Saia PCD® Supervisor

Manuel de sécurité

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

0

0

0.1 Historique du document

Version	Date de publication	Modifications	Commentaires
FRA01	2019-07-01	Document entier	- Extrait du manuel 27-651 FRA01
FRA02	2019-07-02	Chaptre 3.13	- Nouveau sous-chapitre: « Configuration de l'authentification à 2 facteurs Google »
FRA03	2019-11-21	Chaptre 3.15	- Nouveau sous-chapitre: « Règlement général sur la protection des données (RGPD) »

0.2 Marques de commerce

Saia PCD® est une marque déposée de Saia-Burgess Controls AG.

Les modifications techniques sont soumises à l'état actuel de la technique.

Publié en Suisse

3 Sécurisation du Saia PCD® Supervisor

3.1 Introduction

Cette section fournit les informations requises aux personnes en charge des opérations d'installation et de maintenance d'un produit ou d'un système afin de comprendre les exigences de configuration et de gestion de la sécurité du produit ou système concerné.

Bonnes pratiques de sécurité générale pour les produits IP de Saia Burgess Controls (26-776_Manual_TCP-IP-Ethernet et 26-867_Manual_TCP-IP-Enhancements).

Ces deux documents sont disponibles sur le site Web d'assistance de Saia Burgess Controls www.sbc-support.com.

3.2 Plan de reprise après sinistre

Il s'agit d'un processus documenté ou d'un ensemble de procédures destinées à récupérer et à protéger une infrastructure informatique professionnelle en cas de sinistre. Ce plan définit les procédures qu'une organisation doit respecter en cas de sinistre.

Lors de la définition d'un plan de reprise après sinistre, vérifiez qu'il inclut TOUTES les données requises pour rétablir le fonctionnement du système, notamment :

- Les fichiers de configuration pour le(les) plates-forme(s) et la(les) station(s)
- Les objets de la base de données
- Les fichiers de licences et de certificats
- La sauvegarde des stations
- Les copies des stations

Pour plus d'informations, consultez le manuel 27-651
au chapitre « *6.8 Sauvegarde et restauration* ».

3.3 Considérations physiques et environnementales

Le PC qui exécute le Saia PCD® Supervisor doit, dans la mesure du possible, être protégé contre tout accès physique non autorisé.

3.4 Mises à jour de sécurité et packs de services

Vous devez vérifier que les dernières mises à jour du système d'exploitation sont installées sur le PC qui exécute le Saia PCD® Supervisor et les dispositifs clients et que la dernière version du Saia PCD® Supervisor est utilisée.

Le logiciel Saia Burgess Controls a été testé avec les derniers packs de services et mises à jour applicables à sa date de commercialisation. Pour les mises à jour/packs de services importants du système d'exploitation et de Java, consultez le site Web d'assistance de

Saia Burgess Controls www.sbc-support.com en cas de problèmes de compatibilité.

3.5 Protection contre les virus

Vérifiez que le PC qui exécute le Saia PCD® Supervisor et les dispositifs clients sont dotés d'un logiciel antivirus et que les définitions des virus sont actualisées.

Certains logiciels antivirus peuvent affecter les performances du Saia PCD® Supervisor. Vous devez alors demander d'exclure le répertoire du Saia PCD® Supervisor du balayage effectué à l'accès.

Pour plus d'informations, consultez le site Web d'assistance de Saia Burgess Controls www.sbc-support.com.

3.6 Planification et sécurité du réseau

Il est recommandé de séparer le réseau Ethernet utilisé par le système de gestion des bâtiments (*Building Management System*, BMS) du réseau bureautique normal au moyen d'un entrefer (câblage et dispositifs séparés ou commutateur de couche 3 ou réseau privé virtuel (*Virtual private network*, VPN)). L'accès physique à l'infrastructure du réseau Ethernet doit être limité. Vous devez également vérifier que l'installation respecte la politique informatique de votre société.

L'utilisation d'un pare-feu et d'un système de détection des intrusions (*Intrusion Detection System*, IDS) conçus par un fournisseur de produits de sécurité renommé est recommandée pour toute installation du Saia PCD® Supervisor. Vous devez respecter les bonnes pratiques des produits choisis ainsi que la politique informatique de la société où l'installation est effectuée. Verrouillez les produits au niveau du port que vous avez configuré pour les protocoles HTTPS et HTTP du Saia PCD® Supervisor.

Respectez scrupuleusement les directives des documents PDF suivants :

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

Vous devez également prendre des mesures pour garantir la sécurité des autres réseaux connectés au Saia PCD® Supervisor (par exemple, BACnet).

3.7 Environnements virtuels

Vous devez respecter les bonnes pratiques des produits choisis ainsi que la politique informatique de la société où l'installation est effectuée.

3.8 Sécurisation des dispositifs sans fil

Si un réseau sans fil est utilisé, il devra être sécurisé conformément à la politique informatique de votre société.

3.9 Surveillance du système

Pour toute installation du Saia PCD® Supervisor, notamment si elle est connectée à Internet, Saia Burgess Controls recommande d'utiliser un IDS provenant d'un fournisseur de produits de sécurité renommé. Vous devez respecter les bonnes pratiques des produits choisis ainsi que la politique informatique de la société où l'installation est effectuée.

Le Saia PCD® Supervisor consigne (historique des audits) les modifications apportées à sa propre configuration et les ajustements effectués au système de commande Saia Burgess Controls. Plusieurs IDS et pare-feux offrent une solution complète pour l'enregistrement de l'ensemble du trafic en provenance et à destination du PC exécutant le Saia PCD® Supervisor en permettant aux utilisateurs d'enregistrer toutes les activités au niveau le plus bas.

3.10 Sécurisation de l'accès au système d'exploitation

Vérifiez que le PC qui exécute le Saia PCD® Supervisor et tous les PC utilisés pour les clients du Saia PCD® Supervisor sont sécurisés conformément à la politique informatique de la société.

3.11 Contrôle de l'accès

Tous les fichiers du Saia PCD® Supervisor doivent être protégés en lecture et en écriture pour empêcher les personnes et les logiciels non autorisés d'y accéder. Saia Burgess Controls recommande de respecter les bonnes pratiques de sécurisation des objets du système, tels que les fichiers, en utilisant la fonction de contrôle de l'accès de manière appropriée.

Si les utilisateurs Windows bénéficient d'un accès à l'emplacement du système d'archivage du projet du Saia PCD® Supervisor, ils peuvent ouvrir, supprimer ou modifier involontairement (ou délibérément) les fichiers de configuration et de données indépendamment de leurs paramètres de groupe de travail Saia PCD® Supervisor.

Sécurisation du Saia PCD® Supervisor

3.12 Sécurisation du Saia PCD® Supervisor

Le logiciel Saia PCD® Supervisor doit être configuré pendant l'installation et l'utilisation en respectant les bonnes pratiques. Respectez la procédure d'installation décrite dans ce manuel. Vous pouvez également consulter l'aide et les instructions de sécurité de Niagara 4.

3.12.1 Utilisateur Admin par défaut d'une station

La configuration initiale du système est effectuée au moyen d'un compte utilisateur d'administration/d'ingénierie par défaut configuré lors de la création d'une station.

3.12.2 Phrase secrète

La phrase secrète, définie pendant le processus d'installation du Saia PCD® Supervisor, protège les données sensibles des stations que vous créez et sera requise si la station Saia PCD® Supervisor est déplacée vers un autre PC (par exemple, déplacée vers le PC du site ou restaurée après une défaillance du PC).

3.12.3 Configuration des autres utilisateurs pour la station

Une fois la configuration terminée (au moyen de l'utilisateur Admin par défaut), d'autres comptes utilisateur doivent être ajoutés en accordant des droits d'accès spécifiques aux utilisateurs en fonction de leur rôle. Le Saia PCD® Supervisor exige d'utiliser des mots de passe forts.

Pour plus d'informations, consultez le manuel 27-651
au chapitre « *7 Utilisation du Saia PCD® Supervisor* ».

3.13 Configuration de l'authentification Google à 2 facteurs

Le schéma d'authentification de Google est un mécanisme d'authentification à deux facteurs qui oblige l'utilisateur à entrer son mot de passe ainsi qu'un jeton (token) à usage unique lorsqu'il se connecte à une station. Cela protège le compte d'un utilisateur même si son mot de passe est compromis.

Ce schéma d'authentification repose sur TOTP (mot de passe à utilisation unique basée sur le temps) et sur l'application Google Authenticator sur le périphérique mobile de l'utilisateur pour générer et vérifier des jetons (token) d'authentification à usage unique. L'authentification Google étant basée sur le temps, il n'ya aucune dépendance sur la communication réseau entre le périphérique mobile de l'utilisateur, la station ou des serveurs externes. Comme l'authentificateur est basé sur l'heure, l'heure dans la station et l'heure dans le téléphone doivent rester relativement synchronisées. L'application fournit un tampon de plus ou moins 1,5 minute pour tenir compte du décalage d'horloge.

Conditions préalables :

Le téléphone mobile de l'utilisateur nécessite l'application Google Authentication.

Vous travaillez dans Workbench.

- L'utilisateur existe dans la base de données de la station.

Effectuez les étapes suivantes :

1. Ouvrez la palette GAuth et ajoutez le programme **GoogleAuthenticationScheme** au nœud **Services > Authenticationservice** de l'arborescence de navigation.
2. Cliquez avec le bouton droit de la souris sur **Userservice** et double-cliquez sur l'utilisateur dans la table.
   La vue Edition de l'utilisateur s'ouvre.
3. Configurez la propriété *Authentication Scheme Name* à *GoogleAuthenticationScheme* et cliquez sur **Save** « Enregistrer ».
4. Cliquez sur le bouton situé à côté de *secret Key* sous l'authentificateur de l'utilisateur et suivez les instructions.
5. Pour terminer la configuration, cliquez sur **Save** « Enregistrer ».
   Selon l'affichage que vous utilisez, vous devrez peut-être rouvrir l'utilisateur ou actualiser après l'enregistrement.

3.14 Liste de contrôle de sécurité du Saia PCD® Supervisor

- ❑ La dernière version du Saia PCD® Supervisor est utilisée.
- ❑ Les fichiers d'installation, les fichiers de configuration (y compris la sauvegarde de la station), les certificats et les licences du Saia PCD® Supervisor sont inclus dans le plan de reprise après sinistre.
- ❑ Le PC qui exécute le Saia PCD® Supervisor doit être, dans la mesure du possible, protégé contre tout accès physique non autorisé.
- ❑ Le réseau Ethernet (et les autres réseaux) auquel le PC est connecté est sécurisé (par exemple, au moyen de pare-feux et de systèmes de détection des intrusions).
- ❑ Le PC exécute la dernière version du système d'exploitation Windows avec l'ensemble des mises à jour et des packs de services.
- ❑ Le PC exécute un logiciel antivirus.
- ❑ Les comptes utilisateur appropriés sont configurés sur le PC et l'accès aux fichiers est exclusivement réservé aux personnes autorisées.
- ❑ Le Saia PCD® Supervisor est configuré pour utiliser le protocole HTTPS en utilisant un certificat provenant d'une autorité de certification de confiance.
- ❑ Les utilisateurs du Saia PCD® Supervisor sont configurés tel que requis.
- ❑ Vérifiez que le Saia PCD® Supervisor est configuré pour sauvegarder les données régulièrement dans un emplacement sûr conformément à la politique de sauvegarde de votre société.

3.15 Règlement général sur la protection des données (RGPD)

Anglais: General Data Protection Regulation (GDPR)

Le règlement général sur la protection des données (UE) 2016/679 (RGPD) est un règlement de la législation de l'UE sur la protection des données et de la vie privée pour tous les citoyens de l'Union européenne (UE) et de l'Espace économique européen (EEE). Il traite également du transfert de données à caractère personnel hors des zones de l'UE et de l'EEE. Le RGPD contient des dispositions et des exigences relatives au traitement des données personnelles des individus (sujets de données) au sein de l'EEE et s'applique à toute société établie dans l'EEE ou (indépendamment de son emplacement et de la nationalité de la personne concernée) qui traite les données personnelles des sujets de données au sein de l'EEE.

Selon les termes du GDPR, les données personnelles comprennent toute information pouvant être utilisée pour identifier une personne. Cela comprend (mais ne sont pas limités à):

noms d'utilisateur,

mots de passe,

numéros de téléphone,

adresses e-mail,

- adresses professionnelles ou résidentielles.

Toutes les informations saisies dans Saia PCD® Supervisor seront cryptées et stockées sur le PC où l'application Saia PCD® Supervisor est installée sur le site du client. Ni Honeywell ni Saia Burgess Controls ne sont impliqués dans le stockage et/ou le traitement des données à caractère personnelles au sein de Saia PCD® Supervisor.

La responsabilité de la conformité aux exigences du RGPD incombe entièrement à l'intégrateur de système ou à l'administrateur de système, qui doit donc veiller à ce que des systèmes techniques et organisationnels adéquats soient en place pour:

obtenir le consentement explicite de chaque personne concernée pour que les données à caractère personnel soient stockées, utilisées et / ou traitées,

permettre aux individus d'avoir accès à leurs données personnelles afin de vérifier leur exactitude,

permettre aux individus de retirer leur consentement à tout moment et d'effacer définitivement leurs données personnelles,

maintenir la sécurité et l'intégrité du stockage et de l'accès aux données en tout temps,

signaler toutes les violations de données (qui peuvent affecter la vie privée des utilisateurs) à l'autorité compétente dans les 72 heures suivant la survenue d'une violation.

3

A Annexe

A.1 Icônes

Dans les manuels, ce symbole sert à renvoyer le lecteur vers d'autres informations contenues dans le même document ou dans d'autres guides ou documents d'informations techniques. En règle générale, vous ne bénéficierez d'aucun lien d'accès direct à ces documents.

Ce symbole accompagne des instructions qui doivent être scrupuleusement respectées.

A.2 Versions du logiciel

Version du livre	Extrait du manuel	Saia PCD® Supervisor	Niagara
27-624 FRA01	**27-651 FRA01**	Version V1.1	Basé sur Niagara V4.3
27-624 FRA02	**27-651 FRA02**	Version V1.2	Basé sur Niagara V4.7
27-624 FRA03	**27-651 FRA05**	Version V2.0	Basé sur Niagara V4.7U1

A

A.3 Informations de contact

Saia-Burgess Controls AG
Bahnhofstrasse 18
3280 Murten
Suisse

Téléphone ..... +41 26 580 30 00
Téléphone de l'assistance technique..... +41 26 580 31 00
Fax ..... +41 26 580 34 99

Email de l'assistance technique : ..... support@saia-pcd.com
Site de l'assistance technique : ..... www.sbc-support.com
Site SBC : ..... www.saia-pcd.com

Représentants internationaux et
sociétés commerciales SBC : ..... www.saia-pcd.com/contact

L'assistance technique de Saia Burgess Controls fournit une assistance uniquement pour le Saia PCD® Supervisor et pour les fonctions du pilote Saia Burgess Controls décrits dans ce manuel. Elle ne fournit aucune assistance technique pour les pilotes tiers et les aspects non documentés du fonctionnement du Saia PCD® Supervisor.

Publications techniques
Vous pouvez envoyer vos commentaires sur cette publication technique ou sur toute autre publication de Saia Burgess Controls à l'adresse suivante : support@saia-pcd.com.

A