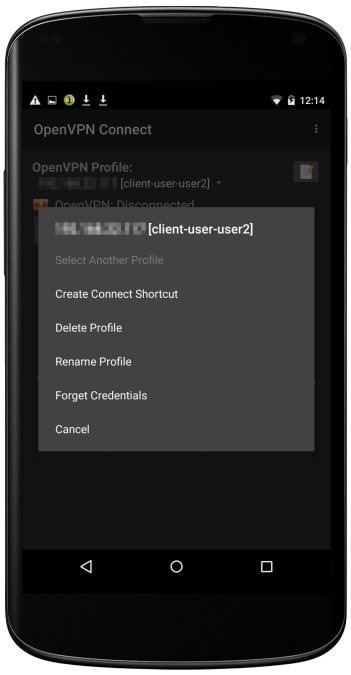


… and is connected now. In the status bar a key symbol is shown. Now you can use any desired app that needs a connection to your network. The connection can be shut down with the „Disconnect“ button.

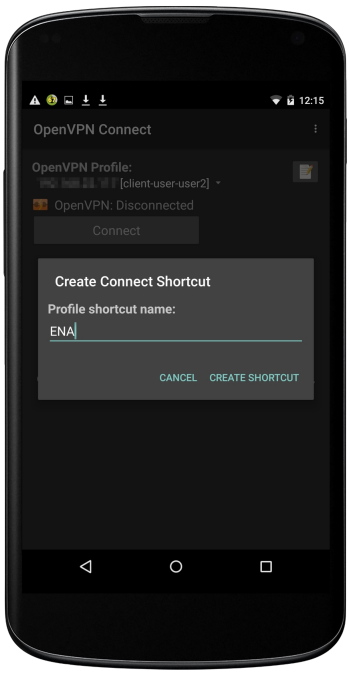
Optionally a widget can be added to the Android home screen for faster connection start:



Step 1: When the VPN is disconneted press the button to modify the connection (the small notepad icon)...



… and chose „Create Connect Shortcut“.



Step 2: Enter a name for the widget.

The widget is placed on your home screen. Pressing the symbol starts the connection.

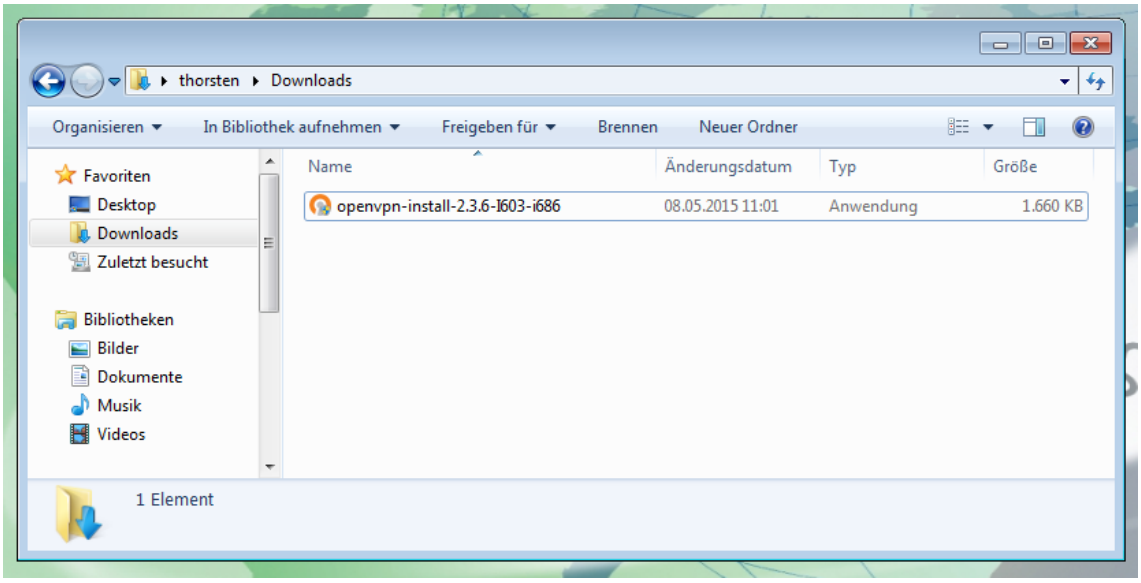
Hinweis

After importing a user certificate to the Keystore, after each reboot Android shows a notification that the network may be monitored. This cannot be disabled.

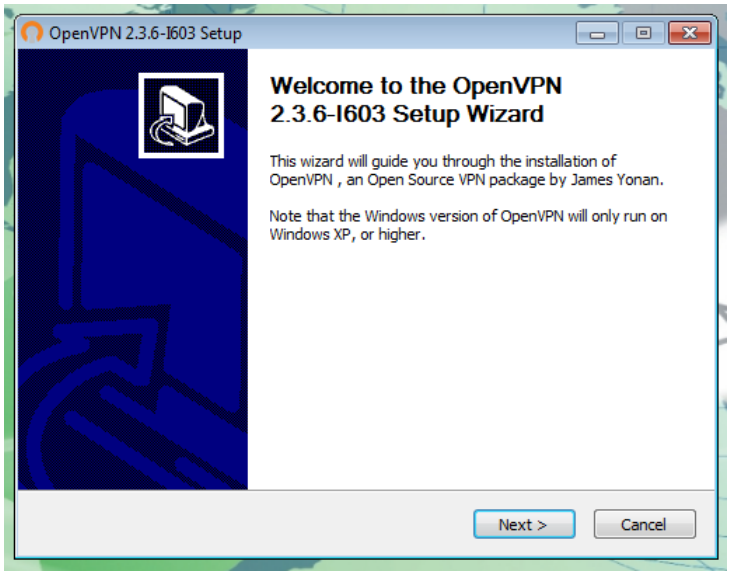
Windows 7

First download the installer for the application „OpenVPN GUI“ from the OpenVPN website (https://openvpn.net/index.php/open-source/downloads.html):

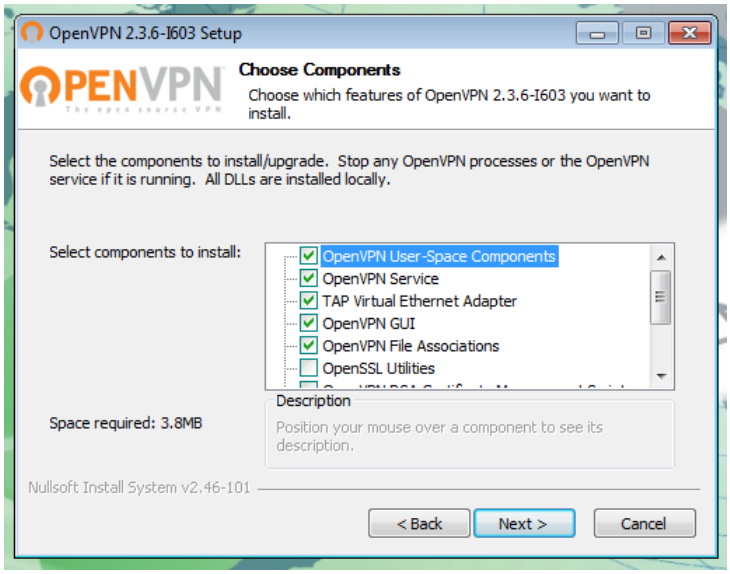
The installer can be found in the Download folder:

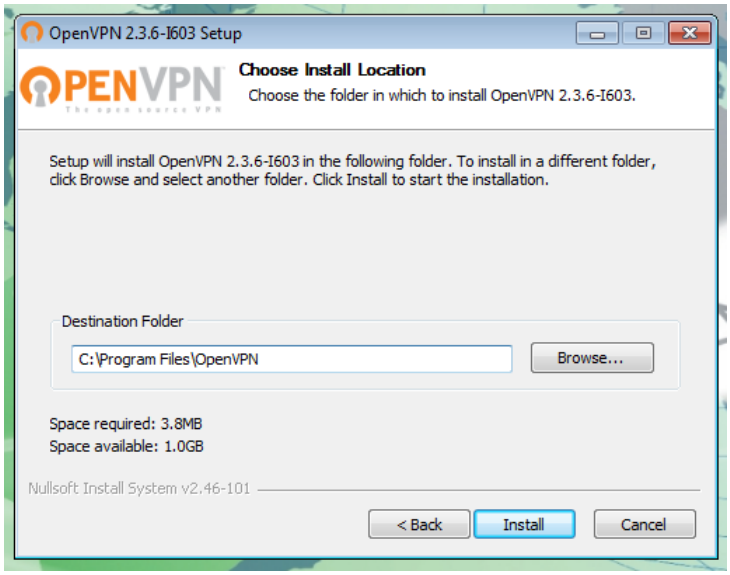


Install the application:



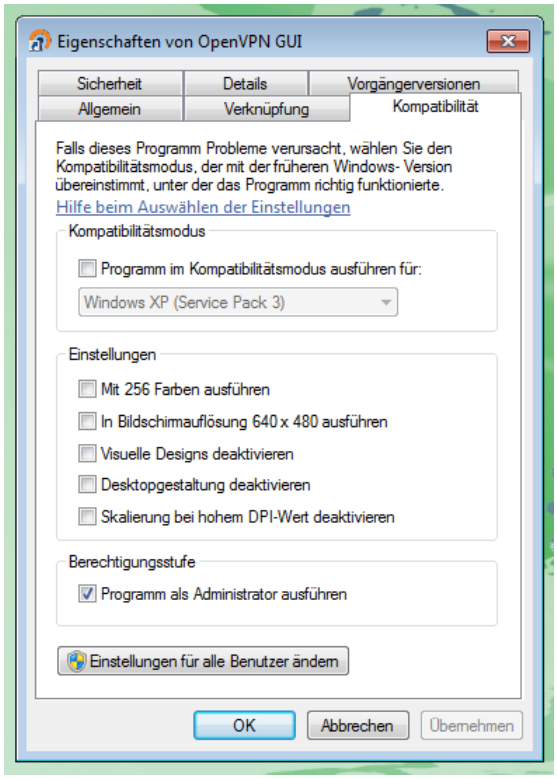
Standard settings can be used to install:



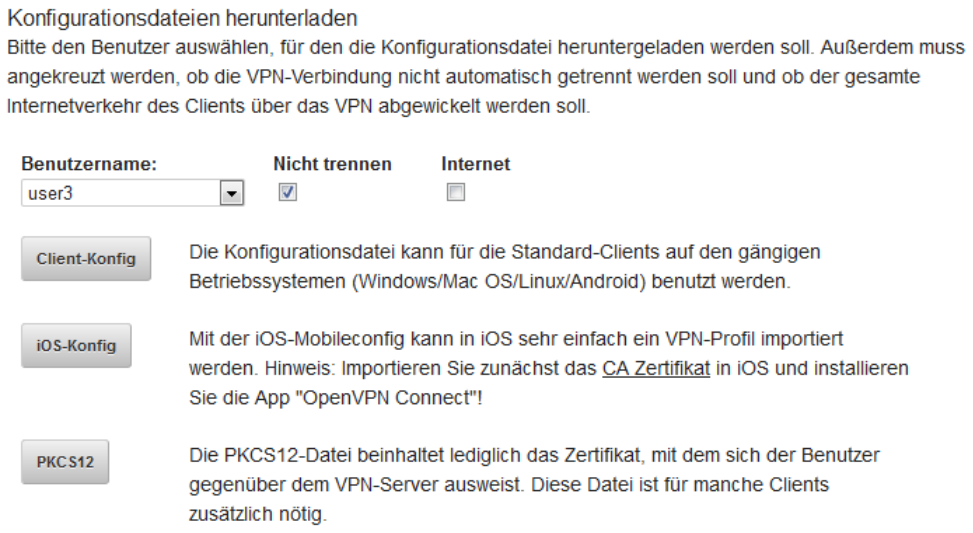


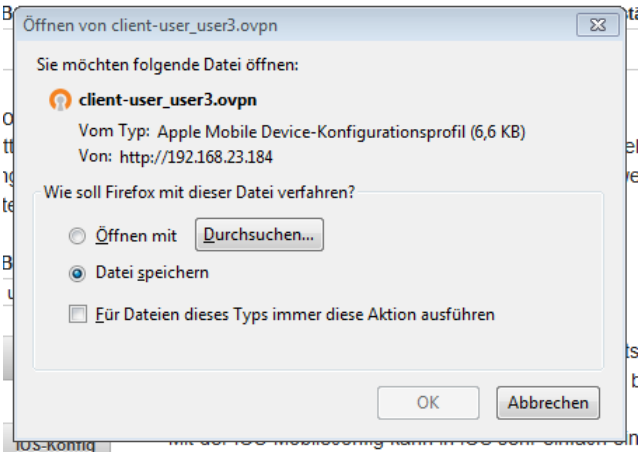
After installation the application symbol is on the desktop:

Make sure that the program is run as administrator. Therefore use the right mouse button to open properties of the symbol and set the option:

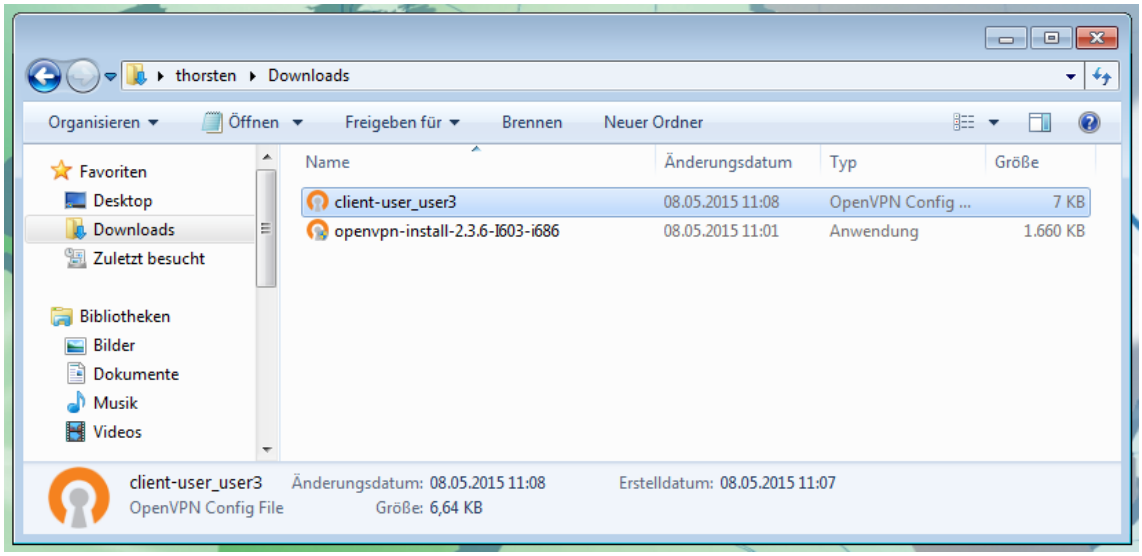


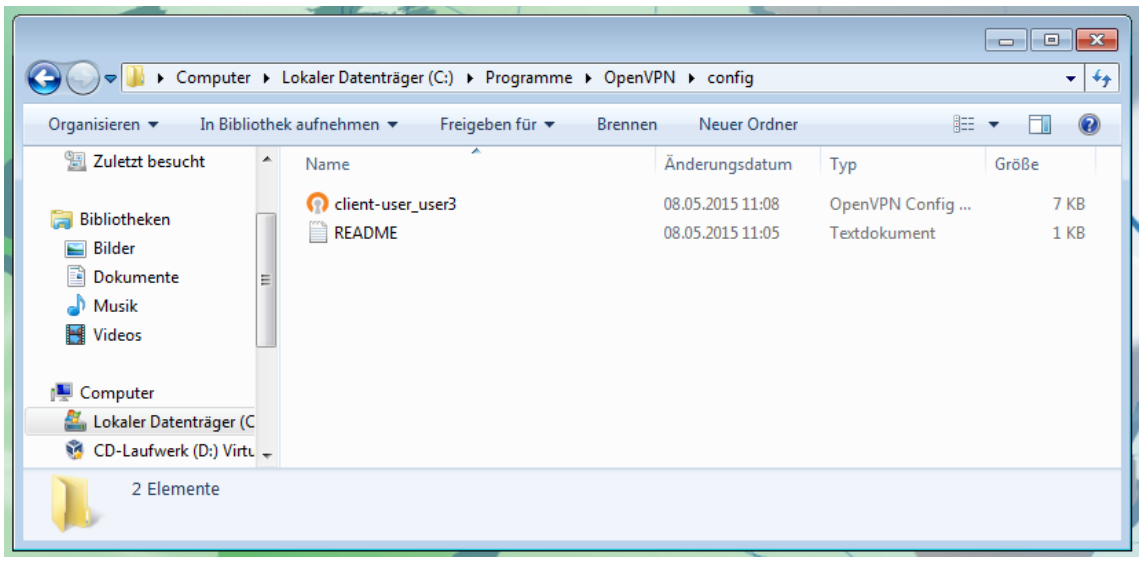
Open the ENA web interface with a browser. On the page „OpenVPN“ chose the desired user. If the connection should not be disconnected automatically set the checkmark at „Stay connected“. Afterwards press the „Client config“ button to download the configuration file:



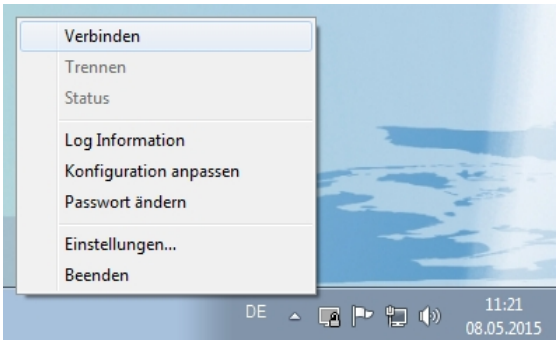


Copy the downloaded file from the Download folder to the folder „C:\Program Files\OpenVPN\config“:

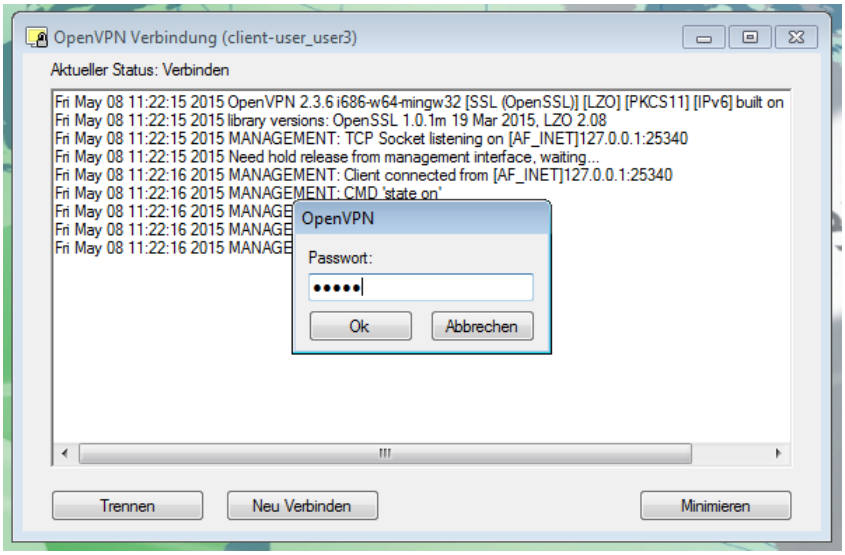




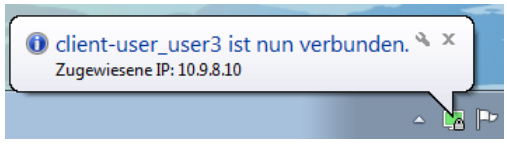
Now you can connect to OpenVPN. Therefore click on the OpenVPN GUI icon in the systray with the right mouse button and chose „Connect“:



You will be prompted for the password that was assigned when creating the VPN user in the ENA:



Afterwards you are connected:



KNX Connection

Via KNX group addresses specified functions can be triggered e.g. the OpenVPN server can be started or stopped. Thereby the IP address of the KNXnet/IP interface or of a KNXnet/IP router has to be configurated in order to build a tunneling connection to the KNX bus.

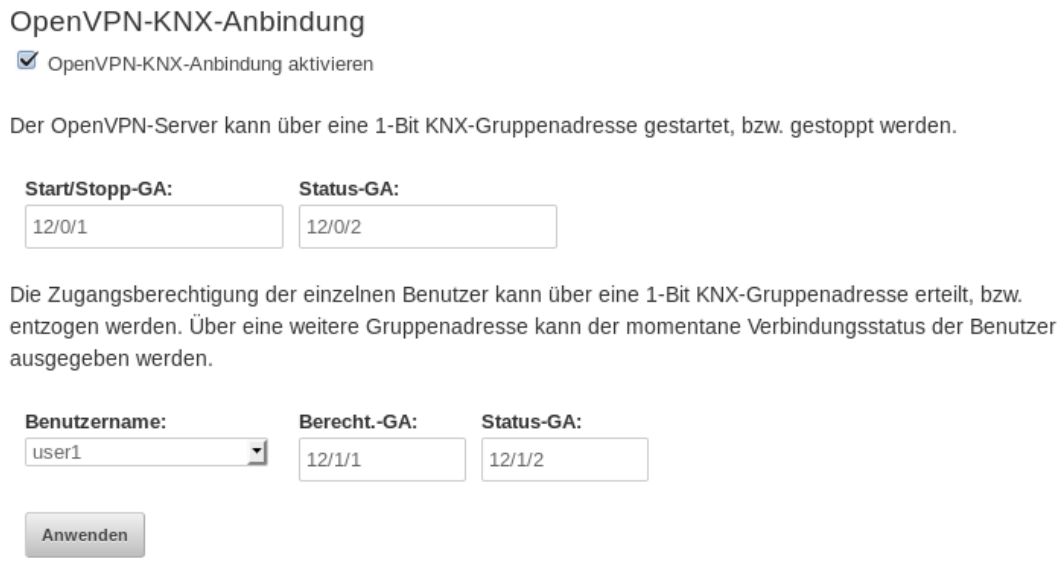
KNXnet/IP Connection

Here the IP address of the KNXnet/IP interface or of the KNXnet/IP router has to be specified. (Picture 12)

Picture 12: KNXnet/IP Tunneling Connection

OpenVPN-KNX connection

The OpenVPN server can be started or can be stopped via a 1 bite KNX group address. Via another 1 bite KNX group address an actual status can be output. (Picture 13)



Picture 13: OpenVPN KNX Connectivity

For up to 16 users the access authorisation via an 1 bite KNX group address can be instructed respectively detracted.

Via another group address the actual connection status of the users can be output.

Note

If the access authorisation will be dispossessed of the user, the connection of the user is not unlinked, whether the user is just logged in.

The refreshing of the connection status of the user can be delayed up to two minutes.

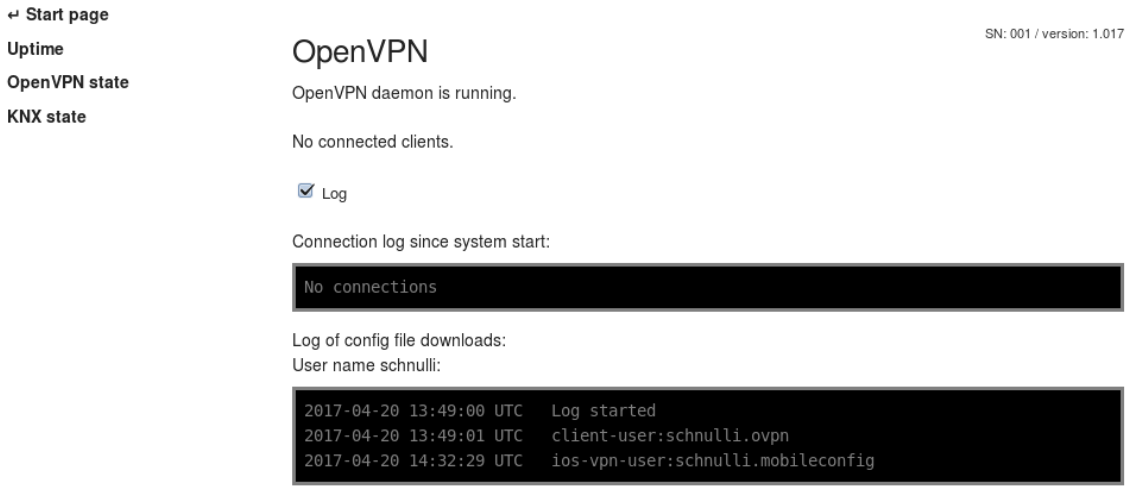
Administration

Change login to the Webadmin interface

Here the login details for the administrative web surface of the ENA can be changed.

Public area

ENA can provide a public area with status information on it's web interface. These information are available without password protection inside the LAN. For example it can be shown when OpenVPN config files have been downloaded:



Reboot

The device will be restarted. The process takes about one minute.

Restore Factory Defaults

The factory defaults will be restored and the device will be restarted. The process takes about two minutes.

Note

If the webinterface no longer reachable, the factory defaults can be restored as follows: While operating (LED flashing every second); keep pushing the resetbutton min. 10 seconds; as soon as the LED is flashing faster; you can stop pushing the button. Then the ENA restarted and can restore the factory defaults.

Update Firmware

Choose and upload a firmware upgrade data file. The device restarted after the upgrade. The process takes about two minutes.

Save the Configuration

The current configuration can be saved and can be downloaded in a data file. It can be restored anytime.

Note

In the safety are contained neither certifications nor OpenVPN users.

Restore Configuration

Restore a former saved configuration.

Änderungsverzeichnis

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

- Initialversion

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

- Anpassungen für Firmwareversion 1.000

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

- Funktionsbeschreibung erweitert

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

- OpenVPN-Einrichtung auf Clients erweitert

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

- OpenVPN-Einrichtung auf Clients erweitert

6: 1.6.2015 , C. Sykosch

- Sprachliche Korrekturen

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

- Korrekturen

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

- Korrekturen
- OpenVPN on demand Kapitel aktualisiert.

9: 8.10.2015 , Dipl.-Ing. (FH) T. Mühlfelder

- OpenVPN on demand Kapitel verbessert

10: 16.6.2016 , Dipl.-Ing. (FH) T. Mühlfelder

- Gira DynDNS Zugangsdaten erläutert

11: 21.4.2017 , Dipl.-Ing. (FH) T. Mühlfelder

- Öffentlicher Bereich (ab v1.017) hinzugefügt