

Instructions for connecting Saia PCD controllers to the internet



Document History

Version	Bearbeitung	Veröffentlichung	Bemerkungen
EN01	15.05.2013	15.05.2013	
EN03	26.07.2013	26.07.2013	Translation from Version DE03
EN04	14.02.2014	14.02.2014	New company Logo



Contents

1.	Introduction	3
2.	Building a virtual private network (VPN)	6
	2.1 Tested VPN Router	7
3.	Protecting the PCD.Web-Server	9
	Function of password mechanism	9
	3.1 Settings in PG5 Device Configurator	9
	Enabling the PCD.Web-Server password	10
	3.2 Entering the password in the web client	12
	3.2.1 Micro-Browser panel	12
	3.2.2 Micro Browser Windows CE and eXP	14
	3.2.3 iOS Micro-Browser app	15
	3.2.4 PC browser with Java applet	15
	3.2.5 SBC.Net Web Connect / WebFTP	16
	3.3 Compatibility PG5 and COSinus firmware versions	18
	3.3.1 Activating the SBC Web-Server password with the Device Configurator	19
	3.3.2 Activating the SBC Web-Server password with the Web Server project (.wsp)	19
4.	FTP server protection	21
5.	Ethernet S-Bus protection	23
6.	IP access filter (IP Access List, ACL)	25
	6.1 Device Configurator	25
	6.2 Fupla FBoxen	27
7.	Edit device templates in PG5 Device Configurator	28
8.	New user management with access control in WebEditor 8	29
	8.1 User database	29
	8.2 Download of user database and service key	30
	8.3 Assigning rights to functions or elements in WebEditor 8	32
	8.4 Templates for user control	33
	8.4.1 Login template	33
	8.4.2 Logout template	33
	8.4.3 Automatic logout during inactivity	34
	8.4.4 Change password	34
	8.5 Compatibility of new access control and old user identification	35



1. Introduction

The present document contains important information regarding protective measures that must be observed when connecting Saia PCD controllers to the internet. The most recent edition is available on our Support homepage: http://www.sbc-support.com/en/product-category/communication-protocols/pcd-on-internet.html

The first edition of the document was released early May 2013. That edition described the measures with the protection functions available at that time in the PCD COSinus operating system and the PG5 software tool. We have now adjusted our software tools so that the protection functions in the PCD controllers are activated by default. In addition, we have improved the password mechanism in the WebEditor. The IP filter function, implemented in the PCD controllers, is also new.

It must still be noted:

Safe operation of the PCD controllers on the internet can only be guaranteed with additional external IT components offering integrated protection functions such as VPN, firewall, proxy servers, etc.

To that end, we have evaluated several VPN routers and tested them with our PCD controllers. This document lists the devices successfully tested and their suppliers. A detailed description for configuration and initial operation is available in document 30-004 'VPN-Router' on our support site.

Saia PCD controllers can be connected to the internet in a variety of ways. The diagram below shows some frequently used connection options.





For smaller installations, a Saia PCD controller is in most cases connected to the internet with a DSL or 3G router. A PCD3.WAC is connected directly with the integrated GPRS modem. Saia PCD controllers that operate in a protected local company network are normally only accessible from the outside via a secure firewall and a virtual private network (VPN). In such cases, access protection is ensured by these components.

If the PCD controllers are operated behind an unprotected DSL or 3G router, the IP services are usually forwarded by means of port forwarding on the local PCD controller. **In these cases they can easily be attacked.**

Following is a brief overview of possible protection functions:

• Secure solution with Virtual Private Network (VPN)

A PCD controller should only be connected to the internet behind a router or a proxy server with firewall and a protected VPN. Chapter 2 includes devices that we have tested and recommended.

Web-Server password protection

Access to the PCD.Web-Server can be protected with a 4-level password mechanism. This involves simple unencrypted password protection. The passwords entered are verified in the controller. For the PG5 Device Configurator, the Web-Server is deactivated by default starting with Version 2.1.200. When it is activated, access can be protected with a password. A description of this is available in Chapter 3.

• FTP-Server access protection

Access to the FTP server and thereby to the data in the PCD.Filesystem can likewise be protected with a separate unencrypted password. For the PG5 Device Configurator, the FTP-Server is deactivated by default starting with Version 2.1.200. When it is activated, the standard user "root" and "rootpasswd" are no longer used. The programmer must set up his/her own user name to gain access. More information is available in Chapter 4.

• Ether-S-Bus access protection

The PG5 programming device uses the S-Bus protocol with extended services for programming and initial operation of PCD controllers.

In the PG5 Device Configurator from Version 2.1.200 and PCD COSinus Version > 1.22.10, the Ether-S-Bus communication is deactivated by default. The Ethernet interface therefore does not support S-Bus protocol (data exchange and programming). When it is activated, access with the PG5 programming device can be additionally protected with a simple, unencrypted password. More information is available in Chapter 5.

• IP access filter

Starting with COSinus Version 1.22.10, the PCD controllers feature an integrated IP access filter. Authorized and non-authorized IP addresses can be entered into a "white" or "black" list. More information is available in Chapter 6.

Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



• Password mechanism in WebEditor

The password mechanism included in the WebEditor and used by the Java applet and micro browser serves the user identification for role-based management in the HMI application. This mechanism was improved with the new COSinus version 1.22.10 and PG5 version 2.1.200. The password entered is now encrypted with a hash code. The password entered is verified in the controller. More information is available in Chapter 8.

Changing the default settings in the Device Configurator

The default setting can be modified and saved in a separate template. These default settings can thereby be transferred to a new CPU when it is created. More information is available in Chapter 7.

In order to use the protection functions outlined above in the way they are described, a PG5 Version 2.1.200 or higher is required. Some of the functions likewise require new PCD-COSinus Versions 1.22.10. Detailed information is available in the respective chapters.

The present document and the new PG5 and COSinus versions are available on the support page under the following link: <u>http://www.sbc-support.com/en/product-category/communication-protocols/pcd-on-internet.html</u>



2. Building a virtual private network (VPN)

A VPN tunnel offers a safe way of accessing devices in a private network by internet (WAN).

Basically, this kind of structure comprises a VPN server and a VPN client. We recommend the use of a router with VPN server functionality. The VPN client is usually installed as software on the client device (PC, tablet, smart-phone, etc.).

The VPN client (or VPN client software) logs on to the VPN server by internet. If login is successful, the device on which the VPN client was started finds itself inside the VPN server's intranet, having entered via a secure tunnel. From this moment, it can access all devices in the assigned address range of the VPN server and use all services.



When choosing a router, various points should be considered, depending on the application.

The router used should have VPN server functionality. For establishing VPN connections, routers use different protocols. The communications protocol must be supported by both the router and the VPN client device (PC, tablet, smartphone). It is therefore necessary to ensure that the appropriate VPN client software is available for the client device. IPSec is probably the most widely used technology and is supported directly by many devices. However, IPsec is quite complex to configure and use.

OpenVPN, which is available in an open source version, is easier to configure. It too uses the SSL encryption protocol and is therefore less problematic with firewalls. OpenVPN client software is available for many devices and operating systems.



2.1 Tested VPN Router

DrayTek Vigor 2850Vn Router



This router is intended for use in the home office segment and features a range of connection options (Ethernet, DSL, USB, WLAN, ...) and powerful functions (firewall, VPN, ...). It is well suited for establishing and managing VPN connections for smaller to medium-sized networks. Its functionality and user interface are easy to use. It supports standard VPN clients from Windows, I-OS and Android.

Туре:	Vigor 2850Vn
Suppliers:	Online suppliers, specialty retailers, distributors,
Internet:	http://www.draytek.de/produkte/modem-router/vigor2850-serie.html

eurogard Service Router V2



The EuroGard Service Router V2 is an industrial router for top-hat rail assembly with a 24 VDC power supply. It also features a variety of connection options (Ethernet, 3G) and lets users establish secure connections using OpenVPN or SSL. Configuration and user guidance for creating the VPN connection are quick and easy to follow. It has an OpenVPN server and requires OpenVPN clients accordingly.

Туре:	eurogard Service Router V2
Suppliers:	eurogard GmbH
	Kaiserstrasse 100
	D-52134 Herzogenrath
Internet:	http://www.eurogard.de



Vigor 2850Vn and EuroGard Service Router V2 technical data comparison

	DrayTek Vigor 2850Vn	EuroGard Service Router V2 (WLan)	EuroGard Service Router V2 (UMTS)
Order data	2850Vn	ER 1201-WLAN	ER 1201-UMTS
Additional	http://www.draytek.de/produkte/m	http://www.eurogard.de/	http://www.eurogard.de/
information	odem-router/vigor2850-serie.html	en/	en/
Application/ Type	Business/Home	Industrial	Industrial
Top-hat rail	No	Yes	Yes
Flectrical supply	230 \/AC	24.VDC	
VPN Features	230 VAC	24 000	24 VDC
Number of WAN interfaces	3: LAN/Modem/USB	1: LAN	2: LAN/UMTS
Integrated ADSL/VDSL modem	Yes	No	No
VPN PPTP	Yes	No	No
VPN L2TP/IPSec	Yes	No	No
openVPN	No	Yes	Yes
No. VPN clients	32 connections	30 connections	30 connections
Windows client	Yes (integrated in Windows)	Yes (EurogardSRConnect)	Yes (EurogardSRConnect)
IOS Client	Yes (IPSec/L2TP, integrated in IOS)	No*	No*
Android Client	Yes (IPSec/L2TP, integrated in Android)	No*	No*
Extensions			
3G/4G modem	Yes, with USB stick	No	Yes, with integrated UMTS modem

* IOS or Android systems can now be connected to the router via WLAN. This requires two routers. One VPN server and one VPN client. Support for VPN on mobile devices is in preparation.

Details on the configuration and use of the router for secure VPN connections with Saia PCD controllers are available in document 30-004.



3. Protecting the PCD.Web-Server

Access to the PCD.Web-Server can be protected with a password mechanism.

Function of password mechanism

With this password mechanism, general access to files and all PCD media (registers, flags, DBs/text, etc.) can be blocked. If the PCD web server is accessed via a browser device (PC browser, microbrowser panel, iPad,), the server checks whether the password stored in the PCD controller has been entered correctly. If no password has been entered, or if a directly transmitted password is invalid, a dialog box will be displayed on the browser device requesting password entry. Password comparison takes place in the web server of the PCD controller. This ensures that when a connection is established, defined passwords are not transferred during the check. The passwords entered are transmitted without encryption.

3.1 Settings in PG5 Device Configurator

The configuration settings of the Saia PCD controller are carried out in the PG5 Device Configurator. The settings for the Web-Server are located in the menus "IP Transfer Protocols" and "Device Type".

When creating a new CPU in the Device Configurator starting with PG5 2.1.200, the Web-Server is now deactivated by default.

		-		HTTP 1.0 Downgrade Enab	No
Ethernet Protocols				Chunk Mode Enabled	Yes
Section Description		Ξ	۵	HTTP Direct / First Liste	ner
				HTTP TCP/IP Port Enabled	No
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.			TCP Port Number	80
IP Protocols	DNS, SNTP, SNMP protocols.			+ Advanced Parameters	Hide
HTTP Portal	HTTP Portal Communication For P	c	۵	HTTP Direct / Second Lis	stener
				HTTP TCP/IP Port Enabled	No
				TCP Port Number	81
				+ Advanced Parameters	Hide

The Web-Server must be activated in the Device Configurator.

In addition, password protection is now activated with an activated Web-Server.

Type Description	Default Page start.htm	
PCD3.M5560 CPU with 1024 KBvtes BAM, 4 I/O slots (expand	Display Root Content Enabled Yes	
	Access Timeout [s] 60	
	Access Controls Form Page pwdform.htm	_
	Files Access Password	
	Read CGI Access Password	
	Read/Write CGI Access Password	

A password must be configured with this setting. Please find more information in the next section. In the event that a password is not to be configured, the parameter "Access Checks Enabled" must be deactivated.



Access Check Enabled:

Activates the password mechanism of the PCD.Web-Server

Default: "Yes" Recommended setting: "**Yes**"

Enabling the PCD.Web-Server password

The password will only be checked if the parameter "Access Checks Enabled" is set to "Yes".

Sala Device Configurator - (Device 1)		Web Server	
	L	Default Page	start.htm
Orevice Type Description PCD3M5560 CPU-web 1024 KBytes RAM, 4 (K) slots (expandeble), USB, Prof-S-Net, RS		Display Root Content Enabled	Yes
		+ Advanced Parameters	Show
Memory Skie Skit Description M1 M2		Access Checks Enabled	Yes
		Access Timeout [s]	60
	L	Access Controls Form Page	pwdform.htm
	L	Files Access Password	File Access
	L	Read CGI Access Password	Read CGI Access
		Read/Write CGI Access Password	Read/Write CGI Access
		Global Access Password	Global Access

Access Timeout

If communication with an S-Bus http connection is interrupted, querying of the password will be required again after a set time has elapsed. This parameter is only used with http via S-Bus.

Default: **"60s"** Recommended setting: "Do not change default"

Access Controls Form Page

In the case of access without a valid password, this password entry page is called.

Default: **"pwdform.htm**" Recommended setting: "Do not change default"

Note: this page is stored in the web server's system. If necessary, the programmer can also create his/her own login page.

Setting passwords for access protection

The PCD.Web-Server has 4 levels of access protection:

"File Access"	ightarrow Level 1
"Read CGI Access"	\rightarrow Level 2
"Read/Write CGI Access"	\rightarrow Level 3

"Global Access" → Level 4

In most cases, general protection of access to the PCD.Web-Server is sufficient. For this purpose, a **level 1 password (file access)** must be defined. We recommend that this password should always be defined! For all other passwords, definition is not required. After a successful login, all levels 1-4 are automatically unlocked.

Internet Security Instructions | Documentation 30/002 ; Edition EN04 | 2014-02-14



If despite this it should ever be necessary to use a password login to differentiate between read and write permissions, the following rules apply:

- If no password has been defined at any level, there is no active protection and the user has full access to all functions without entering a password.
- A defined password activates access protection from this level. Example: only one password has been defined for level 1. → In this case, the web server is protected for all access and password entry will be requested. After password entry, all higher levels (levels 2 to 4) will also be unlocked, as long as they are not themselves password protected.
- A defined password unlocks access to its own level and all higher ones, or as far as the next one up that has password protection. Example: password defined for level 1 and password defined for level 3. → In this case, entry of the level 1 password also unlocks level 2. Entry of the level 3 password unlocks levels 1 to 4.

File Access Password:

This password protects or unlocks read access to files and all levels above.

Default: "" Recommended setting: "**define password**"

 \rightarrow Always define. This provides the web server with full protection.

Caution: the password dialog box is only displayed generally (for all levels) if a password has been defined for that level.

Read CGI Access Password:

This password protects or unlocks read access to the CGI interface and all levels above it. The CGI interface is protected for reading PCD media (registers, DBs, flags, text, ...).

Default: "" Recommended setting: ""

If a user is only required to have read access (e.g. to read log data or display system states), it is sufficient to define a password for level 1 (**File Access)** and level 3 (**Read/Write CGI Access)**.

Read/Write CGI Access Password:

This password protects write access to the CGI interface and all levels above it. The CGI interface is protected for writing PCD media (registers, DBs, flags, text, ...).

Default: "" Recommended setting: "only define a write protection password if necessary"

If a user is required to have write access only after password entry, a password must be defined here.

Global Access Password:

This password remains available for historical reasons. Definition is not necessary.

Internet Security Instructions | Documentation 30/002 ; Edition EN04 | 2014-02-14

Saia-Burgess Controls AG Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



Default: "" Recommended setting: "not necessary"

Rules for selecting a password:

The password may be up to 31 characters long and must not include special characters, umlauts, or spaces. No distinction is made between uppercase and lowercase letters.

To obtain the best possible protection, we recommend choosing at least 10 characters (the longer the more secure) comprising both letters and numbers. Words that are easy to guess must not be used (e.g. the system name).

3.2 Entering the password in the web client

3.2.1 Micro-Browser panel

PCD.Web-Server password protection is supported by Micro-Browser panels from version **1.20.3x**.

From this version, passwords can be stored in the setup menu of the Micro-Browser panel. See below for password configuration instructions.

If there is no stored password, the message: "**PCD Password required!**" will be displayed on the screen of the panel while a connection is being established. For a successful connection, the presence of a stored password in the Setup menu is mandatory.

Step 1) Open Setup menu

The Setup menu can be opened either during device start-up or by prolonged pressing (10 sec) on a blank area in the application.

Step 2) Edit Start-up Web Connection

- → Setup menu → Web Connection → Remote login
- ➔ Remote Password
 - The password for access to the web server must be entered here.
 - It is possible to set this password as a default password. In this case, this password will always be used if a password is requested from the web server during a connection. If a password is defined for a station on the Connection List, this will be used first. If it is not possible to establish a successful web server login with the password stored in the station, the default password defined for the start-up connection will be used for another login attempt.

Saia-Burgess Controls AG

Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



\triangleleft	Back to application	Setup		Setup	Sta	rtup Connection	
9	Network		>	Cor	nection	22	>
\bowtie	Web Connection		۶	Тур	e	HttpDirect	>
	System		>	Star	rt Page	Basic.html	۶
9	Display		>	Ren	note host IP	172.23.5.22	۵
\bigcirc	Keyboard		>	Ren	note port	80	>
	Password		>	Ren	note login		۵
-	Language		>				
				Cor	nnection List		>
<	Startup Connection	Remote login					
	Remote password	******		5	>		
	Default password			ť	•		

Step 3) Edit Connection List

If a single Micro-Browser panel is to be used for accessing multiple controllers with different passwords, a connection must be created in the Connection List for each controller, with the appropriate password.

	Startup Connection	
Connection	22	>
Туре	HttpDirect	>
Start Page	Basic.html	>
Remote host I	IP 172.23.5.22	>
Remote port	80	>
Remote login		>
Connection Li	ist	>

Saia-Burgess Controls AG

Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



Connection List Edit	Connection	
Connection Name	test.myhmi.ch	۵
Start Page	Basic.html	>
Remote host IP	test.myhmi.ch	>
Remote port	80	>
Remote password	84848A	>

3.2.2 Micro Browser Windows CE and eXP

Micro-Browsers for Windows-based devices support the web server password login from version 1.5.15.131c.

In a PCD controller with an activated web server password, users must first log on for web server access and then, in the WebEditor application, identify themselves again for user prompting.



Web-Server login

WebEditor application login





3.2.3 iOS Micro-Browser app

The Micro-Browser app for Apple devices supports web server password login from version 1.5.15.130



3.2.4 PC browser with Java applet

PC browsers with a Java applet support the SBC Web-Server password mechanism. When accessing a password-protected SBC Web-Server, the file "pwdform.htm", which is defined in the Device Configurator, is loaded automatically. This lets you send the password entered to the SBC Web-Server. If entry is correct, the "start.htm" defined in the Device Configurator is loaded and starts visualization.

NOTE: If a web application is to be loaded directly, the HTML page of the WebEditor project must be entered in the Device Configurator.

Tip: The PCD Web-Server's status page can be displayed at any time in the PC browser by typing "status.htm".





3.2.5 SBC.Net Web Connect / WebFTP

SBC.Net already has its own integrated account management, which is available via the web interface SBC.Net.

	<u>⊂</u> onfigure
Web-Connect Settings Help Show All Stations Import :	Help About
Conn	on T Shutdown

Account Management is located in the SBC.Net settings. Users and passwords can be defined here, together with the relevant rights for selected users.

A password must be defined for the "admin" user, otherwise all stations will be fully accessible.

- 1) Add a new user. Each user needs a user name and associated password.
- 2) List of users currently in existence. A user may be edited or deleted.
- 3) Rights of the currently selected user. Rights will change, depending on the functions enabled in SBC.Net
- 4) Select WebConnect or Web FTP functions
- 5) Apply changes to selected user.

+Add user 1 <pre></pre>	Account Manager					
Admin X user1 Specify the stations and/or groups which are accessible by the selected user. This user has access to all stations Test Test Test3 Info! The group name '[No Group]' allows access to PCDs which are not in a group.	+Add user	WebConnect Web FTP 4	access to all stations	if there is no 'admin' password	l set.	
Test Image: Constraint of the second sec	✓ admin → ✓ × User1 2 →	Specify the stations and/or group	os which are accessil]] This user has acc	ole by the selected user. ess to all stations		
Test X Test3 X Info! The group name '[No Group]' allows access to PCDs which are not in a group.		Test	- +	[No Group]	• +	
Test3 X Info! The group name '[No Group]' allows access to PCDs which are not in a group.		Test	×	[No Group]	×	
		Test3	×	Info! The group name '[No access to PCDs which are	Group]' allows e not in a group.	
	5					
5						

The Web FTP tab allows user rights to be defined for the local Web FTP server of SBC.Net

Saia-Burgess Controls AG



Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>

- 1) Add a new directory for the currently selected user
- 2) Location of local directory to be unlocked via Web FTP.

The user has the following rights:

- 3) Browse: View current contents of directory
- 4) Push: Write to files in the directory
- 5) Get: Read from files in the directory
- 6) Del: Delete files in the directory
- 7) MkDir: Make subdirectories
- 8) RemDir: Rename existing directories
- 9) Recursive: Include all subdirectories in the currently defined chain of rights.

VebConnect Web 1 11								
Warning! Everyone will ha	we full access if there is no	o 'admin' p	assword	l set.				
pecify the access privileges	for the selected user. You This user has full a	i can spec iccess	ify the u	iser righ	ts on direc	tories.		
+ 1	Privileae	95						
+ 1 Directory	Privilege Browse	es Push	Get	Del	MkDir	RemDir	- Recursive	
+ 1 Directory C:\Temp 2	Privilege Browse	es Push ☑	Get	Del	MkDir 🔽	RemDir	Recursive	×

On opening SBC.Net WebConnect, you are asked to enter a user name and password. After this login, you will have the rights of the logged in user. Clicking on any of the stations that are available to this user will allow access to the SBC Web-Server.

		Stations	PCD Web-Server Login	
		[No Group]		
		DemoVK		_
		Develop	Saia PCD Web-Server X	
		EMSolar	← → C 🗋 168.152.35.67/ogin.cg 😭	=
Authentication Required		KundeErnst	Web-Server	
The server http://localhost:81 requires a username and password. The server says: Setup Area.		Local	Start Login Varlists Status Program	
		Password	Into history	Í
User Name:		PCD1Solar		ŀ
Password:		PCD3M5560		
		PCD7D450	PCD3.M5560	
Login Cancel		w2canteenem6	FW Version: 1.20.25	
	Sala.Net - Version 2.1.14.0	xx7		



3.3 Compatibility PG5 and COSinus firmware versions

The protection functions described have been supported by Saia PCD controllers for quite some time. To use them correctly, the functions must also be supported by browser devices and the PG5 Device Configurator.

The following versions of Micro-Browser devices support the Web-Server password mechanism:

Product	Product type	Firmware from version	Notes
	PCD7.D4xxWTPF	1.20.36	
VGA and SVGA	PCD7.D457VTCF	1.20.36	
Micro-Browser	PCD7.D410VTCF	1.20.36	
Web-Panel	PCD7.D412VTPF	1.20.36	
	PCD7.D4xxVT5F	1.20.25	
Product	Product type	Firmware version	Notes
OVCA Miero Browcor	PCD7.D457BTCF	Not supported	
QVGA MICro-Browser	PCD7.D457STCF	Not supported	
Failei	PCD7.D457SMCF	Not supported	
Product	Product type	Firmware from version	Notes
	PCD7.D51xxTX010	1.5.15.131c	
eWinCE Micro-Browser	PCD7.D51xxTL010	1.5.15.131c	
	PCD7.D51xxTA010	1.5.15.131c	
	PCD7.D61xxTL010	1.5.15.131	
ewinter witcid-blowser	PCD7.D61xxTA010	1.5.15.131	
Product	Product type	Firmware version	Notes
iOS MB App		1.5.15.130	
iOS MB LITE App		1.5.15.130	
Android MB App		Not yet supported	New version will be available soon

The following table shows interdependencies concerning the web server configuration in PG5 and COSinus firmware version of PCD controllers.

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

*With PG52.x Firmware Version < 1.14.nn must be set in the Device Configurator.

For activation of the web server password, **no** update of the PG5 programming tool is necessary.

For firmware versions below 1.14.nn, the password and web server settings must be defined with the web server project (.wsp).

Firmware versions in the range 1.14.nn to 1.16.nn support configuration both via web server project and via the Device Configurator.

From firmware version 1.20.nn, web server settings can only be modified via the Device Configurator.



3.3.1 Activating the SBC Web-Server password with the Device Configurator

Web server configuration is defined in the Device Configurator. Settings are located on the CPU tab.

UserPasswordDialog_V01 [Device1] - Project Mana		
<u>File Edit View Project Device Online Tools Help</u>		
n 🚅 🕼 🕼 🚟 📥 🖌 🐖 🌐 🦌		
- : 🛃 🕼 I 😋 🔲 🙀 🧩 🙀		
Project Tree		
Fell Project 'LicerPasswordDialog V01' + 1 Device		
Properties		
Common Files		
Library Manager		
Device1 - PCD3.M5560 - 168.152.35.67. 5-Bus Stn 4		
Properties		
Build Options		
🖃 💼 Program Files		
.\WEB\UserWe5.prj		
Main.fup		
Server.wsp		
E - Eisting Files		
由 Listing Files ⊡ Documentation Files		
⊕-		
Listing Files Documentation Files		
	Properties	
Listing Files Documentation Files Device Configurator - [Device1 *] Ele Edt View Online Icols Window Help Set 1 ■ Set 2 ■ Construction Files Set 2 ■ Se	Properties	
Listing Files Documentation Files Device Configurator - [Device1 *] Ele Edt View Online Icols Window Help Device Device	Properties Device : PED3:MS560	
	Properties Device : PED3.M5560 Device : PED3.M5560 Default Page	start.htm
Isting Files Isting Files Image: Documentation Files Device Configurator - [Device1 *] File Edt Yew Onine Image: I	Properties Device : PCD3/MSS60 Web Server Default Page Display Root Content Enabled	start.htm Yes
Listing Files Documentation Files Device Configurator - [Device1 *] File Edit View Qnine Look Window Help File Time Description FOO3 M5560 CPU with 1024 KBytes RAM, 4 I/O slots (expandable), USB, Profi-S-Net, RS-232, Ethernet Memory Slots Stot	Properties Device : PED3.MS560 Web Server Default Page Display Root Content Enabled + Advanced Parameters	start.htm Yes Show
Listing Files Documentation Files Device Configurator - [Device1 *] File Edit View Online Tools Window Help File Edit View Online Tool		start.htm Yes Show Yes
Listing Files Documentation Files Device Configurator - [Device1*] File Edt View Online Icols Window Help File Edt View Online Icols Window Help File Edt View Online Icols Window Help Pevice Device Type Description PCD3.M5560 CPU with 1024 KBytes RAM, 4 I/O slots (expandable), USB, Profi-S-Net, RS-232, Ethernet Kernory Slots Slot Type Description M1	Properties Device : PED3.MS560 E Web Server Default Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Controls Form Page	start.htm Yes Show Yes 60 pwdform.htm
Listing Files Documentation Files Device Configurator - [Device1 *] Ele Edt Yew One Origon Image: Solution in the image in	Properties Device : PED3.M5560 Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Cherchs Form Page Files Access Controls Form Page Files Access Password	start.htm Yes Show Yes 60 pwdform.htm
Listing Files Documentation Files Device Configurator - [Device1 *] Ele Edt View Online Tools Window Help Ele Edt View Online Tools Window Help Elevice Type Description PCD3 M5560 CPU with 1024 KBytes RAM, 4 I/O slots (expandable), USB, Profi-S-Net, RS-232, Ethernet Aemory Slots Slot Type Description M1 M1	Properties Device : PED3.MSS60 Web Server Defail: Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Checks Enabled Access Checks Fambled Access Controls Form Page Files Access Password Read CGI Access Password	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS
Listing Files Documentation Files Device Configurator - [Device1 *] File Edt View Qnine Iools Window Help File Edt View Qnin	Properties Device : PCD3.MSS60 Web Server Default Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Timeout [s] Access Controls Form Page Files Access Password Read (Cdi Access Password Read/Write CGI Access Password	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS
Listing Files Documentation Files Device Configurator - [Device1 *] File Edit View Online Tools Window Help Pile Edit View Online Tool	Properties Device : PED3M5560 Veb Server Default Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Controls Form Page Files Access Password Read CGI Access Password Read/Write CGI Access Password Global Access Password	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS GLOBALACCESS
Listing Files Documentation Files Ele Edt View Online Tools Window Help File Edt View Onl	Properties Device : PED3.M5560 Web Server Default Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Controls Form Page Files Access Password Read (Vinite CGI Access Password Global Access Password Global Access Password Current Available V+ [mA]	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS GLOBALACCESS
Listing Files Documentation Files Device Configurator - [Device1 *] File Edt View Online Icols Window Help Perice Type Description PCD3.M5560 CPU with 1024 KBytes RAM, 4 I/O slots (expandable), USB, Profi-S-Net, RS-232, Ethernet Memory Slots Slot Type Description M1	Properties Device : FED3.MS560 E Web Server Default Page Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Controls Form Page Files Access Password Read (Sit Access Password Read/Write CGI Access Password Global Access Password Current Available V+ [nA] Current available at V+ (24V) for I/O c	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS GLOBALACCESS ards (in mA).
Listing Files Documentation Files Device Configurator - [Device1 *] Ele Edit View Online Tools Window Help Ele Edit View Online Tools Monitoring Monitoring and logging of meter data. Automatical scanning of S-Bus meters and gateways. Onboard Communications Type Description	Properties Device : PED3.MSS60 Display Root Content Enabled + Advanced Parameters Access Checks Enabled Access Timeout [5] Access Controls Form Page Files Access Password Read/Write CGI Access Password Read/Write CGI Access Password Current Available Y + [mA] Current available at V + (24V) for I/O c	start.htm Yes Show Yes 60 pwdform.htm READCGIACCESS GLOBALACCESS ards (in mA).

3.3.2 Activating the SBC Web-Server password with the Web Server project (.wsp)

Web server configuration is defined by the web server project. This is included among the program files and loaded into the controller with the program download.

Saia-Burgess Controls AG



Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



In the Web-Server project (.wsp), files may be loaded and passwords set for 4 levels.

Level 1: File Access Password: Level 2: Read CGI Access Password: Level 3: Read/Write CGI Access Password: Level 4: Global Access Password:



In WebEditor 8 the following settings in the project setting will be made

B General	Build
Man Sattings Project Configuration Duild Duild Puntime Sommonad (Web) Web View Editor Crid Data User Groups	Germand Advanced Options: Web-builder Image: Server data file to in include in PLC program Use this cyclicit to ended the WebEldbur project into the PLC program and configure the PCD's web server (non- SBC_PCDs). For mewer PCD's web internal or external lists use the download option. NUTE: If endedd, you have to add and the File Sweb_serve_data.arC to the PGD device. Web Server Access advanced Level & Password:
	Files to Include If Units and Variable-Definition IF If this and Variable-Definition IF Web Mews IF Sphares IF Longuages IF Jewa Burbles Units Definition IF Bes matchings Include Definition



4. FTP server protection

		۵	FTP Server	
Ethernet Protocols			FTP Server Enabled	No
			TCP Port Number	21
Section	Description		User Name 1	
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.		User Name 2	
IP Protocols	Protocols DNS_SNTP_SNMP protocols		+ Advanced Parameters	Show
			Connection Timeout [s]	300
HITPPortal	HTTP Portal HTTP Portal Communication For P		Maximum FTP Connections	3
			Remove Default Liser	Vec

When creating a new CPU in the Device Configurator starting with PG5 2.1.200, the FTP-Server is now deactivated by default. The default user "root", "rootpasswd" is now likewise deactivated. For security reasons, the FTP-Server should be activated and a new user created when necessary. FTP Server parameters are stored under the Ethernet Protocols tab.

At the same time, the user's individual password should also be defined with a length of up to 20 characters overall.

Ethernet Protocols		E FTP Server
Section	Description	FTP Server Yes
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.	TCP Port Ni 21
IP Protocols	DNS, SNTP, SNMP protocols.	User Name
HTTP Portal	HTTP Portal Communication For PCD Over Private	Network. + Advance: Show
	FTP Server User Name and Access Rights	
	User Name :	Remove De Yes
	SBC_Support	
	Password :	
	Support	
	User's Groups	
	C Group 1 C Group 2	
	C Group 3 C Group 4	
	 WEB Group 	
	Access To Files Created By Other Groups	
	I Group 1 I Group 2	
	Group 3 Group 4	
	WEB Group	
	Access Rights	
	© Read/Write C Read Only	
		ancel

Rules for selecting a password:

To obtain the best possible protection, we recommend choosing at least 10 characters (the longer the more secure) comprising letters, numbers and special characters. Easy-to-guess words, such as the system name, should not be used.



FTP Server (Yes/No)

Activation or deactivation of the FTP server

Default: "No" Recommended setting: "No" for critical systems

If the FTP-Server is needed, it must be activated and a new user with password created.

Remove Default User

The default user is now deactivated in order to block unauthorized access via known and publicly communicated passwords. At least 1 new user should be created in order to access the FTP-Server.

Default: "Yes" Recommended setting: "Yes"

User Name

Allows the creation of up to 10 individual users with group membership and read or write access rights. Each user can be assigned to a group. In addition, it is possible to allow the user the access rights of other groups. An "administrator" or "root user" should be defined with an access authorization to all groups with "Read/Write" rights.

TCP Port Number

Port 21 is defined as the default port for FTP communication. The FTP server's port number can be changed with this parameter.

Default: "21" Recommended setting: "only change if necessary"

Connection Timeout (s)

If a connection has been established to the FTP server but is not being used to exchange data with the server, after the specified timeout period the existing connection will be closed by the FTP server. To ensure that the FTP connection will be closed by the server, even if the client does not terminate it properly, a default value of 5 minutes (300 seconds) is recommended.

Default: "300" Recommended setting: "300"

Maximum FTP Connections

Defines the maximum number of parallel connections to the FTP server

Default: "3" Recommended setting: "only change if necessary"



5. Ethernet S-Bus protection

Ether-S-Bus supports all services and functions for data exchange, programming, commissioning and service of Saia PCD controllers. Access is with the PG5 programming tool, a Scada system or OPC server (only for data exchange).

Ether-S-Bus access rights can be defined in the PG5 Device Configurator.

One change is in the PG5 Device Configurator from Version 2.1.200 and a PCD COSinus Version > 1.22.10, where Ether-S-Bus communication is now deactivated by default. It should be noted, that the S-Bus communication can be used neither with the PG5 programming tool nor with any other system (Scada, OPC server).

Onboard Com	munications				
Туре	Description	۵	Ether-S-Bus Chappel Number	9	
RS-485/S-Net	RS-485 port for Profi-S-Bus or gener		Ether-S-Bus Enabled	No	٦
USB	Universal Serial Bus port, PGU or g		IP Node	0	
RS-232/PGU	RS-232, PGU or general-purpose s		PGU Port	Yes	
RS-485	RS-485 port for general-purpose co		Slave	Yes	
Ethernet	Ethernet port. IP Settings, DHCP.		Network Groups	(Default)	

When Ether-S-Bus is activated, access with the PG5 programming device can be additionally protected with a password.

Device				
Туре	Description		Password	
PCD3.M6860	CPU with 1024 KBytes RAM, 4 I/U si	DIS	Password Enabled	Yes
			Password	*Hototote
			Inactivity Timeout [minu	J 1

The following rules apply:

If the password is disabled, all services on all PGU interfaces (Ethernet, USB, serial) are supported without restriction.

The password defined can have a total length of 25 characters and must consist of uppercase letters (A, B, C) or numbers (0-9).

For good protection, we recommend the selection of at least 10 characters (the longer the more secure), comprising letters and numbers. Easy-to-guess words, such as the system name, should not be used.

Caution: if the password is lost, the controller must be reset with the reset function.



If a password has been defined, a password must be entered for all PGU interfaces (Ethernet, USB, serial) when establishing a connection with the PG5 programming tool. The following login dialog appears:

Ele Onvice1 - Salia I Ele Online Tools	Online Debiog Optogs Help			[Device1] - Saia Online Co	nfigurator	_ 🗆 🗙
Stn:	Type:	Status:		Password Protection Acti	ieep	×
	Password Protection Active For full access to the PCD, enter the o For reduced access to Registers, Cou Dutputs and the Diock only, press "Co Password Help	Unerit password and press "DK". https://mass. https://mass. DK Cancel		For full access to the PCD For reduced access to Re Outputs and the Clock on Password:	I, enter the current password and pr sgisters, Counters, Timers, Flags, Ing ly, press "Cancel".	ress "OK".
COMMUNICATIO	HS: SOCKET: TCP/IP, 168.152.	35.67, Stn Auto	2	Help Bun	Stop Restart	Exit

Note: Access (read and write) to the PCD media (R, F, I/O, T/C) is always enabled with Ether-S-Bus (even with a configured password).



6. IP access filter (IP Access List, ACL)

Starting with COSinus Version 1.22.10 and PG5 2.1.200, PCD controllers support the IP access filter. Authorized and non-authorized IP addresses are entered into a "white" or "black" list.

- Access and telegrams from IP addresses belonging to the White list are identified and handled by the COSinus operating system. Telegrams from other IP addresses are rejected.
- Access and telegrams from IP addresses belonging to the Black list are identified and rejected by the COSinus operating system. Telegrams from other IP addresses are handled.



In a local network, it can be practical and necessary to protect access to a controller with the IP access filter.

6.1 Device Configurator

The White list or Black list are defined in the PG5 Device Configurator in the "Onboard Communications" – "Onboard Ethernet" section.

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

In order for the properties of the IP filter to be edited, the parameters in "+ Access Control List" must be set to "Show".

- 1) "IP Filtering Enabled"
 - Turn the IP access filter on or off

Saia-Burgess Controls AG

Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



2) "IP Filter Policy"

Set the filter mode

White list = block everything \rightarrow only allow those addresses on the list Black list = block everything \rightarrow only block those addresses on the list

3) "IP Filtering List"

List of IP address and associated "mask", which is either handled or rejected by the COSinus operating system depending on the mode selected.

No	IP Address	Mask	Description	_
0	192.168.10.1	255.255.255.0	Sub-Net 1	=
1	192.168.11.1	255.255.255.255	Sub-Net 2	
2	0.0.0.0	255.255.255.255		_
3	0.0.0.0	255.255.255.255		
4	0.0.0.0	255.255.255.255		
5	0.0.0.0	255.255.255.255		
6	0.0.0.0	255.255.255.255		
7	0.0.0.0	255.255.255.255		
8	0.0.0.0	255.255.255.255		
9	0000	255 255 255 255		
•		1		•

The mask can also be used to define entire subnetworks for the filter. The IP address and mask define the network or subnetwork address.

For example,

The IP address 192.168.10.1 with a defined mask of 255.255.255.0 allows or blocks communication of all devices in the network 192.168.10.0/24 (255 addresses) The IP address 192.168.11.1 with a defined mask of 255.255.255.255 allows or blocks communication exclusively from this IP address.

The list can	be exported	or imported	as a .csv file.
The list curr	se exported	or imported	us u .csv me.

92.168.11	.1	255.255.255.250	Sub-Net 2
0.0.0	Î	Import	
0.0.0		Export	
0.0.0			
0.0.0	2	Check Table	
000		255 255 255 255	



6.2 Fupla FBoxen

The IP access filter can be managed from the PCD user program by means of FBoxen.

1) ACL IP Filter FBox

Allows the IP filter to be turned on and off



2) ACL IP Open FBox

Allows an IP address to be opened for access to the device. This FBox can be used, for instance, to temporarily open an IP address for a mail server so the controller can send a mail. Up to 32 IP addresses (32 FBoxes) can thereby be added to the White list.



More information is available in the FBox online help.



7. Edit device templates in PG5 Device Configurator

In order for you to consistently configure a CPU with the same settings, it is possible to define a configured device template as a default for use with all of the same CPU types.

All settings that are defined in the Device Configurator template are thereby transferred to the new CPU when it is created.

Saia Device Configurator - [Device1]				
😥 Datei Bearbeiten Ansicht Online Werkzeu	g <u>F</u> enster <u>H</u> ilfe			
E 🗅 🚅 🐟 🔲 🗗 🗶 🖻 😤 💆 Mod	emliste			
	tten Editor	_		
Steuerung 1 Als D	Tefault Steuerung speichern		Eigenschaften	
Tun Resolvail		- 1	Steuerung : PCD1.M0160E0	
PCD1 M0160E0 Steuerung mit 1 MBvtec Pro	uran Ingram (Toxt/DB Flach Spoicher und 1 MBster Enveiterungsspoicher (DAM für Text/	.	Standardseite	start.htm
	igranių rexpositilasin speicner ana rimovies Limenerangsspeicner (PAImilai rexp	-	Erlauben, den Inhalt des Hauptverzeichnis z	u sehe Ja
Speicher Slots		- 11	+ Erweiterte Parameter	Angezeigt
		- 1	Zugangskontrolle aktiviert	Nein
Project Tree	Project Tree		Zugriffkontrolle Timeout [s]	60
PterPasswordDialog_V01' + 1 Device	E 20 Device1 - PCD1.M0160E0 - S-Bus Sto 0		Zugriffskontrollseite	pwdform.htm
New Device	Pronerties		Passwort für Dateizugriff	niS8vPm7SGI6MWv
R At Import Device	Contract Con		Passwort für CGI-Lesezugriff	N279017nNR j0Q84
Common File Paste Device Ctrl+V	E Device Configurator	- 1	Passwort für CGI-Lese-/Schreibzugriff	KB2mBdYibNyTp7w
Library Mana	- In Build Options	- 11	Passwort für globalen Zugriff	R94L77i2iI1WP01
E Device1 - P Copy Project	αys.		Webserver Ressourcen	
Propertie Backup	.\WEB\UserWe5.prj	- 11	Taskzeitlimitierung	5
Coline Se Restore	.\WebEditor8\UserWe8.sln		RAM Disk Grösse	72
Device C	- 🔛 Main.fup		🖂 Webserver über S-Bus	
Build Opt Rebuild All Programs	Server.wsp		Web S-Bus aktiviert	Ja
Program Online Commands	🗄 🧰 Listing Files			-
Print Ctrl	E Documentation Files		RAM Disk Grösse	
	E 🛃 Device2 - PCD1.M0160E0 - S-Bus Stn 0		Grösse der Webserver RAM Disk in [KByte]. De	efiniert die Cache Grösse des Web
Han Eind Ctrl+	Properties			
Properties Alt+Enter	- Kg: Unine Settings		Elements Grad Martin Marcine	
		•	Eigenscharten Media Mapping	
	Dispersion Files			
	E Contraction Files			
	Light countries			

- 1) Make the current settings in the CPU Device Configurator the default settings for this CPU type.
- 2) Add a new device
- 3) The new device is created with the device configuration defined in point 1.

Make a one-time definition of your active CPU components, such as the Web server and FTP server, as well as your security levels, ServiceKey or authorized users; save these settings for this CPU type.



8. New user management with access control in WebEditor 8

Beginning with COSinus Version 1.22.10 and PG5 V2.1.200, there is a new user management and access control available in WebEditor 8. The templates for the new mechanism are listed in the WebEditor 8 template library in the section "Access Control". The templates are only usable in connection with the user database generated by WebEditor 8. The new access control replaces the previous "User Identification" (old password mechanism) in which only 4 user levels could be defined.

The access control allows a user to be organized into 16 groups. These groups do not form levels. If a user is a member of a group, he/she can access or use the elements and functions of this group.

8.1 User database

WebEditor 8 was enhanced to include a user management system. Up to 100 users can be defined in the user database. A user consists of a user name, password, home page and language. In addition, every user is assigned to different user groups.

🛞 TempTest - Users* - WebEditor								
Elle Edit View Broject Build Iools Window Help								
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □								
Solution _ ×	Logout.wev × - Ho	ome.wev × 🛄 Start.wev × 🛄	MACRO.wev × - ChangeUserTemplate.u	wev × LUsers* ×				
🗉 🔝 Solution UserWe8					Constant and the			
🗄 🛅 S_Demo	Users				Group Membership			
🗆 🖃 TempTest	Name	Password	Initial View	Language	Group 1 🔽 Group 2			
L Users	Service	PCD7D450WTPF	ChangeUserTemplate	default.csv				
🗄 🛄 Media	Service_1	PCD7D450WTPF	ChangeUserTemplate	default.csv	🖌 Group 3 🖌 Group 4			
🛁 ChangeUserTemplate.wev					🗍 Group 5 🔲 Group 6			
🐴 default.csv								
- Home.wev					Group /Group 8			
Logout.wev					🔲 Group 9 🔲 Group 10			
MACRO.wev					Group 11 Group 12			
- MsgBox.wev					j Group II j Group Iz			
Start.wev					🔲 Group 13 🔲 Group 14			
 TempTest.wvar 					Group 15 Group 16			
🗄 🛅 UserWe8								

The user database is saved in a secure area of the controller.



8.2 Download of user database and service key

In order for WebEditor 8 to be able to load the user database in the protected area of the PCD controller, the service key must be defined in the Device Configurator.

The service key is used by the WebEditor 8 to identify itself to the controller (FTP-Server). The service key is entered in the Device area of the PG5 Device Configurator.

Properties	
Device : PCD3.M5560	
🗆 Firmware	
Firmware Version	From 1.22.00 or more recent and compatible
🗄 Memory	
User Code/Text/DB Memory	2 MBytes ROM
Extension Text/DB Memory	1 MBytes RAM
User Code/Text/DB Memory Backup (Flash)	On File System
User File System Size (Flash)	128 MBytes
Program Directory	Onboard Flash
3 Options	
Reset Output Enable	Yes
XOB 1 Enabled	No
Run/Stop Switch Enable	Yes
Time Zone Code	

For downloading the user database in WebEditor 8, a download target "WebFTP", "FTP Server (PCD)" or "PG5 CPU (S-Bus)" must be used with the service key. The service key entered here must be the same one entered for the PG5 Device Configurator.

Project Options - TempTest		×
General	S Download (Web)	
Project Configuration	FTP Server (PCD) ×	
Build	Destination Type FTP Server (PCD)	
🔩 Download (Web)	Host name 168.152.35.69	
Web View Editor Orid	Use Service Key MyServiceKey1213	
Data User Groups	Degtination Internal Flash	
	Files to Include	
	✓ HTML and Variable Definition ✓ Web Views	
	✓ Pictures ✓ Languages	
	🔽 Java Runtime 🔽 User Database	
	Elles matching:	
	Download Options	
	Clean Destination 🔽 Update if Possible	
	Add Target	:
	<u>O</u> K <u>C</u> ancel	

Saia-Burgess Controls AG

Bahnhofstrasse 18 I CH-3280 Murten I Switzerland T +41 26 672 72 72 I F +41 26 672 74 99 I <u>www.saia-pcd.com</u>



WebEditor

peration successfully completed.	
	⊡ose
Details	
Downloading file '\$CI_1r4jfp7.gif'	▲
Downloading file '\$CI_1d58qed.gif'	
Downloading file '\$CI_u1pk8q.gif'	
Downloading file '\$CI_pquxxw.gif'	
Downloading file MACRO.teq	
Downloading file \$CI_10020q2.gir Downloading file \$CI_1cae.v0m gif	
Downloading file \$CL_1157uc3_cif	
Downloading file "Changel KerTemplate teg"	
Downloading file (\$CT, smzux8, gif)	
Downloading file 'Logout.teg'	
Downloading file 'default.csv'	
Downloading file '\$CIV_168dtzd.itg'	
Downloading file '\$CPV 168dtzd.tcr'	
Downloading file 'IMasterSaia5 15 02.jar'	
Downloading file 'start.htm'	
Downloading file 'start.html'	
Downloading User Database	



8.3 Assigning rights to functions or elements in WebEditor 8

Every element of WebEditor 8, including buttons, editing boxes, groups or layers, can be assigned to one or more user groups. User rights are entered in the application when a user logs on. The registered user can thereby use the functions and elements corresponding to his/her group assignment. If the box "Hide if not accessible" is activated, the element and its associated functions are deactivated and hidden for users who are not defined in the group.

Properties of Button: 'L	.ogout\Ma	in Layer\Button'	_ ×
General Actions	Access	Other	
Access limited	to _		
		Group 1	🔲 Group 9
		🔲 Group 2	🔲 Group 10
Button		Group 3	🔲 Group 11
Dation		🔲 Group 4	🔲 Group 12
		🔲 Group 5	🔲 Group 13
		🔲 Group 6	🔲 Group 14
		🔲 Group 7	🔲 Group 15
		🔲 Group 8	🔲 Group 16
Hide if not acce	ssible	V	



8.4 Templates for user control

The templates for user control can only be used in connection with the new user management.

8.4.1 Login template

At login, the controller verifies the user name and password with the user database. The password is transmitted with hash code encryption. If the user name and password are correct, the user (or the HMI application) is given the relevant rights with a group assignment, language and home page.

Log	in			
2	Dai	niel		

Login	Daniel		<u>a</u>	
		←	After a	a successful login

8.4.2 Logout template

If a user logged in via the login template, internal variables are set with the respective group, language and home page. The logout button resets these variables and changes the page to the logout view indicated in the template.





8.4.3 Automatic logout during inactivity

If a user logged in via the login template, internal variables are set with the respective group, language and home page. The "Logout on Timeout" template resets these variables after a specified period of time and changes the page to the logout view indicated in the template. The timeout value can be defined in seconds in the template.

🗖 📕 Logout on Timeout			
💋 Logout on Timeout			
Properties of \	/iewElementTemplateElementReferenceElement: 'Logout\Main Layer\Logout on T 🚊 🛪		
Template	General Access Other		
Logout J	lump		
Jump Vie	ew E MACRO.wev		
Timeout	[s] = 300		

8.4.4 Change password

The user can change his/her own password using the "Change Password Template". In order to change the password, the current password must first be entered correctly. The new password must then be entered twice and then confirmed. The new password is then active. The old password immediately loses its validity!

Change Password	Change Password	Change Password
Old	Old	Old
New	New newPassword	New newPassword
New	New repeatPassword	New newPassword
0	0	0



8.5 Compatibility of new access control and old user identification

The access control templates are not compatible with the existing user identification solution. Unlike the 4 levels of the old user identification process, the new access control involves 16 groups. Rather than representing levels, they are individually configurable. An element is displayed or active if the registered user possesses the rights of the group(s).

A project created with WebEditor 5.15 or the old user identification system can be ported to the new user management system with little effort. This can be done in WebEditor 8 using new templates for access control; 4 users need to be defined and their rights displayed on the internal variable "userLevel". No other modifications to the project are needed.

- 4 users must be defined (1 to 4) After a successful login, the rights for the users are stored in the internal variables "?S_User_L0..3".
- 2) The rights for the users must now be displayed on the internal variable "userLevel". The internal variables "?S_User_L0..3" may contain "0" or "1".
- 3) An "Invisible Box Event" can be used for this purpose.

ibraries : TempTest	
filter by name	
Name	▲
File Viewer	
😰 Image	
🏸 Invisible Event Box	

4) The "Invisible Box Event" is placed on the page with the login template and the user rights are transferred to the internal variable "userLevel" when the page is closed.

Properties of EventBox: 'Logout')Main Layer')Event Box'			-	×
General Actions Access Other				
	On refresh	Do Nothing	•	
On view open		Do Nothing	•	
	On view close	Call Function	•	
		Groups to userLevel	2	



- 5) This function for transferring user rights to the "userLevel" can be implemented as follows:
 - → Reset the internal variable "userLevel"
 - → Set the internal variable "userLevel" on the basis of the user rights; when entering the levels, the highest user (4) then obtains the internal variable "userLevel"

Name:	Name: Groups to userLevel Owner: EventBox: 'Event Box'			
Write	▼ = ▼ 0	to INT - userLevel		
If	▼ INT ▼ S_User_L0	= • = • 1		
Writ	e 🔻 = 🖛 1	to 🕅 🔻 userLevel		
If	▼ INT ▼ S_User_L1	= 👻 = 💌 1 🛛 📲		
Writ	e ▼ = ▼ 2	to 🔤 🔻 userLevel		
If	▼ INT ▼ S_User_L2	= 🕶 = 🕶 1 😽		
Writ	e ▼ = ▼ 3	to 🔤 🖛 userLevel		
If	▼ INT ▼ S_User_L3	= 🕶 = 🕶 1 😽		
Writ	e • E • 4	to INT - userLevel		

?S_User_L0	\rightarrow Level 1	ightarrow userLevel == <1>
?S_User_L1	\rightarrow Level 2	\rightarrow userLevel == <2>
?S_User_L2	\rightarrow Level 3	\rightarrow userLevel == <3>
?S_User_L3	\rightarrow Level 4	\rightarrow userLevel == <4>

6) Existing "Logout" macros must be replaced by the "User Indentification" template in WebEditor 8.

