
SPC Bridge KNX gen 2 User Manual

Revision 1.0



History Record

Revision	Date	Author	Comment
1.0	October-2023	Lundix IT	First version

©2023 Lundix IT

Lundix IT
Renvägen 22
S-433 70 Sävedalen
Sweden
info@lundix.se

Contents

1	INTRODUCTION.....	5
1.1	SPC Bridge KNX (gen 2)	5
1.2	Main Features.....	5
1.3	Prerequisites.....	5
1.4	Package Content.....	6
1.5	Case Options	6
1.6	Hardware	7
1.6.1	Reset Button	7
1.7	Default Credentials	7
2	GETTING STARTED.....	8
2.1	EULA Agreement.....	8
2.2	Install the KNX Interface	8
2.3	Ethernet Connection	8
2.4	Power On.....	8
2.5	Access the Web Admin GUI	8
2.6	Assign a Static IP Address.....	10
2.7	Setup Communication with the SPC Panel.....	10
2.8	KNX ETS Configuration.....	10
2.9	SPC Bridge Security Hardening.....	10
3	BASIC SYSTEM ADMINISTRATION	11
3.1	Network	11
3.2	Time.....	12
3.3	Web GUI.....	12
4	CONFIGURATION.....	13
4.1	SPC Communication (FlexC).....	13
4.1.1	Setup FlexC Communication in the SPC Panel.....	13
4.1.2	Setup FlexC Communication in the SPC Bridge.....	14
4.2	SPC Communication Test.....	15
4.2.1	SPC Areas.....	15
4.2.2	SPC Zones.....	15
4.2.3	SPC Outputs (MG).....	16
4.2.4	SPC Doors.....	17
4.2.5	API Test Tool	17
4.3	KNX	21
4.3.1	KNX Interface	21
4.3.2	KNX Datapoints	22
4.3.3	KNX Scenes.....	23

4.4	Overview	24
4.4.1	Services.....	24
4.4.2	System Status	25
4.4.3	System Info.....	25
5	ETS KNX CONFIGURATION.....	26
5.1	First Time Configuration	26
5.2	Communication Objects.....	27
5.2.1	KNX Datapoint Map.....	27
5.2.2	Global System Objects.....	27
5.2.3	SPC Area Commands	28
5.2.4	SPC Zone Commands.....	29
5.2.5	SPC Output Commands.....	29
5.2.6	SPC Door Commands.....	30
5.2.7	SPC Area Status Objects	30
5.2.8	SPC Zone Status	32
5.2.9	SPC Output Status	32
5.2.10	SPC Door Status Objects.....	32
6	ADVANCED SYSTEM ADMINISTRATION.....	34
6.1	SSH	34
6.1.1	SSH User	34
6.1.2	SSH Keys.....	34
6.2	Firmware	36
6.2.1	Factory Reset.....	36
6.2.2	Upgrade Firmware	36
6.3	Enable HTTPS.....	38
7	TROUBLESHOOTING.....	39
7.1	Log	39
7.1.1	SPC Bridge System Events.....	39
7.1.2	All System Events	39
7.2	FlexC Communication Tests.....	40
7.3	Invalid Network Settings.....	40
8	FACTORY RESET.....	40
9	APPENDICES	41
9.1	Hardware Specification.....	41
9.2	SPC Command Error Codes.....	41
9.3	End-User License Agreement for SPC Bridge (EULA)	44
9.4	Open Source Software	45

1 Introduction

1.1 SPC Bridge KNX (gen 2)



SPC Bridge

Weinzierl KNX interface 332

Weinzierl KNX interface 312

SPC Bridge KNX (gen 2) allows interfacing Vanderbilt SPC intrusion system to a KNX system. Using the SPC Bridge you are able to use events from all your SPC connected motion detectors, door/window contacts, fire detectors and alarm status for automations in your KNX system. SPC Bridge KNX includes a certified Weinzierl KNX interface (332 or 312) for a reliable and approved connection to the KNX bus.

1.2 Main Features

- Local network communication based on Vanderbilt's official IP protocol FlexC.
- Direct connection to KNX-bus using Weinzierl KNX interface 332 or 312. The standard KNX tool ETS is used for the configuration.
- Provides status and states of SPC areas, zones, outputs and doors.
- Support for commands to control SPC areas, zones, outputs and doors. e.g. arm/disarm, inhibit zones and set outputs. The commands allowed are determined by the SPC panel's settings.
- Web based Admin GUI.
- Versatile tools for troubleshooting.
- Technically, a maximum of 256 zones, 16 areas, 8 doors and 16 outputs (mapping gates) are supported. However, in practice, it is advisable not to exceed more than 128 zones to ensure optimal performance.

1.3 Prerequisites

- Vanderbilt SPC panel with firmware ≥ 3.6 (3.6 was the first version with support for FlexC)
- Network router with DHCP server enabled
- SPC Bridge and SPC panel connected to same local network

- Internet access (to be able to use time synchronization via NTP)
- KNX system
- KNX configuration tool ETS version ≥ 5

1.4 Package Content

- SPC Bridge device
- Ethernet cable, 0.8 meter
- Power adapter 5V, 2.4A
- USB A to C power cable, 1.5 meter
- KNX interface Weinzierl 332 or 312 (If 312 an USB A-B cable, 0.5m is also included)

1.5 Case Options

SPC Bridge KNX is available with two different case options, frosted aluminium alloy or lavender colored ABS plastic.

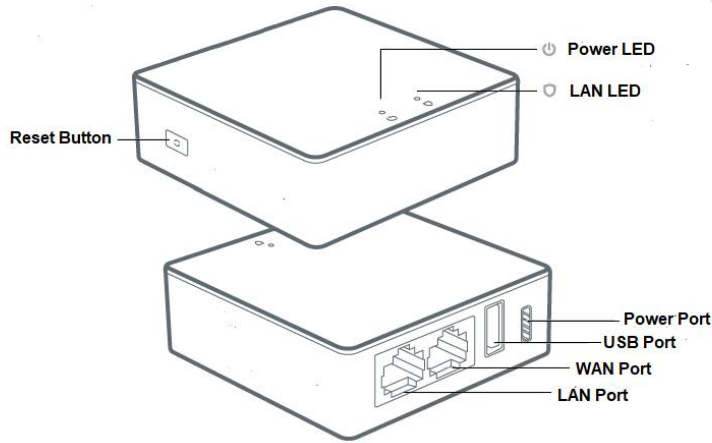


Aluminium alloy



ABS plastic, lavender colored

1.6 Hardware



Buton/LED	Description
Reset Button	Button to reboot or factory reset the SPC Bridge. See details in section 1.6.1
Power LED	Steady green during startup. Steady white when device is in normal mode. For indications during reset see section 1.6.1
LAN LED	Flashing white when device is connected to a LAN with activity

1.6.1 Reset Button

Depending on how long you hold down the reset button, the function will vary as follows:

Press and hold	Description	Power LED
Less then 3 seconds	No function	Steady green
3 to 10 seconds	The device will reboot (No settings are changed)	Slow flashing green
10 to 20 seconds	The device will be factory reset. All settings will be reset to default values. See section 1.7 for the default values.	Fast flashing green
More then 20 seconds	No function	Steady green

1.7 Default Credentials

As default the SPC Bridge has following credential values:

Setting	Value
Web GUI login	Username: spcbridge Password: Spcbridge!
SSH login	Username: root Password: Spcbridge!
FlexC ATP Encryption Key	0000111122223333444455556666777788889999aaaabbbbccccdddeeeeffff
FlexC SPC Username / Password	Username: spcbridge

	Password: spcbridge!
FlexC SPC Password	spcbridge!

Please note, for security reasons, all default values should be changed to your own.

2 Getting Started

2.1 EULA Agreement

Read carefully **End-User License Agreement for SPC Bridge (EULA)** in section 9.3 in this document. If you do not agree to the terms of the EULA, do not install or use the SPC Bridge.

2.2 Install the KNX Interface

Connect the included KNX interface, Weinzierl 332 or 312, to the SPC Bridge USB port. Connect the KNX bus cable to the KNX bus connector on the KNX interface. **Please note**, the default individual device address of the KNX interface is **15.15.255**. If this address already is in use you should change the address (see section 4.3.1) before you physically connect the interface to the KNX-bus.

2.3 Ethernet Connection

Default network protocol is DHCP. Connect the SPC Bridge **LAN** port, with a regular network cable (included), to your network switch or router.

2.4 Power On

Connect the power adapter to the SPC Bridge using the included power cable. Plug the power adapter into a wall outlet.

2.5 Access the Web Admin GUI

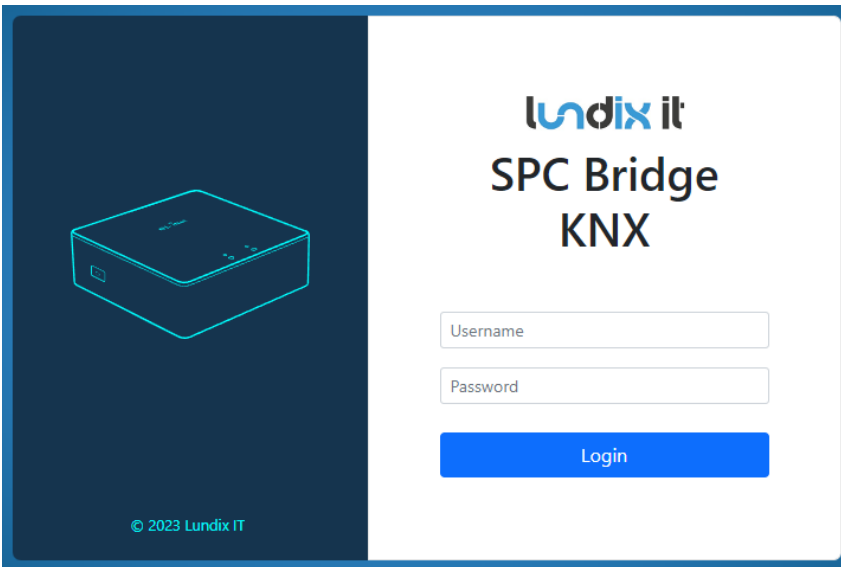
Wait (~3 minutes) until the SPC Bridge has started up. Get the **Device ID** (7 characters) from the back of your SPC Bridge device.

To visit the Login page, open a web browser (we recommend Chrome) and go to:

```
http://SPC-BRIDGE-DEVICE_ID.local
```

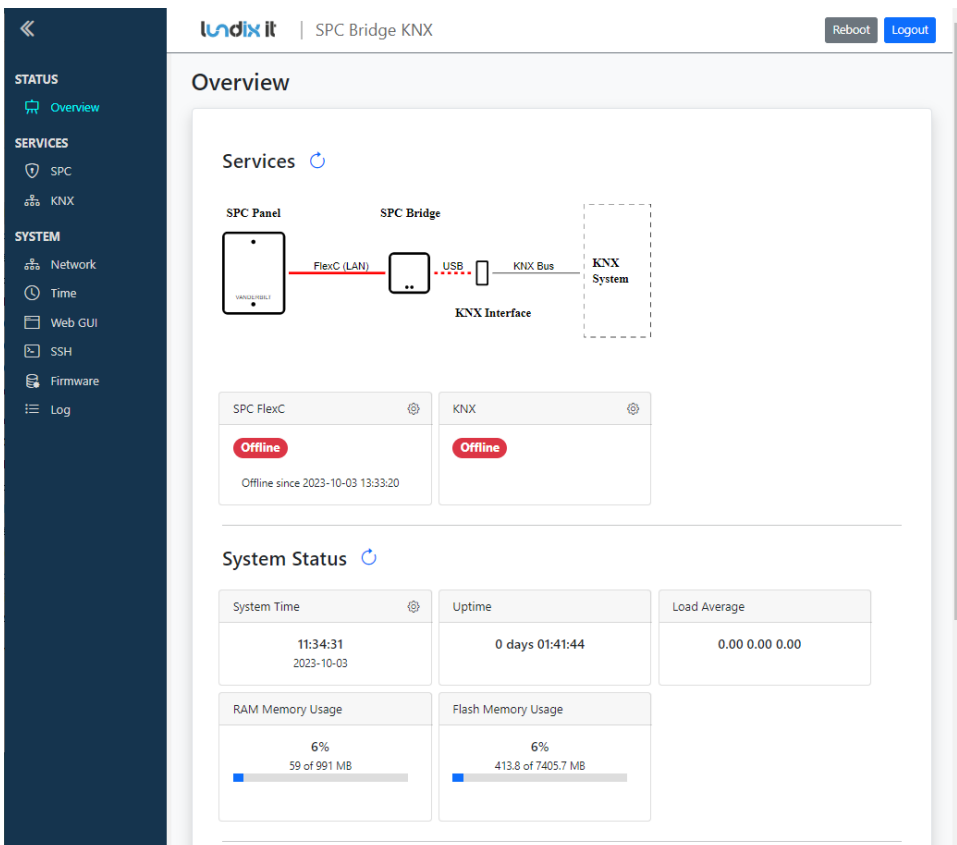
Example: If your device has ID *aj4c5ab* you should give the url: <http://SPC-BRIDGE-aj4c5ab.local>

Please note, if the url <http://SPC-BRIDGE-<Device ID>.local> isn't working you can check your router for the IP address of the SPC Bridge and use the url http://SPC_BRIDGE_IP instead.



On the login page, login with the username **spcbridge** and the password **Spcbridge!** (default).

After succesful login you will see the Overview page. This page provides a summarized overview of the Bridge's services and system status.



2.6 Assign a Static IP Address

As default the network protocol is DHCP, but it is recommended to assign a static IP address to the SPC Bridge. Follow the instructions in section **Basic System Administration, Network** (section 3.1) to set a static IP address.

2.7 Setup Communication with the SPC Panel

Configure the FlexC communication to the SPC Panel by following the instructions in section **Configuration, SPC Communication** (section 4.1) .

2.8 KNX ETS Configuration

Add the SPC Bridge KNX to your ETS project by following the instructions in section **Configuration, ETS KNX configuration** (section 5).

2.9 SPC Bridge Security Hardening

For reasonable security you should always change the default settings for:

- Web GUI user password. (*System > Web GUI – Login User*).
- SSH user password. (*System > SSH*)
- FlexC encryption key and user credentials. (*Services > SPC > FlexC*).

In sensitive environments, it may also be wise to enhance security further by:

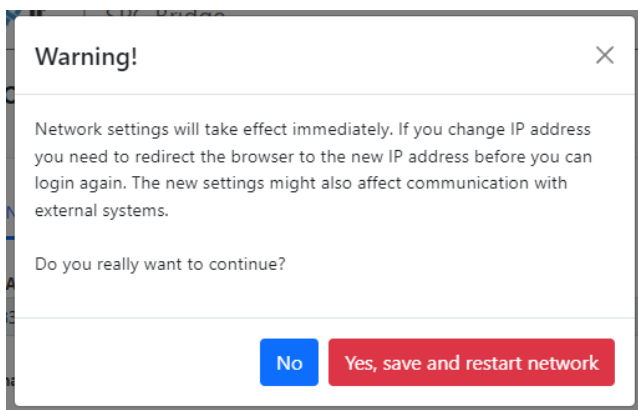
- Only allow HTTPS when accessing the Web GUI (see section 6.3).
- Only allow key-based authentication for SSH access (see section 6.1).

3 Basic System Administration

3.1 Network

As default the SPC Bridge uses DHCP to obtain an IP Address. To ensure that the Bridge retains the same IP address on the LAN port, for example, after the router has been restarted, the Bridge should be assigned a static IP address. You change the LAN settings in **System > Network**. Uncheck **Enable DHCP** to set a static IP and check/alter all the other network settings before saving.

The settings will take effect immediately when you **Save & Apply** and have acknowledged the warning message. You have to manually redirect your browser if you have changed the IP address.



Please note, the WAN port should only be used as a last resort if you are unable to connect to the LAN port. The WAN port always uses DHCP and cannot be changed via the WEB GUI.

3.2 Time

In **System > Time** you can change the time zone, sync the time with the current time of your browser and also configure the NTP (Network Time Protocol) service.

Time

Local Time

2023-09-16 11:01:57
Sync with browser

Time Zone

UTC
▼

Enable NTP

NTP servers

Save & Apply

Please note, the device has no RTC clock. During boot the Bridge can have incorrect time. Events that occur before the Bridge has received the current time via NTP can therefore have incorrect timestamps.

3.3 Web GUI

In **System > Web GUI**, you can change the password for the Web GUI login user. The username is not changeable, it is always spcbridge.

Web GUI

Login User

Login User

Username

spcbridge

New Password

Password
👁

Retype Password

Password
👁

Save & Apply

4 Configuration

4.1 SPC Communication (FlexC)

SPC Bridge is using Vanderbilt's official IP protocol FlexC to communicate with the SPC Panel. The communication is entirely local with no dependency on any cloud service. The communication is initialized by the SPC Panel. The Bridge acts as a FlexC client, RCT.

To set up the communication, it's easiest to first configure the SPC Panel and then the SPC Bridge.

4.1.1 Setup FlexC Communication in the SPC Panel.

Log in locally to the SPC Panel using SPC's web interface and follow the following instructions:

1. Select **Full Engineer** mode
2. Create a specific user for the SPC Bridge communication, e.g **spcbridge**. User profile should be **Manager** and you need also to define a **web password** for the user.

Note! The username must be 4 to 16 characters and the password 6 to 16 characters. Username and password may only include following characters: a-z A-Z 0-9 . ! @ # \$ % _ + - = ; < > ?

Hint! To set a web password for a new user in SPC you need to login as the specific user first, using the pin code and go to Configuration -> Change Own Pin -> Change Web Password

3. Select **Communications -> FlexC -> Event Profiles**. Click on **Add** to add a new event profile. Give the event profile the name **SPC Bridge Events** and select (check) the report checkboxes for all event types. (You may consider reducing these settings later to just necessary events for the third-party application)
4. Select **Communications -> FlexC -> FlexC ATS**. Select **Add Custom ATS** and change following from the default settings:
 - ATS Name = SPC Bridge
 - Event Profile = SPC Bridge Events (created in step 3)
 - ATS Polling Timeout = 60 seconds
 - Uncheck Generate FTC and Re-queue Events
5. Select **Add ATP to FlexC RCT** and change following from the default settings:
 - SPT Account Code = 999
 - RCT URL or IP Address = IP Address of the SPC Bridge
 - ATP Category = Cat 6 [Ethernet]
6. Open **Advanced ATP Settings** and change following from the default settings:
 - Encryption Key Mode = Fixed Encryption
 - Encryption key (64 hex digits) = Your own key (This key should be copied to the SPC Bridge)

Please note, in Full Engineer mode, the panel does not report any events to the bridge, so it's very important to be logged out of Engineer mode during communication tests.

4.1.2 Setup FlexC Communication in the SPC Bridge

To configure the FlexC communication in the SPC Bridge goto **Services > SPC > FlexC**. If you have followed the SPC Panel instructions in previously section you only have to update the form with the encryption key and the user credentials you created in the SPC Panel.

The screenshot shows the SPC FlexC configuration interface. At the top, there are navigation tabs: FlexC (selected), SPC Areas, SPC Zones, SPC Outputs (MG), SPC Doors, and API Test Tool. Below the tabs, there are several input fields with labels and icons for clearing, copying, and toggling visibility:

- ATP Encryption Key:** A long text input field with a 'Generate random key' icon (X), a 'Copy key to clipboard' icon (C), and a 'Show/Hide key' icon (E). Below it is a note: "64 hex digits key (0-9, a-f, A-F). Leave blank if you don't want to change the current key."
- SPT Account Code:** A text input field containing the value "999".
- RCT ID:** A text input field containing the value "1".
- RCT TCP Port:** A text input field containing the value "52000".
- SPC Username:** A text input field containing the value "spcbridge".
- SPC Password:** A text input field with a 'Show/Hide key' icon (E). Below it is a note: "Leave blank if you don't want to change the current password (and haven't changed the username)".

A blue "Save & Apply" button is located at the bottom right of the form.

Element	Description
ATP Encryption Key	ATP Encryption Key. 64 hex numbers (0-9, a-f, A-F). Must match corresponding key in SPC Panel FlexC settings. (Default key: 000011112222...ddddeeeeffff) NOTE! Of security reason a saved encryption key is never shown again. Just leave the field blank if you don't want to change the key.
Generate random key	Button to generate a random keyvalue. NOTE! If you use this feature do not forget to update the SPC Panel with same value.
Copy key to clipboard	Button to copy the key in the input field to clipboard.
Show/Hide key	Button to show the key in plain text. Only valid during editing of a new key. Saved key is not possible to show again.
SPT Account Code	SPT Account Code. Must match corresponding key in SPC Panel FlexC settings.
RCT ID	RCT Id. Must match corresponding id in SPC Panel FlexC settings.
RCT TCP Port	RCT TCP Port. Must match corresponding value in SPC Panel FlexC settings.
SPC Username and Password	User Credentials for FlexC communication. User must be defined in the SPC Panel and have a corresponding web password. Valid username: 4 to 16 characters (a-z, A-Z, 0-9, .!@#\$%_+~;<>?) Valid password: 6 to 16 characters (a-z, A-Z, 0-9, .!@#\$%_+~;<>?)

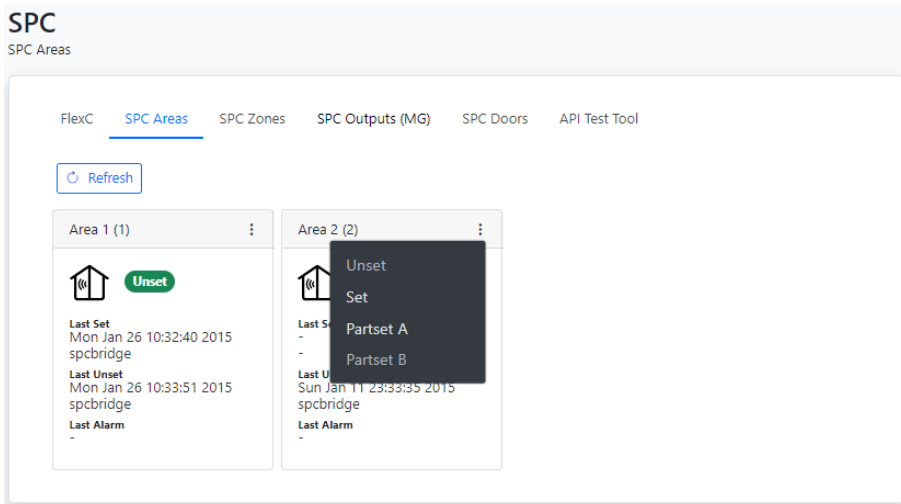
NOTE! Of security reason a saved password is never shown again. Just leave the field blank if you don't want to change the password.

4.2 SPC Communication Test

To ensure that communication functions correctly between the SPC Bridge and the SPC Panel, you can use the tests provided in **Services > SPC > SPC Areas, Zones, Outputs (MG), Doors** and for more advanced tests you can use the **API Test Tool**.

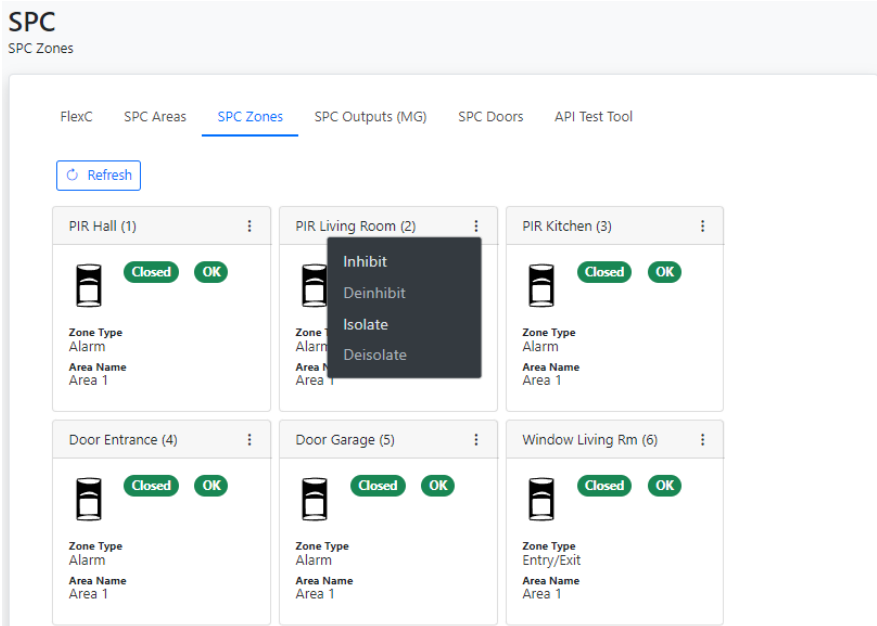
4.2.1 SPC Areas

On the page **Services > SPC > SPC Areas**, the status of your alarm areas are displayed. It is also possible to send commands, such as arming (set) and disarming (unset) the areas. The commands are available in the popup menu for each alarm area.



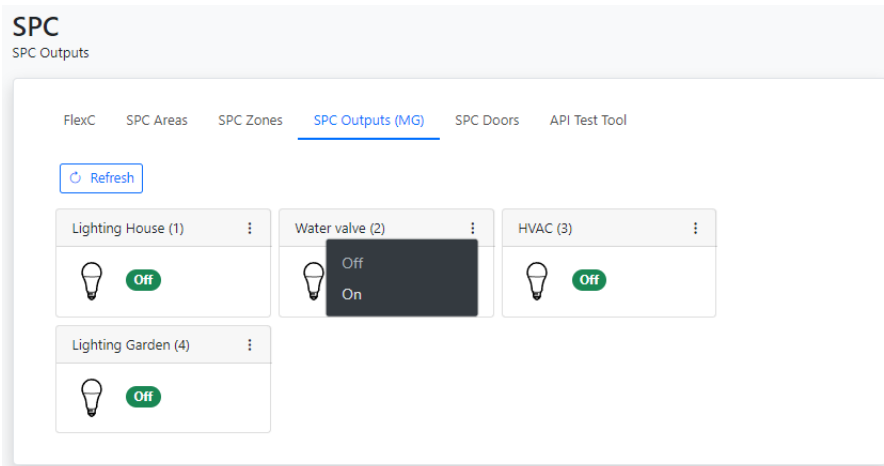
4.2.2 SPC Zones

On the page **Services > SPC > SPC Zones**, the status of your alarm zones are displayed. It is also possible to send commands, such as inhibit and isolate the zones. The commands are available in the popup menu for each alarm zone.



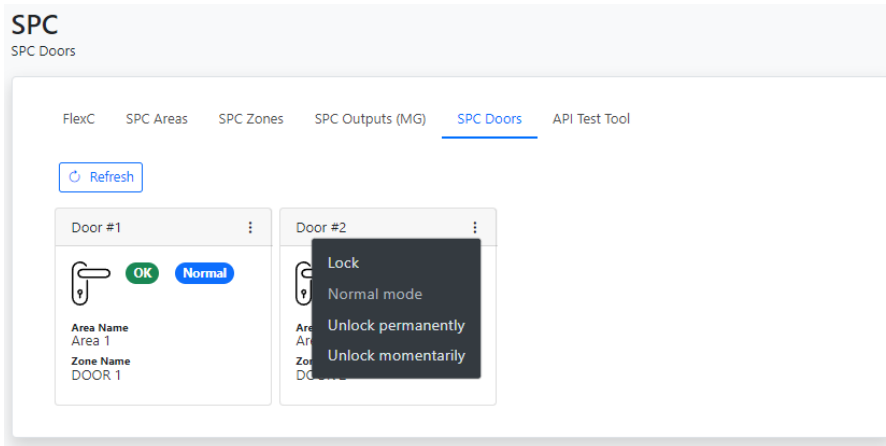
4.2.3 SPC Outputs (MG)

On the page **Services > SPC > SPC Outputs (MG)**, the status of your outputs, actually mapping gates, are displayed. It is also possible to send commands to control the outputs. The commands are available in the pop up menu for each output.



4.2.4 SPC Doors

On the page **Services > SPC > SPC Doors**, the status of your door locks are displayed. It is also possible to send commands the doors. The commands are available in the popup menu for each door.



4.2.5 API Test Tool

The API Test Tool is a very useful tool for testing and troubleshooting the Bridge's REST/Websockets API. The tool is also very helpful for integrators who want to learn the API.

SPC
API Test Tool

FlexC SPC Areas SPC Zones SPC Outputs (MG) SPC Doors API Test Tool

Request

Change Area Mode (specific area) ▼

Inhibit open zones (forced)

Area ID

Unset (Disarm)
 Partset A
 Partset B
 Fullset (Arm)
 Delayed Fullset

PUT Send request to SPC

[Show description](#)

Reply

Tree View ⌕ ⌵ success

```

reply
  status: success
  data
    reply_area_change_mode
      result: 0
      cmd_result: OK
      area_change_mode
        area_id: 1
        result: 0
        
```

Events

List View ▶ || × ↺ connected

Partset A	2015-01-28 01:39:29
Area: Area 1 (1), User: spcbridge (7),	
SIA: NL (1), Event ID: 3502	
#155	
Remote Partset A	2015-01-28 01:39:29
Area: Area 1 (1), User: spcbridge (7),	
Event ID: 3506	
#156	

The tool has three sections:

- Request. Here, you “build” and send an API request.
- Reply. Displays the response from the API on a request.
- Events. Displays real-time events from the API.

Request

Request

Change Area Mode (specific area) ▼

Inhibit open zones (forced)

Area ID

Unset (Disarm)
 Partset A
 Partset B
 Fullset (Arm)
 Delayed Fullset

PUT /spc/area/1/set_a Send request to SPC

[Show description](#)

In the Request section of the test tool you “build” and send an API request.

First, select the type of request you want to build from the options menu.

Request

Change Area Mode (specific area) ▼

- Area**
 - Get Area Status
 - Change Area Mode (specific area)**
 - Change Area Mode (all areas)
- Door**
 - Get Door Status
 - Control Door
- Output**
 - Get Output Status
 - Control Output
- Zone**
 - Get Zone Status
 - Control Zone

Then, choose the parameter settings you desire. Only parameters that are applicable to the selected request type will be displayed.

Inhibit open zones (forced)

Area ID

Unset (Disarm)
 Partset A
 Partset B
 Fullset (Arm)
 Delayed Fullset

The API request string will be displayed in plain text.

PUT /spc/area/1/set Send request to SPC

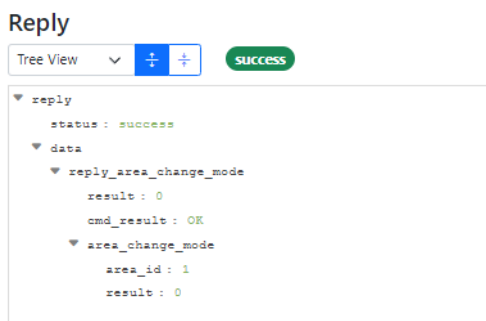
[Show description](#)

Finally, send the command by clicking the **Send request to SPC** button. The response will be shown in the Reply section.

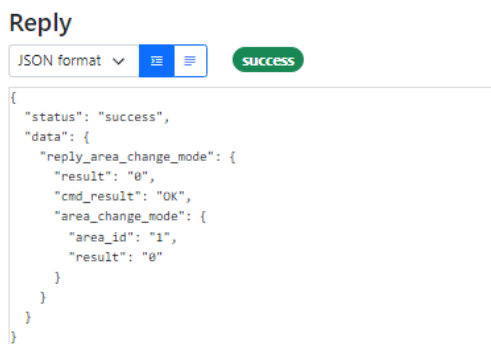
For a detailed protocol description of the selected request type, click on **Show description**.

Reply

The response on a request is shown in the Reply section. You can choose to display the response in Tree view or JSON format.



Reply in tre view format



Reply in JSON format

Events

Real-time events (SIA Events) are shown in the Events section. You can choose to display the events in list view or JSON format. You can also pause, resume and clear the eventlog. If you have lost the websocket connection you can click on the Reconnect button to resume the connection.

Events

List View ▶ ⏸ ✕ 🔄 connected

Partset A Area: Area 1 (1), User: spcbridge (7), SIA: NL (1), Event ID: 3502	2015-01-19 02:12:58	#69
Remote Partset A Area: Area 1 (1), User: spcbridge (7), Event ID: 3506	2015-01-19 02:12:58	#70

Events in list view format

Events

JSON format ☰ ☰ ▶ ⏸ ✕ 🔄 connected

```

{
  "ev_seq": "79",
  "ev_grp": "9",
  "ev_id": "3502",
  "ev_desc": "Partset A",
  "timestamp": "1421633108",
  "timestamp_spc": "01050819012015",
  "sia_code": "NL",
  "sia_address": "1",
  "cid_code": "456",
  "cid_qual": "3",
  "area_id": "1",
  "area_name": "Area 1",
  "user_id": "7",
  "user_name": "spcbridge"
}
[
  {
    "ev_seq": "80",
    "ev_grp": "9",
    "ev_id": "3506",
    "ev_desc": "Remote Partset A",

```

Events in JSON format

4.3 KNX

4.3.1 KNX Interface

On the page **Services > KNX > KNX Interface** you can configure the KNX interface.

KNX
KNX Interface

[KNX Interface](#) [KNX Datapoints](#) [KNX Scenes](#)

Programming Mode
Off 🔄 Activate

Individual Address
15.15.255 Save

KNX Bus State
Offline

Manufacturer
Weinzierl

Serial Number
00 c5 01 01 d4 f1

Protocol Version
2.0

Configured Datapoints
0 of 1000

Element	Description
---------	-------------

Programming Mode	Click on Activate/Deactivate button to set/unset the interface programming mode. NOTE! The interface has no physical programming mode button, so you need to use this feature when ETS ask you to set the interface in programming mode. Normally this will only happen when you do a full download.
Individual Address	Individual KNX address of the interface. Can also be changed using ETS.
KNX Bus State	Shows state of the KNX connection. Online or Offline.
Manufacturer	KNX interface manufacturer
Serial Number	KNX interface serial number
Protocol Version	KNX interface protocol version
Configured Datapoints	Number of datapoints that are linked to Group Addresses.

4.3.2 KNX Datapoints

On page **Services > KNX > KNX Datapoints**, you can view the current values of the KNX datapoints.

The screenshot shows the 'KNX Datapoints' interface. At the top, there are tabs for 'KNX Interface', 'KNX Datapoints' (which is active), and 'KNX Scenes'. Below the tabs is a dropdown menu set to 'SPC Zone States', a refresh button, and a checked checkbox for 'Hide unused datapoints'. The main area contains a table with the following data:

Datapoint #	Description	DPT	Value	KNX Update Status	Last update
301	Zone 1 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
302	Zone 2 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
303	Zone 3 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
304	Zone 4 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
305	Zone 5 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
306	Zone 6 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
307	Zone 7 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
308	Zone 8 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
309	Zone 9 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
311	Zone 11 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19
313	Zone 13 state	DPT1	0	Not connected to Group Address	2023-10-03 11:53:19

Element	Description
Hide unused datapoints	If this is checked, only datapoints that have been accessed (from SPC side) is shown.
Datapoint #	Datapoint address
Description	Datapoint description
DPT	KNX data type
Value	Current value
KNX Update Status	Access status reported from the KNX interface.

	<p>OK: The value was successfully sent to KNX bus Not connected Group Address: Datapoint is'nt linked to a Group Address (by ETS)</p> <p>Other possible error status (should'nt normally appear) : Internal Error, Not found, Buffer Error, Write Error, Unsupported, Invalid service, Invalid command, Invalid length, Invalid message, Busy, Failed request</p>
Last update	Last time the value was updated from the SPC system.

4.3.3 KNX Scenes

On page **Services > KNX > KNX Scenes**, you can configure the KNX scene numbers that should be sent to the KNX-bus when different SPC events occur. The scene number is sent to the KNX-bus via a common datapoint (Scene Control Output), each time the assigned event occurs. The scene numbers are configured per alarm area and can have values between 1 to 64 (Set 0 will disable the event).

An individual scene number can be assigned to following SPC events:


- Area becomes unset
- Area becomes partset A
- Area becomes partset B
- Area becomes fullset
- Area reports an intrusion alarm
- Area reports a fire alarm

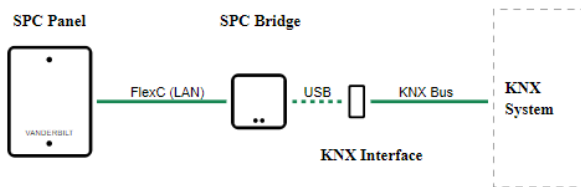
- Area reports a tamper alarm
- Area reports a confirmed alarm


4.4 Overview

The Overview page provides a summarized overview of the Bridge’s services and system status.

4.4.1 Services


Services 



SPC FlexC 

Online

Online since 2023-10-03 14:11:50

KNX 

KNX Bus Online

Data in sync with SPC

Section	Description	Status values
SPC FlexC	Shows the status of the FlexC communication with the SPC panel	Initializing: SPC Bridge is waiting for SPC Panel to connect first time. Online: Communication is up and running Offline: Communication is lost. SPC Bridge is waiting for SPC Panel to reconnect.
KNX	Shows the status of the KNX service	KNX Bus Online: KNX Interface is connected to the KNX bus. KNX Bus Offline: KNX interface isn't connected to the KNX bus. KNX Bus Unknown state: Unable to read the state, probably the KNX interface isn't connected to the USB port of the SPC Bridge. Data in sync with SPC: KNX service is available and data is in sync with the SPC Panel. Data may be out of sync with SPC: KNX data may be unreliable, probably due to communication problem with the SPC panel.

Use the refresh button if you want to update the status.

4.4.2 System Status

System Status

System Time	Uptime	Load Average
09:23:14 2023-09-26	0 days 22:54:42	0.00 0.00 0.00
RAM Memory Usage	Flash Memory Usage	
6% 64 of 991 MB	6% 414.0 of 7405.7 MB	

Section	Description
System Time	Shows the time of the SPC Bridge
Uptime	Shows how long time the SPC Bridge has been up and running.
Load Average	Cpu load average; last minute, last 5 minutes, last 15 minutes
RAM Memory Usage	Shows current RAM memory usage
Flash Memory Usage	Shows current flash memory usage

The system status is updated automatically every 5 seconds. You can also use the refresh button to update the status.

4.4.3 System Info

System Info

System Name	IP Address	Operating System
SPC-BRIDGE-vc4c0ca	192.168.0.137 dhcp	OpenWrt 21.02 SNAPSHOT r15812+869-46b6ee7ffc
Application	Firmware Version	Hardware Model
spc-bridge-knx-mt2500 - 1.0-1	v2.0.1	GLiNet GL-MT2500

Section	Description
System Name	Shows the system name
IP Address	Shows the IP Address and network protocol.
Operating System	Shows name and version the operating system.
Application	Shows name and version of the SPC Bridge application.
Firmware Version	Shows version of the firmware.
Hardware Model	Shows hardware model the SPC Bridge is based on

Use the refresh button if you want to update the status.

5 ETS KNX Configuration

5.1 First Time Configuration

To configure the KNX interface you should use the KNX standard configuration tool ETS. The configuration is based on a generic product database from Weinzierl, but adapted according to the Communication Objects below. For a quick start please copy and paste the configuration from one of the attached ETS project templates:

1. On **ETS project** page, import the template project file that best match your size of SPC system.
2. Open the template project. In the **Topology** tree, select and copy the item **1.1.1 SPC KNX SPC Bridge**.
3. Switch to your ordinary project and paste the copied item to the Topology tree (see example below).
4. Change the individual address to desired address of the KNX interface.
5. Download (full) configuration to the KNX interface. **NOTE!** To set the KNX interface in **programming mode** you need to use SPC Bridge Web GUI, see section **KNX Interface Info (Programming Mode)**.

After successful first time configuration you can link the communication objects (datapoints) to group addresses as usual.

Number	Name	Object Function	De	Gr	Length	C	R	W	T	U
1	SPC sync status	DPT 5			1 byte	C	R	-	T	-
10	Scene control output	DPT 18			1 byte	C	-	-	T	-
11	Area unset command	DPT 5			1 byte	C	-	W	-	-
12	Area partset A command	DPT 5			1 byte	C	-	W	-	-
13	Area partset B command	DPT 5			1 byte	C	-	W	-	-
14	Area fullset command	DPT 5			1 byte	C	-	W	-	-
15	Area delayed fullset command	DPT 5			1 byte	C	-	W	-	-
20	Area command reply status	DPT 5			1 byte	C	R	-	T	-
21	Zone inhibit command	DPT 5			1 byte	C	-	W	-	-
22	Zone deinherit command	DPT 5			1 byte	C	-	W	-	-
23	Zone isolate command	DPT 5			1 byte	C	-	W	-	-
24	Zone deisolate command	DPT 5			1 byte	C	-	W	-	-
30	Zone command reply status	DPT 5			1 byte	C	R	-	T	-
31	Area 1 unset	DPT 1			1 bit	C	R	-	T	-
32	Area 1 partset A	DPT 1			1 bit	C	R	-	T	-
33	Area 1 partset B	DPT 1			1 bit	C	R	-	T	-

5.2 Communication Objects

5.2.1 KNX Datapoint Map

States, status and commands from /to the SPC system are mapped to predefined datapoints/group objects on the KNX interface. The datapoint map has following main structure:

Datapoint Address	Usage
1 to 10	Global system objects
11 to 20	SPC area command objects
21 to 30	SPC zone command objects
31 to 270	SPC area status objects
301 to 556	SPC zone state objects
561 to 816	SPC zone status objects
821 to 830	SPC output command objects
831 to 846	SPC output state objects
851 to 860	SPC door command objects
861 to 940	SPC door status objects
941 to 1000	<i>Available for future features</i>

The map is designed for an absolute maximum of 16 areas, 256 zones, 16 outputs and 8 doors.

5.2.2 Global System Objects

Following global system global Group Objects will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
1	SPC com status	<p>0 = SPC communication is under initialization (datapoint values are not reliable), 1 = SPC communication is OK, 2 = SPC communication has failed (datapoint values are not reliable)</p> <p>To test SPC communication please see section 4.2.</p>	DPT 5	1-byte	CR-T-
10	Scene control output	<p>Common output for scene numbers sent to the KNX system when specified events occur. An individual scene number can be assigned to following SPC events:</p> <ul style="list-style-type: none"> • Area X becomes unset • Area X becomes partset A • Area X becomes partset B • Area X becomes fullset • Area X reports an intrusion alarm * • Area X reports a fire alarm ** • Area X reports a tamper alarm *** 	DPT 18	1-byte	C—T-

		<ul style="list-style-type: none"> Area X reports a confirmed alarm Area X reports all alarms are restored <p>(X = 1 to maximum number of areas, e.g. 16)</p> <p>The scene number is sent each time the assigned event occurs.</p>			
--	--	--	--	--	--

* Value is based on Alarm status for zone types Alarm, Exit/Entry, Glassbreak and Exit/Entry2.

** Value is based on Alarm status for zone type Fire.

*** Value is based on Alarm status for zone type Tamper and Tamper status for all zone types.

5.2.3 SPC Area Commands

Common for all SPC areas following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
11	Area unset command	ID of area to unset The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
12	Area partset A command	ID of area to partset A The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
13	Area partset B command	ID of area to partset B The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
14	Area fullset command	ID of area to fullset (immediately) The success/error of the command is reported in "Area command reply status". The fail to set reason is reported in "Area fail to set reason"	DPT 5	1-byte	C-W--
15	Area delayed fullset command	ID of area to fullset when exit time has expired The success/error of the command is reported in "Area command reply status". The fail to set reason is reported in "Area fail to set reason" (after exit time has expired or been canceled)	DPT 5	1-byte	C-W--
20	Area command reply status	0 = Last area command succeeded, 1-255 = Area command failed error code.	DPT 5	1-byte	CR-T-

		Codes are listed in section 7.1 SPC Command Error Codes.			
--	--	--	--	--	--

Area ID = 1 to maximum number of areas (16).

5.2.4 SPC Zone Commands

Common for all SPC zones following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Attributes
21	Zone inhibit command	ID of zone to inhibit The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
22	Zone deinhibit command	ID of zone to deinhibit The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
23	Zone isolate command	ID of zone to isolate The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
24	Zone deisolate command	ID of zone to deisolate The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
30	Zone command reply status	0 = Last zone command succeeded, 1-255 = Zone command failed error code. Codes are listed in section 7.1 SPC Command Error Codes.	DPT 5	1-byte	CR-T-

Zone ID = 1 to maximum number of zones (256).

5.2.5 SPC Output Commands

Common for all SPC outputs (mapping gates) following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Attributes
821	Output Off command	ID of output (mapping gate) to switch Off The success/error of the command is reported in "Output command reply status".	DPT 5	1-byte	C-W--

822	Output On command	ID of output (mapping gate) to turn On The success/error of the command is reported in "Output command reply status".	DPT 5	1-byte	C-W--
830	Output command reply status	0 = Last output command succeeded, 1-255 = Output command failed error code. Codes are listed in section 7.1 SPC Command Error Codes.	DPT 5	1-byte	CR-T-

Output ID = 1 to maximum number of outputs (mapping gates) (16).

5.2.6 SPC Door Commands

Common for all SPC doors following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Attributes
851	Door unlock momentarily command	ID of door to unlock momentarily The success/error of the command is reported in "Door command reply status".	DPT 5	1-byte	C-W--
852	Door set normal mode command	ID of door to set to normal mode The success/error of the command is reported in "Door command reply status".	DPT 5	1-byte	C-W--
853	Door set locked mode command	ID of door to set to locked mode The success/error of the command is reported in "Door command reply status".	DPT 5	1-byte	C-W--
854	Door set unlocked mode command	ID of door to set to unlocked mode The success/error of the command is reported in "Door command reply status".	DPT 5	1-byte	C-W--
860	Door command reply status	0 = Last door command succeeded, 1-255 = Door command failed error code. Codes are listed in section 7.1 SPC Command Error Codes.	DPT 5	1-byte	CR-T-

Door ID = 1 to maximum number of doors (8).

5.2.7 SPC Area Status Objects

For each SPC area following Group Objects will be available:

Relative address *	Name	Values	Datapoint Type	Length	Flags
+1	Area X unset	0 = Area is not unset, 1 = Area is unset (disarmed)	DPT 1	1-bit	CR-T-
+2	Area X partset A	0 = Area is not partset A, 1 = Area is partset A	DPT 1	1-bit	CR-T-
+3	Area X partset B	0 = Area is not partset B, 1 = Area is partset B	DPT 1	1-bit	CR-T-
+4	Area X fullset	0 = Area is not fullset, 1 = Area is fullset (armed)	DPT 1	1-bit	CR-T-
+5	Area X intrusion alarm	0 = Area has no intrusion alarm **, 1 = Area has at least one intrusion alarm **	DPT 1	1-bit	CR-T-
+6	Area X fire alarm	0 = Area has no fire alarm ***, 1 = Area has at least one fire alarm ***	DPT 1	1-bit	CR-T-
+7	Area X tamper alarm	0 = Area has no tamper alarm ***, 1 = Area has at least one tamper alarm ****	DPT 1	1-bit	CR-T-
+8	Area X confirmed alarm	0 = Area has no confirmed alarm **, 1 = Area has at least one confirmed alarm **	DPT 1	1-bit	CR-T-
+13	Area X unset user id	1 – 255 = SPC User ID of user who last unset the area, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus every time Area mode changes to Unset and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-
+14	Area X fullset user id	1 – 255 = SPC User ID of user who last fullset the area, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus when Area mode changes to Fullset (and if value changes of other reason e.g at startup)	DPT 5	1-byte	CR-T-
+15	Area X fail to set reason	0 = Area fullset succeeded, 1 = Interlocked, 2 = Calendar was preventing area fullset, 100 (0x64) = An area was preventing area fullset, 101 (0x65) = A (open) zone was preventing area fullset, 102 (0x66) = An alert was preventing area fullset, 200 (0xC8) = Other reason was preventing area fullset Will be sent to KNX bus every time Area mode changes to new value and if value changes of other reason e.g at exit delay and startup.	DPT 5	1-byte	CR-T-

--	--	--	--	--	--

X = 1 to maximum number of areas (16).

* Datapoint address = 30 + (X-1) * 15 + 'relative address'.

** Value is based on Alarm status for zone types Alarm, Exit/Entry, Glassbreak and Exit/Entry2.

*** Value is based on Alarm status for zone type Fire.

**** Value is based on Alarm status for zone type Tamper and Tamper status for all zone types.

5.2.8 SPC Zone Status

For **each SPC zone** (input) following Group Objects will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
300 + X	Zone X state	0 = Zone is Closed, 1 = Zone is Open	DPT 1	1-bit	CR-T-
560 + X	Zone X status	0 = OK, 1 = Inhibited, 2 = Isolated, 3 = Soak, 4 = Tamper, 5 = Alarm, 6 = OK, 7 = Trouble, 8 = Masked, 9 = Post Alarm	DPT 5	1-byte	CR-T-

X = 1 to maximum number of zones (256).

5.2.9 SPC Output Status

For **each SPC output (mapping gate)** following Group Objects will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
830 + X	Output X state	0 = Output is Off, 1 = Output is On	DPT 1	1-bit	CR-T-

X = 1 to maximum number of outputs (mapping gates) (16).

5.2.10 SPC Door Status Objects

For **each SPC door** following Group Objects will be available:

Relative address *	Name	Values	Datapoint Type	Length	Flags
+1	Door X normal mode	0 = Door is not in normal mode, 1 = Door is in normal mode	DPT 1	1-bit	CR-T-
+2	Door X locked mode	0 = Door is not in locked mode, 1 = Door is in locked mode	DPT 1	1-bit	CR-T-

+3	Door X unlocked mode	0 = Door is not in unlocked mode, 1 = Door is in unlocked mode	DPT 1	1-bit	CR-T-
+5	Entry granted user	1 – 255 = SPC User ID of user who last was granted entry, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus every time someone is granted entry and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-
+6	Entry denied user	1 – 255 = SPC User ID of user who last was denied entry, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus every time someone is denied entry and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-
+7	Exit granted user	1 – 255 = SPC User ID of user who last was granted exit, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus every time someone is granted exit and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-
+8	Exit denied user	1 – 255 = SPC User ID of user who last was denied exit, 0 = User Id is unknown For user ids > 255 (e.g the FlexC user) the value will be 255. Will be sent to KNX bus every time someone is denied exit and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-

X = 1 to maximum number of doors (8).

* Datapoint address = 860 + (X-1) * 10 + 'relative address'.

6 Advanced System Administration

6.1 SSH

As default the Bridge has SSH access via password authentication enabled. Username is always **root** and default password is **Spcbridge!**.

6.1.1 SSH User

In **SYSTEM > SSH > SSH User** you can change the password for the ssh user root. You can also disable the service if you are not allowing access via ssh password authentication.

The screenshot shows the 'SSH' configuration page with the 'SSH User' sub-tab selected. The page title is 'SSH' and the sub-tab is 'SSH User'. There are two tabs: 'SSH User' (active) and 'SSH Keys'. A checkbox labeled 'Enable Password Authentication' is checked. Below this, there are three input fields: 'Username' with the value 'root', 'New Password' with the placeholder 'Password', and 'Retype Password' with the placeholder 'Password'. Each password field has a toggle icon to the right. A blue 'Save & Apply' button is located at the bottom right of the form.

6.1.2 SSH Keys

In **SYSTEM > SSH > SSH Keys** you can upload a public key to allow SSH access via key authentication.

SSH

SSH Keys

SSH User
SSH Keys

i Public keys allow for the passwordless SSH logins with a higher security compared to the use of plain passwords. In order to upload a new key to the device, paste an OpenSSH compatible **public** key line into the input field below. It will be a long string starting with **ssh-rsa** and ending with something like **some-name@some-host**. For instance you can use the utility **ssh-keygen** to generate the key.

Type	Bits	Comment	Key
RSA	4096	gol@Probook	AAAAB3NzaC1yc2EAAAADAQABAAQCAQCxu...SNCeNOesRGmGNc84F5WJtw67wda3j9Q

Paste SSH key here...

Save & Apply

Public keys allow for passwordless SSH logins with a higher security compared to the use of plain passwords. In order to upload a new key to the device, paste an OpenSSH compatible public key line into the input field in the upload form. It will be a long string starting with ssh-rsa and ending with something like some-name@some-host. For instance you can use the utility *ssh-keygen* to generate the key. Here is an example how to generate a key on an Ubuntu system:

```
$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lundix/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lundix/.ssh/id_rsa.
Your public key has been saved in /home/lundix/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:47sizC5Vc42tiNmxAgiHjm545k19Q+rvcZrrwt23HC8 lundix@Probook
The key's randomart image is:
+---[RSA 4096]-----+
+----[SHA256]-----+
```

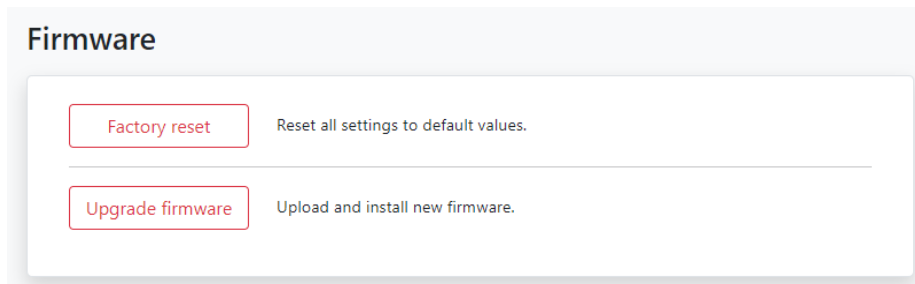
In the example above the **public key** will be in the file **id_rsa.pub**. It is the **content** of that file you should copy and paste to the input field in the upload form.

After successful upload of the key you should be able to do a SSH login, from the system that has the private key, without entering any password. (If you have given your own filename for the key you can use the SSH option **-i** to reference the private key file).

Please note, don't forget to disable SSH with password, in *System > SSH > SSH User*, if you only want to allow SSH access for those who have the correct key.

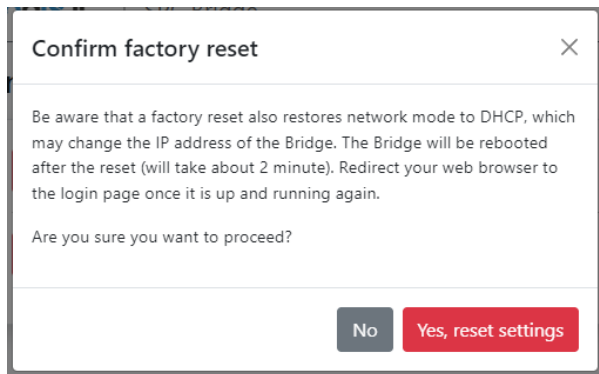
6.2 Firmware

On the **System > Firmware** page you can factory reset the device or upgrade the firmware on the SPC Bridge.



6.2.1 Factory Reset

If you want to reset all settings to factory default values you can click on the **Factory reset** button and acknowledge the warning message.

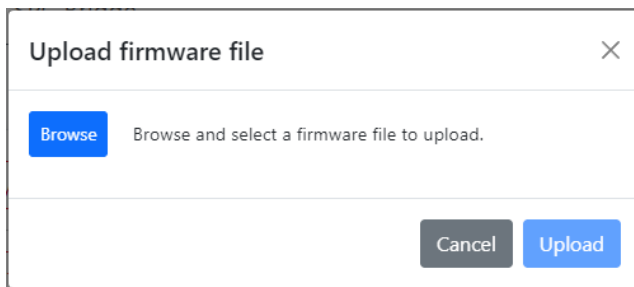


The factory reset will take about 2 minutes. Once the Bridge is up and running again, you have to redirect your web browser to the potentially new IP address (or <http://spc-bridge.local>).

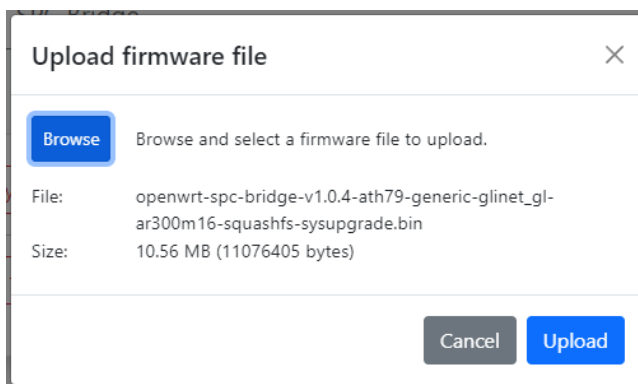
6.2.2 Upgrade Firmware

Firmware is upgraded by downloading and installing a firmware file. The file is provided by Lundix IT.

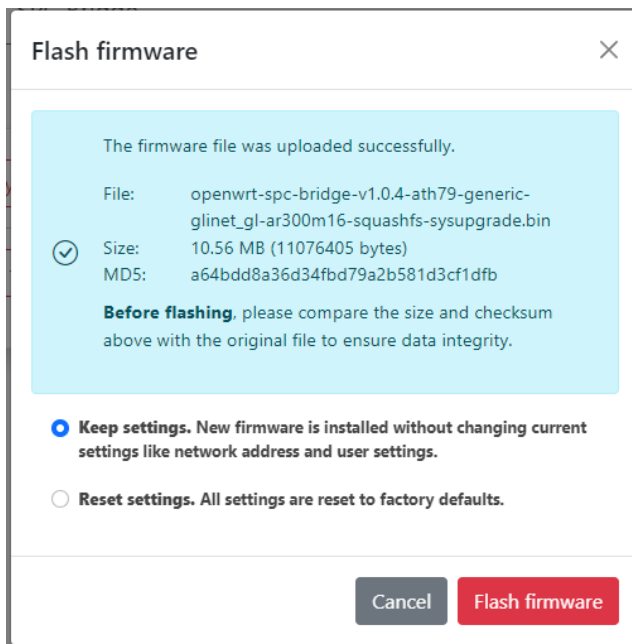
1. Click on the Firmware Upgrade button.
2. In the Upload firmware file window, browse and select the firmware file.



3. Upload the file to the SPC Bridge by clicking on the Update button.



4. On successful upload and validation you see the Flash firmware window. Check the size and checksum with the original file that was provided by Lundix IT.
For minor upgrades you can keep your current settings by selecting **Keep settings** that will upgrade the firmware without changing the current settings. For major upgrades it is preferable to select **Reset settings** instead, because the current settings may be incompatible with the new firmware. Reset settings will set all values to factory defaults.
Install the firmware by clicking on the **Flash firmware** button.



5. Finally you will get a message that confirms that the flashing has started. The flashing will take approximately 3 minutes. Once the installation is successfully completed, the Bridge will undergo an automatic reboot. Redirect your browser to the login page once the Bridge is up and running again..

Do not power off the Bridge during the firmware installation to prevent any disruptions.

6.3 Enable HTTPS

The SPC Bridge is intended to be used only on a secured local network (LAN). As default you can use HTTP to access the Web GUI. But, in some more sensitive environments you may consider to only allow HTTPS, for access of the Web GUI. Follow this instructions to enable HTTPS:

1. Login to the SPC Bridge using SSH.
2. Run the script `/opt/spc-bridge/scripts/enable_https.sh`

The script creates a self-signed certificate and configures the Bridge's web server to only allow HTTPS.

If you want to switch back to HTTP you can use the script `/opt/spc-bridge/scripts/disable_https.sh`

Please note, when switching between HTTPS and HTTP and vice versa, you may probably also need to clear the history cache in your web browser, to get the Web GUI to work as expected.

7 Troubleshooting

7.1 Log

7.1.1 SPC Bridge System Events

Shows all specific events related to the SPC Bridge application. The log is cleared on reboot. Click on the refresh button to update the view.

Log

SPC Bridge System Events

SPC Bridge System Events
All System Events

Refresh

```

Mon Sep 18 11:25:02 2023 daemon.info spc-bridge: spc-flex-gateway: FlexC connection is reestablished
Tue Jan 3 00:24:58 2023 daemon.info spc-bridge: spc-flex-gateway: Waiting for SPC panel to connect...
Tue Jan 3 00:24:57 2023 daemon.info spc-bridge: spc-flex-gateway: Starting up...

```

7.1.2 All System Events

Shows all events in the device system log. The log is cleared on reboot. Click on refresh button to update the view.

Log

All System Events

SPC Bridge System Events
All System Events

Refresh

```

Mon Sep 18 11:25:02 2023 daemon.info spc-bridge: spc-flex-gateway: FlexC connection is reestablished
Tue Jan 3 00:24:59 2023 user.notice firewall: Reloading firewall due to ifup of lan (br-lan)
Tue Jan 3 00:24:59 2023 daemon.info urandom_seed[1977]: Seed saved (/etc/urandom.seed)
Tue Jan 3 00:24:58 2023 daemon.info avahi-daemon[1490]: Registering new address record for 192.168.0.11
3 on br-lan.IPv4.
Tue Jan 3 00:24:58 2023 daemon.notice netifd: Interface 'lan' is now up
Tue Jan 3 00:24:58 2023 daemon.info avahi-daemon[1490]: New relevant interface br-lan.IPv4 for mDNS.
Tue Jan 3 00:24:58 2023 daemon.info avahi-daemon[1490]: Joining mDNS multicast group on interface br-la
n.IPv4 with address 192.168.0.113.
Tue Jan 3 00:24:58 2023 daemon.info procd: - init complete -
Tue Jan 3 00:24:58 2023 daemon.info spc-bridge: spc-flex-gateway: Waiting for SPC panel to connect...
Tue Jan 3 00:24:56 2023 daemon.notice netifd: lan (1816): udhcpd: lease of 192.168.0.113 obtained from
192.168.0.1, lease time 86400
Tue Jan 3 00:24:58 2023 daemon.notice netifd: lan (1816): udhcpd: broadcasting select for 192.168.0.11
3, server 192.168.0.1
Tue Jan 3 00:24:57 2023 daemon.info spc-bridge: spc-flex-gateway: Starting up...
Tue Jan 3 00:24:56 2023 daemon.info procd: /etc/rc.d/S99spc-bridge: mv: can't rename '/tmp/spc-bridg
e.log': No such file or directory
Tue Jan 3 00:24:56 2023 daemon.info avahi-daemon[1490]: Registering new address record for fe80::9683:c
4ff:fe1b:300e on br-lan.*.
Tue Jan 3 00:24:56 2023 daemon.info avahi-daemon[1490]: New relevant interface br-lan.IPv6 for mDNS.

```

7.2 FlexC Communication Tests

See section 4.2 how you can test that you have a working FlexC communication.

7.3 Invalid Network Settings

The WAN port has always DHCP enabled, so if you by mistake have saved incorrect network settings, causing you to no longer be able to access the SPC Bridge, you can move the network cable to the WAN port on the bridge, log in as usual in the Web GUI, and correct the LAN settings. Afterward, move the network cable back to the LAN port.

8 Factory Reset

If the Web GUI still is available you can reset all settings to default values on the page **System > Firmware**, see section 6.2. Otherwise you can do factory reset by press and hold the Reset button according to section 1.6.1. The factory reset will, for example, reset the LAN port protocol to DHCP and the credentials to the values listed in section 1.7.

9 Appendices

9.1 Hardware Specification

SPC Bridge KNX gen 2	
CPU	MediaTek MT7981B Dual-core, @1.3GHz
Storage	EMMC 8GB
Memory	DDR4 1GB
Power input	USB Type-C, 5V/2A
Power Consumption	<2.6W
Operating Temperature	0 – 40°C
Storage Temperature	-20 – 70°C
Dimension	70 x 70 x 22mm
Weight	60g (ABS plastic case) 157g (Aluminium alloy case)
Ethernet	1 x LAN port, 10/100/1000 Mbps 1 x WAN port (only used in emergency)
USB	1 x USB 3.0 Type-A port (host)
Buttons	1 x Reset button
Type Approval	CE, FCC, RoHS Compliant

9.2 SPC Command Error Codes

Error Code	Error Message
0	OK: Command succeeded
10	ERROR: Generic
11	ERROR: Unknown
12	ERROR: Missing ID
13	ERROR: Invalid ID
14	ERROR: Unknown Tag
15	ERROR: Memory Full
16	ERROR: Invalid Data
17	ERROR: Missing Data
18	ERROR: Invalid CRC
19	ERROR: Invalid Length
20	ERROR: Not ready
21	ERROR: Invalid Sequence No
22	ERROR: Invalid Decryption
23	ERROR: Invalid Connection Details
24	ERROR: Invalid Username

25	ERROR: Invalid Password
40	ERROR: Generic check failed
50	ERROR: Active
51	ERROR: Inactive
52	ERROR: Invalid User
53	ERROR: Invalid Number
54	ERROR: Authentication Failed
55	ERROR: Engineer Not Authorized
56	ERROR: Invalid Name
57	ERROR: Invalid Profile
58	ERROR: Invalid Site Code
59	ERROR: Invalid PIN
60	ERROR: Duplicate
61	ERROR: Invalid Card Number
62	ERROR: In use
63	ERROR: Global ID in use
64	ERROR: Global Data Protected
65	ERROR: No Rights
66	ERROR: System Set
67	ERROR: Cannot delete
68	ERROR: Cannot delete last
69	ERROR: Date
70	ERROR: Calendar
71	ERROR: Area
72	ERROR: Door
73	ERROR: Web password not enabled
74	ERROR: Null data
75	ERROR: Bad Command
76	ERROR: Pin Expired
77	ERROR: Blocked
78	ERROR: Not allowed in Engineer mode
79	ERROR: Cannot delete default profile
80	ERROR: Cannot edit default profile
100	ERROR: XML – Buffer Fail
101	ERROR: XML – Bad Format
102	ERROR: XML – Bad Data
103	ERROR: XML – Unknown Tag
104	ERROR: XML – Compulsory Parameter Not Found
120	ERROR: File – Fail
121	ERROR: File – No Space
122	ERROR: File –Not Found
123	ERROR: File – Header
124	ERROR: File – Flash
125	ERROR: File – Flash Verify

126	ERROR: File – Flash Erase
140	ERROR: HTTP – Compulsory Parameter Not Found
160	ERROR: SAM – WD Output
255	ERROR: SPC Communication error

9.3 End-User License Agreement for SPC Bridge (EULA)

IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SPC BRIDGE SOFTWARE OR HARDWARE.

SPC Bridge End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Lundix IT, Sweden, for the SPC Bridge software and hardware product(s) (referred to as the "PRODUCT") which may also include associated software components, media, printed materials, and "online" or electronic documentation. By installing, copying, or otherwise using the PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the PRODUCT between you and Lundix IT (referred to as "licenser"), and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not install or use the PRODUCT.

The PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The software is licensed, not sold.

GRANT OF LICENSE.

The PRODUCT is licensed as follows:

- The FlexC communication program is based on Vanderbilt propriety protocol FlexC and therefore **NOT open-source**.
- **All other software in SPC Bridge** is licensed under many different open source licenses.
- **Backup Copies.** You may make copies of the software as may be necessary for backup and archival purposes.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

- **Maintenance of Copyright Notices.**
You must not remove or alter any copyright notices on any and all copies of the PRODUCT.
- **Prohibition on Reverse Engineering, Decompilation, and Disassembly.**
You may not reverse engineer, decompile, or disassemble the program SPC Flex Gateway.
- **Support Services.**
Lundix IT may provide you with support services related to the PRODUCT ("Support Services"). Any supplemental software code provided to you as part of the Support Services shall be considered part of the PRODUCT and subject to the terms and conditions of this EULA.
- **Compliance with Applicable Laws.**
You must comply with all applicable laws regarding use of the PRODUCT.

COPYRIGHT

All title, including but not limited to copyrights, in and to the PRODUCT and any copies thereof are owned by Lundix IT or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by Lundix IT.

NO WARRANTIES

Lundix IT expressly disclaims any warranty for the PRODUCT. The PRODUCT is provided 'As Is' without any express or implied warranty of any kind, including but not limited to any warranties of

merchantability, noninfringement, or fitness of a particular purpose. Lundix IT does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the PRODUCT. Lundix IT makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb, or other such computer program. Lundix IT further expressly disclaims any warranty or representation to Authorized Users or to any third party.

LIMITATION OF LIABILITY

In no event shall Lundix IT be liable for any damages (including, without limitation, lost profits, business interruption, or lost information) rising out of 'Authorized Users' use of or inability to use the PRODUCT, even if Lundix IT has been advised of the possibility of such damages. In no event will Lundix IT be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise. Lundix IT shall have no liability with respect to the content of the PRODUCT or any part thereof, including but not limited to errors or omissions contained therein, libel, infringements of rights of publicity, privacy, trademark rights, business interruption, personal injury, loss of privacy, moral rights or the disclosure of confidential information.

9.4 Open Source Software

The SPC Bridge software is based on OpenWrt, a Linux distribution that bundles lots of third party software, under many different licenses. Source code for OpenWrt is available on <http://dev.openwrt.org>.

The most frequently used licenses are:

GNU General Public License (GPL) and GNU Lesser General Public License (LGPL) version 2. These firmware images contain software licensed under the GPLv2. A copy of that license can be found at <http://www.gnu.org/licenses/gpl-2.0.txt>.

Apache License version 2.0. These firmware images contain software licensed under the APLv2. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>. Modified files carry prominent notices stating who made the changes.

MIT License. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

END OF DOCUMENT