SIEMENS

Ingenuity for life

Setting up a Secure VPN Connection between a PC and LOGO! 8

LOGO! 8, LOGO! CMR

https://support.industry.siemens.com/cs/ww/de/view/109747067

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Task and Solution

1.1 Task

The LOGO! controller is an intelligent logic module from Siemens for small automation projects, for example, in building automation. The entire LOGO! 8 product family is equipped with Ethernet interfaces and thus offers new options of communication. LOGO! modules can communicate with each other via Ethernet and the Ethernet standard also makes remote access possible, for example, for remote maintenance.

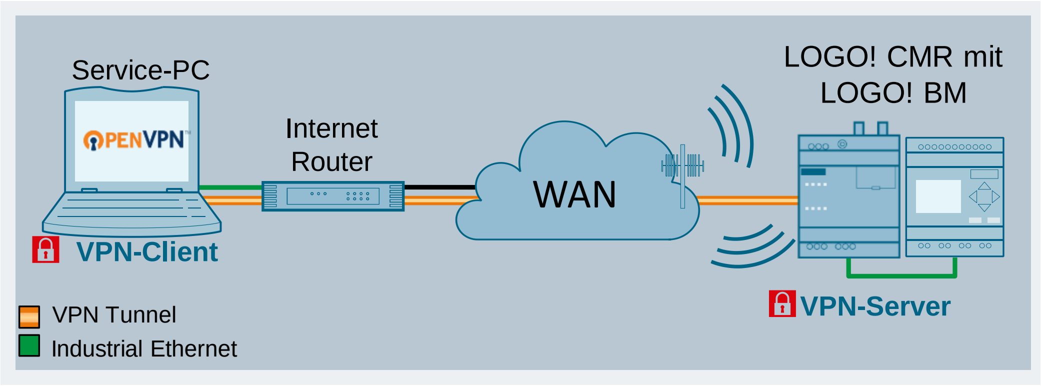
The task is to establish a secure connection between a service PC and LOGO! CMR (Communication Module Radio) via Internet and the mobile wireless network.

1.2 Solution

General overview

The following graphic shows an approach in order to realize a secure connection between a PC and LOGO! .

Figure 1-1



The connection between the service PC and LOGO! is secured by a VPN tunnel.

In this example, the service PC and LOGO! CMR form the two tunnel end points for the secure connection. LOGO! CMR acts as VPN server, the PC as VPN client.

Access to LOGO! CMR (VPN server) from the WAN is predefined by the use of a static WAN IP address.

WAN access on the client side is flexible; the IP address of the WAN access is not relevant.

The role distribution when establishing the VPN tunnel is specified as follows:

Table 1-1

Component	VPN role
Service PC	Initiator (VPN client); starts the VPN connection
LOGO! CMR	Responder (VPN server); waits for VPN connection

Logo!

LOGO! Siemens is an intelligent logic module and ideally suitable for the realization of simple automation tasks in industry and building technology. The use of expansion modules enables LOGO! to control even complex plants without any problems.

Using LOGO! CMR in combination with the LOGO! 8 basic modules (BM) makes it possible for you to monitor and control distributed plants and systems via text messages. You can remotely access the web interface of LOGO! CMR and LOGO! BM via mobile wireless network. The remote access makes it possible, for example, to install the LOGO! BM program remotely.

Note You can access the LAN interface of LOGO! CMR via the VPN tunnel and you can therefore also access LOGO! BM remotely. If you want to communicate with LOGO! BM via LOGO! CMR, you have to enter the local IP address of LOGO! CMR as default router in LOGO! BM.

LOGO! CMR offers the following functions for secure remote access via mobile wireless network:

- OpenVPN (version V2.3.11) for remote maintenance
- Support of OpenVPN server function in pre-shared key mode
- Implementation of OpenVPN in routing mode
- Encryption of data to be transferred with the AES-128 CBC method.
- Authentication of the connection partners via the SHA-256 hash algorithm
- Support of the DynDNS function "DynDNS.org" and "NoIP.com" DynDNS providers are supported.
- Support of https function

1.3 Characteristics of the solution

- Economical and intuitive remote control and remote monitoring of LOGO! 8 logic module via text message and/or email.
- Convenient commissioning and diagnostics via the web-based management.
- Secure remote access to LOGO! CMR and the connected LOGO! 8 basic module.
- Via an OpenVPN connection, it is possible to directly access the LOGO! basic module for routing via LOGO! CMR. This makes it possible to access the LOGO! basic module web pages and to carry out an upload or download of the program to/from the LOGO! basic module.
- Can be used internationally thanks to communication via GSM, UMTS and LTE networks.
- Suitable for applications in industrial and industry-related branches.

2 Configuration and Settings

2.1 Prerequisites for the use of

SIM card for LOGO! CMR

To be able to use the mobile wireless network communication via the WAN interface of the LOGO! CMR you need a cell phone contract with a suitable mobile wireless network provider.

If you want to use OpenVPN via to the mobile wireless network, you have to observe the following prerequisites for the data contract:

- The SIM card requires a public, static IP address in the mobile wireless network. Alternatively, you can also use DynDNS.
- The SIM card has to be enabled for mobile data communication.
- The SIM card has to be at least enabled for the "OpenVPN" und "https" data services.

Note

If you are using a SIM card with a public and dynamic IP address, remember that this IP address changes as soon as LOGO! CMR dials into the mobile wireless network again. If the IP address changes again and again, you have to continuously adapt the configuration file for the OpenVPN (see chapter 2.3.1).

If you are using a SIM card with a public and dynamic IP address, you should use DynDNS. Using DynDNS makes it possible not to directly connect to the possibly changing public IP address but for the current IP address to always be resolved to the current IP address via the DNS name.

OpenVPN client

The OpenVPN client software on the service PC has to support the following functions:

- OpenVPN V2.3.11 or higher
- The pre-shared key method

Note

You can find numerous "OpenVPN client" software packages on the internet that can be downloaded for free or can be purchased.

Browser

In order to configure LOGO! CMR you can use all common browsers. It is recommended to always use the most current browser version. LOGO! CMR is released for the following browsers:

- Internet Explorer Version 10 and 11
- Microsoft Edge Version 38.0
- Mozilla Firefox Version 47.0
- Google Chrome Version 54.0
- Apple Safari V9

Note If you access LOGO! CMR remotely, directly via the IP address using https and not via the VPN tunnel, you have to use a browser that allows communication via one single connection. In this case, Mozilla Firefox is recommended.

Logo! BM

The configuration of the LOGO! basic module is not part of this documentation. It is assumed that you have downloaded a program into LOGO! BM and configured the IP address and the default router in accordance with Table 2-1.

Note If you would like to access LOGO! BM and LOGO! CMR via the OpenVPN tunnel, check that the local IP address of LOGO! CMR in LOGO! BM is entered as default router. Otherwise it is not possible to communicate via the OpenVPN tunnel.

2.2 Preparing environment

2.2.1 Required components and IP address overview

Software packages

The service PC requires a suitable “OpenVPN client" software. Install it onto your service PC (OpenVPN client).

If you load a program onto LOGO! BM or you would like to obtain it via remote access, you will additionally need the "LOGO! Soft Comfort V8.1" engineering software.

Required devices and components

For the configuration you need the following components:

- A service PC with the following installed software packages:
  - Optionally the "LOGO! Soft Comfort V8.2" software
  - A "OpenVPN client" software, e.g., "OpenVPN GUI"
- A configuration PC with the following installed software packages:
  - a browser,
  - a text editor, e.g., Notepad++
- A SIM card of your mobile network operator that meets the requirements (see chapter 2.1).
- A DSL access and a DSL router
- A LOGO! 8 basic module and the LOGO! CMR 2020 communication module
- A LOGO! Power 24 V / 1.3 A (or similar module)
- Optionally the LOGO! TDE text display, when the basic module does not have its own LCD display.
- The required network cables, TP cable (twisted pair) according to the IE FC RJ45 standard for Industrial Ethernet.

Note Instead of the DSL access you can also use another Internet access (e.g., UMTS). You also can use LOGO! CMR 2040.
The configuration described below explicitly refers to the components listed in "Required devices and components".

Note Only insert the SIM card into the LOGO! CMR once you have configured the mobile wireless settings in LOGO! CMR
(according to chapter 2.2.2). Otherwise your SIM card may be blocked due to an incorrect PIN.

IP addresses

Assigning the IP addresses for this example is specified as follows:

Figure 2-1

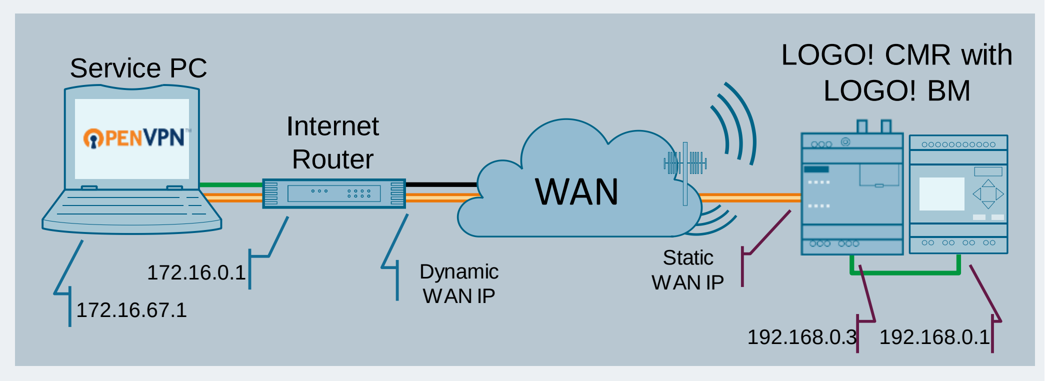


Table 2-1

Component	Port	IP address	Router	Subnet mask
Service PC	LAN port	172.16.67.1	-	255.255.0.0
Router on VPN client	LAN port	172.16.0.1	-	255.255.0.0
Router on VPN client	WAN port	Dynamic IP address of provider	-	Assigned by provider
LOGO! CMR	WAN port	Static IP address of provider	-	Assigned by provider
LOGO! CMR	LAN port	192.168.0.3		255.255.255.0
LOGO! 8 BM	LAN port	192.168.0.1	192.168.0.3	255.255.255.0
Configuration PC (not displayed in the graphic)	LAN port	192.168.0.4		255.255.255.0

Setting up the infrastructure

Connect all the components involved in this solution with each other.

Table 2-2

Component	Local port	Partner	Partner port
Service PC	LAN port	Router on VPN client	LAN port
LOGO! CMR	LAN port	LOGO! BM	LAN port

2.2.2 Basic configuration of LOGO! CMR

Opening web-based management

Connect to the Web user interface of the LOGO! CMR via the configuration PC.

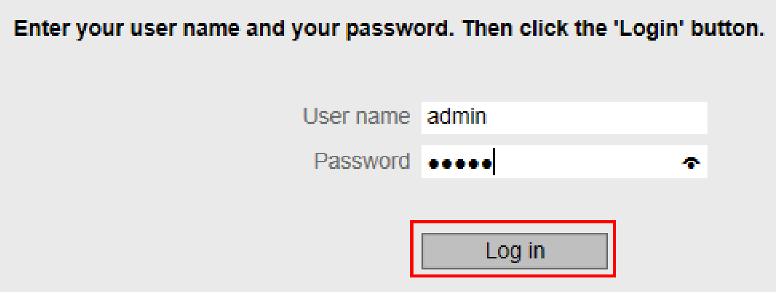
Open the web-based management via the address "http://192.168.0.3".

Web-based management login

When you log in for the first time or after setting to factory settings, the login data is specified as follows:

- Name: admin
- Password: admin

1. Enter name and password into the appropriate input fields.
   Click the "Login In" button.



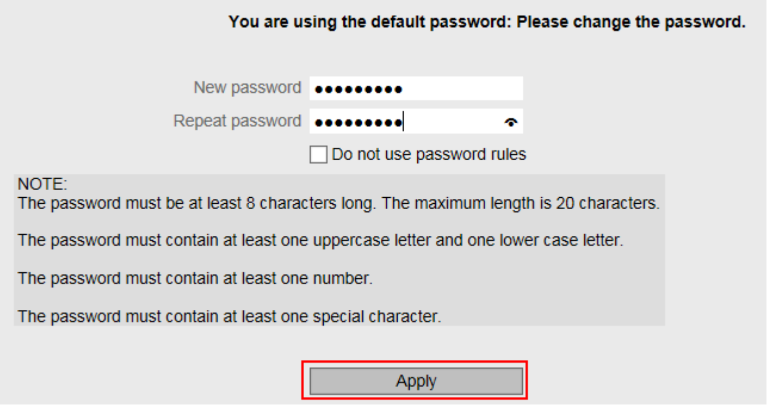
Enter your user name and your password. Then click the 'Login' button.

User name admin

Password ●●●●●

2. When you log in for the first time or after setting to factory settings, you are prompted to change the password.
   Enter the new password. The new password has to fulfil at least the following requirements:
   - At least eight characters long
   - One special character
   - Upper and lower case
   - One number

   Click the "Apply" button to complete the process and to activate the new password.



You are using the default password: Please change the password.

New password ●●●●●●●●●

Repeat password ●●●●●●●●●

□ Do not use password rules

NOTE:
The password must be at least 8 characters long. The maximum length is 20 characters.

The password must contain at least one uppercase letter and one lower case letter.

The password must contain at least one number.

The password must contain at least one special character.

3. When you have logged in, the CMR start page will appear in the web browser. The start pages gives you an overview of the operating status of the device.

Result

The password for the "admin" user has been changed. In future, log in with the changed password.

Setting up mobile communications

The following access parameters are required for access to the mobile wireless network and to the mobile wireless services:

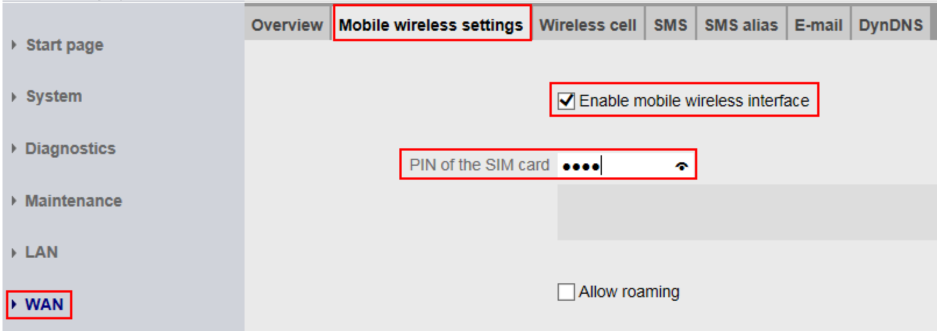
- PIN to protect the SIM card from unauthorized use of the device
- APN as name of the gateway between the mobile wireless network and, for example, the Internet.
- Access data to APN

These access parameters can be obtained from your mobile network operator.

To set up the mobile wireless network, proceed as follows:

1. Go to “WAN > Mobile wireless settings” menu.

2. In order to make the mobile wireless interface ready to work, enable the "Enable mobile wireless interface" checkbox.
   In order to store the PIN number of the SIM card in CMR, enter the PIN number in the input field. If you are using a SIM card without PIN, leave this field empty.

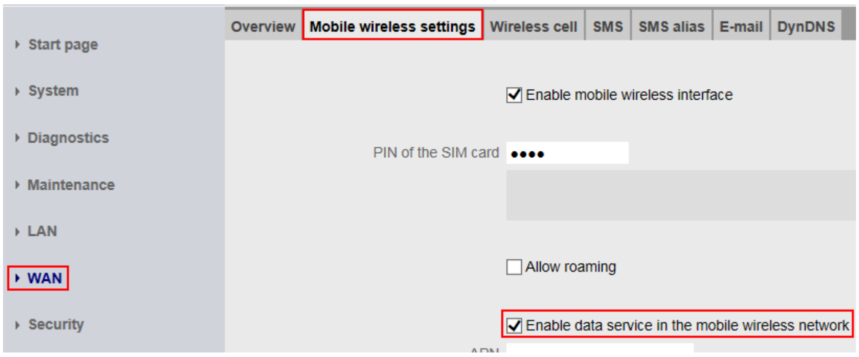


☑ Enable mobile wireless interface

PIN of the SIM card ••••

□ Allow roaming

3. Enable the "Enable data service in the mobile wireless network" checkbox in order to release the data service in mobile network.



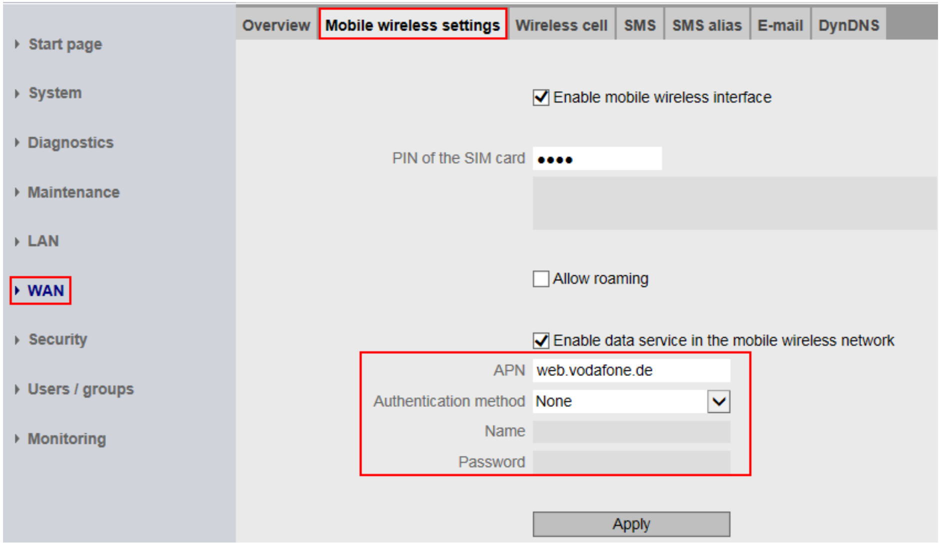
☑ Enable mobile wireless interface

PIN of the SIM card ••••

☐ Allow roaming

☑ Enable data service in the mobile wireless network

4. In order to configure the APN and the access data to the APN, you have to perform the following steps:
   - Enter the APN of your mobile network operator in the input field
   - Select a method from the “Authentication method" with which the name and password of the APN is to be transferred to the communication partner.
   - Enter the name and password you were given by your mobile network operator in the input field.
     Note:
     Some mobile network operator require no access control by name and password. If this is the case, leave the input fields empty.



☑ Enable mobile wireless interface

PIN of the SIM card ••••

☐ Allow roaming

☑ Enable data service in the mobile wireless network

APN web.vodafone.de

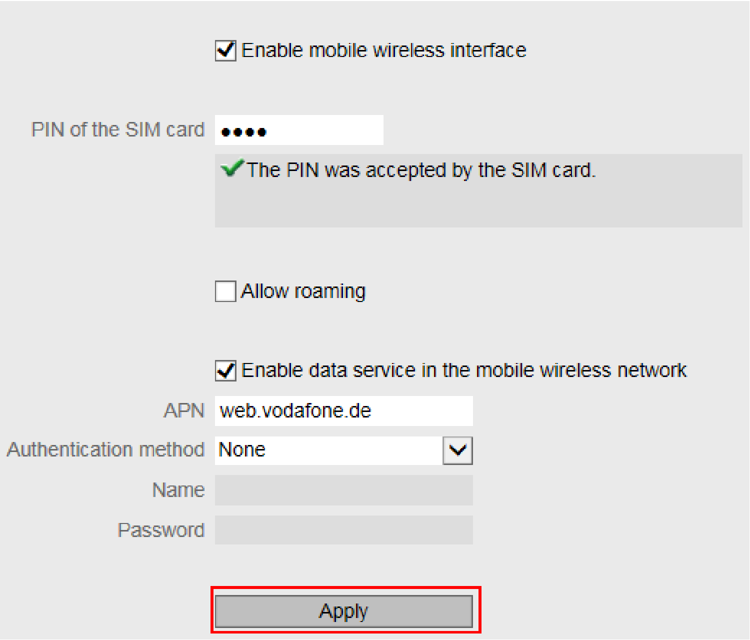
Authentication method None

Name

Password

5. In order to save the PIN and the other settings, click on “Apply”.
   A green tick below the input field shows that the PIN was saved successfully in the device.

   A red dot with a white cross underneath the input field shows that the configuration is not correct. A respective error message is shown. There will be no mobile network connection.



☑ Enable mobile wireless interface

PIN of the SIM card ●●●●

✓ The PIN was accepted by the SIM card.

□ Allow roaming

☑ Enable data service in the mobile wireless network

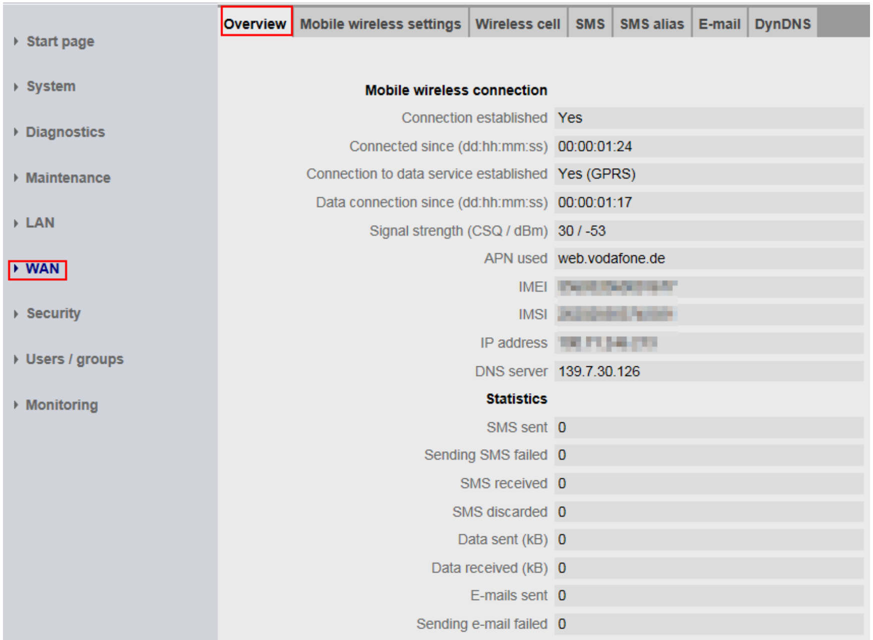
APN web.vodafone.de

Authentication method None

Name

Password

Result
LOGO! CMR logs into the mobile network connection using the correct access data. LOGO! CMR can be reached via an external, public IP address. The current operating status of the device and the assigned IP address can be viewed in "WAN > Overview".



Mobile wireless connection	
Connection established	Yes
Connected since (dd:hh:mm:ss)	00:00:01:24
Connection to data service established	Yes (GPRS)
Data connection since (dd:hh:mm:ss)	00:00:01:17
Signal strength (CSQ / dBm)	30 / -53
APN used	web.vodafone.de
IMEI	[redacted]
IMSI	[redacted]
IP address	[redacted]
DNS server	139.7.30.126
Statistics	
SMS sent	0
Sending SMS failed	0
SMS received	0
SMS discarded	0
Data sent (kB)	0
Data received (kB)	0
E-mails sent	0
Sending e-mail failed	0

Setting time

In order to establish a secure communication it is essential to set the current time and date on LOGO! CMR. The certificates used are considered invalid without valid time, and a secure VPN communication is not possible. LOGO! CMR supports the following processes:

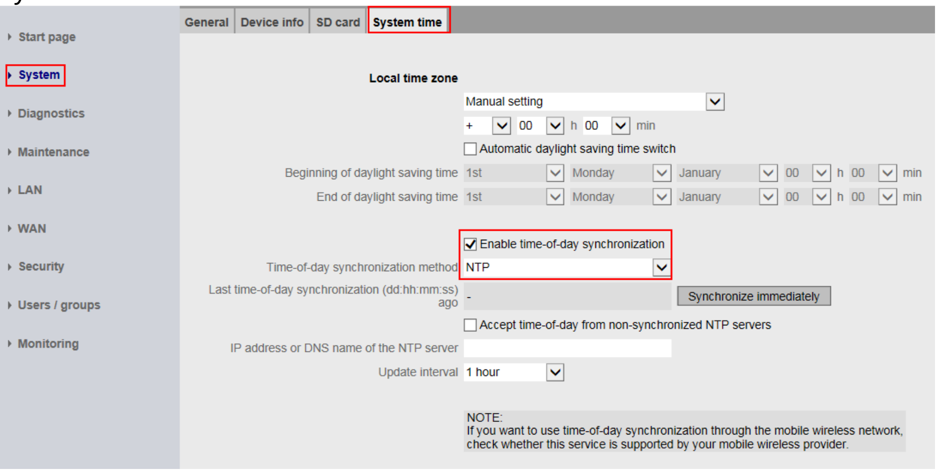
- Automatic time-of-day synchronization, e.g., via NTP
- Manual setting
- Accept PC time

Note

> The time is reset when LOGO! is restarted. You always have to use a time-of-day synchronization for the current time.
>
> If you are using the NTP process, the CMR only establishes a connection to the NTP server via the mobile wireless interface and not via the Ethernet interface.

To set up the time-of-day synchronization via the NTP process, proceed as follows:

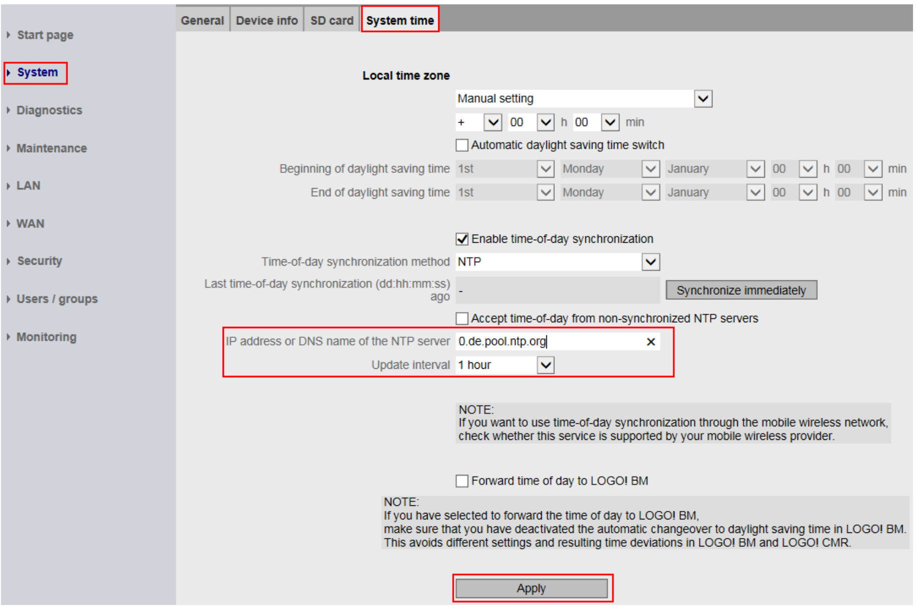
1. Navigate to “System > System time” in the navigation bar. Enable the time-of-day synchronization of the CMR via the checkbox. Select the “NTP" synchronization method.



Local time zone: Manual setting
+ 00 h 00 min
□ Automatic daylight saving time switch
Beginning of daylight saving time: 1st Monday January 00 h 00 min
End of daylight saving time: 1st Monday January 00 h 00 min
☑ Enable time-of-day synchronization
Time-of-day synchronization method: NTP
Last time-of-day synchronization (dd:hh:mm:ss) ago: -
□ Accept time-of-day from non-synchronized NTP servers
IP address or DNS name of the NTP server:
Update interval: 1 hour

NOTE:
If you want to use time-of-day synchronization through the mobile wireless network, check whether this service is supported by your mobile wireless provider.

2. Enter the IP address or DNS name of the NTP server and select at what periodic intervals the time-of-day synchronization is to take place. There are numerous time servers on the internet, from which the current time can be precisely obtained.
   In order to accept the settings of the local time zone, click on the "Apply" button.



Local time zone

Manual setting

+ 00 h 00 min

□ Automatic daylight saving time switch

Beginning of daylight saving time 1st Monday January 00 h 00 min

End of daylight saving time 1st Monday January 00 h 00 min

☑ Enable time-of-day synchronization

Time-of-day synchronization method NTP

Last time-of-day synchronization (dd:hh:mm:ss) ago -

□ Accept time-of-day from non-synchronized NTP servers

IP address or DNS name of the NTP server 0.de.pool.ntp.org

Update interval 1 hour

NOTE:
If you want to use time-of-day synchronization through the mobile wireless network, check whether this service is supported by your mobile wireless provider.

□ Forward time of day to LOGO! BM

NOTE:
If you have selected to forward the time of day to LOGO! BM,
make sure that you have deactivated the automatic changeover to daylight saving time in LOGO! BM.
This avoids different settings and resulting time deviations in LOGO! BM and LOGO! CMR.

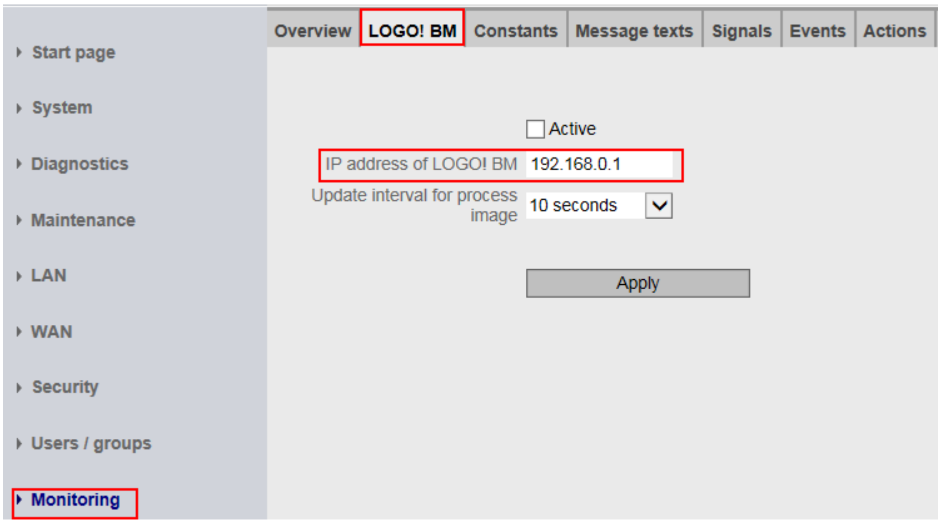
Result

The time is synchronized via the NTP process.

Establishing communication between BM and CMR

To establish a communication between basic device and the LOGO! CMR, proceed as follows:

1. Navigate to "Monitoring > LOGO! BM" in the navigation bar. Enter the IP address of your BM in the input field "IP address of LOGO! BM" (see Table 2-1).

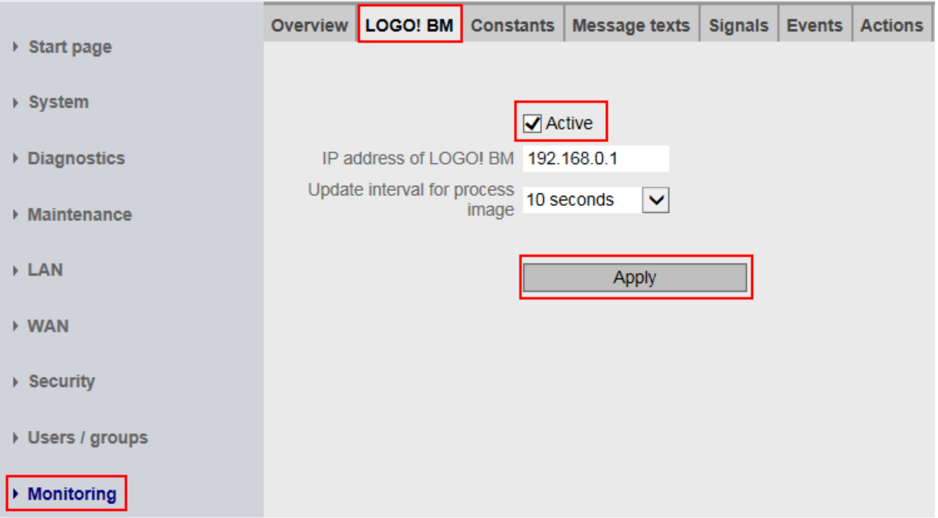


□ Active

IP address of LOGO! BM 192.168.0.1

Update interval for process image 10 seconds

2. Enable the “Active” checkbox. This option enables a connection between CMR and BM.
   In order to save the settings, click on the “Apply” button.



☑ Active

IP address of LOGO! BM: 192.168.0.1

Update interval for process image: 10 seconds

Result:
You have established the communication between the devices. Via an OpenVPN connection, it is now possible to directly access the LOGO! basic module for routing via LOGO! CMR.

2.3 Setting up remote access

You can use the VPN technology of OpenVPN for the secure transmission of data via the mobile network connection of CMR. A VPN tunnel is established between CMR and the service PC. CMR is the OpenVPN server, the service PC is the OpenVPN client.

You can furthermore use OpenVPN for direct communication with the BM when CMR is entered at BM as router.

2.3.1 Configuring remote access on the LOGO! CMR

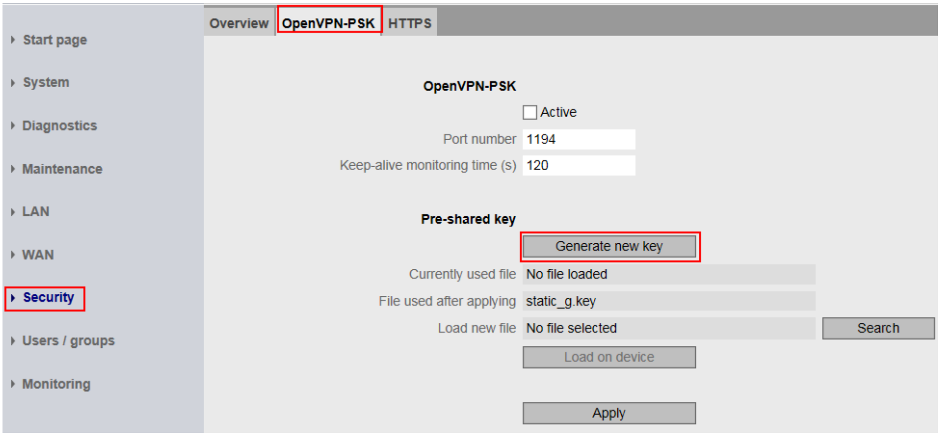
Checking mobile network connection

Check whether LOGO! CMR has established a mobile network connection in "WAN > Overview". If there is no mobile network connection, check the mobile wireless settings and customize the settings.

Creating pre-shared key

In order to encrypt the data in the VPN tunnel, the pre-shared key method is used.

1. Navigate to "Security > OpenVPN-PSK" in the navigation bar.
   In order to create a new pre-shared key click on the "Generate new key" button.



OpenVPN-PSK

□ Active

Port number 1194

Keep-alive monitoring time (s) 120

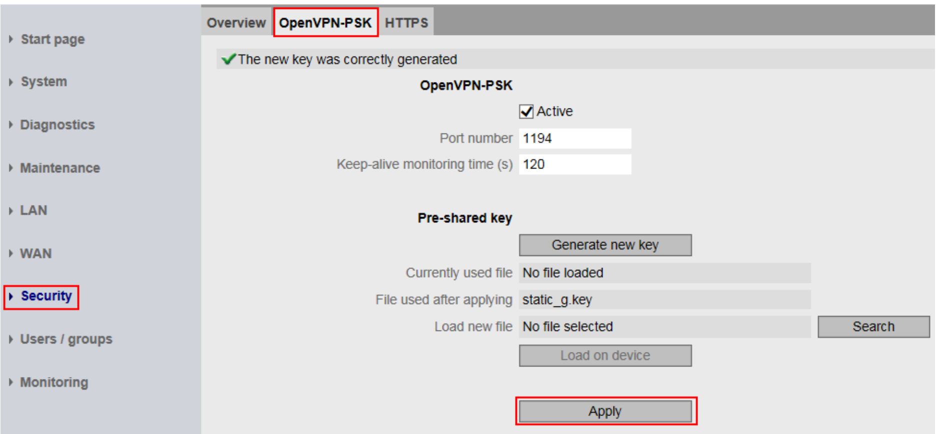
Pre-shared key

Currently used file No file loaded

File used after applying static_g.key

Load new file No file selected

2. A message underneath the navigation shows that the key was generated successfully. The secure communication via OpenVPN is automatically released. In order to save the settings, click on the “Apply” button.



✓ The new key was correctly generated

OpenVPN-PSK

☑ Active

Port number	1194
Keep-alive monitoring time (s)	120

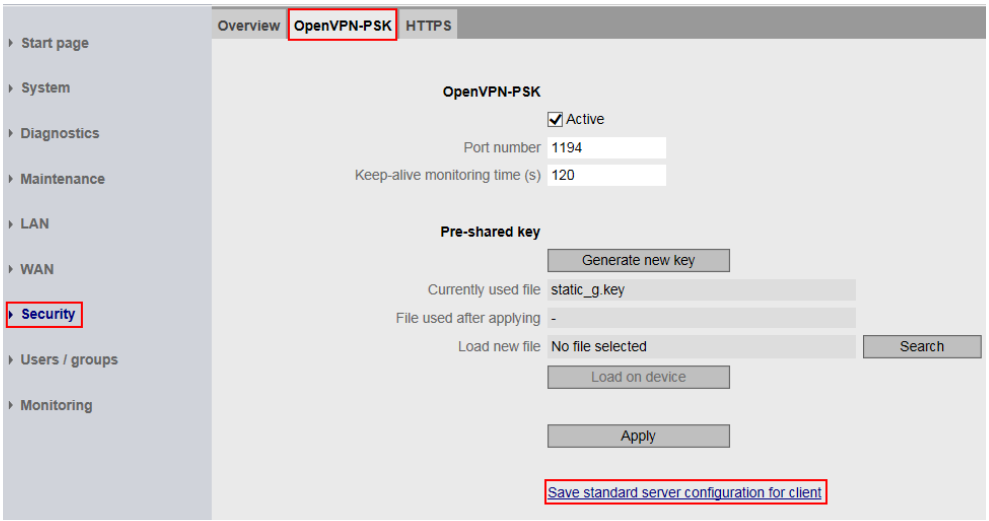
Pre-shared key

Currently used file	No file loaded
File used after applying	static_g.key
Load new file	No file selected

Saving default settings

CMR offers the option to export separate default settings (OpenVPN server) for the OpenVPN client via the "vpnpeer.conf" file into file system of the connected PC. The file includes settings, which ensure that a connection of CMR with the OpenVPN client will be established. This file can be imported to the OpenVPN client.

Click the "Save standard server configuration for client" entry. The configuration file of CMR can be saved in the file system of your configuration PC, using this entry. The file is named "vpnpeer.conf" and also includes the pre-shared key created by CMR.



OpenVPN-PSK

☑ Active

Port number	1194
Keep-alive monitoring time (s)	120

Pre-shared key

Currently used file	static_g.key
File used after applying	-
Load new file	No file selected

Note

The configuration file is not encrypted for the OpenVPN client. The pre-shared key is unencrypted in the file. Only transfer the file secured to partners, e.g., using HTTPS.

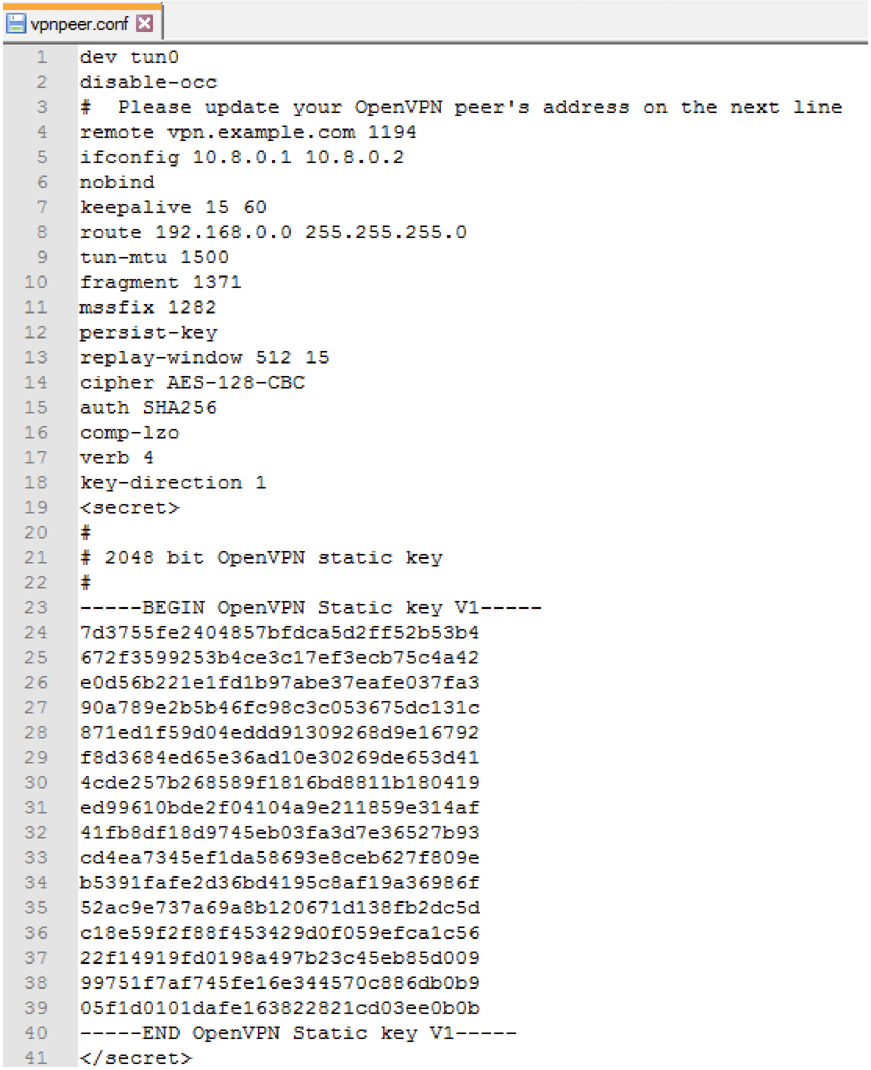
Adjusting file

Handling the "vpnpeer.conf" file, depends on the method of address assignment of CMR:

- When you use DynDNS, you can use the file directly for the OpenVPN client.
- If you do not use DynDNS, you have to adjust the address data in the "vpnpeer.conf" file. To do this, the file can be edited with a text editor.

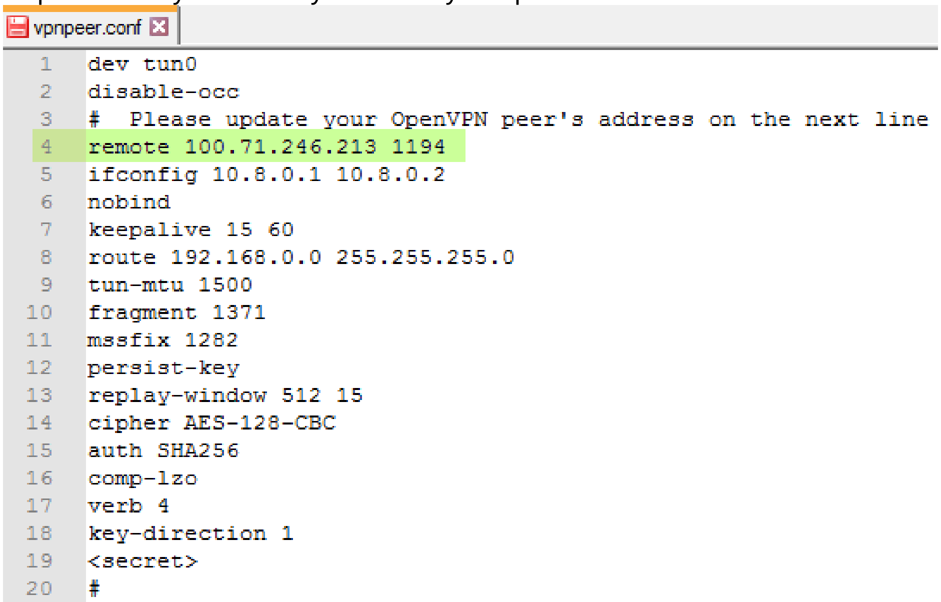
To adjust the file for the use of OpenVPN without DynDNS , proceed as follows:

1. Open the "vpnpeer.conf" file with a text editor, e.g., Notepad++.



```
dev tun0
disable-occ
#  Please update your OpenVPN peer's address on the next line
remote vpn.example.com 1194
ifconfig 10.8.0.1 10.8.0.2
nobind
keepalive 15 60
route 192.168.0.0 255.255.255.0
tun-mtu 1500
fragment 1371
mssfix 1282
persist-key
replay-window 512 15
cipher AES-128-CBC
auth SHA256
comp-lzo
verb 4
key-direction 1
<secret>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
7d3755fe2404857bfdca5d2ff52b53b4
672f3599253b4ce3c17ef3ecb75c4a42
e0d56b221e1fd1b97abe37eafe037fa3
90a789e2b5b46fc98c3c053675dc131c
871ed1f59d04eddd91309268d9e16792
f8d3684ed65e36ad10e30269de653d41
4cde257b268589f1816bd8811b180419
ed99610bde2f04104a9e211859e314af
41fb8df18d9745eb03fa3d7e36527b93
cd4ea7345ef1da58693e8ceb627f809e
b5391fafe2d36bd4195c8af19a36986f
52ac9e737a69a8b120671d138fb2dc5d
c18e59f2f88f453429d0f059efca1c56
22f14919fd0198a497b23c45eb85d009
99751f7af745fe16e344570c886db0b9
05f1d0101dafe163822821cd03ee0b0b
-----END OpenVPN Static key V1-----
</secret>
```

2. If CMR has logged in successfully in the mobile network connection, the provider will assign a public IP address to the SIM card. You can view the assigned IP address in the web-based management of CMR in "WAN > Overview".
   Replace the DynDNS entry in line 4 by this public IP address.



```
 1  dev tun0
 2  disable-occ
 3  #  Please update your OpenVPN peer's address on the next line
 4  remote 100.71.246.213 1194
 5  ifconfig 10.8.0.1 10.8.0.2
 6  nobind
 7  keepalive 15 60
 8  route 192.168.0.0 255.255.255.0
 9  tun-mtu 1500
10  fragment 1371
11  mssfix 1282
12  persist-key
13  replay-window 512 15
14  cipher AES-128-CBC
15  auth SHA256
16  comp-lzo
17  verb 4
18  key-direction 1
19  <secret>
20  #
```

3. Save the edited "vpnpeer.conf" file.

Note

If your “OpenVPN client" software needs a different file ending, e.g., "vpnpeer.ovpn", you have to rename the file to "vpnpeer.conf".
To do this, go to "Save as…" and save the edited file in the new form, for example, "vpnpeer.opvn".

2.3.2 Establishing remote connection to the service PC

The remote access between service PC and LOGO! CMR is secured via an OpenVPN connection. Initiator of the connection is a “OpenVPN client" software that is installed on the service PC.

Transferring configuration file

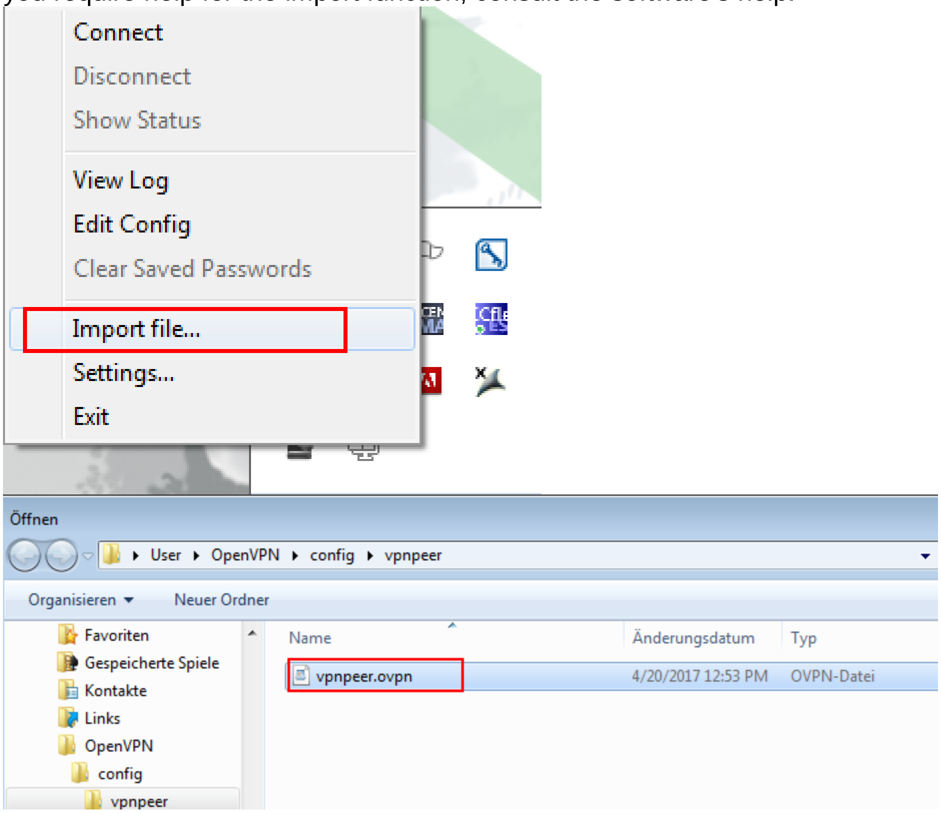
In order to configure the OpenVPN client on the service PC, use the "vpnpeer" configuration file. This configuration file has to be transferred from the configuration PC to the service PC.

Importing configuration file

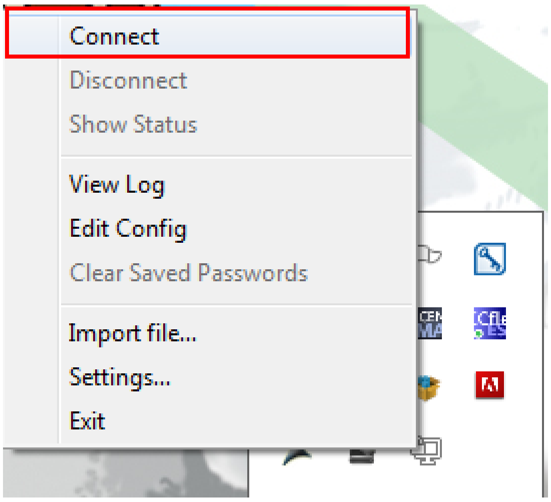
Note The screenshots from this section have been created using the “OpenVPN client” software "OpenVPN GUI".

1. Open the “OpenVPN client" software on your service PC.

2. Import the "vpnpeer" configuration file in your “OpenVPN client" software. If you require help for the import function, consult the software's help.

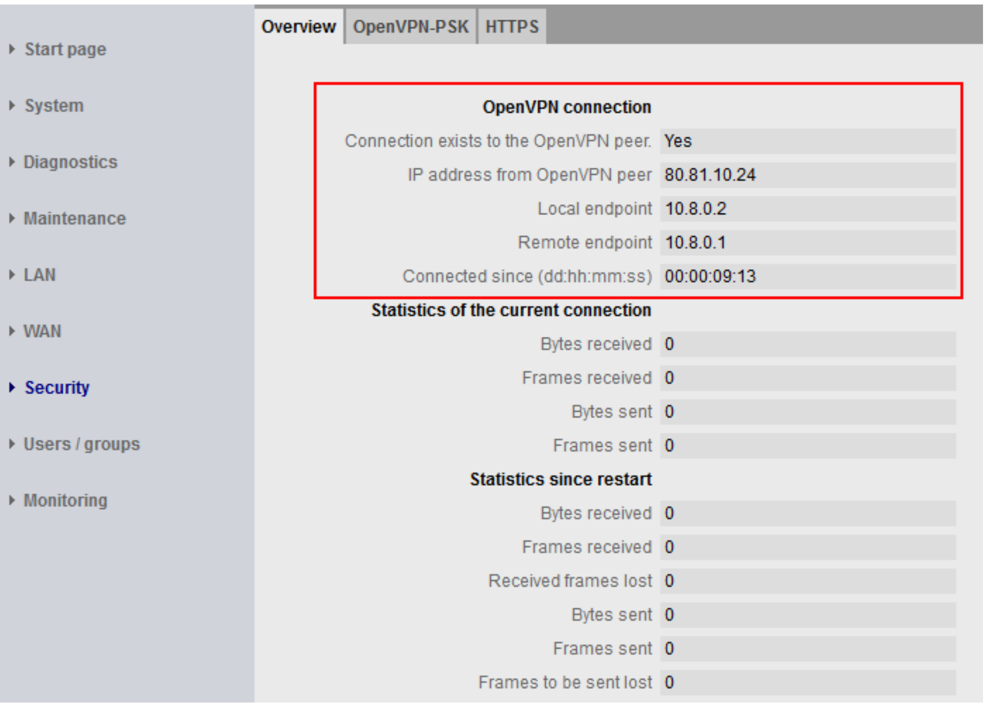


3. Establish the VPN tunnel to LOGO! CMR using the appropriate function in your "OpenVPN" client software, for example, via a "Connect" button.



Result

The OpenVPN client establishes a VPN tunnel to LOGO! CMR.
Usually, you can view the status of the VPN connection in the "OpenVPN client" software.
Alternatively, you can view the status of the VPN connection in the web-based management of the CMR in "WAN > Overview".



OpenVPN connection

Connection exists to the OpenVPN peer.	Yes
IP address from OpenVPN peer	80.81.10.24
Local endpoint	10.8.0.2
Remote endpoint	10.8.0.1
Connected since (dd:hh:mm:ss)	00:00:09:13

Statistics of the current connection

Bytes received	0
Frames received	0
Bytes sent	0
Frames sent	0

Statistics since restart

Bytes received	0
Frames received	0
Received frames lost	0
Bytes sent	0
Frames sent	0
Frames to be sent lost	0

3 Testing the Tunnel Function

Chapter 2 completes the commissioning of the configuration, and service PC and LOGO! CMR modules have established a VPN tunnel for secure communication. You now have the following options to communicate securely via the VPN tunnel with the LOGO!:

- You can access the CMR and, for example, configure the CMR and/or operate the I/Os. You reach the LOGO! CMR either via the internal OpenVPN IP address or via the set LAN IP address (192.168.0.3).
- You can access the LAN interface of LOGO! CMR via the VPN tunnel and you can therefore also access the LOGO! BM remotely. If you would like to communicate with LOGO! BM via LOGO! CMR, you have to enter the local IP address of LOGO! CMR as default router in LOGO! BM. If you have entered LOGO! CMR as default router, you can access the local IP address of the basic module (192.168.0.1).
- In the "Logo! Soft Comfort" that is installed on the service PC with active OpenVPN connection, you also only have to enter the local IP address of the LOGO! BM with the LOGO! CMR as default router. You can then download or upload the program to/from LOGO! BM remotely.

4 History

Table 4-1

Version	Date	Modifications
V1.0	06/2017	First version