Description Secure TCP/IP connection

for UMG 604, UMG 605, UMG 508, UMG 509, UMG 511 and UMG 512



Janitza electronics GmbH Vor dem Polstück 1 D-35633 Lahnau Support tel. +49 (0) 64 41 9642-22 Fax +49 (0) 64 41 9642-30 e-mail: info@janitza.com Website: http://www.janitza.com



Content

General information	3
Copyright	3
Trademarks	3
Disclaimer	3
Comments on the manual	3
Secure TCP/IP connection	5
Change FTP password	6
Firewall settings	8
Display password	11
Homepage password	12
Security - Modbus TCP/IP communication	14
Security - Modbus RS485 communication	14
Security - "UMG 96RM-E" communication	14

General information

Copyright

This functional description is subject to the statutory provisions of copyright law and may neither be photocopied, reprinted, or reproduced - in whole or in part, by mechanical or electronic means - nor otherwise duplicated or republished, without the binding written permission of:

Janitza electronics GmbH, Vor dem Polstück 1, D 35633 Lahnau, Germany

Trademarks

All trademarks and the resulting rights are the property of their respective owners.

Disclaimer

Janitza electronics GmbH accepts no responsibility for errors or deficiencies within this functional description, and makes no commitment to keep the contents of this functional description up to date.

Comments on the manual

We welcome your comments. If anything in this manual seems unclear, please let us know by sending an e-mail to: info@janitza.de

Meaning of symbols

This manual uses the following pictograms:



Dangerous voltage!

Risk to life or serious injury. Before commencing work on the system and the device, they must first be de-energised.



Attention!

Please pay attention to the documentation. This symbol is intended to warn you of potential dangers, which could occur during installation, commissioning and use.



Note

Secure connection

Secure TCP/IP connection

The communication with the measurement devices from the UMG series is customarily implemented via Ethernet. To do so, the measurement devices have various protocols for the respective connection ports. This enables software applications such as GridVis, to communicate with the measurement devices via FTP, Modbus or HTTP protocols.

Network security plays an increasingly important role here.

This guideline is intended to support you with the secure incorporation of the measurement devices into the network and thus to effectively protect the measurement devices from unauthorised access. The guide relates to firmware > 4.057 as the following HTML changes have been carried out

- Improvement of the challenge evaluation
- After three failed logins the IP is locked (by the client) for 900 seconds
- GridVis settings reworked
- HTML password: 8 characters can be set
- HTML configuration can be completely locked

If the measurement device is set up in GridVis, there are multiple connection protocols available: A standard protocol is the FTP protocol – i.e. the GridVis reads files from the measurement device via FTP port 21 with the respective data ports 1024 to 1027. An unsecure connection can be implemented via FTP in the "TCP/IP". A secure connection can be established with the "TCP" type of connection.

Lonfigure co	nnection (UMG512)	x
Connection type		
Connection type		•
UMG512 [TCP/IP]		
Host	Modbus RTU(RS485/RS232)	
-	Ethernet gateway (eg. for devices over RS485)	
Time out [millise	нттр	=
	HTTP Secured	
	EasyGateway EG400-HE	-
	Lasydateway Lohoon IL (Secured connection)	
	OK Cancel H	elp



Change FTP password

- An FTP user and an FTP password are required for the secure connection.
- These are set to user "admin" and password "Janitza" at the factory.
- For a secure connection, the password for administrator access (admin) can be changed in the configuration menu.

Step 1.)

- Call up the "Configure connection" dialogue
 Example 1: To do so, mark the corresponding device in the project window with the mouse button
 and select "Configure connection" in the context menu with the right mouse button
 Example 2: Double-click on the respective device to open the overview window and select
 the "Configure connection" button
- Select the "TCP secured" connection type
- Set the host address of the device
- Fill in the username and password with Username: admin Password: Janitza
- Set the "Encrypted" menu point This enabled an **AES 256-bit data encryption**.

#		
File Edit View Tools Window Help		Q Search in Projects (Ctrl+I
🔛 🖬 🤊 🥙 🕼 🖗 🖉 🖬 🕷	33	
Projects 28 Overview Window 28		
Project-A Ready		
By Type	ningure Contigure connection Connection test Reset values	
UMG 96RM		
UMG 511	512 Hardware revision: 0000	
UMG 512		
Basic Te Show overview	: 5/12/15 7:51:19 AM	Configure connection (UMG512)
Graph Properties	No Timeplan	
Topolog Copy Exports		Connection type TCP Secured
Alarm N Delete device		UMG512 [TCP Secured]
Databa Takeover device Generic Transfer device	alues %	
	view	Host 192.168.3.63
Configure connection	a value.	Time out [millisec.] 5,000
connection text	a value.	University and a second s
Configure Show phasor graph	Month Day	admin
Download memory		Password ••••••
Reset values	Y	Encrypted
Configure time synchronisation		
Configure automatic synchronisation		Ba Connection test
	-	
- m +		
	-	
Fig : Configuration	1	
rig Configuration		
of the device		
connection		
connection		
		OK Cancel Help

Step 2.)

- Call up the configuration window
 Example 1: To do so, mark the corresponding device in the project window with the mouse button
 and select "Configure" in the context menu with the right mouse button

 Example 2: Double-click on the respective device to open the overview window and select
 the "Configure" button
- Select the "Passwords" button in the configuration window. Change the administrator password, if desired.
- Save the changes by transferred the data to the device ("Transmit" button).



Attention!

MAKE SURE THAT YOU DON'T FORGET THE PASSWORD. THERE IS NO MASTER PASSWORD. IF THE PASSWORD IS NO LONGER AVAILABLE THE DEVICE MUST BE SENT BACK TO THE FACTORY!



The admin password may be max. 30 characters long and can comprise numerals, letters and special characters (ASCII codes 32 - 126).



Firewall settings

• The measurement devices have an integrated firewall that enables ports that are not required to be disabled.

Step 1.)

- Call up the "Configure connection" dialogue
 Example 1: To do so, mark the corresponding device in the project window with the mouse button
 and select "Configure connection" in the context menu with the right mouse button
 Example 2: Double-click on the respective device to open the overview window and select
 the "Configure connection" button
- Select the "TCP secured" connection type
- Log in as administrator

Mage Configure conne	ection (UMG512)	×
Connection type TO	CP Secured	•
UMG512 [TCP Secure	ed]	
Host	192.168.3.63	
Time out [millisec.]		5,000 ≑
Username	admin	
Password	•••••	
		Connection test
	ОК	Cancel Help

Fig.: Configuration of the device connection (Admin)

Step 2.)

- Call up the configuration window
 Example 1: To do so, mark the corresponding device in the project window with the mouse button and select "Configure" in the context menu with the right mouse button
 Example 2: Double-click on the respective device to open the overview window and select the "Configure" button
- Select the "Firewall" button in the configuration window.



- The firewall is switched on via the "Firewall" button.
 - From release X.XXX, this is already activated at the factory.
 - The protocols that you do not require can be deactivated here.
 - With the firewall switched on, the device only permits requests on the respective activated protocols

Protocols	Port
FTP	Port 21, data port 1024 to 1027
HTTP	Port 80
SNMP	Port 161
Modbus RTU	Port 8000
Debug	PORT 1239 (for service purposes)
Modbus TCP/IP	Port 502
BACnet	Port 47808
DHCP	UTP Port 67 and 68
NTP	Port 123
Name Server	Port 53

• For rudimentary communication with GridVis and via the homepage, the following settings are sufficient:



- Please be very careful when selecting the closed ports! Depending on the connection protocol selected, it is possible to communicate only via http, for example.
- Save the changes by transferred the data to the device ("Transmit" button).

Display password

• The device configuration via the device buttons can also be protected. i.e. configuration is only possible after entering a password. The password can be set in the device itself or via GridVis in the configuration window.



The display password may be max. 5 characters long and may contain only numerals.



Fig.: Display -Set password

Step 1.)

• Call up the configuration window

Example 1: To do so, mark the corresponding device in the project window with the mouse button and select "Configure" in the context menu with the right mouse button

Example 2: Double-click on the respective device to open the overview window and select the "Configure" button

- Select the "Passwords" button in the configuration window. If desired, change the "User password for the configuration menue of the device" option
- Save the changes by transferred the data to the device ("Transmit" button).

After this, the configuration on the device can only be changed after entering a password.



Homepage password

- The homepage can also be protected from unauthorised access. The following modes are available:
 - Do not lock homepage

The homepage can be accessed without logging in. Configuration can be carried out without logging in.

Lock homepage

After logging in, the homepage and the configuration for the IP of the user is enabled for 3 minutes. The time is set to 3 minutes again with every access implemented.

- Lock configuration separately The homepage can be accessed without logging in. Configuration can only be carried out after logging in.
- Lock homepage and configuration separately
 - After logging in, the homepage for the IP of the user is enabled for 3 minutes.
 - The time is set to 3 minutes again with every access implemented.
 - Configuration can only be carried out after logging in.



Note: Only the variables that are in init.jas or that have "Admin" rights apply to the configuration.



The homepage password may be max. 8 characters long and may contain only numerals.

Overview Window 🛛 🕺 🌄 Co	nfiguration[UMG512] %	
S S	Ø F	a
Transmit Transmit to	Reload Factory default Save to file L	oad from file
Identity Admi	n	lanitza
Transformer		10045
Phase mapping	password for the configuration menue of the device	12345
Measuringvariants HTML		0
Nominalvalues Home	epage mode	Do not lock homepage 🚽 🥥
Ripple control Activ	ation code for BACNet	Do not lock homepage
Events	ation and a fee Eller	Lock homepage
Event recording Acuv	auon code for EMax	Lock configuration separately
Device off event		Lock homepage and configuration separately
RCM configuration	18 ¹⁰	
Transients		
Transient recording		
Averaging intervals	- 1	
Recording configuration		
memory configuration	Pass	sword for
time	HTN	11 access
Timezone		12 400000
Inputs		
value adjustment		
Digital outputs		
Serial ports		
field bus profiles		
ip configuration		
Firewall		
Passwords		
Flicker		
Bacnet		
peak demand		
I/O naming		
Online recording		
		10 2015 2:02:54 AM (EST (CMT (02:00)

Fig.: Set homepage password

After activation, a login window appears after the device homepage is called up.

Jani	tza - Homepage login
	Login
	Bitte geben Sie das Gerätepasswort an: Please enter the password to logon: Password: Login
	Name: RISK Test Description: 1

Fig.: Homepage login

Security - Modbus TCP/IP communication

It is not possible to secure the Modbus TCP/IP communication (port 502). The Modbus standard does not provide for secure communication. Integrated encryption would no longer be compliant with the Modbus standard and the interoperability with other devices would no longer be guaranteed. For this reason, no password can be assigned with Modbus communication.

If the IT department mandates that only secured protocols are permitted, the Modbus TCP/IP port must be deactivated in the device firewall. The device administrator password should be changed and the communication must be implemented via "TCP secured" (FTP) or "http secured".

Security - Modbus RS485 communication

It is not possible to secure the Modbus RS485 communication. The Modbus standard does not provide for secure communication. Integrated encryption would no longer be compliant with the Modbus standard and the interoperability with other devices would no longer be guaranteed. This also affects the Modbus-Master functionality. This means that no encryption can be activated for devices on the RS485 interface.

If the IT department mandates that only secured protocols are permitted, the Modbus TCP/IP port must be deactivated in the device firewall. The device administrator password should be changed and the communication must be implemented via "TCP secured" (FTP) or "http secured".

As a result however, devices on the RS485 interface can no longer be read out!

The alternative in this case is to waive the Modbus-Master functionality and the exclusive use of Ethernet devices such as the UMG 604 / 605 / 508 / 509 / 511 or UMG 512.

Security - "UMG 96RM-E" communication

The UMG 96RM-E does not offer a secure protocol. With this device, the communication is implemented exclusively via Modbus TCP/IP. It is not possible to secure the Modbus TCP/IP communication (port 502). The Modbus standard does not provide for secure communication. This means, that if encryption is integrated, this would no longer be compliant with the Modbus standard and the interoperability with other devices would no longer be guaranteed. For this reason, no password can be assigned with Modbus communication.