SpaceLogic KNX BMS IP Gateway

LSS100300

User guide

LSS100300
Release date 07/2025

Schneider Electric

www.se.com

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 documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this 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 follow 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.

⚠ 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.

The addition of this 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 follow 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.

⚠ 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.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

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

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions,

government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

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

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.

- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

Document Scope

This document describes the LSS100300 **SpaceLogic KNX BMS IP Gateway** application software, device features, and user interface.

It is intended for system integrators, engineers, and technical users who are responsible for setting up communication between KNX systems and IP-based Building Management Systems (BMS).

Validity Note

This user guide is valid for the **SpaceLogic KNX BMS IP Gateway** software as of the software version specified in the document. It applies to the configuration and operation of the software features available at the time of publication.

Any future updates, enhancements, or changes to the software may not be reflected in this guide. Users are encouraged to consult the latest documentation or contact technical support for information regarding newer versions or additional functionalities.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Product Related Cybersecurity Information

- Network security must be configured appropriately. The Gateway should operate within a secure network with restricted access. If connected to the Internet, it is strongly recommended to use a **VPN** or an **HTTPS**-encrypted channel.
- Always access the Gateway using a secure protocol, such as `https://<IP>:<Port>`.

- The overall security level depends on the capabilities of other network components, such as firewalls and protection against viruses and malware.
- Backup files should be stored in a secure location, inaccessible to unauthorized individuals.
- Ensure that the Gateway does not have a publicly accessible IP address.
- Avoid using port forwarding to access the Gateway from the public Internet.
- The Gateway should be placed on a dedicated network segment to isolate it from other devices.
- If your router supports guest networks or VLANs, it is advisable to place the Gateway within such a segment for additional isolation.

You can read more on system hardening here: https://www.se.com/ww/en/download/document/AN002_107/.

Available Languages of the Document

The document is available in these languages:

- **English** (LSS100300_SW_EN)
- Chinese (LSS100300_SW_ZH)
- French (LSS100300_SW_FR)
- German (LSS100300_SW_DE)
- Italian (LSS100300_SW_IT)
- Spanish (LSS100300_SW_ES)

Related Documents

Title of documentation	Reference number
SpaceLogic KNX BMS IP Gateway, LSS100300, Installation and connection	LSS100300_HW
Wiser for KNX, SpaceLYnk - System Hardening Guideline	AN002_107

How to find documents online:

1. Go to www.se.com/ww/en/download/.
2. In the top left corner, select your **country** from the dropdown menu.
3. In the search bar, enter the **document name** or **reference number**.
4. Click the magnifying glass icon to start the search.
5. From the search results, select the **Documents** tab.
6. **Open the document** you need from the list.

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

Introduction

SpaceLogic KNX BMS IP Gateway (hereinafter referred to as Gateway) is a multifunctional device designed to integrate KNX installations with building automation systems.

Its primary communication interfaces are KNX TP and IP, with support for the **BACnet** protocol.

The Gateway combines three key components in a single device:

- KNX IP router (up to 500 objects)
- KNX IP interface
- DPSU choke

This integration allows professional installers to deploy KNX systems more efficiently in terms of both cost and time, thanks to the combination of features in one unit.

The system architecture is simplified, as there is no longer a need to use separate KNX routers and KNX power supplies, provided the installation meets the specified parameters.

The Gateway is intended for use in commercial installations.

Secure Remote Access via VPN

When accessing a KNX installation over the Internet, data traffic may be exposed to third parties. To ensure secure communication, the following precautions must be taken:

- Always use a VPN (Virtual Private Network) connection with strong encryption to protect all data packets.
- The required hardware (such as a VPN router) and the capabilities of mobile service providers can vary significantly depending on the country or region.
- VPN access should always be configured and commissioned by a qualified VPN service provider. The provider will select appropriate hardware and a suitable mobile service provider, and ensure that the VPN is set up by a certified specialist.

Schneider Electric is not responsible for performance issues or incompatibilities caused by third-party applications, services, or devices. Additionally, Schneider Electric does not provide technical support for VPN setup.

Failure to follow these guidelines may result in equipment damage.

A VPN allows a remote device to securely access the local network – and therefore the KNX installation – via the Internet.

Benefits of using a VPN

- Only authorized users can access the local network.
- All data is encrypted during transmission.
- Data remains intact and protected from interception, manipulation, or redirection – commonly referred to as a VPN tunnel.

Requirements for setting up a VPN connection

- An active Internet connection.
- A portable device and router that support VPN connections (with a VPN client installed).

- The Gateway should be placed on a dedicated network segment.
- If the router supports guest networks or VLANs, it is recommended to place the Gateway within such a segment.

Password Security Best Practices

- Your password should include a mix of uppercase and lowercase letters, numbers, and special characters.
- Use a minimum of 8 characters.
- Choose passwords that are difficult to guess or find in cybercriminal dictionaries.
- Prefer using passphrases instead of single words.
- Change your password regularly, at least once a year.
- Always change the default administrator password immediately after receiving it or performing a factory reset.
- Never reuse passwords across different accounts or systems.

Device Specification

Specification	Description	Note
Terminals, Interface	1 × RJ45 – ethernet 10BaseT/100BaseTx 1 × KNX TP 1 × Reset push-button	
Connectivity	IP LAN connection 10/100 Mbit KNX/EIB TP Bus	
LED indicators	2 × LED, CPU, (Operation + Reset)	
KNX IP routing	500 objects (automatically disabled when over this limit)	You can use up to 4000 BACnet points. See Performance, page 16.
KNX IP tunneling	For commissioning of KNX devices via ETS	
KNX TP limitation	The bandwidth limit of the KNX TP medium is limited to 9.6 kbits/s. Between 20 – 40 telegrams per second can be transferred on each single KNX TP line.	
OS (firmware)	Flashsys	
Applications	Embeded configuration application with webserver.	
IP interface setting	By default – static IP 192.168.0.10/255.255.255.0	
BACnet Protocol Revision	22	
BACnet Device Profile	B – ASC, B – GW	

Compatibility

The Gateway is compatible with the following standards:

- KNX/EIB TP
- KNXnet/IP
- BACnet IP

Performance

Number of BACnet objects	4000	Maximum number of points that can be defined in the virtual BACnet device inside the Gateway. Objects exceeding limit are silently discarted.
Number of BACnet subscriptions (COV) requests	4000 (1500*)	Maximum number of BACnet subscriptions (COV) requests accepted by the Gateway.
KNX group objects	4000	Maximum number of different KNX group addresses that can be imported/defined.

*BACnet COV support provides fast data communication while reducing BACnet network traffic.

*1500 for SXWAUTSVR10001 – Automation server by Schneider Electric.

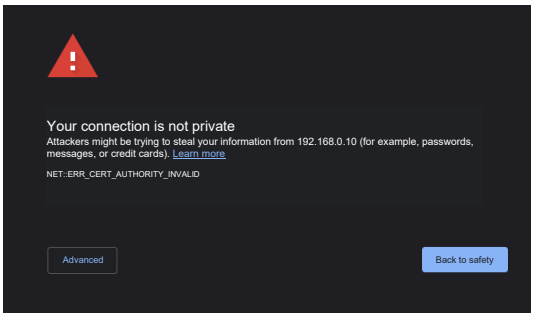
Getting Started

Before you begin, ensure that the Gateway is properly connected according to the installation instructions.

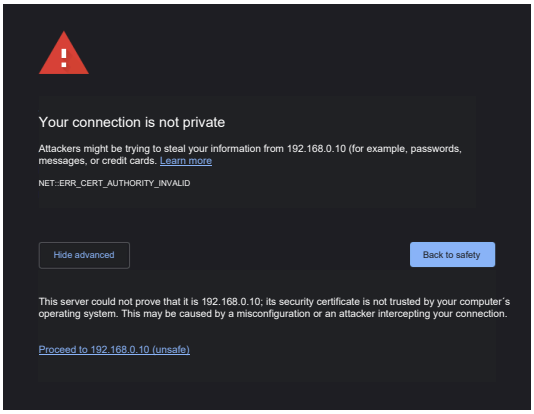
To configure the Gateway, you will need a standard web browser. We recommend using Google Chrome or Mozilla Firefox for the best experience.

First-Time Access Steps:

1. Open your browser and enter the default IP address: 192.168.0.10. Press **Enter**.
2. Since the Gateway uses a self-signed certificate, your browser will likely display a warning that the connection is not private.



3. Proceed anyway by clicking **Advanced** and then proceed to 192.168.0.10. The Gateway uses HTTPS to ensure encrypted communication between your browser and the device.



4. Sign in using the default credentials and click **Enter**.

   login: `admin`

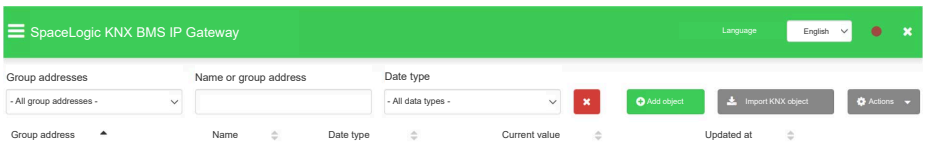
   password: `admin`

5. You will be prompted to change your password (Password Security Best Practices, page 13). Enter a new password and click **Save**.

   Your new password must include at least:

   - 8 characters
   - One uppercase letter
   - One lowercase letter
   - One digit

6. After signing in, you will be taken to the start page:



There you can:

- Select your preferred language (top right corner)
- Access Gateway settings via ☰
- Use object filters and tools
- Click the **Import KNX project** button

In the next steps, you will import your KNX project and configure the device parameters.

Importing a KNX Project

The **Import KNX project** button in the top-left corner of the interface, allows you to upload a `.knxproj` file directly to the Gateway. The import process preserves:

- The project structure
- Group address DPTs (Data Point Types)
- Units and suffixes

NOTE: Objects with identical names are treated as duplicates and may be discarded during the import.

You can also import objects without predefined data types and assign structure-level names to them if needed.

If your `.knxproj` file is password-protected, you must enter the password set in ETS. The project cannot be imported without it.

KNX Secure Devices handling

During the import, the Gateway preserves the **identification of KNX secure devices** included in the project. This affects how the Gateway processes the telegrams.

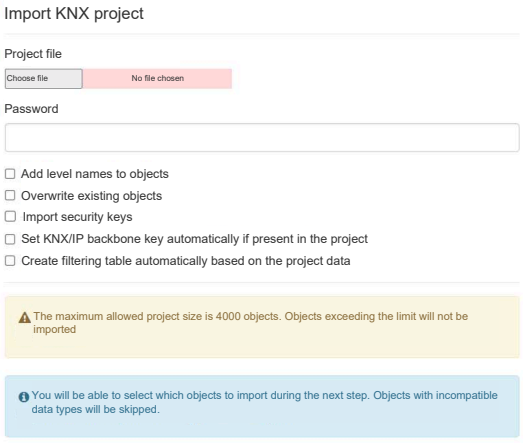
- **Secure telegrams** from secure devices are accepted only on secure group addresses.
- **Non-secure telegrams** sent to **secure group addresses** are **rejected** by the Gateway for security reasons.
- On **non-secure group addresses**, the Gateway accepts telegrams from **any non-secure source**.

This ensures that secure communication remains protected while allowing open communication on non-secure channels.

How to Import a KNX Project

1. Click the **Import KNX project** button and select your `.knxproj` file.
2. If prompted, enter the correct password.
3. (Optional) Check **Add level names to objects** if you want to include object names and their structure locations.
4. (Optional) Check **Overwrite existing objects** if you want to replace any existing objects in the Gateway.
5. To enable secure communication with KNX Secure devices, it is recommended to check the **Import security keys** option. This step is crucial, as it allows the Gateway to import the necessary encryption keys directly from the ETS project. These keys are linked to specific group addresses, enabling the gateway to correctly interpret and enrich KNX telegrams with the required security information for proper operation.
6. (Optional) Check **Create filtering table automatically based on the project data** to let the Gateway generate a filtering table using the imported group addresses. This helps optimize performance and security by allowing only relevant group addresses to be processed.
7. (Optional) Check **Set filtering policy to Accept selected group addresses** to ensure that only the group addresses defined in the project will be accepted by the Gateway.

8. Click **Next** to proceed.



Once imported, the filtering tables are automatically populated based on the KNX project and can be adjusted as needed. The backbone key is also imported automatically.

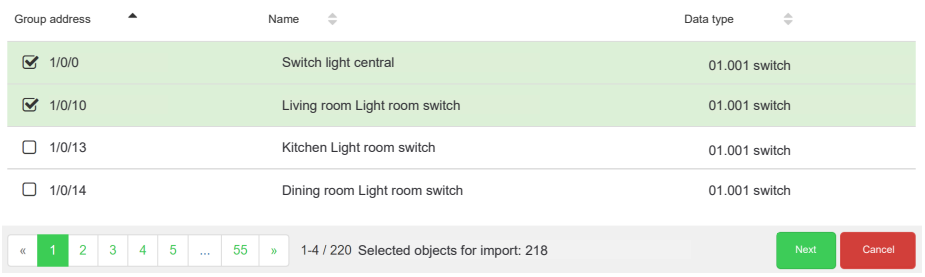
NOTE: KNX routing is not supported for projects containing more than 500 objects.

Selecting Objects for BACnet Export

In the next step, you'll choose which KNX objects to import to the Gateway. Only the selected objects will be added to the Gateway database.

You can filter objects by name, group address, or data type to simplify selection. For more details, see Filtering and Editing Object Properties, page 23.

1. Select the objects you want to export and click **Next**.



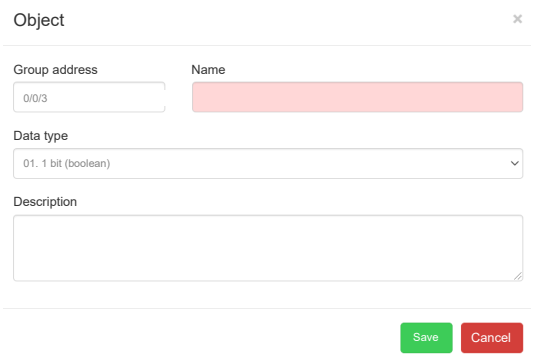
2. A pop-up window will confirm how many objects are being imported.
3. Click **OK** to complete the import process.

Adding an Object

The **Add object** feature is useful when you want to manually add a single object without re-importing the entire `.knxproj` file.

To add a new object:

1. Click the **Add object**.



2. Fill in the required object details, such as name, group address, data type, and any additional parameters.
3. Click **Save** to confirm and add the object to the list.

Actions

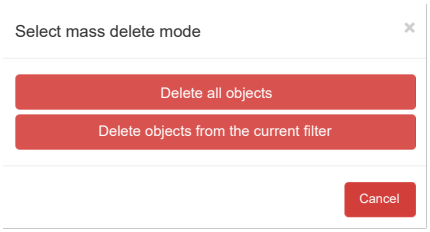
Mass Deleting Objects

The **Mass delete** feature allows you to quickly remove multiple objects from the Gateway database in one action.

You can choose between two options:

- **Delete all objects** – removes every object from the database.
- **Delete objects from the current filter** – removes only the objects currently displayed based on your filter settings.

After selecting your preferred option, the system will proceed to delete the objects accordingly.



TIP: Use filters to narrow down your selection before using mass delete, especially if you only want to remove specific groups of objects.

Mass Editing Objects

The **Mass edit** feature allows you to quickly update the units and COV (Change of Value) increment for multiple objects at once.

To edit objects in bulk:

1. Use the filter to display the objects you want to modify.
2. Click **Actions** > select **Mass edit** from the dropdown menu.
3. Choose the parameters you want to update:
   - **Units**
   - **COV increment value**
4. Click **Save** to apply the changes to all selected objects.

Exporting Objects to CSV

You can easily export all objects to a `.csv` file for further analysis or record-keeping.

To export:

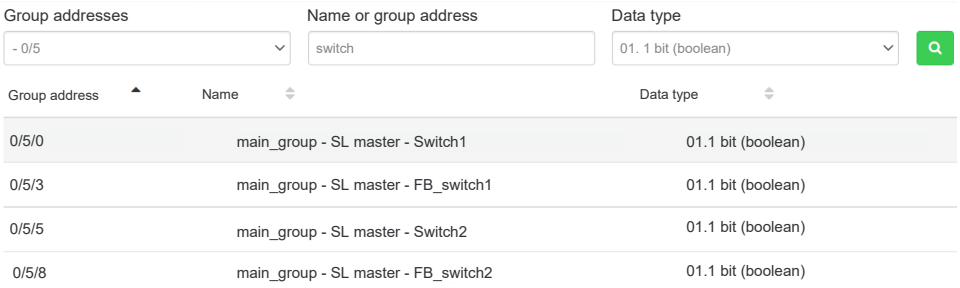
1. Click **Actions**.
2. Select **Export to CSV** from the dropdown menu.

The `.csv` file will be automatically downloaded to your computer's **Downloads** folder. You can open it using Microsoft Excel or any spreadsheet application to view and work with the data.

TIP: Use filters before exporting if you only want to include specific objects in the file.

Filtering and Editing Object Properties

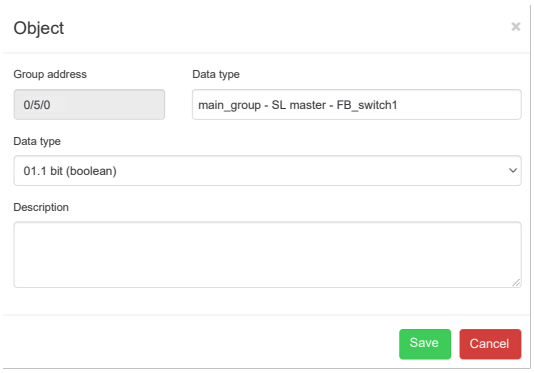
You can easily filter and manage your objects using various criteria such as **name**, **group address**, or **data type**. Simply type your search term or select from the drop-down menu to narrow down the list.



Once filtered, you can edit object properties, update values, or delete objects individually as needed.

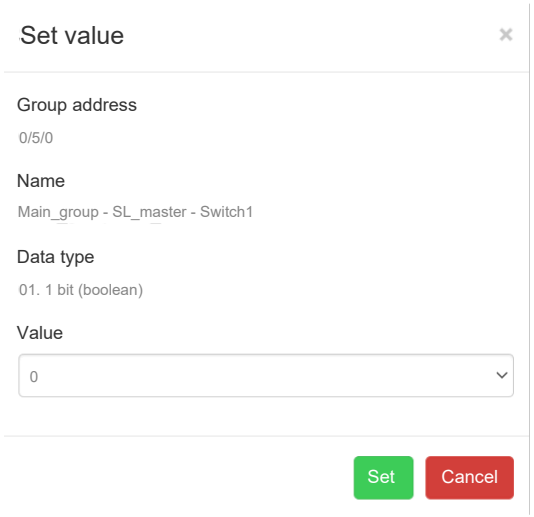
To edit object properties:

1. Click  .
2. Modify the desired properties in the pop-up window.
3. Click **Save** to apply the changes.



To set an object value:

1. Click  .
2. Choose a value from the drop-down **Value** list.
3. Click **Set** to confirm.



To delete an object:

1. Click .
2. Confirm the deletion by clicking **Yes** in the confirmation dialog.

Application Settings Overview

Once you've set up the user interface and imported your ETS project, you can configure the Gateway's parameters to suit your installation needs.

From the main menu, you have access to the following settings and tools:

- **Backup**: Save your current configuration for future recovery.
- **Restore**: Load a previously saved configuration.
- **Change password**: Update your login credentials for improved security.
- **Hostname**: Set a custom name for your Gateway on the network.
- **BACnet configuration**: Adjust BACnet-specific settings.
- **KNX configuration**: Manage KNX-related parameters.
- **Network configuration**: Set IP address, subnet, gateway, and DNS.
- **HTTP server configuration**: Customize web server settings.
- **HTTP SSL certificate**: Upload or manage your HTTPS certificate.
- **NTP client configuration**: Synchronize time using a network time server.
- **Date and time**: Manually set or adjust the system clock.
- **System log**: View system activity and diagnostic logs.
- **Ping**: Test network connectivity to other devices.
- **Toggle device identification**: Activate visual identification (e.g., LED)
- **Upgrade firmware**: Install the latest firmware version.
- **Factory reset**: Restore the Gateway to its default settings.
- **Reboot**. Restart the device.
- **Shutdown**: Power off the Gateway safely.

Creating a Backup

Creating a backup allows you to save a copy of your Gateway configuration, which can be restored later in case of data loss or system failure.

How to create a backup:

1. Open the main menu by clicking  .
2. Select the **Backup** option from the drop-down list.

The backup file will be automatically downloaded to your browser's **Downloads** folder.

Backup file name format:

```
[Hostname]-backup-[YYYY.MM.DD]-[HH.MM].bckp
```

The filename includes the Gateway's hostname and the exact date and time the backup was created. You can rename the file and move it to a different folder for safekeeping.

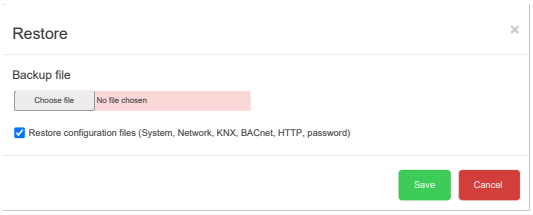
> **TIP:** Store your backup files in a secure location and avoid sharing them with unauthorized users.

Restoring a Backup

The **Restore** function allows you to recover your Gateway's data from a previously saved backup. This is useful if data has been lost, corrupted, or if you need to transfer settings to a new device.

To restore your data:

1. Open the main menu by clicking .
2. Select **Restore** from the drop-down list.
3. Click **Choose File** and locate your backup file on your computer.
4. (Optional) If you want to restore configuration files as well, check the **Restore configuration files** option.



5. Click **Save** to begin the restore process.

After clicking **Save**, a pop-up window will appear asking if you want to reboot the system:

- Click **Yes** to reboot and complete the restore.
- Click **No** to cancel the operation. If you choose **No**, no data will be imported.

  TIP: Always verify that you are restoring the correct backup file to avoid overwriting important data.

Changing Your Password

To keep your Gateway secure, it is important to update your password regularly.

Follow these steps to change it:

1. Open the main menu by clicking .
2. Select **Change password** from the menu.
3. Enter your current password, then type your new password.
4. Click **Save** to confirm the change.

Changing the Gateway Hostname

The hostname is the unique name assigned to your Gateway on the network. It helps you easily identify the device, especially when managing multiple installations. The hostname is also used in the filename of backup files, making it easier to track and organize them.

Why change the hostname?

- To clearly identify the Gateway in your network.
- To personalize the device name for easier management.

- To make backup files more recognizable (e.g.,`Office1-backup-2025.05.23-14.30.bckp`).

How to change the hostname:

1. Open the main menu by clicking .
2. Select **Hostname** from the menu.
3. Enger your desired hostname.
   - Use only letters, numbers, and hyphens.
   - Avoid spaces or special characters.
   - Keep it short and descriptive (e.g., `Lobby-Gateway`,`KNX-BMS-01`).
4. Click **Save** to apply the changes.

   NOTE: Changing the hostname does not affect the IP address or network configuration. However, it may require a reboot for the new name to appear in some network tools or logs.

BACnet Configuration

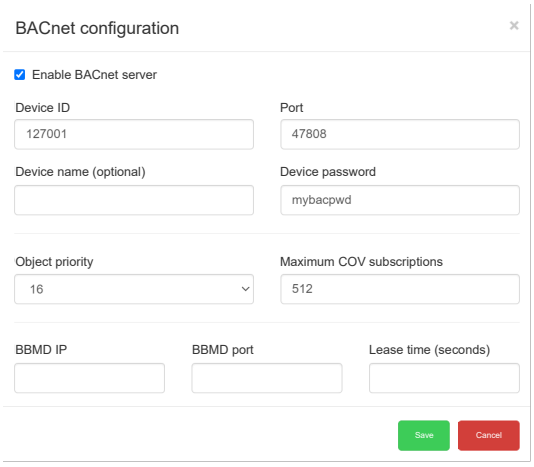
The Gateway functions as a BACnet server, enabling communication between KNX group objects and BACnet client devices. This allows seamless integration of building automation systems across different platforms.

BACnet (Building Automation and Control Network) is a standardized protocol used for exchanging data between devices in building automation systems—regardless of their specific function (e.g., lighting, HVAC, security). The Gateway connects to the BACnet network via the Ethernet interface and serves data from KNX group objects that have been exported to BACnet.

- Binary KNX objects are mapped as binary values in BACnet.
- Numeric KNX objects are mapped as analog values.
- Other data types are not supported.

How to configure BACnet settings:

1. Open the main menu by clicking .
2. Select **BACnet configuration** from the menu.



3. Configure the following BACnet parameters and click **Save**.

Parameter	Note
Enable BACnet server	Enables or disables BACnet functionality. Disabled by default.
Device ID	A unique identifier for the Gateway on the BACnet network. Must not conflict with other devices.
Port	Communication port for BACnet. Default is 47808.
Device name (optional)	Custom name for the device. If left blank, the default is `hostname_DeviceID`.
Device password	Optional password for BACnet services like `DeviceCommunicationControl` and `ReInitializeDevice`. If not set, no password is used.
Object priority	Sets the default priority array position for BACnet objects.
Maximum COV subscriptions	Maximum number of Change of Value (COV) subscriptions. Default is 4000. See Performance, page 16 for more details.
BBMD IP	IP address of the BACnet Broadcast Management Device (BBMD), if used.
BBMD port	Port used by the BBMD.
Lease time (seconds)	Interval for BBMD registration renewal.

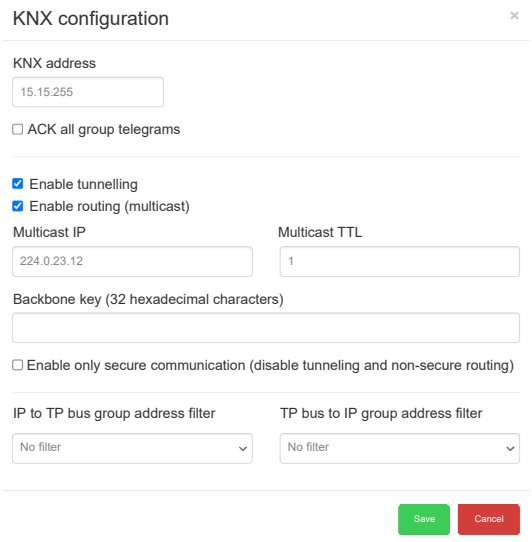
TIP: Make sure the Device ID is unique within your BACnet network to avoid communication conflicts.

KNX Configuration

The **KNX configuration** menu allows you to set up the Gateway when it is used as a **KNX IP interface** or **router**.

Follow the steps below to access and configure the settings:

1. Open the main menu by clicking  .
2. Select **KNX configuration** from the menu.



3. Adjust the following parameters as needed, then click **Save** to apply your changes.

Parameter	Note
KNX address	The individual KNX address of the device. Default: 15.15.255.
ACK all group telegrams	Enable this if the Gateway communicates directly with other KNX devices and needs to acknowledge received telegrams. Disable if the Gateway is only monitoring group addresses (sniffer mode).

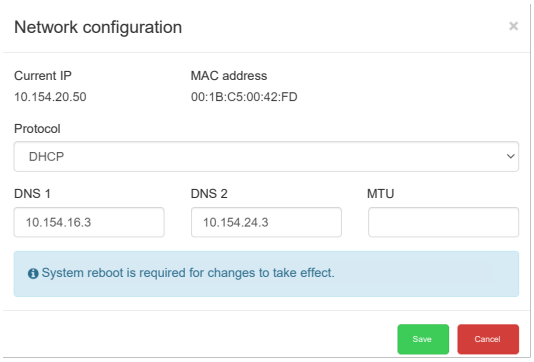
Parameter	Note
Enable tunneling	Allows multiple devices to share a public IPv4 address by modifying IP headers during transmission. This enables faster IP communication (up to 1000 × faster than TP-UART). The Gateway acts as a server using unicast and acknowledged data exchange. Each tunneling connection requires a unique individual address.
Enable routing (multicast)	Enables multicast-based, unacknowledged data transfer. The Gateway functions as a Line or Backbone Coupler.
Multicast IP	The multicast IP address used for routing. Default: 224.0.23.12.
Multicast TTL	Time-to-live value for multicast packets. Default: 1. This allows communication across sub-networks.
Backbone key (32 hexadecimal characters)	A 32-character hexadecimal key used to encrypt and decrypt secure telegrams for IP routing.
Enable only secure communication	When enabled, only secure communication is allowed. Tunneling and non-secure routing are disabled.
IP to TP bus group address filter	No filter
TP bus to IP group address filter	Accept selected group addresses Drop selected group addresses Filter entry examples: • Single address (1/1/1) • Range (1/1/1-1/1/100) • Wildcard (1/1/* or 1/*/*)

Network Configuration

Network configuration involves setting up the controls and parameters that manage how the device communicates over a network. After updating any network settings, a system restart is required for the changes to take effect.

Accessing the network configuration:

1. Open the main menu by clicking  .
2. Select **Network configuration**.



3. Adjust the following network parameters as needed, then click **Save** to apply your changes:

Parameter	Note
Current IP	Network configuration involves setting up the controls and parameters that manage how the device communicates over a network. After updating any network settings, a system restart is required for the changes to take effect.
MAC address	A unique hardware identifier assigned to the device.
Protocol	Specific protocol used for addressing: Static IP: Manually assign an IP address.

Parameter	Note
	DHCP: Automatically obtain an IP address from the network.
IP address	The device's IP address. Default: 192.168.0.10.
Network mask	Defines the subnet. Default: 255.255.255.0.
Gateway IP	The IP address of the network gateway. Default: None.
DNS 1	Primary DNS server IP address.
DNS 2	Secondary DNS server IP address.
MTU	Maximum Transmission Unit – the largest packet size that can be sent. Default: 1500.

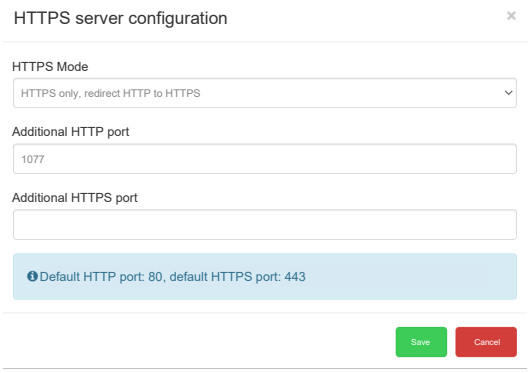
After saving the configuration, a confirmation window will appear. Click **Yes** to reboot the system and apply the new settings.

HTTP Server Configuration

In this section, you can configure the security level of the Gateway's communication with the web server and set additional HTTP/HTTPS ports.

Steps to Configure the HTTP Server

1. Open the main menu by clicking .
2. Select **HTTPS server configuration**.



3. Adjust the parameters listed below and click **Save**.
4. Restart the system for the changes to take effect.

HTTPS Server Parameters

Parameter	Note
HTTPS mode	Choose the desired security mode: **HTTP and HTTPS enabled**: Both secure and non-secure communication are allowed. **HTTPS only, redirect to HTTPS**: All HTTP traffic is automatically redirected to HTTPS for secure communication. **HTTPS only, HTTP port is disabled**: Only secure HTTPS communication is allowed. HTTP is completely disabled.
Additional HTTP port	Optional: Specify an additional HTTP port. Default is 80.
Additional HTTPS port	Optional: Specify an additional HTTPS port. Default is 443.

HTTP SSL Certificate

SSL certificates are digital files that securely link a cryptographic key to a device's identity. When installed on a web server, they enable secure HTTPS connections and activate the padlock icon in the browser.

How to configure an SSL Certificate:

1. Open the main menu by clicking .
2. Select **HTTP SSL certificate** from the menu.
3. Select the desired **Mode**:
   - **Upload new private key/certificate**: Use this option to upload an existing RSA private key and SSL certificate.
   - **Generate new private key/certificate**: Use this option to generate a new RSA key and SSL certificate based on the currently installed one.
4. Click **Save** to apply your changes.

5. Restart the system for the new certificate settings to take effect.

NTP Client Configuration

The NTP (Network Time Protocol) client ensures that the Gateway stays synchronized with Coordinated Universal Time (UTC), maintaining accurate time across all connected devices. It compensates for network delays to provide precise timekeeping.

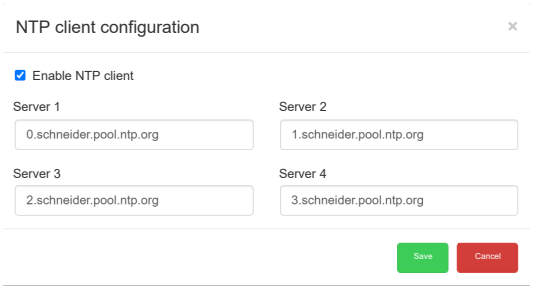
Key features:

- Synchronizes the Gateway's internal clock with up to **4 NTP servers**, prioritized from 1 to 4.
- Helps ensure accurate timestamps for logs, events, and data communication.

How to configure the NTP client:

1. Open the main menu by clicking .
2. Navigate to **NTP client configuration**.
3. Enter the IP addresses or domain names of up to four NTP servers, in order of priority.

4. Click **Save** to apply the settings.



5. Restart the system to activate the new configuration.

TIP:

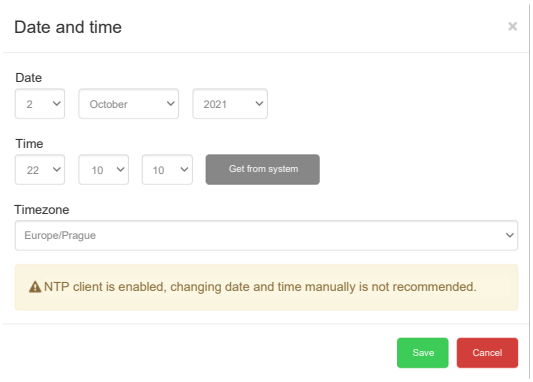
- If you are unsure whether an NTP server is reachable, use the **ping tool** to check its availability.
- For best results, use reliable and geographically close NTP servers.

Date and Time

The Gateway uses Network Time Protocol (NTP) to automatically synchronize its internal clock with an internet-based time server. This ensures accurate timekeeping without manual input.

How to set the date and time:

1. Open the main menu by clicking .
2. Select **Date and time** from the menu.
3. If the Gateway is not connected to the internet, click **Get from system** to synchronize the time with your PC.
4. Choose your time zone from the list.
5. Click **Save** to apply the settings.



System Log

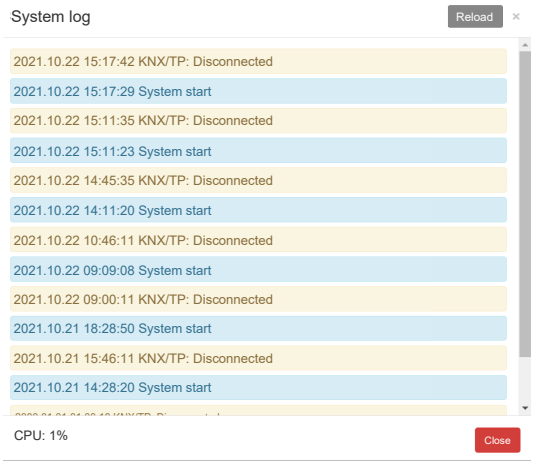
The **System log** provides a chronological record of key events on the Gateway, such as:

- System startups
- TP/KNX disconnection

These events are automatically logged by the Gateway in a simple, easy-to-read format.

How to view the system log:

1. Open the main menu by clicking .
2. Select **System log** from the menu.



The system log displays when you go to and click **System log**.

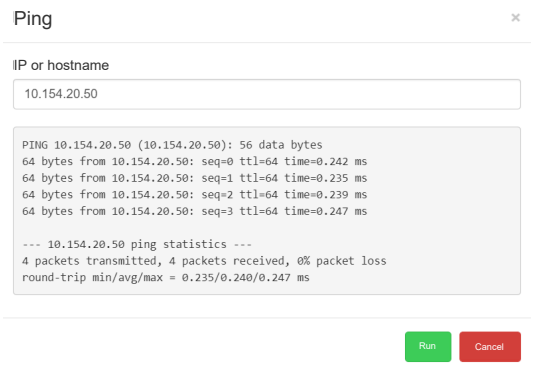
At the bottom of the log screen, you can also view the **CPU load**, which provides insight into the current processing activity of the Gateway.

Ping

The **Ping** tool helps you test whether a specific device or server is reachable over an IP network. It measures the **round-trip time** for data packets sent from the Gateway to the target host and back.

How to use the **Ping** tool:

1. Open the main menu by clicking .
2. Select **Ping** from the menu.
3. Enter the IP address or hostname of the device you want to test.
4. Click **Run** to start the ping test.



The results will show the response time, helping you determine if the destination is reachable and how quickly it responds.

Toggle Device Identification

The **Toggle device identification** feature helps you locate a specific Gateway device on the network by activating a visual signal.

How it works:

When identification is enabled, **LED 2** on the selected device will flash **red and green**, making it easy to spot the device among others.

How to use it:

1. Open the main menu by clicking .
2. Select **Toggle device identification** from the menu.
3. Observe the device – LED 2 should begin flashing to indicate its location.

This feature is especially useful when managing multiple devices in a networked environment.

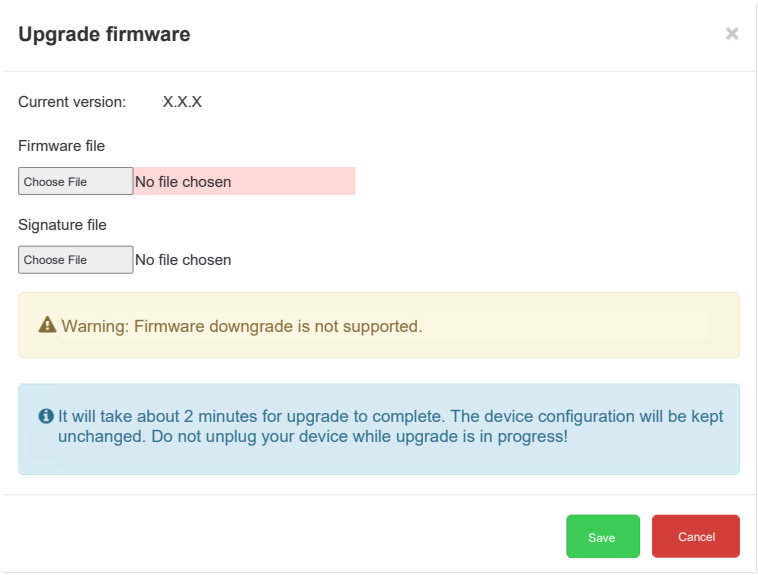
Upgrade Firmware

Upgrading the firmware updates your Gateway with the latest features and improvements – without changing your existing configuration or requiring any hardware modifications.

> **IMPORTANT:** Do not unplug the Gateway during the upgrade process. The device will restart several times, and **LED 1 will flash red and green** to indicate the upgrade is in progress.

How to Upgrade the Firmware

1. Open the main men by clicking .
2. Select **Upgrade firmware** from the menu.
3. Choose the firmware file you want to install.
4. Select the corresponding signature file (required for validation).
5. Click **Save** to begin the upgrade.



After the Upgrade

- The Gateway will automatically reboot.
- It is **strongly recommended** to **clear your browser cache** after the upgrade to avoid display issues.
- Firmware downgrades are not supported.

NOTE: A valid **signature file** is required for every firmware upgrade. Firmware packages are always distributed with their corresponding signature files.

Factory Reset

A factory reset erases all data and settings on the Gateway and restores it to its original factory state. This action is irreversible, so use it with caution.

You can perform a factory reset in two ways:

- **Via the application**: Use the software interface to initiate a reset from the settings menu.
- **Using the hardware reset button**: Press and hold the physical reset button on the device to trigger a reset manually.

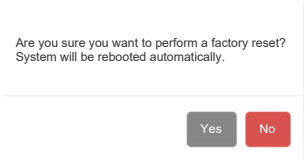
Application Factory Reset

You can reset your Gateway to its factory settings directly through the application. This process will erase all user configurations and restore the device to its original state.

NOTE: A factory reset will delete all custom settings and configurations. Use this option only when necessary.

How to perform a factory reset via the application:

1. Open the main menu by clicking .
2. Select **Factory reset** from the menu.
3. Confirm the reset when prompted. The system will automatically reboot.



Device parameters after reset:

Parameter	Result
Device name	LSS100300
IP address	Preserved (remains unchanged)
No objects	Cleared (BACnet/KNX configuration is removed)

Hardware Factory Reset

A hardware factory reset is useful when the Gateway becomes inaccessible due to incorrect settings or network configuration issues.

When to use:

- The Gateway is unresponsive.
- You cannot access the web interface.
- Network settings prevent connection.

How to perform a hardware reset:

1. Locate the red **RESET** button on the device.
2. Follow one of the reset procedures below:

Action	Result
Press and hold for **less than 10 seconds**	Reboots the device (no settings are changed).
Press and hold for **more than 10 seconds**	Resets **network settings** only. IP address is restored to factory default: 192.168.0.10.
Press and hold for **more than 10 seconds**, release, then press and hold again for **more than 10 seconds**	Performs a **full factory reset**, restoring all settings to default.

NOTE: A full reset will erase all configurations, including BACnet and KNX settings.

Reboot

If your Gateway is not responding as expected, you can perform a **reboot** to restart the system.

Rebooting shuts down the device and powers it back on – without affecting your configuration or data.

How to reboot the Gateway:

1. Open the main menu by clicking  .
2. Select **Reboot** from the menu.
3. When prompted, click **Yes** to confirm.

The Gateway will restart automatically. This process usually takes a few moments.

Gateway Shutdown and Restart

Putting the Gateway into sleep mode ensures that all data operations are safely completed, maintaining system stability and preventing data loss or corruption.

IMPORTANT: Do not disconnect the power supply until the LED 2 turns off.

Entering Sleep Mode

To safely shut down the Gateway:

1. Open the main menu by clicking the menu icon  .
2. Select **Shutdown**.
3. Confirm by clicking **Yes**.

What Happens During Sleep Mode

The Gateway enters a temporary **3-minute sleep mode**. During this time:

- LED 1 (green) turns **off**.
- LED 2 (green) turns **off**.

- The Gateway becomes **unresponsive to network communication**.

If the device is **not disconnected** from the power supply during this period, it will **automatically reboot**.

Restarting the Gateway Manually

To manually restart the Gateway:

- Disconnect and reconnect the power supply after **LED 2** turns off.
- The Gateway does **not** have a dedicated power button.

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

2507_LSS100300_SW