

# SpaceLogic KNX BMS IP Gateway

LSS100300

## User guide

10/22 – SpaceLogic KNX BMS IP Gateway



## Legal information

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

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an “as is” basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change 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 material or consequences arising out of or resulting from the use of the information contained herein.

## Trademarks

Other brands and registered trademarks are the property of their respective owners.

## Warnings

Read through the following instructions carefully and familiarise yourself with the Hybrid Module prior to installation, operation and maintenance. The warnings listed below can be found throughout the documentation and indicate potential risks and dangers, or specific information that clarifies or simplifies a procedure.



The addition of a symbol to "Danger" or "Warning" safety instructions indicates an electrical danger that could result in serious injuries if the instructions are not followed.



This symbol represents a safety warning. It indicates the potential risk of personal injury. Follow all safety instructions with this symbol to avoid serious injuries or death.



### DANGER

**DANGER** indicates an imminently hazardous situation that will inevitably result in serious or fatal injury if the instructions are not observed.



### WARNING

**WARNING** indicates a possible danger that could result in death or serious injuries if it is not avoided.



### CAUTION

**CAUTION** indicates a possible danger that could result in minor injuries if it is not avoided.

### NOTE

**NOTE** provides information about procedures that do not present any risk of physical injury.

## Symbols



Additional information



The information provided must be complied with, otherwise program or data errors may occur.

# Table of contents

<b>1</b>	<b>For your safety</b>	<b>5</b>
<b>2</b>	<b>Introduction</b>	<b>6</b>
2.1	Security recommendation	6
2.2	Create a strong password	7
<b>3</b>	<b>Device specification</b>	<b>8</b>
<b>4</b>	<b>Compatibility</b>	<b>9</b>
<b>5</b>	<b>Performance</b>	<b>10</b>
<b>6</b>	<b>Getting started</b>	<b>11</b>
<b>7</b>	<b>Import KNX project</b>	<b>13</b>
7.1	Add object	15
7.2	Actions	15
	Mass delete	15
	Mass edit	16
	Export CSV	16
7.3	Filtering and changing object properties	16
<b>8</b>	<b>Application settings</b>	<b>18</b>
8.1	Backup	18
8.2	Restore	18
8.3	Change password	19
8.4	Hostname	20
8.5	BACnet configuration	20
8.6	KNX configuration	21
8.7	Network configuration	22
8.8	HTTP server configuration	23
8.9	HTTP SSL certificate	24
8.10	NTP client configuration	25
8.11	Date and time	25
8.12	System log	26
8.13	Ping	26
8.14	Toggle device identification	27
8.15	Upgrade firmware	28
8.16	Factory reset	28
	Application factory reset	29
	Hardware factory reset	29
8.17	Reboot	29
8.18	Shutdown	30

# 1 For your safety



## WARNING

**Risk of serious damage to property and personal injury due to incorrect electrical installation.**

Safe electrical installation can only be ensured if the person in question can prove basic knowledge in the following areas:

- Connection to installation networks
- Connecting several electrical devices
- Laying electric cables
- Connecting and establishing KNX networks
- Commissioning KNX installations

These skills and experience are normally only possessed by certified specialists who are trained in the field of electrical installation technology. If these minimum requirements are not met or are disregarded in any way, you will be personally liable for any damage to property or personal injury.



## 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 message 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.

## Qualified personnel

This document is aimed at personnel who are responsible for setting up, installing, commissioning and operating the device and the system in which it is installed.

Detailed expertise gained by means of training in the KNX system is a prerequisite.

## 2 Introduction

**SpaceLogic KNX BMS IP Gateway** (hereinafter referred to as **Gateway**) is a multifunctional device that allows you to integrate KNX installation with building automation devices.

The main communication interface is KNX TP and IP supporting BACnet protocol.

There are three components combined in one device:

- KNX IP router (max 500 objects)
- KNX IP interface
- DPSU choke

The Gateway allows professional installers to deploy KNX installations more cost and time effectively thanks to features combination.

The architecture is simpler because it is no longer necessary to use KNX routers and KNX power supplies with respect to given parameters.

The Gateway is designed for commercial installations.

This document describes the Gateway application software, device features, and user interface.

### 2.1 Security recommendation

- Network security must be set up at the appropriate level. Gateway should be part of a secure network with limited access. In case of Internet connection, it is strictly recommended to use VPN or HTTPS channel.
- Use secure protocol access HTTPS://IP:Port.
- The security method is determined by the ability of other network elements (firewall, protection against viruses and malware threats).
- It is strictly recommended to store the files containing your backups in a safe place without access of unauthorized persons.
- Make sure your Gateway does not have a publicly accessible IP address.
- Do not use port forwarding to access your Gateway from the public Internet.
- The Gateway should be located on its own network segment.
- If your router supports a guest network or VLAN, it is preferable to locate your Gateway there.

In case you find cyber security incidents or vulnerabilities, please contact us through this page:

<https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp>.

You can read more on system hardening here:

[https://www.se.com/ww/en/download/document/AN002\\_107/](https://www.se.com/ww/en/download/document/AN002_107/).

## NOTE

### MATERIAL DAMAGE THROUGH UNAUTHORIZED ACCESS TO THE KNX INSTALLATION

As soon as you access the KNX installation via the Internet, the data traffic can be read by third parties.

- Only use a VPN access for this connection with a secure encryption for all data packages.
- The required hardware (VPN router) and the features offered by mobile service providers differ significantly with regard to the settings and technical possibilities depending on the country or region.
- Always have the VPN access set up and commissioned by a specialist VPN service provider. The VPN service provider selects a suitable mobile service provider and suitable hardware for the VPN access and ensures that the VPN is set up by a qualified specialist.

**Schneider Electric cannot be held responsible for performance problems and incompatibilities caused by applications, services or devices from third-party providers. Schneider Electric offers no technical support when setting up a VPN access.**

**Failure to follow these instructions can result in equipment damage.**



The VPN access (VPN = Virtual Private Network) authorises the portable device to access the local network, and therefore also the KNX installation, via the Internet.

Benefits of VPN:

- Only authorised users have access to the local network.
- All data is encrypted.
- The data is not changed, recorded or diverted during the transfer. This is often referred to as a VPN tunnel.

Requirements for setting up a VPN connection:

- Internet connection.
- The portable device and the router are enabled for a VPN connection (VPN client installed).
- The Gateway should be located on its own network segment.
- If your router supports a guest network or VLAN, it is preferable to locate your Gateway there.

## 2.2 Create a strong password

- Your password can be any combination of upper case and lower case characters, numbers, and special characters.
- Use a minimum of 8 characters.
- Make your password hard to guess or find in the cybercriminal dictionaries.
- Prefer phrases.
- Change your password frequently, at least once a year.
- Change a default Admin password immediately after you get it and after a factory reset.
- Never re-use your passwords.

### 3 Device specification

Specification	Description	Note
Terminals, Inter-face	1 x RJ45 – ethernet 10BaseT/100BaseTx 1 x KNX TP 1 x Reset push-button	
Connectivity	IP LAN connection 10/100 Mbit KNX / EIB TP Bus	
LED indicators	2 x LED, CPU, (Operation + Reset)	
KNX IP routing	500 objects (automatically disabled when over this limit)	You can use up to 4000 BACnet points. See <a href="#">Performance → 10</a> .
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	Embedded 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	



## 4 Compatibility

The Gateway is compatible with the following standards:

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

## 5 Performance

Parameter	Note	
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 discarded.
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.

# 6 Getting started

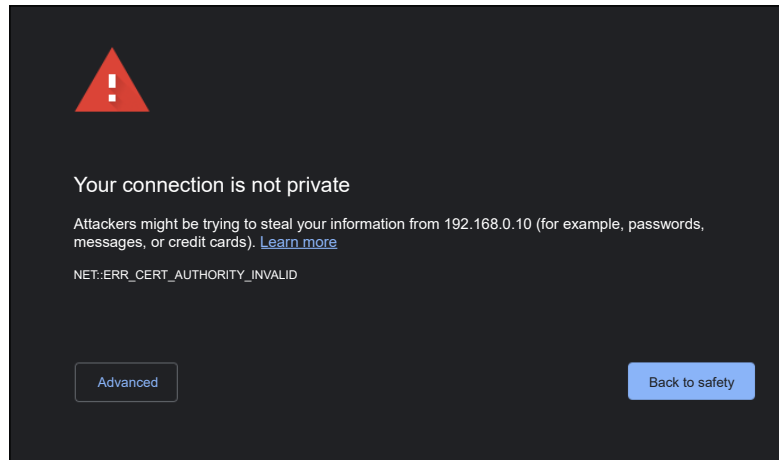
Before you start, make sure that the Gateway is properly connected according to the installation instructions.

You need a standard web browser to work with the application and set up the Gateway. Google Chrome or Mozilla Firefox web browsers are recommended.

When accessing for the first time:

- Default IP address
1. Type the default IP address 192.168.0.10 in the address bar of your web browser and click *Enter*.

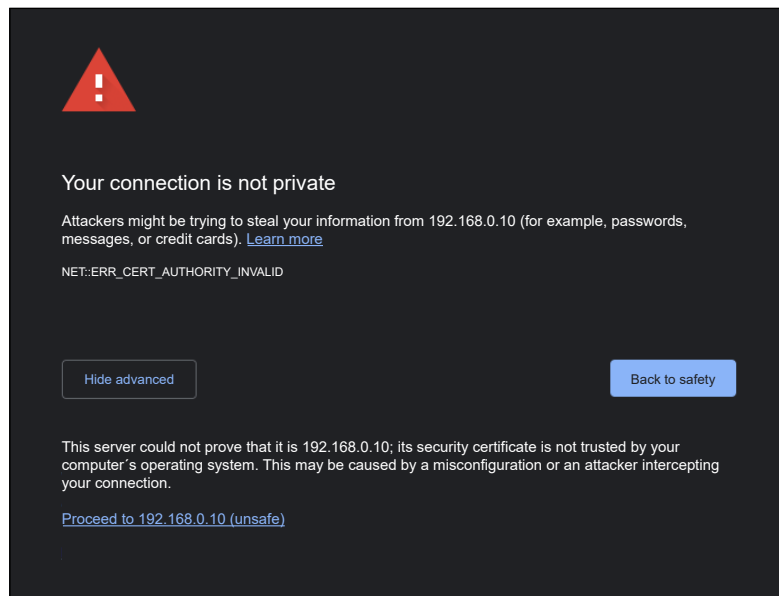
The Gateway uses a self-signed certificate, and the following message shows:



Pic. 1 Warning: Your connection is not private

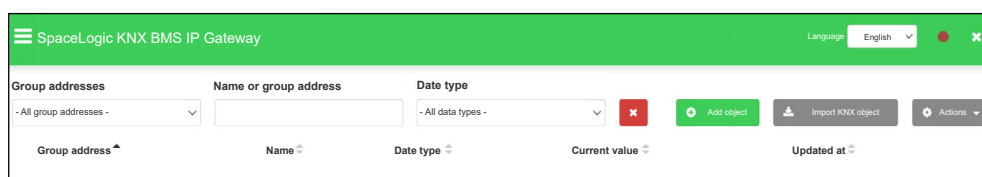
By default, the gateway uses an HTTPS communication mode. Because of the used self-signed certification, you have to confirm the exception to proceed. HTTPS provides encrypted communication between the Gateway and the client.

2. Click *Advanced > Proceed to 192.168.0.10*.



Pic. 2 Warning: Proceed to 192.168.0.10

- Username and password 3. Enter the default login details and click *Enter*.  
 username: **admin**  
 password: **admin**
- Password change prompt 4. You will get prompted to change your password. Type it and click *Save*.  
 Your new password has to contain at least 8 characters as following:
- one uppercase letter
  - lowercase letter
  - a digit
- Start page 5. The next step gets you to the start page.

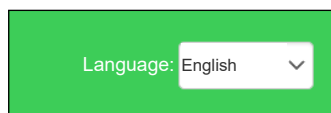


Pic. 3 Start page

You can find there:

- Language settings
- The Gateway settings (☰)
- Tool for filtering and working with objects
- *Import KNX project* button

- Language settings First, select your preferred application language from the drop-down menu.



Pic. 4 Select your language

In the following steps, you will import your KNX project and set the device parameters.

# 7 Import KNX project

*Import KNX project* button top right allows you to import the \*.knxproj file directly to the Gateway. It preserves the structure of the project and DPTs of the group addresses, including automatic units and suffixes.



**Objects with the same name are considered duplicates and might not be imported and marked as discarded.**

You can add objects without data types defined and also add structure level names to objects.

Password protected \*.knxproj files requests password set in ETS. You cannot import the project without knowing correct password.

Import your project by following these steps:

Import KNX project

1. Click *Import KNX project* button and choose your file.
2. Type the correct password if applicable.
3. Check *Add level names to objects* if you want to import also object names and their structure location designation.
4. You can check the *Overwrite existing objects* if you want to overwrite existing objects.
5. Click *Next*.

Filtering tables are filled in automatically according to the imported KNX project and can be further modified.

The backbone key is also automatically imported from the KNX project.

Pic. 5 Import your KNX project.

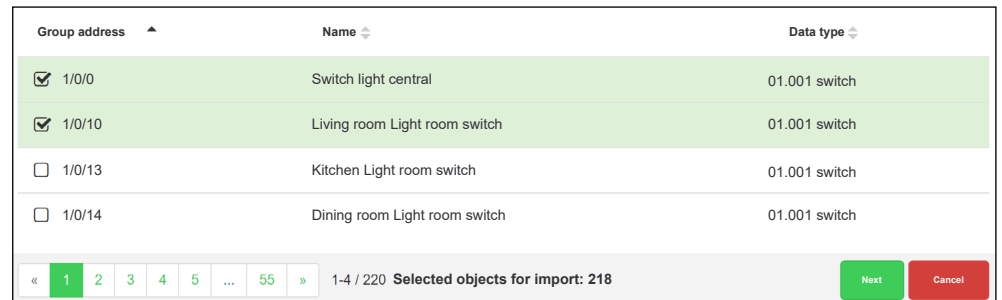


**KNX routing cannot be enabled for projects larger than 500 objects.**

Select objects to import In the next step, you choose which objects from the KNX project you want to export to BACnet. Only selected objects are imported to the Gateway database.

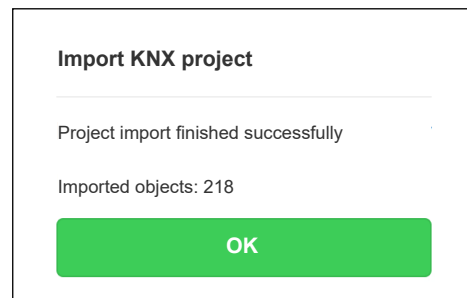
You can filter objects by name, group address, or data type to make it easier to find your object. See more in [Filtering and changing object properties → 16](#).

Choose your objects and click *Next*.



Pic. 6 Choosing objects to import.

Finish importing objects A pop-up window appears informing you how many objects are being imported.



Pic. 7 Import KNX project final dialog.

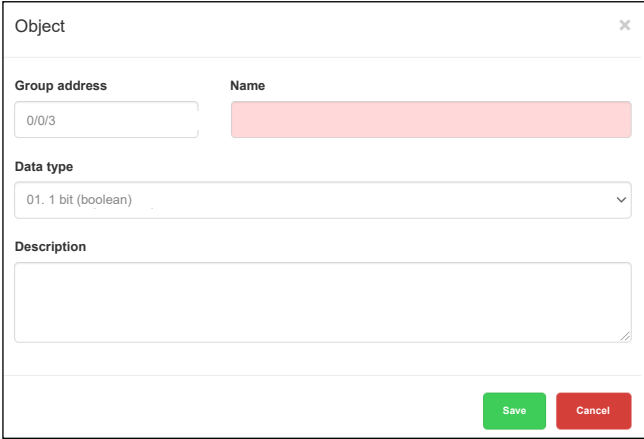
Click *OK* and your import process is complete.

## 7.1 Add object

The *Add object* function is handy when you need to add an individual object later and, you do not want to import the entire \*.knxproj file again.

Add objects Follow the steps below to add new object:

1. Click on *Add object*.
2. Fill in the object details.
3. Click *Save*.



The screenshot shows a dialog box titled "Object" with a close button (X) in the top right corner. It contains the following fields and controls:

- Group address:** A text input field containing "0/0/3".
- Name:** A text input field that is currently empty and highlighted in red.
- Data type:** A dropdown menu showing "01. 1 bit (boolean)".
- Description:** A large text area for entering a description.
- Buttons:** "Save" (green) and "Cancel" (red) buttons at the bottom right.

Pic. 8 Adding objects.

## 7.2 Actions

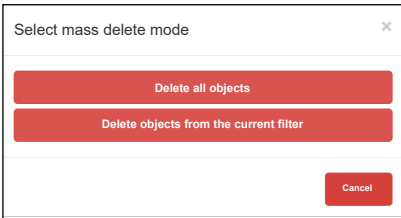
### Mass delete

The *Mass delete* feature allows you to delete objects in bulk.

You have two options:

- *Delete all objects*
- *Delete objects from the current filter*

In the next step, the objects are deleted the way you select.



The screenshot shows a dialog box titled "Select mass delete mode" with a close button (X) in the top right corner. It contains two main options, each in a red button:

- Delete all objects**
- Delete objects from the current filter**

A "Cancel" button is located at the bottom right of the dialog.

Pic. 9 Deleting objects in bulk

## Mass edit

You can edit units and COV increments of your objects in bulk.

1. Filter the objects you want to edit.
2. Click on *Actions > Mass edit*.
3. Select parameters – units and/or COV increment value and click *Save*.

## Export CSV

You can export objects to a .csv file.

Click *Actions > Export to CSV*.

The .csv file with all the objects is automatically downloaded to your local *Downloads* folder, from where you can open it in MS Excel.

## 7.3 Filtering and changing object properties

Filtering objects

You can filter objects by name, group address, or data type. You can either select from the drop-down menu or type what you are looking for.

Group addresses	Name or group address	Data type
- 0/5	switch	01.1 bit (boolean)

Group address	Name	Data type
0/5/0	main_group - SL master - Switch1	01.1 bit (boolean)
0/5/3	main_group - SL master - FB_switch1	01.1 bit (boolean)
0/5/5	main_group - SL master - Switch2	01.1 bit (boolean)
0/5/8	main_group - SL master - FB_switch2	01.1 bit (boolean)


Pic. 10 Filtering objects

Changing object properties

You can edit properties of objects and their values later as needed. Or you can delete them individually.

Edit the object properties by following these steps:

Editing the object properties

1. Click .
2. Edit object properties.
3. Click *Save*.

Object ✕

---

Group address:       Data type:


Data type:

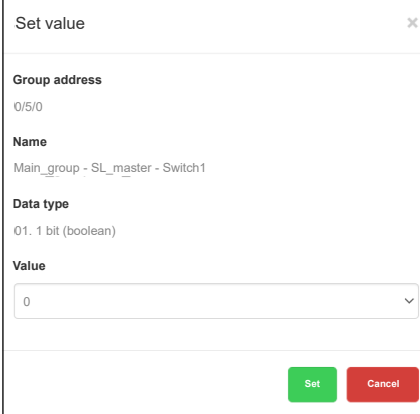
Description:

Pic. 11 Editing object properties



Setting the object value You can set the value of your object.

1. Click .
2. Select in the drop-down *Value* list.
3. Click *Set*.



Set value

Group address  
0/5/0


Name  
Main\_group - SL\_master - Switch1

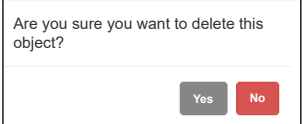
Data type  
01. 1 bit (boolean)

Value  
0

Set Cancel

Pic. 12 Setting the value of the object

Deleting the object If you want to delete an object, click . Click Yes to confirm.



Are you sure you want to delete this object?

Yes No

Pic. 13 Deleting the object

# 8 Application settings


After you set up the user interface of the application and import the ETS project, you can set the individual parameters of your Gateway.

In the main menu you have the following options:

- Backup
- Restore
- Change password
- Hostname
- BACnet configuration
- KNX configuration
- Network configuration
- HTTP server configuration
- HTTP SSL certificate
- NTP client configuration
- Date and time
- System log
- Ping
- Toggle device identification
- Upgrade firmware
- Factory reset
- Reboot
- Shutdown

## 8.1 Backup

The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure.

To create a backup file, go to  and select the *Backup* option from the drop-down menu.

Your backup file is immediately downloaded to the browser *Downloads* folder. The name of the backup file consists of the following data:


*Hostname-backup-yyyy.mm.dd-hh.mm.bckp*

Actual Gateway time and date is used when the backup is generated. You can later rename the file and save it to another folder.

## 8.2 Restore

A restore is performed to return data that has been lost, stolen or damaged to its original condition or to move data to a new location. Use backup files to restore your Gateway data to an earlier point in time.

To restore your data, do the following:

- Data restore
1. Go to .
  2. Click *Restore*.

3. Click *Choose File* and find your backup file.

If you also want to restore the configuration files, check the *Restore configuration files* option.

Pic. 14 Restoring application configuration

After you click *Save*, a pop-up window appears asking if you want to reboot the system. Select *Yes* or *No*. If you select *No*, nothing is imported.

Pic. 15 Rebooting the system

## 8.3 Change password

For changing your password, do the following:

1. Go to .
2. Click *Change password*.
3. Enter your current password and the new password.
4. Click *Save*.

Pic. 16 Changing the password

## 8.4 Hostname

You can change the hostname of your Gateway for easy identification. It displays in backup file name.

To change the hostname, do the following:

Changing the hostname

1. Go to .
2. Select *Hostname*.
3. Type your hostname.
4. Click *Save*.

## 8.5 BACnet configuration

BACnet server

The Gateway acts as a BACnet server. It serves data readable for BACnet client devices, and BACnet client devices can write data to the server.

BACnet protocol allows the information exchange for building automation devices, regardless of the particular building service they perform.

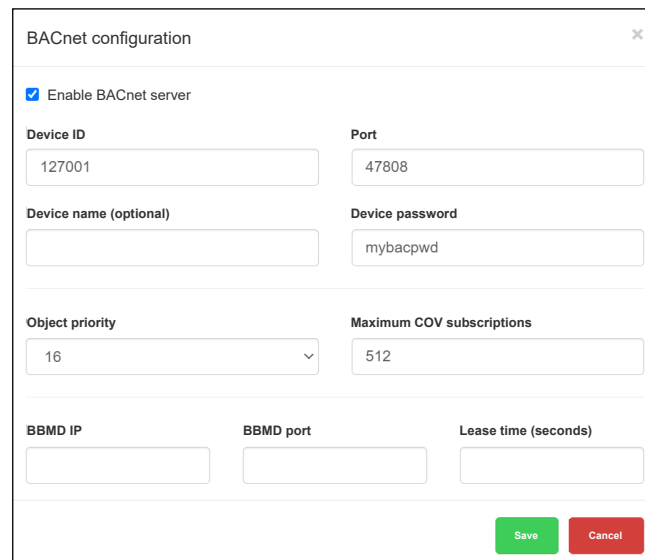
The devices are connected via Ethernet physical layer.

The connection to the BACnet network comes from KNX group objects, which are exported to BACnet.

Binary objects appear as binary values, numeric values will appear as analogue values. Other data types are not supported.

BACnet configuration

1. Go to .
2. Select *BACnet configuration*.



BACnet configuration

Enable BACnet server

Device ID: 127001      Port: 47808

Device name (optional):      Device password: mybacpwd

Object priority: 16      Maximum COV subscriptions: 512

BBMD IP:      BBMD port:      Lease time (seconds):

Save      Cancel

Pic. 17 BACnet configuration

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

Parameter	Note
Enable BACnet server	Disabled by default
Device ID	Choose unique network ID
Port	BACnet port, 47808 by default
Device name (optional)	Controller’s hostname_Device ID by default If you fill in the device name here, then BACnet name = device name.
Device password	BACnet password The password will be used for BACnet services (e.g., “DeviceCommunicationControl” and “ReinitializeDevice” – re-initialization of the device). If a password is not defined, it is not sent to the BACnet device.
Object priority	Default priority array position
Maximum COV subscriptions	4000 (See <a href="#">Performance → 10</a> )
BBMD IP	BACnet router IP
BBMD port	BACnet router port
Lease time (seconds)	BBMD registration resend interval

## 8.6 KNX configuration

In the *KNX configuration* menu, you can configure detail setting of KNX when The Gateway is used in a role of KNX IP interface or router.

KNX configuration

1. Go to .
2. Click *KNX configuration*.


Pic. 18 KNX configuration

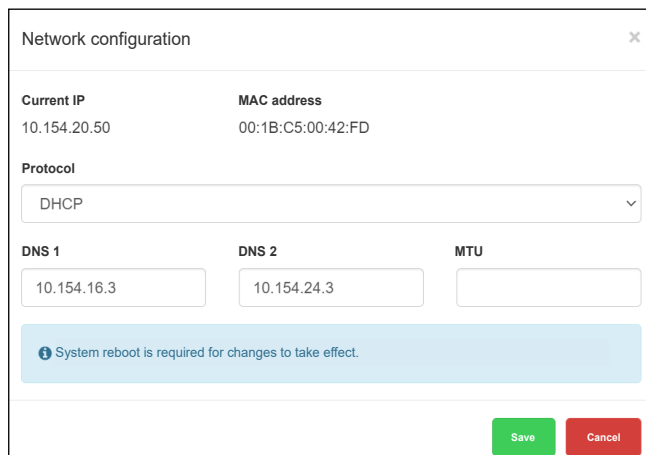
3. Configure the following BACnet parameters and click *Save*.

Parameter	Note
KNX address	KNX individual address of the device. 15.15.255 by default.
ACK all group telegrams	If the Gateway communicates directly with another KNX device it must acknowledge received telegrams. Uncheck if the Gateway operates as a sniffer of group addresses only.
Enable tunneling	Allows multiple devices to connect to public network using the same public IPv4 address. It modifies the IP address information in the IPv4 headers while in transit across a traffic routing device. IP connection, is 1000x faster than TP-UART. The Gateway as a server. Unicast, acknowledged data exchange, additional individual address per tunneling connection.
Enable routing (multicast)	Multicast, unacknowledged data transfer. The Gateway as a Line or Backbone Coupler.
Multicast IP	Multicast IP address, 224.0.23.12 by default.
Multicast TTL	Default value is 1; it allows communication between different sub-networks.
Backbone key (32 hexadecimal characters)	Backbone key for encrypting and decrypting secured telegrams for IP routing.
Enable only secure communication -	Tunnelling 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/*/*)

## 8.7 Network configuration

Network configuration is the process of setting a network’s controls, flow and operation to support the network communication. After setting the network parameters, it is necessary to restart the system for the changes to take effect.

- Network configuration
1. Go to .
  2. Click *Network configuration*.

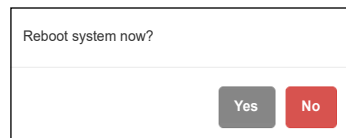


Pic. 19 Network configuration

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

Parameter	Note
Current IP	The IP address given by the DHCP server or the static IP address. This field appears only if the IP address is given otherwise it is hidden.
MAC address	Each device has its own unique MAC address.
Protocol	Specific protocol used for addressing: Static IP DHCP
IP address	192.168.0.10 by default
Network mask	255.255.255.0 by default
Gateway IP	None by default
DNS 1	Primary DNS server IP address.
DNS 2	Secondary DNS server IP address.
MTU	Maximum transmission unit, the largest size of the packet which could be passed in the communication protocol. (Default 1500).

In the pop-up window, click *Yes* and confirm the system reboot for the changes to take effect.




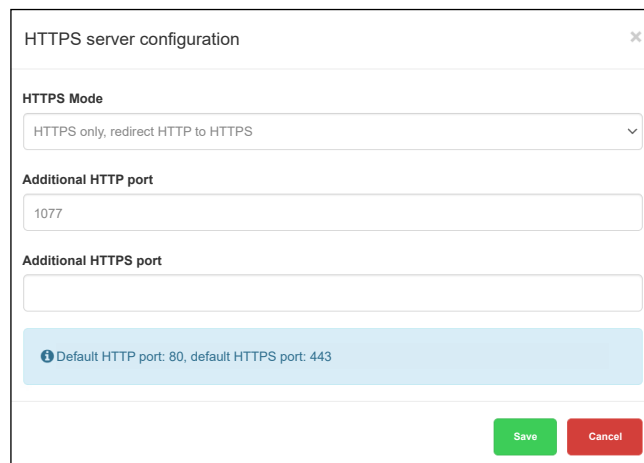
Pic. 20 Rebooting the system

## 8.8 HTTP server configuration

In this section you set the security level of the Gateway’s communication with the web server and additional HTTP/S ports.

HTTP server configuration

1. Go to .
2. Select *HTTPS server configuration*.



Pic. 21 Configuration of HTTP server

3. Configure the following HTTPS server parameters and click *Save*.
4. Reboot for the changes to take effect.

Parameter	Note
HTTPS mode	HTTP and HTTPS enabled HTTPS only, redirect to HTTPS HTTPS only, HTTP port is disabled
Additional HTTP port	Select the number. (Default HTTP port: 80.)
Additional HTTPS port	Select the number. Default HTTPS port: 443.

HTTPS modes:

- **HTTP and HTTPS enabled** – both HTTP and HTTPS communication is allowed
- **HTTPS only, redirect HTTP to HTTPS** – all communication on HTTP ports will be redirected to HTTPS
- **HTTPS only, HTTP port is disabled** – only secured communication is enabled




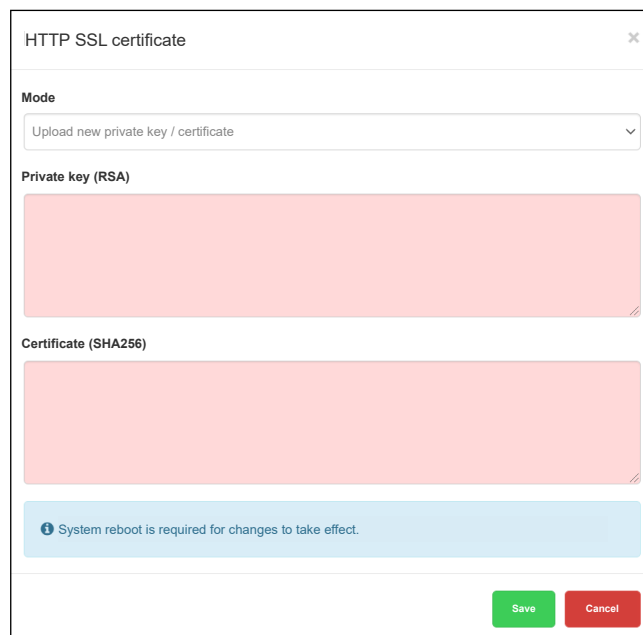
For security reasons, HTTPS communication mode is recommended.

## 8.9 HTTP SSL certificate

SSL certificates are data files that digitally bind a cryptographic key to a device's details. When installed on a web server, it activates the padlock and the HTTPS protocol and allows secure connections from a web server to a browser.

HTTP SSL certificate settings

1. Go to .
2. Click *HTTP SSL certificate*.
3. Choose your *Mode*:
  - *Upload new private key/certificate*: upload existing RSA key/SSL certificate
  - *Generate new private key/certificate*: generate RSA key/SSL certificate from one already installed
4. Click *Save* and reboot for changes to take effect.



Pic. 22 HTTP SSL certificate

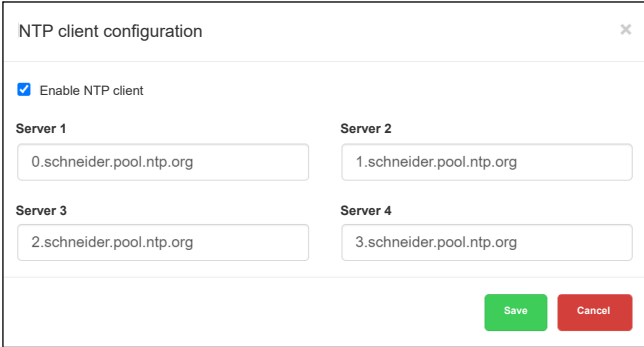


## 8.10 NTP client configuration

NTP (Network Time Protocol) is intended to synchronize all participating devices to within a few milliseconds of Coordinated Universal Time (UTC). It is designed to mitigate the effects of variable network latency.

If the NTP client is enabled, the Gateway can collect data from up to 4 selected servers (priority 1 to 4 in a row).

Define the server from which date and time is obtained.



Pic. 23 NTP client configuration

You need to reboot after NTP client configuration.

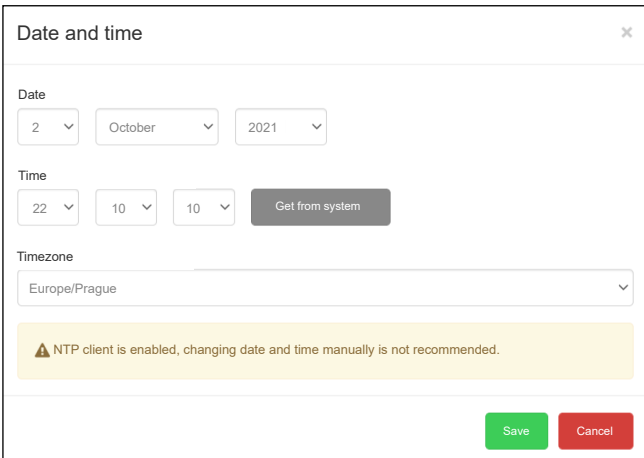
Check availability of NTP server with ping tool if necessary.

## 8.11 Date and time

Network time protocol (NTP) is implemented. Along with the internet connection, The Gateway automatically updates time from an NTP server.

Date and time setting


1. Go to .
2. Click *Date and time*.
3. If there is no internet connection, click on *Get from system* to adopt time from your PC.
4. Select your time zone and click *Save*.



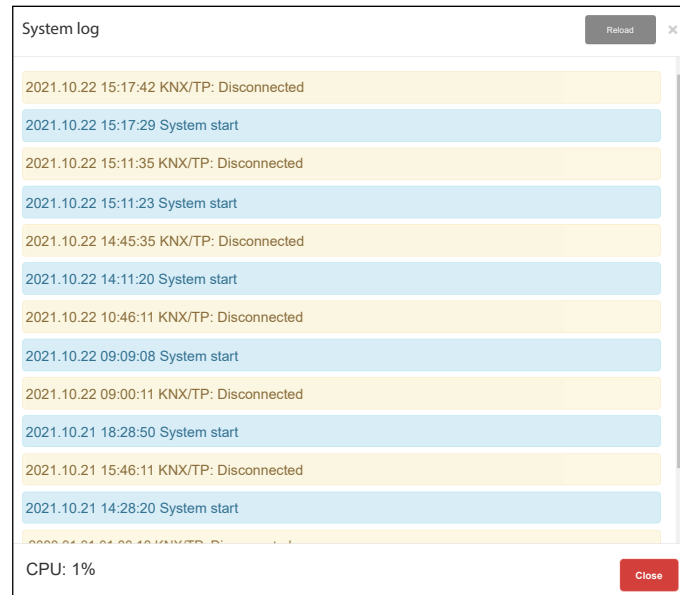
Pic. 24 Date and time setting

## 8.12 System log

The Gateway records each system start and TP / KNX disconnection. Transactions are recorded chronologically in a simple log file. Log file is automatically created and maintained by the Gateway.

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

At the bottom you can see the CPU load information.




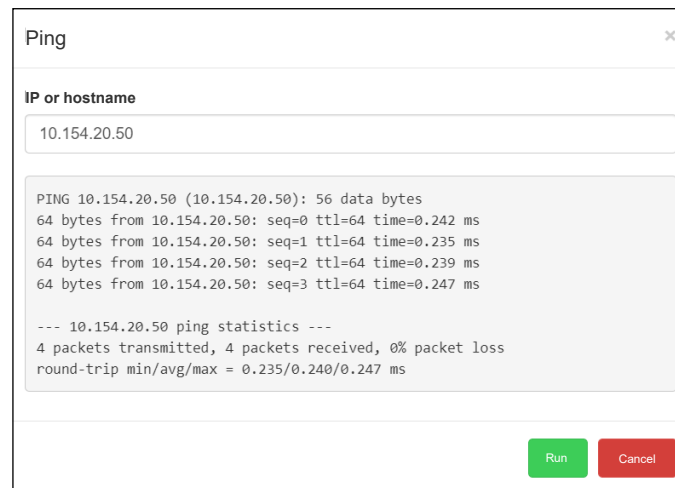
Pic. 25 Log file

## 8.13 Ping

Ping is a tool to test the reachability of a host on an Internet Protocol (IP) network. Ping measures the round-trip (path) time for packets sent from the originating host to a destination that are echoed back to the source.

Ping the host To ping the host, do the following:

1. Go to .
2. Select *Ping*.
3. Type the IP or hostname.
4. Click *Run*.



Pic. 26 Ping statistics.

## 8.14 Toggle device identification

*Toggle device identification* is a feature for searching the individual the Gateway devices on a network. Turning on the identification flashes the LED 2 (red/green) on the specific device.


Toggle device identification    Go to , click *Toggle device identification*. Check the device signaling.

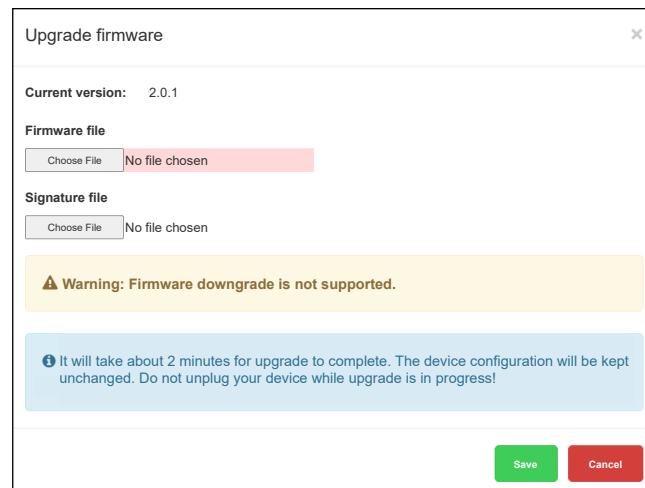
## 8.15 Upgrade firmware

A firmware upgrade updates your the Gateway with advanced operational instructions without needing any upgradation in the hardware. Upgrade does not change the Gateway configuration.

**During the firmware upgrade, the device does not respond and restarts several times.**

LED1 is flashing red/green during the upgrade. Do not unplug the Gateway while LED1 flashes.

- Firmware upgrade
1. Go to .
  2. Click *Upgrade firmware*,
  3. Choose your firmware file.
  4. Choose your signature file.
  5. Click *Save*.



Pic. 27 Upgrading firmware.

After each upgrade, it is strongly recommended to clean the browser cache.

**Downgrade of the Gateway with firmware is not supported.**



You cannot upgrade without a signature file. The firmware is always distributed with the appropriate signature file.


## 8.16 Factory reset

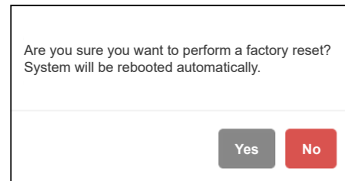
A factory reset erases all of the information on the Gateway and restores the software to its original state.

There are two ways you can factory reset your Gateway:

- In the application
- With the hardware reset button

## Application factory reset

To reset your device via the application, go to , click *Factory reset* and confirm. The system automatically reboots.



Pic. 28 Application factory reset.

### The device parameters after factory reset:

Parameter	Result
Device name	LSS100300
IP address	IP is preserved after the factory reset
No objects	Configuration as BACnet, KNX

## Hardware factory reset

Hardware factory reset is suitable for situations when the Gateway is unavailable due to incorrect settings.

Long press (10 s) on the red RESET button on the front side. Release and press again for 10 seconds.

IP address after HW factory reset with hardware button is always 192.168.0.10.

3 types of HW button press

Press and hold for <10 sec – reboot the device

Press and hold for >10 sec – reset networking with IP to factory default

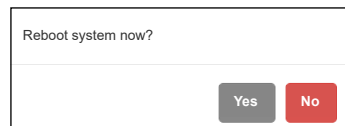
Press and hold for >10 sec and again press and hold for >10 sec – full reset of configuration to factory defaults

## 8.17 Reboot

You can reboot (restart) the Gateway if the device does not act as you expect. A reboot is a single step that involves both shutting down and then powering on.

Reboot the Gateway


To restart the device, go to , select *Reboot* and click *Yes*.



Pic. 29 Rebooting the Gateway.

## 8.18 Shutdown

*Shutdown* is to power off the Gateway in a way that ensures that no data is lost and that the system is not corrupted. All the settings will be saved.

Shutting down To properly shut down your device, go to , select *Shutdown*, click *Yes* to confirm.

**Do not disconnect the power until LED 1 (green) stops flashing!** Otherwise, the database may not be saved securely.

The only way how to switch the Gateway back on is to disconnect and re-connect power supply.

**Schneider Electric SA**

35 rue Joseph Monier  
92500 Rueil Malmaison - France  
Phone: +33 (0) 1 41 29 70 00  
Fax: +33 (0) 1 41 29 71 00

**Schneider Electric Limited**

Stafford Park 5, Telford  
Shropshire, TF3 3BL, UK  
Phone: +44 (0) 370 608 8 608  
Fax: +44 (0) 870 608 8 606

If you have technical questions, please contact the Customer Care Centre in your country.  
[schneider-electric.com/contact](https://www.schneider-electric.com/contact)

© 2022 Schneider Electric, all rights reserved

LSS\_100300\_SW\_EN 10/22