MARTEM
KAUGJUHTIMISSÜSTEEMID
TELECONTROL SYSTEMS

Configuration tool TELEM-GWS

User Manual

Martem AS
2025

Contents

Laki 25
12915 Tallinn
ESTONIA
Tel: +372 639 7979
E-mail: martem@martem.eu
Fax: +379 639 7980
www.martem.eu

1 Introduction

The *Telem-GWS* configuration tool is designed for the setup and management of Telem series devices, including Telem-GW5, Telem-GW6, Telem-GWM, and Telem-AGC data concentrators, as well as RTU-T modules.
Developed by *Martem AS*, Telem-GWS is actively maintained to support the latest device capabilities. The tool is free to use, user-friendly, and compatible with Microsoft Windows operating systems from Windows Vista up to the latest Windows versions. The latest release of Telem-GWS can be downloaded either from the *Martem AS* website or provided directly by *Martem AS* representatives.
Telem-GWS executable is 32-bit and works on both 32-bit and 64-bit systems.

Laki 25
12915 Tallinn
ESTONIA

Tel: +372 639 7979
E-mail: martem@martem.eu
Fax: +379 639 7980
www.martem.eu

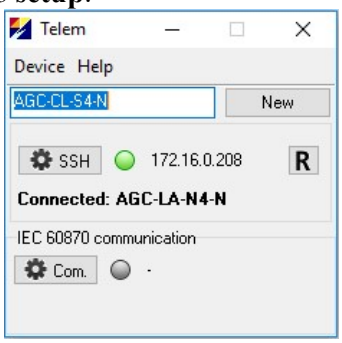
2 Getting started

2.1 Installation

Telem-GWS does not require installation. To launch the tool, simply run the downloaded `.exe` file.

2.2 Initial Startup

Upon launching Telem-GWS, the Telem Configurator window will open. This window provides options for establishing communication with supported devices using either the SSH protocol or the IEC 60870 protocol.
Note: Protocol selection and communication parameters (non SSH) can be configured from the menu: **Device > IEC 60870-5 setup**.



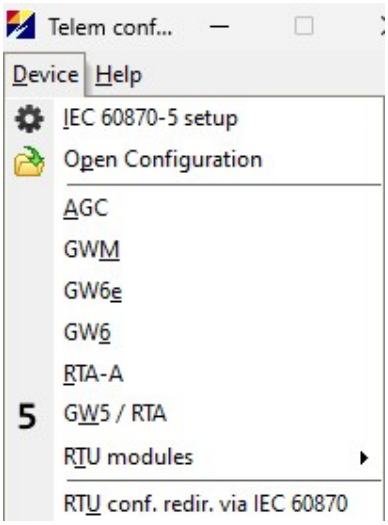
Element	Description	Behavior/Notes
Device Model Input Field (Top)	Enter Martem RTU device model code	Required only when creating a new configuration using the “New” button. If invalid, field turns red. Codes are defined in a separate RTU technical document.
New Button	Creates a new blank configuration	Opens a new configuration window based on the entered device model code. No connection to a physical device required.
SSH Icon & Connection	Initiates SSH connection	Device model code and configuration are read automatically from the connected device. No need to manually enter code. **This is most common for post 2013 Telem devices**
Bold R button	Initiates read out of configuration via SSH	
IEC 60870 Communication	Displays IEC 60870 connection status	Visual indicator: Green = Connected, Red = Disconnected

2.3 Communication Methods

Option	Description
Serial (COM port)	Supported only for RTU-T modules and legacy Telem devices (RTA, RTA-A GW5, GW6). Pre 2013
Ethernet (SSH)	Used for newer Telem devices (AGC, GWM, GW6-e). Default and recommended connection method.

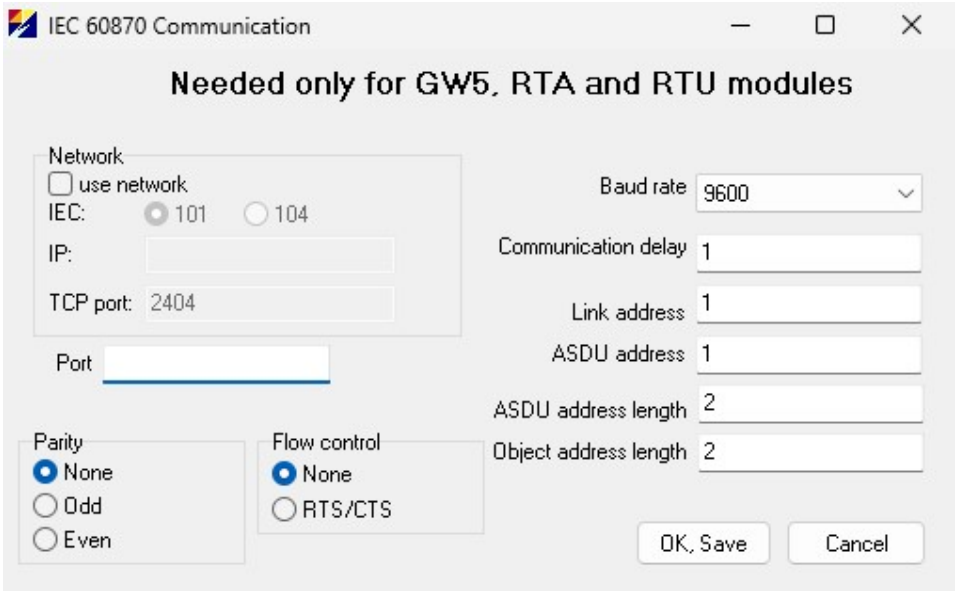
2.4 Default setup

To open default setup, either input correct device model in Device Model Input Field, or device has to be chosen from the device menu. General model options of the Telem devices are provided as seen in the illustration above.



2.5 Connect with device using serial connection

Serial connection can be used with RTU-T modules, Telem AI-12T, Telem DI24-T, Telem DO5-T and older Telem devices like RTA, RTA-A, GW5, GW6.
Serial connection uses IEC 60870-5-101 protocol. To establish connection the corresponding parameters have to be set in the **Device > IEC 60870-5 setup.**



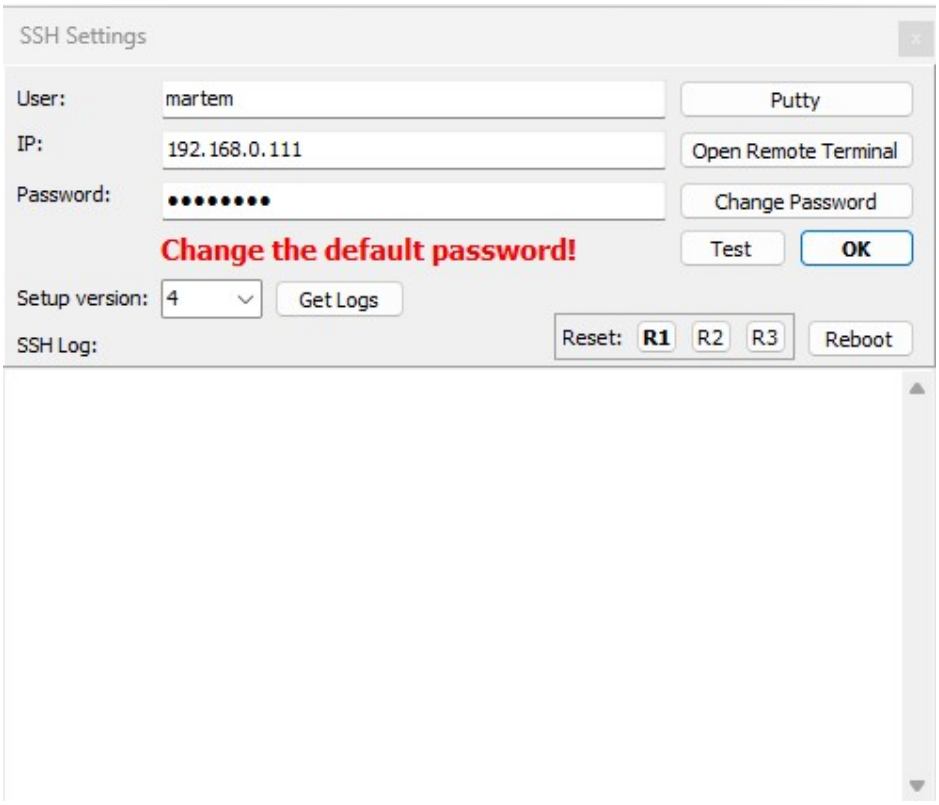
Field	Description
Network	Select whether to use IEC 60870-5-101 or 104 over network for Telem device communication
IP / TCP port	Defines IP address to connect to and TCP port (default: 2404)
Port	COM port number used for direct serial communication from PC
Parity	Parity setting for serial line: None (default), Odd, Even
Flow control	Select flow control method: None (default), RTS/CTS (hardware-based)
Baud rate	Serial communication speed (e.g., 9600)
Communication delay	Delay in milliseconds between data reception and next query (default: 0)
Link address	Logical address of the Telem device in IEC protocol (e.g., 1)
ASDU address	Application Service Data Unit address of the Telem device (e.g., 1)
ASDU address length	Number of bytes for ASDU address: 1 or 2
Object address length	Number of bytes for information object address: 1, 2, or 3 (default: 2)

2.6 Connect with device using SSH connection over network.

To connect to a Telem device over Ethernet:

1. In the main setup window, select the target device.
2. Click the **SSH** button to open the SSH Settings dialog.
3. Enter connection parameters: `User`, `IP`, and `Password`.
4. Click **Test**. If the connection is successful, **Access granted** will be displayed and the SSH indicator light will turn **green**.
5. Click **OK** to save the connection parameters.
6. Once connected, the user can:
   - Read (`R`) configuration from the device
   - Write (`W`) configuration to the device

- Cancel the operation with c



Any SSH client, e.g. Putty, can be used to connect with the device. Baudrate 115200bps is used. Necessary user names and passwords are provided by Martem AS.

Field	Description
User	Device login username (default: martem)
IP	Target device IP address (in default conf for ETH0: 192.168.0.111)
Password	Login password (default provided by Martem AS)
Setup version	Protocol setup version (only version 4 is supported by GW6-e, GWM, AGC)
Putty	Launches an external terminal window (e.g. PuTTY) with current credentials
Open Remote Terminal	Opens shell with provided SSH parameters; use `su -l` for root access
Change Password	Allows user to set a new device password
Test	Tests SSH connection to the device
OK	Saves parameters and closes the window
SSH Log	Output of underlying SSH application. If having issues with reading/writing configuration and/or updating device firmware, then copy all this text and email to martem@martem.ee with a short description about the issue.
Reboot	Reboots the device
R1	Resets the device

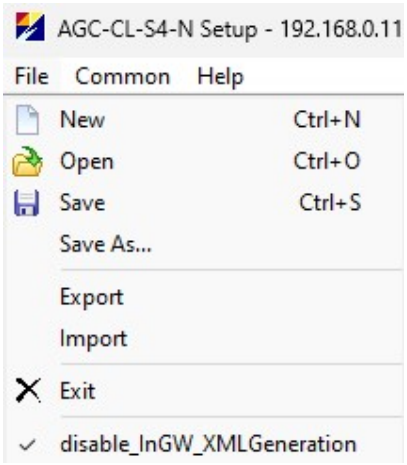
R2	Resets device and clears memory buffers
R3	Performs full reset and restores factory setup

Notes:

- Baudrate for all SSH connections is fixed at **115200 bps**.
- Any SSH client (e.g., PuTTY) may be used independently with the provided credentials.
- Use the `thelp` command in terminal for built-in command-line tool help.
- Login as `root` via `su -l` to access advanced configuration and diagnostics tools.

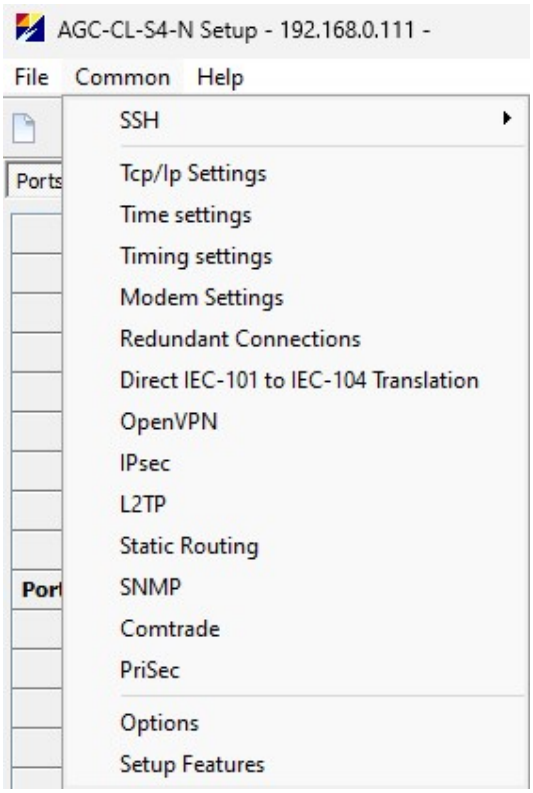
3 File menu

This menu is located in the top-left corner under `File` in the main GWS application window. Keyboard shortcuts are indicated for faster access.



Menu Item	Description
New	Open new blank device setup
Open	Load existing configuration
Save	Save current configuration to file
Save As	Save current configuration under new name
Export	Export configuration to .csv format
Import	Import configuration from a .csv file
Exit	Close the application
disable_inGW_XMLGeneration	Must be selected to prevent automatic XML generation inside the GW device

4 Common menu



4.1 SSH Settings:

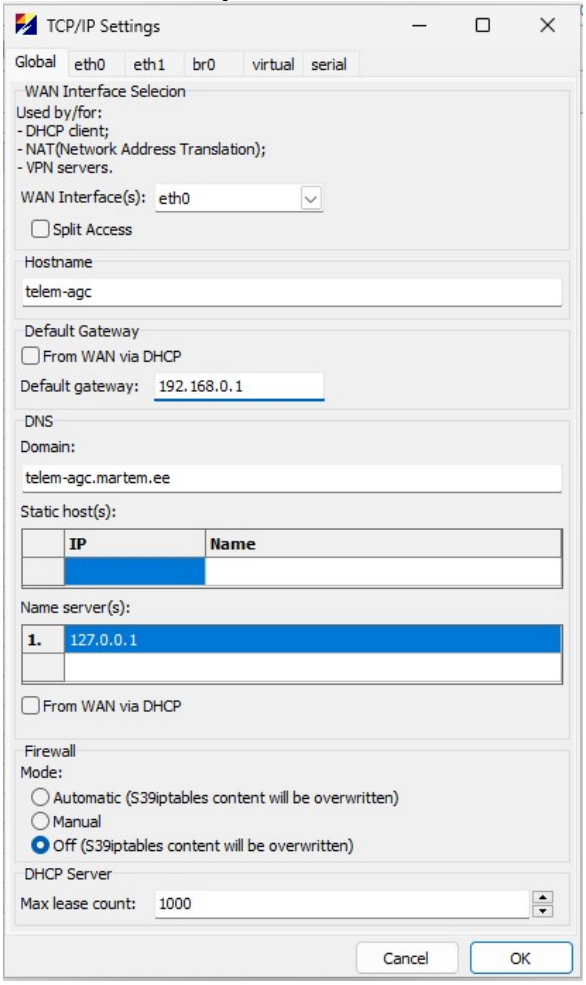
Duplicates SSH settings in the device setup window (described in previous chapter)

4.2 TCP/IP Settings

Used for determine TCP/IP communication parameters and firewall functionality in Telem device

4.2.1 Global tab

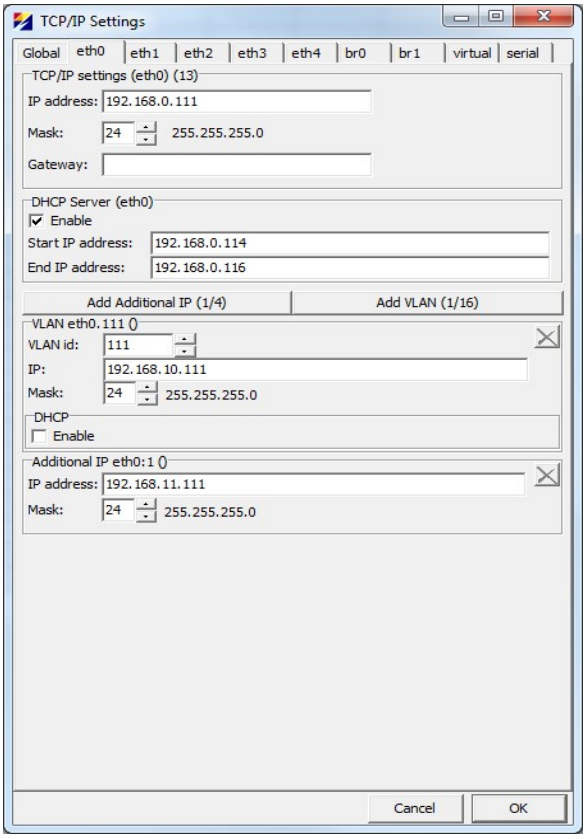
The Global tab within the TCP/IP Settings section is used to configure basic network parameters and firewall options for Telem devices. These settings are essential for defining device connectivity in both local and wide area networks.



Section	Description
WAN Interface	Selects which physical or virtual network interface is used for WAN (Wide Area Network) connectivity. Options depend on available interfaces of the specific device.
Hostname	Defines the device's hostname (used in network identification and DNS).
Default Gateway	Specifies the default gateway IP address for outbound traffic. Can be set manually or obtained automatically via DHCP from WAN interface.
DNS	Allows specification of DNS server IP addresses used by the device for domain name resolution. Multiple servers can be defined.
Firewall	Enables firewall configuration if necessary. Available modes: Automatic, Manual, Off.
DHCP Server	Sets the maximum number of DHCP client leases that this device will serve if DHCP Server functionality is enabled.

Element	Description	Behavior/Notes
WAN Interface Selection	Dropdown list of available interfaces (e.g., eth0, eth1, ...)	Used for NAT, VPN, and DHCP Client connections.
Split Access Checkbox	Optional setting	Question: What exactly does enabling Split Access do in Martem devices?
Hostname Field	User-defined device hostname	e.g., telem-gw6e
Default Gateway Section	Defines the route to the internet	Checkbox for auto-obtaining from DHCP or manual input.
Static Host(s) Section	Allows static DNS entries mapping IP to name	Empty by default.
Name Server(s) Section	List of DNS server IP addresses	e.g., 127.0.0.1 shown.
Firewall Mode	Mode selection for firewall	Options: Automatic / Manual / Off
DHCP Server Max Lease Count	Defines the limit of devices allowed to obtain IP addresses from this DHCP server	Example value: 1000

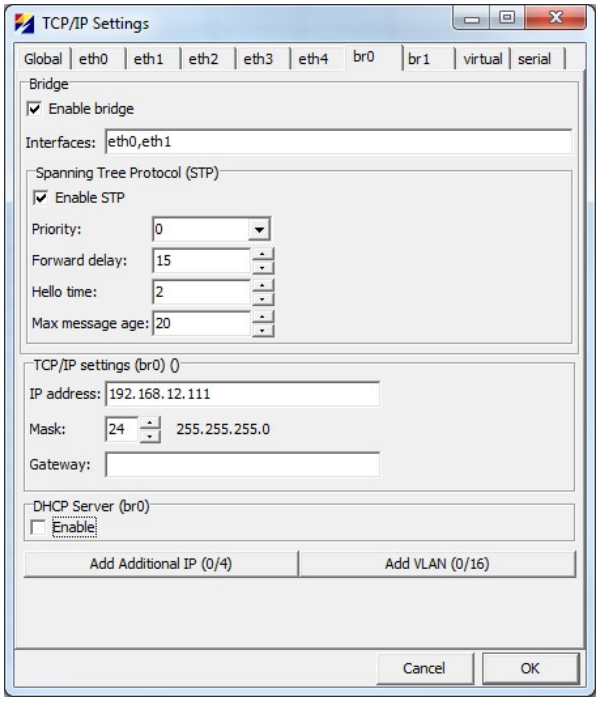
4.2.2 EthX Tabs (Eth0, Eth1, ...)



The EthX tabs in the TCP/IP Settings window correspond to the physical Ethernet ports available on the Telem device. The number of available Ethernet interfaces depends on the specific hardware model.
Each Ethernet port (Eth0, Eth1, Eth2, etc.) can be individually configured with its own IP address settings, VLAN configuration, DHCP server options, and additional network parameters.

Section	Description
TCP/IP Settings	Configures the primary IP address, subnet mask, and optional gateway for the selected Ethernet port.
DHCP Server	Enables the built-in DHCP server for the selected Ethernet port. Allows setting Start and End IP address range for dynamic lease allocation.
Additional IP	Allows adding up to 4 additional static IP addresses to the same physical interface.
VLAN Interface	Supports creation of up to 16 tagged VLAN interfaces per Ethernet port. Each VLAN has its own IP addressing.

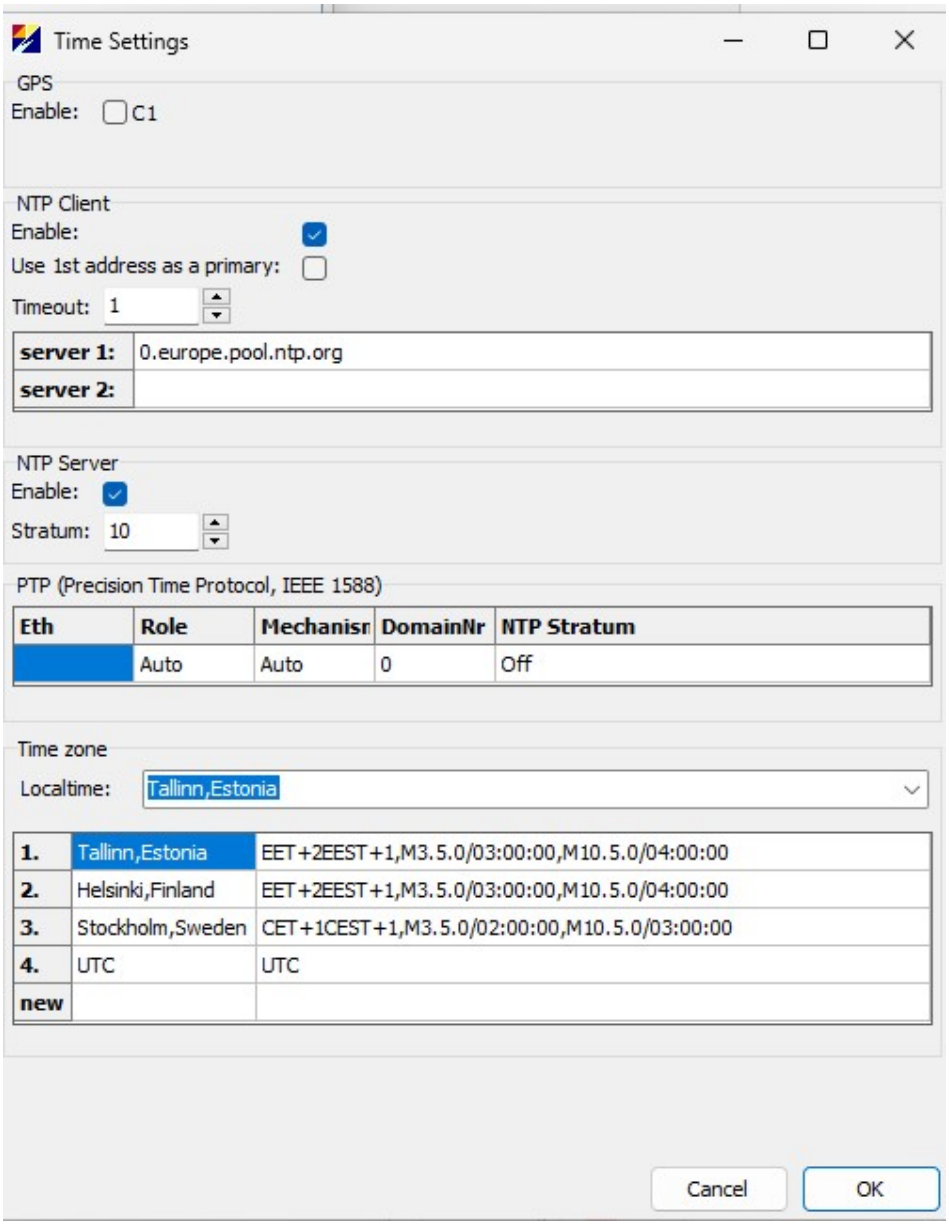
4.2.3 Br0/br1 tab



Combine two ethernet ports to work as a bridge.

Section	Field	Description
Bridge	Enable bridge	Enable Ethernet bridging for selected interfaces (e.g. eth0, eth1)
Bridge	Interfaces	Comma-separated list of interfaces to include in the bridge (e.g. eth0,eth1)
Spanning Tree Protocol (STP)	Enable STP	Enable STP for loop prevention and topology management
Spanning Tree Protocol (STP)	Priority	Bridge priority (0 = highest). Default: 32768
Spanning Tree Protocol (STP)	Forward delay	Time in seconds for port state transitions (listen → learn → forward). Default: 15s
Spanning Tree Protocol (STP)	Hello time	Time interval (in seconds) for sending STP hello packets. Default: 2s
Spanning Tree Protocol (STP)	Max age	Time in seconds before path is considered invalid without hello messages. Default: 20s
TCP/IP settings	IP address	Primary IP address for the bridge interface
TCP/IP settings	Mask	Subnet mask
TCP/IP settings	Gateway	Default gateway
DHCP Server	Enable	Enable internal DHCP server for this interface
DHCP Server	Range (not visible in this view)	Set address range for DHCP assignments
Advanced	Add Additional IP	Add up to 4 secondary IP addresses
Advanced	Add VLAN	Add up to 16 VLAN-tagged virtual interfaces

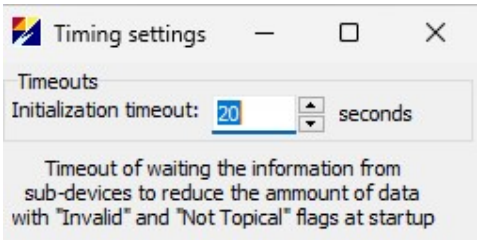
4.3 Time settings



Section		Field	Description
GPS	Enable	Toggle GPS time synchronization	
GPS	C1	Enable synchronization via Telem GPS interface using C1 signaling	

NTP Client	Enable	Enable NTP client for time sync with external servers
NTP Client	Use 1st address as a primary	If checked, server 1 is used as the primary NTP server
NTP Client	Timeout	Response wait time in seconds for NTP request
NTP Client	Server 1	Primary NTP server address (e.g. 0.europe.pool.ntp.org)
NTP Client	Server 2	Secondary NTP server address
NTP Server	Enable	Enable this device to act as NTP server to other systems
NTP Server	Stratum	NTP stratum level (default: 10). Lower = higher precision
PTP (IEEE 1588)	Eth	Interface used for Precision Time Protocol (e.g. Auto)
PTP (IEEE 1588)	Role	Role for PTP (e.g. Auto)
PTP (IEEE 1588)	Mechanism	Sync mechanism for PTP (e.g. Auto)
PTP (IEEE 1588)	DomainNr	PTP domain number (e.g. 0)
PTP (IEEE 1588)	NTP Stratum	Stratum level used when PTP is active. "Off" disables influence on NTP stratum
Time zone	Localtime	Predefined or custom time zone (e.g. Tallinn,Estonia)
Time zone	Zone definition	Details of selected time zone including UTC offset and DST rules (e.g. EET+2EEST+1,M3.5.0/03:00:00,M10.5.0/04:00:00)

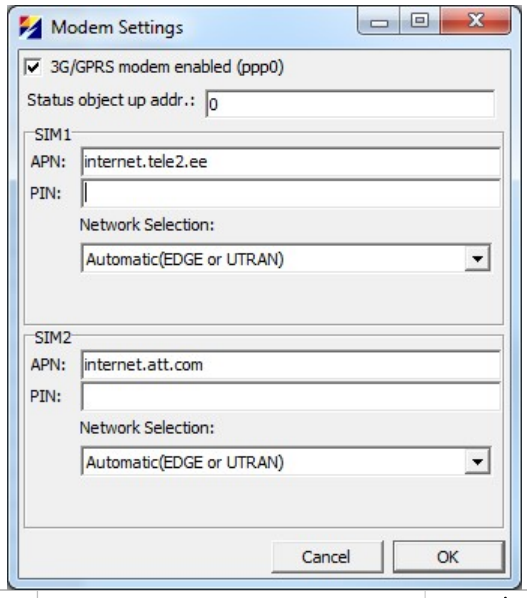
4.4 Timing settings



Initialization timeout: Time in seconds after reboot before communication starts. Must exceed device setup time. Must exceed total device boot/setup time. For IEC 61850 v: recommended 60s (1–5 IEDs), 120s (5–15). Raise if Not-Topical or Invalid values appear after reboot.

4.5 Modem Settings (Telem AGC and GWM)

The Modem Settings section is used to configure 4G/GPRS modem connectivity parameters for Telem AGC and GWM devices. This configuration applies to devices equipped with built-in cellular modems, enabling mobile network access for remote connectivity.



Element	Description	Notes/Behavior
3G/GPRS Modem Enabled (ppp0)	Enables or disables the use of the internal modem (interface ppp0).	If enabled and the Telem device does not manage to connect it shall **restart periodically** around every 6 minutes.
Status Object Up Addr.	Specifies the IEC 60870-5-101/104 IOA (Information Object Address) used for uplinking the modem connection status (M_SP). This value is also transmitted via Modbus Server as Function Code 2 (FN 2) for status monitoring.	0 is disabled. Modbus addressing has offset + 1 from the real register address in this field. I.e., 101 shall request FN2 A100,
APN	Access Point Name provided by the mobile network operator.	
PIN	SIM card PIN code (if required).	Optional. You can lockout your SIM because device retries incorrect PIN multiple times.
Network Selection	Determines preferred network type.	Usually set to Automatic for flexibility.

4.6 Redundant IEC 60870-5-104 Server protocol connections

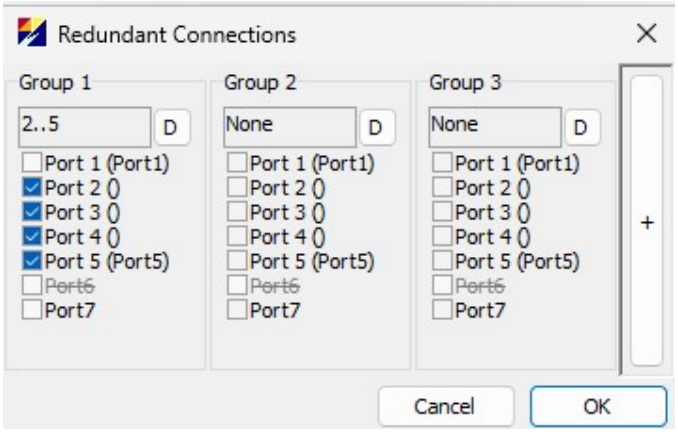
This section allows configuration of redundant connections for IEC 60870-5-104 server protocol according to the IEC 60870-5-104 standard (section 10).
Redundant connections provide fault tolerance by allowing multiple communication channels between the Telem device and SCADA systems. These connections share the same event buffer. Events are sent to only one active channel at a time. If the primary channel becomes unavailable, the Client side SCADA system is expected to automatically switch to a redundant (backup) channel. Detailed configuration of Ports and Protocols is described in Configuring data concentrator.

4.6.1 Use Case

This feature is designed for SCADA environments where redundancy is required due to multiple possible client connections or strict availability requirements.

4.6.2 Config

Maximum number of ports per redundant group: 4



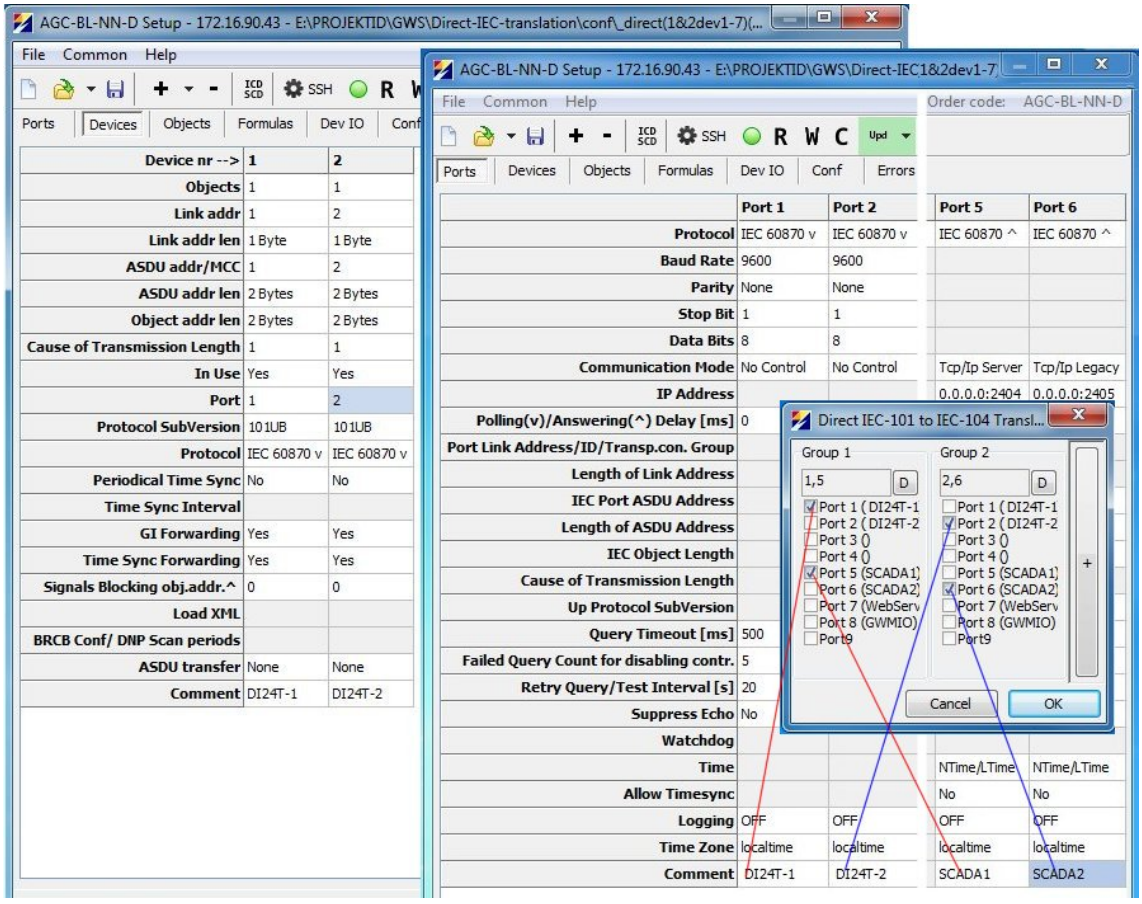
Element	Description	Notes/Behavior
Group comma separated	Textual input like:1,2,6 indicating 3 ports in the group. Can be grouped by two dots if ports numbers are sequential as in example	Is autofilled on tick box clicks
Port Checkboxes	Select specific ports to be included in the redundancy group	Max 4 per group
D (Delete)	Clears the selected group configuration	
+ (Add Group)	Adds a new redundancy group	

4.7 Direct IEC-101 to IEC-104 Translation configuration

This is common in Telem device with Base license.
Determine groups of ports (up to 2 ports in each group) for direct protocol translation (without intermediate database in Telem device) from IEC 60870-5-101 to IEC 60870-5-104 and vice versa. Lower-level device still has to be configured in GWS to determine communication parameters: address, address length etc. Detailed configuration of lower-level devices in described in Configuring data concentrator.

4.7.1 Configuring direct IEC translation (one device per one port)

- Set up Ports and Devices (in upcoming chapters)
- Open menu "Common / Direct IEC-101 to IEC-104 Translation"
- Group ports (one lower channel and one upper channel port in each group)

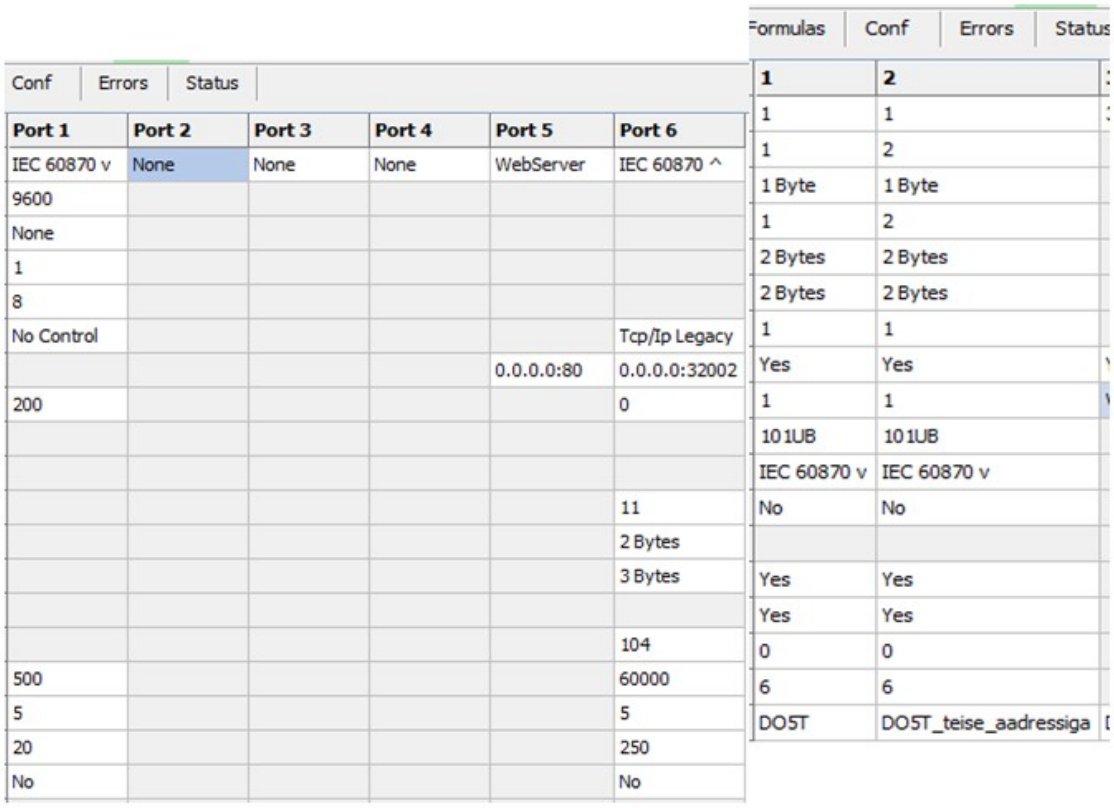


Do not add any rows to the Objects table with Base License, it disables RTU communication if Objects count is greater than 10 (maximum 10 Objects).

4.7.2 Configuring direct IEC translation with ASDU transfer

This method allows to connect several RTU-T modules with one lower-level communication port (example, data translation from 2 devices on the port 1 to port 6).

- Set up Ports (configure parameter for one upper and one lower-level port)
- Configure parameters for devices connected to lower-level port (1 in example below), choose parameter "ASDU transfer" for each device equal to upper-level port number (6 for this example)
- In SCADA use upper level ASDU Address (11 in example below) to reach the Data Concentrator Object Tab data points (if any exist). Use ASDU Addresses in Devices Tab (1 and 2 in examples) to reach the lower-level devices circumventing Data Concentrator Object Tab data points.



Formulas | Conf | Errors | Status

1	2
1	1
1	2
1 Byte	1 Byte
1	2
2 Bytes	2 Bytes
2 Bytes	2 Bytes
1	1
Yes	Yes
1	1
101UB	101UB
IEC 60870 v	IEC 60870 v
No	No
Yes	Yes
Yes	Yes
0	0
6	6
DOST	DOST_teise_aadressiga

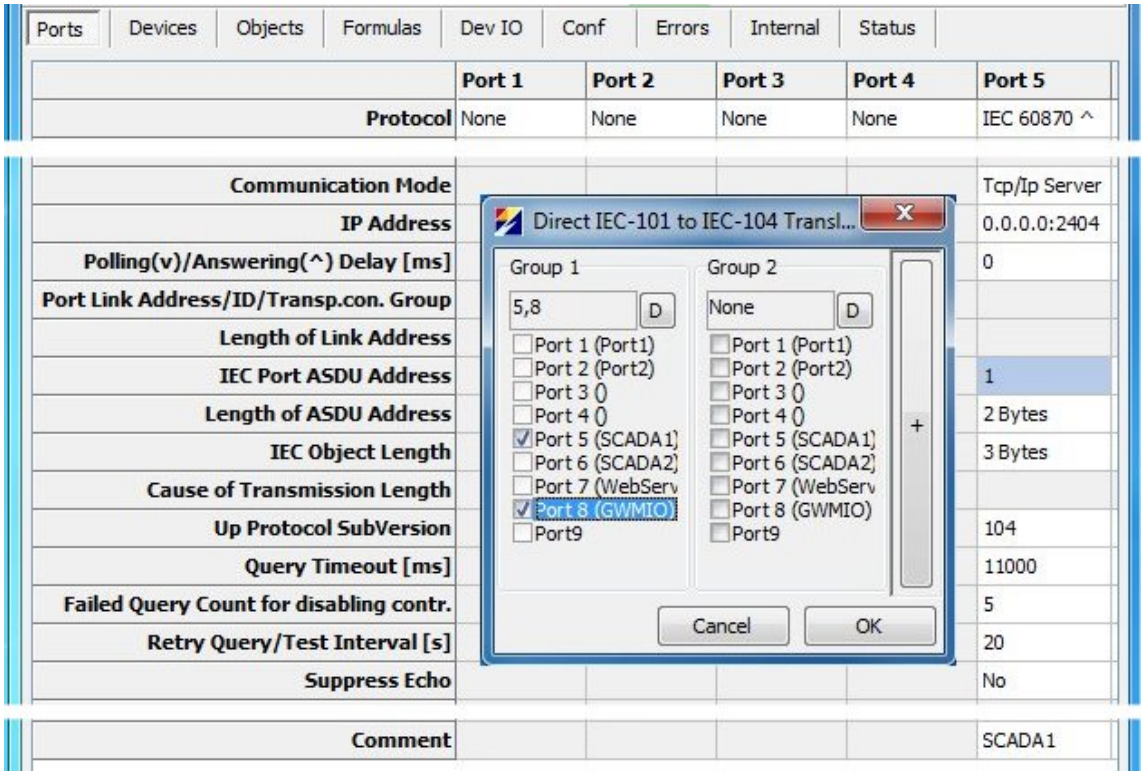
Conf | Errors | Status

Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
IEC 60870 v	None	None	None	WebServer	IEC 60870 ^
9600					
None					
1					
8					
No Control					Tcp/Ip Legacy
				0.0.0.0:80	0.0.0.0:32002
200					0
					11
					2 Bytes
					3 Bytes
					104
500					60000
5					5
20					250
No					No

4.7.3 Configuring direct IEC translation for AGC device IO (Inputs/Outputs)

If Telem-AGC device has IO Digital Inputs/Outputs Board.

- Open menu "Common / Direct IEC-101 to IEC-104 Translation"
- Group device IO port - Port8 (GWMIO) in this example - and one upper-level channel port for SCADA



It is not possible to assign addresses in the 'Dev IO' table if GWMIO is enabled in any 'Direct 101 to 104 Translation' group. Inputs (DI) and Outputs (DO) have fixed addresses:

- The device DI addresses starts from 1 (1, 2, 3, ... and so on)
- The device DO addresses starts from 101 (101, 102, 103, ... and so on)

Other parameters in the Device IO table are configurable excluding "Invert" for DI. Additionally, could be used communication status DI signal of Device IO. This signals address is 0.

Ports | Devices | Objects | Formulas | Dev IO | Conf | Errors | Internal | Status

DI

Nr	SubType ^	Invert	Obj. Addr. ^	Comment	Forb. Ports	Tolerant ph. [ms]	Intolerant ph. [ms]	Base per. [ms]	Change cnt.	Lock ^
1	Single			DI 1	None	10	10	1000	10	1
2	Single			DI 2	None	5	5	500	5	1
3	Single			DI 3	None	5	5	500	5	1
4	Single			DI 4	None	5	5	500	5	1

DO

Nr	SubType v	Invert	Obj. Addr. ^	Comment	Forb. Ports	Pulse Len [ms]	Pulse count	IFR Enabled
1				DO 1	None	1500	1	No
2				DO 2	None	1500	1	No
3				Do 3	None	1500	1	No

4.7.4 Direct IEC translation example - using device IO and RTU-T modules

- Set up Ports and Devices
- Group ports (group 1 for external RTU-T modules, group 2 for AGC device IO)

Ports | Devices | Objects | Formulas | Dev IO | Conf

Device nr -->	1	2
Objects	1	1
Link addr	1	2
Link addr len	1 Byte	1 Byte
ASDU addr/MCC	1	2
ASDU addr len	2 Bytes	2 Bytes
Object addr len	2 Bytes	2 Bytes
Cause of Transmission Length	1	1
In Use	Yes	Yes
Port	1	1
Protocol SubVersion	101UB	101UB
Protocol	IEC 60870 v	IEC 60870 v
Periodical Time Sync	No	No
Time Sync Interval		
GI Forwarding	Yes	Yes
Time Sync Forwarding	Yes	Yes
Signals Blocking obj.addr.^	0	0
Load XML		
BRCB Conf/ DNP Scan periods		
ASDU transfer	5	5
Comment	DI24T-1	DI24T-2

Ports | Devices | Objects | Formulas | Dev IO | Conf | Errors | Internal | Status

	Port 1	Port	Port	Port	Port 5	Port 6	Port 7
Protocol	IEC 60870 v	None	None	None	IEC 60870 ^	IEC 60870 ^	WebServer
Baud Rate	9600						
Parity	None						
Stop Bit	1						
Data Bits	8						
Communication Mode	No Control				Tcp/Ip Server	Tcp/Ip Server	
					0.0.0.0:2404	0.0.0.0:2405	0.0.0.0:80
					0	0	
					11	2	
					2 Bytes	2 Bytes	
					3 Bytes	3 Bytes	
					104	104	
					11000	11000	
					5	5	
					20	250	
Comment	RTU Modules	Port2			SCADA1	SCADA2	WebServer

Direct IEC-101 to IEC-104 Transl...

Group 1: 1,5 D
- [x] Port 1 (Port1)
- [ ] Port 2 (Port2)
- [ ] Port 3 ()
- [ ] Port 4 ()
- [x] Port 5 (SCADA1)
- [ ] Port 6 (SCADA2)
- [ ] Port 7 (WebServ
- [ ] Port 8 (GWMIO)
- [ ] Port9

Group 2: 6,8 D
- [ ] Port 1 (Port1)
- [ ] Port 2 (Port2)
- [ ] Port 3 ()
- [ ] Port 4 ()
- [ ] Port 5 (SCADA1)
- [x] Port 6 (SCADA2)
- [ ] Port 7 (WebServ
- [x] Port 8 (GWMIO)
- [ ] Port9

Cancel | OK

- Configure Objects table, including only RTU-T modules communication status signals
- For communication with RTU-T modules use in SCADA upper level ASDU Address as LINK address and lower-level device address as ASDU address

AGC Objects Table - only communication status signal

Ports | Devices | Objects | Formulas | Dev IO | Conf | Errors | Internal | Stati

	Dev. No.	Obj. No.	Type	SubType ^	SubType v	Obj. Addr. ^	Comment
⊟	1	1	DI	Single	Normal	65001	DI24T-1 com error
⊟	2	1	DI	Single	Normal	65002	DI24T-2 com error

LINK and ASDU addresses in SCADA:

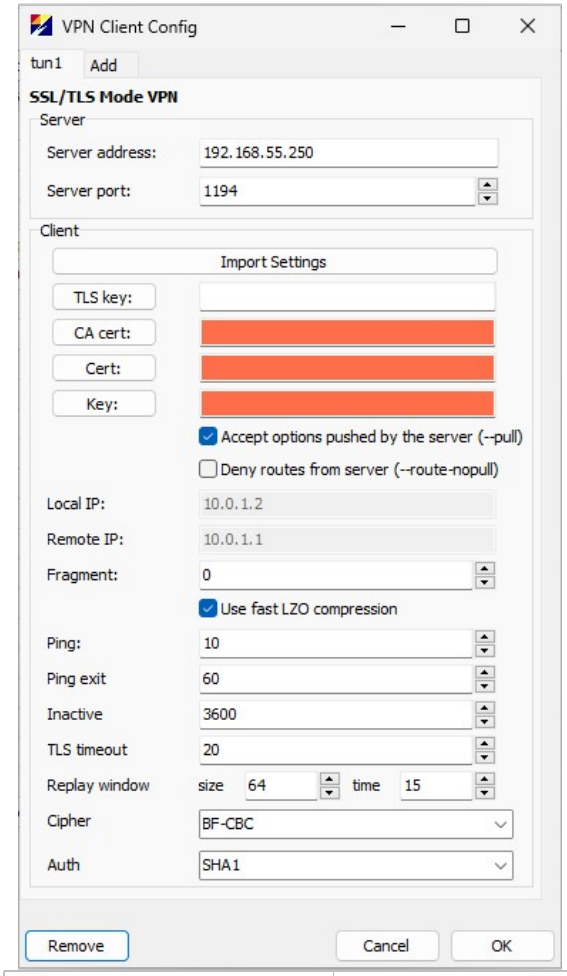
Link addr.	ASDU addr.	Link addr	Comment
11	1	1	DI24T-1 (SCADA 1)
11	2	1	DI24T-2 (SCADA 1)
2	2	1	AGC-DI (SCADA 2)

4.8 OpenVPN

The *OpenVPN* feature enables secure remote communication over public or untrusted networks by establishing encrypted VPN tunnels between the Telem device and remote servers.

This functionality is used to securely integrate Telem devices into isolated networks or remote SCADA systems over the Internet or other intermediary networks.

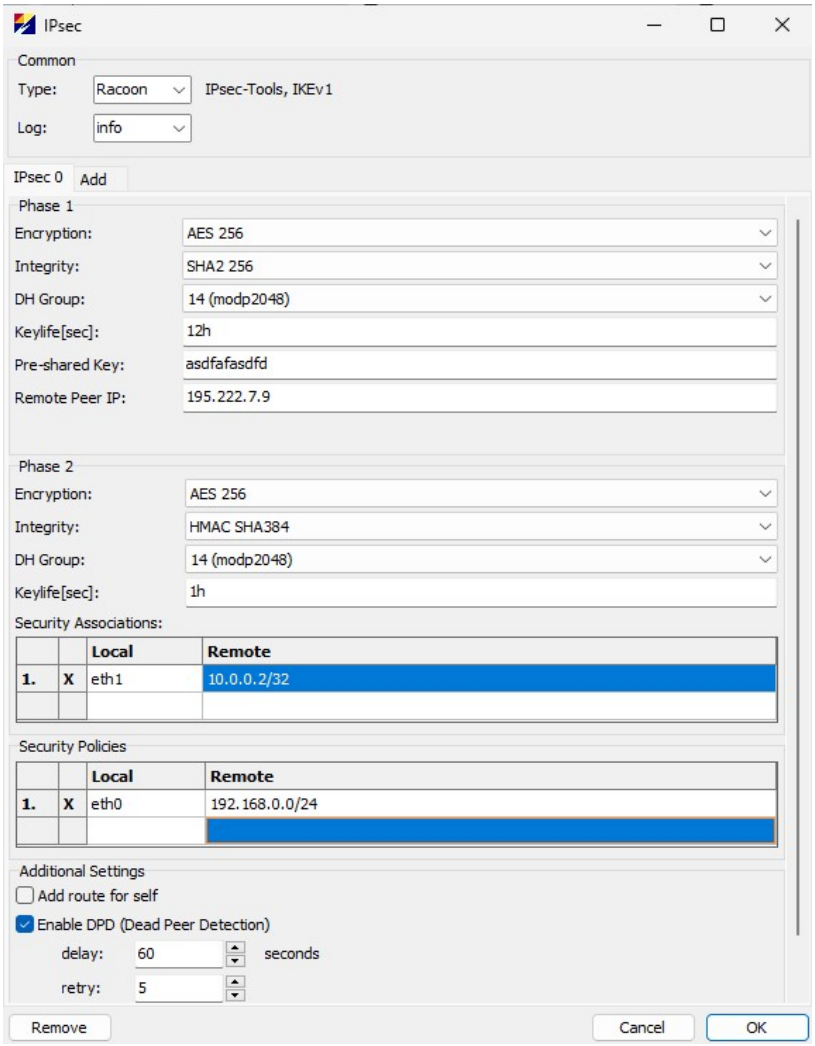
Key Characteristics:
Up to 4 independent OpenVPN tunnels are supported per device.
Supports standard OpenVPN configuration principles.
Supports both manual configuration and import from .ovpn configuration files.



Field	Purpose	Example / Notes

Import Settings	Imports configuration from a standard OpenVPN .ovpn file.	Automatically fills most fields.
TLS Key	SSL/TLS pre-shared key used for session authentication.	Optional based on server config.
CA Cert	Certificate Authority root certificate used to verify server identity.	Same for all clients connecting to the same VPN server.
Cert	Client certificate for device authentication.	Provided per device/user.
Key	Private key corresponding to the client certificate.	Must match the provided Cert.
Server Address	VPN server IP address or hostname.	
Server Port	VPN server listening port.	Default: 1194
Accept options pushed by the server	Accept configuration pushed from VPN server (--pull).	Recommended default.
Deny routes from server	Prevents server from altering client routing table. (--route-nopull).	Optional.
Local IP	Local virtual VPN interface IP.	
Remote IP	VPN server virtual IP.	
Fragment	Packet fragmentation size in bytes.	Usually 0 (disabled).
Use fast LZO compression	Enables LZO data compression.	Optional.
Ping	Keepalive ping interval (seconds).	Default: 10
Ping Exit	Time (seconds) to terminate connection without response.	Default: 60
Inactive	Idle timeout (seconds).	Default: 3600
TLS Timeout	TLS negotiation timeout (seconds).	Default: 20
Replay Window Size	Anti-replay protection window size (packets).	Default: 64
Replay Window Time	Anti-replay time window (seconds).	Default: 15
Cipher	Encryption cipher algorithm.	
Auth	Authentication algorithm.	

4.9 IPsec



The IPsec functionality in Telem devices enables secure site-to-site or remote access VPN tunnels using the IKE (Internet Key Exchange) protocol, providing confidentiality, integrity, and authentication for communication over untrusted networks.
Telem-GWS supports both IKEv1 and IKEv2 standards with flexible configuration for Phase 1 (IKE negotiation) and Phase 2 (ESP data protection).

4.9.1 Supported Backends for IPsec

Backend	Notes
Racoon	Requires manual configuration of Security Associations (SAs) and Security Policies. Generates racoon.conf and dynamic SPD handling via setkey.
StrongSwan / Stroke / VICI	Phase 1 and Phase 2 settings and SAs .No GUI field for Security Policies.

4.9.2 General IPsec Configuration Structure in GUI

Section	Purpose
Phase 1	Defines IKE negotiation parameters (encryption, hashing, DH group, lifetime, peer address, pre-shared key).
Phase 2	Defines ESP data protection parameters (encryption, hashing, DH group, lifetime).
Security Associations (Local / Remote)	Manually defines which local interface and remote network are protected by the IPsec tunnel. Mandatory for all backends.
Security Policies (Local / Remote)	Specific to Racoon. Defines SPD entries (protected traffic selectors) for dynamic insertion via setkey. Required to actually encrypt traffic.
Additional Settings	Dead Peer Detection (DPD), Route insertion, etc.

4.9.3 Phase 1 Parameters (IKE Negotiation)

Parameter	Supported Options
Encryption Algorithms	DES, 3DES, Blowfish, AES 128, AES 256
Integrity (Hash)	MD5, SHA1, SHA2 (SHA256, SHA384, SHA512)
DH Groups	1 (modp768), 2 (modp1024), 5 (modp1536), 14 (modp2048), 15 (modp3072), 16 (modp4096)
Key Lifetime	Configurable (e.g., 12h)
Remote Peer IP	Remote VPN peer address
Pre-shared Key	Secret key shared between peers

4.9.4 Phase 2 Parameters (ESP Protection)

Parameter	Supported Options
Encryption Algorithms	DES, 3DES, Blowfish, AES 128, AES 256
Integrity (Hash)	DES, 3DES, HMAC MD5, HMAC SHA1, HMAC SHA256[1], HMAC SHA384, HMAC SHA512
DH Groups	Same as Phase 1
Key Lifetime	Configurable (e.g., 1h)

4.9.5 Security Associations (Manually Configured)

Defines which local interface (ethX) is used for IPsec and which remote network the tunnel protects.

Field	Purpose
Local	Local interface (e.g., eth1)
Remote	Remote protected network (e.g., 10.0.0.2/32)

[1]HMAC SHA256 is nonstandard 96bit, latest standard uses 128bit version of HMAC SHA256

4.9.6 Racoon-Specific: Security Policies (Mandatory)

Defines which traffic should be protected (SPD entries). This generates dynamic `setkey` commands in runtime scripts.

Field	Purpose	Example
Local	Local network or interface	eth0 or 192.168.0.0/24
Remote	Remote network to protect	192.168.0.0/24

Both Security Association and Security Policy entries must match to enforce IPsec encryption.

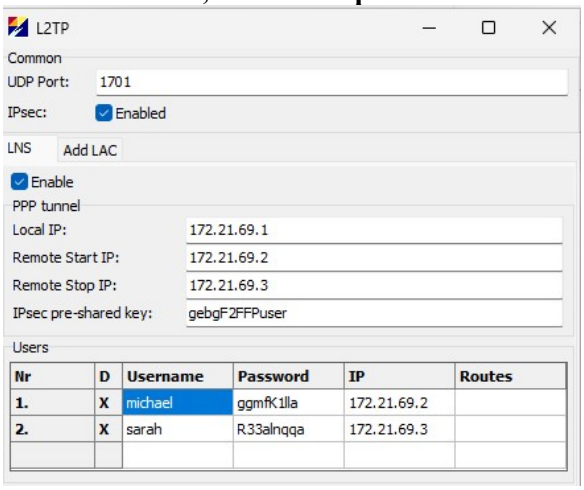
4.9.7 Additional Settings

Field	Purpose
Add route for self	Inserts static route to remote peer via tunnel.
Enable DPD (Dead Peer Detection)	Monitors peer availability and cleans SAs on failure.
DPD Delay / Max Fail	Retry and fail parameters for DPD.

4.10 L2TP

The L2TP configuration section in Telem-GWS provides settings to establish Layer 2 Tunneling Protocol (L2TP) VPN tunnels for remote client access. L2TP allows remote users to securely connect to a private network over public or shared infrastructure. It is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.

Important: L2TP itself does not provide encryption or confidentiality. To ensure secure communication, the IPsec option should be enabled in conjunction with L2TP tunnels.



4.10.1 Functions

Remote access VPN for user devices.

Provides static IP address assignment per user.

Supports user-based authentication using CHAP (Challenge Handshake Authentication Protocol).

Optional IPsec encryption for confidentiality and integrity.

4.10.2 GUI Elements — L2TP Configuration Window

Field	Purpose	Example
UDP Port	Specifies the L2TP server listening port. Default: 1701	
IPsec	Enables or disables IPsec protection for the L2TP tunnel.	Recommended: Enabled
Enable PPP Tunnel	Enables L2TP server functionality.	Checkbox

4.10.3 PPP Tunnel Parameters

Field	Purpose	Example
Local IP	The internal IP address assigned to the Telem device (VPN server side) within the L2TP tunnel.	172.21.69.1

Remote Start IP	First IP address in the pool allocated to connecting clients.	172.21.69.2
Remote Stop IP	Last IP address in the pool allocated to clients.	172.21.69.3
IPsec Pre-shared Key	Pre-shared key used for authenticating and securing L2TP over IPsec connections.	Example: geb9r2FFPUser

4.10.4 User Management Section

Defines individual VPN user accounts and their assigned IP addresses within the L2TP tunnel.

Field	Purpose	Example
Username	Username for L2TP client authentication.	michael
Password	Password for CHAP authentication.	ggmfK1lla
IP	Static IP address assigned to the user within the VPN tunnel. Must match Remote Start/Stop IP range.	172.21.69.2

4.10.5 Authentication and Connection Behavior

- VPN users are authenticated based on their configured Username and Password credentials.
- Each user is assigned a static IP address as specified in the configuration.
- The supported authentication protocol for L2TP users is CHAP (Challenge Handshake Authentication Protocol).

Note: Other methods (PAP, MSCHAP, MSCHAPv2, EAP) are explicitly disabled in order to enforce secure authentication practices and to simplify configuration management in SCADA and industrial network environments.
The combination of CHAP for authentication and IPsec for tunnel encryption ensures secure user access without the need for additional external authentication infrastructure.

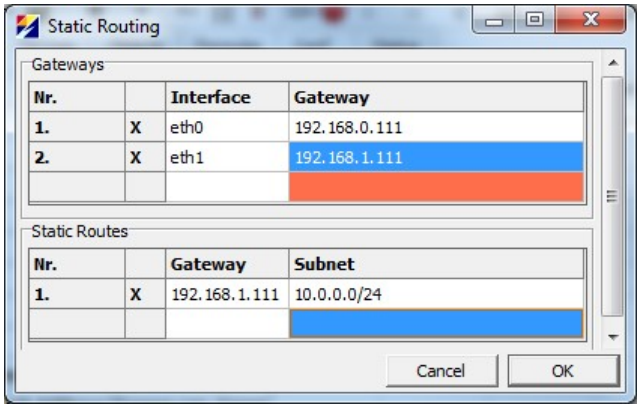
- VPN connection and disconnection events are logged.
- When IPsec is enabled, VPN traffic between the client and the device is encrypted. If IPsec is disabled, VPN traffic will be transmitted unencrypted (plaintext).

4.10.6 Operational Notes

- The number of VPN users is limited by the available IP address range and device resources.
- IP addresses assigned to users must be within the configured Remote Start IP and Remote Stop IP range.
- Duplicate usernames are not allowed.
- The device automatically handles session establishment, user authentication, IP address assignment, and basic routing of VPN client traffic.

4.11 Static Routing

This command adds a static route to the system routing table.



"To reach the network 10.0.0.0/24, send packets through the gateway 192.168.1.111."

In linux terms: ip route add 10.0.0.0/24 via 192.168.1.111

This means that any traffic the system needs to send to IP addresses in the 10.0.0.0 to 10.0.0.255 range will be forwarded to the gateway 192.168.1.111 via interface eth0.

4.11.1 Gateways Section

Defines gateway addresses associated with specific interfaces.

Field	Purpose	Example
Interface	Device network interface used to reach the gateway.	eth0
Gateway	IP address of the gateway.	192.168.0.111

4.11.2 Static Routes Section

Defines routing rules linking destination subnets to specific gateways.

Field	Purpose	Example
Gateway	Previously defined gateway used for this route.	192.168.1.111
Subnet	Destination network in CIDR notation (IP/mask).	10.0.0.0/24

4.11.3 Operational Behavior

When the device needs to send traffic to a destination within the defined subnet, it forwards the traffic to the specified gateway.

The gateway must be reachable via one of the configured interfaces.

The system determines the outgoing interface automatically based on the gateway's IP address.

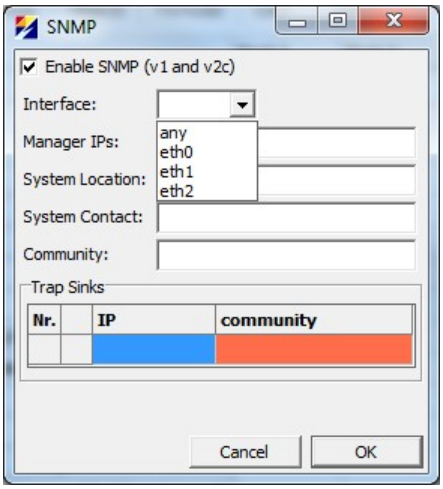
Routes are static — no automatic updates or dynamic routing protocols are used.

4.12 SNMP

The *SNMP* (Simple Network Management Protocol) feature in Telem-GWS provides monitoring and management capabilities for network-connected Telem devices. SNMP enables remote systems, such as network management platforms (NMS), to collect status information and receive event notifications (traps) from the device.

Supported SNMP versions:

- SNMPv1
- SNMPv2c



4.12.1 SNMP Configuration Window

Field	Purpose	Example / Notes
Enable SNMP (v1 and v2c)	Enables or disables SNMP service on the device.	Checkbox
Interface	Selects the network interface(s) where SNMP will listen for requests.	Options: any, eth0, eth1, eth2
Manager IPs	Restricts SNMP access to specified IP addresses. If empty → any source is allowed.	List of trusted NMS IP addresses
System Location	Descriptive text string identifying physical or logical location of the device.	Example: Data Center R1
System Contact	Contact person or responsible party for the device.	Example: admin@example.com
Community	SNMP community string used for authentication (read-only or read-write).	Example: public

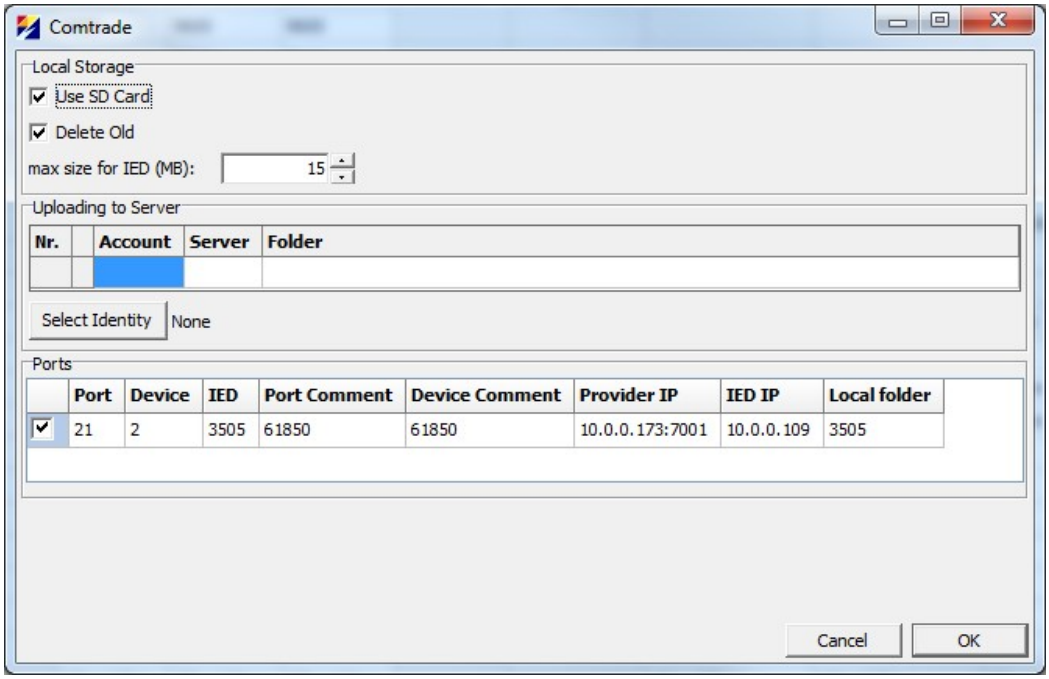
4.12.2 Trap Sinks Section

Defines SNMP trap recipients (management systems to which the device will send notifications).

Field	Purpose	Example
IP	IP address of the SNMP trap receiver.	192.168.1.100
Community	SNMP community string used for traps sent to this IP.	public

4.13 Comtrade

This functionality enables to automatically read comtrade file via IEC61850 file I/O from IED-s and save them. It is possible to upload files to remote server or save them in TELEM-AGC internal memory or save on SD card.
TELEM-AGC can be used for comtrade saving only as an addition to already working RTU. It could be convenient upgrade to an already working substation.



4.14 PriSec System

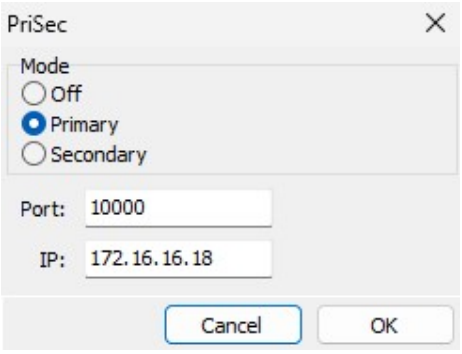
Using two Telem device it is possible to create physical redundancy (failover) system - PriSec System. One RTU (PRI) shall be active, while other RTU (SEC) is in “hot standby mode”, i.e. mirroring the internal state of PRI. On PRI failure, SEC takes over communication role of PRI.
According to IEC 60870-5-104 Part 10, the *Redundancy aware SCADA* establishes TCP connections to both Telem devices in the PriSec System and may choose any one of the connections to start the protocol level communication. If SCADA starts protocol level communication over the connection with SEC Telem device, the device forwards the data packets to PRI for processing.

4.14.1 PriSec – Pri device configuration

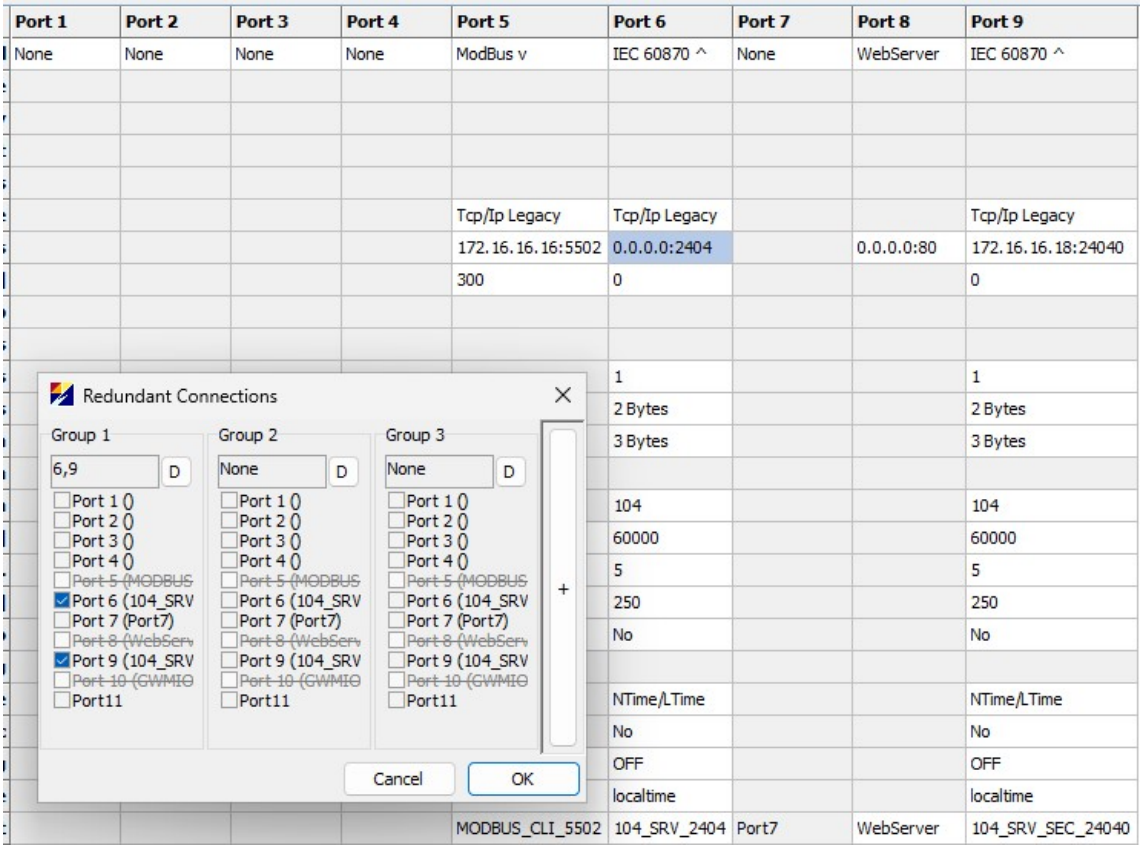
Example PRI conf below: 2242-PS-PRI-from-tx-2_13032025.tar.xz

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Protocol	None	None	None	None	ModBus v	IEC 60870 ^	None	WebServer
Baud Rate								
Parity								
Stop Bit								
Data Bits								
unication Mode					Tcp/Ip Legacy	Tcp/Ip Legacy		
IP Address					172.16.16.16:5502	0.0.0.0:2404		0.0.0.0:80
(^) Delay [ms]					300	0		
nsp.con. Group								
of Link Address								
t ASDU Address						1		
f ASDU Address						2 Bytes		
Object Length						3 Bytes		
mission Length								
ocol SubVersion						104		
y Timeout [ms]					500	60000		
disabling contr.					5	5		
est Interval [s]					20	250		
Suppress Echo					No	No		
Watchdog								
Time						NTime/LTime		
Allow Timesync						No		
Logging					OFF	OFF		
Time Zone					localtime	localtime		
Comment					MODBUS_CLI_5502	104_SRV_2404	Port7	WebServer

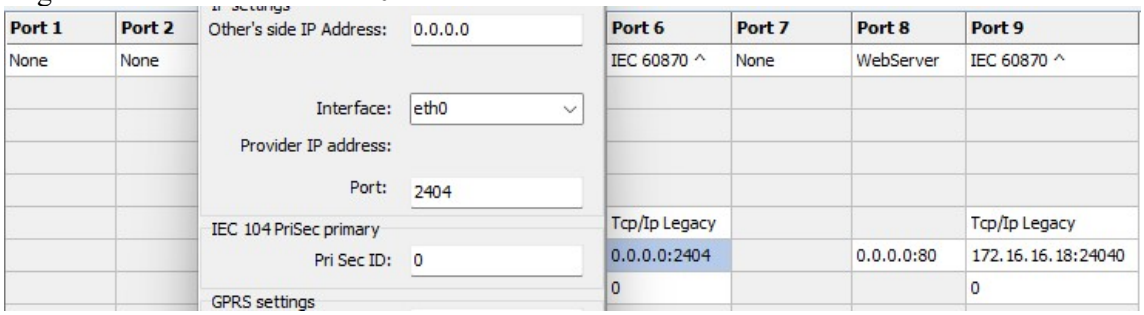
Create all the required Ports , Devices, Objects, Dev IO and Formula Tab entries. These have to be initially identical between PRI and SEC in terms of amount (and position) of Ports, Devices and all Objects. Comments, IP parameters, timeouts can differ. All other GWS setup does not have to identical. Save this config, this shall be used as base for SEC. Proceed with PRI configuration.
Under **Common** open the **PriSec** configuration window and select **Mode** as **Primary**. Enter **Port** number not used by any Server protocol in Ports tab. Set **IP** to the IP address of the SEC RTU. Click **OK**.



Below is the image of same PRI conf, but with an additional „IEC 60870 ^“ (Port 9). PRI RTU must have one *additional* „IEC 60870 ^“ Port per each „IEC 60870 ^“ Port that the redundancy aware SCADA connects to. Use an unused TCP port for the additional „IEC 60870 ^“ Port. And the original „IEC 60870 ^“ (Port 6) must be in the same **Redundant Connections** Group with the additional PRI RTU specific (Port 9). The additional „IEC 60870 ^“ Port on PRI is for SEC device to transfer data if SCADA happens to start communication on SEC.



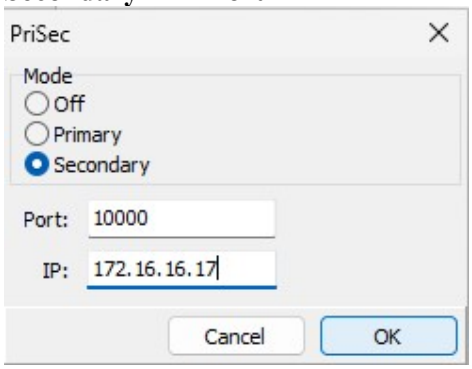
Note that initial example conf did not require any **Redundant Connections** configuration without PriSec.
In **IP Settings** for Port 6 and Port 9 there is **Pri Sec ID**. It must be the same for each pair of original/additional Port. Value 0 is valid.



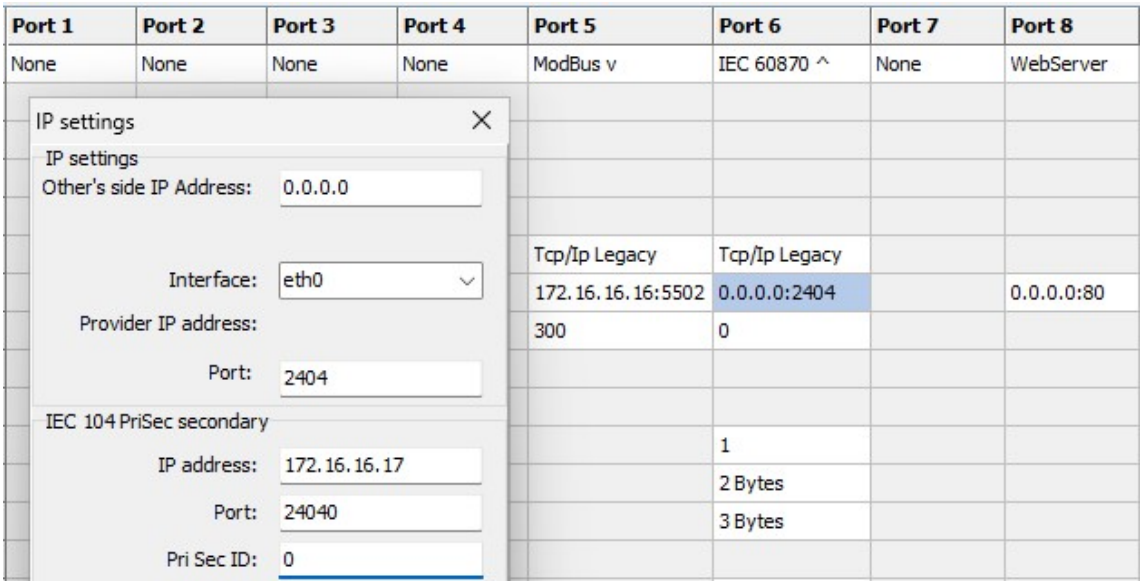
4.14.2 PriSec – SEC device conifguration

Example SEC conf used in following examples: 2242-PS-SEC-from-tx-2_13032025.tar.xz

Open the previously saved base conf from PRI config step (Before additional „IEC 60870 ^“ Port was added). Under **Common** open the **PriSec** configuration window and select **Mode** as **Secondary**. The **Port** has to be identical to PRI conf and **IP** must be set to point back to PRI.



The **IP Settings** of „IEC 60870 ^“ Port for SCADA must be configured for SEC. In **IEC 104 PriSec secondary** section in the **IP Settings** input the parameters of the *additional* „IEC 60870 ^“ Port in PRI. SEC shall redirect traffic from SCADA in case SCADA chooses to establish communication with SEC.



SCADA that connects to 4 Ports
There can be 2 RTUs in the PriSec system, but if SCADA needs to do 4 connections. Then each RTU shall have two original „IEC 60870 ^“ Ports with different **Pri Sec ID** in the **IP Settings** tab. This shall be used as base for SEC later. In addition PRI must have two *additional* „IEC 60870 ^“ Ports per each original with matching **Pri Sec Id**s in the **IP Settings** window. For PRI all the original and additional Ports must be in the same **Redundant Connections** group. In this case for SEC the two „IEC 60870 ^“ Ports must also be in the same **Redundant Connections** group.

5 Configuring data concentrator

Parameters described in the previous chapters were mainly about, how to setup network connection and overall settings of the device. In this chapter data concentrator functionality of Telem Devices is described.

5.1 Shortcut icons

New: Open new default configuration
Open: Open saved configuration
Save: Save configuration

Add: ports/devices/objects/formulas.
Remove: ports/devices/objects/formulas

ICD/SCD: Import IEC61850 ICD/SCD file (described in the following chapters)

R: No function
SSH Settings:
R: Read configuration from device
W: Write configuration to device
C: Cancel procedure
Upd.: Update firmware

Export: Export configuration to .csv file format
Import: Import configuration from .csv file format (previously exported)

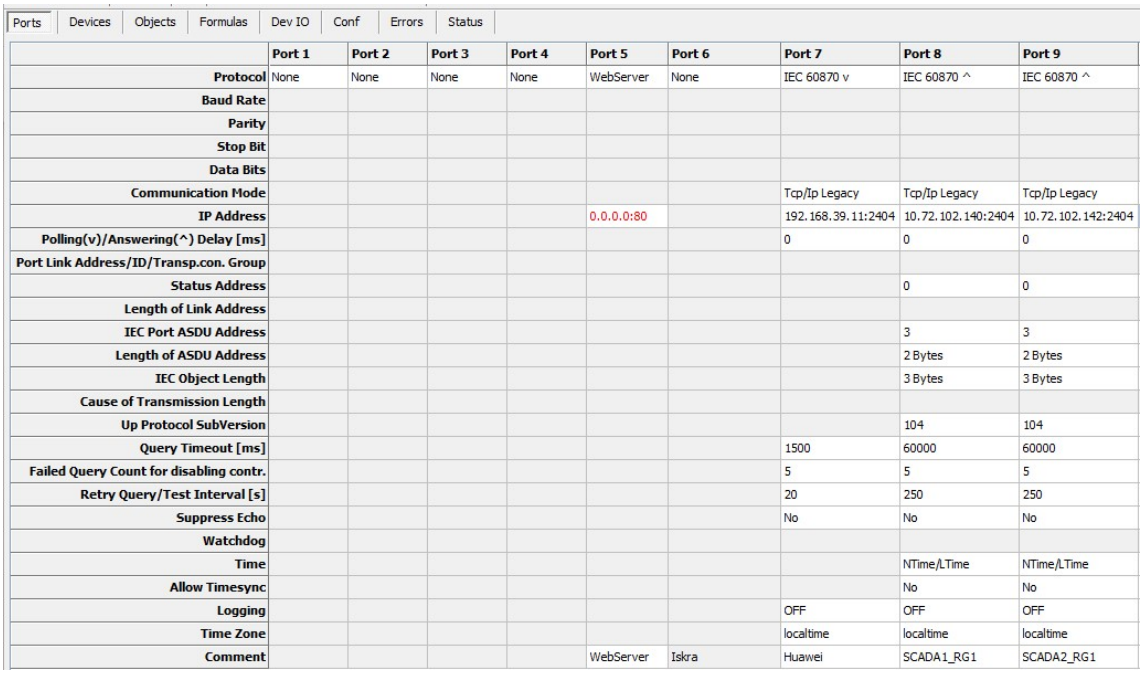
WWW: Opens webserver, if it is configured, button appears only if Webserver is found in configuration.

5.2 Tab cards

Most of the data concentrator parameters have to be set in the tab cards. In this chapter functionality and purpose of each tab card is described.

5.2.1 Ports Tab Card

The *Ports* tab in Telem-GWS allows configuring communication parameters for all physical and logical ports available on the device. The type and number of ports vary depending on the specific hardware model. Typically, the first ports listed correspond to physical serial ports, while subsequent ports may represent TCP/IP-based interfaces or other virtual ports.
Port usage assignment to devices is performed in the *Devices* tab, where the specific port assigned to each device is configured.
Each port supports a variety of communication protocols and operational parameters, allowing integration with different SCADA systems, remote units, and communication standards.



Ports | Devices | Objects | Formulas | Dev IO | Conf | Errors | Status

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9
Protocol	None	None	None	None	WebServer	None	IEC 60870 v	IEC 60870 ^	IEC 60870 ^
Baud Rate									
Parity									
Stop Bit									
Data Bits									
Communication Mode							Tcp/Ip Legacy	Tcp/Ip Legacy	Tcp/Ip Legacy
IP Address					0.0.0.0:80		192.168.39.11:2404	10.72.102.140:2404	10.72.102.142:2404
Polling(v)/Answering(^) Delay [ms]							0	0	0
Port Link Address/ID/Transp.con. Group									
Status Address								0	0
Length of Link Address									
IEC Port ASDU Address								3	3
Length of ASDU Address								2 Bytes	2 Bytes
IEC Object Length								3 Bytes	3 Bytes
Cause of Transmission Length									
Up Protocol SubVersion								104	104
Query Timeout [ms]							1500	60000	60000
Failed Query Count for disabling contr.							5	5	5
Retry Query/Test Interval [s]							20	250	250
Suppress Echo							No	No	No
Watchdog									
Time								NTime/LTime	NTime/LTime
Allow Timesync								No	No
Logging							OFF	OFF	OFF
Time Zone							localtime	localtime	localtime
Comment					WebServer	Iskra	Huawei	SCADA1_RG1	SCADA2_RG1

5.2.2 Protocol Direction Indicators

Protocols assigned to ports are displayed with additional symbols:

Symbol	Meaning
^ (Up arrow)	Uplink — The port operates in Server mode, waiting for incoming client connections.
v (Down arrow)	Downlink — The port operates in Client mode, initiating outbound connections to remote servers.

Example:
`Modbus v` → The port uses the Modbus protocol in Client mode (actively connects to a server).
`IEC 60870 ^` → The port uses IEC 60870 protocol in Server mode (listens for incoming connections).

5.2.3 Ports Configuration Parameters

Parameter	Purpose	Example / Notes
Protocol	Communication protocol assigned to the port.	Modbus, IEC 60870, WebServer, etc.
Baud Rate	Communication speed for serial ports.	Typical values: 9600, 19200
Parity	Parity bit usage.	None, Even, Odd
Stop Bit	Number of stop bits.	1 or 2
Data Bits	Number of data bits per character.	7 or 8

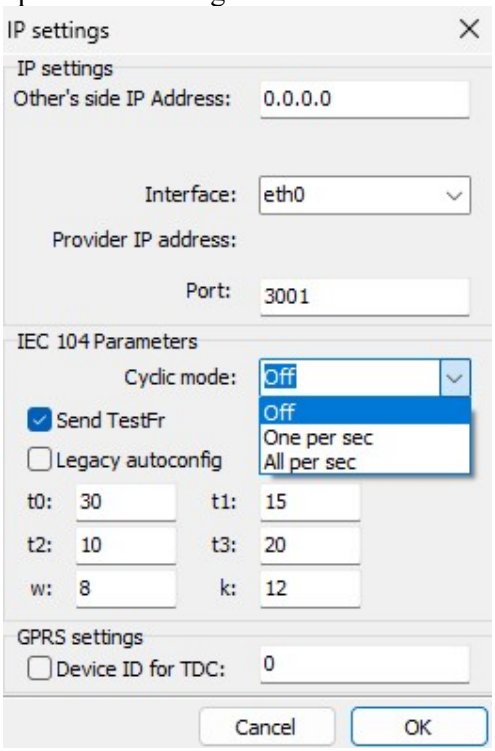
Modem Settings	GPRS modem connection check period.	Applicable only if GPRS modem selected as protocol.
Communication Mode	Defines connection type and subtype: No Control (Serial comm) TCP/IP Legacy TCP/IP Client TCP/IP Server	No Control applicable only for physical serial ports. TCP/IP Legacy means tcp socket type (connect or listen) is derived from Protocol Parameter
IP Address / Other side IP Address	IP address of remote device or server mask (when using TCP/IP modes).	On click opens more configurations depending on Protocol Parameter. Described in details in another table further.
Polling(v)/Answering(^) Delay [ms]	Delay before sending next query.	Integer ms
Port Link Address/ID/Transp.com. Group	Depends on protocol.	Port Link (IEC 870, Modbus) address for Server "^" type protocols. ID for OPC UA. More info in own chapter.
Status Address	Enables server status checking.	0 disables, >0 enables Valid values 0- 16777215.
Length of Link Address	Byte length of link address on uplink.	1 or 2
IEC Port ASDU Address	ASDU address for IEC protocols.	Integer
Length of ASDU Address	Byte length of ASDU address.	1 or 2
IEC Object Length	Byte length of IEC object address.	1, 2, 3
Cause of Transmission Length	IEC 60870-5-101 type protocols. IEC 60870-5-104 hardcoded to 2 bytes as per standard.	1 or 2 bytes
Up Protocol SubVersion	Protocol sub-version for uplink communication.	Drop down list. Depends on Protocol Parameter.
Query Timeout [ms]	Time before query/request is considered failed.	Integer ms
Failed Query Count for disabling contr.	Number of failed sequential queries before marking device as down.	Integer
Retry Query/Test Interval [s]	Time to retry communication with failed device.	Integer s
Suppress Echo	Disable echo of sent data.	If the sent messages are echoed back by the connected devices then they need to be suppressed
Watchdog	Enable watchdog reset on ICMP failure	ICMP Protocol only
Time	Time tag type for events.	Short time or Long time
Allow Timesync	Enable/disable time synchronization over this port.	Yes / No
Logging	Additional logging capabilities.	Possibility to log pcap directly to Wireshark or other pcap capable

		server.
Time Zone	Time zone setting for event timestamping.	localtime / UTC / region... selectable from predefined time zones. This feature has own chapter.
Comment	Free-text field for notes.	Any

5.2.4 IP address Parameters window

5.2.4.1 IEC 60870-5-104

This section defines the IP communication parameters and IEC 60870-5-104 specific operational settings for the selected communication port.



IP Settings Section

Field	Purpose	Example / Notes
Other's side IP Address	Defines the IP address of the remote IEC 104 server if Protocol Parameter is type Client "v". Defines the IP mask of allowed remote IEC 104 client if Protocol Parameter is type Server "^".	Example: 0.0.0.0 — wildcard to accept any address (used for Server mode).
Interface	Selects the physical Ethernet interface used for communication on this port. This works only if firewall is enabled.	Example: eth0

Provider IP Address	Not used	
Port	Defines the TCP port number used for IEC 104 communication.	Typical default: 2404

IEC 104 Parameters Section

Field	Purpose	Example / Notes
Cyclic mode	Controls the automatic transmission of AI (Analog Input) values cyclically. **Only Server ^ protocol type.**	Options: • `Off` — No cyclic sending of AI values (default). • `One per sec` — Send one AI value per second in round-robin order. • `All per sec` — Send all AI values every second.
Send TestFr	Controls sending of IEC 104 Test Frames.	Enabled → Device sends `TestFrame` messages and accepts `TestFrame` from peer (Client or Server). Disabled → Device only accepts incoming `TestFrame` but does not send them actively.

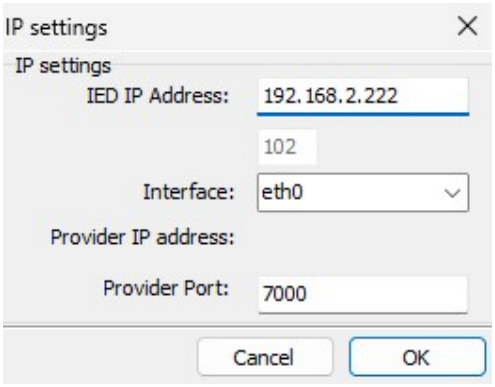
Legacy autoconfig	Automatic calculation of IEC 104 timing parameters t1, t2, t3 based on query settings in *Ports* tab.	Disabled → User must manually configure all timing parameters t1, t2, t3, w, k.
		Enabled → Device derives t1, t2, t3 automatically based on *Query Timeout* and *Retry Query* values as:
		t1 = Query Timeout
		t2 = Retry Query / 2
		t3 = Retry Query
		Requirements:
		`t2 < t1`
		`t1 < t3`
		If these requirements are not met, RTU program applies the following algorithm:
		`Query timeout = Retry Query - Retry Query / 4`
		More info on these params below.

GPRS Settings: for GPRS modem ID detection from TDC/IEC software.

IEC timing parameters explanation

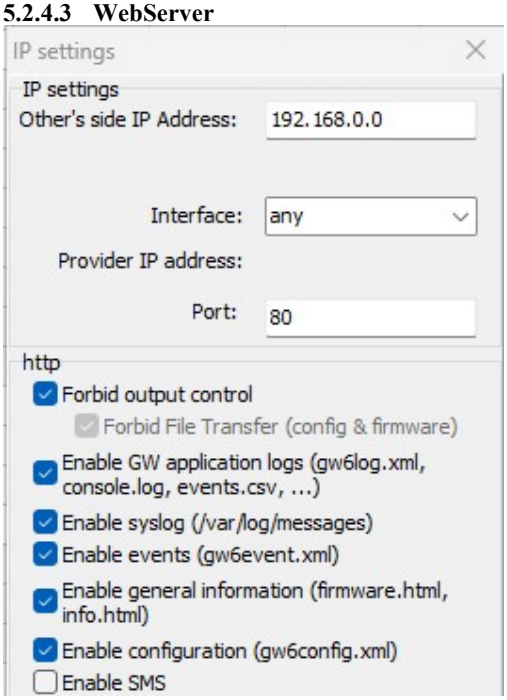
Field	Purpose	Example
t0	Maximum time allowed for establishing the initial connection, in seconds. Only TCP Client	30
t1	Maximum time to wait for a confirmation response after sending an APDU (Application Protocol Data Unit), in seconds.	15
t2	Minimum time to wait before sending a confirmation for a received APDU, in seconds.	10
t3	Maximum idle time before automatically sending a test APDU to check connection health, in seconds.	20
w	Maximum number of received APDUs allowed before sending a confirmation.	8
k	Maximum number of unconfirmed sent APDUs allowed before requiring confirmation.	12

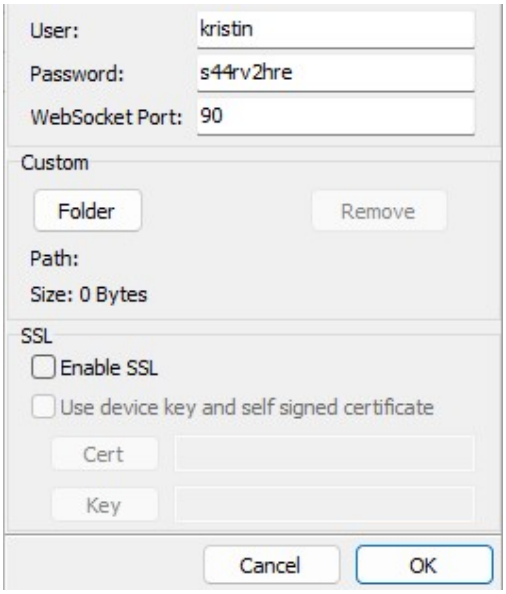
5.2.4.2 IEC 61850 v



Field	Purpose	Example / Notes
Other's side IP Address	Defines the IP address of the remote IEC 104 server if Protocol Parameter is type Client "v". Defines the IP mask of allowed remote IEC 104 client if Protocol Parameter is type Server "^".	IEC 61850 is Client only on application and TCP level. IED IP must be set.
Interface	Selects the physical Ethernet interface used for communication on this port. **This works only if firewall is enabled.**	Example: eth0
Port	For IEC 61850 it is always 102	Not configurable
Provider port	Internal TCP port of IEC 61850 provider within RTU. Port 7000, 7001, ... is recommended. In each network segment different port number has to be used.	Only set different port numbers if there are multiple IEC 61850 IEDs in different LANs (they commonly have different interfaces).

5.2.4.3 WebServer





The *WebServer* port configuration in Telem-GWS allows defining the HTTP/HTTPS access settings for the embedded web interface. It also provides fine-grained control over what types of web content, configuration files, and log outputs are accessible via HTTP/S.
This port enables both standard web access (for monitoring and maintenance) and WebSocket-based services (used by front-end tools or custom dashboards).

GUI Elements — WebServer IP Settings

Field	Purpose	Example
Other's side IP Address	Restricts incoming web access to the specified IP or subnet. Use 0.0.0.0 to allow all.	192.168.0.0
Interface	Selects which Ethernet interface is used to listen for incoming web requests.	any, eth0, eth1, etc.
Provider IP address	Unused	
Port	TCP port for HTTP access.	Default: 80

HTTP Access Options

Option	Description
Forbid output control	Disables any remote switching or control commands via the web interface. Safety feature for monitoring-only access.
Forbid File Transfer (config & firmware)	Prevents downloading or uploading of configuration files and firmware over HTTP.
Enable GW application logs	Exposes gateway application logs via the web server (e.g., gw6log.xml, console.log, events.csv).
Enable syslog	Allows viewing logs from /var/log/messages through the web interface.
Enable events	Publishes system event log in XML format (e.g., gw6event.xml).
Enable general information	Enables firmware info, runtime status pages (e.g., firmware.html, info.html).
Enable configuration	Allows retrieval of current configuration snapshot (gw6config.xml).
Enable SMS	Enables web access to SMS-related services (if supported by hardware). Currently unchecked — feature availability may vary.

Field	Description	Example
User	Username for plaintext access authentication.	kristin
Password	Password for plaintext authentication.	s44rv2hre
WebSocket Port	TCP port for WebSocket connections. Used by custom tools or browser-based dashboards.	90

Custom File Hosting (Optional)

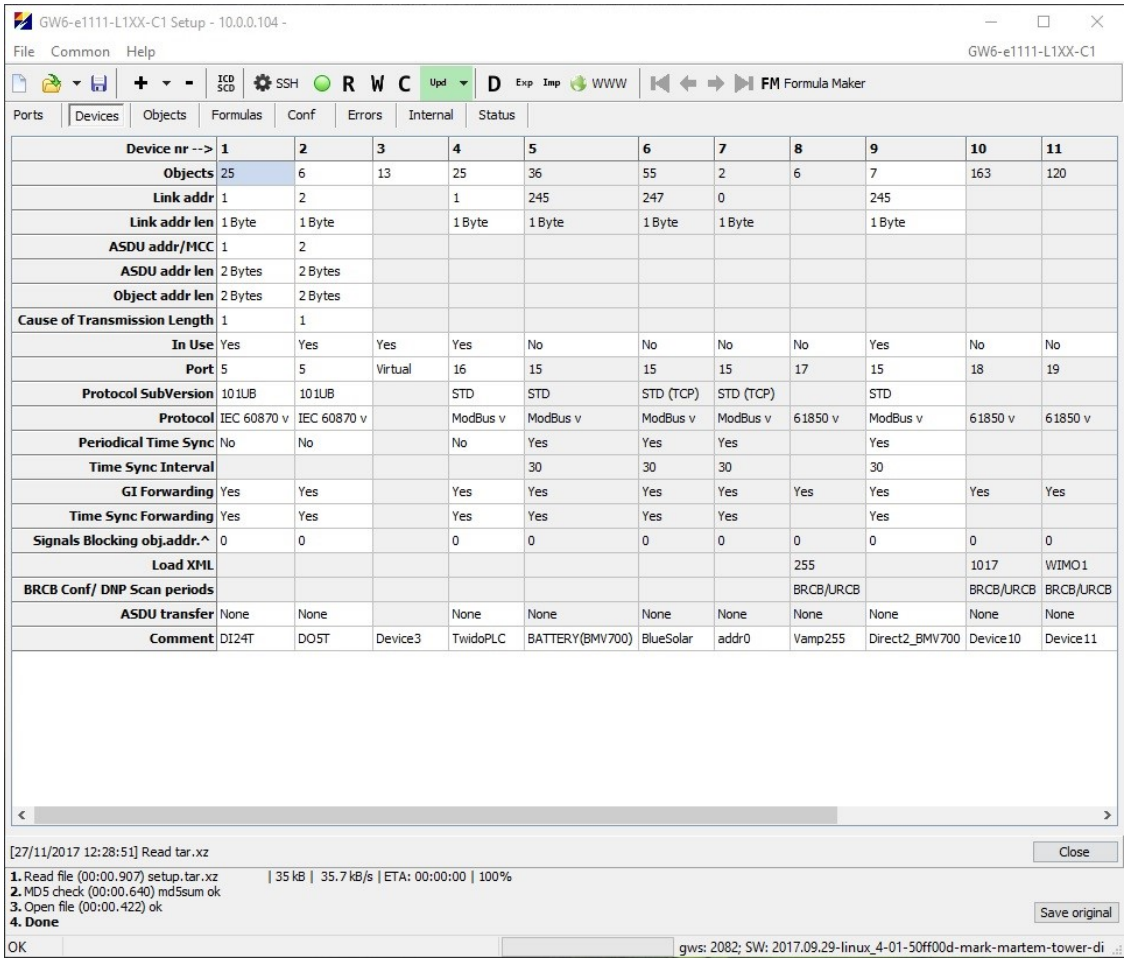
Field	Description
Folder / Path	Allows uploading and serving custom HTML/JS/JSON files via embedded HTTP server. Useful for custom dashboards or visualization.
Size	Displays total size of uploaded custom content.

SSL / HTTPS Settings

Field	Description
Enable SSL	Enables HTTPS encryption for web interface and WebSocket services.
Use device key and self-signed certificate	Uses automatically generated device certificates (no external CA needed).
Cert / Key	Manual upload of SSL certificate and private key if custom CA-signed certificates are used.

5.2.5 Devices Tab Card

The *Devices* tab in Telem GWS provides a detailed overview and configuration interface for all logical devices connected to the Telem device. Each row in the table represents a distinct logical or physical device, and the columns define parameters relevant to communication, addressing, protocol behavior, and synchronization.
Devices may be connected via serial, Ethernet, 1-wire. Device parameters are automatically or manually defined based on protocol selection and port assignment.



Field	Description	Example
Device no.	Unique identifier assigned to each device (auto-generated).	1, 2, 3...
Objects	Total number of communication objects associated with the device (auto-calculated).	13, 25
Link address	Link-layer address of the device, typically used in serial or IEC protocols.	1, 245
ASDU address	Application Service Data Unit (ASDU) address of the device.	1, 247
ASDU address length	Byte length of the ASDU address. Valid values: 1 or 2.	1 Byte, 2 Bytes
Object address length	Byte length of object addresses. Valid values: 1, 2, or 3.	2 Bytes
In use	Indicates if the device is currently active. If No, the row is visually grayed out.	Yes / No

Port	Communication port used for this device. Links to the configured port number in the Ports tab.	2, 5, 9 – Depends on Ports tab card configuration Virtual – Creates a virtual device capable of creating data points meant for SCADA control or internal logic (Formula/Python). See separate chapter.
Protocol SubVersion	Specific variant or version of the protocol, depending on the device type or vendor.	Opens a new window on click. Content depends on set Protocol Parameter under Ports tab card.
Protocol	The protocol in use for the communication. Populated automatically based on the assigned port's protocol.	IEC 60870, Modbus v, 61850 v
Periodical Time Sync	Enables/disables periodic time synchronization from the Telem device to this target.	Yes / No
Time Sync Interval	Time interval between periodic sync operations (unit assumed to be seconds or minutes).	30, 60
GI Forwarding	Enables forwarding of General Interrogation (GI) requests to the device.	Yes / No
Time Sync Forwarding	Forwards received time synchronization from uplink (e.g., SCADA) to this device.	Yes / No
Signals Blocking Object Addr.	Address of a virtual object used to block all outgoing signals from this device. If set, blocks alarm/control updates.	e.g., 255
Load XML	Allows loading an external XML definition file for IEC 61850 IEDs (structure, addresses, objects). This is useful when CID/ICD/SCD document has been	Opens a new window on click. Content depends on set Protocol Parameter under Ports tab card. See separate chapter.
BRCB Conf / DNP Scan Periods	Manual Buffered Report Control Block configuration for IEC 61850 or DNP scanning intervals.	Opens a new window on click. Content depends on set Protocol Parameter under Ports tab card. See separate chapter regarding IEC 61850 BRCB.
ASDU Transfer	Enables direct IEC 60870 data passthrough from lower-level devices to the upper-level communication port without mapping via the Object Tab. Used for data forwarding in multi-RTU configurations	The value must match the upper-level port number (e.g., 6 for Port 6). See separate chapter.
Comment	User-defined description for the device (label, usage notes).	TwidoPLC, Device3, BlueSolar

Adding devices

By clicking on the shortcut icon, a new device with default settings is added. It is also possible to add new devices with a right mouse click which makes the extended control menu to appear.

Add Devices dialog box appears.

Set the **Add Devices** options:

Number of devices to add

Default settings or the device number from where the settings are derived

Copy Objects Also

Click the Add button.

Adding devices from template

User has the possibility to create personal device templates, also some templates are provided by Martem AS.  Using template configuration may save a lot of time while configuring. To create template, user first has to make configuration as needed. Then click on the arrow next to the sign or right click on some Device or Port and **Create Template**. It really does not matter where you click on **Create Template**, you can select desired Port or Device on Template creation form, it defaults to one that you clicked on. When create template is clicked new template will appear in the template list.

Removing Devices

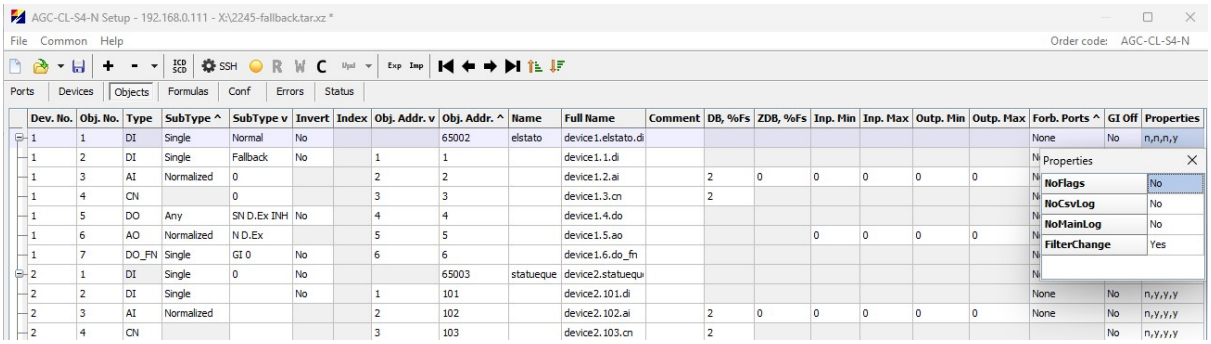
To remove a device, select **Remove Devices** from the extended control menu or click on the shortcut icon. Select the range of the removed devices and click the **Remove** or **Remove All** button. The selected device is also removed after the warning dialog when is clicked.

Clearing Devices

To clear the Device Tab Card, select Clear from the extended control menu. A warning window always appears before removing all devices. Select **Yes** to accept or **No** to cancel the removal operation of the devices.

5.2.6 Objects Tab Card

Objects tab card is used to define all parameters of I/O points. Each device as its own object list.



Dev. No.	Obj. No.	Type	SubType ^	SubType v	Invert	Index	Obj. Addr. v	Obj. Addr. ^	Name	Full Name	Comment	DB, %Fs	ZDB, %Fs	Inp. Min	Inp. Max	Outp. Min	Outp. Max	Forb. Ports ^	GI Off	Properties
1	1	DI	Single	Normal	No			65002	elstato	device1.elstato.di								None	No	n,n,n,y
1	2	DI	Single	Fallback	No		1	1		device1.1.di										
1	3	AI	Normalized	0			2	2		device1.2.ai		2	0	0	0	0	0			
1	4	CN		0			3	3		device1.3.cn		2								
1	5	DO	Any	SN D.Ex INH	No		4	4		device1.4.do										
1	6	AO	Normalized	N D.Ex			5	5		device1.5.ao				0	0	0	0			
1	7	DO_FN	Single	GI 0	No		6	6		device1.6.do_fn										
2	1	DI	Single	0	No			65003	statueque	device2.statueque										
2	2	DI	Single		No		1	101		device2.101.di								None	No	n,y,y,y
2	3	AI	Normalized				2	102		device2.102.ai		2	0	0	0	0	0	None	No	n,y,y,y
2	4	CN					3	103		device2.103.cn		2							No	n,y,y,y

Objects are shown by devices and identified by hierarchical names ─ “Full name” which consist of device, name (in device) and type.

The first object of every device is used as the communication status signal of the device. If its value is “2” then communication with this device is broken. The object (first object) of communication status signal is not counted in the **Objects** row of the **Devices Tab Card.**

Columns:

Type – Object’s type: digital input (DI), analog input (AI), counter (CN), digital output (DO), analog output (AO), digital output with function (DO_FN)

Sub Type^ – Uplink Formats

Object Type	Subtype ^	Explanation
DI	Single	IEC 870: Single-bit digital input (e.g. open/closed contact)
	Double	IEC 870: Double-bit input for states with intermediate/transition values
	Object diagnostics	Switches state to ON if related data point has Not Topical or Invalid flags set. Relation is defined by assigning another object Obj.Addr.^ in this objects Obj.Addr.v Only in Virtual device Only with special firmware
	Formula diagnostics	Switches state to ON if any formula result has Not Topical or Invalid flags set Only in Virtual device
DO	Any	IEC 870: Accept any type DO
	NTtime	IEC 870: Accept only DO without time tag
	WTime	IEC 870: Accept only DO with time tag
AI	Normalized	IEC 870: Value scaled to 0–1 or per-unit format
	Floating Point	IEC 870: IEEE 754 floating-point value
	Step Position	IEC 870: Discrete position with step levels
	Scaled	IEC 870: Scaled integer values with defined range
	Bitstring w. T	IEC 870: Bitstring values with time tagging Only in Virtual device. Currently only used for VHPReady enabled projects
AO	Normalized	IEC 870: Normalized output value in 0–1 format
	Scaled	IEC 870: Scaled integer output for direct application
	Floating Point	IEC 870: Floating-point output value
	Normalized w.T.	IEC 870: Normalized output value in 0–1 format with time tag
	Scaled w.T.	IEC 870: Scaled integer output for direct application with time tag
	Floating Point w. T.	IEC 870: Floating-point output value with time tag
	Any	IEC 870: Accept any type
CN	-	Counters do not define specific subtypes for uplink
DO_FN	(See section below)	Handled separately: GI/Reset parameters and data format options

Sub Type v – Object's subtype for downlink.

Object Type	Subtype	Explanation
DI	Normal	Standard digital input behavior
	Fallback	Falls back to OFF automatically
	battery-bad	Battery failure status Only in Event Generator
	battery-empty	Battery fully depleted Only in Event Generator
	battery-tester-status	Status from battery test function Only in Event Generator
	battery-testing	Indicates battery test is in progress

		Only in Event Generator
	gps-invalid	GPS signal invalid or unavailable Only in Event Generator
	missing-power	Indicates loss of power input Only in Event Generator
	ntp-invalid	Invalid time received from NTP source Only in Event Generator
	power1	Only in Event Generator
	power2	Only in Event Generator
	AI-bit	Links a bit from analog input to digital logic Only in Modbus
DO	Single Direct Execute	IEC 870: C_SC_XX_1
	Single Select Execute	IEC 870: C_SC_XX_1
	Double Direct Execute	
	Double Select Execute	
	Regulating Step Direct Execute	IEC 870: C_RC_XX_1
	Regulating Step Select Execute	
	Inherited	IEC 870: Uses behavior from parent or default object type
	No additional definition	IEC 870: Default execution, no extended behavior configured
	Short pulse duration	IEC 870: Generates short-duration output pulse
	Long pulse duration	IEC 870: Generates long-duration output pulse
	Persistent Output	IEC 870: Output remains latched until overridden
AI	cps-api-ai	Energy price value from Central Price Server Only in Event Generator
	Int16 (16-bit signed integer)	Signed 16-bit integer format Only in Modbus
	Floating Point (legacy)	Same as big endian but reordered as 2,3,0,1 if Modbus device subtype is 'Integra Inverted'. word[0]=2,3; word[1]=0,1. Byte index: 0 = low Only in Modbus
	32-Bit Integer word swapped	Only in Modbus
	Floating Point (Big Endian)	Standard Big-Endian float encoding Only in Modbus
	Floating Point (Big Endian - byte swapped)	Big Endian float with byte-level swap reordered as 1,0,3,2, where index is byte order number. word[0]=1,0; word[1]=3,2. Byte index: 0=low Only in Modbus
	Floating Point (Little Endian)	Standard Little-Endian float encoding Only in Modbus
	Floating Point (Little Endian - byte swapped)	Little Endian float with byte-level swap reordered as 1,0,3,2, where index is byte order number. word[0]=1,0; word[1]=3,2. Byte index: 0=low Only in Modbus
	uint16 (16-bit	Only in Modbus

	unsigned integer)	
	64-Bit Integer	Only in Modbus
	FP64 (Big Endian)	Big Endian 64-bit float Only in Modbus
	FP64 (Big Endian - Byte Swapped)	Big Endian 64-bit float with byte swap 1,0,3,2,5,4,7,6 where index is byte order number. word[0]=1,0; word[1]=3,2 etc. Byte index: 0=low Only in Modbus
	FP64 (Little Endian)	Little Endian 64-bit float Only in Modbus
	FP64 (Little Endian - Byte Swapped)	Little Endian 64-bit float with byte swap 1,0,3,2,5,4,7,6 where index is byte order number. word[0]=1,0; word[1]=3,2 etc. Byte index: 0=low Only in Modbus
	32-Bit Integer	Only in Modbus
	UInt32	Unsigned 32-bit integer Only in Modbus
	UInt32 (word swapped)	Unsigned 32-bit integer with word swap 1,0,3,2,5,4,7,6 where index is byte order number. word[0]=1,0; word[1]=3,2. Byte index: 0=low Only in Modbus
	default	Default analog input mapping Only in Virtual device
	temperature sensor	Used for temperature input channel from 1-wire Only in Virtual device
	humidity sensor	Used for humidity input channel from 1-wire Only in Virtual device
	light sensor	Used for light intensity input channel 1-wire Only in Virtual device
	voltage	Voltage measurement input Only in Virtual device
	current	Current measurement input Only in Virtual device
	VHPReady_vAO1	VHPReady-specific analog output 1 reference Only in Virtual device
	VHPReady_vAO2	VHPReady-specific analog output 2 reference Only in Virtual device
	VHPReady_vAI_response	Response parameter from VHPReady control Only in Virtual device
	VHPReady_vAI_t1	Time parameter t1 Only in Virtual device
	VHPReady_vAI_t2	Time parameter t2 Only in Virtual device
	VHPReady_vAI_value	Setpoint value Only in Virtual device
AO	Direct Execute	IEC 870: Value written immediately without selection
	Select Execute	IEC 870: Value written with select-exec
	Normalized	IEC 870: Value sent as normalized per-unit (0 to 1 range)
	Scaled	IEC 870: Scaled integer mapped to defined engineering range
	Floating point	IEC 870: IEEE 754 floating-point value

	Int32	Signed 32-bit integer value Only in Modbus
	UInt32	Unsigned 32-bit integer value Only in Modbus
	Int32 (word swapped)	Signed 32-bit integer with word order reversed Only in Modbus
	UInt32 (word swapped)	Unsigned 32-bit integer with word order reversed Only in Modbus
	Floating Point (Big Endian)	Standard Big Endian float encoding Only in Modbus
	Floating Point (Big Endian – byte swapped)	Big Endian float with byte-level swap Only in Modbus
	Floating Point (Little Endian)	Standard Little Endian float encoding Only in Modbus
	Floating Point (Little Endian – byte swapped)	Little Endian float with byte-level swap Only in Modbus
CN	minutes-from-year-begin	Counts minutes elapsed since start of year Only in Event Generator
	seconds-from-sunrise	Seconds elapsed since sunrise Only in Event Generator
	seconds-from-sunset	Seconds elapsed since sunset Only in Event Generator
	seconds-since-day-begin	Seconds since start of current day Only in Event Generator
	seconds-since-day-begin-utc	Seconds since day start (UTC time) Only in Event Generator
	seconds-to-sunrise	Countdown seconds to next sunrise Only in Event Generator
	seconds-to-sunset	Countdown seconds to next sunset Only in Event Generator
DO_FN	GI Parameter 0	Global GI group (default)
	GI Parameter 1…15	User-assigned GI group (1–15)
	GI Parameter > 15	Counter GI with param 5
	Reset process 1	Reset device or signal state
	Reset process 2	Reset and clear associated buffers or memory

Column Name	Description
Dev. No.	Device number (logical index) this object belongs to
Obj. No.	Object number within the device's object list
Type	Object type: DI, DO, AI, AO, CN DO_FN relevant for IEC 60870-5-101 Balanced, Unbalanced and IEC 60870-5-104 ST, TX relevant for OPC UA
SubType^	Uplink data format (see Sub Type^ table)
SubType v	Downlink behavior or data format (see Sub Type v table)

Invert	If set to "Yes", the object's logical value is inverted
Index	Index on IEC 60870-5-103 protocol; It indicates the order number of the object in message types 3 and 9 of analog measurements. In Modbus it is used only if DI object type is “AI-bit”. It indicates which bit is retrieved as Boolean state value.
Info no	Information number on the IEC 60870-5-103
Fn.code	Function code on the IEC 60870-5-103
Obj. Addr. v	Downlink address (IEC101, Modbus etc.).
61850 v	61850 address
Obj. Addr. ^	Uplink address. Can differ per SCADA system; allows duplicate downlink and distinct uplink configs
Name	Object tag name (free-text, used internally in Formulas)
Full Name	Hierarchical name: device.name.object (e.g. device2.101.ai)
Comment	User-supplied description or device comment
DB %Fs	Deadband as % of full scale. If value change is below threshold, it won't be transmitted
ZDB, %Fs	Zero deadband. Below this % change, values are treated as zero
Inp. Min	Minimum raw input value before scaling
Inp. Max	Maximum raw input value before scaling
Outp. Min	Minimum raw output value before scaling
Outp. Max	Maximum raw output value before scaling
Forb. Ports^	Uplink ports where object transmission is blocked. Double-click to configure allowed ports
On Ev. No; Off Ev. No	Corresponding event number used in SPA-bus
Ch. No	Channel no. for SPA-bus communication protocol
GI Off	Disables General Interrogation for this object if set to "Yes"
Properties	Additional runtime behavior, encoded as `NoFlags, NoCsvLog, NoMainLog, FilterChange`

Expanded "Properties" Field Definitions

Property	Explanation
NoFlags	Removes 'Invalid', 'Not Topical', and 'Overflow' flags from uplink status
NoCsvLog	Prevents value changes from being logged to events.csv
NoMainLog	Prevents value changes from being logged to console.log
FilterChange	No shall allow same value/flags events propagation to upper channels and formulas. Default: Yes

Adding Objects

By clicking on the „+“ button, a new object with default settings is added. Objects can also be added with a right click on the device tab card. Extended control menu appears where user can choose number of objects to add, into which device objects will be added, where in the list the object will be located, user can also choose if new object will be with default setup or copy some other object.

Removing Objects

To remove an object, click the „-“ button. Objects can also be removed with a right click on the device tab card. Window appears where user can choose which objects to remove.

Hints

• Repeated object addresses are shown on yellow background.

• To transfer the same measurement object to separate SCADA using different uplink address (separate cross-reference for separate SCADA):

1. Create a copy of an object and give a different uplink address “Object. Addr ^” to this copied object.
2. Exclude the original object from the SCADA that it is not supposed to reach. Use the “Forb. Ports ^” field.
3. Exclude the copied object from the second SCADA that it is not supposed to reach.

5.2.7 Measurement Objects Scaling

This description is valid from firmware ver. 2015-11-05.

Input value is converted to Output value using the Inp. Min, Inp. Max and Outp. Min, Outp. Max parameter pairs. The input range is linearly transformed to output range.

Attention

- Usually Input and output value pairs have to be both bipolar or both unipolar, but there are exceptions, usually on Modbus protocol variations.
- On Normalized values of IEC 60870-5 protocols the Min.and Max parameters can be left zeros, then the deault values -1 and +1 are used
- If all 4 parameters are left zero, then no conversion is made

Relationship with DeadBand

The Deadband is calculated as percentage from the positive side of output range.

Thus on Float and Scaled values the Outp. Min and Outp. Max parameters are usually needed even if no conversion is made

On Normalized values the default positive range is 0 ...1 and the parameters can be left zeros.

Examples:

1) IEC 60870-5 protocol, Normalized -> Normalized

Input value	Input Min	Input Max	Output Min	Output Max	Output value
0,5 (16384)	0	0	0	0	0,5 (16384)
0,5 (16384)	-1	1	-1	1	0,5 (16384)
Don't use:					
0,5 (16384)	0	0	-32767	32767	536854528

2) IEC 60870-5 protocol, Normalized -> Float

Input value	Input Min	Input Max	Output Min	Output Max	Output value
0,5 (16384)	0	0	-5000	5000	2500
0,5 (16384)	0	1	0	5000	2500
Don't use:					
0,5 (16384)	0	0	0	5000	3750

3) IEC 60870-5 protocol, Float -> Normalized

Input value	Input Min	Input Max	Output Min	Output Max	Output value
2500	-5000	5000	0	0	0,5 (16384)
2500	0	5000	0	1	0,5 (16384)
Don't use:					
2500	0	5000	0	0	0
500	0	5000	0	0	-0,8 (-26214)

4) Any protocol, Float -> Float

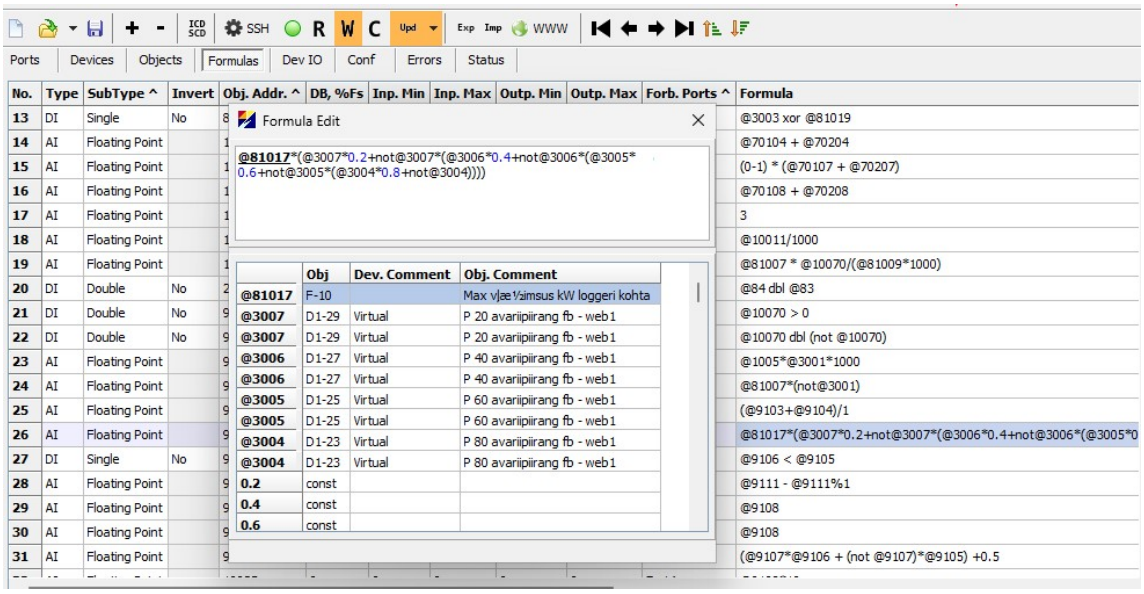
Input value	Input Min	Input Max	Output Min	Output Max	Output value
2500	-5000	5000	-5000	5000	2500

5) Modbus protocol, Int16 -> Int16 or Int16 -> Float

Input value	Input Min	Input Max	Output Min	Output Max	Output value
1000	-10000	10000	-5000	5000	500
1000	0	10000	0	5000	500
1000	0	0	0	0	1000
If zero is shifted:					
1000	0	10000	-5000	5000	-4000
Don't use:					
300	0	0	-5000	5000	1500000

5.2.8 Formulas Tab Card

Logical operations are configured on Formula tab card. Logic is described in the form of formulas list (similar to ladder logic) which may be combined with Python language functions.



Columns:

Type, Sub Type , Invert, Object Adr ^, DB %Fs, Inp. Min, Inp. Max, Outp. Min, Outp. Max, Forb.Ports - as in **Objects Tab Card**

Formula: Formula expression

Comment: Comment of the formula

DO/AO addr.: Address of the object controlled by formula. The control operation is made on change of the formula value, except on "if" operation when the control operation is made also on every condition change despite the result changes or not.

Execution count: The maximum number of control operations executed until control confirmation is received from device.

Delay – Delay in seconds, delay applies to on and off state

Forb. DO – The number of DO, which control is forbidden with the result of this formula

Enable First Control: If set to Yes, then control described in DO/AO will take place right after Telem device restart on initial calculation.

Formulas can be created between the values of analog and/or digital objects.

Referencing to object values

To use the measurement object in the formula, insert an @ sign together with the object's **Full name** or **Obj. addr. up.**

Example:

- `@dev1.var1.DI` points to the digital type object (values "0" / "1").
- `@101` points to the object with an address to uplink 101.

Brackets

Brackets can be used in formulas to determine the priority of operations.

Example: `sqrt(@dev1.v1.AI / 2 + @dev1.v2.AI)`

Oper.	Obj. type	Description	Sample	Priority*
and	DI	Logical conjunction	@dev1.dv1.DI and @dev1.dv2.DI	5
or	DI	Logical disjunction	@201or@202	6
xor	DI	Exclusive disjunction	@201xor@202	6
not	DI	Logical negation	not@ dev1.dv1.DI	0
dbl	DI	Converts 2 single digital inputs into a double signal	@dev1.closed.DI dbl @ dev1.open.DI where @dev1.closed.DI – ON state signal @dev1.open.DI – OFF state signal	7
if	DI	*"if X then Y"* or *"if X then Y else Z"* sentence	if (@dev1.v8.AI : @ dev2.v1.AI : @ dev3.v1.AI) {i.e. if @101then @201 else @301}	0
+	AI/CN	Addition	@dev1.v1.AI + 3,2	3
-	AI/CN	Subtraction	@dev1.v1.AI – @dev1.v2.AI	3
*****	AI/CN	Multiplication	@dev1.v1.AI * @dev2.dv2.DI	2
/	AI/CN	Division	@dev1.v1.AI / 2	2
%	AI/CN	Remainder of the division	@dev1.v1.AI % 2	2
^	AI/CN	Exponentiation	@dev1.v1.AI ^2	1
<, >, =	AI/CN	Greater, Less, Equal	@dev1.v1.AI <= @dev1.v2.AI	4
sqr	AI/CN	Square	sqr @dev1.v1.AI	0
sqrt	AI/CN	Square route	sqrt(@dev1.v1.AI *10)	0
sin	AI/CN		sin@dev1.v1.AI	0
cos	AI/CN		cos@dev1.v1.AI	0
tan	AI/CN		tan@dev1.v1.AI	0
arcsin	AI/CN		arcsin@dev1.v1.AI	0
arccos	AI/CN		arccos@dev1.v1.AI	0
arctan	AI/CN		arctan@dev1.v1.AI	0
bwand	AI/CN	To INT and bitwise and	@dev1.v1.AI bwand dev1.v2.AI	X
bwor	AI/CN	To INT and bitwise or	@dev1.v1.AI bwor dev1.v2.AI	X
bwxor	AI/CN	To INT and bitwise xor	@dev1.v1.AI bwxor dev1.v2.AI	X

*Priority determines the order of operations in the formula (highest priority is 0)

Formula Management

Formula rows can be added and removed by clicking the „+“ and “-” buttons or more conveniently by using the extended control menu like in the Object Tab Card. It appears with a right mouse click on the Formula Tab Card.

- To add a Formula, select **Add Formulas**,
- To remove a Formula, select **Remove Formula**
- and to clear all formulas, select **Clear.**
- All analog values should be scaled before making calculations; therefore, it is very important to fill the **Inp. Min, Inp. Max, Outp. Min, Outp. Max** fields with Normalized values that are used in calculations.
- AI values can be comma separated values, while CN have only full-scale values. (AI=1,7 while CN=2)
- After editing the formula, the program automatically validates this formula and shows the result in the status area. If the formula is incorrect, the background of the edited formula is changed to pink and an error message is displayed in the status area. **This formula will not be written to the device nor will it be saved.**
- The formulas of DI type of objects can contain AI values and floating-point constants. If the result of the formula is greater than 0, the value of the DI object is “1”; if the result of the formula is less than or equal to 0, the value of the DI object is “0”.
- < or > statement: if the statement is true, the value of the DI object is 1; if the statement is false, the value of the DI object is 0.

Editing formula expression

Formulas can be edited form the formula string directly. In the formulas tab card, but it is more convenient to right click on the formula expression and choose edit formula then more information about the formula is visible.

Python language defined functions (since GWS 6.1.0.2242)

Users can create their own functions using Python language.

Usage of Python created function in formula: `py_user_func1 (param1; param2; …)`
All python function names must begin with `**py_**`.

Only one Python function can be used inside one formula and nothing else. E.g. **this is not allowed** as formula code:

```
@dev1.var1.AI + sin(@dev1.var2.AI + @dev1.var3.AI) +
 py_user_func1(@dev2.var4.AI; @dev3.var5.AI; @dev4.var6.AI)
```

User can define `py_user_func1(@dev2.var4.AI; @dev3.var5.AI; @dev4.var6.AI)` as a separate formula object with address, e.g. 1122, and use it in a formula that adds it to other logic:

```
@dev1.var1.AI + sin(@dev1.var2.AI + @dev1.var3.AI) + @1122
```

If some formula has a function that begins with `**py_**` GWS creates a file called **functions.py** in Conf Tab. The real Python function can be defined there. It must be with the same name starting with `**py_**`.

Python usage Nr.1: Get intermediate value for Double DI (M_DP_NA_1)

Historically Telem device alters the value of incoming Double DI (IEC60870 M_DP_XX_1) if certain conditions are met:

If input value is either 0 or 3.

In this case the value is discarded and INValid flag is set. This results in data loss of the state real intermediate value.

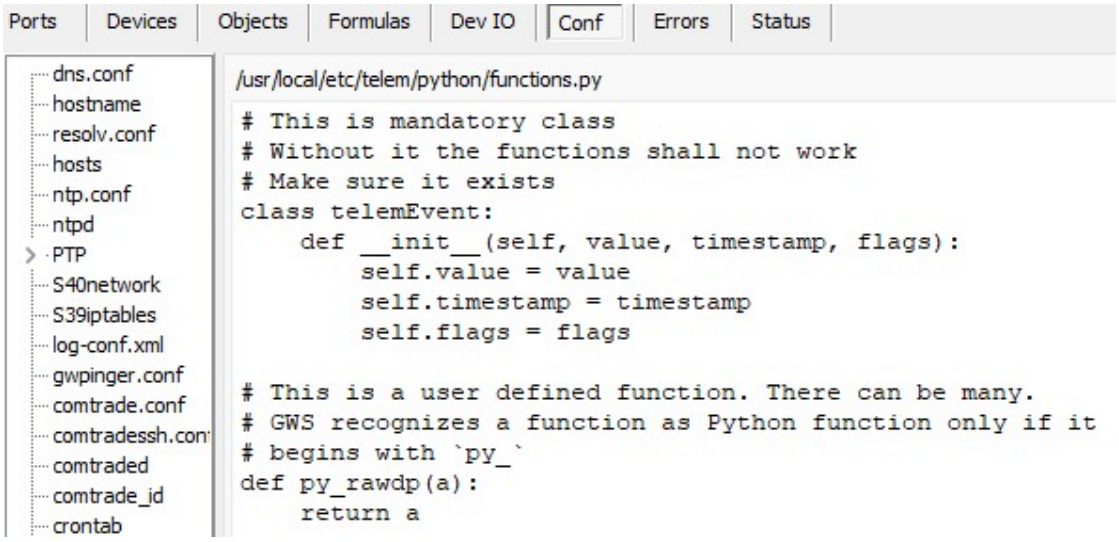
Python allows to extract the raw value without RTU processing:

1	12	DI	Double	Normal	No		1111	2222
1	13	DO	Any	DB D.Ex	No		2222	1111

The screenshot above illustrates the virtual DI/DO pairs used in this example conf. Object Tab

AI	Floating Point		102	0	0	0	0	0	None	py_rawdp(@2222)

The screenshot above is Formula Tab



Simple Python function definition with same number of arguments. First create the `**py_...**` function in formula and then functions.py shall appear in the list of Conf tab.

Code in picture:

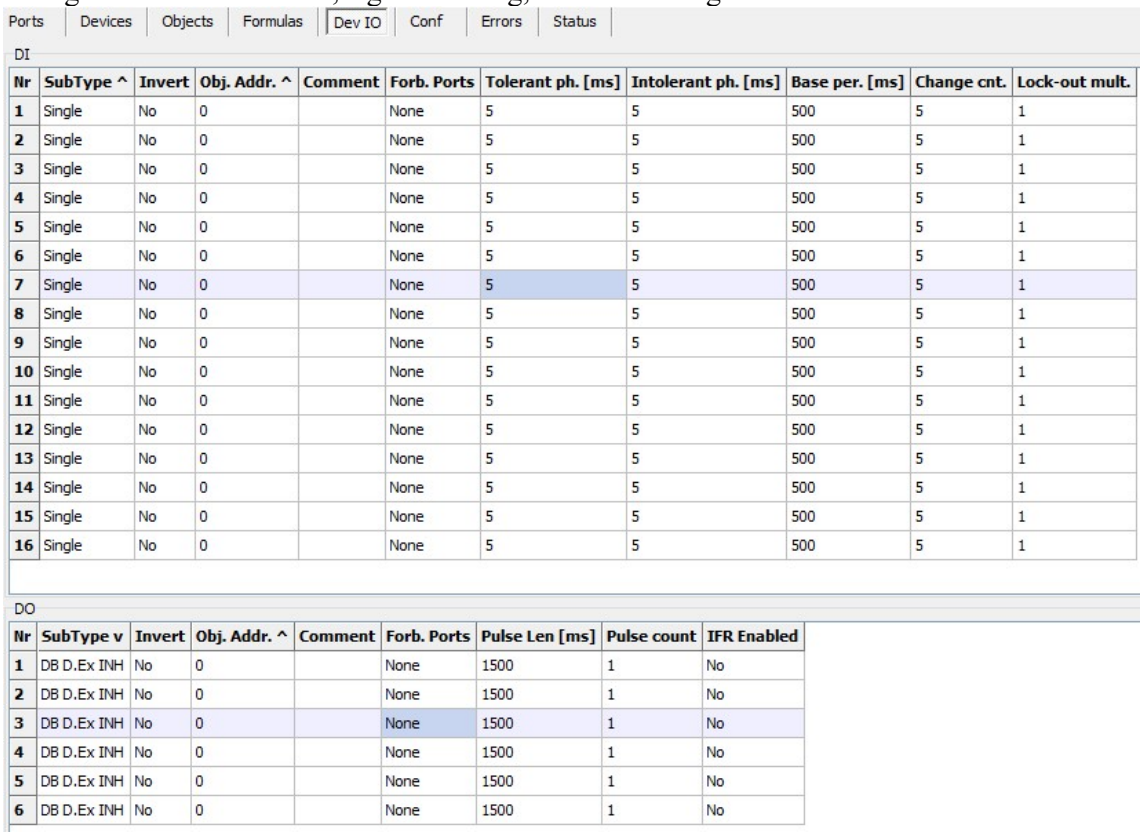
```
# This is mandatory class
# Without it the functions shall not work
# Make sure it exists
class telemEvent:
    def __init__(self, value, timestamp, flags):
        self.value = value
        self.timestamp = timestamp
        self.flags = flags

# This is a user defined function. There can be many.
# GWS recognizes a function as Python function only if it
# begins with `py_`
def py_rawdp(a):
    return a
```

Example conf: 2245-python-05052025.tar.xz

5.2.9 Dev IO (IO Board)

The **Dev IO tab** is visible only if the connected device (or selected order code, e.g. `AGC-CL-S4-DD`) includes hardware support for physical digital inputs and outputs. It is used to configure runtime behavior, signal filtering, and contact logic for both DI and DO terminals.



Digital Input (DI) Parameters

Field	Description
Nr	Internal index of the DI terminal
SubType	Contact logic: `Single` or `Double`. In `Double`, the current and next DI channels form a logical pair.
Invert	If `Yes`, logical value is inverted (e.g. high becomes low)
Obj. Addr.^	Uplink object address for SCADA binding
Comment	Optional description field
Forb. Ports	Communication ports to which this signal is not transmitted (blacklist)
Tolerant ph. [ms]	Debounce: Ignore toggles within this duration (default: 5 ms)
Intolerant ph. [ms]	Debounce hold: Must stay stable this long before accepting new value

Base per. [ms]	Chatter filter window duration for change counting
Change cnt.	Allowed number of changes inside one base period
Lock-out mult.	Multiplier of `Base per.` during which no further events are accepted after chatter is detected

Digital Output (DO) Parameters

Field	Description
Nr	Output terminal index
SubType	`Single`, `Double`, `Direct Execute`, `Select & Execute`
Invert	If `Yes`, reverses output logic (e.g. pulse low instead of high)
Obj. Addr.^	Uplink object address (used for mapping DO control)
Comment	Free-form annotation
Forb. Ports	Forbidden uplink transmission ports
Pulse Len [ms]	Length of output pulse in milliseconds
Pulse Count	Number of times pulse should repeat
IFR Enabled	`Yes` to enable interlock fault reset output logic

Notes:

- Chatter filtering on DI prevents rapid toggling from false detections (e.g. contact bounce).
- Debouncing and chatter filtering operate in parallel.
- `IFR Enabled` is used in alarm logic configurations to reset fault latches via DO contact.
- DO control commands can use IEC 60870-5-104 Select-Before-Operate (SBO) or direct execute patterns.

The Dev IO tab allows no dynamic reordering—channel assignments are fixed by physical terminal layout.

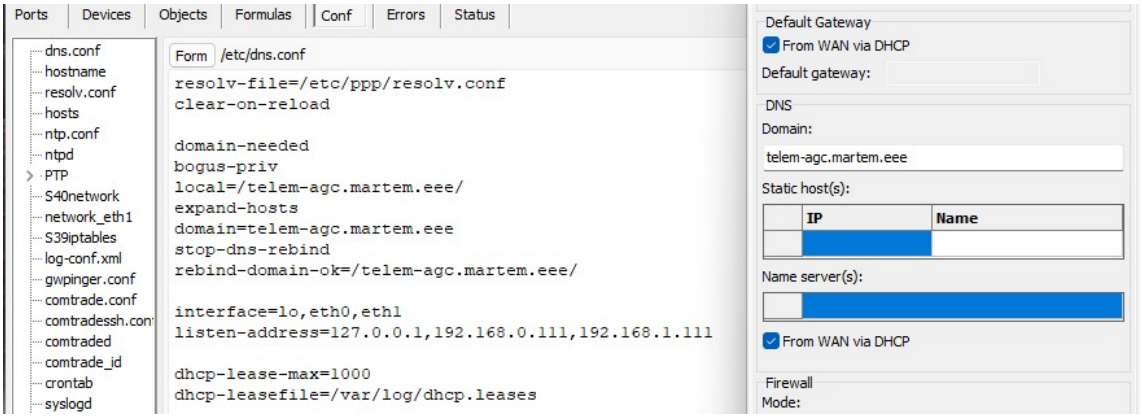
5.2.10 Conf tab card

This tab contains a list of configuration text files that are normally generated by Telem-GWS automatically when user changes parameters via the GUI. Files are displayed in the left pane; selecting a file opens its current content in editable form on the right.

This implies that any manual changes in this tab are overwritten by the program if the user makes changes via the GUI.

The contents inside this tab are familiar to technical **Linux users**.

dns.conf



Purpose: */etc/dns.conf* – file contains host Domain Name System (DNS) settings configuration information

Field	Source (GUI)	Description
resolv-file=/etc/ppp/resolv.conf	From WAN via DHCP	Points to /etc/resolv.conf if the GUI tick box is unchecked
clear-on-reload	Implicit	Clears DNS state on config reload
domain-needed	Fixed	DNS queries must include domain suffix
bogus-priv	Fixed	Filters out RFC1918 responses from upstream
local=/telem-agc.martem.eee/	Domain field	Defines local DNS domain (reverse path)
expand-hosts	Enabled if static host list used	Expands hostnames to FQDNs using `domain`
domain=telem-agc.martem.eee	Domain field	Sets default search domain
stop-dns-rebind	Fixed	Prevents DNS rebind attacks
rebind-domain-ok=/telem-agc.martem.eee/	Domain field	Allows rebind from internal domain
interface=lo,eth0,eth1	Based on interfaces	Interfaces DNS listens on
listen-address=127.0.0.1,192.168.0.111,...	GUI IPs	Local IPs bound for DNS listen socket
dhcp-lease-max=1000	Max lease count	Max DHCP leases allowed
dhcp-leasefile=/var/log/dhcp.leases	Fixed	Location of active DHCP leases file

GUI Behavior Notes:

- **Static host(s)**: Maps IP-to-name pairs written to `hosts` or `dnsmasq` entries.

- **Name server(s)**: Populates `server=` directives (not shown in `dns.conf`, applied runtime).
- **From WAN via DHCP**: Auto-fills domain and DNS server list from upstream DHCP reply.

hostname

Purpose: */etc/hostname* – Defines the system hostname used during boot and by network services.

Notes for Linux Users:

Applied at boot via init scripts or `systemd-hostnamed` depending on system generation.

Propagates to:

`uname -n`

DHCP client hostname field

Local resolver context

Hostname must be a valid DNS-compatible label: no spaces, underscores, or special characters. Recommended: lowercase, hyphen-separated.

If the GUI interface (as shown) is used, editing the file manually is not persistent.

Split access toggle is unrelated to hostname logic — part of WAN routing/firewall settings.

Use consistent device naming (e.g., `telem-agc`, `gw6e-core`) to maintain traceability in DHCP leases, log output, and remote management tools.

resolv.conf

Purpose: */etc/resolv.conf* – the DNS servers to be used are indicated in the file, one per line, with the nameserver keyword preceding an IP address, as in the following example:

```
nameserver 127.0.0.1
nameserver 212.27.32.177
nameserver 8.8.8.8
```

DNS (Domain Name Service) is a distributed and hierarchal service mapping names to IP addresses, and vice-versa.

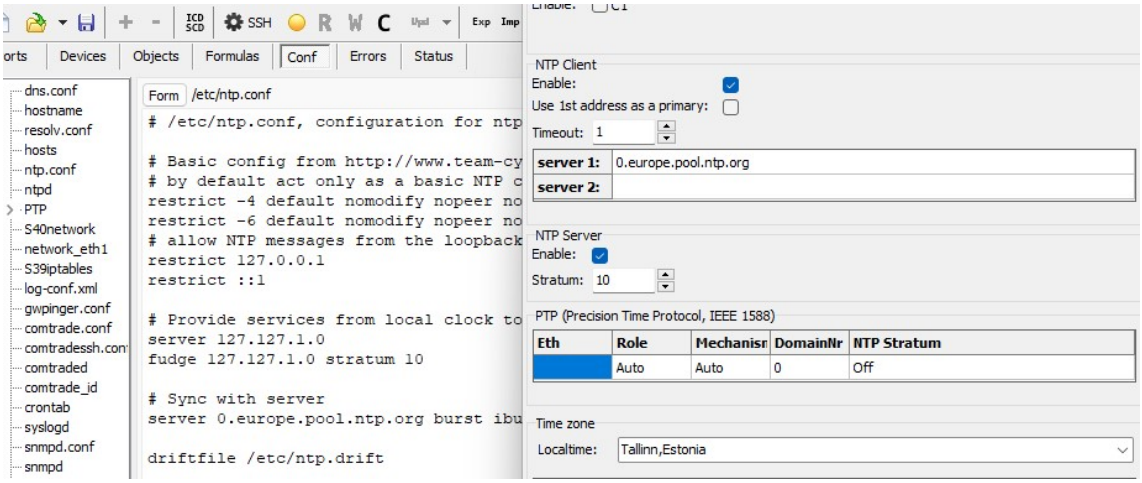
GWS changes it at "TCP/IP Settings" "Name servers" table. In addition, its content can be replaced by modem scripts, if modem is enabled.

hosts

Purpose: /etc/hosts – this file is a simple text file that associates IP addresses with hostnames, one line per IP address. For each host a single line should be present with the following information: IP_address canonical_hostname [aliases...] Fields of the entry are separated by any number of blanks and/or tab characters. Text from a "#" character until the end of the line is a comment, and is ignored. Host names may contain only alphanumeric characters, minus signs ("-"), and periods (".). They must begin with an alphabetic character and end with an alphanumeric character. Optional aliases provide for name changes, alternate spellings, shorter hostnames, or generic hostnames (for example, localhost). For additional information, use this source: http://linux.die.net/man/5/hosts

ntp.conf

Purpose: */etc/ntp.conf* – Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packetswitched, variable-latency data networks. User have rights to change time server names or servers IP-s. NTP provides Coordinated Universal Time (UTC) including scheduled leap second adjustments. No information about time zones or daylight saving time is transmitted; this information is outside its scope and must be obtained separately.



Parameter	Source/Mapping	Description
restrict -4 default nomodify nopeer noquery notrap	Static	Deny all IPv4 external control/query except defined servers
restrict -6 default nomodify nopeer noquery notrap	Static	Same as above for IPv6
restrict 127.0.0.1/::1	Static	Allow local access

server 127.127.1.0	GUI NTP Server (Enable)	Uses internal clock as stratum fallback
fudge 127.127.1.0 stratum 10	GUI NTP Server (Stratum)	Marks local source as fallback (low priority)
server 0.europe.pool.ntp.org burst iburst	GUI NTP Client (Server 1)	Primary external time source
driftfile /etc/ntp.drift	Static	Tracks oscillator drift for better long-term accuracy

ntpd

Purpose: */etc/default/ntpd* – The Network Time Protocol daemon is an operating system **daemon** program that maintains the **system time** in synchronization with time servers using the **Network Time Protocol** (NTP).

This file is not native Linux NTP daemon config file. It is used by Telem device internal wrapper applications to set up ntpd.

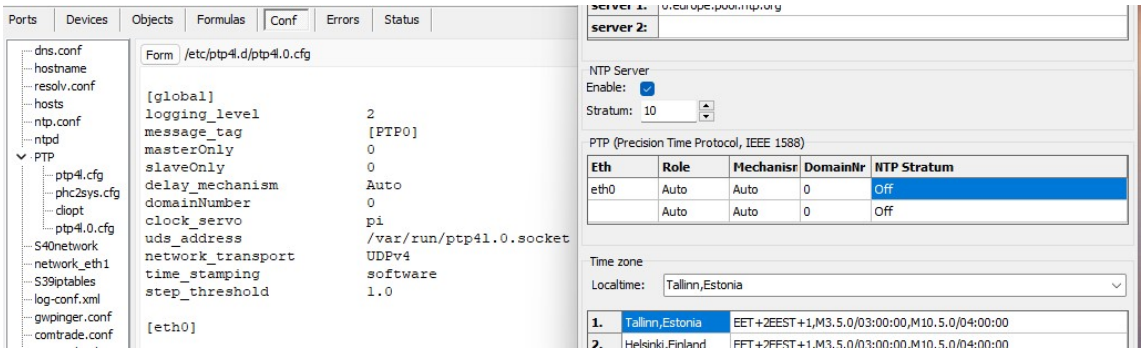
PTP

Configuration for IEEE 1588-2008 (PTPv2) time synchronization using `ptp4l`

Ptp4l.cfg

Phc2sys.cfg

cliopt



Parameter	Value (Example)	Description
logging_level	2	Verbosity level of log output (0 = none, 6 = debug)
message_tag	[PTP0]	Log message prefix (helps distinguish multiple PTP instances)
masterOnly	0	Whether this device operates only as PTP master (0 = allow slave mode)
slaveOnly	0	Whether this device is restricted to slave mode (0 = can be master)
delay_mechanism	Auto	Mode for path delay measurement (Auto, E2E, P2P)

domainNumber	0	PTP domain number; isolates sync trees logically
clock_servo	pi	Algorithm used to adjust clock (e.g. pi, linreg)
uds_address	/var/run/ptp4l.0.socket	Unix socket path for ptp4l instance
network_transport	UDPv4	Transport mode (typically UDPv4)
time_stamping	software	Timestamping method (hardware/software)
step_threshold	1.0	Max offset (in seconds) for which gradual time correction is applied

S40network
Purpose: */etc/init.d/S40network* – script will configure network interfaces, VLAN's and routes

This is a "common bash script" that is used during system init to configure network. It is not a common native Linux env config file.

Acts as a replacement for `/etc/network/interfaces` or `systemd-networkd` in embedded environments.

network_eth1 and network_eth2
Purpose: */etc/init.d/network_eth1* and */etc/init.d/network_eth2* – script will configure network interfaces, VLAN's and routes

S39iptables
Purpose: */etc/init.d/S39iptables* – script will configure network interfaces, VLAN's and routes

PRO TIP: to quickly turn of firewall during Telem device operation without rewriting the configuration and having to wait login as root user and execute:
`/etc/init.d/S39iptables stop`

To start the firewall:
`/etc/init.d/S39iptables start`

Beware of potential issues if working remotely with Telem device and using **Manual** firewall configuration and the remote connection relies on some post/pre forwarding rules in this script. You may lock yourself out by stopping it.

log-conf.xml
Purpose: /usr/*local/etc/telem/log-conf.xml* – xml-file, which contains logging information for the main RTU program. It determines the amount of logs in
`/var/log/telem/console.log`

```
/var/log/telem/console.X.log
/var/log/telem/events.csv
/var/log/telem/events.X.csv
/var/log/telem/error.log
```

By default it is empty and not overwritten by Telem-GWS GUI in any way. In order to enable most verbose RTU, copy the following text from appendix A:

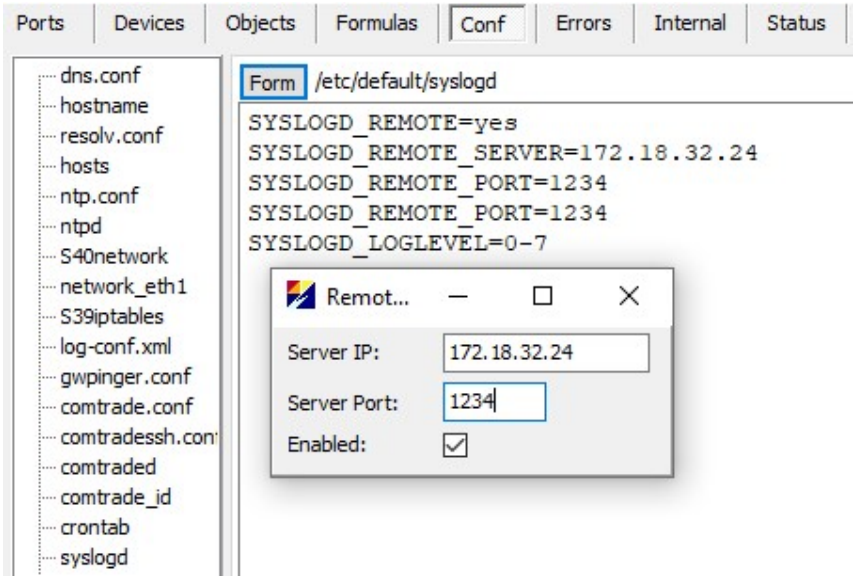
Any custom modifications that introduce XML errors and unknown XML elements, attributes and values may result in no logging of RTU application within the device. Normal operation for SCADA shall remain unchanged.

Custom modification to log file sizes and rotation cycles may result in:

1. Memory depletion
2. Inability to obtain GetLogs, because of service timeouts

gwpinger.conf
comtrade.conf
comtradessh.conf
comtraded
comtrade_id
crontab

syslogd
Purpose: */etc/default/syslogd* - file, which contains cumulative data of devices connections to the other devices



snmpd.conf
update.conf
telem-gps.conf

TZ
Purpose: */etc/TZ* – to set a time zone. Example:
echo "CET-1CEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00" > /etc/TZ
NOTE: This sets the time zone for CET/CEST (Central European Time UTC+1 / Central European Summer Time UTC+2) and the start (5th week of March at 02:00) and end times (5th week of October at 03:00) of DST (Daylight Saving Time).
Time zone settings for Tallinn, Estonia: EET-2EEST-3,M3.5.0/03:00:00,M10.5.0/04:00:00

sim1_chat and sim2_chat (old)
Purpose: */etc/ppp/peers/sim1_chat* – chat scripts are strings of text used to send commands for modem dialing, logging in to remote systems, and initializing asynchronous devices connected to an asynchronous line. For further information use link: http://linux.die.net/man/8/chat

sim1_chat and sim2_chat (new)
Purpose: */etc/ppp/peers/VMX53/sim1_chat* – for first SIM card (based on the new CPU i.MX53)

sim1.conf and sim2.conf
Configurable variables:
APN
PIN

NETWORK
NETWORK_V2
REBOOT_TIMEOUT
variable reboot timeout [min] on modem recovery. If is not set, then SLC device will use 60 minutes and other devices will use 2 minutes.

ssh_config
Purpose: */etc/ssh_config* - this file is the ssh client system-wide configuration file. This file provides defaults for users, and the values can be changed in per-user configuration files or on the command line.

sshd_config
Purpose: */etc/sshd_config* – OpenSSH SSH daemon configuration file. SSHD reads configuration data from */etc/sshd_config* (or the file specified with -f on the command line). The file contains keyword-argument pairs, one per line.Lines starting with '#' and empty lines are interpreted as comments. Arguments may optionally be enclosed in double quotes (") in order to represent arguments containing spaces. This file should be writable by root only, but it is recommended (though not necessary) that it be world-readable.
Additional information: http://linux.die.net/man/5/sshd_config

VPN
A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.

PPP
- **cdma_chat**
- **options**
- **chap-secrets-cdma**

network_eth3
network_eth4

L2TP configuration

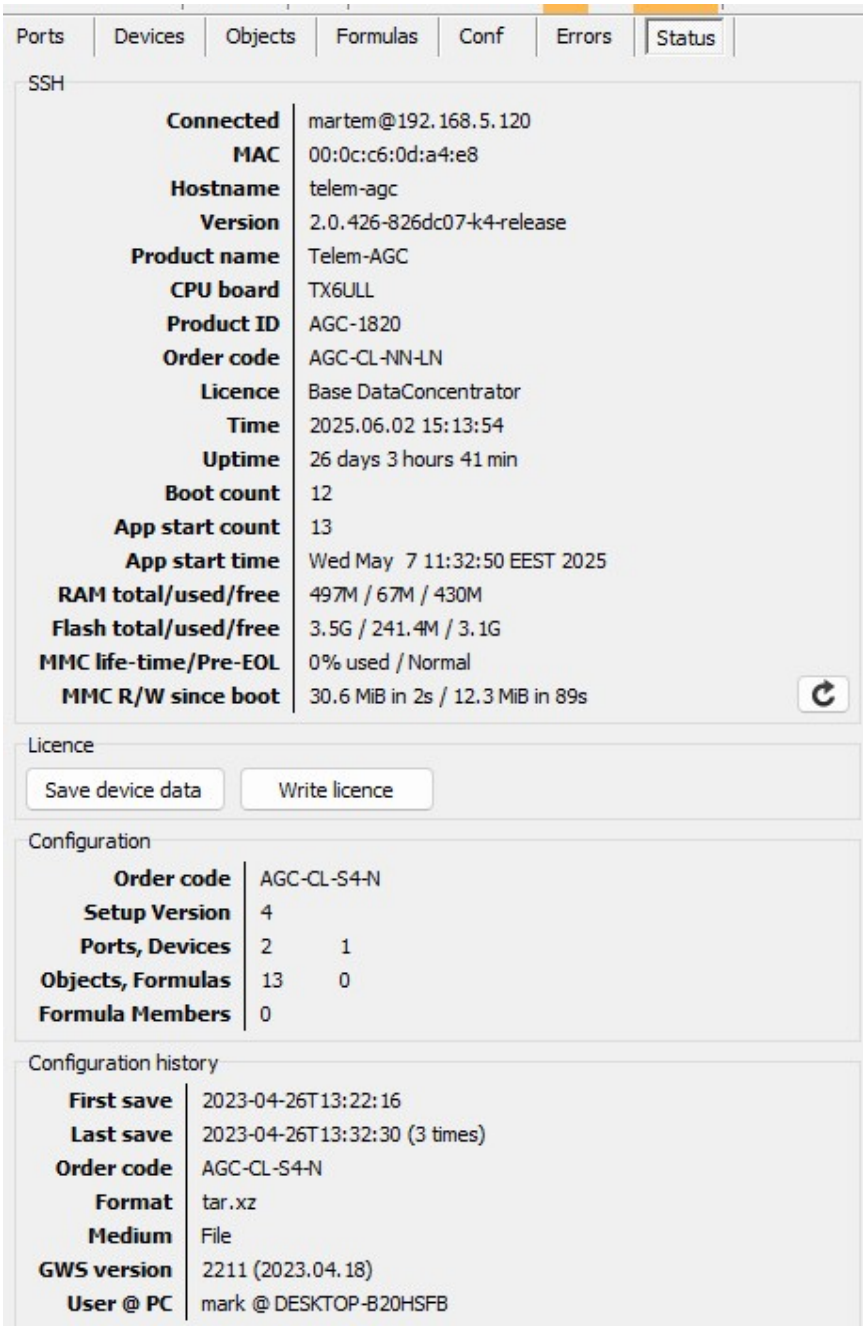
In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

5.2.11 Errors Tab Card

Possible errors found in the configuration are described in this tab. When writining configuration to device Telem-GWS automatically checks configuration or possible errors. If found, errors are described in this window. User can always manually check or errors, using Recheck button.

5.2.12 Status Tab Card

The `Status` tab provides a read-only runtime summary of the connected Telem-GWS device. Data is retrieved via SSH and is grouped into three sections: **Device Runtime Info**, **Licence and Configuration**, and **Configuration History**. This view is critical for diagnostics, licensing validation, memory usage analysis, and firmware traceability.



SSH – Device Runtime Info

Field	Description

Connected	Active SSH session identifier (user@IP)
MAC	MAC address of primary Ethernet interface
Hostname	Current system hostname as reported by OS
Version	Full firmware version string
Product name	Hardware-specific device label (e.g. Telem-AGC)
CPU board	SoC or module identifier (e.g. NXP i.MX6ULL)
Product ID	Internal device model ID
Order code	Full product configuration string
Licence	Installed feature license tier
Time	Current system time
Uptime	Elapsed time since last boot
Boot count	Total system reboots since install
App start count	Application-level restarts
App start time	Timestamp of last application start (process-level uptime)
RAM total/used/free	Memory summary in MiB
Flash total/used/free	NAND or eMMC summary (MiB/GB granularity)
MMC life-time/Pre-EOL	Non-volatile flash memory indicator (% used or wearout status) If there is any color logging should be reduced as much as possible.
MMC R/W since boot	Measured I/O traffic to storage device (read/write in MiB) Value can be high on startup. Wait an hour for average value. If there is any color logging should be reduced as much as possible.
↻ Icon	Manual refresh trigger for runtime values

Licence

Control	Function
Save device data	Export runtime hardware data required for license generation
Write license	Apply license file to activate product features

Configuration

Field	Description
Order code	Current loaded configuration's target model string
Setup Version	Format version of configuration file (must match firmware parser)
Ports, Devices	Total configured communication ports and connected devices
Objects, Formulas	Count of I/O points and active formula rows
Formula Members	Total signals referenced inside formulas

Configuration History

Field	Description
First save	Initial configuration creation timestamp
Last save	Most recent save timestamp, including save count
Code	Configuration identifier string
Format	Storage type (e.g. `tar.xz`)
Medium	Transfer or save method (`File`, `Network`)
GWS version	GUI build version used for last save
User @ PC	Logged Windows user + hostname used for last modification

5.3 Configuring the OPC UA for streetlighting system

5.3.1 OPC UA channel configuration

Create “OPC^” Port and set the ID (1 in the example):

AGC-LA-N4-N Setup - 172.16.0.208 - *

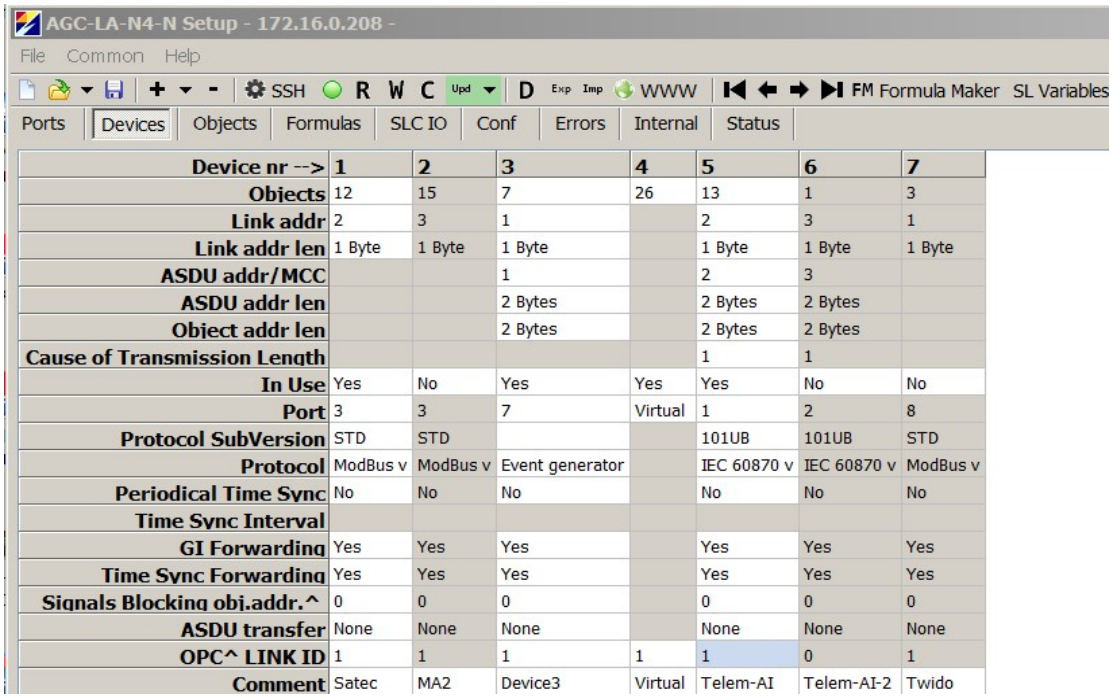
File Common Help

SSH R W C Upd D Exp Imp WWW FM Formula Maker SL Variables

Ports | Devices | Objects | Formulas | SLC IO | Conf | Errors | Internal | Status

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Protocol	IEC 60870 v	IEC 60870 v	ModBus v	IEC 60870 ^	WebServer	OPC^
Baud Rate	9600	9600	9600			
Parity	None	None	None			
Stop Bit	1	1	1			
Data Bits	8	8	8			
Modem Settings						
Communication Mode	No Control	No Control	No Control	Tcp/Ip Legacy		Tcp/Ip Server
IP Address				0.0.0.0:2404	0.0.0.0:80	0.0.0.0:48020
Polling(v)/Answering(^) Delay [ms]	0	0	20	0		0
Port Link Address/ID/Transp.con. Group						1
Length of Link Address						1 Byte
IEC Port ASDU Address				1		1
Length of ASDU Address				2 Bytes		2 Bytes
IEC Object Length				3 Bytes		3 Bytes
Cause of Transmission Length						
Up Protocol SubVersion				104		4
Query Timeout [ms]	500	500	500	60000		60000
Failed Query Count for disabling contr.	5	5	5	5		5
Retry Query/Test Interval [s]	5	5	2	250		20
Suppress Echo	No	No	No	No		No
Watchdog						
Time				NTime/LTime		NTime/LTime
Allow Timesync				No		No
Logging	OFF	OFF	OFF	OFF		OFF
Time Zone	localtime	localtime	localtime	localtime		localtime
Comment	Port1	Port2	Satec	SCADA	WebServer	OPC

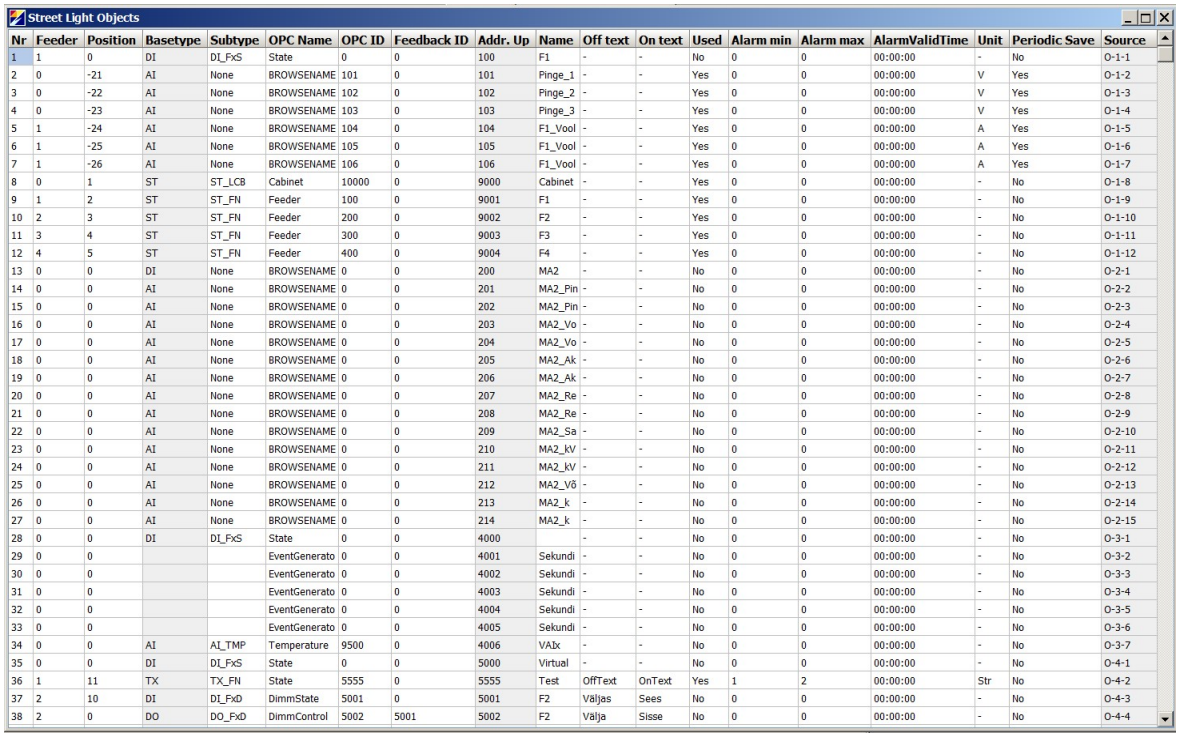
To establish communication with SCADA the **OPC ^ LINK ID** (OPC LINK ID UP) is needed for every IO-object. This parameter must be filled in **SLC IO** tab and **Formulas** tab for all objects used by street light SCADA. For **Object tab** data points the **OPC ^ LINK ID** must be described in the **Devices** and **Ports** tabs (parameter **Port Link Address/ID/...** must be equal with **OPC ^ LINK ID)**



Device nr -->	1	2	3	4	5	6	7
Objects	12	15	7	26	13	1	3
Link addr	2	3	1		2	3	1
Link addr len	1 Byte	1 Byte	1 Byte		1 Byte	1 Byte	1 Byte
ASDU addr/MCC			1		2	3	
ASDU addr len			2 Bytes		2 Bytes	2 Bytes	
Object addr len			2 Bytes		2 Bytes	2 Bytes	
Cause of Transmission Length					1	1	
In Use	Yes	No	Yes	Yes	Yes	No	No
Port	3	3	7	Virtual	1	2	8
Protocol SubVersion	STD	STD			101UB	101UB	STD
Protocol	ModBus v	ModBus v	Event generator		IEC 60870 v	IEC 60870 v	ModBus v
Periodical Time Sync	No	No	No		No	No	No
Time Sync Interval							
GI Forwarding	Yes	Yes	Yes		Yes	Yes	Yes
Time Sync Forwarding	Yes	Yes	Yes		Yes	Yes	Yes
Signals Blocking obj.addr.^	0	0	0		0	0	0
ASDU transfer	None	None	None		None	None	None
OPC^ LINK ID	1	1	1	1	1	0	1
Comment	Satec	MA2	Device3	Virtual	Telem-AI	Telem-AI-2	Twido

5.3.2 OPC UA objects configuration

The Street Light Objects table is combined from object tab, SLC IO tab and Formulas tab of this AGC-L device. Additionally, this table includes text information and variables for street light SCADA, needed for establishment of OPC connection and used configuring user interface



Street Light Objects

Nr	Feeder	Position	Basetype	Subtype	OPC Name	OPC ID	Feedback ID	Addr. Up	Name	Off text	On text	Used	Alarm min	Alarm max	AlarmValidTime	Unit	Periodic Save	Source
1	1	0	DI	DI_FxS	State	0	0	100	F1	-	-	No	0	0	00:00:00	-	No	O-1-1
2	0	-21	AI	None	BROWSENAME	101	0	101	Pinge_1	-	-	Yes	0	0	00:00:00	V	Yes	O-1-2
3	0	-22	AI	None	BROWSENAME	102	0	102	Pinge_2	-	-	Yes	0	0	00:00:00	V	Yes	O-1-3
4	0	-23	AI	None	BROWSENAME	103	0	103	Pinge_3	-	-	Yes	0	0	00:00:00	V	Yes	O-1-4
5	1	-24	AI	None	BROWSENAME	104	0	104	F1_Vool	-	-	Yes	0	0	00:00:00	A	Yes	O-1-5
6	1	-25	AI	None	BROWSENAME	105	0	105	F1_Vool	-	-	Yes	0	0	00:00:00	A	Yes	O-1-6
7	1	-26	AI	None	BROWSENAME	106	0	106	F1_Vool	-	-	Yes	0	0	00:00:00	A	Yes	O-1-7
8	0	1	ST	ST_LCB	Cabinet	10000	0	9000	Cabinet	-	-	Yes	0	0	00:00:00	-	No	O-1-8
9	1	2	ST	ST_FN	Feeder	100	0	9001	F1	-	-	Yes	0	0	00:00:00	-	No	O-1-9
10	2	3	ST	ST_FN	Feeder	200	0	9002	F2	-	-	Yes	0	0	00:00:00	-	No	O-1-10
11	3	4	ST	ST_FN	Feeder	300	0	9003	F3	-	-	Yes	0	0	00:00:00	-	No	O-1-11
12	4	5	ST	ST_FN	Feeder	400	0	9004	F4	-	-	Yes	0	0	00:00:00	-	No	O-1-12
13	0	0	DI	None	BROWSENAME	0	0	200	MA2	-	-	No	0	0	00:00:00	-	No	O-2-1
14	0	0	AI	None	BROWSENAME	0	0	201	MA2_Pin	-	-	No	0	0	00:00:00	-	No	O-2-2
15	0	0	AI	None	BROWSENAME	0	0	202	MA2_Pin	-	-	No	0	0	00:00:00	-	No	O-2-3
16	0	0	AI	None	BROWSENAME	0	0	203	MA2_Vo	-	-	No	0	0	00:00:00	-	No	O-2-4
17	0	0	AI	None	BROWSENAME	0	0	204	MA2_Vo	-	-	No	0	0	00:00:00	-	No	O-2-5
18	0	0	AI	None	BROWSENAME	0	0	205	MA2_Ak	-	-	No	0	0	00:00:00	-	No	O-2-6
19	0	0	AI	None	BROWSENAME	0	0	206	MA2_Ak	-	-	No	0	0	00:00:00	-	No	O-2-7
20	0	0	AI	None	BROWSENAME	0	0	207	MA2_Re	-	-	No	0	0	00:00:00	-	No	O-2-8
21	0	0	AI	None	BROWSENAME	0	0	208	MA2_Re	-	-	No	0	0	00:00:00	-	No	O-2-9
22	0	0	AI	None	BROWSENAME	0	0	209	MA2_Sa	-	-	No	0	0	00:00:00	-	No	O-2-10
23	0	0	AI	None	BROWSENAME	0	0	210	MA2_kV	-	-	No	0	0	00:00:00	-	No	O-2-11
24	0	0	AI	None	BROWSENAME	0	0	211	MA2_kV	-	-	No	0	0	00:00:00	-	No	O-2-12
25	0	0	AI	None	BROWSENAME	0	0	212	MA2_Võ	-	-	No	0	0	00:00:00	-	No	O-2-13
26	0	0	AI	None	BROWSENAME	0	0	213	MA2_k	-	-	No	0	0	00:00:00	-	No	O-2-14
27	0	0	AI	None	BROWSENAME	0	0	214	MA2_k	-	-	No	0	0	00:00:00	-	No	O-2-15
28	0	0	DI	DI_FxS	State	0	0	4000		-	-	No	0	0	00:00:00	-	No	O-3-1
29	0	0			EventGenerato	0	0	4001	Sekundi	-	-	No	0	0	00:00:00	-	No	O-3-2
30	0	0			EventGenerato	0	0	4002	Sekundi	-	-	No	0	0	00:00:00	-	No	O-3-3
31	0	0			EventGenerato	0	0	4003	Sekundi	-	-	No	0	0	00:00:00	-	No	O-3-4
32	0	0			EventGenerato	0	0	4004	Sekundi	-	-	No	0	0	00:00:00	-	No	O-3-5
33	0	0			EventGenerato	0	0	4005	Sekundi	-	-	No	0	0	00:00:00	-	No	O-3-6
34	0	0	AI	AI_TMP	Temperature	9500	0	4006	VAIx	-	-	No	0	0	00:00:00	-	No	O-3-7
35	0	0	DI	DI_FxS	State	0	0	5000	Virtual	-	-	No	0	0	00:00:00	-	No	O-4-1
36	1	11	TX	TX_FN	State	5555	0	5555	Test	OffText	OnText	Yes	1	2	00:00:00	Str	No	O-4-2
37	2	10	DI	DI_FxD	DimmState	5001	0	5001	F2	Väljas	Sees	No	0	0	00:00:00	-	No	O-4-3
38	2	0	DO	DO_FxD	DimmControl	5002	5001	5002	F2	Välja	Sisse	No	0	0	00:00:00	-	No	O-4-4

Nr Row order number (not editable)

Feeder Feeder's identification number, where this object belongs

Position Position of this IO objekt in street light SCADA user interface tables (used for reorder rows of table)

Basetype Object's type (from tab Objects): digital input (DI), analog input (AI), counter (CN), digital output (DO), analog output (AO), digital output with function (DO_FN). The Basetype is not editable in this table.

Subtype Special fixed type description for regular streetlight objects. Choosing this parameter generates OPC Name - corresponding parameter used by OPC

OPC Name Special name-description used by OPC for identifying object type

Description of the logical relationships between SubType and OPC Name:

Basetype	Subtype	OPC Name
DI	DI_FxS	State
	DI_CA	AlarmState
	DI_ACT	Active
	DI_VA	VoltageAlarm
	DI_CB	CBStatus
	DI_DRS	DoorState
	DI_DRA	DoorAlarm
	DI_FxD	DimmState
	DI_GRD	GuardState
	DI_MAN	ManualOverrideState
DO	DO_FxD	DimmControl
	DO_GRD	GuardControl
	DO_MAN	ManualOverrideControl
	DO_FxC	Control
AI	AI_LLS	LocalLightSensor
	AI_TMP	Temperature
	AI_HUM	Humidity
	AI_CLS	CentralLightSensor
AO	AO_CLS	CentralLightSensor_RV
	AO_D_1	AO_D_1
	AO_D_2	AO_D_2
	...	...
	AO_D_100	AO_D_100
ST	ST_LBC	text information about this AGC-L
	ST_FN	text information about this AGC-L feeder

OPC ID Unique identification number of this object for OPC
Feedback ID of DI or AI signal, logically linked with this DO or AO object
Addr. up Address up (Object.Addr ^ from Objects Tab Card)
Name Correct object's Name for SCADA (Comment from Objects Tab Card)
Off text Explanation text of BI signals off state (for SCADA user interface)
On text Explanation text of BI signals on state (for SCADA user interface)
Alarm min Minimum value of measurement, which generates "alarm" message
Alarm max Maximum value of measurement, which generates "alarm" message

AlarmValidTime
Time (format hh:mm:ss) when Alarm min and Alarm max values are checked for generating alarm messages. If empty - alarm values are checked continuously.

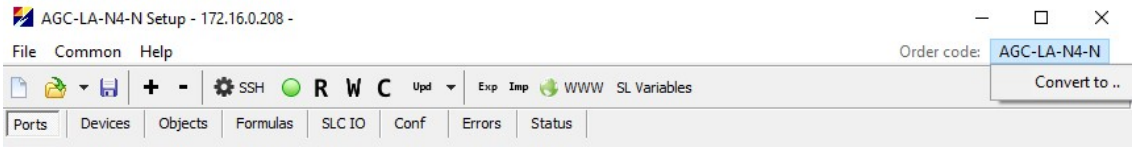
Unit Unit only for AI (analog input) objects

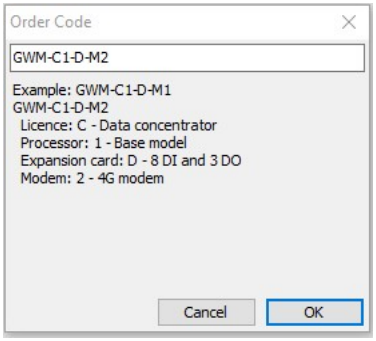
Periodic Save Values "Yes" or "No". Periodical logging measurements

Source Reference to table where this objects also exsists (O - Objects, IO - SLC IO, F-Formulas and number of table row)

5.4 Converting existing configuration for other device type or modification

For converting the existing configuration for another Telem device press the order code field on upper right corner of the device configuration window and select the „Convert to“ option.





After inserting the order code the configuration is accordingly converted for this device.

In case the Telem-GWS has active SSH connection with some device and the configuration of ohter device type or modification is opened from the file, the warning is displayed on bottom of the window and configuration conversion for connected device is offered. Also the conversion suggestion is displayed in upper right corner.

5.5 Configuration of Telem RTU I/O modules via data concentrator

Configuration Redirection is used to configure RTU-T modules via data concentrator using 101 or 104 connection. Data concentrator has to have 101 or 104 port upwards configured to enable conf redirection. Using that function all Telem RTU-T devices are configurable using ethernet connection.

It is recommended to create another port in the data concentrator configuration: **IEC setup**, if conf. redirection is needed.

Following steps should be performed:

- Create IEC setup port to configuration or use already active 101 or 104 up for establishing connection with data concentrator over ethernet.
- Make connection to data concentrator via 101 or 104 over Ethernet. From the **Telem configurato**r window choose **device-> communication setup**
    - check use Network
    - define protocol (101 or 104)
    - insert IP address of data concentrator
    - insert TCP port number that is used
- Find out the device number (from devices tab card) You want to configure (e.g. device no 1)
- Activate conf redirection using device number (from configuration, devices tab card). From the **Telem configurator** window choose **device-> RTU conf. redir. via IEC 60870.**
- Number in that window cannot be entered from keyboards (right-handed) num pad. Current window must be opened during configuration I/O module.
- Choose which module You want to configure.
- Read or Write configuration of I/O module.

Hint: If for example Telem-RTA is connected to Telem-AGC serial port as sub- RTU (one collects data from another), then the configuration of RTA can be remotely read and written through the Tele-AGC using the configuration program.

5.6 Transparent connections

To send information from one port to another (incl. tcp to serial).

Objects | Formulas | Conf | Errors | Status

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Protocol	None	None	None	Transp.con.	None	Transp.con.
Baud Rate				9600		
Parity				None		
Stop Bit				1		
Data Bits				8		
Communication Mode				No Control		Tcp/Ip Server
IP Address						0.0.0.0:2404
ıswering(^) Delay [ms]						
s/ID/Transp.con. Group				199		199

Create two ports as Protocol type „Transp.con.“ and bind them using ‘**Transp.con. Group**’ field by using equal integer values. This shall transfer all application layer data from one port to another. TCP-TCP, TCP-Serial, Serial-Serial pairs allowed. For TCP ports determine ‘**Communication Mode**’ either ‘**Tcp/Ip Client**’ for connecting side or ‘**Tcp/Ip Server’** for listening side. Note that ‘**Tcp/Ip Client**’ constantly attempts to establish and keep up an active connection.

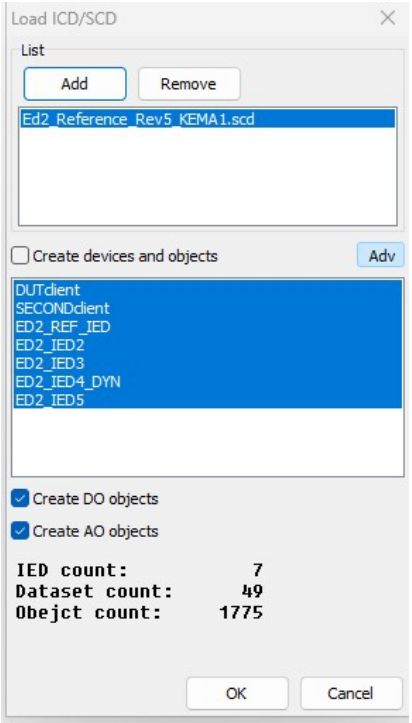
5.7 Configuring IEC 61850 devices

IEC 61850 standard defines configuration file structure for describing IED (or multiple IEDs) setup. Telem-GW6 and Telem-AGC support IEC 61850 Client protocol and configuring it has been made straightforward in Telem-GWS. Following chapter describes configuring of IEC 61850 device step by step.

Import ICD/SCD

Click on **ICD/SCD** shortcut. Load ICD/SCD window opens. Click on **Add** to choose the ICD/SCD file with IED/IEDs. Also check **Create devices and objects** (**Adv** button on the right for additional options). Click **OK**.

Example conf below 61850-k2-multiple-connections-2.tar.xz



Telem-GWS program ICD/SCD parser commonly results in the following list of necessary information filled automatically:

- Port configuration with correct IP parameters (Port tab card)
- devices configuration (Devices tab card)
- objects configuration, with lower-level addresses. (Objects tab card)

To get the system working only upper-level addresses require configuration in the Objects tab card.

It is possible to remove/add/modify objects in the Objects tab card.

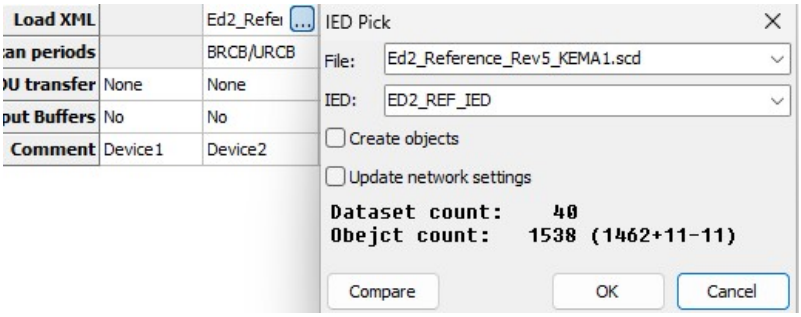
Change ICD/SCD file

It is quite common that ICD/SCD file in the IED-s changes during configuring period.

1. Click on **ICD/SCD** shortcut.
2. **Add** the modified ICD/SCD.
3. Uncheck **Create devices and objects.**

Then the file is imported to configuration but not yet applied.

To proceed with applying changes it is required to specify ICD/SCD file and IED to use for each Device.



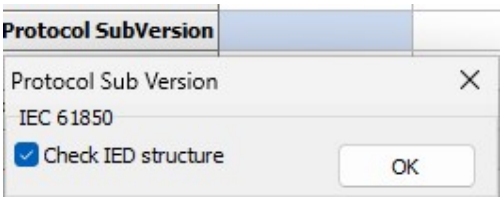
Click on the **Load XML** box on the Device configuration that is subject to change. Choose the file and the IED and also check **Create objects** to load objects again. When this is done the user view in O**bjects** tab card visually highlights the changes (green- added to object list), old (yellow-not changed), missing (red - will be deleted).

Define RCB and Dataset, Dynamic dataset

It is possible to define or enable specific RCB and dataset. Click on the **BRCB conf**. box in Devices tab card. Then **BRCB Conf.** window is opened. User can choose RCB and dataset.
Also, it is possible to create dynamic dataset by checking **Create first dataset.** in the **BRCB Conf.** window. User has to choose which BRCB to use and define a new **dataset.** Telem-AGC creates dataset with the name user has defined and with the objects defined in the Objects tab card.
Objects used in the dataset have to be defined in the IED (set "In Use"), otherwise creating dataset fails. IED name in the Logical Nodes (LN) has to be the same as in IED configuration.

Additional parameters under Device Tab->Protocol SubVersion

"Check IED structure" checkbox (ON by default) – RTU IEC 61850 Client performs ICD structure checks in IED if ON.



If connection between RTU and IED fails by RTU TCP disconnecting soon after successful connect then turning this OFF may solve this.

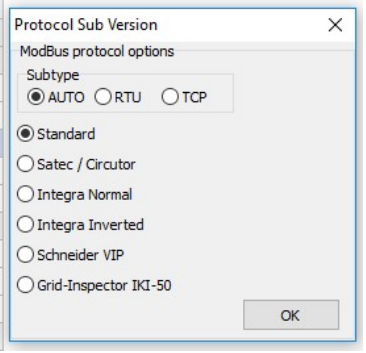
5.8 Configuring ModBus devices (ModBus Client)

Supported Modbus options

Telem devices support Modbus RTU via serial line and Modbus TCP over Erhernet (ver. 1.1b3).
There is also possibility to choose device specific Modbus application in „**Devices**" -> „**Protocol SubVersion**". Device specific Modbus options are legacy. In general Modbus RTU and Modbus TCP meet most of requirements, so „**Standard**" is the default value. If in **Ports tab** on certain port is chosen Communication Mode „**No Control**", then Modbus RTU serial is used, if „**TCP/IP Client**" is chosen, then Modbus TCP is used. For some applications, e.g. Modbus RTU over TCP/IP, it is required to specify the mode also in „**Devices**" -> „**Protocol SubVersion**" choosing „**RTU**".

	Port 4	Port 14
Protocol	ModBus v	ModBus v
Baud Rate	9600	
Parity	None	
Stop Bit	1	
Data Bits	8	
Modem Settings		
Communication Mode	No Control	Tcp/Ip Client
IP Address		0.0.0.0:502

Link addr	1	1
Link addr len	1 Byte	1 Byte
ASDU addr/MCC		
ASDU addr len		
Object addr len		
Cause of Transmission Length		
In Use	Yes	Yes
Port	4	14
Protocol SubVersion	STD	STD
Protocol	ModBus v	ModBus v
Periodical Time Sync	No	No
Time Sync Interval		
GI Forwarding	Yes	Yes
Time Sync Forwarding	Yes	Yes
Signals Blocking obj.addr.^	0	0
Load XML		



Since GWS 2157 under „**Devices**" -> „**Protocol SubVersion**" there is a tick box:

If ON – If a configured data point object in GWS (register in Modbus) returns error code 2 (ILLEGAL DATA ADDRESS) during polling from RTU, it shall be discarded from the set if polled addresses and shall not be polled anymore until at least RTU r1 reset (default),
If OFF – All data points configured by GWS shall always be polled.

Modbus addressing and function codes

Modbus addressing scheme is separated to have an address and a function code. In Telem-GWS function code is determined in the cell **Obj. Addr. V** of objects tab. I.e. function code and address of the Modbus register are written together in same cell.
Input objects function code is determined from the address. For example holding register with Modbus address 107 should be addressed in Telem-GWS 40108. Object address supplement 10000 is used for addresses less than 10000. For bigger addresses the supplement 100000 is used.
Digital output (Force coils) function codes are determined by their '**SubType**^' type in Telem-GWS.
Analog output (Preset Single Register and Preset Multiple Registers) function codes are determined by their '**SubType v**' type in Telem-GWS.

In Telem Application next function codes and Object Address Supplements are used:

Modbus function name	Function code	Object Address supplement	Subtype
Function Unsupported	0x00	-	-
Read Coil Status	0x01	10000 or 100000	-
Read Input Status	0x02	20000 or 200000	-
Read Holding Registers	0x03	40000 or 400000	-
Read Input Registers	0x04	30000 or 300000	-
Force Single Coil	0x05	-	^ Single
Preset Single Register	0x06	60000 or 600000	v Normalized
Force Multiple Coils	0x0F	-	^ Double
Preset Multiple Registers	0x10	40000 or 400000	v INT32, UINT32

Telem-GWS Modbus addresses configuring examples:

Object Type	Function code	Register address	Obj. Addr. V in Telem-GWS
AI	0x3	238	40239
AI	0x4	23358	323359
AO	0x10	23358	423359
DI	0x2	238	20239
AO	0x6	23358	23359 or 623359
DO	0x5	100	101

Mapping of Modbus to IEC60870-5-104 protocol:

Modbus fn.code hex	Name	IEC60870-5-104 type identification		COT	
Data				S	GI
0x03,0x04	Read holding, input register	9	M_ME_NA_1	3	20
0x03,0x04	Read holding, input register	11	M_ME_NB_1	3	20
0x03,0x04	Read holding, input register	13	M_ME_NC_1	3	20
0x01, 0x02	Read coil, input status	1	M_SP_NA_1		20
0x01, 0x02	Read coil, input status	3	M_DP_NA_1		20
0x01, 0x02	Read coil, input status	30	M_SP_TB_1	3	
0x01, 0x02	Read coil, input status	31	M_DP_TB_1	3	
Commands				Act	
0x05	Force single coil	45	C_SC_NA_1	6	
0x0F	Force multiple coils	46	C_DC_NA_1	6	
0x06, 0x10	Preset single or multiple register	48	C_SE_NA_1	6	
0x06, 0x10	Preset single or multiple register	49	C_SE_NB_1	6	
0x06, 0x10	Preset multiple registers	50	C_SE_NC_1	6	

As subtype in Telem-GWS is defining Modbus function code for commands, then mapping can have some possibilities which are considered depending on slave device specification. Time tagged commands are also supported. Time tag of the command is checked by RTU.

Also in Telem-GWS is possible to configure obtaining of status information from input or holding registers (analog datapoints) using option „AI-bit" in DI **SubType v**. User should know required bit position in register and type it's number into the cell „Index". So when the value of this bit equals to 1 then event „ON" occurs.

Dev. nr.	Obj. nr.	Type	SubType ^	SubType v	Invert	Fn. Code	Info nr.	Index	Obj. Addr. v	61850 DS	61850 v	Obj. Addr. ^
1	1	DI	Single	Normal	No							200
1	2	DI	Single	AI-Bit	No			4	30721			201

5.9 ModBus Server

Addressing Configuration
Same as ModBus Client but **Obj. Addr.** ^ is used with same addressing parsing scheme.

In Telem Application next function codes and Object Address Supplements are used:

Object Type	Modbus function name	Function code	Object Address supplement	Subtype
DI	Read Coil Status	0x01	10000 or 100000	-
DI	Read Input Status	0x02	20000 or 200000	-
AI	Read Holding Registers	0x03	40000 or 400000	-
AI	Read Input Registers	0x04	30000 or 300000	-
DO	Force Single Coil	0x05	-	-
AO	Preset Single Register	0x06	-	-
DO*	Force Multiple Coils	0x0F	-	-
AO**	Preset Multiple Registers	0x10	-	-

* - DO data point objects must have have sequential addresses in GWS from up to bottom and **Force Mutliple Coils** shall set as many as requested.
** - A register in ModBus is size 2 byte. If **SubType** ^ is **Norm** then during **Preset Multiple Registers** request all the sequential AO data point objects shall be set with 2 byte value. I.e. the request data is parsed in 2byte chunks in RTU. Often it is requried to treat the incoming analog comand value as 4 bytes and this is possible if **SubType** ^ is **Float AND** the adresses are **NOT** sequential; they are spaced apart by one, with each address increasing by two. E.g. 100,102,104.

Telem-GWS Modbus addresses configuring examples:

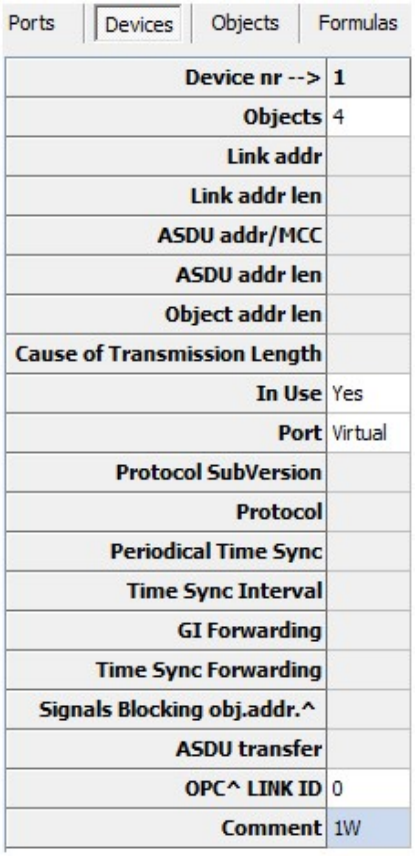
Object Type	Function code	Register address	Obj. Addr. V in Telem-GWS
AI	0x3	238	40239
AI	0x4	23358	323359
AO	0x10	23358	423359
DI	0x2	238	20239
AO	0x6	23358	23359 or 623359

DO	0x5	100	101

ModBus Server and IEC Select
ModBus Protocol does not support Select as in IEC. By default any command given to ModBus Server results in Exec in lower-level channels even if the lower-level object is configured as Select. To enable ModBus Server to do Select add "**auto-select**" (no quotes) to ModBus Server Port **Comment**.

5.10 1-Wire sensor configuration

Martem devices have possibility to use 1-Wire sensors: temperature, humidity and light sensors. To configure device for using 1-Wire sensors, it is needed to make "Virtual device" in **Devices tab** and create necessary amount of objects.



Ports | Devices | Objects | Formulas | GWM IO | Conf | Errors | Internal | Status

	Dev. nr.	Obj. nr.	Type	SubType ^	SubType v	Invert	Fn. Code	Info nr.	Index	Obj. Addr. v	61850 v	Obj. Addr. ^	Comment
⊟	1	1	DI	Single	Normal	No						65001	1W
	1	2	AI	Floating Point	0					1		1	
	1	3	AI	Floating Point	0					1		2	
	1	4	AI	Floating Point	0					1		3	

From drop down menu in column **SubType v** appropriate sensor should be chosen. In address column type „auto-detect“. **NB!** Auto-detect function works only if there is one sensor of each type connected to the device.

Ports | Devices | Objects | Formulas | GWM IO | Conf | Errors | Internal | Status

	Dev. nr.	Obj. nr.	Type	SubType ^	SubType v	Invert	Fn. Code	Info nr.	Index	Obj. Addr. v	61850 v	Obj. Addr. ^	Comment
⊟	1	1	DI	Single	Normal	No						65001	1W
	1	2	AI	Floating Point	temp						auto-detect	1	
	1	3	AI	Floating Point	hum						auto-detect	2	
	1	4	AI	Floating Point	light						auto-detect	3	

“Auto-detect” is not usable in case of multiple sensors of one type. Instead of “auto-detect” in address column should be written sensor’s address on 1-Wire bus. This address can be found from **SSH->Open Remote terminal**. When remote terminal is open: type “ls -l /sys/bus/w1/devices/“ and list of connected sensors should appear.

```
root@telem-gw6e ~ # ls -l /sys/bus/w1/devices/
total 0
lrwxrwxrwx    1 root     root             0 Oct 11 10:12 28-000008d93e01 -> ../../../devices/w1_bus_master1/28-000008d93e01
lrwxrwxrwx    1 root     root             0 Oct 11 10:12 w1_bus_master1 -> ../../../devices/w1_bus_master1
root@telem-gw6e ~ #
```

1-Wire sensor’s address looks like 28-000008d93e01 in current example. The user should figure out if there is a required sensor and then put it’s address to address **v** column. Input of certain sensor address in Telem-GWS is precise way to find sensors on 1-Wire bus and works as with single as with multiple sensors of the same type.

Ports | Devices | Objects | Formulas | GWM IO | Conf | Errors | Internal | Status

	Dev. nr.	Obj. nr.	Type	SubType ^	SubType v	Invert	Fn. Code	Info nr.	Index	Obj. Addr. v	61850 v	Obj. Addr. ^	Comment
⊟	1	1	DI	Single	Normal	No						65001	1W
	1	2	AI	Floating Point	temp						28-000008d93e01	1	
	1	3	AI	Floating Point	temp						28-000008dd5e01	3	

5.11 VHPReady

VHPReady is a standardized IEC 60870-5-104 signal model for virtual power plants, enabling uniform communication between control centers and distributed energy resources (DERs).
Telem devices implement **VHPReady schedule transmission**.

VHPReady schedule transmission defines how DERs receive time-based power schedules via IEC 60870-5-104 using predefined information objects. It enables remote setting of active power setpoints for specific future time slots (typically 15-minute intervals). The DER interprets these as binding commands, replacing the need for vendor-specific scheduling logic. Use this only if the device must participate in automated VPP dispatch with standard-compliant schedule reception.

VHPReady schedule transmission is an application layer on top of IEC 60870-5-104 application layer protocol. In Telem-GWS configuration it is necessary to create a virtual device (or use existing virtual device) and within **Objects tab** at least one set of specific „SubType v“ objects that are grouped using „Obj.Addr.v“.

Ports | Devices | Objects | Formulas | Dev IO | Conf | Errors | Status

Dev. No.	Obj. No.	Type	SubType ^	SubType v	Invert	Index	Obj. Addr. v	Obj. Addr. ^	Comment
3	10	AO	Bitstring w.T	N D.Ex VHP.AO1			1	421889	VHPReady_vAO1 (103)
3	11	AO	Bitstring w.T	N D.Ex VHP.AO2			1	425985	VHPReady_vAO2 (104) ? %
3	12	AI	Bitstring w.T	VHP.response			1	430081	VHPReady_vAI_response (105)
3	13	AI	Floating Point	VHP.t1			1	1106	VHPReady_vAI_t1 Start time (min)
3	14	AI	Floating Point	VHP.t2			1	1107	VHPReady_vAI_t2 Duration (min)
3	15	AI	Floating Point	VHP.value			1	1108	VHPReady_vAI_value
3	16	AI	Floating Point	VHP.AO1			1	1109	VHPReady_vAO1_raw
3	17	AI	Floating Point	VHP.AO2			1	1110	VHPReady_vAO2_raw
3	18	DI	Single	Normal	No		1	1105	VHPReady_schedule Not active=0/Active=1

Type	SubType v	VHPReady Schedule Transmission Role
AO	VHPReady_vAO1	1st analog output in the schedule transmission pair.
AO	VHPReady_vAO2	2nd analog output in the schedule transmission pair.
AI	VHPReady_vAI_response	AI to send a spontaneous event to SCADA after both AOs are received.
AI	VHPReady_vAI_t1	Stores the "minutes since year begin" value from the 1st AO.
AI	VHPReady_vAI_t2	Stores the "duration" value from the 1st AO.
AI	VHPReady_vAI_value	Stores the "set point value" from the 2nd AO.
AI	VHPReady_vAO1	Stores raw value from received AO of “SubType v” VHPReady_vAO1
AI	VHPReady_vAO2	Stores raw value from received AO of “SubType v” VHPReady_vAO2
DI	Single	Single DI in the group acts as indicator whether any schedule is currently active.

5.12 Event Generator

Event Generator enables Telem device to generate events. It can be assigned to any Port in **Ports tab**. Next it is necessary to create a device in **Device tab** and begin adding data points in **Objects tab**. Similar to any other lower-level device configuration.
AI/DI/CN objects with empty **SubType v** periodically create spontaneous events. DI objects toggle from ON to OFF and back, while AI and CN gradually increase values. This enables to test unsupervised data transmission for long periods of time and stress testing.

Specific **SubType v** for **Event Generator** protocol are provided in Objects Tab Card.

6 System surveillance

6.1 Remote monitoring of operation

The status and operation of the device can be examined from log files. The log files can be accessed via built in Web interface or can be downloaded via SSH connection. The status information is recorded in status log files and the events archive is retained in events log files.

6.2 Syslog

Detected status changes and errors are stored in text files named *messages.x* and are physically saved to device's flash memory. The following information is recorded:

- The communication breaks and recoveries with substation equipment
- Starts
- Watchdog operations
- Software error messages
- Communication ports failures
- TCP/IP channels open and close operations, failures

Remote syslog can be configured according to p. 5.2.6 for log file transfer to remote server.

6.3 Events archiving

Console log files, events and errors are collected and archived in the form of text files and are physically saved to device's flash memory. By default, each log file have size at 5 MB. Events log will be updated only if any events occur. If no events are detected, nothing will be written to events text file. Device has 4 opportunities to download data files to your personal computer.

1. Use Web browser. Logs are opened and viewed in text format on the screen.
2. In case with Martem's software Telem-GWS, under **Set** button in opened window use button "**Get Logs**". Saved data is compressed archive in *.tar.gz* format.
3. Use a command prompt.

Use FTP client (e.g. WinSCP), download files from the device. Log files location:
root/var/log/telem/

Event files: *events.x.csv*
Console log files*:console.x.log*
4G/GPRS modem log file: *modem_st.csv*

Laki 25

12915 Tallinn

ESTONIA

Tel: +372 639 7979
E-mail: martem@martem.eu
Fax: +379 639 7980
www.martem.eu

6.4 Logging of communication protocol dataflow

Communication protocol dataflow can be logged:

Locally in RTU to pcap format file
To remote pcap logging server (For example Netcat + Wireshark)
Locally to Console log files (Console.x.log) in text format together with Hex values

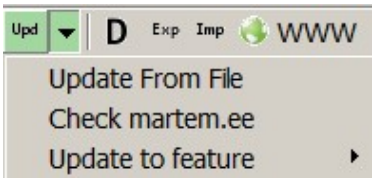
The logging is configured under *Conf tab card / log-conf.xml* (p.5.2.6). Configuration procedure of logging is described in document *Configuration of communication protocol logging on Telem-GWM and Telem-AGC devices.*

Pcap format dataflow can be analyzed with Wireshark, which is capable to interpretate most widespread communication protocols or with other similar software

7 Firmware Update

NB! Before updating to new firmware read the setup from your device, and make a backup.

- Set up the SSH connection with the device
- Press the **Upd▼** button next to **R W C** buttons



- If you have compressed .7z firmware update file (provided by Martem AS) choose **Update From File**
- If you do not have .7z firmware update file choose **Check martem.ee** to refresh exsisting firmware versions list for this AGC-L device
- Press **Update to feature** and choose needed firmware version. Download is starting...
- After firmware is downloaded **Confirm** window appears. Press **Yes** button, the update process starts
- Wait until the device resumes to its normal operation state (**RUN** LED will start slow blinking again)
- Firmware update is complete.

Checking results of the firmware update operation:

- Press **R** button to read back the device setup data
- Check the **Version** from Telem-GWS **Status** tab

8 Security measures

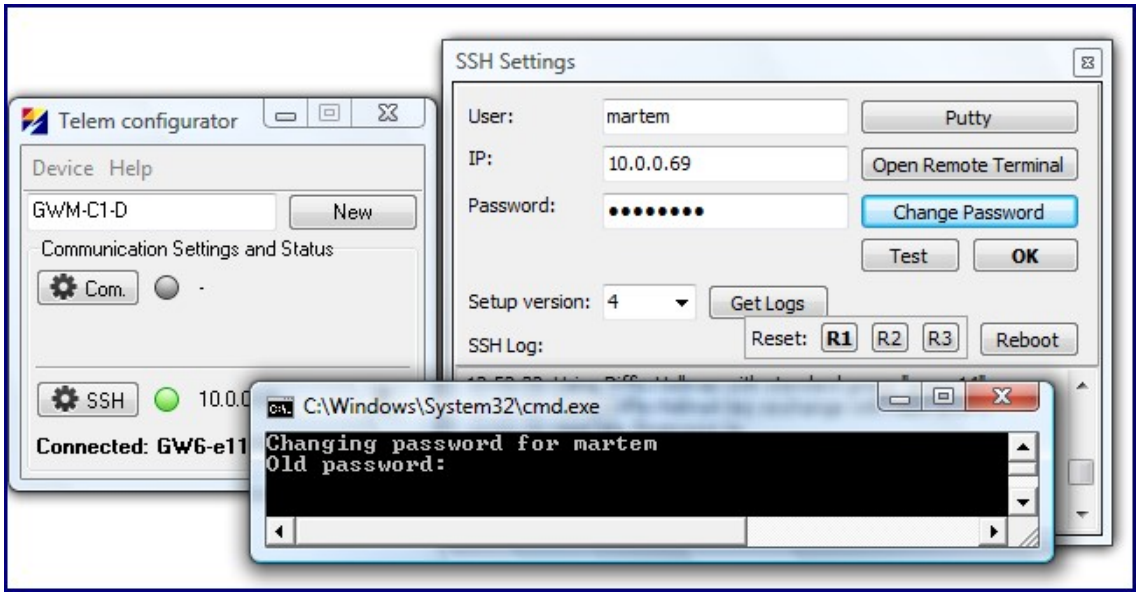
There are many ways to affect unsecurely configured device remotely and on site. To mitigate risks of unauthorized and unwanted access to Telem devices by third persons, certain steps should be performed:

Strong user access password policy
SSH access restriction via firewall
Authorization with SSH public key without or with password and username&password authorization disabling
Configuration file should be transported securely (encrypted by ID-card, GnuPG)
Trusted connection definition (other's side IP) in channel configuration
Proper filtering of incoming connections via firewall
Using secure VPN connections
Remove Web interface if it is not used
Protect Web interface access by strong password and defining other's side IP
Keep firmware up to date
Keep Telem-GWS software up to date
Keep PuTTY up to date
Be aware of updates with Martem AS security advisories

8.1 Changing default passwords

All parameters used in device „out of box“ have default values to ensure quick start and are a subject for change. It is strongly not recommended to use default passwords or IP addresses on site as it is not secure. To change default user password some actions should be taken:

Run Telem-GWS software
Connect to the device, press „SSH“ button, press „Change password“
In appeared window type old and new passwords for user „martem“
Bad password example: 123456qwer. Good password example: PYZn?<jH,g%Y)5Gn



To change „root“ user password it is needed to login as „root“ user in „Open remote terminal“ and type „passwd“. Then there will appear text „New password:“. After new password confirmation the „root“ user password is changed.

8.2 SSH connection restriction via firewall

Restriction of SSH connection via firewall can be done : „Common“-> „TCP/IP settings“->“General“. Turn the firewall on by clicking „Automatic“. There is a possibility to choose the interface and multiple networks/IP address from which is allowed to connect via SSH with comma separated list. Press „OK“ to save changes and „Write“ to write into device. Firewall rules can be checked in „Conf“->“S39iptables“. SSH rules are commented with abbriveation „SSH“.

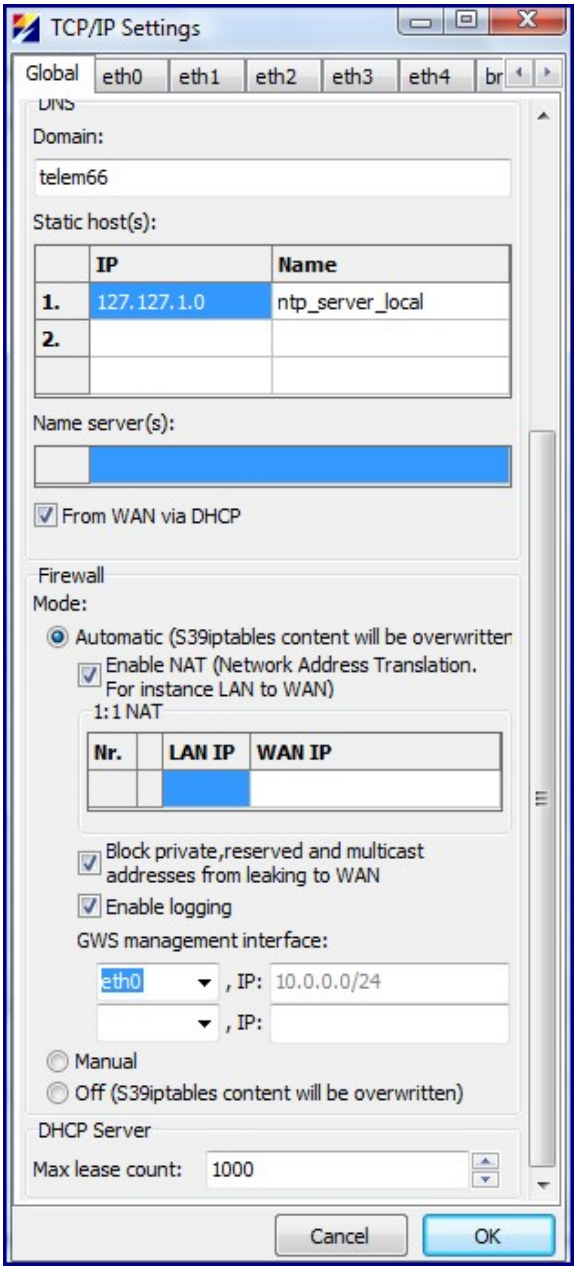
.

Laki 25

12915 Tallinn

ESTONIA

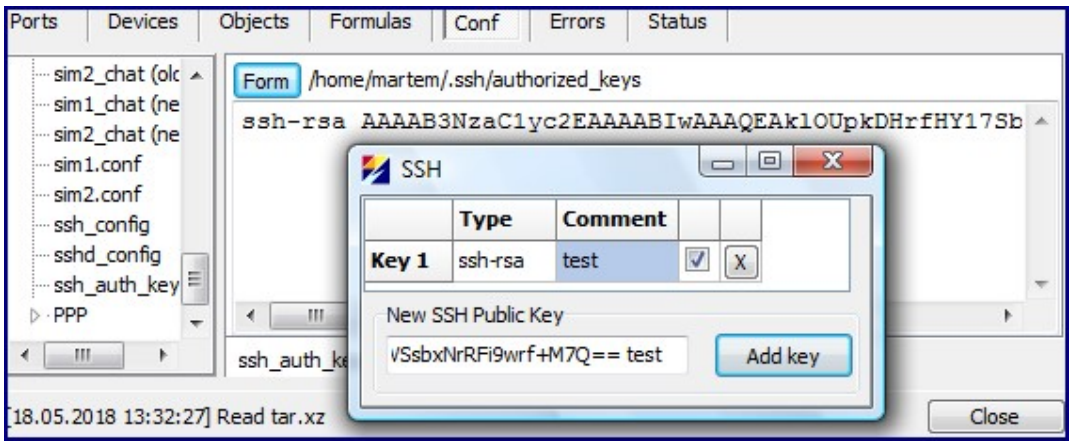
Tel: +372 639 7979
E-mail: martem@martem.eu
Fax: +379 639 7980
www.martem.eu

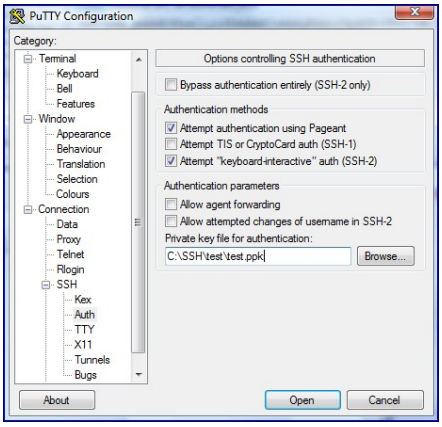

TCP/IP Settings
Global
eth0
eth1
eth2
eth3
eth4
br
DNS
Domain:
telem66
Static host(s):
IP
Name
1.
127.127.1.0
ntp_server_local
2.
Name server(s):
From WAN via DHCP
Firewall
Mode:
Automatic (S39iptables content will be overwritter
Enable NAT (Network Address Translation. For instance LAN to WAN)
1:1 NAT
Nr.
LAN IP
WAN IP
Block private,reserved and multicast addresses from leaking to WAN
Enable logging
GWS management interface:
eth0
, IP:
10.0.0.0/24
, IP:
Manual
Off (S39iptables content will be overwritten)
DHCP Server
Max lease count:
1000
Cancel
OK

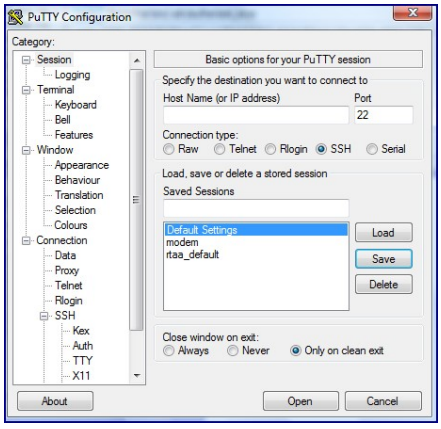
8.3 Authorization with SSH public key

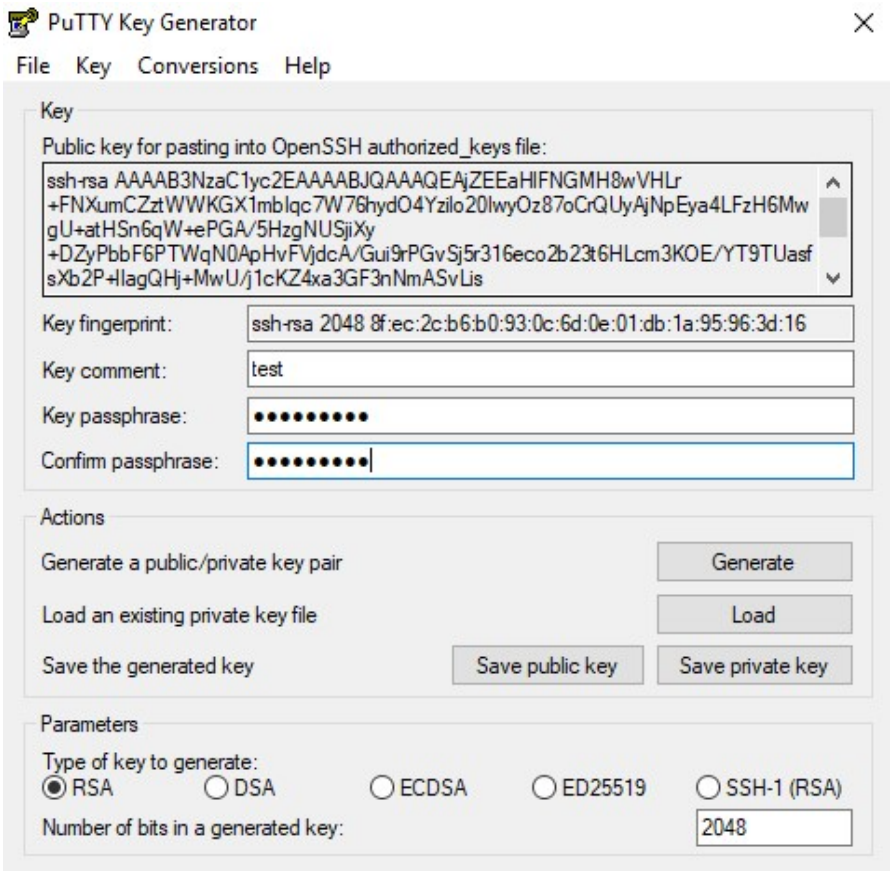
It is recommended to authorize with SSH public key for access the Telem device. The SSH public and private key pair should be created (e.g. PUTTYGen). The private key should be saved on the PC.
Public key should be put into „Conf"-> „ssh_auth_keys". This can be done by copying the key as text directly or filling the „Form". Every string in this file is a separate public key. Press „Write" to write changes into device.
To start using the private key it is required to open PuTTY tab SSH and choose „Auth". The path to the private key file should be defined. After that in „Session" tab button „Save" should be pressed. If there was not defined a „Key passphrase" in PuTTYGen, then there is no password required for making an SSH connection as public key and key signatures are used. Just type device IP address and press „OK" -> connection should be established. Authorization via SSH public key can be used without or with password. To set a password for the private key fill the field „Key passphrase" in PuTTYGen. In that way you should type the key passphrase into the field „Password" in Telem-GWS "SSH" window. This authorization way is safer, than authorization just with username and password.
There is also required a modification of „sshd_config" file. Before modifying „sshd_config" file it should be clearly sure, that authorization with key is working. The changes to „sshd_config" file are needed to disable possibility of using username and password for authorization in same time, when using authorization with the key.
These lines should be written into „sshd_config":

ChallengeResponseAuthentication no
PasswordAuthentication no
UsePAM no
PermitRootLogin no


Ports
Devices
Objects
Formulas
Conf
Errors
Status
sim2_chat (olc
sim1_chat (ne
sim2_chat (ne
sim1.conf
sim2.conf
ssh_config
sshd_config
ssh_auth_key
PPP
Form
/home/martem/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAklOUpkDHrfHY17Sb
SSH
Type
Comment
Key 1
ssh-rsa
test
New SSH Public Key
VSsbxNrRFi9wrf+M7Q== test
Add key
[18.05.2018 13:32:27] Read tar.xz
Close

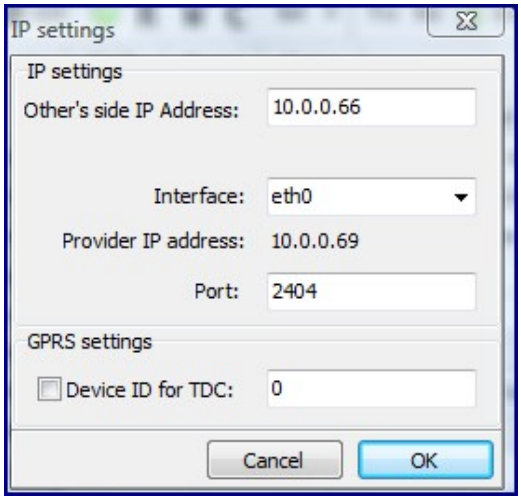

PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Options controlling SSH authentication
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\SSH\test\test.ppk
Browse...
About
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
modem
rtaa_default
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAjZEEaHIFNGMH8wVHLr
+FNXumCZztWWKGX1mbIqc7W76hydO4Yzilo20IwyOz87oCrQUyAjNpEya4LFzH6Mw
gU+atHSn6qW+ePGA/5HzgNUSjiXy
+DZyPbbF6PTWqN0ApHvFVjdcA/Gui9rPGvSj5r316eco2b23t6HLcm3KOE/YT9TUasf
sXb2P+IlagQHj+MwU/j1cKZ4xa3GF3nNmASvLis
Key fingerprint:
ssh-rsa 2048 8f:ec:2c:b6:b0:93:0c:6d:0e:01:db:1a:95:96:3d:16
Key comment:
test
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048

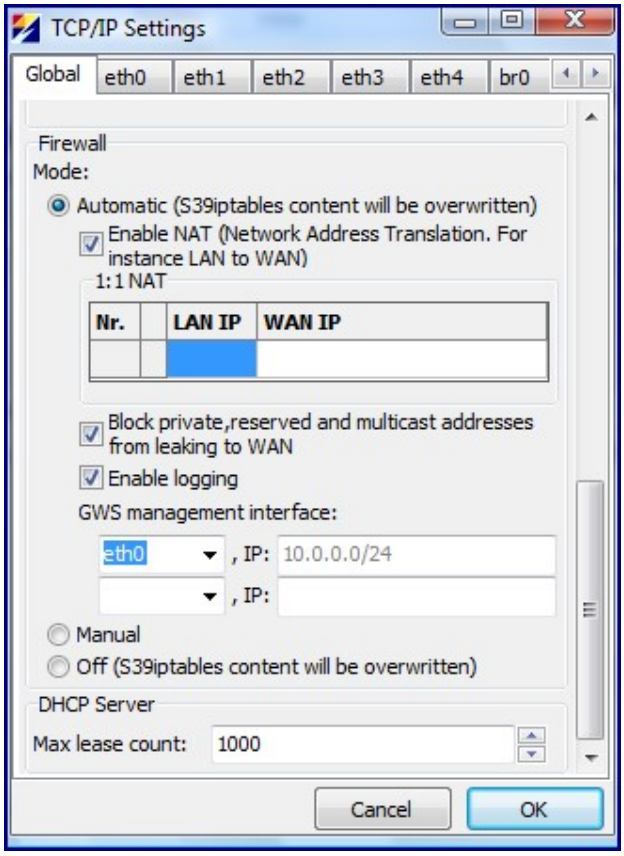
8.4 Trusted connection definition in channel setup

If there is defined trusted other's side IP address, then nobody else except of this IP address can connect to the device via chosen channel. This security feature works even if there is no firewall enabled. To define other's side IP address tab „Ports" should be open and click on IP address cell should be done. After that all necessary settings are configured and „OK" should be cliked to save changes and „Write" to write changes onto device.



8.5 Enabling firewall in Telem devices

To ensure proper filtering of incoming connections the firewall should be used. To enable firewall next steps need to be performed „Common“ -> “TCP/IP Settings“ -> „Global“ -> „Firewall Automatic“ -> „OK“ -> „Write“. Firewall rules are generated automatically according to current network confiiguration.



1.1 Secure VPN connections

There are several variants of setting up VPN connections with Telem devices. IPSec, L2TP+IPSec, OpenVPN features are available. When using VPN connections the correct interface should be chosen for each channel. Then there is a guarantee, that all traffic is securely transported via the VPN tunnel. More info about VPN connections with Telem devices can be found on Martem WIKI page.

8.6 Considering the security of WebServer usage

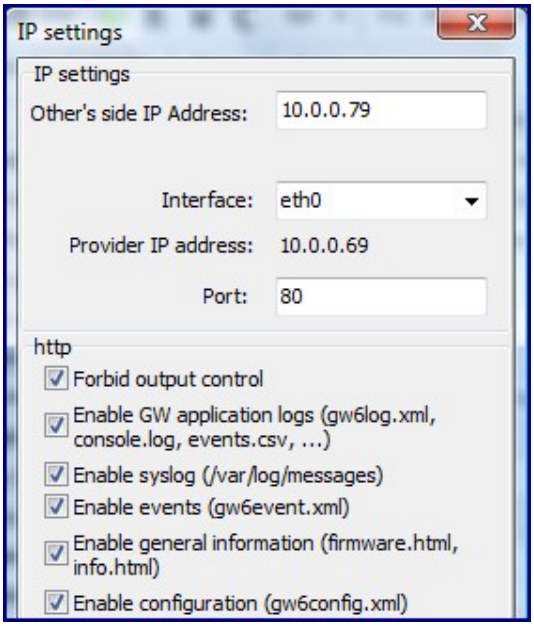
WebServer can be unsecure in front of cyber-attacks. To reduce risk of unwanted outages and to avoid usage of dangerous exploits it is recommended to:

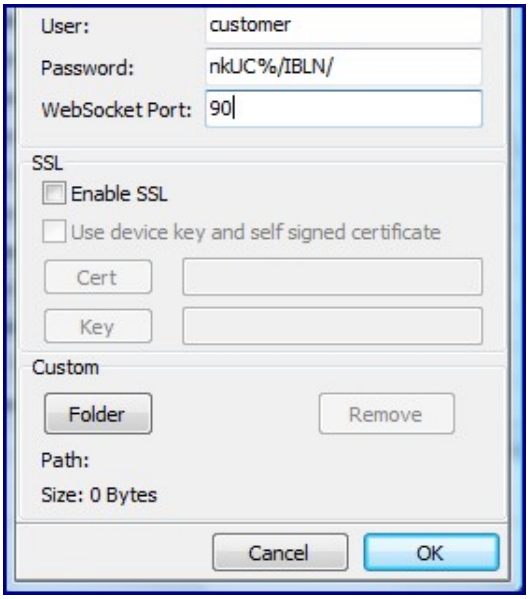
- Use WebServer only if there is necessity and turn it off when it is not needed.

Turning the WebServer off means removing port with it from the configuration.

- Use WebServer securely

Other's side IP should be defined and VPN interface should be used for access. Reasonably strong password for WebServer should be chosen. Firewall should be turned on.





8.7 Keep PuTTY up to date

By default Telem-GWS uses PuTTY embeded inside .exe file. The PuTTY binaries Telem-GWS uses are: Plink, PSCP, and PuTTY. Telem-GWS will prefer putty binaries present in same folder. To make Telem-GWS use different PuTTY version, copy desired PuTTY binaries to same folder as Telem-GWS binary.
Link to download PuTTY:
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html.

9 Appendix A

log-conf.xml to enable verbose TRACE logging

```
<?xml version="1.0" encoding="UTF-8"?>
<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">
    <appender name="Console" class="org.apache.log4j.ConsoleAppender">
        <param name="Target" value="System.out"/>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d %-5p %c - %m%n"/>
        </layout>
    </appender>
    <appender name="ConsoleFile"
class="org.apache.log4j.rolling.MartemRollingFileAppender">
        <param name="append" value="true"/>
        <param name="file" value="/var/local/telem/log/console.log"/>
        <param name="Threshold" value="TRACE"/>
        <param name="ImmediateFlush" value="false"/>
        <param name="BufferSize" value="8192"/>
        <param name="BufferedIO" value="true"/>
        <rollingPolicy
class="org.apache.log4j.rolling.FixedWindowRollingPolicy">
            <param name="FileNamePattern"
value="/var/local/telem/log/console.%i.log"/>
            <param name="MaxIndex" value="10"/>
        </rollingPolicy>
        <triggeringPolicy
class="org.apache.log4j.SizeBasedTriggeringPolicy">
            <param name="MaxFileSize" value="10MB"/>
        </triggeringPolicy>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d{yyyy-MM-dd
HH:mm:ss.SSS} [%p] %c - %m%n"/>
        </layout>
    </appender>
    <appender name="LatestErrorsFile"
class="org.apache.log4j.rolling.MartemRollingFileAppender">
        <param name="append" value="true"/>
        <param name="file" value="/var/local/telem/log/error.log"/>
        <param name="Threshold" value="ERROR"/>
        <param name="ImmediateFlush" value="false"/>
        <param name="BufferSize" value="8192"/>
        <param name="BufferedIO" value="true"/>
        <rollingPolicy
class="org.apache.log4j.rolling.FixedWindowRollingPolicy">
            <param name="FileNamePattern"
value="/var/local/telem/log/error.%i.log"/>
            <param name="MaxIndex" value="1"/>
        </rollingPolicy>
```

```
        <triggeringPolicy
class="org.apache.log4j.SizeBasedTriggeringPolicy">
            <param name="MaxFileSize" value="10KB"/>
        </triggeringPolicy>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d{yyyy-MM-dd
HH:mm:ss.SSS} %c - %m%n"/>
        </layout>
    </appender>
    <appender name="EventsCSV"
class="org.apache.log4j.rolling.MartemRollingFileAppender">
        <param name="append" value="true"/>
        <param name="Threshold" value="DEBUG"/>
        <param name="file" value="/var/local/telem/log/events.csv"/>
        <param name="ImmediateFlush" value="false"/>
        <param name="BufferSize" value="8192"/>
        <param name="BufferedIO" value="true"/>
        <rollingPolicy
class="org.apache.log4j.rolling.FixedWindowRollingPolicy">
            <param name="FileNamePattern"
value="/var/local/telem/log/events.%i.csv"/>
            <param name="MaxIndex" value="4"/>
        </rollingPolicy>
        <triggeringPolicy
class="org.apache.log4j.SizeBasedTriggeringPolicy">
            <param name="MaxFileSize" value="5MB"/>
        </triggeringPolicy>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d{yyyy-MM-dd
HH:mm:ss.SSS};%m%n"/>
        </layout>
    </appender>
    <appender name="syslog" class="org.apache.log4j.net.SyslogAppender">
        <param name="append" value="true"/>
        <param name="Threshold" value="INFO"/>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d{MMM dd HH:mm:ss}
telem-gw: [%p] %c - %m%n"/>
        </layout>
        <param name="SyslogHost" value="127.0.0.1"/>
    </appender>
    <appender name="GpsLog"
class="org.apache.log4j.rolling.MartemRollingFileAppender">
        <param name="append" value="true"/>
        <param name="file" value="/var/local/telem/log/gps.log"/>
        <param name="ImmediateFlush" value="false"/>
        <param name="BufferSize" value="8192"/>
        <param name="BufferedIO" value="true"/>
        <rollingPolicy
class="org.apache.log4j.rolling.FixedWindowRollingPolicy">
            <param name="FileNamePattern"
value="/var/local/telem/log/gps.%i.log"/>
```

```
            <param name="MaxIndex" value="1"/>
        </rollingPolicy>
        <triggeringPolicy
class="org.apache.log4j.SizeBasedTriggeringPolicy">
            <param name="MaxFileSize" value="300KB"/>
        </triggeringPolicy>
        <layout class="org.apache.log4j.PatternLayout">
            <param name="ConversionPattern" value="%d{yyyy-MM-dd
HH:mm:ss.SSS} [%p] %c - %m%n"/>
        </layout>
    </appender>
    <logger name="Gateway.Filter" additivity="false">
        <priority value="TRACE"/>
        <appender-ref ref="ConsoleFile"/>
    </logger>
    <logger name="Gateway.Formula" additivity="false">
        <priority value="TRACE"/>
        <appender-ref ref="ConsoleFile"/>
    </logger>
    <logger name="Gateway.HAL-gpio-fs" additivity="false">
        <priority value="OFF"/>
        <appender-ref ref="ConsoleFile"/>
    </logger>
    <logger name="Gateway.GWMIO" additivity="false">
        <priority value="TRACE"/>
        <appender-ref ref="ConsoleFile"/>
    </logger>
    <logger name="Gateway.Gps" additivity="false">
        <priority value="INFO"/>
        <appender-ref ref="GpsLog"/>
    </logger>
    <logger name="events_csv" additivity="false">
        <priority value="INFO"/>
        <appender-ref ref="EventsCSV"/>
    </logger>
    <logger name="Gateway.cmd" additivity="false">
        <priority value="INFO"/>
        <appender-ref ref="Console"/>
    </logger>
    <root>
        <priority value="TRACE"/>
        <appender-ref ref="LatestErrorsFile"/>
        <appender-ref ref="ConsoleFile"/>
        <!--<appender-ref ref="syslog"/>-->
    </root>
</log4j:configuration>
```