SPC Web Gateway Installation Guide

Revision 1.2

lundix it

History Record

Revision	Date	Author	Comment
1.0	10-Apr-2014	Göran Lundquist, Lundix IT	First edition
1.1	18-May-2014	Göran Lundquist, Lundix IT	Added support for: • Encrypted communication • User/password control
1.2	24-May-2014	Göran Lundquist, Lundix IT	Added missed dependency to package libssl-dev

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

Contents

1 INTRODUCTION 4

1.1 Purpose of the document 4

1.2 Document References 4

1.3 Terminology and Abbreviations 4

2 INSTALLATION ON RASPBERRY PI OR UBUNTU 5

2.1 Installation Prerequisites 5

2.2 Installation Steps 5

3 SPC PANEL SETTINGS 9

3.1 EDP settings 9

3.2 EDP receiver settings 10

4 TESTING THE INSTALLATION 12

4.1 Using the embedded Testpanel 12

4.2 Using a Web Browser 13

4.3 Using the command tool curl 13

4.4 Print debug information 14

5 LICENSE AGREEMENTS 15

5.1 End-User License Agreement for SPC Web Gateway (EULA) 15

5.2 Open Source Libraries 16

1 Introduction

1.1 Purpose of the document

This document will guide you through the process of installing SPC Web Gateway on a Linux system.

1.2 Document References

Id	Description	Revision
[LUNDIX_SPC_WEB_GW_SPEC]	Lundix SPC Web Gateway Specification	1.0
[SPC_INST_CONF]	Siemens SPC42xx/43xx/52xx/53xx/63xx, Installation & Configuration Manual	3.2

1.3 Terminology and Abbreviations

Term	Description
JSON	JavaScript Object Notation
SIA	Security Industry Association
SPC panel	Siemens SPC intrusion panel
URL	Uniform Resource Locator
WebSocket	Two-way TCP protocol RFC 6455
XML	Extensible Markup Language

2 Installation on Raspberry Pi or Ubuntu

2.1 Installation Prerequisites

- Raspberry Pi with standard Debian Wheezy image or Linux system with Ubuntu (x86_64 release >= 12.04)
- Package **openssl** and **libssl-dev.** You can install it with: **sudo apt-get install openssl libssl-dev**
- Siemens SPC panel with firmware > 3.2
- Network connection between the Linux system and the SPC

2.2 Installation Steps

1. Read carefully **End-User License Agreement for SPC Web Gateway (EULA)** in chapter 5 in this document. If you do not agree to the terms of the EULA, do not install or use the SPC Web Gateway.

2. Copy the SPC Web Gateway package file, **spc-web-gateway-X-X.X.tar.gz**, to a directory of your choice on the Linux system.

3. Uncompress and unpack the package file:

```
tar xzvf spc-web-gateway-X-X.X.tar.gz
```

4. Run the install script:

```
cd ./spc-web-gateway-X-X.X
sudo ./install.sh
```

The script asks you some questions (You have to accept EULA and enter which user should run the gateway) and will then install the product in /opt/spc-web-gateway.

Note

User root is, of security reasons, not allowed to run spc-web-gateway in normal mode. If you would like to change the user after you have run the install script you have to change the variable RUN_AS in the file /etc/init.d/spc-web-gateway.

5. Open the file, **/opt/spc-web-gateway/config.xml,** in an editor and check and adjust the SPC Web Gateway settings. Normally, you don't need to change the default settings.

```
<!--
   CONFIGURATION OPTIONS

   enable_get_auth
      Set this flag to yes to enable user and password control for GET
      requests (queries).
      Run spc-web-gateway -A to set user and password.
      Valid values: yes or no. Default: yes

   enable_put_auth
      Set this flag to yes to enable user and password control for PUT
      requests (commands).
      Run spc-web-gateway -A to set user and password.
      Valid values: yes or no. Default: yes

   enable_ws_auth
      Set this flag to yes to enable user and password control for Websocket
      access.
      Run spc-web-gateway -A to set user and password.
      Valid values: yes or no. Default: yes

   enable_edp_encryption
      Set this flag to yes to enable encrypted communication to the
      SPC Panel. The EDP configuration in the SPC Panel must match this
      setting. Run spc-web-gateway -A to set encryption key.
      Valid values: yes or no. Default: yes

   enable_ssl_encryption
      Set this flag to yes to enable SSL encrypted communication to the
      embedded web server. With SSL enabled, web pages can only be accessed
      by using the https prefix.
      Valid values: yes or no. Default: yes

   access_control_list
      Access control list (ACL) for web client connections. ACL is a
      comma separated list of IP subnets, each subnet is prepended by
      '-' or '+' sign. Plus means allow, minus means deny. If subnet mask
      is omitted, like "-1.2.3.4", then it means single IP address.
      Mask may vary from 0 to 32 inclusive. On each request, full list is
      traversed, and last match wins. Default: if not set, ALLOW ALL.

      Example: -0.0.0.0/0,+192.168.0.0/24
      Deny connections from everywhere, allow only all IP addresses from
      subnet 192.168.0.0 mask 255.255.255.0 to connect.

   http_port
      Port to listen on for web client connections. Default: 8088

   tcp_port
      TCP/UDP port to listen on for SPC panel connections.
      Must match value in SPC EDP communication settings.

   spc_id
      SPC EDP Panel ID. A number which will be used by the SPC Web Gateway to
      identify the SPC panel. Must match value in SPC EDP communications
      settings.

   gateway_id
      SPC Gateway ID. A number which will be used by the SPC panel to
      identify the SPC Web Gateway as a EDP receiver. Must match value in
      SPC EDP Receiver settings.

   spc_time_diff
      How many hours the normal time differs between the SPC panel and the
      SPC Web Gateway system. Set to 0 if both systems have same time
      setting.
```

```
      Example: If SPC Panel has local Swedish time (CET) and the
      SPC Web Gateway system has Greenwich Mean Time (GMT) the value should
      be +1.
      Valid values: -24 to +24. Default: 0

   spc_dst
      Set this flag to yes if Automatic Daylight Saving Time is enabled in
      the SPC panel.
      Valid values: yes or no. Default yes.

-->
<config>
   <enable_get_auth>yes</enable_get_auth>
   <enable_put_auth>yes</enable_put_auth>
   <enable_ws_auth>yes</enable_ws_auth>
   <enable_edp_encryption>yes</enable_edp_encryption>
   <enable_ssl_encryption>yes</enable_ssl_encryption>
   <access_control_list>-0.0.0.0/0,+192.168.0.0/24</access_control_list>
   <http_port>8088</http_port>
   <tcp_port>16000</tcp_port>
   <spc_id>1000</spc_id>
   <gateway_id>1100</gateway_id>
   <spc_time_diff>0</spc_time_diff>
   <spc_dst>yes</spc_dst>
</config>
```

Note

To achieve a high level of security it is highly recommended to enable all security functions by setting enable_get_auth, enable_put_auth, enable_ws_auth, enable_edp_cryption and enable_ssl_encryption to **yes**. This is the default setting. You should also set the access_control_list as restrictive as possible, to prevent access from unauthorized IP

6. The default EDP encryption key is ***00112233445566778899AABBCCDDEEFF***. The default user/password for GET requests (queries) are **get_user/get_pwd**, for PUT requests (commands) **put_user/put_pwd** and for Websocket access **ws_user/ws_pwd**.

   Define your own EDP encryption key, usernames and passwords by running the application with option –A:

```
sudo /opt/spc-web-gateway/spc-web-gateway –A

-- Define user for GET requests –
Username[get_user]: <my_get_user>
New password: <my_get_password>
Re-type password: <my_get_password>

-- Define user for PUT requests –
Username[put_user]: <my_put_user>
New password: <my_put_password>
Re-type password: <my_put_password>

-- Define user for Websocket access –
Username[ws_user]: <my_ws_user>
New password: <my_ws_password>
```

```
Re-type password: <my_ws_password>

-- Enter EDP encryption –
EDP encryption key: <my_32_hex_digits_key>
```

Note

- The EDP encryption key must match the key defined in the SPC panel.
- User root is required to run spc-web-gateway –A.
- You can change these settings at any time, but remember to stop the running instance of spc-web-gateway first.
- If you would like to keep an old username and password just enter RETURN on both username and password.
- It is not possible to delete a user or password, just modify them. (But you can of course still disable the user/password control in the config file)

7. You can now start the SPC Web Gateway:

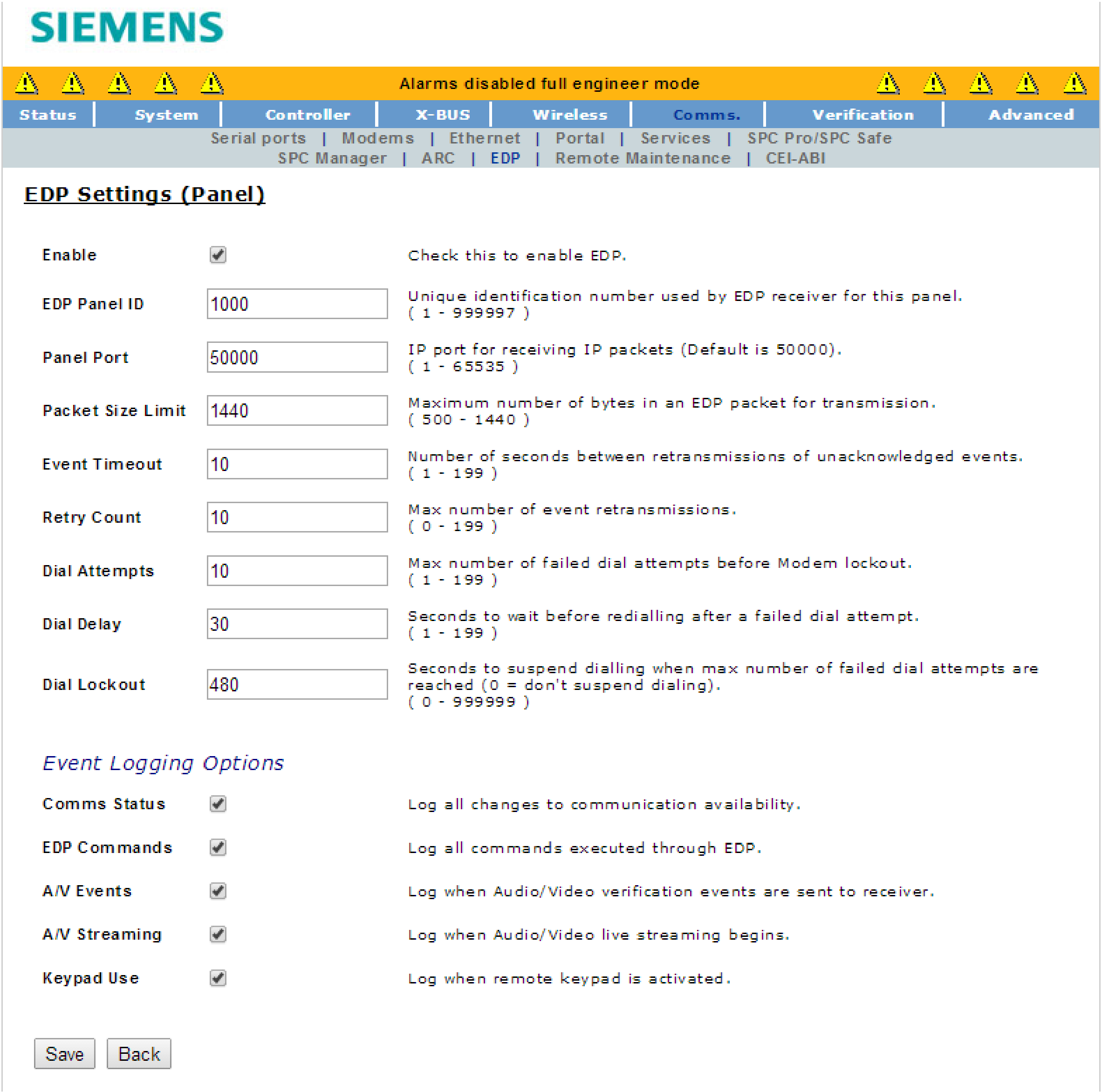
```
sudo /etc/init.d/spc-web-gateway start
```

3 SPC panel settings

Use SPC Pro or SPC Web interface to configure the connection to the SPC Web Gateway (EDP receiver) as explained below.

3.1 EDP settings

Adjust the common EDP Settings in accordance to following figure:


SIEMENS
Alarms disabled full engineer mode
Status
System
Controller
X-BUS
Wireless
Comms.
Verification
Advanced
Serial ports | Modems | Ethernet | Portal | Services | SPC Pro/SPC Safe
SPC Manager | ARC | EDP | Remote Maintenance | CEI-ABI
Save
Back

EDP Settings (Panel)

Enable	☑	Check this to enable EDP.
EDP Panel ID	1000	Unique identification number used by EDP receiver for this panel. (1 - 999997)
Panel Port	50000	IP port for receiving IP packets (Default is 50000). (1 - 65535)
Packet Size Limit	1440	Maximum number of bytes in an EDP packet for transmission. (500 - 1440)
Event Timeout	10	Number of seconds between retransmissions of unacknowledged events. (1 - 199)
Retry Count	10	Max number of event retransmissions. (0 - 199)
Dial Attempts	10	Max number of failed dial attempts before Modem lockout. (1 - 199)
Dial Delay	30	Seconds to wait before redialling after a failed dial attempt. (1 - 199)
Dial Lockout	480	Seconds to suspend dialling when max number of failed dial attempts are reached (0 = don't suspend dialing). (0 - 999999)

Event Logging Options

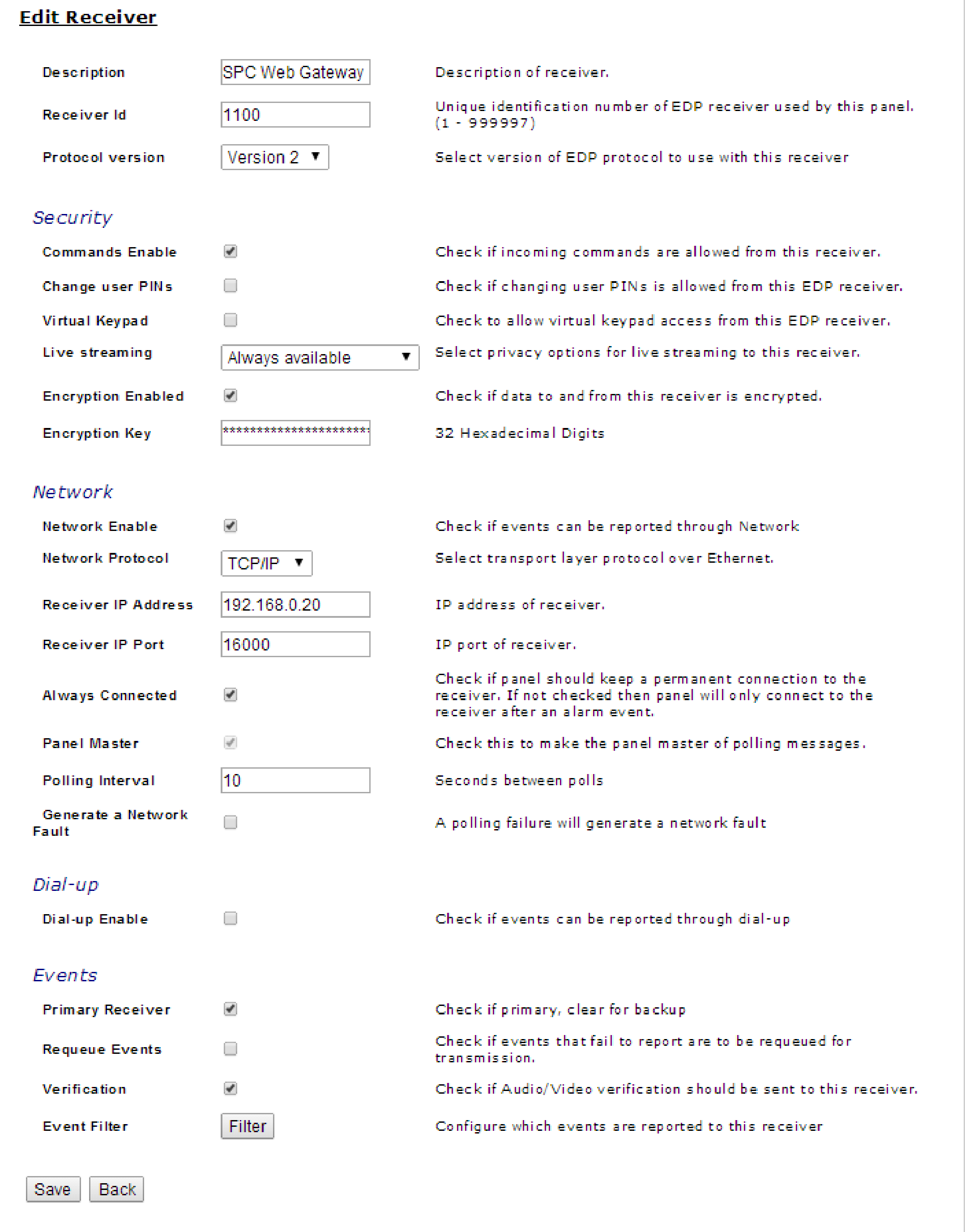
Comms Status	☑	Log all changes to communication availability.
EDP Commands	☑	Log all commands executed through EDP.
A/V Events	☑	Log when Audio/Video verification events are sent to receiver.
A/V Streaming	☑	Log when Audio/Video live streaming begins.
Keypad Use	☑	Log when remote keypad is activated.

Note

- EDP Panel ID must match spc_id in SPC Web Gateway configuration.

3.2 EDP receiver settings

Add and edit a new EDP receiver according to following figure:



Edit Receiver

Description	SPC Web Gateway	Description of receiver.
Receiver Id	1100	Unique identification number of EDP receiver used by this panel. (1 - 999997)
Protocol version	Version 2 ▼	Select version of EDP protocol to use with this receiver

Security

Commands Enable	☑	Check if incoming commands are allowed from this receiver.
Change user PINs	☐	Check if changing user PINs is allowed from this EDP receiver.
Virtual Keypad	☐	Check to allow virtual keypad access from this EDP receiver.
Live streaming	Always available ▼	Select privacy options for live streaming to this receiver.
Encryption Enabled	☑	Check if data to and from this receiver is encrypted.
Encryption Key	**********************	32 Hexadecimal Digits

Network

Network Enable	☑	Check if events can be reported through Network
Network Protocol	TCP/IP ▼	Select transport layer protocol over Ethernet.
Receiver IP Address	192.168.0.20	IP address of receiver.
Receiver IP Port	16000	IP port of receiver.
Always Connected	☑	Check if panel should keep a permanent connection to the receiver. If not checked then panel will only connect to the receiver after an alarm event.
Panel Master	☑	Check this to make the panel master of polling messages.
Polling Interval	10	Seconds between polls
Generate a Network Fault	☐	A polling failure will generate a network fault

Dial-up

Dial-up Enable	☐	Check if events can be reported through dial-up

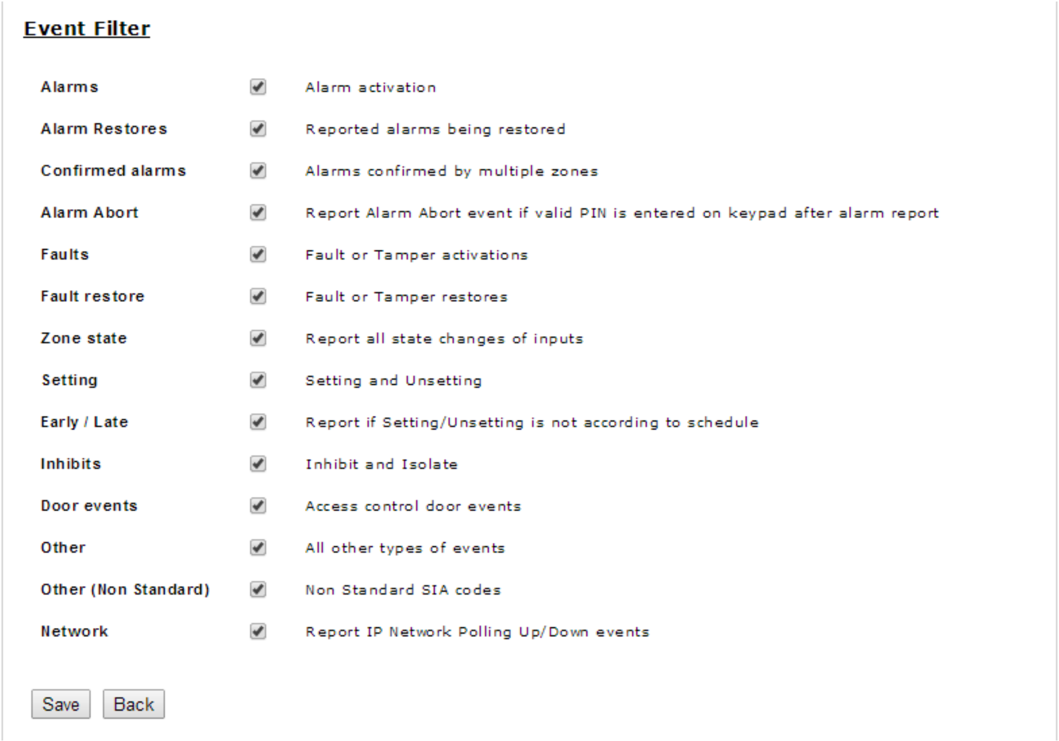
Events

Primary Receiver	☑	Check if primary, clear for backup
Requeue Events	☐	Check if events that fail to report are to be requeued for transmission.
Verification	☑	Check if Audio/Video verification should be sent to this receiver.
Event Filter	Filter	Configure which events are reported to this receiver

Note

- Receiver ID must match gateway_id in SPC Web Gateway configuration.
- Receiver IP Address must match SPC Web Gateway IP Address, i.e Raspberry Pi IP Address.
- Receiver IP Port must match tcp_port in SPC Web Gateway configuration.
- Encryption Key must match the key set with spc-web-gateway -A

If you would like to use SPC Web Gateway WebSocket you should also configure which (SIA) events are reported, in the Event Filter section, see following figure:



Event Filter

Alarms	☑	Alarm activation
Alarm Restores	☑	Reported alarms being restored
Confirmed alarms	☑	Alarms confirmed by multiple zones
Alarm Abort	☑	Report Alarm Abort event if valid PIN is entered on keypad after alarm report
Faults	☑	Fault or Tamper activations
Fault restore	☑	Fault or Tamper restores
Zone state	☑	Report all state changes of inputs
Setting	☑	Setting and Unsetting
Early / Late	☑	Report if Setting/Unsetting is not according to schedule
Inhibits	☑	Inhibit and Isolate
Door events	☑	Access control door events
Other	☑	All other types of events
Other (Non Standard)	☑	Non Standard SIA codes
Network	☑	Report IP Network Polling Up/Down events

4 Testing the Installation

After you have finished installation on the Raspberry Pi and the configuration of the SPC panel you can test that everything works by using the methods described below.

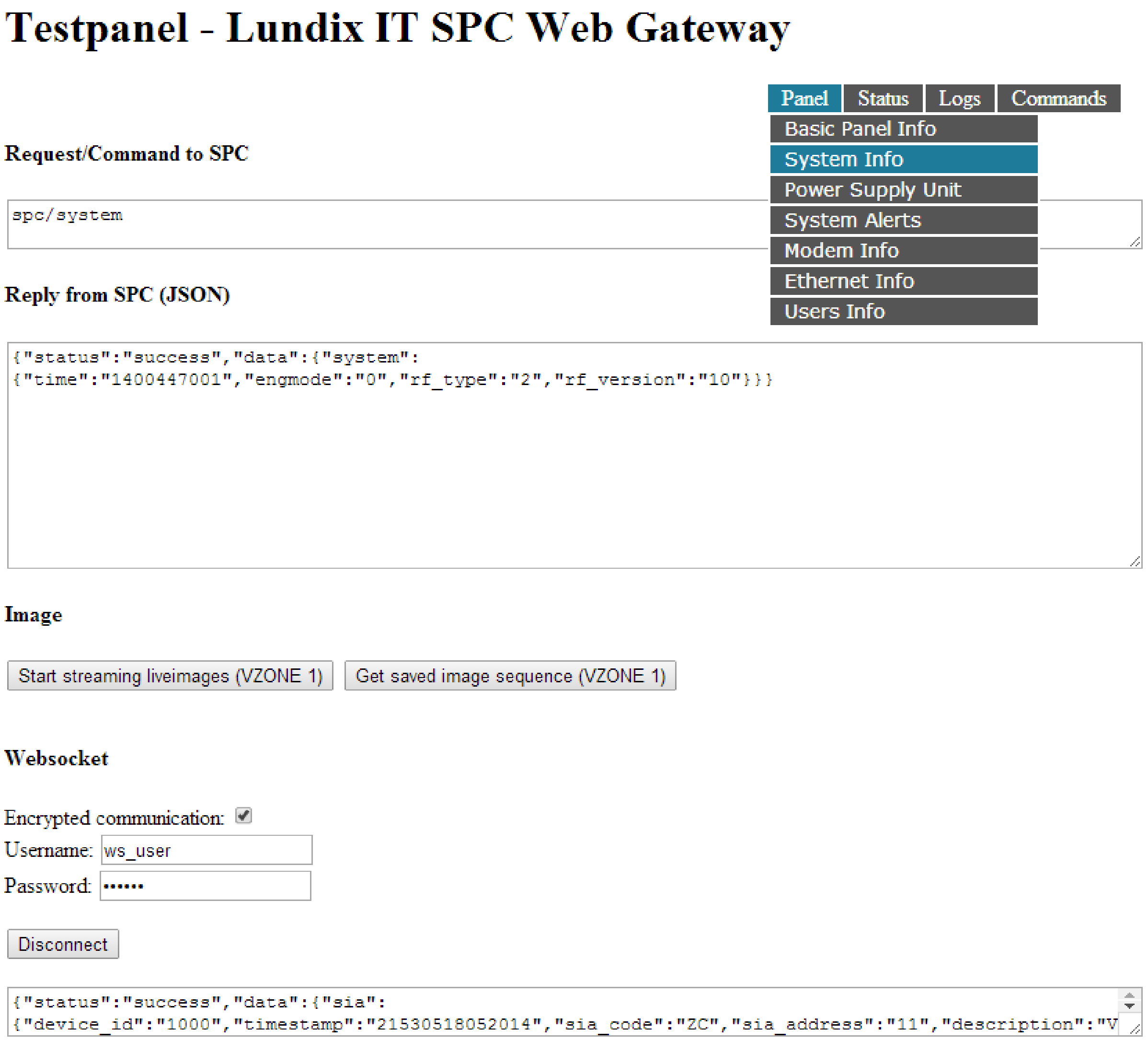
4.1 Using the embedded Testpanel

In the embedded test panel you can test most of the commands and queries in the protocol by selecting functions in a menu. The corresponding query or command and the reply are displayed in plain text.

In a web browser go to https://IP_OF_RASPBERRY:SPC_WEB_GATEWAY_TCP_PORT, e.g. https:// 192.168.0.20:8088. Use http instead of https if you have disabled SSL-encryption.

If you would like to display SIA events from the SPC panel you have to push on Connect button in the Websocket section.

If you have connected an IP camera to the SPC panel it is also possible to view images from the camera by selecting **Start streaming liveimages** and **Get saved image sequence**.



Testpanel - Lundix IT SPC Web Gateway

Request/Command to SPC

```
spc/system
```

Reply from SPC (JSON)

{"status":"success","data":{"system":
{"time":"1400447001","engmode":"0","rf_type":"2","rf_version":"10"}}}

Image

Websocket

Encrypted communication: ☑
Username: ws_user
Password: ••••••

{"status":"success","data":{"sia":
{"device_id":"1000","timestamp":"21530518052014","sia_code":"ZC","sia_address":"11","description":"V

4.2 Using a Web Browser

You can also test the SPC Web Gateway by simple entering the query as a URL path in a web browser. This way you can test all queries based on GET methods, but not PUT methods. The reply will be displayed in plain text.

Example: Get the status of zone 1:

Go to URL https://192.168.0.20:8088/spc/zone/1 and enter GET user/password in the authentication dialog window that will pop up.

If you have disabled SSL-encryption use http instead of https and if you have disabled GET user/password control no authentication window will appear.

4.3 Using the command tool curl

To test the SPC Web Gateway protocol from the command line or from a script it is very convenient to use the standard command tool **curl**.

On the Raspberry Pi you can install it with:

```
sudo apt-get install curl
```

Curl has support for both GET and PUT methods.

Example GET method: Get the status of zone 1:

```
curl -X GET https://192.168.0.20:8088/spc/zone/1 -u get_user:get_pwd \
-k --digest

{"status":"success","data":{"zone":[{"id":"1","type":"0","zone_name":
"Entrance","area":"1","area_name":"Area 1","input":"0","status":"0"}]}}
```

The same query if you have disabled SSL-encryption and GET user/password control:

```
curl -X GET http://192.168.0.20:8088/spc/zone/1

{"status":"success","data":{"zone":[{"id":"1","type":"0","zone_name":
"Entrance","area":"1","area_name":"Area 1","input":"0","status":"0"}]}}
```

Example PUT method: Isolate zone 1:

```
curl -X PUT https://192.168.0.20:8088/spc/zone/1/isolate \
-u put_user:put_pwd -k --digest

{"status":"success","data":"null"}
```

The same command if you have disabled SSL-encryption and PUT user/password control:

```
curl -X PUT http://192.168.0.20:8088/spc/zone/1/isolate

{"status":"success","data":"null"}
```

4.4 Print debug information

To print debug information you can start the SPC Web Gateway with start option **–d** or **--debug**:

```
sudo /etc/init.d/spc-web-gateway stop
cd /opt/spc-web-gateway
./spc-web-gateway -d
```

5 License Agreements

5.1 End-User License Agreement for SPC Web Gateway (EULA)

IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL. SPC Web Gateway 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 Web Gateway software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the program 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 SOFTWARE PRODUCT.
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

GRANT OF LICENSE.
The SOFTWARE PRODUCT is licensed as follows:

- **Installation and Use.** Lundix IT grants you the right to install and use copies of the SOFTWARE PRODUCT on your computer.
- **Backup Copies.** You may also make copies of the SOFTWARE PRODUCT 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 SOFTWARE PRODUCT.
- **Prohibition on Reverse Engineering, Decompilation, and Disassembly.**
  You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT.
- **Support Services.**
  Lundix IT may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE 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 SOFTWARE PRODUCT.

TERMINATION
Without prejudice to any other rights, Lundix IT may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT in your possession.

COPYRIGHT
All title, including but not limited to copyrights, in and to the SOFTWARE 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 SOFTWARE 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 SOFTWARE PRODUCT. The SOFTWARE 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 SOFTWARE 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 SOFTWARE 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 SOFTWARE 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.

5.2 Open Source Libraries

The following open source libraries, licensed under MIT license, are used and included within the SPC Web Gateway:

- **CivetWeb** - Copyright (c) 2004-2013 Sergey Lyubka
- **ezXML** - Copyright (c) 2004-2006 Aaron Voisine aaron@voisine.org

The MIT License (MIT)

END OF DOCUMENT