SPC Bridge gen 2 - User Manual

Revision 1.0

History Record

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

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

Contents

1 Introduction

1.1 SPC Bridge (gen 2)

SPC Bridge (gen 2) allows integration of Vanderbilt SPC intrusion system with a third-party system, e.g. a home or building automation system. Using the SPC Bridge you are able to use events from all your SPC connected motion detectors, door/window contacts, smoke detectors and alarm status for automations in the third-party system.

1.2 Main Features

- Local network communication based on Vanderbilt's official IP protocol FlexC.
- 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.
- Recommended for maximum 128 zones and 16 areas.

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)

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

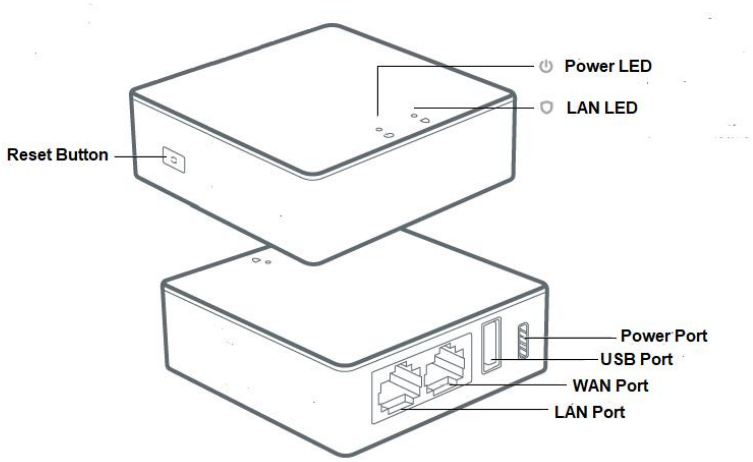
1.5 Case Options

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

Aluminium alloy

ABS plastic, lavender colored

1.6 Hardware



Button/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	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
FlexC SPC Username / Password	Username: spcbridge Password: spcbridge!
FlexC SPC Password	spcbridge!
Bridge API Credentials - Queries	Username: get_user Password: get_pwd
Bridge API Credentials - Commands	Username: put_user Password: put_pwd
Bridge API Credentials - Events	Username: ws_user Password: ws_pwd

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 8.3 in this document. If you do not agree to the terms of the EULA, do not install or use the SPC Bridge.

2.2 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.

2.3 Power On

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

2.4 Access the Web Admin GUI

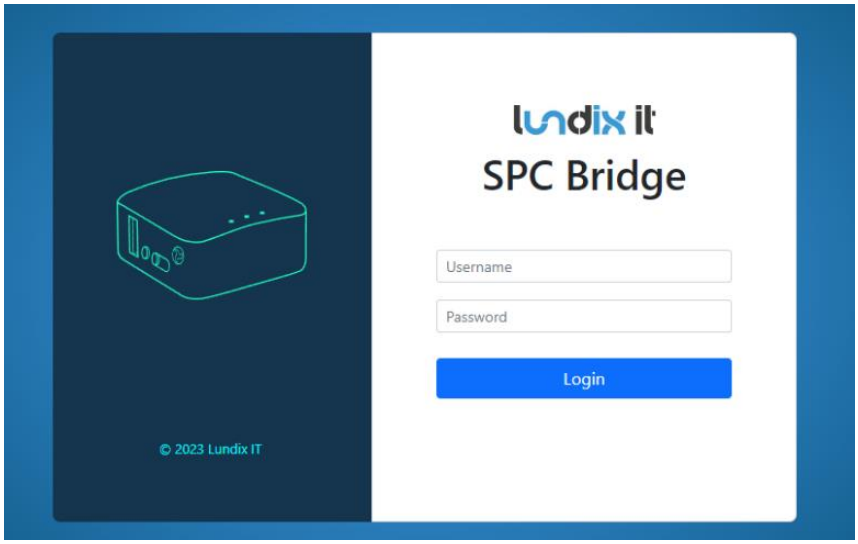
Wait (~3 minutes) until the SPC Bridge has started up. Get the ***Device ID*** (7 characters) from the back of your SPC Bridge device.

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

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

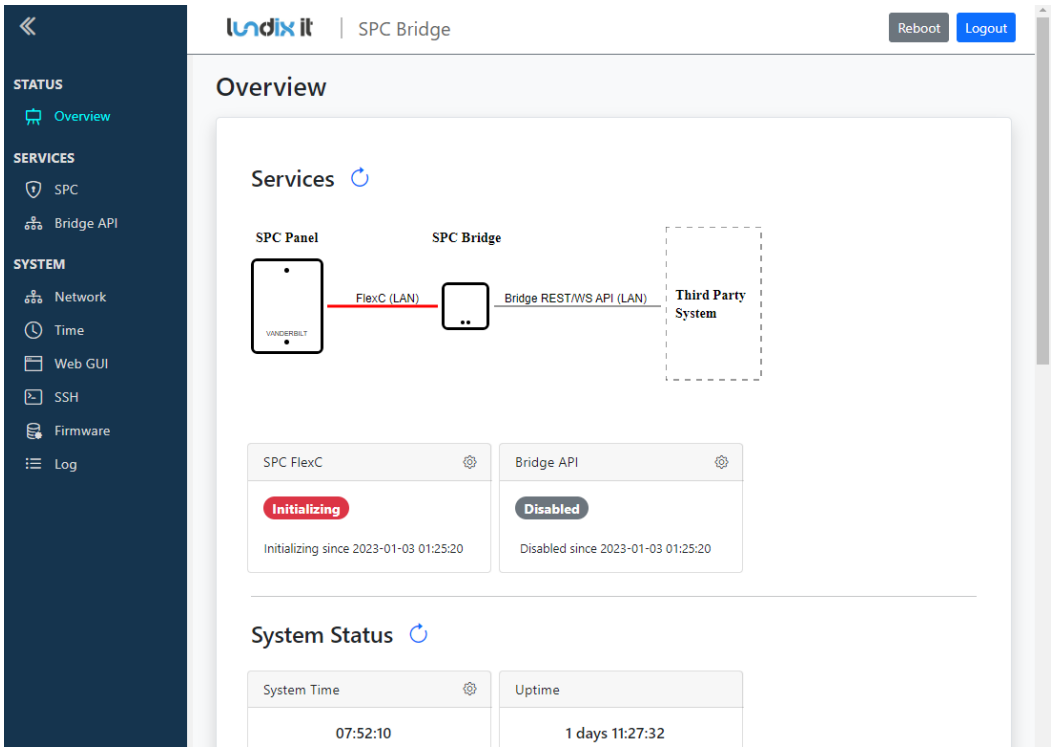
Example: If your device has ID *aj4c5ab* you should give the url: *http://SPC-BRIDGE-aj4c5ab.local*

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.



2.5 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's LAN port. Follow the instructions in section **Basic System Administration, Network** (section 3.1) to set a static IP address.

2.6 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) .

2.7 Configure the Bridge API Server

Configure the API server by following the instructions in section **Configuration, Bridge API** (section 4.3).

2.8 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*).

- Bridge API credentials. (*Services > Bridge API > API Credentials*).

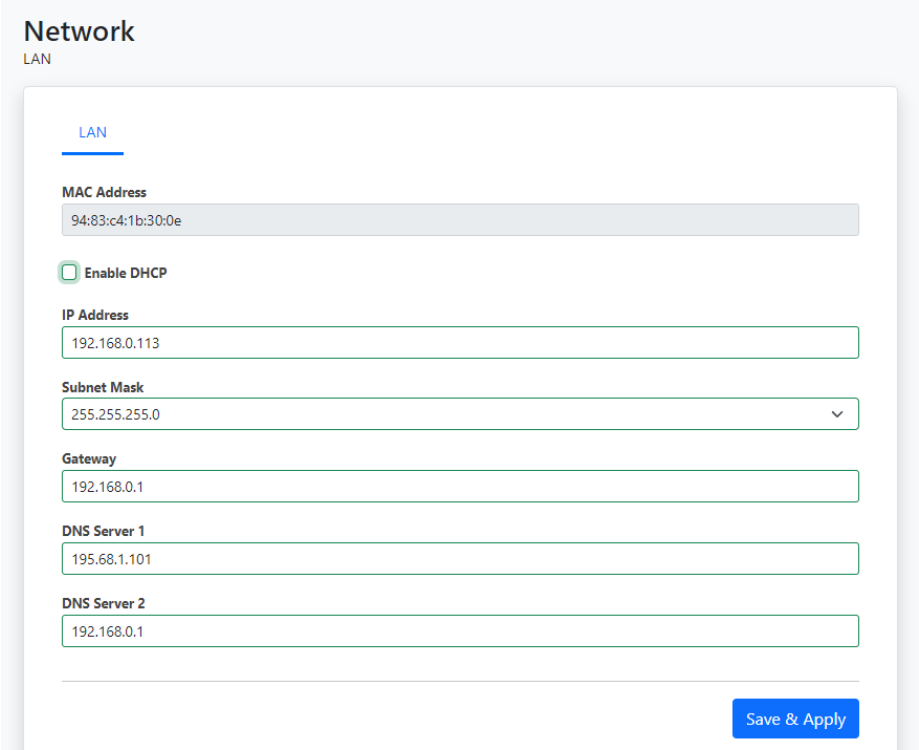
In sensitive environments, it may also be wise to enhance security further by:

- Only allow HTTPS when accessing the Web GUI (see section 5.3).
- Only allow key-based authentication for SSH access (see section 5.1).

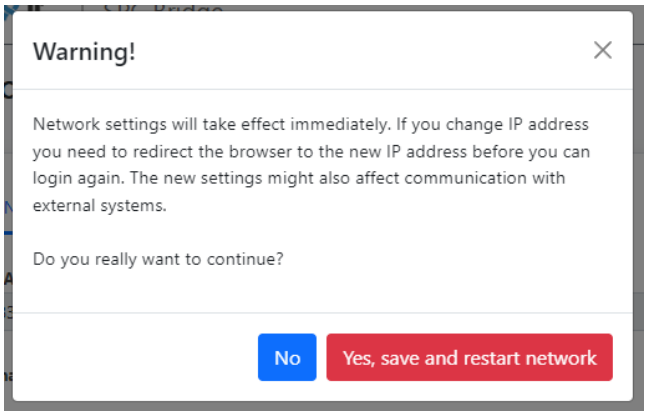
3 Basic System Administration

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 can 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.



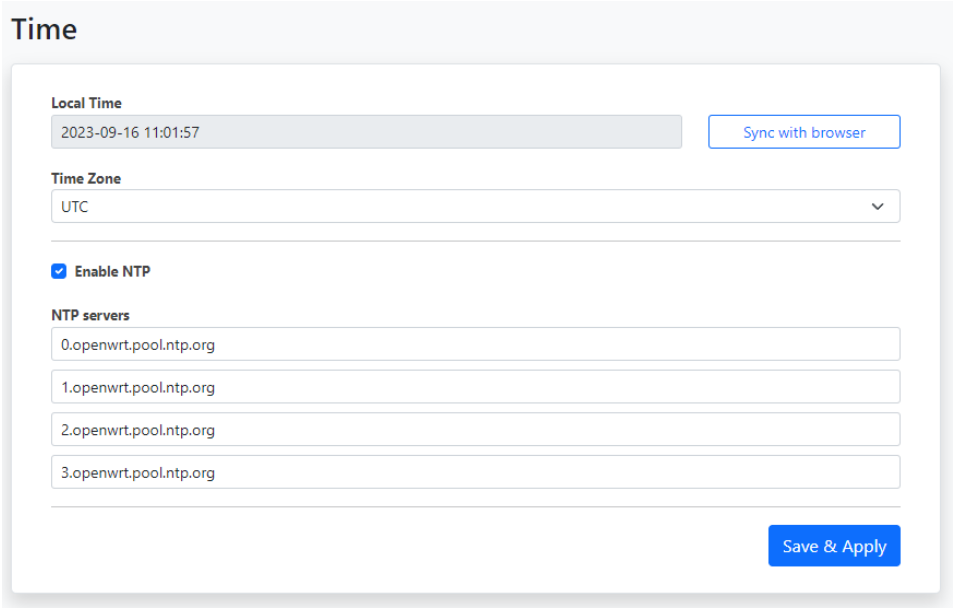
The settings will take effect immediately when you **Save & Apply** and have acknowledged the warning message. You have to manually redirect your browser if you have changed the IP address.



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

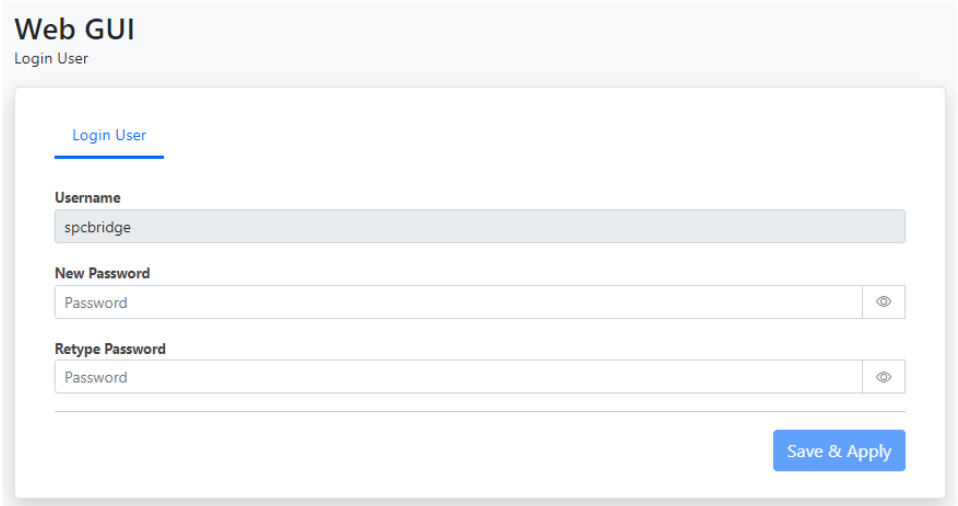
In ***System > Time*** you can change the time zone, sync the time with the current time of your browser and also configure the NTP (Network Time Protocol) service.



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.



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 -> Command Profile**. Click on **Add** to add a new command profile. Give the command profile the name **SPC Bridge Commands** and select (check) the checkbox for **Get the configuration of a User**. Keep the defaults for all other settings.
   Please note, this step is only mandatory if you use the API request type ***user*** in your integration.

5. 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)
   - Command Profile = SPC Bridge Commands (if created in step 4, otherwise keep the default setting)
   - ATS Polling Timeout = 60 seconds
   - Uncheck Generate FTC and Re-queue Events

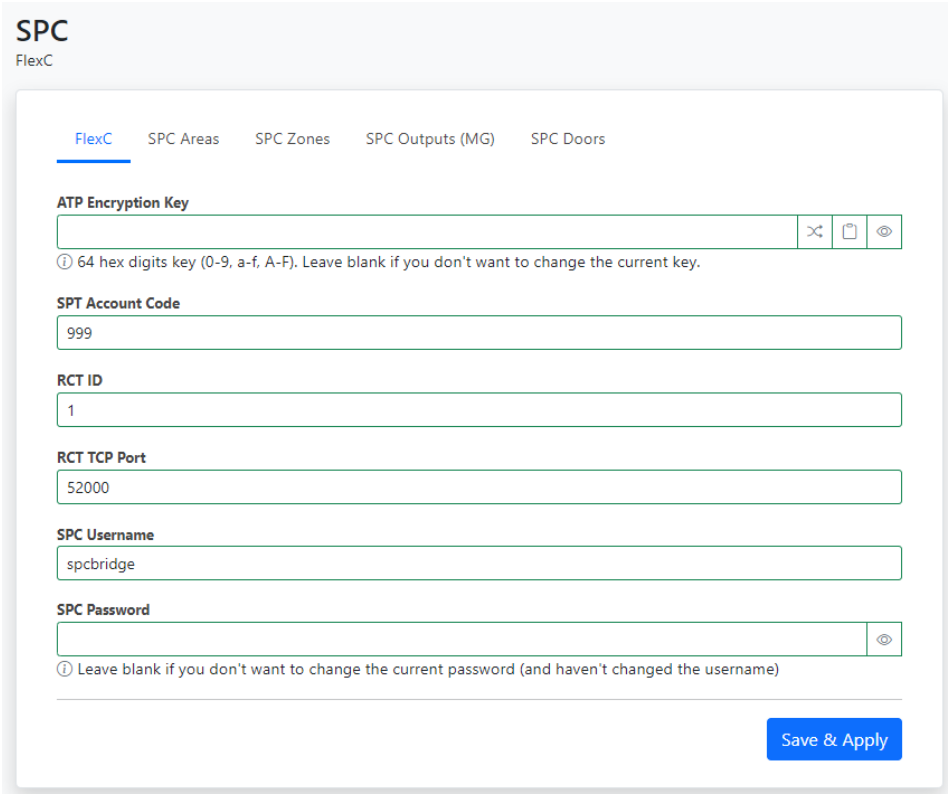
6. Select **Add ATP to FlexC RCT** and change following from the default settings:
   - SPT Account Code = 999
   - RCT URL or IP Address = IP Address of the SPC Bridge
   - ATP Category = Cat 6 [Ethernet]

7. 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.



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.

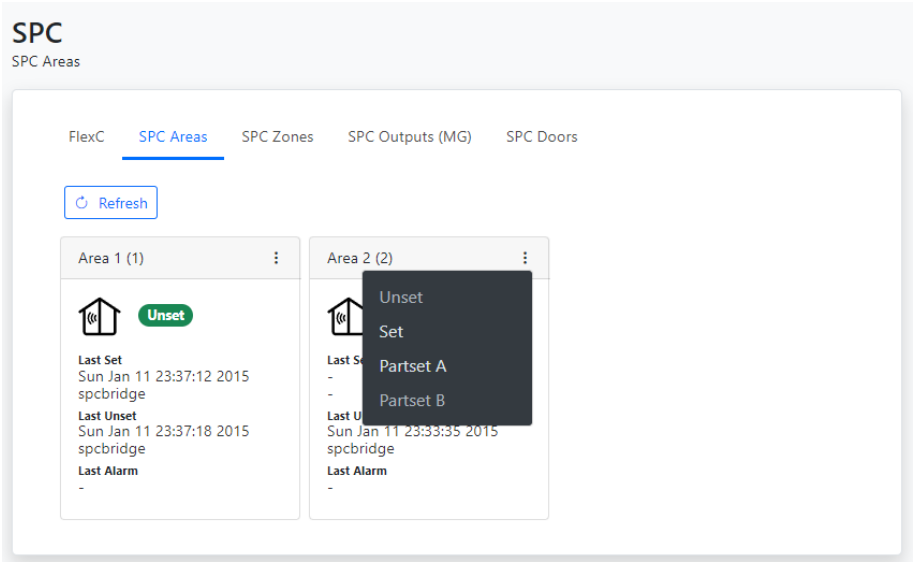
Show/Hide key	Button to show the key in plain text. Only valid during editing of a new key. Saved key is not possible to show again.
SPT Account Code	SPT Account Code. Must match corresponding key in SPC Panel FlexC settings.
RCT ID	RCT Id. Must match corresponding id in SPC Panel FlexC settings.
RCT 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***. For more advanced tests you can also use the API Test Tool, see section 4.3.3.

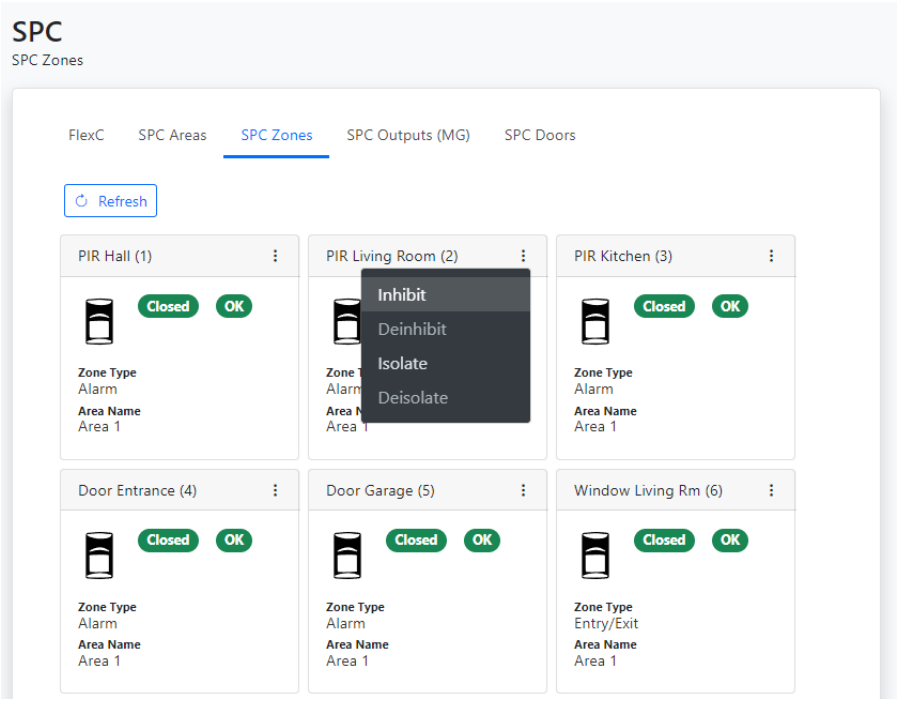
4.2.1 SPC Areas

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.



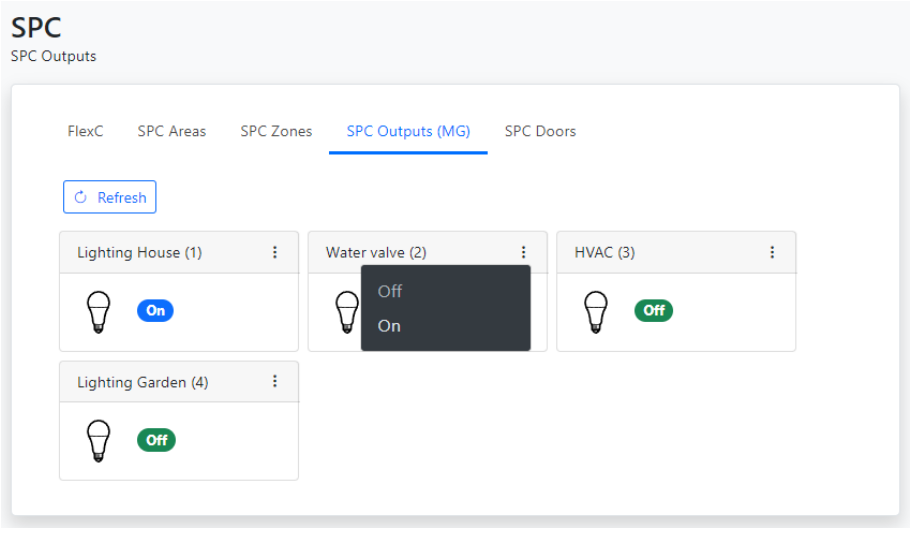
4.2.2 SPC Zones

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.



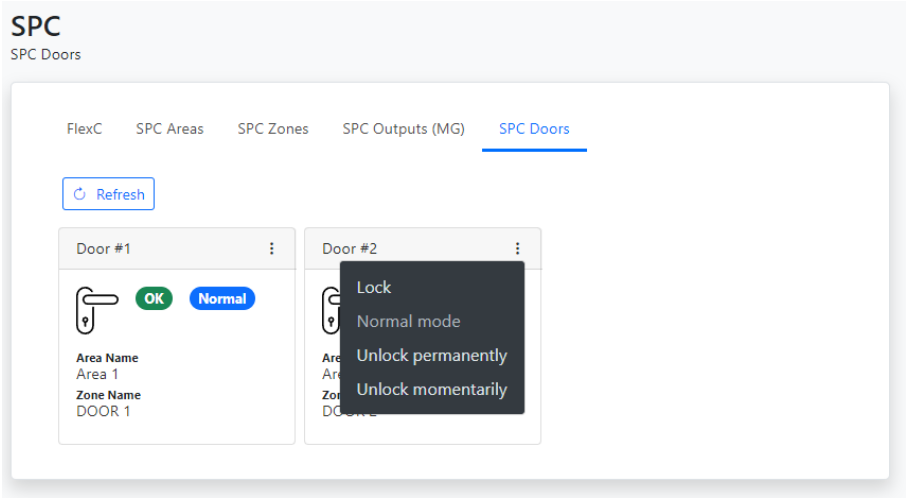
4.2.3 SPC Outputs (MG)

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 popup menu for each output.



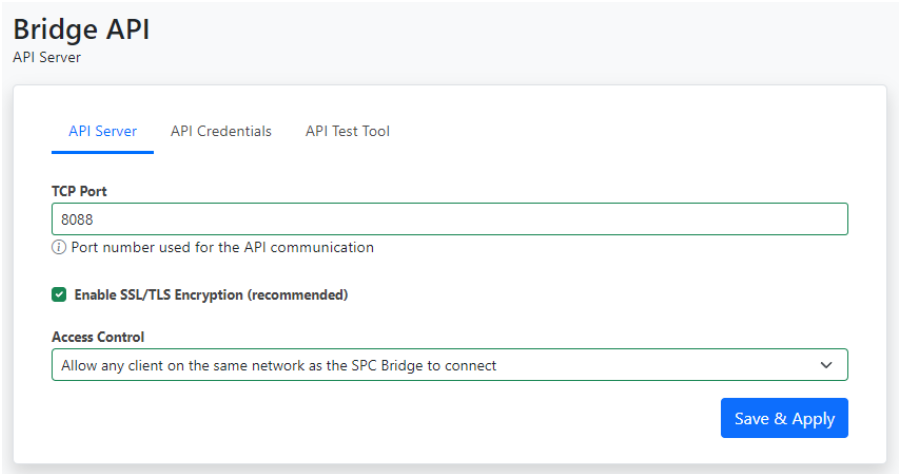
4.2.4 SPC Doors

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.



4.3 Bridge API

4.3.1 API Server



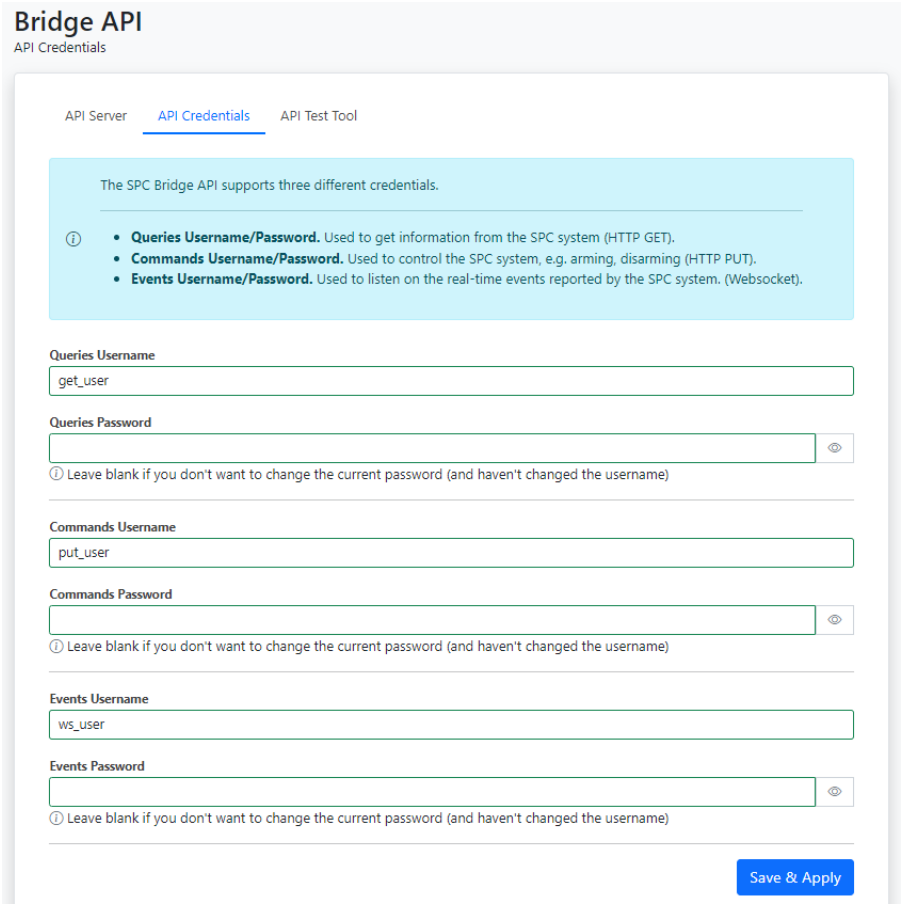
Element	Description
TCP Port	API Server IP port. Default 8088.
Enable SSL/TLS Encryption	If checked, the REST/Websocket communication is encrypted and only connections via HTTPS and WSS are allowed. Recommended is to only allow encrypted communication.
Access Control	If you select “Allow any client on the same network as the SPC Bridge to connect.” all devices on your local network (LAN) are allowed to connect to the API. If you select “Only allow certain client to connect (advanced)”, you need to also enter a Access Control List (ACL). The ACL restricts which clients are allowed to connect to the API server. The ACL is a comma separated list of IP subnets, where each subnet is pre-pended by either a - or a + sign. A plus sign means allow, where a minus sign means deny.

	Example 1: +192.168.0.0/24 Allow only IP addresses on subnet 192.168.0.0 mask 255.255.255.0 to connect. Example 2: +192.168.4.0/24 Allow only IP addresses on subnet 192.168.4.0 mask 255.255.255.0 to connect.

4.3.2 API Credentials

The SPC Bridge API supports three different types of credentials (username and password):

- **Queries**. Credentials for allowing queries to the SPC system, e.g. get area and zone status (HTTP GET).
- **Commands.** Credentials for allowing commands to the SPC system, e.g. arming, disarming (HTTP PUT).
- **Events**. Credentials for obtaining the real-time events reported by the SPC system. (Websocket).

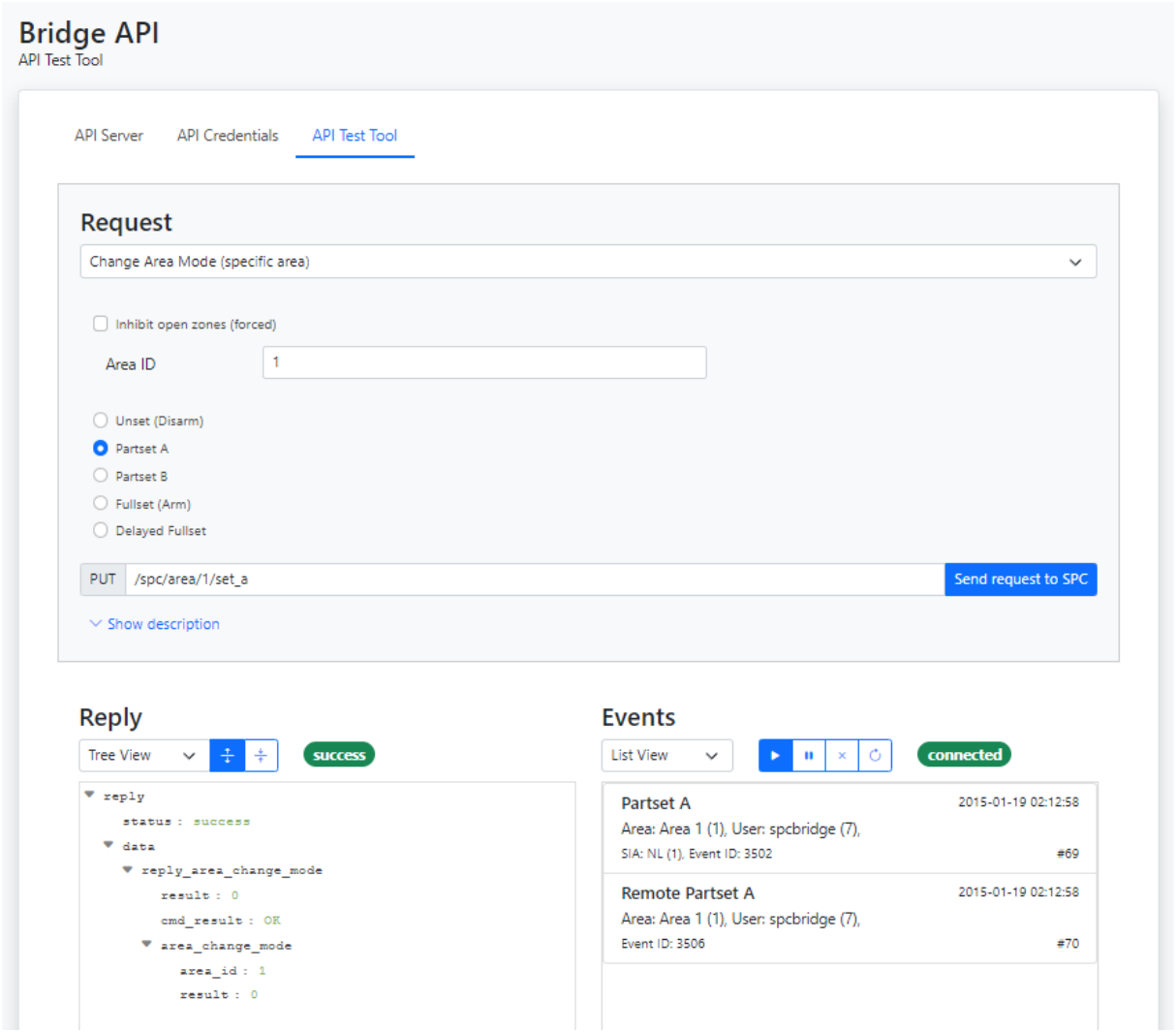


Element	Description
Queries Username and Password	Username and password for queries to SPC Bridge/SPC Panel. Default username is get_user and password get_pwd.

	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.
Commands Username and Password	Username and password for commands to SPC Bridge/SPC Panel. Default username is put_user and password put_pwd. 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.
Events Username and Password	Username and password for websockets events from SPC Bridge/SPC Panel. Default username is ws_user and password ws_pwd. 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.

4.3.3 API Test Tool

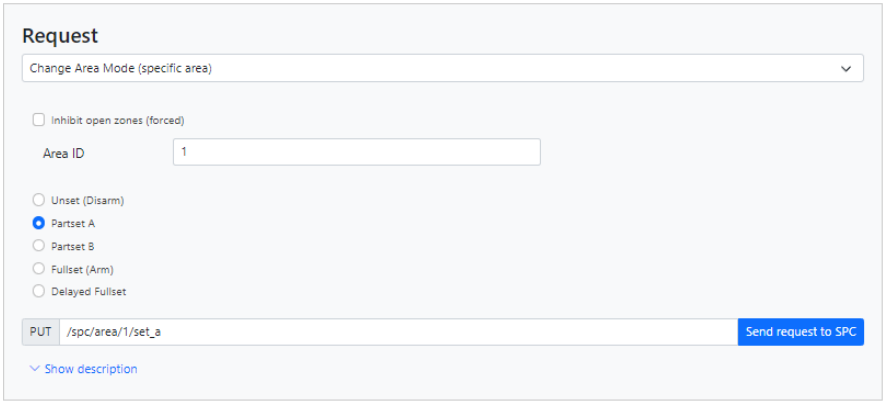
The API Test Tool is a very useful tool for testing and troubleshooting the Bridge's REST/Websockets API. The tool is also very helpful for integrators who want to learn the API.



The tool has three sections:

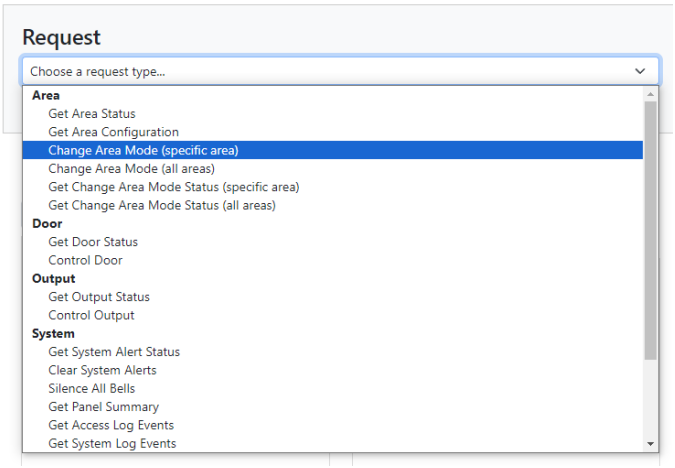
- Request. Here, you “build” and send an API request.
- Reply. Displays the response from the API on a request.
- Events. Displays real-time events from the API.

Request

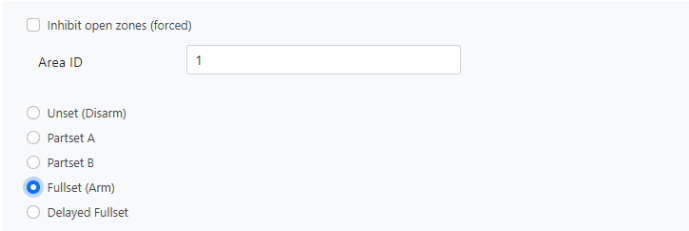


In the Request section of the test tool you "build" and send an API request.

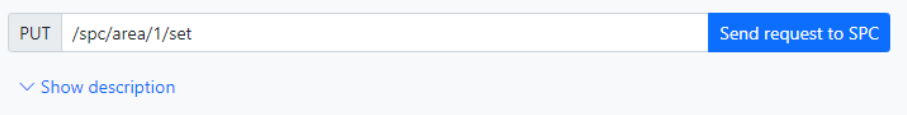
First, select the type of request you want to build from the options menu.



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



The API request string will be displayed in plain text.

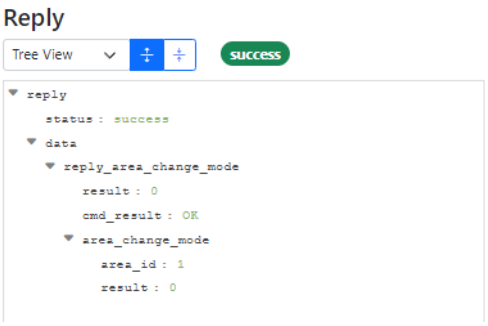


Finally, send the command by clicking the **Send request to SPC** button. The response will be shown in the Reply section.

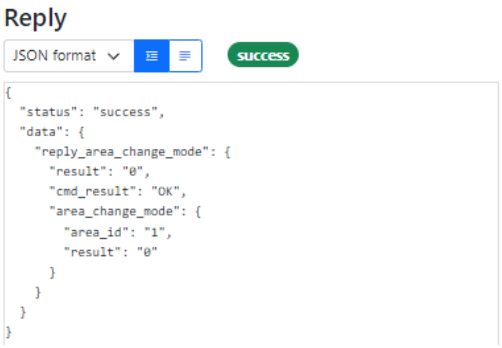
For a detailed protocol description of the selected request type, click on **Show description**.

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.



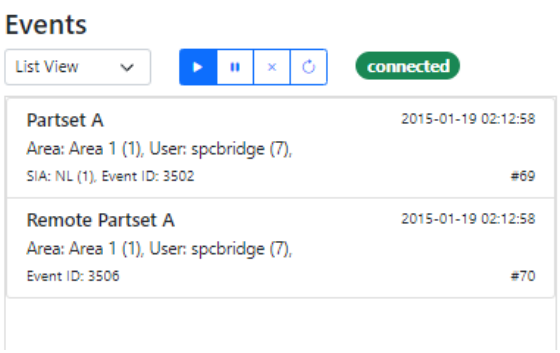
Reply in tre view format



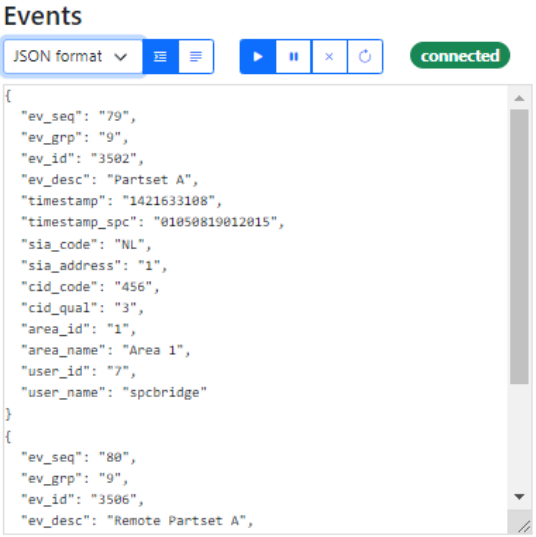
Reply in JSON format

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 in list view format

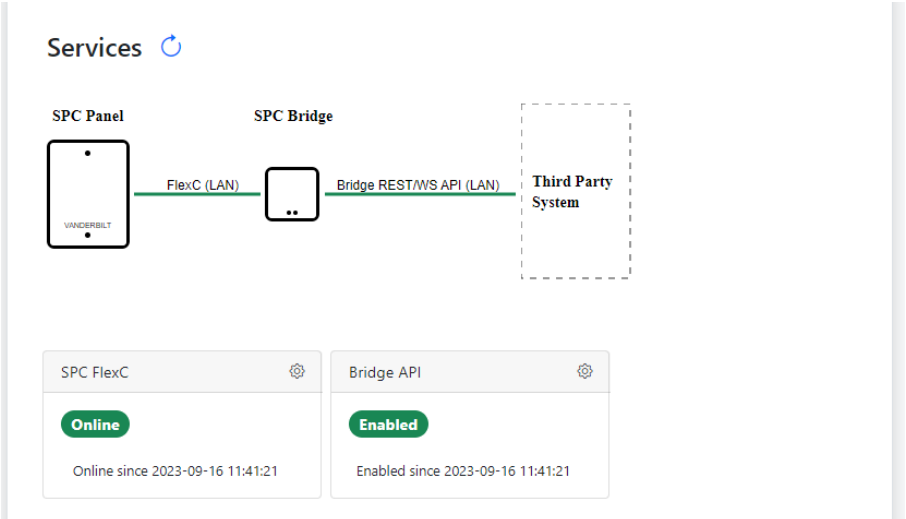


Events in JSON format

4.4 Overview

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

4.4.1 Services

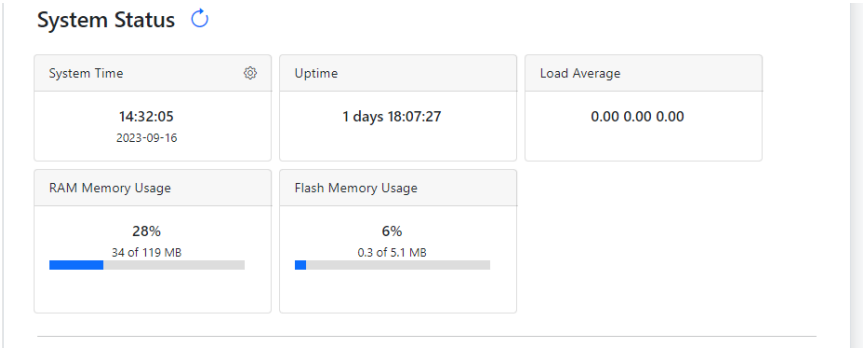


Section	Description	Status values
SPC FlexC	Shows the status of the FlexC communication with the SPC panel	Initializing: SPC Bridge is waiting for SPC Panel to connect first time. Online: Communication is up and running Offline: Communication is lost. SPC Bridge is wating for SPC Panel to reconnect.

Bridge API	Shows the status of the Bridge API service	Disabled: API is not available (FlexC is initializing or offline) Enabled: API is available (FlexC is Online)

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

4.4.2 System Status



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

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 the version of the installed firmware.
Hardware Model	Shows hardware model the SPC Bridge is based on

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

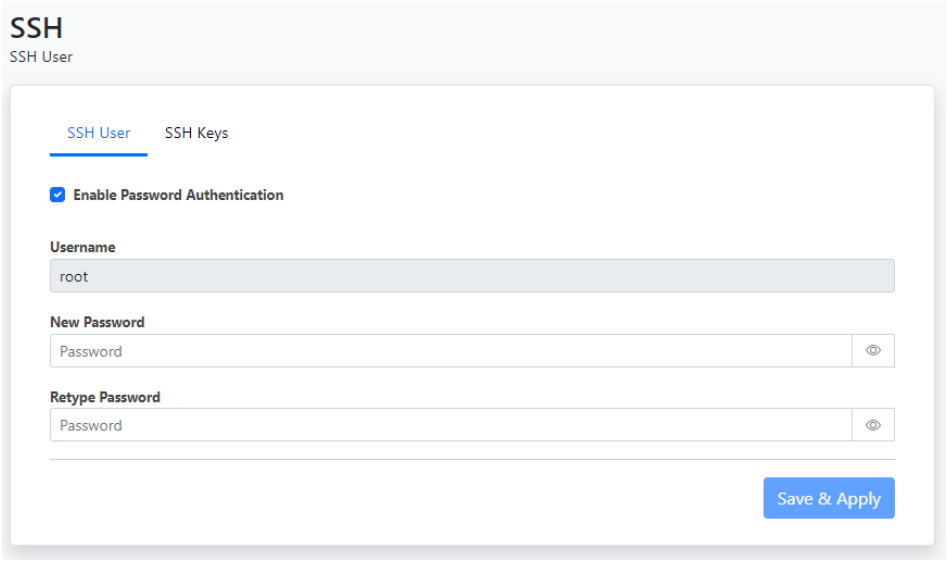
5 Advanced System Administration

5.1 SSH

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

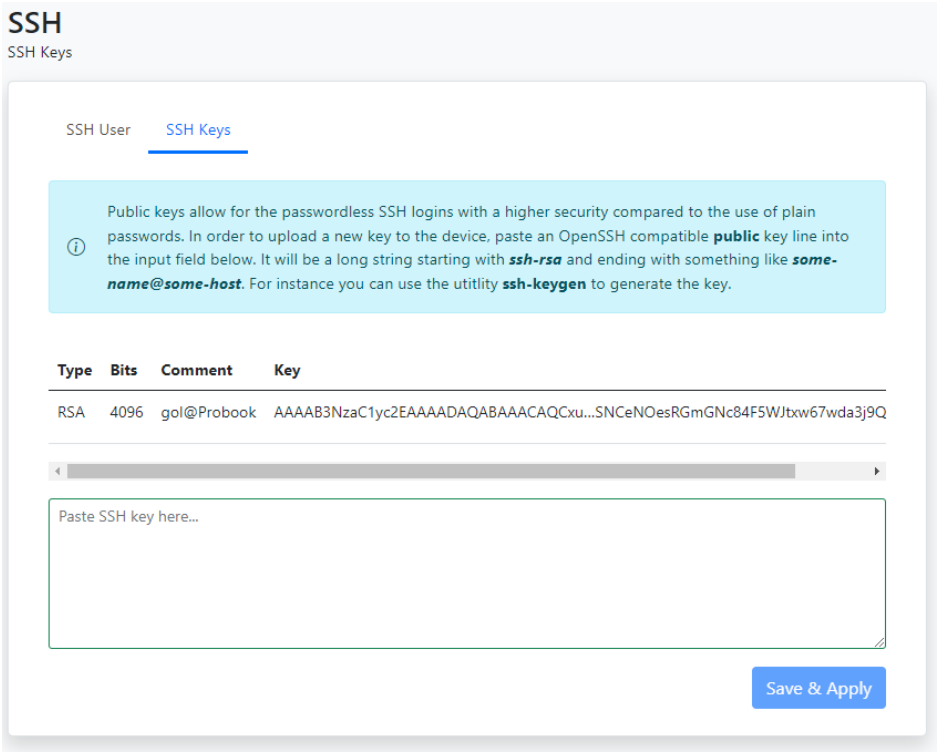
5.1.1 SSH User

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.



5.1.2 SSH Keys

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



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 utitlity *ssh-keygen* to generate the key. Here is an example how to generate a key on an Ubuntu system:

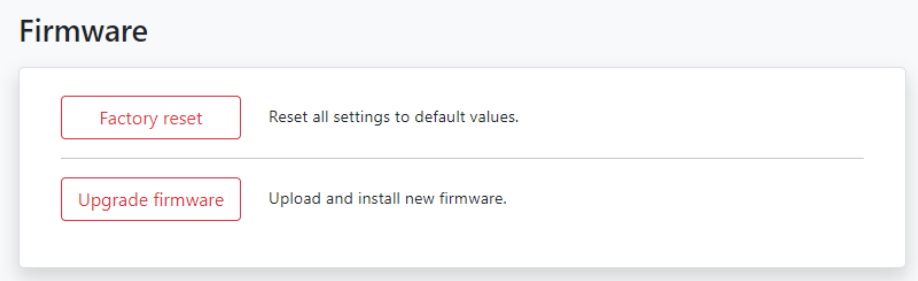
```
$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lundix/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lundix/.ssh/id_rsa.
Your public key has been saved in /home/lundix/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:47sizC5Vc42tiNmxAGIhjm545kl9Q+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 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.

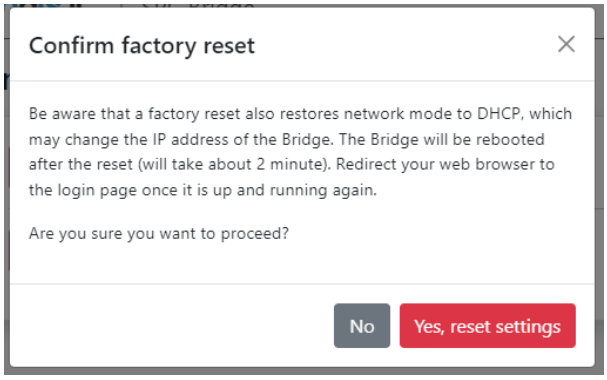
5.2 Firmware

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



5.2.1 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.

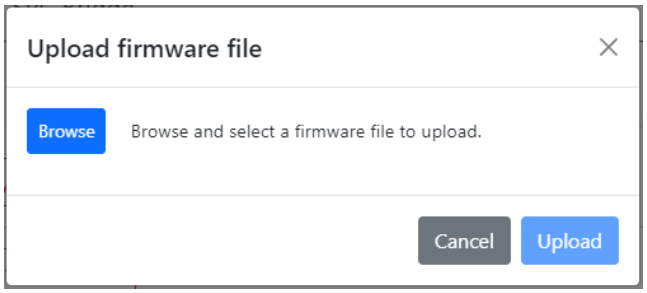


The factory reset will take about 2 minutes. Once the Bridge is up and running again, you have to redirect your web browser to the potentially new IP address (or http://spc-bridge.local).

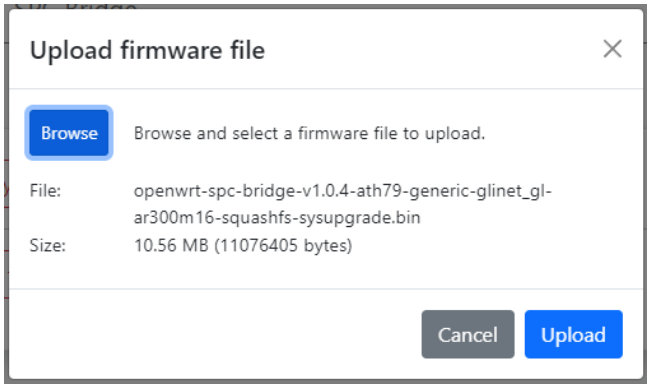
5.2.2 Upgrade Firmware

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

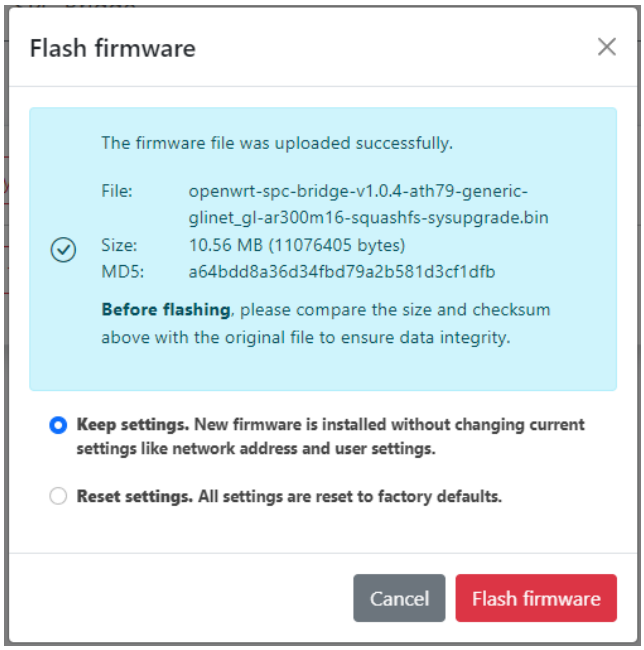
1. Click on the Firmware Upgrade button.
2. In the Upload firmware file window, browse and select the firmware file.



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



4. On successful upload and validation you se 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.

5.3 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

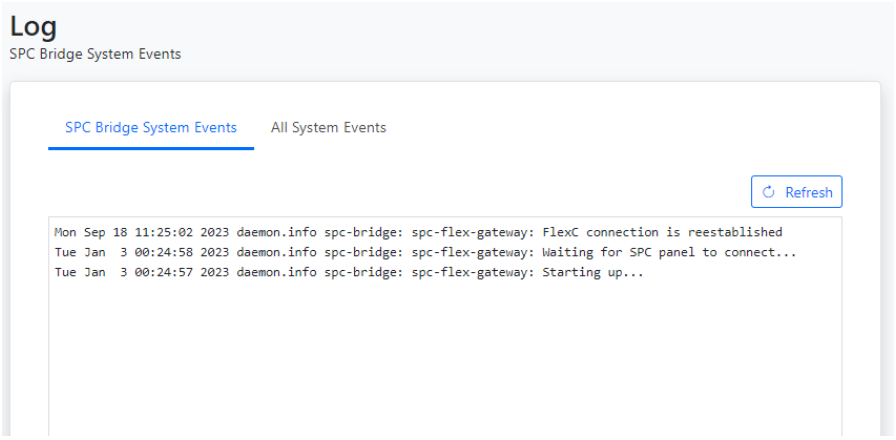
Please note, when switching between HTTPS and HTTP and vice versa, you may probably also need to clear the history cache in your web browser, to get the Web GUI to work as expected.

6 Troubleshooting

6.1 Log

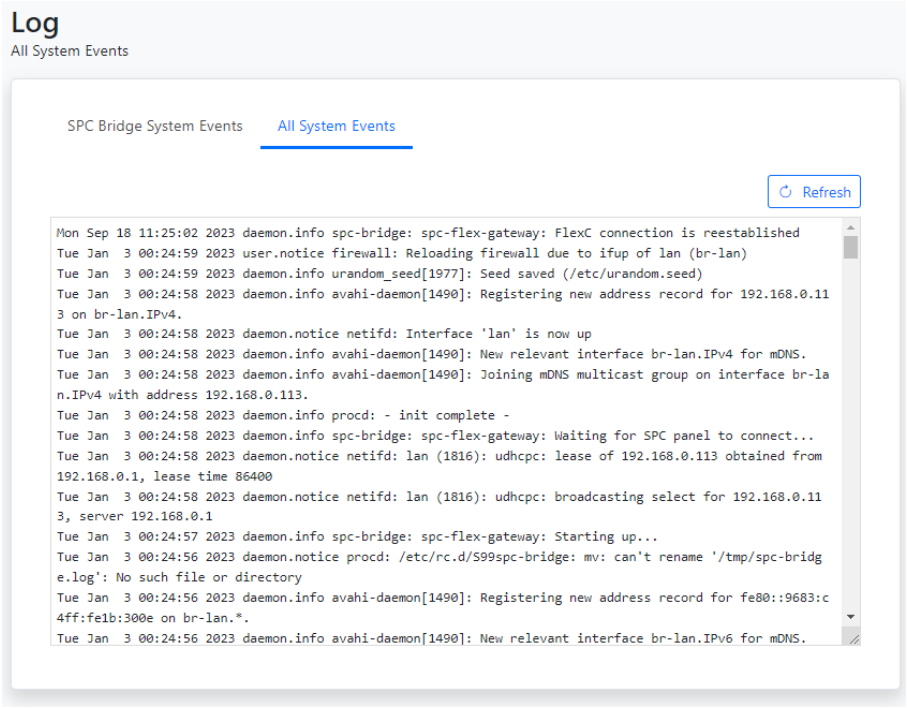
6.1.1 SPC Bridge System Events

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.



6.1.2 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.



6.2 FlexC Communication Tests

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

6.3 API Communication Tests

Use the API test tool described in section 4.3.3 to test the communication on the API level.

6.4 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.

7 Factory Reset

If the Web GUI still is available you can reset all settings to default values on the page ***System > Firmware,*** see section 5.2. 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.

8 Appendices

8.1 Hardware Specification

SPC Bridge 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 platic 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

8.2 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 Authorizedl
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
991	ERROR: Waiting for SPC to connect
999	ERROR: Unknown error

8.3 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.

8.4 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