

OT/IT NETWORK GATEWAY

# IGW/936A

with DNP/8331



## System Reference

# CONTENT

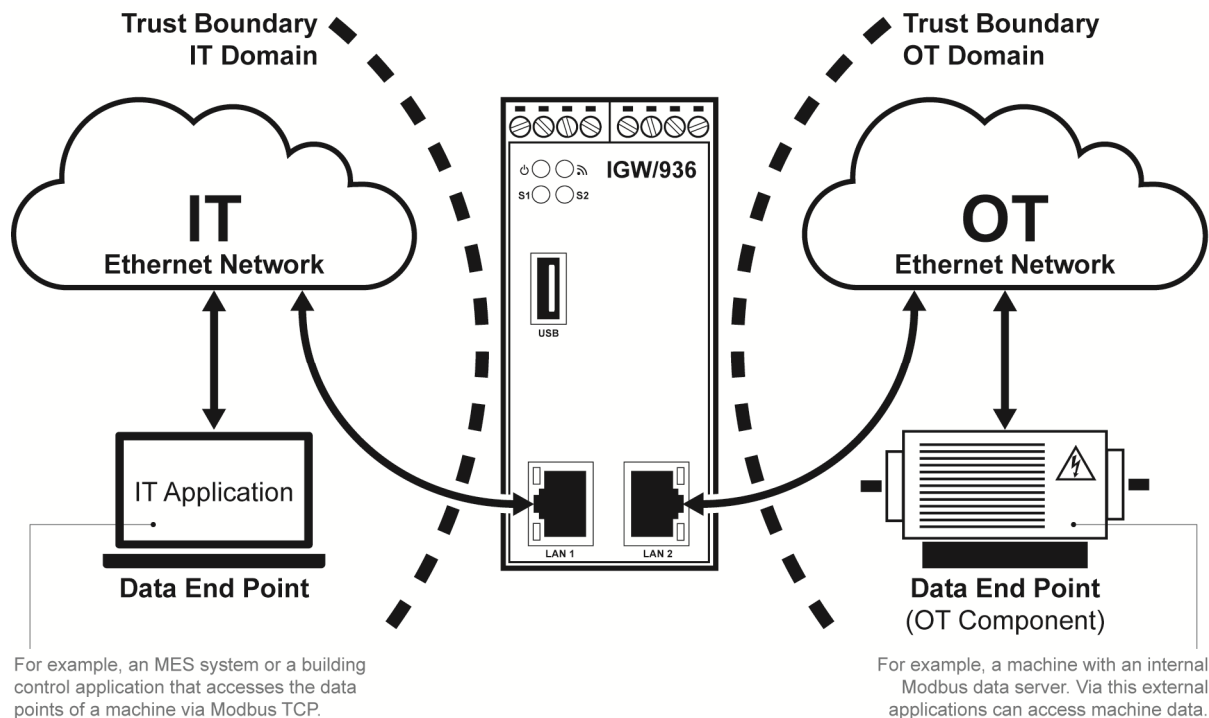
<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	Checklist .....	5
1.2	Required Equipment .....	5
1.3	Document Conventions.....	5
<b>2</b>	<b>SAFETY GUIDELINES .....</b>	<b>6</b>
<b>3</b>	<b>OVERVIEW.....</b>	<b>7</b>
3.1	Control Elements.....	7
3.2	Features and Technical Data .....	8
<b>4</b>	<b>PINOUTS .....</b>	<b>9</b>
4.1	10/100 Mbps Ethernet Interface LAN1 .....	9
4.2	10/100 Mbps Ethernet Interface LAN2 .....	9
4.3	USB 2.0 Host Port .....	9
4.4	Screw Terminals .....	10
4.5	LED Functions .....	10
<b>5</b>	<b>CABLE CONNECTIONS .....</b>	<b>11</b>
5.1	Ethernet Link .....	11
5.2	Power Supply.....	12
<b>6</b>	<b>SSV/WEBUI.....</b>	<b>13</b>
6.1	Status.....	14
6.2	System .....	15
6.2.1	System > System Identification .....	15
6.2.2	System > System Management .....	15
6.2.3	System > Firmware Update .....	16
6.2.4	System > Time and Date .....	17
6.2.5	System > COM Ports (Serial Ports) .....	17
6.2.6	System > Watchdog.....	18
6.2.7	System > Logging .....	20
6.3	Network.....	21
6.3.1	Network > WAN.....	21
6.3.2	Network > LAN1.....	22
6.3.3	Network > LAN2.....	23
6.3.4	Network > Firewall and NAT.....	24
6.4	Services.....	25
6.4.1	Services > General .....	25
6.4.2	Services > OpenVPN .....	26
6.4.3	Services > DynDNS.....	27
6.4.4	Services > DHCP Server.....	28
6.4.5	Services > SNMP .....	28
6.4.6	Services > Remote Access (OpenSSH) .....	29
6.4.7	Services > SSV/WebUI .....	30
6.5	Proxies .....	31



6.5.1	Proxies > Web.....	31
6.5.2	Proxies > DNS.....	32
6.5.3	Proxies > FTP.....	32
6.5.4	Proxies > TCP .....	33
6.5.5	Proxies > UDP .....	33
6.6	Logout.....	34
<b>7</b>	<b>APPLICATION EXAMPLES .....</b>	<b>35</b>
7.1	OT/IT Domain Isolation .....	35
<b>8</b>	<b>CREATING A VPN CONNECTION .....</b>	<b>39</b>
<b>9</b>	<b>HELPFUL LITERATURE .....</b>	<b>42</b>
	<b>CONTACT .....</b>	<b>42</b>
	<b>DOCUMENT HISTORY .....</b>	<b>42</b>

# 1 INTRODUCTION

This document describes the basic hardware components, the necessary cable connections as well as the web-based user interface (SSV/WebUI) of the OT/IT Network Gateway IGW/936A.



**Figure 1: Typical application with the IGW/936A**

**Figure 1 shows the IGW/936A** as an infrastructure module for domain isolation between the Ethernet based networks of an IT and OT environment. In addition, various OT modules in RS485-based bus systems, such as Modbus RTU, can be accessed from an IT Ethernet LAN via an IGW/936A. Thereby an access rights management down to the single Modbus data point is possible.

Further applications for the IGW/936A are:

- Industrial OT/IT Firewall
- Proxy Server
- VPN Gateway
- Linux Device Server



**Please note:**

To operate the IGW/936A further equipment is needed. Please see **chapter 1.2**.

## 1.1 Checklist

---

Compare the content of your IGW/936A package with the checklist below. If any item is missing or appears to be damaged, please contact SSV.

- ✓ OT/IT Network Gateway IGW/936A

## 1.2 Required Equipment

---

To configure the IGW/936A a computer with the following features is required:

- Windows 7 or higher
- Web browser (e.g. Firefox, Chrome)
- 10/100 Mbps Ethernet LAN interface and TCP/IP configuration

## 1.3 Document Conventions

---

Convention	Usage
<b>bold</b>	Important terms
<code>monospace</code>	Filenames, Pathnames, program code, command lines

**Table 1: Conventions used in this document**

## 2 SAFETY GUIDELINES

---

Please read the following safety guidelines carefully! In case of property or personal damage by not paying attention to this document and/or by incorrect handling, we do not assume liability. In such cases any warranty claim expires.



**ATTENTION!**  
**OBSERVE PRECAUTIONS FOR HANDLING – ELECTROSTATIC SENSITIVE DEVICE!**

- The power supply should be in immediate proximity to the device.
- The power supply must provide a stable output voltage between 12 – 24 VDC. The output power should be at least 2.5 W.
- Please pay attention that the power cord or other cables are not squeezed or damaged in any way when you set up the device.
- Do NOT turn on the power supply while connecting any cables, especially the power cables. This could cause damaged device components! First connect the cables and THEN turn the power supply on.
- The installation of the device should be done only by qualified personnel.
- Discharge yourself electrostatic before you work with the device, e.g. by touching a heater of metal, to avoid damages.
- Stay grounded while working with the device to avoid damage through electrostatic discharge.

## 3 OVERVIEW

### 3.1 Control Elements

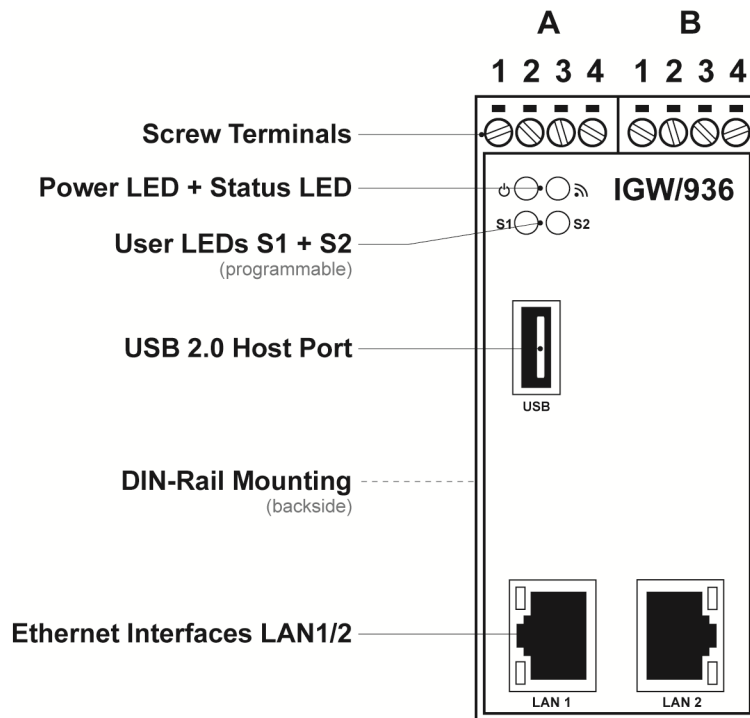


Figure 2: Front view

## 3.2 Features and Technical Data

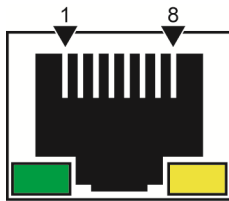
<b>Processor</b>	
Manufacturer / Type	Sochip S3 with ARM Cortex-A7 CPU (DNP/8331)
Clock speed	1008 MHz
<b>Memory</b>	
RAM	128 MB DDR3 SDRAM
Storage media	8 GB NAND Flash mass storage for operating system and application software
<b>Interfaces</b>	
Ethernet	2x 10/100 Mbps (RJ45)
USB	1x USB 2.0 Host
Serial I/Os	1x RS485 serial port (screw terminal) 1x RS232/RS485 serial port (screw terminal)
<b>Special Functions</b>	
RTC	1x Real Time Clock
Watchdog	1x Timer watchdog (hardware-based, software-configurable) 1x Power supervisor (hardware-based)
Boot loader	U-Boot boot loader with A/B dual boot partitions
Operating system	SSV Debian Buster Linux
Administration	SSV/WebUI plus firmware
Security	TCP/IP protocol stack with IPv4 and IPv6 support and various security protocols Firewall with netfilter + iptables, setup via SSV/WebUI
<b>Displays / Control Elements</b>	
LEDs	1x Power 1x Status 1x System status (programmable) 1x VPN status (programmable)
<b>Electrical Characteristics</b>	
Power supply	12 .. 24 VDC (typ. 24 VDC) from external power supply
Power consumption	< 10 W
<b>Mechanical Characteristics</b>	
Protection class	IP20 industrial case for 35 mm DIN-rail mounting
Mass	< 270 g
Dimensions	112 mm x 100 mm x 45 mm
Operating temperature	0 .. 60 °C
<b>Standards and Certifications</b>	
EMC	CE
Environmental standards	RoHS, WEEE

Table 2: Technical Data



## 4 PINOUTS

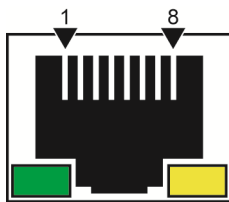
### 4.1 10/100 Mbps Ethernet Interface LAN1



Pin	Name	Function
1	TX+	10/100 Mbps LAN, TX+
2	TX-	10/100 Mbps LAN, TX-
3	RX+	10/100 Mbps LAN, RX+
4	---	Not Connected
5	---	Not Connected
6	RX-	10/100 Mbps LAN, RX-
7	---	Not Connected
8	---	Not Connected

Table 3: Pinout Ethernet interface LAN1

### 4.2 10/100 Mbps Ethernet Interface LAN2



Pin	Name	Function
1	TX+	10/100 Mbps LAN, TX+
2	TX-	10/100 Mbps LAN, TX-
3	RX+	10/100 Mbps LAN, RX+
4	---	Reserved
5	---	Reserved
6	RX-	10/100 Mbps LAN, RX-
7	---	Reserved
8	---	Reserved

Table 4: Pinout Ethernet interface LAN2

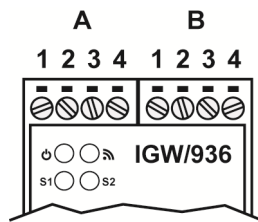
### 4.3 USB 2.0 Host Port



Pin	Name	Function
1	VCC5	5 VDC Power Output
2	DATA-	USB Host -
3	DATA+	USB Host +
4	GND	Ground

Table 5: Pinout USB host port

## 4.4 Screw Terminals



Terminal	Signal
A1	COM2 Serial Port: RS485 RX/TX+
A2	COM2 Serial Port: RS485 RX/TX-
A3	Vin + (12 .. 24 VDC)
A4	Vin -
B1	---
B2	COM3 Serial Port: TXD (RS232), RX/TX- (RS485)
B3	COM3 Serial Port: RXD (RS232), RX/TX+ (RS485)
B4	Signal Ground

Table 6: Pinout screw terminals

## 4.5 LED Functions



LED	Description	Off	Flash	On
	Power	No Power	---	Power On
	Reserved	Always Off	---	---
S1	System	Not ready	Booting	Ready
S2	VPN	Off	Connecting	Ready

Table 7: LED functions

## 5 CABLE CONNECTIONS

For the IGW/936A commissioning, only a LAN connection to a PC must be established and the 24 VDC supply voltage must be provided.

### 5.1 Ethernet Link

Connect the **LAN2 interface** of the IGW/936A with an **Ethernet LAN cable** to a PC.

The **IP address** of the LAN2 interface is ex-factory set to **192 . 168 . 1 . 126**.

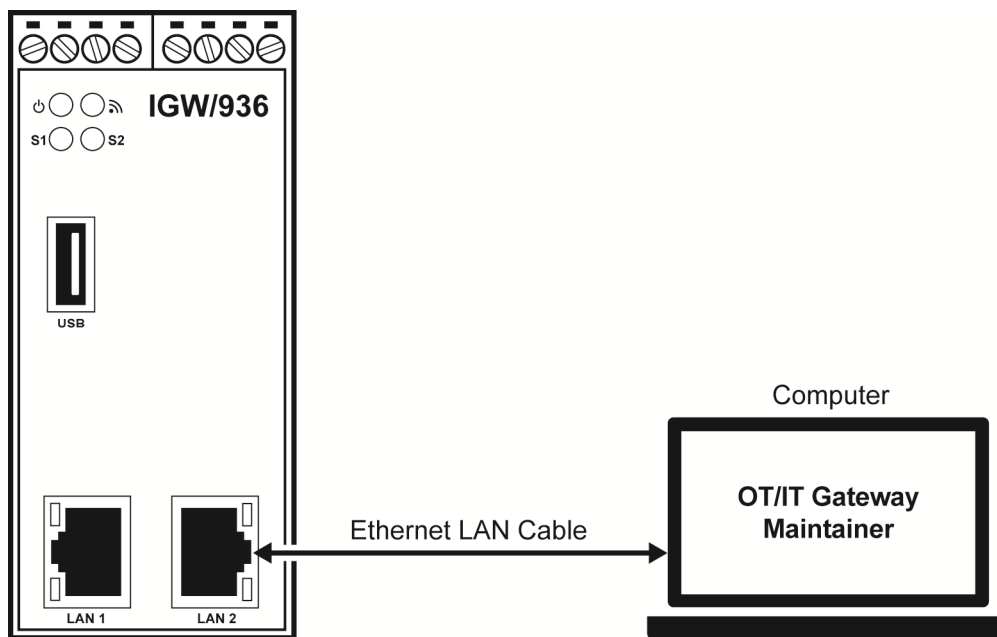
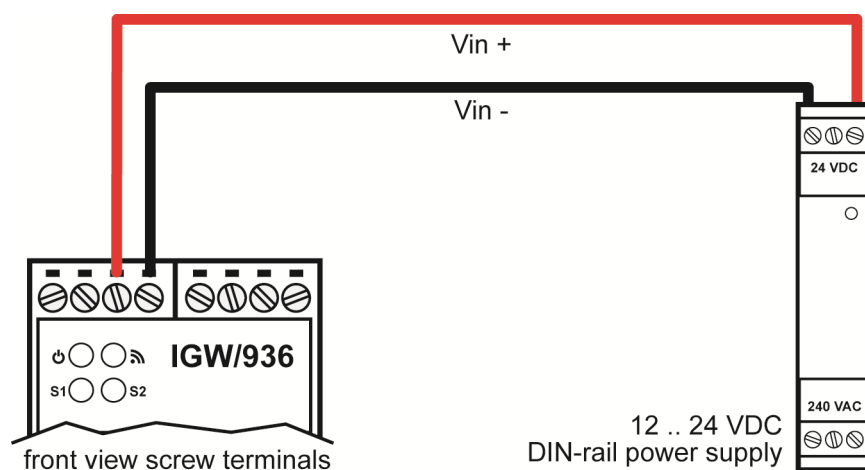


Figure 3: Ethernet LAN connection

## 5.2 Power Supply

The IGW/936A needs a supply voltage of 12 .. 24 VDC to work.

Connect the cables of the provided plug-in power supply with the screw terminals of the IGW/936A like shown in **fig. 4**.



**Figure 4: Connecting the power supply**

Terminal	Signal
A3	Vin + (12 .. 24 VDC)
A4	Vin -

**Table 8: Screw terminal power pins**



**CAUTION!**

Providing the device with a higher voltage than the regular 12 .. 24 VDC could cause damaged device components!

Do NOT power up the device while connecting the power supply or any other cables. This could cause damaged device components! First connect the power supply and THEN turn it on.

The boot process starts immediately after power up and can take up to one minute.

**LED S1** flashes during the boot process and is permanently on when the IGW/936A is ready.

## 6 SSV/WEBUI

The SSV/WebUI is the web-based user interface of SSV gateways. It enables configuration of interfaces, protocols, services and so on.

To open the login page of the SSV/WebUI enter the ex-factory **IP address and port number** of LAN2 of the IGW/936A manually in a web browser:

**192.168.1.126:7777**

Enter the supplied **username** and **password** and click on **[Login]**.



**Figure 5: Login page of the SSV/WebUI**

After a successful login, the SSV/WebUI shows a horizontal menu bar with all available functions divided into groups.



**Figure 6: Menu bar of the SSV/WebUI**

## 6.1 Status

Status		
System status		
System name :	emblinux1	System host name
System location :	SSV Embedded Systems	Location information
Contact :	support@ssv-embedded.de	Contact information
Version :	23.01.27-1110, 0.3.12-rc17	Software version
Time and date :	Thu Jun 15 12:42:17 CEST 2023	Current time and date of this system
Uptime :	2:01	System uptime
CPU load :	0.00, 0.00, 0.00	System load average
Memory :	Total: 116M, Free: 81M, Used: 34M	Random access memory
Storage :	Total: 2.6G, Free: 2.3G, Used: 99M	RootFS partition memory
Status LAN1 connection		
MAC address :	02:00:10:e4:bb:77	Physical media address
IPv4 address :	192.168.0.109/24	Current device IP addresses
IPv4 auto IP address :	169.254.12.18/16	Link local IP address
Status LAN2 connection		
MAC address :	12:00:10:e4:bb:77	Physical media address
IP address :	192.168.0.231/24	Current device IP address
IPv6 auto IP address :	fe80::5935:a53a:9f66:5a6f/64	Link local IP address
Status DNS		
Primary DNS server :	192.168.0.4	Current 1st DNS server address
Secondary DNS server :	192.168.3.1	Current 2nd DNS server address
Status route		
Default gateway :	192.168.0.4 192.168.0.4	Current default gateway

**Figure 7: Status page**

Figure 7 shows an example system status page with the addresses of all IP interfaces plus additional information about DNS servers and the default gateway.

## 6.2 System

### 6.2.1 System > System Identification

System identification

System identification			
Host name :	emblinux		Enter a device host name
Location :	SSV Embedded Systems		Enter the location of device
Contact :	support@ssv-embedded.de		Enter contact information
Serial number :	00000222386A7BB		Serial number of device
Identify device through front LED :	Flash		Flash front LED for 5 seconds

Apply
Cancel

**Figure 8: System identification**

This page summarizes various properties for gateway identification.

#### Host name

Input of an arbitrary name to be able to identify a certain gateway reliably.

#### Location

Location information or details to find the installation location of a specific gateway.

#### Contact

E-mail address input to be able to reach the person responsible for the gateway.

#### Serial number

Preset serial number of the gateway. This number can be used to answer queries about the production week, factory settings, delivery, etc. with the help of the manufacturer database.

#### Identify device through front LED

Clicking on **[Flash]** causes one of the gateway's front panel LEDs to flash for approx. 5 seconds. This allows a specific gateway to be visually identified.

### 6.2.2 System > System Management

System management

System			
Reboot system :		Reboot	Reboot will shut down and restart

System configuration			
Configuration download :		Download	Download device configuration
Configuration upload :	Datei auswählen Keine ausgewählt	Upload	Upload system configuration
Configuration reset :		Reset	Set default configuration settings and reboot

**Figure 9: System management**

The functions summarized here can be used to force a system reboot (restart) and to duplicate the configuration settings or reset them to the factory default state.

### Reboot system

Clicking on **[Reboot]** causes the gateway's operating system to shut down. This is followed by a reboot. The SSV/WebUI session must then be restarted. ***This action may cause the loss of unsaved settings.***

### Configuration download

The configuration settings of the gateway can be downloaded and saved as a file to the PC.

### Configuration upload

A configuration file saved on the PC can be uploaded to the gateway to apply the settings from this file.



#### IMPORTANT!

**This action causes the current gateway settings to be overwritten by the uploaded file. This may lock you out of the SSV/WebUI for further access.**

### Configuration reset

Allows to reset the to the factory default state. ***All individual settings made via the SSV/WebUI will be overwritten.***

## 6.2.3 System > Firmware Update

Firmware update			
Firmware info			
Firmware version :	23.01.27-1110	Current system version	(log)
Firmware hash :	026724c0a4aab531aafbb897561e19c658c73da256415a38a19a1da5fd64f588	Current firmware SHA256 hash	
Firmware slot :	A	Current firmware slot, A or B	
Firmware update via APT			
APT server address:	https://packages-debian.ssv-connect.de	Get updates from this server	
Online update :		Check	Check for new firmware

Figure 10: Firmware update

### Firmware info

Current firmware version and hash value for integrity checks on the installed firmware image.

### Firmware update via API

Check if there is a firmware update available. Download and install a new firmware image from a trusted SSV server. ***Software updates are a critical matter. In case of doubt, contact our support before performing an update.***



## 6.2.4 System > Time and Date

Time and date configuration		
<b>Local time zone configuration</b>		
Time zone :	CET Europe/Berlin ▼	Choose your time zone (log)
<b>Time and date configuration</b>		
Time setup :	<input checked="" type="radio"/> automatically <input type="radio"/> manually	Set time and date manually or over NTP
NTP server :	EU europe.pool.ntp.org ▼	Choose an NTP server
Time synchronize interval :	24 Hours ▼	Choose synchronize interval
NTP server test :	<input type="button" value="Sync"/>	Synchronize now
<b>Current system time</b>		
Time and date :	Mon Sep 19 2022 17:14:08	Time and date of this system is shown
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 11: System time and date

### Local time zone configuration

The time zone in which the gateway is located can be set here. The setting is required in order to carry out the necessary correction during a time synchronization with time servers on the Internet (correction with respect to Greenwich Mean Time (GMT)).

### Time and date configuration

The internal gateway real-time clock can be synchronized automatically via an external time server (in a LAN or on the Internet) or manually.

## 6.2.5 System > COM Ports (Serial Ports)

Serial port configuration		
<b>COM1 Properties</b>		
Application :	Remote console ▼	Application the port is used with
<b>COM2 Properties</b>		
Application :	Com port redirector ▼	Application the port is used with
Work as :	<input checked="" type="radio"/> server <input type="radio"/> client	Configure this end as server or client
Redirector port :	TCP ▼ 2222	Port to listen on
Bits per second :	115200 ▼	Choose the speed to use
Data/Parity/Stop bits :	8 ▼ None ▼ 1 ▼	Choose data,parity,stop bits
Flow control :	None ▼	Choose flow control
Hardware line driver :	<input type="radio"/> RS232 <input checked="" type="radio"/> RS485	Line driver RS232 or RS485
<b>COM3 Properties</b>		
Application :	None ▼	Application the port is used with
Hardware line driver :	<input type="radio"/> RS232 <input checked="" type="radio"/> RS485	Line driver RS232 or RS485
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 12: Serial port settings

The serial interfaces of the gateway can be used universally for different applications. Via this page individual interfaces can be reserved for operation as a **serial console (remote console)** or as a **COM port redirector**. By such a reservation the respective interface is no longer available for other applications.



**Please note:**

The **COM1 port** of this gateway is located inside the housing. It is not accessible from the outside. The COM1 port is fixed as a serial console for service purposes. **Any other usage is not possible.**

### None

The serial interface can be used by any application, e.g. by Node-RED for Modbus-based communication with external modules.

### Remote console

The respective serial port forms a console for communication with the Linux operating system. Please note that a login with username and password is required to access the console.

### Com port redirector

This function forms a protocol converter between the IP-based transport protocols UDP or TCP, which are available e.g. for the LAN interfaces, and the respective assigned serial port. The UDP or TCP side can be operated in client or server mode.

## 6.2.6 System > Watchdog

Watchdog configuration			
<b>Watchdog configuration</b>			
Enable watchdog service :	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enable or disable watchdog service
<b>Default watchdog</b>			
Enable default watchdog :	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enable or disable default watchdog script
Reboot interval :	0	minutes	Reboot system in this interval (0=off)
VPN1: Start delay :	60	minutes	Reboot if VPN not online in this time after system start
VPN1: Offline delay :	30	minutes	Reboot if VPN is offline for this time
WAN: Traffic threshold :	100	bytes per minute	Minimal incoming WAN traffic
WAN: Start delay :	60	minutes	Reboot if no WAN traffic after system start
WAN: Idle delay :	30	minutes	Reboot if no WAN traffic in online state
Mobile: reset count :	12	(~0 minutes)	Reset modem after faulting connect cycles
Mobile: reboot count :	100	(~0 minutes)	Reboot after faulting connect cycles
			<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

**Figure 13: Watchdog settings**

The gateway has various watchdog timers (or counters) intended to ensure the most trouble-free 24/7 operation possible. There are individual configuration options available for these watchdogs.

**Enable watchdog service**

Enable or disable watchdog services of the gateway.

**Enable default watchdog**

Activate the individual watchdogs listed here with the factory default settings.

**Reboot interval**

Set a time interval after which a gateway reboot is automatically triggered. The gateway reboot sets all system processes to a (defined) initial state.

**A typical use case** for this gateway is operation as a VPN client in a remote maintenance application. For this, depending on the configuration, it is important that a permanent VPN connection to an external VPN server exists. If this VPN connection is interrupted, the gateway must automatically try to reach the server again.

**The following two setting options** can be used to trigger a reboot if no VPN server connection is established within a certain time or if no VPN connection exists for a certain time.

**VPN1: Start delay**

Monitors whether a VPN connection is established within a certain time. The gateway can automatically contact a VPN server after each boot process in order to integrate itself as a client in a VPN. If this integration does not work within the time specified here, a reboot is triggered.

**VPN1: Offline delay**

Monitors how long no VPN connection to an external server has existed. If a VPN connection to the server has been interrupted and no new connection has been established, a reboot is triggered after the set time has elapsed.

In many use cases, a gateway simultaneously maintains local connections to other systems as well as various external connections to the Internet (so-called WAN connections = Wide Area Network connections), e.g., to a time server and other special cloud and IoT service platforms. WAN connections are much more vulnerable to interference than a local connection.

**The following three setting options** can be used to configure data volume-based WAN condition monitoring to trigger an automatic restart of the WAN interface hardware in case of malfunction (e.g., a reset of an internal cellular modem).

**WAN: Traffic threshold**

Number of bytes per minute that must be transferred at least from the WAN to the gateway if there is a functioning WAN connection. This threshold determines whether the WAN connection is classified as OK or critical (undetermined). ***This function is only useful for gateways with an internal cellular modem.***

**WAN: Start delay**

Time period within which the number of bytes per minute specified by the threshold value (see Traffic threshold) must be reached after a gateway boot process. Otherwise a WAN interface hardware restart is triggered after the set time has elapsed. ***This function is only useful for gateways with an internal cellular modem.***

**WAN: Idle delay**

Maximum time that may elapse without reaching the number of bytes per minute specified by the threshold (see Traffic threshold). Otherwise a WAN interface hardware restart is triggered after the set time has elapsed. ***This function is only useful for gateways with an internal mobile modem.***

### Mobile: reset count

This function is only for gateways with an internal cellular modem.

### Mobile: reboot count

This function is only intended for gateways with an internal cellular modem.

## 6.2.7 System > Logging

System logfile

Systemlog

```
-- Logs begin at Thu 2019-02-14 11:12:00 CET, end at Thu 2023-06-15 12:54:59 CEST. --
Jun 15 11:50:08 systemd[1]: Created slice system-ssv\x2dtelnetd.slice.
Jun 15 11:50:08 systemd[1]: Started Telnet Per-Connection Server (192.168.0.117:30911).
Jun 15 11:50:13 login[3979]: pam_unix(login:auth): authentication failure; logname=.telnet uid=0 euid=0 tty=/dev/pts/0 ruser=
rhost=ene.terminal user=root
Jun 15 11:50:16 login[3979]: FAILED LOGIN (1) on '/dev/pts/0' from 'ene.terminal' FOR 'root', Authentication failure
Jun 15 11:50:21 login[3979]: pam_unix(login:session): session opened for user root by .telnet(uid=0)
Jun 15 11:50:21 systemd-logind[563]: New session c2 of user root.
Jun 15 11:50:21 systemd[1]: Started Session c2 of user root.
Jun 15 11:50:21 login[3991]: ROOT LOGIN on '/dev/pts/0' from 'ene.terminal'
Jun 15 11:50:24 telnetd[3978]: telnetd: peer died
Jun 15 11:50:24 systemd-logind[563]: Session c2 logged out. Waiting for processes to exit.
Jun 15 11:50:24 systemd[1]: ssv-telnetd@0-192.168.0.109:23-192.168.0.117:30911.service: Succeeded.
Jun 15 11:50:24 systemd[1]: session-c2.scope: Succeeded.
Jun 15 11:50:24 systemd-logind[563]: Removed session c2.
Jun 15 11:50:34 login[3996]: pam_unix(login:session): session opened for user root by SHELLINABOX(uid=0)
Jun 15 11:50:34 systemd-logind[563]: New session c3 of user root.
Jun 15 11:50:34 systemd[1]: Started Session c3 of user root.
Jun 15 11:50:34 login[4006]: ROOT LOGIN on '/dev/pts/0' from '192.168.0.117'
Jun 15 11:50:54 webconfig[4028]: [admin]: changed: /etc/ssvconfig/config/openssh.cfg (WUI_chk_service='on')
Jun 15 11:50:54 webconfig[4028]: [admin]: changed: /etc/ssvconfig/config/openssh.cfg (WUI_password='****')
Jun 15 11:50:55 systemd[1]: Reloading.
Jun 15 11:50:58 systemd[1]: Reloading.
Jun 15 11:51:00 systemd[1]: Reloading.
Jun 15 11:51:03 systemd[1]: Starting OpenBSD Secure Shell server...
Jun 15 11:51:03 sshd[4100]: Server listening on 0.0.0.0 port 22.
Jun 15 11:51:03 sshd[4100]: Server listening on :: port 22.
Jun 15 11:51:03 systemd[1]: Started OpenBSD Secure Shell server.
Jun 15 11:51:10 sshd[4118]: Accepted password for root from 192.168.0.117 port 30926 ssh2
Jun 15 11:52:13 systemd[1]: session-c3.scope: Succeeded.
Jun 15 11:52:13 systemd-logind[563]: Session c3 logged out. Waiting for processes to exit.
Jun 15 11:52:13 systemd-logind[563]: Removed session c3.
Jun 15 11:52:22 webconfig[4127]: [admin]: changed: /etc/ssvconfig/config/openssh.cfg (WUI_password='****')
Jun 15 11:52:23 sshd[4100]: Received signal 15; terminating.
Jun 15 11:52:23 systemd[1]: Starting OpenBSD Secure Shell server...
```

Download log file :
Download
Download and save log as file
Download service startup graph :
Download
SVG graphic showing service initialization

**Figure 14: Logging settings**

The gateway generates a log file with extensive entries at runtime. It is used for diagnostics and for finding the cause of unusual system behaviour and other events.



**Please note:**

The log file is regenerated with every gateway boot process and is lost when the supply voltage is switched off.

### Download log file

Download and save the log file to the PC.

### Download service startup graph

Download and save a graph in SVG-format with an overview of the start-up of individual system services to the PC.

## 6.3 Network

### 6.3.1 Network > WAN

Wide area network configuration

WAN configuration			
WAN interface :	LAN1 ▾	WAN main interface	(log)
WAN watchdog			
WAN test interval :	Disabled ▾	Ping check interval	
Internet :	kernel.org	Check	Ping test to address
			<div>Apply</div> <div>Cancel</div>

**Figure 15: WAN settings**

In many use cases, a gateway simultaneously maintains local connections to other systems as well as various external connections to the Internet (so-called WAN connections = Wide Area Network connections), e.g., to a time server and other special cloud and IoT service platforms. WAN connections are much more susceptible to disturbances than local connections.

The following setting option can be used to configure ping-based WAN status monitoring (ping watchdog) in order to select a different physical gateway interface as the WAN interface in the event of a disturbance (**WAN fallback interface**, for example LAN2 instead of LAN1).

#### WAN configuration

Select a gateway interface for the WAN connection (only IP-capable interfaces can be selected here, e.g. LAN1).

#### WAN watchdog

The ping watchdog for the WAN interface can be activated here. To activate it, a ping test interval time must be selected (e.g. one ping test every 15 minutes). Furthermore, the DNS name or the IP address of the system that is to be reached via the WAN interface by ping test must be selected. In addition, the action to be performed in the event of an error in the ping test can be defined (see **WAN fallback interface**).

### 6.3.2 Network > LAN1

Local area network configuration		
<b>Interface configuration for LAN1 (10/100 MBit)</b>		
Enable/Disable interface :	<input checked="" type="checkbox"/>	Enable or disable interface LAN1
<b>IPv4 address configuration</b>		
IPv4 address setup :	<input checked="" type="radio"/> automatically <input type="radio"/> manually	IP configuration through DHCP or static
Add more addresses:	<input type="checkbox"/>	Enable or disable alias IP address
Use a DNS server address :	<input type="checkbox"/>	Use specific DNS server
<b>IPv6 address configuration</b>		
IPv6 address setup :	<input checked="" type="radio"/> automatically <input type="radio"/> manually	IP configuration for IPv6
<b>Expert configurations</b>		
MTU :	<input checked="" type="radio"/> default <input type="radio"/> 1500	The maximum transmission unit in bytes
Metric :	10	The metric of the route
Bridge :	<input type="checkbox"/> VPN1	Bridge this interface with VPN1
Enable AutoIP address :	<input type="checkbox"/>	Enables link local address
Enable UPnP discovery :	<input checked="" type="checkbox"/>	Enables UPnP discovery
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 16: LAN1 settings

#### Interface configuration for LAN1

Enable or disable the LAN1 interface.

#### IPv4 address configuration

IPv4 address setting options for the LAN1 interface. An automatic IP address assignment via DHCP or manual address entry are possible. Please note that more than one IP address can be assigned to the LAN1 interface.

#### IPv6 address configuration

IPv6 address setting options for the LAN1 interface. Similar to the IPv4 address assignment, automatic address assignment via DHCP or manual address entry of IPv6 addresses are possible.

#### Expert configurations

Various "expert settings" are available. Changes should only be made by appropriately trained personnel. **Enable UPnP discovery** (UPnP = Universal Plug and Play) is a special case. If this function is enabled, the gateway can be searched in a local network with an UPnP-capable device without knowing the IP address of the LAN1 interface.

### 6.3.3 Network > LAN2

Local area network configuration		
<b>Interface configuration for LAN2 (10/100 MBit)</b>		
Enable/Disable interface :	<input type="checkbox"/>	Enable or disable interface LAN2
<b>IPv4 address configuration</b>		
IPv4 address setup :	<input type="radio"/> automatically <input checked="" type="radio"/> manually	IP configuration through DHCP or static
Address :	192.168.1.126 / 24	Device IP address
Add more addresses:	<input type="checkbox"/>	Enable or disable alias IP address
Default gateway :		Enter default gateway address
Use a DNS server address :	<input type="checkbox"/>	Use specific DNS server
<b>IPv6 address configuration</b>		
IPv6 address setup :	<input checked="" type="radio"/> automatically <input type="radio"/> manually	IP configuration for IPv6
<b>Expert configurations</b>		
MTU :	<input checked="" type="radio"/> default <input type="radio"/> 1500	The maximum transmission unit in bytes
Metric :	20	The metric of the route
Bridge :	<input type="checkbox"/> VPN2	Bridge this interface with VPN2
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 17: LAN2 settings

#### Interface configuration for LAN2

Enable or disable the LAN2 interface.

#### IPv4 address configuration

IPv4 address setting options for the LAN1 interface. An automatic IP address assignment via DHCP or manual address entry are possible. Please note that more than one IP address can be assigned to the LAN2 interface.

#### IPv6 address configuration

IPv6 address setting options for the LAN1 interface. Similar to the IPv4 address assignment, automatic address assignment via DHCP or manual address entry of IPv6 addresses are possible.

#### Expert configurations

Various "expert settings" are available. Changes should only be made by appropriately trained personnel.

### 6.3.4 Network > Firewall and NAT

IPv4 firewall and NAT configuration

IPv4

IPv6

Firewall configuration

Enable service :	<input checked="" type="checkbox"/>	Enable or disable firewall (log)
Enable log :	<input type="checkbox"/>	<div>Show log</div> <div>Log dropped packets</div>
Show current settings :	<div>Active rules</div> <div>Script rules</div>	Show settings and state

Firewall and NAT rules preconfigured sets

All incoming ports closed, VPN allowed :	<input checked="" type="radio"/>	Best protection for VPN server
Selective ports allowed :	<input type="radio"/>	This opens more application ports
User uploaded script :	<input type="radio"/>	Use self created rules

Extra firewall rules

Enable forwarding :	<input checked="" type="checkbox"/>	Full routing from internal to WAN interface
Enable rules again DDoS :	<input checked="" type="checkbox"/>	Rules against DDoS attacks

Firewall is on

Apply

Cancel

Figure 18: Firewall and NAT settings

The gateway has a complex firewall system that can be used to monitor and filter the data traffic of all existing IP interfaces. The options are very extensive. To configure the firewall, an appropriately trained expert is definitely required. ***Alternatively you can contact always our support.***



**Please note:**

The gateway firewall supports both IPv4 and IPv6. However, both IP protocol variants require their own rules in each case.

#### Firewall configuration

View the current firewall rules/settings, enable or disable logging, and view the log file for firewall diagnostic tasks.

#### Firewall and NAT rules preconfigured sets

The gateway has some predefined firewall rules, e.g. for applications in a remote access VPN. These preconfigured sets can be activated here or adapted to individual requirements. Furthermore, the function **User uploaded script** allows to **upload a file with complete firewall and NAT rules** from the PC to the gateway.

#### Forwarding with IP-Masquerading and NAT

Switch on and off the NAT-based routing between the gateway and the WAN (Wide Area Network).



## 6.4 Services

### 6.4.1 Services > General

General service configuration

General service configuration		
Telnet server :	<input type="checkbox"/>	<input type="checkbox"/> Enable or disable Telnet server
FTP server :	<input type="checkbox"/>	<input type="checkbox"/> Enable or disable FTP server
Shellinabox service :	<input type="checkbox"/>	<input type="checkbox"/> Enable or disable <a href="#">web console</a> (port 4200)

Apply Cancel

Figure 19: General services settings



**IMPORTANT!**

The gateway has both a Telnet and FTP server for compatibility with older SSV products. Both protocols are now considered insecure because they are based on unencrypted data transmission. In this respect, these protocols should be disabled for practical use of the gateway!

#### General service configuration

Enable or disable access to the gateway via Telnet or FTP. Furthermore, the **Shellinabox service** can be enabled or disabled. Shellinabox (Shell-in-a-box) allows communication with the gateway via a Linux console within a web browser.

## 6.4.2 Services > OpenVPN

OpenVPN 1 configuration

Client 1 Client 2 Client 3 Server

OpenVPN 1 configuration

Enable service : ☐ ■ Enable or disable OpenVPN (log)

Status : DISCONNECTED Server or client status

OpenVPN client configuration

Configuration mode : ☒ default ☐ pki ☐ expert

Server address : vpn1.ssv-connect.de : 80 VPN server address and port

Alternative server address : : Alternative server address and port

Device : ☒ TUN ☐ TAP TUN for routing, TAP for bridging

Protocol : ☐ UDP ☒ TCP UDP protocol is preferred

VPN compression : ☐ Choose compression

Firewall rules from server : ☒ Read firewall rules after connecting

Firewall server URL : Optional server URL with rules

Notify server : ☐ Send notification to server

Connect via an HTTP proxy : ☐

OpenVPN certificates and keys

Authentication mode : Certificate Choose authentication mode

Authentication : Default (SHA1) Choose authentication algorithm

Cipher : Default (BF-CBC) Choose cipher algorithm

TLS min version : 1.0 TLS minimal version to use

Status root CA certificate : ca.crt Info Currently used root CA certificate

Status client key : client-0-18.key Info Currently used client key

Status client certificate : client-0-18.crt Info Currently used client certificate

Import key or certificates : Datei auswählen Keine ausgewählt Import Import single file or configuration bundle

Apply Cancel

Figure 20: OpenVPN settings

A typical application example for industrial gateways is their use in virtual private networks (VPNs) to implement remote maintenance applications. Here, the gateway forms a VPN client endpoint and enables a service engineer to securely remotely access the assemblies located behind the gateway (e.g., controllers in a local OT LAN). In such an application, all VPN clients connect to a central VPN server.

The gateway can simultaneously maintain connections to a maximum of **3 external VPN servers** (see tabs Client 1, Client 2 and Client 3). Each connection can be configured individually with different certificates. In addition, the gateway can also be used as a VPN server (see Server tab).

### OpenVPN client configuration

For each client connection to an external OpenVPN server, different protocol parameters can be set in addition to the OpenVPN server IP address or the OpenVPN server DNS name. These configurations have to be done by an appropriately trained expert. **Alternatively, you can contact always our support.**

### OpenVPN certificates and keys

Here the certificate and key management for a VPN client connection takes place in order to be able to connect to the respective OpenVPN server.

### 6.4.3 Services > DynDNS

DynDNS configuration	
<b>DynDNS configuration</b>	
Enable service :	<input type="checkbox"/> <span style="float: right;">■ Enable or disable DynDNS service</span>
DynDNS service provider :	(generic) ▼
Host (FQDN) :	<input type="text"/> <span style="float: right;">Click <a href="#">here</a> for available domain names</span>
Update period :	1 minute ▼ <span style="float: right;">How often the IP is checked</span>
<b>Change DynDNS username and password</b>	
Username :	<input type="text"/> <span style="float: right;">DynDNS account name</span>
New password :	<input type="password"/> <span style="float: right;">Enter your new DynDNS password</span>
Confirm new password :	<input type="password"/> <span style="float: right;">Confirm your new DynDNS password</span>
<b>Notification to webserver after IP address changes</b>	
Enable/disable notifications :	<input type="checkbox"/> <span style="float: right;">Enable or disable notify</span>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Figure 21: DynDNS settings**

The gateway enables applications in which it must itself be accessible via a DNS name on the Internet. One example would be operation as a VPN server. As such a gateway usually does not receive a static IP address on the Internet, DynDNS can be used as an alternative.

DynDNS or DDNS are abbreviations for **dynamic DNS**. This is a technique for dynamically updating the IP addresses of individual services in the Domain Name System (DNS). The purpose is that a computer system with a globally accessible service automatically and quickly changes the corresponding entry in the DNS after changing its IP address.

#### DynDNS configuration

Enable/Disable the DynDNS update service. Selection of the DynDNS provider with which a corresponding account exists and the complete host name (FQDN = Fully-Qualified Domain Name). Furthermore, the update period can be set.

#### Change DynDNS username and password

Change the password for a specific username.

#### Notification to webserver after IP address changes

Enable/disable a notification service in case the IP address of the gateway has changed on the Internet.

#### 6.4.4 Services > DHCP Server

DHCP server configuration		
<b>General configuration</b>		
Enable service :	<input checked="" type="checkbox"/>	<input type="checkbox"/> Enable or disable server
<b>Address range</b>		
Range start :	192.168.0.200	Range starts from this IP address
Range end :	192.168.0.254	Range ends on this IP address
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

**Figure 22: DHCP server settings**

The gateway can be used as a DHCP server because it supports automatic IP address assignment via Dynamic Host Configuration Protocol (DHCP) to OT modules (DHCP client modules) connected to a gateway LAN interface.

##### General configuration

Enable/Disable the DHCP server.

##### Address range

Specify the IP address range from which IP addresses are assigned to the client modules via DHCP.

#### 6.4.5 Services > SNMP

SNMP configuration		
<b>SNMP configuration</b>		
Enable service :	<input type="checkbox"/>	<input type="checkbox"/> Enable or disable SNMP service
SNMP version :	<input checked="" type="checkbox"/> SNMPv2c <input type="checkbox"/> SNMPv3	SNMP version to use
Username / community :	public	Username for SNMPv3 or community for SNMPv2c
Enable read/write access :	<input type="checkbox"/>	
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

**Figure 23: SNMP settings**

The Simple Network Management Protocol (SNMP) is a network protocol to monitor gateways and other network modules from a central management system and to change certain parameters. SNMP manages the communication between the monitored modules and the management system.

##### SNMP configuration

Enable/Disable SNMP. Selection of the SNMP version and other parameters.

## 6.4.6 Services > Remote Access (OpenSSH)

Remote access configuration

OpenSSH configuration		
Enable service :	<input checked="" type="checkbox"/>	Enable or disable OpenSSH service
Port :	22	Port to listen on
Key regeneration interval [sec] :	3600	Interval until the key will be regenerated
Permit root login :	<input checked="" type="checkbox"/>	Allow or deny root to login
Permit empty passwords :	<input type="checkbox"/>	Allow or deny empty user passwords
RSA key fingerprint :	SHA256:If2MB6hsRGUqUITultR/RMWD6K9564IBxrPrUKX1GOA	<a href="#">Recreate key</a>
Change password for user "root"		
New password :		Enter new password for 'root'
Confirm new password :		Confirm new password for 'root'
		<a href="#">Apply</a> <a href="#">Cancel</a>

Figure 24: Remote access settings

### OpenSSH configuration

SSH-based administrator access to the gateway (SSH Secure Shell). An OpenSSH daemon (SSHD) runs within the gateway operating system for this purpose. The SSHD can be enabled, disabled and configured. Furthermore, the current RSA key fingerprint is displayed.

### Change password for user "root"

SSH access to the gateway is always performed with administrator rights (user "root"). The password for this user can be changed here.

## 6.4.7 Services > SSV/WebUI

SSV/WebUI configuration

SSV/WebUI configuration	
Enable service :	<input checked="" type="checkbox"/> <span>Enable or disable WebUI service (log)</span>
Protocol :	<input type="radio"/> HTTPS <input type="radio"/> HTTP <input checked="" type="radio"/> Both <span>Server protocol to access WebUI</span>
HTTP Port :	7777 <span>Server unsecure port to access WebUI</span>
HTTPS Port :	443 <span>Server secure port to access WebUI</span>
HTTPS certificate fingerprint :	60:ad:79:11:58:68:1e:bc:02:f6:25:22:33:41:00:3b:b5:b0:e6:75 <span>Recreate key</span>
Session timeout [minutes]:	20 <span>Idle time in minutes, 0 = no time out</span>
WebUI style :	SSV default <span>▼</span>

Change admin access account	
Username :	admin <span>Username</span>
New password :	<input type="password"/> <span>Enter your new password</span>
Confirm new password :	<input type="password"/> <span>Confirm your new password</span>

Change user access account	
Username :	<input type="text"/> <span>Leave empty to disable user account</span>
Password :	<input type="password"/> <span>Enter user password</span>

Apply
Cancel

**Figure 25: SSV/WebUI settings**

The SSV/WebUI of the gateway supports two different user classes: 1. an administrator (admin) with all rights and 2. a user (user) with restricted rights, who is also only presented with an adjustable selective view of the SSV/WebUI.

### SSV/WebUI configuration

In this area the whole SSV/WebUI can be disabled. Furthermore, various settings are possible; e.g. the choice between the unprotected HTTP or the secure HTTPS protocol, the selection of the TCP port for HTTP or HTTPS access as well as the appearance (theme) of the SSV/WebUI.

### Change admin access account

Change the username and password for SSV/WebUI access with administrator rights (admin)

### Change user access account

Set or change the username and password for SSV/WebUI access with restricted user rights (user).

## 6.5 Proxies

### 6.5.1 Proxies > Web

Web proxy configuration		
<b>General configuration</b>		
Enable service :	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable or disable proxy
<b>Proxy redirections</b>		
<b>Create / edit a redirection entry</b>		
Encryption :	<input type="checkbox"/>	Use HTTPS encrypted tunnel
Relay to :	<input type="text"/> : <input type="text"/>	Enter IP address and port number (80 HTTP, 433 HTTPS)
Listen on port :	<input type="text"/>	<input type="button" value="Add"/> Enter port number
<b>SSL certificate</b>		
Create SSL certificate :	<input type="button" value="Create"/>	
Fingerprint MD5 :	<input type="text"/>	
Fingerprint SHA1 :	<input type="text"/>	
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 26: Web proxy service settings

If HTTP servers exist in the automation modules of an OT network, the web proxy function of the gateway can be used to increase IT security for access to these servers. For this purpose, a web proxy is configured for each HTTP server, which converts the insecure HTTP protocol into the secure HTTPS protocol. This creates an **HTTP-to-HTTPS proxy**. Subsequently, browser access by an external user no longer takes place directly to the HTTP server in the automation module, but via HTTPS to the proxy in the gateway.

#### General configuration

Enable/Disable the web proxy service.

#### Proxy redirection

The individual web proxy connections are displayed as an overview. Each individual proxy connection can be edited and deleted.

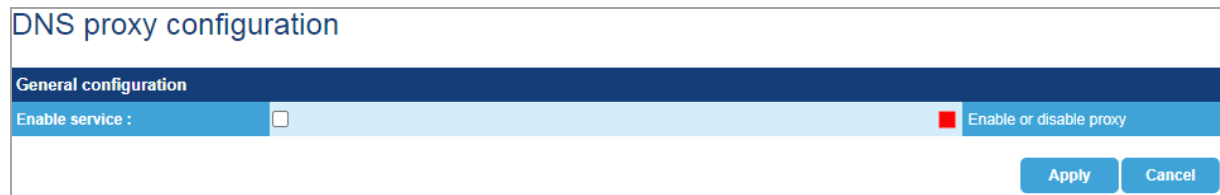
#### Create / edit a redirection entry

Create a new web proxy connection. This requires the following entries: 1. The TCP port number for the **Listen on port** (LoP). 2. The IP address and the port number for the **Relay to** system (RtS) part. Furthermore, for an HTTP-to-HTTPS proxy, the **Encryption** (i.e. the SSL or TLS function) must be explicitly enabled. Otherwise, the result is an HTTP-to-HTTP proxy (i.e., a port redirection for external web access).

#### SSL certificate

A certificate is required for the HTTP-to-HTTPS proxy. This certificate can be created here.

## 6.5.2 Proxies > DNS



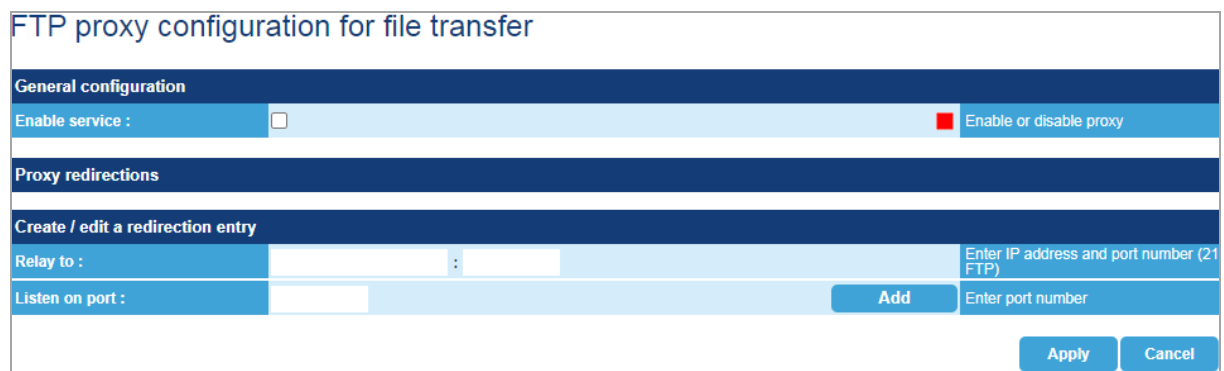
**Figure 27: DNS proxy settings**

A DNS proxy routes DNS requests and DNS responses between DNS clients and a DNS server. The DNS proxy simplifies network management. For example, if the DNS server address changes, only a change in the configuration is required for the DNS proxy, not for each individual DNS client.

### General configuration

Enable/Disable the DNS proxy service.

## 6.5.3 Proxies > FTP



**Figure 28: FTP proxy settings**

If FTP servers exist in the automation systems of an OT network, the FTP proxy function of your gateway can be used to redirect access to these servers to other TCP ports.

### General configuration

Enable/Disable the FTP proxy server.

### Proxy redirection

The individual FTP proxy connections are displayed as an overview. Each individual proxy connection can be edited and deleted.

### Create / edit a redirection entry

Create a new FTP proxy connection. This requires the following entries: 1. The TCP port number for the **Listen on port** (LoP). 2. The IP address and the port number for the **Relay to** system (RtS) part.



### 6.5.4 Proxies > TCP

TCP proxy configuration for Telnet, SSH and others

General configuration	
Enable service :	<input type="checkbox"/> <span style="float: right;"><input checked="" type="checkbox"/> Enable or disable proxy</span>
Proxy redirections	
Create / edit a redirection entry	
Relay to :	<input type="text"/> : <input type="text"/> <small>Enter IP address and port number (22 SSH, 23 Telnet)</small>
Listen on port :	<input type="text"/> <span style="float: right;"><input type="button" value="Add"/> <small>Enter port number</small></span>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 29: TCP proxy settings

A TCP proxy creates a TCP socket under a specified TCP port number (**Listen on port** socket, LoP) and a bidirectional data connection between this socket and another adjustable TCP socket (**Relay to** system, RtS), which can be located on the same gateway or on an external system with a static IP address.

#### General configuration

Enable/Disable the TCP proxy server.

#### Proxy redirection

The individual TCP proxy socket connections are displayed as an overview. Each individual socket connection can be edited and deleted.

#### Create / edit a redirection entry

Create a new TCP proxy socket connection. This requires the following entries: 1. The TCP port number for the **LoP**. 2. The IP address and port number for the **RtS**.

### 6.5.5 Proxies > UDP

UDP proxy configuration

General configuration	
Enable service :	<input type="checkbox"/> <span style="float: right;"><input checked="" type="checkbox"/> Enable or disable proxy</span>
Proxy redirections	
Create / edit a redirection entry	
Relay to :	<input type="text"/> : <input type="text"/> <small>Enter IP address and port number</small>
Listen on port :	<input type="text"/> <span style="float: right;"><input type="button" value="Add"/> <small>Enter port number</small></span>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 30: UDP proxy settings

A UDP proxy creates a UDP socket under a specified UDP port number (**Listen on port** socket, LoP) and creates a bidirectional data connection between this socket and another adjustable UDP socket (**Relay to** system, RtS), which can be located on the same gateway or on an external system with a static IP address.

**General configuration**

Enable/Disable the UDP proxy server.

**Proxy redirection**

The individual UDP proxy socket connections are displayed as an overview. Each individual socket connection can be edited and deleted.

**Create / edit a redirection entry**

Create a new UDP proxy socket connection. This requires the following entries: 1. The UDP port number for the **LoP**. 2. The IP address and the port number for the **RtS**.

## 6.6 Logout

---

Logout from the SSV/WebUI session.

## 7 APPLICATION EXAMPLES

### 7.1 OT/IT Domain Isolation

The primary purpose of an IGW/936A OT/IT Network Gateway is to isolate two different Ethernet LAN domains.

A typical application example would be the coupling of the information technology (IT) within a company-wide network with the networked assemblies and systems of an operation technology (OT) network on the production floor.

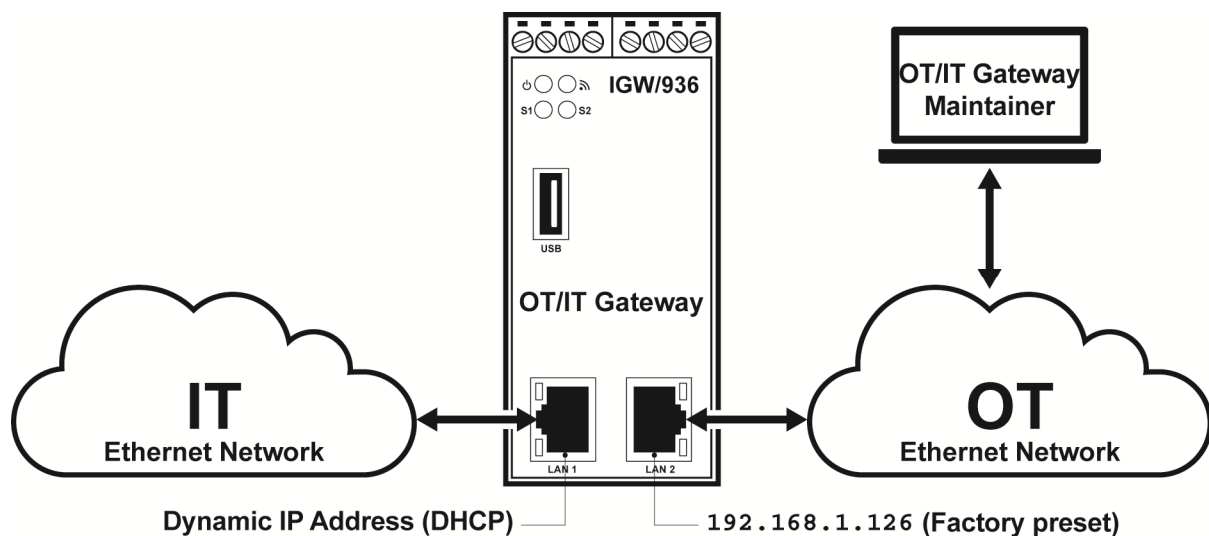


Figure 31: Schema of an OT/IT domain isolation with the IGW/936A

Two physically independent 10/100 Mbps Ethernet LAN interfaces, each with an own MAC and PHY hardware part, serve as coupling links. Both interfaces are only logically connected via the IGW/936A Linux operating system.

To establish a connection via the IGW/936A between the two networks, either the proxy server system plus the internal firewall must be configured accordingly or a suitable **Firewall and NAT rules script** must be loaded.

Ex-factory the IGW/936A LAN1 interface is prepared for a dynamic IP address assignment from an external **DHCP server**. The LAN2 interface is preset with the static IPv4 address **192.168.1.126/24** (i.e. with the subnet mask **255.255.255.0**).

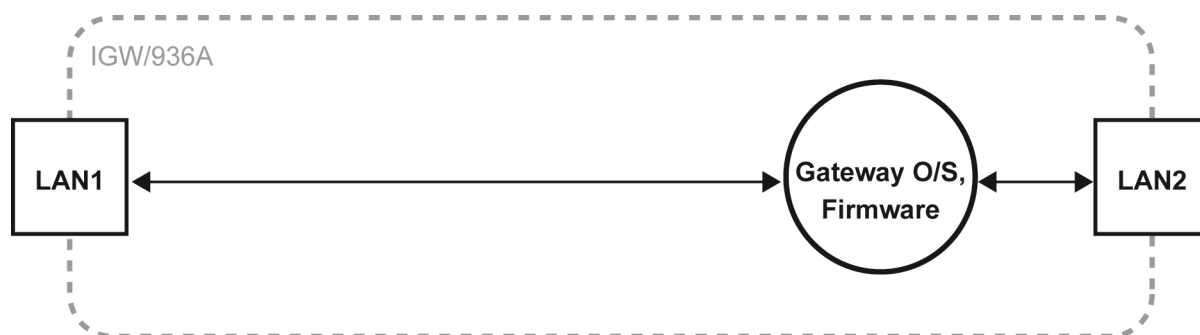
The internal proxy server system and the **netfilter/iptables firewall** of an IGW/936A are disabled ex-factory. This blocks all Ethernet LAN traffic between LAN1 and LAN2. **In this state, no connections from the IT network to the OT network and vice versa are possible.**

A complete TCP proxy server and firewall configuration example for a Modbus TCP scenario is available on request. This allows a Modbus TCP master (TCP client) in the IT Ethernet network to access a Modbus TCP slave (TCP server, TCP port 502) in the OT Ethernet network via the IGW/936A.

Due to the proxy server system and the netfilter/iptables firewall, there are several different paths for connections between the IT network at the LAN1 interface and the OT network at the LAN2 interface in a data flow diagram representation. **There are 3 important data paths:**

#### All off

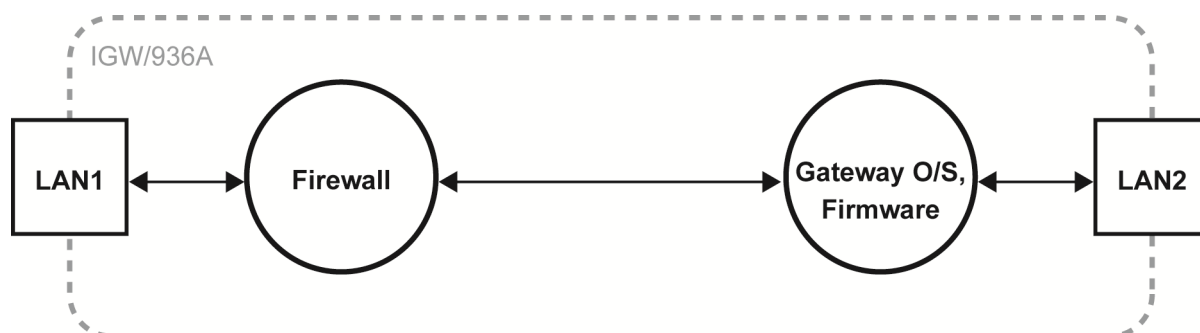
The firewall and the proxy server system are off. LAN1 and LAN2 each have a direct connection to the respective device drivers in the Linux operating system. However, there is no bridge or router connection between LAN1 and LAN2.



**Figure 32: Data flow between LAN1 and LAN2 with firewall and proxy server off**

#### Firewall = On

The firewall is enabled. A packet filter is now active between the IT network at LAN1 and the LAN1 Ethernet driver in the Linux operating system. Only if a corresponding firewall rule exists for the payload, a certain Ethernet packet between the IT network and the Linux operating system (gateway O/S, firmware) can pass the firewall in both directions.

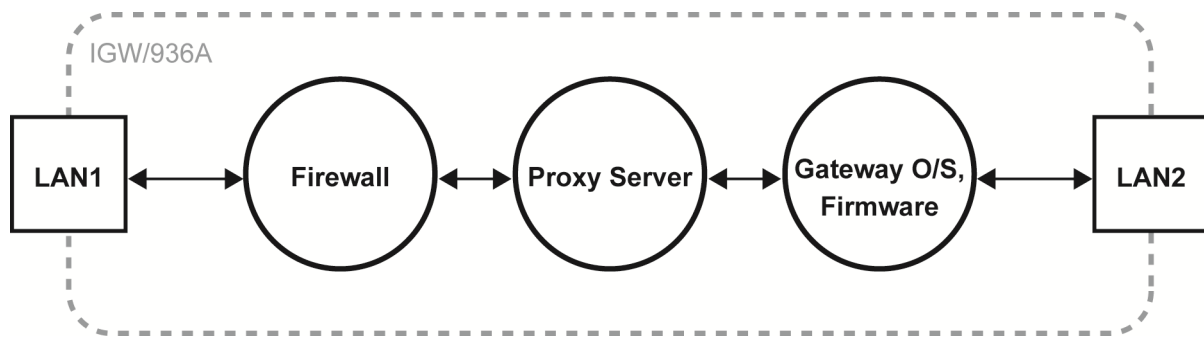


**Figure 33: Data flow between LAN1 and LAN2 with firewall enabled and proxy server off**

#### Firewall and proxy= On

At least one proxy server in the IGW/936A firmware is configured. From the direction of the IT network (LAN1), the proxy server can then be reached via the respectively selected listen-on port (LoP). This is connected to the preset relay-to system (RtS) via LAN2 (see also **chapter 6.5 and 6.5.4**).

Using such a connection, a TCP client in the IT network, for example, can use any TCP server within the OT network without there being a direct Ethernet LAN or routed IP connection between the two networks. The TCP client does not even need to know the IP address of the TCP server for this, but only the LoP number.



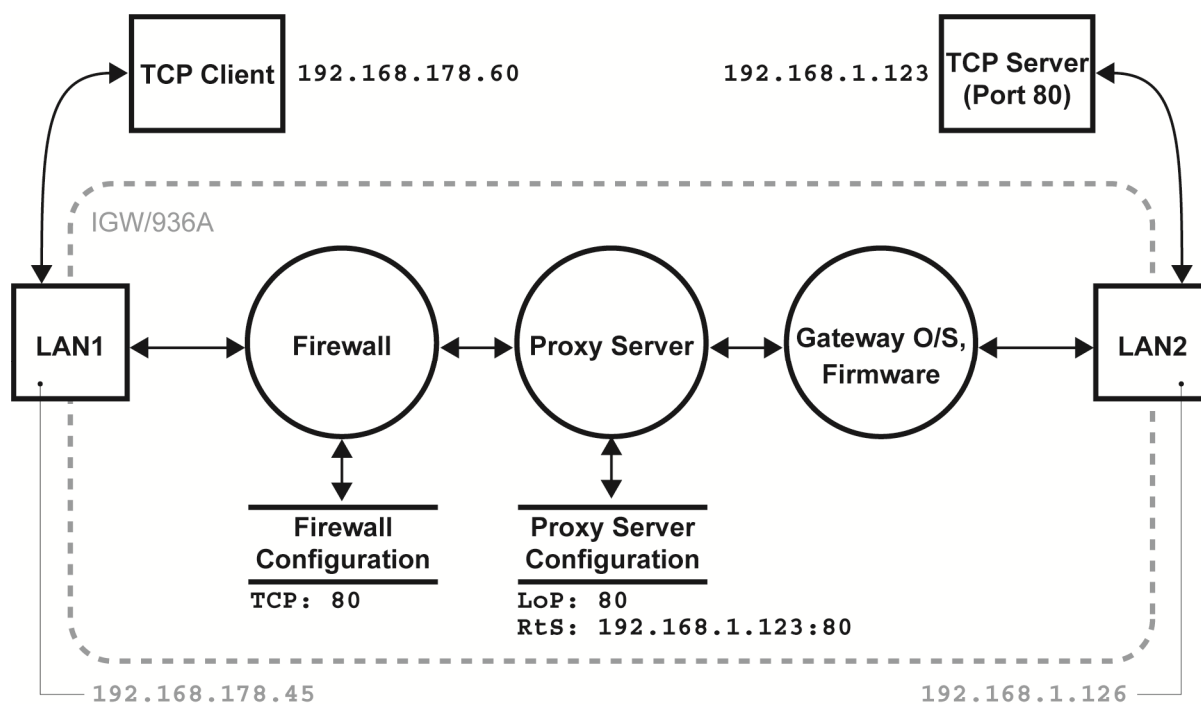
**Figure 34: Data flow between LAN1 and LAN2 with firewall and proxy server on**

There are **5 different proxy server variants** included in the IGW/936A proxy server system by default, which can be configured directly via the SSV/WebUI:

- HTTP proxy with an optional HTTPS-to-HTTP service
- DNS proxy
- FTP proxy
- TCP proxy
- UDP proxy

For more complex applications, an **IGW/936A Software Development Kit (SDK)** is available. This SDK can be used to develop Modbus or MQTT application firewall solutions, for example.

**Figure 35 shows a configuration example** with the TCP proxy server functions. A TCP client in the IT network LAN1 can access the TCP port 80 of a server in the OT network LAN2 via the IGW/936A. Further access possibilities from the IT to the OT network are not provided with this configuration.



**Figure 35: Data flow of a TCP proxy server example configuration**

For this application purpose, the firewall is enabled and TCP port 80 is released for data traffic via firewall rule. In addition, a TCP proxy is started with LoP = 80 (Listen-on port) and the RtS = 192.168.1.123:80 (Relay-to system, e.g. the IP address and destination port number of the TCP server in the OT network).

## 8 CREATING A VPN CONNECTION

The IGW/936A can be used as a VPN (Virtual Private Network) gateway to enable secure access from a remote computer. Therefore the IGW/936A uses the open source software from **OpenVPN**. To set-up your own VPN infrastructure you need the OpenVPN server and client software which can be obtained here: <https://openvpn.net>.

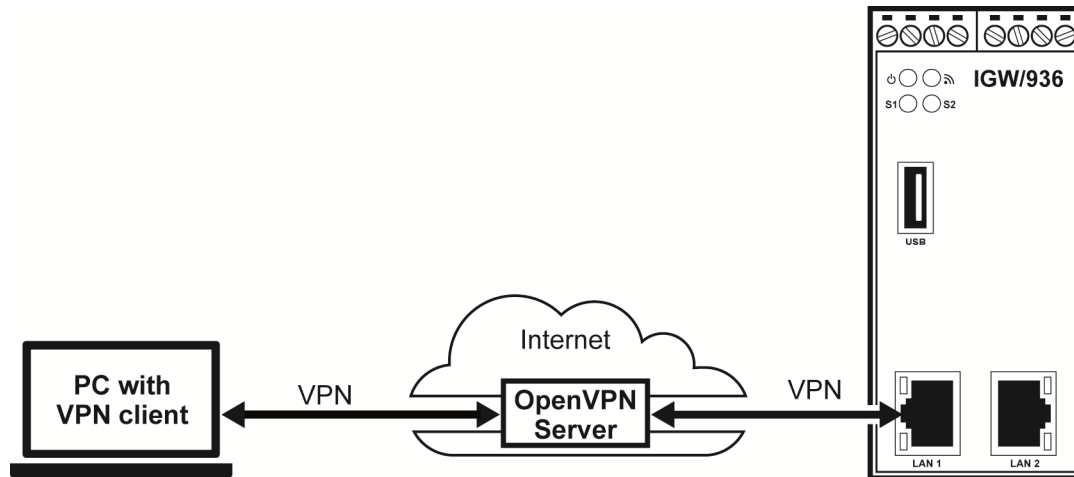


Figure 36: Example of a VPN connection



**Please note:**

Make sure that the IGW/936A uses the **current time and date** to avoid problems during the VPN configuration. We recommend using an NTP server instead of a manual setup, otherwise the IGW/936A cannot automatically reconnect to the VPN after an interruption of the power supply. Please refer to **chapter 6.2.4!**

To setup and configure a VPN choose from the menu **Services > OpenVPN**. Here you can configure each detail of a VPN like the protocol, firewall or authentication mode. The IGW/936A can be connected with **up to 3 different VPNs** at the same time.

### OpenVPN Server Docker Container for Evaluation

SSV offers a **ready-to-run Docker container with a preinstalled OpenVPN server** for evaluation purposes. All information about installation and resources can be found on GitHub:

<https://github.com/SSV-embedded/RMG-OpenVPN>

*Please follow the instructions on GitHub to setup and run the OpenVPN Docker container and to create the VPN client configuration files.*

**IMPORTANT!**

The proposed setup is **NOT RECOMMENDED FOR PRODUCTION** and shall be used for evaluation purposes only!

All required secrets are generated on the OpenVPN server Docker container and copied to all VPN clients. This implies that a security breach on the VPN server compromises all deployed secrets.

OpenVPN 1 configuration

Client 1 Client 2 Client 3 Server

OpenVPN 1 configuration

Enable service : ☒ Enable or disable OpenVPN (log)

Status : CONNECTED Server or client status

OpenVPN client configuration

Configuration mode : ☐ default ☐ pki ☒ expert

Configuration :

```
dev tun1
#### Start OF VPN CONFIG FILE ####
# File: client-2.ovpn
#####
# client-side OpenVPN 2.4.x config file      #
# for connecting to multi-client server.    #
#                                           #
# On Windows, you might want to rename this #
# file so it has a .ovpn extension         #
#####

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
```

For syntax refer (openvpn.net)

Upload

OpenVPN certificates and keys

Import key or certificates :  Keine ausgewählt  Import single file or configuration bundle

**Figure 37: Example of a VPN configuration file**

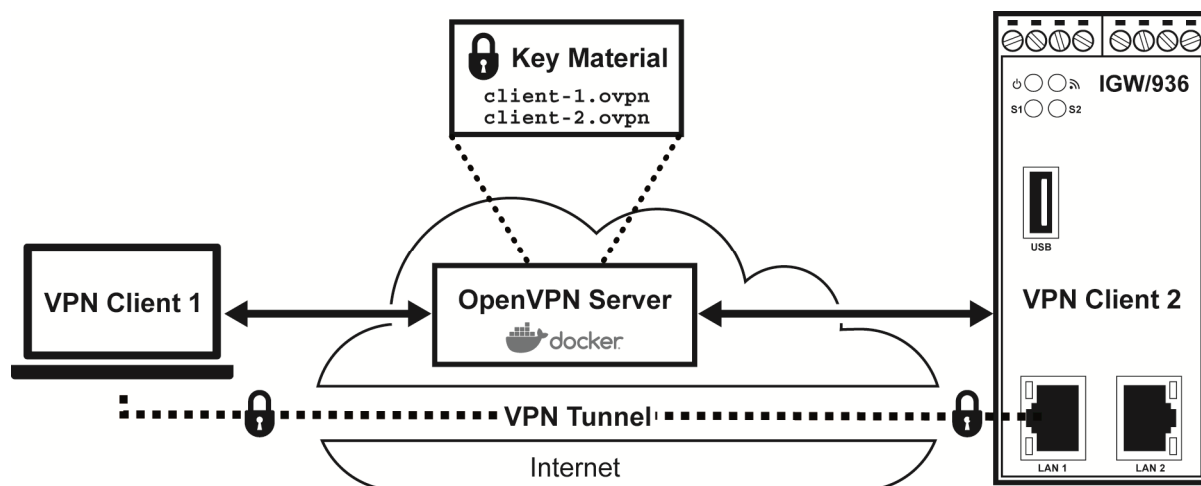
To **import the VPN client configuration** into the IGW/936A log into the SSV/WebUI, choose **Services > OpenVPN** and follow these steps:

1. Click the checkbox **Enable service** and the radio button **expert** in the line **Configuration mode**.
2. Click on **[Apply]**.
3. Now mark all lines inside the text field **Configuration** (Ctrl-A) and paste the complete content of the VPN client configuration file **client-2.ovpn** into the text field.
4. Click on **[Upload]** to update the text field.
5. Click on **[Apply]**. This will start the VPN connection.
6. After a few seconds click on the tab **Client 1** to refresh the connection status in the line **Enable service**. It should now show a **green arrow symbol**.



**IMPORTANT!**

Please do **NOT** click again on [Apply]! This would terminate the current VPN connection and start a new one.



**Figure 38: Schema of the OpenVPN evaluation setup**

To see some **VPN connection details** choose from the menu **System > Logging**.

The **current VPN IP address** of the IGW/936A is shown on the **status page** in the section **Status VPN1**.

Status VPN1		
IP address :	10.126.0.10	Current device IP address
Status DNS		

**Figure 39: VPN IP address on the status page**

When the IGW/936A as well as the PC are connected with the OpenVPN server, you can **access the SSV/WebUI via VPN**.

To do this, enter the VPN IP address of the IGW/936A with the port number 7777 in your browser. For example:

**10.126.0.10:7777**

## 9 HELPFUL LITERATURE

---

- DNP/8331 Hardware Reference
- SSV on GitHub: <https://github.com/SSV-embedded/RMG-OpenVPN>

## CONTACT

---

### SSV Software Systems GmbH

Dünenweg 5  
D-30419 Hannover

Phone: +49 (0)511/40 000-0

Fax: +49 (0)511/40 000-40

E-mail: [sales@ssv-embedded.de](mailto:sales@ssv-embedded.de)

Web: [www.ssv-embedded.de](http://www.ssv-embedded.de)

Forum: [www.ssv-comm.de/forum](http://www.ssv-comm.de/forum)

Social: [www.linkedin.com/company/ssv-software-systems](https://www.linkedin.com/company/ssv-software-systems)

## DOCUMENT HISTORY

---

Revision	Date	Remarks	Name	Review
1.0	2022-08-11	First version	WBU	SSC
1.1	2023-06-13	Added chapter 7 and 8	WBU	KDW

The contents of this document are subject to change without prior notice. SSV does not assume any liability and does not guarantee that the presented information is accurate or complete. The information in this document is provided 'as is' without warranty of any kind. Some names within this document may be trademarks of their respective holders.

© 2023 SSV SOFTWARE SYSTEMS GMBH. All rights reserved.