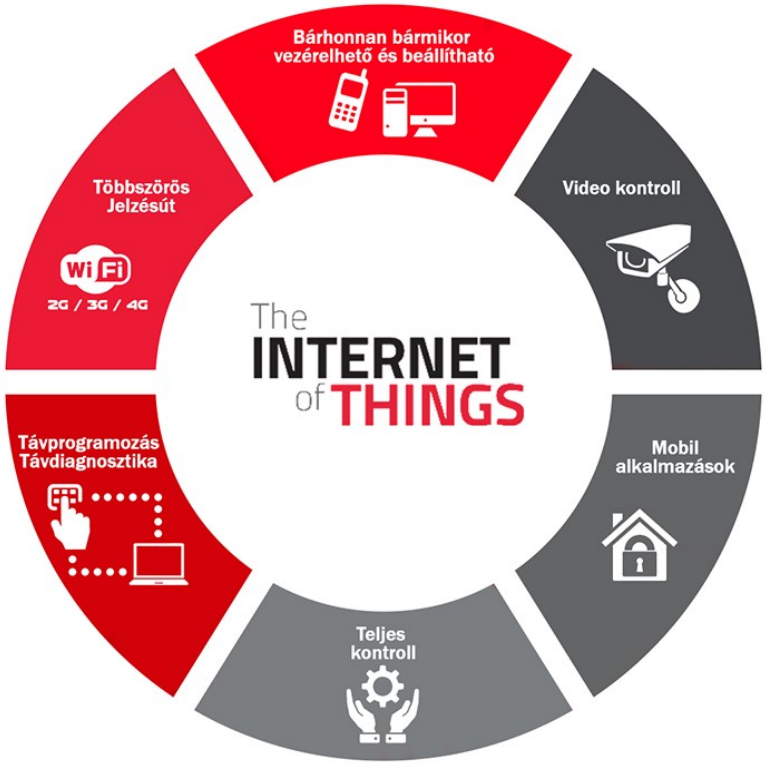
SINGULAR WIFI

Internet based alarm monitoring communicator with remotely manageable features

Manual v1.0



Content

1 Introduction

SINGULAR product line are a modern WIFI connection based IP network (internet) communicator for alarm monitoring with a „basic" function: ***Forwarding Contact ID reports from any alarm panel to monitoring station through IP network to selected SIA DC 09 receivers, in safe and stabile mode.***
Besides that, these devices also present following new possibilities:

- Contact ID events forwarding to smartphone application, with „push notification" and detailed event list with authentication (Android OS)
- Controlling of alarm panels (arm/disarm through keyswitch input, 2 separate partitions) with the smartphone application
- Remote programming of alarm panel

1.1 Main features

- 2 selectable WiFi networks (main and auxiliary communication path)
- Contact ID reports forwarding to 2 independent SIA DC-09 receivers
- AES-128 encrypted communication
- 2 controlled outputs (from a WEB page, or smartphone application)
- Serial port for alarm panels remote programming
- Earpiece output for audio supervision of alarm panel communication
- Status supervision and control of alarm panel from a smartphone application
- Network settings from WEB site, provided directly from device (hotspot mode)
- Remote settings and firmware upgrade from WEB page, through Internet

1.2 Usage Areas

- Providing a IP path for forwarding of Contact ID reports from Alarm panel to monitoring station
- Remote programming of Alarm panels, Fire panels, or any standalone device with serial connection to a software (vending machines, car diagnostic, sensor reading..), through internet
- Complete supervision of alarm system from smartphone:
    - Identified Control (arm/disarm) without keypad
    - 3 notification interfaces: Status viewing, event list review and "push notification" warnings
    - Events filtering and displaying differently (alarm, arming, trouble,...)
    - Displaying of alarm system status (armed, trouble, online, etc...)
    - Multiple devices in one Smartphone account (home, office, weekend house, etc..)
    - One device can be added to many accounts, more notified persons at the same time.

1.3 Advantages

- No need for a cellular network and a SIM card (no contract with provider and monthly fees)
- Unlimited number of reports and users
- Simple installation (NO router settings)

2 Parts and connectors

1. WIFI antenna connector (SMA)
2. Status signaling LED
3. Serial port connector (SERIAL)
4. Power supply terminals (DC+ / DC-)
5. Communication line (TIP / RING)
6. Open Collector Output 1 (OUT1)
7. Open Collector Output 2 (OUT2)
8. Earpiece plug (3.5mm mono jack)
9. Setup pushbutton (Hotspot mode switch)

2.1 Status Signals

The small LED, located next to a antenna connector is providing a device status information with following signals:

Continuous Red	No SIM or no settings
Flashing Red	Connecting (if it flashing again after 30 sec, the settings are bad)
Flashing Green	Idle mode
Continuous Green	Alarm panel transmitting message
Green/Red alternately	Hotspot mode, device programming in progress

3 Functional description

3.1 Communicating to monitoring station *PROCEDURE*

Communication between the alarm panel and the monitoring station through a SINGULAR communicator is happening this way:

- Alarm panel takes (hook off) the emulated phone line (TIP/RING terminals) and dials a number defined in it's setting (eg. 1111). If the line signal was not „ free" (The communicator is not able to forward the message), the alarm will drop the line (hook on), and try again after few seconds.
- Communicator senses dialing, and transmits a „Handshake" signal (a signal for alarm to start sending report code, normally emitted by the phone line receiver)
- Alarm panel transmits the Contact ID code of the event that is to be reported
- Communicator takes over the codes, converts them to IP packages and sends them to the IP receiver on programmed address. After that it waits for a confirmation.
- The receiver forwards the message to the monitoring software, and receives a confirmation that the message was delivered (presented to the operator). Then the receiver sends the receipt (confirmation) to the communicator.
- While waiting for a „kiss of" signal (sound from receiver, confirming that the message was received), the alarm panel will transmit the Contact ID code, since the timing of confirmation in PSTN system is really short (usually 1-2 seconds).
- When the communicator receives the confirmation signal from IP receiver, waits for the repeated report to be finished and transmits the „kisoff" signal to alarm panel (on the emulated phone line, TIP/RING terminals).
- The Alarm panel considers that the message was delivered and starts transmitting the Report code of the following event that should be reported (the procedure is repeated from second point). If there are no more new events to be reported, the Alarm panel hangs up the line

The communicator builds a connection to the primary receiver before each reporting of an event or a test report, and closes it after the successful sending. If the Primary receiver is not reachable, the communicator tries to build a connection to the second receiver.

The confirmation of received message is generated at the monitoring software. Some receivers can generate a confirmation, without sending the message to the software (operator). Ensure that the receiver is set properly, to void „ lost messages".

3.2 Sending messages to Smartphone *PROCEDURE*

- Alarm panel sends the report codes as described in previous section.
- The communicator takes over the Contact ID message and forwards it to the IP receiver. At the same time, it sends the event report code to the Puloware IoT server.
- Puloware IoT server sends the push notification to all smartphone devices that have added this communicator to it's account, and enabled the push notification for this message type.

The smartphone application will present only those events that were reported to a real or virtual monitoring station. Therefore, the alarm panel must be set to send reports on all events that happened in the alarm system (arm/disarm/alrm/trouble/...).

3.3 Switching to auxiliary connection WiFi2

If the connection to internet through primary WiFi network is broken, Singular communicator will automatically switch the communication toward Internet to the auxiliary network. While the communication is maintained through the auxiliary network (WiFi2), the device continuously checks the main connection (through WiFi1), and when it becomes available, communication is switched back to it .

3.4 Outputs

Singular device contains 2 open collector type outputs (OUT1, OUT2. This means that when they are OPENED, this output is „floating", and when CLOSED, the output will be on negative (DC-). Control of these outputs is possible from a Puloware server web site, or from the smartphone application. Typical usage for these outputs is arming/disarming of two separate partitions, with these outputs wired to a keyswitch input of alarm system.

4 Installation guide

4.1 Setting the WiFi connection

Singular communicator can be set with any device that can connect to a Wireless network and has a internet browser available (Smartphone, Laptop, Tablet,...).
Settings of the parameters for internet connection through a local router (SSID and Password) can be entered while device is in HOTSPOT mode, providing a new Wireless Network. A smart device connected to this network can open a web site that contains these parameters, and edit them. For this operation any available Internet browser can be used.

4.2 Activating Hotspot mode

Push the SETUP button shortly and the status LED will start blinking green/red alternately, displaying that device is in HOTSPOT mode.

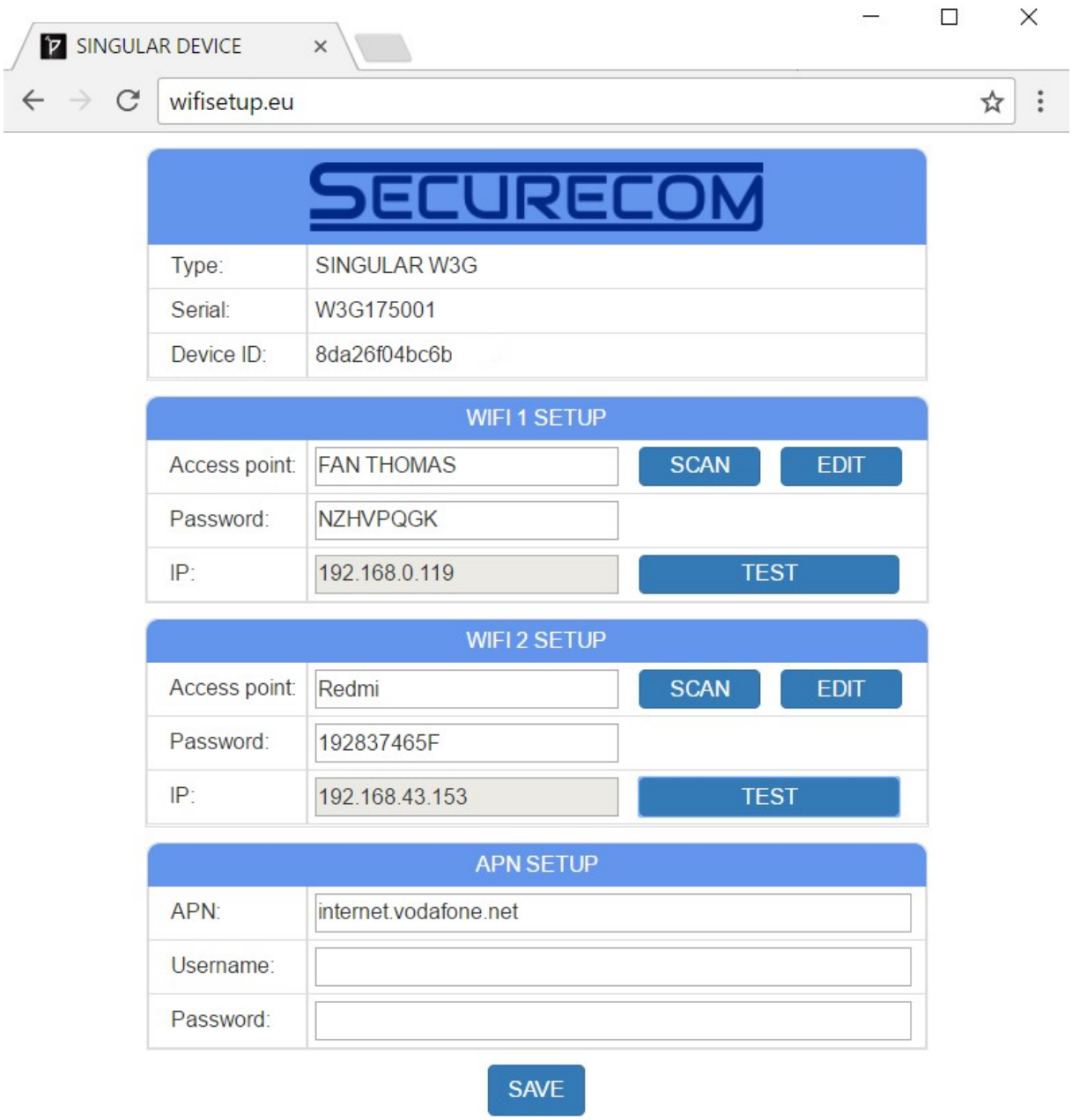
4.3 Connecting to Device in Hotspot mode

Use and go to network selection page and check the available WiFi networks. A network named **SECURECOM DEVICE** should be listed among them. Connect your device to that network.
After connecting to SECURECOM DEVICE network, some devices will show an error, since it can not connect to Internet through this network. Ignore this message and open an Internet browser.

In the address field type in **a wifisetup.eu** address, like if you would be going to this web site (picture on next page showing this).

4.4 Setting the Internet connection

If your smart device is connected to the **SECURECOM DEVICE** network, the web site **wifisetup.eu** should present a page looking like this:



The primary connection settings should be entered in the WIFI1 SETUP area, and the auxiliary connection parameters in the WIFI2 SETUP. These settings can be made with following steps:

1. List the available (visible) networks -> click the SCAN button
2. Select the desired network -> Scroll down the list and click on the wanted name
3. Enter the appropriate password -> Type the password in the „ Password" field
4. Test the connection -> Click on the TEST button
5. Save the settings -> Click on the SAVE button

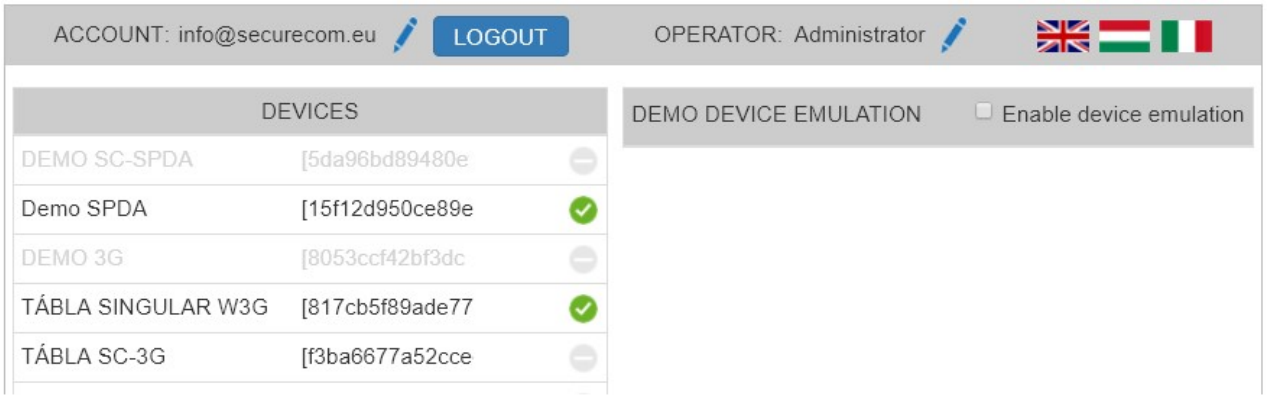
4.5 Change from hotspot to regular mode

After saving the settings, press shortly the SETUP button. This will restart the device in regular mode, and it will try to connect to a wireless network(s), according to the settings. When the connection is successful, the blinking green light on status LED will be showing the device is in normal status.

All additional settings can be made through the web page on www.puloware.com site.

4.6 PULOWARE service WEB site (device monitoring, remote settings, firmware upgrade)

As mentioned in previous chapter, device settings can be reached on the www.puloware.com web site. An account must be created, and after logging in with account credentials, the site will provide the list of all devices that were added to the account.



To add the device to your account, a serial number of the device (printed on the sticker, on device back) and the password are required. Initially, the password is BLANK, and it should be changed to void unauthorized access to the device.

NOTE: in case that the device was already added or the number is invalid, the software „kicks out" from the account, and you must log in again. This way the user knows that there is something wrong with the number that was entered.

When one device from the list (on left side of the window) is selected, the handling platform for that device will appear. Device detailed status, all settings, event list, as well as Event filter and user list tables are displayed. All values that are presented are actual and valid.

4.6.1 Basic information and operations

The selected module type and version number are displayed in this area. Also, the device name and output control mode, are presented. These values can be modified, by clicking the pen next to the field.

Warning: If you want the output to comply with "pushbutton" arming of alarm panel, the "negative impulse" mode should be selected. Every command (either from smartphone application or the web site) will turn on the output for 1 seconds, and return back to "off" status.

Below these data, there is a line of icons that provide following options:

Restart of device

Control of output- the number on the icon presents the output number (OUT1, or OUT2)

The way for the output state changing on control signal can be changed in the „ ARM mode" field. The „ Change NO/NC state" means that every control signal will change the output state. The „Negative impulse" setting will result that on every control signal the output turns ON for one second, and then automatically goes back to OFF state.

Open previously saved settings from file

Save displayed settings to a file

Load (write) presented settings to the communicator (must be used after changes were made on page!)

4.6.2 Device status display

MODULE STATUS	
WIFI network:	dlink
WIFI signal:	
Monitoring station 1:	
Monitoring station 2:	
Dial capture:	ONHOOK
OUT 1	INACTIVE
OUT 2	INACTIVE

The presented real values are showing the status online and change as the device status change. This way we can remotely check the momentary state of the device.

4.6.3 Self-generated event codes

COMM. EVENT CODES	
Setup changed:	306
OUT controlled:	206

This area contains settings for the event codes that will be sent by Communicator to monitoring station, if the defined event has occurred. If the field is left blank, the event will not be reported. Setting the appropriate value (that will be recognized in monitoring software), the monitoring station will be notified when the communicator settings have changed, or when some output was turned ON or OFF.

4.6.4 Monitoring station settings

To set up the Singular device for reporting to the monitoring station in a required way, following settings are available:

MONITORING STATION 1 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9998
Protocol:	UDP ▾
SIA prefix:	
Object identifier:	9005
Replace obtained identifier:	YES ▾
Link test period:	1 min ▾
Link test code:	

MONITORING STATION 2 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9999
Protocol:	TCP ▾
SIA prefix:	
Object identifier:	1050
Replace obtained identifier:	NO ▾
Link test period:	3 mins ▾
Link test code:	

IP address	IP address or domain name of the monitoring station
Port	Port number of the monitoring station's IP address
Protocol	Selectable communication IP protocol: TCP, UDP
SIA prefix	2 characters long SIA prefix, it can be used if the identifier of the connected alarm control panel is just 4 characters long, but the necessary identifier of receiver is 6 characters long
Object identifier	The self identifier of the SINGULAR device (4 characters long).
Replace obtained identifier	If it is enabled than the SINGULAR device exchange the alarm control panel's identifier, to given self object identifier. **YES**: exchange, **NO**: not change
Link test period	Sending test report to the monitoring station • **NO**: test report is not sent • **30sec – 24 hours**: the device sends test reports to the monitoring station by the given interval
Link test code	Any code can be defined. If this field is empty than the communicator sends Null Message, as defined by standard.

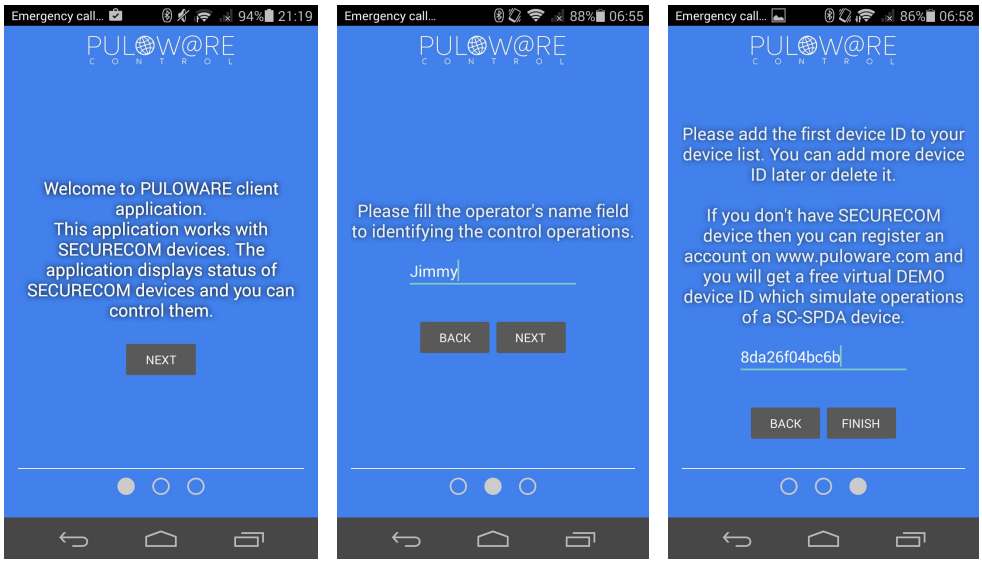
4.6.5 Communication details

This view presents a detailed communication between the Alarm panel and monitoring receiver.
All messages and feedback data, as well as error messages are presented with a source and a time stamp (date, hour, minute, second), when was the signal received.

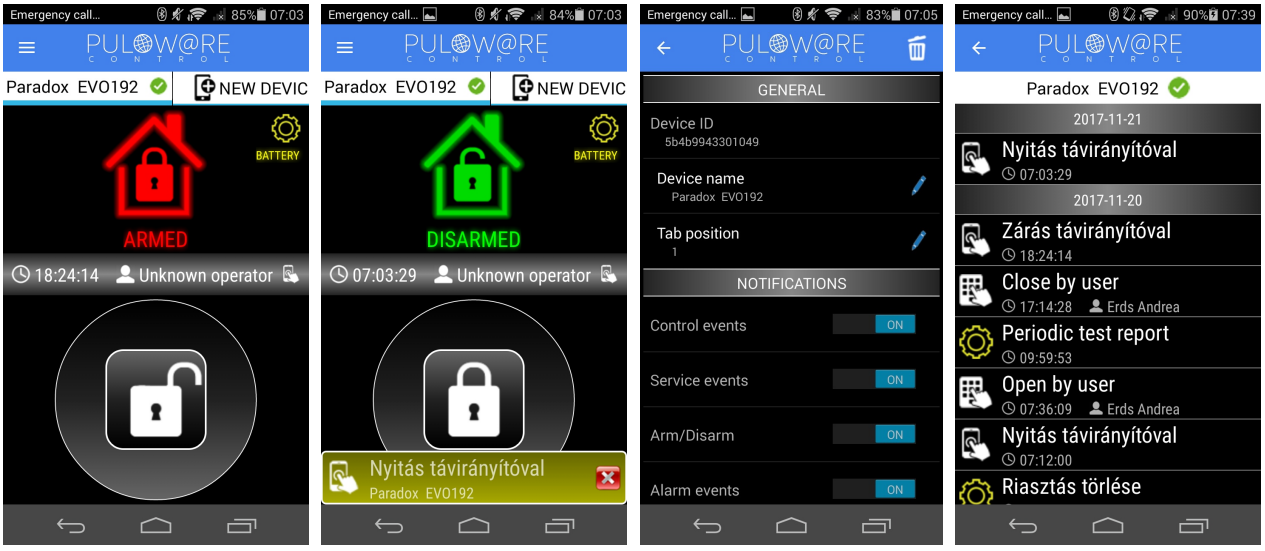
4.7 Android application

You can download the application from a play shop. Look for a PULOWARE CLIENT, with a icon looking like show

When you start the application first time, a setup wizard requires an operator name to be entered. This name is used for identification in event list (who activated the output, i.e disarmed the system...). After that, a device that you want to control with this application must be added, entering it's serial number. After the number is typed in, you can finish the setup.



This application can be used to handle more than one device, other devices (different device types as well) can be added within the application. The look of the application „ main screen" is:



Note: Application can not show alarm status until some reports (events) are made. Therefore, disregard the displayed status on application first start, until first arming/ disarming.

It presents the status of the alarm panel and contains a button that is used to control the alarm output- it must be held for 3 seconds in order to activate it. The button also shows the alarm status- “padlock closed” for armed, and unlocked for disarm.

The application second page is opened by swiping the main page to left. Shows the event list, filtered with names that were made on web site. For example: If user 003 armed the system, and the filter on web site says that user 003 is Jimmy, the event list will display that Jimmy has armed the system.

NOTE: The alarm panel must be properly programmed and connected to the device, in order to have the application working correctly.

4.8 Transparent forwarding of serial port

The purpose of this feature is to replace a physical connection between a serial port on alarm panel (or any other device that can be controlled or programmed through it’s serial port) and a computer serial port, with connection from serial port on Singular device to the virtual serial port on the computer. This way you can use the programming software same way as if the alarm panel was physically attached to the COM port created by RemoteSerial.exe, since it „ thinks” that is the reality. All signals (on Bit level) that come in on the Singular physical serial port, goes out on the virtual com, and vice-versa- regardless of the fact that these two are far away from each other. This „ tunnel connection” is going through the WiFi network and internet, and it is provided by the PULOWARE IoT server. So the „ remote programming” of alarm panel can be done from any place, only an internet connection is needed.

The remote serial port should be set with following steps:

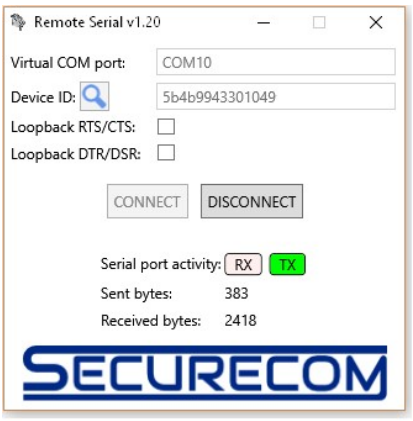
1. The serial port of the Singular device should be set to fit the alarm panel serial port operating mode. These settings can be made on the www.puloware.com web site. Default settings are as shown below, and they fit to most of the alarm panel types.

SERIAL SETTINGS	
Baud rate:	9600 ▾
Data bits:	8 ▾
Parity:	None ▾
Stop bit:	1 ▾

2. Connect the Alarm panel to the communicator with appropriate cable.
Important: The serial connection cables differ for different alarm panels. Appropriate connector, and signal level adjustment is required. Please use the appropriate cables, check before plugging on. Connection with wrong contacts or levels may damage the communicator or the alarm panel.

3. Run the RemoteSerial.exe and fill the required fields. You can download the setup for this software from this link: http://puloware.com/public/RemoteSerialSetup.exe

4. Run the Alarm panel programming software (eg. WINLOAD, Babyware, DLS, Proste,...) and start the connection like if the panel was connected directly with programming cable.



➔ Serial port that is set for „ cable connection" in alarm panel software
➔ Communicator Serial number (written on sticker, on device backside)

5 Installation tips

- The smartphone application can present reported Contact ID events only. Therefore, the receiver must confirm the sent events (it can be a „ virtual receiver", as long as it confirms the report) alarm panel must be set properly, with following :
    - The alarm panel communication protocol must be set to Contact ID
    - All events must be set for reporting (disarming without alarm, zone bypassing, ...)
    - The arming method of keyswitch (to which the communicator outputs are connected) must be „pulse" (not „ maintained switch").

Connected services

PULOWARE IoT server
http://puloware.com

SIA DC-09 virtual receiver (for testing purposes only)
http://siatest.securecom.eu

Android application
https://play.google.com/store/apps/details?id=com.puloware.app

Virtual serial port for remote programming

http://puloware.com/public/RemoteSerialSetup.exe

6 Technical data

Electronic and telecommunication parameters

Connections to Internet	
Primary communication channel (AP1)	WIFI (IEEE 802.11 b/g/n)
Secondary communication channel (AP2)	WIFI (IEEE 802.11 b/g/n)
Communication features	
Simulated phone line for alarm panel connection (**TIP / RING**)	Line voltage: 48V Line loop current: 25mA Load impedance: 100-470 Ohm
Communication Protocol	To alarm panel: SIA DC-05-1999: Contact ID Protocol To WIFI IP connection: SIA DC-09-2013: Internet Protocol
Self-generated and transmitted signals	Settings changed Output controlled Test report
Controllable outputs (OUT1, OUT2)	
Open collector outputs (Output connects to negative power supply **(DC-)**, otherwise „floating” (Cannot be resistance measured with ohm meter or volt meter, until a pull-up resistor or load is applied.)	Nominal load: 50mA (protected from shortcut or overload)
Power supply (DC+ / DC-)	
Supply voltage	9-24V DC
Maximum consumption	200mA @ 12V DC
Nominal consumption	100mA @ 12V DC
Maximum dimensions	98x75x24 mm