www.janitza.de

Dok. Nr. 2.047.013.1 / V 0.5 - 15.08.2016

Beschreibung

Sichere TCP/IP-Verbindung

für UMG 604, UMG 605, UMG 508, UMG 509, UMG 511 und UMG 512

Janitza electronics GmbH
Vor dem Polstück 1
D-35633 Lahnau
Support Tel. (0 64 41) 9642-22
Fax (0 64 41) 9642-30
e-mail: info@janitza.de
Internet: http://www.janitza.de

Janitza®

Inhalt

Allgemeines

Copyright

Markenzeichen

Haftungsausschluss

Kommentare zum Handbuch

Ihre Kommentare sind uns willkommen. Falls irgend etwas in diesem Handbuch unklar erscheint, lassen Sie es uns bitte wissen und schicken Sie uns eine EMAIL an: info@janitza.de

Bedeutung der Symbole

Im vorliegenden Handbuch werden folgende Piktogramme verwendet:

Gefährliche Spannung!

Lebensgefahr oder schwere Verletzungsgefahr. Vor Beginn der Arbeiten Anlage und Gerät spannungsfrei schalten.

Achtung!

Bitte beachten Sie die Dokumentation. Dieses Symbol soll Sie vor möglichen Gefahren warnen, die bei der Montage, der Inbetriebnahme und beim Gebrauch auftreten können.

Hinweis

Sichere TCP/IP-Verbindung

Die Kommunikation mit den Messgeräten der UMG-Serie erfolgt für gewöhnlich über Ethernet. Die Messgeräte stellen dazu verschiedene Protokolle mit den jeweiligen Verbindungsports zur Verfügung. Softwareapplikationen wie die GridVis kommunizieren hierbei mit den Messgeräten über das FTP-, Modbus- oder HTTP-Protokoll.

Die Netzwerksicherheit im Unternehmensnetzwerk spielt hierbei eine immer wichtigere Rolle.

Dieser Leitfaden soll Sie unterstützen, die Messgeräte sicher ins Netzwerk einzubinden und damit die Messgeräte vor Fremdzugriff effektiv zu schützen.
Die Anleitung bezieht sich auf eine Firmware > 4.057 da folgende HTML Änderungen durchgeführt wurde

- Verbesserung der Challenge-Berechnung
- Nach drei falschen Logins wird die IP (vom Client) für 900 Sekunden gesprerrt
- GridVis-Einstellungen überarbeitet
- HTML-Passwort: 8 Stellen einstellbar
- HTML-Konfiguration komplett sperrbar

Wird das Messgerät in der GridVis eingerichtet stehen mehrere Verbindungsprotokolle zur Verfügung. Ein Standard-Protokoll ist das Protokoll FTP – d.h die GridVis liest Dateien vom Messgerät über den FTP-Port 21 mit den jeweiligen Daten-Ports 1024 bis 1027. In der Einstellung „TCP/IP“ erfolgt die Verbindung ungesichert über FTP. Eine gesicherte Verbindung kann über die Verbindungsart „TCP“ aufgebaut werden.

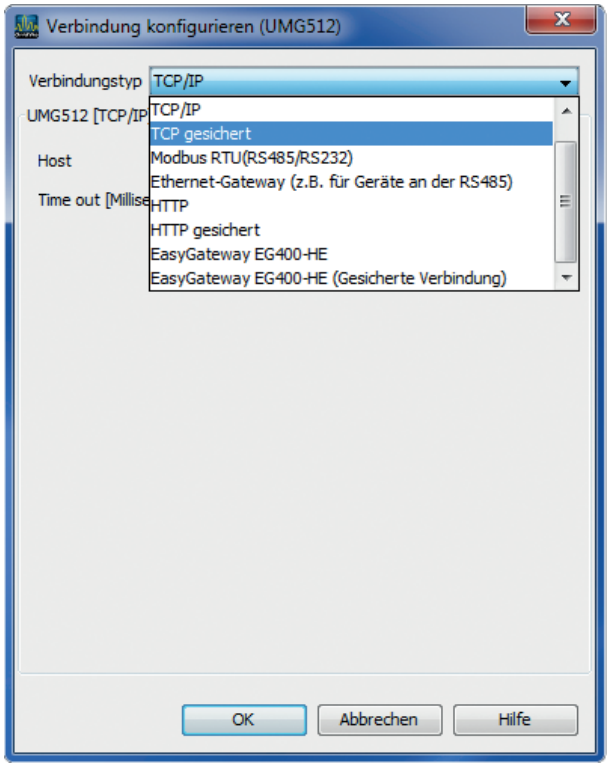


Abb.: Einstellungen zum Verbindungstyp unter „Verbindung konfigurieren“

FTP Passwort ändern

- Für die gesicherte Verbindung ist ein FTP-User und ein FTP-Passwort erforderlich.
- In der Werksauslieferung ist der User „**admin**“ und das Passwort „**Janitza**“.
- Für eine sichere Verbindung kann das Passwort für den Administrator-Zugang (admin) im Konfigurationsmenü geändert werden.

Step 1.)

- Rufen Sie den Dialog „Verbindung konfigurieren“ auf
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste „Verbindung konfigurieren“
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende Gerät das Übersichtsfenster und wählen Sie die Schaltfläche „Verbindung konfigurieren“ aus
- Wählen Sie den Verbindungstyp „TCP gesichert“
- Setzen Sie die Host-Adresse des Gerätes
- Füllen Sie Benutzername und Passwort aus mit
  Benutzername: admin
  Passwort: Janitza
- Setzen Sie den Menüpunkt „Verschlüsselt“.
  Hierdurch wird eine **AES256-Bit-Verschlüsselung** der Daten aktiviert.

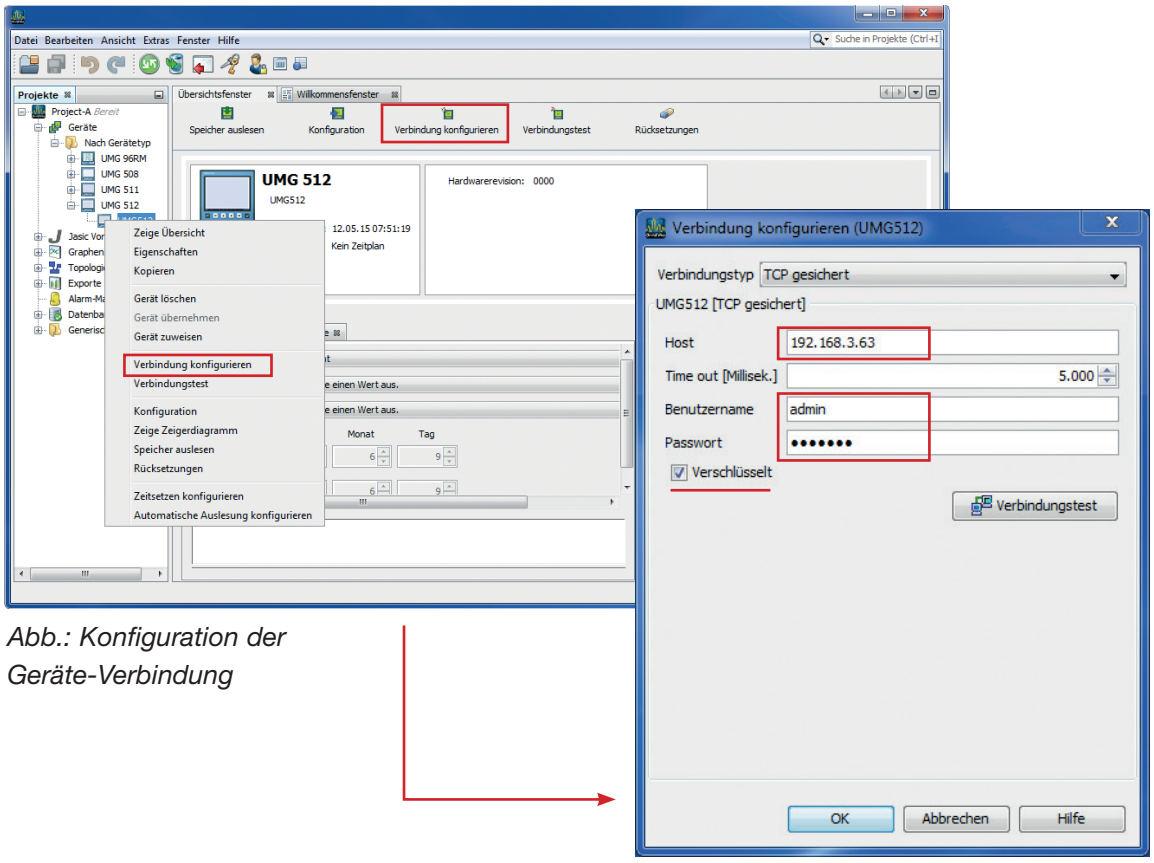


Abb.: Konfiguration der Geräte-Verbindung

Step 2.)

- Rufen Sie das Konfigurationsfenster auf
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste „Konfiguration“
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende Gerät das Übersichtsfenster und wählen Sie die Schaltfläche „Konfiguration“ aus
- Wählen Sie im Konfigurationsfenster die Schaltfläche „Passwörter“ aus.
  Ändern Sie - wenn gewünscht - das Administrator-Passwort.
- Sichern Sie die Änderungen mit der Übertragung der Daten an das Gerät (Schaltfläche „Übertragen“)

Achtung!

VERGESSEN SIE DAS PASSWORT AUF KEINEN FALL. ES GIBT KEIN MASTER PASSWORT. SOLLTE DAS PASSWORT NICHT MEHR VORLIEGEN, MUSS DAS GERÄT INS WERK EINGESCHICKT WERDEN!

Das Admin-Passwort darf maximal 30 Stellen lang sein und kann aus Zahlen, Buchstaben und Sonderzeichen bestehen (ASCII-Code 32 ... 126).

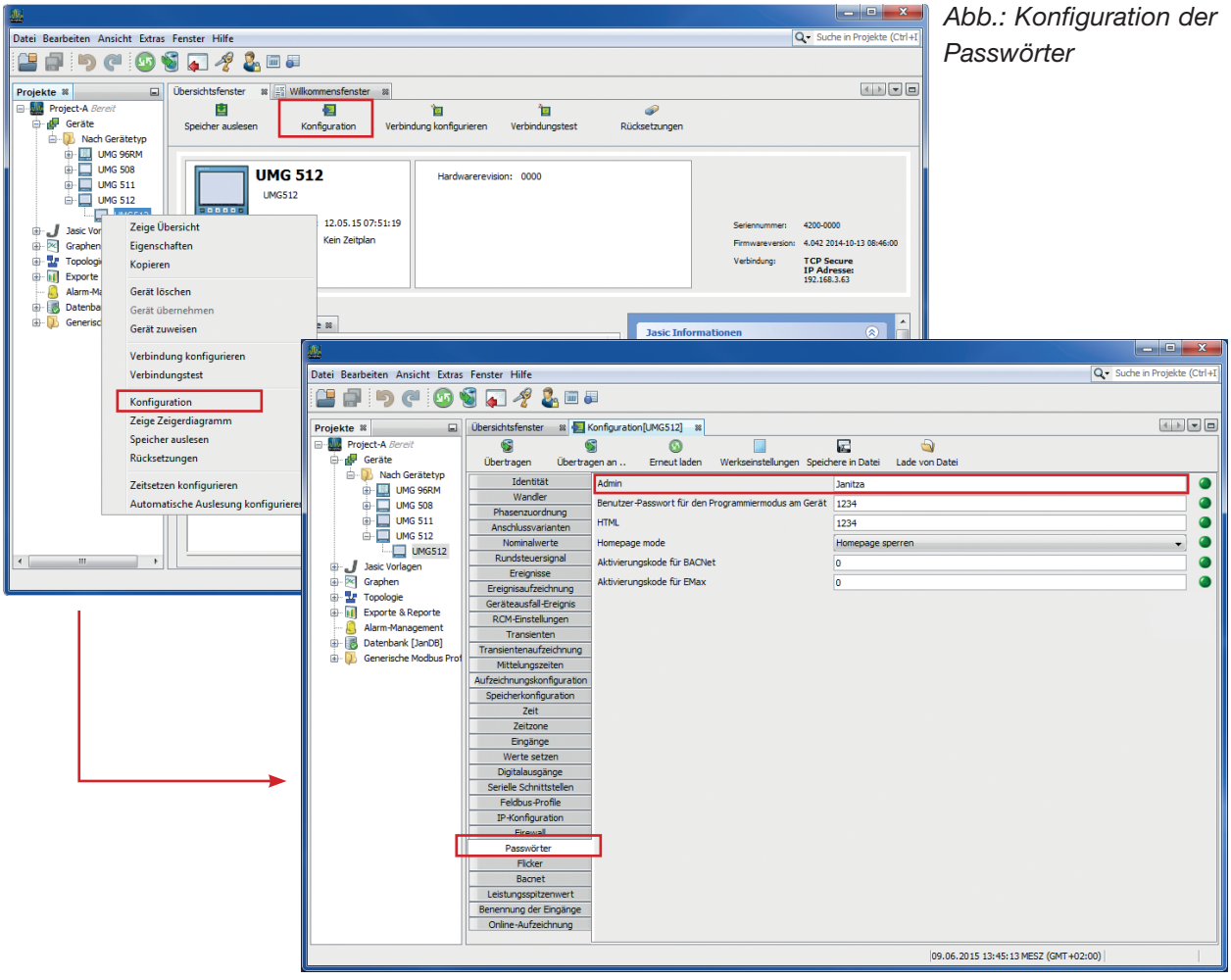


Abb.: Konfiguration der Passwörter

Firewall-Einstellungen

- Die Messgeräte haben eine integrierte Firewall, die es ermöglicht, Ports die man nicht benötigt zu sperren.

Step 1.)

- Rufen Sie den Dialog „Verbindung konfigurieren“ auf
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste „Verbindung konfigurieren“
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende Gerät das Übersichtsfenster und wählen Sie die Schaltfläche „Verbindung konfigurieren“ aus
- Wählen Sie den Verbindungstyp „TCP gesichert“
- Melden Sie sich als Administrator an

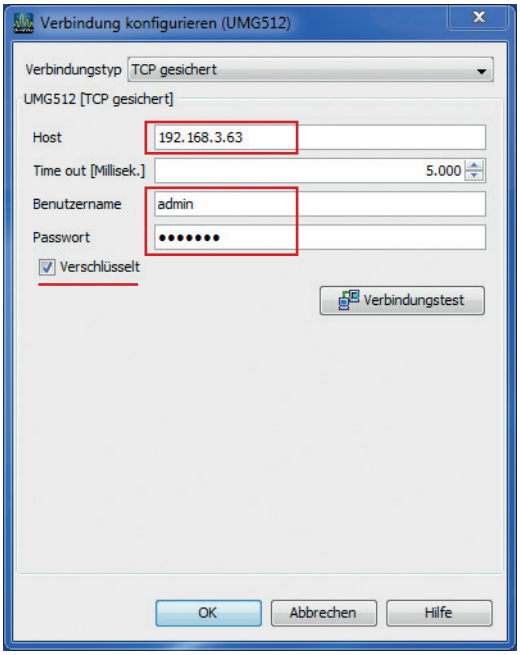


Abb.: Konfiguration der Geräte-Verbindung (Admin)

Sep 2.)

- Rufen Sie das Konfigurationsfenster auf
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste „Konfiguration“
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende Gerät das Übersichtsfenster und wählen Sie die Schaltfläche „Konfiguration“ aus
- Wählen Sie im Konfigurationsfenster die Schaltfläche „Firewall“ aus.

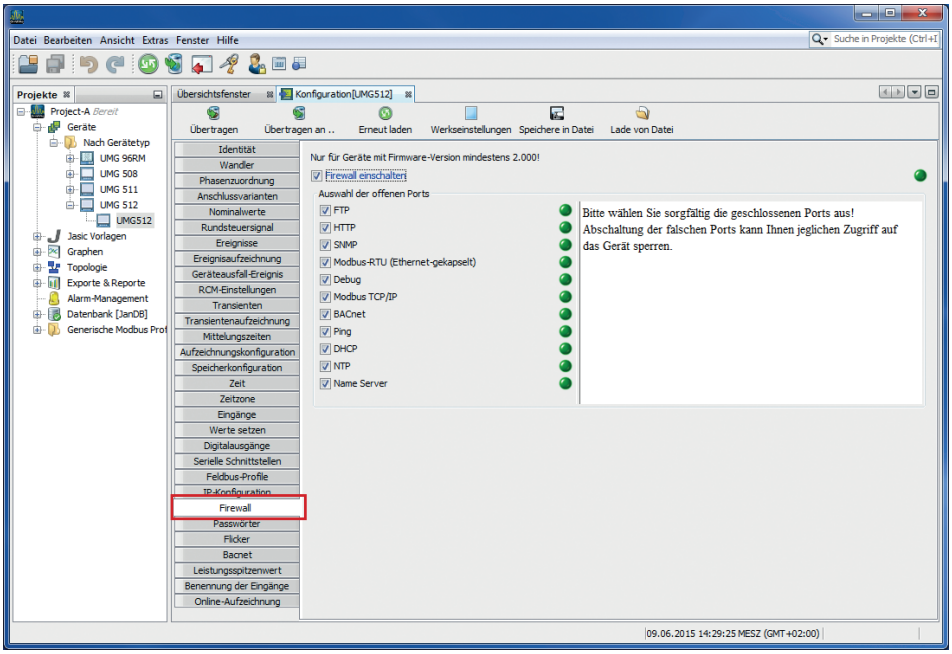


Abb.: Konfiguration der Firewall

- Über die Schaltfläche „Firewall“ wird die Firewall eingeschaltet.
  - Ab Release X.XXX ist diese bereits in der Werksauslieferung aktiviert.
  - Protokolle die Sie nicht benötigen, können hier deaktiviert werden.
  - Das Gerät lässt bei eingeschalteter Firewall nur Anfragen auf den jeweils aktivierten Protokollen zu

Protokolle	Port
FTP	Port 21, Datenport 1024 bis 1027
HTTP	Port 80
SNMP	Port 161
Modbus-RTU	Port 8000
Debug	PORT 1239 (für Service-Zwecke)
Modbus TCP/IP	Port 502
BACnet	Port 47808
DHCP	UTP Port 67 und 68
NTP	Port 123
Name Server	Port 53

- Für die rudimentäre Kommunikation mit der GridVis und über die Homepage sind die folgende Einstellung schon ausreichend:

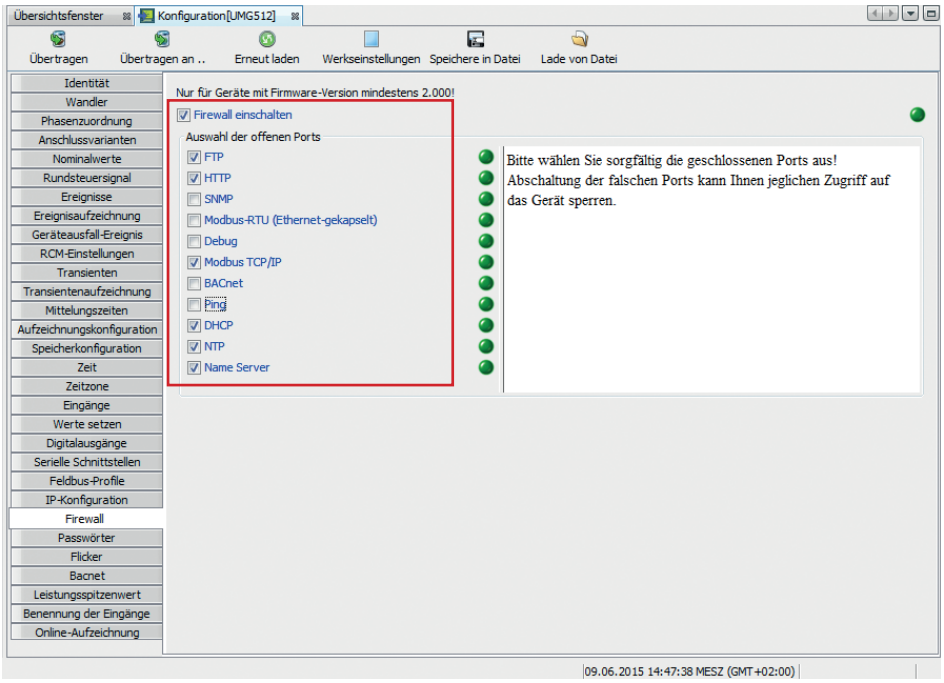


Abb.: Konfiguration der Firewall

- **Bitte wählen Sie aber sorgfältig die geschlossenen Ports aus!** Je nach gewähltem Verbindungsprotokoll kann z.B. auch nur über http kommuniziert werden.
- Sichern Sie die Änderungen mit der Übertragung der Daten an das Gerät (Schaltfläche „Übertragen“)

Display-Passwort

- Die Gerätekonfiguration über die Gerätetasten kann auch geschützt werden. D.h. nur nach der Eingabe eines Passwortes ist die Konfiguration möglich. Das Passwort kann am Gerät selbst oder über die GridVis im Konfigurationsfenster eingestellt werden.

Das Display Passwort darf maximal 5 Stellen lang sein und darf nur Zahlen enthalten.

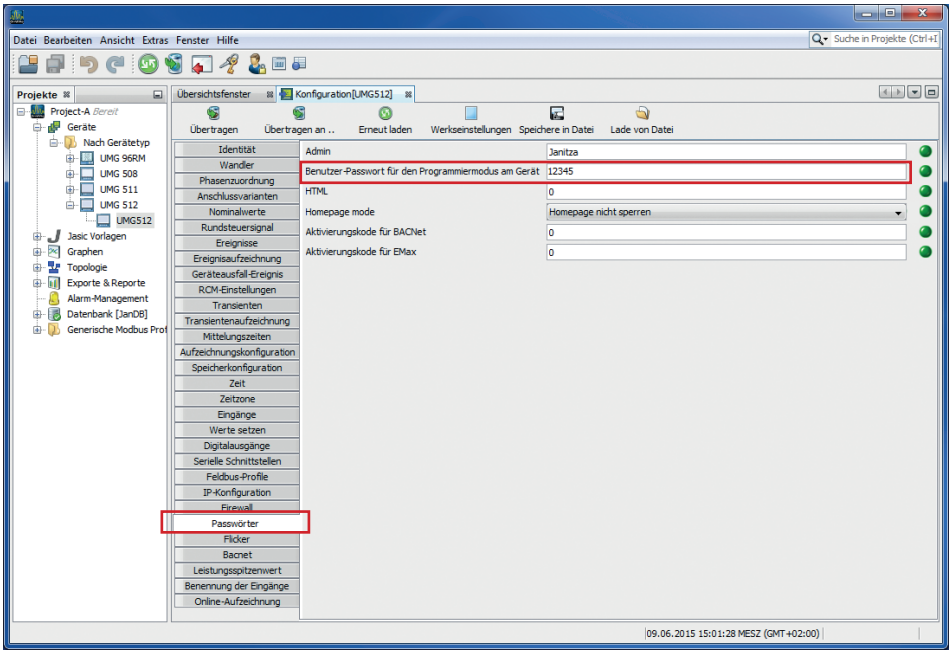
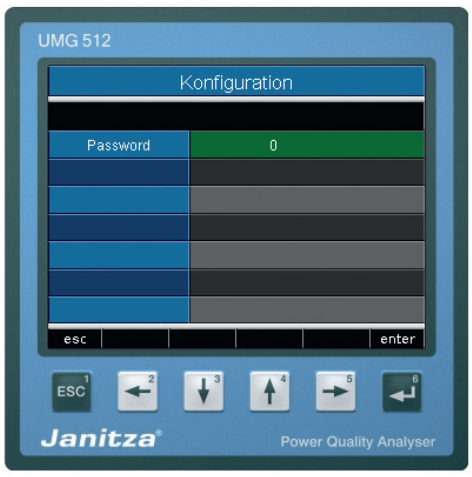


Abb.: Display-Passwort setzen

Step 1.)

- Rufen Sie das Konfigurationsfenster auf
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste „Konfiguration“
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende Gerät das Übersichtsfenster und wählen Sie die Schaltfläche „Konfiguration“ aus
- Wählen Sie im Konfigurationsfenster die Schaltfläche „Passwörter“ aus.
  Ändern Sie - wenn gewünscht - die Option „Benutzer-Passwort für den Programmiermodus am Gerät“
- Sichern Sie die Änderungen mit der Übertragung der Daten an das Gerät (Schaltfläche „Übertragen“)



Die Konfiguration am Gerät kann anschließend nur noch durch die Eingabe eines Passwortes geändert werden.

Homepage-Passwort

- Auch die Homepage kann vor unberechtigten Zugriff geschützt werden. Es gibt die folgenden Modi:

  - **Homepage nicht sperren**
    Die Homepage ist ohne Login erreichbar; Konfigurationen können ohne Login vorgenommen werden.
  - **Homepage sperren**
    Nach einem Login wird die Homepage und die Konfiguration für die IP des Benutzers für 3 Minuten freigegeben. Mit jedem Zugriff wird die Zeit wieder auf 3 Minuten gesetzt.
  - **Konfiguration separat sperren**
    Die Homepage ist ohne Login erreichbar; Konfigurationen können nur mit Login vorgenommen werden.
  - **Homepage und Konfiguration separat sperren**
    - Nach einem Login wird die Homepage für die IP des Benutzers für 3 Minuten frei gegeben.
    - Mit jedem Zugriff wird die Zeit wieder auf 3 Minuten gesetzt.
    - Konfigurationen können nur mit Login vorgenommen werden.

Hinweis: Als Konfiguration gelten nur die Variablen die in der init.jas liegen oder die Berechtigung „Admin“ haben

Das Homepage-Passwort darf maximal 8 Stellen lang sein und darf nur Zahlen enthalten.

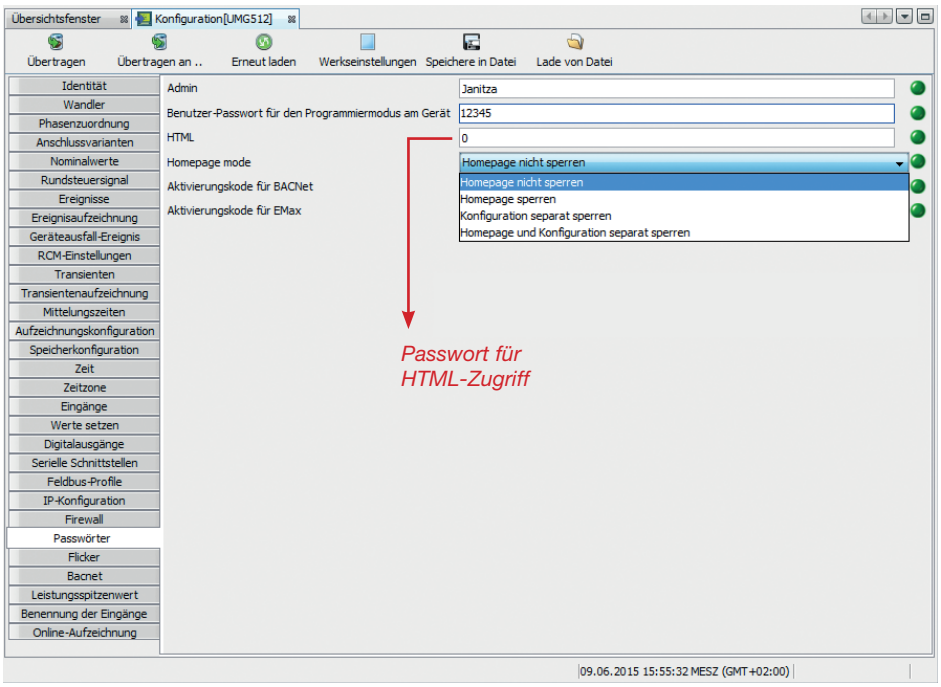


Abb.: Homepage-Passwort setzen

Nach der Aktivierung erscheint nach dem Aufruf der Gerätehomepage ein Login Fenster.

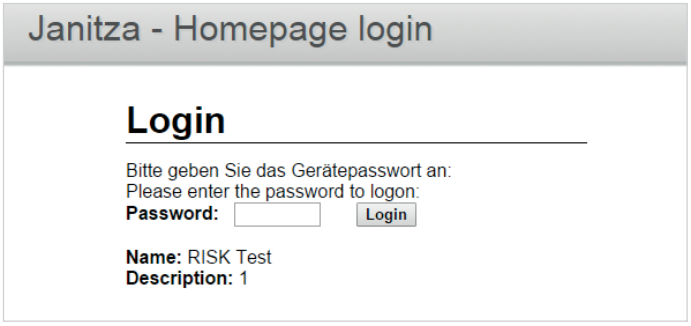


Abb.: Homepage-Login

Sicherheit Modbus-TCP/IP-Kommunikation

Eine Absicherung der Modbus-TCP/IP-Kommunikation (Port 502) ist nicht möglich. Der Modbus-Standard sieht keine Absicherung vor. Eine integrierte Verschlüsselung wäre nicht mehr nach Modbus-Standard und die Interoperabilität mit anderen Geräten wäre nicht mehr gewährleistet. Aus diesem Grund kann bei der Modbus-Kommunikation kein Passwort vergeben werden.

Wird von der IT vorgeschrieben, das nur abgesicherte Protokolle verwendet werden dürfen, muss in der Gerätefirewall der Modbus-TCP/IP-Port deaktiviert werden. Das Geräteadministrator-Passwort ist zu ändern und die Kommunikation muss über „TCP gesichert“ (FTP) oder „http gesichert“ erfolgen.

Sicherheit Modbus-RS485-Kommunikation

Eine Absicherung der Modbus-RS485-Kommunikation ist nicht möglich. Der Modbus-Standard sieht keine Absicherung vor. Eine integrierte Verschlüsselung wäre nicht mehr nach Modbus-Standard und die Interoperabilität mit anderen Geräten wäre nicht mehr gewährleistet. Dies betrifft auch die Modbus-Master-Funktionalität. D.h. für Geräte an der RS485-Schnittstelle kann keine Verschlüsselung aktiviert werden.

Wird von der IT vorgeschrieben, das nur abgesicherte Protokolle verwendet werden dürfen, muss in der Gerätefirewall der Modbus-TCP/IP Port-deaktiviert werden. Das Geräteadministrator Passwort ist zu ändern und die Kommunikation muss über „TCP gesichert“ (FTP) oder „http gesichert“ erfolgen.

Geräte an der RS485 Schnittstelle können jedoch dann nicht mehr ausgelesen werden!

Die Alternative ist in diesem Fall der Verzicht auf die Modbus-Master-Funktionalität und der ausschließliche Einsatz von Ethernet Geräten wie dem UMG 604 / 605 / 508 / 509 / 511 oder UMG 512.

Sicherheit „UMG 96RM-E“-Kommunikation

Das UMG 96RM-E bietet kein abgesichertes Protokoll. Die Kommunikation erfolgt bei diesem Gerät ausschließlich über Modbus-TCP/IP. Eine Absicherung der Modbus-TCP/IP-Kommunikation (Port 502) ist nicht möglich. Der Modbus-Standard sieht keine Absicherung vor. D.h. würde man eine Verschlüsselung integrieren, wäre diese nicht mehr nach Modbus-Standard und die Interoperabilität mit anderen Geräten wäre nicht mehr gewährleistet. Aus diesem Grund kann bei der Modbus-Kommunikation kein Passwort vergeben werden.