System Hardening Guidelines for Wiser for KNX and spaceLYnk Controllers LSS100100 LSS100200

Application Note

This application note outlines essential instructions for enhancing the security and robustness of your Wiser for KNX and spaceLYnk controllers.

AN 107.2.0

Basic / Intermediate / Expert

Release date 04/2024

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety information

Important information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that accompany this symbol to avoid possible injury or death.

⚠⚠DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Safety Notice: Electrical Equipment Handling

Electrical equipment is critical for various applications, but it must be handled with care and expertise. Please adhere to the following guidelines:

1. **Qualified Personnel Only:**
   - Installation, operation, servicing, and maintenance of electrical equipment should be carried out exclusively by qualified personnel.
   - A qualified person possesses the necessary skills and knowledge related to the construction, installation, and operation of electrical systems.
   - Such individuals have also received safety training to recognize and mitigate potential hazards.
2. **Schneider Electric Disclaimer:**
   - Schneider Electric assumes no responsibility for any consequences arising from the use of this material.
   - Users must exercise caution and follow best practices when dealing with electrical equipment.

Safety Precautions

⚠WARNING

HAZARD OF INCORRECT INFORMATION

- Do not incorrectly configure the software, as this can lead to incorrect reports and/or data results.
- Do not base your maintenance or service actions solely on messages and information displayed by the software.
- Do not rely solely on software messages and reports to determine if the system is functioning correctly or meeting all applicable standards and requirements.
- Consider the implications of unanticipated transmission delays or failures of communications links.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Introduction

The Wiser for KNX and spaceLYnk controllers serve as freely programmable logic controllers, playing diverse roles in various integration scenarios.

To ensure maximum security, it is crucial to understand how to configure these controllers effectively.

This system hardening guideline outlines best practices that you can apply to your projects.

> **NOTE:** Throughout this document, the term “controller” refers to both Wiser for KNX and spaceLYnk unless specified otherwise.

Controller Security Measures

Passwords

Passwords should include a combination of:

- Upper case letters
- Lower case letters
- Numbers
- Special characters

The password must have a minimum of 8 characters.

- Avoid easily guessable passwords; consider using phrases.
- Change passwords periodically (at least once a year).
- Immediately change the default Admin password upon initial receipt or after a factory reset.
- Never reuse passwords across different systems.
- After the first login, change the default password for local access.

IMPORTANT: Make sure to securely store your password. In the event of password loss, you will lose the ability to modify controller configurations, install new plugins, and perform other essential tasks.

General Configuration

For enhanced security, we strongly recommend enabling the blocking of unsafe functions within your controller scripts. These functions have the potential to cause harm. Follow these steps to activate the feature:

1. Log in to your controller.
2. Navigate to **Configurator** > **Utilities** > **General configuration**.
3. Enable the option labeled **Block unsafe functions in scripts**.

By enabling this setting, the following functions will be blocked in your scripts:

- io.output
- io.readfile
- io.input
- io.lines
- io.open
- io.popen
- io.readproc
- io.tmpfile
- io.write
- io.writefile
- os.execute
- os.kill
- os.remove
- os.removepid
- os.rename
- os.symlink

- os.tmpname
- os.writepid

Take this precaution to safeguard your system from potential risks associated with these functions.

Project Backups

Remember to **create a project backup** after each configuration change and store it in a secure location.

Additionally, ensure that you have the **project password readily available** in case it is needed, as project backups cannot be retrieved without the valid password set at the time of backup.

User Access Settings

To harden the security of your system, we recommend configuring the following settings within the **User access** section of your controller:

1. **Disable password for Visualization**:
   - Activating this option allows you to access basic controller plugins (such as **PC/Tablet**, **Smartphone**, **Scheduler**, and **Trends**) directly from the main page without a password.
   - However, we advise against activating this option or, at the very least, recommend setting a PIN code for visualization access (as mentioned in the **Visualization PIN code** paragraph below).
2. **Enable password for Applications**:
   - By default, this option is active. It ensures that a password (either administrator or user passwords) is mandatory for accessing all other plugins.
   - We recommend keeping this option enabled. Alternatively, consider limiting individual users' access to specific plugins through the **Configurator** (navigate to **User access** > **User** > **Applications**).
3. **Enable password for User directory**:
   - This option is enabled by default. Accessing the FTP (File Transfer Protocol) requires a password, which you can set in the **Configurator** under **System** > **Services** > **FTP Server** > **Password**.
   - We strongly recommend keeping this option enabled for security reasons.
4. **Visualization PIN code**:
   - Set a PIN code to access the four basic plugins (**PC/Tablet**, **Smartphone**, **Scheduler**, and **Trends**).
   - If you have also set a password for visualization (as mentioned in the **Disable password for Visualization** section), you will need to enter both the password and the PIN code to access these plugins.
5. **Remember login and password**:
   - By default, your browser remembers the login and password only while it remains open. If you close and reopen the browser, you will need to log in to the controller again.
   - Enabling this option allows the browser to remember login credentials. It creates a cookie that stores the login and password (whether administrator or user) and lasts for the specified number of days (as set in **User cookies expiration days**).

Network Configuration

Network Isolation:

- Use the controller exclusively within your personal home network.
- Ensure the controller does not have a publicly accessible IP address.
  A public IP address serves as an entry point for external cyber attacks, which can lead to severe consequences such as functional disruptions or complete system outages in your installation.
- Avoid using port forwarding to access the controller from the public internet.
- Ideally, place the controller on its own network segment.
  If your router supports a guest network or VLAN, consider locating the controller there.
- Utilize the strongest Wi-Fi encryption available.
- Implement HTTPs within the local network.

Controller Plugins and LMUP Files

Safe plugin downloads:

- Download plugins only from the Schneider Electric Marketplace accessible directly from the controller.
- Follow the steps outlined in the user guide's "*Application Store*" chapter.
- Avoid installing plugins or LMUP files from untrusted vendors, as they may introduce vulnerabilities or backdoors.
- Rely solely on Schneider Electric webpages for downloading scripts or controller firmware.
- Obtain LMUP files from trusted sources such as se.com website, Yammer, or The Exchange.

Connectivity

Voice Control

To enable or disable voice control, follow the steps outlined in the following application notes:

- Wiser for KNX Alexa voice control
- Google assistant integration in Wiser for KNX

VPN

- By default, VPN is enabled for Wiser for KNX.
- If you are not using the Wiser for KNX remote app, consider turning off your VPN connection in the controller. Refer to the user guide's *Remote Connectivity* chapter for detailed instructions.

Wiser for KNX and spaceLYnk Firmware

Always use the latest firmware:

- Ensure your controller runs the latest firmware to access new features, cybersecurity fixes, and improvements.
- Download the controller's firmware exclusively from Schneider Electric webpages:
  - Firmware for spaceLYnk
  - Firmware for Wiser for KNX
- For factory reset instructions, consult the user guide's *3.6 Factory Reset* chapter.
- To perform a partial project delete, refer to the *Reset / Clean-up* chapter.

Wiser for KNX Device

Secure placement:

- Ensure your Wiser for KNX device is securely placed in a **locked cabinet with restricted access**.

Wiser for KNX Plugins

Auto update feature:

- We strongly recommend enabling the auto-update feature for each plugin installed via the Marketplace.
- By doing so, you ensure that all functional and security patches are deployed automatically in an unattended mode.

System and Configuration Backups

- Create regular backups:
  - **Highly recommended**: Before performing any firmware or configuration updates, create backups of your current project and configuration.

- Utilize Schneider Electric cloud:
  - As soon as a new Management Plugin is released to the Marketplace, consider using project backups to the **Schneider Electric cloud**.
  - This ensures that your data is securely stored and easily accessible when needed.

5 Secure Disposal Guidelines

When disposing of Wiser for KNX/spaceLYnk controllers, follow these key steps to ensure data security and proper handling of the device:

1. **Backup project data:**
   - Before initiating the disposal process, back up your project data stored on the SD card.
   - This backup will serve as a reference for future needs or for transferring data to another controller.
2. **Dismantle device:**
   - Follow the **Product End of Life** instructions available at the following link: https://download.schneider-electric.com/files?p_Doc_Ref=ENVEOLI1305030&p_enDocType=Circularity+Profile&p_File_Name=ENVEOLI1305030EN.pdf.
3. **Secure storage of SD card:**
   - Store the SD card taken from the controller in a protected place.
   - Alternatively, consider physically damaging it to prevent any misuse of the data it contains.

By adhering to these guidelines, you can ensure the secure disposal of Wiser for KNX/spaceLYnk controllers while safeguarding data integrity and contributing to responsible waste management practices.

Trademarks

- Microsoft Windows®, Windows 10®, and Windows 11® are trademarks or registered trademarks of the Microsoft Corporation in the USA and/or other countries.
- iTunes® is a registered trademark of the Apple Inc. in the USA and/or other countries.
- Google Chrome™, Google Play™, Google Maps™, Google Assistant™, and YouTube™ are trademarks of the Google Inc. in the USA and/or other countries.
- Firefox® is registered trademark of the Mozilla Corporation in the USA and/or other countries.

Printed in:
Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison - France
+ 33 (0) 1 41 29 70 00

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

AN 107.2.0