MARTEM
KAUGJUHTIMISSÜSTEEMID
TELECONTROL SYSTEMS

Configuration tool TELEM-GWS

User Manual

Martem AS
2018

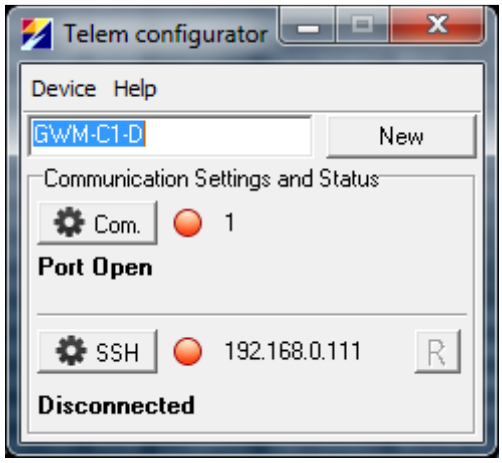
Contents

1 Introduction

Configuration tool Telem GWS is used to configure Telem devices. It is developed by Martem AS and is in constant development to keep up with latest functionality of Telem devices. Telem GWS is designed to be user friendly. Interface is similar to Microsoft Windows. Telem GWS is free of charge and the latest version can be downloaded from Martem AS homepage, or is provided by Martem AS.

2 Getting started

- GWS does not need any installation, to open program run downloaded .exe file.
- When program starts **Telem configurator** window is opened. Communication settings and Status shown on the **Telem configurator** window apply only if serial connection is used. Those parameters can be changed from **device -> Communication setup.**



- Serial connection can be used only with RTU-T modules and older Telem devices (RTA, RTA-A GW5, GW6). Communication between newer Telem devices (GWM, GW6-e) can be establish over ethernet and is described in the following chapters.
- To open default setup, device has to be chosen from the device menu. General configurations of the Telem devices can be chosen. When connection to the device is established, Telem GWS suggests to convert configuration to exact version of the device. It is also possible to define exact device type and convert configuration. It can be done by using convert to button on the upper right hand corner of device setup window.

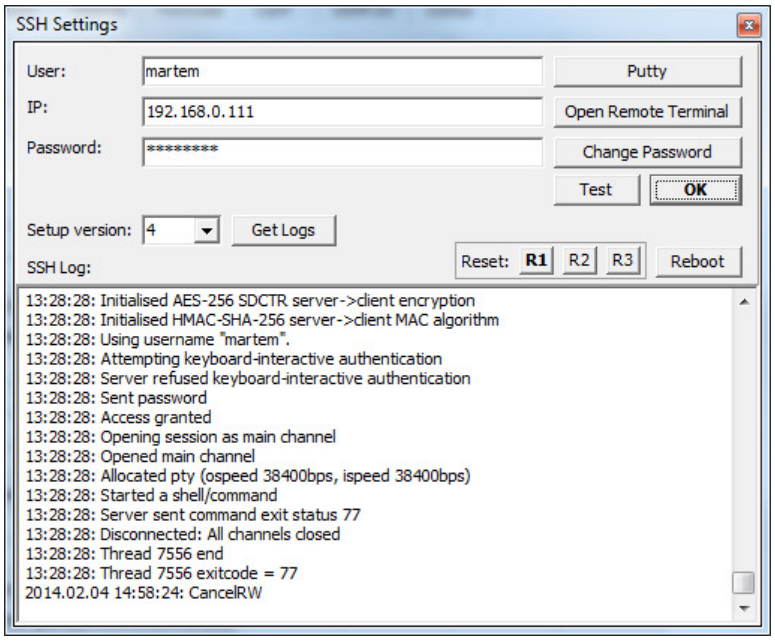
2.1 Connect with device using serial connection

- 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 corresponding parameters have to be set in the **Device-> Communication Setup.**
- **Network:** Define network to use connecting with Telem device
- **Port:** Com port of PC used for communication
- **GW6 USB interface:** Not supported
- **Parity:** Use of parity control bit (default: none)
- **Baud rate:** Data communication rate (9600)
- **Link Address:** link address of Telem device (1)
- **ASDU address:** ASDU address of Telem device (1)
- **Status:** Status of the connection. RED – no connection, GREEN – connection OK
- **Communication delay:** Delay between reception of data and the next query in milliseconds (0)
- **ASDU address length:** The length of the ASDU address in bytes: possible values are 1 or 2. (2)
- **Object address length** – Length in bytes. Possible values are 1, 2 or 3. (2)

2.2 Connect with device using Ethernet connection

- To establish connection with the device using Ethernet connection, device has to be chosen. When device is chosen, **Set** button opens SSH settings window, where communication parameters can be set. When parameters are set **Test** button should be clicked to conform the connection. When **Access granted** line appears, connection is OK and user can save parameters by cliking **OK. Red** light next to **SSH** setting in device setup window should turn **green.** Connection with the device is established. Then user can read (**R**) or write (**W**) configuration from/to device. **C** is for cancelling.
- Parameters in the SSH settings window:
- **User:** Username of the device (default: martem)
- **IP:** IP address of the device (default addresses are for ETH0: 192.168.0.111)
- **Password:** password of the device (default password is provided by Martem AS)
- **Setup version:** GW6-e and GWM support only version 4
- **Putty:** Opens remote terminal
- **Open Remote Terminal:** Opens remote terminal with log in parameters described in User, IP and Password string.
- **Change password:** Enables user to change device password

- **Test:** Test connection between PC and Telem device
- **OK:** Saves the parameters and closes window
- **Reboot:** Reboots the device
- **R1:** Reset the device
- **R2:** Reset and also clear memory buffers
- **R3:** Reset and restore the default setup



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.

3 File menu

New: Open new blank device setup
Open: Open configuration
Save: Save configuration
Save AS: Save configuration as new
Export: export configuration to .csv
Import: import configuration from .csv
Exit: exit program
disable_inGW_XMLGeneration: Should be selected

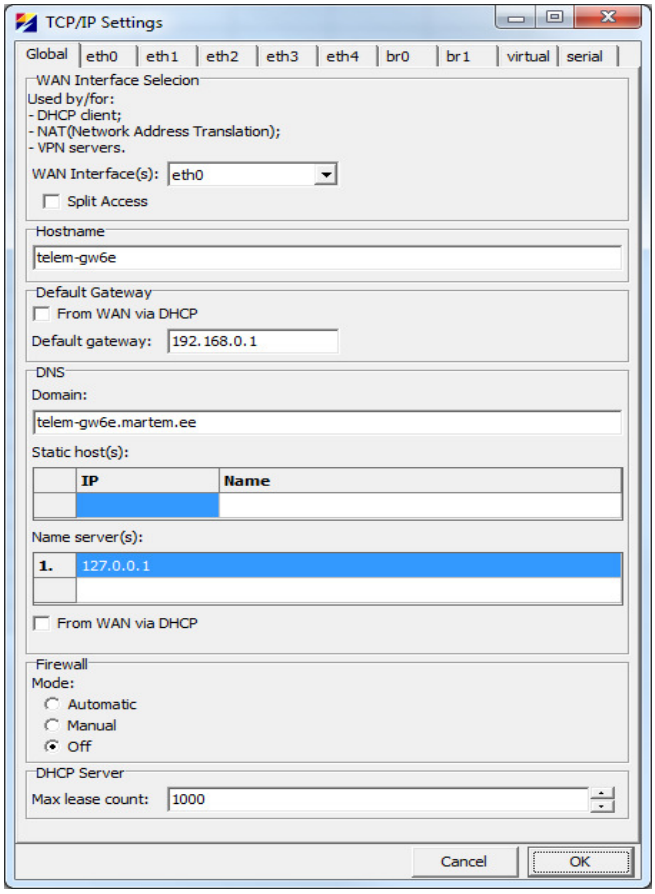
4 Common menu

4.1 SSH Settings:

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

4.2 TCP/IP Settings

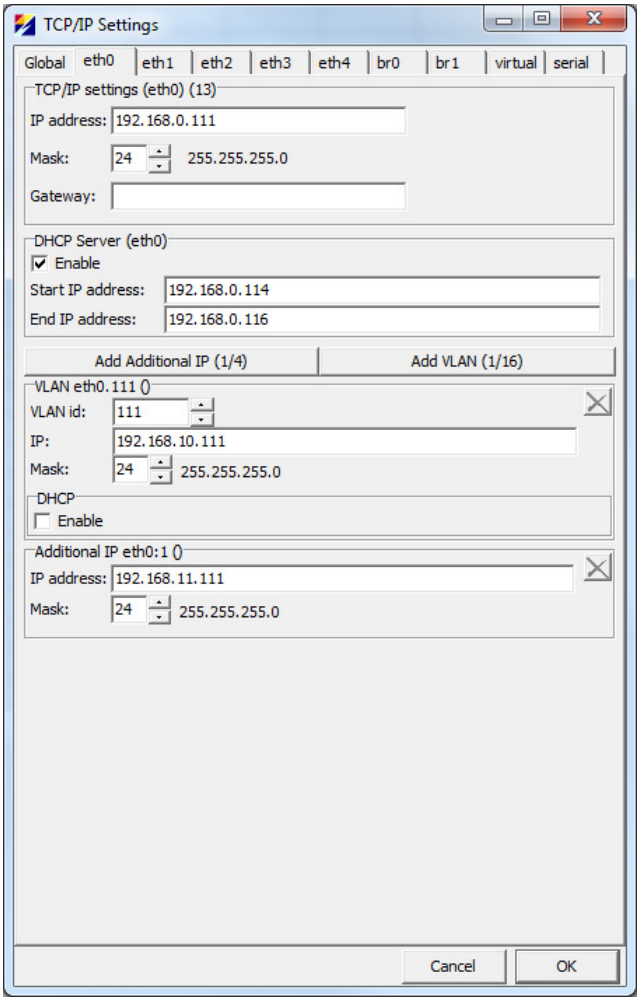
Used for determine TCP/IP communication paramaters and firewall functionality in Telem device



4.2.1 Global tab

In **Global** tab following parameters can be set:
WAN interface: Choose which interface is used for WAN connection
Hostname: Name of the device.
Default gateway: Default gateway of the device
DNS: Set DNS parameters.
Firewall: Set firewall parameters if necessary.
DHCP server: Define max lease count for DHCP server.

4.2.2 Eth0...EthX tab



Ethernet tabs have similar structure, each tab correspond to physical ethernet port on Telem device. There are different number of ethernet ports with different hardware. Each port can be configured with multi IP address and VLAN interfaces

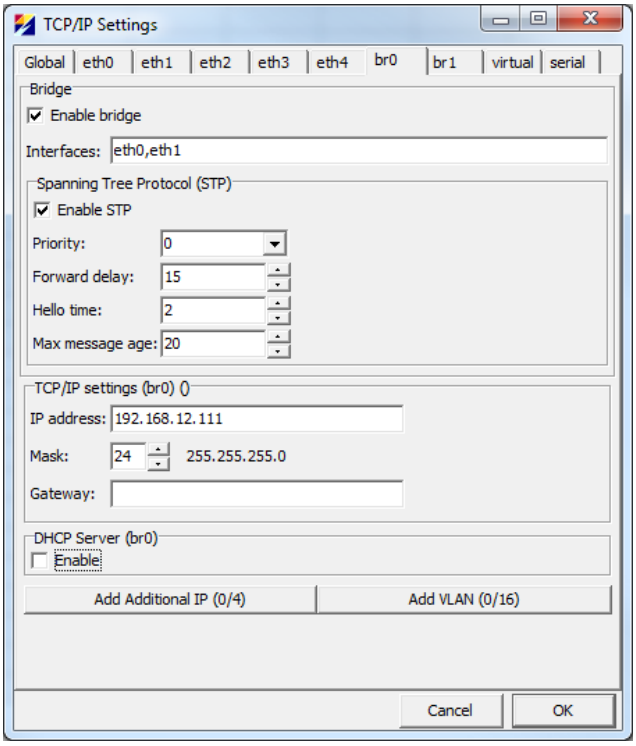
TCP/IP settings: define primary IP settings for current port. Ports using this interface are shown in the brackets. If split access in the Global tab is chosen then additional gateway to each interface can be chosen.

DHCP Server: enable DHCP server for current interface, define address range for current DHCP server.

Add additional IP: up to 4 additional IP addresses to each interface

Add VLAN: up to 16 tagged VLAN-s for each interface.

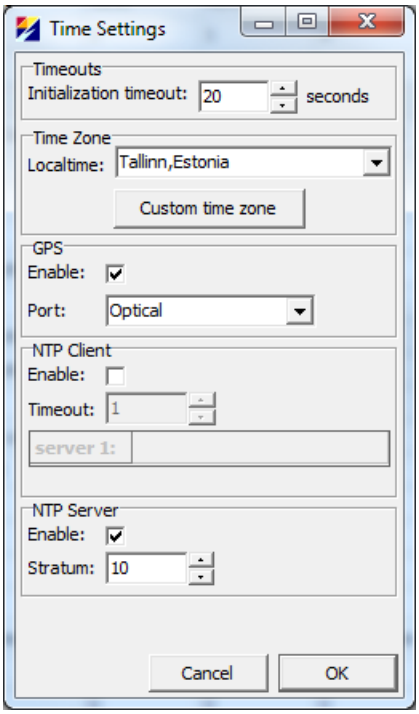
4.2.3 Br0/br1 tab



Combine two ethernet ports to work as a bridge.
Bridge: enable bridge, choose interfaces to use.
STP: enable STP protocol
TCP/IP settings: Define primary IP settings for current port.
DHCP Server: enable DHCP server for current interface, define address range for current DHCP server.
Add additional IP: up to 4 additional IP addresses to interface
Add VLAN: up to 16 tagged VLAN-s for interface.

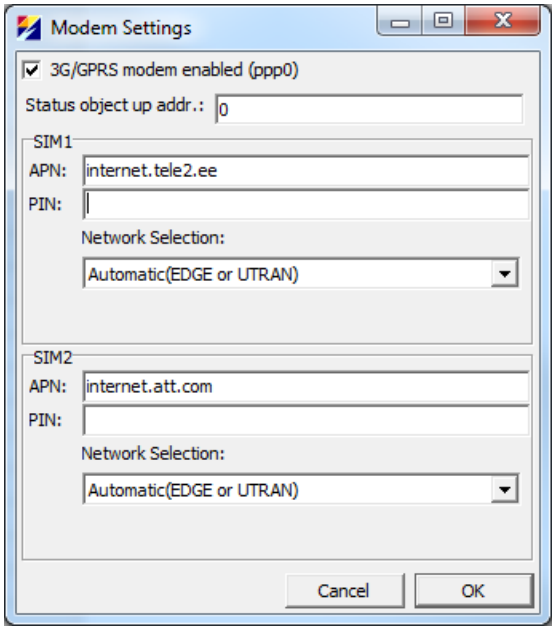
4.3 Time settings

Define different time parameters
Timeout: Communication timeout after device reboot, should be set higher than device setup time.
Time zone: Choose correct time zone, predefined in the drop down menu or define Your own.
GPS: Enable GPS time syncro, choose the connection type (with Telem GPS interface)
NTP Client: Choose server for NTP time syncronization
NTP Server: Define stratum for Telem device to work as NTP server.Time zone custamization
User can define custom time zone



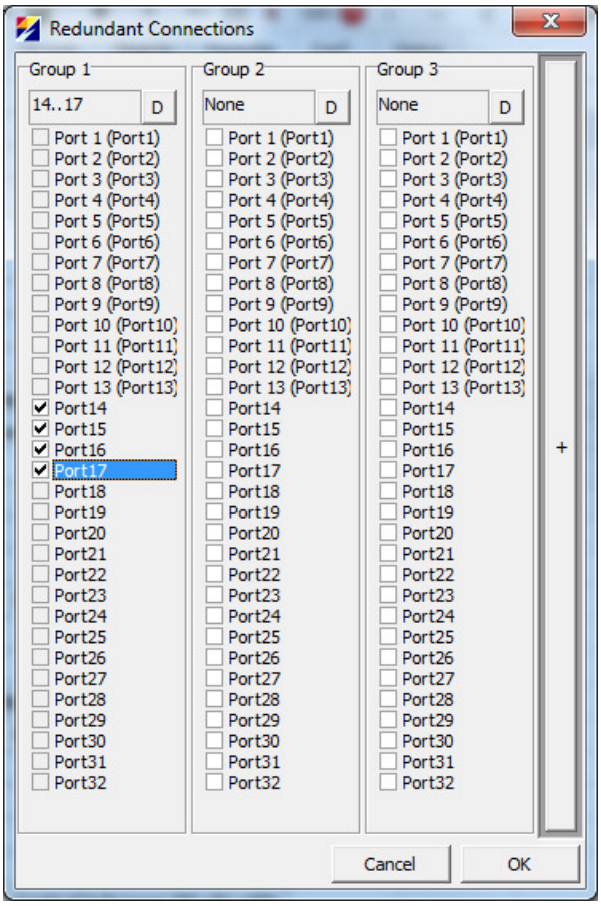
4.4 Modem Settings (Telem GWM)

Configure settings for 3G/GPRS modem.



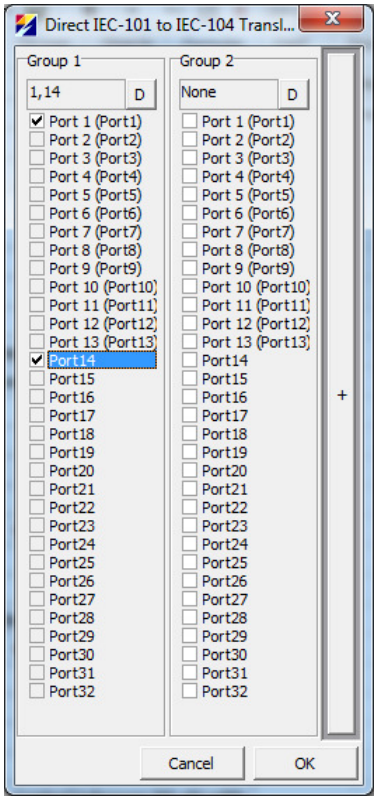
4.5 Reduntant connections

Define redundant connections. Connections use the same event buffer, event will be sent to only one channel. When one channel closes, automatically redundant channel is used.
Used for networks where SCADA system is reserved with many servers, event will be sent to only one server. Maximum number of ports in one reduntunt connection is 4
Choose ports to work as redundant.
D: Delete



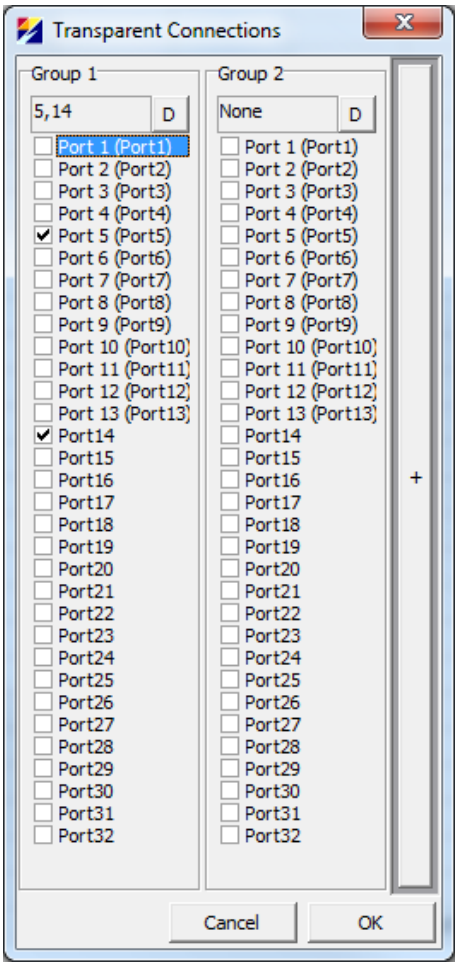
4.6 Direct IEC-101 to IEC-104 Translation

Determine groups of ports (up to 2 ports in each group) for direct protocol translation (without intermediate database) from IEC 60870-5-101 to IEC 60870-5-104 and vice versa. Lower lewel device still has to be configured to determine communication parameters: address, address length etc. Configuring lower lewel devices in described in the following chapters.



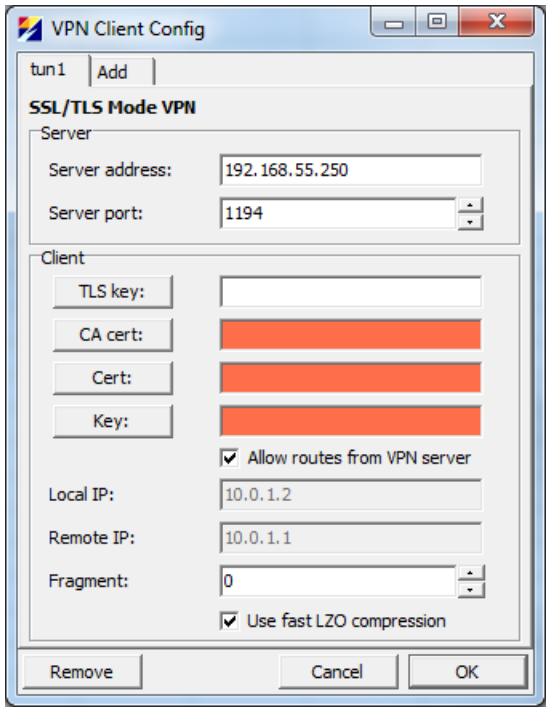
4.7 Transparent connections

Send information from one port to another without changing it.



4.8 OpenVPN

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.
Determine OpenVPN (virtual private networking) settings. Currently only 4 OpenVPN tunnels are supported
TLS key: SSL/TLS (Secure Socket Layer/Transport Layer Security) pre-shared key
CA cert: SSL/TLS root certificate. Same for all clients
Cert: client certificate
Key: client public key
Local IP:
Remote IP:
Fragment:
LZO:



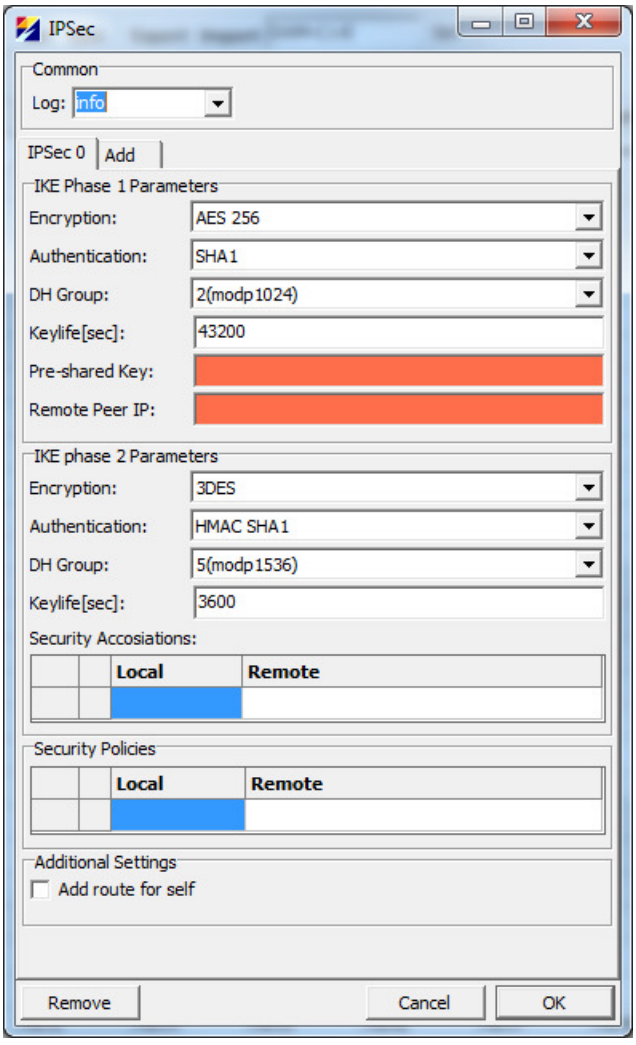
4.9 IPsec

For IPSec configuration IKE (Internet Key Exchange) Phase 1 is available next parameters:

- Encryption algorithms: DES, 3DES, Blowfish, AES 128, AES 256
- Authentication hash functions: MD5, SHA1, SHA2 (SHA 256, SHA 384, SHA 512)
- DH Groups- Diffie-Hellman algorithm: 1(modp768), 2(modp1024), 5(modp1536), 14(modp2048), 15(modp3072), 16(modp4096)

In box of IKE Phase 2 is available:

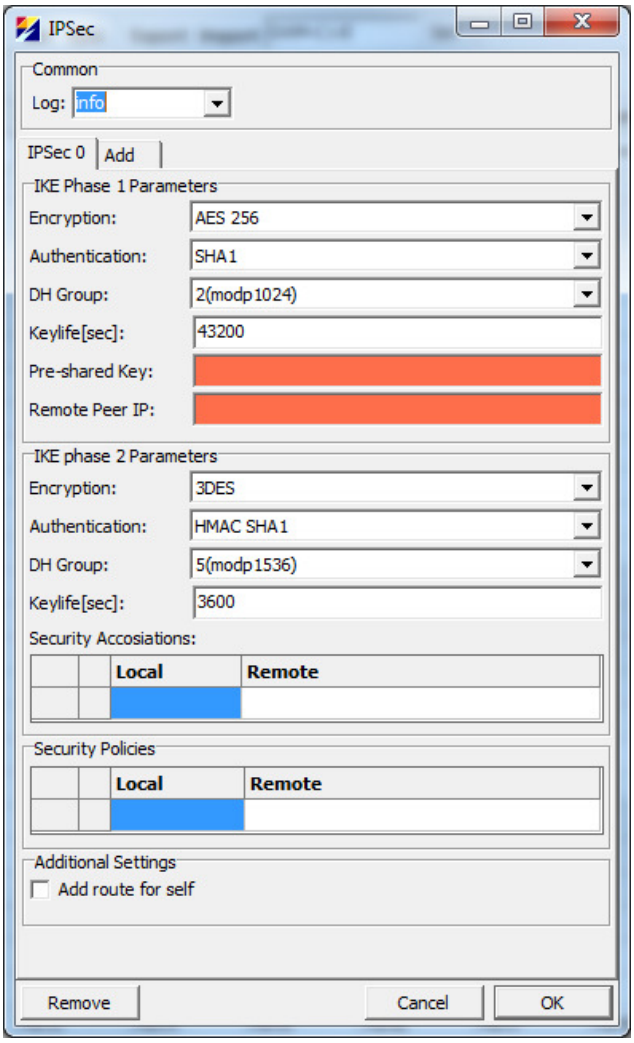
- Authentication hash functions: DES, 3DES, HMAC MD5, HMAC SHA1, HMAC SHA256[1], HMAC SHA384, HMAC SHA512



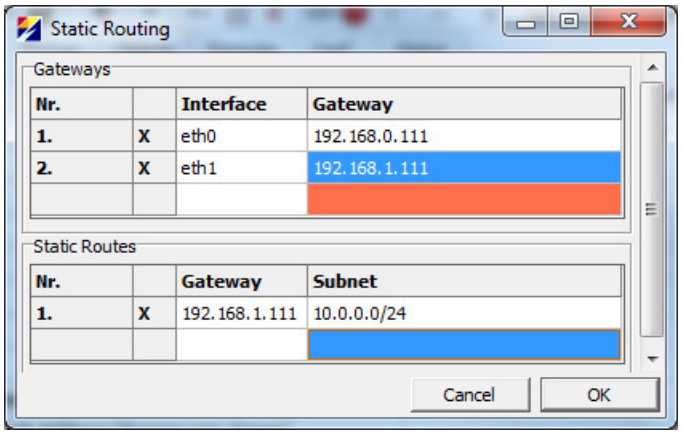
[1] HMAC SHA256 is nonstandard 96bit, latest standard uses 128bit version of HMAC SHA256

4.10 L2TP

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.

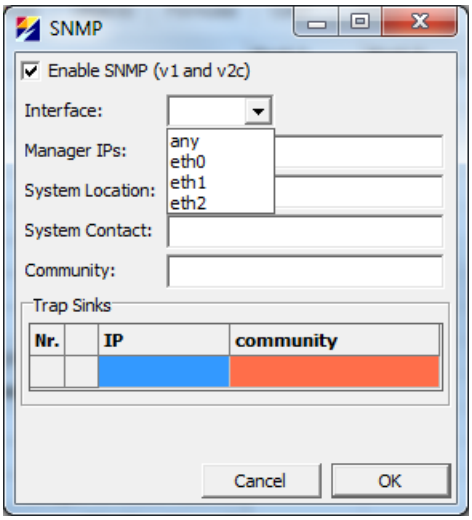


4.11 Static Routing



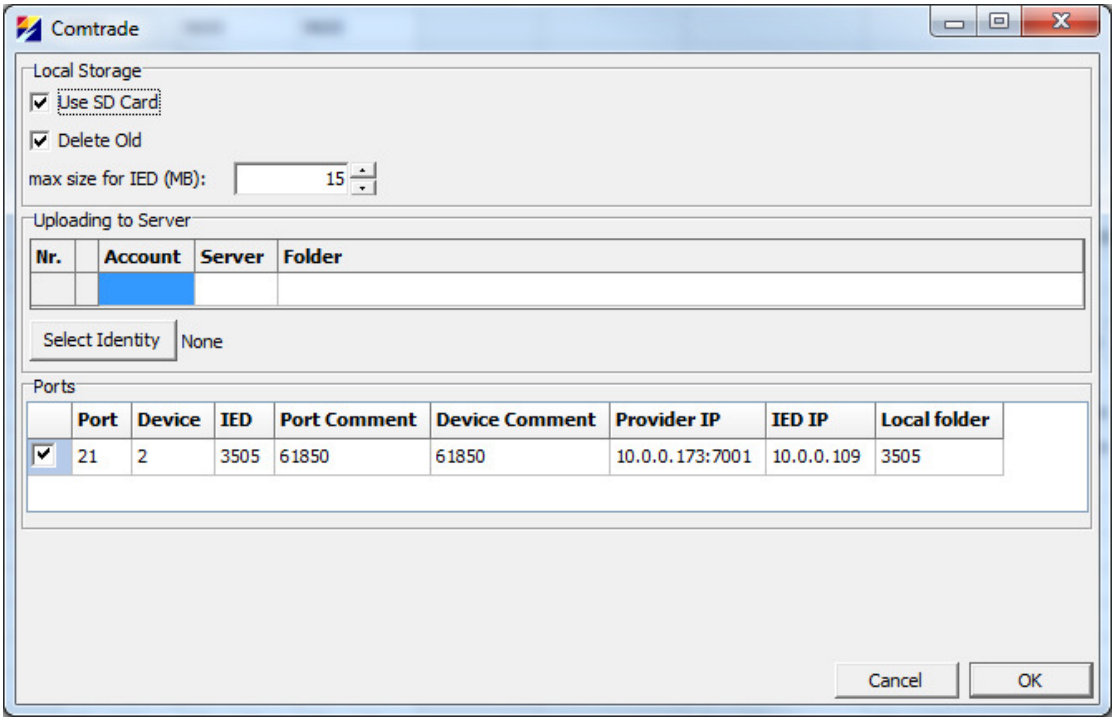
4.12 SNMP

Enable SNMP functionality, and set parameters.



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-GW6 internal memory or save on SD card.
TELEM-GW6 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 Options

Used for changing general options of GWS. In general no modifications needed

5 Configuring data concentrator

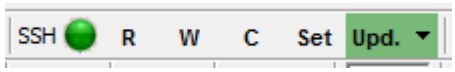
Parameters described in the previous chapters were mainly about, how to setup network connection and overall settings of the device. In this chapter data concentrator functionality of Telem Devices is described.

5.1 Shortcut icons

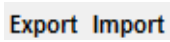
New: Open new default configuration
Open: Open saved configuration
Save: Save configuration

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

PLC: Configure ormulas using plc logic (described in the following chapters)
ICD/SCD: Import IEC61850 ICD/SCD file (described in the following chapters)



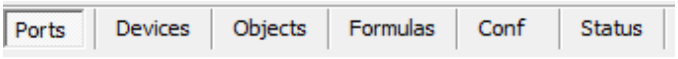
R: No function
SSH Settings:
R: Read configuration from device
W: Write configuration to device
C: Cancel procedure
Set: Set SSH parameters (described in previous chapters)
Upd.: Update firmware, (see chapter 6)



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



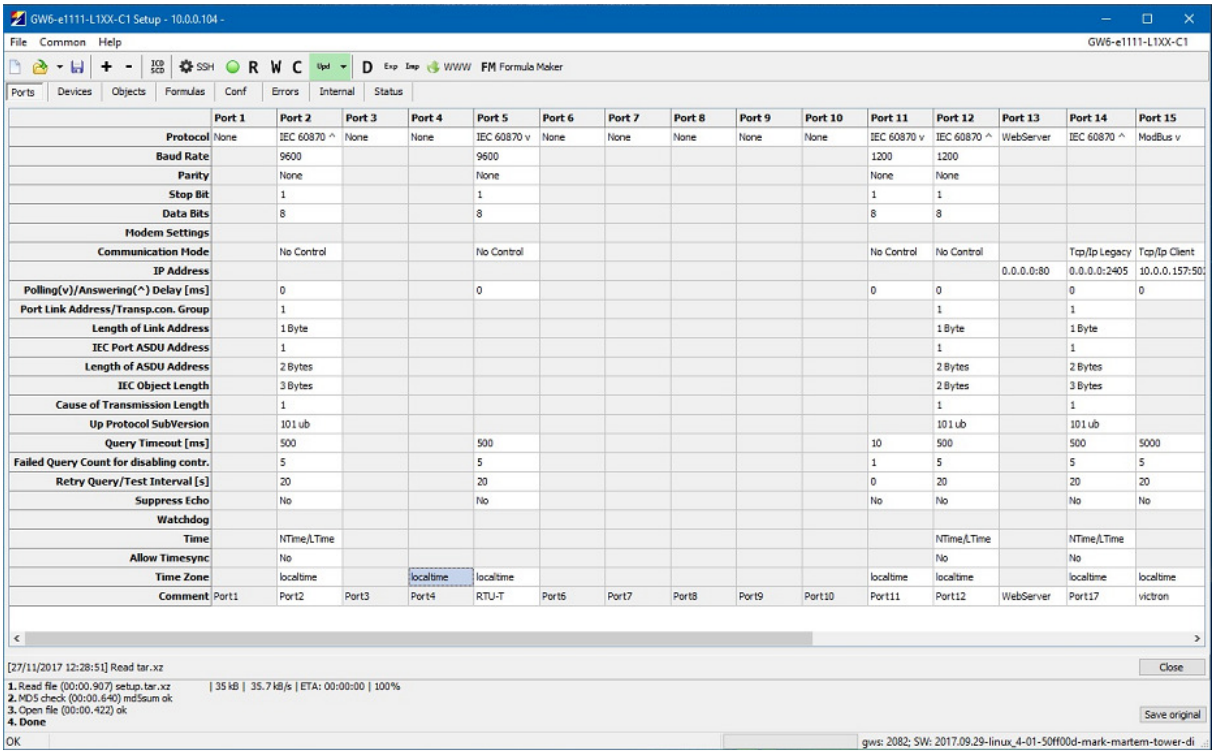
Most of the data concentrator parameters have to be set in the tab cards. In this chapter functionality and purpose of each tab card is described.

5.2.1 Ports Tab Card

Each communication port has its own parameters. Depending on the hardware, first ports in line are always physical serial ports and following them are TCP/IP ports using physical Ethernet ports number of ethernet ports user can choose also depends on hardware.

One communication port can be used by many devices, selection which port is used by each device is done in **devices** tab card, under device **port** selection.

Protocol: Communication protocol used by all the devices that toconfigured this port. Each protocol name is accompanied with a symbol "**^**" or "v" which indicates whether the port is used for an uplink or a downlink channel. For example, "Modbus v" means that this port is used for downlink with Modbus protocol.



	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15
Protocol	None	IEC 60870 ^	None	None	IEC 60870 v	None	None	None	None	None	IEC 60870 v	IEC 60870 ^	WebServer	IEC 60870 ^	ModBus v
Baud Rate		9600			9600						1200	1200			
Parity		None			None						None	None			
Stop Bit		1			1						1	1			
Data Bits		8			8						8	8			
Modem Settings															
Communication Mode		No Control			No Control						No Control	No Control		Tcp/Ip Legacy	Tcp/Ip Client
IP Address													0.0.0.0:80	0.0.0.0:2405	10.0.0.157:50
Polling(v)/Answering(^) Delay [ms]		0			0						0	0		0	0
Port Link Address/Transp.con. Group		1										1		1	
Length of Link Address		1 Byte										1 Byte		1 Byte	
IEC Port ASDU Address		1										1		1	
Length of ASDU Address		2 Bytes										2 Bytes		2 Bytes	
IEC Object Length		3 Bytes										2 Bytes		3 Bytes	
Cause of Transmission Length		1										1		1	
Up Protocol SubVersion		101 ub										101 ub		101 ub	
Query Timeout [ms]		500			500						10	500		500	5000
Failed Query Count for disabling contr.		5			5						1	5		5	5
Retry Query/Test Interval [s]		20			20						0	20		20	20
Suppress Echo		No			No						No	No		No	No
Watchdog															
Time		NTime/LTime										NTime/LTime		NTime/LTime	
Allow Timesync		No										No		No	
Time Zone		localtime		localtime	localtime						localtime	localtime		localtime	localtime
Comment	Port1	Port2	Port3	Port4	RTU-T	Port6	Port7	Port8	Port9	Port10	Port11	Port12	WebServer	Port17	victron

Baud rate: Data communication rate
Parity: Use of parity bit for all the devices on this channel
Stop Bit: possible values are 1, 2
Data Bits: possible values are 7, 8

Modem Settings: GPRS modem connection check period (if **GPRS modem** is chosen as **protocol**)
Communication Mode: Makes it possible to choose between the following handshaking options:
1 - No control
2 - TCP/IP Legacy
3 - TCP/IP Client
0 - TCP/IP Server
IP address – communication IP address (used if **Communication Mode** is set to TCP/IP)

IEC ^ or IEC v

Other's side IP Address: an address of the device which can connect with Telem device using corresponding port e.g. SCADA server (if set to 0.0.0.0 – all devices can connect)

Interface: Choose which Ethernet interface ise used in current port

Port: Available network communication port (in case of IEC 60870-5-104 protocol, port 2404 is recommended)

61850 v

IED IP Address: an IP address of the 61850 device (server) 102 – (RFC 1006) IEC 61850 port of ISO Transport on top of TCP

Interface: Choose which Ethernet interface ise used in current port

Provider Port:TCP port of IEC 61850 provider, port 7001 is recommended, in each network segment different port number has to be used

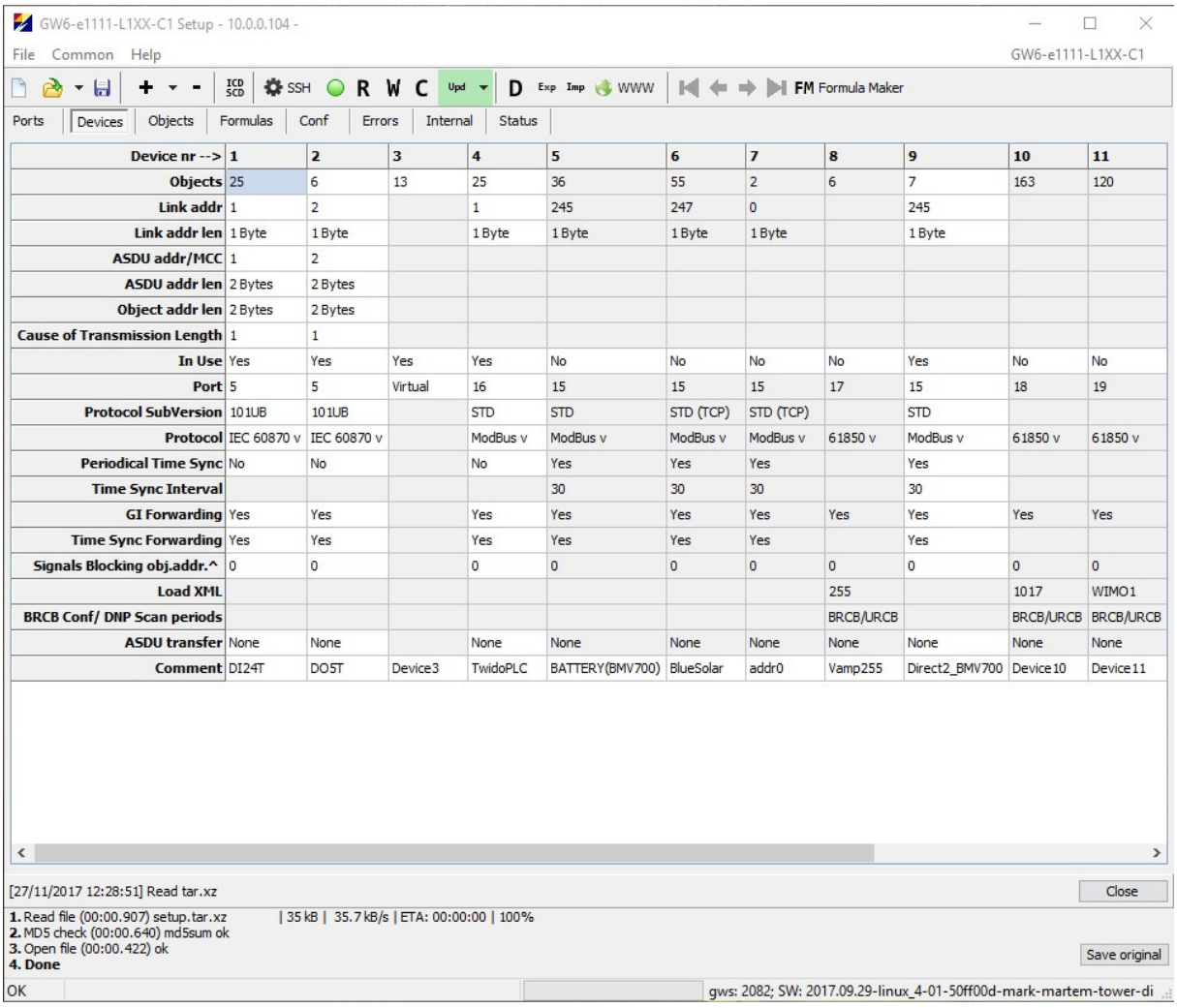
GPRS settings: for GPRS modem ID detection from TDC/IEC software

Polling(v)/Answering(^) Delay [ms]: Delay between reception and the next query
Port Link Address/Transp.con.Group: Link address of the device on uplink channels
Length of Link Address: Length of the link address in bytes on uplink channels. Possible values are 1 or 2
IEC Port ASDU Address: ASDU address on uplink channels
Length of ASDU Address: Length of the ASDU address in bytes on uplink channels. Typically 2, possible values are 1 or 2
IEC Object Length: Length of the IEC object address in bytes on uplink channels. Typically 3, possible values are 1, 2 and 3
Up Protocol SubVersion: Number of protocol subversion on uplink channels
Query Timeout [ms]: Query timeout for devices on downlink channels
Failed Query Count for disabling contr.: Count of timeouts after which the error flag is raised and the query of this device temporarily suspended
Retry Query/Test Interval [s]: Time period after which the suspended device is queried again

Suppress Echo: If the sent messages are echoed back by the connected devices then they need to be suppressed
Replace Event hrs: Yes/No. If Yes, events are sent to control centre with UCT time (the time correction value is set in Common Menu, Timing Settings)
Time: Determines the time tag of events
Allow Timesync: Yes or No
Time Zone: Determines time zone, localtime or Tallinn, Estonia, or UTC
Comment: useful field for comments of port property

5.2.2 Devices Tab Card

Devices tab card is used to define each lower lewel device communication parameters.



Device nr -->	1	2	3	4	5	6	7	8	9	10	11
Objects	25	6	13	25	36	55	2	6	7	163	120
Link addr	1	2		1	245	247	0		245		
Link addr len	1 Byte	1 Byte		1 Byte	1 Byte	1 Byte	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	Yes	Yes	No	No	No	No	Yes	No	No
Port	5	5	Virtual	16	15	15	15	17	15	18	19
Protocol SubVersion	101UB	101UB		STD	STD	STD (TCP)	STD (TCP)		STD		
Protocol	IEC 60870 v	IEC 60870 v		ModBus v	ModBus v	ModBus v	ModBus v	61850 v	ModBus v	61850 v	61850 v
Periodical Time Sync	No	No		No	Yes	Yes	Yes		Yes		
Time Sync Interval					30	30	30		30		
GI Forwarding	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time Sync Forwarding	Yes	Yes		Yes	Yes	Yes	Yes		Yes		
Signals Blocking obj.addr.^	0	0		0	0	0	0	0	0	0	0
Load XML								255		1017	WIMO1
BRCB Conf/ DNP Scan periods								BRCB/URCB		BRCB/URCB	BRCB/URCB
ASDU transfer	None	None		None	None	None	None	None	None	None	None
Comment	DI24T	DO5T	Device3	TwidoPLC	BATTERY(BMV700)	BlueSolar	addr0	Vamp255	Direct2_BMV700	Device10	Device11

Device no: Sequence number of the device (generates automatically)
Objects: Number of objects in the device (generates automatically)
Link address: Link address of the connected device

ASDU address: ASDU address of the connected device
ASDU address len: Length in bytes, possible values are 1 or 2
Object address len: Length in bytes, possible values are 1, 2 or 3
In use: Indicates whether the device is in use or not. If the device is not in use, the whole row has a grey background
Port: Port no. of Telem device to which the device is connected
Protocol SubVersion: Define Sub version of the protocol
Protocol: For information only. It is filled automatically according to the number of the used port, and protocol configured in current port..
Periodical Time Sync: Yes/No. If Yes, time synchronisation is sent to device by Telem GW
Time Sync Interval: interval when time synchronisation is sent to device.
GI Forwarding: Yes/No. General interrogation forwarding
Time Sync Forwarding: Yes/No. If Yes, the time synchronisation which is received from upper channel, it is forwarded to the device
Signals blocking obj. addr.^: The address of an object which determines blocking of all signals from that device. No signals are sent to control centre from that device.
*the object must be determined under a virtual device in objects table
Load XML: Load XML file with object data to the device (IEC 61850)
BRCB Conf: Buffered report control block configuration
Comment: Description of devices
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. Choose **creat template** and the parameters used in the template. 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.

Load XML / IEC 61850
Load XML is used with IEC 61850 protocol. To generate ICD file again, more information about that in following chapters.
BRCB conf
Used to define RCB-s, and data sets in IEC61850 configuration more about that in following chapters.

5.2.3 Objects Tab Card

Objects tab card is used to define all parameters of I/O points. Each device as its own object list. 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^ – Object’s subtype for uplink.

DI digital input	Single
	Double
AI Analog input	Normalized
	Floating point
	Step position
CN Counter	-
DO digital output	Same as **Sub Type v**
AO analog output	Normalized
	Scaled
	Floating point
DO_FN	-

Sub Type v – Object's subtype for downlink.

DI digital input	Normal
	Fallback
AI Analog input	-
CN Counter	-
DO digital output	Single Direct Execute
	Single Select Execute
	Double Direct Execute
	Double Select Execute
	Inherited
	No additional definition
	Short pulse duration
	Long Pulse duration
	Persistent Output
AO analog output	Single Direct Execute
	Single Select Execute
	Double Direct Execute
	Double Select Execute
	Inherited
	No additional definition
	Short pulse duration
	Long Pulse duration
	Persistent Output
DO_FN	GI Parameter
	0 - Global GI (default)
	1…15 - GI Groups
	Reset process
	1 - reset
	2 - reset + clear buffers

Invert: Object's value will be inverted
Fn.code: Function code on the IEC 60870-5-103 protocol
Info no: Information number on the IEC 60870-5-103 protocol
Index: Object index on the IEC 60870-5-103 protocol.
It indicates the order number of the object in message types 3 and 9 of analog measurements. In IEC 60850 it is used to match "Integer and Enum Values" for example AutoRecSt="Successful" index should be 3.
Object.Addr: Object's downlink address e.g. IEC101, Modbus protocol
61850 v: 61850 address (loaded from device's XML file), can be modified manually.
Object.Addr ^: Object's uplink address

It is possible to send the same object to control centre with different addresses by creating several object with identical downlink addresses and different uplink addresses.
Comment: comments of devices
DB %Fs: Deadband (% of full scale, Outp.max-Outp.min).
If the value has changed less than the deadband then it is not spontaneously transferred.
DB2 %Fs: Zero Zone Deadband, if measurement value is less than given deadband it is considered as 0.
Inp. Min, Inp. Max: Minimum and maximum values of analog measurement (before scaling). Necessary when value scaling is needed. (floating point to normalized)
Outp. Min, Outp. Max: Minimum and maximum values of analog measurement. Necessary when value scaling is needed. (normalized to floating point)
Forb. Ports ^: Uplink port to which the object's value transfer is blocked.
To select uplink ports, which should not be used for transferring these object values, double-click on the cell of the **Forb. Ports^** column and select the corresponding ports from the window that has appeared.
On Ev. No; Off Ev. No: Corresponding event number used in SPA-bus
Ch. No.: Channel no. for SPA-bus communication protocol
NoFlags: If set to Yes, removes Invalid and Not Topical flags from object status. Used for objects, which statuses are not received with General Interval time (short circuit current, fault distance etc.)
NoCsvLog: If set to Yes, does not save values to csv log. (events.csv)
NoMainLog: If set to Yes, does not save values to main log. (console.log)
Last to parameters are used to keep log files clear and save less amount of unnecessary info.

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 a 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.

• Lower lewel object can have multiple **Object.Addr ^**, duplicate object parameters and add new **Object.Addr ^**

5.2.4 Formulas Tab Card

Formulas are used quite often to group some signals, to control many objects with one command or do to some other logic.

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 string

Comment: Comment of the formula

DO/AO addr.: Address of the object controlled by formula.

Execution count: The number of control operations executed.

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, otherwise change in the formula is necessary for control command.

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 address up.** Example: @101 points to the value of the object with an address to uplink 101.

Constants

Constants can be used in formulas. Example: 1.1+2.2+3.0 consists of 3 floating point constants. Analog constants should have at least one place after comma. (e.g. 1.0)

Brackets

Brackets should be used in formulas to change the priority of the operation. Example: sqrt(@101/2+@102); (@201+@202+@203)/3

Oper.	Obj. type	Description	Sample	Priority*
and	DI	Logical conjunction	@201and@202	5
or	DI	Logical disjunction	@201or@202	6
xor	DI	Exclusive disjunction	@201xor@202	6
not	DI	Logical negation	not@201	0
dbl	DI	Converts 2 single digital inputs into a double signal	@202dbl@201,where @202 – ON state signal @201 – OFF state signal	7
+	AI/CN	Addition	@101+3,2	3
-	AI/CN	Subtraction	@101-0,49	3
*	AI/CN	Multiplication	@101*2	2
/	AI/CN	Division	@101/2	2
^	AI/CN	Exponentiation	@101^2	1
<	AI/CN	Greater than	@101<0,499	4
>	AI/CN	Less than	@101>0,5	4
sqr	AI/CN	Square	sqr(@101*10)	0
sqrt	AI/CN	Square route	sqrt(@101*10)	0
sin	AI/CN		sin@301	0
cos	AI/CN		cos@301	0
tan	AI/CN		tan@301	0
arcsin	AI/CN		arcsin@301	0
arccos	AI/CN		arccos@301	0
arctan	AI/CN		arctan@301	0

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

- By clicking on the „+“ button, a new formula row with default settings is added.
- By clicking on the button „-“ , the selected formula row is removed.

Formula rows can also be added, removed or cleared 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 formulas

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

Telem GW has the possibility to create formulas using PLC functionality. For enabling the PLC functionality, two folders: ActivePLC and plcEditor (provided by Martem AS) have to be copied to the same location as configuration tool GWS.

Using PLC or editing formulas

- Open configuration window and click on PLC button. PLC configuration window opens.
- Double click on **Main** button in the upper left hand corner to open PLC configuration window. When main window is opened, user can choose logical function and variables. When PLC window is closed, logic functions are exported to formulas tab.

Another method or creating and changing formulas is to use Formula Maker (provided by Martem AS).

To use formula maker or editing formulas configuration has to be exported to .csv file format.

For opening or saving .csv file in formula maker choose:

- system>GWs
- file>open

Saved .csv file has to be opened with Formula Maker.

Note: PLC function changes only formula line, other parameters in the formula tab card such as Type, subtype etc. have to be changed in the GWS.

5.2.5 Conf tab card

NB! The contents inside this tab should be modified only by advanced **Linux users.** Commonly this tab is used for controlling purposes.

dns.conf

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

hostname

Synopsis: */etc/hostname* – node name

resolv.conf

Synopsis: */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.

hosts

Synopsis: /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

Synopsis: */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.

ntpd

Synopsis: */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).

S40network
Synopsis*: /etc/init.d/S40network* – script will configure network interfaces, VLAN's and routes
network_eth1 and network_eth2
Synopsis: */etc/init.d/network_eth1* and */etc/init.d/network_eth2* – script will configure network interfaces, VLAN's and routes
S39iptables
Synopsis: */etc/init.d/S39iptables* – script will configure network interfaces, VLAN's and routes
log-conf.xml
Synopsis: /usr*/local/etc/telem/log-conf.xml* – xml-file, which contains cumulative data of configuration stages
gwpinger.conf
comtrade.conf
comtradessh.conf
comtraded
comtrade_id
crontab
syslogd
Synopsis: */etc/default/syslogd* - file, which contains cumulative data of devices connections to the other devices
snmpd.conf
update.conf
telem-gps.conf
TZ
Synopsis: */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 More information about TZ: http://www.sonoracomm.com/support/20-voice-support/107-uclibc-tz
sim1_chat and sim2_chat (old)
Applies only on Telem-GWM!
Synopsis: */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)
Applies only on Telem-GWM!
Synopsis: */etc/ppp/peers/VMX53/sim1_chat* – for first SIM card (based on the new CPU i.MX53)

ssh_config

Synopsis: */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

Synopsis*: /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.

IPSec configuration

For IPSec configuration IKE (Internet Key Exchange) Phase 1 is available next parameters :

- Encryption algorithms: DES, 3DES, Blowfish, AES 128, AES 256
- Authentication hash functions: MD5, SHA1, SHA2 (SHA 256, SHA 384, SHA 512)
- DH Groups- Diffie-Hellman algorithm: 1(modp768), 2(modp1024), 5(modp1536), 14(modp2048), 15(modp3072), 16(modp4096) In box of IKE Phase 2 is available:
- Authentication hash functions: DES, 3DES, HMAC MD5, HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512

PPP

cdma_chat
options
chap-secrests-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.

5.2.6 Errors Tab Card

Possible errors found in the configuration are described in this tab. When writining configuration to device 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.

5.2.7 Status Tab Card

Status tab card presents the information of the device connected, its configuration and configuration histroy.

6 Configuration advices

6.1 Configuration of connected Telem RTU I/O modules remotely 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-> GW6/RTA-A conf. redirection.**
- 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-A is connected to GW6 (RTU) serial port as sub-RTU (one collects data from another), then the configuration of RTA-A can be remotely read and written through the GW6 using the configuration program.

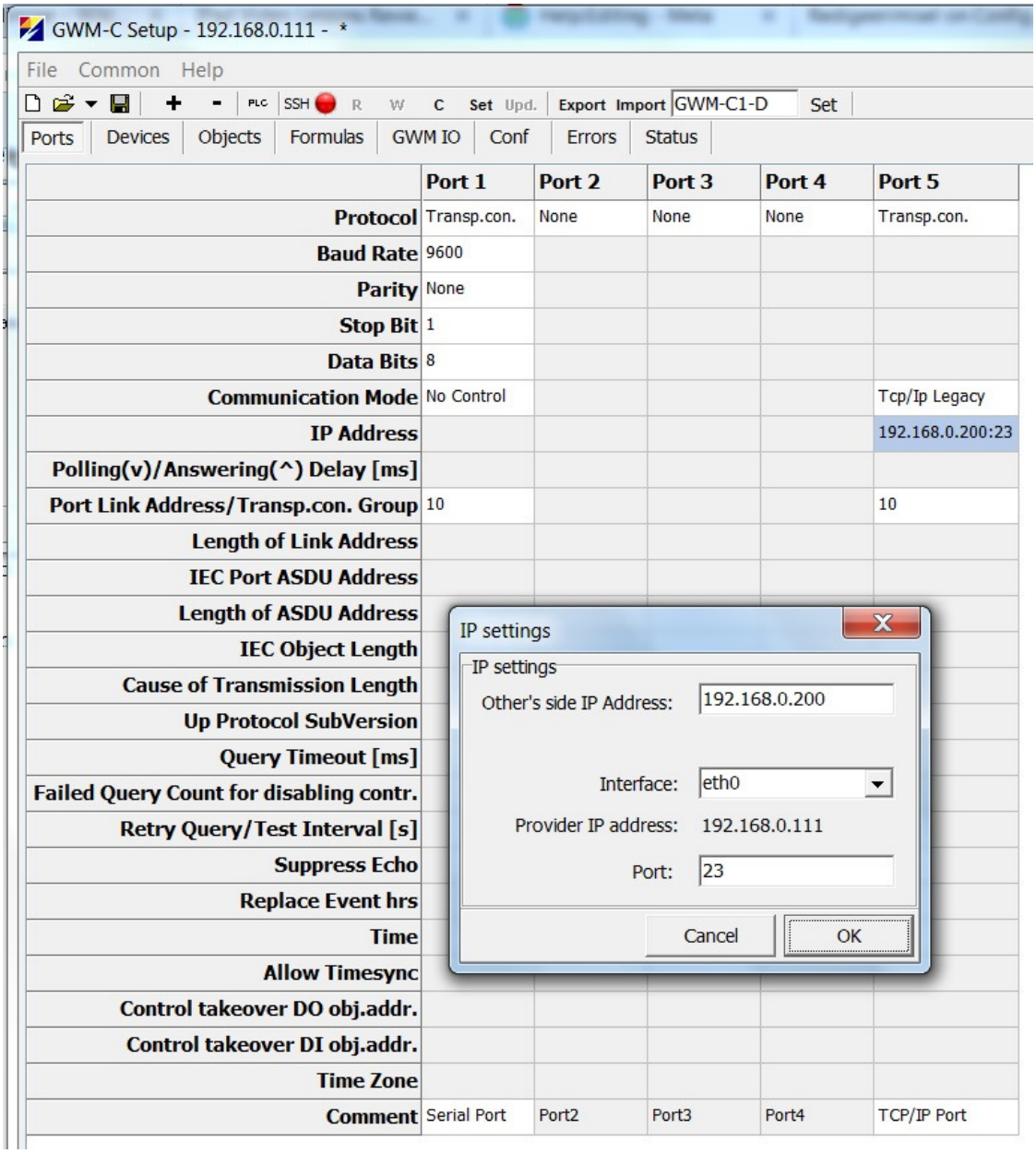
6.2 Remote management of other serial devices

It is possible to use TELEM data concentrators as RS-232/422/485 terminal to Ethernet server for remote management purposes of other devices. Transparent connection should be used in the configuration.

Transparent Connections is a feature to transfer raw data between two ports. Hence the term "transparent connection".
For example, transparent connections may be used as a serial-to-ethernet converter for devices with serial communication interface. This way, the device could be remotely configured via serial-to-ethernet connection.
Transparent connections enables transferring data in the following configurations:

- serial to serial
- serial to TCP/IP and
- TCP/IP to serial
- TCP/IP to TCP/IP (i.e port forwarding)

Here is an example configuration of Transparent connections:



There is a configuration for serial to TCP/IP transparent connection. (Serial-to-Ethernet converter).

Port5 is configured as TCP/IP port of the transparent connection.

Note the parameter "Transp. con. group" (in this case, it is 10).

This parameter is used to identify the two transparent ports that belong to the same connection group. If another pair of transparent connections is needed, create two more transparent ports and pair them together with the "Transp. con. group" parameter. Obviously, the second pair of transparent connections requires another value for the "Transp. con. group" parameter (in this case, some value other than 10).

Incoming TCP/IP connection is accepted from TCP port 23.

Access is limited to client IP 192.168.0.200

If this limitation is not needed, configure the "Other side address" as 0.0.0.0

In this example, all the data that is sent to server @ 192.168.0.111, tcp port 23 by client 192.168.0.200 is sent to serial line (Port1) @ 9600 baud, 8N1

6.3 Configuring IEC 61850 devices

IEC61850 tends to be most common communication protocol in substations. Telem-GW6 supports IEC61850 protocol and configuring it has been made simple in GWS. Following chapter describes configuring of IEC61850 device step by step.

Import ICD/SCD
Click on **ICD/SCD** shortcut. Load ICD/SCD window opens. Click on **select** to choose the ICD/SCD file You want to use. Also check **Create devices and objects**. Click **OK**

As You can see most of the neccessary information is filled automatically.

- Port configuration with correct IP parameters (Port tab card)
- devices configuration (devices tab card)
- objects configuration, with lower lewel aadresses. (objects tab card)

To get the system working only upper level addresses are needed.
In most cases user wants to modify the configuration to make it more handy or use more options. It is possible to remove/add/change 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. Best way to update that file also in GWS is to use **ICD/SCD** shourtcut again, but this time uncheck **Create devices and objects.** Then the file is imported to configuration but not yet used.
User can choose which file and which IED is used for each devices objects. Click on the **Load XML** box on the device configuration You want to change. Choose the file and the IED and also check **Create objects** to load objects again. When this is done user can view from O**bjects** tab card which object where found new (green- added to object list), old (yellow-not changed), missing (red - will be deleted).

Define RCB and Dataset, Dynamic dataset
If user needs to define RCB and dataset it is possible to to that. User should click on the **BRCB conf**. box. Then **BRCB Conf.** window is opened. User can choose BRCB 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-GW6 creates dataset with the name user has defined and with the objects defined in the **object 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.

6.4 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.

6.5 Status log

Detected status changes and errors are stored in text files 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

6.6 Events archiving

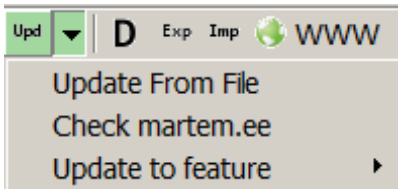
Console log files, events and errors are collected and archived in the form of text files and are physically saved to device’s flash memory. By default, each log file have size at 5 MB. Events log will be updated only if any events occur. If no events are detected, nothing will be written to events text 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 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.
4. Use FTP client (e.g. WinSCP), download files from the device. Log files location: root/var/log/telem/

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 GWS **Status** tab

8 Security considerations

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:

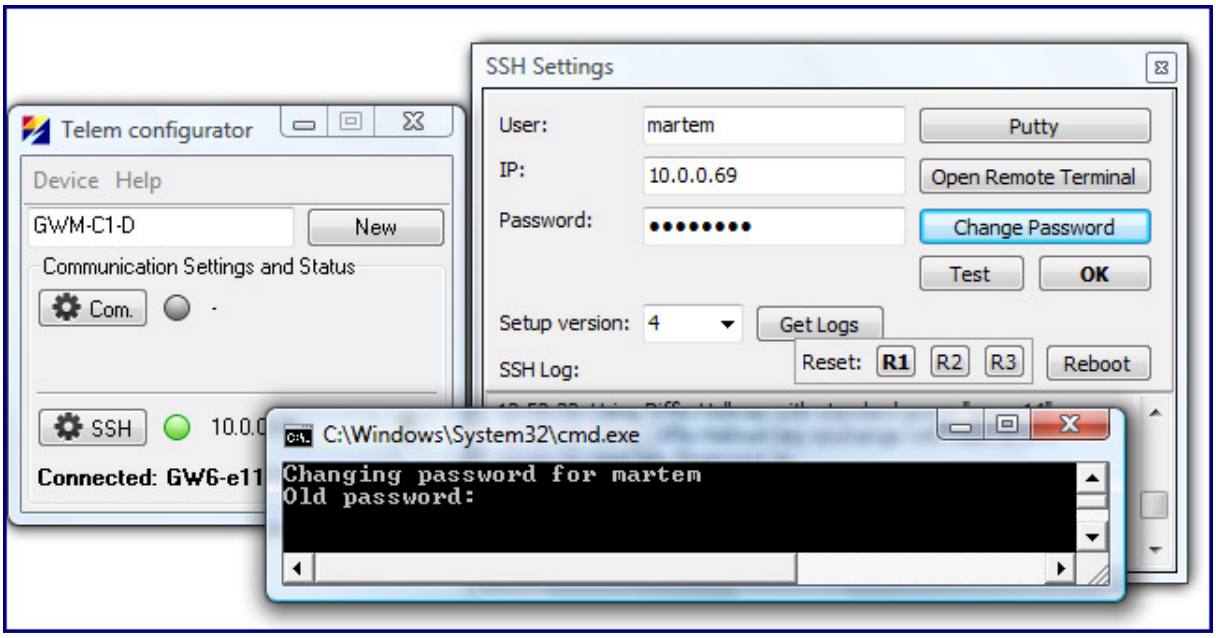
- Strong user access password policy
- SSH access restriction via firewall

- 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 GWS.exe 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:

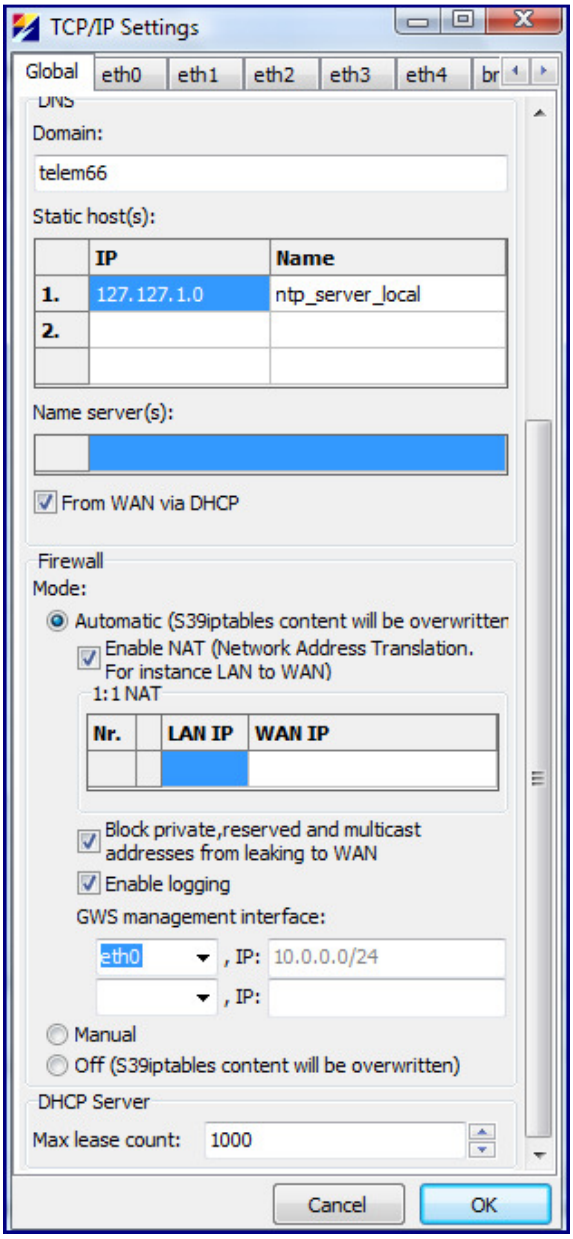
- Open GWS.exe
- Connect to the device, press „SSH" button, press „Change password"
- In appeared window type old and new passwords for user „martem"
- Bad password example: 123456qwer. Good password example: PYZn?<jH,g%Y)5Gn



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

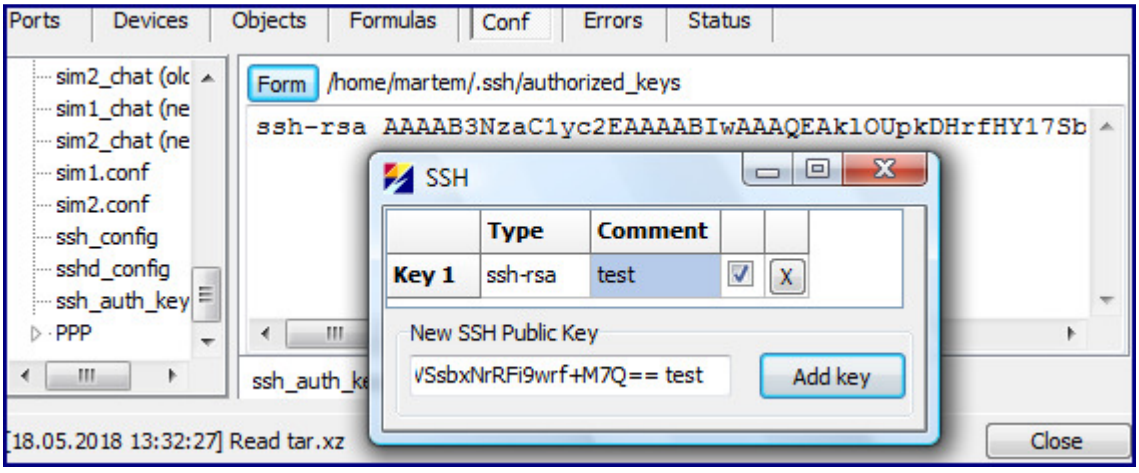
Restriction of SSH connection via firewall can be done : „Common“-> „TCP/IP settings“->“General“. Turn the firewall on by clicking „Automatic“. There is a possibility to choose the interface and multiple networks/IP address from which is allowed to connect via SSH with comma separated list. Press „OK“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

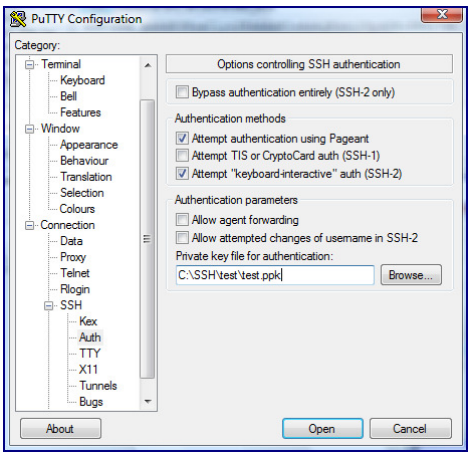


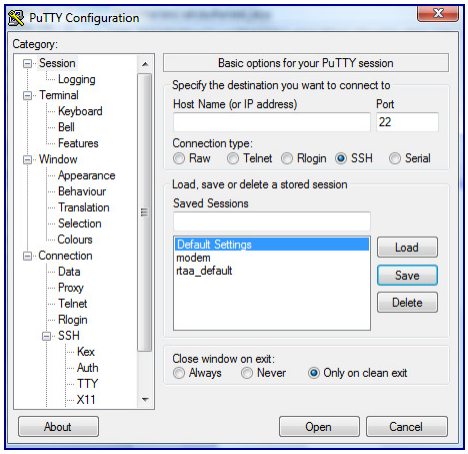
8.3 Authorization with SSH public key

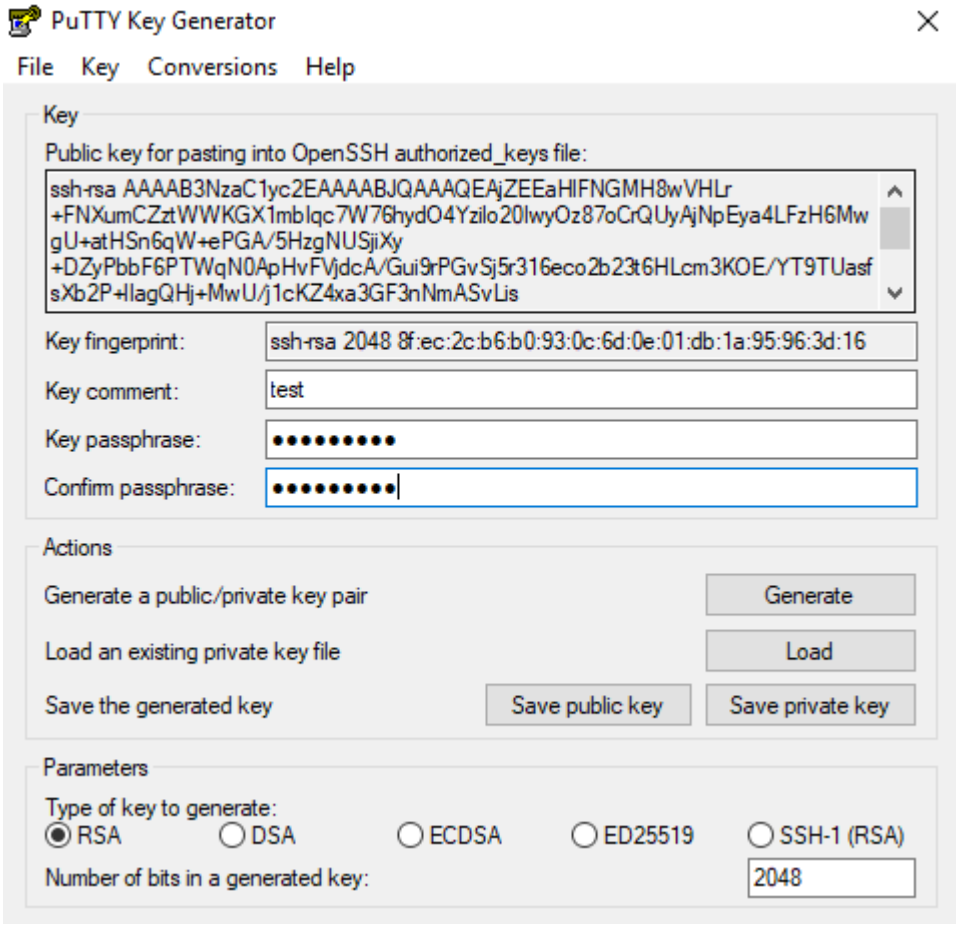
It is recommended to authorize with SSH public key for access the Telem device. The SSH public and private key pair should be created (e.g. PUTTYGen). The private key should be saved on the PC.
Public key should be put into „Conf“-> „ssh_auth_keys“. This can be done by copying the key as text directly 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 GWS.exe “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



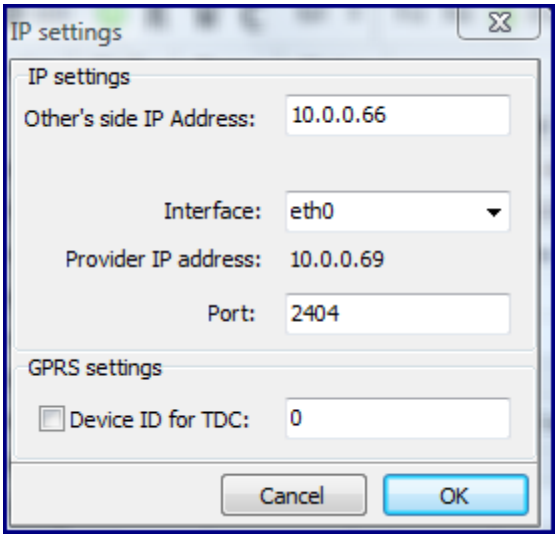






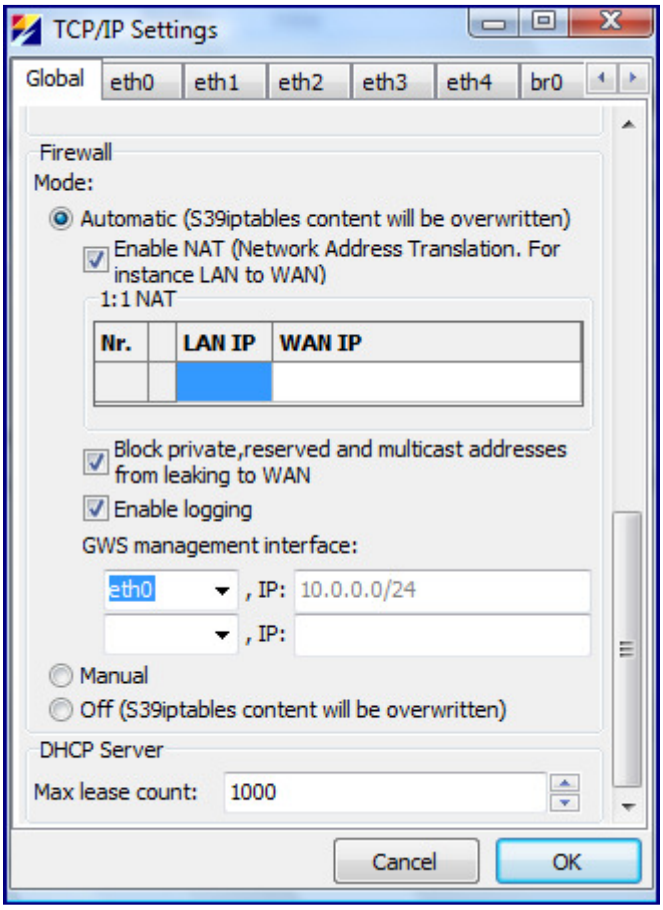
8.4 Trusted connection definition in channel setup

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.



8.6 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.

8.7 Considering the security of WebServer usage

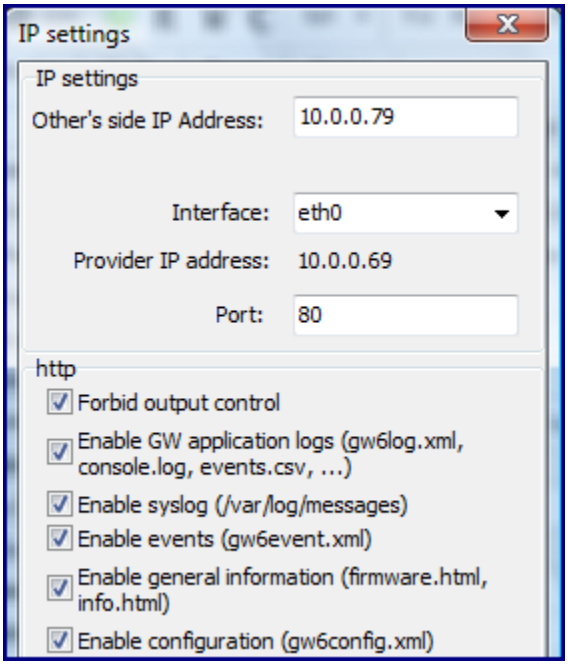
WebServer can be unsecure in front of cyber-attacks. To reduce risk of unwanted outages and to avoid usage of dangerous exploits it is recommended to:

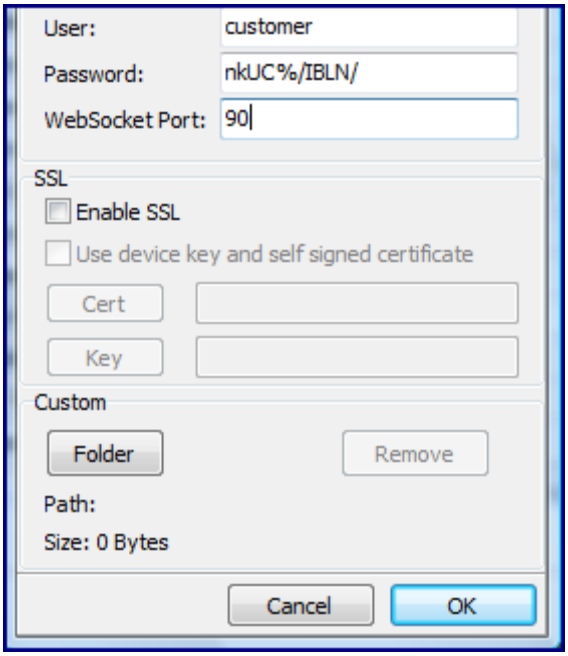
- Use WebServer only if there is necessity and turn it off when it is not needed.

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.





8.8 Keep PuTTY up to date

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