

Description

Secure TCP/IP Connection

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



Contents

General	3
Copyright	3
Trademarks	3
Disclaimer	3
Comments on the manual	3
Secure TCP/IP connection	5
Change password	6
Firewall settings	9
Display password	12
Homepage password	13
Modbus TCP/IP communication security	15
Modbus RS485 communication security	15
"UMG 96RM-E" communication security	15



General

Copyright

This functional description is subject to the legal provisions of copyright protection and may not be photocopied, reprinted, reproduced or otherwise duplicated or republished in whole or in part by mechanical or electronic means without the legally binding, written consent of

Janitza electronics GmbH, Vor dem Polstück 6,
35633 Lahnau, Germany

Trademarks

All trademarks and the rights arising from them are the property of the respective owners of these rights.

Disclaimer

Janitza electronics GmbH assumes no responsibility for errors or defects within this functional description and assumes no obligation to keep the contents of this functional description up to date.

Comments on the manual

Your comments are welcome. If anything in this manual seems unclear, please let us know and send us an email at: info@janitza.com



Meaning of symbols

The following pictograms are used in this manual:



Dangerous voltage!

Risk of fatality or serious injury. Disconnect the system and device from the power supply before starting work.



Attention!

Please refer to the documentation. This symbol is intended to warn you of possible dangers that may arise during installation, commissioning and use.



Note



Secure TCP/IP connection

Communication with the measuring devices of the UMG series is usually via Ethernet. The measuring devices provide different protocols with the respective connection ports for this purpose. Software applications such as the GridVis® communicate with the measuring devices via the FTP, Modbus or HTTP protocol.

Network security in the company network plays an increasingly important role here.

This guide is intended to support you in securely integrating the measuring devices into the network, thus effectively protecting the measuring devices from unauthorized access.

The guide refers to firmware > 4.057, as the following HTML changes have been made:

- Improvement of the challenge calculation
- After three incorrect logins, the IP (of the client) is blocked for 900 seconds
- GridVis® settings revised
- HTML password: can be set, 8 digits
- HTML configuration completely lockable

If the measuring device is used in the GridVis®, several connection protocols are available. A standard protocol is the FTP protocol – i.e. the GridVis® reads files from the measuring device via FTP port 21 with the respective data ports 1024 to 1027. In the "TCP/IP" setting, the connection is made unsecured via FTP. A secured connection can be established using the "TCP secured" connection type.

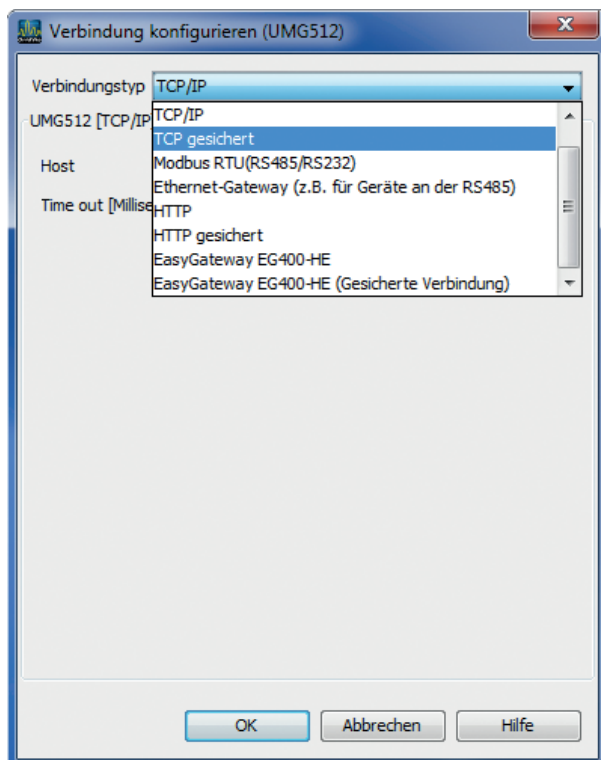


Fig.: Settings for the connection type under "Configure connection"

Change password

- A user and password are required for the secure connection.
- By default, the user is *admin* and the password is *Janitza*.
- For a secure connection, the password for administrator access (*admin*) can be changed in the configuration menu.

1. Step

- Open the "Configure connection" dialog
 Example 1: To do this, use the mouse button to highlight the corresponding device in the projects window and select "Configure connection" in the context menu of the right mouse button
 Example 2: Double-click on the corresponding device to open the overview window and select the "Configure connection" button
- Select the connection type "TCP secured"
- Set the host address of the device
- Fill in the username and password.
 Factory settings:
 Username: *admin*
 Password: *Janitza*
- Set the "Encrypted" menu item.
 An **AES256-bit encryption** of the data is then activated.

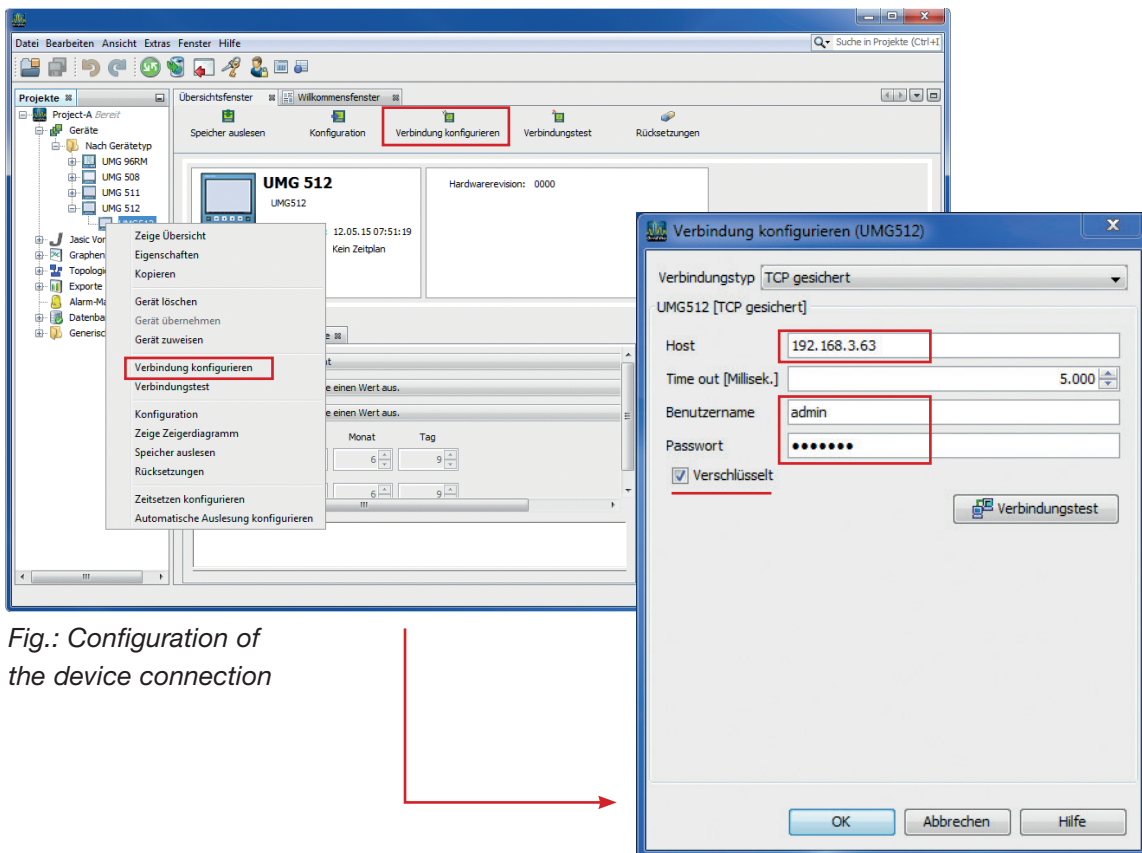


Fig.: Configuration of the device connection

2. Step

- Open the configuration window
Example 1: To do this, use the mouse button to highlight the corresponding device in the projects window and select "Configuration" in the context menu of the right mouse button
Example 2: Double-click on the corresponding device to open the overview window and select the "Configuration" button
- Select the "Passwords" button in the configuration window.
Change the administrator password, if desired.
- Save the changes with the transfer of the data to the device ("Transfer" button)



Attention!

DO NOT FORGET THE PASSWORD UNDER ANY CIRCUMSTANCES. THERE IS NO MASTER PASSWORD. IF THE PASSWORD IS FORGOTTEN, THE DEVICE MUST BE SENT TO THE FACTORY!



The admin password may be a maximum of 30 digits long and can consist of numbers, letters and special characters (ASCII code 32 to 126, except for the characters listed below). Also, the password field must not be left blank.

The following special characters must not be used:

" (code 34)
 \ (code 92)
 ^ (code 94)
 ` (code 96)
 | (code 124)

Space (code 32) is allowed only within the password. It is not allowed as the first and last character.

When you have updated to a GridVis® version > 9.0.20 and use one of the special characters described above, you will be prompted to change the password according to these rules when you open the device configurator.



The description "Change password" with its password rules also applies to the connection type "HTTP secured".



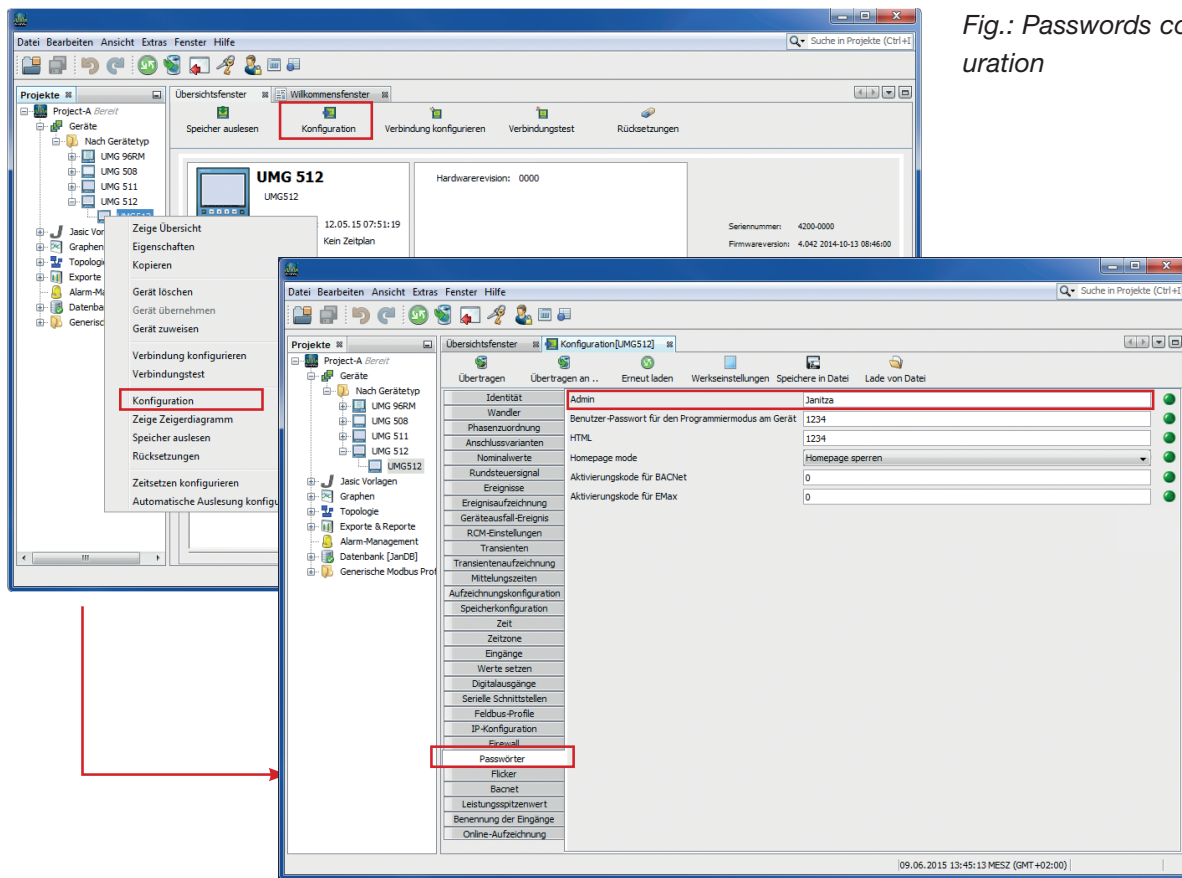


Fig.: Passwords configuration

Firewall settings

- The measurement devices have an integrated firewall that allows you to block ports you don't need.

1. Step

- Open the "Configure connection" dialog
 Example 1: To do this, use the mouse button to highlight the corresponding device in the projects window and select "Configure connection" in the context menu of the right mouse button
 Example 2: Double-click on the corresponding device to open the overview window and select the "Configure connection" button
- Select the connection type "TCP secured"
- Log in as administrator

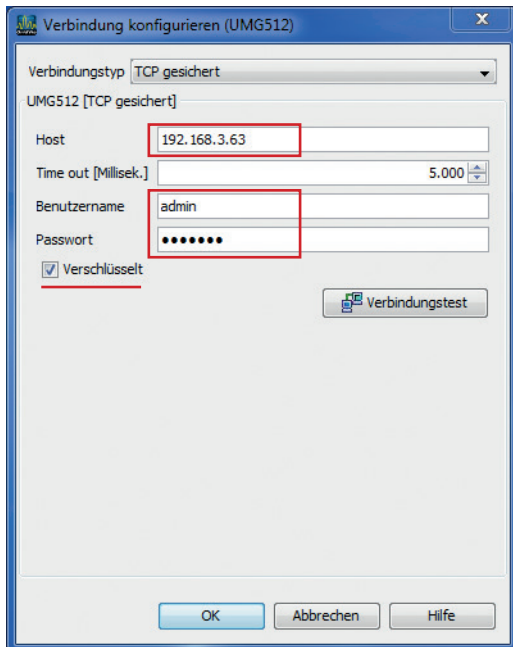


Fig.: Configuration of the device connection (admin)

2. Step

- Open the configuration window
 Example 1: To do this, use the mouse button to highlight the corresponding device in the projects window and select "Configuration" in the context menu of the right mouse button
 Example 2: Double-click on the corresponding device to open the overview window and select the "Configuration" button
- Select the "Firewall" button in the configuration window.

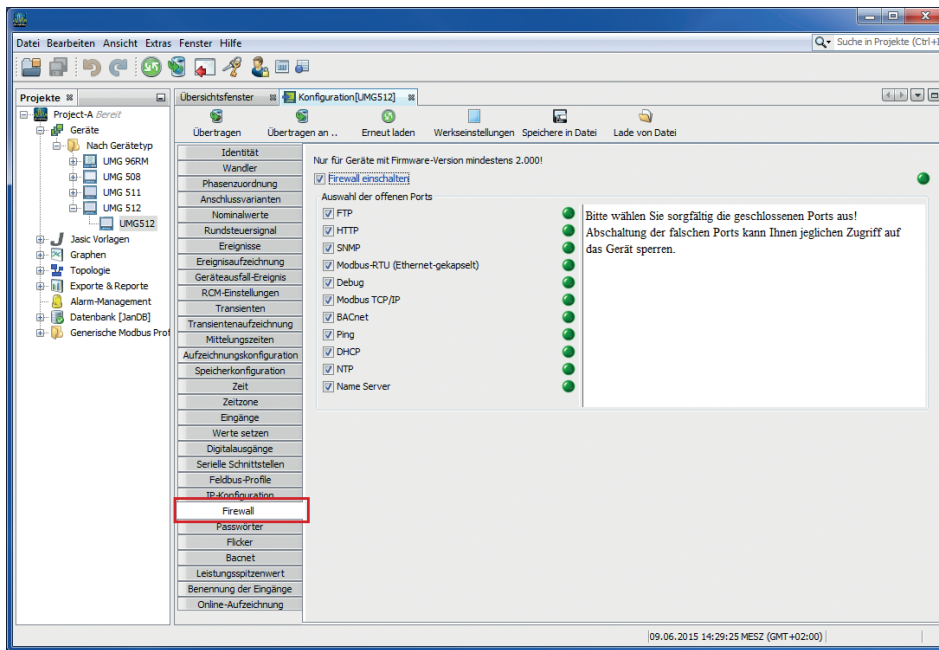


Fig.: Firewall configuration

- The firewall is switched on via the "Firewall" button.
 - As of release X.XXX, this is the default setting.
 - Protocols that you do not need can be deactivated here.
 - When the firewall is switched on, the device only allows requests on the protocols activated in each case

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
Server name	Port 53



- For rudimentary communication with the GridVis® and via the homepage, the following settings will suffice:

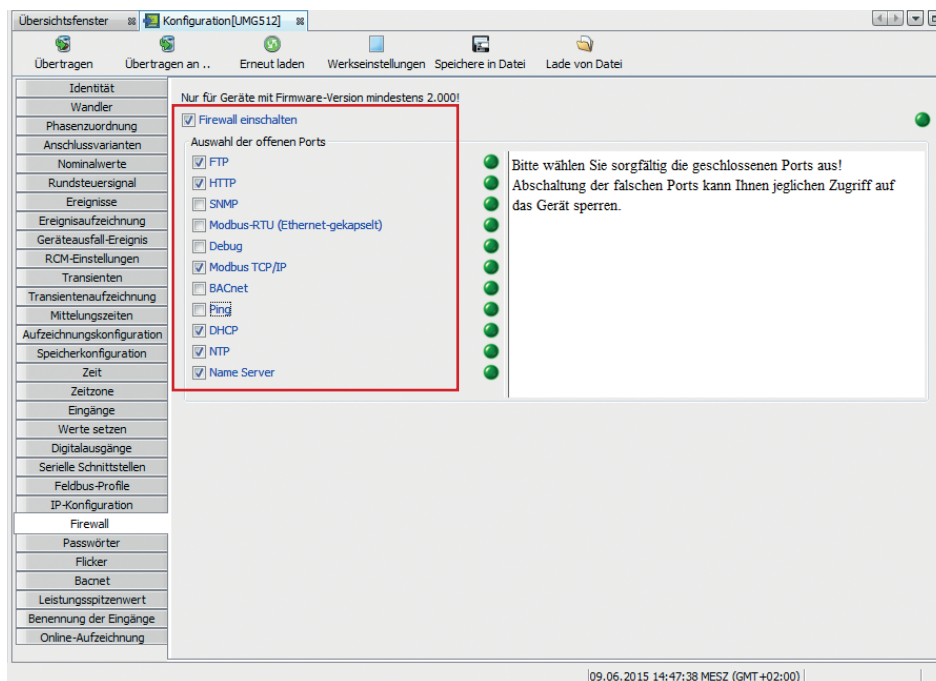


Fig.: Firewall configuration

- But please choose the closed ports carefully!** Depending on the selected connection protocol, it may only be possible to communicate via HTTP, for example.
- Save the changes with the transfer of the data to the device ("Transfer" button)

Display password

- The device configuration via the device keys can also be protected. I.e. only after entering a password is the configuration possible. The password can be set on the device itself or via the GridVis® in the configuration window.



The display password must be a maximum of 5 digits long and only contain numbers.

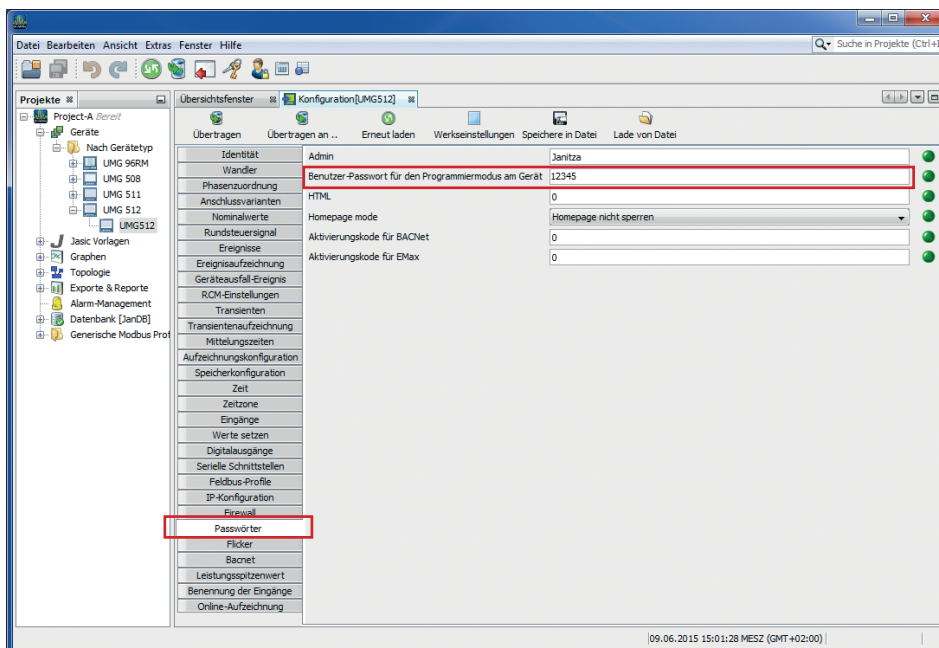
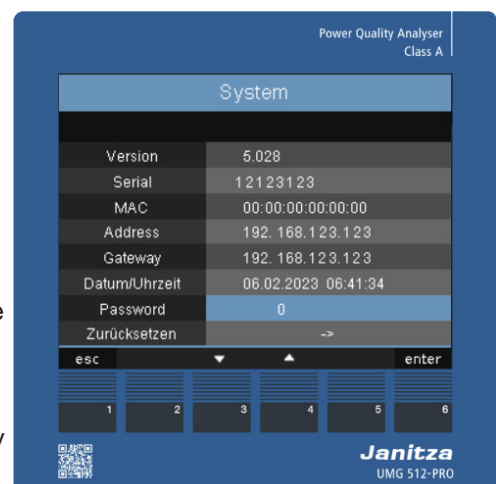


Fig.: Setting the display password

Procedure:

- Open the configuration window
Example 1: To do this, use the mouse button to highlight the corresponding device in the projects window and select "Configuration" in the context menu of the right mouse button
Example 2: Double-click on the corresponding device to open the overview window and select the "Configuration" button
- Select the "Passwords" button in the configuration window. If so desired, change the option "User password for the programming mode on the device"
- Save the changes with the transfer of the data to the device ("Transfer" button)

The configuration on the device can then only be changed by entering a password.



Homepage password

- The homepage can also be protected from unauthorized access. The following options are available:
 - **Do not lock homepage**
The homepage is accessible without login; configurations can be made without logging in.
 - **Lock homepage**
After a login, the homepage and the configuration for the user's IP will be unlocked for 3 minutes. With each access the time is set to 3 minutes again.
 - **Lock configuration separately**
The homepage is accessible without login; configurations can only be made by logging in.
 - **Lock homepage and configuration separately**
 - After a login, the homepage is unlocked for the user's IP for 3 minutes.
 - With each access the time is set to 3 minutes again.
 - Configurations can only be made by logging in.



Note: Only the variables that are in the init.jas or have "Admin" authorization are considered as configuration



The homepage password must be a maximum of 8 digits long and only contain numbers.

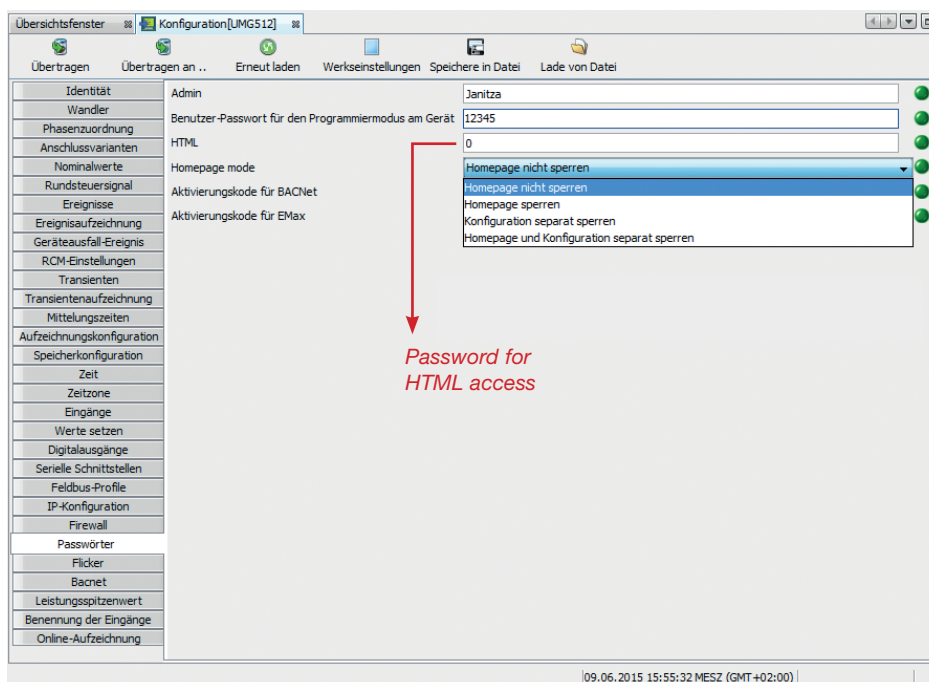
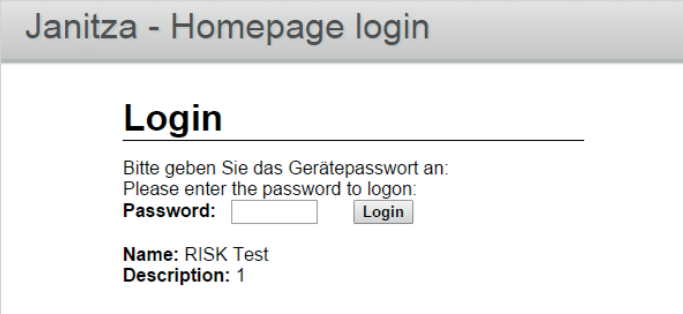


Fig.: Set homepage password

After activation, a login window appears after opening the device homepage.



Janitza - Homepage login

Login

Bitte geben Sie das Gerätepasswort an:
Please enter the password to logon:

Password:

Name: RISK Test
Description: 1

Fig.: Homepage login



Modbus TCP/IP communication security

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

If IT specifies that only secured protocols may be used, the Modbus TCP/IP port must be deactivated in the device firewall. The device administrator password must be changed and communication must take place via "TCP secured" (FTP) or "HTTP secured".

Modbus RS485 communication security

Protection of the Modbus RS485 communication is not possible. The Modbus standard does not provide for any protection. Integrated encryption would no longer be according to Modbus standard and interoperability with other devices would no longer be guaranteed. This also concerns the Modbus master functionality. I.e. no encryption can be activated for devices at the RS-485 interface.

If IT specifies that only secured protocols may be used, the Modbus TCP/IP port must be deactivated in the device firewall. The device administrator password must be changed and communication must take place via "TCP secured" (FTP) or "HTTP secured".

However, devices at the RS485 interface can then no longer be read out!

The alternative in this case is to dispense with the Modbus master functionality and to exclusively use Ethernet devices such as the UMG 604 / 605 / 508 / 509 / 511 or UMG 512.

"UMG 96RM-E" communication security

The UMG 96RM-E does not offer a secured protocol. Communication with this device is 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 any protection. I.e. if encryption were to be integrated, it would no longer be in accordance with the Modbus standard and interoperability with other devices would no longer be guaranteed. For this reason, no password can be assigned during Modbus communication.



Janitza[®]

Janitza electronics GmbH
Vor dem Polstück 6 | 35633 Lahnau
Germany

Tel. +49 6441 9642-0
info@janitza.com | www.janitza.com

