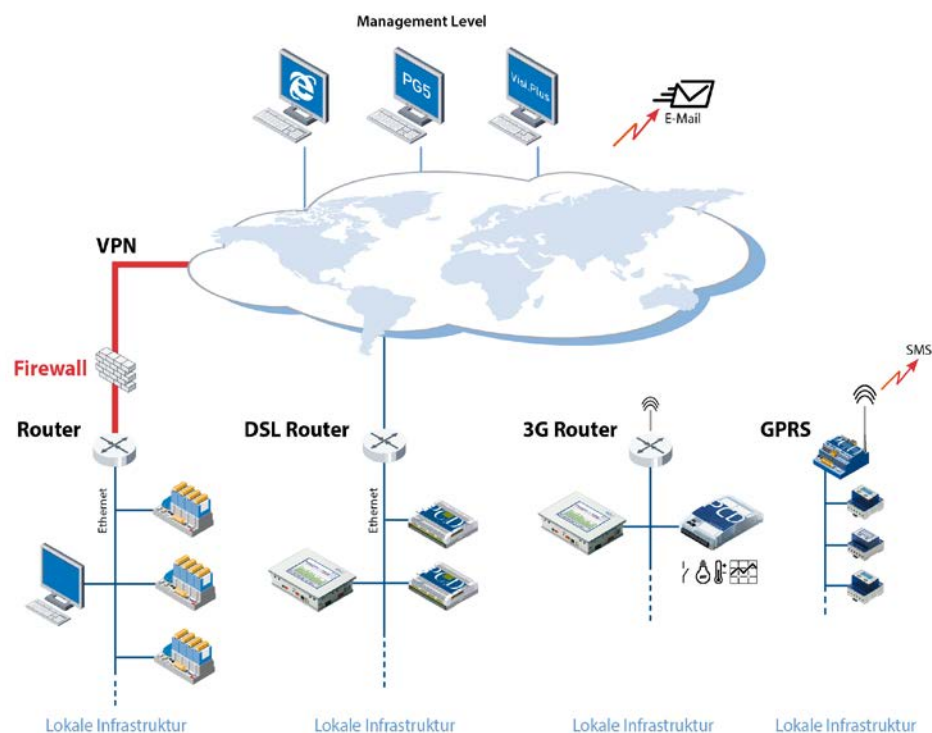


Hinweise für den Anschluss von Saia PCD-Steuerungen ans Internet



Dokument Historie

Version	Bearbeitung	Veröffentlichung	Bemerkungen
DE01	01.05.2013	01.05.2013	
DE02	03.05.2013	03.05.2013	Regeln für die Wahl eines Passwortes (S 7) Ether-S-Bus im Devicekonfigurator (S 18)
DE03	10.07.2013	11.07.2013	Komplette Überarbeitung nach Security Upgrade
DE04	14.02.2014	14.02.2014	Neues Firmenlogo

Inhalt

1. Einführung	3
2. Aufbau eines Virtual Private Network (VPN).....	6
Getestete VPN Router	7
3. Schutz des SBC Web-Servers	9
Funktion des Passwort-Mechanismus.....	9
3.1 Einstellungen im PG5 Devicekonfigurator.....	9
Konfigurieren des SBC Web-Server Passwortes.....	10
3.2 Eingabe des Passwortes im Web-Client	12
3.2.1 Micro-Browser Panel.....	12
3.2.2 Micro Browser Windows CE und eXP	14
3.2.3 iOS Micro-Browser App	15
3.2.4 PC-Browser mit Java Applet	15
3.2.5 SBC.Net Web Connect / WebFTP	16
3.3 Kompatibilität PG5 und COSinus Firmware Versionen	18
3.3.1 Aktivieren des SBC Web-Server Passwortes mit Device Konfigurator	19
3.3.2 Aktivieren des SBC Web-Server Passwortes mit Web Server Projekt (.wsp).....	19
4. FTP-Server Schutz.....	21
5. Ethernet S-Bus Schutz	23
6. IP Zugriffs Filter (IP Access List, ACL)	25
6.1 Device Konfigurator.....	25
6.2 Fupla FBoxen	27
7. Device Templates bearbeiten im PG5 Devicekonfigurator	28
8. Neue Benutzerverwaltung mit Zugriffsteuerung im WebEditor 8.....	29
8.1 Benutzerdatenbank.....	29
8.2 Download der Benutzerdatenbank und Service Key (Service Schlüssel)	30
8.3 Vergabe der Rechte auf Funktionen oder Elemente im WebEditor 8.....	32
8.4 Vorlagen für Benutzersteuerung.....	33
8.4.1 Login Vorlage.....	33
8.4.2 Logout Vorlage	33
8.4.3 Automatisches Logout bei Inaktivität.....	34
8.4.4 Passwort Ändern	34
8.5 Kompatibilität neue Zugriffsteuerung und alte Benutzeridentifikation.....	35

1. Einführung

Das vorliegende Dokument enthält wichtige Hinweise betreffend Schutzmassnahmen, die bei einem Anschluss von Saia PCD Steuerungen an das Internet beachtet werden müssen.

Die aktuellste Ausgabe findet man auf unserer Support Homepage:

<http://www.sbc-support.com/de/produktkategorie/kommunikationsprotokolle/pcd-im-internet.html>

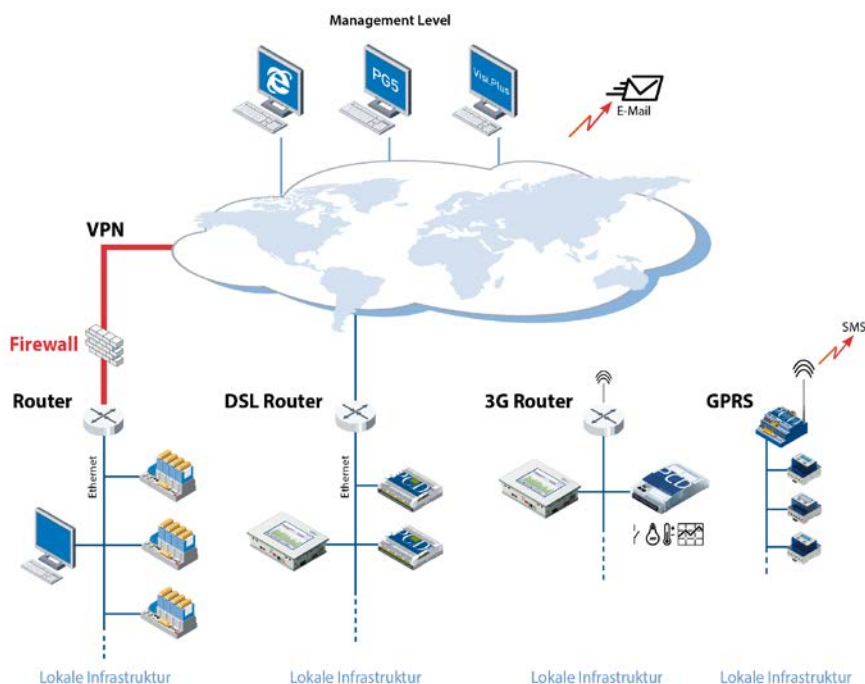
Die erste Ausgabe des Dokumentes haben wir Anfang Mai 2013 veröffentlicht. Darin wurden die Massnahmen mit den damals im PCD COSinus Betriebssystem und dem PG5 Softwarewerkzeug verfügbaren Schutzfunktionen beschrieben. Zwischenzeitlich haben wir unsere Softwarewerkzeuge angepasst, damit die Schutzfunktionen in den PCD-Steuerungen standardmässig aktiviert sind. Weiter haben wir den Passwort-Mechanismus im WebEditor verbessert. Neu ist ebenfalls die in den PCD-Steuerungen implementierte IP-Filter Funktion.

Trotzdem:

ein sicherer Betrieb der PCD-Steuerungen am Internet ist nur mit zusätzlichen externen IT-Komponenten mit integrierten Schutzfunktionen wie VPN, Firewall, Proxy-Server, etc. gewährleistet.

Zu diesem Zweck haben wir mehrere VPN-Router evaluiert und mit unseren PCD-Steuerungen getestet. In diesem Dokument sind die erfolgreich getesteten Geräte mit deren Bezugsquellen aufgeführt. Die detaillierte Beschreibung für die Konfiguration und Inbetriebnahme findet man im Dokument 30-004 „VPN-Router“ auf unserer Support Home Page.

Saia PCD-Steuerungen können auf unterschiedliche Arten ans Internet angeschlossen werden. Das nachfolgende Diagramm zeigt oft benutzte Anschlussmöglichkeiten.



Bei kleineren abgesetzten Installationen erfolgt der Anschluss einer Saia PCD-Steuerung an das Internet in den meisten Fällen mit einem DSL- oder 3G-Router. Ein PCD3.WAC wird direkt mit dem integrierten GPRS-Modem angeschlossen. Saia PCD-Steuerungen welche in einem geschützten lokalen Firmennetzwerk betrieben werden, sind in der Regel nur via einer sicheren Firewall und einem Virtual Private Network (VPN) von aussen zugänglich. In diesem Fall ist der Zugriffsschutz durch diese Komponenten sichergestellt.

Werden die PCD-Steuerungen hinter einem ungeschützten DSL- oder 3G-Router betrieben, so werden die IP-Dienste meist mittels Port-Forwarding auf die lokale PCD-Steuerung weitergeleitet. **In diesen Fällen sind sie einfach angreifbar.**

Nachfolgend eine kurze Auflistung der möglichen Schutzfunktionen:

- **Sichere Lösung mit Virtual Private Network (VPN)**
Eine PCD-Steuerung nur soll nur hinter einem Router oder einem Proxy-Server mit Firewall und einem geschützten VPN an das Internet angeschlossen werden. Von uns getestete und empfohlene Geräte findet man im Kapitel 2
- **Web-Server Passwortschutz**
Der Zugriff auf den SBC Web-Server kann mit einem 4 stufigen Passwort geschützt werden. Es handelt sich um einen einfachen unverschlüsselten Passwortschutz. Die Überprüfung der eingegebenen Passwörter erfolgt in der Steuerung. Im PG5 Devicekonfigurator ist ab Version 2.1.200 der Web-Server in den Standardeinstellungen neu deaktiviert. Wenn aktiviert, kann der Zugriff mittels einem Passwort geschützt werden. Die Beschreibung dazu findet man im Kapitel 3.
- **FTP-Server Zugriffsschutz**
Der Zugriff auf den FTP-Server und damit auf die Daten im PCD.Filesystem kann ebenfalls mit einem eigenen unverschlüsselten Passwort geschützt werden. Im PG5 Devicekonfigurator ist ab Version 2.1.200 der FTP-Server in den Standardeinstellungen neu deaktiviert. Wenn aktiviert, gibt es keinen Standard-User „root“, „rootpasswd“ mehr. Für den Zugriff muss der Programmierer einen eigenen User anlegen. Mehr Informationen dazu im Kapitel 4.
- **Ether-S-Bus Zugriffsschutz**
Das PG5 Programmiergerät nutzt das S-Bus Protokoll mit erweiterten Diensten für die Programmierung, und Inbetriebnahme der PCD-Steuerungen.
Im PG5 Devicekonfigurator ab Version 2.1.200 und ab einer PCD COSinus Version > 1.22.10 die Ether-S-Bus Kommunikation in den Standardeinstellungen deaktiviert. Damit wird auf der Ethernet-Schnittstelle kein S-Bus Protokoll (Datenaustausch und Programmierung) unterstützt. Wenn aktiviert, kann der Zugriff mit dem PG5 Programmiergerät zusätzlich mit einem einfachen, unverschlüsselten Passwort geschützt werden. Mehr Informationen dazu im Kapitel 5.
- **IP Zugriffs Filter**
Die PCD-Steuerungen verfügen neu ab COSinus Verson 1.22.10 über einen integrierten IP Zugriff Filter. In einer „White“ oder „Black“ Liste können berechnigte bzw. nicht berechnigte

IP-Adressen eingetragen werden. Mehr Informationen im dazu Kapitel 6.

- **Passwort-Mechanismus im WebEditor**

Der im WebEditor enthaltene und vom Java-Applet sowie Micro-Browser genutzte Passwortmechanismus dient der Benutzeridentifikation zur rollenbasierten Führung in der HMI-Applikation. Dieser Mechanismus wurde mit der neuen COSinus 1.22.10 und PG5 2.1.200 Version verbessert. Neu wird das eingegebene Passwort mit einem Hashcode verschlüsselt übertragen. Die Überprüfung des eingegebenen Passwortes erfolgt in der Steuerung. Weitere Informationen dazu im Kapitel 8.

Ändern der Standardeinstellungen im Devicekonfigurator

Die Standardeinstellungen können geändert und in einer eigenen Vorlage gespeichert werden. Damit werden beim Neuanlegen einer CPU die eigenen Standardeinstellungen übernommen. Mehr Informationen dazu im Kapitel 7.

Um die oben aufgeführten Schutzfunktionen in der beschriebenen Art nutzen zu können, benötigt man ein PG5 ab Version 2.1.200. Für einen Teil der Funktionen sind ebenfalls neue PCD-COSinus Versionen 1.22.10 erforderlich. Details findet man den entsprechenden Kapiteln.

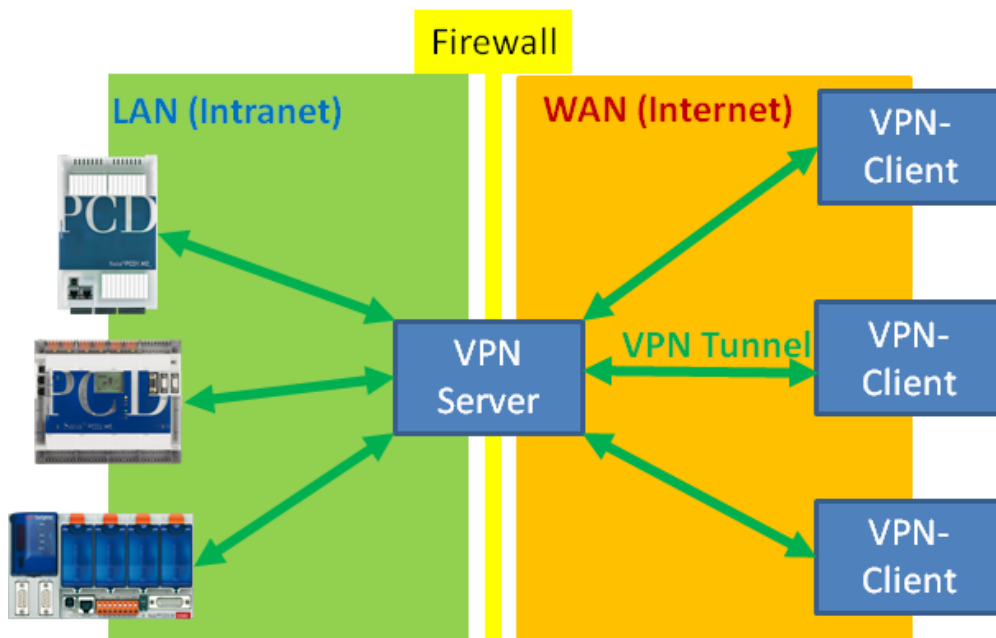
Das vorliegende Dokument sowie die neuen PG5 und COSinus Versionen sind auf der Supportseite unter dem folgenden Link verfügbar: <http://www.sbc-support.com/de/produktkategorie/kommunikationsprotokolle/pcd-im-internet.html>

2. Aufbau eines Virtual Private Network (VPN)

Mit einem VPN Tunnel ist es möglich über das Internet (WAN) auf Geräte in einem privaten Netzwerk auf eine sehr sichere Art und Weise zuzugreifen.

Grundsätzlich besteht ein solcher Aufbau aus einem VPN-Server und einem VPN-Client. Wir empfehlen die Nutzung eines Routers mit VPN Server Funktionalität. Der VPN Client wird meist als Software auf dem Client-Gerät (PC, Tablet, Smartphone, etc.) installiert.

Der VPN-Client bzw. die VPN-Client Software meldet sich über das Internet beim VPN-Server an. Ist die Anmeldung erfolgreich, befindet sich das Gerät auf welchem der VPN-Client gestartet wurde über einen gesicherten Tunnel im Intranet des VPN-Servers. Er kann ab diesem Moment alle Geräte im zugewiesenen Adressbereich des VPN-Servers erreichen und alle Dienste nutzen.



Bei der Wahl eines Routers sind je nach Anwendung unterschiedliche Punkte zu beachten.

Es soll ein Router mit VPN-Server Funktionalität verwendet werden. Für den Aufbau von VPN-Verbindungen nutzen die Router unterschiedliche Protokolle. Das Kommunikationsprotokoll muss sowohl vom Router wie auch vom VPN-Client Gerät (PC, Tablets, Smartphone) unterstützt werden. Das heisst, es muss sichergestellt werden, dass für das Client-Gerät die entsprechende VPN-Client Software verfügbar ist. IPSec ist wohl die am weitesten verbreitete Technologie und wird von vielen Geräten direkt unterstützt. IPSec ist jedoch in der Konfiguration und Anwendung recht komplex.

Einfacher zu konfigurieren ist die als OpenSource verfügbare Variante OpenVPN. Diese nutzt (auch) das SSL-Verschlüsselungsprotokoll und ist deshalb unproblematischer bei Firewalls. Für OpenVPN ist für viele Geräte und Betriebssysteme Client-Software verfügbar.

Getestete VPN Router

Draytek Vigor 2850Vn Router



Dieser Router ist für den Home Office Bereich bestimmt und verfügt über vielfältige Anschlussmöglichkeiten (Ethernet, DSL, USB, WLAN, ...) und leistungsstarke Funktionen (Firewall, VPN, ...). Er eignet sich gut zum Erstellen und Verwalten von VPN-Verbindungen für kleinere bis mittlere Netzwerke. Seine Funktionalität und Benutzeroberfläche sind leicht zu bedienen. Er unterstützt Standard VPN Clients von Windows, I-OS und Android.

Typenbezeichnung: Vigor 2850Vn

Bezugsquellen: Onlinehandel, Fachmärkte, Distributoren, ...

Internet: <http://www.draytek.de/produkte/modem-router/vigor2850-serie.html>

eurogard Service Router V2



Der EuroGard Service Router V2 ist ein industrieller Router für Hutschienenmontage mit 24VDC Spannungsversorgung. Er verfügt ebenfalls über unterschiedliche Anschlussmöglichkeiten (Ethernet, 3G) und ermöglicht den Aufbau von sicheren Verbindungen mit OpenVPN oder SSL. Die Konfiguration und die Benutzerführung für die Erstellung einer VPN-Verbindung ist schnell und einfach realisierbar. Er verfügt über einen OpenVPN Server und benötigt entsprechend OpenVPN Clients.

Typenbezeichnung: eurogard Service Router V2

Bezugsquellen: eurogard GmbH

Kaiserstrasse 100

D-52134 Herzogenrath

Internet: <http://www.eurogard.de>

Technische Daten Vigor 2850Vn und eurogard Service Router V2 im Vergleich

	DreyTek Vigor 2850Vn	EuroGard Service Router V2 (WLAN)	EuroGard Service Router V2 (UMTS)
Bestelldaten	2850Vn	ER 1201-WLAN	ER 1201-UMTS
Weitere Informationen	http://www.draytek.de/produkte/modem-router/vigor2850-serie.html	http://www.eurogard.de	http://www.eurogard.de
Einsatz/Bauform	Business / Home	Industriell	Industriell
Hutschienenmontage	Nein	Ja	Ja
Spannungsversorgung	230 VAC	24 VDC	24 VDC
VPN Eigenschaften			
Anzahl WAN Interfaces	3: LAN/Modem/USB	1: LAN	2: LAN/UMTS
Integriertes ADSL/VDSL Modem	Ja	Nein	Nein
VPN PPTP	Ja	Nein	Nein
VPN L2TP/IPSec	Ja	Nein	Nein
openVPN	Nein	Ja	Ja
Anz. VPN Clients	32 Verbindungen	30 Verbindungen	30 Verbindungen
Windows Client	Ja (in Windows integriert)	Ja (EurogardSRConnect)	Ja (EurogardSRConnect)
IOS Client	Ja (IPSec/L2TP, integriert in IOS)	Nein *	Nein *
Android Client	Ja (IPSec/L2TP, integriert in Android)	Nein *	Nein *
Erweiterungen			
3G / 4G Modem	Ja, mit USB-Stick	Nein	Ja, mit integriertem UMTS Modem

* IOS oder Android Systeme können heute via WLAN an den Router angebunden werden. Dafür werden jeweils 2 Router benötigt. Ein VPN-Server sowie ein VPN-Client. Unterstützung von VPN auf mobilen Geräten ist in Vorbereitung.

Details zur Konfiguration und Verwendung der Router für sichere VPN-Verbindungen mit Saia PCD Steuerungen findet man in der Dokumentation 30-004

3. Schutz des SBC Web-Servers

Der Zugriff auf den SBC Web-Server kann mit einem Passwort-Mechanismus geschützt werden.

Funktion des Passwort-Mechanismus

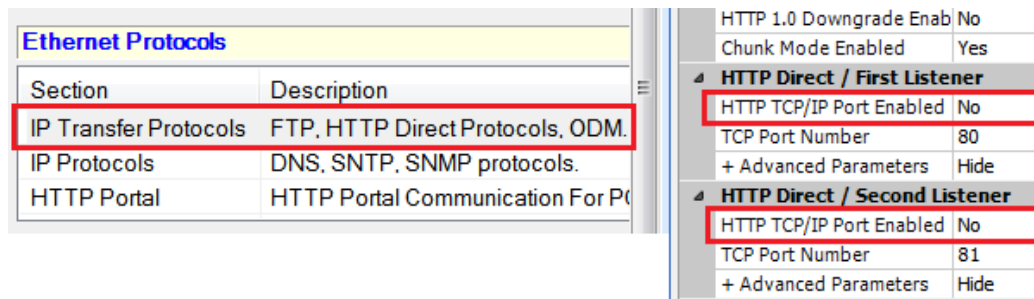
Dieser Passwort-Mechanismus erlaubt es den generellen Zugriff auf Dateien als auch auf alle PCD-Medien (Register, Flag, DB/Texte, etc.) zu blockieren. Bei einem Zugriff mit einem Browsergerät (PC-Browser, Micro-Browser Panel, iPad,) auf den SBC Web-Server überprüft der Server ob das in der PCD-Steuerung hinterlegte Passwort korrekt eingegeben wurde. Wurde kein Passwort eingegeben oder das direkt übergebene Passwort ist ungültig, erscheint im Browser-Gerät ein Dialog das Passwort einzugeben. Der Vergleich des Passwortes findet im Web-Server der PCD-Steuerung statt. Die eingegebenen Passwörter werden unverschlüsselt übertragen.

3.1 Einstellungen im PG5 Devicekonfigurator

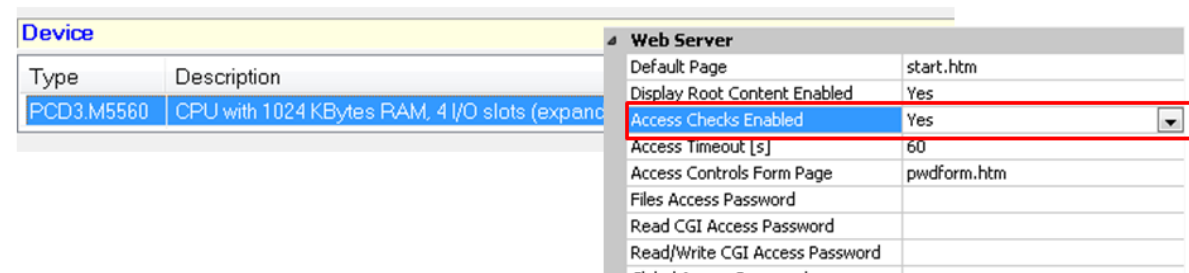
Im Device Konfigurator vom PG5 Programmierwerkzeug werden die Konfigurationseinstellungen der Saia PCD-Steuerung vorgenommen. Die Einstellungen für den Web-Server befinden sich in den Menüs „IP Transfer Protocols“ sowie im „Device Type“.

Beim Anlegen einer neuen CPU im Device Konfigurator vom PG5 2.1.200 ist der Web-Server neu in den Standardeinstellungen deaktiviert!

Der Web-Server kann bzw. muss im Device Konfigurator aktiviert werden.



Bei aktiviertem Web-Server ist neu auch der Passwortschutz aktiviert.



Mit dieser Einstellung muss ein Passwort konfiguriert werden. Siehe dazu im nächsten Abschnitt. Falls kein Passwort konfiguriert werden soll, muss der Parameter „Access Checks Enabled“ deaktiviert werden.

Access Check Enabled:

Aktiviert den Passwortmechanismus des SBC Web-Servers

Standardeinstellung: „Yes“

Empfohlene Einstellung: „Yes“

Konfigurieren des SBC Web-Server Passwortes

Das Passwort wird nur überprüft wenn der Parameter „Access Checks Enabled“ auf „Yes“ gesetzt ist.

Device		Web Server	
Type	Description		
PCD3.M5560	CPU with 1024 KBytes RAM, 4	Default Page	start.htm
		Display Root Content Enabled	Yes
		Access Checks Enabled	Yes
		Access Timeout [s]	60
		Access Controls Form Page	pwdform.htm
		Files Access Password	
		Read CGI Access Password	
		Read/Write CGI Access Password	
		Global Access Password	

Access Timeout

Unterbricht bei einer S-Bus http Verbindung die Kommunikation, so wird nach Ablauf der eingestellten Zeit die Abfrage des Passworts erneut angefordert. Der Parameter kommt nur bei http via S-Bus zur Anwendung.

Standardeinstellung: „60s“

Empfohlene Einstellung: „Standardwert nicht ändern“

Access Controls Form Page

Bei einem Zugriff ohne gültiges Passwort wird diese Seite zur Eingabe eines Passwords aufgerufen.

Standardeinstellung: „pwdform.htm“

Empfohlene Einstellung: „Standardwert nicht ändern“

Bemerkung: diese Seite ist im System des Web-Servers gespeichert. Bei Bedarf kann der Programmierer auch seine eigene Login-Seite erstellen.

Einstellung der Passwörter für den Zugriffschutz

Der SBC Web-Server verfügt über einen 4 stufigen (Level) Zugriffschutz:

- „File Access“ → Level 1
- „Read CGI Access“ → Level 2
- „Read/Write CGI Access“ → Level 3
- „Global Access“ → Level 4

In den meisten Fällen reicht es den Zugriff auf den SBC Web-Server generell zu schützen. Dazu muss das **Level 1 Passwort (File Access)** definiert werden. Wir empfehlen unbedingt dieses Passwort zu definieren! Alle anderen Passwörter müssen nicht definiert werden! Nach dem erfolgreichen Login sind automatisch alle Level 1-4 freigeschaltet.

Sollte es trotzdem einmal notwendig sein mit Passwort-Login zwischen Lese- und Schreibrechten zu unterscheiden, gelten die nachfolgenden Regeln:

- ist bei keiner Stufe ein Passwort definiert, so ist kein Schutz aktiv und der Benutzer hat ohne Passwortheingabe den vollen Zugriff auf alle Funktionen
- ein definiertes Passwort aktiviert den Zugriffsschutz ab dieser Stufe(Level). Beispiel: es ist nur ein Passwort für Level 1 definiert. → Ist der Web-Server für alle Zugriffe geschützt und es wird die Eingabe eines Passwortes verlangt. Nach Eingabe des Passwortes sind alle darüber liegenden „Level 2-4“ auch freigeschaltet, sofern diese keinen PW-Schutz haben.
- ein definiertes Passwort gibt den Zugriff für diesen Level und alle höheren frei bzw. bis zum nächst höheren Level mit einem Passwortschutz. Beispiel: Passwort für Level 1 und Passwort für Level 3 definiert. → Eingabe Passwort Level 1 schaltet auch Level 2 frei. Eingabe Passwort Level 3 schaltet Level 1-4 frei.

File Access Password:

Mit diesem Passwort wird der Lesezugriff für Dateien und alle darüber liegenden Level geschützt bzw. freigegeben.

Standardeinstellung: „“

Empfohlene Einstellung: „**Passwort definieren**“

→ Unbedingt definieren, der Web-Server ist damit vollständig geschützt.

Achtung: der Passwort-Dialog wird generell (für alle Stufen) nur dann angezeigt, wenn für diese Stufe ein Passwort definiert wurde.

Read CGI Access Password:

Mit diesem Passwort wird der Lesezugriff auf das CGI Interface und alle darüber liegenden Level geschützt bzw. freigegeben. Das CGI-Interface ist für das Lesen der PCD-Medien (Register, DB`s, Flags, Texte, ...) geschützt.

Standardeinstellung: „“

Empfohlene Einstellung: „“

Soll ein Benutzer nur mit Passwort Lesezugriff haben, um bspw. Log-Daten auszulesen oder Anlagenzustände anzuzeigen, reicht es das Level 1 (**File Access**) und Level 3 (**Read/Write CGI Access**) Passwort zu definieren.

Read/Write CGI Access Password:

Mit diesem Passwort wird der Schreibzugriff auf das CGI Interface und alle darüber liegenden Level geschützt. Das CGI-Interface ist für das Schreiben der PCD-Medien (Register, DB`s, Flags, Texte, ...) geschützt.

Standardeinstellung: „“

Empfohlene Einstellung: „nur falls notwendig ein Passwort definieren für Schreibschutz“

Soll ein Benutzer nur mit Passwortheingabe Schreibzugriff haben, muss hier ein Passwort definiert werden.

Global Access Password:

Diese Passwort ist aus historischen Gründen noch vorhanden und muss nicht definiert werden.

Standardeinstellung: „“

Empfohlene Einstellung: „nicht notwendig“

Regeln für die Wahl eines Passwortes:

Das Passwort kann bis zu 31 Zeichen lang sein und darf keine Sonderzeichen, Umlaute oder Leerzeichen enthalten. Es findet keine Unterscheidung zwischen Groß- und Kleinbuchstaben statt.

Um einen möglichst guten Schutz zu erhalten, empfehlen wir mindestens 10 Zeichen (je länger desto sicherer) bestehend aus Buchstaben und Zahlen zu wählen. Es sollen keine einfach zu erratende Wörter wie z.B. der Anlagenname genutzt werden.

3.2 Eingabe des Passwortes im Web-Client

3.2.1 Micro-Browser Panel

Der SBC Web-Server Passwortschutz wird von den Micro-Browser Panel ab Version **1.20.36** unterstützt.

Ab dieser Version können die Passwörter im Setup-Menü der Micro-Browser Panel hinterlegt werden. Nachfolgend die Anleitung zur Konfiguration der Passwörter.

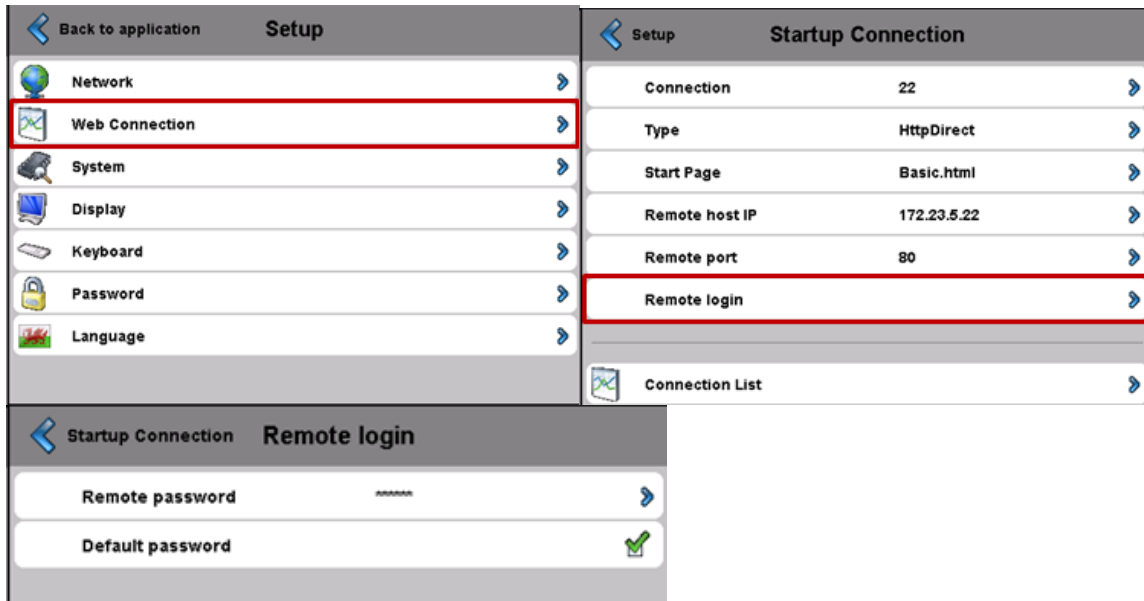
Ist kein Passwort hinterlegt, wird beim Verbindungsaufbau die Meldung „**PCD Password required!**“ auf dem Bildschirm des Panels ausgegeben. Für einen erfolgreichen Verbindungsaufbau muss das Passwort zwingend im Setup-Menü hinterlegt sein.

Schritt 1) Setup Menü öffnen

Das Setup Menü kann beim Starten des Gerätes als auch durch das längere Drücken (10sek) einer leeren Fläche in der Applikation geöffnet werden.

Schritt 2) Startup Web Connection bearbeiten

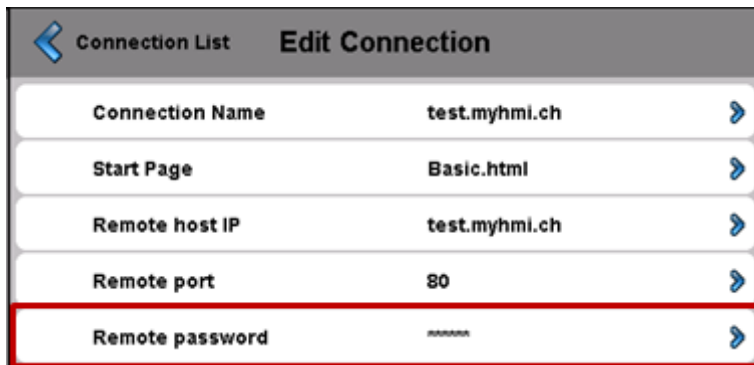
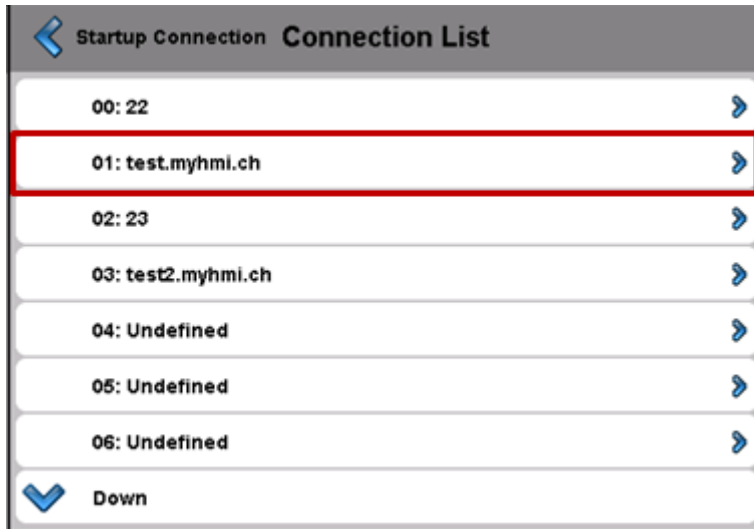
- ➔ Setup Menü ➔ Web Connection ➔ Remote login
- ➔ Remote Password
 - Hier muss das Password für den Zugriff auf den Web-Server eingetragen werden.
 - Es ist möglich dieses Password als default Password zu setzen. In diesem Fall wird dieses Password immer verwendet wenn bei einer Verbindung ein Password vom Web-Server gefordert wird. Wird ein Password in einer Station der Connection List definiert wird dieses zuerst verwendet. Ist es nicht möglich mit dem in der Station hinterlegten Passwords einen erfolgreichen Login zum Web-Server herzustellen, wird das in der Startup Verbindung definierte Default Password für einen weiteren Login-Versuch verwendet.



Schritt 3) Connection List bearbeiten

Wenn mit dem gleichen Micro-Browser Panel auf mehrere Steuerungen mit unterschiedlichen Passwörtern zugegriffen werden soll, muss für jede Steuerung eine Connection in der Connection List mit dem dazugehörigen Passwort erstellt werden.

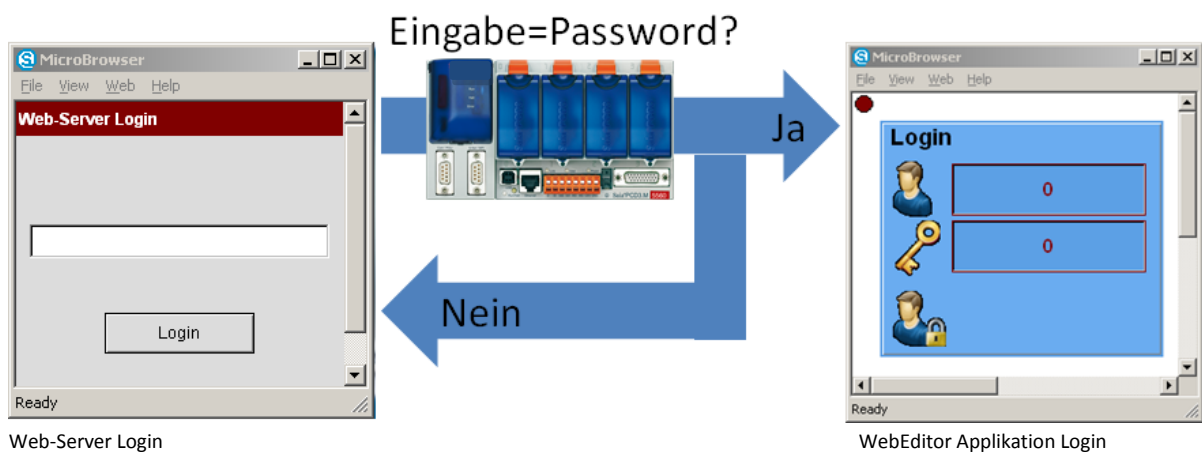




3.2.2 Micro Browser Windows CE und eXP

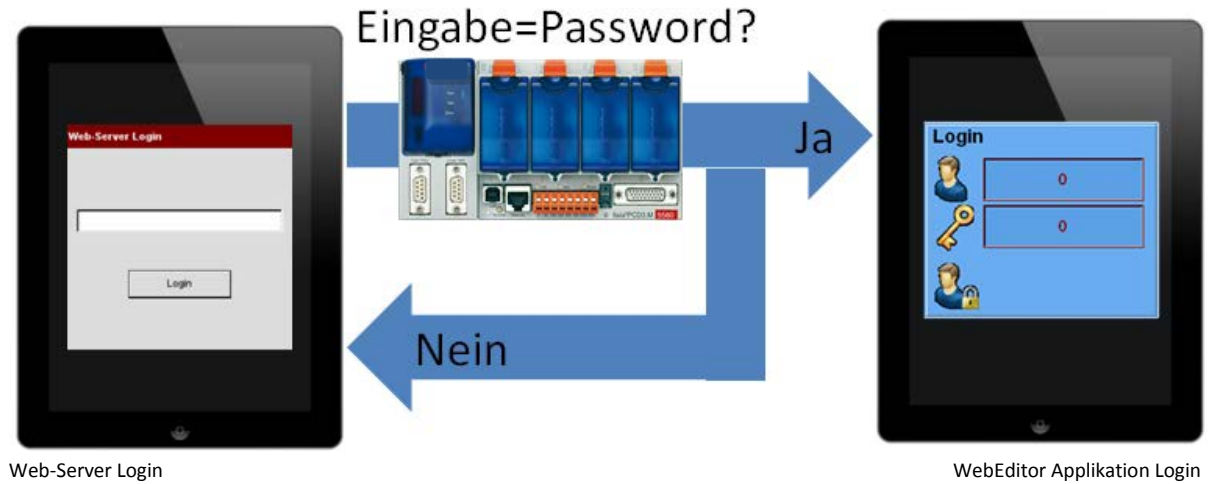
Der Micro-Browser für Windows basierende Geräte unterstützt das Web-Server Passwort-Login ab Version 1.5.15.131c.

Bei einer PCD-Steuerung mit aktiviertem Web-Server Passwort muss sich der Benutzer zuerst für den Web-Server Zugriff anmelden und anschliessend sich noch für die Benutzerführung in der WebEditor Applikation identifizieren.



3.2.3 iOS Micro-Browser App

Die Micro-Browser App für Apple-Geräte unterstützen das Web-Server Passwort-Login ab Version 1.5.15.130

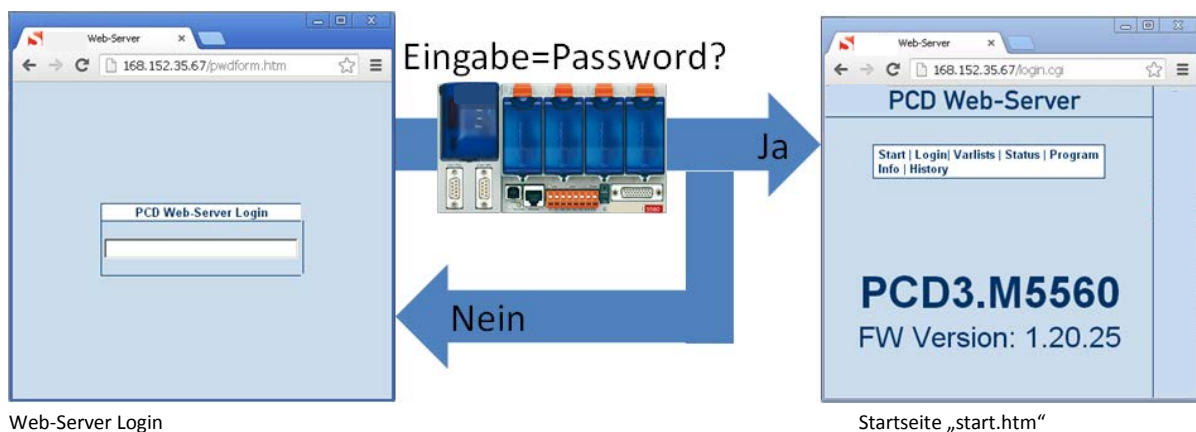


3.2.4 PC-Browser mit Java Applet

Die PC-Browser mit Java Applet unterstützen den Passwort-Mechanismus des Saia PCD Web-Server. Beim Zugriff auf einen durch ein Passwort geschützten Saia PCD Web-Server wird automatisch die im Device Konfigurator hinterlegte Datei „pwdform.htm“ geladen. Diese erlaubt es ihnen das eingebene Passwort an den Saia PCD Web-Server zu senden. Ist die Eingabe korrekt wird die im Device Konfigurator hinterlegte „start.htm“ geladen und die Visualisierung gestartet.

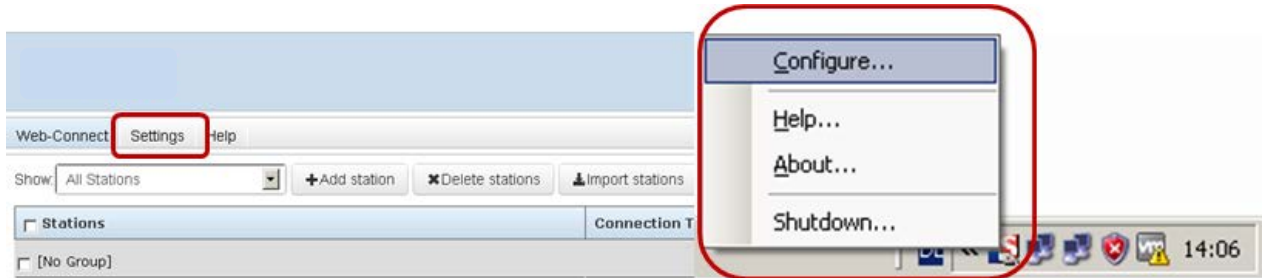
Bemerkung: soll direkt die Web-Applikation geladen werden, so muss im Devicekonfigurator die HTML-Seite des WebEditor Projektes eingetragen werden.

Hinweis: die Statusseite des SBC Web-Servers kann jederzeit im PC-Browser durch die Eingabe von „Status.htm“ angezeigt werden.



3.2.5 SBC.Net Web Connect / WebFTP

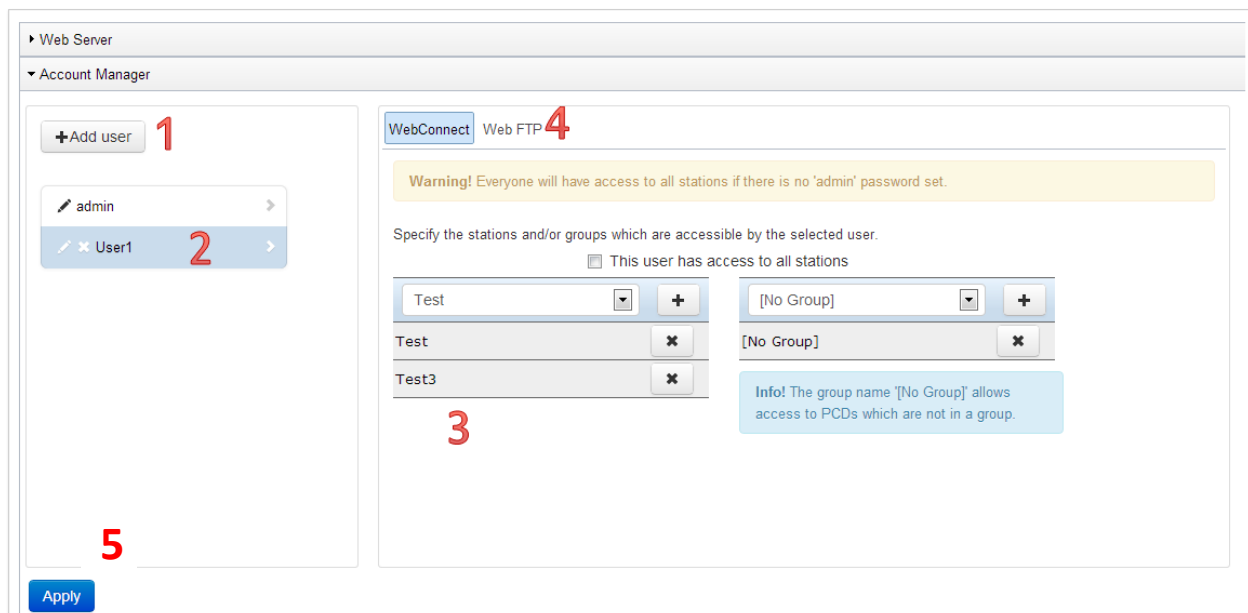
SBC.Net verfügt bereits über ein eigenes integriertes Account Management, welches über die SBC.Net Web-Oberfläche verwaltet werden kann.



In den Settings von SBC.Net befindet sich das Account Management. Hier können User und Passwörter als auch die für den selektierten User relevanten Rechte definiert werden.

Ein Password für den Benutzer „admin“ muss definiert werden da sonst der Zugriff auf alle Stationen möglich ist.

- 1) Hinzufügen eines neuen Benutzers. Jeder Benutzer benötigt ein Benutzername und dazugehöriges Password.
- 2) Liste der aktuell existierenden Benutzer. Es ist möglich den Benutzer zu bearbeiten oder zu löschen.
- 3) Rechte des aktuell selektierten Benutzers. Die Rechte verändern sich in der Anhänglichkeit aktivierter Funktionen von SBC.Net
- 4) Selektieren der Funktionen Web Connect oder Web FTP
- 5) Apply, Übernehmen der Änderungen des selektierten Benutzers.

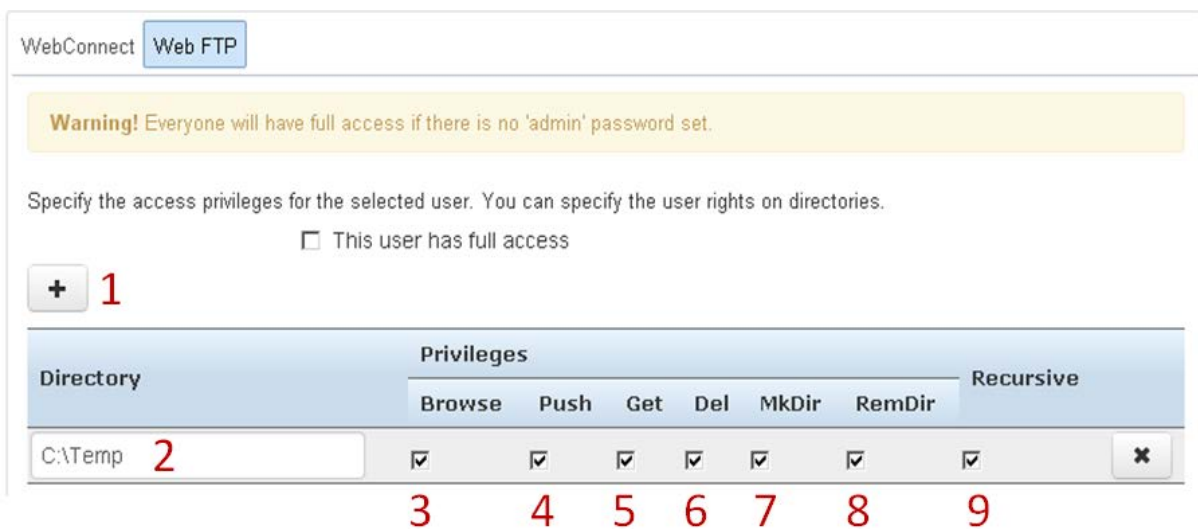


Das Tab WebFTP ermöglicht das Setzen von Benutzerrechten des lokalen WebFTP Servers von SBC.Net

- 1) Hinzufügen eines neuen Verzeichnisses für den aktuell selektierten Benutzer
- 2) Ort des lokalen Verzeichnisses welches über WebFTP Freigegeben werden soll.

Der Benutzer hat Rechte für das

- 3) Browse: Einsehen des aktuellen Inhaltes des Verzeichnisses
- 4) Push: Schreiben von Dateien in das Verzeichnis
- 5) Get: Lesen aus von Dateien aus dem Verzeichnis
- 6) Del: Löschen von Dateien im Verzeichnis
- 7) Mkdir: Erstellen von Unterverzeichnissen
- 8) RemDir: Umbenennen von existierenden Verzeichnissen
- 9) Recursive: Einschließen aller Unterverzeichnisse in die aktuell definierte Rechte kette.

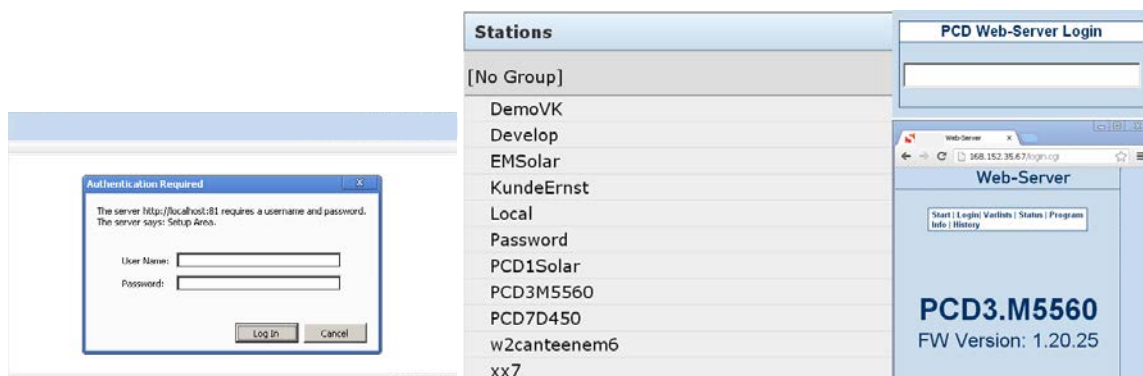


The screenshot shows the 'WebConnect' interface with the 'Web FTP' tab selected. A yellow warning box states: 'Warning! Everyone will have full access if there is no 'admin' password set.' Below this, a message says 'Specify the access privileges for the selected user. You can specify the user rights on directories.' There is a checkbox labeled 'This user has full access' which is unchecked. A red '+ 1' button is visible. Below is a table with columns for 'Directory', 'Privileges', and 'Recursive'. The 'Directory' column contains 'C:\Temp' with a red '2' next to it. The 'Privileges' columns are 'Browse', 'Push', 'Get', 'Del', 'Mkdir', and 'RemDir'. The 'Recursive' column has a checkbox. All privilege checkboxes are checked. Below the table, red numbers 3 through 9 are placed under the corresponding privilege columns.

Directory	Privileges						Recursive
	Browse	Push	Get	Del	Mkdir	RemDir	
C:\Temp 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

3 4 5 6 7 8 9

Beim Öffnen von SBC.Net WebConnect kommt eine Aufforderung zur Eingabe von Benutzer und Password. Nach der Anmeldung stehen ihnen die Rechte des angemeldeten Benutzers zur Verfügung. Durch das Klicken einer für diesen Benutzer zur Verfügung gestellte Station kann auf den Saia-PCD Web Server zugegriffen werden.



The image shows three screenshots related to the authentication process. On the left is an 'Authentication Required' dialog box with fields for 'User Name' and 'Password', and 'Log In' and 'Cancel' buttons. In the center is a 'Stations' list with the following entries: [No Group], DemoVK, Develop, EMSolar, KundeErnst, Local, Password, PCD1Solar, PCD3M5560, PCD7D450, w2canteenem6, and xx7. On the right is a 'PCD Web-Server Login' window with a text input field and a 'Web-Server' window showing the login page for 'PCD3.M5560' with 'FW Version: 1.20.25'.

3.3 Kompatibilität PG5 und COSinus Firmware Versionen

Die beschriebenen Schutzfunktionen werden von den Saia PCD Steuerungen schon seit längerem unterstützt. Zur korrekten Anwendung müssen die Funktionen auch von den Browsergeräten und dem PG5 Devicekonfigurator unterstützt werden.

Folgende Versionen der Micro-Browser Geräte unterstützen den Web-Server Passwortmechanismus:

Produkt	Product Typ	Firmware ab Version	Bemerkungen
VGA und SVGA Micro-Browser Web-Panel	PCD7.D4xxWTPF	1.20.36	
	PCD7.D457VTCF	1.20.36	
	PCD7.D410VTCF	1.20.36	
	PCD7.D412VTPF	1.20.36	
	PCD7.D4xxVT5F	1.20.25	
Produkt	Product Typ	Firmware Version	Bemerkungen
QVGA Micro-Browser Panel	PCD7.D457BTCF	Nicht unterstützt	
	PCD7.D457STCF	Nicht unterstützt	
	PCD7.D457SMCF	Nicht unterstützt	
Product	Product Typ	Firmware ab Version	Bemerkungen
eWinCE Micro-Browser	PCD7.D51xxTX010	1.5.15.131c	
	PCD7.D51xxTL010	1.5.15.131c	
	PCD7.D51xxTA010	1.5.15.131c	
eWinXP Micro-Browser	PCD7.D61xxTL010	1.5.15.131	
	PCD7.D61xxTA010	1.5.15.131	
Product	Product Typ	Firmware Version	Bemerkungen
iOS MB App		1.5.15.130	
iOS MB LITE App		1.5.15.130	
Android MB App		Noch nicht unterstützt	Neue Version in Kürze verfügbar

Die nachfolgende Tabelle zeigt die Abhängigkeiten zwischen den verschiedenen Komponenten. Es ist zu beachten, dass die Versionen bei allen Micro-Browser Geräten upgedated werden müssen.

	Web Server Project (.wsp)	Device Konfigurator
FW < 1.14.nn	Yes*	No
FW ≥ 1.14.nn < 1.20.nn	Yes*	Yes
FW ≥ 1.20.nn	No	Yes

*Mit PG52.x muss im Device Konfigurator die Firmware Version < 1.14.nn eingestellt werden

Für das Aktivieren des Web-Server Passwortes ist **kein** Update des PG5 Programmierwerkzeuges erforderlich.

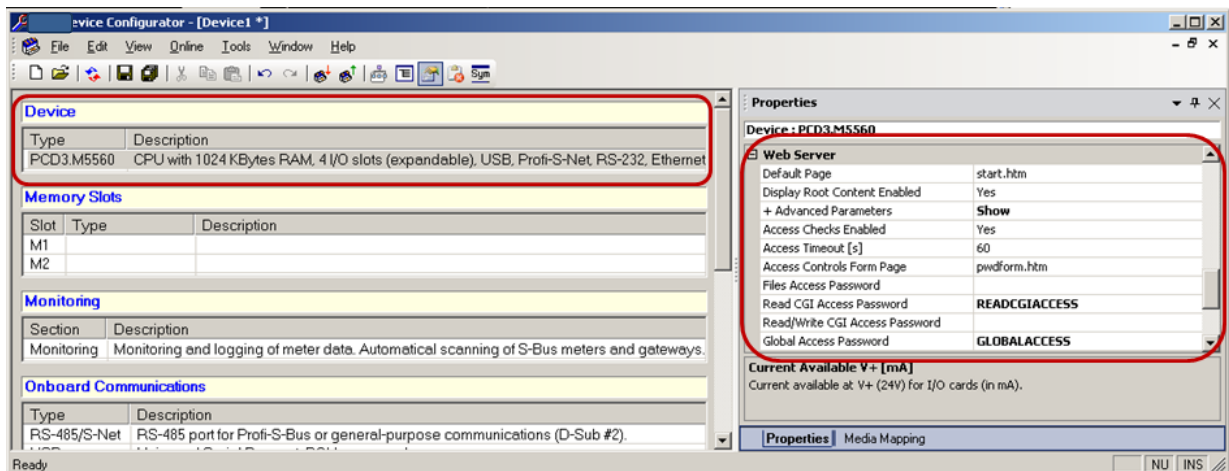
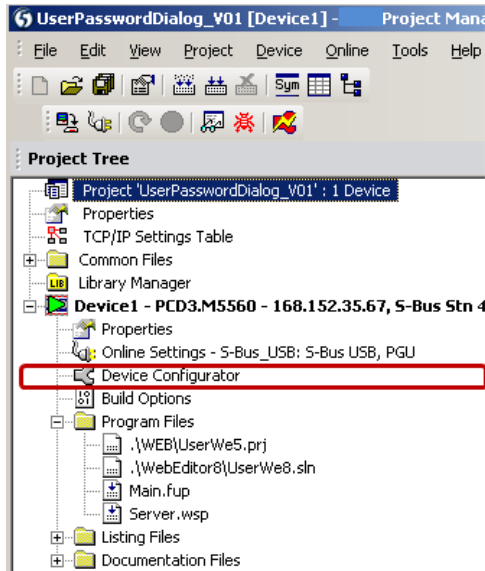
Bei Firmware Versionen kleiner 1.14.nn muss das Passwort und die Web-Server Einstellungen mit dem Web Server Projekt (.wsp) definiert werden.

Firmware Versionen im Bereich von 1.14.nn bis 1.16.nn unterstützen sowohl die Konfiguration über das Web Server Projekt als auch über den Device Konfigurator.

Ab Firmware Version 1.20.nn sind Web-Server Einstellungen nur noch über den Device Konfigurator änderbar.

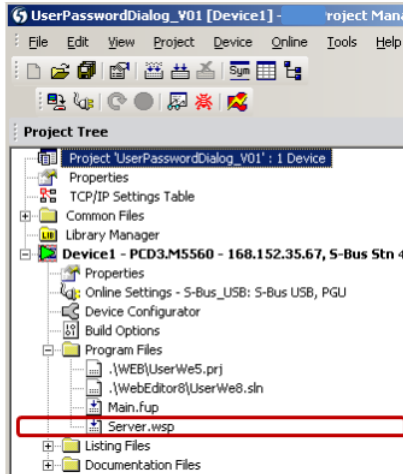
3.3.1 Aktivieren des SBC Web-Server Passwortes mit Device Konfigurator

Die Konfiguration des Web Servers wird im Device Konfigurator definiert. Die Einstellungen befinden sich im Tab der CPU



3.3.2 Aktivieren des SBC Web-Server Passwortes mit Web Server Projekt (.wsp)

Die Konfiguration des Web Server wird durch das Web Server Projekt definiert. Dieses ist Bestandteil der Program Files und wird beim Programm-Download in die Steuerung geladen.



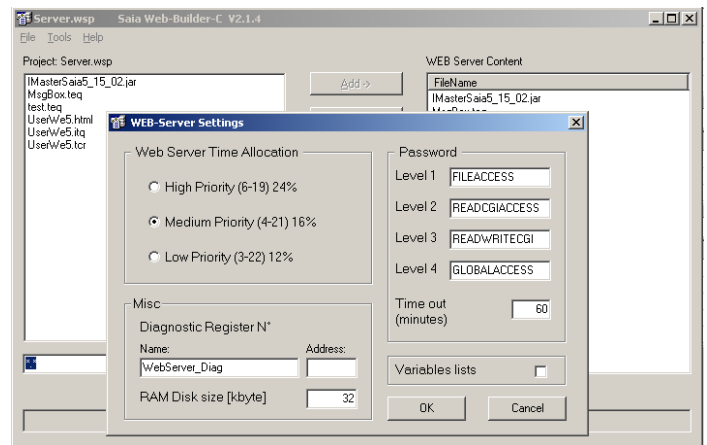
Im Web-Server Projekt (.wsp) können Dateien geladen als auch die Passwörter für 4 Level gesetzt werden.

Level 1: File Access Password:

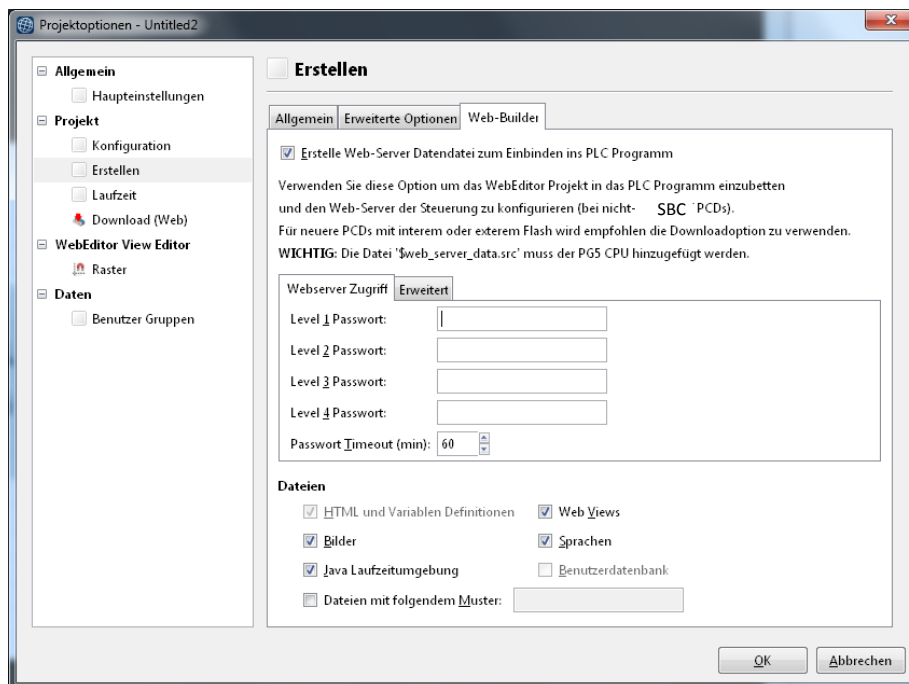
Level 2: Read CGI Access Password:

Level 3: Read/Write CGI Access Password:

Level 4: Global Access Password:



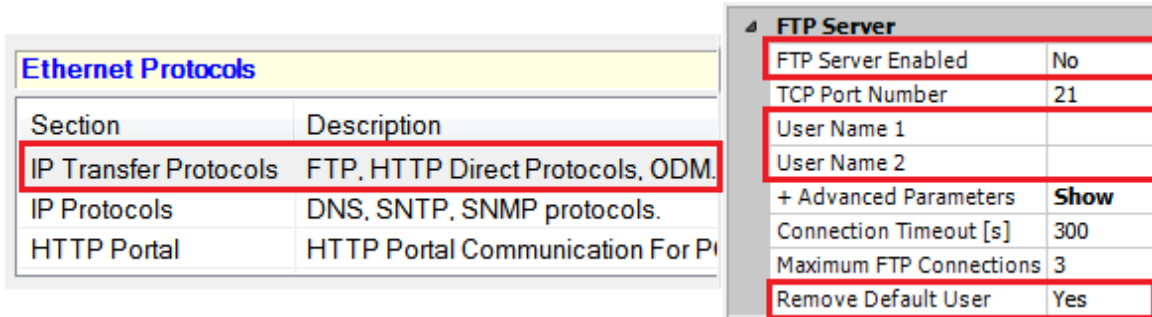
Im WebEditor 8 werden diese Einstellungen in rojektsettings vorgenommen.



4. FTP-Server Schutz

Beim Anlegen einer neuen CPU im Device Konfigurator ab PG5 2.1.200 ist der FTP-Server in den Standardeinstellungen neu deaktiviert. Der Default User „root“, „rootpasswd“ ist neu ebenfalls deaktiviert. Aus Sicherheitsgründen soll falls notwendig, der FTP-Server aktiviert und ein neuer Benutzer angelegt werden.

Die Parameter des FTP Servers sind unter dem Tab Ethernet Protocols hinterlegt.

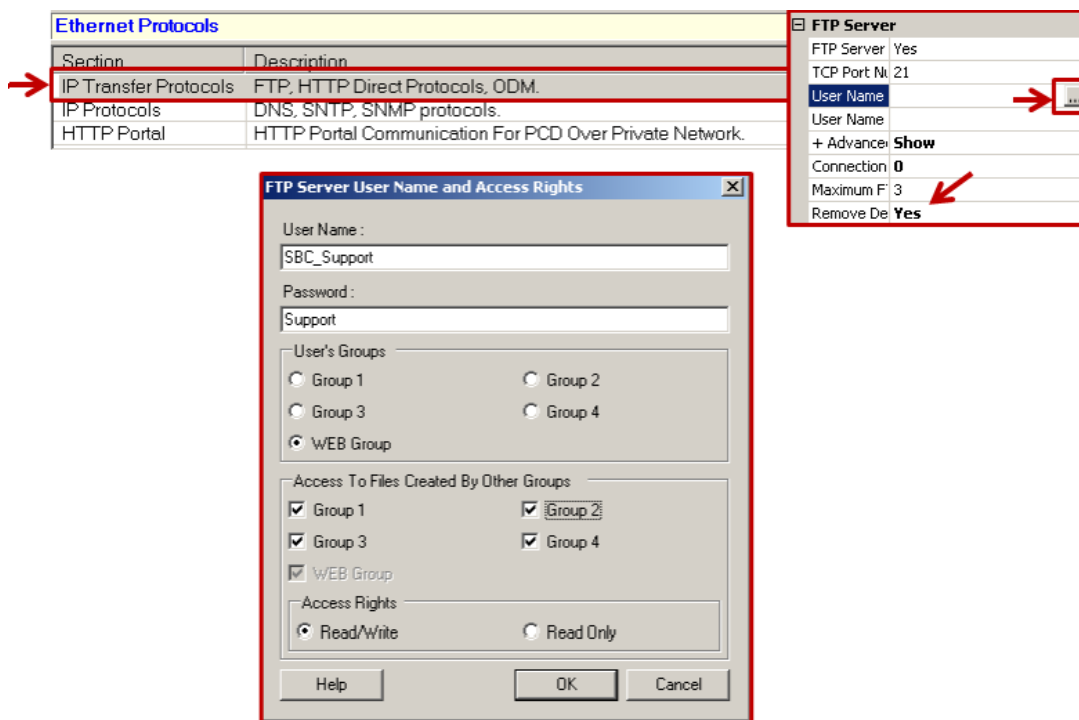


The screenshot shows two parts of the configuration interface. On the left, a table under 'Ethernet Protocols' lists various protocols. The 'IP Transfer Protocols' row is highlighted with a red box. On the right, a 'FTP Server' configuration panel is shown with several fields highlighted by red boxes: 'FTP Server Enabled' (No), 'TCP Port Number' (21), 'User Name 1', 'User Name 2', '+ Advanced Parameters' (Show), 'Connection Timeout [s]' (300), 'Maximum FTP Connections' (3), and 'Remove Default User' (Yes).

Section	Description
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.
IP Protocols	DNS, SNTP, SNMP protocols.
HTTP Portal	HTTP Portal Communication For P...

FTP Server Enabled	No
TCP Port Number	21
User Name 1	
User Name 2	
+ Advanced Parameters	Show
Connection Timeout [s]	300
Maximum FTP Connections	3
Remove Default User	Yes

Einem Benutzer muss auch das dazugehörige Passwort mit einer Gesamtlänge von bis zu maximal 20 Zeichen definiert werden.



The screenshot shows the 'FTP Server' configuration panel with the 'User Name' field highlighted. A red arrow points to a small icon next to the field. Below this, a dialog box titled 'FTP Server User Name and Access Rights' is open. It contains fields for 'User Name' (SBC_Support) and 'Password' (Support). There are also sections for 'User's Groups' (with 'WEB Group' selected), 'Access To Files Created By Other Groups' (with checkboxes for Group 1, Group 2, Group 3, and Group 4), and 'Access Rights' (with 'Read/Write' selected). Buttons for 'Help', 'OK', and 'Cancel' are at the bottom.

Regeln für die Wahl eines Passwortes:

Um einen möglichst guten Schutz zu erhalten, empfehlen wir mindestens 10 Zeichen (je länger desto sicherer) bestehend aus Buchstaben, Zahlen und Sonderzeichen zu wählen. Es sollen keine einfach zu erratende Wörter wie z.B. der Anlagenname genutzt werden.

FTP Server (Yes/No)

Aktivierung resp- Deaktivierung des FTP-Servers

Standardeinstellung: „No“

Empfohlene Einstellung: „**No**“ bei kritischen Anlagen

Wenn der FTP Server benötigt wird, muss er aktiviert und ein neuer Benutzer mit Passwort angelegt werden.

Remove Default User

Der Default User ist neu deaktiviert um einen unberechtigten Zugriff über bekannte und öffentlich kommunizierte Passwörter zu sperren. Für den Zugriff auf den FTP-Server muss mindestens 1 neuer User angelegt werden.

Standardeinstellung: „**Yes**“

Empfohlene Einstellung: „**Yes**“

User Name

Ermöglicht das Erstellen von bis zu 10 individuellen Benutzern mit einer Gruppenzugehörigkeit als auch einer Zugriffsberechtigung lesend oder schreibend. Dabei kann der Benutzer einer Gruppe zugeordnet werden. Zusätzlich ist es möglich dem Benutzer Zugriffsrechte weiterer Gruppen zu ermöglichen. Ein „Administrator“ oder auch „root user“ sollte mit einer Zugriffsberechtigung auf alle Gruppen mit „Read/Write“ rechten definiert werden.

TCP Port Number

Standardmäßig ist der Port 21 für eine FTP Kommunikation definiert. Mit diesem Parameter kann die Port-Nummer des FTP-Servers geändert werden.

Standardeinstellung: „21“

Empfohlene Einstellung: „nur bei Bedarf ändern“

Connection Timeout (s)

Ist eine Verbindung mit dem FTP-Server hergestellt, welche jedoch keine Daten mit dem Server austauscht, wird nach der eingestellten Timeout Zeit die bestehende Verbindung vom FTP-Server geschlossen. Damit die FTP – Verbindung vom Server geschlossen wird, auch wenn der Client diese nicht ordentlich beendet, wird ein Standardwert von 5 Minuten (300 Sekunden) empfohlen.

Standardeinstellung: „300“

Empfohlene Einstellung: „nur bei Bedarf ändern“

Maximum FTP Connections

Definiert die maximale Anzahl an parallelen Verbindungen zum FTP-Server

Standardeinstellung: „3“

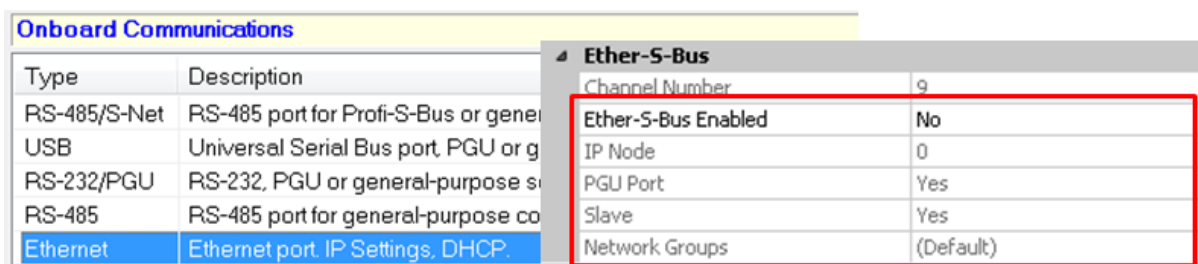
Empfohlene Einstellung: „nur bei Bedarf ändern“

5. Ethernet S-Bus Schutz

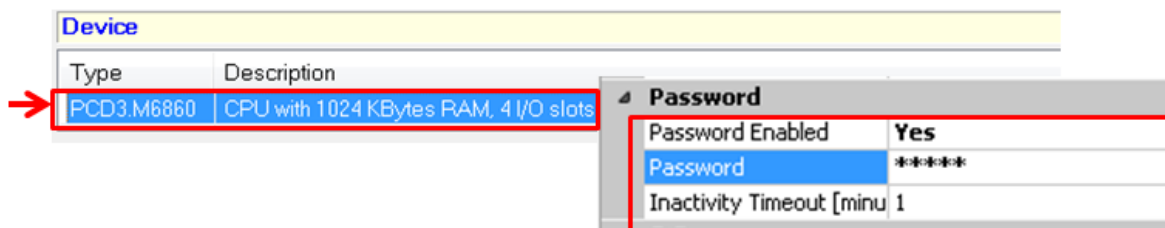
Ether-S-Bus unterstützt alle Dienste und Funktionen für den Datenaustausch, die Programmierung, Inbetriebnahme und Service von Saia PCD-Steuerungen. Der Zugriff erfolgt mit dem PG5 Programmierwerkzeug oder einem Scada-System bzw. OPC-Server (nur für Datenaustausch).

Im PG5 Devicekonfigurator können die Zugriffsrechte für Ether-S-Bus eingestellt werden.

Neu ist im PG5 Devicekonfigurator ab Version 2.1.200 und einer COSinus Version > 1.22.10 die Ether-S-Bus Kommunikation in den Standardeinstellungen deaktiviert. Es ist zu beachten, dass damit die S-Bus Kommunikation weder mit dem PG5 Programmierwerkzeug noch mit einem anderen System (Scada, OPC-Server) genutzt werden kann.



Wenn Ether-S-Bus aktiviert ist, kann der Zugriff mit dem PG5 Programmiergerät zusätzlich mit einem Passwort geschützt werden.



Es gelten folgende Regeln:

Bei deaktiviertem Passwort werden alle Dienste auf allen PGU-Schnittstellen (Ethernet, USB, Seriell) uneingeschränkt unterstützt.

Das Passwort kann mit einer Gesamtlänge von 25 Zeichen definiert werden und muss aus Großbuchstaben (A,B,C) oder Zahlen (0-9) generiert werden.

Für einen guten Schutz empfehlen wir mindestens 10 Zeichen (je länger desto sicherer) bestehend Buchstaben und Zahlen zu wählen. Es sollen keine einfach zu erratende Wörter wie z.B. der Anlagenname genutzt werden.

Achtung: bei einem Verlust des Passwortes muss die Steuerung mit der Reset-Funktion zurückgesetzt werden.

Bei einem definierten Passwort muss beim Verbindungsaufbau mit dem PG5 Programmierwerkzeug für alle PGU-Schnittstellen (Ethernet, USB, Seriell) ein Passwort eingegeben werden. Es erscheint der folgende Login-Dialog:

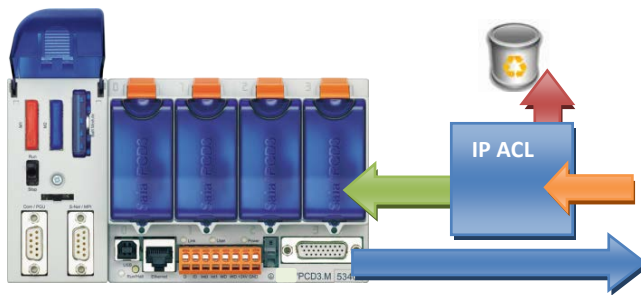


Bemerkung: der Zugriff (Lesen und Schreiben) auf die PCD-Medien (R, F, I/O, T/C) mit Ether-S-Bus ist immer möglich (auch mit konfiguriertem Passwort).

6. IP Zugriffs Filter (IP Access List, ACL)

Ab der COSinus Version 1.22.10 und PG5 2.1.200 unterstützen die PCD-Steuerungen den IP Zugriffs Filter. Erlaubte bzw. nicht erlaubte IP-Adressen werden in einer White- bzw. Black List eingetragen.

- Zugriffe bzw. Telegramme von IP-Adressen, welche in der „White List“ eingetragen sind, werden vom Betriebssystem COSinus erkannt und verarbeitet. Telegramme von anderen IP-Adressen werden verworfen.
- Zugriffe bzw. Telegramme von IP-Adressen, welche in der „Black List“ eingetragen sind, werden vom Betriebssystem COSinus erkannt und verworfen. Telegramme von anderen IP-Adressen werden verarbeitet.



In einem lokalen Netz kann es sinnvoll und notwendig sein den Zugriff auf eine Steuerung mit dem IP Zugriffs Filter zu schützen.

6.1 Device Konfigurator

Die „White List“ oder „Black List“ werden im PG5 Device Konfigurator im Bereich „Onboard Communications“ – „Onboard Ethernet“ definiert.

Onboard Communications		TCP/IP	
Type	Description	Channel Number	9
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-pur...	TCP/IP Enabled	Yes
USB	Universal Serial Bus port, PGU or general...	Ethernet RIO Network	None
RS-232/PGU	RS-232, PGU or general-purpose serial p...	IP Address	192.168.1.2
RS-485	RS-485 port for general-purpose communi...	Subnet Mask	255.255.255.0
Ethernet	Ethernet port. IP Settings, DHCP.	Default Router	0.0.0.0
		+ Access Control List	Show
		IP Filtering Enabled	Yes
		IP Filtering Policy	White List
		IP Filtering List	Configure

Damit die Eigenschaften des IP Filters bearbeitet werden können, muss der Parameter bei „+ Access Control List“ auf „Show“ gesetzt werden.

- 1) „IP Filtering Enabled“
Einschalten oder Abschalten des IP Zugriff Filters

2) „IP Filter Policy“

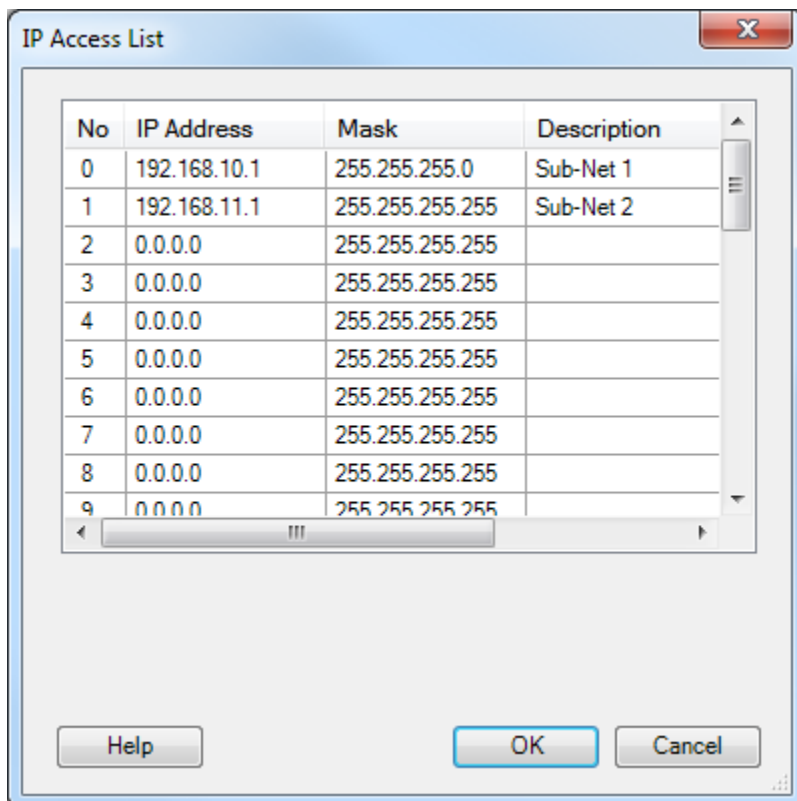
Einstellen des Filter Modus

White List = alles blocken → nur in Liste eingetragene Adressen erlauben

Black List = alles erlauben → nur in Liste eingetragene Adressen blocken

3) „IP Filtering List“

Liste der IP-Adressen und dazugehörige „Mask“, welche je nach ausgewähltem Modus vom Betriebssystem COSinus bearbeitet bzw. verworfen werden.



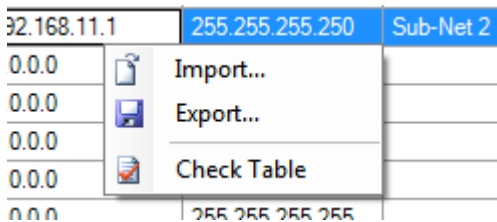
Mit der „Mask“ können auch ganze Subnetze für den Filter definiert werden. Die IP-Adresse und die Mask definieren die Netz- bzw. Subnetzadresse.

Z.B.

Die IP Adresse 192.168.10.1 mit einer definierten Mask von 255.255.255.0 erlaubt bzw. blockiert die Kommunikation von allen Geräten im Netz 192.168.10.0/24 (255 Adressen)

Die IP Adresse 192.168.11.1 mit einer definierten Mask von 255.255.255.255 erlaubt bzw. blockiert die Kommunikation ausschließlich von dieser IP-Adresse

Die Liste kann als .csv Datei exportiert oder importiert werden.



6.2 Fupla FBoxen

Der IP Zugriffs Filter kann aus dem PCD Anwenderprogramm mit Hilfe von FBoxen gesteuert werden.

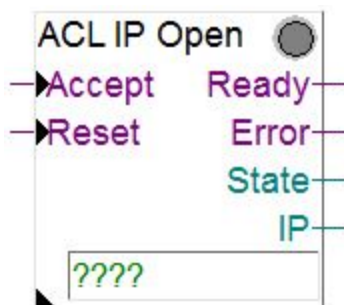
1) ACL IP Filter FBox

Erlaubt es den IP Filter ein- sowie auszuschalten



2) ACL IP Open FBox

Erlaubt es eine IP-Adresse für den Zugriff auf das Gerät zu öffnen. Diese FBox kann z.B. verwendet werden, um eine IP-Adresse temporär für einen Mail Server zu öffnen, damit die Steuerung eine Mail versenden kann. Es können so bis zu 32 IP-Adressen (32 FBoxen) der White Liste hinzugefügt werden.

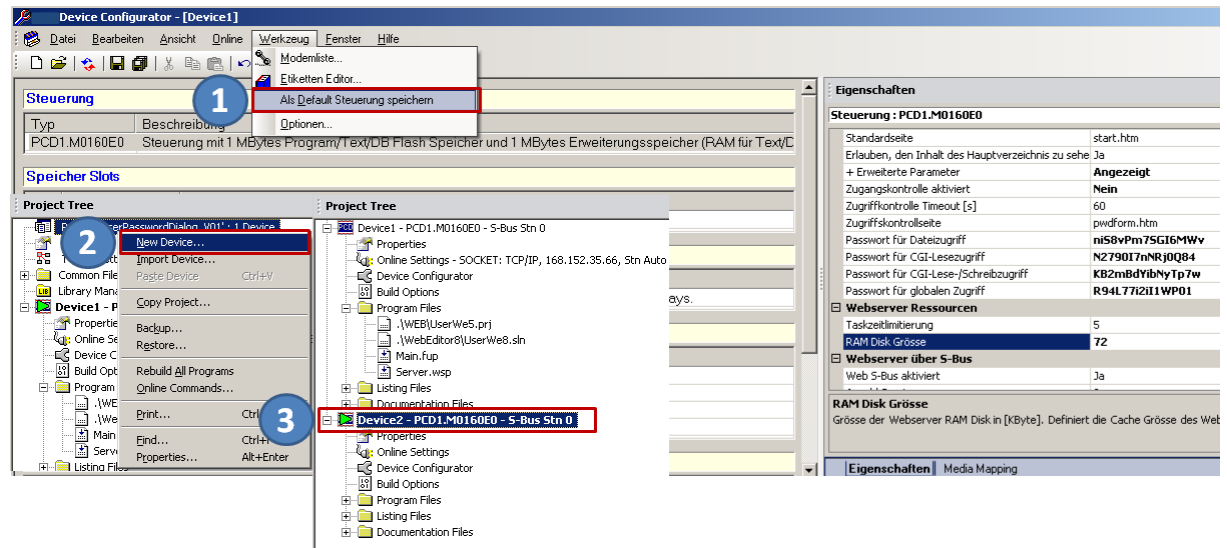


Mehr Informationen findet man im Online Help der FBoxen.

7. Device Templates bearbeiten im PG5 Devicekonfigurator

Damit Sie ihre Einstellungen für eine CPU stetig auf der gleichen Konfiguration aufbauen, ist es möglich ein konfiguriertes Device Template als Default für alle gleichen CPU Typen zu definieren.

Dabei werden alle Einstellungen welche im Devicekonfigurator Template definiert wurden beim Anlegen einer neuen CPU übertragen.



- 1) Setzen der aktuellen Einstellungen im Device Konfigurator der CPU als Default Settings für diesen CPU-Type
- 2) Hinzufügen einer neuen Gerätes
- 3) Das neue Gerät wird mit der in Punkt 1 definierten Device Konfiguration erzeugt.

Definieren Sie einmalig ihre aktiven Komponenten der CPU wie Web Server, FTP Server als auch ihre Sicherheitsstufen, ServiceKey oder Benutzer für berechtigte Zugänge und Speichern Sie diese Einstellungen für diesen CPU Type ab.

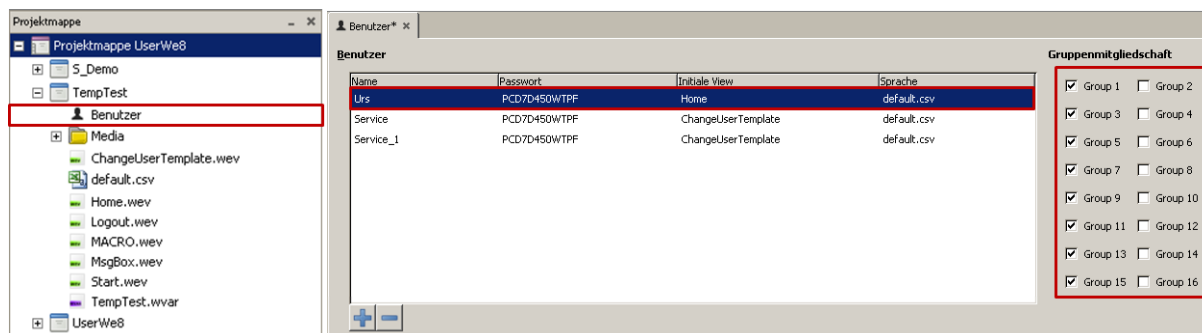
8. Neue Benutzerverwaltung mit Zugriffsteuerung im WebEditor 8

Ab der COSinus Version 1.22.10 für PCD-CPU's, 1.22.09 für Micro-Browser Panel und PG5 V2.1.200 ist im WebEditor 8 eine neue Benutzerverwaltung und Zugriffsteuerung verfügbar. Die Vorlagen für den neuen Mechanismus sind im WebEditor 8 in der Vorlagen-Bibliothek im Bereich „Zugriffssteuerung“ aufgeführt. Die Vorlagen sind nur in Verbindung mit der vom Web Editor 8 generierten Benutzerdatenbank verwendbar. Die neue Zugriffssteuerung ersetzt die bisherige „Benutzer Identifikation“ (alter Passwort Mechanismus), bei welcher lediglich 4 Benutzerlevels definiert werden konnten.

Die Zugriffssteuerung erlaubt es einen Benutzer in bis zu 16 Gruppen einzuteilen. Diese Gruppen bilden keine Levels. Ist ein Benutzer in der Gruppe enthalten, kann er auf die Elemente und Funktionen dieser Gruppe zugreifen oder verwenden.

8.1 Benutzerdatenbank

Der Web Editor 8 wurde mit einer Benutzerverwaltung erweitert. In der Benutzerdatenbank können bis zu 100 Benutzer definiert werden. Ein Benutzer besteht dabei aus einem Benutzernamen, Passwort, Start Seite und Sprache. Zusätzlich wird jeder Benutzer verschiedenen Benutzergruppen zugeordnet.

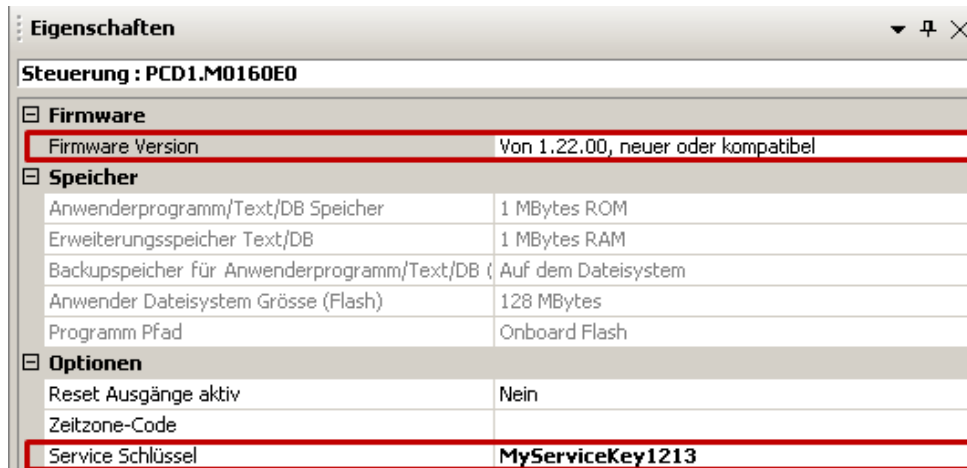


Die Benutzerdatenbank wird in einem sicheren Bereich in der Steuerung gespeichert.

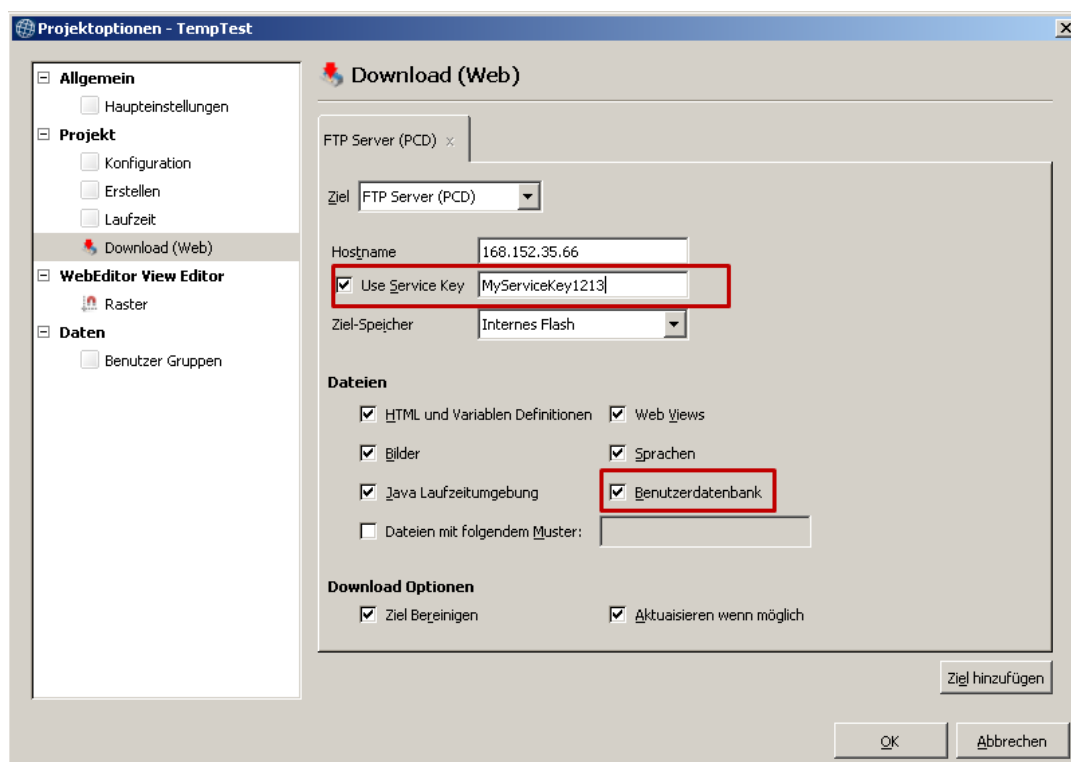
8.2 Download der Benutzerdatenbank und Service Key (Service Schlüssel)

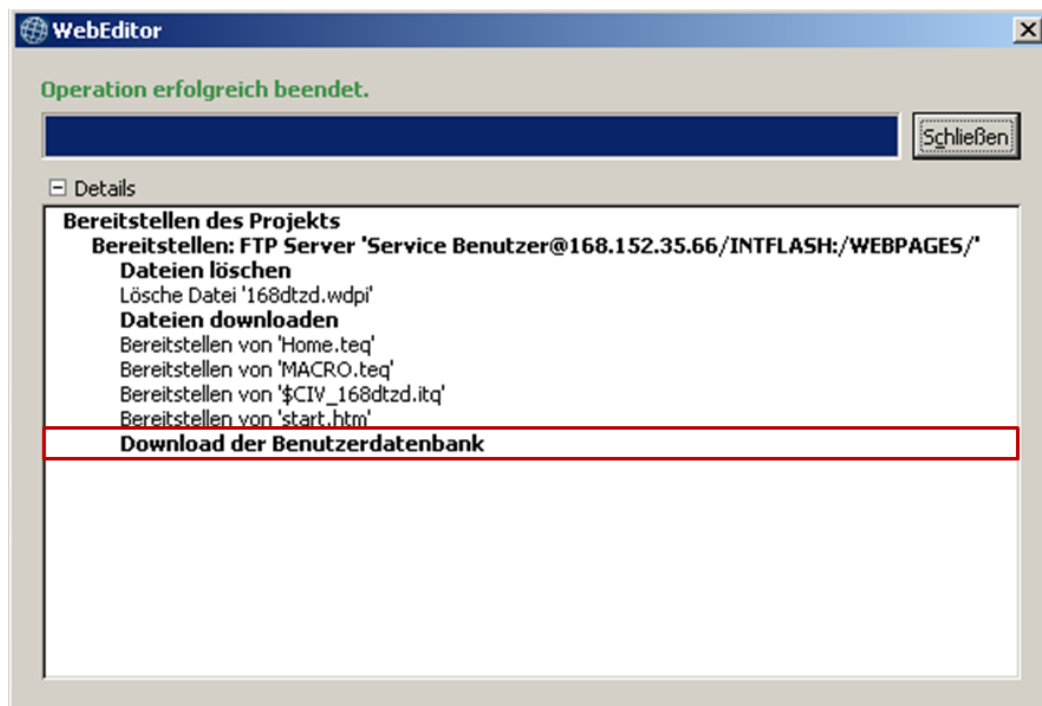
Damit der Web Editor 8 die Benutzerdatenbank in den geschützten Bereich der PCD-Steuerung laden kann, muss der Service Schlüssel (Key) im Device Konfigurator definiert werden.

Mit dem Service Schlüssel identifiziert sich der WebEditor 8 bei der Steuerung (FTP-Server). Der Service Schlüssel wird im PG5 Device Konfigurator im Bereich Device eingetragen.



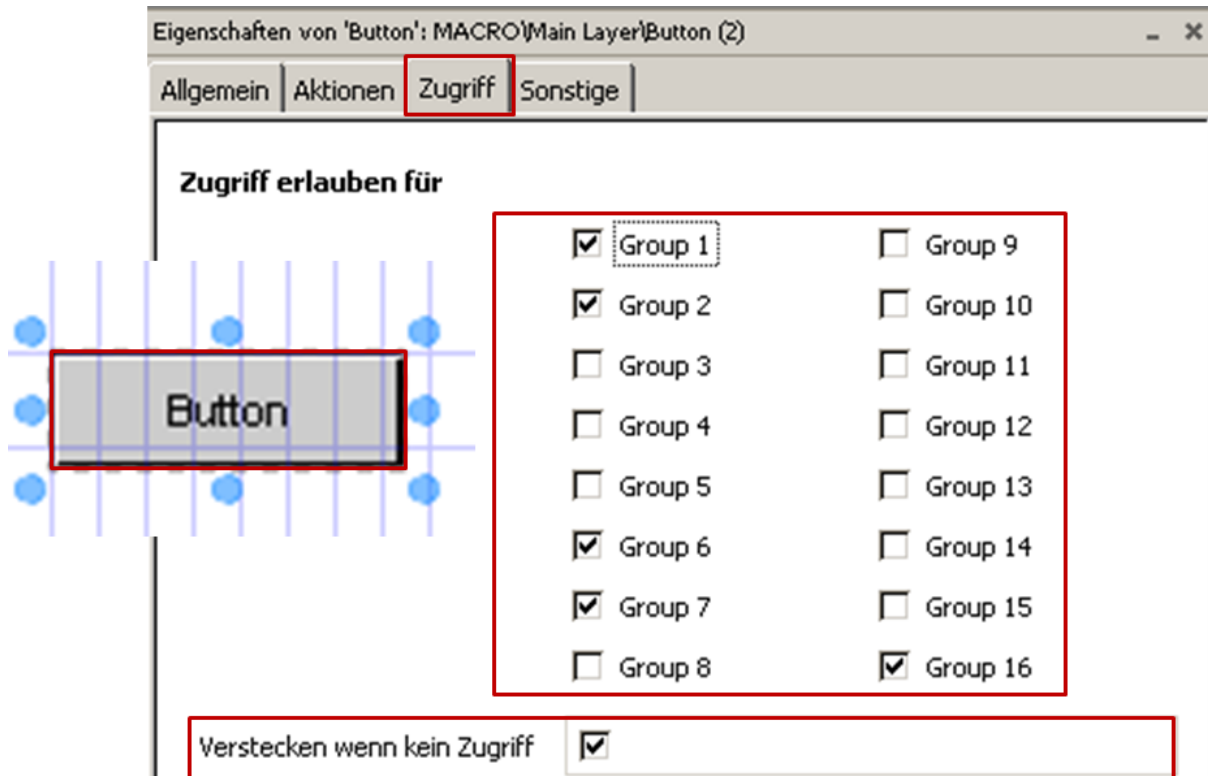
Für den Download der Benutzerdatenbank im Web Editor 8 muss ein Download Ziel „WebFTP“, „FTP Server (PCD)“ oder „PG5 CPU (S-Bus)“ mit Service Schlüssel (Key) verwendet werden. Hier muss der gleiche Service Schlüssel wie im PG5 Devicekonfigurator eingegeben werden.





8.3 Vergabe der Rechte auf Funktionen oder Elemente im WebEditor 8

Im WebEditor 8 kann jedes Element wie Button, Edit Boxen, Gruppen oder Layer einer oder mehreren Benutzergruppen zugeordnet werden. Bei einem Benutzer Login werden die Benutzerrechte in der Applikation hinterlegt. Der eingeloggte Benutzer kann so, mit seinen zugeordneten Gruppen die entsprechenden Funktionen bzw. Elemente verwenden. Ist die Checkbox „Verstecken wenn kein Zugriff“ aktiviert, wird das Element und die dahinter verlinkten Funktionen für Benutzer, welche in der Gruppe nicht definiert sind, deaktiviert und ausgeblendet.

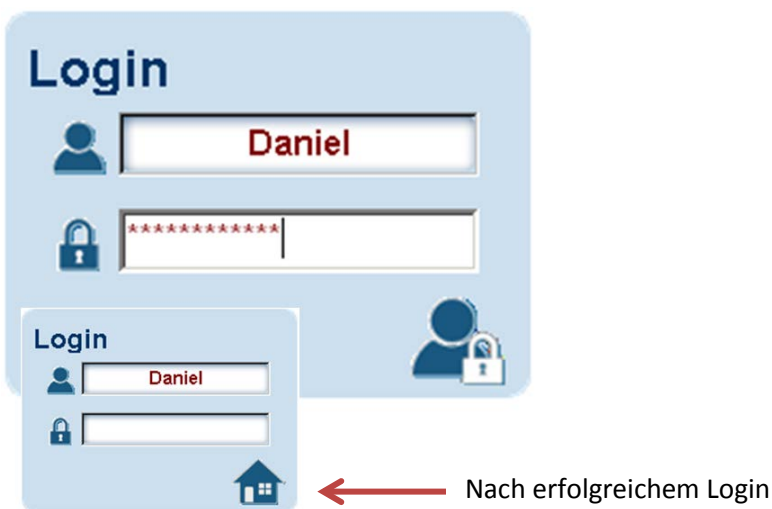


8.4 Vorlagen für Benutzersteuerung

Die Vorlagen für die Benutzersteuerung können nur in Verbindung mit der neuen Benutzerverwaltung genutzt werden

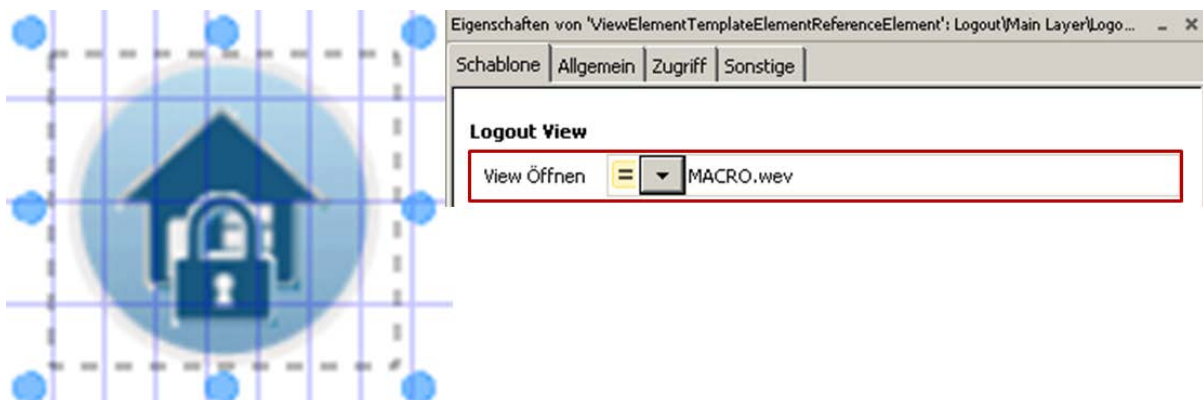
8.4.1 Login Vorlage

Beim Login wird der eingegebene Benutzernamen und das Passwort von der Steuerung in der Benutzerdatenbank überprüft. Das eingegebene Passwort wird mit einem Hash Code verschlüsselt übertragen. Wenn der Benutzername und Passwort korrekt sind, werden dem Benutzer (bzw. der HMI-Applikation) die entsprechenden Rechte mit Gruppenzugehörigkeit, Sprache und Startseite übergeben.



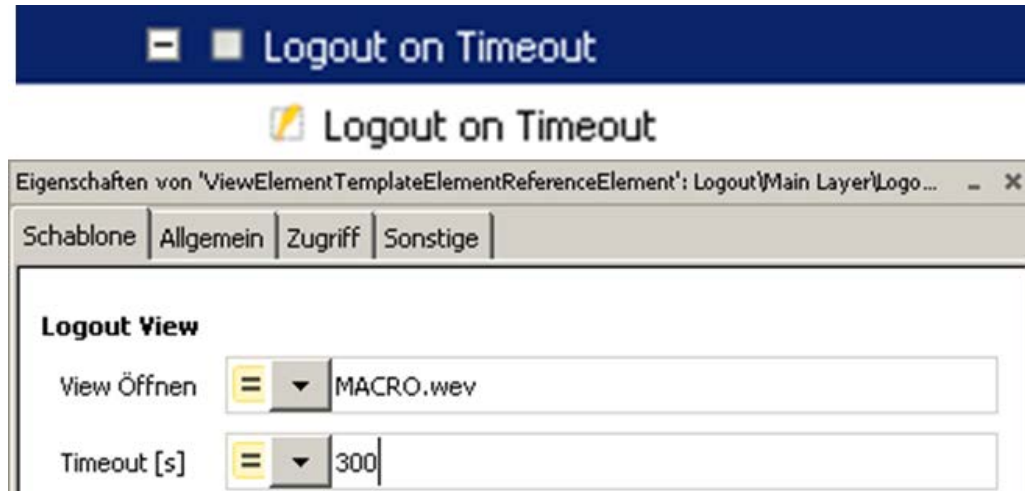
8.4.2 Logout Vorlage

Ist ein Anwender über die Login Vorlage eingeloggt, werden interne Variablen mit seiner Gruppe, Sprache und Start Seite gesetzt. Der Logout Button setzt diese Variablen zurück und macht einen Seitenwechsel zu der in der Vorlage angegebenen Logout View.



8.4.3 Automatisches Logout bei Inaktivität

Ist ein Anwender über die Login Vorlage eingeloggt, werden interne Variablen mit seiner Gruppe, Sprache und Start Seite gesetzt. Die „Logout on Timeout“ Vorlage setzt diese Variablen nach Ablauf einer definierten Zeit zurück und macht einen Seitenwechsel zu der in der Vorlage angegebenen Logout View. Der Timeout Wert kann in der Vorlage in Sekunden definiert werden.



8.4.4 Passwort Ändern

Mit der „Change Password Vorlage“ kann der Benutzer sein eigenes Passwort ändern. Damit er sein Passwort ändern kann, muss zuerst das aktuelle Passwort korrekt eingegeben werden. Das neue Passwort muss zwei Mal eingegeben und danach bestätigt werden. Anschliessend ist das neue Passwort aktiv. Das alte Passwort ist ab diesem Moment nicht mehr gültig!

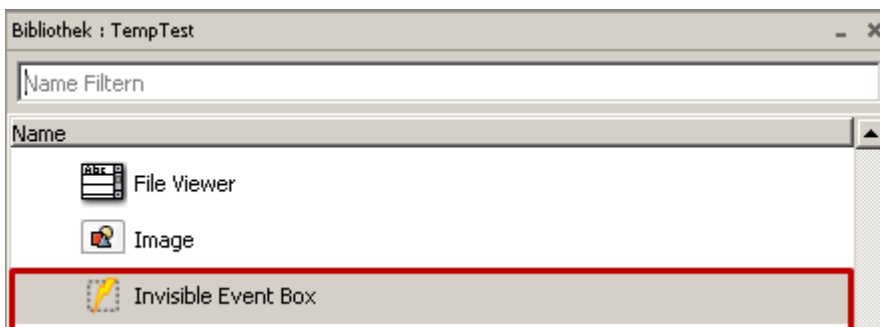


8.5 Kompatibilität neue Zugriffssteuerung und alte Benutzeridentifikation

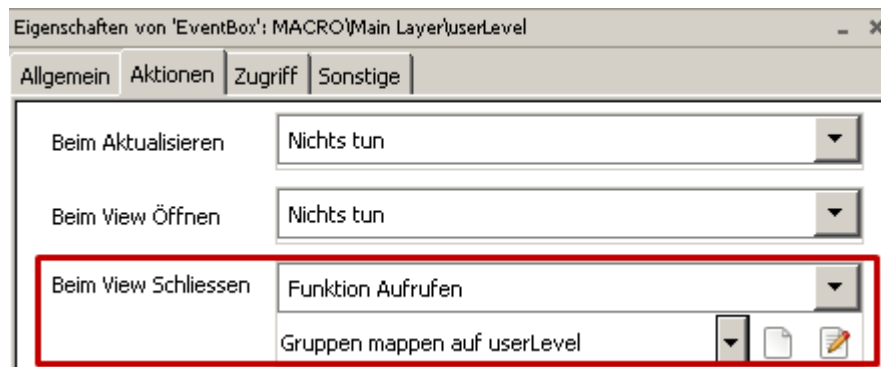
Die Vorlagen der Zugriffssteuerung sind nicht mit der bestehenden Lösung der Benutzeridentifikation kompatibel. Im Gegensatz zu den 4 Level mit der alten Benutzeridentifikation, arbeitet die neue Zugriffssteuerung mit 16 Gruppen. Diese Gruppen stellen keine Level dar, sondern sind individuell konfigurierbar. Ein Element wird angezeigt oder aktiv, wenn der eingeloggte Benutzer die Rechte dieser Gruppe(n) besitzt.

Ein mit dem Web-Editor 5.15 resp. mit der alten Benutzeridentifikation erstelltes Projekt, kann mit wenig Aufwand auf die neue Benutzerverwaltung portiert werden. Dazu werden im WebEditor 8 die neuen Vorlagen für die Zugriffssteuerung genutzt, vier Benutzer definiert und deren Rechte auf die interne Variable „userLevel“ abgebildet. Weitere Anpassungen am Projekt sind nicht erforderlich.

- 1) Es müssen 4 Benutzer definiert werden (1 bis 4)
Die Rechte der Benutzer werden bei erfolgreichem Login in den internen Variablen „?S_User_LO..3“ hinterlegt
- 2) Die Rechte der Benutzer müssen nun auf die interne Variable „userLevel“ abgebildet werden.
Die internen Variablen „?S_User_LO..3“ können „0“ oder „1“ beinhalten.
- 3) Dazu kann eine „Invisible Event Box“ verwendet werden.

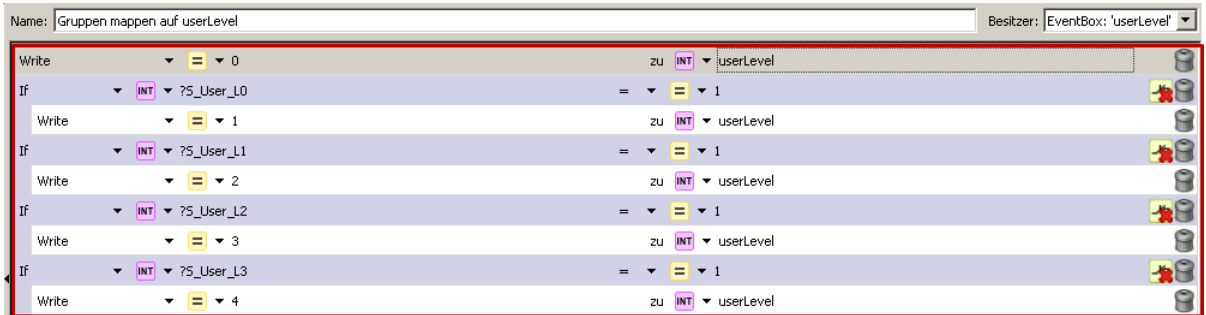


- 4) Die „Invisible Event Box“ wird auf der Seite mit der Login Vorlage platziert und beim Schliessen der Seite werden die Benutzerrechte in die interne Variable „userLevel“ übertragen.



5) Die Funktion zum Übertragen der Benutzerrechte in den „userLevel“ kann wie folgt implementiert werden:

- ➔ Rücksetzen der internen Variable „userLevel“
- ➔ Setzen der internen Variable „userLevel“ anhand der Benutzerrechte, dabei gewinnt der höchste Benutzer (4) beim Eintragen des Levels in die interne Variable „userLevel“



- ?S_User_L0 → Level 1 → userLevel == <1>
- ?S_User_L1 → Level 2 → userLevel == <2>
- ?S_User_L2 → Level 3 → userLevel == <3>
- ?S_User_L3 → Level 4 → userLevel == <4>

6) Bestehende „Logout“ Makros müssen durch die im WebEditor 8 enthaltenen „User Identifikation“ Vorlagen ersetzt werden

