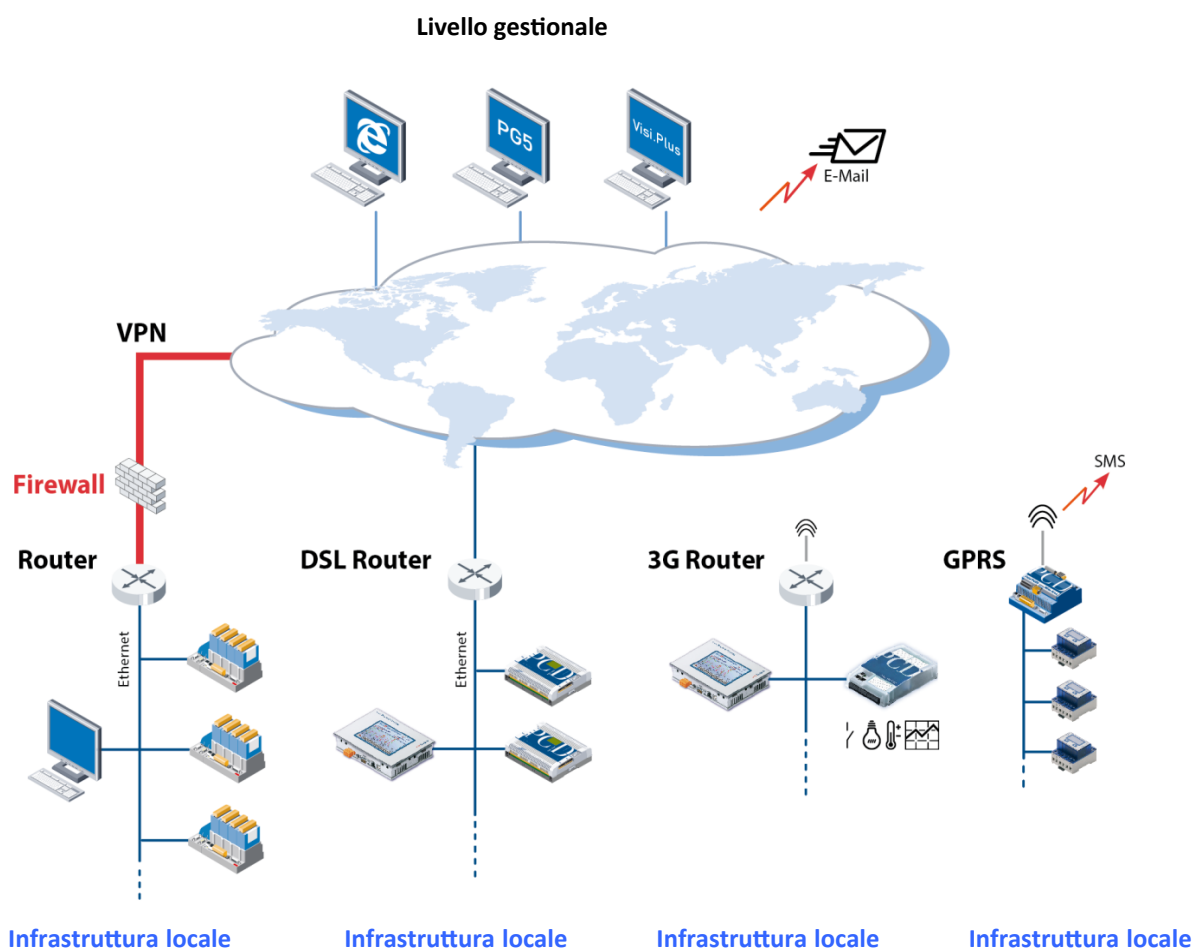


Istruzioni per la connessione dei controllori Saia PCD® alla rete internet



Cronologia del documento

Versione	Editazione	Pubblicazione	Commenti
IT01	15.05.2013	15.05.2013	
IT03	10.10.2013	10.10.2013	Traduzione dalla Versione EN03
IT04	14.02.2014	02.02.2014	Nuovo logo

Contenuti

1. Introduzione	3
2. Creazione di una rete privata virtuale (VPN).....	6
2.1 Router VPN testati	7
3. Protezione del PCD.Web-Server.....	9
Funzione del meccanismo di password	9
3.1 Impostazioni nel Device Configurator PG5.....	9
Abilitazione della password del PCD.Web-Server	10
3.2 Introduzione della password nel web client	12
3.2.1 Pannello Micro-Browser.....	12
3.2.2 Micro Browser Windows CE ed eXP	14
3.2.3 iOS Micro-Browser app	15
3.2.4 Browser PC con Java applet	15
3.2.5 Saia.Net Web Connect / WebFTP.....	16
3.3 Compatibilità PG5 e versioni firmware COSinus	18
3.3.1 Attivazione della password Saia PCD.Web-Server con il Device Configurator.....	19
3.3.2 Attivazione della password Saia PCD.Web-Server con il progetto Web Server (.wsp)	19
4. Protezione FTP server.....	21
5. Protezione Ethernet S-Bus	23
6. Filtro di accesso IP (IP Access List, ACL).....	25
6.1 Device Configurator.....	25
6.2 FBox Fupla	27
7. Editazione dei template dei dispositivi nel Device Configurator PG5.....	28
8. Nuove gestione utente con controllo di accesso nel WebEditor 8.....	29
8.1 Database utente	29
8.2 Download del database utente e service key	30
8.3 Assegnazione dei diritti alle funzioni o agli elementi in WebEditor 8.....	32
8.4 Template per il controllo utente	33
8.4.1 Template di Login	33
8.4.2 Template di Logout	33
8.4.3 Logout automatico durante l'inattività	34
8.4.4 Cambio password	34
8.5 Compatibilità del nuovo controllo di accesso e la vecchia identificazione utente	35

1. Introduzione

Il presente documento contiene informazioni importanti riguardanti le misure protettive che devono essere osservate quando si connettono i controllori Saia PCD alla rete internet. L'edizione più recente è disponibile sulla homepage del nostro sito di supporto:

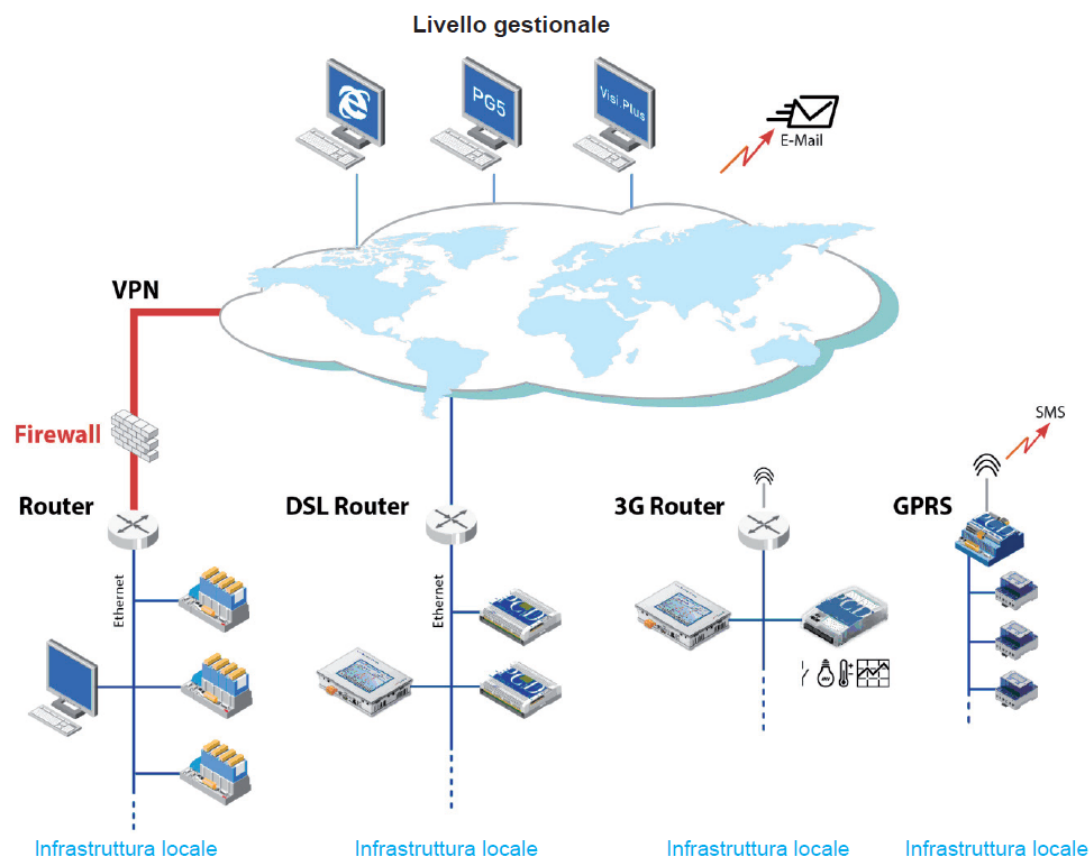
<http://www.sbc-support.com/en/product-category/communication-protocols/pcd-on-internet.html>

La prima edizione del documento è stata rilasciata all'inizio di Maggio 2013. Quella edizione descriveva le misure con le funzioni di protezione disponibili a quel tempo nel sistema operativo PCD COSinus e nel tool software PG5. Abbiamo ora adeguato i nostri tool software in modo che, nei controllori PCD, le funzioni di protezione siano attivate di default. Inoltre, nel WebEditor abbiamo migliorato il meccanismo di password. E' nuova anche la funzione IP filter, implementata nei controllori PCD.

Si deve ancora far notare: l'operatività sicura dei controllori PCD nella rete internet può essere garantita solamente con componenti IT esterni aggiuntivi che offrono funzioni integrate di protezione, quali: VPN, firewall, proxy server, ecc.

Infine, abbiamo valutato diversi router VPN e li abbiamo testati con i nostri controllori PCD. Questo documento elenca i dispositivi testati con successo ed i loro fornitori. Una descrizione dettagliata per la configurazione e per le operazioni iniziali è disponibile nel documento 30-004 'VPN-Router' sul nostro sito di supporto.

I controllori Saia PCD si possono connettere alla rete internet in una varietà di modi. Il diagramma sottostante mostra alcune delle opzioni di connessione frequentemente utilizzate.



Per le installazioni più piccole, nella maggior parte dei casi, un controllore Saia PCD è connesso alla rete internet con un router DSL o 3G. Un PCD3.WAC è connesso direttamente tramite il modem GPRS integrato. I controllori Saia PCD che operano in una rete aziendale locale protetta, normalmente sono accessibili dall'esterno solo mediante un firewall sicuro e una VPN (rete privata virtuale). Solo in questo caso, la protezione di accesso è assicurata da questi componenti.

Se i controllori PCD sono operanti a valle di un router DSL o 3G non protetto, di solito i servizi IP sono instradati al controllore PCD locale attraverso il "port forwarding". **In questi casi, questi controllori possono essere facilmente attaccati.**

Di seguito, trovate una breve panoramica delle possibili funzioni di protezione:

- **Soluzione sicura con Virtual Private Network (VPN)**

Un controllore PCD dovrebbe essere connesso alla rete internet a valle di un router o di un proxy server con firewall e una VPN protetta. Il capitolo 2 include i dispositivi che abbiamo testato e che raccomandiamo.

- **Password di protezione del Web-Server**

Si può proteggere l'accesso al PCD.Web-Server con un meccanismo di password a 4-livelli. Questo comprende una password di protezione non-criptata. Le password introdotte sono verificate nel controllore. Per il Device Configurator PG5, a partire dalla versione 2.1.200, il Web-Server è disattivato di default. Quando è attivato, si può proteggere l'accesso con una password. Maggiori informazioni sono disponibili nel capitolo 3.

- **Protezione accesso FTP server**

Allo stesso modo, l'accesso all'FTP server e quindi ai dati del PCD.Filesystem si può proteggere con una password separata non-criptata. Per il PG5 Device Configurator, a partire dalla versione 2.1.200, l'FTP-Server è disattivato di default. Quando è attivato, la password standard "root" e l'utente standard "rootpasswd" non sono più utilizzate. Il programmatore deve impostare il proprio nome utente per ottenere l'accesso. Maggiori informazioni sono disponibili nel capitolo 4.

- **Protezione accesso Ether-S-Bus**

Il dispositivo di programmazione PG5 utilizza il protocollo S-Bus con servizi estesi per la programmazione e per l'operatività iniziale dei controllori PCD.

Nel Device Configurator PG5, a partire dalla versione 2.1.200 e nel firmware PCD COSinus a partire dalla versione 1.22.10, la comunicazione Ether-S-Bus è disattivata di default.

Pertanto, l'interfaccia Ethernet non supporta il protocollo S-Bus (scambio dati e programmazione). Quando è attivata, l'accesso con il dispositivo di programmazione PG5 può essere ulteriormente protetto con una semplice password, non-criptata. Maggiori informazioni sono disponibili nel capitolo 5.

- **Filtro per l'accesso IP**

Partendo dalla versione 1.22.10 del firmware COSinus, i controllori PCD sono dotati di un filtro di accesso IP integrato. Gli indirizzi IP autorizzati e non-autorizzati possono essere introdotti in una "white" o "black" list. Maggiori informazioni sono disponibili nel capitolo 6.

- **Meccanismo di password nel WebEditor**

Il meccanismo password è incluso nel WebEditor ed utilizzato sia dall'applet Java che dal micro browser, viene utilizzato per l'identificazione utente nella gestione di specifiche richieste nell'applicazione HMI. Questo meccanismo è stato implementato con il nuovo firmware COSinus versione 1.22.10 e PG5 versione 2.1.200. La password introdotta è ora criptata con un "hash code". La password introdotta è verificata nel controllore. Maggiori informazioni sono disponibili nel capitolo 8.

Modifica delle impostazioni di default nel Device Configurator

Le impostazioni di default si possono modificare e salvare in un modello separato. Quindi, queste impostazioni di default possono essere trasferite ad una nuova CPU, quando questa viene creata. Maggiori informazioni sono disponibili nel capitolo 7.

Per poter utilizzare le funzioni di protezione sopra indicate nel modo nel quale sono descritte, è necessario disporre del pacchetto PG5, versione 2.1.200 o superiore. Allo stesso modo, alcune funzioni richiedono il nuovo firmware PCD-COSinus, versione 1.22.10. Nei rispettivi capitoli, sono disponibili informazioni dettagliate.

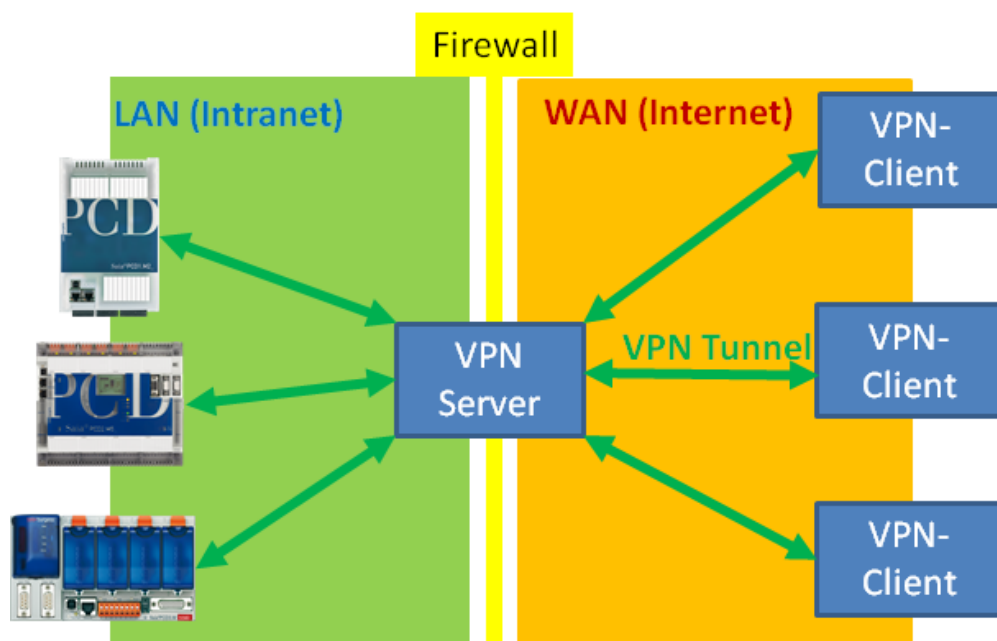
Il presente documento e le nuove versioni di PG5 e di firmware COSinus sono disponibili sulla pagina del sito di supporto al seguente link: <http://www.sbc-support.com/en/product-category/communication-protocols/pcd-on-internet.html>

2. Creazione di una rete privata virtuale (VPN)

Un tunnel VPN offre un modo sicuro di accesso, via internet, ai dispositivi in una rete privata (WAN).

Tipicamente, questo tipo di struttura comprende un server VPN e un client VPN. Raccomandiamo l'utilizzo di un router con funzionalità VPN server. Di solito, il VPN client è installato come software sul dispositivo client (PC, tablet, smartphone, ecc.).

Il VPN client (o software VPN client) accede al VPN server, via internet. Se il login avviene con successo, il dispositivo sul quale il VPN client è stato lanciato, trova se stesso all'interno del VPN server dell'intranet, essendo entrato tramite un tunnel sicuro. Da questo momento, questi può accedere a tutti i dispositivi nella gamma di indirizzi assegnati del VPN server e ne può utilizzare tutti i servizi.



Quando si sceglie un router, si devono considerare diversi punti, dipendenti dall'applicazione.

Il router utilizzato dovrebbe avere la funzionalità server VPN. Per stabilire le connessioni VPN, i router utilizzano protocolli differenti. Il protocollo di comunicazione deve essere supportato sia dal router che dal dispositivo VPN client (PC, tablet, smartphone). Pertanto, è necessario assicurarsi che l'appropriato software VPN client sia disponibile per il dispositivo client. Probabilmente, IPsec è la tecnologia più utilizzata ed è supportata direttamente da molti dispositivi. In ogni caso, IPsec è abbastanza complesso da configurare e da utilizzare.

OpenVPN, che è disponibile in versione "open source", è più facile da configurare. Questo utilizza il protocollo di crittazione SSL ed è quindi meno problematico con i firewall. Il software "OpenVPN client" è disponibile per molti dispositivi e sistemi operativi.

2.1 Router VPN testati

DrayTek Vigor 2850Vn Router



Questo router è destinato all'utilizzo nel segmento casa / ufficio e dispone di una gamma di opzioni di connessione (Ethernet, DSL, USB, WLAN, ...) e di potenti funzioni (firewall, VPN, ...).

E' particolarmente indicato per stabilire e gestire connessioni VPN per reti di piccole e medie dimensioni. Le sue funzionalità e l'interfaccia utente sono di facile utilizzo. Supporta VPN client standard da Windows, I-OS e Android.

Tipo: Vigor 2850Vn

Fornitori: Fornitori online, rivenditori specializzati, distributori, ...

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

eurogard Service Router V2



L'EuroGard Service Router V2 è un router industriale per il montaggio su guida DIN, con alimentazione a 24 VCC. Dispone di numerose opzioni di connessione (Ethernet, 3G) e permette agli utenti di stabilire connessioni sicure utilizzando OpenVPN o SSL. La configurazione e la guida dell'utente per creare la connessione VPN sono veloci e facili da eseguire. Dispone di un OpenVPN server e di conseguenza necessita di un client OpenVPN.

Tipo: eurogard Service Router V2

Fornitori: eurogard GmbH
Kaiserstrasse 100

D-52134 Herzogenrath

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

Comparazione dei dati tecnici fra Vigor 2850Vn e EuroGard Service Router V2

	DrayTek Vigor 2850Vn	EuroGard Service Router V2 (WLAN)	EuroGard Service Router V2 (UMTS)
Codice	2850Vn	ER 1201-WLAN	ER 1201-UMTS
Informazioni aggiuntive	http://www.draytek.de/produkte/modem-router/vigor2850-serie.html	http://www.eurogard.de/en/	http://www.eurogard.de/en/
Tipo di applicazione	Business/Domestica	Industriale	Industriale
Montaggio su guida DIN	No	Si	Si
Alimentazione	230 VCA	24 VCC	24 VCC
VPN Features			
Numero di interfacce WAN	3: LAN/Modem/USB	1: LAN	2: LAN/UMTS
Modem ADSL/VDSL integrato	Si	No	No
VPN PPTP	Si	No	No
VPN L2TP/IPSec	Si	No	No
openVPN	No	Si	Si
Nr. VPN client	32 connessioni	30 connessioni	30 connessioni
Windows client	Si (integrato in Windows)	Si (EurogardSRConnect)	Si (EurogardSRConnect)
IOS Client	Si (IPSec/L2TP, integrato in IOS)	No*	No*
Android Client	Si (IPSec/L2TP, integrato in Android)	No*	No*
Estensioni			
3G/4G modem	Si, con chiave USB	No	Si, con modem UMTS integrato

* Sistemi IOS o Android si possono ora connettere al router via WLAN. Questo richiede due router. Uno VPN server e l'altro VPN client. Supporto per VPN su dispositivi mobili è in preparazione.

Dettagli sulla configurazione e sull'utilizzo del router per connessioni VPN sicure con i controllori Saia PCD sono disponibili nel documento 30-004.

3. Protezione del PCD.Web-Server

L'accesso al PCD.Web-Server si può proteggere con un meccanismo di password.

Funzione del meccanismo di password

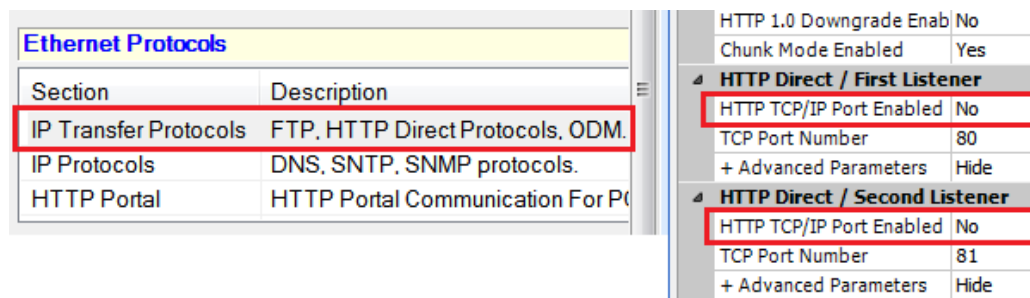
Con questo meccanismo di password, si può bloccare l'accesso generale ai file e a tutti gli elementi del PCD (registri, flag, DB/testi, ecc.). Se si accede al web server del PCD mediante un dispositivo browser (browser PC, pannello micro-browser, iPad,), il server verifica che la password memorizzata nel controllore PCD sia stata introdotta correttamente. Se non è stata introdotta la password, o se una password trasmessa direttamente non è valida, sul dispositivo browser sarà visualizzata una finestra di dialogo richiedente l'introduzione della password. La comparazione della password avviene nel web server del controllore PCD. Questo garantisce che, quando si stabilisce una connessione, le password definite non siano trasferite durante la verifica. Le password introdotte sono trasmesse senza criptazione.

3.1 Impostazioni nel Device Configurator PG5

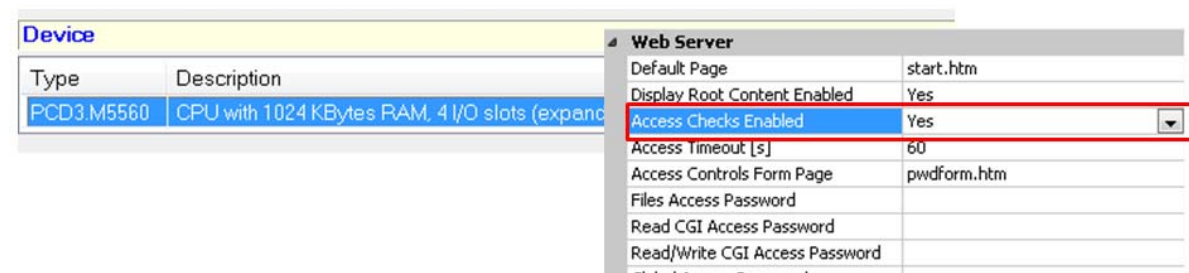
Le impostazioni di configurazione del controllore Saia PCD sono eseguite nel Device Configurator PG5. Le impostazioni per il Web-Server sono allocate nei menù "IP Transfer Protocols" e "Device Type".

Quando si crea una nuova CPU nel Device Configurator, a partire dalla versione PG5 2.1.200, il Web-Server è ora disattivato di default.

Il Web-Server deve essere attivato nel Device Configurator.



Inoltre, la password di protezione è ora attivata quando è attivo il Web-Server.



Si deve configurare una password con queste impostazioni. Maggiori informazioni sono disponibili nel paragrafo successivo. Nel caso in cui la password non debba essere configurata, si deve disattivare il parametro "Access Checks Enabled".

Access Check Enabled:

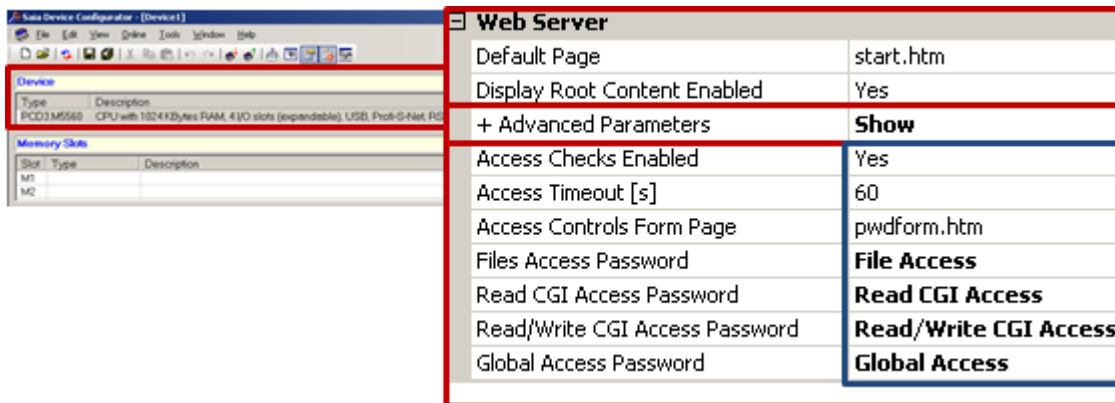
Attiva il meccanismo di password del PCD.Web-Server

Default: "Yes"

Impostazione raccomandata: "Yes"

Abilitazione della password del PCD.Web-Server

La password sarà verificata solo se il parametro "Access Checks Enabled" è impostato su "Yes".



Access Timeout

Se la comunicazione con una connessione http S-Bus è interrotta, sarà richiesta nuovamente l'interrogazione della password, dopo che è trascorso il tempo impostato. Questo parametro è utilizzato solo con http via S-Bus.

Default: "60s"

Impostazione raccomandata: "Non cambiare il valore di default"

Access Controls Form Page

In caso di accesso senza una password valida, verrà chiamata questa pagina di introduzione password.

Default: "pwdform.htm"

Impostazione raccomandata: "Non cambiare il valore di default"

Nota: questa pagina è memorizzata nel sistema del web server. Se necessario, il programmatore può anche creare la propria pagina di login.

Impostazione delle password per la protezione dell'accesso

Il PCD.Web-Server ha 4 livelli di protezione dell'accesso:

"File Access" → Livello 1

"Read CGI Access" → Livello 2

"Read/Write CGI Access" → Livello 3

"Global Access" → Livello 4

Nella maggior parte dei casi, la protezione di accesso generale al PCD.Web-Server è sufficiente. A questo proposito, si deve definire una **password di livello 1 (file access)**. Raccomandiamo che questa password sia sempre definita! Per tutte le altre password, non è richiesta la definizione. Dopo un login con successo, tutti i livelli 1-4 sono automaticamente sbloccati.

Se nonostante questo, si rendesse necessario utilizzare un login delle password per differenziare i permessi di lettura e scrittura, si devono applicare le seguenti regole:

- Se non è stata definita nessuna password a nessun livello, non vi è protezione attiva e l'utente ha l'accesso completo a tutte le funzioni, senza dover introdurre nessuna password.
- Una password definita, attiva la protezione di accesso da questo livello. Esempio: è stata definita solo una password per il livello 1. → In questo caso, il web server è protetto per tutti gli accessi e sarà richiesta l'introduzione della password. Dopo la sua introduzione, anche i livelli superiori (livelli da 2 a 4) saranno sbloccati, fintanto che non saranno anch'essi protetti da password.
- Una password definita sblocca l'accesso al proprio livello ed a quelli superiori, o fino al prossimo superiore che ha la password di protezione. Esempio: password definita per il livello 1 e password definita per il livello 3. → In questo caso, introducendo la password del livello 1, sblocca anche il livello 2. Introducendo la password di livello 3 sblocca i livelli da 1 a 4.

File Access Password:

Questa password protegge o sblocca l'accesso in lettura ai file ed a tutti i livelli superiori.

Default: ""

Impostazione raccomandata: **"definire password"**

→ Definire sempre. Questo fornisce la piena protezione al web server.

Attenzione: la finestra di dialogo password è generalmente visualizzata (per tutti i livelli) solo se è stata definita una password per quel livello.

Read CGI Access Password:

Questa password protegge o sblocca l'accesso in lettura all'interfaccia CGI ed a tutti i livelli superiori. L'interfaccia CGI è protetta per la lettura degli elementi PCD (registri, DB, flag, testi, ...).

Default: ""

Impostazione raccomandata: ""

Se un utente necessita di avere accesso solo in lettura (es. per leggere i dati di log o per visualizzare gli stati di sistema), è sufficiente definire una password per il livello 1 (**File Access**) e per il livello 3 (**Read/Write CGI Access**).

Read/Write CGI Access Password:

Questa password protegge l'accesso in scrittura all'interfaccia CGI ed a tutti i livelli superiori. L'interfaccia CGI è protetta per la scrittura degli elementi PCD (registri, DB, flag, testi, ...).

Default: ""

Impostazione raccomandata: **"definire una password di protezione alla scrittura solo se necessario"**

Se un utente richiede di avere accesso in scrittura solo dopo aver introdotto la password, è qui dove si deve definire una password.

Global Access Password:

Questa password rimane disponibile per ragioni storiche. La definizione non è necessaria.

Default: ""

Impostazione raccomandata: "non necessaria"

Regole per scegliere una password:

La password può contenere fino a 31 caratteri e non deve contenere caratteri speciali, diresis o spazi. Non viene fatta distinzione tra lettere maiuscole e minuscole.

Per ottenere la migliore protezione possibile, raccomandiamo di scegliere almeno 10 caratteri (più è lunga, più è sicura), comprendenti sia lettere che numeri. Non vanno utilizzate parole che siano facili da indovinare (es. il nome del sistema).

3.2 Introduzione della password nel web client

3.2.1 Pannello Micro-Browser

La password di protezione del PCD.Web-Server è supportata dai pannelli Micro-Browser a partire dalla versione firmware **1.20.3x**.

Da questa versione, le password si possono memorizzare nel menu di setup del pannello Micro-Browser. Vedere sotto le istruzioni per la configurazione della password.

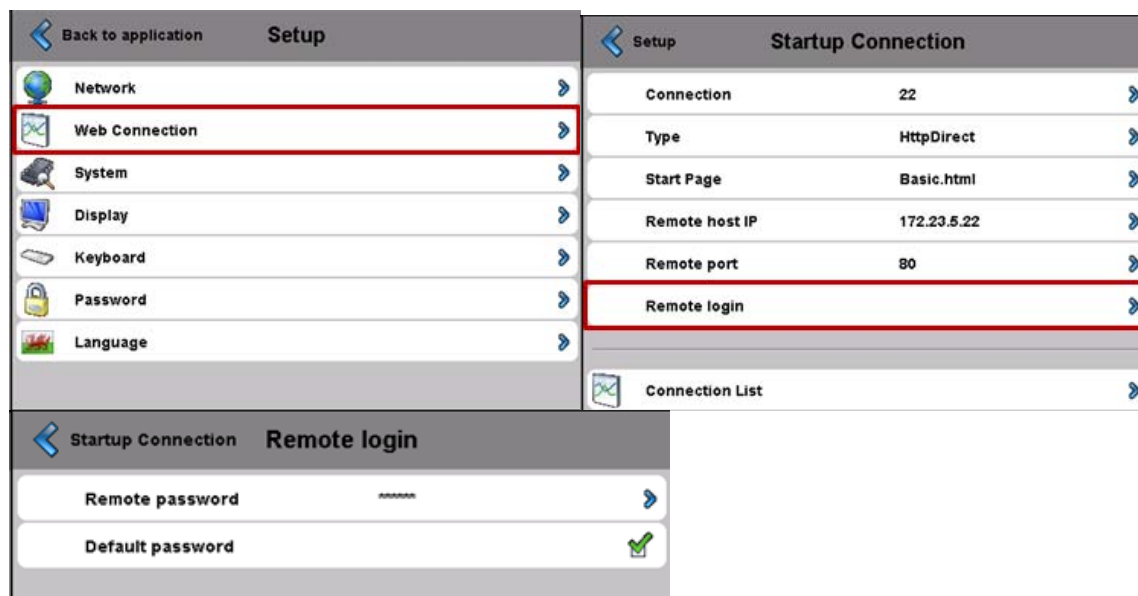
Quando si tenta di stabilire una connessione, se non è memorizzata nessuna password, sullo schermo del pannello sarà visualizzato il messaggio: "**PCD Password required!**". Per il successo di una connessione è obbligatoria la presenza di una password memorizzata nel menu di Setup.

Passo 1) Aprire il menu di Setup

Il menu di Setup si può aprire sia durante l'avvio del dispositivo o con una pressione prolungata (10 secondi) su un'area libera nell'applicazione.

Passo 2) Editare Start-up Web Connection

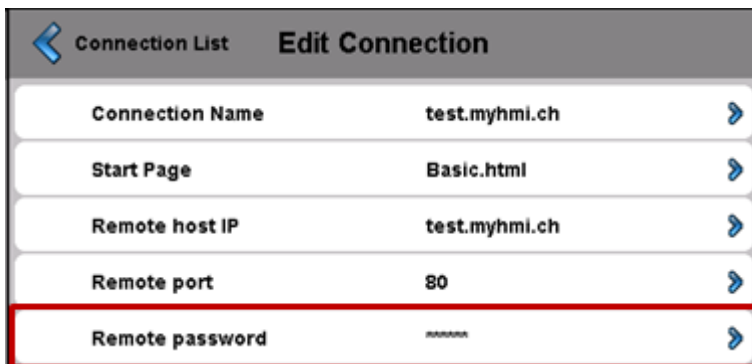
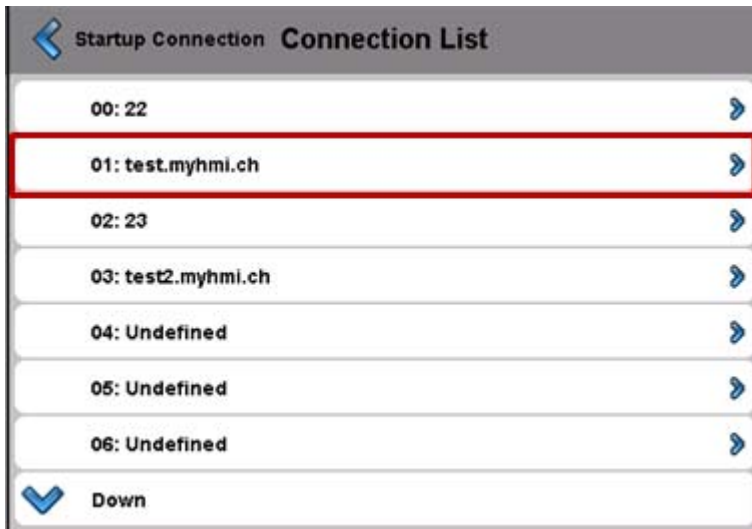
- ➔ Setup menu ➔ Web Connection ➔ Remote login
- ➔ Remote Password
 - Qui si deve introdurre la password per l'accesso al web server.
 - E' possibile impostare questa password come password di default. In questo caso, questa password sarà sempre utilizzata se, durante una connessione, il web server richiede una password. Se una password è definita per una stazione sulla Connection List, questa sarà utilizzata per prima. Se non è possibile stabilire con successo un web server login con questa password memorizzata nella stazione, sarà utilizzata la password definita di default per un altro tentativo di login al fine di attivare la connessione.



Passo 3) Editazione della Connection List

Se si deve utilizzare un singolo pannello Micro-Browser per l'accesso a controllori multipli con differenti password, si deve creare una connessione nella Connection List per ogni controllore, con la password appropriata.

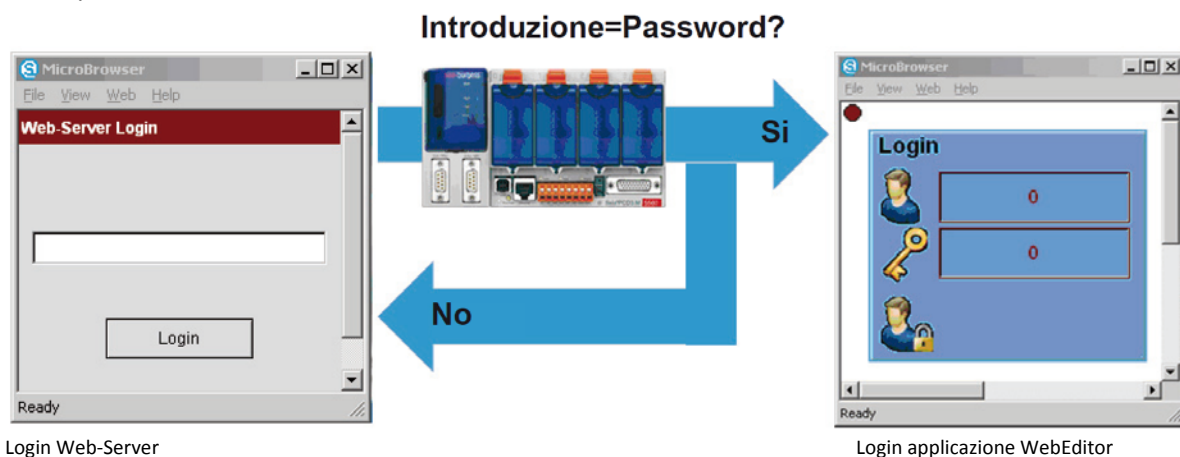




3.2.2 Micro Browser Windows CE ed eXP

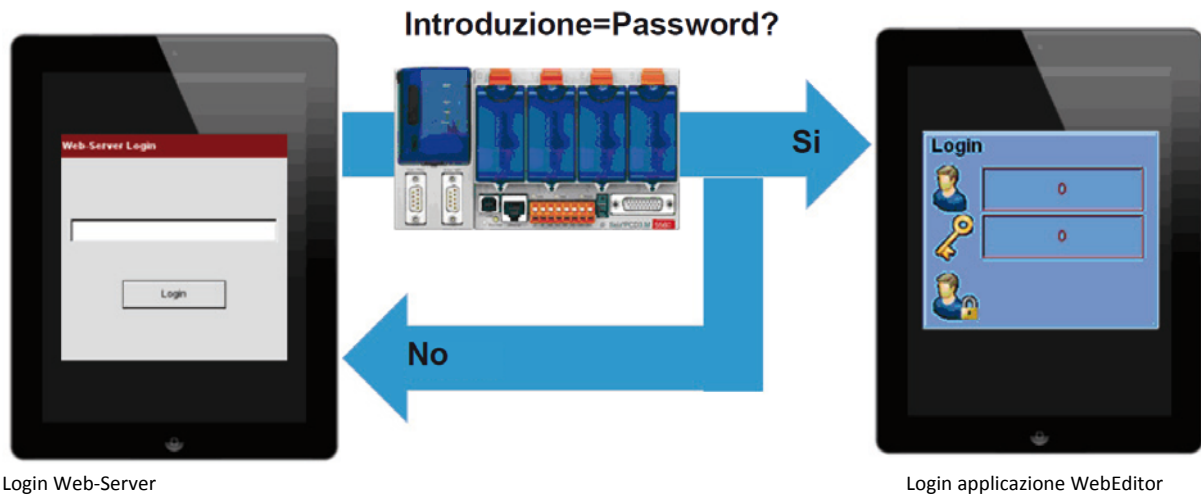
I Micro-Browser per i dispositivi su base Windows supportano il login password per il web server dalla versione 1.5.15.131c.

In un controllore PCD con attivata una password per il web server, gli utenti devono prima effettuare il log on per accedere al web server e poi, nell'applicazione WebEditor, identificare nuovamente se stessi per la richiesta utente.



3.2.3 iOS Micro Browser app

L'app Micro-Browser per I dispositivi Apple supporta il login password per il web server a partire dalla versione 1.5.15.130

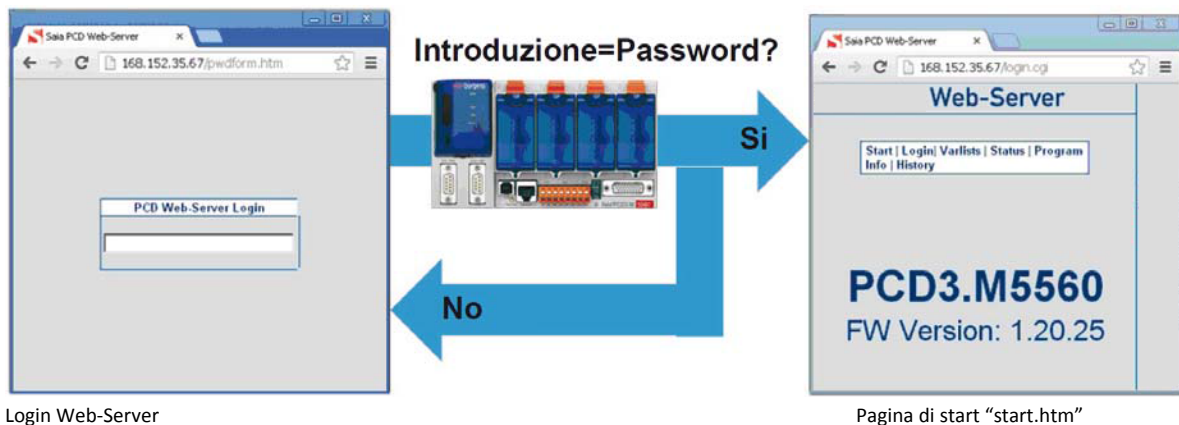


3.2.4 Browser PC con Java applet

I browser PC con una Java applet supportano il meccanismo di password per il Saia PCD.Web-Server. Quando si accede ad un Saia PCD.Web-Server protetto da password, viene caricato automaticamente il file "pwdform.htm", che è definito nel Device Configurator. Questo vi permette di inviare la password introdotta al PCD.Web-Server. Se l'introduzione è corretta, viene caricato il file "start.htm" definito nel Device Configurator e parte la visualizzazione.

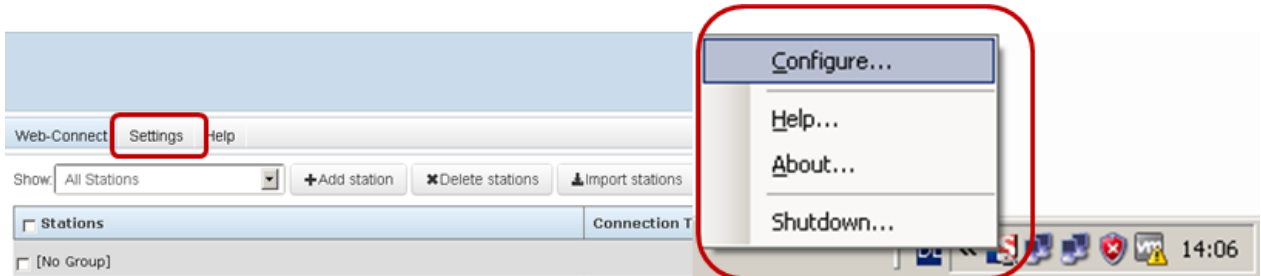
NOTA: Se si deve caricare direttamente un'applicazione web, il nome della pagina HTML del progetto WebEditor deve essere introdotto nel Device Configurator.

Suggerimento: Nel PC browser, in qualsiasi momento si può visualizzare la pagina di stato del PCD.Web-Server digitando "status.htm".



3.2.5 SBC .Net Web Connect / WebFTP

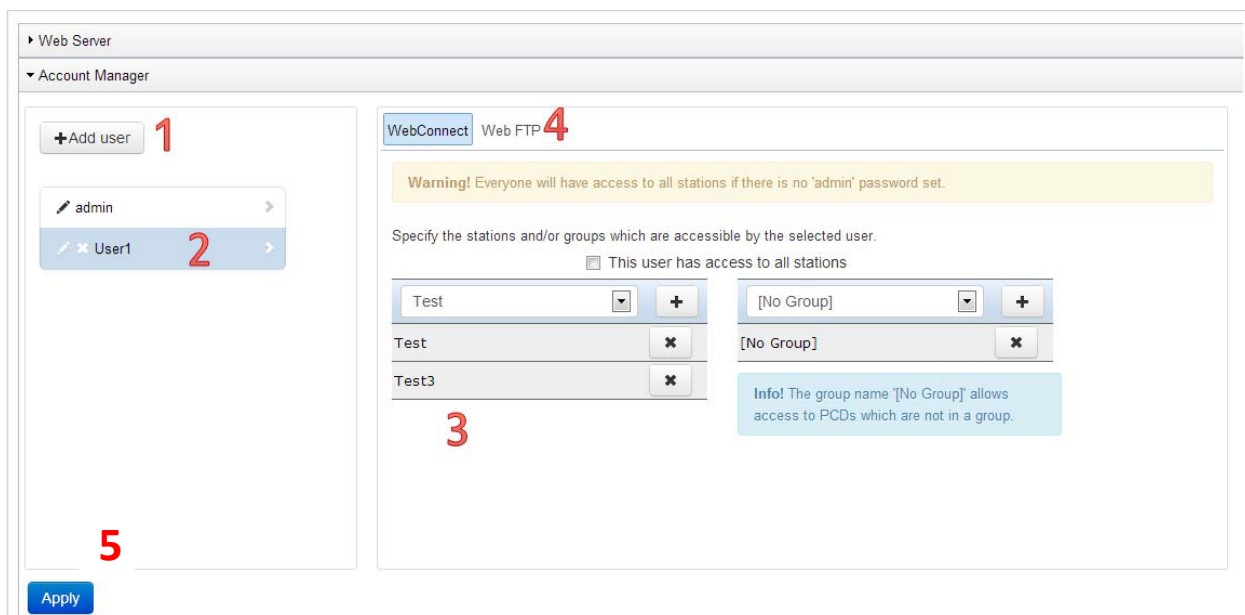
SBC.Net ha già integrata la propria gestione dell'account, che è disponibile tramite l'interfaccia web SBC.Net.



La gestione dell'account è allocata nelle impostazioni di SBC.Net. E' qui che si possono definire gli utenti e le password, insieme con i relativi diritti per gli utenti selezionati.

Si deve definire una password per l'utente "admin", altrimenti tutte le stazioni saranno completamente accessibili.

- 1) Aggiungere un nuovo utente. Ogni utente necessita di un nome utente e di una password associata.
- 2) Elenco degli utenti attualmente esistenti. Si può editare o cancellare un utente.
- 3) Diritti dell'utente attualmente selezionato. I diritti cambieranno, in base alle funzioni abilitate in Saia.Net
- 4) Selezionare le funzioni WebConnect o Web FTP
- 5) Applicare le modifiche all'utente selezionato.

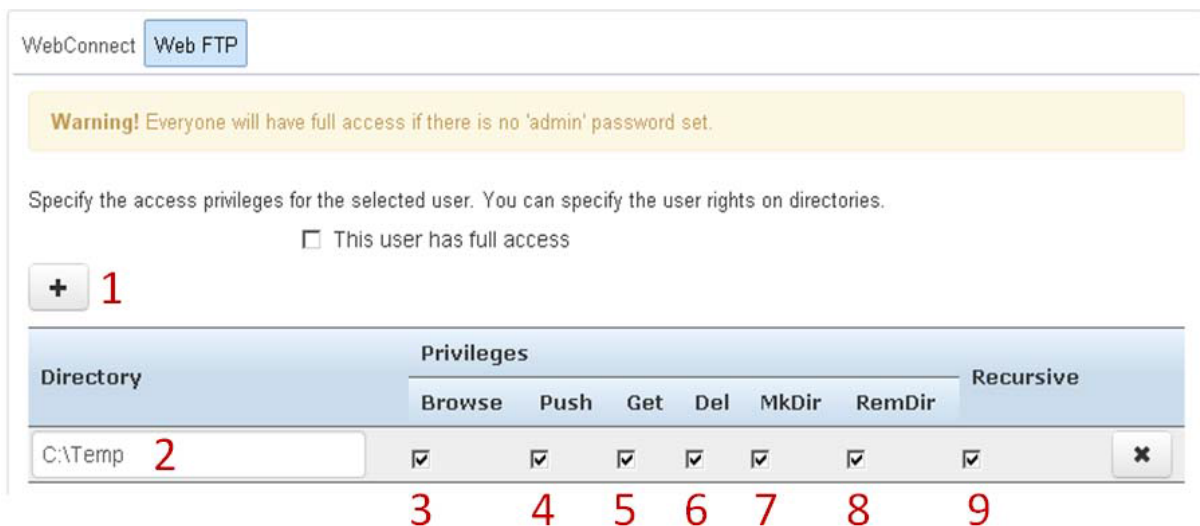


La tabella Web FTP consente di definire i diritti utente per il Web FTP server locale di SBC.Net

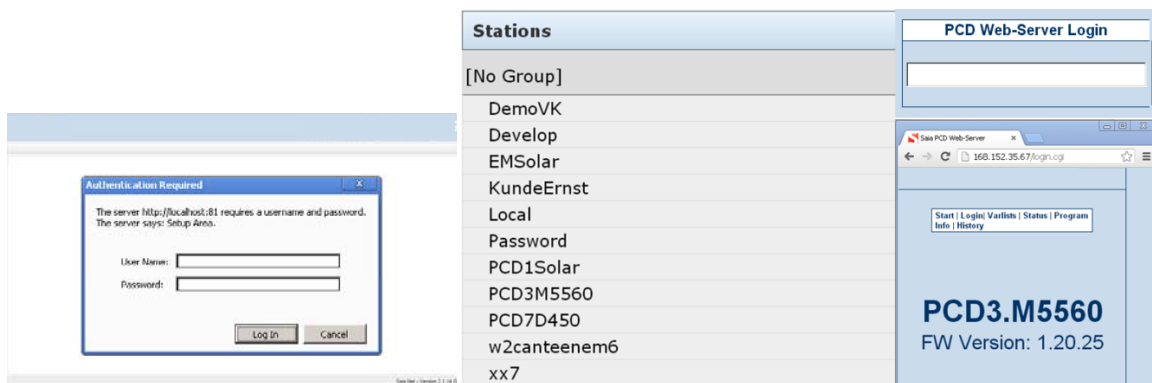
- 1) Aggiungere una nuova directory per l'utente attualmente selezionato
- 2) La locazione della directory locale si deve sbloccare via Web FTP.

L'utente ha i seguenti diritti:

- 3) Browse: Visione del contenuto corrente della directory
- 4) Push: Scrittura dei file nella directory
- 5) Get: Lettura dei file nella directory
- 6) Del: Cancellazione dei file nella directory
- 7) Mkdir: Creazione di sottodirectory
- 8) RemDir: Rinominare le directory esistenti
- 9) Recursive: Includere tutte le sottodirectory nell'attuale catena definita dei diritti.



All'apertura di SBC.Net WebConnect, vi sarà richiesto di introdurre il nome utente e la password. Dopo questo login, avrete i diritti dell'utente "loggato". Cliccando su una qualsiasi delle stazioni disponibili per questo utente, sarà consentito l'accesso al Saia PCD.Web-Server.



3.3 Compatibilità PG5 e versioni firmware COSinus

Le funzioni di protezione descritte sono, da tempo, supportate dai controllori Saia PCD. Per utilizzarle correttamente, le funzioni devono essere supportate anche dai dispositivi browser e dal Device Configurator PG5.

Le seguenti versioni dei dispositivi Micro-Browser supportano il meccanismo password Web-Server:

Prodotto	Codice prodotto	Dalla versione firmware	Note
Web-Panel Micro-Browser VGA e SVGA	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	
Prodotto	Codice prodotto	Dalla versione firmware	Note
Pannello Micro-Browser QVGA	PCD7.D457BTCF	Non supportato	
	PCD7.D457STCF	Non supportato	
	PCD7.D457SMCF	Non supportato	
Prodotto	Codice prodotto	Dalla versione firmware	Note
Micro-Browser eWinCE	PCD7.D51xxTX010	1.5.15.131c	
	PCD7.D51xxTL010	1.5.15.131c	
	PCD7.D51xxTA010	1.5.15.131c	
Micro-Browser eWinXP	PCD7.D61xxTL010	1.5.15.131	
	PCD7.D61xxTA010	1.5.15.131	
Prodotto	Codice prodotto	Dalla versione firmware	Note
App MB iOS		1.5.15.130	
App MB iOS LITE		1.5.15.130	
App MB Android		Non ancora supportato	Nuova versione presto disponibile

La seguente tabella mostra le interdipendenze riguardanti la configurazione web server in PG5 e la versione firmware COSinus dei controllori PCD.

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

*Con PG52.x e con versioni firmware < 1.14.nn, devono essere impostate nel Device Configurator.

Per l'attivazione della password web server, **non è necessario** l'aggiornamento del pacchetto PG5.

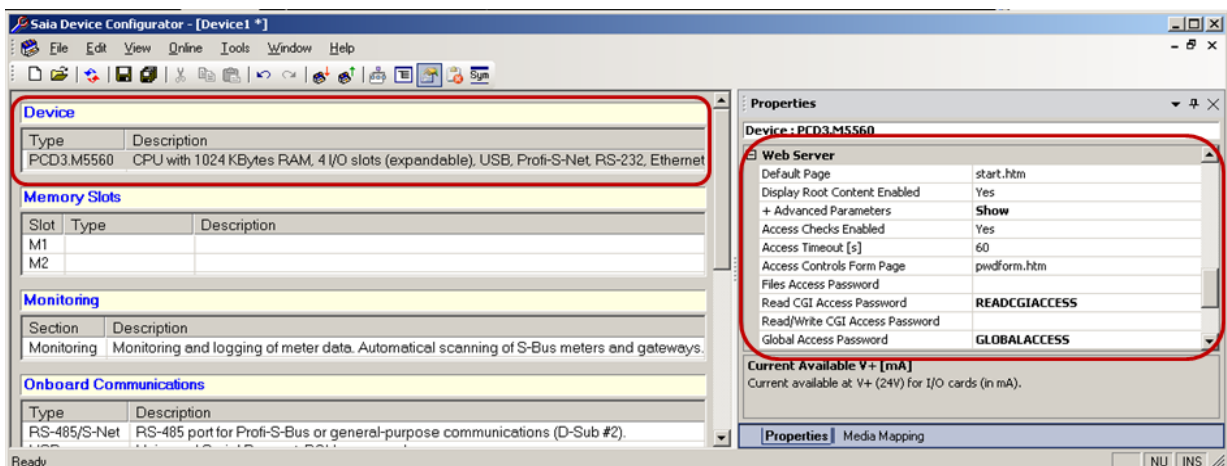
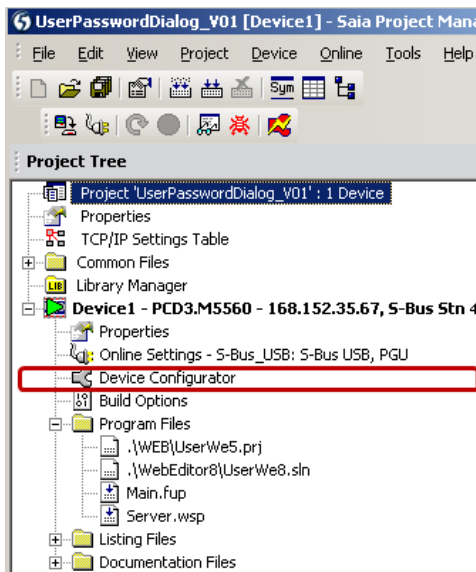
Per le versioni firmware inferiori alla 1.14.nn, le impostazioni della password e del web server devono essere definite con il progetto web server (.wsp).

Le versioni firmware comprese tra le versioni 1.14.nn e 1.16.nn supportano la configurazione sia mediante il progetto web server, sia mediante Device Configurator.

Dalla versione firmware 1.20.nn, le impostazioni del web server si possono modificare solamente mediante Device Configurator.

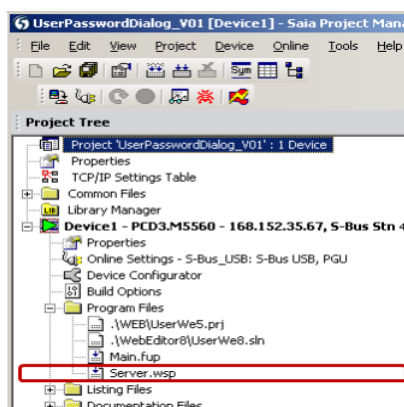
3.3.1 Attivazione della password PCD.Web-Server con il Device Configurator

La configurazione del web server è definita nel Device Configurator. Le impostazioni sono allocate sulla scheda CPU.



3.3.2 Attivazione della password Saia PCD.Web-Server con il progetto Web Server (.wsp)

La configurazione del web server è definita dal progetto web server. Questo è incluso fra i file di programma caricati nel controllore con il programma di download.



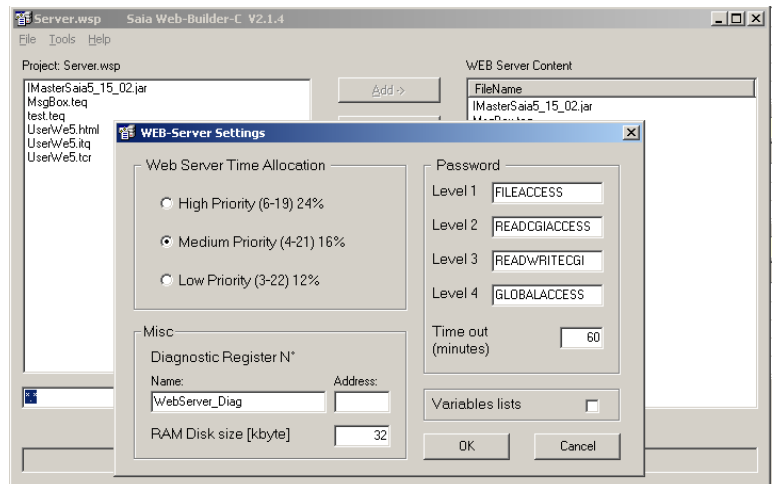
Nel progetto Web-Server (.wsp), si possono caricare i file e si possono impostare le password a 4 livelli.

Livello 1: File Access Password:

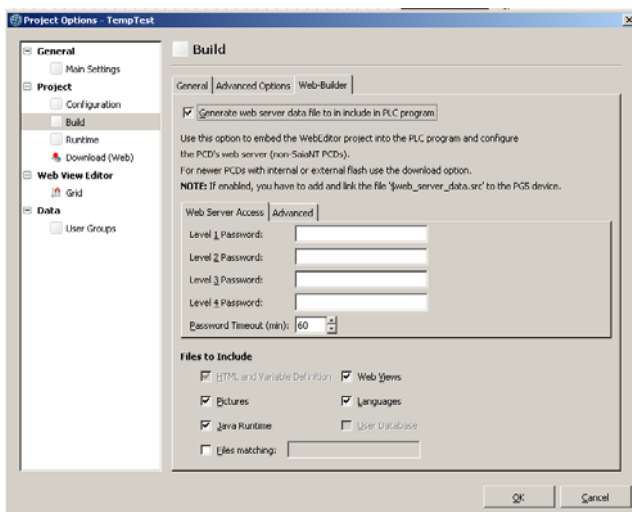
Livello 2: Read CGI Access Password:

Livello 3: Read/Write CGI Access Password:

Livello 4: Global Access Password:



Nel WebEditor 8 le impostazioni seguenti saranno effettuate nelle impostazioni di progetto



4. Protezione FTP server

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

FTP Server	
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

A partire dalla versione PG5 2.1.200, quando nel Device Configurator si crea una nuova CPU, l'FTP-Server è ora disattivato di default. Anche la password "root" e l'utente "rootpasswd" di default sono disattivate. Per ragioni di sicurezza, si dovrebbe attivare l'FTP-Server e creare un nuovo utente, quando necessario. I parametri dell'FTP Server sono memorizzati nella scheda IP Transfer Protocols.

Allo stesso tempo, anche la password individuale dell'utente è definita con una lunghezza massima complessiva di 20 caratteri.

Ethernet Protocols	
Section	Description
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.
IP Protocols	DNS, SNMP, SNMP protocols.
HTTP Portal	HTTP Portal Communication For PCD Over Private Network.

FTP Server	
FTP Server	Yes
TCP Port No.	21
User Name	
User Name	
+ Advance	Show
Connection	0
Maximum F	3
Remove De	Yes

FTP Server User Name and Access Rights

User Name : SBC_Support

Password : Support

User's Groups

Group 1 Group 2

Group 3 Group 4

WEB Group

Access To Files Created By Other Groups

Group 1 Group 2

Group 3 Group 4

WEB Group

Access Rights

Read/Write Read Only

Help OK Cancel

Regole per selezionare una password:

Per ottenere la maggiore protezione possibile, raccomandiamo di sceglierla di almeno 10 caratteri (più è lunga, maggiore è la protezione) comprendenti sia lettere che numeri. Non vanno utilizzate parole che siano facili da indovinare (es. il nome del sistema).

FTP Server (Yes/No)

Attivazione o disattivazione dell'FTP server

Default: "No"

Impostazione raccomandata: "No" per sistemi critici

Se è necessario l'FTP-Server, questi deve essere attivato e va creato un nuovo utente con password.

Remove Default User

L'utente default è ora disattivato per bloccare accessi non autorizzati mediante password conosciute e comunicate pubblicamente. Per accedere all'FTP-Server, si dovrebbe creare almeno 1 nuovo utente.

Default: "Yes"

Impostazione raccomandata: "Yes"

User Name

Consente la creazione di un massimo 10 utenti individuali con l'appartenenza al gruppo e con diritti di accesso in lettura e scrittura. Ogni utente può essere assegnato ad un gruppo. Inoltre, è possibile consentire all'utente i diritti di accesso di altri gruppi. Si dovrebbe definire un "administrator" o "root user" con un'autorizzazione di accesso a tutti i gruppi con diritti di "Lettura/Scrittura".

TCP Port Number

La porta 21 è definita come porta di default per la comunicazione FTP. Il numero di porta dell'FTP server si può cambiare con questo parametro.

Default: "21"

Impostazione raccomandata: "only change if necessary"

Connection Timeout (s)

Se è stata stabilita una connessione con l'FTP server, ma non è stata utilizzata per scambiare dati con il server, dopo il periodo di timeout specificato, la connessione esistente sarà chiusa dall'FTP server. Per assicurarsi che la connessione FTP sia chiusa dal server, anche se il client non l'ha terminata correttamente, si raccomanda un valore di default di 5 minuti (300 secondi).

Default: "300"

Impostazione raccomandata: "300"

Maximum FTP Connections

Definisce il numero massimo di connessioni parallele con l'FTP server

Default: "3"

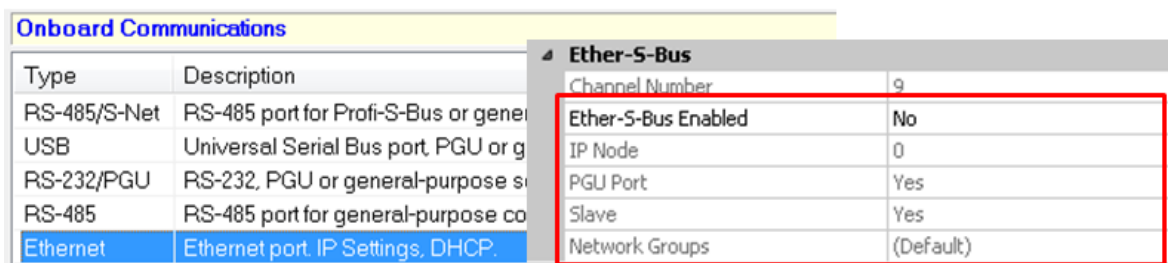
Impostazione raccomandata: "only change if necessary"

5. Protezione Ethernet S-Bus

Ether-S-Bus supporta tutti i servizi e le funzioni per lo scambio dati, per la programmazione, per la messa in servizio e la manutenzione dei controllori Saia PCD. L'accesso avviene mediante il tool di programmazione PG5, un sistema Scada o un OPC server (solo per lo scambio dati).

I diritti di accesso all'Ether-S-Bus si possono definire nel Device Configurator PG5.

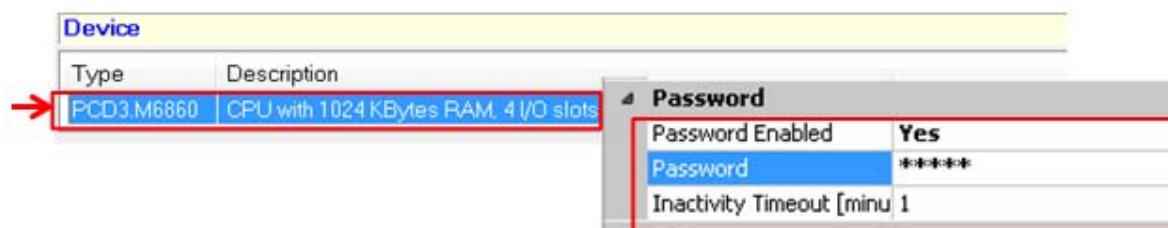
Vi è un cambiamento nel Device Configurator PG5 a partire dalla versione 2.1.200 e nel firmware PCD COSinus a partire dalla versione > 1.22.10, dove la comunicazione Ether-S-Bus è ora disattivata di default. Si fa notare che, la comunicazione S-Bus non può essere utilizzata ne con il tool di programmazione PG5, ne con nessun altro sistema (Scada, OPC server).



Type	Description
RS-485/S-Net	RS-485 port for Profi-S-Bus or general purpose
USB	Universal Serial Bus port, PGU or general purpose
RS-232/PGU	RS-232, PGU or general-purpose serial port
RS-485	RS-485 port for general-purpose communication
Ethernet	Ethernet port. IP Settings, DHCP.

Ether-S-Bus	
Channel Number	9
Ether-S-Bus Enabled	No
IP Node	0
PGU Port	Yes
Slave	Yes
Network Groups	(Default)

Quando è attivato l'Ether-S-Bus, l'accesso con il dispositivo di programmazione PG5 può essere ulteriormente protetto con una password.



Type	Description
PCD3.M6860	CPU with 1024 KBytes RAM, 4 I/O slots

Password	
Password Enabled	Yes
Password	*****
Inactivity Timeout [min]	1

Sono applicate le seguenti regole:

Se la password è disabilitata, su tutte le interfacce PGU (Ethernet, USB, seriale) sono supportati tutti i servizi senza restrizioni.

La password definita può avere una lunghezza totale di 25 caratteri e deve comprendere lettere maiuscole (A, B, C) o numeri (0-9).

Per una buona protezione, raccomandiamo la scegliere almeno 10 caratteri (più è lunga, più è sicura), comprendente lettere e numeri. Parole facili da indovinare, come ad es. il nome del sistema, non si dovrebbero utilizzare.

Attenzione: se si perde la password, si deve resettare il controllore con la funzione di reset.

Se è stata definita una password, quando si stabilisce una connessione con il tool di programmazione PG5, si deve introdurre una password per tutte le interfacce PGU (Ethernet, USB, seriale).

Appaiono le seguenti finestre di dialogo:

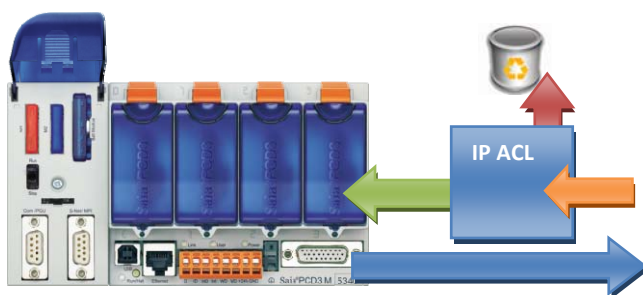


Nota: Con Ether-S-Bus è sempre abilitato l'accesso (lettura e scrittura) agli elementi interni PCD (R, F, I/O, T/C) (anche con una password configurata).

6. Filtro di accesso IP (IP Access List, ACL)

A partire dalle versioni firmware COSinus 1.22.10 e PG5 2.1.200, i controllori PCD supportano il filtro di accesso IP. Gli indirizzi IP autorizzati e non autorizzati sono inseriti in una “white” o “black” list.

- L’accesso ed i telegrammi dagli indirizzi IP appartenenti alla White list sono identificati e gestiti dal sistema operativo COSinus. Telegrammi da altri indirizzi IP sono rifiutati.
- L’accesso ed i telegrammi dagli indirizzi IP appartenenti alla Black list sono identificati e rifiutati dal sistema operativo COSinus. Telegrammi da altri indirizzi IP sono gestiti.



In una rete locale, può essere pratico e necessario proteggere l’accesso al controllore con il filtro di accesso IP.

6.1 Device Configurator

La “White list” o la “Black list” sono definite nel Device Configurator di PG5 nelle “Onboard Communications” – sezione “Onboard Ethernet”.

Onboard Communications		TCP/IP	
Type	Description	Channel Number	Value
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purp	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

Per poter editare le proprietà del filtro IP, in “+ Access Control List” il parametro deve essere impostato su “Show”.

1) “IP Filtering Enabled”

Commuta il filtro di accesso IP in On o in Off

2) "IP Filter Policy"

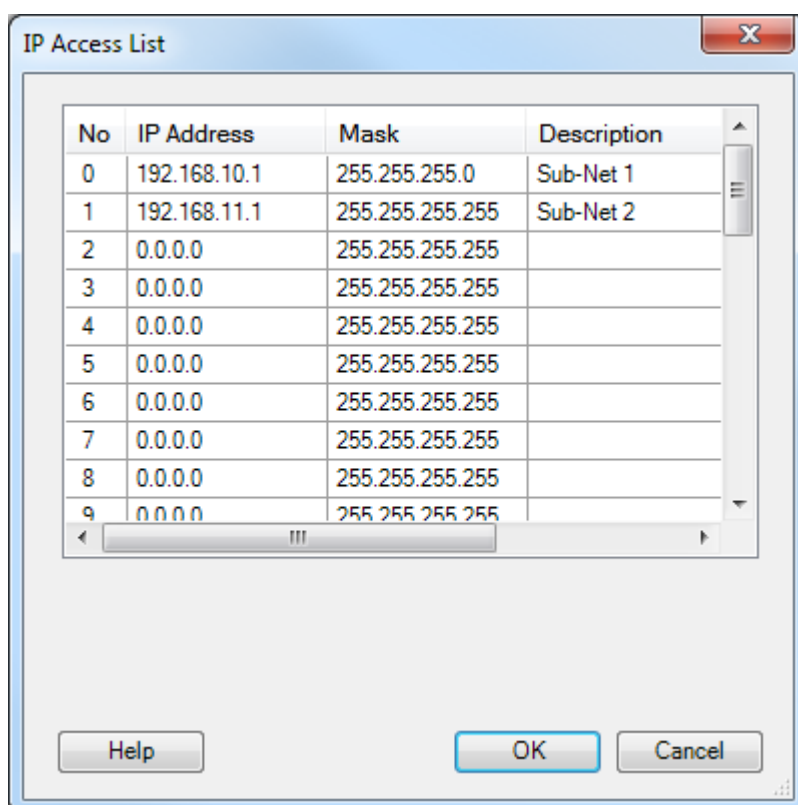
Impostazione della modalità filtro

"White list" = blocca tutto → sono permessi solo gli indirizzi presenti sulla lista

"Black list" = blocca tutto → blocca solo gli indirizzi presenti sulla lista

3) "IP Filtering List"

Elenco degli indirizzi IP e "mask" associati, che sono sia gestiti che rifiutati dal sistema operativo COSinus in funzione della modalità selezionata.



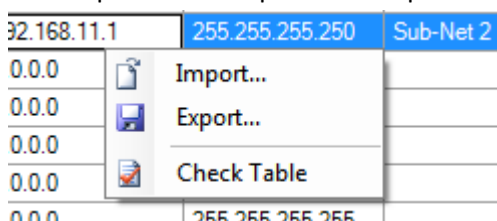
La mask può essere utilizzata anche per definire intere sottoreti per il filtro. L'indirizzo IP e la mask definiscono la rete o l'indirizzo della sottorete.

Per esempio,

L'indirizzo IP 192.168.10.1 con un mask definito di 255.255.255.0 permette o blocca la comunicazione di tutti i dispositivi nella rete 192.168.10.0/24 (255 indirizzi)

L'indirizzo IP 192.168.11.1 con un mask definito di 255.255.255.255 permette o blocca la comunicazione esclusivamente da questo indirizzo IP.

La lista può essere esportata o importata come file .csv



6.2 FBox Fupla

Il filtro di accesso IP può essere gestito dal programma utente PCD mediante FBox.

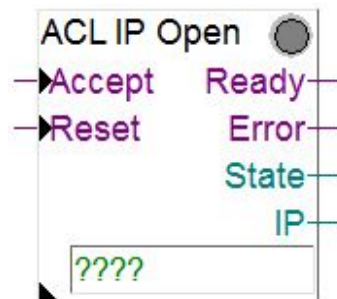
1) FBox ACL IP Filter

Consente di attivare o disattivare il filtro IP



2) FBox ACL IP Open

Permette di aprire un indirizzo IP per accedere al dispositivo. Questo FBox può essere utilizzato, ad esempio, per aprire temporaneamente un indirizzo IP per un mail server in modo che il controllore possa inviare una mail. In questo modo, si possono aggiungere alla "White list" fino a 32 indirizzi IP (32 FBox).

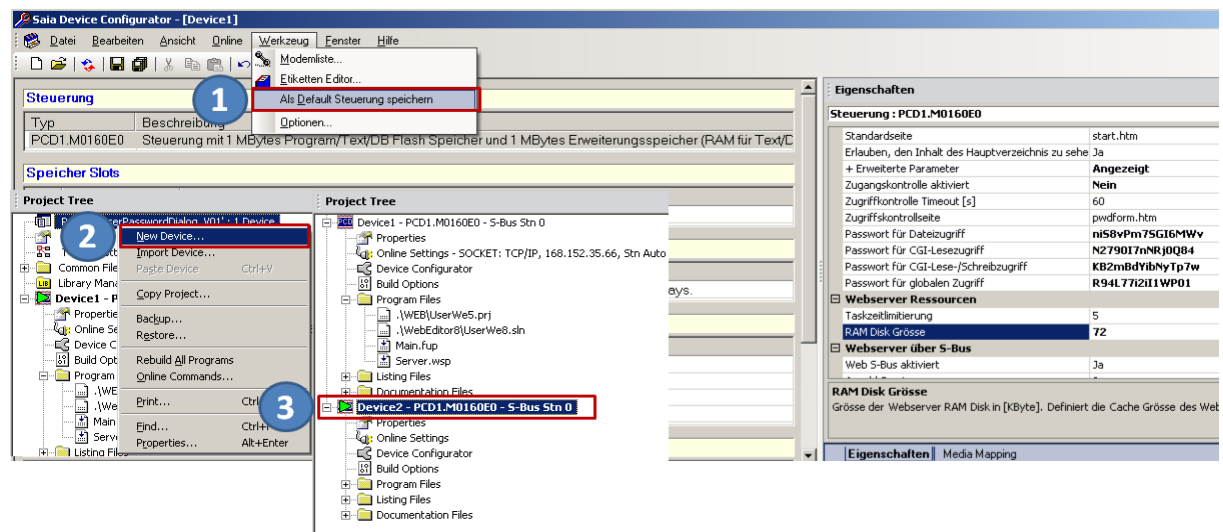


Maggiori informazioni sono disponibili nell'help online dell'FBox.

7. Editazione dei template dei dispositivi nel Device Configurator PG5

Per consentirvi di configurare coerentemente una CPU con le medesime impostazioni, come default, è possibile definire un modello del dispositivo configurato, per utilizzarlo con le altre CPU dello stesso tipo.

In questo modo, tutte le impostazioni definite nel template del Device Configurator saranno trasferite alla nuova CPU, quando questa sarà creata.



- 1) Rendere le impostazioni attuali del Device Configurator della CPU, come impostazioni di default per questo tipo di CPU.
- 2) Aggiungere un nuovo dispositivo
- 3) Il nuovo dispositivo viene creato con la configurazione del dispositivo definita al punto 1.

Fare una sola volta la definizione dei vostri componenti attivi della CPU, quali il Web server e l'FTP server, così come i vostri livelli di sicurezza, ServiceKey o utenti autorizzati; salvare queste impostazioni per questo tipo di CPU.

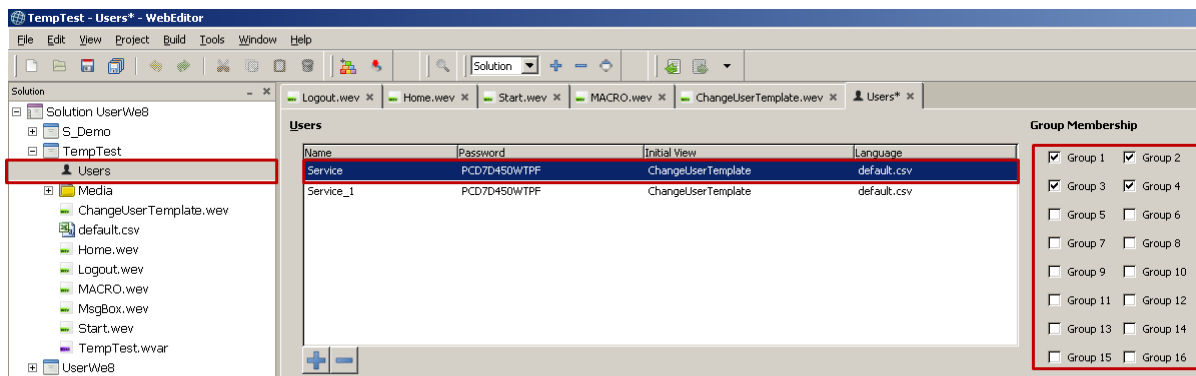
8. Nuova gestione utente con controllo di accesso nel WebEditor 8

A partire dalle versioni firmware COSinus 1.22.10 e PG5 V2.1.200, nel WebEditor 8 è disponibile una nuova gestione dell'utente ed un controllo di accesso. I template per il nuovo meccanismo sono elencati nella libreria dei template di WebEditor 8, nella sezione "Access Control". I template sono utilizzabili solamente in connessione con il database utente generato dal WebEditor 8. Il nuovo controllo di accesso sostituisce la precedente "User Identification" (vecchio meccanismo di password) nel quale era possibile definire solo 4 livelli utente.

Il controllo di accesso permette ad un utente di essere organizzato in 16 gruppi. Questi gruppi non formano i livelli. Se un utente è membro di un gruppo, questi può accedere o utilizzare gli elementi e le funzioni di questo gruppo.

8.1 Database utente

Il WebEditor 8 è stato ampliato per includere un sistema di gestione utente. Si possono definire fino a 100 utenti all'interno del database utente. Un utente consiste di un nome utente, password, pagina di avvio e lingua. Inoltre, ogni utente è assegnato a differenti gruppi di utenti.

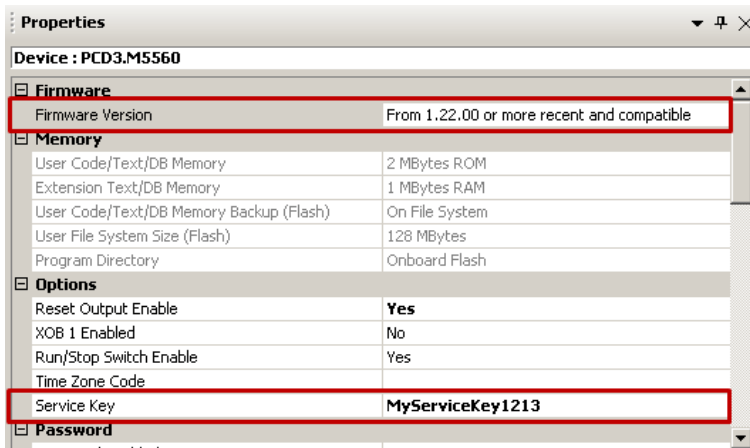


Il database utente è salvato in un'area sicura del controllore.

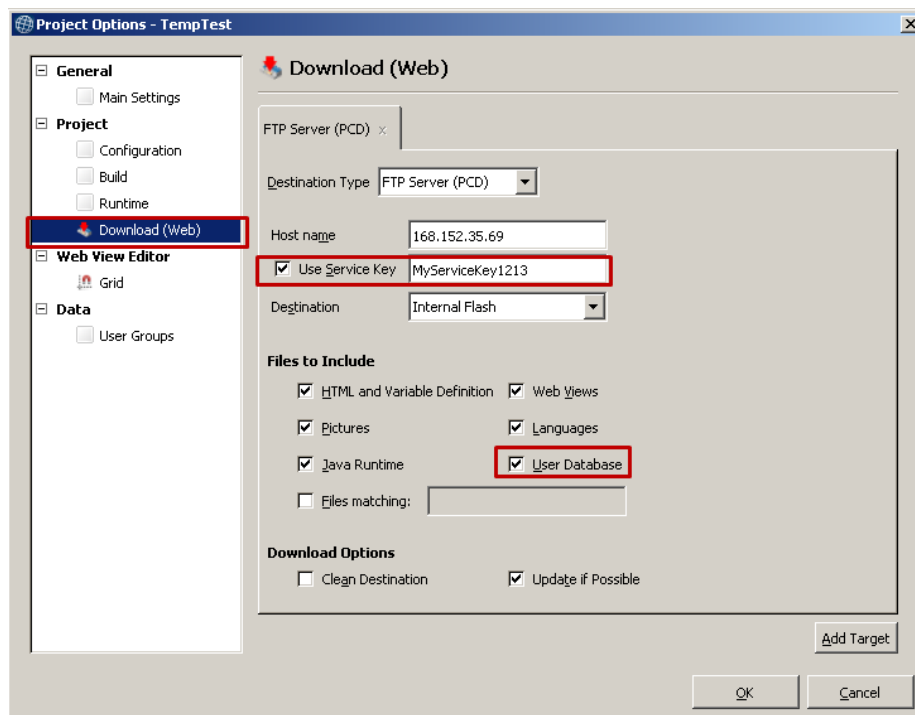
8.2 Download del database utente e service key

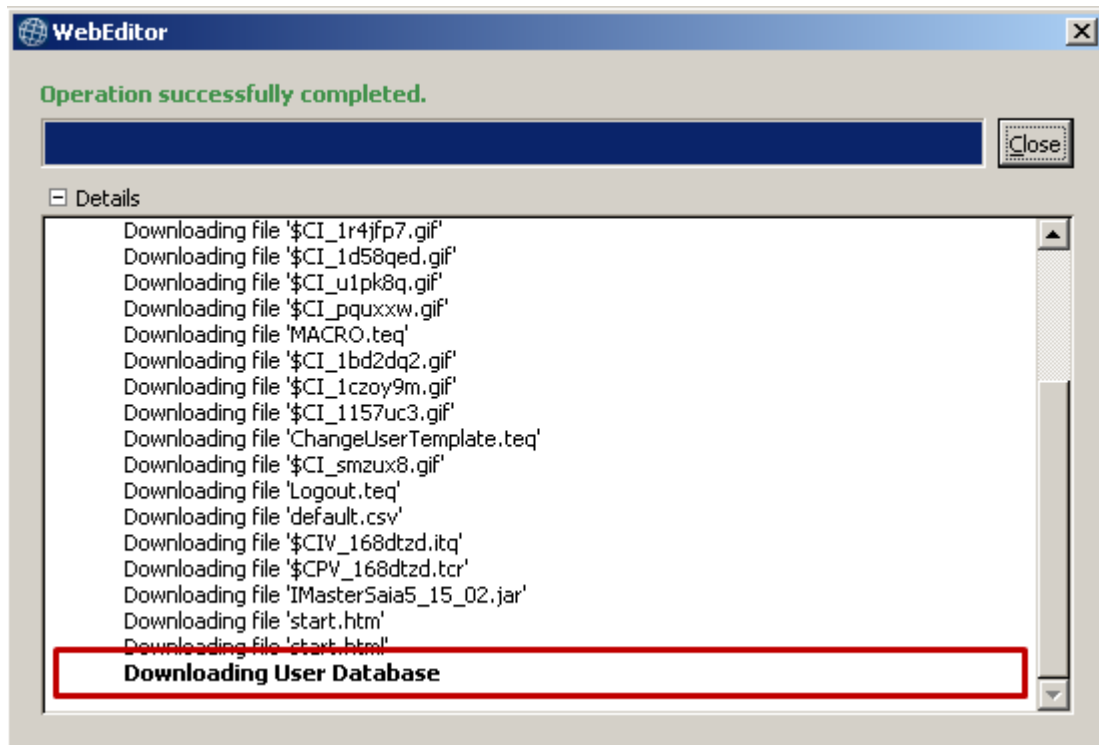
Per abilitare il WebEditor 8 a caricare il database utente nell'area protetta del controllore PCD, la service key deve essere definita nel Device Configurator.

La service key è utilizzata dal WebEditor 8 per farsi identificare dal controllore (FTP-Server). La service key è introdotta nell'area Device del Device Configurator PG5.



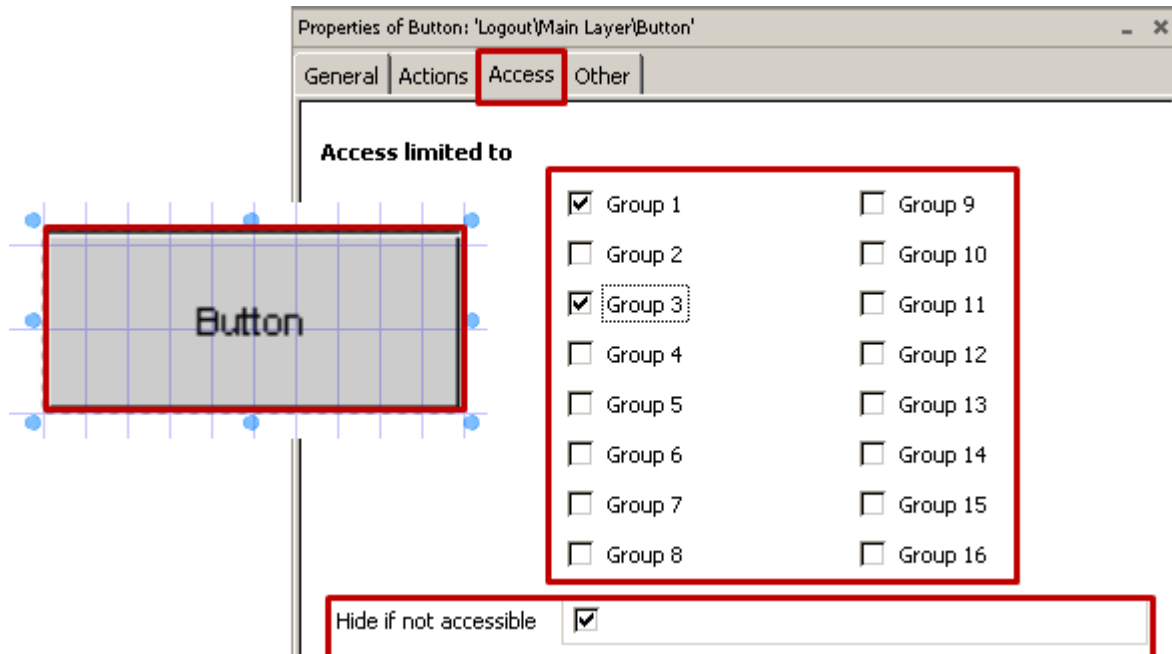
Per il download del database utente nel WebEditor 8, insieme con la service key, si deve utilizzare una destinazione di download: "WebFTP", "FTP Server (PCD)" o "PG5 CPU (S-Bus)". La service key qui introdotta, deve essere uguale a quella introdotta per il Device Configurator PG5.





8.3 Assegnazione dei diritti alle funzioni o agli elementi in WebEditor 8

Ogni elemento del WebEditor 8, compresi i pulsanti, i box di editazione, i gruppi o i livelli, può essere assegnato ad uno o più gruppi utente. I diritti utente sono introdotti nell'applicazione quando un utente effettua il log on. In questo modo, l'utente registrato può utilizzare le funzioni e gli elementi corrispondenti al suo gruppo di assegnazione. Se il box "Hide if not accessible" è attivato, l'elemento e le sue funzioni associate sono disattivate e nascoste agli utenti che non sono definiti nel gruppo.

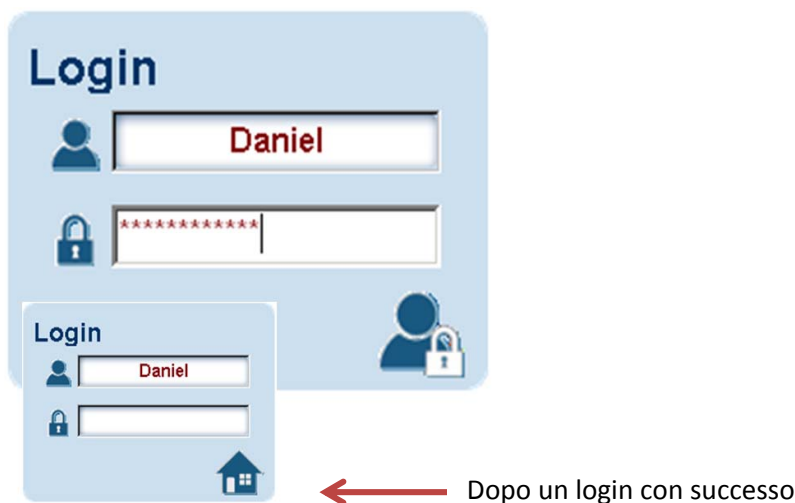


8.4 Template per il controllo utente

I template per il controllo utente possono essere utilizzati congiuntamente con la nuova gestione utente.

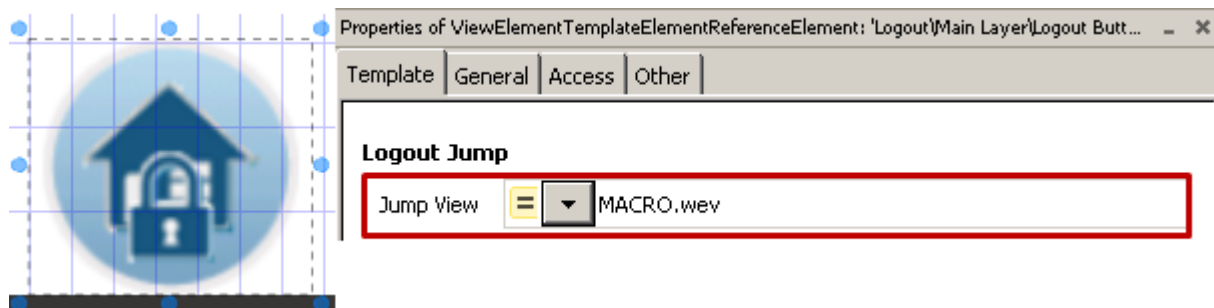
8.4.1 Template di login

Al login, il controllore verifica il nome utente e la password con il database utente. La password è trasmessa in modo criptato con hash code. Se il nome utente e la password sono corrette, all'utente (o all'applicazione HMI) vengono dati i relativi diritti con un gruppo di assegnazione, lingua e home page.



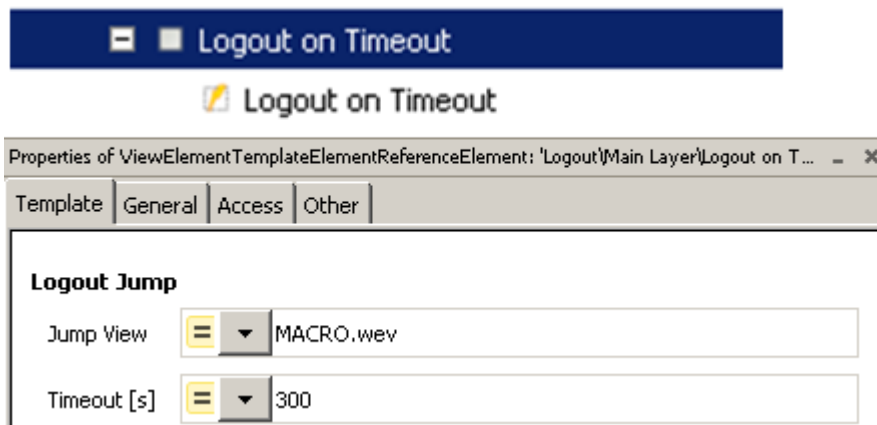
8.4.2 Template di logout

Se un utente è loggato mediante il template di login, le variabili interne sono impostate con il rispettivo gruppo, lingua e home page. Il pulsante di logout resetta queste variabili e cambia la pagina sulla visualizzazione di logout indicata nel template.



8.4.3 Logout automatico durante l'inattività

Se un utente è loggato mediante il template di login, le variabili interne sono impostate con il rispettivo gruppo, lingua e home page. Il template "Logout on Timeout" resetta queste variabili dopo un periodo di tempo specificato e cambia la pagina sulla visualizzazione di logout indicata nel template. Il valore di timeout può essere definito in secondi nel template.



8.4.4 Cambio password

L'utente può cambiare la propria password utilizzando il "Change Password Template". Per poter cambiare la password, si deve prima introdurre correttamente la password attuale. La nuova password deve essere introdotta due volte e poi confermata. La nuova password è quindi attiva. La vecchia password perde immediatamente la sua validità!

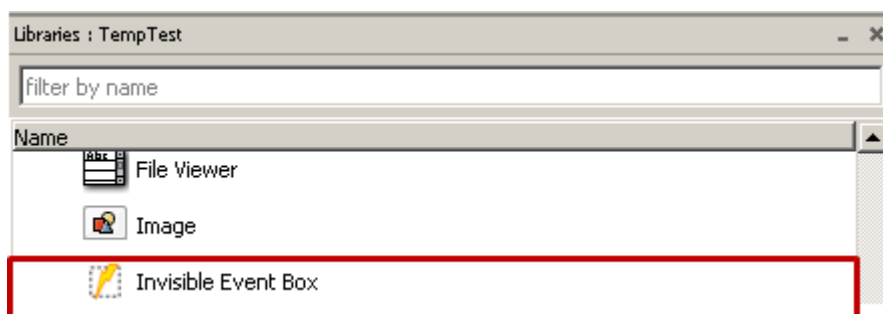


8.5 Compatibilità del nuovo controllo di accesso e la vecchia identificazione utente

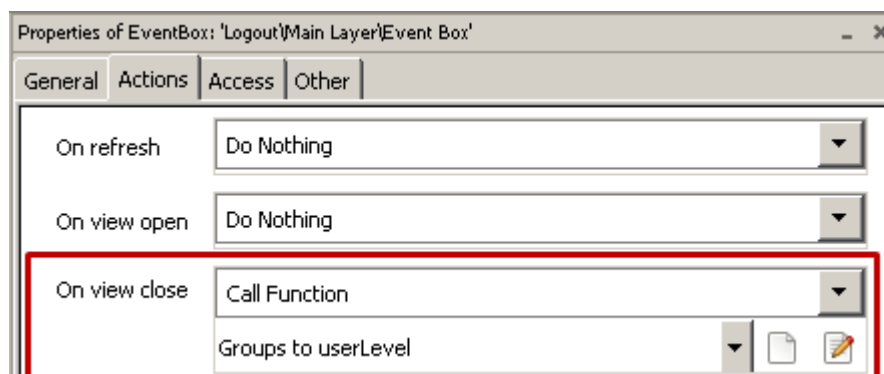
I template di controllo di accesso non sono compatibili con la soluzione di identificazione utente esistente. A differenza del vecchio processo di identificazione a 4 livelli, il nuovo controllo di accesso coinvolge 16 gruppi. Piuttosto che rappresentare i livelli, questi sono configurabili individualmente. Un elemento è visualizzato o attivo se l'utente registrato possiede i diritti del gruppo o dei gruppi.

Un progetto creato con WebEditor 5.15 o il vecchio sistema identificazione utente può essere portato sul nuovo sistema di gestione utente con un piccolo sforzo. Questo può essere fatto in WebEditor 8 utilizzando i nuovi template per il controllo di accesso; si devono definire 4 utenti ed i loro diritti visualizzati sulla variabile interna "userLevel". Non sono necessarie altre modifiche al progetto.

- 1) Si devono definire 4 utenti (da 1 a 4)
Dopo un login con successo, i diritti per gli utenti sono memorizzati nelle variabili interne "?S_User_L0..3".
- 2) I diritti per gli utenti si devono ora visualizzare sulla variabile interna "userLevel". Le variabili interne "?S_User_L0..3" possono contenere "0" o "1".
- 3) A questo proposito, può essere utilizzato un "Invisible Box Event".

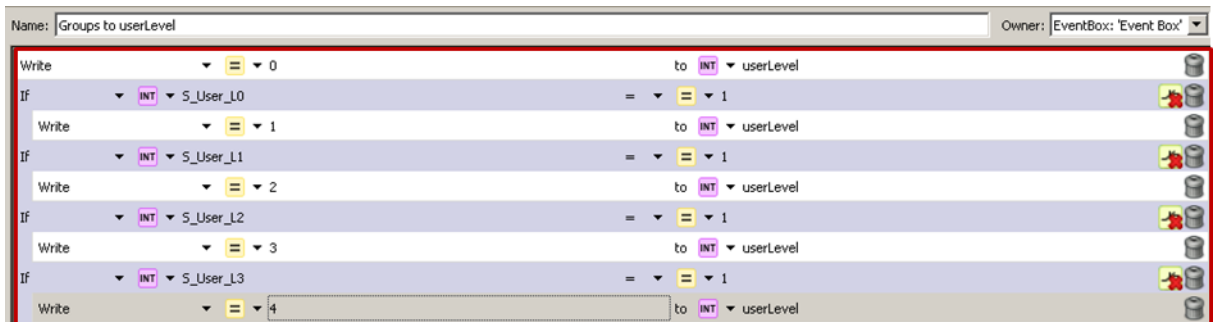


- 4) L' "Invisible Box Event" è posizionato sulla pagina con il template di login ed i diritti utente sono trasferiti alla variabile interna "userLevel" quando viene chiusa la pagina.



5) Questa funzione per il trasferimento dei diritti utente allo “userLevel” può essere implementata in questo modo:

- ➔ Resetare la variabile interna “userLevel”
- ➔ Impostare la variabile interna “userLevel” sulle basi dei diritti utente; quando si introducono i livelli, l’utente più ato (4) ottiene poi la variabile interna “userLevel”



?S_User_L0 ➔ Livello 1 ➔ Livello utente == <1>
 ?S_User_L1 ➔ Livello 2 ➔ Livello utente == <2>
 ?S_User_L2 ➔ Livello 3 ➔ Livello utente == <3>
 ?S_User_L3 ➔ Livello 4 ➔ Livello utente == <4>

6) Le macro “Logout” esistenti devono essere sostituite dal template “User Identification” nel WebEditor 8.

