INSEVIS

S7-IIoT Gateway Manual

- S7-Panel-PLC
- S7-Compact-PLC
- S7-Panel-HMI
- Periphery
- Software
- Energy management
- S7-IIoT-Gateway

Indes of contents

Changes to older versions of the manual

Rev. 01 / 2019:
new: Initial version

Rev. 01 / 2020:
new: Chapter MQTT and openVPN added
changed: All descriptions improved, order of chapters changed

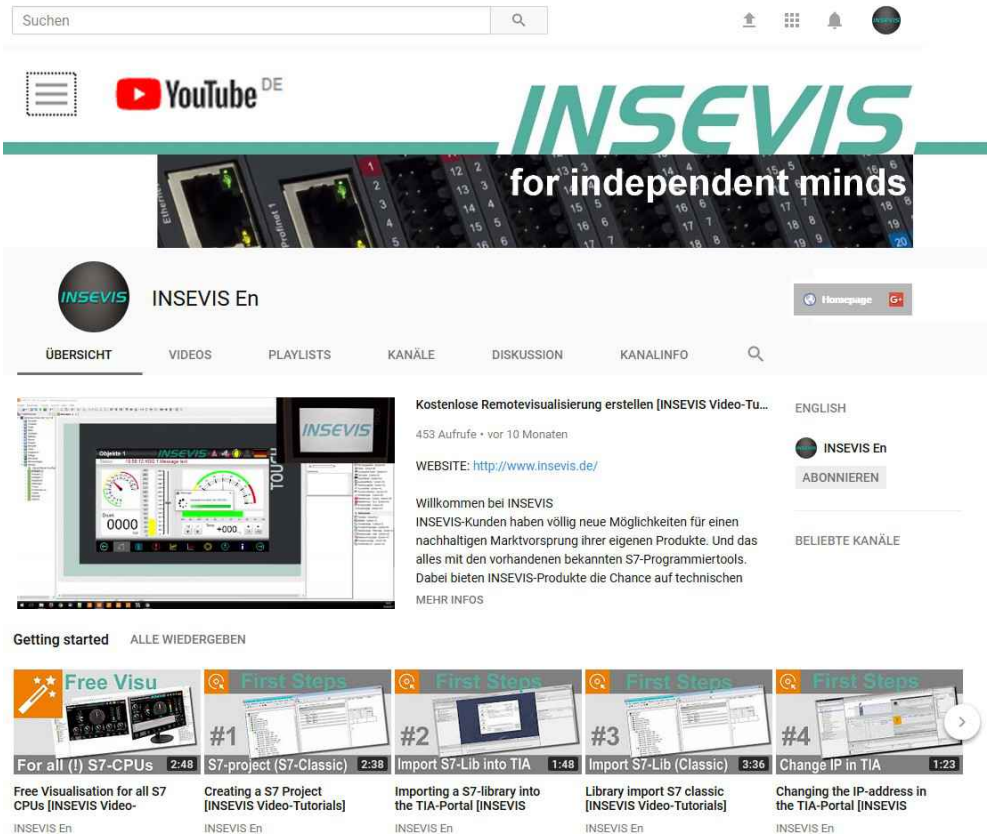
Rev. 02 / 2020:
changed: Description Update and OPCUA, screenshoots updated to V 3.3.1
small corrections in all texts
Import of S7-Variablen moved from „Connections“ to „Datenpoints“

Rev. 03 / 2020:
new: Additions in OPCUA und NodeRed

Rev. 04 / 2020:
changed: typos, example OPCUA warnings removed
new: Hint WAN at 192.168.80.60, MQTT unsecure

Hint for better understanding by application videos

In the English YouTube-channel INSEV IS En we supply different playlists with handling videos for single details referring to functions, described in this manual. This will help you to get familiar with INSVEIS much faster – PLEASE use it beside this manual!



General instructions

Safety instructions

This manual contains instructions to avoid material damage and must be carefully attended for your own safety. These instructions are identified with a warning triangle with a note of exclamation inside and a signal word *(Signal word)* below.

Danger	Death, heavy bodily harm or material damage will appear, if appropriated precautions are not taken over.
Warning	Death, heavy bodily harm or material damage will appear, if appropriated precautions are not taken over.
Caution	Bodily harm or material damage will appear, if appropriated precautions are not taken over.
Attention	means, that a not wished results or states can occur, if the appropriated instruction is not noticed.
Important	means the commitment to a special behaviour or operation for the safe treatment of the controller / machine.

Qualified personnel

All devices described in this manual may only be used, built up and operated together with this documentation. Installation, initiation and operation of these devices might only be done by instructed personnel with certified skills, who can prove their ability to install and initiate electrical and mechanical devices, systems and current circuits in a generally accepted and admitted standard.

Operation according to regulations

This device might be only used for this operation written in this manual and only in combination with other certified external devices. For a correct operation a proper transportation, storage, initiation and maintenance is necessary.
All valid safety instructions and regulations for the prevent of industrial accidents are to be attended carefully.
The power supply must be connected to a central ground potential in a star likely wiring.

Maintenance

Modifications / repairs of an INSEVIS device might be done only by special educated and trained personnel of INSEVIS in an ESD safe area. Every unauthorized opening might cause damages and will terminate all warranty claims.

Data security

Each customer is responsible by himself for protecting his IT-environment against illegal external attacks. INSEVIS shall not be held liable for any direct, indirect or consequential damages respect to any claims arising from the possible illegal external access to their PLCs or HMIs by Ethernet. If you are not sure, how to protect your environment ask for help at professional legal IT-companies.

Copyright

Trade Marks

INSEVIS refers that all trade marks of particular companies used in own documentation as e.g.
- STEP®, SIMATIC® and other as reserved trade mark of Siemens AG.
- CANopen® and other as reserved trade mark of CAN in Automation eG
- WINDOWS® and other as reserved trade mark of MICROSOFT AG

and more reserved trade marks are property of the particular owners and are subjected to common protection of trade marks.

Disclaimer

All technical details in this documentation were created by INSEVIS with highest diligence. Anyhow mistakes could not be excluded, so no responsibility is taken by INSEVIS for the complete correctness of this information. This documentation will reviewed regulary and necessary corrections will be done in next version.

With publication of this manual all other versions are no longer valid.

Essential knowledge and experiences

To understand this documentation basic knowledge and experiences of the automation technology in general and the programming with STEP®7 are essential.

About INSEVIS

S7-system components for industrial automation technology

The range of INSEVIS- product families enables an integrated solution and easy to handle for small and medium automation application with latest technology, very high quality level and with additional interfaces like CANopen® and Modbus, to be configured easily.

The easy integration of INSEVIS-products into the S7-world meanwhile is famous and exemplary. Complex communication settings will be assigned easily and intuitively, so that these properties expand the common S7-world by far. A large and multilingual visualization in a modern design is done by a few clicks and the work flow is known by every WinCCflex user. It can be simulated on the visualization PC and is accessible remote.

The S7-CPUs -V and -P are the base of the successfully INSEVIS product families with Profibus DP Master/Slave.
With the new S7-CPU-T Panel-PLCs and Compact-PLCs are available with Profinet IO Controller.

Step®7-Programmability

INSEVIS-S7-CPUs are programmable by STEP 7® - AWL, KOP, FUP, S7-SCL, S7-Graph from Siemens and in general command-compatible to Siemens-CPU S7-315-2PNDP. Some special INSEVIS blocks expand the functionality and allow outstanding solutions. The S7-programming will be done by good known tools SIMATIC®-Manager or by TIA-Portal® from Siemens always.

Independence

INSEVIS-PLCs and HMIs does not base on Windows or Linux, they have an own firmware. Thereby the hard- and software can be exactly designed for a perfect co-ordination with this firmware and a low power consumption. Booting times of less than 4 seconds and completely no software licenses and a current drain of <100mA @ 24V are the result of these facts.

Get your software rid of licenses

INSEVIS stands for a clear and honest license policy, what gives the customer sustainable cost benefits. Because of the ownership of BIOS, firmware and PC-software for visualization, configuration and remote access INSEVIS can offer its products completely without licenses.

Made in Germany

Development, PCB-design and -production, test and mounting of all INSEVIS-products - all this is made in Germany. So every product is a proof for the combination of German engineering and economy and is available with a certification of German origin.


Certificato Certyfikat Certificate Certificado Certificat

Zertifikat

TAW Cert

Die Zertifizierungsstelle TAW Cert
Zertifizierungsgesellschaft mbH für QM-Systeme und Personal

bescheinigt hiermit, dass das Unternehmen

INSEVIS
Gesellschaft für industrielle Systemelektronik und Visualisierung mbH
Am Weichselgarten 7
91058 Erlangen

für den Geltungsbereich
Entwicklung, Service und Vertrieb von Systemelektronik und Software für industrielle Automatisierungslösungen

ein Qualitätsmanagementsystem eingeführt hat und anwendet.

Durch ein Audit am 31.07.2014 wurde der Nachweis erbracht, dass die Anforderungen der
DIN EN ISO 9001
(Ausgabe 2008)
erfüllt sind.

Ersterzertifizierung: 14.09.2011

Dieses Zertifikat ist gültig bis 13.09.2017

Zertifikat-Registrier-Nr.: 19010511

TAW Cert

DAkkS

Altdorf, den 14.09.2014

Dr.-Ing. Dietmar Winner, Geschäftsführer TAW Cert GmbH

TAW Cert GmbH • Fritz-Bauer-Str. 13 • 90518 Altdorf

Dieses Zertifikat ist Eigentum der TAW Cert GmbH

INSEVIS operates a yearly certified quality management system ref. to DIN EN ISO 9001.

All suppliers of INSEVIS obligate to this quality management and contribute to the high quality level of INSEVIS-products.

Already during planning these families one goal was indicated as most important: to design highest quality and ergonomics into all products.

These products were put into comprehensive validation tests before they were produced in selected and certified production lines.

INSEVIS - Made in Germany

Product family S7-IIoT Gateways

INSEVIS-S7-IIoT-Gateway – compatible but independent up to the cloud

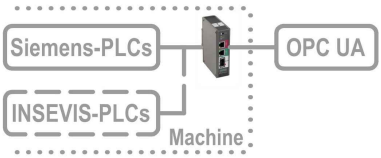
INSEVIS is known for independent and sustainable solutions in the S7-world. With the IIoT-gateways these experience should be broadened to the „Industrial Internet of Things“ or „Industry 4.0“. The large know-how for S7-technology, combined with most modern security-, communication- and operation philosophy allow optimal combination of S7-solutions with the big-data-world on one side and, secure connections between S7-islands completely without a portal or a cloud.

Referring to the „Reference architecture model Industry 4.0 – RAMI4.0“ INSEVIS supplies all configuration shells onboard, so that a single browser is enough to assign and configure all the settings. But not for anyone, because a sophisticated user management cares for a considerably protection and allows released connections only. External access is possible by openVPN in a safe way. An internal project and version management guarantees a better overview.

With huge projections by the implemented „NodeRed“ you can let you imagination run; create tweeds, emails or convert text to speech and get it read to you by an artificial voice. The integrated project- and version management cares for a better overview or backups of previous versions.

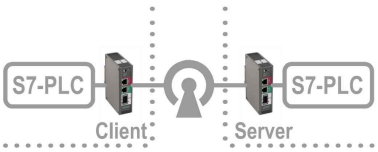
Fields of application

Add S7-controllers by OPC UA-interface to I4.0



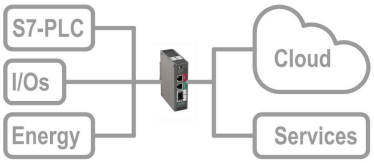
Secure integrating of the S7- Welt by OPC UA to MES, HMI, SCADA ref. to RAMI4.0 (administration shell)

Secure connection of PLC-islands without Cloud/Portal



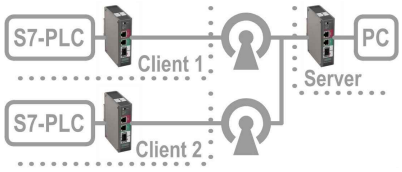
By Site-To-Site-open-VPN directly and secure client/server connection of two S7-islands without need of a clouds or portal

Data acquisition, -processing and -forwarding by IIoT



Data acquisition in S7- and field-layer and transfer by OPC UA or MQTT into cloud or by FTP, email, Twitter, etc.

Secure remote maintenance of multiple systems



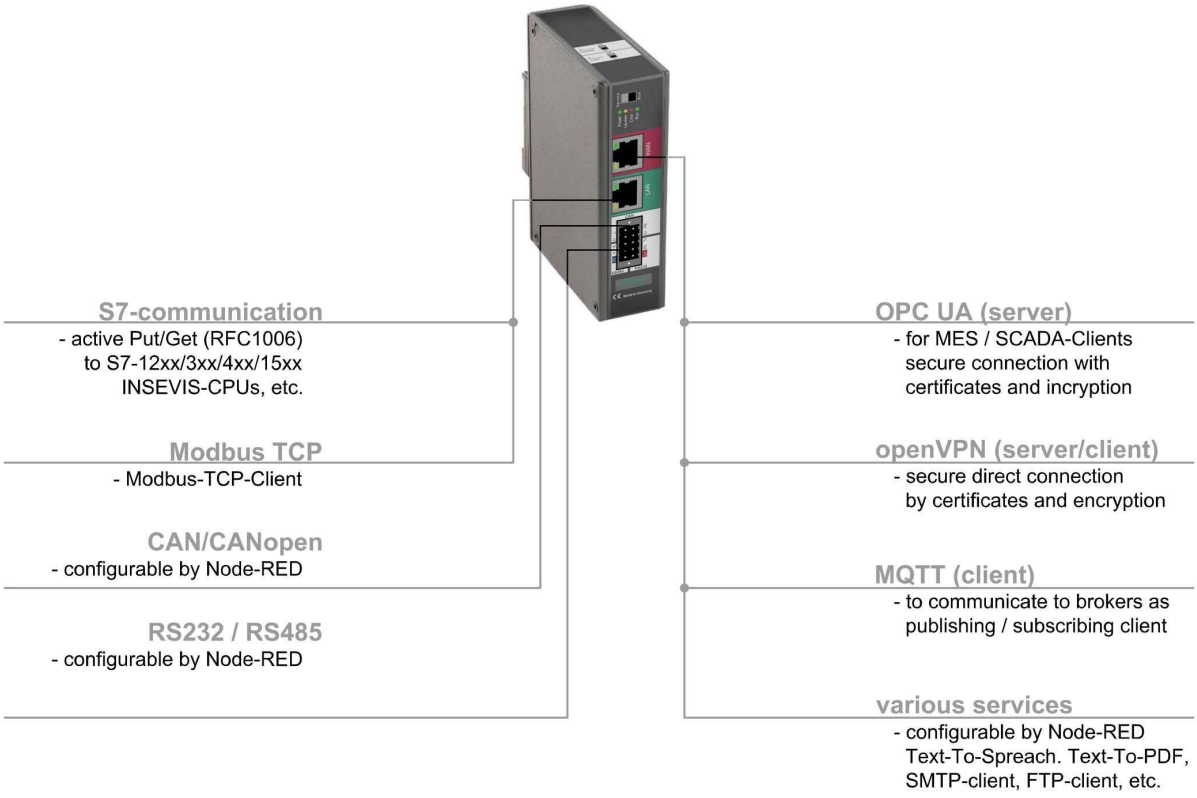
Secure remote maintenance of multiple S7-islands by openVPN from a central station

Product family S7-IIoT Gateways

Communication in LAN and WAN

The S7-IIoT-Gateway communicates to control- and field-level by Ethernet RFC1006 (S7-communication, active Put/Get) and Modbus-TCP. Other interfaces like CAN/ CANopen, RS485 and RS232 may be configured by Node-RED.

At the WAN-side a firewall protects the device against unauthorized communication attempts. The IIoT-Gateway offers OPC UA-server functionality for data exchange with SCADA-, MES- or other management systems. The MQTT-client functionality allows the process data supply for cloud systems.



Most important properties at a glance

S7-variables import and register mapping

Import S7-variables from Simatic-Manager or TIA-Portal including symbols and supply it as data point. Map Modbus registers to OPC UA-data points.

Web-Configuration

One onboard-configuration tool saves all external PC-tools Secure access control by integrated user-management, comprehensive backup-, restore- and update functionalities

LAN @Node-RED: CAN, RS485 and RS232

Activated by Node-RED: Easy data exchange by additional protocols to communicate to different kinds of field devices like energy meters, decentral I/Os, FCs, etc.

LAN: S7-Ethernet and Modbus-TCP

Communicate by RFC1006 (S7-communication, active Put/Get) easily and with all Siemens-S7-CPUs Integrate energy meters into your system by Modbus-TCP.

openVPN: secure S7-communication

Setup of openVPN-connections including certificate-management by onboard-configuration to connect 2 S7-islands completely without portal or cloud. Or as simple secure remote maintenance.

MQTT: onboard configuration

Data handling with MQTT-brokers as (pubishing or subscribing) client.

Services @ NodeRED: Create own value

Use imported data points in available Node-RED-nodes to multiple different services and create a unique selling proposition and added value

Dashboard @ NodeRED: web visualization for free

Visualize imported data points in available Node-RED-nodes as dashboard and provide it as free web visualization

Product family S7-IIoT Gateways

Technical data

S7-IIoT-Gateway for 35mm DIN-rail

Standard configuration:

RS232
(for Node-RED-projects)

RS485
(for Node-RED-projects)
- with switchable teminate resistors for RS485

CAN
(for Node-RED-projects)-
- with switchable teminate resistors)

Ethernet with
- RFC1006 (S7-communication, Send/ Receive (active)
- Modbus-TCP

Switch
for operation mode

State LEDs for
Power, Update, Error, Run

Inserting stripes
(for Logo and identification)
- thereby customized adaption possible easy

Scope of delivery:
- Grounding terminal
- Technical data sheet

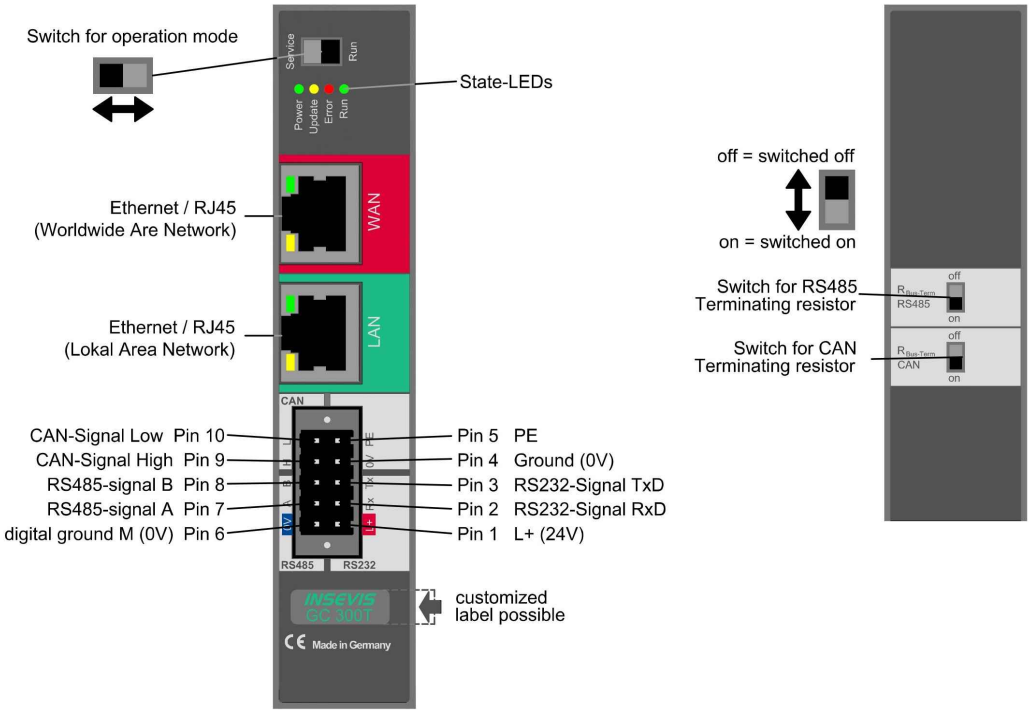


Image: view of GC300T

Importand information to data transfer direction for download- and upload procedures:

Starting from the PC the IIoT-Gateway is situated in the internet, so the data will be

- send there by **UPLOAD** from the PC and
- received from there by **DOWNLOAD** into the PC.

Starting from PC the HMI / PLC are situated in the control- or field layer; so the data will be

- send there by **DOWNLOAD** from the PC and
- received from there by **UPLOAD** into the PC.

Product family S7-IIoT Gateways

Technical data	
Dimensions W x H x D (mm) Cut out W x H (mm) Protection class Weight	28 x 116 x 84 35mm DIN rail IP41 ca. 350g
Operating temperature range Storage temperature range	-20°C ... +60°C (without condensation) -30°C ... +80°C
Connection technology	removable connector with 2 bolt flanges aside (cage clamp technology) for cross section up to max. 1,5mm^2
Load voltage L+	24V DC (11 V ... 30V DC)
Start-up current	< 3A

Technical data	CPU
CPU-type	**Typ T** (GC300**T**)
Working memory	256 MByte
internal memory	4 GByte, thereof ca. 1 GByte for user data (visualizations, etc)
Programming languages Programming system	JavaScript Node-RED
Serial interfaces (protocols)	COM1: RS 232 (via Node-RED) COM2: RS 485 (via Node-RED)
Ethernet (protocols)	ETHERNET: 10/100 MBit S7-communication (active put/get), Modbus-TCP (more by Node-RED)
OPC UA Server SecurityPolicy	Predefined namespace,compatible to S7-1500 + max. 100 user-variables alternatively user defined namespace with external modeler (via binary data export) optionally OPC UA DI able to provide datapoints from all other interfaces including history history configurable in sample time and number of samples subscriptions: max. 8 monitored items per subscription: max. 200 monitored items total: max. 500 none / Basic 256 Sha 256 sign / Basic 256 Sha 256 sign & encrypt (can be enabled and disabled separately)
MQTT	Client (subscriber / publisher)
Node-RED	performance limit approx. 50 variables actualise cyclic data points from all other interfaces
CAN (protocols)	Baudrate 10 kBaud ... 1 MBaud – via Node-RED
Data security	open source packages OpenSSH and OpenVPN

Commissioning

The IIoT-Gateway is shipped with LAN-address 192.168.80.60. If the own net differs from it, act as follows:

- Connect LAN-interface of the IIoT-Gateway (Do not mix it with the WAN-interface) with the LAN- interface of your computer.
- Assign your PC an IP-address in the subnet of the IIoT-Gateway (for example 192.168.80.65).
- For the first configuration of the IIoT-Gateway open a compatible browser (see technical data sheet) in your computer. and enter the IP-address of the IIoT-Gateway
- If the browser informs about a security risk, add an exceptional rule.

The login credentials for the first login are

Name	admin
Password	admin

ATTENTION:

The Admin-password must be changed for security reasons immediately after first login!

Change now the IP-address of the IIoT-Gateway as written below:

- Navigate to : **System / Network** and
- insert at **LAN Address** a new IP-address, which fits into your local net.
- By **Save to device** (lower right) the new settings will be applied.

Restore IP-address

It is easy to detect a forgotten IP-address:

- Switch from run → service mode to
- restart by power OFF/ON (boots 1-2min).
- in service mode the LAN IP address of the IIoT gateway is always 192.168.80.60
- on the default address 192.168.80.60 that mask (below) appears.
  If not → clear the browser cache or reload the page in your browser!
- Left at “Network” is displayed the assigned LAN-address (here: 192.168.80.60),
- than switch service → run mode,
- restart by power OFF/ON or press the button right in „Restart Gateway“ (boots 1-2min),
- insert right IP-address in your browser and ready!

Restore password

If the admin - password has been lost, a reset of the device with all data is necessary.
To be able to enter a “super-password” now and all will be fine, this IIoT-Gateway would have a “backdoor”.
→ **But it hasn't.**

- boot device in service mode
- Press button “Restore” in „Restore factory settings“ field.
- All will be reset and user data will be deleted completely.
- The IIoT-Gateway is now empty and available at 192.168.80.60 with login „admin“ and password „admin“.

Update firmware

Hint: Create a backup before start to update the firmware!
In general, however, all settings - unless it is a new or modified function - are retained.

Requirement:

- Internet connection via WAN-port and DHCP-server
  During the update, the WAN port is reconfigured via DHCP (!) regardless of any settings made before.

Update in **service-mode** :
In Service Mode, the WAN port is temporarily switched to DHCP, regardless of the settings in Run Mode.
This allows to check

- in the browser with **"Check for updates"**

whether the INSEVIS update server is accessible and which version is kept there.
If the update server cannot be reached, the update process should NOT be started either, because the IIoT Gateway will then never again be accessible via the web interface.

Start the update:

- in the browser at **“Update Firmware”**

update in **run-mode**
If an update is to take place without physical access to the device, the update can and must be started in run mode.
It must be ensured, however, that the IIoT Gateway gets Internet access via DHCP over the WAN port mentioned above - regardless of current WAN Port settings.
Even in run mode, the INSEVIS update server can be checked for new versions:

- in the browser at „System“ - „Backup and Update“ - and „**Check for updates“**

However, the current WAN settings are used (valid settings assumed). This does not tell us whether the update server can be found in update mode.

Start the update:

- in the browser at "System” - „Backup and Update“ - **„Update Firmware“**

update procedure:

- The IIoT Gateway is thus set to firmware update mode and boots a standard configuration with DHCP on the WAN port and loads the firmware via it (i.e. the settings under System - Network are irrelevant)
- The yellow LED flashes for ~5..10 min about 50x in irregular speed.
  (Devices delivered from Sept. 2020 on additionally flash green with ~ 1 Hz)
- When the update is completed the IIoT Gateway will boot back into run or service mode, depending on the switch position.
  i.e. RUN = green LED permanently on / SRV = yellow LED permanently on

ATTENTION:

If the WAN network also randomly operates in the address range 192.168.80.0, the LAN and WAN port of the IIoT gateway must be connected to the network.

Example project

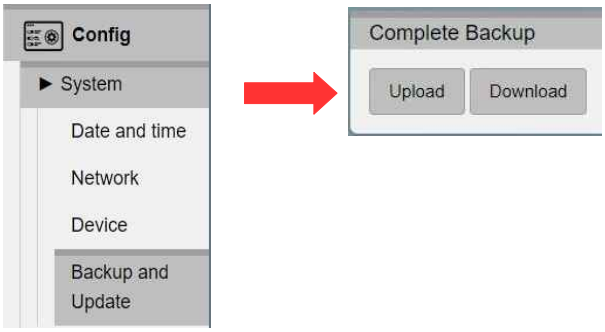
VIDEO-Tutorial available
For this example you find a link to a instructional YouTube® video in the download section of Insevis.com

The variables in the demo project correspond to the variables in the demo visualisations for the Insevis HMIs, Panel-PLCs and Remote visualizations.
We recommend to keep a device with such a demo visualisation, or at least a PLC with PUT/GET enabled, in the same LAN network as the IIoT-Gateway

You can download the demo-project at www.insevis.com/downloads under the section **Gateway.**

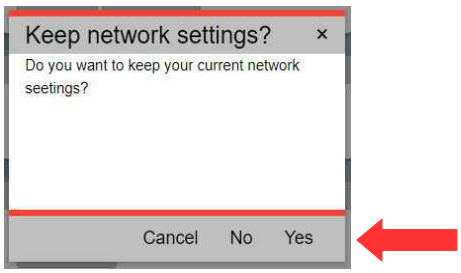
After the download has finished you can log in and navigate to **System / Backup and Update**.

This section is only accessible as the user admin. Now press the button **Upload** in the tile **Complete Backup** to upload the demo project.



In the popup dialog you can choose to keep your network settings.

The demo project comes with the LAN IP 192.168.80.60. If this differs from your settings choose Yes



Now navigate to the demo project and confirm.

The project is now being processed and the IIoT-Gateway will restart itself.

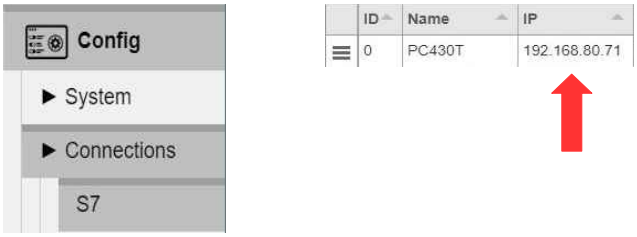
This may take 1-2 minutes.

After the restart has finished you can login with the standard credentials (admin : admin).

You will find now a pre-configuration including connections and data points.

First check if the IP address of the defined connection corresponds to the address of the PLC in your network. If it differs from the configuration change the settings of the PLC or the settings in the IIoT-Gateway.

To adjust the IIoT-Gateway navigate to **Connections / S7** and alter the address in the ip column in the table.
Save your changes with Save to device (bottom right)



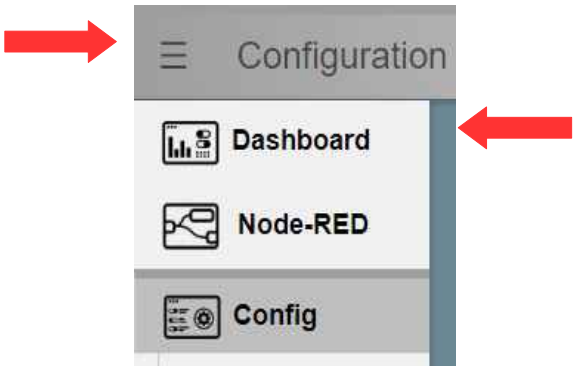
The IIoT-Gateway is now able to get data from the PLC and pass them on to Node-RED, MQTT and OPC UA .

Example project

Dashboard-Visualisation

An Example for the Node-RED dashboard is also included an is already being executed.

To access the dashboard open the sidebar menue (the three horizontal bars) and select **Dashboard**



The dashboard will open in a new tab.
The structure of the dasboard corresponds to the deomo visualisations for the Insevis HMIs and Panel-PLCs.

Example project

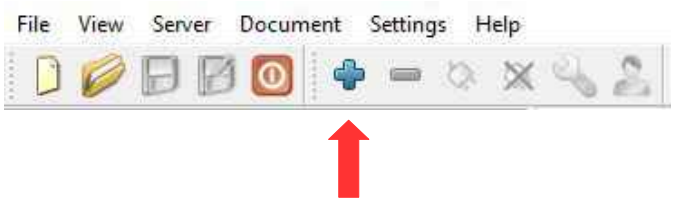
OPC UA-Server

The OPC UA server is also already accessible with a corresponding client. We demonstrate this here by the example of **UA-Expert**.

You will find the program at www.unified-automation.com. Instructions on how to download the software are provided on the website.

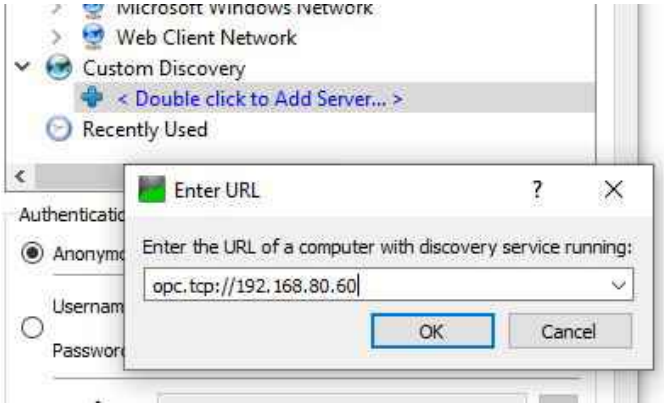
When you open UA-Expert for the first time you have to create a client certificate. To do so follow the instructions and fill out all requested fields.

To connect to the OPC UA server on the IIoT-Gateway add the server with a click on the **+** Symbol



Choose in the popup menue

Custom Discovery / + < Double click to Add Server... >.



Now enter the IP address of the IIoT-Gateway

opc.tcp://192.168.80.60

and submit it.
The server is now added to the list below.

Open the server with the **>** symbol
and the underlying entry aswell.

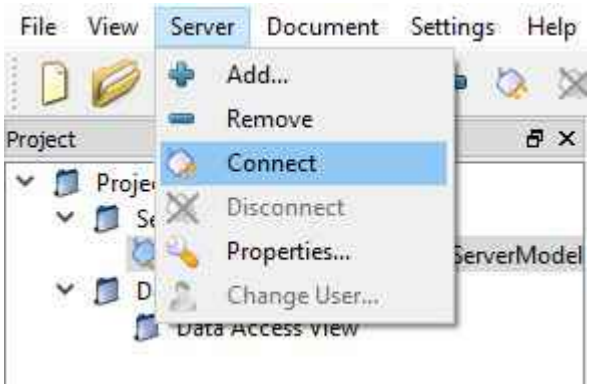
Now choose the encryption.

Select here: **Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary).**

Example project

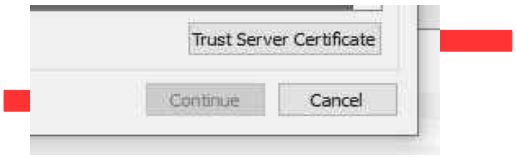
OPC UA-Server

The server has now been added to the project tree on the left side.
To connect to the server select it and choose from the menue bar **Server / Connect**.



In the following popup you are beeing warned that the certificate from the server is not trustworthy.

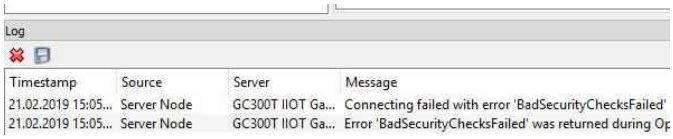
Select **Trust Server Certificate** and **Continue** after that.



In the log output at the bottom window a new error message will show up:

Connecting failed with error 'BadSecurityChecksFailed'.

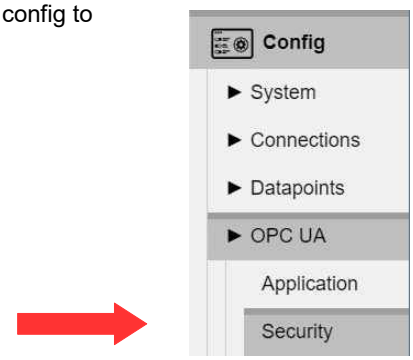
This means the server has rejected the client certificate



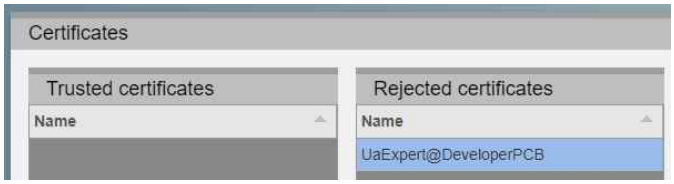
Example project

OPC UA-Server

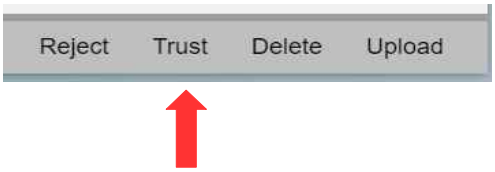
To trust the client certificate navigate in the web config to **OPC UA / Security.**



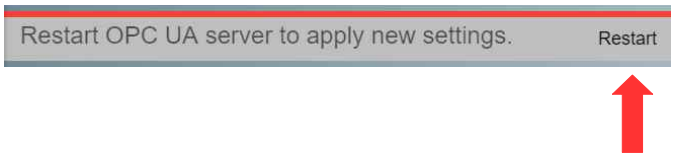
Under **Certificates** in the list **Rejected certificates** the certificate of the client is listed.



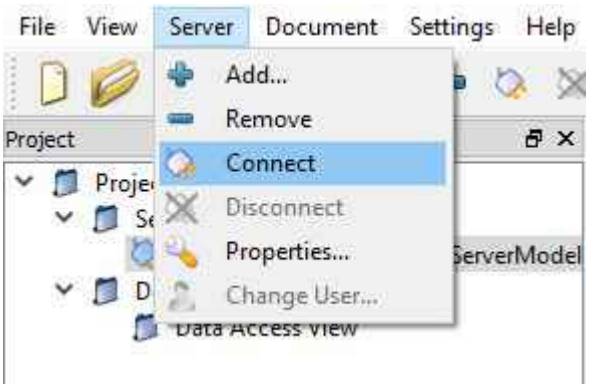
Select now the certificate and trust it with the **Trust** button in the function bar below. Save your changes with **Save settings to device** (bottom right)



Now restart the OPC UA server to apply your changes. To do so select **Restart** in the red popup at the top.



Back in UA Expert try to connect again to the server (menu bar **Server / Connect**)



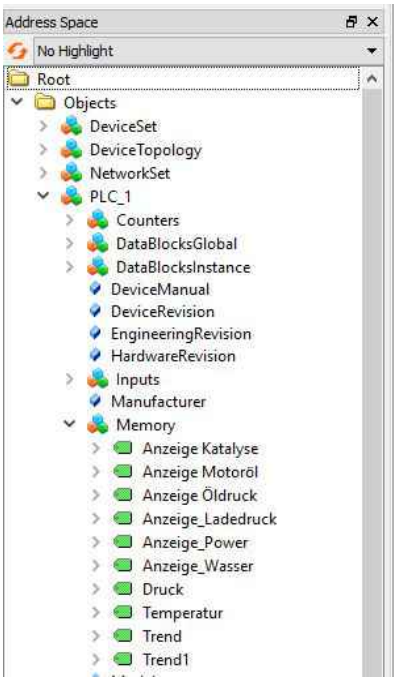
Example project

OPC UA Server

UA Expert is now connected to the server.

In the bottom left window below the project tree you can see the namespace of the server.

At **Root / Objects / PLC_1 / Memory** are all variables listed which are configured for this example.



To read the variables just drag and drop them to the middle section where they can be observed and controlled.

Data Access View

#	Server	Node Id	Display Name	Value	Datatype	ource Timestamp	Server Timestamp	Statuscode
1	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige Katalyse	28	Int16	15:53:26.632	15:53:26.632	Good
2	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige Motoröl	73	Int16	15:53:26.731	15:53:26.731	Good
3	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige Öldruck	58	Int16	15:53:26.841	15:53:26.841	Good
4	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige_Ladedruck	40	Int16	15:53:26.939	15:53:26.939	Good
5	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige_Power	32	Int16	15:53:27.053	15:53:27.053	Good
6	GC300T IIOT Ga...	NS3|String|Anze...	Anzeige_Wasser	61	Int16	15:53:27.161	15:53:27.161	Good
7	GC300T IIOT Ga...	NS3|String|Druck	Druck	0	Int16	15:53:27.261	15:53:27.261	Good
8	GC300T IIOT Ga...	NS3|String|Tem...	Temperatur	0	Int32	15:53:27.372	15:53:27.372	Good
9	GC300T IIOT Ga...	NS3|String|Trend	Trend	65	Int16	15:55:22.836	15:55:22.836	Good
10	GC300T IIOT Ga...	NS3|String|Trend1	Trend1	353	Int16	15:55:22.842	15:55:22.842	Good

System settings

Date and time

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust the date and time for the IIoT-Gateway. These settings are persistent to restarts and power loss and are beeing updated by the included real time clock.

Caution:

If the IIoT-Gateway has a established internet connection date and time are beeing set automatically and manual input will be ignored.

Set the system time hours:minutes:seconds

Set the system date. day.month.year

Set the time zone. Open the list of available time zones with the arrow **v** and search for your time zone in the search bar

Write the PCs time and date to the IIoT-Gateway.

Network

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

Under Network you can access the network settings for the device. Applying these settings can take a few seconds and are only possible if all inputs are correct.

WAN port Address with which the device communicates "to the public world outside".

WAN port netmask, matching the WAN subnet default: 255.255.255.0

This address is used to communicate with all devices that are not in the LAN or WAN network (= connection to the internet, usually the internet router)

LAN port address with which the device communicates in the internal network (This Config interface is only available in the LAN network)

LAN port netmask, matching the LAN subnet default: 255.255.255.0

The name server is required for all URLs that are not (numeric) IP addresses. Usually the internet router is also name server.

Specifies in which network the above mentioned gateway is located. (MUST match the above gateway IP address)

something tricky:
When the IoT Gateway sends data, the LAN or WAN address and the destination address are logically ANDed with the respective MASK. If the result is identical, the data is sent on the respective LAN or WAN port.
Otherwise, the data will be forwarded to the set gateway.
This definition of mutually exclusive IP address ranges separates WAN and LAN.
The **addresses of LAN and WAN MUST differ** within the defined masks.
Otherwise, no assignment is possible and all data is sent via the LAN connection.

Device

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust device specific settings.

The system-internal device name may be passed on to the name server with DHCP.

The device domain is part of the device FQN and is stored in certificates and name servers. default: local

Password of the admin account. The name admin can not be changed. The standard password is **admin**.

Restart Gateway restarts the complete device which corresponds to a power cycle. **Restart Server** only restarts the server software. After both actions you have to log in again.

Shows you the status of the server.
Memory usage equals to the memory used and reserved.
Uptime Server shows the runtime of the server software.
Uptime Gateway shows the runtime of the whole device

Backup & Update

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can archive, restore and update your device.

Warning:

File Upload overwrites the current settings.
With an Upload Complete Backup, settings not present in the backup are not deleted.
For a clear recovery, we recommend a Restore factory settings beforehand.

Contains all connections, datapoints and OPC UA and history settings of these datapoints.

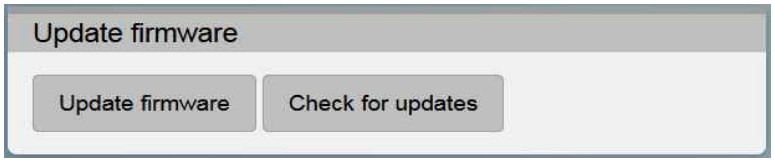
Contains all settings of the webconfigurator exept connections, datapoints, users, admin, certificates and Node-RED projects.

All users exept admin.

All settings for admin.

Complete backup including connections, datapoints, users, admin, certificates and Node-RED projects.

see chapter “Update firmware”

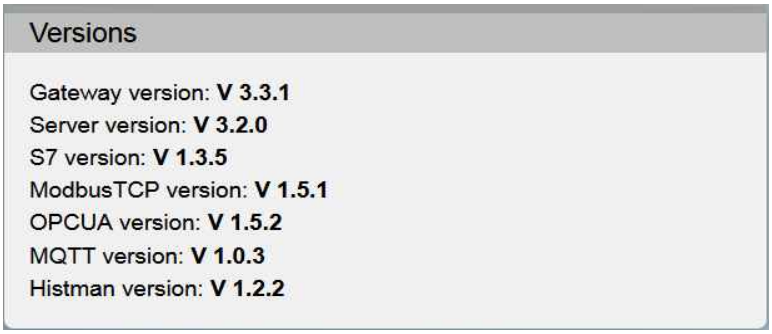


Remove all user data and settings. After this action the LAN address of the device is 192.168.80.60

Backup & Update

Download the log files to analyse what happened in case of an error.

Shows you the versions of all software components.

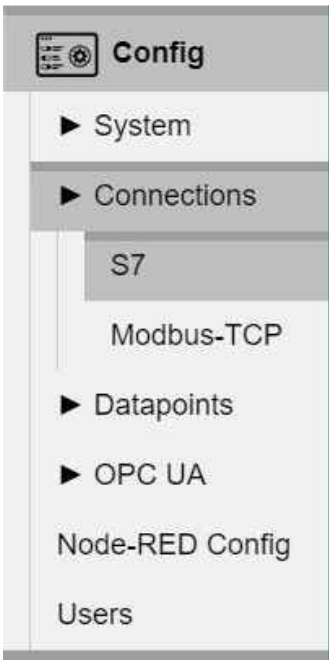


Connections

S7-Connections

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can manage the connections between the IIoT-Gateway and S7 PLCs.



Row handle to select row. Use shift or ctrl to select multiple.

Internal ID of the connection. Is used to get data from this connection in Node-RED.

Name of the connection. (freely selectable)

IP address of the PLC.

Ressource-ID (see left, part of the TSAP)

Rack number (see left, part of the TSAP)

Slot number (see left, part of the TSAP)

Tsap of the PLC. (see left, automatically calculated)

Status of the connection. As long as no data points were configured: **inactiv** If otherwise the state **running** is not stable, an error has occured.

Check for accessibility of the entered IP address, No indication that the S7 protocol works

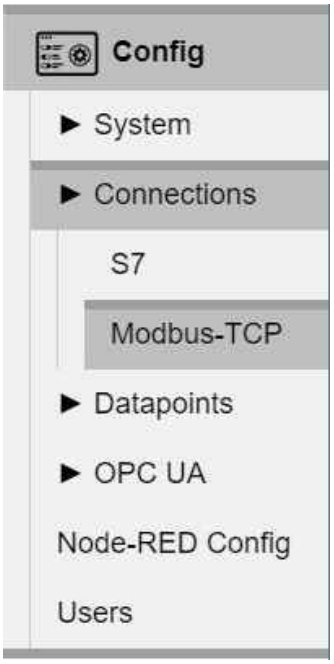
Hint 1:
TSAP will be created of
Rack-no. and slot-no. Of the CPU and of
Connection-resource-no. 00...FF(hex).
→ for Siemens-CPUs 300/ 400 it is normally **0, 2, 02**,
→ for Siemens-CPUs 1200/1500 it is normally **0, 1, 02**

Hint 2:
For connection with-CPUs 1200/1500; in TIA-Portal must
→ „Allow Put/Get“ be activated and
→ no optimized DBs may be used!

Modbus-TCP

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can manage the connections between the IIoT-Gateway and Modbus-TCP enabled devices.



Row handle to select row. Use shift or ctrl to select multiple.

Internal ID of the connection.
Is used to get data from this connection in Node-RED.

Name of the connection.
(freely selectable)

IP-address of ModbusTCP-device (server)

Port at the Modbus-TCP device
default: 502

Status of the connection.
As long as no data points were configured: **inactiv**
If otherwise the state **running** is not stable, an error has occured.

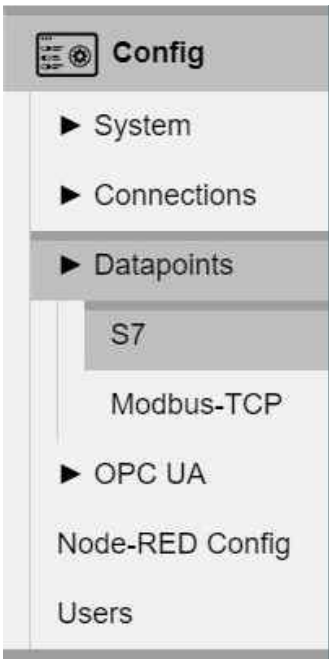
Check for accessibility of the entered IP address,
No indication that the Modbus protocol works.

Data points

S7-Data points

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can manage the data points for the configured S7 PLC's.



Row handle to select row. Use shift or ctrl to select multiple.

Name of the connection to which this data point is assigned to.

Name of the data point.
Freely selectable or assigned from an import.

Location of the data point in the PLC.

Number of the data block if space is set to DB

S7-300 Data type

Address-offset

Bit-index if data type is BOOL

Amount of data points.
Values >1 create an array which is read as a whole block at once.

The calculated address based on the provided information.

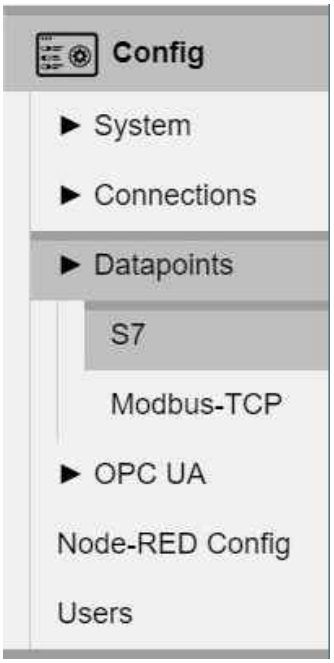
Checkbox to pass this variable to the OPC UA server.

Imported comment of the variable

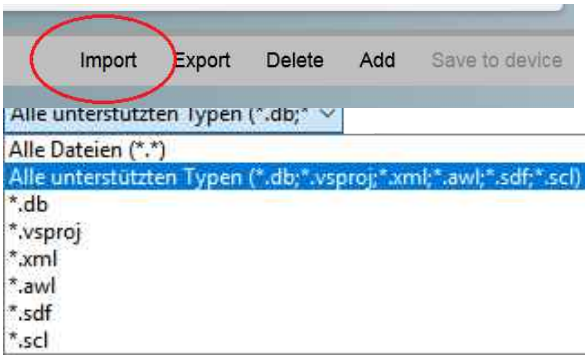
Import of S7-Variables

As an alternative to the manual configuration of the S7 variables, the import function can be used to make work easier.

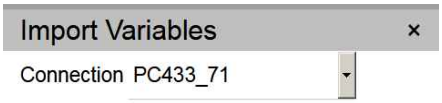
- Global variables of a Simatic Manager or TIA project can be exported as sdf file and read in here.
- Mostly data structures in DBs are interesting. For this purpose, the relevant DBs have to be exported as sources (with Simatic Manager as .awl file, TIA generates a db file) and imported here.
  Unfortunately, the DB number is lost for symbolic awl sources and the DB name for absolute awl sources.
  This information must be added manually later.
- If a visualisation with VisuStage was already implemented and the relevant variables match, an import via the VisuStage project file *.vsproj may be useful.
  In general, the VisuStage import functions for variables including symbols (also from data blocks with a few mouse clicks) are very convenient.
  However, a visualisation does not necessarily have to be created. After the variable import in the "VisuStage" program, an "empty" visualisation file *.vsproj also contains the information of all variables defined there, which are required here for the import of S7 variables.



In the S7 Datapoints window, individual or groups of variables can be added via "Import":
The following file formats can be imported:



The relevant S7 connection must be selected to which the variables to be imported are assigned.

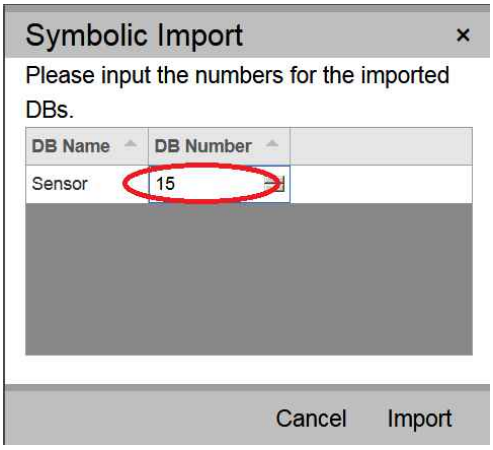


The import button is used to upload a file

Depending on the source, missing information may be queried.

When importing symbolic sources, the (correct !) DB number must (unconditionally !) be specified (Here in the example DB number 15)

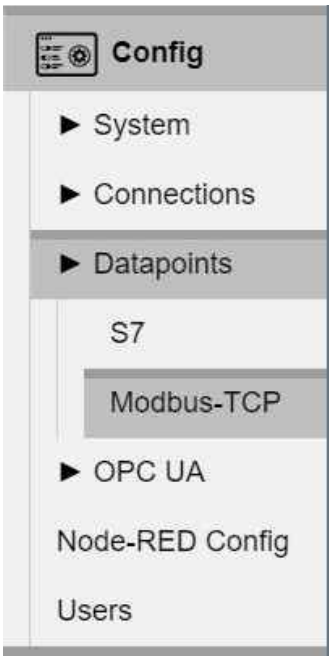
If an absolute awl source is imported, the DB names must be reassigned. (This is then "optics only", symbol names are freely selectable.)



Modbus-TCP

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menu item the data points of the connected Modbus-TCP devices are managed.



Row handle to select row. Use shift or ctrl to select multiple.

Name of the connection to which this data point is assigned to.

Name of the datapoint.
(freely selectable)

Location of the data point in the Modbus device.
IR=Input Register, HR=Holding Register,
DI=Discret Input, CL=Coil

Word- or bit-index of the data point

Datatype of the data point
for processing by the IIoT Gateway

Amount of words or bits
Values >1 create an array which is read as a whole block at once.

Word order
Only for data types with 4 bytes (DINT, DWORD, REAL).

Checkbox to pass this variable to the OPC UA server.

Comment of the variable

	Connection	Name	Space	Index	Datatype	Count	Endianess	OPC UA	Comment
	Connection_0	REG_01	IR	0	DWORD	1	Big	✗	

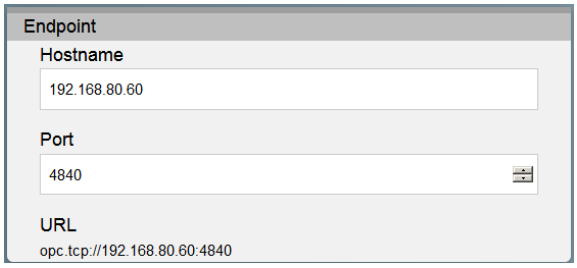
OPC UA

Application

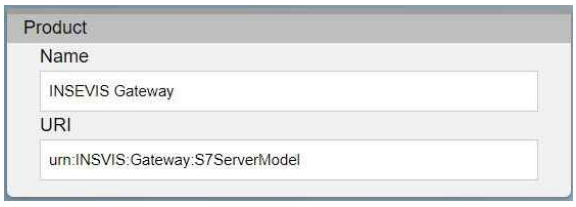
VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust the application settings of the OPC UA server.

Here the server 's URL is stored in the server, to which the client connects to the server..
Usually this is the IP address.
The client can check the match.
UA-Expert warns if there is no match, other clients evaluate it as an error (and refuse the connection).

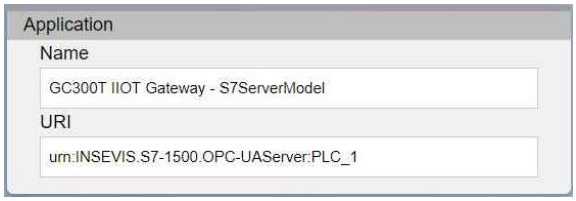


Product Name and **Product URI** are displayed under ServerStatus - BuildInfo and are freely selectable

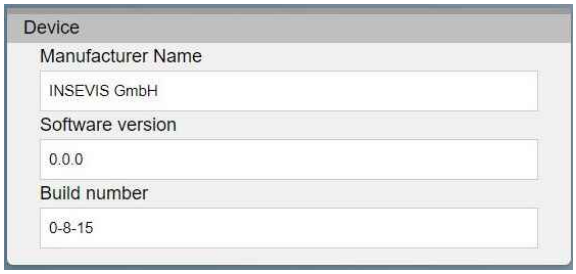


The **Application Name** represents the application in a human readable form.

The **Application URI** must be globally unique.



The **Manufacturer Name** , **Software version** and **Build number** are displayed under ServerStatus - BuildInfo and are freely selectable

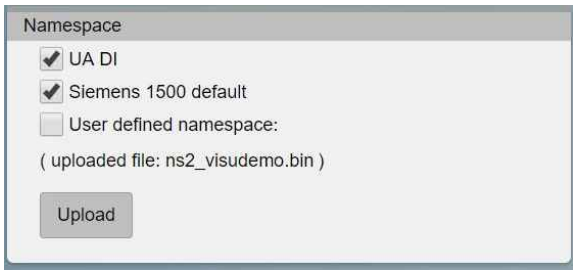


Activating of the integrated namespaces.

The **UA DI** namespace contains typedefinitions which can be referenced by other namespaces.

Siemens 1500 default represents the structure of a Siemens 1500 PLC.

User defined namespace activates a namespace uploadet by the user.

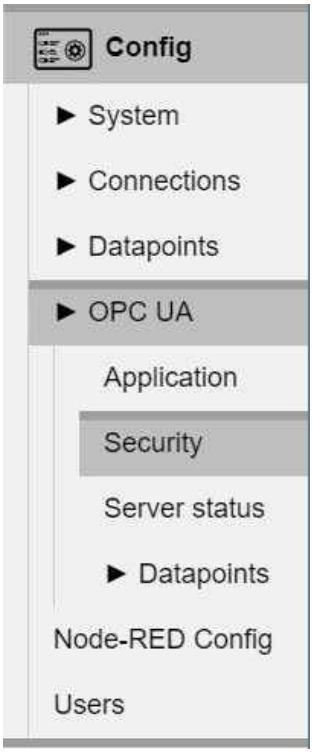


Security

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust to security settings for the OPC UA server.

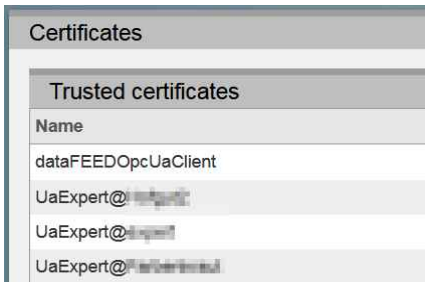
ATTENTION:
An encrypted and signed connection is strongly recommended for the transmission of machine data.
The setting **Encryption none** enables an unencrypted access and data transmission to the OPC UA server.
This poses a substantial security risk and should only be enabled for testing purposes.



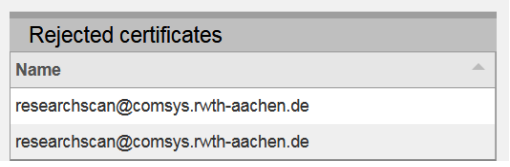
Defines the permitted connection types.
none : no encryption or signature
Basic – Sign : signed transmission
Basic – Sign & Encrypt : Encrypted and signed transmission.

Provides a **Download** for the server certificate. **Regenerate** deletes the current certificate and generates a new one. This new certificate hast to be distributed to the clients as the old one is no longer useable.
The certificate also includes the IP addresses. If access is made directly via IP addresses, the certificate should be updated after the IP address has been changed,
otherwise a connection could also be denied

Trusted certificates contains a list of certificates which are beeing trusted.



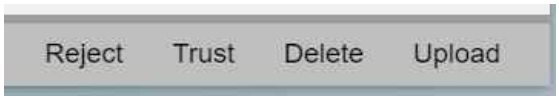
Rejected certificates contains a list of certificates which have been rejected. Upon first connection every certificate is rejected at first and has to be manually added to the trusted list.



Security

Selecting a certificate displays further information about it in this window.

Selected certificates can be moved to the corresponding list with **Reject** and **Trust**. **Delete** deletes the selected certificate and **Upload** enabels you to manually add a certificate.



ATTENTION:
The setting **Encryption none** enables an unencryptet access and data transmission to the OPC UA server.
This poses a substantial security risk and should only be enabled for testing purposes.

Server status

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menu item the status of the OPC UA server can be monitored and controlled.

Start and **Stop** controls the OPC UA server.

Start on startup starts the server with the IIoT-Gateway.

If the status indicator remains at Stop after starting the server, there is probably a configuration error.
Error messages can be read out by downloading the log file.

S7 Datapoints in the OPC UA Server

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust to previously submitted data points for the OPC UA server.

Row handle to select row. Use shift or ctrl to select multiple.

Name of the connection to which this data point is assigned to.
(taken from data points)

Name of the data point.
(taken from data points)

Address of the data point
(taken from data points)

Data type in the OPC UA namespace.
Here a different data type can be defined for OPC UA
(Must have same storage width as S7 datatype)

Node ID* of the data point
In the S7-1500 mode the variable appears automatically in the namespace under this name - according to the address under Inputs/Outputs/Memory ...
In the user defined name space the node ID must be entered here matching the defined node in the name space, to be able to map the user data to the nodes in the name space.

Type of the Node ID
(String or Numeric)
In S7-1500 mode always string

Browse name
(OPCUA browse name for the data point in the namespace)

Checkbox to activate the history for this data point.
This starts the recording of the variable value with time stamp in the time grid below in a ring buffer of the length below.

Time between samples.

The data points are updated every 100ms.
only larger values make sense.

Number of samples.
Only limited by the available storage.

* Note: For variables in data blocks it is essential that the S7 syntax "block_name.variable_name" is used.
The Node-ID is used to insert the variable into the tree, the browser name to display.

Modbus-TCP im OPC UA Server

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you can adjust to previously submitted datapoints for the OPC UA server.

Row handle to select row. Use shift or ctrl to select multiple.

Name of the connection to which this data point is assigned to.
(taken from data points)

Name of the data point.
(taken from data points)

Address of the data point
(taken from data points)

Datatype in the OPC UA namespace.
Here a different data type can be defined for OPC UA
Must have same storage width as Modbus-TCP datatype

Node ID of the data point
In the S7-1500 mode the variable appears automatically in the namespace under this name - according to the address under Inputs or Outputs
In the user defined name space the node ID must be entered here matching the defined node in the name space, to be able to map the user data to the nodes in the name space.

Type of the Node ID
String or Numeric
In S7-1500 mode always string

Browse name
(OPCUA browse name for the data point in the namespace)

Checkbox to activate the history for this data point.
This starts the recording of the variable value with time stamp in the time grid below in a ring buffer of the length below.

Time between samples.

(The data points are updated every 100ms.
only larger values make sense)

Number of samples.
Only limitet by the available storage.

MQTT

MQTT (Message Queue Telemetry Transport) has become one of the standard protocols for IoT and M2M communication. The MQTT protocol works as publish-subscribe communication. There is one broker and several clients.The clients can post messages as publishers and receive messages as subscribers. The broker's task is to manage and distribute the messages.

Broker-Settings

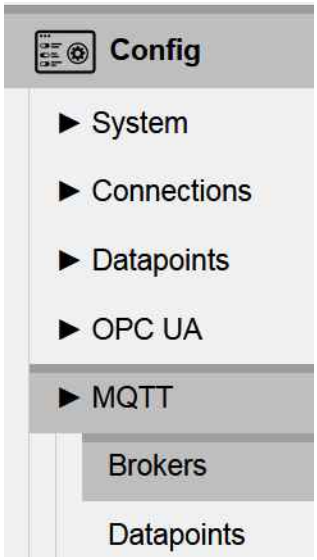
The IIoT-Gateway does not contain a MQTT-broker. Here the general settings to connect a external broker (in the local net or in the cloud) are done. The IIoT-Gateway communicates with multiple brokers but always as one client only.

The MQTT-broker is distributing messages. All communication is event-controlled.

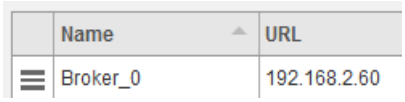
- At activated „Retain“-function the last message will be stored by the broker and on reconnection of a client delivered immediately (Otherwise he needs to wait for the next change).

MQTT supports the optional “Birth” and “Last Will and Testament” (LWT) messages.

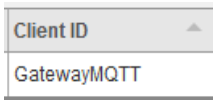
- The “Birth” message will be sent at the start of a connection of a client to inform other clients about the new client.
- The “Will” message („Last Will and Testament“, LWT) will be sent to inform other clients about the disconnected client.



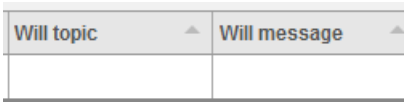
Internal **Name** of the external MQTT-Broker, (freely selectable)
and **URL** of the broker in the local net or in the cloud (either static IP-address or URL e.g. mqtt.eclipse.org)



Client ID (freely selectable),
needs to be clearly (unique) at the broker

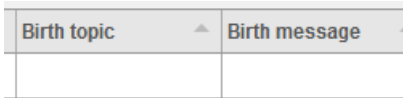


Will (last will) **-Topic** and **-payload** (optional)
will be sent when the connection of these client will be closed
(default: unused)



Will-Quality of Service
0: maximum 1x
1: minimum 1x
2: exactly 1x
Will - retainflag:
If activated, the “Will”-message will be delivered at reconnect and subscribe of a client

Birth -Topic and **-payload** (optional)
Will be sent when the connection of these client is started

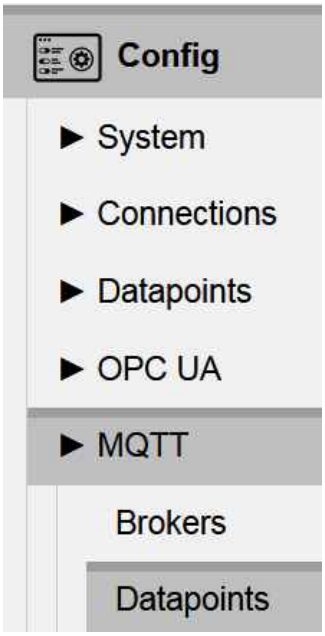


Birth - Quality of Service
0: maximum 1x
1: minimum 1x
2: exactly 1x
Birth - retainflag:
If activated, the “Birth”-message will be delivered at reconnect and subscribe of a client

Connection status
As long as no data points were configured: **inactiv**
If otherwise **running** does not stay, there is an error at the configuration
Ping as Check for accessibility of the entered IP address, no indication that the MQTT protocol works

MQTT

Datapoints-Settings



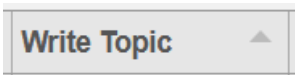
Handle, to mark lines
Mark areas by Ctrl / Shift

Name of the local (S7- or Modbus-) connection, to whom the variable belongs

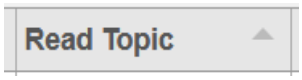
Name of the variable.
Selection of existing variables of existing connections by drop-down-menue

Assigning the variables to a configured broker

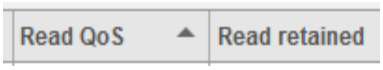
Definition of a **Topic to Write** data into the PLC
Therefore a subscription will be created at the broker
(i.e. the IIoT-Gateway works a **Subscriber**)



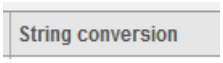
Definition of a **Topic to Read** data from PLC.
If these data change they will send from IIoT-Gateway to broker by publish
(I.e. the IIoT-Gateway works as **Publisher**)



Read Topic - Quality of Service
0: maximum 1x
1: minimum 1x
2: exactly 1x
Read Topic - retainflag:
If activated, the message will be delivered at reconnect and subscribe of a client



The PLC-data usually will be sent binary
If this option is activated, the PLC-data will be converted referring to their configured type information into a string.



ATTENTION:

MQTT is currently only available unencrypted.
Data could theoretically be read or manipulated by third parties.
Sensitive data should only be transmitted via trustworthy networks.

Node-RED
Config

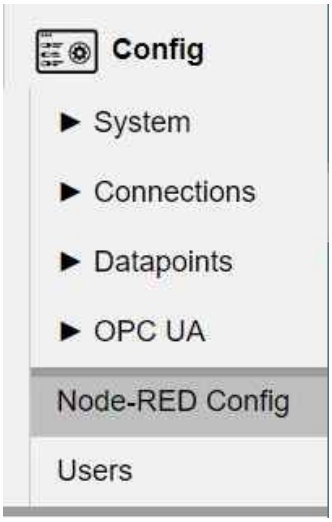
external VIDEO-Tutorials available
For the work with Node-RED are available multiple instructional YouTube® videos.

In this menue you can adjust the behaviour of Node-RED. The Node-RED-server is an additional function without any warranty or service from INSEVIS. Use only well-known and successfully tested Node-RED-nodes for your projects.

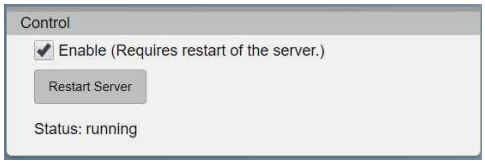
Warnung

CAUTION:
Do not activate Node-RED if you don't need it as it consumes substantial system resources.

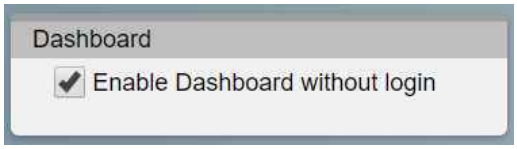
By the unknown origin of Node-RED-nodes INSEVIS does not takes over any warranty for their functions or service for Node-RED-projects.



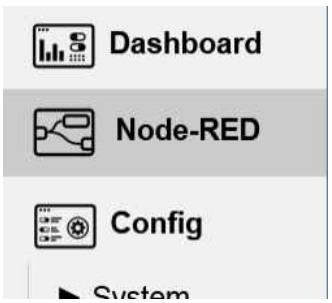
Enable starts Node-RED together with the IIoT-Gateway. **Restart Server** restarts the software of the IIoT-Gateway to immediately apply the changes to **Enable**.



Enables the access to the dashboard without a prior login.



Routes



Menue entry „Node-Red“ opens a new window containing the Node-Red „Routes-Editor“.

The communikation between NodeRed and the configured variables uses MQTT.

An internal MQTT broker must be configured for this:
Server localhost, port 1883, no SSL/TLS.

To read the variables the following MQTT-topic is used:
gateway_internal/<Connection-ID>/<Address>/R
To write the variables the following MQTT-topic is used:
gateway_internal/<Connection-ID>/<Address>/W
z.B. gateway_internal/0/MD420/R

The payload data is binary. A conversion can be done via a script: e.g.

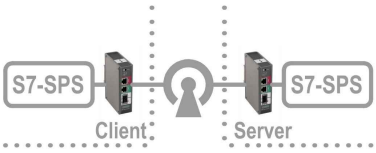
```
var buffer = Buffer.from(msg.payload);
msg.payload = buffer.readInt32LE(0);
return msg;
```

openVPN

The IIoT Gateway uses openVPN with openSSL to transfer machine data via an encrypted connection.

Site-To-Site-Topology

Secure client/server connection between two S7-“islands“



This topology is to realize a direct and secure client/server connection between 2 S7-“islands“ through a „insecure“ company net without using a cloud or portal.

Requirements:

- IP-address settings in the company net are static,
- address of the „unsecure“net (e.g. 192.168.2.0) is normally pre-defined
- a local net for the IIoT-Gateway as openVPN-server (e.g. 192.168.80.0) and
- a local net for the IIoT-Gateway as openVPN-client (e.g. 192.168.90.0) will be defined

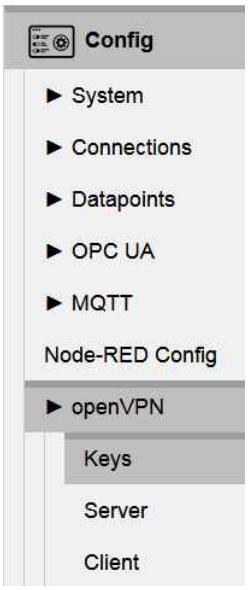
Hint:

- The local nets of both „islands“ must be different.

Procedure:
1: Configuration on the openVPN-**Server-IIoT-Gateway**:

Step 1.0: Before generating of certificates the system time must be checked to be correctly so that valid expiry dates are generated. (If the IIoT-Gateway was longer powered off, the low battery could cause a wrong system time.)

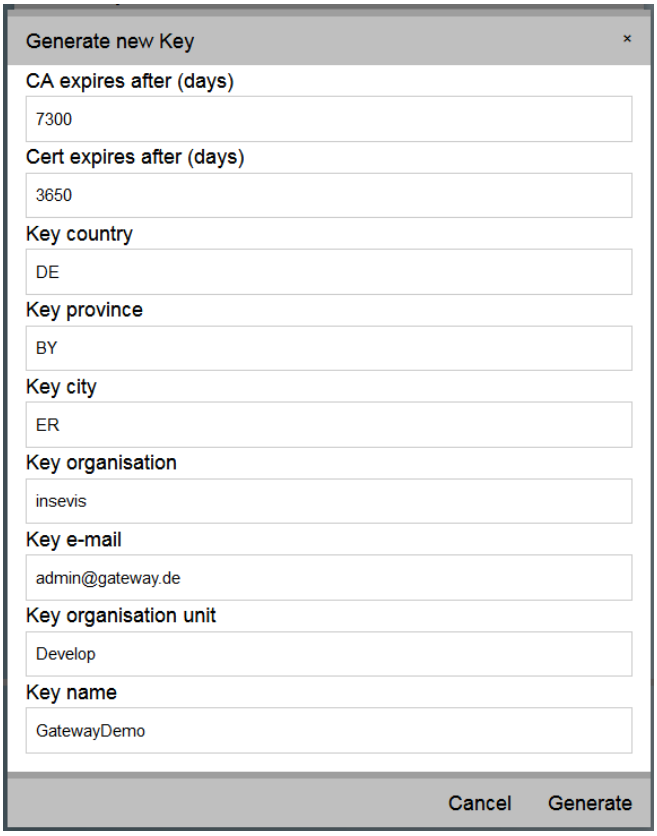
Step 1.1: Generate a local certificate authority = CA on the openVPN-**Server-IIoT-Gateway**:



Fill the mask with usefull content

These data will be bounded to the certificates

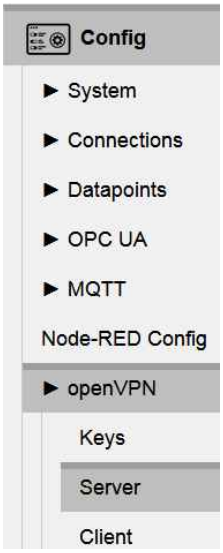
Caution:
The entries in „... expires after ...“ determines the period of validity of the certificates



openVPN

Site-To-Site-Topology

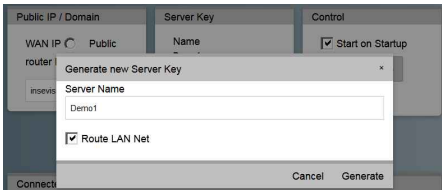
Step 1.2: Create a client on the openVPN-**Server-IIoT-Gateway**



- Assign the static public IP-address of the server:
  Button „WAN-IP“ + WAN-adress
- activate „Start on Startup“
- „Save to device“
- Create server by button „Generate new“

Create a **Server name**, with which the "island" can be assigned

(Option „Route LAN Net“ means, that network addresses in the server-LAN (in sample 192.168.80.0) are accessible form the other “island”)



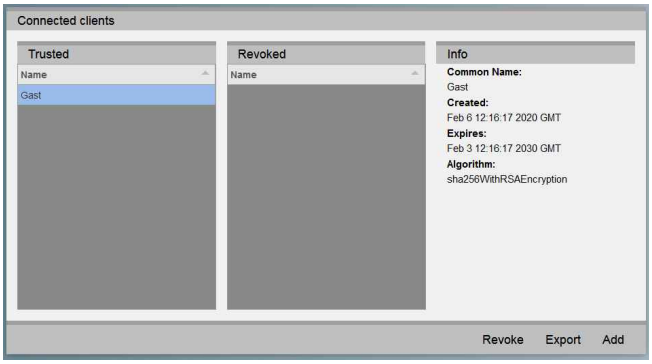
Create a **Client** in „Connected Clients“ by button „Add“

- Create a **Client name** with which the other "island" can be assigned

(Option „Route LAN Net“ means, that network addresses in the client-LAN (in sample 192.168.90.0) are accessible form the server-“island”)
Hint: Because this network is unknown until yet, this address needs to be typed in.

Mark the yet generated client and save it by the button „Export“.

(is exported at the PC normally to „Download“-directory to file „servername_clienname.tar.gz“)



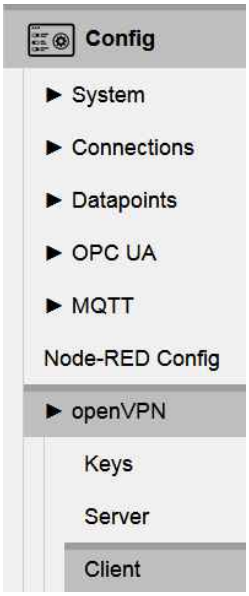
openVPN

Site-To-Site-Topology

2: Configurations on the openVPN-**Client-IIoT-Gateway**:

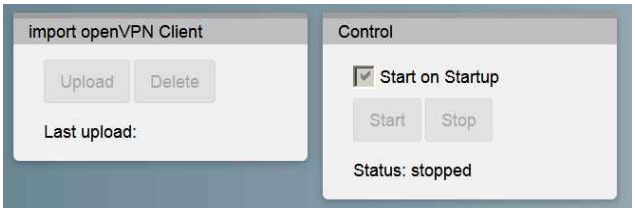
Step 2.0: Before using of certificates the system time must be checked to be correctly.

Step 2.1: Import configuration on the openVPN-Client-IIoT-Gateway



In the Webconfig of the client-IIoT-Gateway:

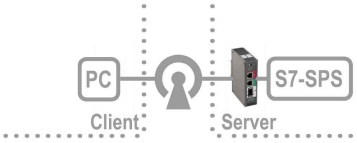
- Upload of the configuration file „servername_clienname.tar.gz“exported from server
- activate „Start on Startup“
- „Save to device“



openVPN

Remote maintenance 1-Topology

Secure client/server connection betweenS7-“island“ and a PC



If a client „island“ in the Site-To-Site-open-VPN-Topology will be replaced by a PC, arises a remote access to the configuration shell of the IIoT-Gateways (via WAN-port(!) as well to the PLC(s) behind (– with minor restrictions – you can not search in the remote network, you need to know it).

Requirements:

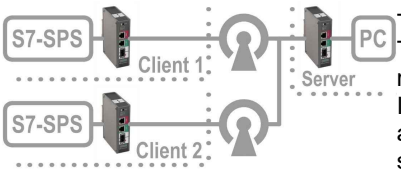
- openVPN must be installed on the PC
- decompress the exported file „servername_clienname.tar.gz“ (e.g. Win-7z).
- Rename the file "client.conf" into a meaningful client name with suffix „.ovpn“ (e.g. machine_xy.ovpn)
- move all 4 decompressed files to C:\Program Files (x86)\openVPN\config\clientname\...
  or use the gui's import function
- start a VPN-connection via openVPN-GUI („machine_xy – connect).

Hints:

- In practice, this is imaginable within a static configured company net.
  (Rare a IIoT-Gateway will be accessible by a fixed IP-address via internet directly.)
- The option „Route LAN Net“ of the server configuration allows the PC-access to the PLC (and further components at the LAN-port of the IIoT-Gateway). Without this option only the IIoT-Gateway-shell is accessable.
- The option „Route LAN Net“ of the client configuration is not useful for that case.

Remote maintenance 2-Topology

Secure client/server connection of multiple two S7-“islands“ by openVPN through a switchboard



This scenario arises when a PC is inserted at the server side in the Site-To-Site-open-VPN-Topology.
Thereby this PC has a remote-access to the PLC(s) of the remote network (– with minor restrictions – you can not search in the remote network, you need to know it).
Is the server-side e.g. in a home-office, what does not belong to to a company-IT-administration, it is possible to “tunnel” vie internet as long the client-IIoT-Gateways have a standard internet access.

Requirements:

- IP-address settings in the company net are static,
- a local network for the IIoT-Gateway as openVPN-Server and
- each one local network for the IIoT-Gateway as openVPN-Client will be assigned.

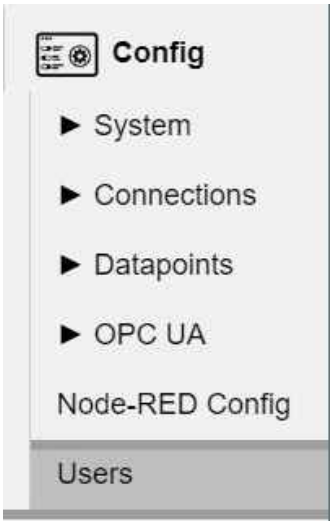
Hints

- If communication takes place via the "real" Internet, a global IP address is required for the server
  (e.g. by DynDNS) and this is to be assigned as „Public router IP“ and in the router is to configure a referring port-forwarding (see referring router-manuals).
  The external address of the server does not matter, but the WebConfigurator needs to insert it into the client-configuration.
- If the openVPN-server at the WAN-port will be configured by DHCP, a name server must exist.
  (perhaps the DHCP-Server takes over the device-FQN of the IIoT-Gateway automatically.
  This must be assigned in the server als „Public router IP“ *.
- If IP-addresses changes, this configuration must be repeated.

Users

VIDEO-Tutorial available
For this menue you find a link to a instructional YouTube® video in the download section of Insevis.com

In this menue you find the user management. **Doubleclick** on an entry to **edit** it.



Name of the user.
Freely selectable.

E-Mail address of the user.
Freely selectable.

Information text about the user.

Privileges of the user.
Used to limit access to specific sections of the webconfigurator.

Startpage of the user.
The page to which the user will be redirected to after login.
Make shure the user has sufficient privileges to access this site.

INSEVIS

INSEVIS - Gesellschaft für industrielle
Systemelektronik und Visualisierung mbH

Am Weichselgarten 7
D - 91058 Erlangen

Fon: +49(0)9131-691-440
Fax: +49(0)9131-691-444
Web: www.insevis.de
E-Mail: info@insevis.de

Zertifiziert nach DIN EN ISO 9001:2015

Qualifiziertes Personal

Die hier beschriebenen Installationen dürfen nur von qualifiziertem Personal (fachlich ausgebildete Personen, die die Berechtigung nachgewiesen haben, Geräte, Systeme und Stromkreise nach allgemeinen gültigen Standards in Betrieb zu nehmen, zu erden und zu kennzeichnen) vorgenommen werden.

Hinweise zur Sicherheit

Diese Anweisung beinhaltet Hinweise, die zur ersten Kommunikation mit den INSEVIS-Geräten dienen und ersetzt kein Handbuch. Informieren Sie sich vor der weiteren Programmierung im Handbuch über die jeweiligen Sicherheitshinweise über bestimmungsgemäßen Gebrauch, qualifiziertes Personal und Instandhaltung.

Marken

Haftungsausschluss