SAIA BURGESS CONTROLS

Saia PCD® Supervisor

Security Manual

Document 26-624 | Edition ENG03 | 2019-11-21

0

0

0.1 Document History

Version	Published	Changes	Comments
ENG01	2019-07-01	whole document	- Extract from Manual 27-651 ENG01
ENG02	2019-07-02	3.13	- New subchapter “Setting up Google 2 factor authentication”
ENG03	2019-11-21	3.15	- New Sub-chapter added: General Data Protection Regulation (GDPR)

0.2 Trademarks

Saia PCD® is a registered trademark of Saia-Burgess Controls AG.

Technical changes are subject to the state of technology.

Published in Switzerland

3 Securing Saia PCD® Supervisor

3.1 Introduction

The purpose of this section is to provide the information necessary for those involved in the installation and maintenance of a product or system to understand the requirements for configuring and managing the security of the product or system.

General Security Best Practice for Saia Burgess Controls IP Based Product manuals „26-776_Manual_TCP-IP-Ethernet“ and „26-867_Manual_TCP-IP-Enhancements“.

Both documents are available from the Saia Burgess Controls support web site www.sbc-support.com.

3.2 Disaster Recovery Planning

It is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, specifies procedures an organization is to follow in the event of a disaster.

When developing the disaster recovery plan ensure that it includes ALL data required to restore system operation, including:

- Configuration files for platform(s) and station(s)
- Database objects
- License and certificate files
- Station Backup
- Station Copies

See book 27-651 chapter *“6.8 Backup&Restore”* for details.

3.3 Physical and Environmental Considerations

The PC running Saia PCD® Supervisor should, where possible, be secured against unauthorised physical access.

3.4 Security Updates and Service Packs

Ensure the PC running Saia PCD® Supervisor and any client devices have the latest operating system updates installed, and the latest version of Saia PCD® Supervisor is being used.

Saia Burgess Controls software is tested against the latest service packs and updates applicable at the time of release. For significant operating system and Java updates / service packs, please check the Saia Burgess Controls support web site www.sbc-support.com for any compatibility issues.

3.5 Virus Protection

Ensure the PC running Saia PCD® Supervisor and any client devices are running virus protection software, and the virus definitions are kept up-to-date.

Some virus protection software may have an adverse impact on the performance of Saia PCD® Supervisor. In such cases request that the Saia PCD® Supervisor directory be excluded from on-access scan.

Further details can be found on the Saia Burgess Controls support web site www.sbc-support.com.

3.6 Network Planning and Security

It is recommended that the Ethernet network used by the Building Management System (BMS) is separated from the normal office network using an air gap (separated wiring and devices or layer 3 switches or virtual private network (VPN)). Physical access to the Ethernet network infrastructure must be restricted. You must also ensure that the installation complies with your company's IT policy.

The use of a firewall and Intrusion Detection System (IDS) from a reputable provider of security products is recommended for any Saia PCD® Supervisor installation. Follow best practice for the products chosen as well as any corporate IT policy where the installation is made. Lock down the products to the particular port you've configured for Saia PCD® Supervisor HTTPS and HTTP.

Always follow the guidelines PDF-Documents:

manual	26-776_Manual_TCP-IP-Ethernet
manual	26-867_Manual_TCP-IP-Enhancements.
manual	26-620_Manual_Security-Rules
manual	Niagara^{AX} Hardening Guide
instruction	30-002_Internet-Security-Instructions_SBC
instruction for using VPN router	30-004_VPN-Router

You must also take steps to ensure the security of any other networks connected to Saia PCD® Supervisor (e.g. BACnet).

3.7 Virtual Environments

Follow best practice for the products chosen as well as any corporate IT policy where the installation is made.

3.8 Securing Wireless Devices

If a wireless network is being used it must be secured according to your company's IT policy.

3.9 System Monitoring

For any Saia PCD® Supervisor installation, especially when connected to the internet, Saia Burgess Controls recommends the use of an Intrusion Detection System (IDS) from a reputable provider of security products. Follow best practice for the products chosen as well as any corporate IT policy where the installation is made.

Saia PCD® Supervisor logs (Audit History) changes made to its own configuration and adjustments to the Saia Burgess Controls control system. Many IDS and firewall products offer a complete solution for recording all the traffic coming in and out of the Saia PCD® Supervisor PC, providing users with the ability to record all activity at the lowest level.

3.10 Securing Access to the Operating System

Ensure the PC running the Saia PCD® Supervisor and any PCs used for Saia PCD® Supervisor clients are secured according to your company's IT policy.

3.11 Access Control

All Saia PCD® Supervisor files should be protected from read and write access by people and software not authorized. Saia Burgess Controls recommends following best practice for securing system objects, such as files, and using access control appropriately.

If Windows users are granted access to the filing system location of the Saia PCD® Supervisor project then it is possible for them to inadvertently (or deliberately) open, delete or edit any of the configuration and data files of independently of their Saia PCD® Supervisor workgroup settings.

3.12 Securing Saia PCD® Supervisor

The Saia PCD® Supervisor software should be configured during installation and operation following best practice. Follow the installation procedure as described in this manual. In addition, refer to the Niagara 4 help system and Niagara 4 security guidelines.

3.12.1 Default Admin User of a Station

Initial system configuration is achieved using a default admin/engineering user account which is set up with a strong password when a Station is created.

3.12.2 Passphrase

The passphrase, specified during the Saia PCD® Supervisor installation process, protects sensitive data on any station that you create and will be required if the Saia PCD® Supervisor station is to be moved to another PC e.g. moved to the site PC, or restored after a PC failure.

3.12.3 Set up Other Users for the Station

Once configuration is complete (using the default admin user) further user accounts must be added that grant different users specific access rights according their role. Saia PCD® Supervisor enforces the use of strong passwords.

For further details, see book 27-651 chapter 7 *"Using Saia PCD® Supervisor"*

3.13 Setting up Google 2 factor authentication

The Google Authentication Scheme is a two-factor authentication mechanism that requires the user to enter their password as well as a single-use token when logging in to a station. This protects a user's account even if their password is compromised.

This authentication scheme relies on TOTP (Time-based One Time Password) and the Google Authenticator app on the user's mobile device to generate and verify single-use authentication tokens. Google authentication is time based, so there is no dependency on network communication between the user's mobile device, the Station, or external Servers. Since the authenticator is time based, the time in the station and time in the phone must stay relatively in sync. The app provides a buffer of plus or minus 1.5 minutes to account for clock skew.

Prerequisites:

- The user's mobile phone requires the Google Authentication app.
- You are working in Workbench.
- The user exists in the station database.

Perform the following steps:

1. Open the GAuth palette and add the **GoogleAuthenticationScheme** to the **Services > Authenticationservice** node in the Nav tree.
2. Right-click **Userservice**, and double-click the user in the table.
   The Edit view for the user opens.
3. Configure the *Authentication Scheme Name* property to *GoogleAuthenticationScheme* and click **Save**.
4. Click the button next to *secret Key* under the user's authenticator and follow the prompts.
5. To complete the configuration, click **Save**.
   Depending upon the view you are using, you may have to open the user again or refresh after saving.

3.14 Saia PCD® Supervisor Security Check List

- ❑ Latest version of Saia PCD® Supervisor is being used.
- ❑ Saia PCD® Supervisor installation files, configuration files (including station back-up), certificates and licenses are included in disaster recovery plan.
- ❑ The PC running Saia PCD® Supervisor should, where possible, be secured against unauthorized physical access.
- ❑ The Ethernet network (and any other networks) that the PC is connected to is secured, e.g. by the use of firewalls and intrusion detection systems.
- ❑ The PC is running the latest version of the Windows operating system, with all updates and service packs.
- ❑ The PC is running virus protection software.
- ❑ Appropriate user accounts are set up on PC and access to files is restricted to only those who are authorized.
- ❑ Saia PCD® Supervisor is configured to use HTTPS using a certificate from a trusted Certificate Authority.
- ❑ Saia PCD® Supervisor users are configured as required.
- ❑ Ensure Saia PCD® Supervisor is configured to backup data regularly to a secure location as per your company's backup policy.

3.15 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR contains provisions and requirements related to the processing of personal data of individuals (data subjects) inside the EEA, and applies to any enterprise established in the EEA or (regardless of its location and the data subjects' citizenship) that is processing the personal information of data subjects inside the EEA.

Under the terms of the GDPR personal data includes any information that may be used to identify an individual. This includes (but is not limited to):

- user names,
- passwords,
- phone numbers,
- email addresses,
- work or residential addresses.

Any such information entered into Saia PCD® Supervisor is encrypted and stored on the PC where the Saia PCD® Supervisor application is installed on a customer's premises. Neither Honeywell or Saia Burgess Controls have any involvement with the storage and/or processing of personal data within Saia PCD® Supervisor.

Responsibility for compliance with the requirements of the GDPR lies fully with the system integrator or system administrator and, as such, they must ensure that adequate technical and organisational systems are in place to:

- obtain explicit consent from each data subject for personal data to be stored, used and/or processed,
- allow individuals to have access to their personal data in order to verify accuracy,
- allow individuals to withdraw their consent at any time and to have their personal data to be permanently erased,
- maintain the security and integrity of data storage and access at all times,
- report any breaches of data security (that may affect user privacy) to the relevant authority within 72 hours of the breach occurring.

3

A Annex

A.1 Icons

In manuals, this symbol refers the reader to further information in this manual or other manuals or technical information documents. As a rule there is no direct link to such documents.

This sign accompanies instructions that must always be followed.

A.2 Sofware-Versions

Book-Version	Extract from Book-Version	Saia PCD® Supervisor	Niagara
26-624 ENG01	**27-651 ENG01**	Version V1.1	Based on Niagara V4.3
26-624 ENG02	**27-651 ENG02**	Version V1.2	Based on Niagara V4.7
26-624 ENG03	**27-651 ENG05**	Version V2.0	Based on Niagara V4.7U1

A

A.3 Contact

Saia-Burgess Controls AG
Bahnhofstrasse 18
3280 Murten
Switzerland

Phone..... +41 26 580 30 00
Phone support..... +41 26 580 31 00
Fax..... +41 26 580 34 99

Email support: ..... support@saia-pcd.com
Supportsite: ..... www.sbc-support.com
SBC site: ..... www.saia-pcd.com

International Represetatives &
SBC Sales Companies: ..... www.saia-pcd.com/contact

Saia Burgess Controls Technical Support are only able to provide support for Saia PCD® Supervisor and the Saia Burgess Controls driver features described in this manual. They are unable to provide support for 3rd party drivers and undocumented aspects of Saia PCD® Supervisor's operation.

Technical Publications
Please send any comments on this or any other Saia Burgess Controls technical publication to support@saia-pcd.com.

A