



SDN-3030-SPT-DP-3G/4G

Technical manual
Release 2.3.6 revision 1.2

Copyright © 2026 by Swissdotnet SA - All rights reserved.

Swissdotnet SA

Route du Pâqui 4
1720 Corminboeuf
Switzerland

Phone : +41 (0)26 510 29 30
Fax : +41 (0)26 510 29 34
E-Mail : info@swissdotnet.ch
Web : <http://www.swissdotnet.ch>

Every conceivable measure has been taken to ensure the correctness and completeness of this documentation. However, as errors can never be fully excluded we would appreciate any information or ideas at any time.

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally trademark or patent protected.

Table des matières

Acronymes	8
1. Overview	10
1.1. Icon description	10
1.2. Online resources	10
1.3. Compliances	10
1.4. Safety guidelines	11
2. Device Description	12
2.1. What is the SDN-3030-SPT-DP-3G/4G?	12
2.1.1. Product variants	12
2.1.1.1. Modem variants	12
2.1.2. Additional modules	13
2.2. SDN-3030-SPT-DP-3G/4G features	13
2.3. SDN-3030-SPT-DP-3G/4G compatibility	15
2.4. Hardware specifications	15
2.5. Package contents	17
2.6. Physical Overview	18
2.6.1. Top view	18
2.6.2. Bottom view	19
2.6.3. Product view	20
2.6.3.1. EN 50131-10:2014, EN 50136-2:2013, EN 54-21:2006 Type 1 compliant 	20
2.6.3.2. Uncertified version	21
2.7. Connectors	21
2.7.1. Digital inputs	21
2.7.2. Intruder inputs	22
2.7.3. Digital outputs	22
2.7.4. Serial	23
2.7.5. Audio 	24
2.7.6. Power supply	24
3. Installing the SDN-3030-SPT-DP-3G/4G	26
3.1. Unpacking	26
3.2. Physical installation and wiring	26
3.2.1. Power and battery	28
3.2.2. Network connection	28
3.2.3. Mobile network connection	28
3.2.4. Connection with the Alarm System (AS)	28
3.3. Basic configuration	29
3.3.1. USB service cable	29
4. Display Elements and buttons	31
4.1. On Printed Circuit Board (PCB)	31
5. Configuration	33
5.1. General information	33
5.1.1. First design	33
5.1.2. Second design	34
5.2. Header	36
5.3. Dashboard	36
5.4. Authentication	37
5.4.1. Users and access levels	37
5.4.2. Certificates	39

5.5. Physical inputs and outputs	41
5.5.1. Inputs	41
5.5.2. Outputs	42
5.6. Network	42
5.6.1. Interfaces	43
5.6.1.1. Status	45
5.6.1.2. More about connection monitoring	46
5.6.1.3. Connection monitoring and PPP	46
5.6.2. General	47
5.6.3. Short Message Service (SMS) input	47
5.7. Alarm transmission - SPT	48
5.7.1. Features	49
5.7.2. Security	49
5.7.3. Alarm Receiving Center (ARC)s	49
5.7.3.1. ARC Configuration	49
5.7.3.2. ARC Supervision	51
5.7.3.3. Check the ARCs	53
5.7.4. ANSI/SIA DC-09-2007/2013	54
5.7.5. CLC/TS 50136-9 (Beta)	55
5.7.5.1. Shared secret commissioning	55
5.7.5.2. Shared secret single commissioning	57
5.7.5.3. Datagram Transport Layer Security (DTLS) commissioning	57
5.7.5.4. Once commissioning is done	58
5.7.6. Inputs	58
5.7.7. Events	59
5.7.7.1. Event Summary	59
5.7.7.2. Event Configuration	60
5.7.7.3. Event Options	62
5.7.8. Remote commands	64
5.7.9. Location	66
5.7.10. DC09	66
5.8. IP Alarm 	66
5.8.1. Endpoints	67
5.8.2. Inputs	67
5.9. Hardware	68
5.9.1. Power Management	68
5.9.2. Serial Interfaces	69
5.9.3. Date and Time	71
5.9.4. LEDs and Buzzer	72
5.9.5. Temperature	72
5.9.6. Information	72
5.10. Modbus 	73
5.10.1. Slaves	73
5.10.1.1. Common Slave configuration	74
5.10.1.1.1. TCP Slave configuration	75
5.10.1.1.2. RTU Slave configuration	75
5.10.2. Inputs	76
5.10.2.1. Coil (FC1) and discret input (FC2)	76
5.10.2.2. Holding register (FC3) and input register (FC4)	77
5.10.3. Outputs	78
5.11. IOT 	78
5.11.1. Clients	79
5.11.2. Inputs	82
5.11.3. Outputs	84
5.12. Notifications	85
5.12.1. SMS / Emails templates	85
5.12.1.1. Email	86
5.12.1.2. SMS	88
5.12.2. Mail servers	89

5.13. Actions	90
5.13.1. Available inputs	93
5.13.2. Available outputs	96
5.14. Scripts	96
5.14.1. Configuration	97
5.14.2. Custom SDN-3030-SPT-DP-3G/4G specific blocks	99
5.14.2.1. Inputs attributes	99
5.14.2.2. Script Input attributes	99
5.14.2.3. Using outputs	100
5.14.2.4. SDN-3030-SPT-DP-3G/4G date and time variables	101
5.14.2.5. SDN-3030-SPT-DP-3G/4G specific variables	101
5.14.2.6. Variables persistence	102
5.14.2.7. Read / write memory slots	102
5.14.3. Points of caution	102
5.14.3.1. For a Script execution only the last value/state/data set matters	103
5.14.3.2. A script using time will be executed every second	103
5.14.3.3. A script using an SDN-3030-SPT-DP-3G/4G input will be executed every time this input has its state change	103
5.14.3.4. Variables are not persisted from one execution to another unless you request it	103
5.14.3.5. Blocks are not all strongly typed	103
5.14.3.6. Lua scripting language is used under the hood	103
5.15. VPN	103
5.15.1. Virtual Private Network (VPN) Connections	104
5.15.2. Remote Access	105
5.16. Video transmission	106
5.17. Activetags 	110
5.17.1. Dongle configuration	110
5.17.2. Groups	112
5.17.2.1. Groups list	112
5.17.2.2. Groups configuration	112
5.17.3. Inputs	114
5.18. Serial alarm	115
5.18.1. Configuration	115
5.18.1.1. Devices	115
5.18.1.2. Inputs	116
5.18.2. ESPA 4.4.4	117
5.18.2.1. Limitations	117
5.18.2.2. Inputs	117
5.18.2.2.1. Direct input	117
5.18.2.2.2. Indirect input	118
5.18.2.3. Configuration	120
5.18.2.4. Debug	121
5.18.2.4.1. Logs	121
5.18.2.4.2. Raw	121
5.18.3. Wago UPS	122
5.18.3.1. Inputs	122
5.19. Modules	123
5.19.1. Advanced features	125
5.20. Maintenance	126
5.20.1. Application log	126
5.20.1.1. Application log Messages	128
5.20.2. System log	130
5.20.3. Network analysis	130
5.20.4. Configuration	131
5.20.5. Update	132
5.20.5.1. Update : how it works	132
5.20.5.2. Different ways of updating	133
5.20.5.3. Update servers	134

6. Device Recovery	136
6.1. Recovery card preparation	137
Appendices	138
A. Getting started : your first alarms	139
A.1. A basic alarm	139
A.2. A more complex alarm	139
B. F.A.Q Frequently Asked Questions	145
B.1. Physical	145
B.2. Install	145
B.3. VPN	145
B.4. Alarm transmission	146
B.5. Hardware	146
B.6. IoT	146
B.7. Network	146
B.8. Video	146
B.9. General	146
C. Cheat Sheet	149

The  symbol indicates that special attention should be paid regarding certifications.

Acronymes

AE

Annunciation Equipment. 53

AES

Advanced Encryption Standard. 49

AMS

Alarm Monitoring System. 52

ARC

Alarm Receiving Center. 4, 13, 14, 32, 39, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 62, 64, 65, 66, 93, 106, 107, 128, 129, 130, 132, 139, 140, 141, 143, 145, 146

AS

Alarm System. 3, 23, 28, 29, 53, 93, 129, 139

ATP

Alarm Transmission Path. 32, 51, 52, 55, 56, 93, 128, 129

ATS

Alarm Transmission System. 12, 51, 52, 53, 93, 147

BLE

Bluetooth Low Energy. 110

CA

Certificate Authority. 58

CRC

Cyclic Redundancy Check. 49

CSV

Comma Separated Values. 127

DHCP

Dynamic Host Configuration Protocol. 43, 44, 47

DNS

Domain Name System. 44, 47, 72, 130

DTLS

Datagram Transport Layer Security. 4, 57

GPRS

General Packet Radio Service. 10, 45

GPS

Global Positioning System. 18, 44, 66, 145

I&HAS

Intrusion and Hold up Alarm System. 24

ICMP

Internet Control Message Protocol. 46

IMEI

International Mobile Equipment Identity. 45

IoT

Internet of Things. 79, 81, 82, 83, 84, 146

LAN

Local Area Network. 10, 11

MQTT

MQ Telemetry Transport. 39, 40, 79, 81, 146

NTP

Network Time Protocol. 44, 72, 129, 130

PCB

Printed Circuit Board. 3, 15, 17, 27, 28, 31, 146

PLC

Programmable Logic Controller. 60, 73, 139, 140

PoE

Power Over Ethernet. 13, 68, 94

PTZ

Pan-Tilt-Zoom. 107, 110

QoS

Quality Of Service. 81

RCT

Receiving Center Transceiver. 49, 51, 52, 53, 55, 56, 57, 58, 93, 130

RTSP

Real Time Streaming Protocol. 110

SMS

Short Message Service. 4, 12, 13, 44, 47, 48, 85, 86, 88, 89, 90, 96

SMTP

Simple Mail Transfer Protocol. 44, 46, 85, 89, 90

SPT

Supervised Premises Transceiver. 12, 13, 14, 29, 32, 37, 44, 46, 49, 51, 53, 55, 57, 67, 69, 93, 101, 103

SSL

Secure Sockets Layer. 14, 81, 90

TCP

Transport Control Protocol. 55

TLS

Transport Layer Security. 39, 81, 104, 105, 107

TNI

Transmission Network Interface. 53, 129

UI

User Interface. 36

VPN

Virtual Private Network. 5, 35, 37, 39, 40, 44, 46, 95, 96, 103, 104, 105, 106, 107, 108, 130, 140, 143, 145

1. Overview

1.1. Icon description

 Note : This symbol indicates a note of interest and that special attention should be paid while using the product.

 Warning : This symbol indicates that caution is needed as something may damage the property or product.

 Standard requirements : This symbol indicates that special attention should be paid to ensure choosing the option meeting the standards requirements.

1.2. Online resources

Swissdotnet website : <http://www.swissdotnet.ch>

1.3. Compliances

 Caution :

 **The Certification Body only tested and certified the software version 1.4.0. Therefore, compliance to any of the following standards can only be achieved with the software version 1.4.0.**

The SDN-3030-SPT-DP-3G/4G can comply with the following standards :

- **EN 50131-10:2014****EN_50131-10**
- **EN 50136-2:2013****EN_50136-2**
- **EN 54-21:2006 Type 1****EN_54-21**
- **EN 50136-1:2013 DP2, DP4****EN_50136-1**

 Certified body : Telefication 0560

- The SDN-3030-SPT-DP-3G/4G is security grade 2¹ and environmental class II².
- The SDN-3030-SPT-DP-3G/4G has 12 inputs (including 4 intruder inputs), a serial input(**in certified installation, used only to receive additional information from Fire system**) and 4 output relays
- The SDN-3030-SPT-DP-3G/4G is using a transmission system EN 54-21:2006 Type 1**EN_54-21** .
- The SDN-3030-SPT-DP-3G/4G transmission paths (Local Area Network (LAN) and General Packet Radio Service (GPRS)) performance criteria are as follow :

1. Low to medium risk : An intruder or robber is expected to have a limited knowledge of Intruder Alarm Systems and have a comprehensive range of tools and portable instruments (e.g a multi-meter)

2. Indoor - General : Environmental influences normally experienced indoors when the temperature is not well maintained (e.g corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouse where heating is intermittent)

Transmission delay classification	Maximum transmission delay	Signal Duration	Availability	Substitution protection	Information protection
D4	M3	T2 (whole path), T5 (network access)	A4	S2	I3

1.4. Safety guidelines

For installing and operating purposes of the relevant device to your system, the following safety precautions shall be observed :

- All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work
- Allow access to such equipment and fixtures to authorized, qualified staff only by means of specific keys or tools
- Do not use in telecommunication circuits. Only use devices equipped with Ethernet or RJ-45 connectors in LANs
- The devices are equipped with electronic components that may be destroyed by electrostatic discharge when touched. Please observe the safety precautions against electrostatic discharge per DIN BS EN 61340-5-1-3 **EN_61340-5-1**. When handling the devices, please ensure that environmental factors (personnel, work space and packaging) are properly grounded

2. Device Description

This document presents the SDN-3030-SPT-DP-3G/4G hardware and software developed by Swissdot-net SA. Its goal is to be used as a reference administrator manual and to educate users on how the device works.

2.1. What is the SDN-3030-SPT-DP-3G/4G ?

The SDN-3030-SPT-DP-3G/4G is our new multi services embedded platform.

Its main focus is the alarm transmission over IP networks. We provide a standard and certified way to transmit alarms over Internet with a very high rate of availability. In this case we speak about Supervised Premises Transceiver (SPT) Mode.

Moreover, the SDN-3030-SPT-DP-3G/4G allows you to :

- Send Emails and SMS
- Communicate with alarm systems
- Transmit video securely to operational centers
- Other features are available on request

2.1.1. Product variants

SDN-3030-SPT-SP	Alarm Transmitter - Single Path (ATS category up to SP6)
SDN-3030-SPT-DP-3G	Alarm Transmitter - Dual Path (3G) (ATS category up to DP4)
SDN-3030-SPT-DP-4G	Alarm Transmitter - Dual Path (4G) (ATS category up to DP4)

 **When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required** only the following variant can be used :

SDN-3030-SPT-DP-3G	Alarm Transmitter - Dual Path (3G) (ATS category DP2 and DP4)
SDN-3030-SPT-DP-4G	Alarm Transmitter - Dual Path (4G) (ATS category DP2 and DP4)

2.1.1.1. Modem variants

Name	Region	Technology	Fallback
HL7692 (used for SDN-3030-SPT-DP-4G)	EMEA	LTE CAT-1 : B3, B8, B20	2G
HL8548 (used for SDN-3030-SPT-DP-3G)	Global	HSPA : B1, B2, B5, B6, B8, B19	2G
MC8790 (used for SDN-2020-SPT-DP-3G)	Global	HSPA : B1, B2, B3, B8, B26	2G
Quectel EC25-E (used for SDN-2020-SPT-DP-3G and SDN-2020-SPT-DP-4G)	Asia/Europe	B1, B3, B5, B7, B8, B20, FDD LTE, B38, B40, B41, TDD LTE, WCDMA	2G, 3G

 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required only the following variant can be used :

Name	Region	Technology	Fallback
HL7692 (used for SDN-3030-SPT-DP-4G)	EMEA	LTE CAT-1 : B3, B8, B20	2G
HL8548 (used for SDN-3030-SPT-DP-3G)	Global	HSPA : B1, B2, B5, B6, B8, B19	2G

2.1.2. Additional modules

PoE	PoE module for the SDN-3030-SPT-DP-3G/4G to be powered through one of its Ethernet interface
-----	--

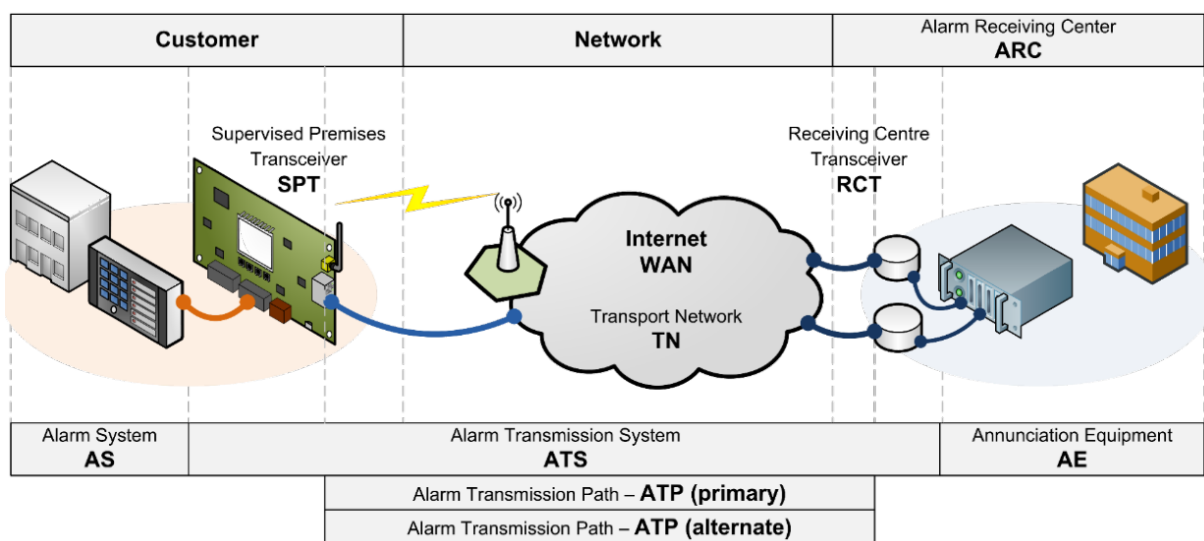
2.2. SDN-3030-SPT-DP-3G/4G features

The SPT software module allow you to transmit fire, security or technical alarms with open protocols such as ANSI/SIA DC-09-2007/2013 or TS 50136-9 (currently in Beta) directly to your ARC.

By using Internet as transport network you can use your existing infrastructure to transmit your alarms. Dual path SDN-3030-SPT-DP-3G/4G and SDN-3030-SPT-DP-4G models also give you an alternate way (3G or 4G WWAN) to improve the availability and enforce the transmission reliability. The mobile network interface requires a SIM card and an appropriate subscription¹ to a mobile network operator.

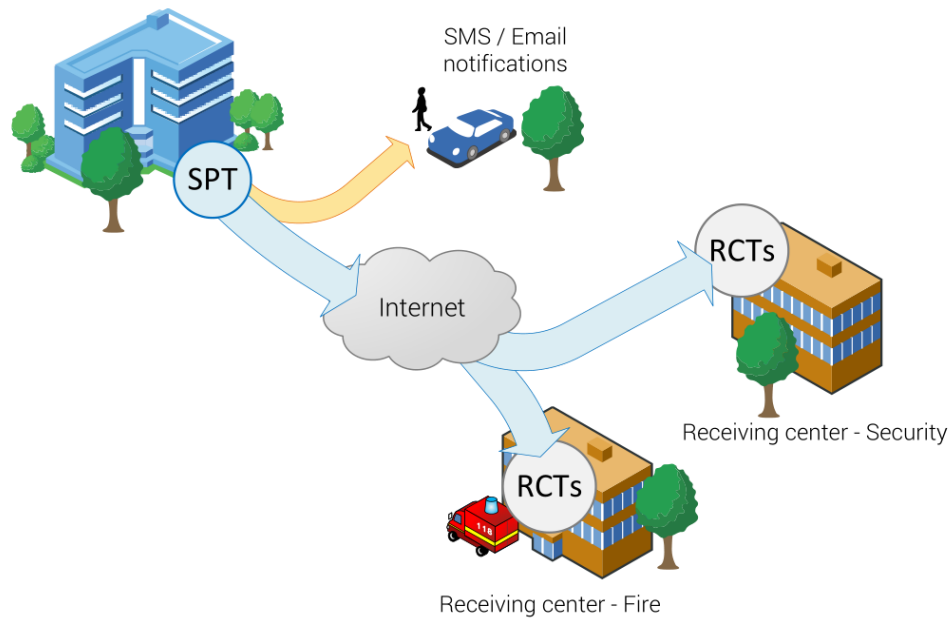
 The single path version of the SDN-3030 still allows you to have an alternate path by using the second Ethernet port on an alternate Internet provider. If you want to keep the compliance with the EN 50136-1 (6.3.3.3.2)EN_50136-1 standard, the connection should use a different technology.

The following picture is an example of a dual path alarm transmission :

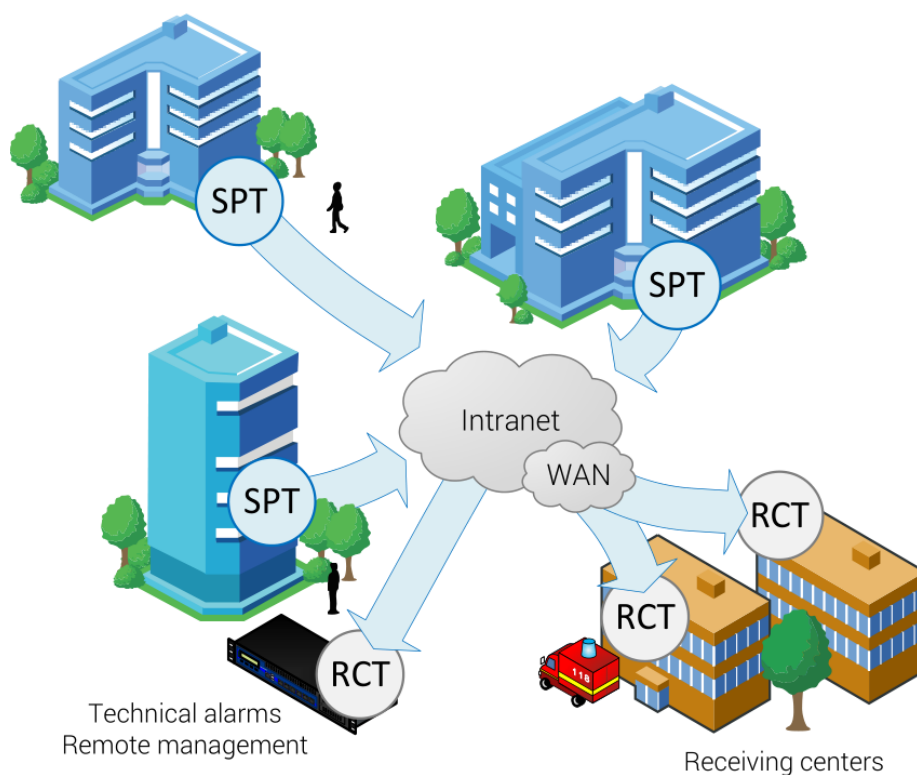


Unlike most other SPT manufacturers, our devices allow to send alarms to several ARCs. You can freely select which alarms needs to be sent to which ARC. Furthermore, the device is able to send SMS or Email notifications directly to notify concerned people that an alarm or a failure is occurring.

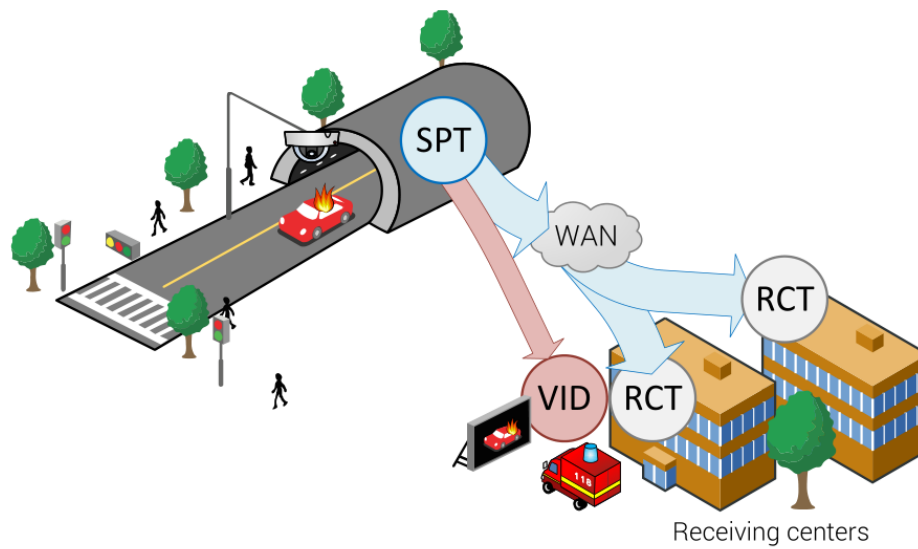
1. The operator for the wired and the wireless network should not be the same



The flexibility of our platform also allows big companies to receive alarms internally and do remote management.



In addition, by using the video transmission module, the SDN-3030-SPT-DP-3G/4G can automatically and securely broadcast video directly to the ARC. This solution is mainly dedicated to safety and alarm verification. However, this functionality is only available if the receiving center is equipped with the appropriate infrastructure. The video transmission is totally secure and is using Secure Sockets Layer (SSL) encryption and certificate for authentication. The video module can also be used without the SPT part.



2.3. SDN-3030-SPT-DP-3G/4G compatibility

The SDN-3030-SPT-DP-3G/4G is compatible with the SDN-IPRCT-SOFT as well as with any alarm receiver compatible ANSI/SIA DC-09-2007/2013 TCP/UDP. CLC/TS 50136-9 compatibility is currently only available as Beta.

2.4. Hardware specifications

Raw SDN-3030-SPT-DP-3G/4G PCB hardware specifications :

Form Factor		Embedded board
Platform	Processor	ARM Cortex-A8
System Memory	Technology, Capacity	DDR3 800MHz / 512 MB
Storage	On-board flash	2 GB
	External flash	microSD, 3.3V
Networking	Ethernet ports	2x 100BASE-TX Ethernet RJ-45 (optional IEEE 802.3af PoE)
	WWAN	Optional Embedded Module 3G : GSM 7 GPRS / EDGE / HSDPA / HSUPA 4G:4G : LET Cat-1 (B3, B8, B20)
	SIM card socket	Standard SIM (2FF)
I/O interface	Intruder inputs	4 (current loop)
	Digital inputs	8 (10-34 VDC) with LED state
	Digital outputs	4 relays Maximum power 60V 125VA, Maximum DC voltage 22VDC, Maximum AC voltage 250 VAV, Maximum current 2A
	Audio	Microphone input, Stereo output, 2.1W/CH @ 40hm, 1.4W/CH @ 80hm
	Serial	RS-232/422/485 on SUB-D 9 or onboard connector
	Reset button	Yes
	LED	1x Power IN 1 (blue), 1x Power IN 2 (blue), 1x Power status (blue), 1x Status LED (red/orange/green)
Expansion	Management port	1x USB client (mini USB)
	USB	1x USB 2.0 Host
	Antenna	1x WWAN, 1x GPS (optional)
Cooling	HMI	Optional HMI expansion
	Other	Optional expansion module
Environmental Parameters	Type	Fanless
	Environmental class	Class II
	Temperature operating	0°C .. 50°C
	Temperature storage	-20°C .. 70°C
	Humidity operating	5 - 90% non-condensing
Miscellaneous	Humidity storage	5 - 95% non-condensing
	Watchdog	Yes
	Accelerometer	Yes
	Temperature	Yes, onboard sensor
	Buzzer	Yes
Physical dimensions	Internal RTC	Yes, with supercap
	Dimensions (WxHxD)	160x100 mm
	Weight	145g
Power	Operating voltage	12V DC
	Input 1	10 - 24 VDC/VAC
	Input 2	10 - 24 VDC/VAC
	Output	1x protected 12VDC output 500mA software controlled
	Battery charger	12V Lead Acid battery charger
Approvals and Compliance	Current consumption	Average : 240mA, Max:950mA ²
		CE Class A, RoHS

Satel APS-412 power supply :

2. This value is only reached on first boot

Dimension (WxHxD)	77x122x59
Weight	306g
Type	A
Security grade	2
Environmental class	II
Operating voltage	230V AC, 50Hz
Max. Output current	4A
Rated output voltage	12V DC
Fuses	3.14A (both)
Battery failure voltage threshold	11.5V +-10%
Battery cut-off voltage	10.5V +-10%
Operating temperature range	-10...+55°C

Swissdotnet SDN-3030-SPT-DP-3G/4G blue cabinet :

Dimension (WxHxD)	300x300x100mm
Weight	2700g
Features	– Transparent screen to check SDN-3030-SPT-DP-3G/4G state without opening the case – Lid switch to be warned when the case is open – Back switch to be warned when the case is not properly backed against the wall

BIG BAT battery :

Dimension (WxHxD)	151x100x65mm
Weight	2150g
Nominal voltage	12V
Capacity	7A
Type	Lead Acid

2.5. Package contents

The minimum content of the package in case of SDN-3030-SPT-DP-3G/4G PCB only request is as follow :

- SDN-3030 PCB board
- 2x female connector with gripping plate; 2-pole
- 2x female connector with gripping plate; 8-pole
- 2x female connector with gripping plate; 3-pole

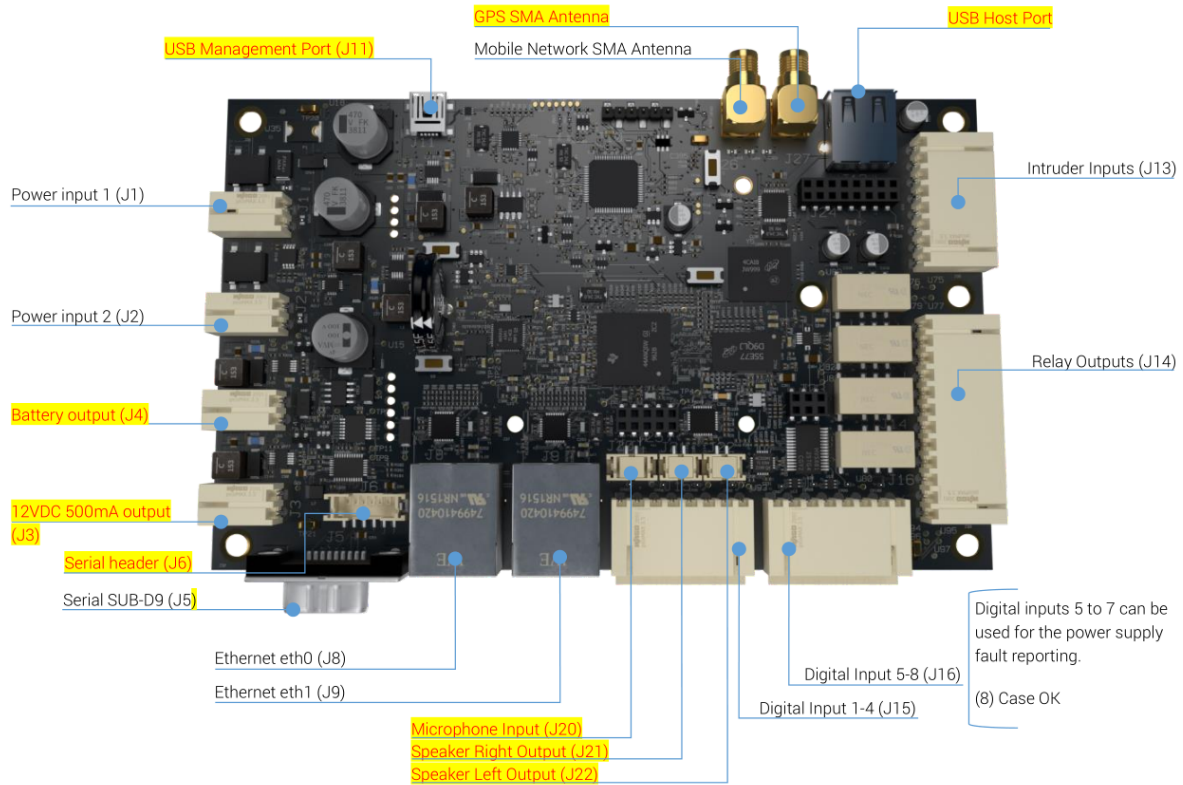
 **SDN-3030-SPT-DP-3G/4G (EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 compliant) package content is as follow :**

- SDN-3030-SPT-DP-3G/4G (PCB board, Swissdotnet SA blue cabinet)
- 2x female connector with gripping plate; 2-pole
- 2x female connector with gripping plate; 8-pole
- 2x female connector with gripping plate; 3-pole

The SDN-3030-SPT-DP-3G/4G can be seen section 2.6.3.1.

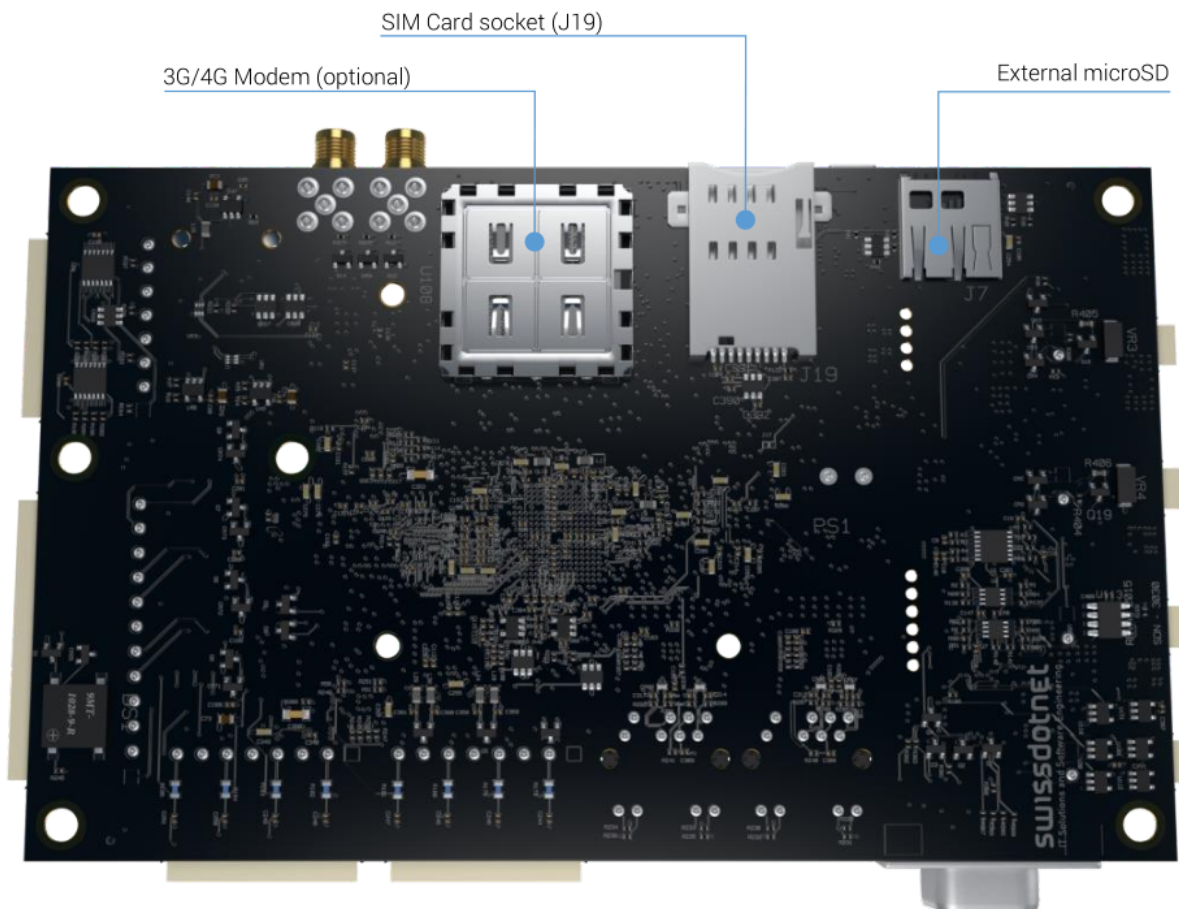
2.6. Physical Overview

2.6.1. Top view



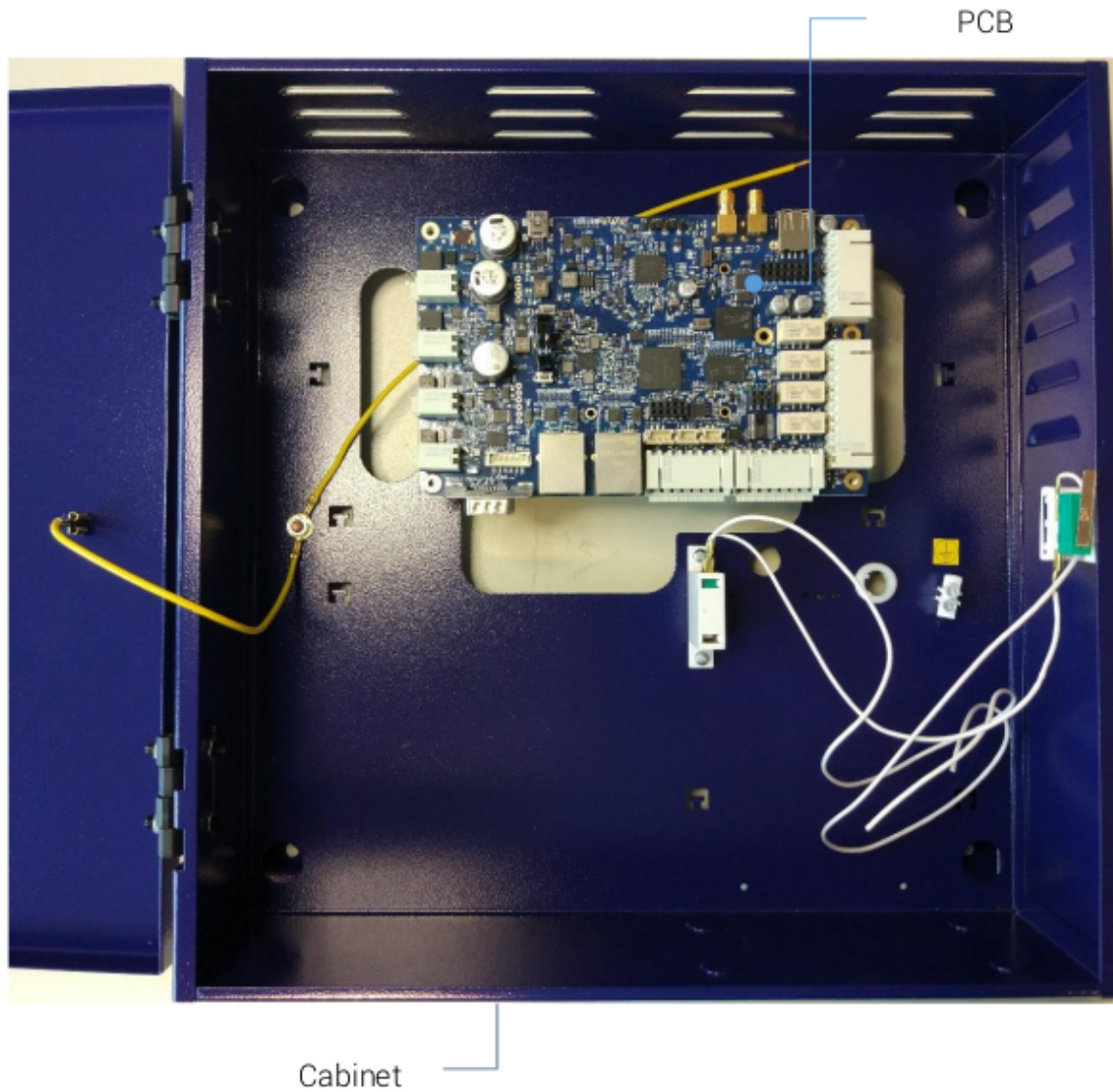
When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required , the following should not be used :
J3, J4, J6, J11, J20, J21, J22, the USB host port and the Global Positioning System (GPS) antenna

2.6.2. Bottow view

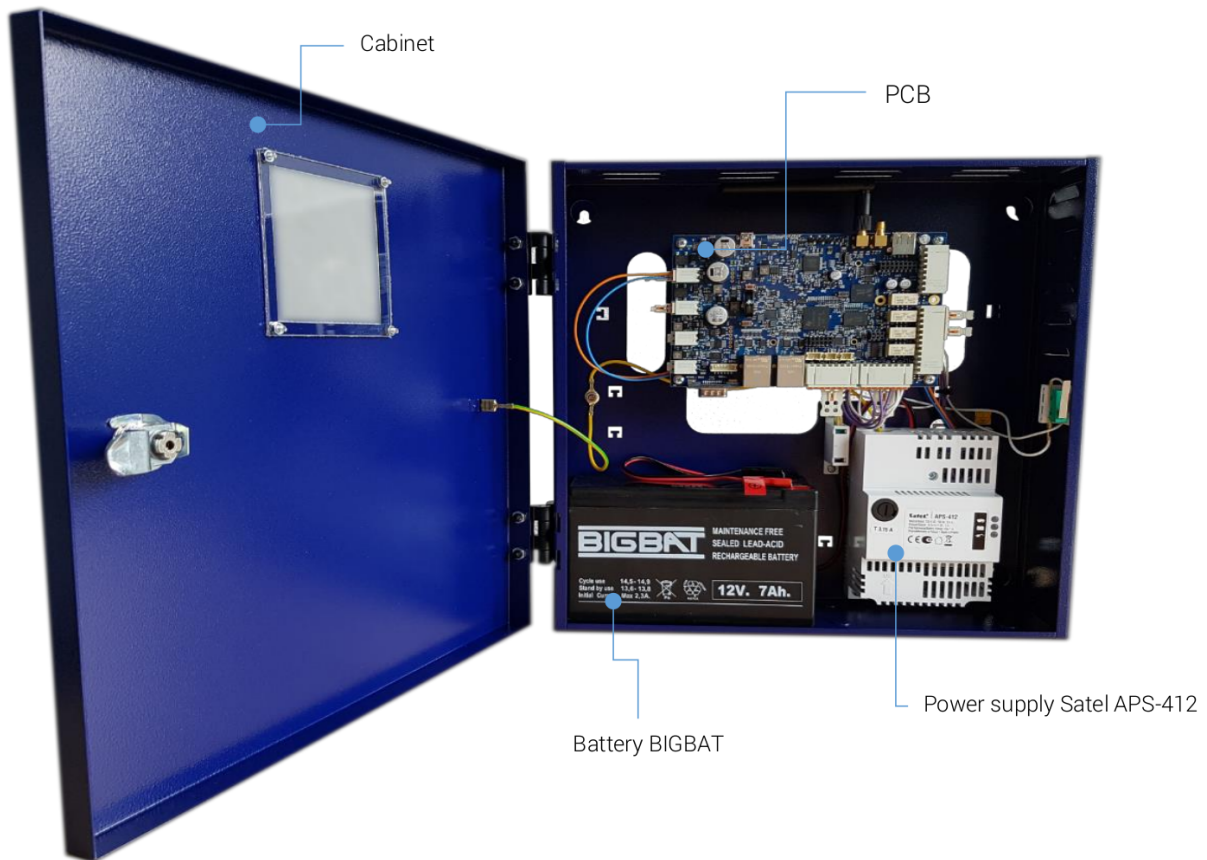


2.6.3. Product view

2.6.3.1. EN 50131-10:2014, EN 50136-2:2013, EN 54-21:2006 Type 1 compliant



2.6.3.2. Uncertified version



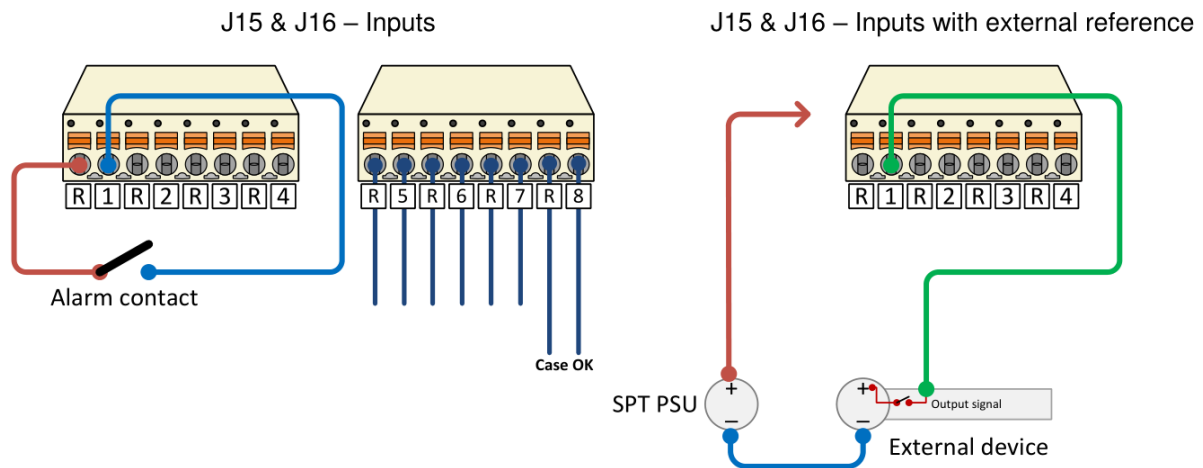
2.7. Connectors

 Cables used for inputs should not be more than 30 meters long.

2.7.1. Digital inputs

The SDN-3030-SPT-DP-3G/4G provides 8 digital inputs. There is a green LED per input showing the current state.

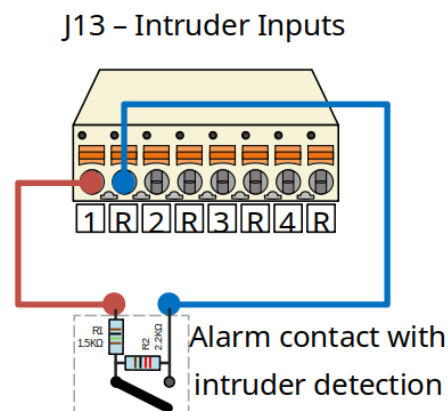
 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required , the inputs 5 to 7 (for example) can be used for the power supply fault reporting.



It is possible to use an external reference signal (10-36 VDC), in this case you need to use the same grounding as the SDN-3030-SPT-DP-3G/4G .

2.7.2. Intruder inputs

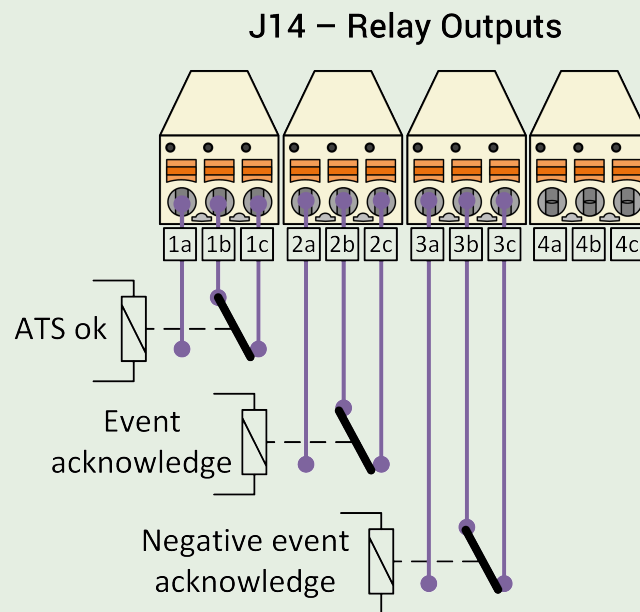
The SDN-3030-SPT-DP-3G/4G incorporates 4 inputs with a current loop which makes it possible to monitor alarm contacts with a fixed resistance ratio (R1, R2), for intruder detection.



2.7.3. Digital outputs

There are 4 free configurable relay outputs on the SDN-3030-SPT-DP-3G/4G . You can use a single 12 pin connector (not provided by default) or multiple 3 pin connectors.

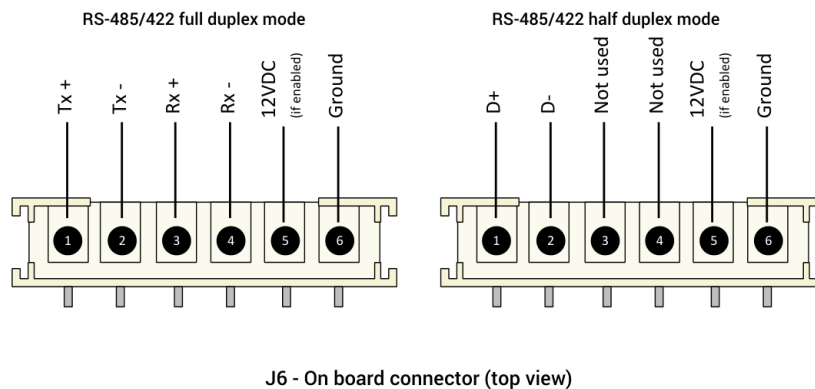
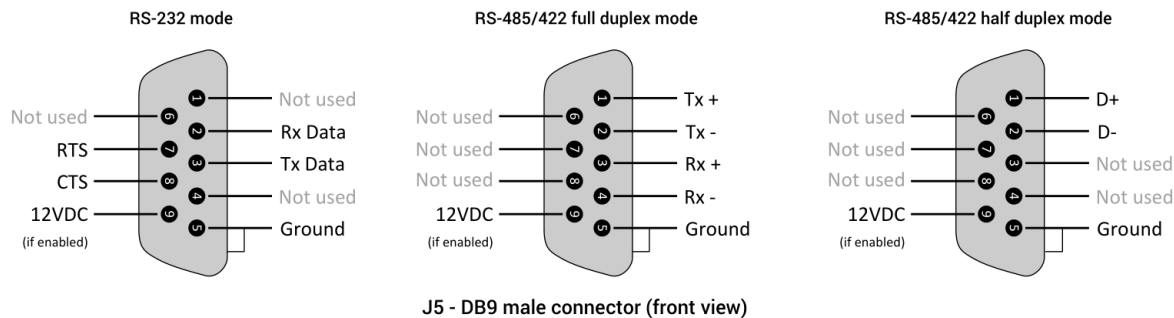
When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required , outputs 1 to 3 (for example) can for be used as interface with the AS as follow :



2.7.4. Serial

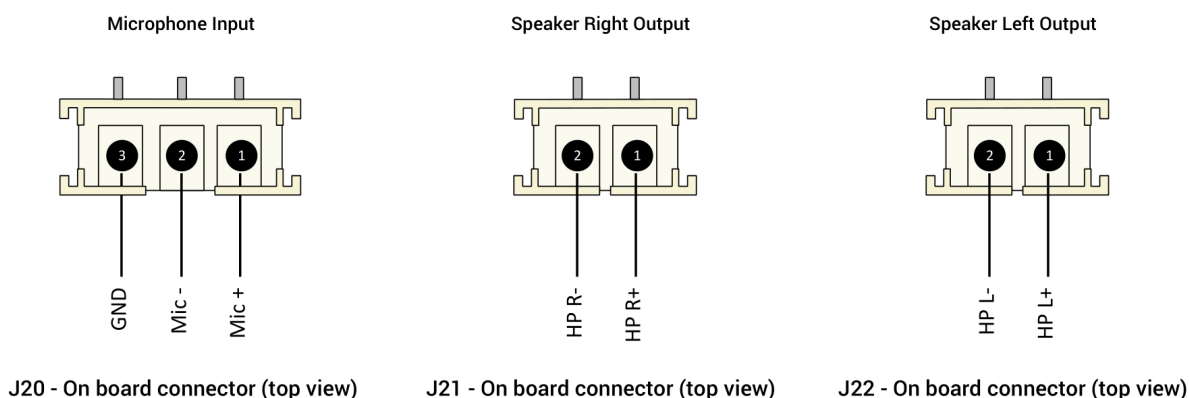
The serial port can be used by various modules (ESPA, Modbus, etc.).

When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required , the serial port can only by used for the ESPA protocol so that additional fire alarm panel information can be added to the triggered fire inputs.



2.7.5. Audio

 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required audio connectors should not be used.



2.7.6. Power supply

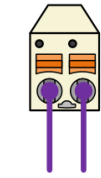
Depending on the type of installation the SDN-3030-SPT-DP-3G/4G is used in (Fire, Intrusion and Hold up Alarm System (I&HAS) J1 and / or J2 will have to be used.

 When compliance with EN 54-21:2006 Type 1EN_54-21 is required both J1 and J2 need to be used.

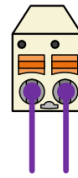
 When compliance with EN 50131-10:2014EN_50131-10 is required only J1 is required.

J1 - Power In 1

J2 - Power In 2



AC/DC +/
AC/DC +/
.



AC/DC +/
AC/DC +/
.

 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required neither J4 (battery) nor J3 (DC 12V out) should be used.

J4 - Battery

J3 – DC 12V out



+ |



+ |

3. Installing the SDN-3030-SPT-DP-3G/4G

3.1. Unpacking

 Do not remove the SDN-3030-SPT-DP-3G/4G from its packaging until ready to install it.

- Carefully open the shipping box by using a cutter

 Be careful not to cut too deep. Failure to do so could damage the device!

- Remove the documentation and set it aside

 It is possible the package includes an outdated version of the documentation stating the URL to reach the SDN-3030-SPT-DP-3G/4G web interface is <https://192.168.128.1>. If this is the case, we are sorry for the inconvenience and ask you to correct it to <http://192.168.128.1>.

- Check that all the components are prepared and ensure that there is no visible damage. The component list is available section 2.5 of the document.

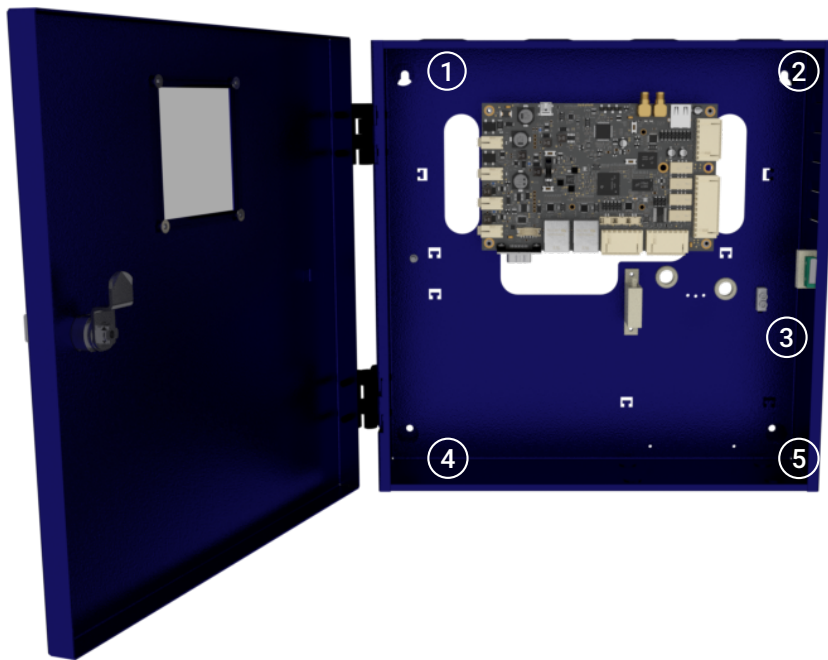
 If the items received do not match your order, or are damaged, contact your re-seller as soon as possible.

- Follow this manual to setup the SDN-3030-SPT-DP-3G/4G and start using it

 Keep the packaging material and the shipment box in case of return.

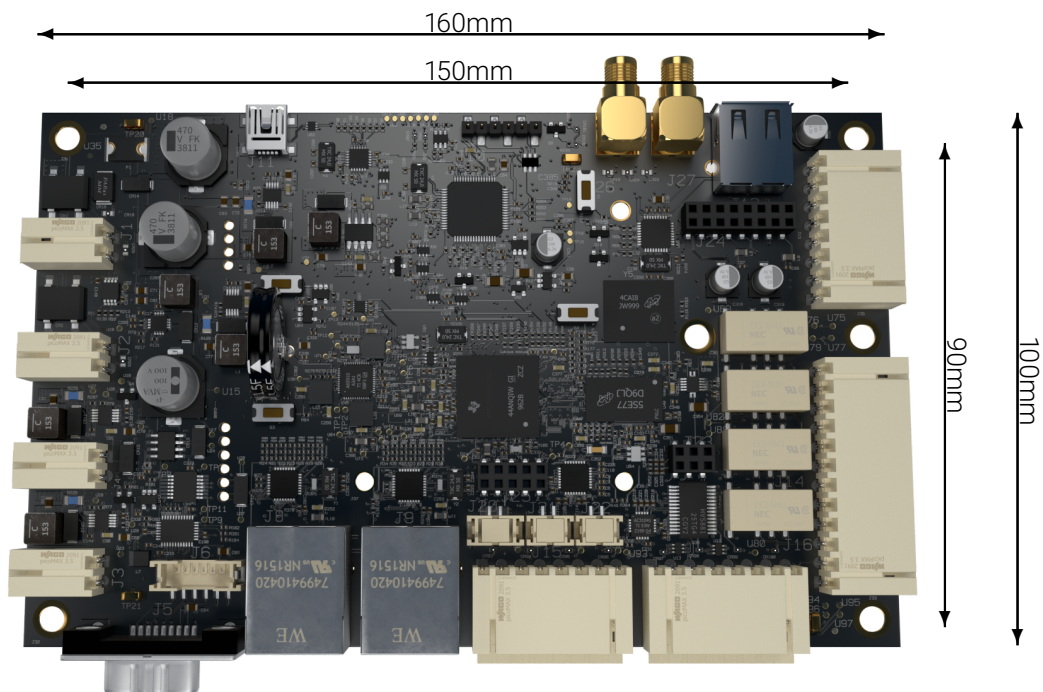
3.2. Physical installation and wiring

The SDN-3030-SPT-DP-3G/4G needs four (non-provided) screws to fix it against a flat wall. Four holes have already been made at the bottom of the case to fix it. (1), (2), (4) and (5).



i It is important not to forget to earth the cabinet using the closest earth available **3**.

The PCB of the SDN-3030-SPT-DP-3G/4G must be **(in uncertified installation)** integrated either in a dedicated box or in an existing installation. This product has not been designed to be installed in an open location. The fixing must be carried out using the four fixing holes provided for this purpose.



i It is recommended to use spacers and metal screws to share the grounding of the equipment with its box.

⚠ Some application areas, including security or fire involve specific provisions. The installer

must comply with current regulations in areas where the product is used.

Section 2.7 describes in detail the cabling of connectors and ports on the SDN-3030-SPT-DP-3G/4G .

3.2.1. Power and battery

Depending on needs, the SDN-3030-SPT-DP-3G/4G PCB can be powered by two power sources. It is possible to use a DC power supply or AC transformer. The supply voltage must conform to the material specifications described in section 2.4.

A 12V battery can be connected directly to the device. We recommend using 12V - 7Ah (BIG BAT) batteries with an operating time of about 24 hours in most use cases.

A protected output 12VDC / 500mA is available to power an external element (striker, relay, lamp, etc.). It is necessary to activate it from the configuration before using.

 **When compliance with EN 54-21:2006 Type 1EN_54-21 is required**, it is mandatory to use an external power supply EN 54-4EN_54-4 compliant.

 **When compliance with EN 50131-10:2014EN_50131-10 is required**, it is mandatory to use an external power supply EN 50131-6EN_50131-6 compliant.

 **When compliance with EN 50131-10:2014EN_50131-10 is required**, the 12VDC / 500mA power output **must not be used**.

3.2.2. Network connection

The SDN-3030-SPT-DP-3G/4G provides two Ethernet interfaces (eth0 and eth1) that can be configured freely. By default, eth0 is connected to the Internet. The second interface can be used to communicate with an auxiliary system such as a detection unit, an IP camera network or a programmable controller.

 Never connect both interfaces on the same subnet.

 Never connect both interfaces on the Internet.

Transmission medium : Twisted Pair UTP (or better) 100 m maximum cable length.

3.2.3. Mobile network connection

If the installed model has a 3G or 4G module, connect the antenna and insert the SIM card into the slot available for this purpose.

 We recommend proceeding to a measurement of the signal on the site in advance to ensure that the operator's coverage area is sufficient. If necessary, use an external antenna (indoor or outdoor) to improve the signal.

3.2.4. Connection with the AS

The SDN-3030-SPT-DP-3G/4G has been designed to provide a parallel interface to the AS which complies with the EN 50136-2:2013EN_50136-2 . To provide this interface, any of the physical inputs / outputs can

be used. More information about how to configure the device physical inputs / outputs are available in section 5.5 of this document.

Furthermore, the SDN-3030-SPT-DP-3G/4G can use its serial port (J5) to receive additional information from the AS.

 The serial cable used to wire the SPT to the AS should not be more than 10 meters.

 When the SDN-3030 is powered by the AS it is possible this one start signaling a ground error. If this is the case you simply have to make the SDN-3030 use the AS ground.

3.3. Basic configuration

To perform the initial configuration, use the USB service cable (not included, must be ordered separately).

 The USB service cable requires a driver to work properly on Windows OS. This driver is available on the [Swissdotnet website](#).

The USB service cable provides access to the device through a network connection on USB. This way it is possible to configure your SDN-3030-SPT-DP-3G/4G without disconnecting it from the infrastructure where it is installed.

The default authentication credentials are username **supervisor** and password **supervisor**. When connecting for the first time using these credentials, a dialog will ask you to change it.

 Be advised that no operation can recover a lost password. Once changed, the password is stored in an encrypted way which cannot be reversed.

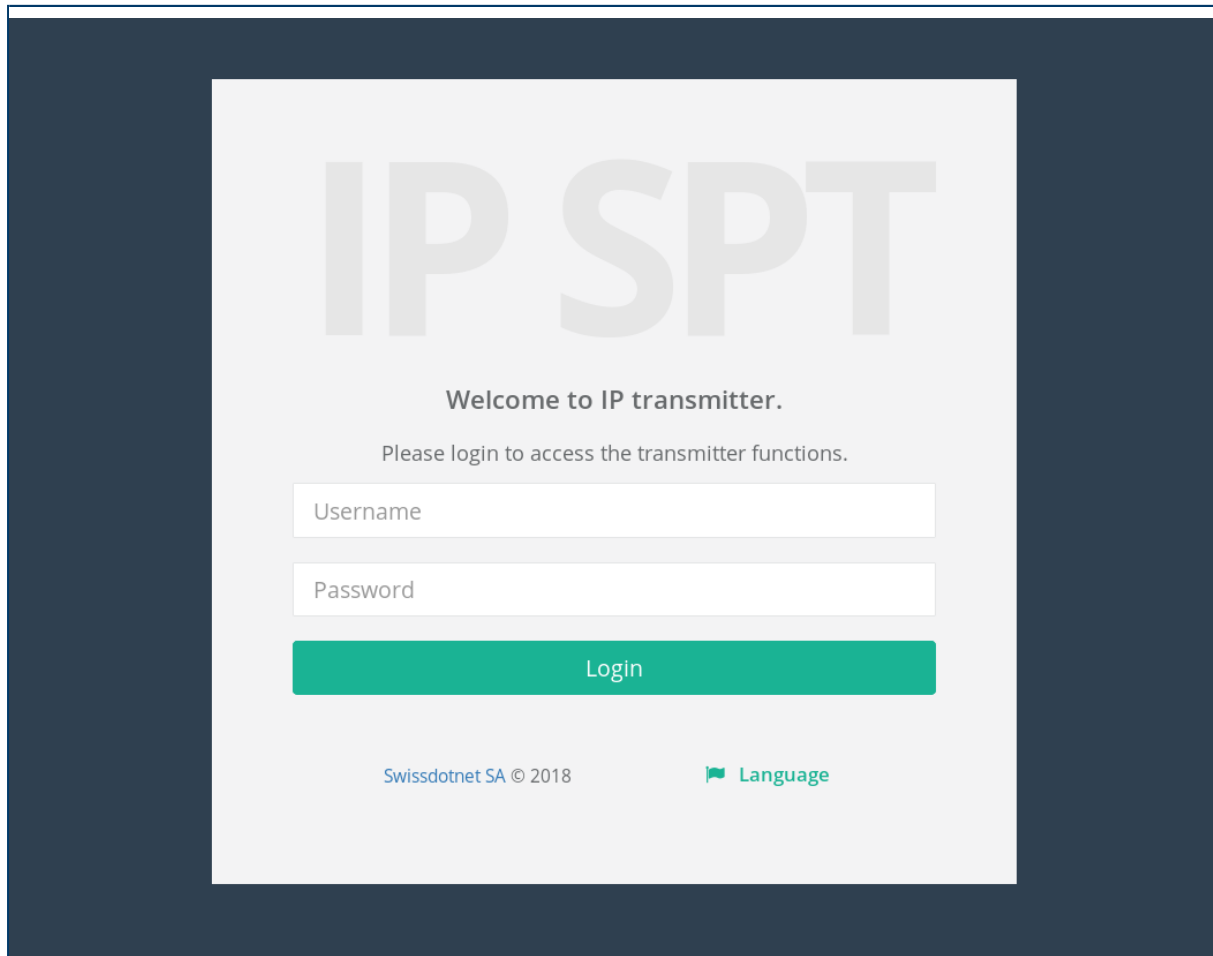
3.3.1. USB service cable

 Power the SDN-3030-SPT-DP-3G/4G on.

When running factory software, the device is configured with IP address 192.168.128.1.

Connect with a browser to <http://192.168.128.1> and authenticate with user **supervisor** and password **supervisor**. After the first authentication, the device will enter in commissioning mode and will ask you to set the supervisor and the client passwords.

 It is highly recommended to use either [Firefox](#) or [Chrome](#) to access the SDN-3030 front interface.



The image shows a login interface for 'IP SPT'. It features a dark blue background with a light gray central panel. At the top of the panel, 'IP SPT' is written in large, light gray letters. Below this, the text 'Welcome to IP transmitter.' is displayed, followed by 'Please login to access the transmitter functions.' There are two input fields: 'Username' and 'Password'. A green 'Login' button is positioned below the password field. At the bottom of the panel, the text 'Swissdotnet SA © 2018' is on the left, and a 'Language' link with a flag icon is on the right.

IP SPT

Welcome to IP transmitter.

Please login to access the transmitter functions.

Username

Password

Login

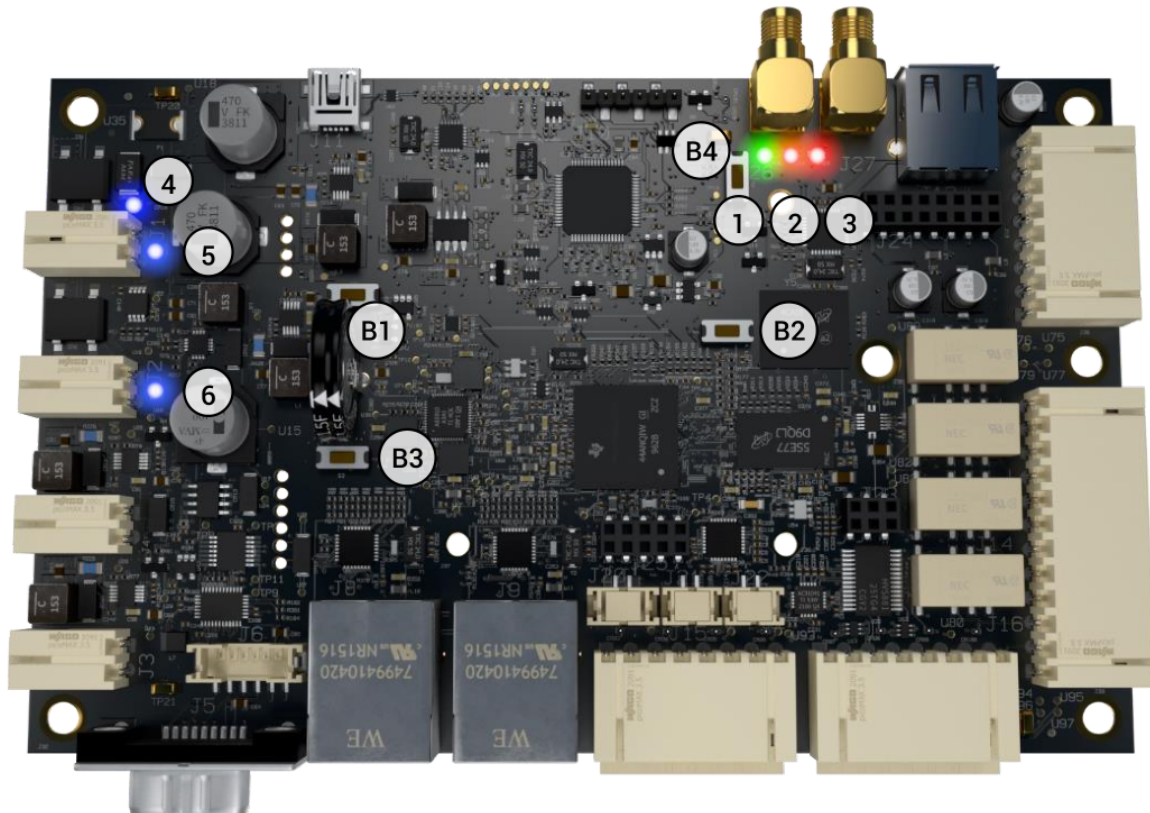
Swissdotnet SA © 2018

 Language

When successfully changed, the web interface will show the dashboard with all information. Refer to section 5.3 to know more about the dashboard and all data available.

4. Display Elements and buttons

4.1. On PCB



①	Green/off	Heartbeat	
		Permanent on	Booting
		Blinking slow	All modules are working fine and are started (200ms On, 1800ms Off)
		Blinking fast	One or more module(s) are not started (300ms On, 300ms Off)
②	Orange/off	Major failure (SPT)	
		Blinking	One ATP is disconnected, alarm transmission is assured (500ms On, 1000ms Off)
③	Red/off	Critical failure (SPT)	
		Blinking	One or more monitored ARC is/are disconnected (300ms On, 600ms Off)
		Permanent on	One or more monitored ARC is/are disconnected and there is pending event(s) to transmit
④	Blue/off	Status of global system power	
		Permanent on	All monitored power supplies are OK
		Blinking slow	One or more monitored power supply input are in failure (200ms On, 1800ms Off)
		Blinking fast	Device is on battery (300ms On, 300ms Off)
⑤	Blue/off	Status of power Input 1	
		Permanent on	Power supply voltage is available on input 1
		Permanent off	Power failure on input 1
⑥	Blue/off	Status of power Input 2	
		Permanent on	Power supply voltage is available on input 2
		Permanent off	Power failure on input 2
B1	Hardware Reset button		
B2	Available for custom usage		
B3	Boot on uSD button		
B4	Acoustic alarm acknowledges		

5. Configuration

This section describes the configuration of the different parameters available on the SDN-3030-SPT-DP-3G/4G .

5.1. General information

Configuration pages are designed in one of two ways.

5.1.1. First design

The modifications you made were applied when you deleted one (or multiple) element(s) or when you exited the "Edition" window by clicking the Apply button. The configuration then needs to be saved for it to be in use.

The image below shows the available operations :

The screenshot shows a web interface titled 'Users'. Below the title is a 'Modify users' section containing three buttons: a green '+' button (1), a green 'Save' button (2), and a grey 'Cancel' button (3). To the right of these buttons is a 'Search' label and a text input field (4). Below this is a table with three columns: 'Username', 'Access level', and 'Actions'. The table contains two rows: 'client' and 'supervisor'. The 'client' row is highlighted with a light blue background. The 'Actions' column for each row contains 'Edit' (pencil icon) and 'Delete' (X icon) links. The table is labeled with a circled 5. The 'Actions' column is labeled with a circled 6.

Username	Access level	Actions
client	Client	Edit / Delete
supervisor	Supervisor	Edit / Delete

① The **+** button allows to add a new item to the current list (e.g : in this case, it will create a new user in the users list)

② Changes to the configuration are applied when the user clicks on the Save button

i Note that this action will restart the module in question.

③ The Cancel button revert all parameters to the running configuration

④ The search field can be used to filter and search an item in the list

⑤ List of all configured items

⑥ Action available for each item

If you added **+** , edited **✎** , or deleted **✕** a configuration, changes are shown highlighted :

Modify users Unsaved changes

+ Save Cancel Search

Username	Access level	Actions
 dane	Supervisor	 Edit /  Delete
 John	Client	-
supervisor	Supervisor	 Edit /  Delete

- ① Indicator of unsaved changes
- ② New or modified configuration item (blue background)
- ③ Removed configuration item (gray background)

Do not forget to request the SDN-3030-SPT-DP-3G/4G to make use of the new changes by clicking the Save button.

5.1.2. Second design

Everything is done in the same windows and as such, before requesting the SDN-3030-SPT-DP-3G/4G to make use of the new changes by clicking the ② Save button you first need to request it to apply them by clicking the ① Apply button.

VPN remote access

① Apply
② Save
Cancel

Mode

▼ Permanent

☒ Enabled

Remote 1

46.14.125.133 19000 + -

+

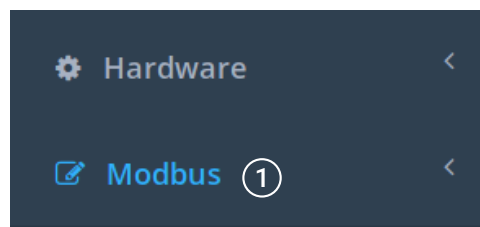
Certificate

▼ RA Server certs

TLS key

▼ RA TLS key

With both design if you have unsaved changes in some modules, the concerned modules will be highlighted in blue (①) in the menu bar :



i Due to their internal working some modules, upon configuration saving, might need to request for other modules to restart. As such you should remember that :

- ➔ Saving the Network module configuration will restart the VPN module
- ➔ Saving the Hardware module configuration will restart the Network module
- ➔ Saving the VPN module configuration will restart the Video streams module

i Modules can make use of one another information (e.g an event created in the alarm transmission module might use the state of a physical input, an action might use the state of a video stream, a script might use the state of a Modbus slave ...) and to do so need to "subscribe" on those information. If when you try to save a configuration you get the Invalid configuration message it often means you tried to remove some item providing information another entity is using. To overcome this you need to check where this item you tried to remove might be used and (if you are sure you really want to remove it) remove its user as well.

5.2. Header

The header part of the User Interface (UI) shows some useful information :



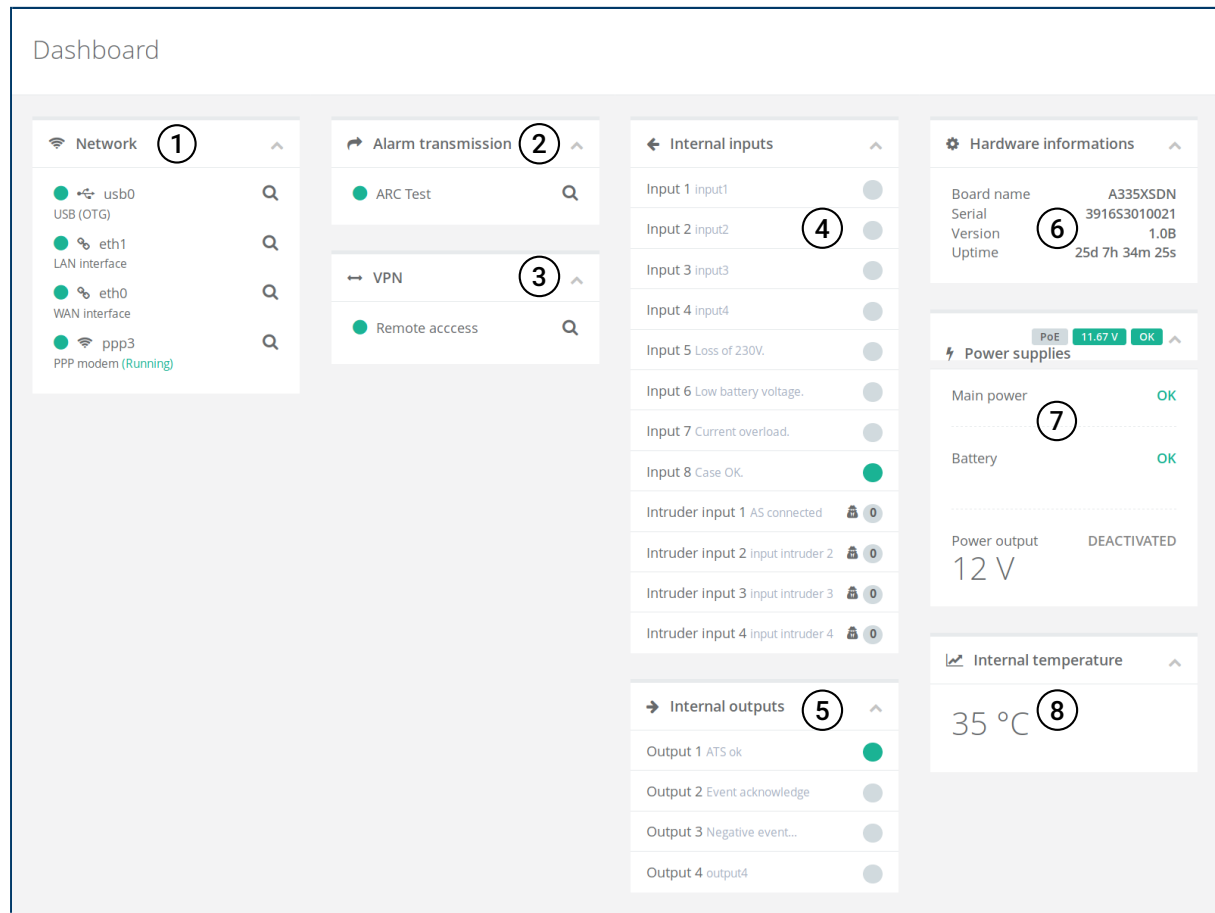
- (1) Device name. You can provide a custom name for your needs.
- (2) Power supply state.
- (3) WWAN signal level (presents if you have a modem configured and receiving a sufficient signal).
- (4) Working mode (Maintenance or Normal).

i Operations which will change the way the SDN-3030-SPT-DP-3G/4G behave (changes to the configuration) are only possible in Maintenance mode. Unintrusive actions such as temporarily changing a module log-level, exporting the configuration, exporting the application logs or sending test notifications are allowed in normal mode.

- (5) Language selector.
- (6) Personal user settings (password reset).
- (7) Log out button to disconnect properly.

5.3. Dashboard

Once logged into the device, you will see a summary of all components in the dashboard :



- ① Network interfaces, click on  to show details information
- ② Alarm transmission (SPT), click on  to show details information
- ③ VPN connection state, click on  to show details information
- ④ Internal inputs states
- ⑤ Internal outputs states
- ⑥ Hardware information
- ⑦ Power supplies information
- ⑧ Internal temperature

5.4. Authentication

5.4.1. Users and access levels

During the initial commissioning, 2 users are automatically created :

-  **Supervisor** Maintenance and commissioning functions. The supervisor is able to modify the whole configuration of the device.
-  **Client** Access to information about to operational status of the device.

The supervisor can create other users with the needed access level.

There is a third user which is already created, the Administrator. Its account is only available to Swiss-dotnet SA , it allows to view the whole configuration and to proceed with software update.

Some general information about the operational status of the SDN-3030-SPT-DP-3G/4G are available without any authentication, it corresponds to the Guest user access level.

 Those access levels can be matched with the ones described in EN 50136-2:2013 **EN_50136-2**

Guest	Level 1	"Access to functions, indications and notifications available to any individual without authentication"
Client	Level 2	"Access to information about the operational status of the SPT. Access level 2 may also allow access to basic functional tests and the management of other access level 2 users"
as follow : Supervisor	Level 3	"Maintenance and commissioning function, access in order to affect the SPT configuration including the addition, removal or replacement of components and other operations that directly, or indirectly, may influence the functions of the SPT"
Administrator	Level 4	"Access to update the software and read-only functions"

The required rights for each configuration parameters will be explained in this document with the corresponding icons : S  , A  , C 

Example with full access for Supervisor and read only access for Client and Administrator :
S   A   C  

The users panel (available in the menu Authentication → Users) allows you to edit, remove and add users.

Click on the **+** button to add a new user account.

supervisor

Username

Access level

▼

Supervisor

Password

Password confirmation

Common parameters to users :

Username	Login credential used by the current user
Access level	User access level (Supervisor, Client)
Password	Password field used to change the current password
Password confirmation	Password confirmation used to change the current password

i Do not change Password and Password confirmation fields unless you want to set a new password.

5.4.2. Certificates

Many features can require certificates and associated files for secured connection (e.g VPN connection, MQ Telemetry Transport (MQTT) clients, ARCs ...). Since it is possible for multiple features to use the same certificates and in order to prevent any unnecessary duplicates, the SDN-3030-SPT-DP-3G/4G offers you to manage those in a single place to later be able to use them where needed.

i It means if any feature you want to use requires a certificate you will have to add it here if it is not already available.

To add certificates you simply have to click the **+** , fill the name and description you want the files to have and then upload the file(s). The SDN-3030-SPT-DP-3G/4G allows you to bundle files by uploading up to two files under the same certificate name/description. This is especially useful if a feature requires both a certificate and a Transport Layer Security (TLS) key for example.

New certificate

Name

Description

File 1

Choose File No file chosen

File 2

Choose File No file chosen

Apply

Cancel

i The second file is only optional.

The SDN-3030-SPT-DP-3G/4G currently accept the following extension :

- .crt
- .key
- .pkcs8
- .p12

i File size is limited to 2Mo.

i Upon saving the configuration you will be disconnected from the SDN-3030-SPT-DP-3G/4G interface. (This happens because the Authentication module is restarted)

🚨 It is very important to remember that if you upload file(s) containing multiple similar kind of data in a same bundle then only the last one will be kept on the SDN-3030-SPT-DP-3G/4G . It means for a bundle (with one or two files), there should be at most one certificate (or certificates chain), and one key. If more are needed, upload them in separate bundles.

Once created, you can see on the certificates list which kind of data the SDN-3030-SPT-DP-3G/4G has been able to extract from the uploaded file(s).

To avoid unwanted behavior it is only possible to modify the description of an already created certificate.

i New SDN-3030-SPT-DP-3G/4G all have default Swissdotnet SA certificates used by the Swissdotnet SA VPN remote access and Swissdotnet SA MQTT client. Their deletion is useless since they will automatically be re-created.

Modify certificates

Search

Name ^①	Description ^②	Types ^③	Actions
SDN - CORE CA	Swissdotnet CORE CA	CRT	Edit / Delete / Info
SDN - Device Management cert/key	Swissdotnet - Device manager cert/key	CRT / KEY / PKCS_12	Edit / Delete / Info
SDN - Device manager	Swissdotnet - Device manager	CRT	Edit / Delete / Info
SDN - Device manager TLS key	Swissdotnet - Device manager TLS key	KEY	Edit / Delete / Info
SDN - MQTT server	Swissdotnet - MQTT server	CRT	Edit / Delete / Info

- ① Bundle name. You can provide a custom name for your needs.
- ② Bundle description. You can provide a custom description for your needs.
- ③ Bundle types. The types the SDN-3030-SPT-DP-3G/4G has been able to extract from the provided file(s).

i The **i** info button allow you to check the information of your bundle (e.g : version, serial number, issuer, validity, ...)

5.5. Physical inputs and outputs

S   A   C  

5.5.1. Inputs

Modify internal inputs

Search

⑧ **Internal input 1** Fire alarm from AS ④ Activated ☒ ^⑤

Description

Fire alarm from AS ^⑥

☒ **Logic inverted** ^⑦

Internal input 2 input2 Deactivated ☐ ^⑤

Internal input 3 input3 Deactivated ☐ ^⑤

The configuration of the physical inputs (Menu Inputs / outputs → Inputs) is limited to the description of the entry and its logic (7). Choosing to inverse an input logic means that when the physical contact is closed, the input will be stated as DEACTIVATED. An icon ❶ (8) is displayed near your input name to highlight the fact that its logic is inverted.

The input electrical state is displayed in real time¹ on the page (5) (if this Logic inverted (7) is checked then the opposite of the electrical state is displayed).

To change the description, it is necessary to click on the edit line (4) and then click Apply (6) to apply the change.

Once inputs configuration is complete, click on Save (1) to permanently apply the changes.

It is possible to undo all changes made (as long as the Save button has not been used) by clicking the Cancel (2) button. This action restores the previous configuration.

Inputs can be filtered by entering the criteria you are looking for in the filter (3) field.

 For certified installation the following configuration can be used for standard inputs :

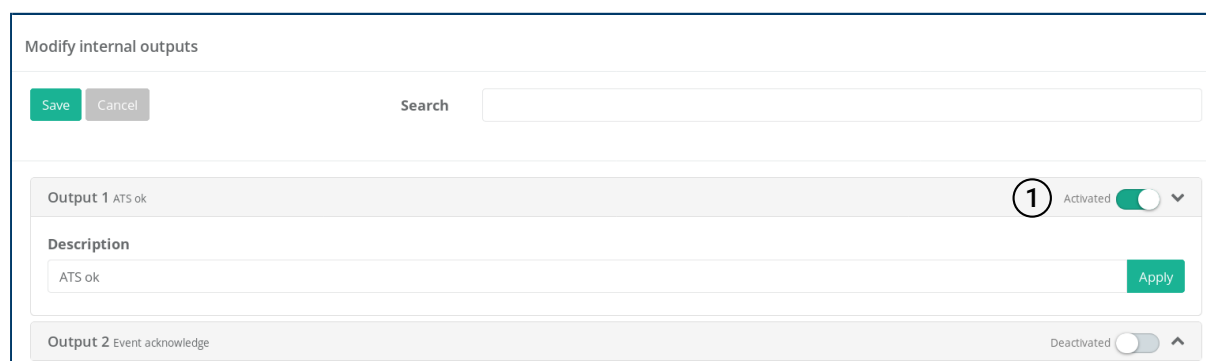
Input name	Input description
Internal input 5	Can be used for the power supply fault reporting
Internal input 6	
Internal input 7	
Internal input 8	Case OK

For certified installation the following configuration can be used for intruder inputs :

Input name	Input description
Intruder input 1	AS connected

5.5.2. Outputs

The configuration of the physical outputs (Menu Inputs / outputs → Outputs) is similar to that of inputs.



In maintenance mode, it is possible to test the output manually by clicking on the button next to its state (1).

5.6. Network

1. It is not exactly in real-time since this web page is only refreshed every 5 seconds

5.6.1. Interfaces

Network interfaces are configured from the Network → Interfaces menu.

The list of available physical interfaces is displayed on this page. It allows you to quickly know the state² of interfaces and which ones are configured as WAN. Since network interfaces are auto discovered during the device startup, it is not possible to manually add a network interface. Click on  Edit to change the configuration of an interface.

Modify network interfaces					
Save Cancel		Search			
Name	Polling supervision	Description	Type	WAN (default gateway)	Actions
eth0	 Activated	WAN interface	 ETH	✓	 Edit /  States
eth1	 Activated	LAN interface	 ETH	✗	 Edit /  States
ppp3	 Activated	PPP modem (Running)	 PPP	✓	 Edit /  States /  Reset /  Pause
usb0	 Deactivated	USB (OTG)	 USB	✗	 Edit /  States

 The ppp interface description is appended with a precision regarding the modem state (e.g here : Running). This state is dissociated of the general state of the interface (the modem can be in operation without being able to poll the monitoring addresses).

 The  Reset button allows to manually reset the PPP interface if needed.

List of available network interfaces :

-  **eth0** Primary Ethernet Interface (type ETH). This interface is configured for DHCP by default. WAN mode is enabled by default.
-  **eth1** Secondary Ethernet Interface (type ETH)
-  **ppp3** 3G/4G module (optional) (type PPP)
-  **usb0** USB management interface "On The Go" (USB type)

Common parameters to all interfaces :

² The state of the interface is labeled as Polling supervision here. If no connection monitoring addresses (refer to section 5.6.1.2 to know more about connection monitoring) have been provided for an interface then its state is computed using the physical layer only (is it physically linked to another device)

Name	Interface name (only for information, read only).
Description	Interface description. You can provide a custom description for your needs.
MAC address	Interface Hardware Address (only for information, read only) (not available for PPP3).
Type	Interface Type (only for information, read only).
Priority	Interface priority.
WAN (default gateway)	Check this box if an Internet access is available through this network interface. This will enable routing for outgoing access.
Accept dynamic DNS	Check this box to use DNS servers provided by the DHCP server. This option is only available if you have configured the IPv4 mode to DHCP.
Connection monitoring	Connection monitoring is used to monitor periodically if the interface is connected to the specified network. More information is available in section 5.6.1.2. By providing a polling frequency and some hosts, the SDN-3030-SPT-DP-3G/4G is able to correctly switch the default route between the primary and the secondary interface. The connection monitoring is required if you use services (SMTP, NTP, VPN, DNS, etc...) and must work even if the primary path is unavailable. SPT Alarm Transmission does not require Connection monitoring to work.

Specific parameters to ETH  interfaces :

IPV4 Mode	Select IPV4 mode (DHCP, static or disabled) — Disable : IPV4 is disabled for this interface — Static : IPV4 address, netmask and gateway are configured manually — DHCP : IPV4 is configured automatically (this requires a DHCP server on the network)
IPV6 Mode	Allows to set the IPV6 configuration. The SDN-3030-SPT-DP-3G/4G is IPV6 ready, but this option is currently not available

Specific parameters to PPP  interfaces :

Operator preset	When checked, reveals a list of operators for which below parameters have already been set (to use it, simply select your operator)
User	PPP Username (provided by your Mobile Network Operator)
Password	PPP Password (provided by your Mobile Network Operator)
PIN code	PIN code of your SIM Card (provided by your Mobile Network Operator) (leave empty if PIN Code has been disabled)
APN	Access Point Name (provided by your Mobile Network Operator)
SCA	Service Center Address (provided by your Mobile Network Operator), used to send SMS
Dev path	Physical path on the device (only for information, read only)
Min signal quality	Minimal signal quality level (if the signal level drops below this limit, a virtual input is activated)
Data enabled	Check this box to use data traffic on this SIM card (mandatory if you want to use this interface as alarm transmission medium)
SMS enabled	Check this box to enable sending of SMS on this interface, in conjunction with the notification module (see section 5.12.1.2)
Roaming enabled	Check this box to allow roaming
GPS enabled	Check this box to enable the GPS (requires to have a GPS)

5.6.1.1. Status

The status panel displays detailed information about an interface (IP, traffic, etc.).

eth0

ETH

Description

MAC address

Priority

WAN (default gateway)

Mode

IP

WAN interface

d0:39:72:49:f4:3c

10

✓

DHCP

/ 0

IPV4

Data outflow

Data inflow

Data output

Data input

Up since

5.59 KB / s

7.1 KB / s

68.11 MB

246.84 MB

27/06/2018 14:35:00

Monitoring

Polling frequency (s)

Monitoring 1

Monitoring 2

60

8.8.8.8

208.67.222.222

For PPP 📶 interfaces, the following information are also displayed :

- Signal level Reception signal to noise ratio
- IMEI IMEI
- Provider Current Network Mobile Operator
- Cell Identification number of the current cell
- Cell location Identification number
- MCC Mobile Network Code of the current registered network
- GPRS technology Current technology used for data access over the mobile network
- Firmware Modem firmware version
- Serial number Modem serial number

IMEI	355465070473943
Provider	Salt
Cell	0034CB03
Cell location	FFFF
MCC	228
MCN	03
GPRS technology	e-utran (LTE)
Firmware	RHL769x.2.26.18...
Serial number	VE820242790310
📶 PPP (Running)	

i The signal strength is also displayed on the top of the web page (provided its value is greater than -110).

5.6.1.2. More about connection monitoring

To get a full redundant Internet connection, the device has to be able to monitor each interface who are connected to Internet (WAN). Through this operation, the equipment can automatically change the default route according to the status of the interfaces and their priority.

This allow you to use SMTP notification, time synchronization, VPN and other network services in a redundant way. The alarm transmission (SPT module) does not use the default route as it directly uses each physical interface.

🔊 Connection monitoring use Internet Control Message Protocol (ICMP) Ping request on one or more Internet IP Address. Please check that the firewall does not block ICMP Ping request on the WAN.



The screenshot shows a web interface titled "Connection monitoring". It features a "Polling frequency (s)" input field with the value "60". Below this, there are two monitoring entries: "Monitoring 1" with IP "8.8.8.8" and "Monitoring 2" with IP "208.67.222.222". Each entry has a green minus button to its right. At the bottom left, there is a green plus button.

Polling frequency (s) This is the connection monitoring control frequency in seconds. Default value is 60 seconds for DP4 (less than 20 seconds for SP6).

🔊 Do not use a too fast frequency for mobile network interfaces because it can significantly increase the traffic.

Monitoring List of IP to monitor. Default value are :

- 8.8.8.8 DNS server from Google
- 208.67.222.222 DNS server from OpenDNS

5.6.1.3. Connection monitoring and PPP

When a PPP interface has one or more monitoring target, the state of the interface is linked to the monitoring state. In fact, if the monitoring status is down during more than 30 minutes, the system will reset the modem. This leads to a disconnection of the PPP link until the re-connection (this can take several minutes).

This feature is helpful in roaming mode, because sometimes the link is up, but the network operator does not send correctly the traffic to the legacy operator, a reset resolve the case.

 When configuring PPP monitoring always use at least two targets. This avoid up/down of PPP link if the target one fail.

5.6.2. General

General Network Parameters (Network → General) let you configure some global network parameters.



Apply Save Cancel

Hostname
sdn-ip-spt-d0397249f43c

Domain
localdomain.com

☐ Allow IP forwarding 

DNS servers

1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0

Hostname	This is the device name on the network ³
Domain	This is the local network domain used by the system
Allow IP forwarding	This option allows for the SDN-3030-SPT-DP-3G/4G to forward traffic to other devices
DNS Servers	Enter the IP addresses to be used by the system for DNS resolution. Per default the device use DNS servers received by the DHCP client of each interfaces

 It is important to note that the DNS provided on this page take priority over any DNS provided by the DHCP server.

 You should not have multiple device with the same hostname on the same network.

 IP forwarding is highly discouraged and is used at your own risk.

5.6.3. SMS input

It is possible to create an input whose state will change upon reception of an SMS. To do so just click the **+** and fill the required information.

³. It can be especially useful when your device does not have a static IP address.

New sms input

Name

Activating data

Deactivating data

☐ **Accept all phone numbers**

Incoming phones white list

Add phone number

Apply

Cancel

Name	The name of the input you are creating
Activating data	The data the input is expecting to switch its state to ACTIVATED
Deactivating data	The data the input is expecting to switch its state to DEACTIVATED
Accept all phone numbers	Check this box to allow any number to be able to change this input state
Incoming phones white list	If you do not allow all phone number to be able to change this input state then you need to provide a list of number which are allowed to do so. Just click the Add phone number to add a new allowed phone number. Phone number configuration requires a Country calling code which you can choose in the list and the actual phone number.

 Do not format the number (e.g. 079/111.11.11 must be written as 791111111).

 The usage of short number is possible by selecting the Short number entry in the Country calling code field.

 International SIM card (e.g. Swissdotnet SA card) do not support short number.

 SMS input reliability highly depends on the network reliability. If you configure the SDN-3030-SPT-DP-3G/4G to act upon an SMS reception it is often a good idea to create an action / script (see section 5.13 and section 5.14 for more information) to send an SMS upon action completion.

5.7. Alarm transmission - SPT

5.7.1. Features

Supported transport protocols :

Protocol version	Security	Transport
ANSI/SIA-DC-09-2007/2013	Unencrypted	UDP / (TCP)
ANSI/SIA-DC-09-2007/2013	AES/CBC 128 bits	UDP / (TCP)
ANSI/SIA-DC-09-2007/2013	AES/CBC 192 bits	UDP / (TCP)
ANSI/SIA-DC-09-2007/2013	AES/CBC 256 bits	UDP / (TCP)
CLC/TS 50136-9	AES 128 bits	UDP
CLC/TS 50136-9	AES 256 bits	UDP

Supported alarm protocols :

Protocol
Contatc ID
SIA DC-03

Mode of acknowledgement operation : pass through.

5.7.2. Security

The SDN-3030-SPT-DP-3G/4G has been designed to be as secured as possible.

It is protected against substitution with the following measures :

- Use of an encrypted alarm transmission protocol (Advanced Encryption Standard (AES) 128,192 or 256 can be selected). It is therefore not possible to generate messages, pretending to be the SDN-3030-SPT-DP-3G/4G without knowing the encryption key
- A timestamp is included in the encrypted part of the message and checked upon reception, preventing message recording and replay
- A Cyclic Redundancy Check (CRC) of the content before encryption is included in the message, preventing the alteration of the message content

The SDN-3030-SPT-DP-3G/4G ensures information security by encrypting every communication from the SPT to a Receiving Center Transceiver (RCT) (AES 128, 192 or 256) with a key provided during commissioning.

5.7.3. ARCs

An ARC corresponds to an Alarm Receiving Center, which receives transmitted alarms. Your device can handle simultaneously up to 10 ARCs. The SDN-3030-SPT-DP-3G/4G has been designed to use multiple transmission protocols and each ARC can use its own protocol.

The factory settings do not contain any ARC. You must create them manually by clicking on the **+** button.

5.7.3.1. ARC Configuration

The first tab allows to configure the transport protocol :

New ARC

Configuration

Supervision

Name

My ARC

Operational state

Normal

Description

This is where security alarms are sent

Primary ATP

WAN interface (eth0)

Alternate ATP

PPP modem (ppp3)

RCT 1

Host IP

Pri. port

Alt. port

-

RCT 2

Host IP

Pri. port

Alt. port

-

+

Protocol

SIA DC 09

Encryption key

☐ Use TCP

☐ Nak update

☒ Nak is ack

Next

Cancel

- | | |
|--------------------------------|--|
| ① Name | ARC name |
| ② Operational state | <p>You can choose between three operational state for your ARC :</p> <ul style="list-style-type: none"> • Normal • Not supervised : works as normal ARC but its connection status is not taken into account for SPT fault and ATS failure (and local indication, i.e buzzer and LEDs) • Deactivated : still in the configuration but does nothing <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>i It is especially important to keep in mind that therefore no associated event will be generated when triggered.</p> </div> |
| ③ Description | ARC description. You can provide a custom description for your needs |
| ④ Primary ATP | Primary Network Path |
| ⑤ Secondary ATP | Alternate Network Path, select none if you want to transmit alarms only on one path |
| ⑥ RCT | RCT IP Address and ports for primary and alternate path (provided by your ARC). If the ARC provides alternate RCT, you can create additional entries by clicking on the + button |
| ⑦ Protocol | Transport protocol to use with this ARC, see section 5.7.4 and section 5.7.5 for more information |
| ⑧ Protocol specific parameters | Specific parameters to configure for the selected Transport Protocol. These parameters are described respectively in section 5.7.4 and section 5.7.5 |

Once you finished to enter these parameters, click on the Next button to configure the ARC supervision.

5.7.3.2. ARC Supervision

The second tab is common to all transport protocols. The following settings are used to configure polling and supervision of ARC.

Configuration
Supervision

DP4

①

Primary frequency (s)

90

②

Alternate frequency (s)

18000

③

☒ Frequency switch

④

Maximum transmission time (s)

30

⑤

Lower retransmission timeout (s)

10

⑥

Upper retransmission timeout (s)

20

⑦

Effective polling (s) 

80

⑧

① **ATS categories**

Select one of the ten normalized categories to automatically configure the next settings (provided by your ARC)

② **Primary frequency**

Polling frequency in seconds on the primary path

③ **Secondary frequency**

Polling frequency in seconds on the alternate path

④ **Frequency switch**

If enabled, use the primary polling frequency on the alternate path when primary path failed

⑧ **Effective polling**

Effective polling time, corresponds to the primary frequency minus the lower re-transmission timeout

⑤ **Maximum transmission timeout**

Duration after which an event is marked as Timeout. When the SDN-3030-SPT-DP-3G/4G fails to send a message (alarm or supervision), it will try to resend it. The time the SDN-3030-SPT-DP-3G/4G waits before re-sending the message is defined by an algorithm based on RFC793 used by the TCP protocol. This time will increase slowly based on previous transmission times. However, this time is bounded by two factors :

⑥ **Lower retransmission timeout**

Should be large enough to allow the RCT to wait for an acknowledgment for the AMS and send back the response (10s is a good default)

⑦ **Upper retransmission timeout**

Should be small enough to allow the SDN-3030-SPT-DP-3G/4G to detect ATP failures according to the reporting time of its ATS category

i Monitoring of Transmission Network Interface (TNI)(s) is done through polling and any failure is reported to the AS through the ATS fault output provided as part of its parallel interface with the AS.

i It is very important for the ATS (from the SPT to the RCT (including the Annunciation Equipment (AE))) to always be available.

Your ARC is now ready to be used. Click on the Apply button. If you want to apply the modified settings and connect the SDN-3030-SPT-DP-3G/4G to the new ARC, you must still click on Save on the ARC list.

5.7.3.3. Check the ARCs

From the moment where your ARCs are configured and saved, you can see each ARC state on the list.

Name	State	Operational state	Protocol	Primary ATP	Alternate ATP	Actions
① ⊙ ARC Test	Connected	● Normal	SIA DC 09	📶 WAN interface (eth0)	📶 PPP modem (ppp3)	② ✏ Edit / ③ 🔔 Events / ④ ➡ Remote commands / ⑤ ● States ⑥ ✖ Delete

② **Edit**

Change previously entered ARC parameters

③ **Events**

Assign events/alarms to this ARC (These must first be created in the Alarm transmission → Events menu)

④ **Remote commands**

Assign remote commands to this ARC (These must first be created in the Alarm transmission → Remote commands menu)

⑤ **States**

Show advanced information about the communication with the ARC

⑥ **Delete**

Remove this ARC

i When trying to save a configuration in which you just deleted an ARC it is possible you get an Invalid configuration error. This usually means that some resources (e.g Events, Action, Script, ...) are bounded to this ARC and cannot exist without it. To be able to delete this ARC you must first remove every resources using it.

The ⊙ symbol ① near the ARC name indicates it follows the Nak update policy (see section 5.7.4 for more information on the Nak update).

Information displayed in the state window :

● ARC Test			
Started on		01/07/2018 16:57:19	
Connected since		01/07/2018 16:57:19	
Sent events		1	
Pending events		0	
Temporized events		0	
Last transmitted event		01/07/2018 16:57:19	
Average transmission time		438 ms	
● eth0 primary		● ppp3 alternate	
Started on	01/07/2018 16:57:19	Started on	01/07/2018 16:57:19
Connected since	01/07/2018 16:57:19	Connected since	01/07/2018 16:57:20
Sent events	1	Sent events	0
Pending events	0	Pending events	0
Last transmitted event	01/07/2018 16:57:19	Last transmitted event	-
Sent messages	3	Sent messages	2
Last transmitted message	01/07/2018 16:57:19	Last transmitted message	01/07/2018 16:57:20
Average transmission time	16 ms	Average transmission time	1072 ms
● 46.14.125.133:44300 primary		● 46.14.125.133:44301 alternate	
Started on	01/07/2018 16:57:19	Started on	01/07/2018 16:57:19
Connected since	01/07/2018 16:57:19	Connected since	01/07/2018 16:57:20
Sent events	1	Sent events	0
Pending events	0	Pending events	0
Last transmitted event	01/07/2018 16:57:19	Last transmitted event	-
Sent messages	2	Sent messages	1
Last transmitted message	01/07/2018 16:57:19	Last transmitted message	01/07/2018 16:57:20
Average transmission time	14 ms	Average transmission time	1068 ms
● 62.2.191.69:44300 primary		● 62.2.191.69:44301 alternate	
Started on	01/07/2018 16:57:19	Started on	01/07/2018 16:57:19
Connected since	01/07/2018 16:57:19	Connected since	01/07/2018 16:57:20
Sent events	0	Sent events	0
Pending events	0	Pending events	0
Last transmitted event	-	Last transmitted event	-
Sent messages	1	Sent messages	1
Last transmitted message	01/07/2018 16:57:19	Last transmitted message	01/07/2018 16:57:20
Average transmission time	20 ms	Average transmission time	1076 ms

This panel is very useful to debug connections with ARC. If the connection does not work, please check your ARC settings and the network configuration.

5.7.4. ANSI/SIA DC-09-2007/2013

By using the SIA DC-09 protocol, you have to configure specific parameters on the ARC :

Protocol

▼
SIA DC 09

Encryption key

☐ Use TCP
☒ Nak update
☐ Nak is ack

Encryption key

Encryption key provided by ARC (into HEX format). If you do not want to use encryption, leave this field empty.

Use TCP

If checked this option will request the SDN-3030-SPT-DP-3G/4G to communicate with the ARC using TCP.

Nak update

If enabled the Nak update option will update the SPT date and time if the RCT answers with a NAK message.

 It is very important to enable this option on only one ARC to avoid time tiling.

Nak is ack

If enabled the Nak is ack option informs the SPT that NAK responses (time synchronisation problem with the RCT) are responses confirming the arrival of the message. Without this tag, the SPT will try to re-send the message until it receives the AK response. It is highly recommended to enable this option.

It is mandatory to select either NAK update or NAK is ack mode, otherwise the alarm transmission could be blocked.

5.7.5. CLC/TS 50136-9 (Beta)

When using the TS 50136-9, you must choose between three kinds of commissioning :

- Shared secret commissioning
- Shared secret single commissioning
- DTLS

 A shared secret represents a connection handle (i.e connection identifier of the SDN-3030-SPT-DP-3G/4G) and an encryption key.

5.7.5.1. Shared secret commissioning

For the shared secret commissioning procedure, you must provide a shared secret for each ATP of each RCT of the ARC.

RCT 1

Host IP

Pri. port

Alt. port

-

RCT 2

Host IP

Pri. port

Alt. port

-

+

Protocol

▼

TS 50136-9

Commissioning type

▼

Shared secret commissioning

Commissioning:

1

RCT 1

2

RCT 2

Primary shared connection handle

3

7

7

Primary shared secret key

4

8

8

Alternate shared connection handle

5

Alternate shared secret key

6

① RCT 1

② RCT 2

③ Primary shared connection handle

④ Primary shared secret key

⑤ Alternate shared connection handle

⑥ Alternate shared secret key

⑦ and ⑧

Configuration tab for commissioning of RCT 1 ①'

Configuration tab for commissioning of RCT 2 ②'

The connection handle to use for the commissioning procedure on the primary ATP of RCT1 ①'

The encryption key to use for the commissioning procedure on the primary ATP of RCT 1 ①'

The connection handle to use for the commissioning procedure on the alternate ATP of RCT 1 ①'

The encryption key to use for the commissioning procedure on the alternate ATP of RCT 1 ①'. If the alternate ATP of the ARC is disabled, this field is not present.

Respectively copy the commissioning connection handle and key for every ATP of every RCT of this ARC.

5.7.5.2. Shared secret single commissioning

The shared secret single commissioning procedure is similar to the shared secret commissioning procedure. However, instead of configuring the list of RCTs to use for the ARC you can only provide a commissioning server. This commissioning server is responsible for providing the list of RCTs to use for alarm transmission.

RCT automatically configured during commissioning.

Protocol

▼
TS 50136-9

Commissioning type

▼
Shared secret single commissioning

Commissioning server host

Port

Shared connection handle

Shared secret key

- | | |
|------------------------------------|---|
| ① Commissioning server host | IP address or hostname of the commissioning server. |
| ② Port | Port of the commissioning server. |
| ③ Shared connection handle | The connection handle to use for the commissioning procedure on the commissioning server. |
| ④ Shared secret key | The encryption key to use for the commissioning procedure on the commissioning server. |

5.7.5.3. DTLS commissioning

The DTLS commissioning procedure is similar to the shared secret single commissioning procedure. However, instead of using a shared secret to identify the SPT, an X.509 certified is used.

RCT automatically configured during commissioning.

Protocol

▼ TS 50136-9

Commissioning type

▼ DTLS

Commissioning server host **Port**

Certificate

▼

CA

▼

- ① **Commissioning server host** IP address or hostname of the commissioning server.
- ② **Port** Port of the commissioning server.
- ③ **Certificate** The SDN-3030-SPT-DP-3G/4G certificate to use. (see section 5.4.2 for more information on how to add and use a certificate)
- ④ **CA** The CA of the RCT. (see section 5.4.2 for more information on how to add and use a certificate)

5.7.5.4. Once commissioning is done

Once the commissioning procedure is finished, new connection handle and encryption key are used to connect to every RCT. These secrets are saved internally and cannot be retrieved. Such an ARC is marked as commissioned in the ARC list.

✓ TS-50136-9 (commissioned)

When an ARC is commissioned, its connection parameters cannot be modified. If the commissioning must be restarted (e.g. when changing the RCTs list), the commissioning can be reset. This will erase the connection handle and encryption key used for the connection and therefore the SDN-3030-SPT-DP-3G/4G will not be able to communicate with the ARC until the commissioning is redone (i.e. commissioning information should also be reset on the RCT).

5.7.6. Inputs

Inputs panel (available in the menu Alarm transmission → Inputs) are virtual inputs (similar to physical inputs) giving you the state of an ARC. These inputs can be used in association with Events, Actions or Script.

ARC [Swissdotnet RCT] connected.	Activated ● ▼
Description ARC [Swissdotnet RCT] connected. Apply	
ARC [Swissdotnet RCT] alarm not transmitted.	Deactivated ● ^
Primary ATP [eth0] of ARC [Swissdotnet RCT] connected.	Activated ● ^
Alternate ATP [ppp3] of ARC [Swissdotnet RCT] connected.	Activated ● ^

5.7.7. Events

Events (available in the menu Alarm transmission → Events) are the alarms that the SDN-3030-SPT-DP-3G/4G should send to one or more ARCs. Once created, they need to be assigned to an ARC.

5.7.7.1. Event Summary

The Summary tab defines which input triggers the event and specifies some additional parameters :

New event

Summary
Configuration
Options

Description
 My Burglary Alarm

Priority
 ▼ Medium

Input module
 ▼ Inputs / outputs

Input type
 ▼ Standard

Input
 ▼ K1 - Effraction

Delay (ms)

☐ Watchdog

Next
Cancel

Description	Event description. You can provide a custom description for your needs.
Priority	Priority used to choose which event to send first when there are more than one waiting to be dispatched.

 **When compliance with EN 54-21:2006 Type 1EN_54-21 is required**
 , Fire alarms priority (and only fire alarms priority) must be set to High and fault alarms priority to Medium.

Input module	Specify from which software module does the event input comes from (use Inputs/Outputs for example if you want to use a physical input as trigger).
Input type	Specify which kind of input you want to use (Standard or Intruder).
Input	Select the corresponding input. If you provided a custom description on your inputs, it is displayed in the list.
Delay	How long (in milliseconds) the input has to change before triggering the event.
Watchdog	Check Watchdog to use the input as watchdog input. The event will be ACTIVATED only if the input does not change during the specified delay. This function is useful if you want to monitor a PLC. (Configured with a Rising Activating edge, the event will be triggered when the input stop oscillating)

-  Basically the idea to decide which priority to give an event is the following :
- **High** for when there are lives involved
 - **Medium** for when there is money involved
 - **Low** for the rest

5.7.7.2. Event Configuration

The configuration tab defines the alarm format :

New event

Summary
Configuration
Options

Event type

▼
Standard

Alarm data identifier

▼
SIA DC 03

Activating edge

▼

Alarm preset

▼
Code filter

▼
Code

▼
Zone

✓

Alarm

Restore preset

▼
Code filter

▼
Code

▼
Zone

✓

Restore

☐ Send restore even though previous state was unknown ⚠

On input read error

☒ Ignore

☐ Send alarm

☐ Send custom

Previous
Next

Apply
Cancel

Event type

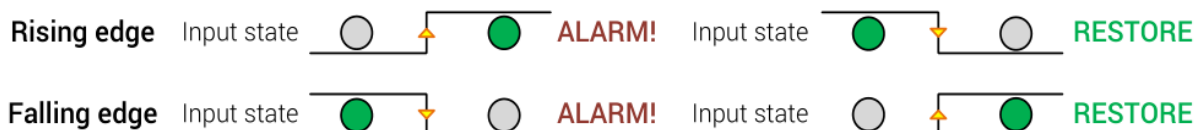
The created event can be a Standard event or a Forward event⁴. It can also be an Intruder event if the input used for this event is an Intruder input.

Alarm data identifier

Select the corresponding alarm format (SIA DC 03 or ADEMCO CONTACT ID).

Activating edge

Specify if the alarm is active on input rising edge or on input falling edge :



4. Forward event are to be used in conjunction with the IP Alarm module event inputs (section 5.8.2).

Alarm preset	The alarm preset allows you to quickly generate an alarm data code based on the format selected above. Once you selected the right parameters, click on ☒ to automatically generate the code.
Alarm	Alarm code in the specified format. This value can be edited manually or generated from the Alarm presets tool.
Restore preset	The restore preset allows you to quickly generate a restore data code based on the format selected above. Once you selected the right parameters, click on ☒ to automatically generate the code.
Restore	Restore code in the specified format. This value can be edited manually or generated from the Restore preset tool.
Send restore even though previous state was unknown	Allows for restore event to be sent even though the event's trigger's state was unknown (and not in alarm)
On input read error	Inputs state readings can sometimes fail, the On input read error parameters allows you to choose which action should be executed in such a case.

 The option **Send restore even though previous state was unknown** should only be used in very specific cases. When the alarm transmission module start (or restart) it considers every inputs of every modules to be in an unknown state. When this option is used, no matter the event's configured Activating edge, switch from unknown to restore of the event trigger's input state will generate a Restore event.

 Events using this option should not be associated with ARC seeking compliance with standards.

5.7.7.3. Event Options

Event Options tab allows you to add optional data into the transport protocol. This allows the ARC to receive detailed Information about the alarm. Fields whose label is followed by either (TS 50136-9) or DC-09) are protocol specific while the others are common.

 Following fields should not contain accent :

- Building name
- Location
- Room
- URL / verification
- Information / alarm text

New event

Summary

⚙ Configuration

🔧 Options

Building name

Main building



Location



Room



Url / verification

The stream URL is \${input-data}



Information / alarm text



IP address (TS 50136-9)



Port (TS 50136-9)



File (TS 50136-9)



MAC address (DC-09)



Validity

60



Add occurrence / time event field



Add position



Add site name

Previous

Apply

Cancel

Building name	Add a custom text to describe the building name
Location	Location of event on site
Room	Room of event
URL/verification	Add a custom URL to the event
Information / alarm text	Alarm text which may be a description of the event or a comment regarding the event
IP address (TS 50136-9)	Add a custom IP address to the event
Port (TS 50136-9)	Add a custom TCP/UDP port to the event
File	Add a custom filename to the event
MAC address (DC-09)	Add a custom MAC address to the event
Validity (in minutes)	Setup custom event validity in minutes (defaults to 60 minutes). Changes the event life duration after generation. This field allows reducing or increasing the event validity. Once the event is no longer valid and not sent to ARC, the event is dropped.
Add occurrence	Time the event occurred (may be different than message time stamp)
Add position	Add configured position from the location panel (see section 5.7.9)
Add site name	Add configured site name from the location panel (see section 5.7.9)

Green  buttons on the right of each field allow you to add internal information provided by the SDN-3030-SPT-DP-3G/4G about the input which triggered the event dispatch.

 Among those additional data, DC09 messages will only be enclosed as much of it as the general DC09 message size allows.

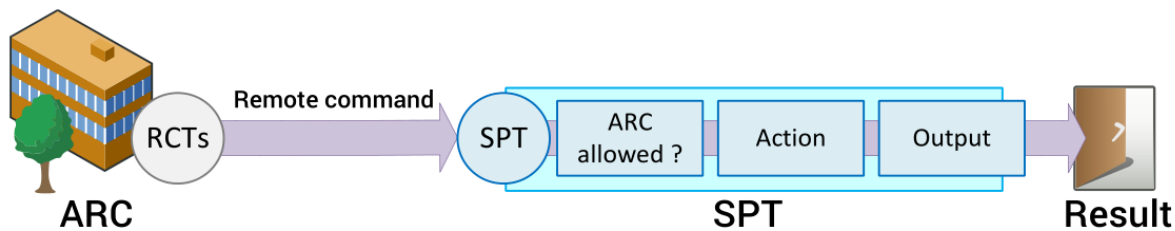
Your Event is now ready to be used. Click on the Apply button. If you finally want to apply the modified settings, you must still click on Save on the Event list. Do not forget to add it to the corresponding ARC as shown in the following example :

Swissdotnet RCT

Non assigned events	Assigned events
1 event(s) Filter → → → SPT fault	11 event(s) Filter ← ← ← AS failure Primary power supply failure Alternative power supply failure Primary ATP of ARC [ARC Test]

5.7.8. Remote commands

Remote commands (available in the menu Alarm transmission → Remote commands) are the remote commands that the SDN-3030-SPT-DP-3G/4G could receive from one or more ARCs. Once created, they should be assigned to an ARC and bounded to an Action or a Script. There is no limitation on the number of remote commands.



For more information about the Action module see section 5.13 and section 5.14 for more information about the Script module.

The factory settings do not contain any Remote command. You must create them manually by clicking on the **+** button.

Name

Activating data

Deactivating data

- Name**
Activating data
Deactivating data
- Remote command name. You can provide a custom name for your needs
Code to be transmitted from the ARC to activate the input associated to this remote command (usually provided by your ARC)
Code to be transmitted from the ARC to deactivate the input associated to this remote command

i If no deactivating data are provided, the remote command will act as a pulse upon reception of the activating data.

Your Remote command is now ready to be used. Click on the Apply button. If you finally want to apply the modified settings, you must still click on Save on the Remote Commands list. Do not forget to bound the remote command to an action and add it to the corresponding ARC as shown in the following example :

Swissdotnet RCT

Non assigned remote commands
No remote command

→ → →

Assigned remote commands
1 remote command(s)

← ← ←
Open front door

5.7.9. Location

You can define in the panel available on the menu Alarm transmission → Location some information about the SDN-3030-SPT-DP-3G/4G location.

Site name	
Dignity Health California Hospital Medical Center	
Latitude	Longitude
34.037871	-118.266138
Altitude	
15	
☐ Use GPS	

These data can be transmitted with the alarms to the ARC to improve the alarm enrichment.

The Use GPS option allows you to use GPS information (for target with GPS which is optional) to fill the Latitude, Longitude and Altitude fields.

5.7.10. DC09

This section contains specific settings for the ANSI/SIA DC-09-2007/2013 protocol.

Account number	This is the transmitter account number used to identify the SDN-3030-SPT-DP-3G/4G . This value is unique and cannot be modified. This number should be transmitted to the ARC before the commissioning.
Account prefix	The account prefix can be programmed into the SDN-3030-SPT-DP-3G/4G to extend the identification provided by the account number. The default value is 0.
Receiver number	In some cases, the SDN-3030-SPT-DP-3G/4G may be programmed to further extend the identification provided by the account number and account prefix by providing a receiver number. This element is optional and consist of 1-6-HEX ASCII digits.

5.8. IP Alarm

 **When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required** this module should not be used.

S   A   C  

The IP Alarm module allows you to use the SDN-3030 to receive DC09 messages making it possible to then forward them to an ARC of your choice.

 This module can be very convenient to extend the number of criteria used to send alarm. With it, we are no longer limited to number of physical inputs the SDN-3030-SPT-DP-3G/4G hardware offers.

5.8.1. Endpoints

The SDN-3030 can accept messages from multiple sources which we will call here endpoints. To add an endpoint just click the **+** and fill the required information.

New IP alarm endpoint

Account

Key

Port

Account prefix

Receiver number

Max polling frequency (s)

Account	This is the account number of the source you are configuring.
Key	This is the encryption key used by the source you are configuring.
Port	This is the port (TCP or UDP) to which the source you are configuring send its messages.
Account prefix	This is the prefix the source you are configuring is using to extend the identification provided by the account number. The default value is 0.
Receiver number	In some cases, sources may be programmed to use a receiver number in order to further extend the identification provided by the account number and account prefix, if this is the case then you need to fill it here.
Max polling frequency	If the SDN-3030 does not receive any messages from the configured endpoint within this time lapse the endpoint will be considered disconnected.

i What is called here a source is in practical most of a time an SPT but it could be any device sending valid DC09 messages.

5.8.2. Inputs

When an endpoint is added two inputs are automatically created.

endpoint connected ACCOUNT NUMBER

This input is ACTIVATED when the SDN-3030 receives messages from the endpoint before Max polling frequency duration is reached. It is in ERROR when the SDN-3030 receives an invalid message from the configured endpoint (the cause of the error can be seen by hovering the mouse over the input state).

event ACCOUNT NUMBER

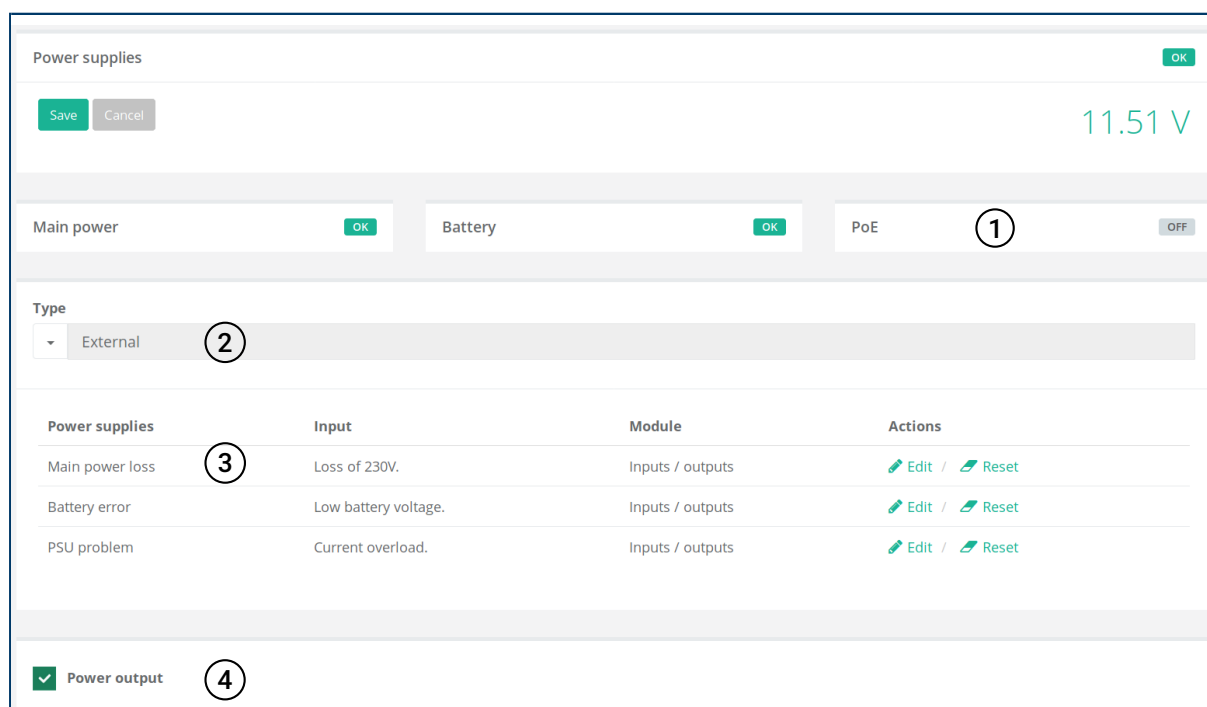
This input switch from DEACTIVATED to ACTIVATED and then back to DEACTIVATED when the SDN-3030 receives an event from the endpoint configured. This input will embeds in its data the event information⁵.

5.9. Hardware



5.9.1. Power Management

Power management panel (Hardware → Power Management) allows you to configure how your device is powered. This page is also used to view the current measured values.



The screenshot shows the 'Power supplies' configuration page. At the top, there are 'Save' and 'Cancel' buttons, and a voltage display showing '11.51 V'. Below this, there are three toggle switches: 'Main power' (ON), 'Battery' (ON), and 'PoE' (OFF, labeled with a circled 1). Under the 'Type' section, a dropdown menu is set to 'External' (labeled with a circled 2). Below this is a table with the following data:

Power supplies	Input	Module	Actions
Main power loss (labeled with a circled 3)	Loss of 230V.	Inputs / outputs	Edit / Reset
Battery error	Low battery voltage.	Inputs / outputs	Edit / Reset
PSU problem	Current overload.	Inputs / outputs	Edit / Reset

At the bottom, there is a 'Power output' checkbox (labeled with a circled 4) which is currently checked.

- ① The PoE panel show you if your device is powered by PoE (Power over Ethernet). PoE is a hardware option and is not available on all SDN-3030-SPT-DP-3G/4G
- ② The type of power supply your SDN-3030-SPT-DP-3G/4G is using. It can either be Onboard or External.
- ③ When using an external power supply, you need to tell the SDN-3030-SPT-DP-3G/4G which of its inputs are linked to the power supply outputs indicating troubles.
- ④ If you want to use the 12VDC 500mA output (on J3 connector) check the Power output box.

Power output (4) should not be used in certified installation

5. Only the event alarm code is forwarded

The global power supply state (top right corner) is compute from the state of the three other inputs (Main power loss, Battery error and PSU problem) provided they are properly configured. If one input is not set it is simply not taken into account to compute the global state. If no input is configured, then the global state is set to ERROR.

i If the SDN-3030-SPT-DP-3G/4G is configured to use an external power supply and the Main power loss and Battery error are properly configured then an error with the battery will be signaled in the interface header (see section 5.2) by a warning  icon.

When using the Onboard power supply, the only thing you have to configure is whether or not your device has a battery plugged in. By checking the Battery available you tell the SPT to use the battery input state for the Battery error state and so, to use it to compute the global state as well.

5.9.2. Serial Interfaces

Several modules could use the serial port. To simplify the configuration, basic serial port settings are grouped in this section (Hardware → Serial interfaces).

Name	Protocol	Module using interface	Actions
ESPA Alarm system 9600 8N1	RS_232	Serial alarms	 Edit

i The "Module using interface" field allows you to know if there is already a module using the serial port (and if so, which one).

Click on the Edit button to change the settings of the corresponding port.

Wago UPS

Name	Wago UPS
Description	UPS Wago
Path	/dev/ttyS2
Bitrate	▼ B_9600
Char size	▼ ASCII_8
Parity	▼ NONE
Stopbit	▼ STOP_1
Hardware control	▼ NO_CONTROL

Name	Serial port name. You can provide a custom name for your needs.
Description	Serial port description. You can provide a custom description for your needs.
Path	Physical device path on the device (read only).
Protocol	Select RS-232 or RS-485 according to your needs.
Bitrate	Serial line bitrate according to your needs.
Char size	Select the serial char size according to your needs. Supported values are : 5, 6, 7 or 8 bit ASCII. Most of modern system are using 8 bits ASCII format as char size.
Parity	Select the serial parity according to your needs. Supported values are : none, even or odd.
Stop bit	Select the number of stop bit(s) according to your needs. Supported values are : 1 or 2.
Hardware control	Select hardware flow control according to your needs. Supported values are : NO_CONTROL or XON_XOFF.
Duplex mode	Select half duplex or full duplex mode according to your needs (only applicable to RS-485 mode). Wiring is described in section 2.7.4.
Termination	Enable line termination resistor (only applicable to RS-485 mode).

Once you have set your settings, click on the Apply button. If you finally want to apply the modified settings, you must still click on Save button on the Serial Interfaces list.

 It is very important to remember that one serial port must only be used once. Using it simultaneously for different purposes (e.g. a Modbus slave and an ESPA Device) will result in an undefined behavior.

5.9.3. Date and Time

The Date and Time configuration page (Hardware → Date and Time) allows you to configure the clock of the SDN-3030-SPT-DP-3G/4G and its timezone.

 It is very important to always configure properly the time and the date on the device, especially for alarm transmission.

First of all, select the appropriate area in the Time zone list. Based on your location, the device will automatically take the summer time into consideration.

Date and time

Transmitter current time

Date
Time

01/07/201817:16:39

Set time

ApplySaveCancel

Time zone

Europe/Zurich

☐ Synchronize with computer time ①

Date
Time

01/07/201817:16:39

☒ Synchronize with NTP server ②

Url
Port

ch.pool.ntp.org123

Refresh time (min)

60

☐ Set manually ③

Date
Time

01/07/201817:16:11

There are three ways to configure the time on the device :

- ① **Synchronize with computer time**
- ② **Synchronize with NTP server**

Check this option to use your computer time as reference.

Use an NTP server to automatically set the time on the device. You can use either an IP address or a hostname. The refresh time defines the time update frequency.

🔊 If you use a domain name as NTP server, please make sure that the DNS resolution is correctly configured in the network parameters.

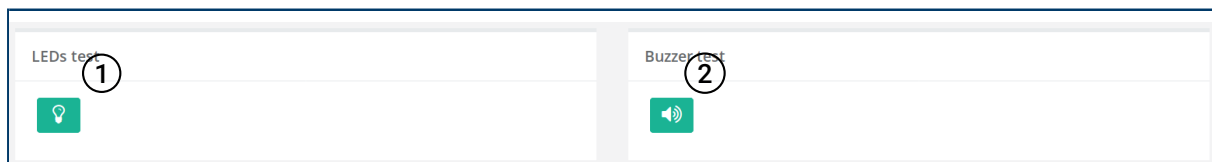
- ③ **Set manually**

Allows you to manually set the time and date.

Click on the Save button to apply the settings. The hardware module will be restarted to apply the changes.

5.9.4. LEDs and Buzzer

LEDs and Buzzer (Hardware → LEDs and Buzzer) configuration page is available to test the proper operation of LEDs and buzzer.

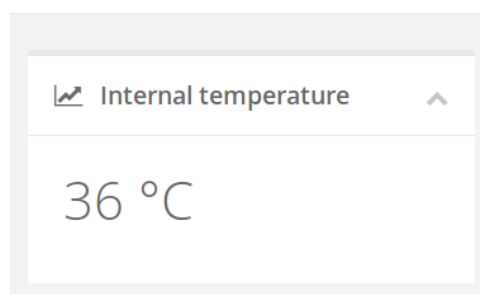


- ① If you click on the 💡 LEDs test button, all software controlled LEDs should blink during five seconds.
- ② If you click on the 🔊 Buzzer test button, the buzzer will ring.

5.9.5. Temperature

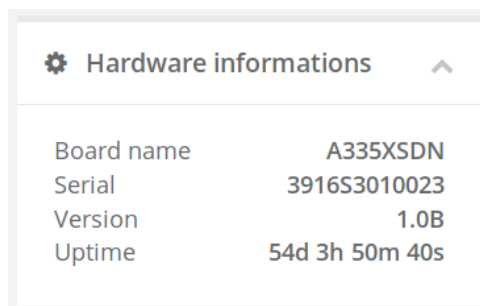
Temperature panel (Hardware → Temperature) allows you to view the current device temperature.

Temperature



5.9.6. Information

The Hardware information panel (Hardware → Informations) allows you to view the hardware identification, the serial number, the hardware version and the SDN-3030-SPT-DP-3G/4G uptime.



5.10. Modbus

 **When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required** this module should not be used.

S   A   C  

Modbus is a serial and IP communication protocol originally published by Modicon (now Schneider Electric) in 1979 to be used with its programmable logic controllers (PLCs). Simple and robust, it has since become a de facto standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices.

With the SDN-3030 you can create several TCP or RTU (RS-232/485 serial) slaves. A slave is a remote device providing inputs and/or outputs. This allows you to create virtual inputs and outputs on your device which are physically deported. These inputs or outputs can be used in combination with the other modules like Notifications, Alarm transmission, Actions, etc.

Name	State	Description	Address	Refresh frequency (ms)	Actions
WAGO PLC 5	 Connected	Heater PLC	1	5000	 Edit /  Delete

5.10.1. Slaves

Slaves configuration is available in Modbus → Slaves panel.

 The State information gives you a feedback if the communication is working properly. But you need at least one input to have a valid state.

Click on the  to add a new TCP or RTU Modbus slave.

5.10.1.1. Common Slave configuration

Name
WAGO PLC 5
Description
Heater PLC
Refresh frequency (ms)
5000
Response timeout (ms)
1000
Address
Number of read failure before being deactivated
5
☒ Discard input error state
Task handling frequency (ms)
1000
Type
▼

Name	Modbus slave name. You can provide a custom name for your needs.
Description	Modbus slave description. You can provide a custom description for your needs.
Refresh frequency	Read frequency in milliseconds on the slave. Every input will be refreshed at this rate. (default value is 5000ms)
Response timeout	Timeout delay in milliseconds for the connection. (default value is 1000ms)
Address	Modbus slave address (1-255)
Number of read failure before being deactivated	To help avoid any oscillation in the Modbus slave state due to some minor network errors, it is possible to configure the number of input reading errors allowed before switching the Modbus slave to DEACTIVATED (default value is 5).
Discard input error state	Checking this box states that in case the SDN-3030 is not able to read an input state then it does not change it (instead of switching it to ERROR) (this option is checked by default)
Task handling	Modbus inputs states are refreshed through Reading Tasks while outputs states are set through Writing Tasks. Both types of Task are put in the same queue from which they are handled at the frequency defined by this parameter. Reading Tasks are added in the queue at the frequency defined by the Refresh frequency parameter chosen above while Writing Tasks are added as soon as requested. (default value is 1000ms)
Type	Select TCP for Modbus TCP slave.

i Modbus slave parameters must respect the following constraints :

- Refresh frequency > Response timeout
- Response timeout > Task handling frequency

5.10.1.1.1. TCP Slave configuration

Type

▼

TCP

IP

10.110.50.20

Port

56842

IP	Modbus slave IP address.
Port	TCP port to use (default value is usually 502 on most devices)

5.10.1.1.2. RTU Slave configuration

Type

▼

RTU

Serial port path

▼

Wago UPS(UPS Wago)

Serial port Select the serial port where the Modbus slave is connected.

i The serial port must be configured in the Hardware module (Hardware → Serial Interfaces). See section 5.9.2 for more information.

5.10.2. Inputs

All Modbus (TCP and RTU) inputs are listed in the Modbus → Serial Inputs panel :

Description	State	Address	Access type	Slave	Value	Actions
Air conditioner	● Activated	0	Read Coil (FC1)	PLC Server room	1	Edit / Duplicate / Delete
Temperature level too high	● Deactivated	1	Read Coil (FC1)	PLC Server room	0	Edit / Duplicate / Delete
Backup power supply available	● Activated	2	Read Coil (FC1)	PLC Server room	1	Edit / Duplicate / Delete
Defect server(s)	● Deactivated	4	Read Holding Registers (FC3)	PLC Server room	0	Edit / Duplicate / Delete

i The state and value information gives you a feedback on the current inputs state.

There are two kinds of Modbus inputs.

Coil (FC1) and discrete input (FC2)

Those inputs can only hold a 1 or 0.

Holding register (FC3) and Input register FC4)

Those inputs can hold any value.

Click on the **+** button to add a new Modbus input.

Description

Type

▼ Standard

Address

Access type

▼ Read Coil (FC1)

All Modbus inputs have some common information they require to be created.

Description You can provide a custom description for your needs.

Type Input type.

Address Modbus address.

Access type Modbus access type.

5.10.2.1. Coil (FC1) and discret input (FC2)

If the input your are creating is of type FC1 or FC2, then you will only have to fill the following :



Slave

PLC Server room

☐ Logic inverted

Slave

Select the previously created Modbus slave where the input comes from.

Logic inverted

This check box allows the SDN-3030 to pretend the input state is inverted (e.g considered ACTIVATED when it reads a 0).

5.10.2.2. Holding register (FC3) and input register (FC4)

If the input you are creating is of type FC3 or FC4 then you will have to configure the SDN-3030 so that it is able to properly interpret the read value.

Value type

ABCD Float

Activated range min

-5.0

☐ Min included

Activated range max

50

☐ Max included

Slave

PLC Server room

☐ Logic inverted

Value type

The type of value the SDN-3030 can expect to find at the address indicated.

Activated range min

The minimum value for which the input you are creating will be considered ACTIVATED.

Min included

This check box allows you to precise whether or not the minimum value configured is part of the ACTIVATED range.

Activated range max

The maximum value for which the input you are creating will be considered ACTIVATED.

Max included

This check box allows you to precise whether or not the maximum value configured is part of the Activated range.

Logic inverted

This check box allows the SDN-3030 to pretend the input state is inverted (i.e if the value read is within the given range the input will be considered DEACTIVATED).

i The SDN-3030 offers the following value type :

- ABCD Float
- DCBA Float
- ABCD signed integer
- DCBA signed integer
- AB unsigned integer
- BA unsigned integer
- ABCD unsigned integer
- DCBA unsigned integer

The Modbus slave datasheet should provides the information needed for your to select the proper value type.

5.10.3. Outputs

All Modbus (TCP and RTU) outputs are listed in the Modbus → Outputs panel :

Description	Address	Access type	Slave	Actions
Server room access allowed	2	Write Coils (FC15)	PLC Server room	 Edit /  Duplicate /  Delete
Rack 1 power supply	4	Write Coils (FC15)	PLC Server room	 Edit /  Duplicate /  Delete
Rack 2 power supply	5	Write Coils (FC15)	PLC Server room	 Edit /  Duplicate /  Delete
Air conditionner backup	7	Write Coils (FC15)	PLC Server room	 Edit /  Duplicate /  Delete

Click on the **+** button to add a new Modbus output.

Description

Address

Access type

 Write Coils (FC15)

Slave

 PLC Server room

Description	Output description. You can provide a custom description for your needs.
Address	Modbus register/coil address.
Access type	Modbus access data type. Supported values are : Write coils (FC15), Write Registers (FC16).
Slave	Select the previously created Modbus slave where the output come from.

5.11. IOT

 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required this module should not be used.

S   A   C  

"The **Internet of things (IoT)** is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators and connectivity which enables these things to connect, collect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions."⁶

5.11.1. Clients

The Clients panel (available from the menu IoT → Clients) allows you to visualize and edit/remove already configured Internet of Things (IoT) client and add new one.

Modify IoT clients





Search

Description	State	Type	Actions
SDN Broker client	 Connected	MQTT	 Edit /  Delete

Description IoT client description. You can provide a custom description for your needs.
State Give you a feedback on the state of this IoT client.
Type Type of the IoT client.

 Currently the SDN-3030 only support MQTT client type :

"MQTT is a machine-to-machine (M2M)/ "Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium."^a

a. <https://mqtt.org/>

To create a new IoT client you simply have to click the  and fill the required information.

6. https://en.wikipedia.org/wiki/Internet_of_things

SDN Broker client

 Configuration

 Advanced

Description

Type

 MQTT

Quality of service

 QoS1 (at least once)

Server certificate

 MQTT SDN Broker certificate

Client certificate



User

Password

☒ Allow system management

☒ SSL

☒ Enable

Endpoint 1





Description	IoT client description. You can provide a custom description for your needs.
Type	IoT client type. Currently only MQTT is available.
Quality of service	QoS used for subscribing and publishing — QOS_0 : The client will try to send the message — QOS_1 : The client will send the message at least once — QOS_2 : The client will send the message exactly once
Server certificate	The certificate of the broker you want to connect to (optional).
Client certificate	The certificate of your SDN-3030 (optional).
Allow system management	Allow system management to be handle through IoT.
SSL	Enable SSL usage.
Enable	Enable the IoT client.
Endpoint	Endpoint you want to connect to, you can add multiple endpoints.

i For more information regarding certificates (and TLS key) see section 5.4.2

Modules white list

Non assigned modules

1 module(s)

Filter

→ → →

Network

Assigned modules

15 module(s)

Filter

← ← ←

Authentication
Input/Output
Web-server
Hardware
Alarm transmission
Action
Modbus
Vpn
Notification
Video
Serial Alarm
Script
Active Tag
IoT
IP Alarm

Modules white list The IoT module can publish some information coming from other modules. To allow this you need to add the desired modules in the white list.

 Choosing an higher QoS means dealing with slower connection establishment and less light-weight messages. It is advised to run some tests before choosing an higher QoS to ensure it meets your needs.

MQTT clients have some advanced parameters which can be configured too.

SDN Broker client

⚙️ Configuration
⚙️ Advanced

Keep alive (s)

Connection timeout (s)

Minimum retry interval ?

Maximum retry interval ?

Apply
Cancel

Keep alive (s)

The polling interval used by the client to ensure it is still connected to a broker

Connection timeout (s)

The maximum duration the client will wait for an answer after sending a polling message, after which if no answer is received the client will be stated as deactivated

Minimum retry interval (s)

The minimum duration the client will wait before retrying to connect to the broker

Maximum retry interval (s)

The maximum duration the client will wait before retrying to connect to the broker

i When disconnected, the client try to reconnect to the broker on its own. As soon as it is stated as disconnected, it waits Minimum retry interval before trying to reconnect. If it fails, it then waits twice as long before retrying again. This doubling stops once the Maximum retry interval duration is reached.

i A client can not be deleted if some inputs/outputs are using it. It means if you want to delete a client, you first need to either delete the inputs/outputs using it or modify their configuration to use another client.

i When a client connects on a broker it provides it with its last will ("Unexpected error.") which will be sent (to every subscriber) upon any unexpected disconnection of the client.

🔊 Every messages the client is requested to send while disconnected will be discarded.

5.11.2. Inputs

The IoT inputs list give you a quick overview of the configured IoT inputs.

Modify IoT inputs					
+ Save Cancel		Search			
Description	State	Client	Activating data	Deactivating data	Actions
 Video stream (ref:A123) trigger	Unknown	SDN Broker client	activate	deactivate	Edit / Duplicate / Delete

Description	The description of the input. Hovering over the  icon will display the topic used by the input.
State	The state of the input (UNKNOWN if neither Activating data nor Deactivating data has been posted on the input topic since the IoT client is connected to the Broker)
Client	The IoT client this input is using
Activating data	The expected data for this input to switch its state to ACTIVATED
Deactivating data	The expected data for this input to switch its state to DEACTIVATED

To add a new input just click the **+** button and fill the required information.

Video stream (ref:A123) trigger

Description

Client

Activating data

Deactivating data

Topic

[Apply](#) [Cancel](#)

Description	The description of the input. You can provide a custom description for your needs.
Client	The client which will subscribe on the topic to manage this input.
Activating data	The data which will trigger the activation of this input.
Deactivating data	The data which will trigger the deactivation of this input.
Topic	The topic on which the client subscribe to monitor if any activating/deactivating data are received.

 The topic is case sensitive. It means buildingx/floory/roomz/video/stream1 will be different than buildingX/floorY/roomZ/video/stream1.

i Activating and deactivating data are case sensitive. It means an input with ACTIVATE as activating data will not be activated upon reception of activate.

5.11.3. Outputs

The IoT outputs list give you a quick overview of the configured IoT outputs.

Modify IoT outputs					
+ Save Cancel		Search			
Description	Client	Activating data	Deactivating data	Actions	
i Building Y entrance fence state ☒ Activate / ☐ Deactivate	SDN Broker client	open	close	Edit / Duplicate / Delete	
i Output camera 2 (floor X room Z) state ☒ Activate / ☐ Deactivate	SDN Broker client	on	off	Edit / Duplicate / Delete	

Description	The description of the output. Hovering over the i icon will display the topic used by the output.
Activate / Deactivate	Click one or the other to send the Activating data or Deactivating data on the output topic
State	The state of the output (UNKNOWN if neither Activating data nor Deactivating data has been posted on the output topic since the IoT client is connected to the Broker)
Client	The IoT client this output is using
Activating data	The data which will be sent when this output is ACTIVATED
Deactivating data	The data which will be sent when this output is DEACTIVATED

To add a new output just click the **+** button and fill the required information.

Building Y entrance fence state

Description

Client
 SDN Broker client

Activating data

Deactivating data

Topic

☐ **Retained data**

Description	The description of the output. You can provide a custom description for your needs.
Client	The client which will be used to publish the output Activating data and Deactivating data.
Activating data	The data which will be sent when this output is ACTIVATED
Deactivating data	The data which will be sent when this output is DEACTIVATED
Topic	The topic on which the client will publish the output Activating data and Deactivating data.
Retained data	When checked this flag instructs the broker to memorize this data so that any client subscribing on the same topic will receive the last value posted on it.

5.12. Notifications

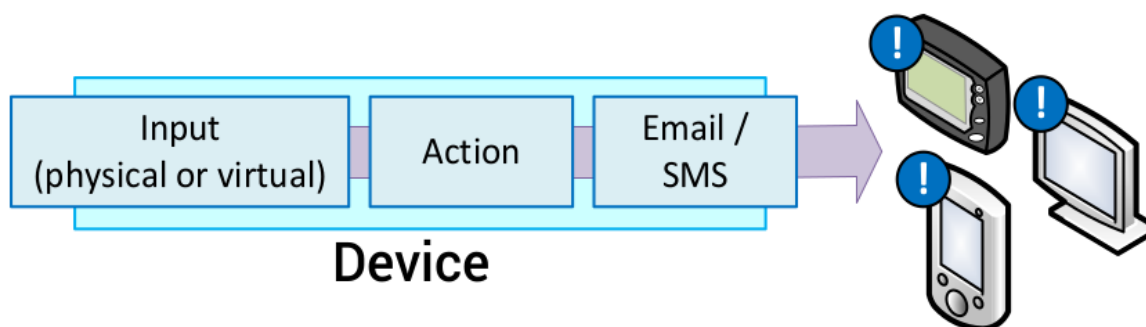
S   A   C  

The Notifications module allows you to send Email and SMS directly from the device :

- SMS (using the WWAN adapter) This option is only available on the dual path version of the SDN-3030-SPT-DP-3G/4G
- Email (using SMTP protocol)

i Before sending SMS with the internal modem, SMS enable check box option must be activated on the PPP interface in the Network → Interfaces configuration and an SCA number need to be provided as well.

The notifications are sent by the Actions or the Script module. For more information about actions, please read section 5.13, for more information about scripts, read section 5.14.



It is also possible to deactivate SMS and Email through the Actions or Scripts modules, this can be especially useful to test an installation without sending notifications to third party not aware you are running tests.

5.12.1. SMS / Emails templates

SMS / mails panel (available in the menu Notifications → SMS / mails) allows you to create Email or SMS templates.

Description	Type	Actions
My sms	 SMS	 Edit /  Duplicate /  Delete /  Test
My Email Example	 Mail	 Edit /  Duplicate /  Delete /  Test

For all templates, you can use the  Test button to send a test message. The other actions are similar to those of the other configuration panels.

 A  warning icon can be displayed next to notifications. It is to catch your attention on the fact those notifications have no recipient configured.

5.12.1.1. Email

Before creating a new Email template, you must first create a Mail Server (see section 5.12.2).

Once you are on the SMS / mail panel, click on the  button to create a new entry.

Description

My Email

1

Type

▼

Mail

2

Mail server

▼

My primary email server

3

💡 Activation

↩ Restore

4

5

Subject

Notification from your SDN-3030 device

6

Message

Available in [input info](#)

🔍

B I U

open sans ▼

13 ▼

A ▼

☰ ☰ ☰

☐ ▼

🔗 - </>

↶ ↷

Dear user,

8

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Best regards

Your support team !

Recipient 1

john.doe@email.com

9

-

+

Specific parameters to  Mail templates :

- ① **Description** Notification template description. You can provide a custom description for your needs.
- ② **Type** Select Mail to create an email template.
- ③ **Mail server** Select the previously created mail server which you want to use to send the message.
- ④ **Activation** Message subject ⑥ and message content ⑧ when the notification is ACTIVATED.
- ⑤ **Restore** Message subject ⑥ and message content ⑧ when the notification is DEACTIVATED.
- ⑦ **Available input info** Allows to insert internal information provided by the SDN-3030-SPT-DP-3G/4G about the input which triggered the email dispatch.
- ⑨ **Recipient** Add one or more email recipients.

5.12.1.2. SMS

The  SMS templates are configured the same way :

Description

Type

SMS

Activation

Restore

Message

Available input info

This is an alert message !
Additionalnnaal info :\${input-description}

Recipient 1

+

Specific parameters to  SMS templates :

- ① **Description** Notification template description. You can provide a custom description for your needs.
- ② **Type** Select SMS to create an SMS template.
- ③ **Activation** Message content ⑥ sent when the notification is ACTIVATED.
- ④ **Restore** Message content ⑥ sent when the notification is DEACTIVATED.
- ⑤ **Available input info** Allows to insert internal information provided by the SDN-3030-SPT-DP-3G/4G about the input which triggered the SMS dispatch.
- ⑦ **Recipient** Add one or more SMS recipients.

i It should be noted some provider use flood filters, preventing multiple identical messages to be sent in a short amount of time. To avoid your SMSs being bloked, add a variable part to their content.

5.12.2. Mail servers

The device can handle several mail servers at the same time. This allows you to choose for selected notifications, what SMTP service you need. With this feature, you can send SMS or Paging messages with a dedicated SMTP server in addition to normal email.

Mail servers panel (available in the menu Notifications → Mail servers) is used to manage your SMTP servers. Click on the **+** button to create a new entry.

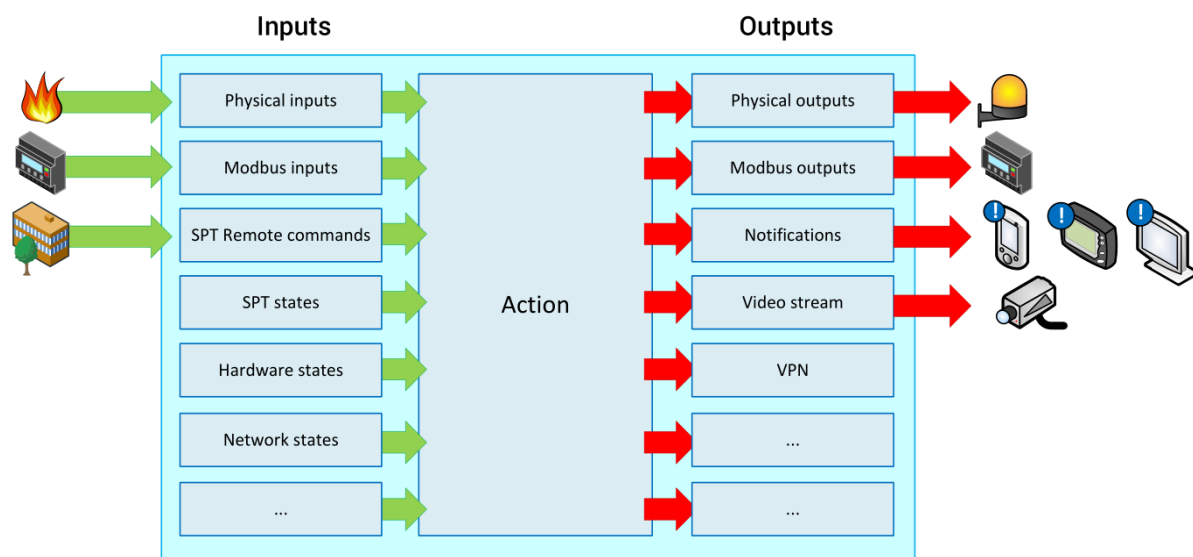
Description	
My primary email server	①
Url	Port
www.longfakeurl.ch	587
	② ③
Sender address	
fakeuser@fakeadress.ch	④
User	
fakeuserwhomaddr adfu	⑤
Password	
.....	⑥
☐ SSL ⑦	

- | | |
|---|--|
| <p>① Description</p> <p>② Url</p> <p>③ Port</p> <p>④ Sender address</p> <p>⑤ User</p> <p>⑥ Password</p> <p>⑦ SSL</p> | <p>SMTP server description. You can provide a custom description for your needs.</p> <p>SMTP server address. Contact your provider to get the correct parameters.</p> <p>SMTP server port. Contact your provider to get the correct parameters.</p> <p>Email address of the email sender.</p> <p>Your SMTP username, leave it blank if you do not need it.</p> <p>Your SMTP password, leave it blank if you do not need it.</p> <p>Check this box to enable SSL connection with the SMTP server.</p> |
|---|--|

5.13. Actions

S   A   C  

The Actions module is an important element. It allows you to link inputs (internal, external or virtual) with outputs. This allows you to customize the device behavior in various situations. For example, you can send email or a SMS if an input changes. The next section describes the available inputs and outputs for each module.



The actions are configured in the menu Actions (Actions → Actions). As for the other modules, you can  Edit,  Duplicate or  Delete items on the list. Click on the  button to create a new action.

While editing or creating an action, you need to configure two items, the trigger (the input who activate the action) and the action itself.

! Trigger
⚡ Action

Description
Relay output on power failure

Input module
Hardware

Input type
Standard

Input
Main power Source OK.

Delay (ms)
5000

☐ Watchdog

Trigger state
Deactivated

☒ Action enabled

Description	Action description. You can provide a custom description for your needs.
Input module	Select the module where the necessary input comes from.
Input type	Select the corresponding input type (Standard or Intruder).
Input	Select the input used as trigger.
Delay	How long (in milliseconds) the input has to change before executing the action. This is useful when you want to temporize the action or if you want to avoid bounces.
Watchdog	Check Watchdog to use the input as watchdog input. The event will be activated only if the input does not change during the specified delay.
Trigger state	Select the input state for which you want to activate the action.
Action enabled	Allows to enable or disable an action (enabled by default).

The second Action tab let you configure the action you want to execute :

! Trigger
⚡ Action

Output module

Output

Action state

Duration (ms)

☒ **Restore action**

Restore action state

Restore action duration (ms)

Output module	Select the module on which you want to execute the action.
Output	Select the output used for the action.
Action state	Select on which state you want to set the selected output when the action is executed.
Duration	Enter an optional duration in milliseconds in the case you only want to set the output for a defined time (pulse) when the action is activated.
Restore action	Check Restore action if you want to change the state of the output when the input state who triggered the action is restored.
Restore action state	Select on which state you want to put the selected output when the action is restored.
Restore action duration	Enter an optional duration in milliseconds in the case you want only to set the output for a defined time (pulse) when the action is restored.

i When an Output module is restarted (e.g when its configuration is saved), the Action module check the last order it sent each of this module Outputs (used as a trigger of an Action) and send it back. It means if you have an Action configured to send an email given a specific trigger and the email has been sent, upon restart the Action module will sent back the order to send the email. If you need to create an Action-like behavior without the retry upon restart mechanism please use a Script instead.

5.13.1. Available inputs

Module - Alarm transmission (SPT)		
Name	Type	Description
Event acknowledge	Standard	This input does a pulse (1 second) every time that an alarm has been successfully sent to an ARC. Use it to acknowledge the alarm transmission to the AS. (typically used with internal outputs)
Negative event acknowledge	Standard	This input is ACTIVATED when an RCT refuses an event from the SPT.
ATS failure	Standard	This input is ACTIVATED on ATS failure. This occurs when an ARC is disconnected from the SPT. (typically used to send an alarm to the AS)
SPT fault	Standard	This input is ACTIVATED if any ATP is disconnected or if the SPT global power state is in ERROR (Hardware Input Power fault ACTIVATED).
ARC [name] connected	Standard	This input is ACTIVATED if the communication is established with the ARC. There is one input per configured ARC.
ARC [name] alarm not transmitted	Standard	This input is ACTIVATED when an alarm is in pending state.
Primary ATP connected	Standard	This input is ACTIVATED if the SPT is connected with the primary network interface on a RCT of an ARC. There is one input per configured RCT and ARC.
Secondary ATP connected	Standard	This input is ACTIVATED if the SPT is connected with the secondary network interface on a RCT of an ARC. There is one input per configured RCT and ARC.

Module - Authentication		
Name	Type	Description
Maintenance mode	Standard	This input is ACTIVATED if the SPT is in maintenance mode. (typically used to send a maintenance alarm to the ARC or a message to the customer)

Module - IP alarm		
Name	Type	Description
endpoint connected [ENDPOINT ACCOUNT NUM]	Standard	This input is ACTIVATED as long as the SDN-3030 has received a valid message from the configured ENDPOINT within the Max polling frequency interval configured (refer to section 5.8.2)
event [ENDPOINT ACCOUNT NUM]	Standard	This input is switched from DEACTIVATED to ACTIVATED then back to DEACTIVATED when the SDN-3030 receives a message from the configured device (refer to section 5.8.2).

Module - Hardware		
Name	Type	Description
Power fault	Standard	This input is ACTIVATED if any configured power input is in ERROR state.
Main power source OK	Standard	This input is ACTIVATED as long as the main power supply state is OK.
Standby power Source OK	Standard	This input is ACTIVATED as long as the battery state is OK (delivered voltage is greater than 11.5V).
Power supply problem	Standard	This input is ACTIVATED when the power supply is experiencing a current overload (current consumption exceeding 4A)
VIN1 OK	Standard	This input is ACTIVATED if power is supplied on the VIN1 connector. (provided when the SDN-3030 uses the internal power supply).
VIN2 OK	Standard	This input is ACTIVATED if power is supplied on the VIN2 connector. (provided when the SDN-3030 uses the internal power supply).
VCC Voltage is OK	Standard	This input is ACTIVATED if the device is correctly supplied. (provided when the SDN-3030 uses the internal power supply).
UBAT	Standard	This input is ACTIVATED if the voltage of the battery is correct. (provided when the SDN-3030 uses the internal power supply).
PoE is available	Standard	This input is ACTIVATED if power is supplied by PoE (only on compatible devices).

Module - Inputs / outputs		
Name	Type	Description
[input name]	Standard	Internal input on the device. The displayed name corresponds to the configured description.
[input name]	Intruder	Internal intruder input on the device. The displayed name corresponds to the configured description.

Module - Network		
Name	Type	Description
Input interface [INTERFACE NAME]	Standard	To understand the behavior of this input state, see section 5.6.1
Signal PPP [ppp3]	Standard	This input is ACTIVATED as long as the PPP signal is stronger than the Min signal quality value configured (refer to section 5.6.1).
PIN code invalid [ppp3]	Standard	This input is ACTIVATED when the configured PIN code is invalid.
PUK code invalid [ppp3]	Standard	This input is ACTIVATED when the configured PUK code is invalid.

Module - Modbus		
Name	Type	Description
Slave [name] connected	Standard	This input is ACTIVATED if the communication is established with the Modbus slave. There is one input per configured slave.
[input name]	Standard	Modbus input from slave, configured on the device. The displayed name corresponds to the configured description.

Module - Internet of Things (IoT)		
Name	Type	Description
[input description]	Standard	This input is ACTIVATED (respectively DEACTIVATED) when its client receives a message on the configured Topic containing the configured Activating data (respectively Deactivating data).

Module - Serial Alarm		
Name	Type	Description
Serial device connection input	Standard	This input is ACTIVATED when the device is connected.
[input name]	Standard	To understand the behavior of this input state, see section 5.18.2.2 and section 5.18.3.1. The displayed name corresponds to the configured description.

Module - VPN		
Name	Type	Description
[vpn name]	Standard	To understand the behavior of this input state, see section 5.15.1. The displayed name corresponds to the configured description.

Module - Scripts		
Name	Type	Description
[script name]	Standard	Script input whose state is computed from the internal logic it has been assigned. The displayed name corresponds to the configured description.

Module - Video Stream		
Name	Type	Description
[v. stream name]	Standard	Stream connection state (ACTIVATED = Stream connected) The displayed name corresponds to the configured description.

Module - Active tags		
Name	Type	Description
[Controller name - Tag online]	Standard	This input is ACTIVATED when the activetag controller is currently detecting at least one tag.
[Controller name - Tag in alarm]	Standard	This input is ACTIVATED when the activetag controller is currently detecting at least one tag broadcasting alarm information (e.g battery low).
[Group name - Tag online]	Standard	This input is ACTIVATED when there is at least one of the tags belonging to this group which is currently detected by the activetag controller.
[Group name - Tag in]	Standard	This input acts as a pulse (ACTIVATED - DEACTIVATED) when the activetag controller detects a tag belonging to this group.
[Group name - Tag out]	Standard	This input acts as a pulse (ACTIVATED - DEACTIVATED) when one of the tags belonging to this group (and which was previously detected) disappeared. A group tag is considered as having disappeared when it stopped being detected by the controller for more than Time before tag disappearance (s) (duration set in the group configuration) or when its signal strength has been less than Max reception level (dbm) (value set in the group configuration) for more than Time before tag disappearance (s).
[Group name - Tag in alarm]	Standard	This input is ACTIVATED when at least one of the tags belonging to this group (and currently detected by the activetag controller) is broadcasting alarm information (e.g battery low).
[Group name - Button pressed]	Standard	The state of this input is toggled by clicking the button of a tag belonging to this group (and currently detected by the activetag controller).

5.13.2. Available outputs

Module - Inputs / Outputs	
Name	Description
[output name]	Relay output on the device. The displayed name corresponds to the configured description.

Module - Hardware	
Name	Description
Test_Melody	Plays the pre-configured Test Melody
Led_Test	Makes all LEDs blink for 5s
Melody UP	Plays two tones, low then high
Melody DOWN	Plays two tones, high then low

Module - Modbus	
Name	Description
[output name]	Modbus output from slave, configured on the device. The displayed name corresponds to the configured description.

Module - VPN	
Name	Description
Remote Access	Enable the remote access (provided it is configured to be in triggered mode)
[vpn name]	Enable or disable manual VPN connection (activated = VPN will connect). The displayed name corresponds to the configured description.

Module - Video Stream	
Name	Description
[v. stream name]	Manually enable or disable video streaming (activated = Streaming will be enabled). The bound VPN connection will be connected automatically (if not already) in this case. The displayed name corresponds to the configured description.

Module - Notifications	
Name	Description
[notification name]	Send a notification (SMS or Email) configured on the device. The displayed name corresponds to the configured description.
SMS disabled	Disable SMS sending.
Email disabled	Disable Email sending.

5.14. Scripts

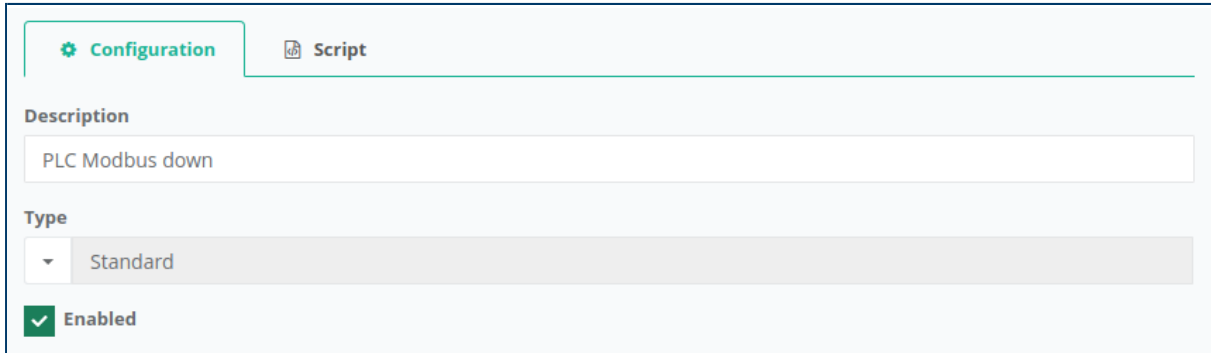


The Scripts module allows to create *Virtual* inputs whose state is computed from a script automatically generated from a visual program the user created. It also allows within its program to set output making it a more sophisticated Actions module.

5.14.1. Configuration

The configuration of a script is done in two steps.

First step consists of giving the script a description and choosing if it should be enabled or not. It is recommended to start by leaving the script disabled (the Enabled box is unchecked by default) and then enable it once you have ensured the SDN-3030 is in the right state.



The screenshot shows a configuration window with two tabs: 'Configuration' (active) and 'Script'. Under the 'Configuration' tab, there is a 'Description' field containing the text 'PLC Modbus down'. Below this is a 'Type' dropdown menu set to 'Standard'. At the bottom, there is a green checkmark icon followed by the text 'Enabled'.

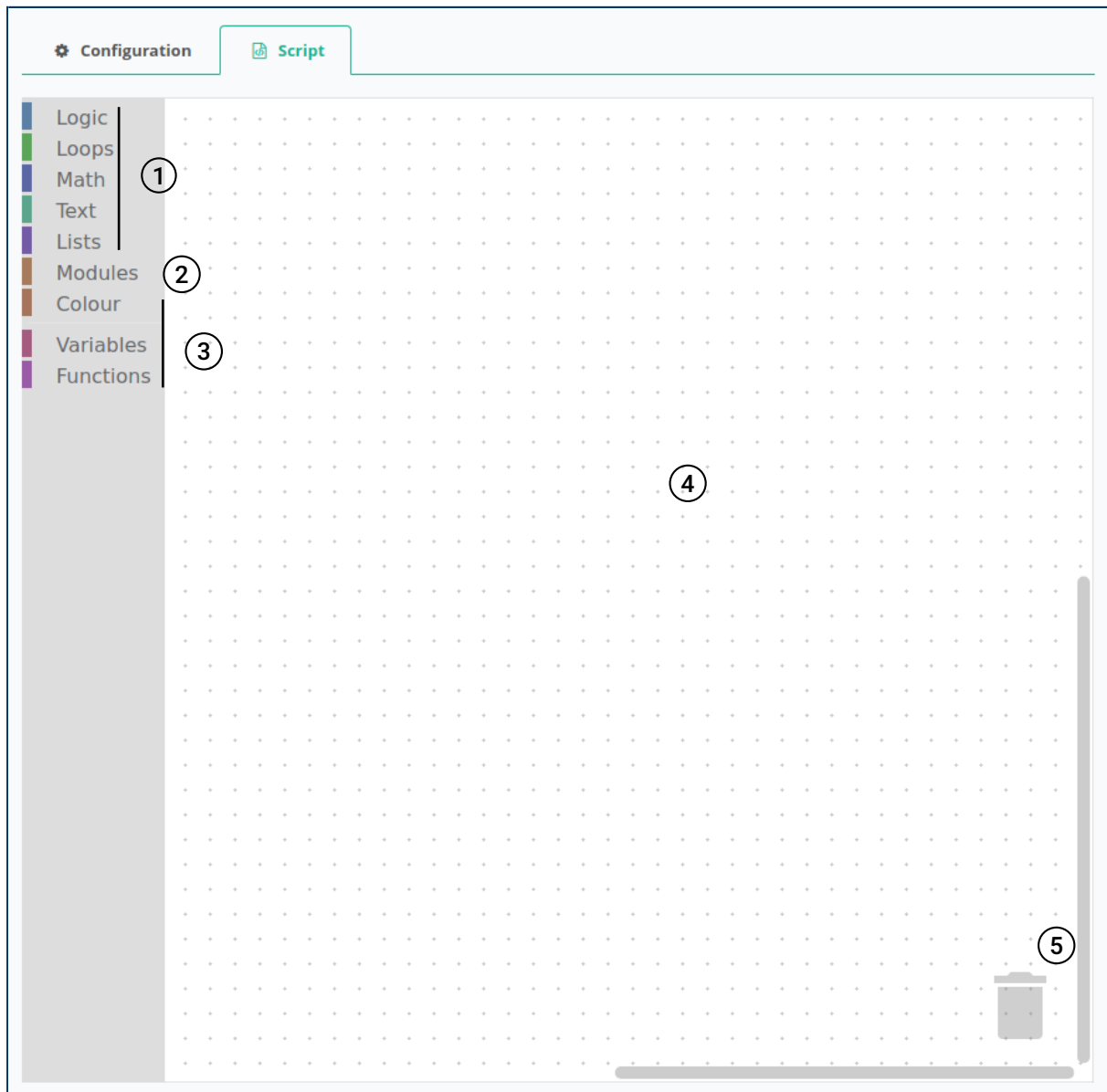
The second step of a scrip configuration is the most important, it consists of programming the behavior you want.

To do that the SDN-3030 offers you a graphical programming interface named Blockly.

"The Blockly editor uses interlocking, graphical blocks to represent code concepts like variables, logical expressions, loops, and more. It allows users to apply programming principles without having to worry about syntax."⁷

First, let's discover what a blank workspace looks like and how to use it.

7. <https://developers.google.com/blockly/guides/overview>



The elements (1), (3), (4) and (5) are directly provided by Blockly and are not specific to the SDN-3030. (1) and (3) provides the base blocks to construct your program, (4) is the grid on which you link your blocks and (5) allows you to delete a block from the grid.

The second element (2) on the other hand is specific to the SDN-3030 and provides blocks interacting with the SDN-3030 features.

Below is a description of those elements, blocks categories and workspace elements :

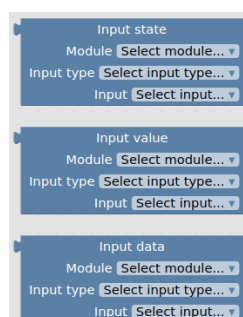
- | | | |
|---|------------------|--|
| ① | Logic | Blocks for comparison, condition, boolean |
| | Loops | Blocks to create and use various kinds of loops |
| | Math | Blocks for mathematical operations |
| | Text | Blocks to create and exploit text |
| | Lists | Blocks to create and exploit lists |
| ② | Modules | Blocks using the SDN-3030 features or allowing to use them |
| ③ | Colour | Blocks to make use of colours |
| | Variables | Blocks to create variables |
| | Functions | Blocks to create functions and function behavior |
| ④ | Grid | The grid for you to place your blocks and define the desired behavior |
| ⑤ | Trash | Allows you to remove blocks from the grid (you can also right click the block and chose Delete Block |

In any case, when wondering what a block does, hover your mouse pointer over it to display its tool-tip.

5.14.2. Custom SDN-3030-SPT-DP-3G/4G specific blocks

While standard blocks (every block belonging to ① and ③) behavior are easy to grasp, SDN-3030 specific blocks (every block belonging to (2)) might need so additional explanation :

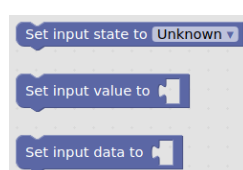
5.14.2.1. Inputs attributes



Section 5.13.1 describes inputs which can be used in the Actions module. All those inputs are also usable in the Scripts module but while the Actions module only allows to use the state attribute of those inputs, the Scripts module allows you to use their state, value and data.

Those three blocks once properly set (Module, Input type and chosen Input) represent the attributes of an input and can be used as you see fit within your program.

5.14.2.2. Script Input attributes

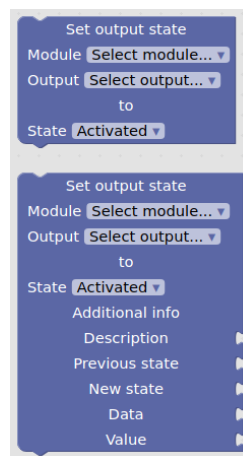


There are different ways to use a script input. It is possible to use it to directly do something (which most of the time means setting some outputs (sending an email, closing a relay, starting a video stream,

...)) but its first purpose is to define inputs with custom behavior for them to be used later (e.g a script input whose state is set to ACTIVATED from 7am to 8pm and DEACTIVATED otherwise, could then be used in the Actions module to open/close a relay opening a door depending on whether or not it is working hours). For the script to represent an input, it needs to have the same attribute, state, value and data. Those three blocks are used to set those attributes. It also means that if you never use the set input state to block then your script input state will always be UNKNOWN.

i The block to set the script input data does not allow to set empty data.

5.14.2.3. Using outputs



If the purpose of the script input you are creating is not to be used by the Actions or Alarm transmission module then it means it is supposed to directly do something within its internal logic. Most of the time this means setting some output to a specific state, this is what those two blocks are for.

Output state are set consequently of some input state change and some of those output can use this input state change (e.g sending an email specifying why it has been sent (change of state from X to Y)). If you simply need to set an output then the first block is enough but if you need to provide additional information, use the second one.

5.14.2.4. SDN-3030-SPT-DP-3G/4G date and time variables



One of the biggest advantage of the Scripts module over the Actions one is its capacity to use time. Instead of being limited to set some output when some input changes its state, you can schedule and timed an operation.

Those blocks are here to help you do so.

You should always remember though that :

- SPT hour, SPT minute and SPT second refer to SPT time
- SPT year, SPT month, SPT week day and SPT day refer to SPT date

So that if SPT date is 24/12/2019 and SPT time is 12:54:26 then :

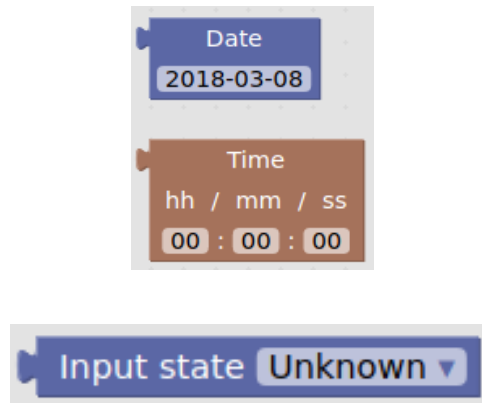
- SPT year : 2019
- SPT month : 12
- SPT day : 24
- SPT hour : 12
- SPT minute : 54
- SPT second : 26

The 24/12/2019, SPT week day value was 2 because it was a Tuesday, second day of the week.

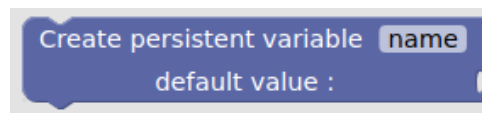
i You should keep in mind values returned by *SPT week day* block start at 0 for sunday.

5.14.2.5. SDN-3030-SPT-DP-3G/4G specific variables

Since the SDN-3030-SPT-DP-3G/4G offers blocks for some of its variables you need blocks of the same type to use them



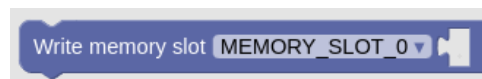
5.14.2.6. Variables persistence



This block allows you to persist the value of a variable between script execution. To use it you first need to create a simple variable then, you add this block and specify the name of the variable you previously created and want to persist. You need to provide a default value so that the first execution of the script does not fail.

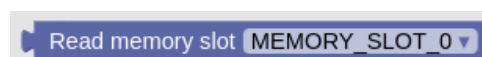
5.14.2.7. Read / write memory slots

Persistent variables being only persisted across script executions, the notion of memory slots was introduced to allow persistence across reboot or module restart. To read / write those memory slots, two blocks are available :



Allows to write a list of entries on the selected memory slot. Blockly offers numerous blocks to create and handle lists which you can use to prepare the list you want to write on a memory slot (tab Lists)

i In order to avoid overflows, the SDN-3030-SPT-DP-3G/4G limits the number of entries (which can be seen as lines in a text file) to 200 and the size of those entries (which can be seen as the number of characters) to 1024.



Allows to read the selected memory slot.

⚠ This block returns a list. This list may not contain the expected number of elements, so make sure your script take this into account or the module will crash.

5.14.3. Points of caution

In order not to be surprised with any unwanted behavior it is very important to understand a few points regarding the Scripts module.

5.14.3.1. For a Script execution only the last value/state/data set matters

During a script execution, only the last value / state / data set will be handled. It means it is not possible to create a Script Input acting as a pulse (DEACTIVATED - ACTIVATED - DEACTIVATED), only the last set state (DEACTIVATED will be reported to potential subscribers).

5.14.3.2. A script using time will be executed every second

It means if your program states something like Do X if current time is past expiration date, then X will be done every second once current time will be over the expiration date.

5.14.3.3. A script using an SDN-3030-SPT-DP-3G/4G input will be executed every time this input has its state change

It means a script using both time and a SPT input will be executed every second AND every time this input has its state change.

5.14.3.4. Variables are not persisted from one execution to another unless you request it

It means if you do not call the Create persistent variable block for the variable you want to persist then its value will be re-initialized every time the script is executed. (e.g If you create a counter to check how many times a Modbus input is DEACTIVATED in a day, you will need to persist your counter variable).

 Only primitive types (boolean, number or string) can be persisted. Trying to persist anything else will result in a crash of the module.

5.14.3.5. Blocks are not all strongly typed

It means while most blocks will not let you connect them to other blocks which are not compatible (e.g, connecting a text block to a conditional one is not possible because the conditional block is expecting blocks which will yield either true or false), some other can be connected despite being incompatible. This is especially true for variable blocks since you can very easily create a variable in which you store a Boolean and then some text or number. So even though most blocks interlocking is valid you should always be careful.

5.14.3.6. Lua scripting language is used under the hood

It means some characters or characters sequences cannot be used directly :

- " - " cannot be used in a variable name
- " .. " cannot be used in a text block
- " , " cannot be used in a text block
- " (" and ") " cannot be used in a text block

5.15. VPN



A virtual private network also known as a VPN is a private network that extends across a public network or internet. It enables devices to securely send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

The VPN features in the SDN-3030-SPT-DP-3G/4G are mostly used for :

- Secure video streaming
- Remote management/monitoring of your device
- Remote management of other equipment connected to the SDN-3030 (requires use of the Swiss-dotnet Cloud Portal platform)

The SDN-3030-SPT-DP-3G/4G currently only supports OpenVPN⁸ tunnels over UDP/IP with certificate and TLS Authentication.

5.15.1. VPN Connections

The Connections panel (available from the menu VPN → Connections) allows you to configure VPN servers configurations for the SDN-3030-SPT-DP-3G/4G to connect to.

To add a new Connection configuration, you need to click the **+** button and fill the following fields :

Name

Description

Mode

▼

☐ Enabled

Add remote

Server certificate

▼

Key / Certificate

▼

TLS key

▼

☐ Force 1.2 as min TLS version

8. <https://openvpn.net/>

Name	The name you want to give to this connection which is also the name which will be used for the input matching the connection state.
Description	Connection description. You can provide a custom description for your needs.
Mode	The mode can take 2 values : – Permanent which means the device will continuously try to establish this connection – Triggered which means the device will only try to establish this connection when requested to (e.g as a consequence to an input change of state within the Actions module)
Enabled	If this check box is not checked, the device will never try to enable this connection. It is mainly used when you want to configure a Connection but you know that the remote server is not ready yet and therefore do not want your SDN-3030-SPT-DP-3G/4G to continuously try to connect to an unavailable server.
Add remote	Add remote button let you enter the VPN endpoint address (or hostname) (also called VPN Server) and port. You can enter multiple redundant addresses.
Server certificate	The VPN server certificate.
Key / certificate	SDN-3030-SPT-DP-3G/4G key and certificate.
TLS Key	The TLS key the SDN-3030-SPT-DP-3G/4G will use to communicate with the VPN server.
Force 1.2 as min TLS version	When checked this option instruct the SDN-3030-SPT-DP-3G/4G the used TLS version should be at least 1.2.

i For more information regarding certificates (and TLS key) see section 5.4.2

Once all of those have been completed you can click the Apply button which will take you back to the Connection list where you can see the newly added connection displayed on a blue background (meaning it still needs to be saved). For the new configuration including the newly configured connection to be used click the Save button.

On the Connections screen displaying the list of configured Connections you can directly see the state of the Connections. If a Connection is displayed as Disconnected first, ensure it has every information and files needed for it to be available.

Modify VPN connections				
+ Save Cancel Search				
Name	State	Description	Mode	Actions
Swissdotnet Receiver	● Connected (10.235.0.56)	Swissdotnet Receiver	Permanent	✎ Edit / ✕ Delete

5.15.2. Remote Access

The Remote Access configuration panel (available in the menu VPN → Remote access) allows you to connect your device on the Swissdotnet SA Device Management platform.

For it to be functional you need to provide it with the IP address (or hostname) and port of the remote server you want it to connect to as well as the certificate and TLS key files. Just as for the standard VPN connections, you can choose the mode it will be in (Permanent or Triggered).

For the Remote Access to be redundant you can add more than one remote server.

Mode

▼

Permanent

☒ Enabled

Remote 1

ra.swissdotnet.ch

19000

↕

—

+

Server certificate

▼

Certificat serveur RA

Key / Certificate

▼

Clé / Certificat RA

TLS key

▼

Clé TLS RA

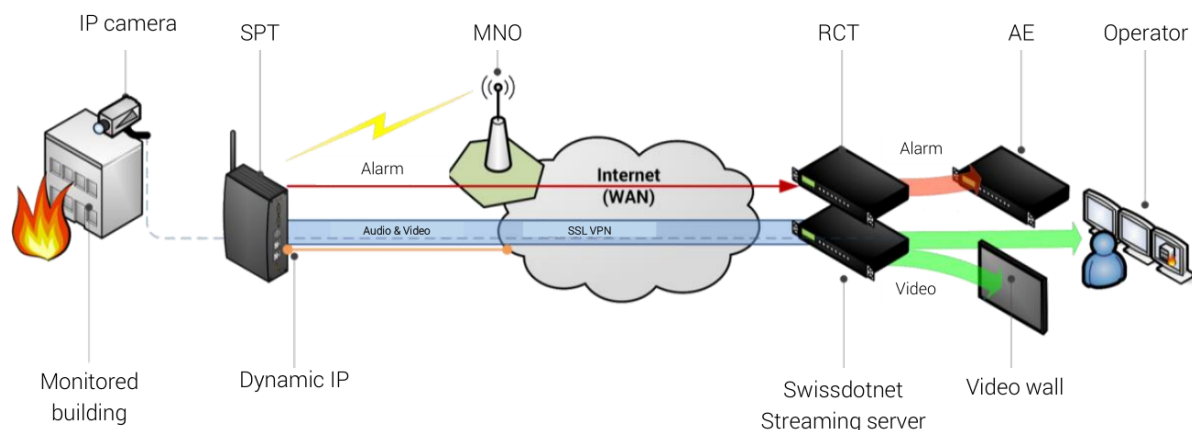
☐ Force 1.2 as min TLS version

5.16. Video transmission

S   A   C  

The SDN-3030-SPT-DP-3G/4G allows you to redirect services provided by video cameras available on a same network to a remote streaming server through a secure connection provided by the module VPN of the SDN-3030-SPT-DP-3G/4G .

This module can be used to redirect a video stream during an alarm to an ARC or a remote location. Please note that this functionality need a compatible video server.



Currently 3 types of service can be redirected :

1. **Management** : which allows to control the video camera orientation (Pan-Tilt-Zoom (PTZ))
2. **Snapshot** : which allows to get instant snapshot of the current video stream
3. **Stream** : which allows to get the current video stream

It is considered that a video camera will at least provide a service to get its video stream and as such, in the following document the configuration related to one video camera is designated as its video stream configuration (even if it includes services for management and snapshot).

Before configuring your IP cameras, you need to setup the VPN connection with the ARC. Contact your technical contact to get the required information. You will need at least one certificate, one TLS key and an IP address.

The video streams are configured in the menu Video streams (Video streams → Video streams). As for the other modules, you can  Edit,  Duplicate or  Delete items on the list. Click on the  button to create a new stream.

Name	
Video Stream	
Description	
This is my first IP Cam on SDN-3030	
IP	Network ITF
10.251.0.5	LAN interface (eth1)
Device model	
AXIS H264	
VPN connection	Streaming server port
Swissdotnet SA Video	8080
☒ Enable ☒ Auto start	

Name	The name you want to give to this video stream which is also the name which will be used for the input matching the stream connection state.
Description	Video stream description. You can provide a custom description for your needs.
IP	IP address of the video camera.
Network ITF	Select the physical network interface from which the IP camera is reachable.
Device model	Select the video camera model. (A list of well-supported models has been provided to ease the configuration). If the model you are using is not available in the list, you can choose the Other entry which will require you to enter manually its configuration parameters.
VPN Connection	Select the VPN connection used to transport the video services (the VPN connection must have been created first, see section 5.15.1 for more information about VPN connections).

i If you are not able to find the connection to your remote Streaming Server in the list, it means it has not been configured yet and so you need to add it first in the VPN module

Streaming server port	Port the SDN-3030-SPT-DP-3G/4G will use to notify the Streaming Server of the availability/unavailability of the video stream (default is 8080).
Enable	If this check box is not checked, the device will never try to connect this video stream. It is mainly used when you want to configure a video stream in advance, but you do not want that the device connects the stream yet.
Auto start	When checked the Streaming Server will start the video stream immediately upon reception.

i Unless under some restriction regarding data usage, there is no reason to disable this option.

Username

Password

Service 1 ([✕ Delete](#))

Type **Protocol**

URL / Port

Service 2 ([✕ Delete](#))

Type **Protocol**

URL / Port

Service 3 ([✕ Delete](#))

Type **Protocol**

URL / Port

Username Username needed to access the video camera

Password Password needed to access the video camera

If you selected a device model, the services are automatically configured. Otherwise you need to configure the services manually :

Type	There are three kinds of service embedded in a video stream : – Management which allows the remote Streaming Server to use PTZ feature – Snapshot which allows the remote Streaming Server to take snapshot of the video – Stream which allows the remote Streaming Server to get the live video stream, it generally uses h264 over RTSP
Protocol	Protocol of the service (it is possible to select Other if you want to use a specific protocol/port)
URL	URL path where the service is available
Port	Port where the service is available

Once every information has been provided you can click the Apply button which will lead you back to the Video streams configuration screen. Here you can see the one you just configured on a blue background, meaning it still need to be saved, which you can do by clicking the Save button.

 Currently, all Streams must be configured to use the same network interface (usually the LAN interface (eth1) but another can be chosen as long as all Streams use it).

5.17. Activetags

 When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required this module should not be used.

S   A   C  

 To ensure a proper working of your dongle you have to power off the SDN-3030 whenever you want to plug or unplug it.

5.17.1. Dongle configuration

To be able to detect active tags, the SDN-3030 requires an additional dongle. It currently only supports Bluetooth Low Energy (BLE) dongles which requires the following fields to be filled :

Tags reader

① ②

Apply Save Cancel

Name

BLE Dongle ③

Description

Bluetooth Low Energy Dongle ④

Checksum

0 ⑤

ID

1 ⑥

⑦

 Dongle Bluetooth LE

⑧ Detected tags	⑨ Description	⑩ Last seen	⑪ Rssi (dbm)
cc:55:79:ce:9d:e0		13/09/2018 18:09:03	-43
31:90:b1:da:27:d9		13/09/2018 18:09:03	-67
c1:50:fd:46:d8:97		13/09/2018 18:09:04	-79
e4:27:52:1b:d6:cf		13/09/2018 18:09:03	-79

- ① ② Action which can be run on the reader configuration
- ③ The name of the reader you are configuring. You can provide a custom name for your needs.
- ④ The description of the reader you are configuring. You can provide a custom description for your needs.
- ⑤ (If no checksum is needed, 0 default value can be used)
- ⑥ The ID of the reader you are configuring.
- ⑦ The current state of the reader.
- ⑧ The IDs of the tags currently detected by the reader.
- ⑨ The descriptions of the tags currently detected by the reader. (if one has been provided)
- ⑩ The last time the currently detected tags have been seen by the reader.
- ⑪ The strength of the signals emitted by the tags currently detected by the reader.

i Tags are considered currently detected if the reader received any signal from them within the last 5 seconds. In addition to currently detected tags, the Detected tags list includes tags which are part of a group (whether they are currently detected or not). Only those tags will have a description.

i Tags listed in the Detected tags list are ordered by signal strength.

5.17.2. Groups

On its own the Activetags module can not do anything, it is simply supposed to expose information for other modules to act upon. E.g, we might want to open a fence when a truck arrives in front of it. To avoid having to duplicate Action/Script/Event reacting to tags status the Activetag module allows you to group some tags (e.g we might want the previous fence to open upon multiple different trucks arrival).

5.17.2.1. Groups list

Name	Description	Actions
Emergency vehicles	Emergency vehicles tags	 Edit /  Duplicate /  Delete
Service trucks	Service trucks tags	 Edit /  Duplicate /  Delete

The activetags groups list contains every groups of tags for which the SDN-3030 will provide inputs for you to use. It means if you want to act upon a tag status it needs to be part of a group.

i A tag can be part of multiple groups.

5.17.2.2. Groups configuration

To create a new group you just have to click the **+** and fill the required information.

Name	Emergency vehicles
Description	Emergency vehicle tags
Max reception level (dbm)	-60
Time before tag disappearance (s)	30
Add tag	

- Name** The name of the group you are creating. You can provide a custom name for your needs.
- Description** The description of the group you are creating. You can provide a custom description for your needs.
- Max reception level** The minimum signal strength a tag of this group should have to be considered online.
- Time before tag disappearance** The maximum duration a tag can spend without sending anything to the reader before being considered offline.

To add a tag to your group you just have to click the Add tag button and fill the required information.

Tag 1			
Name	Description	ID	-

- Name** The name of the tag. You can provide a custom name for your needs.
- Description** The description of the tag. You can provide a custom description for your needs.
- ID** The tag ID.

i If you don't know the ID of your tag you can place it right next to your dongle. Since tags are ordered by signal strength (in the Active tags → Tags reader) your tag should be the first one listed.

5.17.3. Inputs

UD 100 - Tag online	①	Activated 
UD 100 - Tag in alarm		Unknown 
Service trucks - Tag online	②	Activated 
Service trucks - Tag in		Deactivated 
Service trucks - Tag out		Deactivated 
Service trucks - Tag in alarm		Unknown 
Service trucks - Button pressed	③	Deactivated 
Emergency vehicles - Tag online		Deactivated 
Emergency vehicles - Tag in		Deactivated 
Emergency vehicles - Tag out		Deactivated 
Emergency vehicles - Tag in alarm		Unknown 
Emergency vehicles - Button pressed		Unknown 

- | | | | |
|-----|-----------------|----------------|---|
| ① | [DONGLE NAME] - | Tag online | The dongle is currently detecting at least on tag |
| | | Tag in alarm | At least one tag currently detected by the dongle is in alarm |
| ② ③ | [GROUP NAME] - | Tag online | At least one tag of the group is currently detected by the dongle. |
| | | Tag in | One tag of the group appeared in the dongle detection perimeter. |
| | | Tag out | One tag of the group disappeared from the dongle detection perimeter. |
| | | Tag in alarm | At least one tag of the group is in alarm. |
| | | Button pressed | At least one tag of the group has its button pressed. |

 The Button pressed input is currently only working with Swissdotnet SA active-tags.

i Some inputs can embed the following json formatted information in their input data when they are triggered :

```
{
  "action": "Tag [ACTION]",
  "id": "[ID]",
  "name": "[TAG NAME]"
}
```

Where :

- ACTION is the action which triggered the input change :
 - Tag disappeared
 - Tag detected
 - Button pressed
 - Button released
- ID is the id of the tag which triggered the input change
- TAG NAME is the name of the tag which triggered the input change

i Every group inputs follow some common behavior pattern.

- If they have never been triggered then their state is UNKNOWN
- If a dongle has ever been plugged in and it is no longer the case then their state is in ERROR
- If a dongle has been plugged in, plugged out at some point and is now plugged in again, their state will stay in ERROR as long as they have not been triggered again

i The states of inputs [GROUP NAME] - Tag in and [GROUP NAME] - Tag out follow a pulse pattern, meaning it is ACTIVATED then immediately DEACTIVATED every time a tag of the group enter/exit the dongle detection perimeter.

5.18. Serial alarm

S   A   C  

The Serial alarms module is used for serial protocol connected to the SDN-3030-SPT-DP-3G/4G .

5.18.1. Configuration

The configuration is divided into two parts, the serial port configuration and the protocol configuration (inputs and specific parameters).

i The serial port must be configured in the Hardware module (Hardware → Serial Interfaces) . See section 5.9.2 for more information.

5.18.1.1. Devices

The Devices panel allows to configure devices using serial protocols. It is possible to have multiple devices with the same serial protocol, but each device must use a different physical port.

 Do not use the same serial port for two different devices (Modbus included).

Modify serial alarm devices

+
Save
Cancel

Search

Name	State	Description	Type	
ESPA Device	● Connected	ESPA Alarm system	ESPA	✎ Edit / ✕ Delete / ☰ Status

Name Device name

State The state of the device :

- **Connected** The peer is connected
- **Disconnected** The peer is disconnected
- **Unknown** The state is unknown

Description Device description

Type Type of serial device

The ☰ Status button allows you to access the status of the device (including the logs).

5.18.1.2. Inputs

The Inputs tab (Serial alarms → Serial alarms inputs) list the configured serial alarm inputs.

Modify serial alarms inputs

+
Save
Cancel

Search

Description	State	Address	Actions
Feu - appel techniciens	Unknown	6702	✎ Edit / 📄 Duplicate / ✕ Delete
Feu temporisé - appel pompier	Unknown	6702	✎ Edit / 📄 Duplicate / ✕ Delete

Description The description of the input

State The state of the input, see protocols inputs (section 5.18.2.2 and section 5.18.3.1) for details

Address The address of the input, see protocols inputs (section 5.18.2.2 and section 5.18.3.1) for details

5.18.2. ESPA 4.4.4

 **When compliance with EN 50131-10:2014EN_50131-10 , EN 50136-2:2013EN_50136-2 , EN 54-21:2006 Type 1EN_54-21 is required** if an ESPA device is used to receive additional information from Fire System then an event should be created (see section 5.7.7) to signal any lost of communication between the SDN-3030-SPT-DP-3G/4G and the Fire System.

ESPA 4.4.4. is a character protocol, used in bus. It is originally designed for pager, however, it is also frequently used to transmit additional alarm information.

The protocol has two roles :

- Master, the other device linked to the SDN-3030-SPT-DP-3G/4G
- Slave, the SDN-3030-SPT-DP-3G/4G

It is possible to have multiple slaves on the same bus, as each device has its own address.

5.18.2.1. Limitations

As the protocol is design for pager, it has some limitations :

- Supports only ASCII character (no accents)
- Message of max 128 characters

5.18.2.2. Inputs

The ESPA4.4.4 protocol support two different types of inputs.

5.18.2.2.1. Direct input

Direct inputs, send directly all messages received (alarm and restored).

Feu - appel techniciens

Description

Address

Device

▼ ESPA Device

Type

▼ Standard

ESPA type

▼ Direct

Apply

Cancel

Description	The description of the input
Address	The address of the call pager, the value is between 0000 and 9999
Device	The protocol device
Type	The type of the input
ESPA type	Direct or indirect

5.18.2.2.2. Indirect input

Indirect inputs, send an alarm only if another input is triggered (called bound input).

- If there is no valid message when the bound input is triggered, the ESPA input is still ACTIVATED (then switched back to UNKNOWN) but it contains no data from ESPA message.
- ESPA messages have an expiration date (notification timeout), after this date, they are deleted.
- When the bound input is restored, the input is DEACTIVATED (then switched back to UNKNOWN).

Feu temporisé - appel pompier

Description

Feu temporisé - appel pompier

Address

6702

Device

▼ ESPA Device

Type

▼ Standard

ESPA type

▼ Indirect

Input module

▼ Inputs / outputs

Input type

▼ Standard

Input

▼ input1(1)

Trigger state

▼ Activated

Notification timeout (s)

0

Apply

Cancel

Description		The description of the input
Address		The address of the call pager, the value is between 0000 and 9999
Device		The protocol device
Type		The type of the input
ESPA type		Direct or Indirect
Input module		The module source of the bound input
Input		The bounded input
Trigger state		The alarm state of the bound input
Notification timeout	ti-	The validity of the message in seconds. After the validity is reached the message is deleted.

5.18.2.3. Configuration

ESPA Device

Name

Description

Serial path

Protocol

Client address (Decimal-ASCII)

Master address (Decimal-ASCII)

Polling frequency (ms)

Read timer (ms)

Write timer (ms)

SDN-3030-SPT-DP-3G/4G - Technical manual

Name	Device name
Description	Device description
Serial path	The serial device to use
Protocol	The protocol to use
Client address	The address of the SDN-3030-SPT-DP-3G/4G in decimal format (value between 0-255). Default is the character ascii "2"=50
Master address	The address of the master in decimal format (value between 0-255). Default is the character ascii "1"=49
Polling frequency	The maximum value of the polling frequency from the master in milliseconds. The value must be higher than the real polling frequency. Default value : 30000 milliseconds
Read timer	The value until the system wait for a response from the master. Do not change this without reasons. Default value : 2000 milliseconds
Write timer	Wait some time before writing on serial port. This value allows the master to switch between read and write. Default value : 600 milliseconds

5.18.2.4. Debug

ESPA protocol can be painful to debug, to help the debugging the SDN-3030-SPT-DP-3G/4G provides two windows in the Devices tab → Status.

5.18.2.4.1. Logs

The log window gives information about the last major events. The following messages are displayed :

- Connection with valid server : The communication with the master is ok
- Received an alarm message, the master has send a message to this SDN-3030-SPT-DP-3G/4G
- Receiving message for a non-existent entry, the Master has send an ESPA message to an unused input
- Unknown input : A message is received, but no input uses this message

ESPA Device	
 Log	 Raw
Occurrence	Message
23/10/2018 13:34:59	Connection with valid server.
 23/10/2018 13:34:59	Receiving an alarm message.
Address : [6702] Message : [256 /W WC GLYCINE]	
23/10/2018 13:35:10	Connection with valid server.
23/10/2018 13:35:20	Connection with valid server.

5.18.2.4.2. Raw

The last 300 bytes exchanged between the slave and the master. The values are in hexadecimal, newest value at the bottom.

Use this windows, if you are not sure about the serial communication parameters. You must see the polling sequence in the raw data. If the received value does not match this pattern, there is probably a serial communication problem.

Polling sequence :

Master → 0x04 - [address slave] - 0x05

Client → 0x06 (ack)

Master ask to send message :

Master → 0x04 - [address master] - 0x05 - [address slave]

Client → 0x06 (ack)

ESPA Device

 Log
 Raw

Decimal values:
Rx
Tx

32	71	76	89	67	73	78	69	32	32	32	32	3	4	4	50	5	4	4	50	5	4
4	49	5	50	5	6	1	49	2	49	31	54	55	48	50	30	51	31	50	30	54	31
51	30	50	31	50	53	54	32	47	87	32	32	32	87	67	32	71	76	89	67	73	78
69	32	32	32	32	3	6	4	4	50	5	4	4	50	5	4	4	49	5	50	5	6
1	49	2	49	31	54	55	48	50	30	51	31	50	30	54	31	51	30	50	31	50	53
54	32	47	87	32	32	32	87	67	32	71	76	89	67	73	78	69	32	32	32	32	3
6	4																				

Clear
Cancel

5.18.3. Wago UPS

"The 787-850, 787-852 and 787-854 switching power supplies are equipped with an integrated serial RS232 interface. This interface is directed toward the outside and serves to visualize all relevant measured values (voltage/current etc.)."⁹

5.18.3.1. Inputs

The Wago UPS inputs are automatically created and cannot be removed. Only their description can be edited to fit your needs.

Automatically created inputs :

⁹. Wago 787 Power Supply System documentation [wago_ups_doc](#)

Default description	intent
[DEVICE NAME] : Battery needs to be changed	It is recommended to change the battery (hovering over its state will display the battery voltage value)
[DEVICE NAME] : Device error	The UPS is in error state
[DEVICE NAME] : Input voltage below limit	The input voltage has fallen below the limit value (hovering over its state will display the current input voltage value and the minimum value it reached)
[DEVICE NAME] : Low battery	The rechargeable battery voltage (currently being used) is very low (hovering over its state will display the battery voltage value)
[DEVICE NAME] : No battery charging available	It is not possible to recharge the battery
[DEVICE NAME] : On battery	The device is currently running on its battery (hovering over its state will display the battery voltage value as well as the current charge value)
[DEVICE NAME] : Output voltage below limit	The output voltage has fallen below the limit value (hovering over its state will display the current output voltage value)
[DEVICE NAME] : Output current above limit	The output current is above the limit value (hovering over its state will display the current output current value as well as the maximum value it reached)
[DEVICE NAME] : Output deactivated	The output is deactivated
[DEVICE NAME] : Temperature-dependent charging not available	Temperature-dependent charging feature is not available

5.19. Modules



The Modules menu allows you to view the list of installed software modules and their states.

Name	State	Description	Version	Log level	Action
Actions	 Running	Linker action -reaction module.	1.5.0	Warning	 Show
Active tags	 Running	Active tag module	1.5.0	Warning	 Show
Alarm transmission	 Running	Alarm transmission module.	1.5.0	Warning	 Show
Authentication	 Running	User authentication module.	1.5.0	Warning	 Show
Hardware	 Running	Hardware configuration and monitoring module.	1.5.0	Warning	 Show
IP alarm	 Running	IP alarm module	1.5.0	Warning	 Show
Inputs / outputs	 Running	Input/output module.	1.5.0	Warning	 Show
IoT	 Running	IoT module	1.5.0	Warning	 Show
Modbus	 Running	Modbus communication module	1.5.0	Warning	 Show
Network	 Running	Network management module.	1.5.0	Warning	 Show
Notifications	 Running	Notification module	1.5.0	Warning	 Show
Scripts	 Running	Script module	1.5.0	 Debug	 Show
Serial alarms	 Running	Serial Alarm module	1.5.0	Warning	 Show
VPN	 Running	Vpn module	1.5.0	Warning	 Show
Video streams	 Running	Video module	1.5.0	Warning	 Show
Web server	 Running	Web server module.	1.5.0	Warning	 Show

Name	Module name
State	Module state which can be : • Starting The module is starting • Start Error An error occurred during the starting process, will retries • Disconnected The module is currently disconnected • Error The module is encountering an unexpected error • Running The module is running normally • Running previous The module is running with its previous configuration • Running default The module is running with its factory configuration • Unknown The module state is unavailable

i It is especially important to pay attention to this since it implies something was invalid in the last configuration. When a module is running with its previous configuration its menu entry is prefixed with a **⚠** warning icon to further highlight the importance of this information.

Description	Module description
Version	Version of the module
Log level	The current log level of the module

i If the current log level is different from the persisted one (which is the one used after a device restart or a saved module configuration) then it is prefixed with a **⌚** icon. This icon is displayed so that you can quickly note if a module has a changed log level which should probably be set back before switching to normal mode.

5.19.1. Advanced features

S   A   C  

As a supervisor S  it is possible to temporarily change the log level of a module (e.g to allow easier debug). This modification will be discarded if the SDN-3030-SPT-DP-3G/4G is restarted or if the module configuration is saved.

Select log level

Warning

i **Temporarily apply**

Temporarily applies the log level chosen for the module concerned. This change will be undone on transmitter restart or when saving the configuration of the module.

Temporarily apply
Close

As an administrator  , it is possible to either temporarily change the log level or to set a new log level in the configuration so that it will still be used even after the SDN-3030-SPT-DP-3G/4G is restarted or if the module configuration is saved.

Select log level

▼
Warning

 **Temporarily apply**

Temporarily applies the log level chosen for the module concerned. This change will be undone on transmitter restart or when saving the configuration of the module.

 **Apply and save**

Apply and save the log level chosen in the running configuration as well as any configuration changes made to the module concerned. This operation requires a restart of the module

Temporarily apply
Apply and save
Cancel

The following actions are also available from the Modules menu :

Reboot	Reboot the device
Factory reset	Revert the settings to the factory configuration

5.20. Maintenance

5.20.1. Application log









The Application log (menu Maintenance → Application log) shows various information generated by the modules.

Type

▼

All

Status

▼

All

From

22/10/2018

00:00:00

To

22/10/2018

23:59:59

Apply

Reset

Export

Live

Historical

Search

Level	Occurrence	Message
OK	22/10/2018 10:42:16	Login from user "supervisor".
OK	22/10/2018 10:38:58	Date successfully changed by "NTP".
OK	22/10/2018 10:18:28	Configuration of "Script" successfully updated.
OK	22/10/2018 10:15:51	Login from user "supervisor".
OK	22/10/2018 10:00:36	Alarm "NFH0002" transmitted to "ARC Test" via "46.14.125.133:44300 eth0" (ref: "169", info: "", genetated 0.007s ago).
OK	22/10/2018 10:00:36	Alarm "NFH0002" generated for "ARC Test" (ref: "169", info: "").

You can filter the application log by message Type and Status using their respective drop-down list. Fields To and From allow to select the date range (only usable in Historical mode). To apply filters, you must click on the Apply button. The Reset button resets the filters to defaults.

The default mode is Live which mean that new log messages appear in a continuous flow. In Historical mode, you can scroll down to display previous log messages.

It is also possible to export the application logs (in Comma Separated Values (CSV) format) by clicking the  Export button. Some web browser might prevent the pop-up allowing you to save the file in which case you will have to change its configuration (simply allow pop-up from the SDN-3030-SPT-DP-3G/4G).

5.20.1.1. Application log Messages

Type - Alarm	
Status	Message
GENERATED	Alarm "event" generated for "arc" (ref : "ref").
ACCEPTED	Alarm "event" transmitted to "arc" via "atp" (ref : "ref", generated "duration"s ago).
TIMEOUT	Failed to transmit alarm "event" to "arc", timeout (ref : "ref", generated "duration"s ago).
ARC REFUSED	Failed to transmit alarm "event" to "arc", refused (ref : "ref", generated "duration"s ago).
ARC ERROR	Failed to transmit alarm "event" to "arc", invalid response (ref : "ref", generated "duration"s ago).
ARC STOPPED ERROR	Failed to transmit alarm "event" to "arc", ARC was stopped before the successful transmission of the alarm (ref : "ref", generated "duration"s ago).
EXPIRED	Failed to transmit alarm "event" to "arc", alarm expired (ref : "ref", generated "duration"s ago).
ATP REFUSED	Failed to transmit alarm "event" via "atp", refused (ref : "ref", generated "duration"s ago).
ATP ERROR	Failed to transmit alarm "event" via "atp", invalid response (ref : "ref", generated "duration"s ago).
ATP TIMEOUT	Failed to transmit alarm "event" via "atp", timeout (ref : "ref", generated "duration"s ago).
ATP DISCONNECTED	Failed to transmit alarm "event" via "atp", disconnected (ref : "ref", generated "duration"s ago).
ARC DISCONNECTED	Failed to transmit alarm "event" to "arc", disconnected (ref : "ref", generated "duration"s ago).
GENERATED BUT NOT SENT	The event has been generated but no ARC is currently using it.
REMOTE COMMAND RECEIVED	Remote command "remote command name" received : "remote command code" : "state"

Type - Power	
Status	Message
MAIN FAILURE	Main power failure.
MAIN RESTORE	Main power restored.
ALTERNATE FAILURE	Alternate power failure.
ALTERNATE RESTORE	Alternate power restored.
UP	Power up.
RESET	Power reset.

Type - Connection	
Status	Message
AS FAILURE	Connection with the alarm system failed.
AS RESTORE	Connection with the alarm system restored.
ATP FAILURE	Connection with ATP "atp" of "arc" failed.
ATP RESTORE	Connection with ATP "atp" of "arc" restored.
ARC FAILURE	Connection with "arc" failed.
ARC RESTORE	Connection with "arc" restored.
TNI FAILURE	Network interface "tni" failed.
TNI RESTORE	Network interface "tni" restored.

Type - Configuration change	
Status	Message
SUCCESS	Configuration of "module" successfully updated.
ERROR	Configuration of "module" failed : "message".

Type - Software	
Status	Message
SUCCESS	Software successfully updated.
ERROR	Software updated failed.

Type - Date modification	
Status	Message
SUCCESS	Date successfully changed by "user".
ERROR	"user" failed to update the date.
UPDATED BY PRO-TOCOL	Time has been corrected by the NTP.

Type - Login	
Status	Message
SUCCESS	Login from user "user".
ERROR	User "user" failed to log in.

Type - Modules handling	
Status	Message
SPAWNED	Process "process" has been spawned.
KILLED	Process "process" has been killed.
RELOADED	Process "process" has been reloaded ¹⁰ .

¹⁰. A process is logged as reloaded when it has been restarted by another process (e.g when you save the VPN process configuration, the Video module will be reloaded)

Type - Notification	
Status	Message
MAIL SEND	Email "subject" successfully sent.
FAILED TO SEND MAIL	Failed to send email.
SMS SEND	SMS successfully sent after "nb tries" attempt(s).
FAILED TO SEND SMS	Failed to send SMS after "nb tries" attempt(s).
SMS RECEIVED	SMS receive from "sender" with content : "sms content".

Type - Run mode	
Status	Message
FACTORY MODE	Factory mode.
MAINTENANCE MODE	Maintenance mode.
NORMAL MODE	Normal mode.

5.20.2. System log

S   A   C  

The System log (menu Maintenance → System log) shows live operations performed by the system.

You can choose the number of messages displayed on the list by using Page size drop-down list and then clicking on the Apply button.

5.20.3. Network analysis

i The network analysis is only intended as a tool to help you diagnose the network and can be subject to failures.

The Network analysis (menu Maintenance → Network analysis) allows you to quickly check the compliance of the network the SDN-3030-SPT-DP-3G/4G is being used in with its configuration. It extracts and test :

- Interfaces monitoring addresses
- DNS servers addresses
- ARCs RCTs addresses and ports
- NTP servers addresses
- VPN servers addresses, port and certificates
- Cameras addresses (only if they are reachable through ping)

i It should be noted that DNS are tested by trying to resolve swissdotnet.ch and google.com.

i It should be noted that only ARCs hosted on Swissdotnet SA RCTs can be tested. If results always indicate a connectivity error with ARCs which you know are hosted on Swissdotnet SA RCTs then it probably means those RCTs are not up to date.

When the analysis is done, the following will be displayed :

- Potential errors
- Results

— Parameters used

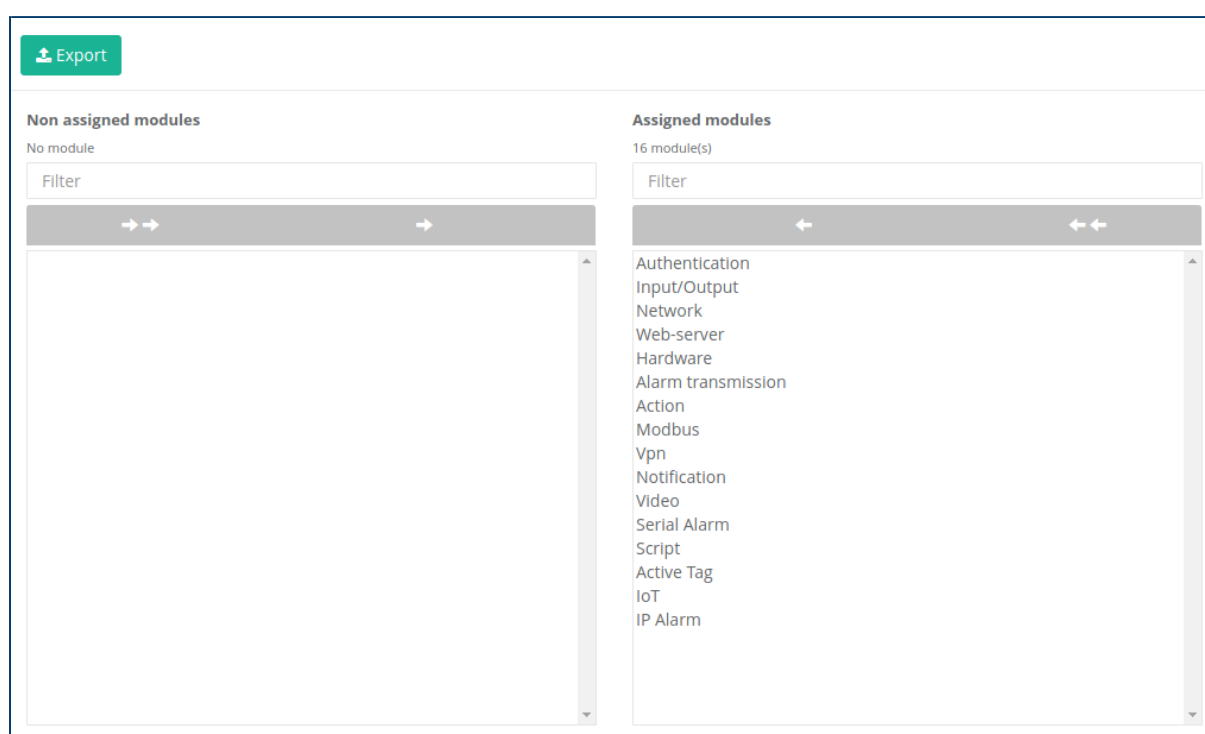
In addition a pop-up window will open, offering you the possibility to download a network capture realized during the analysis ¹¹.

5.20.4. Configuration

S   A   C  

The Configuration panel (available in the menu Maintenance → Configuration) lets you import or export the device configuration. This could be useful if you plan to install several devices and you want to create some configuration presets.

You can choose which module you want to export by moving the modules names in the Assigned modules list. Select the required module and click on the arrows to add or remove an entry in the module list.



 As stated in the information box section 5.1.2, modules can depend on each other to execute some tasks. For this reason it is strongly discouraged to export/import only specific modules configuration. If you are not sure of which modules configurations can be imported/exported separately then just import/export them all at once.

The  Export button will generate a file containing the configuration of the selected modules. Once clicked, a summary windows will show you the export content. Click on Download to load the file from your web browser. The configuration file uses the .tar format.

You can import a configuration file by clicking on the Choose File button. Please check that you select a valid file with the extension .tar. Then click on  Import button.

¹¹. It is possible for the provided capture to be empty, this is a known issue.

 Import

Configuration file

Choose File

No file chosen

After the importation, a dialog box will return the import results. The imported configuration is loaded in memory. To definitively apply the changes, you need to manually save the configuration for all the modules.

 While we strive to achieve backward compatibility for configuration files, we can not guarantee forward compatibility. It means you should not try to import a configuration created with a newer version on an older one.

 You should never import a configuration directly modified (from manually editing the file). A lot of parameters are generated following strict rules which cannot always be reproduced manually. By editing the configuration files you might very well create a configuration the SDN-3030-SPT-DP-3G/4G will be able to run but which will not result in the behavior you expected.

5.20.5. Update

A  

 We recommend keeping your equipment up to date with the latest version available.

 Updating your system should not be taken lightly and that is why some precautions must be taken beforehand :

- the ARCs receiving the alarms should be warned
- the running configuration should be exported

5.20.5.1. Update : how it works

In order to minimize as much as possible the time your SDN-3030-SPT-DP-3G/4G will not be operational, the update mechanism works as follow :

- 2 system partitions (1 running, the other is used to install the update)
- When clicking the install button the update is first downloaded
- Once downloaded the update content is checked
- If the update passes the checks it is installed on the un-active partition (so that no modification is done on the running one, allowing your system to stay functional during the install of the update)
- Once the install is done the SDN-3030-SPT-DP-3G/4G is rebooted on the partition the update has been installed
- On boot, some checks are made to ensure the new release is functional
- If any check fails, the SDN-3030-SPT-DP-3G/4G is rebooted on the previously running partitions otherwise you are good to go

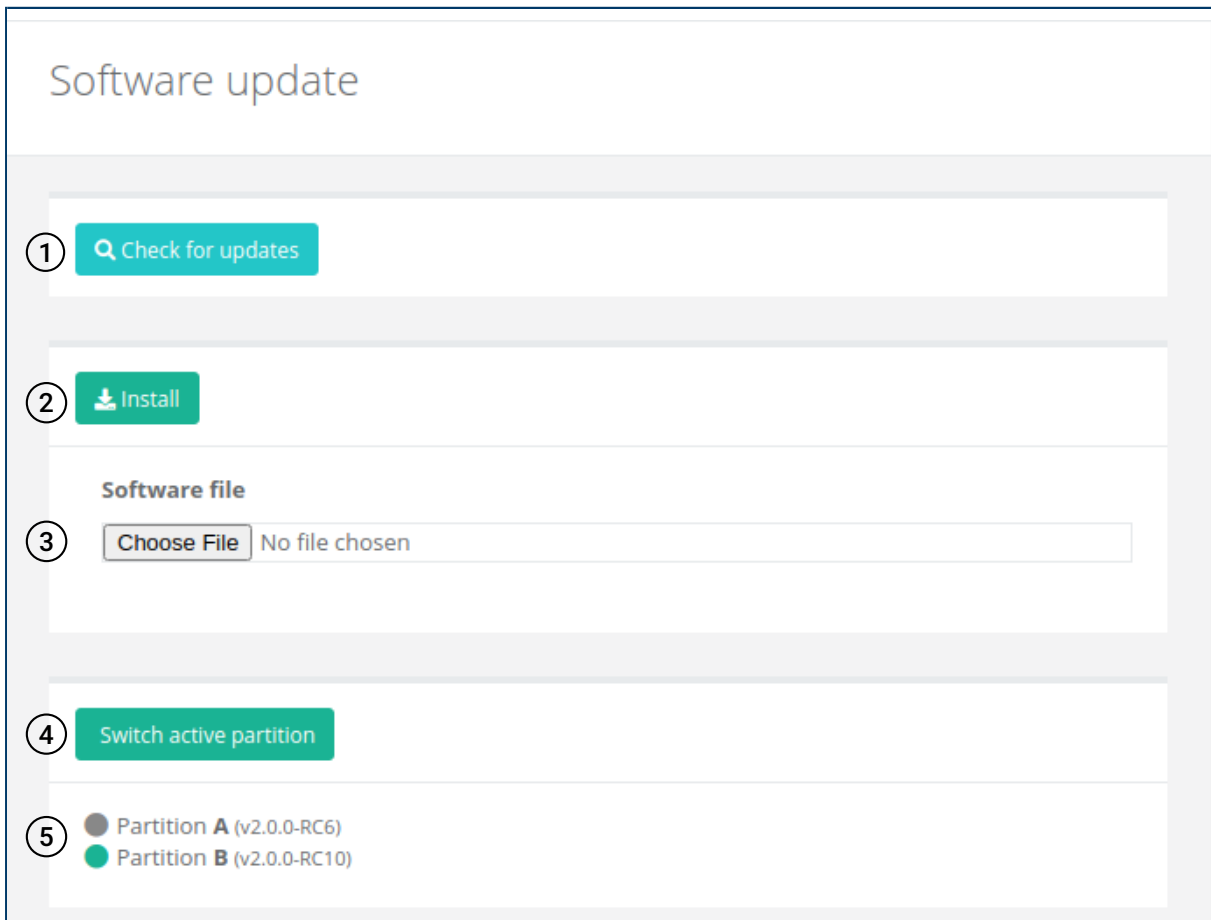
To ease the update general process as much as possible the SDN-3030-SPT-DP-3G/4G data (including its configuration) has been placed on a separate partition untouched during the update. It means on reboot on the new partition you will not have to re-import your configuration.

i Your passwords are included in the configuration so you do not need to commission the SDN-3030-SPT-DP-3G/4G again.

5.20.5.2. Different ways of updating

i The Update management is only available to access-level 4 (administrator) user. Contact Swissdotnet SA if you cannot remember your credentials.

The Update panel (available in the menu Maintenance → Update) is used to update the software of the SDN-3030-SPT-DP-3G/4G . Three different ways of updating your SDN-3030-SPT-DP-3G/4G are offered (local, remote, rollback) and can be used through the following panel :



The screenshot shows the 'Software update' interface. It contains several sections: a 'Check for updates' button (1), an 'Install' button (2), a 'Software file' section with a 'Choose File' button and 'No file chosen' text (3), a 'Switch active partition' button (4), and a list of partitions (5). The partitions are 'Partition A (v2.0.0-RC6)' and 'Partition B (v2.0.0-RC10)', with Partition B highlighted in green.

- ① Allows you to start the search for updates available on your configured Update Server (c.f section 5.20.5.3). Once the search is done, if any updates are available you will be provided with a list from which you will have to choose the update to install.
- ② Allows you to install local updates
- ③ Allows you to browse your computer to find the local update you want to install
- ④ Allows you to change the running partition
- ⑤ List of partitions where the one with the green label is the one currently running

⚠ When updating through local update file it is very important you know exactly what you are doing and what you are installing. Integrity checks can only be done once the file has been completely downloaded which might not be possible if the file you are trying to use is too big.

Update files have a *.raucb* extension and a size around 60MB.

5.20.5.3. Update servers

i The Update management is only available to access-level 4 (administrator) user. Contact Swissdotnet SA if you cannot remember your credentials.

The Update servers panel (available in the menu Maintenance → Update servers allows you to configure the servers on which the SDN-3030-SPT-DP-3G/4G will look for available updates.

Modify update servers

+
Save
Cancel

Search

Name	Description	Actions
SDN Update Server	Swissdotnet Update Server	Edit / Delete

The Swissdotnet SA Update Server is configured by default but you can remove it (using the **✕** button) or add other ones.

To add a new Update Server you just have to click the **+** button and fill the required information.

Name

Description

☐ Use HTTPS

Add host

Name The name of the update server you are creating. You can provide a custom name for your needs.

Description The description of the update server you are creating. You can provide a custom description for your needs.

Use HTTPS Check this check box if the update server you are configuring uses HTTPS.

To add a host you just have to click the Add button **+** and fill the required information.

Host 1		
0.0.0.0	Port	-

IP / Hostname An IP address or an hostname allowing to reach the update server you are configuring

Port The port on which the update server is reachable.

i It is possible to add multiple Update Server and each of them can have multiple host to ensure redundancy but you should know that the SDN-3030-SPT-DP-3G/4G will iterate on them in the order they are listed and will stop its search as soon as it gets a response from one of them.

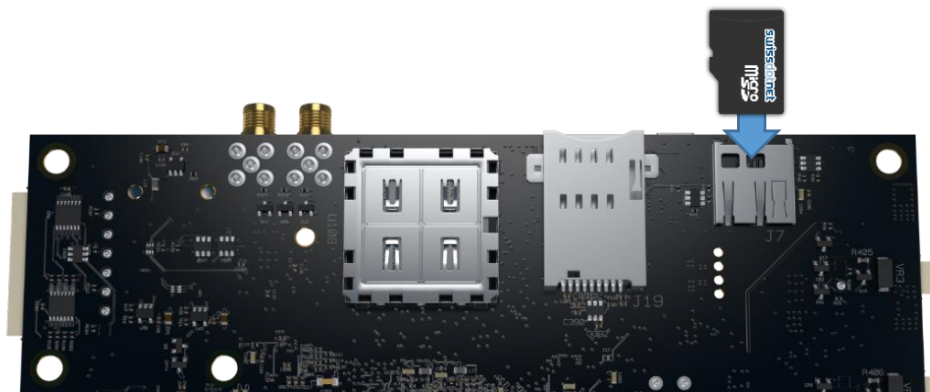
6. Device Recovery

Device recovery allows you to completely update or recover your device whatever its state. This operation is only reserved for registered re-seller.

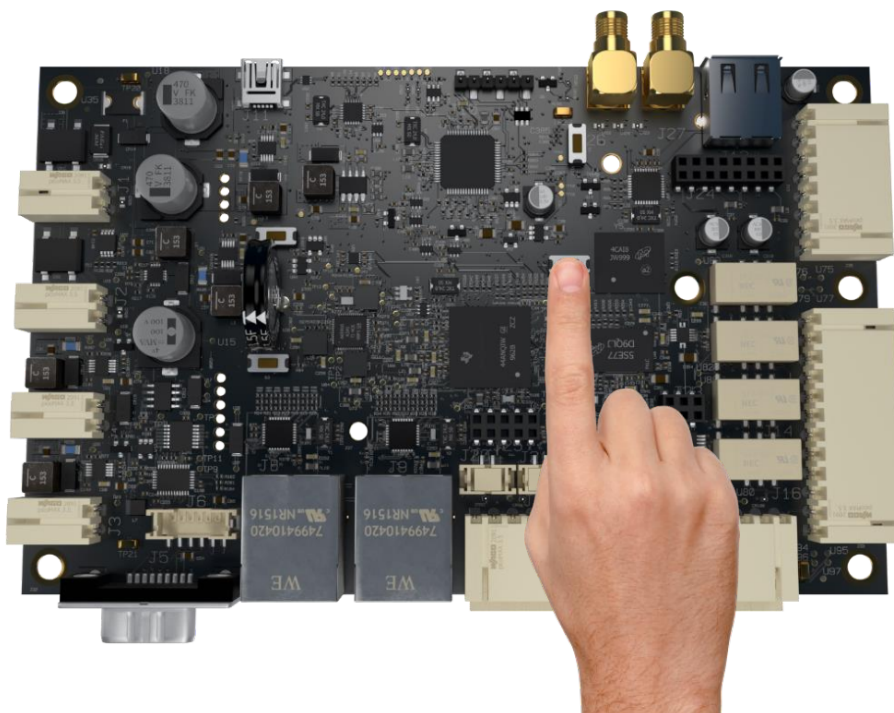
🔊 This procedure totally erases the device, do not forget to make a backup first.

The recovery process uses a factory micro SD card which must be ordered directly from Swissdotnet SA .

1. **Power off** the device
2. Insert the factory micro SD card into the device



3. **Power on** the device while **holding the factory reset button**. You have to press the button until the orange and red LED flash



4. Wait until the LEDs stop blinking and you hear a beep
5. **Power off** the device and remove the micro SD card
6. Your device is now ready!

6.1. Recovery card preparation

Swissdotnet SA approved installers can access various software version (depending of their respective contract) at : <https://swissdotnet.ch/products/ipalarms/ip-spt/partners/>

Those software images need to be flashed on a micro SD card according to the following methodology :

- Download the targeted software version
- Unzip the downloaded archive
- Download win32diskimager at : <https://sourceforge.net/projects/win32diskimager/files/latest/download>
- Launch win32diskimager with the administrator right
- Select the micro SD you want to flash the software on
- Select the the unzipped software
- Click the Write button

 The micro SD card capacity must not be over 8 Go.

This methodology is targeted for windows users but can easily be used with any Linux distribution by replacing win32diskimager by a suitable replacement such as Clonezilla (you can find it here : <http://clonezilla.org/downloads.php>) in graphic mode or the dd utility in command line.

Appendices

A. Getting started : your first alarms

In order for you to know where to start, you will find below a step-by-step guide on how to set your first alarm.

This guide will go over two configurations :

- A basic alarm triggered by an input change (e.g AS trigger an intrusion alarm on the SDN-3030-SPT-DP-3G/4G)
- A more complex alarm triggered by a Modbus input and leading to a video stream made available to check the cause of the alarm (e.g monitoring of a server room temperature through a Modbus PLC and video camera to ensure no one left the door open)

Both of those configurations assume you already logged in the SDN-3030-SPT-DP-3G/4G , if this is not the case then please refer to section 3.3.

A.1. A basic alarm

So lets say we have an AS connected on the SDN-3030-SPT-DP-3G/4G which can trigger an intrusion alarm.

1. Give a name (e.g Intrusion alarm) to the physical input connected to the AS so that you can quickly find it later (refer to section 5.5.1)
2. Create the ARC (refer to section 5.7.3) to which you want the intrusion alarm to be sent
3. Create the Event use to transmit the intrusion alarm (refer to section 5.7.7)
4. Assign the Event to the ARC you previously created (refer to the end of section 5.7.7)

Your new intrusion alarm is now ready to be triggered.

i To check it is properly working you can manually trigger the alarm by temporarily changing its input logic (refer to section 5.5.1) and check in the Application log (refer to section 5.20.1.1 your alarm has been generated.).
⚠ Do NOT forget to set its logic back when you are done with your test.

A.2. A more complex alarm

So now lets say we have a Modbus PLC monitoring the temperature of a server room and a video camera filming the door of the server room. The following steps will configure the SDN-3030-SPT-DP-3G/4G so that when the room temperature exceed some specific value (lets say 25°C) an alarm is sent to the ARC embedding an URL allowing to see the video stream to check if the server room door has been left open.

1. Create the Modbus slave corresponding to the PLC monitoring the room temperature (refer to section 5.10.1)
2. Create the Modbus input corresponding to the room temperature (refer to section 5.10.2)

WARNING Server room temperature

Description

WARNING Server room temperature

Type

▼ Standard

Address

365

Access type

▼ Read Holding Registers (FC3)

Value type

▼ AB unsigned Integer

Activated range min

200

☒ Min included

Activated range max

250

☒ Max included

Slave

▼ PLC Server room

☒ Logic inverted

Apply

Cancel

 Values displayed here are only used as examples. It is assuming the PLC address is 365 and the input it provides for the room temperature gives a value in m°C encoded as an AB unsigned integer.

3. Add the certificates and key which will be used to establish a secure VPN connection (refer to section 5.4.2) (those certificates and keys should have been provided by the ARC the alarm will be sent to)

 The TLS key (.key file) and the bundle (.p12 file) containing the other key / certificates should be imported separately and be imported under different names.

4. Create the VPN connection which will be used to securely access the video stream using the certificates and keys you previously added (refer to section 5.15.1)
5. Create the video stream corresponding to the video camera filming the server room, using the VPN connection you previously created (refer to section 5.16)
6. Create a script which will activate the video stream when the room temperature is out of range and deactivate it when the temperature is in a valid range (refer to section 5.14)

Room server entrance camera triggering

⚙️ Configuration
📜 Script

- Logic
- Loops
- Math
- Text
- Lists
- Modules
- Colour
- Variables
- Functions

if

Input state

=

Input state Activated

Module Modbus
Input type Standard
Input WARNING Server room temperature

do

Set output state
Module Video streams
Output Server room entrance camera
to
State Activated
Set input state to Activated

else if

Input state

=

Input state Deactivated

Module Modbus
Input type Standard
Input WARNING Server room temperature

do

Set output state
Module Video streams
Output Server room entrance camera
to
State Deactivated
Set input state to Deactivated

Apply
Cancel

7. Create the ARC (refer to section 5.7.3) to which you want the alarm to be sent to
8. Create the Event use to transmit the alarm embedding the video stream URL (refer to section 5.7.7)

Alarm server room temperature

Summary

Configuration

Options

Description

Alarm server room temperature

Priority

▼ Medium

Input module

▼ Video streams

Input type

▼ Standard

Input

▼ Server room entrance camera

Delay (ms)

☐ Watchdog

Apply

Cancel

Alarm server room temperature

Summary
Configuration
Options

Building name

Location

Room

Url / verification

Information / alarm text

IP address (TS 50136-9)

Port (TS 50136-9)

File (TS 50136-9)

MAC address (DC-09)

☒ Add occurrence / time event field

☐ Add position

☐ Add site name

Apply
Cancel

i It is very important to notice the \$input-data in the Information / alarm text field as it is the option which will allow for the video stream URL to be embedded in this alarm.

9. Assign the Event to the ARC you previously created (refer to the end of section 5.7.7)

You are done! Now, when the room temperature will be out of its valid range, the Modbus input state created will change to activated. Once the Modbus input state is activated, the script will request the server room video stream to be activated (upon which, the video module will request the vpn module to start its VPN connection). As soon as the VPN connection is established, the SDN-3030-SPT-DP-3G/4G announces to the Streaming Server that the server room video stream is available. The Streaming Server then send the

SDN-3030-SPT-DP-3G/4G - Technical manual

SDN-3030-SPT-DP-3G/4G an URL which can be used to reach the video stream. As soon as the SDN-3030-SPT-DP-3G/4G receives this URL it changes the video stream state to activated which trigger the Alarm embedding the URL.

B. F.A.Q Frequently Asked Questions

B.1. Physical

- **What are the SDN-3030 dimensions?**
PCB is 160*100mm and Case is 300*300*100mm
- **Which antenna connector is for what?**
The connector near the USB port is the one for the GPS, the other one is for the 3G/4G
- **How many inputs does the SDN-3030 has?**
The SDN-3030 provides 4 intruder inputs (able to detect tampering such as short-circuit and open-circuit status) and 8 digital inputs
- **How many outputs does the SPT has?**
The SDN-3030 provides 4 outputs
- **Which of the buttons is the reboot button?**
The reboot button (B1) is located between the micro USB port and the big capacitor
- **Which of the buttons allows to mute the buzzer?**
The B4 button located just under the antenna connectors allows to temporarily mute the buzzer

B.2. Install

- **How to access the front interface to configure the SDN-3030?**
An SDN-3030 with factory settings offers two ways to access the front interface :
 - Connection on the micro USB port allows you to reach the front interface at <http://192.168.128.1> (no https yet). Windows computers might require you to install a driver (which you can find on the company website at <https://swissdotnet.ch/en/sdn-3030-al-transmitter/> bottom of the page).
 - Connection on the second Ethernet port (the one near the inputs connectors) allows you to reach the front interface at <http://192.168.127.10> once you have configure an IP address for your computer on the same sub-network (e.g 192.168.128.1)
- **What are the default credentials?**
An SDN-3030 with factory settings uses the following credentials : supervisor/supervisor
- **What are the network requirements to install an SDN-3030?**
To work properly an SDN-3030 needs the following :
 - To be able to reach its ARCs (IP(s) / port(s))
 - To be able to reach its NTP server (IP(s) / port(s))
 - To be able to reach its VPN servers (IP(s) / port(s))

B.3. VPN

- **What protocol is the module VPN using?**
The SDN-3030 uses UDP
- **What are the Swissdotnet SA Remote Access server information?**
The Swissdotnet SA Remote Access server parameters are as follow 46.14.125.133:9000
- **Do VPNs connections need to be permanently activated?**
No, the SDN-3030 allows you to trigger a connection upon specific events

B.4. Alarm transmission

- **Is it possible to have a "main" and a "backup" ARC?**

It is possible to implement such a behavior (alarm sent on "main" ARC if available, on "backup" ARC otherwise) using the script module.

B.5. Hardware

- **What is the PCB current consumption?**

The current consumption reaches 950mA (max consumption) on startup and then has an average 240mA current consumption

B.6. IoT

- **What protocol(s) the SDN-3030 IoT module offers?**

Currently the SDN-3030 only provides an MQTT client

B.7. Network

- **Why is my network interface labeled as deactivated?**

The SDN-3030 uses two ways to monitor its network interfaces :

- OSI layer 2 (physical) control : is there anything connected (physically) to the interface
- PING control : monitoring IPs addresses are pinged

If no monitoring address is provided then only the first control will be used.

- **Will the 3G modem be able to use 900Mhz once Swisscom in 2020 will stop using 2100Mhz frequency band for 3G?**

Yes, the 3G modems accept the following frequencies band :

- 3G : 800/850/900/1900/2100
- 2G (fallback) : 850/900/1800/1900

B.8. Video

- **Is there a limit of simultaneous streams the SDN-3030 can handle?**

Currently we recommend you not to activate more than 4 simultaneous streams. The network should always be tested to ensure it will be able to support the maximum number of simultaneous streams configured.

- **Is the SDN-3030 able to simultaneously use streams reachable from both interfaces?**

No. Currently all video streams must be reachable on the same interface.

- **Why can't I use the video stream I configured in an Action, a Script or an Event?**

The most likely is your video stream is not enabled (tab Video streams / Video streams,  edit button : "Enable" check box field)

- **The stream seems to be made available to the Streaming Server but there is no image, only a black screen.**

The most likely explanation is your stream is not configured to "auto-start" (tab Video streams / Video streams,  edit button : "Auto start" check box field)

B.9. General

- **Why is my SDN-3030 signaling a power supply ERROR?**

The SDN-3030 power supply can be configured in two different ways :

- Using the "Onboard" management, meaning the SDN-3030 will detect on its own the power supply error by monitoring the voltage its inputs provide. If you are using an "Onboard" power supply type and have a power supply error then it means the tension on (one of or all of) the SDN-3030 input(s) is not enough
- Using the "External" management, meaning the SDN-3030 is informed of power supply error by an external device (most of the time an external power supply). If you are using an "External" power supply type and have a power supply error it either mean you still need to configure the SDN-3030 for it to know on which on its inputs it will receive the information it needs regarding the power supply state or that the power supply you are using is indicating the SDN-3030 it is in error
- **I cannot connect to the SDN-3030 using the micro USB port.**
Windows computers usually require you to install a driver. The default driver can be found on the company website at <https://swissdotnet.ch/en/sdn-3030-al-transmitter/> bottom of the page. Some Windows version are not compatible with the drivers provided on the website, if you encounter any issue please feel free to open a ticket by sending an email at ticketing@swissdotnet.ch

i It is possible to use the SDN-3030 without the need of any external driver but it will require you to do some additional steps :

1. Open the **Device Manager**
2. Select Other devices
3. From the expended list right click **RNDIS**
4. Click **Update Driver Software** from the menu
5. When prompted, click **Browse my computer for driver software**
6. Click **Let me pick from a list of device drivers on my computer**
7. From the **Common hardware types** list, select **Network adapters**
8. Click **Next**
9. Select **Microsoft** in the **Manufacturer** list^a
10. Select **Remote NDIS Compatible Device** in the **Model** list
11. Click **Next**
12. In the **Update Driver Warning** dialog box, click **Yes**

^b

a. On Windows 7, select **Microsoft Corporation** instead of **Microsoft**

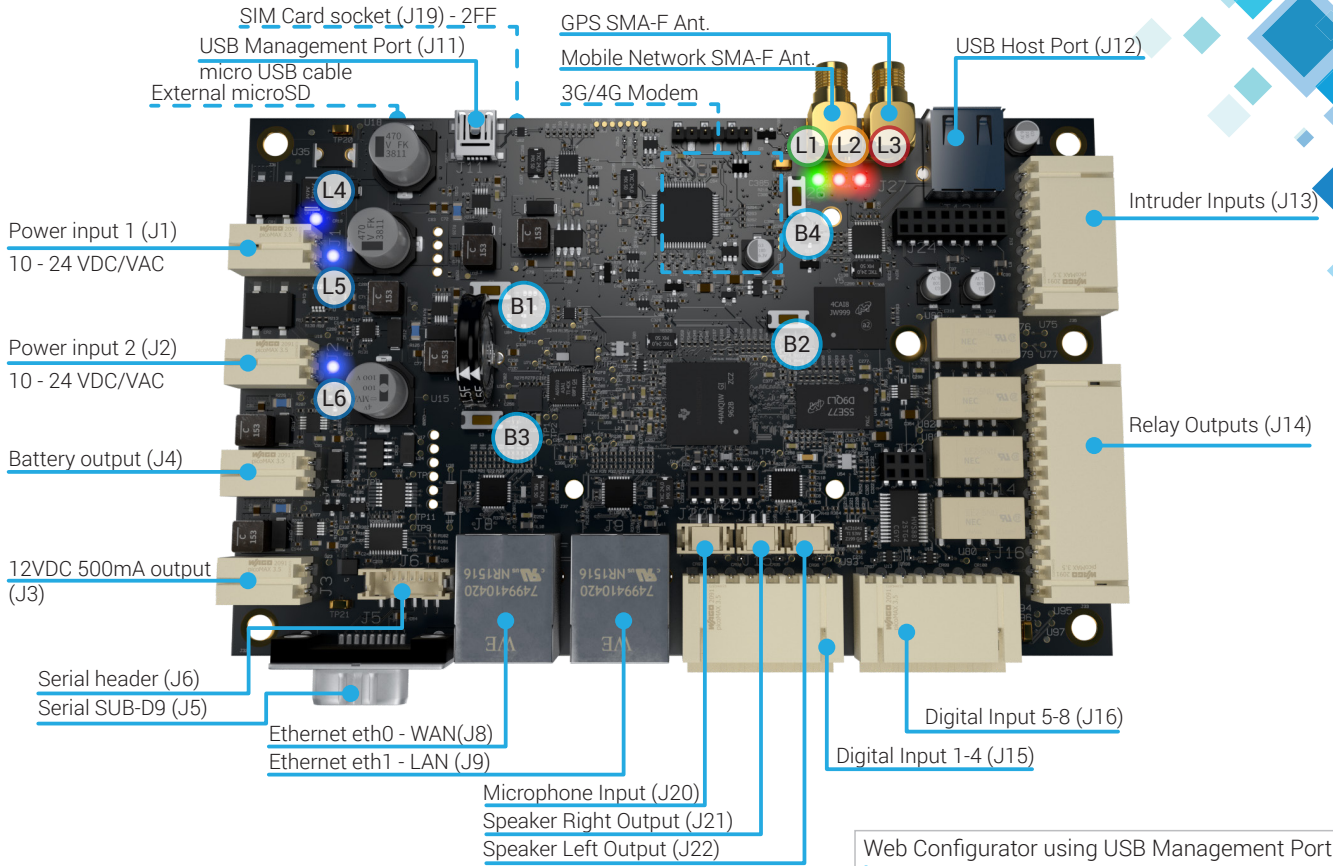
b. This procedure has been extracted from <https://in.mathworks.com/help/supportpkg/parrot/ug/intro.html>

- **Is there a recommended web browser to access the SDN-3030 front interface?**
To ensure the best user experience we recommend either [Google Chrome](#) or [Mozilla Firefox](#)
- **Why is nothing happening when I click the Maintenance / Application log and Maintenance / System log tabs?**
Some ad blockers prevent those pages from being displayed. If the icon representing your ad block has a number on it which is increased each time you try to access one of those pages then it is most likely the one responsible and should be disabled for those pages.
- **Is there a physical button triggering a factory reset?**
No. To run a factory reset you need to connect to the SDN-3030 front interface and click the "Factory reset" button (tab Modules)
- **Is it possible to remotely update the SDN-3030 software?**
No. This feature should soon be available but for now you still need a physical access to the SDN-3030
- **Is there a recommended size for the micro SD used to flash the SDN-3030?**
We recommend to use a 4G micro SD card and not to exceed 8G capacity card
- **Why is the buzzer ringing?**
The SDN-3030 buzzer will ring in the following conditions :
 - Your ATS is down

Still no answer to your question? If it is not in the manual either, you can still email us at info@swissdotnet.ch or open a ticket by sending an email at ticketing@swissdotnet.ch.

C. Cheat Sheet

Cheat Sheet



Web Configurator using USB Management Port
<http://192.168.128.1>
 Default login & password : supervisor / supervisor

LEDS

L1	Off / HW Fail	Booting	Working normally	Software failure
L2	All ATP are OK	Untransmitted event(s) pending	One ATP disconnected, alarm transmission OK	
L3	All ARC are OK	No power trouble	One or more ARC is/are disconnected	
L4	No power on SPT	No power input 1	Power trouble	On battery
L5	No power on input 1	Power input 1 OK		
L6	No power on input 2	Power input 2 OK		

BT

B1	Reset	B2	Custom usage	B3	Boot on uSD	B4	Mute buzzer
----	-------	----	--------------	----	-------------	----	-------------

WIRING

