IP RCT SDN-7573

Administrator Manual

Revision 2.0.0 – IP-RCT version 2.0.0

Swissdotnet SA
Route du Pâqui 4
1720 Corminboeuf

Swissdotnet SA
Route du Pâqui 4
CH-1720 Corminboeuf

Phone: +41 (0)26 510 29 30
Fax: +41 (0)26 510 29 34

E-Mail: info@swissdotnet.ch
Web: http://www.swissdotnet.ch

Version:	2.0.0 (September 15th, 2020)
Author:	Vincent Pasquier, Marc Romanens, Steve Jacot-Guillarmod
Document:	Swissdotnet IP-RCT Administrator Manual

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 of Contents

1 Overview

1.1 Icon description

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

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

1.2 Online resources

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

1.3 Compliances

The SDN IP-RCT complies with the following standards:

- EN 50136-3:2013
- EN 50136-1:2013 DP2, DP4

Refer to Swissdotnet application server for other compliances.

The SDN IP-RCT is certified with ATS categories DP2 and DP4 as defined by the EN 50136-1 standards. All EN 50136-1 ATS categories can also be used.

ⓘ Certification body: CE 0560 Telefication

1.4 Safety guidelines

Refer to Swissdotnet application server safety guidelines.

1.5 Acronyms

The document uses mostly acronyms to refer to alarm components. The following list defines these acronyms.

ATS
Alarm Transmission System.

SPT
Supervised Premises Transceiver.

TNI
Transmission Network Interface.

2 Introduction

This document presents the IP-RCT software developed by Swissdotnet SA. Its goal is to be used as a reference administrator manual and to educate users on how the IP-RCT works.

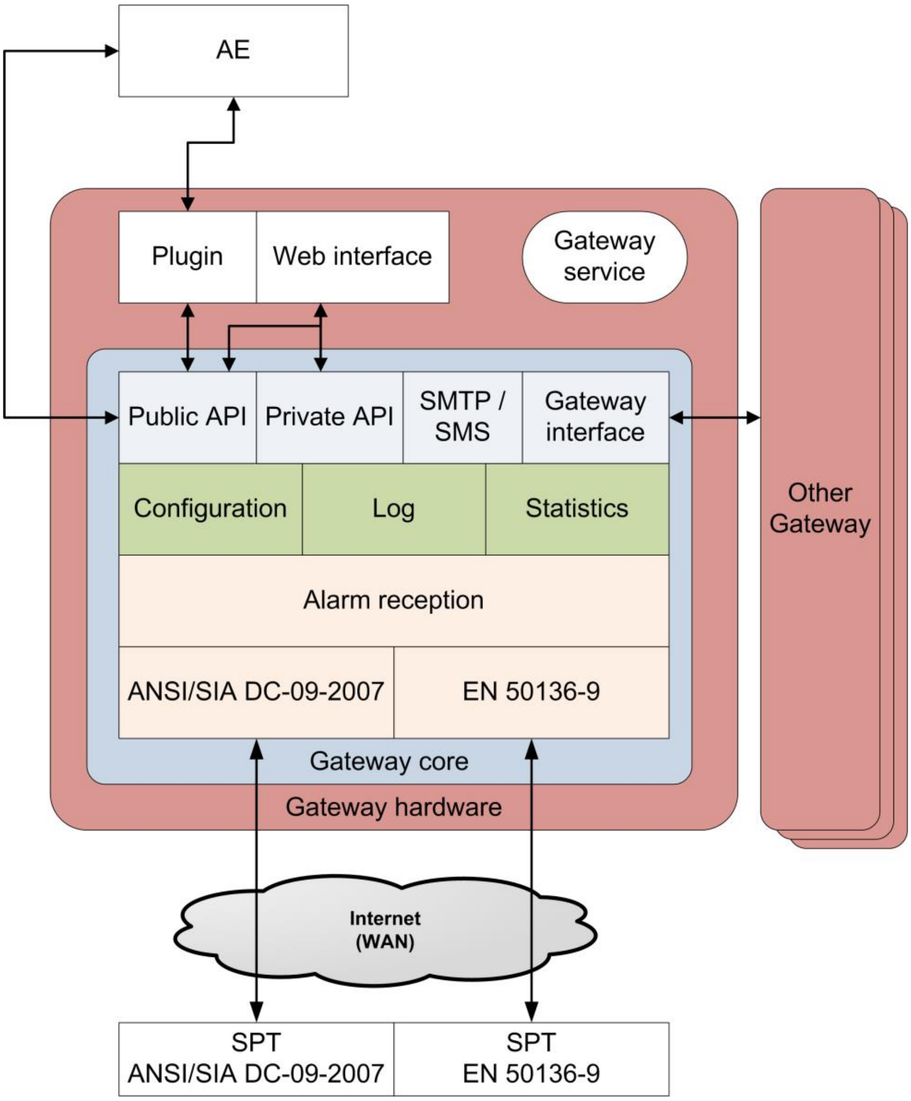
2.1 What is IP-RCT?

The security alarm ecosystem consists of many components and since the Internet bubble burst, a plethora of protocol was created. From the motion sensor to the security officer, many communication paths are used.

First sensors are generally connected to a transmitter (or SPT) which regroups sensors and actuators. Then, usually, a professional is setting the SPT up for public institution and private buildings to relay alarms and notify security companies. Prior the installation, a setup protocol with the security company to define where the alarm is sent is prepared. On the security company side, their job is to add the new connection to their system with all the customer information. This operation is done on an IP-RCT which receive many SPT connections. The last link in the alarm ecosystem is the AE on which security officer receive notification and decide how to intervene based on the transmitter alarm.

The IP-RCT task is to receive alarms and to forward it to all its AE registered. Many incoming protocols are available for the IP-RCT to receive SPT alarms and many AE protocols are available to dispatch to software. It acts as a protocol coder/decoder from incoming and outgoing communication.

The figure below shows the IP-RCT architecture from a layer point of view. All IP alarm protocols are abstracted and all use the same way to communicate with our alarm reception layer. Then once an alarm is received, it goes through the configuration/log/statistics layer to perform routing and monitoring operations. At the top, the public and private API are used to forward the alarm onto AEs and to connect with outside services.



The IP-RCT work, in reference to EN-50136-3, in pass-through mode. This operating mode means that no signals are stored until acknowledged by an annunciation equipment (AE).

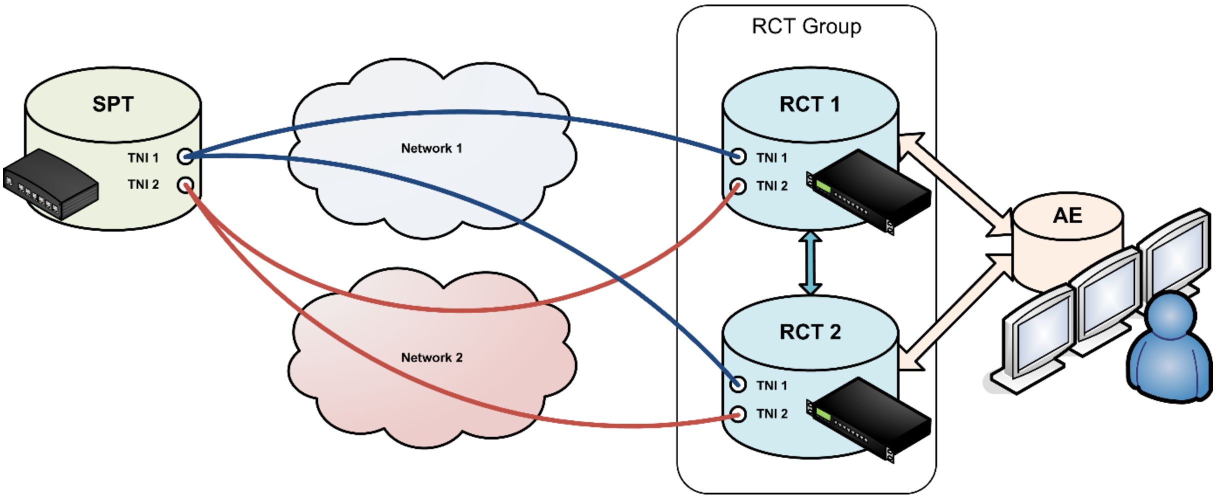
ⓘ It is important to remember the SDN IP-RCT is a plugin for the SDN Core application and as such, most of its limitation (such as the number of alarms it can process per sec) are only set by the hardware the Core is running on.

While running on SDN-7573 we certify up to 25 alarms per seconds received on the RCT.

2.2 Cluster Structure

To improve availability and reliability, IP-RCTs can be connected together in a cluster architecture. The connection pattern is full meshed (all IP-RCTs must reach each other) and work in any network configuration (secure or insecure). All communications are secured through SSL/TLS cipher algorithms.

In the following figure, the cluster is composed of two IP-RCT linked together communicating both with the same AE. They both listen on two interfaces to receive SPT alarms. 4 paths reach the cluster from different network to improve the availability.



3 Installing the IP-RCT

ⓘ Follow first the application server administrator guide to properly setup the server and understand its features.

3.1 Install package

After contacting Swissdotnet, a package containing the IP-RCT software will be provided. Authenticate with a user that possess administrator user level.

Upload the package and follow the guide on how to start an application.

3.2 Network configuration

Make sure that the following network configuration is done to use the IP-RCT to its full potential:

- Add one or multiple DNS servers. Certain plugin will require to access DNS records and may fail doing so if not is setup;
- Add a default gateway on the WAN interface to allow incoming and outgoing traffic to be correctly routed;
- Prefer a static IP address to DHCP and put the IP-RCT in a DMZ;
- Configure the incoming/outgoing traffic on the firewall in the network infrastructure to reach the IP-RCT.

ⓘ The IP-RCT is developed with DDoS attack in mind. We approach all incoming traffic with a fail-fast approach. If a message is not valid, it is dropped promptly.

In any case, contact your ISP and ask for DDoS protection

3.3 Date and time

Since timing is a crucial part of the clustering used by the IP-RCT, configure a NTP server and make sure that all IP-RCT have access to it. Use preferably the same server for all IP-RCTs.

4 Configuring the IP-RCT

ⓘ The steps described below are supposed to be done in order for the initial RCT configuration. Setting NTP server in the core application and configuring network configuration is necessary before RCT cluster.

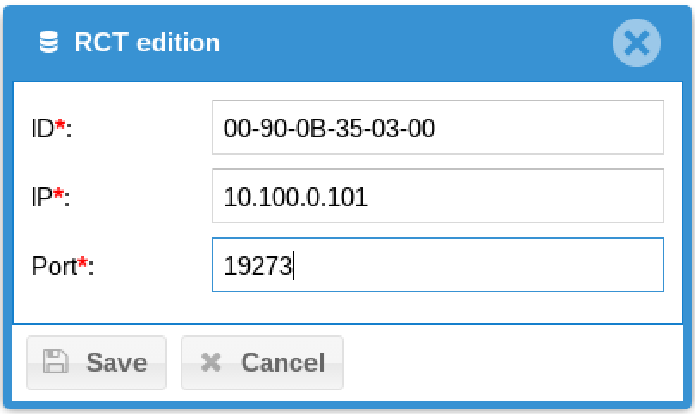
4.1 RCT cluster

The *RCTs* tab is at the heart of the IP-RCT. It allows administrator to synchronize RCTs together. The synchronization will assure data replication on all IP-RCTs for specific collections:

- RCTs: all RCTs share their neighbours with each other. This enables to synchronize a IP-RCT by adding it on any cluster node;
- SPTs: all transmitters are synchronized as well as their state;
- ATS categories: all ATS categories are synchronized;
- Contacts: all contacts are synchronized with all their notification interests;
- Protocols: all protocols instances are synchronized across all IP-RCTs. Global configurations are synchronized and local configuration are left on each IP-RCTs;
- TNIs: all transmitters' paths are synchronized. Upon TNI management, the administrator chooses on which IP-RCT instance the TNI are used;
- AEs: all AEs instances are synchronized. Global configurations are synchronized and local configuration are left on each IP-RCTs;
- Backup: all backup storages are synchronized. Upon backup management, the administrator chooses on which IP-RCT instance backup settings are used;
- Notifications: all notifications settings (email and SMS) are synchronized;
- Users: all users account are synchronized;
- History: the event history is synchronized across all IP-RCTs.

An IP-RCT has a unique ID which identifies it on the cluster. Each IP-RCT listens on one port (19273) and accepts remote connexions. To add an IP-RCT to the cluster, follow these steps:

1. Connect to the first IP-RCT web interface;
2. Go to RCTs tab
   a. Click add;
   b. Input the remote IP-RCT ID, IP and port;
   c. Click save.
3. Connect to the second IP-RCT web interface (the one added at step 2.b);
4. Go to the RCTs tab;
   a. Click add;
   b. Input the first IP-RCT ID, IP and port;
   c. Click save.
5. Monitor the RCT states.



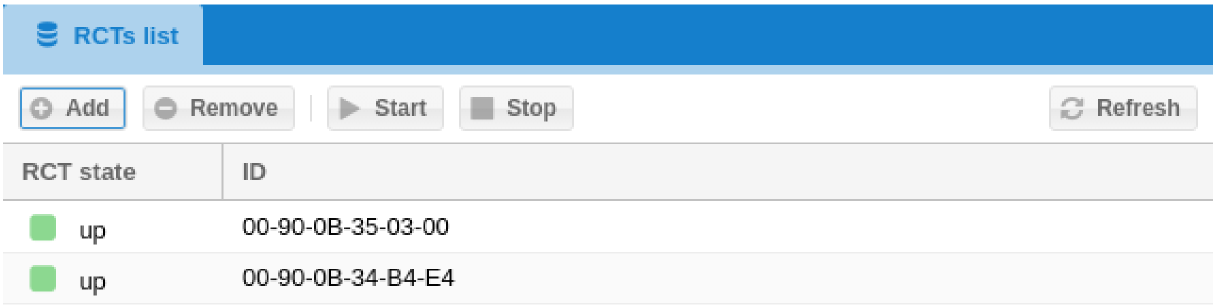
ID*: 00-90-0B-35-03-00

IP*: 10.100.0.101

Port*: 19273

Three states exist for RCTs:

- *Down*: the connection with remote IP-RCT is down;
- *Connected*: the connection with remote IP-RCT is established and not completely synchronized;
- *Up*: the synchronization with remote IP-RCT is finished.



RCT state	ID
🟩 up	00-90-0B-35-03-00
🟩 up	00-90-0B-34-B4-E4

It is possible to start/stop the synchronization engine. By doing so, every connection is dropped or restarted.

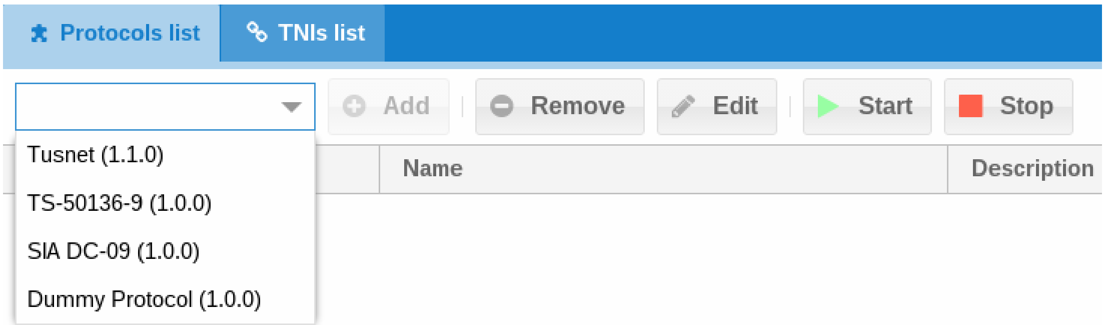
4.2 Protocols and TNI

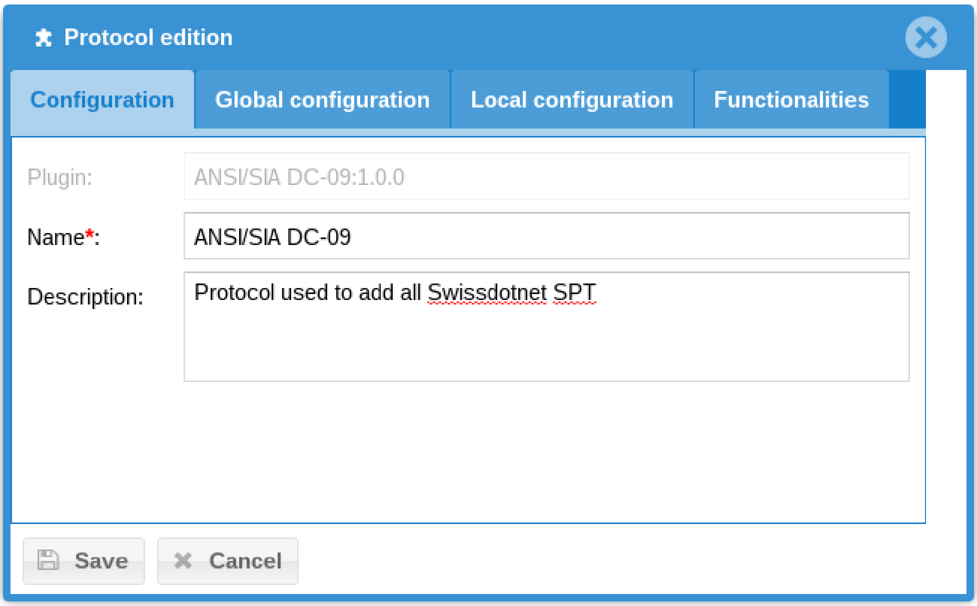
Protocols and TNIs are what SPTs use to communicate with the IP-RCT. Protocols are implementation of alarm transmissions specifications such as SIA-DC09 and TS-50136-9. TNIs are paths on which SPTs communicate.

4.2.1 Protocols list

The IP-RCT scans all available protocols installed on the system. All protocols can be instantiated multiple time on each IP-RCT. Each instance will share global configuration across all IP-RCTs and keep their own local configuration.

To create a new instance, click the combo box and choose the protocol specification as well as protocol version (indicated in parentheses).





Plugin: ANSI/SIA DC-09:1.0.0

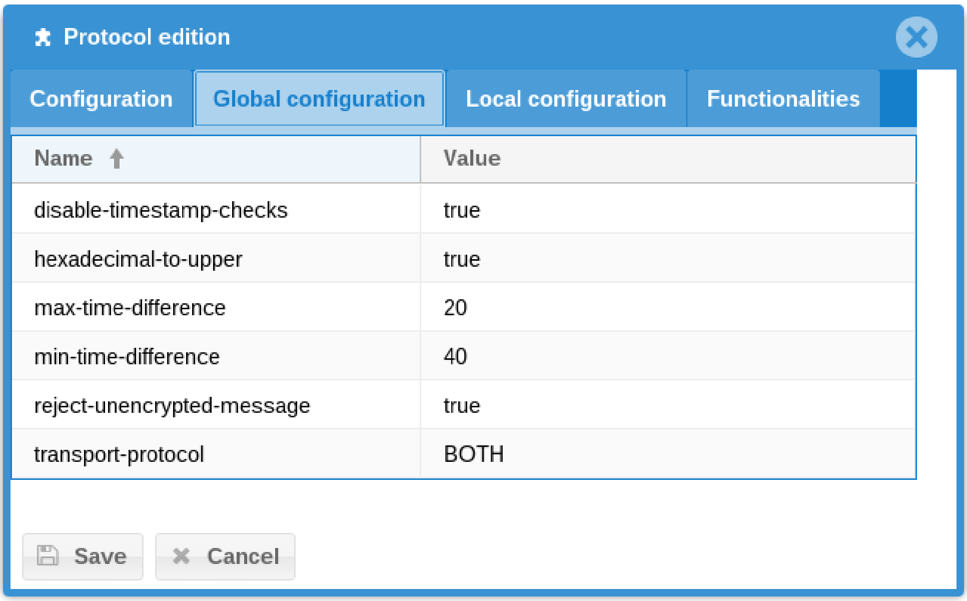
Name*: ANSI/SIA DC-09

Description: Protocol used to add all Swissdotnet SPT

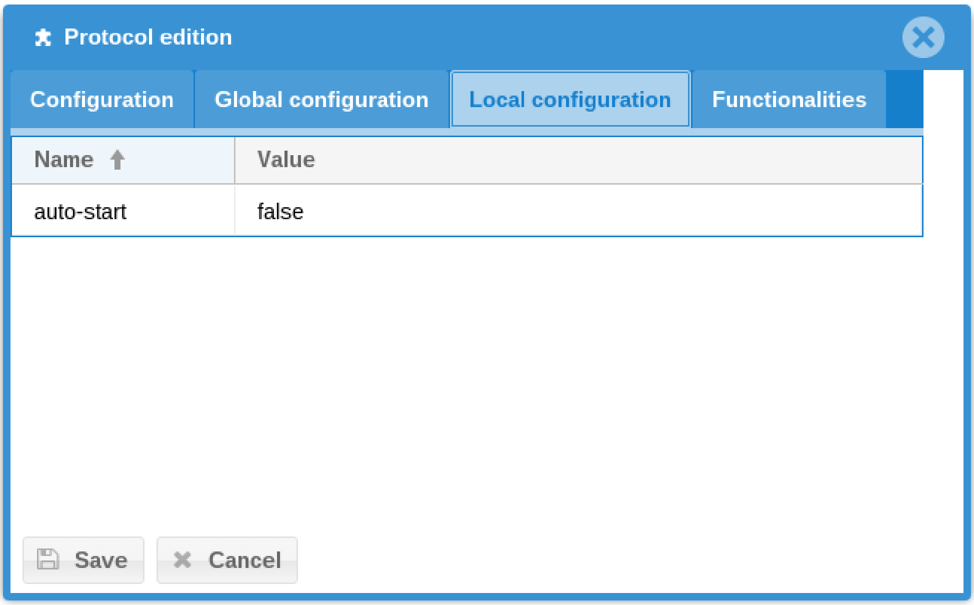
With the protocol selected, press "add", choose a name and a descriptive text and click "save". It automatically synchronizes the new instance across all IP-RCT. Until the protocol is created it is impossible to set global and local configuration. To set global and local configuration up, click the desired protocol and click "edit". The global configuration tab allows to set the protocol instance parameters across all IP-RCT. The local tab sets the protocol instance parameters only on the current IP-RCT.

All protocols have a local property "auto-start" which automatically starts the protocol upon IP-RCT restart. By default, the value is *false* and should be either *false* or *true*.

Refer to additional protocols documentation to know more about configuration parameters.



Name ↑	Value
disable-timestamp-checks	true
hexadecimal-to-upper	true
max-time-difference	20
min-time-difference	40
reject-unencrypted-message	true
transport-protocol	BOTH



Name	Value
auto-start	false

4.2.2 States

By default, all protocols are in state “stopped”. Plugin state are as follows:

- Not found: (displayed as “-“ in plugin state) indicate that the plugin has not been found on the IP-RCT;
- Stopped: the protocol instance is not running; all interactions are not available;
- Started: the protocol listens to interactions and is running properly.

The dashboard displays all IP-RCT in the cluster with their plugin states.

4.2.3 TNIs list

TNIs are path on which SPTs communicate to the IP-RCT. It is characterized by an address on which to listen to and a port. TNIs are associated with protocol and IP-RCT instances.

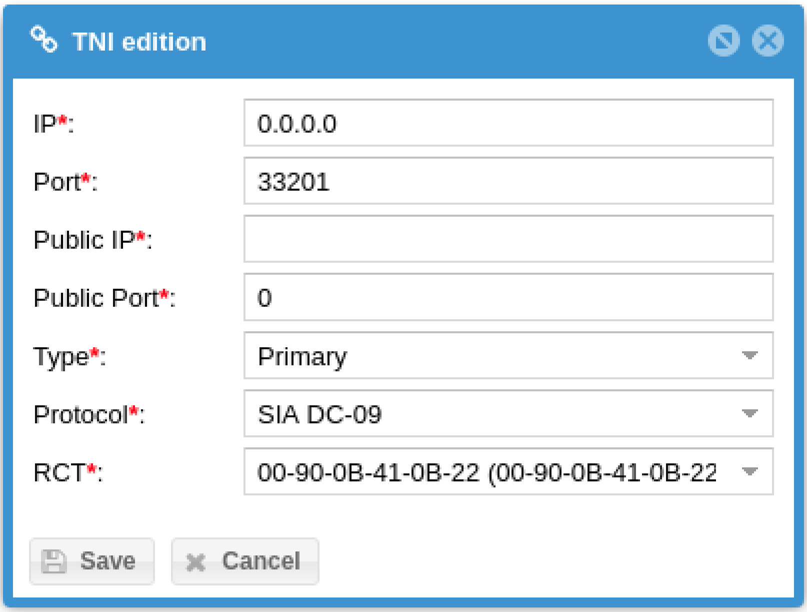
> ⓘ The SDN IP-RCT (software) has no limitation on the number of TNIs it supports, only the hardware running the IP-RCT software will limit the number of TNIs which can be handled.
>
> While running on SDN-7573 we certify up to 20 TNI configured to the RCT.

To manage a TNI, select either “add” or “edit” and fill in the parameters:

- IP: address on which the TNI listens to (usually 0.0.0.0 to listen to all interfaces);
- Port: the TCP/UDP port on which the protocol listens to;
- Public IP: the public address on which the TNI listens to (if NAT is used). This allows commissioning TNI to send the correct configuration to SPTs. It also serves as a documentation for TNIs;
- Public port: the public port on which the protocol listens to (if NAT is used). This is used in addition with public IP and commissioning TNI. It also serves as documentation for TNIs.
- Type: either *primary*, *alternative or commissioning*, defines what the TNI usage. Primary TNIs are usually polled more frequently and connected via wire on the SPT. Alternative TNIs are, frequently, connected through mobile networks on the SPT side and polled less frequently. Depending on the SPT ATS category, a failure to poll is regarded as a path failure. A notification to all AEs is sent. When all TNIs fail to poll, the SPT is treated as ATS failure; Commissioning TNI are used to setup new SPT (protocol dependant).
- Protocol: the protocol instance to which the TNI belongs to;

- RCT: the IP-RCT to which the TNI belongs to.

All polling messages to TNIs are used to compute SPT statistics such as weekly and yearly availability and compliance to ATS category.



TNI edition

IP*:	0.0.0.0
Port*:	33201
Public IP*:	
Public Port*:	0
Type*:	Primary
Protocol*:	SIA DC-09
RCT*:	00-90-0B-41-0B-22 (00-90-0B-41-0B-22

4.3 SPT

The SPT functionalities allows to administrate IP transmitters from the commissioning to states monitoring. The tab also supports ATS category management to match transmitter requirements.

SPTs are defined by their protocol implementation as well as the ATS category associated. Every transmitter also possesses a unique ID which is used by the AE to map each SPT.

> ⓘ The SDN IP-RCT (software) has no limitation on the number of SPTs it supports, only the hardware running the IP-RCT software will limit the number of SPT which can be handled.
>
> While running on SDN-7573 we certify up to 5000 SPT with ATS category DP4 configured to the RCT. More SPT can be achieved for lower ATS categories.

4.3.1 SPTs list

The SPTs list shows all transmitters managed by the IP-RCT with their respective states.

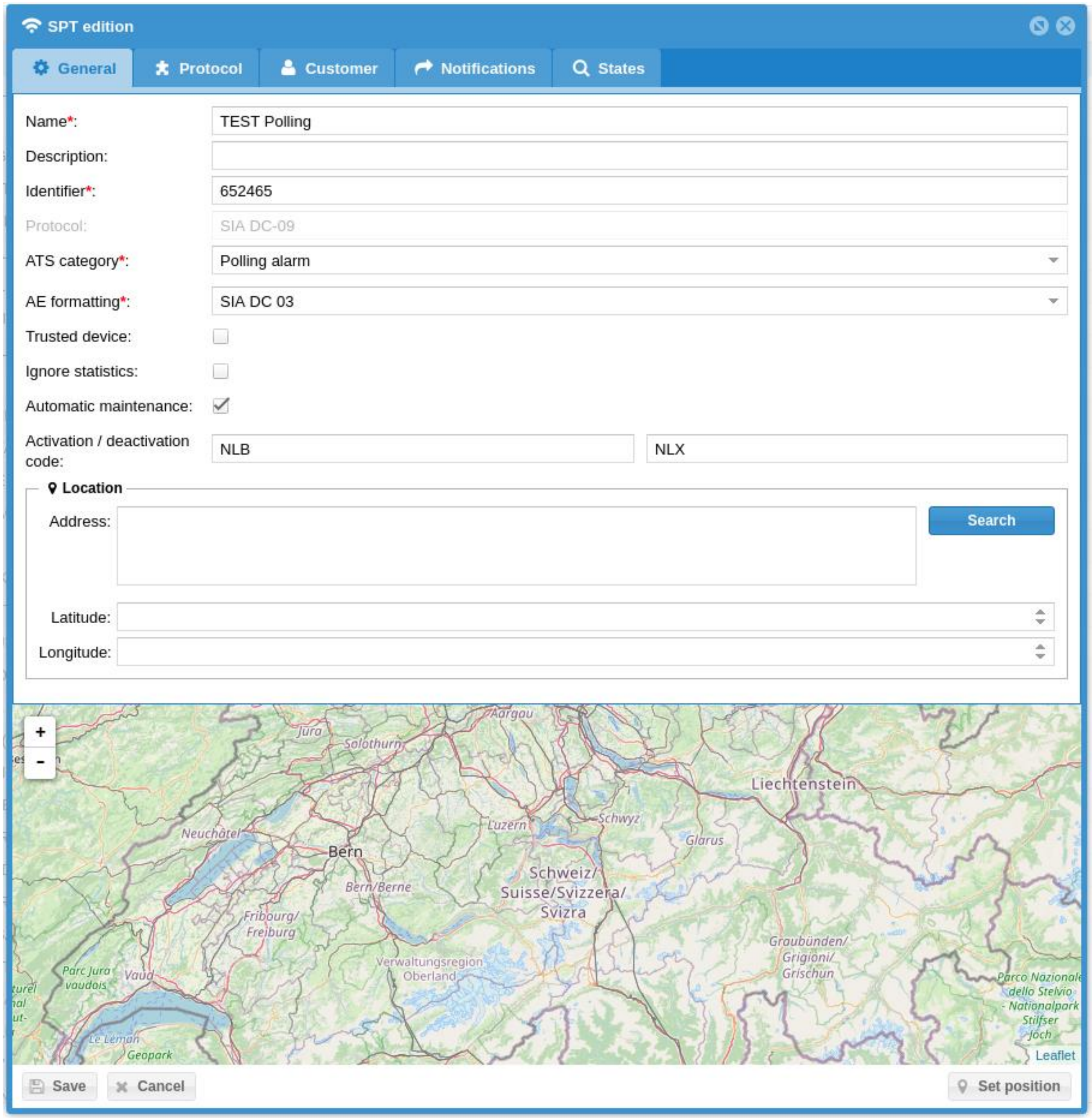
To add a SPT, first select the protocol instance on which to assign the SPT (see 4.2 Protocols and TNI for more information on protocols) and press “Add”. Depending on the protocol, specific fields are shown. Refer to the annex for each protocol available.

4.3.1.1 General

The field in the general tab edition are:

- Name: a string naming the SPT (for instance: SDN192010) which helps identifying the transmitter by the administrator;
- Description: a string describing the SPT (for instance: Rack #12, row #1, Fribourg) which adds more information to the SPT;
- Identifier: the cluster unique identifier used to define the SPT at the AE level. A value is automatically generated with uniqueness guaranteed at the cluster level;
- ATS category: the category by which the SPT is defined (either a standard or a custom category);
- AE formatting: defined the format in which the IP-RCT generated messages are given to the AE (might not be used depending on the AE protocol);
- Trusted device: Whether this SPT allows to transmit other SPTs alarm messages. It serves as some kind of VPN by aggregating alarms on one equipment. Allowing this might cause some identifier overlapping;
- Ignore statistic: Allow to specify, for a given SPT, to ignore it in the statistic computation as it might hinder the ARC performances;
- Automatic maintenance: Whether this SPT support alarm message toggling the maintenance flag or not;
- Activation / deactivation code: Messages the SPT send to activate / deactivate maintenance flag when using automatic maintenance mode.
- Address: specify where the SPT is located and press “Search” to accurately indicate its latitude and longitude (if available online);
- Latitude: the latitude position in form [degrees].[remainder];
- Longitude: the longitude position in similar form as latitude ([degrees].[remainder]).

> ⓘ The SDN IP-RCT supports every ATS categories defined by the EN 50136-1:2012 standard: single path categories from SP1 to SP6 and dual path categories from DP1 to DP4.



Name*:	TEST Polling
Description:	
Identifier*:	652465
Protocol:	SIA DC-09
ATS category*:	Polling alarm
AE formatting*:	SIA DC 03
Trusted device:	□
Ignore statistics:	□
Automatic maintenance:	☑
Activation / deactivation code:	NLB NLX

Location

Address:	
Latitude:	
Longitude:	

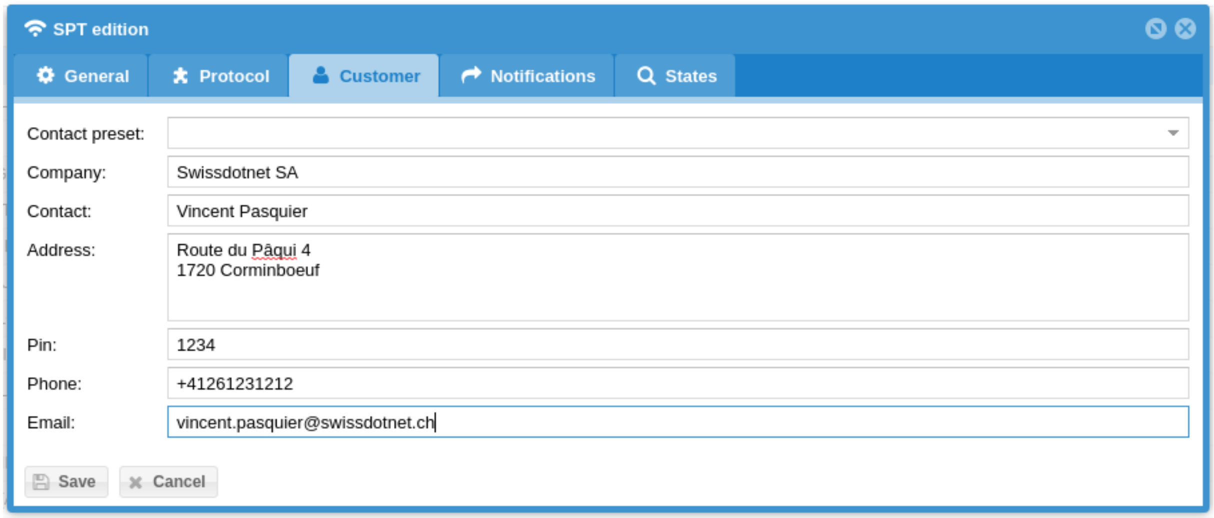
4.3.1.2 Protocol

> ⓘ Plugins may add additional fields. Consult the plugin specific documentation for more information.

4.3.1.3 Customer

The customer form allows to add informative data to the SPT about which customer the SPT is assigned to. The data is appended to all alarms generated by the SPT and may be used by the AE. The fields are:

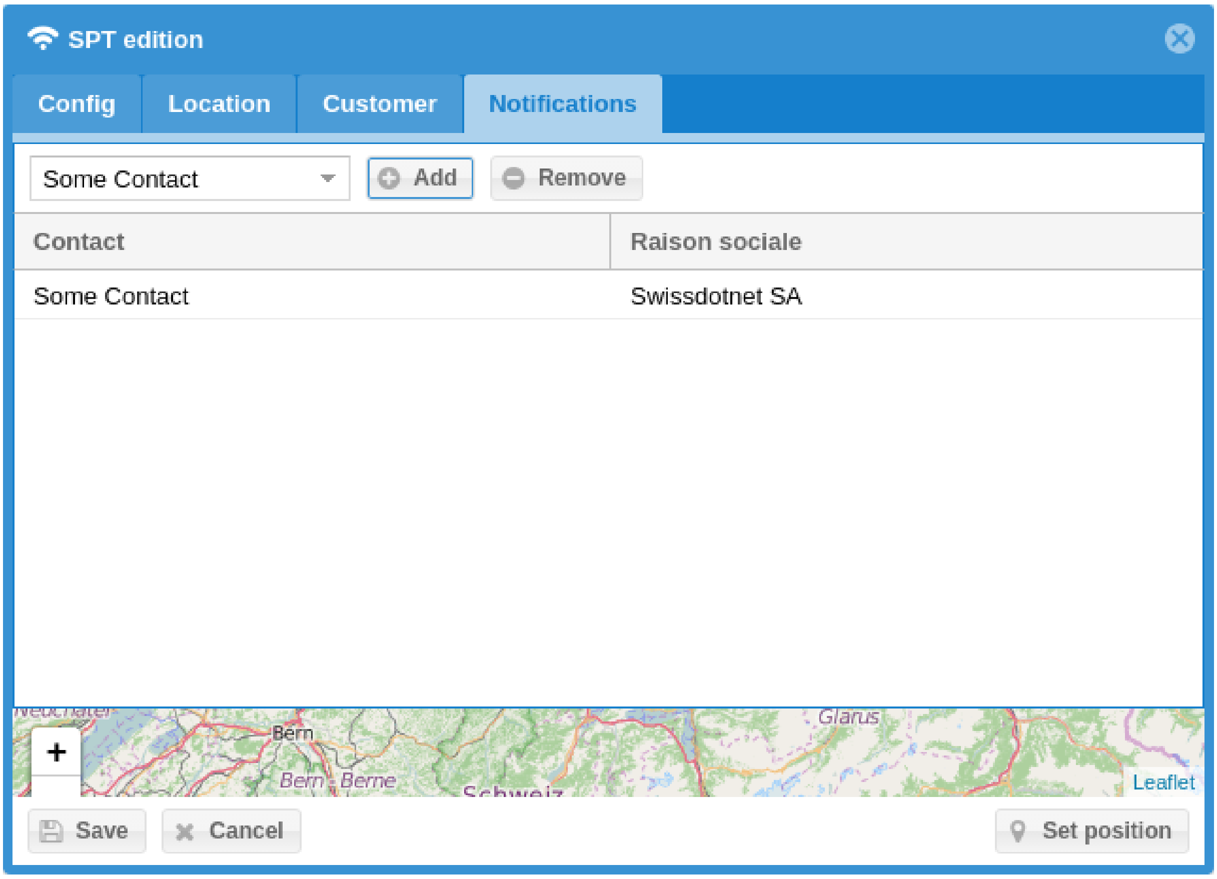
- Contact present: instead of filling all fields below, uses the content of contact specified;
- Company: the company where the SPT is installed;
- Contact: a contact name for the SPT;
- Address: a string to indicate the SPT address;
- Pin: a string which allows customer to identify itself to ARC;
- Phone: a phone number in case to call if a problem may arise;
- Email: an email address to contact the company manager.



Contact preset:	
Company:	Swissdotnet SA
Contact:	Vincent Pasquier
Address:	Route du Pâqui 4 1720 Corminboeuf
Pin:	1234
Phone:	+41261231212
Email:	vincent.pasquier@swissdotnet.ch

4.3.1.4 Notifications

To receive notification upon alarm and path trouble/restoral, it is possible to specify subscriber to each SPT. Select a user from the dropdown and press the “Add” button. The list below shows all subscribers to SPT notifications.

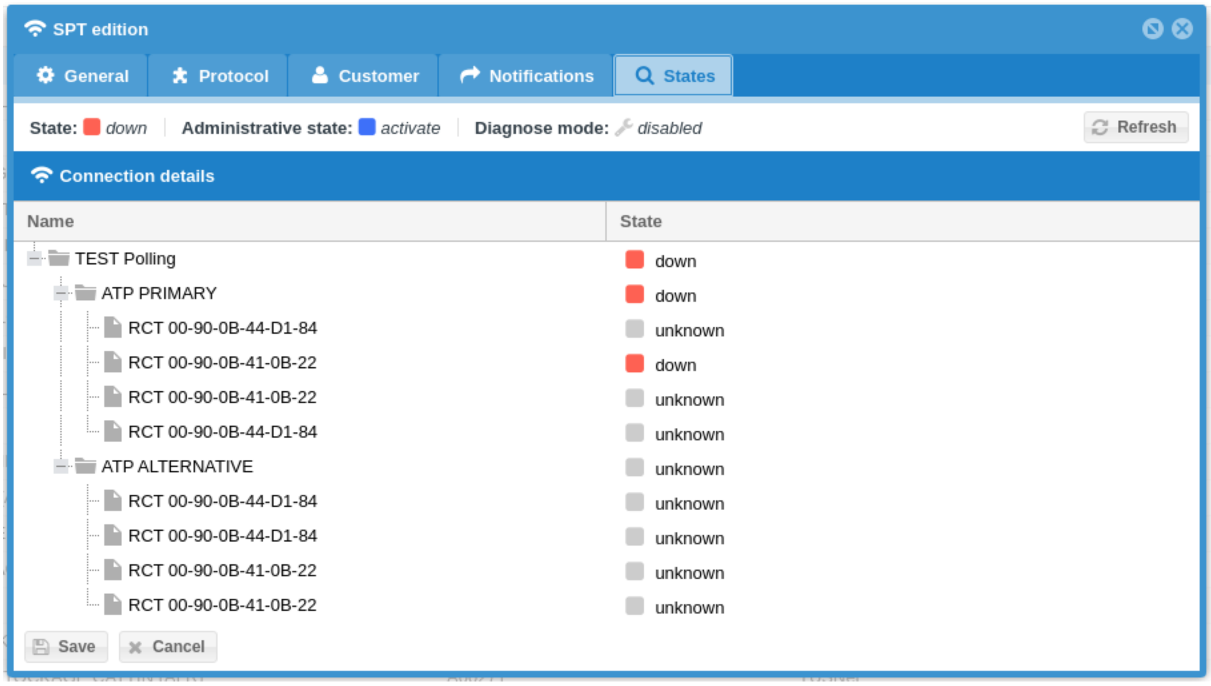


Contact	Raison sociale
Some Contact	Swissdotnet SA

4.3.1.5 States

When editing a SPT, it is possible to get an instant view of its status. It shows :

- Operational state
- Administrative state
- Diagnose mode
- Connection details (ATP states)



State: 🟥 *down* | **Administrative state:** 🟦 *activate* | **Diagnose mode:** *disabled*

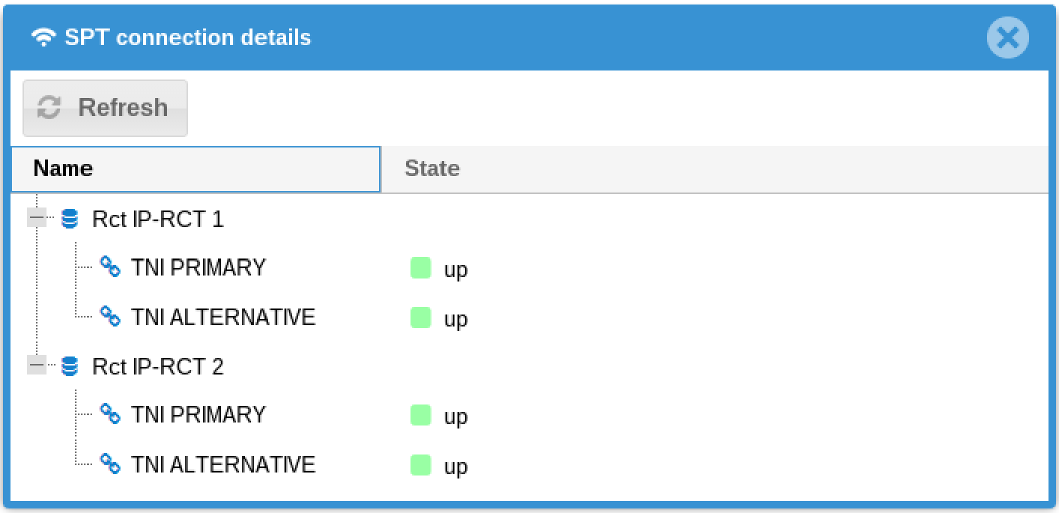
Name	State
TEST Polling	🟥 down
ATP PRIMARY	🟥 down
RCT 00-90-0B-44-D1-84	⬜ unknown
RCT 00-90-0B-41-0B-22	🟥 down
RCT 00-90-0B-41-0B-22	⬜ unknown
RCT 00-90-0B-44-D1-84	⬜ unknown
ATP ALTERNATIVE	⬜ unknown
RCT 00-90-0B-44-D1-84	⬜ unknown
RCT 00-90-0B-44-D1-84	⬜ unknown
RCT 00-90-0B-41-0B-22	⬜ unknown
RCT 00-90-0B-41-0B-22	⬜ unknown

4.3.1.6 Connection states

SPTs administrated by the IP-RCT may have the following connection state:

- *Unknown*: no message received by the IP-RCT;
- *Intermediate*: at least one path is connected and the ATS category requires more than one path to be considered fully operational;
- *Up*: all paths are connected to match ATS category requirements;
- *Down*: all paths are disconnected.

To know more which path is connected, press “Connection details”.



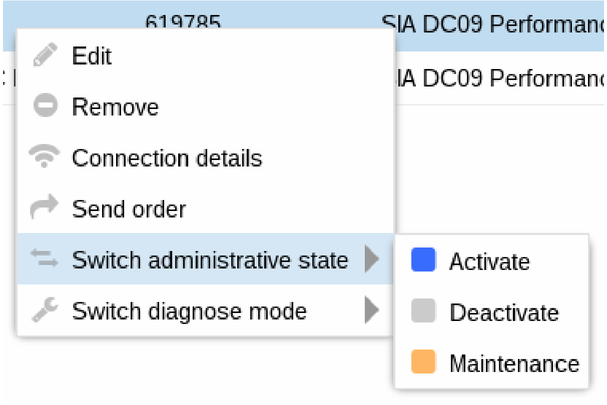
Name	State
Rct IP-RCT 1	
TNI PRIMARY	🟩 up
TNI ALTERNATIVE	🟩 up
Rct IP-RCT 2	
TNI PRIMARY	🟩 up
TNI ALTERNATIVE	🟩 up

4.3.1.7 Administrative states

The administrative states allow the administrator to change the behaviour of SPTs when receiving an alarm or polling messages. The states are:

- *Active*: the SPT is working normally, every alarm and supervision messages are sent to the AE;
- *Maintenance*: the SPT is maintenance, all alarms and polling messages are treated normally but alarms are indicated with the “maintenance” flag;

- *Deactivated*: the SPT is deactivated but still remain in the SPTs for various reasons. All polling messages and alarms are discarded.

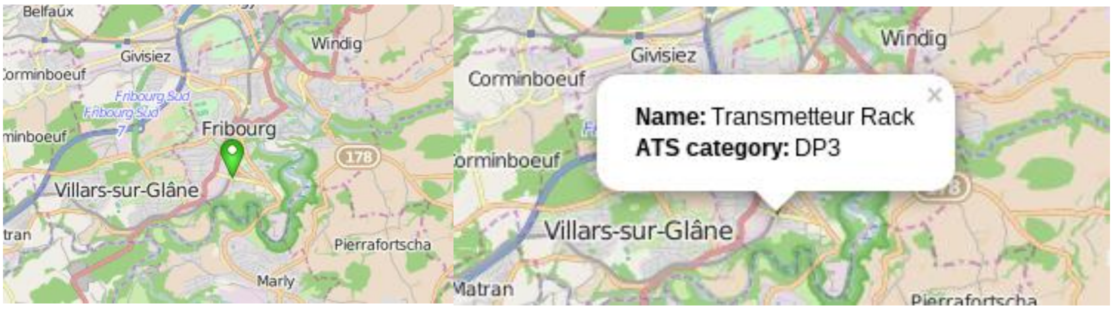


4.3.2 SPTs map

The map displays all located SPTs using a standard map view. The pin shows where the SPT is and its colour the state. When clicking on the pin, it shows the name and the ATS category of the SPT.

The colour codes are:

- *Green*: Up state
- *Yellow*: intermediate state
- *Red*: down state
- *Orange*: maintenance state
- *Grey*: either deactivated or unknown state



Name: Transmetteur Rack
ATS category: DP3

4.3.3 ATS categories list

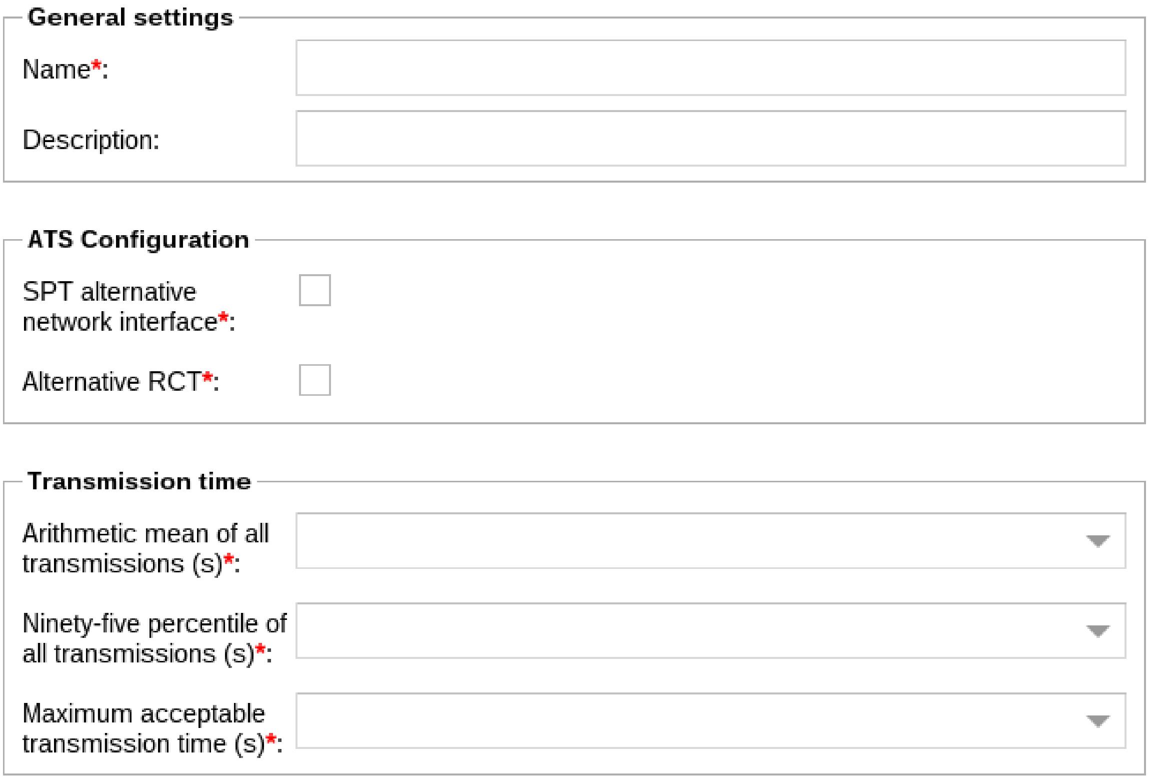
ATS categories defined the rate at which SPTs must send supervision messages as well as other configuration (i.e. redundancy, statistics,). By default, the IP-RCT has 6 single path and 4 dual path categories (standard IEC 60839-5-1:2014) and an unmanaged category which are read only.

The unmanaged category allows to add uncertified transmitters or transmitters which may lack full features when it comes to alarm transmission.

> ⓘ The form to add/edit ATS category requires a lot of user input. It is advised to add a category with knowledge on each parameter beforehand.

The settings to create/edit an ATS category are:

- General settings
  - Name: the category name (printed by system);
  - Description: a small description for the category;
- ATS configuration
  - SPT Alternative network interface: whether the system uses an alternative network interface or not (alternative path);
  - Alternative RCT: whether the system uses an alternative RCT or not;
- Transmission time (refer to 5.3 Statistics and performances for more information)
  - Arithmetic mean of all transmissions: mean of all alarm transmission time (in seconds) received by the RCT. The mean must be below this value otherwise the SPT fails ATS category checks;
  - Ninety-five percentile of all transmissions: the 95% of all transmission time (in seconds) must be below this value otherwise the SPT fails ATS category checks;
  - Maximum acceptable transmission time: the maximum transmission time (in seconds) for each SPT. All transmission time must be below this value otherwise the SPT fails ATS category checks;



General settings

Name*:

Description:

ATS Configuration

SPT alternative network interface*: □

Alternative RCT*: □

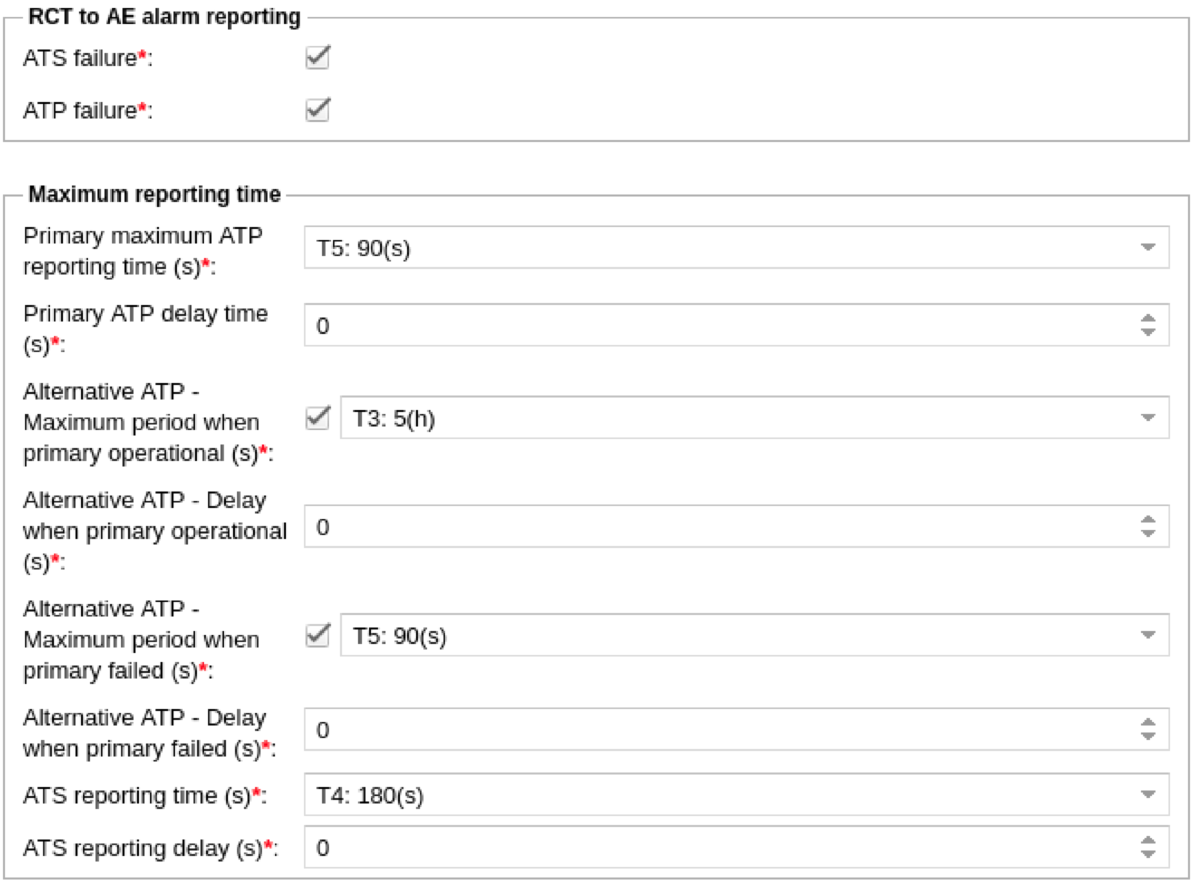
Transmission time

Arithmetic mean of all transmissions (s)*:

Ninety-five percentile of all transmissions (s)*:

Maximum acceptable transmission time (s)*:

- RCT to AE alarm reporting
  - ATS failure: whether the IP-RCT must send ATS failures or not to the AE;
  - ATP failure: whether the IP-RCT must send ATP failures or not to the AE;
- Maximum reporting time (refer to 5.3 Statistics and performances for more information)
  - Primary ATP reporting time: primary path maximum polling time (in seconds). Upon exceeding, the RCT reports an alarm if required (certain protocol count alarm as supervision messages, consult protocol annexes for more information);
  - Primary ATP delay time: how long to wait for the ATP fault to be sent to AE. The log entry will be generated after primary ATP reporting time but sent to AE after delay.
  - Alternative ATP
    - Maximum period when primary operational: period when the primary path is connected. Upon exceeding, the RCT reports an alarm if required (can be disabled);
    - Delay when primary operational: how long to wait for the ATP fault to be sent to AE. The log entry will be generated after alternative ATP reporting time but sent to AE after delay;
    - Maximum period when primary failed: period when the primary path is disconnected. Upon exceeding, the RCT reports an alarm if required. This allow to effectively treat alternative path as primary when the primary is down (can be disabled);
    - Delay when primary failed: Similar to delay when primary operational;
  - ATS reporting time: the period after which the IP-RCT reports an ATS failure when all paths are in error;
  - ATS reporting delay: how long to wait for the ATS fault to be sent to AE. The log entry will be generated after ATS reporting time but sent to AE after delay.



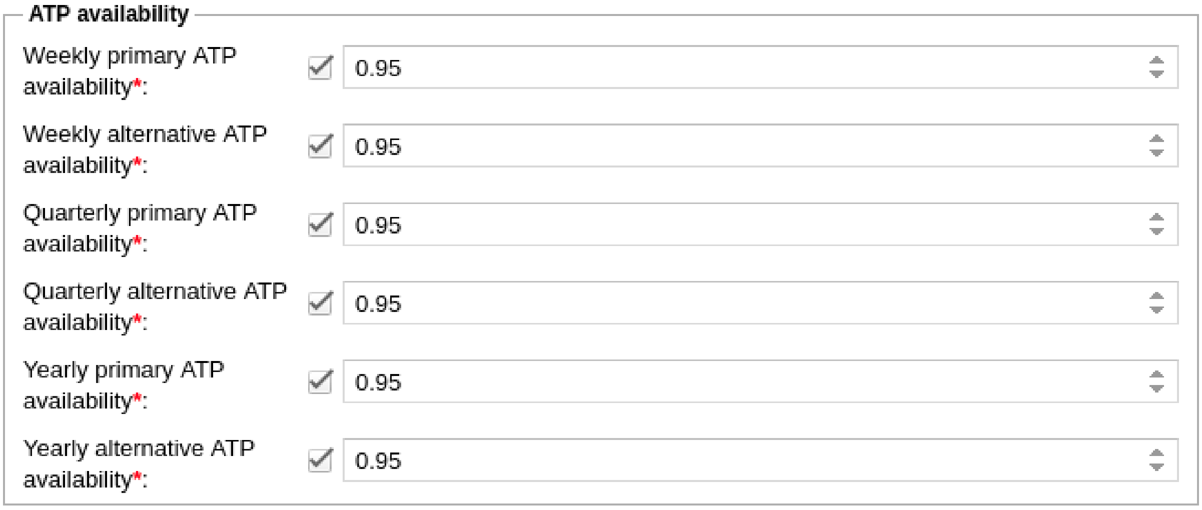
RCT to AE alarm reporting

ATS failure*:	☑
ATP failure*:	☑

Maximum reporting time

Primary maximum ATP reporting time (s)*:	T5: 90(s)
Primary ATP delay time (s)*:	0
Alternative ATP - Maximum period when primary operational (s)*:	☑ T3: 5(h)
Alternative ATP - Delay when primary operational (s)*:	0
Alternative ATP - Maximum period when primary failed (s)*:	☑ T5: 90(s)
Alternative ATP - Delay when primary failed (s)*:	0
ATS reporting time (s)*:	T4: 180(s)
ATS reporting delay (s)*:	0

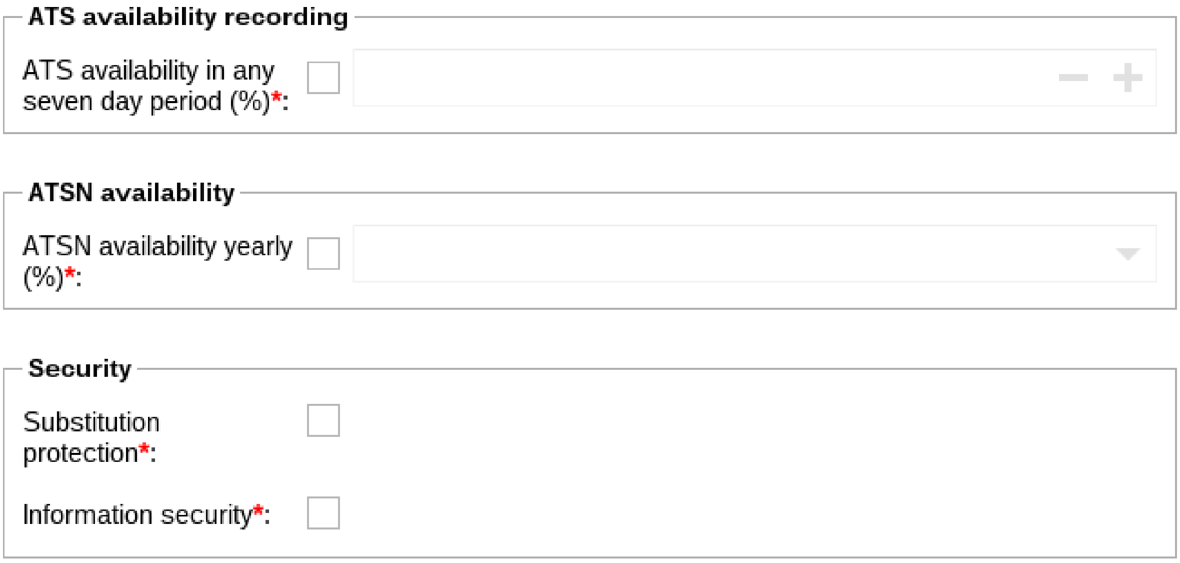
- ATP availability
  - Weekly primary ATP availability: Availability (from 1 to 0) for primary ATP during a week
  - Weekly alternative ATP availability: Availability (from 1 to 0) for alternative ATP during a week
  - Quarterly primary ATP availability: Availability (from 1 to 0) for primary ATP during a quarter
  - Quarterly alternative ATP availability: Availability (from 1 to 0) for alternative ATP during a quarter
  - Yearly primary ATP availability: Availability (from 1 to 0) for primary ATP during a year
  - Yearly alternative ATP availability: Availability (from 1 to 0) for alternative ATP during a year



ATP availability

Weekly primary ATP availability*:	☑	0.95
Weekly alternative ATP availability*:	☑	0.95
Quarterly primary ATP availability*:	☑	0.95
Quarterly alternative ATP availability*:	☑	0.95
Yearly primary ATP availability*:	☑	0.95
Yearly alternative ATP availability*:	☑	0.95

- ATS availability recording (refer to 5.3 Statistics and performances for more information)
  - ATS availability in any seven-day period: availability percentage using all ATS failure/restore to compute an availability statistic;
- ATSN availability (refer to 5.3 Statistics and performances for more information)
  - ATSN availability yearly: availability for a SPT for a yearly period (similar to ATS availability recording)
- Security
  - Substitution security: whether the category must use substitution security or not (i.e. challenges, timestamps,);
  - Information security: whether the category must cipher messages or not.



ATS availability recording

ATS availability in any seven day period (%)*: □

ATSN availability

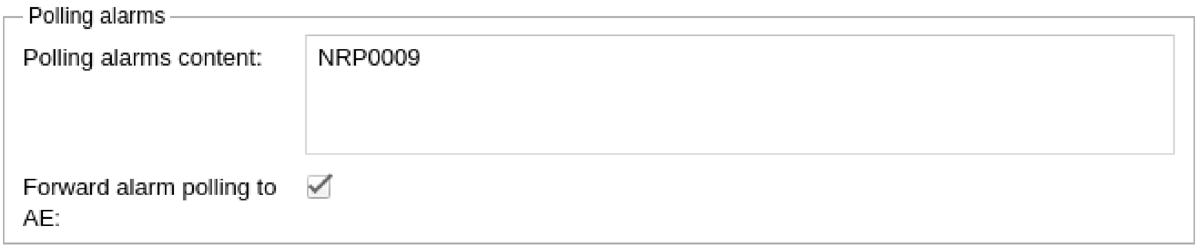
ATSN availability yearly (%)*: □

Security

Substitution protection*: □

Information security*: □

- Polling alarms
  - Polling alarms content: Each line can contain an alarm data which might be handled as a polling message. When an alarm is received, with the content matching one of the lines, the alarm will not be stored in the events logs and forwarded to the AE. The alarm will be acknowledged automatically if the SPT is available;
  - Forward alarm polling to the AE: When this flag is enabled, the IP-RCT will transfer the polling alarm to the AE but still not store it in the events logs.



Polling alarms

Polling alarms content: NRP0009

Forward alarm polling to AE: ☑

ⓘ ANSI/SIA DC-09-2013 offers both substitution protection and information security:

- *Substitution protection* is provided by timestamping every message. If a message has a difference of more than 1 minute, the message will be declined (5.5.1.9. Timestamp DC-09-2013)
- *Information security* is provided by AES CBC 128, 192, 256 bits ciphering (5.4 Encryption).

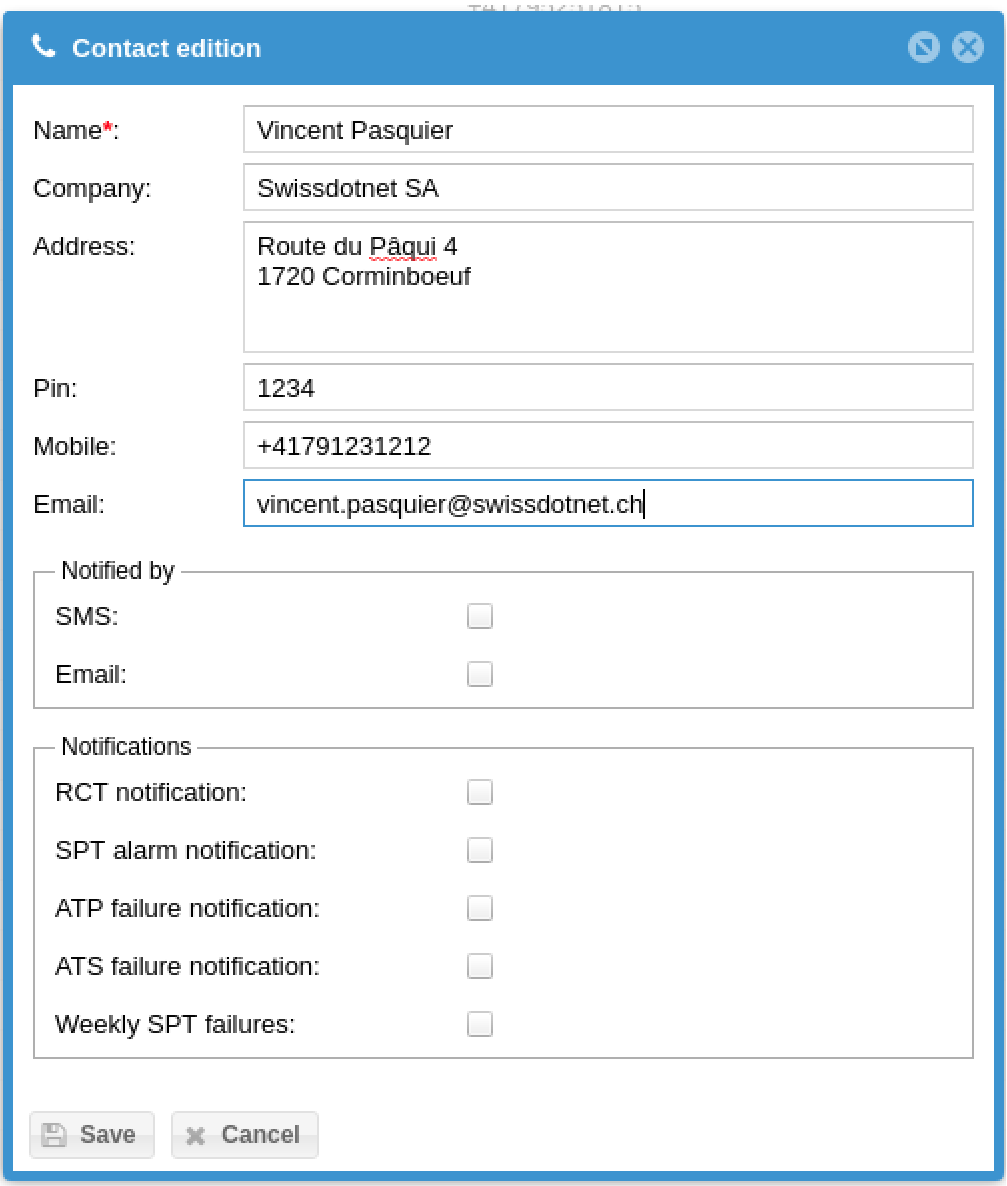
ⓘ EN:50136-9 offers both substitution protection and information security:

- *Substitution protection* is provided by doing an initial commissioning which defines a master connection set only known by the equipment (i.e. SPT and RCT). Then a session key is decided upon connection which is changed throughout the session. Each message sent increase a counter chosen randomly at connection initialization which protects from replay attacks.
- *Information security* is provided by AES CBC 128, 256 bits ciphering.

4.4 Contacts

Contacts allow IP-RCT to send notifications either by SMS and/or email. Can also be used to announce the alarm to the SPT customer. To add/edit a contact, fill the fields:

- Name: Contact first name + last name;
- Company: the contact company;
- Address: the contact address (supports multiline);
- Pin: a string which allows customer to identify itself to ARC;
- Mobile: mobile phone number (used to send SMS);
- Email: email address (used to send emails);
- Notified by
  - SMS: whether to send SMS or not;
  - Email: whether to send emails or not;
- Notifications
  - RCT: whether to send RCT notification to user or not (could generate lot of messages): NTP failure/restore; AE failure/restore; Network failure/restore; RCT synchronization failure/restore; RCT reset/reboot; Software update; Backup failure/success;
  - SPT alarms: whether to send SPT alarm to user or not;
  - ATP: whether to send ATP failure/restore to user or not (if generated, based on ATS category);
  - ATS: whether to send ATS failure/restore to user or not (if generated, based on ATS category).



Name*:	Vincent Pasquier
Company:	Swissdotnet SA
Address:	Route du Pâqui 4 1720 Corminboeuf
Pin:	1234
Mobile:	+41791231212
Email:	vincent.pasquier@swissdotnet.ch

Notified by

SMS: □

Email: □

Notifications

RCT notification: □

SPT alarm notification: □

ATP failure notification: □

ATS failure notification: □

Weekly SPT failures: □

4.5 Annunciation Equipment

Annunciation equipment (AE) are higher level software which shows alarms to operators and allow them to react. Usually it stores the customer information, alarm contacts, reaction plan and all information regarding a connection.

Most annunciation equipment uses their own protocol to receive alarms and notifications. The AE integration is done in two possible ways:

1. the AE protocol is implemented by Swissdotnet and managed internally;
2. the AE itself connects to the Swissdotnet public API to retrieve alarms and notifications.

> ⓘ Contact Swissdotnet if interested in implementing your own AE by using the public API. A non-disclosure agreement will be asked in exchange.

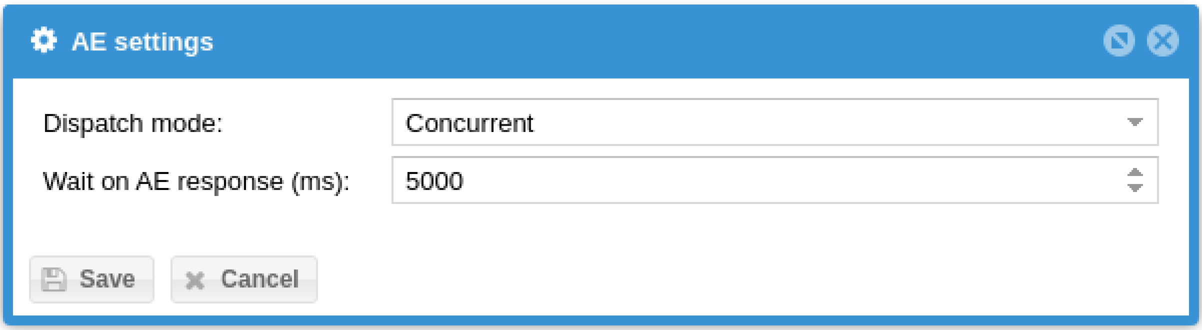
> ⓘ The SDN IP-RCT (software) has no limitation on the number of AEs it supports, only the hardware running the IP-RCT software will limit the number of AE which can be handled.
>
> While running on SDN-7573 we certify up to 10 AE connected simultaneously to the RCT.

4.5.1 Settings

General AE settings allows to manage the behavior of the whole AEs instances.

Two dispatch modes can be used:

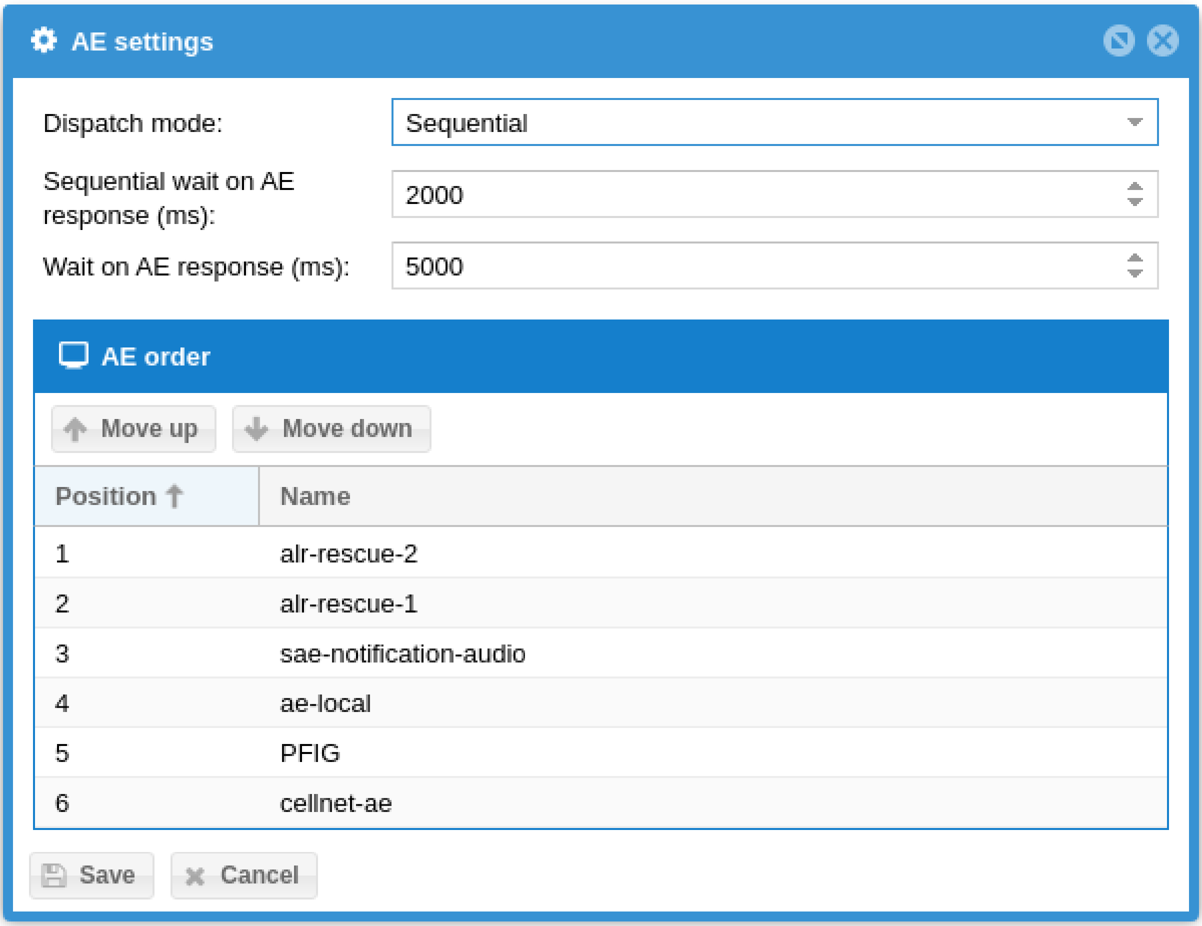
- Concurrent: where all AE receive the alarm concurrently and can all answer the alarm;
- Sequential: where the sequence of alarm is predetermined based on order. The first AE which acknowledge the alarm will stop the AE chain. If the alarm is refused or not handled, the next AE is contacted.



AE settings

Dispatch mode: Concurrent

Wait on AE response (ms): 5000



AE settings

Dispatch mode: Sequential

Sequential wait on AE response (ms): 2000

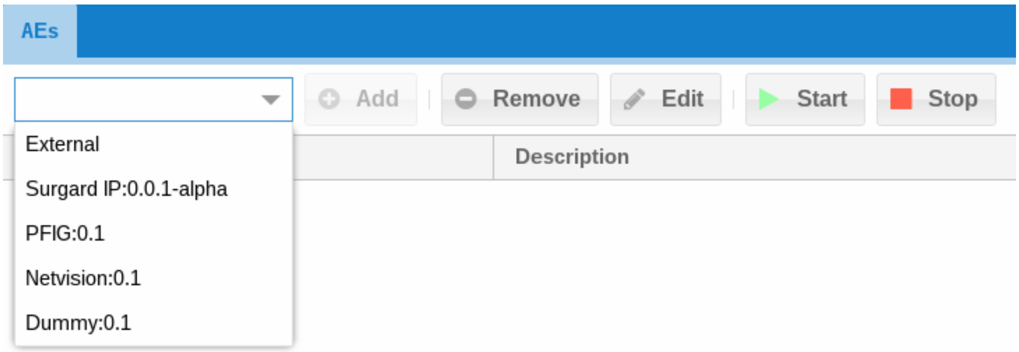
Wait on AE response (ms): 5000

AE order

Position ↑	Name
1	alr-rescue-2
2	alr-rescue-1
3	sae-notification-audio
4	ae-local
5	PFIG
6	cellnet-ae

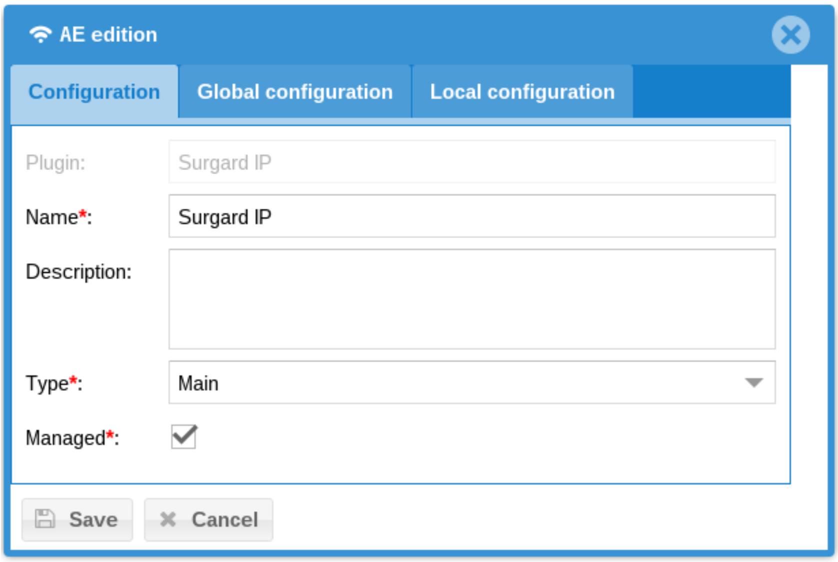
4.5.2 Administration

To add an AE, choose from the combo box which protocol to use. If the protocol is installed on the IP-RCT, it will show up as an entry with its name. It is always possible to add an "External" AE which uses the Swissdotnet public API.



An AE has, upon management, 4 parameters to specify:

- Name: the name by which the AE announce itself to the IP-RCT public API;
- Description: a string which indicates the AE purpose;
- Type: either “Main” or “Observer”
    - Main: standard AE which may acknowledge or refuse alarms;
    - Observer: AE which cannot acknowledge alarms but observes them (if any main AE is connected). It can be used to, for instance, act upon specific alarm reception without responding to the SPT. Once all Main AE are disconnected, the observer is allowed to acknowledge incoming alarms.
- Managed: defined whether the AE is monitored or not. Managed AEs will send SMS/Email upon heartbeat failure or plugin stop.



Plugin: Surgard IP

Name*: Surgard IP

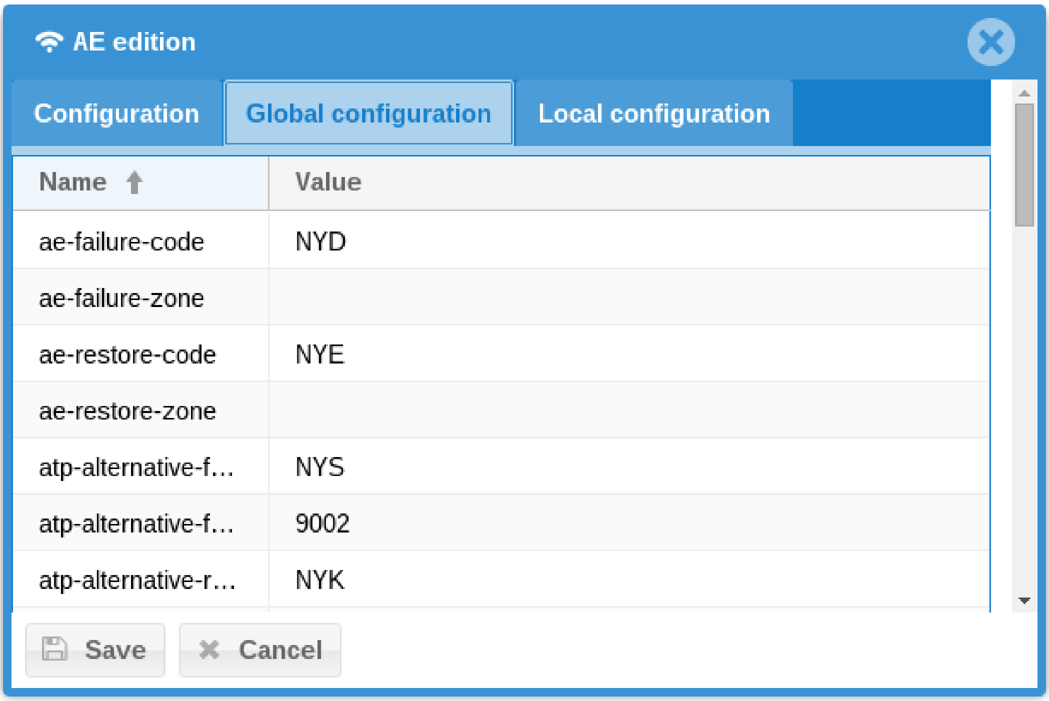
Description:

Type*: Main

Managed*: ☑

For AE implemented by Swissdotnet, the global and local configuration allows to input protocol specifics values. Local configuration is not shared across the RCT cluster as for global configuration, every value is synchronized with all IP-RCT. For more information, refer to the additional AEs documentation provided.

All protocols have a local property “auto-start” which automatically starts the protocol upon IP-RCT restart. By default, the value is *false* and should be either *false* or *true*.



Name	Value
ae-failure-code	NYD
ae-failure-zone	
ae-restore-code	NYE
ae-restore-zone	
atp-alternative-f…	NYS
atp-alternative-f…	9002
atp-alternative-r…	NYK

4.5.3 States

Similar to protocols, AEs have various plugin states:

- *Not found*: (displayed as "-" in plugin state) indicate that the AE plugin has not been found on the IP-RCT;
- *Stopped*: the AE instance is not running; all interaction is not available;
- *Started*: the AE listens to interactions and is running properly;
- *External*: the AE uses the IP-RCT public API to receive alarms and notifications.

In addition to plugin state, a heartbeat task checks each AE for its annunciation. Since a plugin may work properly but the communication failing, the state would be "Started" but its heartbeat state "Down" to indicate a communication failure. Heartbeat states are:

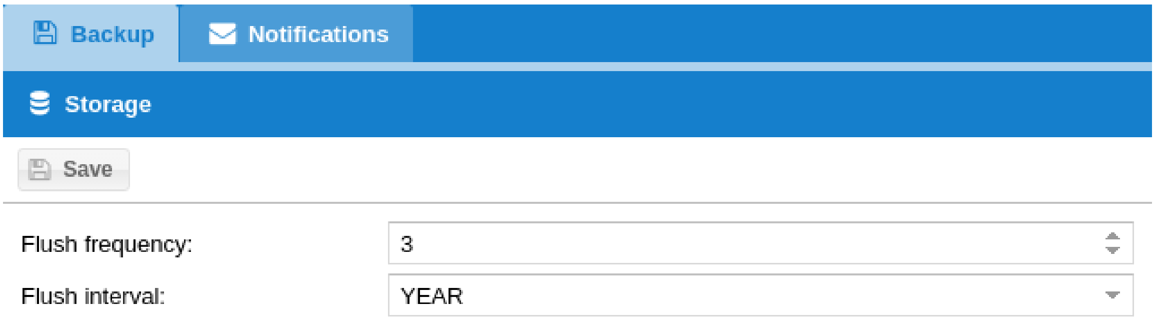
- *Unknown*: the AE has still not contacted the IP-RCT to retrieve alarms or notifications;
- *Down*: the AE has contacted at least once the IP-RCT but failed to re-contact it after a specific amount of time;
- *Up*: the AE has contacted at least once the IP-RCT and is still contacting it.

The dashboard (see 5.1) displays all IP-RCT in the cluster with their AE states and heartbeat states.

4.6 Storage

Storage options allows to backup configuration and event history on a remote server. The storage options specify how long event history are kept. By default, 3 years of event history is kept locally.

> ⓘ By allowing normative log to be stored externally (which has enough storage capacity), we allow a log endurance of 3 years at least. On the SDN IP-RCT we designed the database to handle up to 5000 events every hours for 3 years.



Flush frequency: 3

Flush interval: YEAR

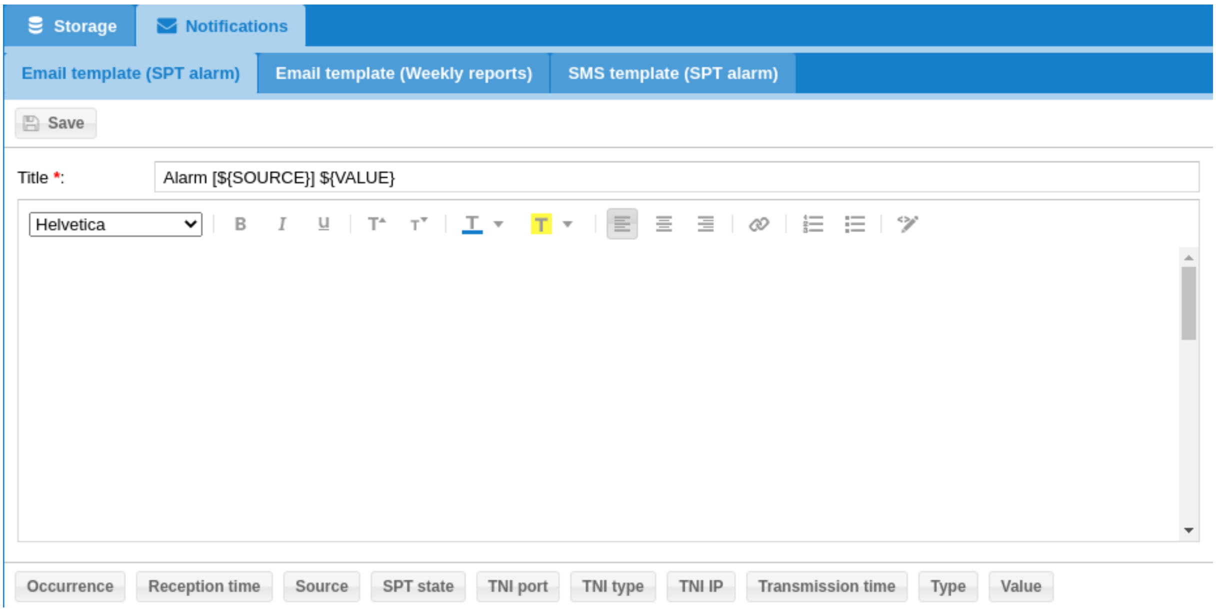
4.7 Notifications

Notifications allow to receive alerts about certain RCT parts and even SPT states or alarms. The alerts are done by the IP-RCT cluster on either a configured email and/or phone by SMS.

4.7.1 Templates

Both Email and SMS messages for SPT alarms can be modified. Special variables allow to create dynamic messages for SPT alarms. Possible variables are:

- Occurrence: when the alarm occurred on SPT;
- Reception time: when the alarm is received by the RCT;
- Source: the SPT identifier;
- SPT state: the state in which the SPT is when sending alarm;
- TNI port: the port on which the message is received;
- TNI type: either PRIMARY or ALTERNATE;
- TNI IP: the IP address on which the message is received;
- Transmission time: the time it arrived on the IP-RCT;
- Type: ALARM;
- Value: the actual alarm payload.



Title *: Alarm [${SOURCE}] ${VALUE}

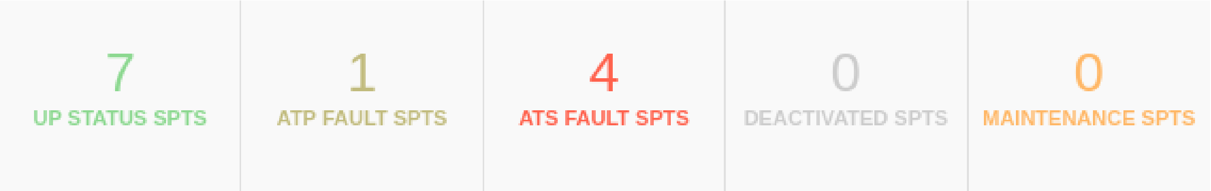
5 Working with the RCT

ⓘ The steps described below explains how to work with the IP-RCT either clustered or non-clustered. The following sections are not in specific order.

5.1 Dashboard

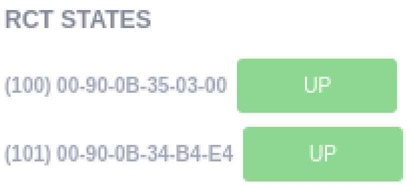
The dashboard gives, in one glance, knowledge of the whole IP-RCT cluster general status. The following information are available:

- Top
  - SPT connection states is displayed by showing a count of each state;



7	1	4	0	0
UP STATUS SPTS	ATP FAULT SPTS	ATS FAULT SPTS	DEACTIVATED SPTS	MAINTENANCE SPTS

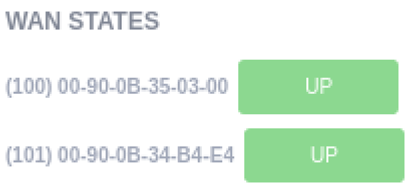
- Centre
  - RCT states shows the cluster state from the current IP-RCT point of view;



RCT STATES

(100) 00-90-0B-35-03-00	UP
(101) 00-90-0B-34-B4-E4	UP

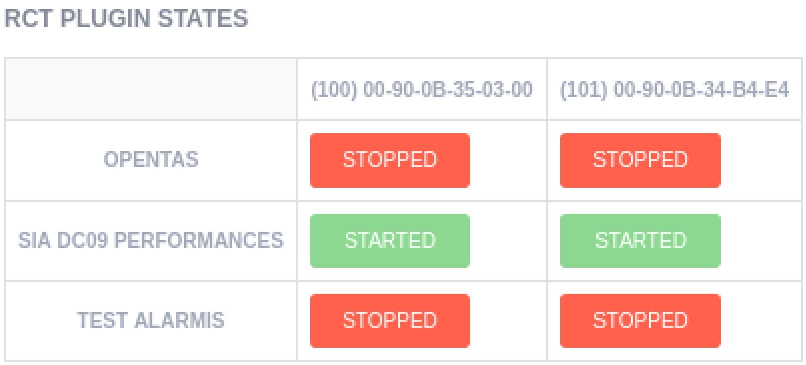
  - WAN states shows the Internet connection monitoring state for each IP-RCT;



WAN STATES

(100) 00-90-0B-35-03-00	UP
(101) 00-90-0B-34-B4-E4	UP

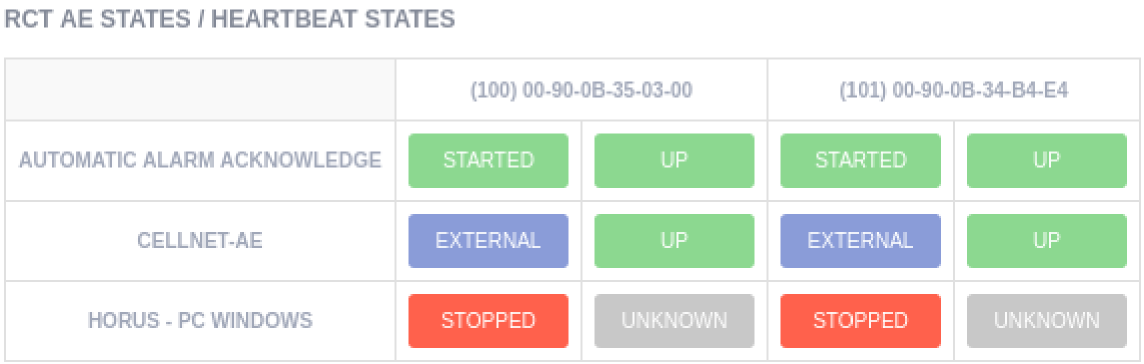
- Bottom
  - RCT Plugin states displays the current IP-RCT states for each protocol module;



RCT PLUGIN STATES

	(100) 00-90-0B-35-03-00	(101) 00-90-0B-34-B4-E4
OPENTAS	STOPPED	STOPPED
SIA DC09 PERFORMANCES	STARTED	STARTED
TEST ALARMIS	STOPPED	STOPPED

  - RCT AE states presents all AE plugin states as well as heartbeat monitoring state;



RCT AE STATES / HEARTBEAT STATES

	(100) 00-90-0B-35-03-00		(101) 00-90-0B-34-B4-E4	
AUTOMATIC ALARM ACKNOWLEDGE	STARTED	UP	STARTED	UP
CELLNET-AE	EXTERNAL	UP	EXTERNAL	UP
HORUS - PC WINDOWS	STOPPED	UNKNOWN	STOPPED	UNKNOWN

5.2 Users and Access Levels

> ⓘ Users and access levels follows the EN-50136-3 (6.2) standard regarding users and access levels.

IP-RCT software users can be managed in the *Users* view, which includes the ability to create, edit and delete application users.

To add/modify a user, the parameters are:

- Login: user account used to authenticate;
- Password: authentication password;
- Access level: specifies all functionalities the account may access (see table below);
- Name: used to indicate the user name.

The access level determines which application features the user can use as shown in the table below:

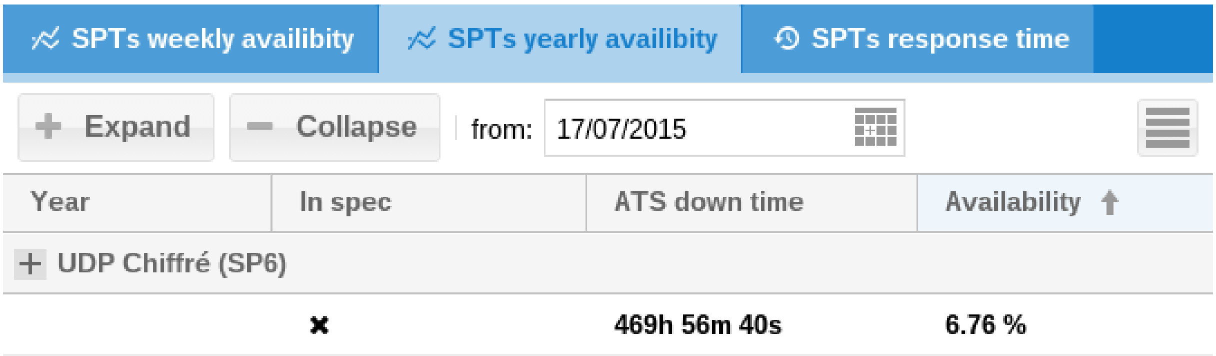
Access level	Guest		Alarm receiver		Admin		Commissioner		Supervisor	
Access type	Visualization	Administration	Visualization	Administration	Visualization	Administration	Visualization	Administration	Visualization	Administration
AE	-	-	-	-	✓	-	✓	-	✓	✓
Alarm protocols	-	-	-	-	✓	-	✓	-	✓	✓
ATS categories	-	-	-	-	✓	-	✓	✓	✓	✓
Contacts	-	-	-	-	✓	-	✓	✓	✓	✓
Dashboard	✓	■	-	■	✓	■	✓	■	✓	■
Event history	-	■	-	■	✓	■	✓	■	✓	■
Notification	-	-	-	-	✓	-	✓	✓	✓	✓
RCT	-	-	-	-	✓	-	✓	-	✓	✓
Remote RCTs	-	-	-	-	-	-		-	✓	✓
SPTs	-	-	-	-	✓	-	✓	✓	✓	✓
SPT connection states	-	■	-	■	✓	■	✓	■	✓	■
SPT Diagnose mode	-	-	-	-	✓	-	✓	✓	✓	✓
Statistics	-	■	-	■	✓	■	✓	■	✓	■
Storage	-	-	-	-	✓	-	✓	-	✓	✓
System monitoring	✓	■	-	■	✓	■	✓	■	✓	■
System performance	✓	■	-	■	✓	■	✓	■	✓	■

TNIs	-	-	-	-	-	-	-	-	✓	✓
Access type	Visualization	Administration	Visualization	Administration	Visualization	Administration	Visualization	Administration	Visualization	Administration
Access level	Guest		Alarm receiver		Admin		Commissioner		Supervisor	

5.3 Statistics and performances

During its usage, the IP-RCT collects information to compute statistics and monitor performance. SPT centric, the *Statistics* view shows three tabs with the following statistics:

- *SPTs weekly availability*: Based on SPT ATS category, compute their weekly availabilities to determine whether they match the specification or not;
- *SPTs yearly availability*: Similar to weekly availability but with year time period;
- *SPTs response time*: Computes the mean, 95 percentile and maximum alarm response time for all SPTs.

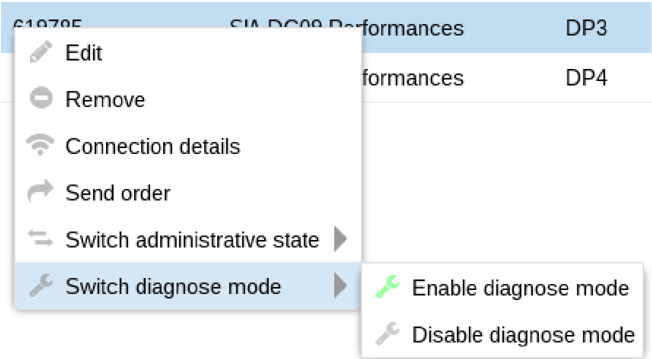


from: 17/07/2015

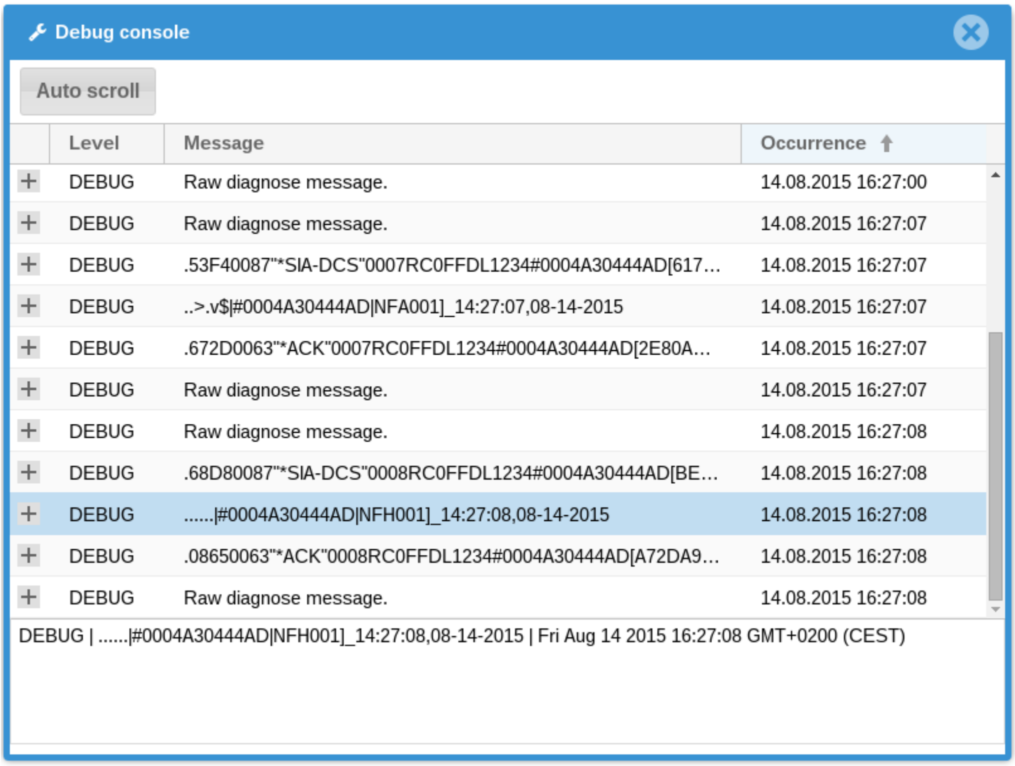
Year	In spec	ATS down time	Availability
UDP Chiffré (SP6)			
	✖	469h 56m 40s	6.76 %

5.4 SPT debugging

It is sometimes interesting to see in details the IP-RCT <-> SPT communication. Each protocol can output the transmission payload which can be accessed from the *SPT* view. Select the transmitter to analyse and press “Switch diagnose mode” -> “Enable diagnose mode”.



Once the flag to diagnose the SPT is set, press “Debug” button to enter the detailed communication view. Usually protocols outputs the raw message as well as the clear content if ciphered. The response is also displayed in the window.



	Level	Message	Occurrence
+	DEBUG	Raw diagnose message.	14.08.2015 16:27:00
+	DEBUG	Raw diagnose message.	14.08.2015 16:27:07
+	DEBUG	.53F40087"*SIA-DCS"0007RC0FFDL1234#0004A30444AD[617…	14.08.2015 16:27:07
+	DEBUG	..>.v$|#0004A30444AD|NFA001]_14:27:07,08-14-2015	14.08.2015 16:27:07
+	DEBUG	.672D0063"*ACK"0007RC0FFDL1234#0004A30444AD[2E80A…	14.08.2015 16:27:07
+	DEBUG	Raw diagnose message.	14.08.2015 16:27:07
+	DEBUG	Raw diagnose message.	14.08.2015 16:27:08
+	DEBUG	.68D80087"*SIA-DCS"0008RC0FFDL1234#0004A30444AD[BE…	14.08.2015 16:27:08
+	DEBUG	......|#0004A30444AD|NFH001]_14:27:08,08-14-2015	14.08.2015 16:27:08
+	DEBUG	.08650063"*ACK"0008RC0FFDL1234#0004A30444AD[A72DA9…	14.08.2015 16:27:08
+	DEBUG	Raw diagnose message.	14.08.2015 16:27:08

```
DEBUG | ......|#0004A30444AD|NFH001]_14:27:08,08-14-2015 | Fri Aug 14 2015 16:27:08 GMT+0200 (CEST)
```

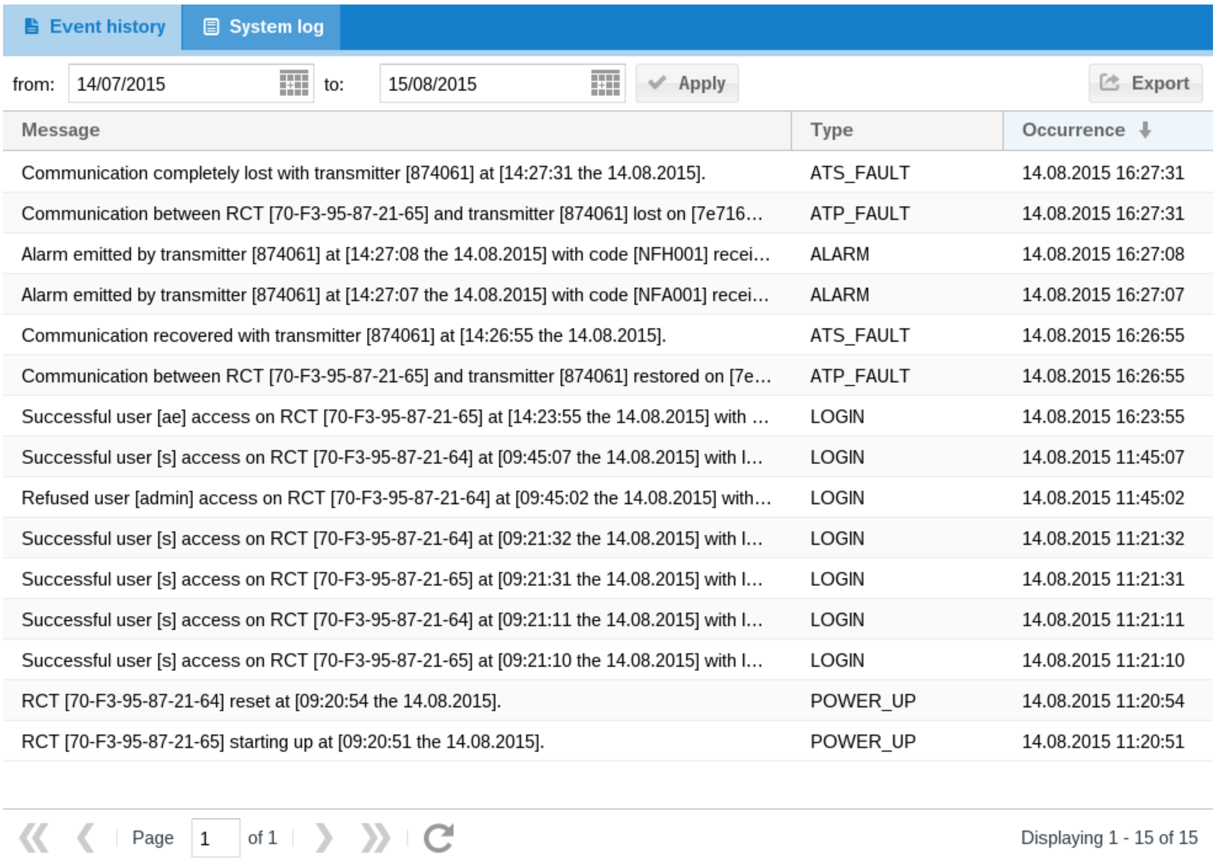
It is not obligatory to keep the window open, the last 5000 messages are stored in memory and can be accessed anytime unless the IP-RCT is restarted, reset or shutdown.

5.5 Event history

During its exploitation, the IP-RCT stores multiple content in an embedded database to perform statistics and performances checks. In the *History* view and *Event History* tab, find a grid with all system and SPT events. Currently, the following entry type exists:

- *ALARM*: stored whenever an alarm is raised by any SPT with all information regarding the transmission;
- *ATP_FAULT*: whenever a ATP fault/restoral is raised;
- *AE_FAULT*: whenever an AE is stopped/started;
- *ATS_FAULT*: whenever a ATS fault/restoral is raised;
- *TNI_FAULT*: whenever a network interface fault/restoral is raised;
- *RCT_FAULT*: whenever a RCT synchronization fault/restoral is raised;
- *CONFIG_CHANGE*: whenever a configuration change occurs;
- *POWER_UP*: whenever the IP-RCT is reset, rebooted or restarted;
- *SOFT_UPDATE*: whenever a IP-RCT update occurs;
- *DATE_UPDATE*: whenever a date update occurs;
- *LOGIN*: whenever a successful or failed login occurs;
- *USER_UPDATE*: whenever a user is modified;
- *UNKNOWN*: unknown change occurred.

It is possible to filter events by their respective fields and to select only certain type. The time interval to select events may be parameterized.



from: 14/07/2015 to: 15/08/2015

Message	Type	Occurrence
Communication completely lost with transmitter [874061] at [14:27:31 the 14.08.2015].	ATS_FAULT	14.08.2015 16:27:31
Communication between RCT [70-F3-95-87-21-65] and transmitter [874061] lost on [7e716…	ATP_FAULT	14.08.2015 16:27:31
Alarm emitted by transmitter [874061] at [14:27:08 the 14.08.2015] with code [NFH001] recei…	ALARM	14.08.2015 16:27:08
Alarm emitted by transmitter [874061] at [14:27:07 the 14.08.2015] with code [NFA001] recei…	ALARM	14.08.2015 16:27:07
Communication recovered with transmitter [874061] at [14:26:55 the 14.08.2015].	ATS_FAULT	14.08.2015 16:26:55
Communication between RCT [70-F3-95-87-21-65] and transmitter [874061] restored on [7e…	ATP_FAULT	14.08.2015 16:26:55
Successful user [ae] access on RCT [70-F3-95-87-21-65] at [14:23:55 the 14.08.2015] with …	LOGIN	14.08.2015 16:23:55
Successful user [s] access on RCT [70-F3-95-87-21-64] at [09:45:07 the 14.08.2015] with l…	LOGIN	14.08.2015 11:45:07
Refused user [admin] access on RCT [70-F3-95-87-21-64] at [09:45:02 the 14.08.2015] with…	LOGIN	14.08.2015 11:45:02
Successful user [s] access on RCT [70-F3-95-87-21-64] at [09:21:32 the 14.08.2015] with l…	LOGIN	14.08.2015 11:21:32
Successful user [s] access on RCT [70-F3-95-87-21-65] at [09:21:31 the 14.08.2015] with l…	LOGIN	14.08.2015 11:21:31
Successful user [s] access on RCT [70-F3-95-87-21-64] at [09:21:11 the 14.08.2015] with l…	LOGIN	14.08.2015 11:21:11
Successful user [s] access on RCT [70-F3-95-87-21-65] at [09:21:10 the 14.08.2015] with l…	LOGIN	14.08.2015 11:21:10
RCT [70-F3-95-87-21-64] reset at [09:20:54 the 14.08.2015].	POWER_UP	14.08.2015 11:20:54
RCT [70-F3-95-87-21-65] starting up at [09:20:51 the 14.08.2015].	POWER_UP	14.08.2015 11:20:51

Page 1 of 1

Displaying 1 - 15 of 15