SecurityBridge:
Get Security Level SL1 for PLC PSS 4000

PILZ
THE SPIRIT OF SAFETY

Product

Type:	PSS4000 Family
Name:	-
Manufacturer:	Pilz GmbH & Co. KG, Safe Automation

Document

Release Number:	02
Release Date:	10 March 2025

Application Note – AN_SecurityBridge_SL1_PSS4000_1006809_EN_02

Document Revision History

Release	Date	Changes	Chapter
01	2023-10-18	Creation	all
02	2025-03-10	Change Table 1	5.1

Validity of Application Note

This present Application Note is valid until a new version of the document is published.
This and other Application Notes can be downloaded in the latest version and for free from www.pilz.com. For a simple search, use our content document (1002400) or the direct search function in the download area.

The Pilz newsletter is free of charge and keeps you up-to-date on all the latest issues and trends in safe automation.

Exclusion of Liability

We have taken great care in compiling our application note. It contains information about our company and our products. All statements are made in accordance with the current status of technology and to the best of our knowledge and belief.
While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, all information on applicable standards, safety-related classifications and time characteristics should be viewed as provisional. In particular it should be noted that statements do not have the legal quality of assurances or assured properties.
We are grateful for any feedback on the contents.

March 2025

Industrial Security

To secure plants, systems, machines and networks against cyberthreats it is necessary to implement (and continuously maintain) an overall Industrial Security concept that is state of the art.
Perform a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care. If necessary, seek advice from Pilz Customer Support.

Abbreviations

Abbreviation / term	Description	Source
AN	**A**pplication **N**ote	www.pilz.com > AN content (1002400)
PSS	Programmable control system (DE: **P**rogrammierbares **S**teuerungs**s**ystem)	www.pilz.com > PSS 4000
SL	**S**ecurity **L**evel	IEC 62443
SLt	**S**ecurity **L**evel **t**arget	IEC 62443
ML	**M**aturity **L**evel	IEC 62443
FR	**F**oundational **R**equirement	IEC 62443
SR	**S**ystem **R**equirement	IEC 62443
CR	**C**omponent **R**equirement	IEC 62443
IAC	**I**dentification and **A**uthentication **C**ontrol	IEC 62443
IACS	**I**ndustrial **A**utomation and **C**ontrol **S**ystem(s)	IEC 62443
UC	**U**se **C**ontrol	IEC 62443
SI	**S**ystem **I**ntegrity	IEC 62443
DC	**D**ata **C**onfidentiality	IEC 62443
RDF	**R**estricted **D**ata **F**low	IEC 62443
TRE	**T**imely **R**esponse to **E**vents	IEC 62443
RA	**R**esource **A**vailability	IEC 62443

Definition of Symbols

Information that is particularly important is identified as follows:

CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.

NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken.
It also highlights areas within the text that are of particular importance.

INFORMATION

This gives advice on applications and provides information on special features.

Contents

1 Useful documentation

Reading the documentation listed below is necessary for understanding this Application Note. The availability of the software used, and its safe handling are also presupposed for the user.

1.1 Documentation from Pilz GmbH & Co. KG

No.	Description	Item No. /Download
1	List of Operating Manuals of the devices of PSS4000-Family (PSSu H ...)	www.pilz.com > OperMan list
2	System Description PSS 4000 (1001467)	www.pilz.com > SysDesc 1001467
3	Application Note SecurityBridge Setup, Version 02 (1005680)	www.pilz.com > ApplNote 1005680
4		

1.2 Documentation from other sources of information

No.	Description
1	VDMA - Guideline IEC 62443 (2021)
2	DGUV - FBHM-102: Safety and Security in Networked Production (10-2018)
3	DIN_IEC_TR_63074_{2021-05}
4	DIN_EN_IEC_62443-4-2_{2019-12}
5	DIN_EN_IEC_62443-3-3_{2020-01}
6	

2 Used hardware and software

2.1 Pilz products

No.	Descriptions	Order number	Version
1	PSSu H PLC2 FS SN SD	312077	V1.0
2	SecurityBridge PCOM sec br2	311502	V2.0
3	PAS4000	--	V1.25.0
4	SecurityBridge VPN Client V1.0.1	--	V1.0.1

3 IEC 62443

3.1 What are the IEC 62443 Security Levels (SL)?

In the IEC 62443-3-3, appendix A.2.2 the term Security Levels (SL) is explained in detail. There are used three different kinds of SL:

- SL-T (T for "Target"): is a result of a risk analysis and describes the minimum level of needed SL
- SL-A (A for "Achieved"): current achieved security levels of a given system
- SL-C (C for "Capable"): SL which the components or systems can deliver when properly configured.

There are five different Security Level values (IEC 62443-3-3 appendix A.3.2), 0–4, and have different meanings depending on the application situation. SL 0 is the lowest level of risk and SL 4 is the maximum. That means that every SL has stricter compliance requirements than the next lower SL. In summary it can be said:

- Security Level 0
  No specific requirements or security protections
- Security Level 1
  Protection against occasional or coincidental violation
- Security Level 2
  Protection against intentional violation using simple means with:
  - Low resources
  - Generic skills
  - Low motivation
- Security Level 3
  Protection against intentional violation using sophisticated means with:
  - Moderate resources
  - IACS specific skills
  - Moderate motivation
- Security Level 4
  Protection against intentional attacks with sophisticated means with:
  - Extended resources
  - IACS specific skills
  - High motivation

3.2 What are the 7 Security Level Foundational Requirements?

There are seven specific foundational requirements that must be met for each SL. Meeting these requirements ensures that an IAC or IACS has the right security safeguards.

The foundational requirements for an SL are:

1) Identification and Authentication Control
   Reliably identify and authenticate all users (humans, software processes, and devices) attempting to access the ICS.

2) Use Control
   Enforce the assigned privileges of an authenticated user (human, software process, or device) to perform the requested action on the system or assets. Monitor the use of these privileges.

3) System Integrity
   Ensure the integrity of the IACS to prevent unauthorized manipulation.

4) Data Confidentiality
   Ensure the confidentiality of information on communication channels and in data repositories. Prevent unauthorized disclosure.

5) Restricted Data Flow
   Segment the control system via zones and conduits to limit the unnecessary flow data.

6) Timely Response to Events
   Respond to security violations. Notify the proper authority reporting needed evidence of the violation. Take timely corrective action when incidents occur.

7) Resource Availability
   Ensure the availability of the control system against the degradation or denial of essential services.

   Each foundational requirement has multiple conditions that need to be met depending on the SL. The higher the SL, the more conditions that must be met for the foundational requirement.

4 Application description

- This application note shows the individual tasks to attain a zone with SL1 (Security Level 1) with one or more PSS4000 devices included. The SL of the PSS4000 itself will not be changed. This AN is no substitution to the official standard IEC 62443. The standards must be read and understood before. The risk assessment must be created before, and if it shows SL1 as needed security level, this AN will help to attain it.

As an example, we will use a PSSu H PLC1 FS SN SD in this example, the results can be transferred to the other PSS4000 head modules.

4.1 Preface

The development of PSS4000 devices, has started years before there has been official standards for security.
Since then, the IEC 62443 has been created. To achieve any demanded security level and maturity level from this standard, different counter measurements must be fulfilled.
A risk assessment must be created, and the result shows which security level is needed and thus which counter measurements must be implemented.
At real live applications are mostly several devices that need different counter measurements. But if the whole system is considered it is often possible to combine several security functions.
In real live applications financial expenses must be faced with the benefit and the minimal security that is needed.

To support our customers in the whole process or individual parts of it, Pilz offers certified services to carry out risk assessment, develop concepts to achieve the desired security levels and trainings for the standard IEC 62443 are offered.

NOTICE

- How to create a risk assessment will not be part of this Application Note.
- The risk assessment must be created before

4.2 Network topology

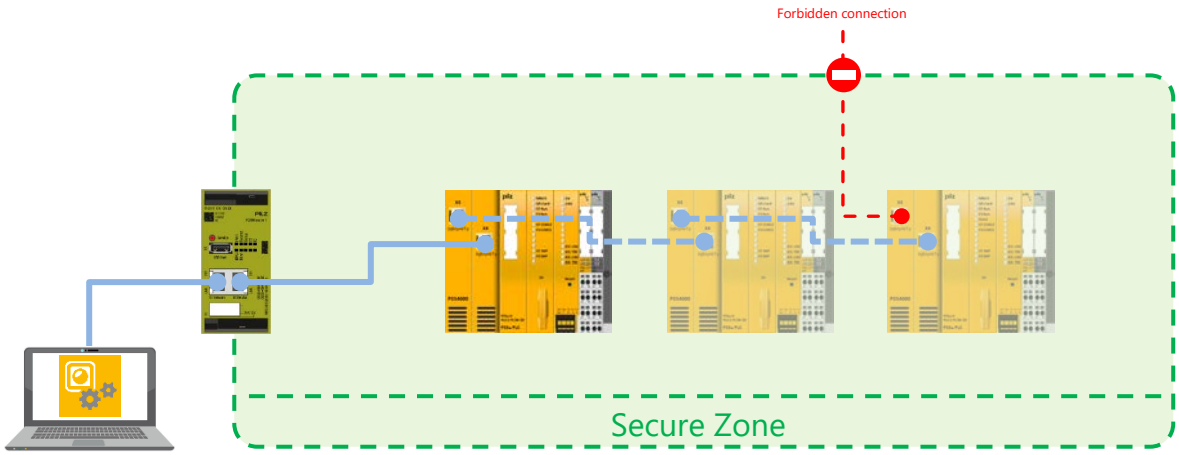

Figure 1: Secure Zone with SecurityBridge in an Ethernet Network

5 Preliminary considerations

5.1 Foundational requirements

In the table below are all 7 foundational requirements (DIN EN IEC 62443-4-2). To use the PSS4000 devices in a SL1 zone, these FRs must be met. The table lists possible countermeasures for each FR.

Foundational Requirements (for SL1)	**countermeasures**
FR1 Identification and Authentication Control	VPN
FR2 Use Control	VPN
FR3 System Integrity	VPN
FR4 Data Confidentiality	VPN
FR5 Restricted Data Flow	Firewall
FR6 Timely Response to Events	Log Server
FR7 Resource Availability	Log Server

Table 1: Foundational Requirements for SL1

Based on this table the conclusion is made, that a device which doesn't meet any of these FRs needs three countermeasures to address all foundational requirements:

- FR1 – FR4 can be met with a VPN.
- FR 5 can be met with a firewall.
- FR6 + FR7 can be met with a log server.

6 Hardware configuration

6.1 Used hardware

6.1.1 PSS4000

The devices of PSS4000 system are used in virtually every area of plant and mechanical engineering, mostly in a network of more than one Head Modules. They can be used to monitor safety functions safely and to perform standard control functions economically.
The PSS4000 system has a modular design to meet the needs of the application. PSS4000 head modules can be connected via Ethernet, Ethernet based field busses and conventional field busses.

Figure 2: PSS4000 System with Head Module, Basic- und E-Modules

6.1.1.1 Functions and Properties

Project engineering
- IEC 61131 Text-based Languages and Ladder Logic to program Fail Safe and Standard
- Multi Language (like Function Block)
- Define Devices and their E-Modules
- Distributing Programs to Devices and Tasks
- Map variables to HW I/Os independently of where they are used.

Network
- Safety NET p
- Ethernet, ProfNet IO Device, Ethernet/IP Adapter
- Profibus-DP Slave

Deep Diagnostics
- All Diagnostic Info's of all Devices, their Hard- and Software in one View (Tool)

Tracing
- Variable Logging of a limited number of all variable types

Tool User Management for Engineering Project Security

6.1.2 SecurityBridge

The SecurityBridge PCOM sec br2 from Pilz GmbH & Co. KG is an industrial Firewall. The configuration is solved hardware (FPGAs) and thus it cannot be compromised during runtime. Furthermore, leads this hardware to a small latency.
The bridge will be connected in the network between two devices/zones and will filter all network traffic, in both directions, based on the configured rules.

Figure 3: SecurityBridge

6.1.2.1 Functions

The SecurityBridge is capable to perform following tasks.

- IP-address filter
- MAC-address filter
- Protocol filter
- Deep-packet-inspection (e.g., SafetyNET)
- Port blocking (whitelist)
- VPN
- Integrity monitoring

6.2 Setup of the countermeasures in the hardware

All countermeasures are based on functions of the SecurityBridge, and this chapter is going to show how to set up those.
Basic installation instruction for the SecurityBridge can be found in the manual and in the application note “AN_SecurityBridge_Setup_1005680-EN-02”.

For the following steps it is assumed that:

- The PC, the SecurityBridge and the PSS4000 are in the same IP address range and are wired up correctly.
- The PC and the SecurityBridge have exchanged security certificates to obtain a secure connection.
- In SecurityBridge a user management is established that contains a password protected user with at least the permission “PSS 4000 DeviceAdmin”.

6.3 Connection via VPN Tunnel

In order to have a secure connection from your PAS4000 to a PSS, you need to open a VPN tunnel between your PC and the PSS. Therefore, you have to install a VPN client on your PC and set some specific options in the SecurityBridge.

Figure 4: PSS VPN connection overview

6.3.1 Requirements

1) Download the “SecurityBridge VPN Client” from the PILZ homepage.

Figure 5: PCOM sec br2 – Download VPN client

2) Download a “PEM” certificate from your SecurityBridge. Therefore, go to the section “System → Certificates”, and select certificate type “CA certificate” and certificate format “PEM”. Press “Download” to download the certificate.

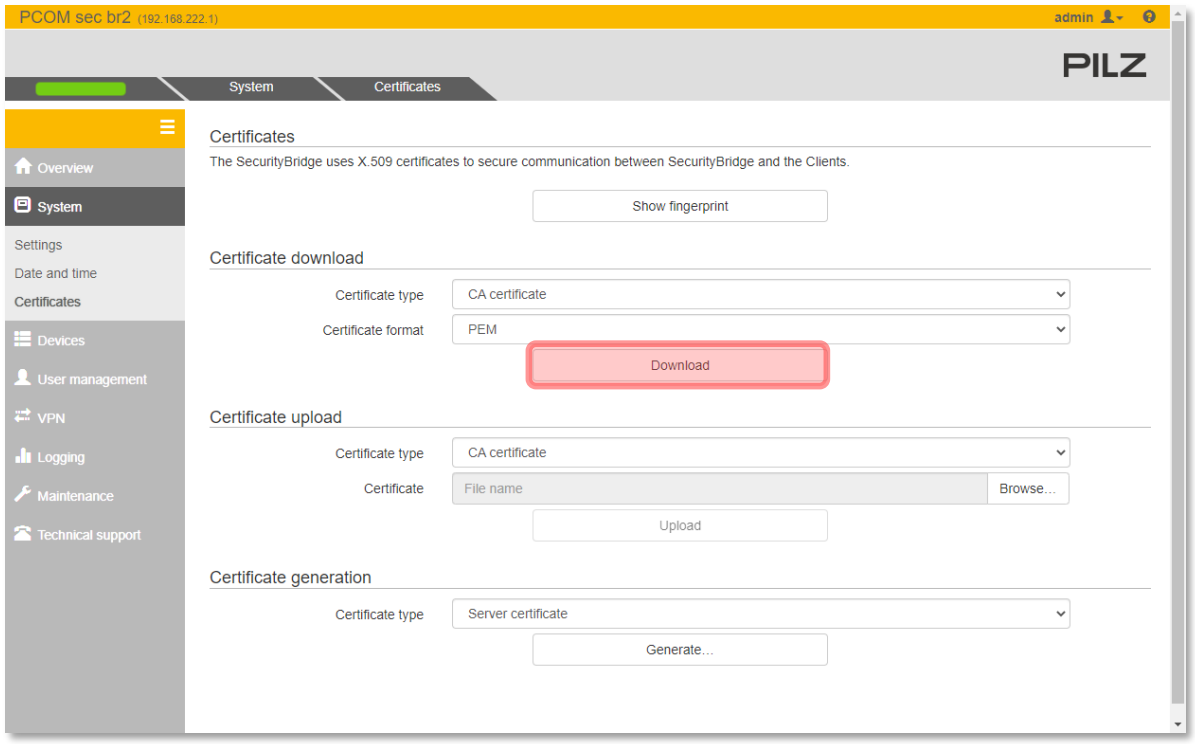

Figure 6: PCOM sec br2 – Download PEM certificate

3) To open a VPN connection a user with permission from the group "PNOZmulti permissions", "Network permission", "PSS 4000 permissions” or "Generic Device permissions" must be created, as shown in *chapter 4.2 User management of document ‘AN_SecurityBridge_Setup_1005680-EN-02,* see Ch. 1.1 Documentation from Pilz GmbH & Co. KG [📖 5].

4) Device (in this case the PSS) must be connected to the SecurityBridge "Device" port via patch cable and must be added to the SecurityBridge devices list. To add the PSS to the SecurityBridge devices, go to the section "Devices", press "NEW" and perform a network scan for PSS4000 devices.

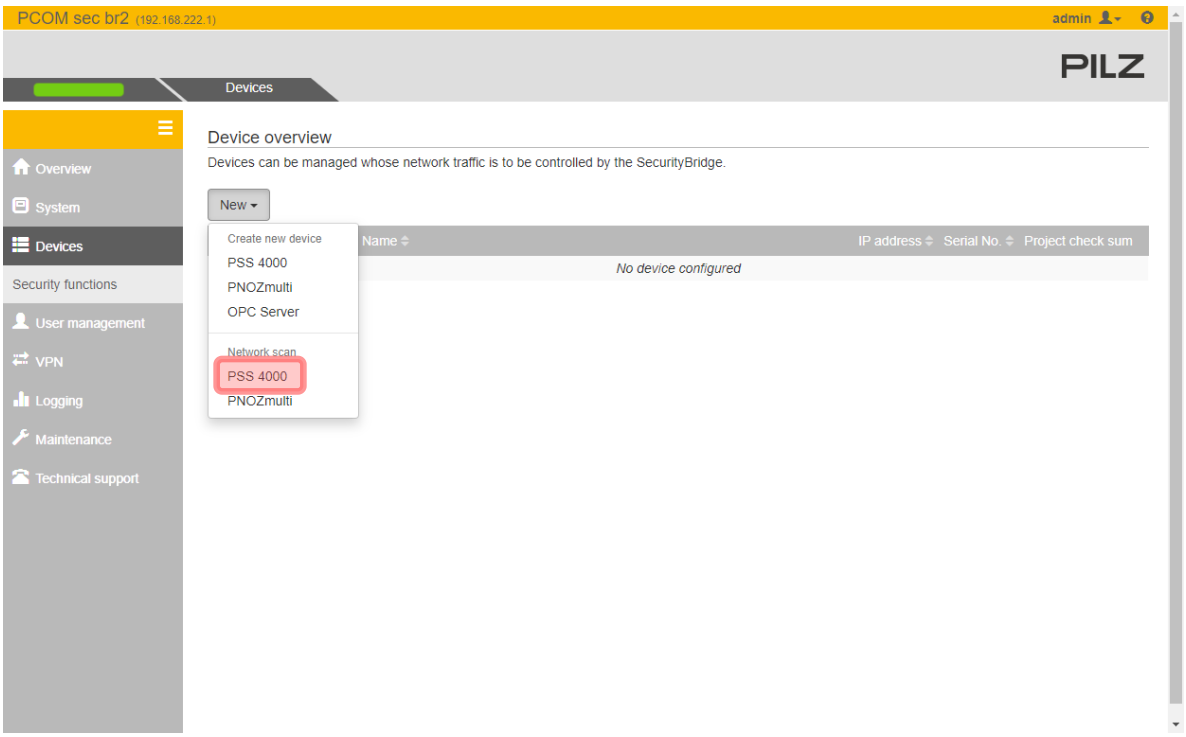

Figure 7: PCOM sec br2 – Perform PSS4000 network scan

5) If your device is wired correctly, it's shown in the list. Select the device and press "Add". If it's not shown, make sure the PC, the SecurityBridge and the device are in the same IP range.

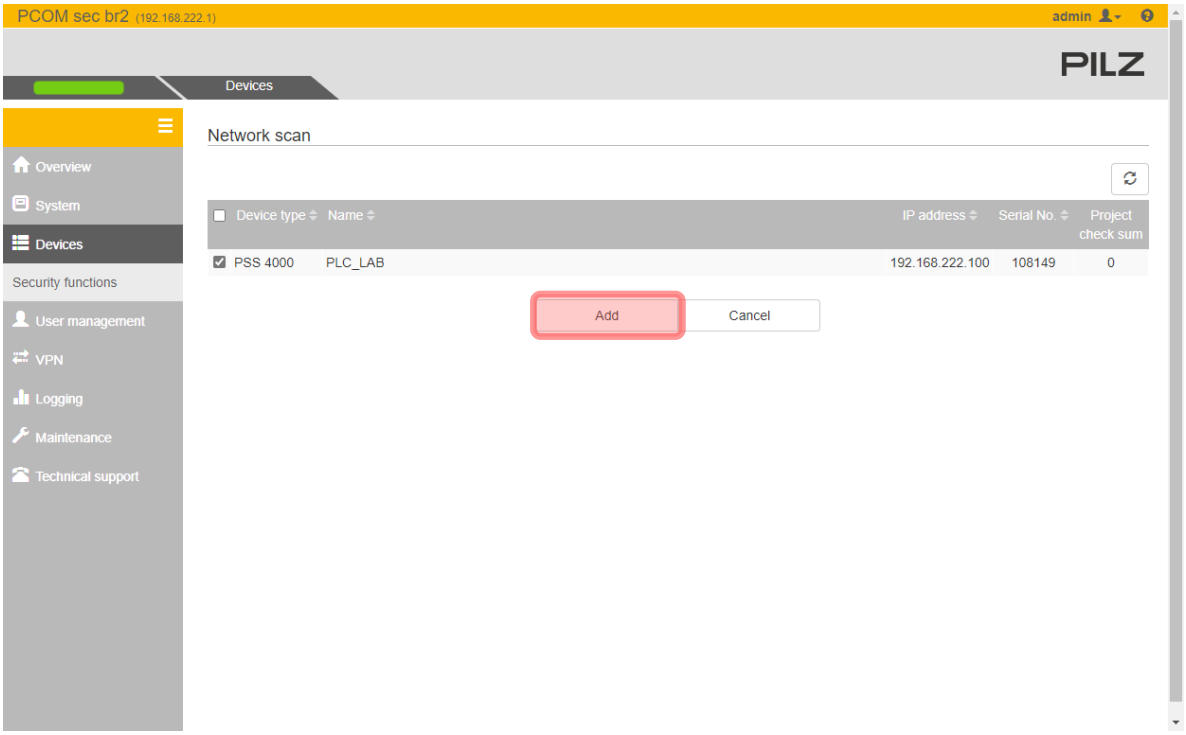

Figure 8: PCOM sec br2 – Add found device

6) If successful, you get a green banner “THE CONFIGURATION WAS CHANGED”.

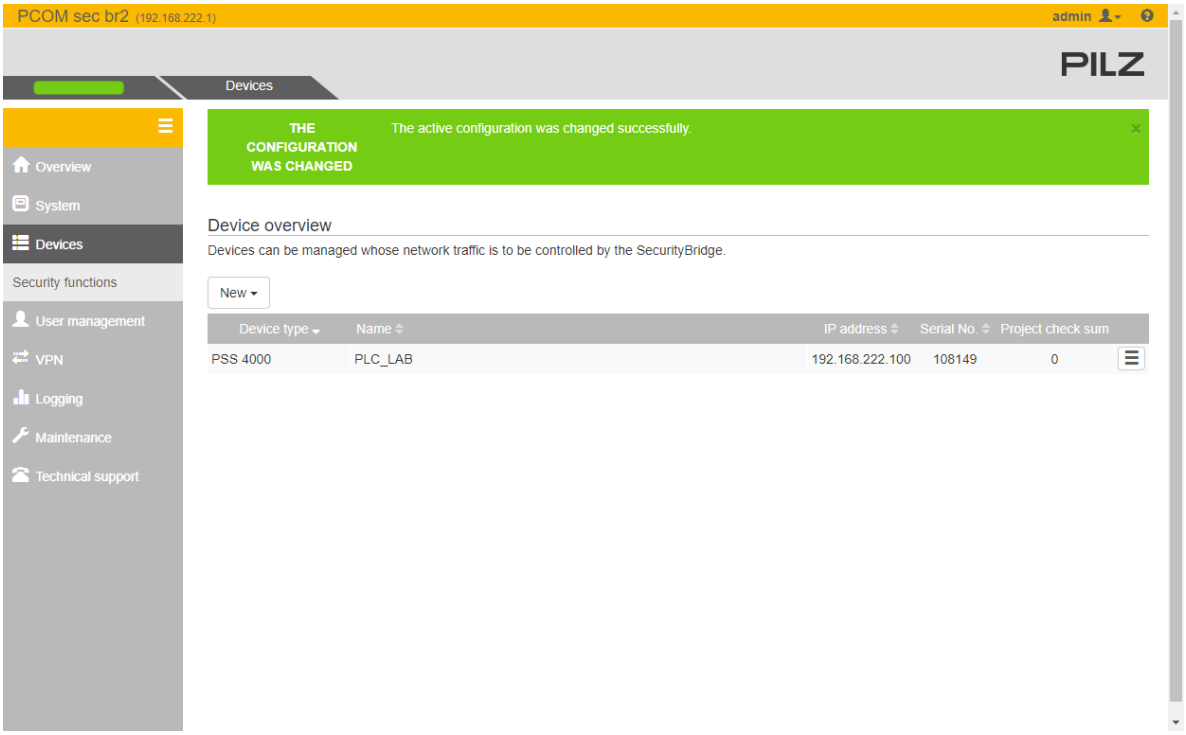

Figure 9: PCOM sec br2 – Changes successful

7) Save changes permanently in the SecurityBridge, see in *chapter 5.1 Save settings permanently of document ‘AN_SecurityBridge_Setup_1005680-EN-02,* see Ch. 1.1 Documentation from Pilz GmbH & Co. KG [📖 5].

6.3.2 Set up a VPN connection

To connect to a PILZ device (in this case a PSS4000) a VPN tunnel connection must be created, and the connection must be established. In the corresponding tool for the device (in this case PAS4000) the VPN tunnel is selected as programming network adapter.

1) Install the downloaded VPN client

Figure 10: SecurityBridge VPN Client – Program

2) Start the VPN client and press "Add Connection"

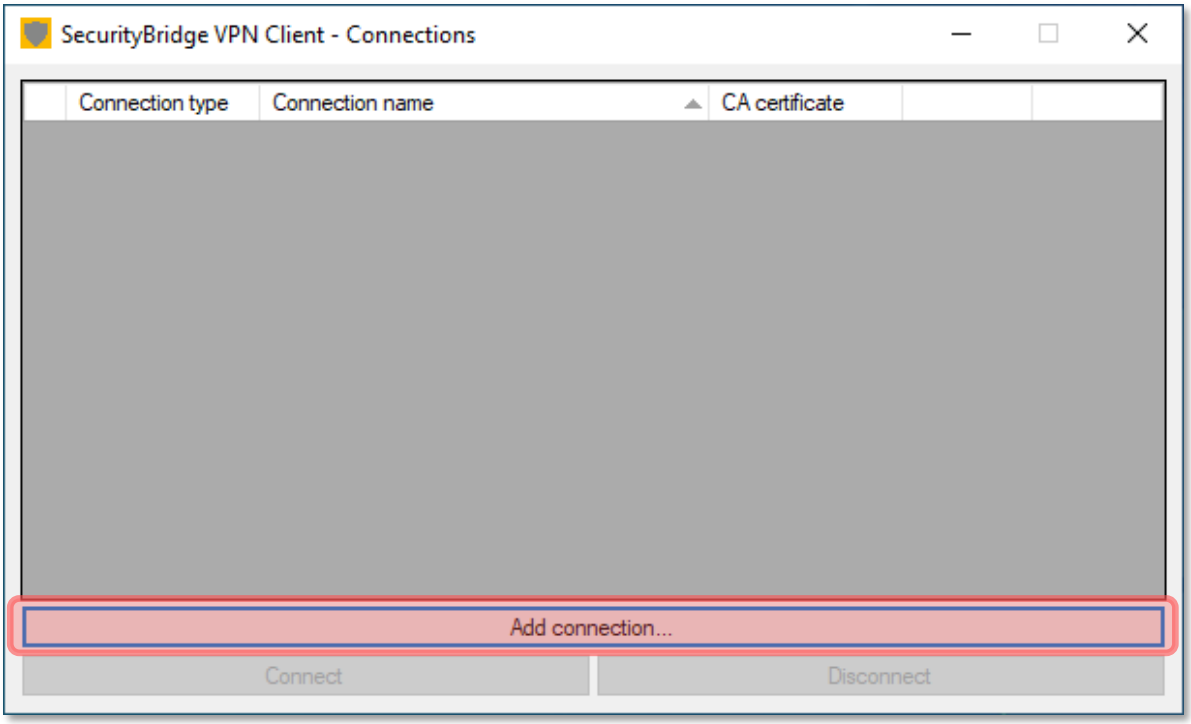

Figure 11: SecurityBridge VPN Client – Add VPN connection

3) Set an appropriate name and enter the IP address of the SecurityBridge. Now browse for the downloaded PEM certificate and select it.

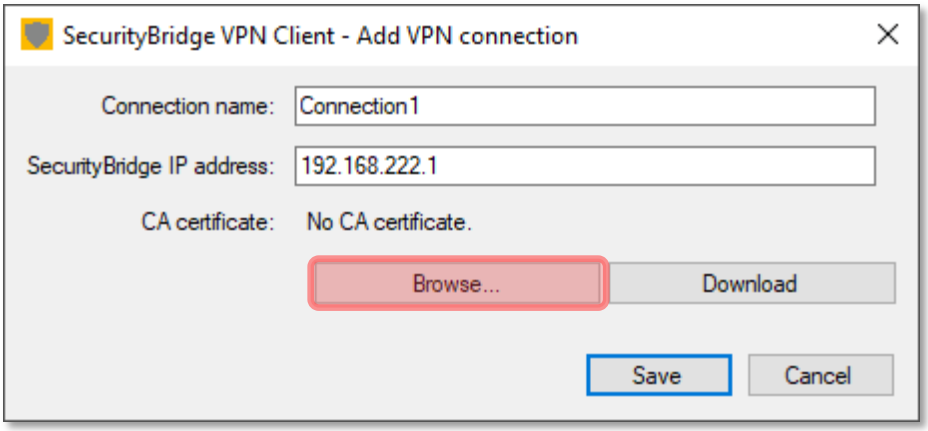

Figure 12: SecurityBridge VPN Client – VPN connection settings 1/2

4) If the certificate is added correctly, it will show “certificate is available”. Save your new connection with “Save”.

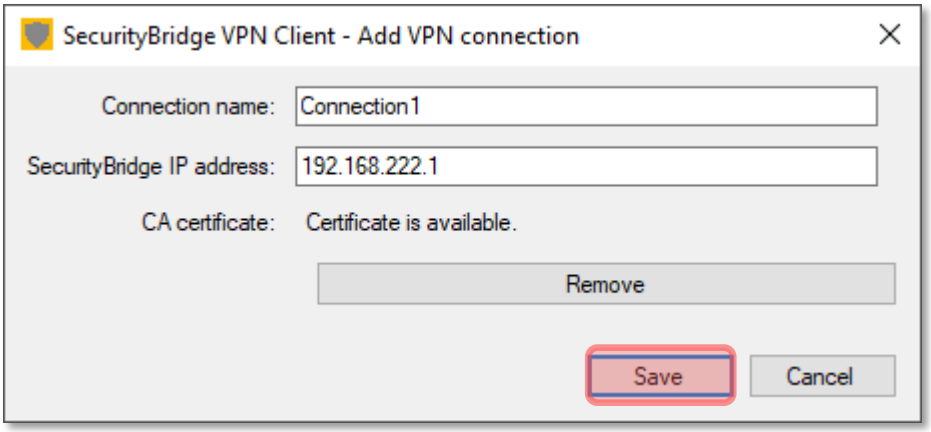

Figure 13: SecurityBridge VPN Client – VPN connection settings 2/2

5) The VPN connection to the SecurityBridge can now be established by pressing “Connect”.

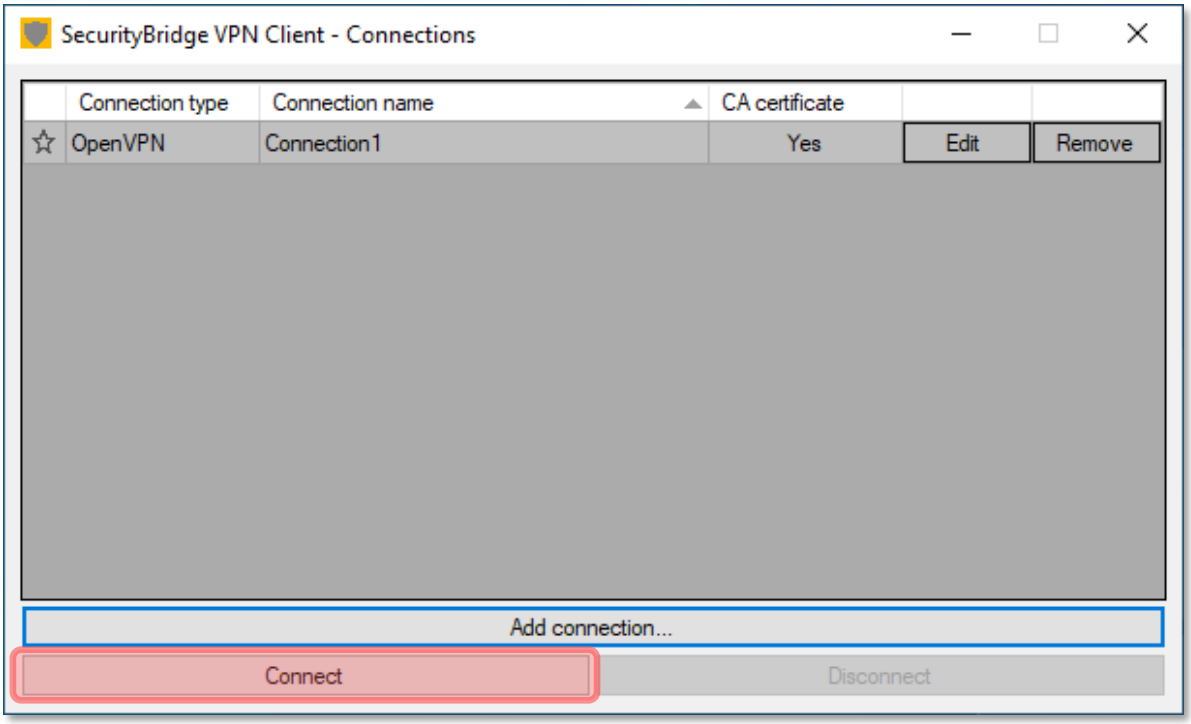

Figure 14: SecurityBridge VPN Client – Connect to VPN

6) In the next window the username and corresponding password needs to be entered, confirm with “OK”.

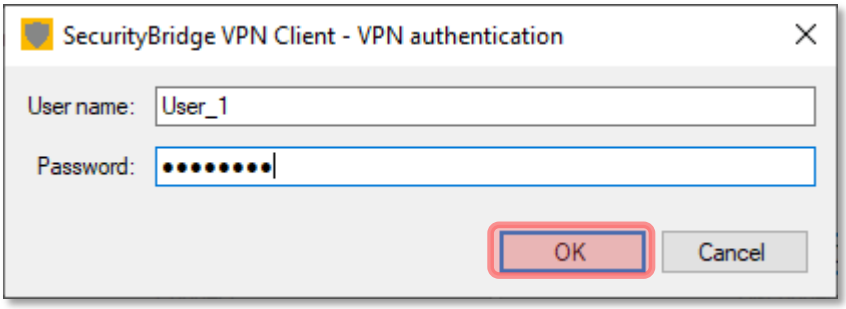

Figure 15: SecurityBridge VPN Client – Enter credentials

7) The VPN connection is established.

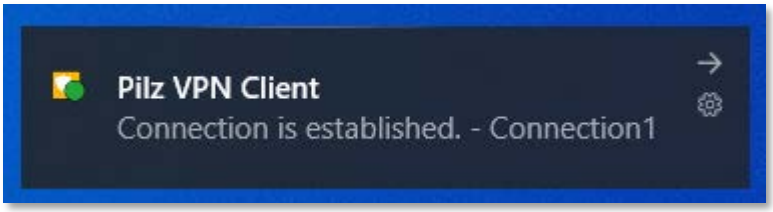

Figure 16: SecurityBridge VPN Client – VPN connection is established

6.3.3 Connect to device

1) Start PAS4000

Figure 17: PAS4000 – Splash screen

2) Open the Online Network editor and select the VPN connection as programming interface. To do so, click on “Select Programming Interface”.

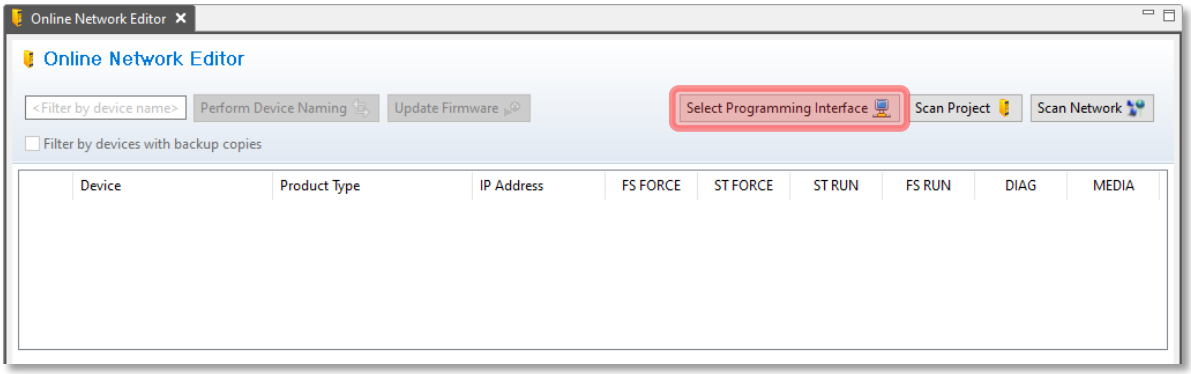

Figure 18: PAS4000 – Online Network Editor » Select programming interface

3) Choose the “Pilz SecurityBridge VPN Adapter”, press “Apply” and close the window with “OK”

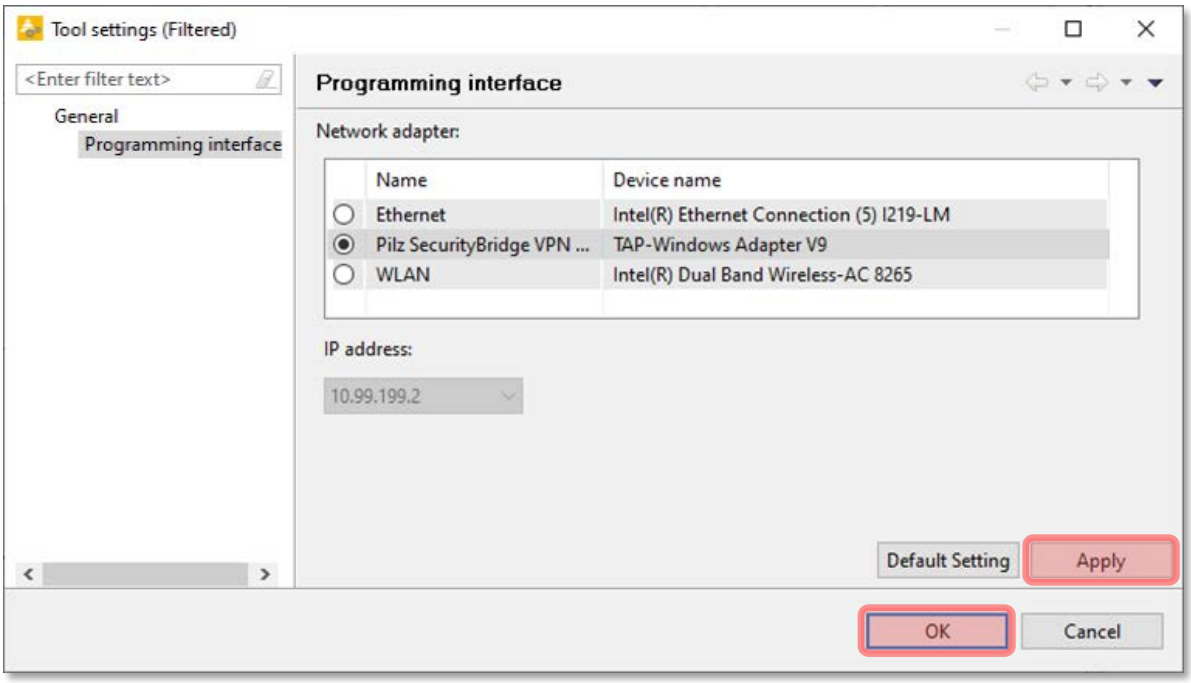

Figure 19: PAS4000 – Tool Settings » Select programming interface

4) After the programming interface is set, a network scan for PAS4000 devices can be performed. Press “Scan Network” to start a network scan.

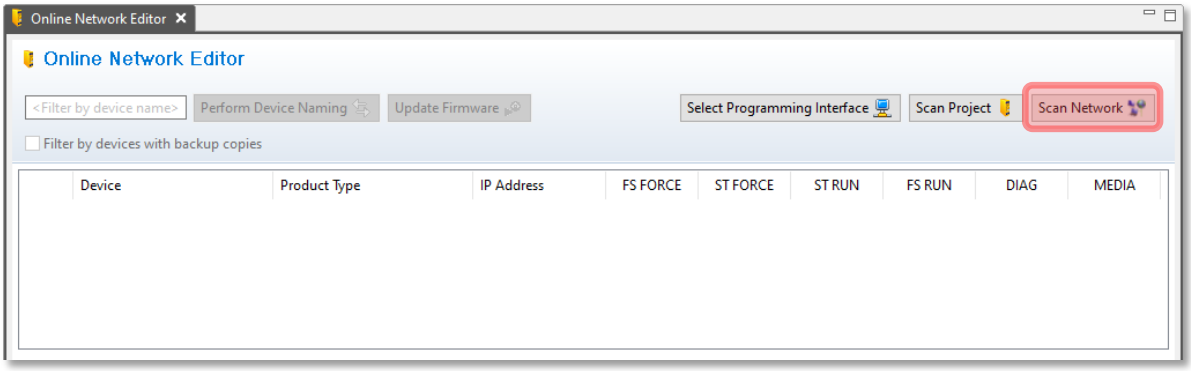

Figure 20: PAS4000 – Online Network Editor » Start network scan

5) The results of the network scan are shown in a list, one of these results should be the PC that started the network scan, and the other one should be the found PSS device. If both LEDs (DIAG and MEDIA) are green, you are able to connect to the PSS4000 and work with it as usual. If the LED doesn’t light up, or the device symbol turns grey, make sure the IP addresses are set correctly and the device is known to the SecurityBridge.

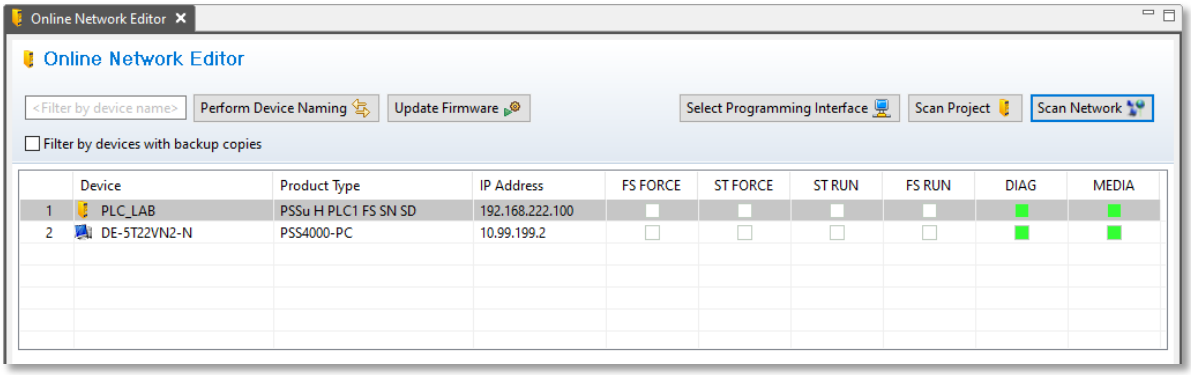

Figure 21: PAS4000 – Online Network Editor » Found network devices

6) When the work is done, the connection can be disconnected.

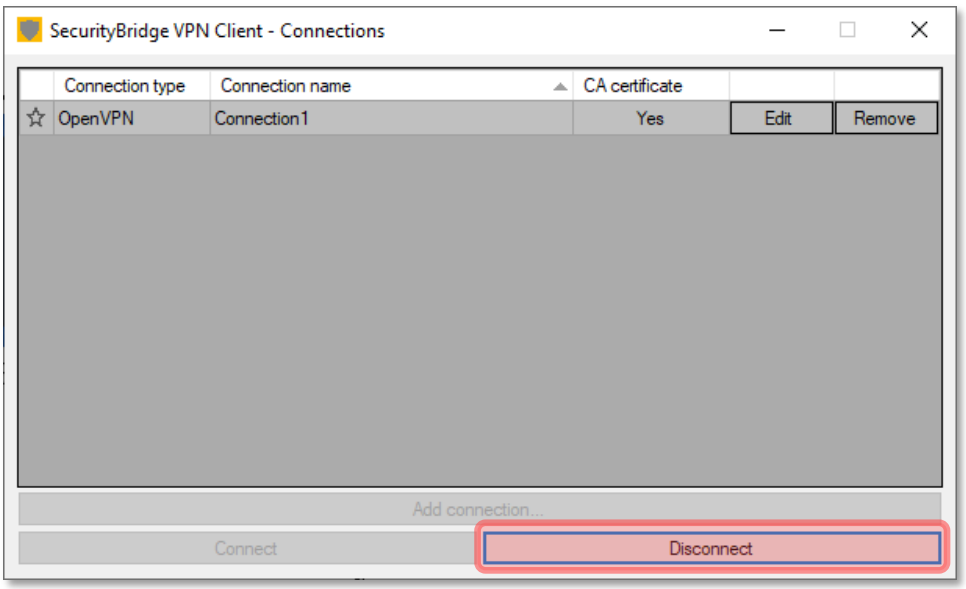

Figure 22: Security Bridge VPN Client – Disconnect VPN connection

6.3.4 Setup a firewall

The second countermeasure is a firewall that restricts the data flow to and from the PSS4000.

The SecurityBridge is a hardware firewall by design. That means, in default / factory settings, all dataflow from and to the PSS4000 is prohibited. These restrictions include IP address filter, Port filter, protocol filter, DOS protection, and many more.

Every dataflow from and to the PSS4000 needs to be activated manually to work properly.

The only option to avoid the complete firewall is, to use the Bypass-Mode. But this needs to be set up in the webserver (disabled by default), it must be activated manually and is indicated by a LED on the SecurityBridge and/or by a digital output, that can be used by the machine controller to respond in a specific way, if the Bypass-Mode is active.

6.3.5 Setup a log server

On the overview page of the SecurityBridge webserver there is a list with the last 5 events that are logged by the SecurityBridge.
The events the SecurityBridge can log are:

- Information
  - Configuration changed
  - User login
  - VPN established
  - System restart
  - Setup mode active
- Warning
  - Log entries lost
  - Failed to send log messages (email / syslog)
  - Access issues USB storage
  - Network issues
- Critical
  - Invalid configuration
  - Network issues
  - Backup on USB storage modified
- Error
  - Hardware defects
  - Firmware issues

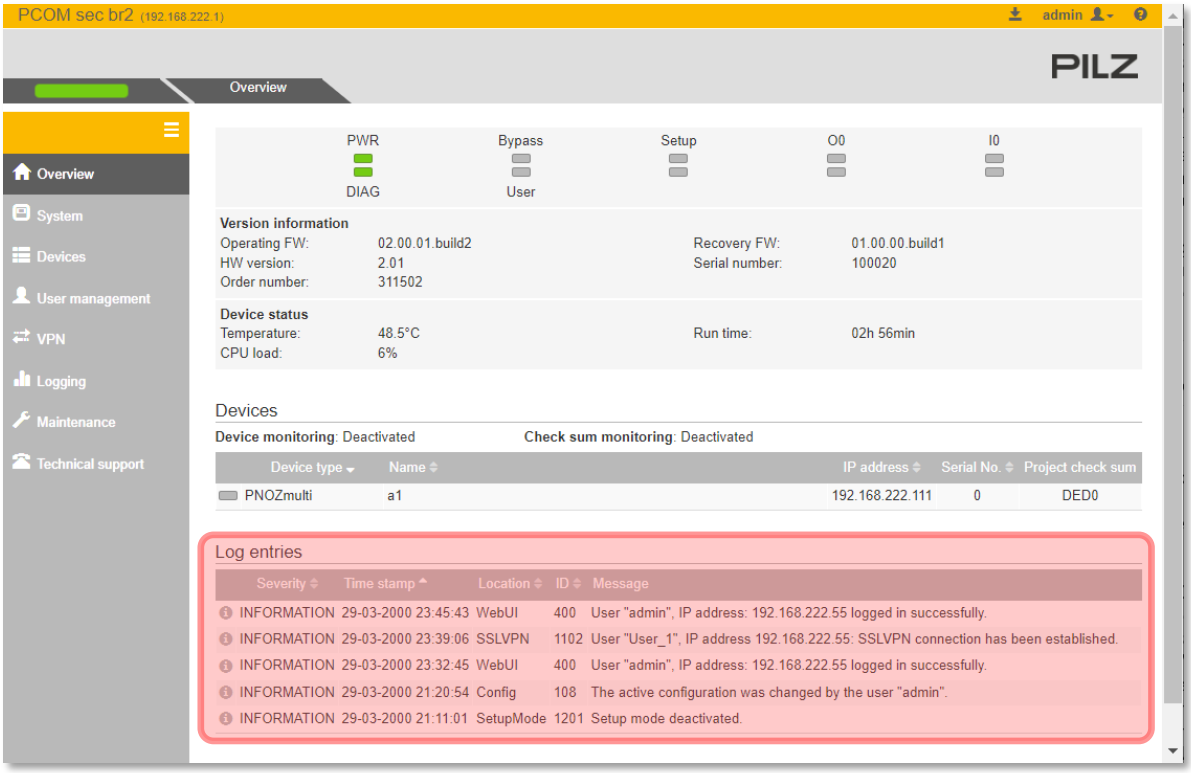

Figure 23: PCOM sec br2 – Log entries Overview page

A longer list is available in the Logging page. There is a maximum of 4096 entries possible, older entries will be deleted (ring memory). The eventlog will be stored permanently to the flash every 15 minutes, if there is a power loss it could happen, that the last 15 minutes in the eventlog will be missing.

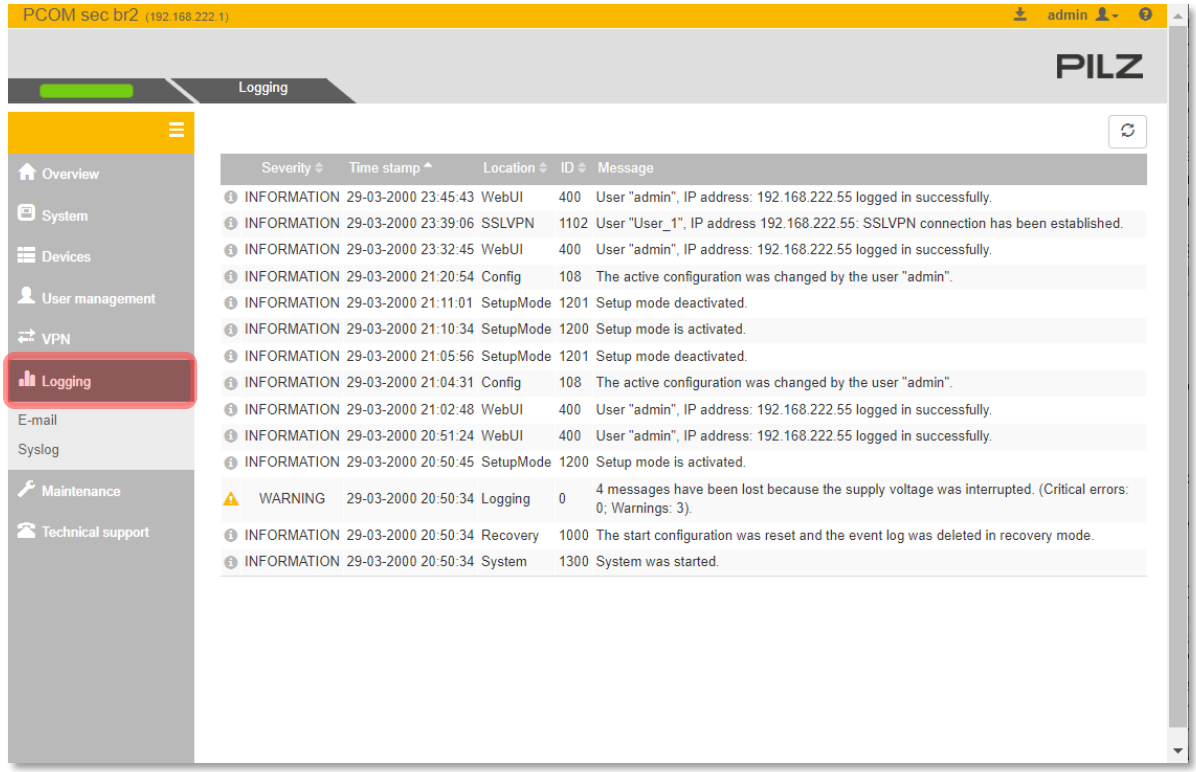

Figure 24: PCOM sec br2 – Log entries Logging page

To prevent a loss of events in the log or prevent manipulation it is possible to forward the events either as E-Mail or to an external Syslog server.

6.3.5.1 Forward via E-Mail

In this case the system forwards all new messages as email at a defined interval. Messages that have not been sent will be sent after a restart.
The severity of the events, that will be sent can be chosen between:

- Information
- Warning
- Critical
- Error

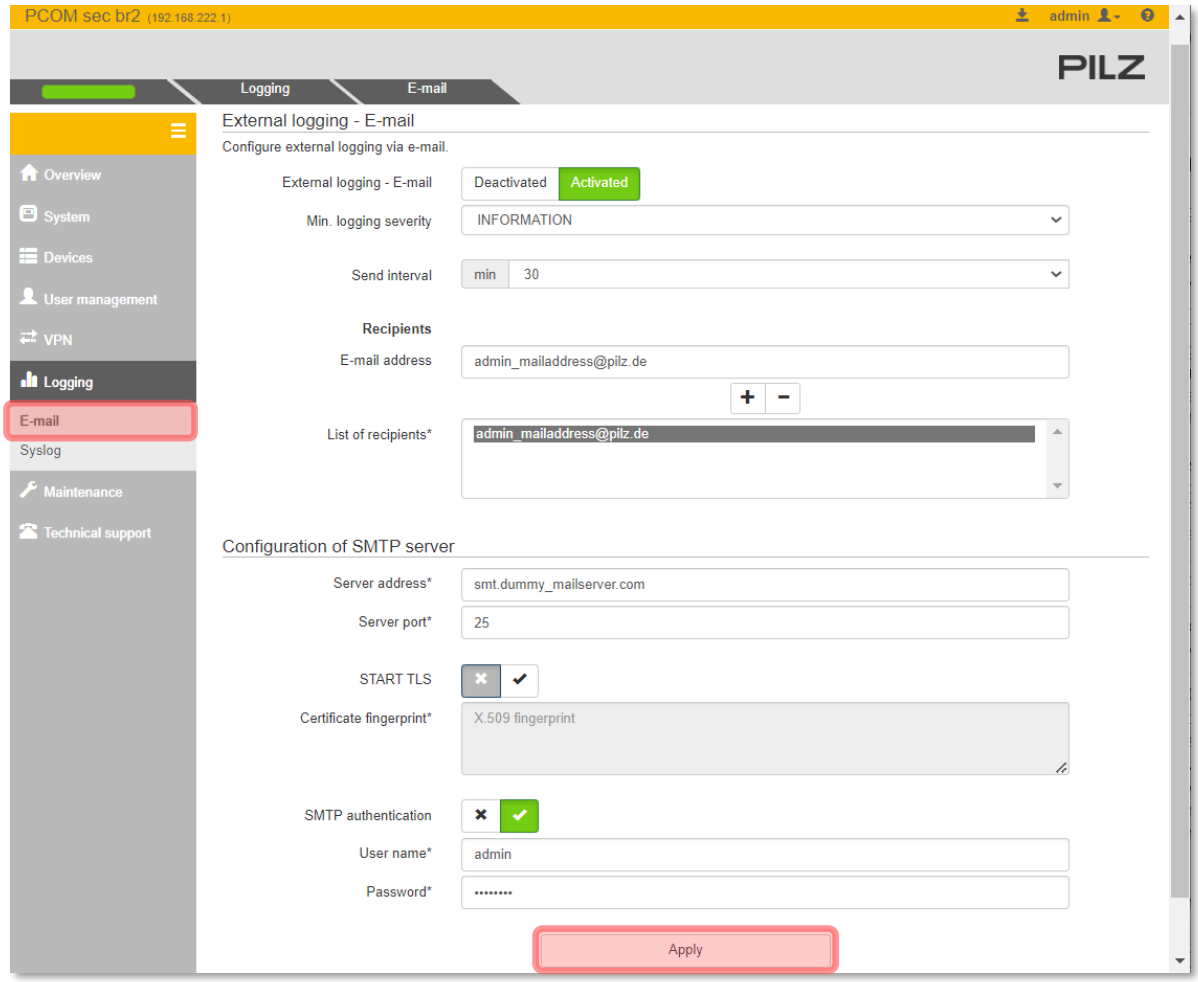

Figure 25: PCOM sec br2 – Logging email settings

If all settings are done, press apply to take the settings to the active configuration. To save it permanently, apply the active configuration as start configuration.

If configuration was successful, there will be a green banner “The Configuration Was Changed”.

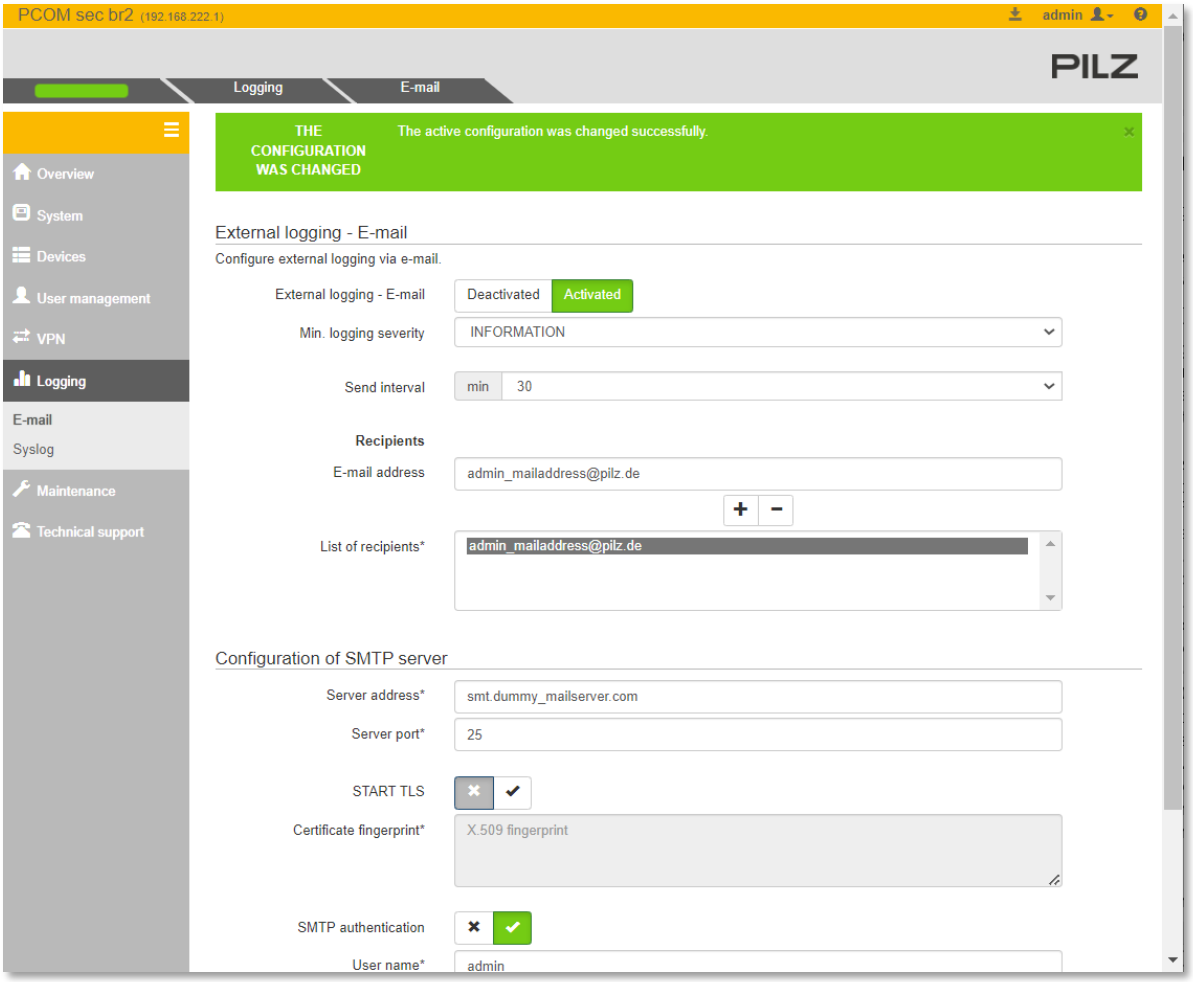

Figure 26: PCOM sec br2 – Changes successful

6.3.5.2 Forward via Syslog

In this case the events will be forwarded to an external Syslog server, as soon as an event is generated. Only one attempt is made to send each Syslog message. If an error occurs or the syslogserver is not available, there will be no attempt to re-send the message.
Note: A Syslog protocol will be transferred unprotected. For this reason, the transfer is not protected from sabotage or data abuse. If necessary, appropriate measures should be taken to protect Syslog communication.
The severity of the events, that will be sent can be chosen between:

- Information
- Warning
- Critical
- Error

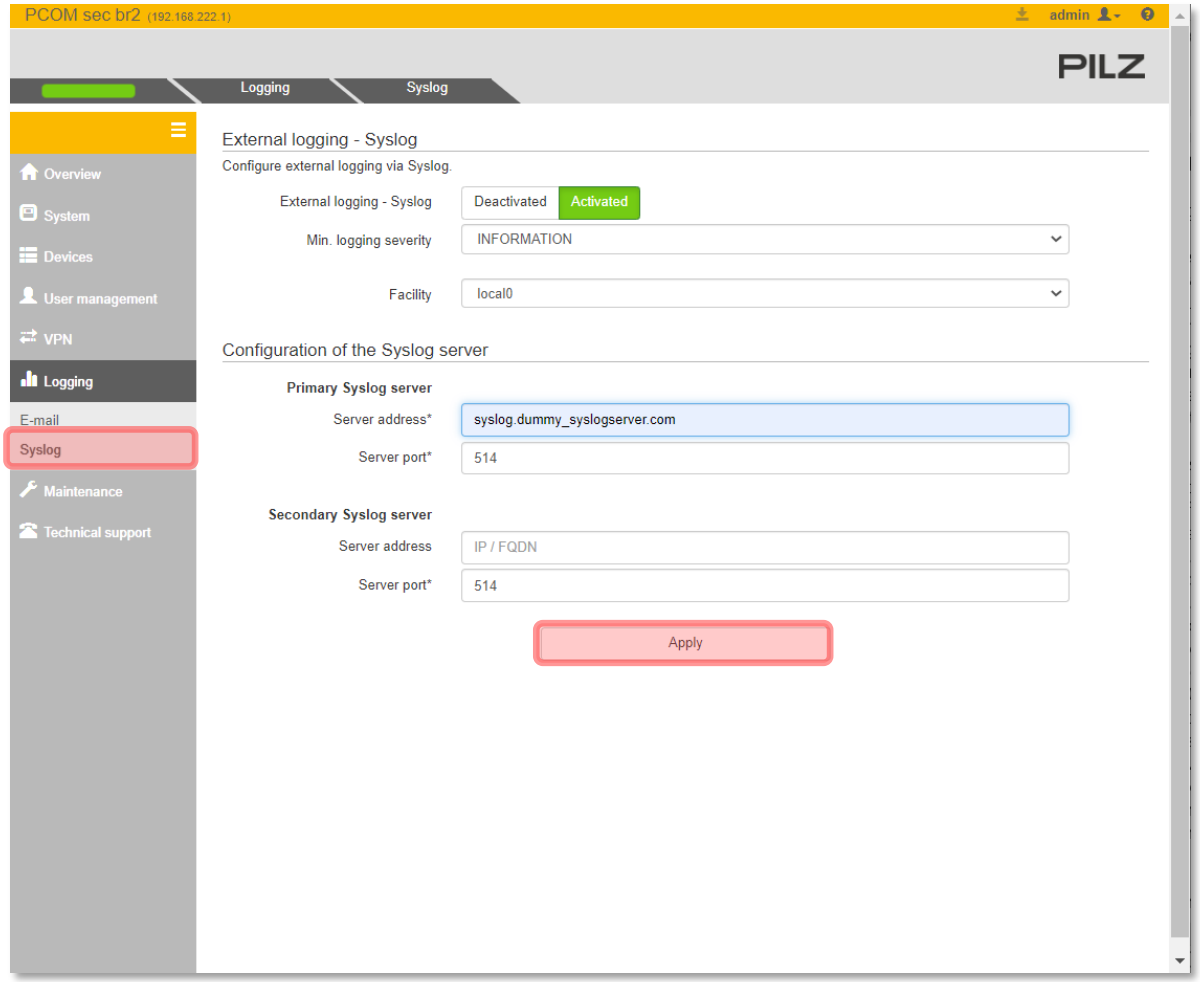

Figure 27: PCOM sec br2 – Logging syslog settings

If all settings are done, press apply to take the settings to the active configuration. To save it permanently, apply the active configuration as start configuration.

If configuration was successful, there will be a green banner “The Configuration Was Changed”.

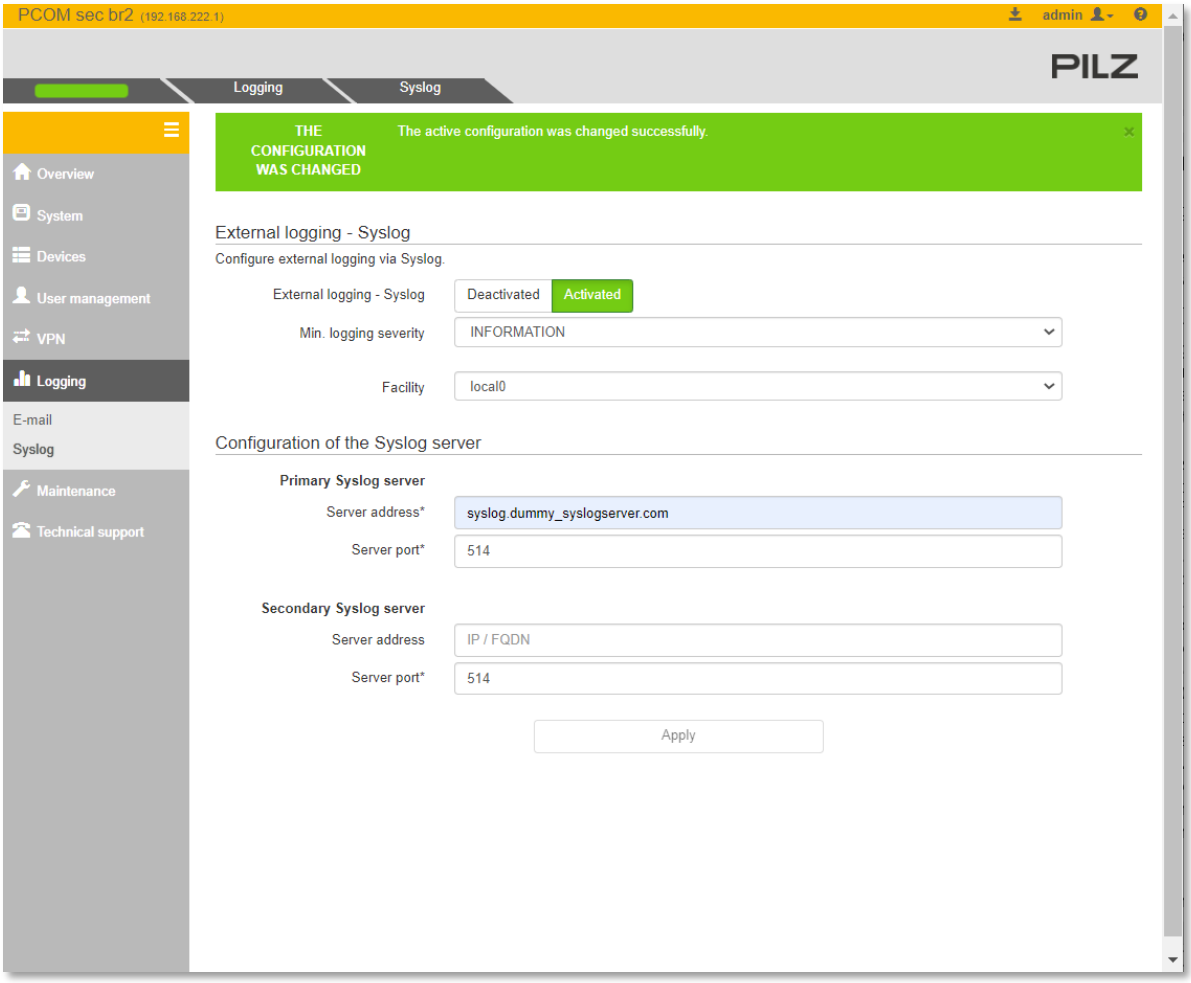

Figure 28: PCOM sec br2 – Changes successful

7 Table of figures

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 21 60880878-216
Japan
+81 45 471-2281
South Korea
+82 31 778 3300

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-0
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Turkey
+90 216 5775552
United Kingdom
+44 1536 462203

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUEcoMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY