Sichere TCP/IP-Verbindung

Folgende Messgeräte verfügen über eine sichere TCP/IP-Verbindung:

- UMG 508
- UMG 509-PRO
- UMG 511
- UMG 512-PRO
- UMG 604-PRO
- UMG 605-PRO

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.

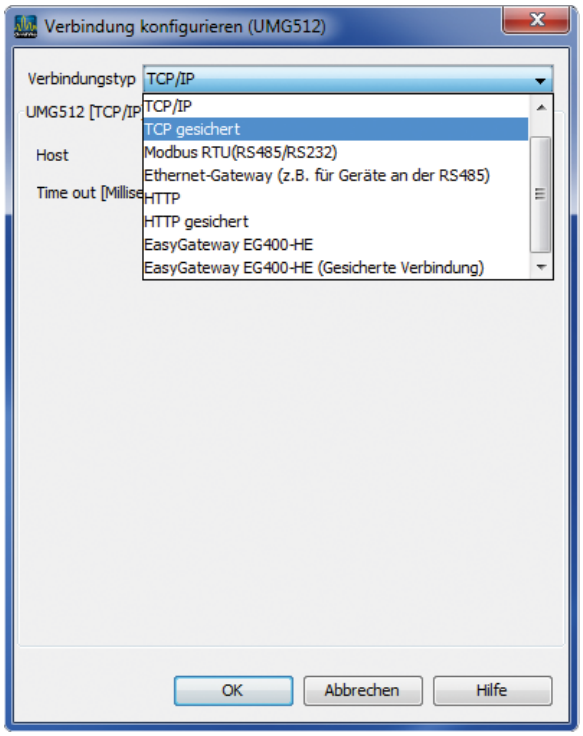
Die Netzwerksicherheit im Unternehmensnetzwerk spielt hierbei eine immer wichtigere Rolle.

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 wurden:

- Verbesserung der Challenge-Berechnung
- Nach drei falschen Logins wird die IP (vom Client) für 15 Minuten gesperrt
- 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 gesichert** auf gebaut werden.



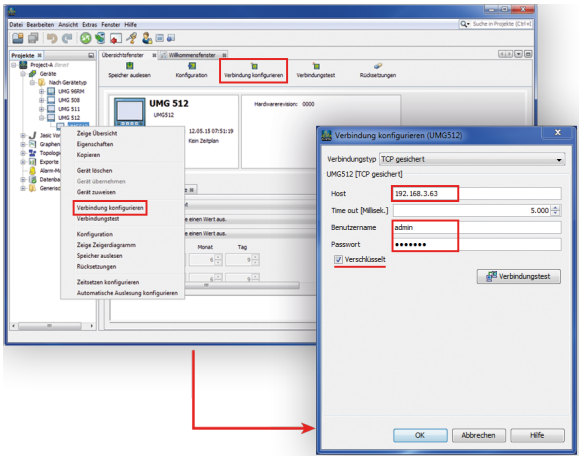
Passwort ändern

Für die gesicherte Verbindung ist ein User und ein 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.

1. Schritt

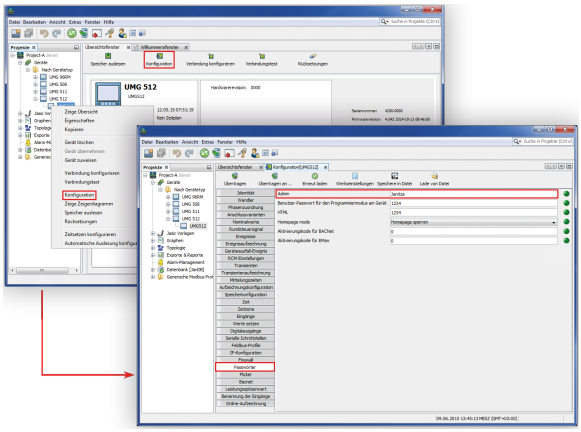
- Rufen Sie den Dialog **Verbindung konfigurieren** auf.
  Beispiel 1: Markieren Sie hierzu mit der Maustaste das entsprechende Gerät im Projekte-Fenster und wählen Sie im Kontextmenü der rechten Maustaste **Verbindung konfigurieren**.
  Beispiel 2: Öffnen Sie mit einem Doppelklick auf das entsprechende 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.
  Werkseinstellungen:
  Benutzername: *admin*
  Passwort: *Janitza*
- Setzen Sie den Menüpunkt **Verschlüsselt**.
  Hierdurch wird eine **AES256-Bit-Verschlüsselung** der Daten aktiviert.



2. Schritt

- 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**).



Hinweis

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!

Hinweis

Das Admin-Passwort darf maximal 30 Stellen lang sein und kann aus Zahlen, Buchstaben und Sonderzeichen bestehen (ASCII-Code 32 ... 126, mit Ausnahme der unten aufgeführten Zeichen). Außerdem darf das Passwortfeld nicht leer bleiben. Folgende Sonderzeichen dürfen nicht verwendet werden:

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

Leerzeichen (Code 32) ist nur innerhalb des Passworts zulässig. Als erstes und letztes Zeichen ist es nicht zulässig.

Wenn Sie auf eine GridVis-Version > 9.0.20 upgedatet haben und eines der oben beschriebenen Sonderzeichen verwenden, werden Sie beim Öffnen des Gerätekonfigurators aufgefordert, das Passwort gemäß dieser Regeln zu ändern.

Hinweis

Die Beschreibung **Passwort ändern** mit ihrem Passwortregeln gilt ebenso für den Verbindungstyp **HTTP gesichert**.