SECURECOM

SINGULAR WIFI, W2G, W4G

Model: 4

Remotely manageable alarm monitoring communicators with Mobile App

Installation and reference manual v2

SINGULAR WIFI

SINGULAR W2G

SINGULAR W4G

Content

1. INTRODUCTION

All information in this manual related to cellular data communication are limited with a product type:

SINGULAR Wifi= NO mobile data connection;
SINGULAR W2G= GPRS (2G) networks only;
SINGULAR W4G= GPRS, HSPA and LTE networks are supported.

SINGULAR product line is a modern IP communicator, based on WIFI and cellular network data (internet) connection, for alarm monitoring with a „basic” function: ***safe and stabile Forwarding of Contact ID reports from any alarm panel to monitoring station through IP network to selected SIA DC 09 receivers***
In addition, these devices also provide following features:

- Contact ID events forwarding to smartphone application, with „push notification” and detailed event list with authentication (Android/IOS)
- Controlling of alarm panels (arm/disarm through keyswitch input, 2 separate partitions) with the smartphone application
- Remote programming of alarm panel, using transparent data forwarding from a physical serial port

1.1. Preferences

- Dual signal transmission via WIFI and/or cellular data network
- Unlimited number of reports and users
- Simple installation (NO router settings)

1.2. Main features

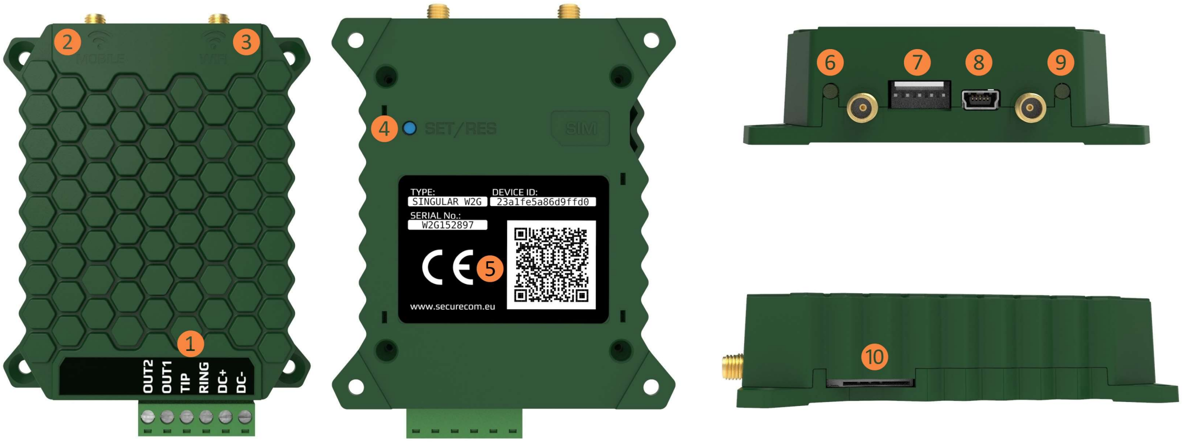
- 2 selectable WiFi networks (main and auxiliary communication path)
- Transmission of alarm reporting through cellular network (2G / 3G / 4G, device dependant)
- Contact ID reports forwarding to 2 independent SIA DC-09 receivers
- AES-128 encrypted communication
- 2 controlled relay outputs (from a 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
- Internet connection setting through device WEB page in hotspot mode
- All settings and firmware upgrade with Internet browser, on Puloware server web site

1.3. Usage Areas

- Providing an 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..)
- Complete supervision of alarm system from smartphone:
  - Identified arming /disarming
  - 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...)
- Multiple smartphone operators, more notified persons at the same time.

2. DEVICE PARTS AND CONNECTORS



Pictured in green is the SINGULAR W2G model

Legends:

1 Terminal block for connecting to the alarm system (pluggable)

OUT2	OUT1	TIP	RING	DC+	DC-
Momentary switch type relay to DC- for partition 2 (open/close)	Momentary switch type relay to DC- for partition 1 (open/close)	Simulated phone line to AS TIP/RING port for Contact ID communication		Positive supply	Negative supply

Switching of the outputs is compared to the DC- negative supply, which, by default, is NO (normally open)! Switching power max.: 60V @ 2A

2 Mobile antenna connector (SMA male)

3 WIFI antenna connector (SMA male)

4 Pushbutton to turn on WIFI hotspot mode, and to reset to factory defaults

5 Device ID sticker

TYPE:	SERIAL No:	DEVICE ID:	QR code
Type ID marking WIFI, W2G, or W4G	Serial number	Device ID for the mobile application and remote WEB access	Device ID for registration in the mobile application

6 WIFI connection status LED

5 Serial connector for remote programming of alarm systems

8 USB mini B connector for PC configuration

6 Mobile network connection status LED

10 SIM card holder for mobile data connection (mini SIM -2FF, push – push)

2.1. Status Signals

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

	Mobile network status 9	**WIFI network status** 6
Continuous Red	APN or SIM missing	No network set
Blinking Red	Connection in progress	Faulty setting
Blinking Green	Normal operation	Normal operation
Continuous Green	Event reporting over mobile net	Event reporting over WIFI net
Green/Red	-	WIFI setup mode

3. DETAILED DESCRIPTIONS OF FUNCTIONALITY

3.1. Communicating to monitoring station

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 its 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 „kissoff” 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 „kissoff” 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 send the report 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”.

If reporting to receiver has failed, or the “acknowledge” signal was not received, the communicator will not send the “kiss off” signal to the alarm panel, so it will repeat the Contact ID code transmission several times. Alarm panel may hook off and dial again, to repeat CID code sending, and the procedure is repeated until the “kiss off” signal is received (message delivered), or the Alarm panel stops repeating and generates “communication error” event, which is shown on it’s keypad. When a next reportable event happens in Alarm panel, it will first try to send the undelivered message, then the “communication trouble restore” code, and finally the new event code.

3.2. Sending messages to Smartphone

- 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 reported events and own events to the Puloware IoT server.
- Puloware IoT server sends the push notification to all smartphone devices where the particular device was assigned and enabled

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/alarm/trouble/...).

The push notification will be sent an application will present t with a sound only if all settings are appropriate, enabled for this message type and all corresponding services are fully operational.

3.3. Mobile data (2G, 3G or 4G) as alternate for Wifi connection

If the connection to internet through primary WiFi network is broken, the communicator will automatically switch the communication to the backup cellular network. While the communication is maintained through the backup cellular data network, the device continuously checks the main connection (through WiFi), and when it becomes available, communication is switched back to it (with appropriate algorithm, series of steps).

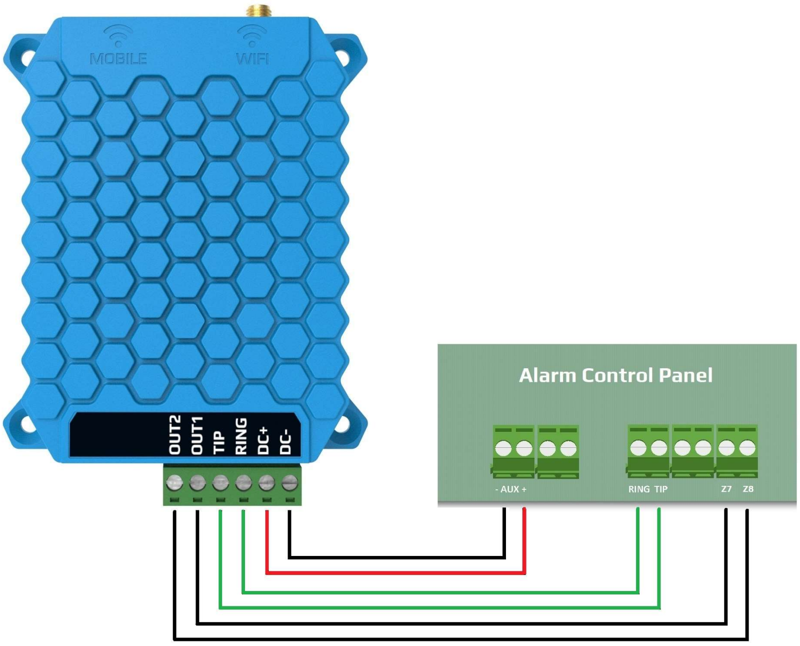
SINGULAR device will connect to a mobile network to provide backup communication path as soon as it is turned on. It will first try to connect to network that has a strongest signal and is authorized to it with inserted SIM card. In case of network failure, it will automatically connect to next strongest authorized network. In case of W4G device, priority for connection is defined with the „network generation”. 4G has a highest, and 2G he lowest priority. Therefore, if a W4G device contains a SIM card that allows access to some 4G network that is available on site, the device will connect to that network. If it can not connect to any available 4G network, the device will first try to connect to strongest available 3G network that is enabled by SIM. If that fails, device will continue trying the connection with next strongest and authorized network, until the connection is successfull or there is no more options. Once connected, the device will use that network for data sending (when commmunication on Wifi fails) until next restart or reconection.

3.4. Outputs

SINGULAR device contains 2 relay outputs (OUT1, OUT2). When activated, output terminal will be connected to negative supply (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

SINGULAR device was built for operation with a standard alarm panel. All wire terminals should be connected to appropriate terminal on alarm panel PCB. After the connection to Internet was established, device settings should be applied in correspondence on required features.



Pictured in blue is the SINGULAR WIFI model

For easier working with wires, terminals on the device are removable. Remove the terminal block from device, screw all wires to appropriate places in terminal block, and only after all wires were fastened apply power to it and plug back the terminal block.

1. Connect the Aux power terminals on alarm panel to terminals DC+ and DC-, with appropriate polarity.

2. Terminals “TIP” and “RING” should be connected to terminals on alarm panel, destined for the PSTN line connection (usually also marked as “Ring” and “Tip”). The polarity is irrelevant in this pair

3. Connect the OUT1 terminal to zone input that will be set as keyswitch, controlling the *Partition 1.* If the keyswitch inputs wiring for the alarm panel requires resistors or the zone doubling is used, connect the resistors as required. The OUT1 terminal is one pole of output relay, and the other pole is the DC- (relay output connects to GROUND when activated)

4. Connect the OUT2 terminal to zone input that will be set as keyswitch, controlling the *Partition 2.* If the keyswitch inputs wiring for the alarm panel requires resistors or the zone doubling is used, connect the resistors as required. The OUT1 terminal is one pole of output relay, and the other pole is the DC- (relay output connects to GROUND when activated)

Warning: If the communicator is not supplied from alarm panel, the negative (gnd) of external power supply must be connected to Aux- (negative pole of power on alarm panel). Outputs (OUT1 and OUT2) are connecting to DC- terminal when active.

5. CONFIGURING THE DEVICE

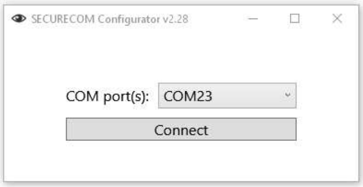
In order to setup the details of communication, install the SECURECOM CONFIGURATOR program first. The program can be downloaded from the site: http://securecom.eu/applications/securecom_configurator

Detailed description of setup is provided on this page.

After running the

SecurecomConfigurator
Alkalmazás

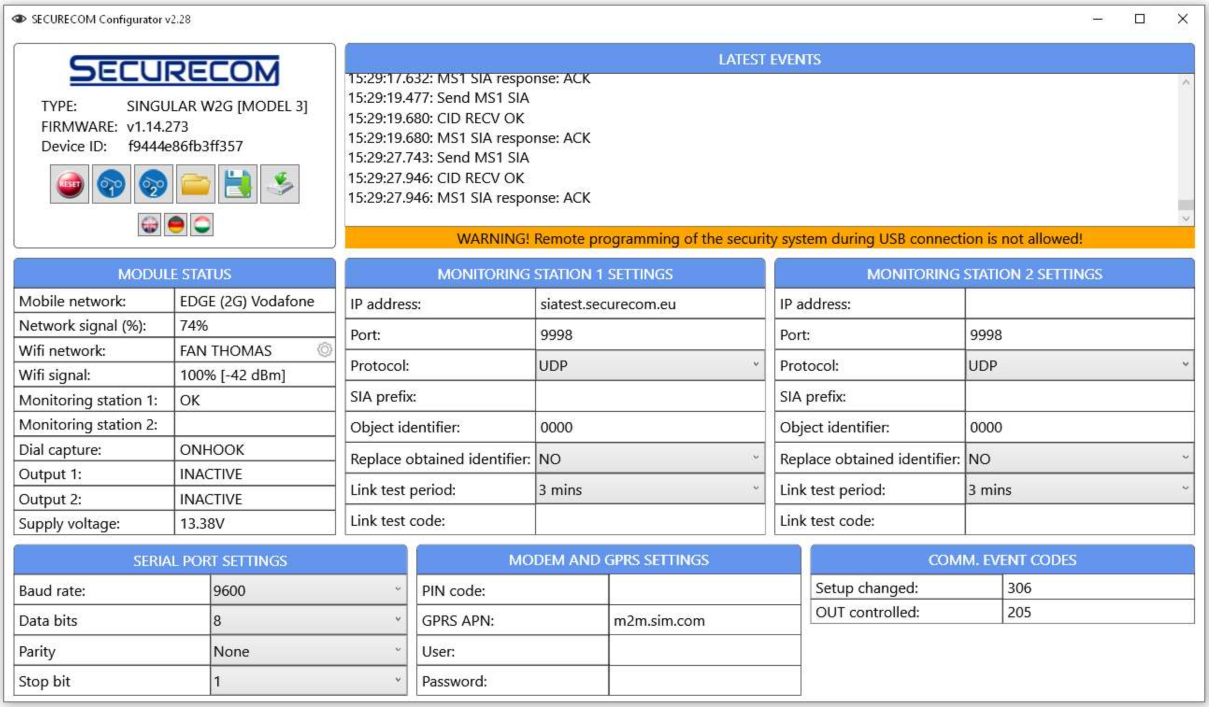
program, connect the USB port of the device to the PC, and select the appropriate serial port, then push the “Connect” button. For example:



SECURECOM Configurator v2.28

COM port(s): COM23

Once connected, device settings can be found on the following interface.



SECURECOM Configurator v2.28

SECURECOM

TYPE: SINGULAR W2G [MODEL 3]
FIRMWARE: v1.14.273
Device ID: f9444e86fb3ff357

LATEST EVENTS

```
15:29:17.632: MS1 SIA response: ACK
15:29:19.477: Send MS1 SIA
15:29:19.680: CID RECV OK
15:29:19.680: MS1 SIA response: ACK
15:29:27.743: Send MS1 SIA
15:29:27.946: CID RECV OK
15:29:27.946: MS1 SIA response: ACK
```

WARNING! Remote programming of the security system during USB connection is not allowed!

MODULE STATUS	
Mobile network:	EDGE (2G) Vodafone
Network signal (%):	74%
Wifi network:	FAN THOMAS
Wifi signal:	100% [-42 dBm]
Monitoring station 1:	OK
Monitoring station 2:	
Dial capture:	ONHOOK
Output 1:	INACTIVE
Output 2:	INACTIVE
Supply voltage:	13.38V

MONITORING STATION 1 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9998
Protocol:	UDP
SIA prefix:	
Object identifier:	0000
Replace obtained identifier:	NO
Link test period:	3 mins
Link test code:	

MONITORING STATION 2 SETTINGS	
IP address:	
Port:	9998
Protocol:	UDP
SIA prefix:	
Object identifier:	0000
Replace obtained identifier:	NO
Link test period:	3 mins
Link test code:	

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

MODEM AND GPRS SETTINGS	
PIN code:	
GPRS APN:	m2m.sim.com
User:	
Password:	

COMM. EVENT CODES	
Setup changed:	306
OUT controlled:	205

Operation of device requires the following basic settings:
- Setting of mobile network connection (APN for W2G and W4G)
- Setting of WIFI connection (required for SINGULAR WIFI, optional for W2G and W4G)
- Setting of remote monitoring receivers (optional, because the unit is operational standalone)

Attention: validity of the modified setting on the unit, require that the new variant is downloaded to the module!

To download, click on the icon, which will initiate the changes displayed in the STATUS INDICATOR window. After modification, the background of the icon becomes red, showing downloading is necessary..

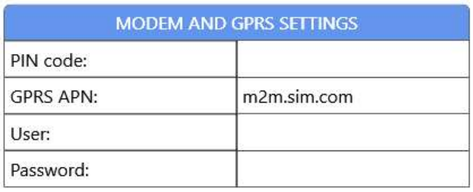
5.1. Mobile Network Connection Settings

This setting for SINGULAR WIFI model is inactive in lack of a mobile unit.

In order to set up the network connection, insert a correct SIM card in the SIM card holder 10, on the side of the device (according to the marking on the back), with the following requirements:

- mobile data capable
- active
- known data of APN connection
- PIN code of the card is known, or PIN is not required

If PIN is required for the SIM card, it has to be entered in the **SIM PIN code** field. In order to establish the data connection, the inserted SIM card's APN data have to be provided. (Generally there is no user name and password, only APN name)



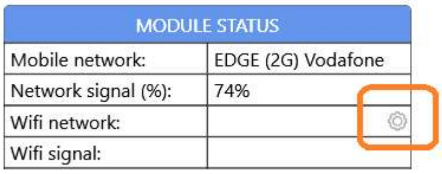
MODEM AND GPRS SETTINGS	
PIN code:	
GPRS APN:	m2m.sim.com
User:	
Password:	

After downloading the data, the module restarts, and connects to the network typically within 30 to 60 seconds. Successful connection is indicated by the green flash of status indicator LED 9, while an error is indicated by a red flash. In addition the information window shows the appropriate status message as well.

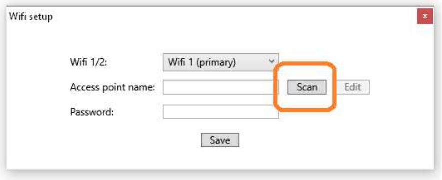
5.2. Setting up the WIFI connection

Setting up a WIFI connection reduces the data traffic on the SIM card, and also increases the signaling transfer speed. If a WIFI network is available at the installation, we recommend setting up access to the network in the unit. However for setting up of SINGULAR WIFI device the local WIFI network access is required, moreover access to 2 different WIFI networks can be set, thus further increasing functional safety!

1. Setup is started by clicking on the gear icon of the **WIFI network** value field in the **MODULE STATUS** window.



MODULE STATUS	
Mobile network:	EDGE (2G) Vodafone
Network signal (%):	74%
Wifi network:	
Wifi signal:	



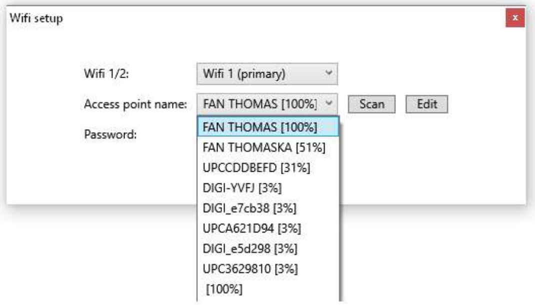
Wifi setup

Wifi 1/2: Wifi 1 (primary)

Access point name:

Password:

2. Accessible WIFI networks are listed by clicking on the **Explore** button.



Wifi setup

Wifi 1/2: Wifi 1 (primary)

Access point name: FAN THOMAS [100%]

Password:

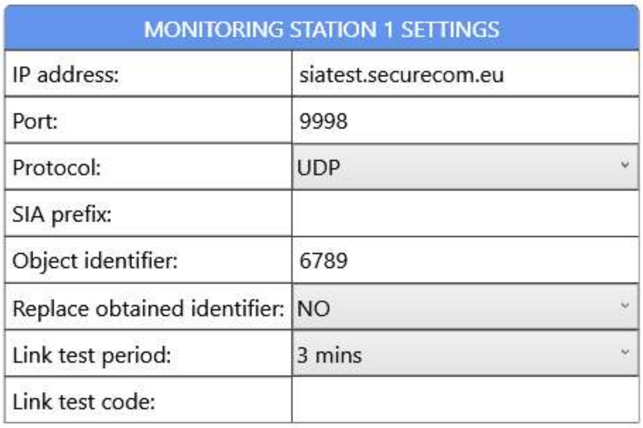
FAN THOMAS [100%]
FAN THOMASKA [51%]
UPCCDDBEFD [31%]
DIGI-YVFJ [3%]
DIGI_e7cb38 [3%]
UPCA621D94 [3%]
DIGI_e5d298 [3%]
UPC3629810 [3%]
[100%]

3. After selecting the appropriate network, and entering the valid password, click on the **Save** button to establish the WIFI connection. Successful connection is indicated by the green flash of status indicator LED 6, while an error is indicated by a red flash. In addition the information window shows the appropriate status message as well.

5.3. Monitoring Station Settings

Setting is optional, to be entered only if required reporting to monitoring station because the device can be operating in standalone mode too.

Connection with SIA DC-09 remote monitoring receivers (e.g. IPR-5000) requires the following settings:



MONITORING STATION 1 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9998
Protocol:	UDP
SIA prefix:	
Object identifier:	6789
Replace obtained identifier:	NO
Link test period:	3 mins
Link test code:	

IP address	IP address or domain name of the receiving station. (e.g. siatest.securecom.eu)
Port	End point of the IP address subnet, where the receiving computer is directed on the router
Protocol	Selectable communication transfer protocol: TCP or UDP
SIA prefix	2-character addition, it is necessary when the monitoring receiver expects a 6-character client ID, but the one generated by the alarm is only 4-character long
Object identifier	Account number of communicator unit (to send own reports: link test code, errors)
Replace obtained identifier	When enabled, replaces the original Account number in Contact ID report to the characters given in **Object identifier**, in all CID signals coming from the alarm
Dialed number by alarm system	The dialed phone number forces the actual signaling towards the given receiver Eg. general reports go to receiver 1, while service events are sent to receiver 2
Link test period	Setting the frequency of the test report
Link test code	Setting the code sent in the test report. If left empty, the null test set in the standard, is sent to the receiver.

The communicator can keep contact up to 2 remote monitoring receivers. The primary direction is the MONITORING STATION 1, thus all signals are sent to this address, until the test report or other signals are successfully completed. If there is no successful acknowledgement from MONITORING STATION 1, the unit switches to the direction of MONITORING STATION 2, and forwarding the signals of the alarm and inputs there.

In case acknowledgement from MONITORING STATION 1 becomes successful again, sending is directed back to the address of the primary receiver.

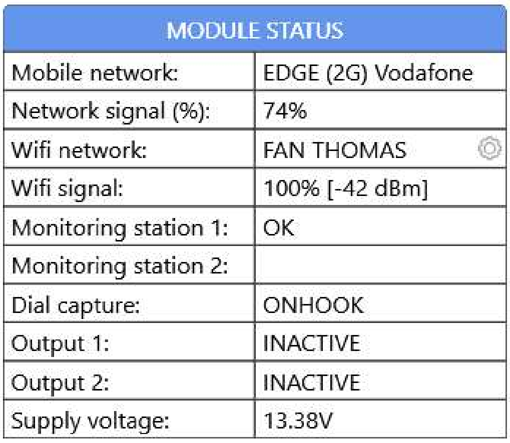
In case you want to send some of the signals (e.g. service reports) to STATION 2, a different phone number has to be entered in the **Dialed number by alarm system** field of STATION 2 in the device. This will force the communicator to send the given report to STATION 2, instead of the primary one.

The communicator takes any phone number from the alarm system, thus can be adapted to old systems without modification the dialled phone number of the alarm system.

The replacement of the client ID enables inserting old systems in the client registry system of the remote monitoring company.

5.4. Status indicators

The current status of the module is shown in the MODULE STATUS window.



MODULE STATUS	
Mobile network:	EDGE (2G) Vodafone
Network signal (%):	74%
Wifi network:	FAN THOMAS
Wifi signal:	100% [-42 dBm]
Monitoring station 1:	OK
Monitoring station 2:	
Dial capture:	ONHOOK
Output 1:	INACTIVE
Output 2:	INACTIVE
Supply voltage:	13.38V

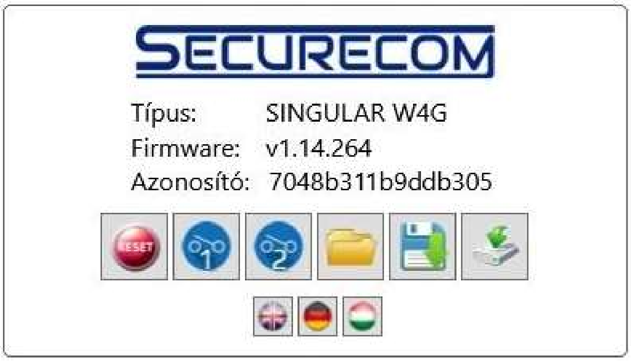
1. SIM card status, and the name of the mobile provider
2. Signal strength of the mobile network (0-100)
3. Name of WIFI network
4. Signal strength of WIFI network
5. REMOTE MONITORING RECEIVER **1** connection status
6. REMOTE MONITORING RECEIVER **2** connection status
7. Status of the alarm dialler (TIP/RING)
8. Status of output relay 1
9. Status of output relay 2
10. Value of supply voltage

5.5. Displaying the text of events, statuses

In the **LATEST EVENTS** window of the configurator, the communication between the communicator and the alarm system, the sending of report codes to the receiver, and the actual operation messages of the unit, can be monitored.

5.6. Administrative window

The administrative window of the **SecurecomConfigurator** software contains the following important data of the device.



Típus: SINGULAR W4G
Firmware: v1.14.264
Azonosító: 7048b311b9ddb305

11.Type ID of the product
12.Program version of the micro controller
13.Unique device ID code

14.Administrative tools

15.Selection of language

Function of the administrative tools is as follows:

Re-starting the module

Opening saved settings and loading to the screen

Saving settings in a file

Download ant activation of settings on the device

Test of relay OUT1

Test of relay OUT2

Using the unique device ID code, the product can be accessed remotely from a WEB page, similarly to the PC setup program. These options are described in a separate document.

5.7. Setting the device through Wifi connection

SINGULAR communicator can be set with any device that can connect to a Wireless network and has an internet browser available (Smartphone, Laptop, Tablet, ...).
Parameters for internet connection through a local router (SSID and Password and APN) should be set while device is in HOTSPOT mode, transmitting a new wireless network, named “SECURECOM DEVICE”. Connect to this network and open a web site that shows these parameters. After entering the required values save the settings and device will restart in “regular mode” and connect to Internet using the new set of parameters.

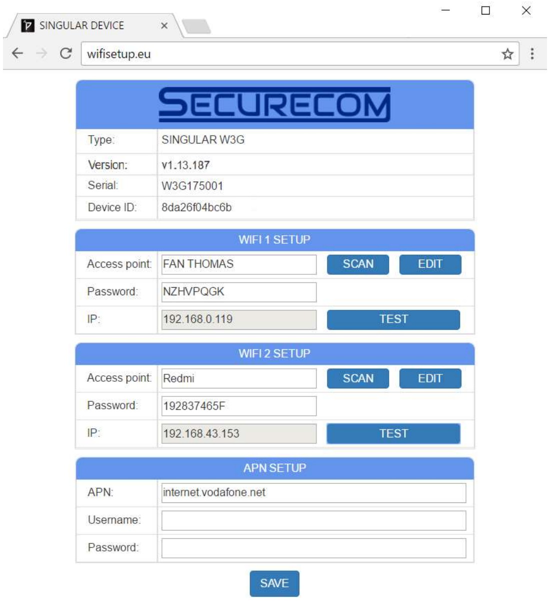
Apply a short press to the SETUP button and the status LED will start blinking green/red alternately, displaying that device is in HOTSPOT mode.

Warning: If the setup button is held pushed for longer than 3 seconds, device will start the “reset procedure”. When LEDs stop blinking, the reset is finished. All settings are restored to default, and a command is sent to Server, device requests to be removed from all accounts and all applications. Therefore, a complete reset can be done only while the device is online on server.

Open network selection page on your smartphone or pc and check the available WiFi networks. A **SECURECOM DEVICE** network should be in the list. Connect your device to that network and disable the mobile data connection. It is also useful to disable the mobile data connection while you want to connect to Securecom device, to avoid opening of real web site instead of device web page.
After connecting to **SECURECOM DEVICE** network, some smart devices will show an error, since the Internet connection is not available through this network. Ignore this message and open an Internet browser and go to **wifisetup.eu** address.

Your smart device should be connected to the **SECURECOM DEVICE** network when you open the site **wifisetup.eu.** if the page in your browser looks like the like picture on the left, your smart device has disconnected from SECURECOM DEVICE network and connected to some other network with internet access, or a mobile data connection is still on. Go to the chapter 4.2.2, and set your smart device as described in that chapter.

When you open the web page of ***Securecom*** device, the browser will display it’s page:



Type:	SINGULAR W3G
Version:	v1.13.187
Serial:	W3G175001
Device ID:	8da26f04bc6b

WIFI 1 SETUP

Access point:	FAN THOMAS
Password:	NZHVPQGK
IP:	192.168.0.119

WIFI 2 SETUP

Access point:	Redmi
Password:	192837465F
IP:	192.168.43.153

APN SETUP

APN:	internet.vodafone.net
Username:	
Password:	

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.	Enter the appropriate APN	->	Type the APN of cellular network
6.	Save the settings and restart in normal mode	->	Click on the SAVE button

To switch from hotspot to regular mode without saving the entered values, press the SETUP button. This will restart the device in regular mode, and it will try to connect to a wireless network(s), according to last saved settings. When the connection is successful, the blinking green light on status LED will be showing the device is in normal status.

Once you have the green LEDs blinking, your device is connected to Internet and ready to use. As soon a device has connected to Internet, it will immediately check in to the Puloware service, and from that moment it becomes available for Puloware service. If default settings satisfie the needs, device can be added to smartphone application and handled with it. All additional settings s and additional features should be set on www.puloware.com web site. This site also provides complete management for all devices that were added to the user account.

6. REQUIRED SETTINGS OF THE SECURITY SYSTEM

In the communication settings of the connected alarm system, the following actions are required:
– Phone communication should be enabled in the alarm centre
– DTMF (Tone) dialling should be selected
– A minimum 4 digit phone number should be set for dialling (anything is acceptable, e.g. 1111)
– Object identifier should be set
– Contact ID (Full) should be selected

1. It should be set, that disarm event can generates report after every disarm (not only after an alarm)

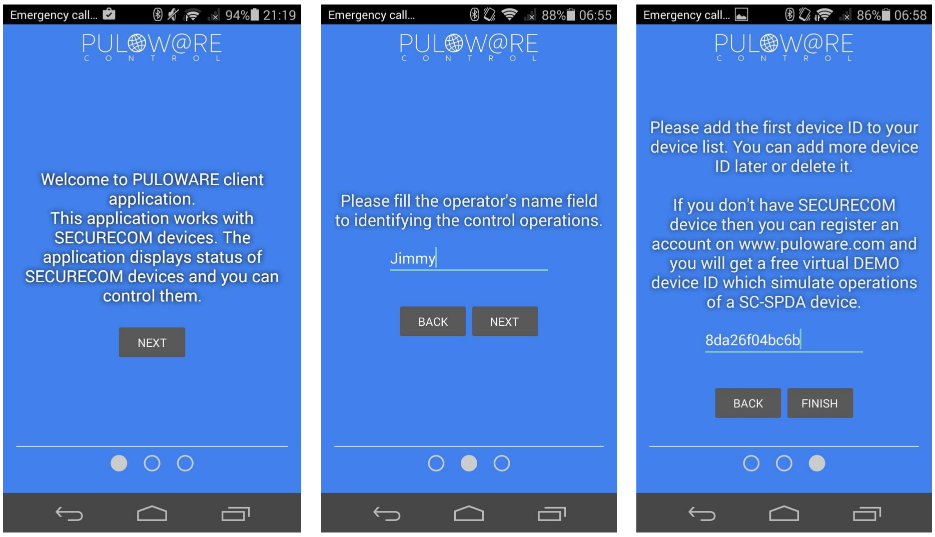
After that the module receives the signals of the alarm centre as a remote monitoring receiver, and forwarding those to the receiver.

The alarm system arm/disarm control happens by 1 second relay pulses, starting by the in application. Thus the arm/disarm zone inputs, arming/disarming the alarm, should be set to momentary key switch, using NC type

7. SMARTPHONE APPLICATION

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

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 you must define the device that you want to control with this application. You can enter the serial number or present the QR code of the device. Both serial number and QR code on the sticker, on the back of the device. For the QR code reader, click on the small icon next to the serial number field.
When the device number and password are provided, finish the setup.



Emergency call... 94% 21:19

PULOWARE CONTROL

Welcome to PULOWARE client application.
This application works with SECURECOM devices. The application displays status of SECURECOM devices and you can control them.

NEXT

Emergency call... 88% 06:55

PULOWARE CONTROL

Please fill the operator's name field to identifying the control operations.

Jimmy

BACK NEXT

Emergency call... 86% 06:58

PULOWARE CONTROL

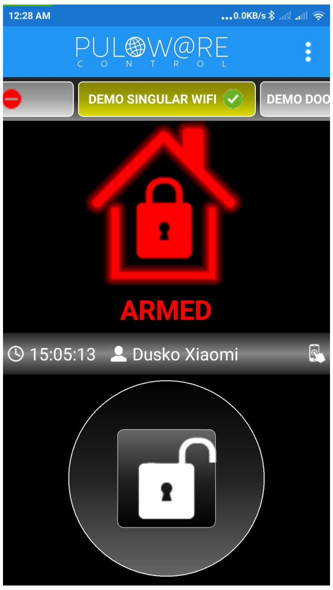
Please add the first device ID to your device list. You can add more device ID later or delete it.

If you don't have SECURECOM device then you can register an account on www.puloware.com and you will get a free virtual DEMO device ID which simulate operations of a SC-SPDA device.

8da26f04bc6b

BACK FINISH

If a wrong serial number or password were entered, the application will exit. If you start the application again, it will start from the same page as on the first run- requiring identification. If a device was successfully added, opened application will present this “main screen”:



12:28 AM ...0.0KB/s

PULOWARE CONTROL

DEMO SINGULAR WIFI ✓ DEMO DOO

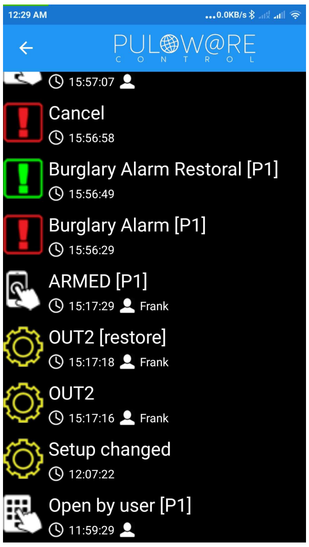
ARMED

15:05:13 Dusko Xiaomi

This application can be used to handle more than one device.
All other devices (different device types as well) should be added with the “New device” tab, positioned on the right end of the tab bar. In the tab bar each device tab shows it’s device serial number, or the “name” of the device (if a device name was set). You can set the device name from the application, or on puloware site.
The bottom of screen is providing a control button.If you hold it down 3 seconds, until the full circle around it is “filled”, the application sends a command to the communicator to activate the output (keyswitch), thus the alarm panel will change it’s status Armed/Disarmed.
Status of the alarm panel is shown with the color of the small house, and a text below it.
The middle area of screen shows the last event, providing the information of WHO changed the status of alarm panel.

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

The menu icon is placed on the top right corner. Clicking on it , 3 menu points are available:



12:29 AM

15:57:07

Cancel
15:56:58

Burglary Alarm Restoral [P1]
15:56:49

Burglary Alarm [P1]
15:56:29

ARMED [P1]
15:17:29 Frank

OUT2 [restore]
15:17:18 Frank

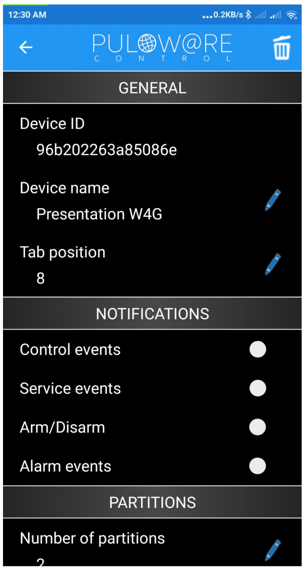
OUT2
15:17:16 Frank

Setup changed
12:07:22

Open by user [P1]
11:59:29

1. Operator (to change the *User name* of the phone, i.e application authentication)

2. Events (to see the list of events in alarm system, along with identification and customized event names)



12:30 AM

GENERAL

Device ID
96b202263a85086e

Device name
Presentation W4G

Tab position
8

NOTIFICATIONS

Control events

Service events

Arm/Disarm

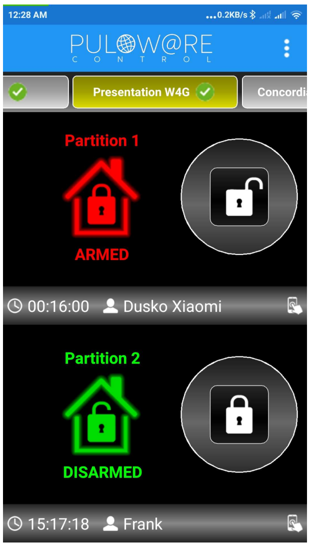
Alarm events

PARTITIONS

Number of partitions
2

3. Settings : In this screen, You can see the device serial number, edit the device name, or change the “tab position” value, which will change the order of device tabs in the main screen.
You can also select which type of event will be notified on this smart device with a push notification. All events are divided into 4 groups. Turning the switch “off” next to the name of group will prevent Push notifications for the events that belong to that group.
On the lower part of screen are options where a number of partitions can be changed (1 or 2), and the name of partitions can be entered.
Options on the bottom of the screen are used to create button on the phone main screen, for direct control of device outputs.

To remove the device from the application, use the basket on the right top corner. This will remove the device only from your phone, will not affect other accounts or smartphone users.



12:28 AM

Presentation W4G

Concordi

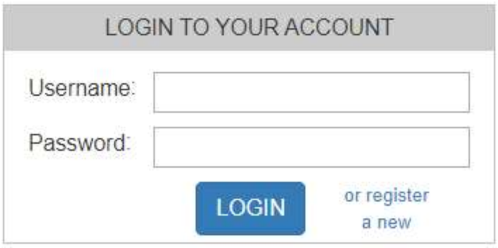
Partition 1
ARMED
00:16:00 Dusko Xiaomi

Partition 2
DISARMED
15:17:18 Frank

If you select to have 2 partitions, the main screen of the device will change. The first control button (next to the first house) is for manipulation of partition 1, and the house next to it is showing the status for partition1. Last event for each partition are shown separately.

NOTE: The alarm panel must be properly programmed and connected to the device, in order to have the application working correctly. Please, check the chapter 8 for the list of required settings in alarm panel.

8. ADDITIONAL SETTINGS AND FEATURES - WEB PAGE ON PULOWARE SERVICE

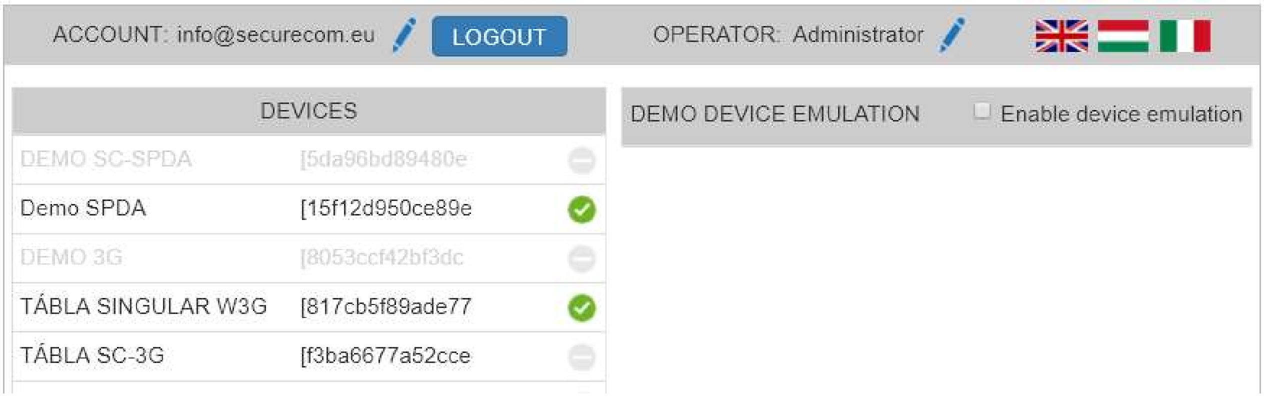


LOGIN TO YOUR ACCOUNT

Username:

Password:

An account must be created, and after logging in to personal account, the site will provide a list of all devices that were added to that account.



ACCOUNT: info@securecom.eu

OPERATOR: Administrator

DEVICES		
DEMO SC-SPDA	[5da96bd89480e	⊖
Demo SPDA	[15f12d950ce89e	✓
DEMO 3G	[8053ccf42bf3dc	⊖
TÁBLA SINGULAR W3G	[817cb5f89ade77	✓
TÁBLA SC-3G	[f3ba6677a52cce	⊖

DEMO DEVICE EMULATION ☐ Enable device emulation

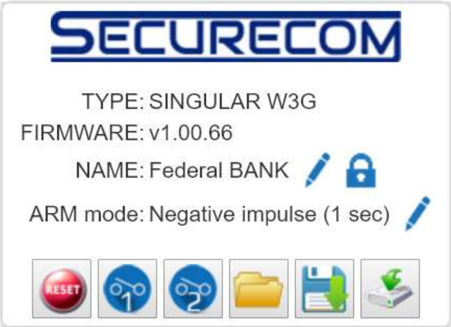
To add the device to your account, a serial number of the device (printed on the sticker, on device back) and the password are required. Initially, the password is BLANK, but it is strongly suggested to change it after the device was set up, to void unauthorized access to the device.

NOTE: in case that the device was already added or the number is invalid, the server will „kick you 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 on the right side of screen. 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.

8.1. Device Information area

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



TYPE: SINGULAR W3G

FIRMWARE: v1.00.66

NAME: Federal BANK

ARM mode: Negative impulse (1 sec)

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.

✐✍🗁✍🗁✍ Controll icons

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

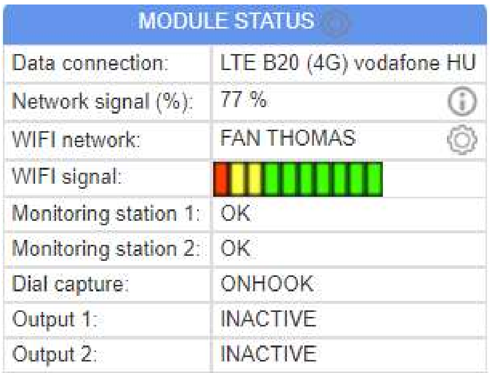
Save displayed settings to a file

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

✐✍🗁✍🗎✍ Device password

Clicking on the 🔒 icon a “Change Password” dialog is opened, where you can add or change the device password. This password is requested when the you want to add the device to a puloware account or to your smartphone application. By default, this password is EMPTY (no characters).

8.2. Device status display

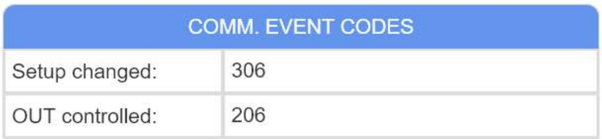


MODULE STATUS	
Data connection:	LTE B20 (4G) vodafone HU
Network signal (%):	77 % ⓘ
WIFI network:	FAN THOMAS ⚙
WIFI signal:	🟥🟨🟨🟩🟩🟩🟩🟩🟩🟩
Monitoring station 1:	OK
Monitoring station 2:	OK
Dial capture:	ONHOOK
Output 1:	INACTIVE
Output 2:	INACTIVE

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.

Addinional information is available under the small icon ⓘ, next to the network signal. Clocking on it will present the ICC ID of the SIM card

8.3. Communicator Events

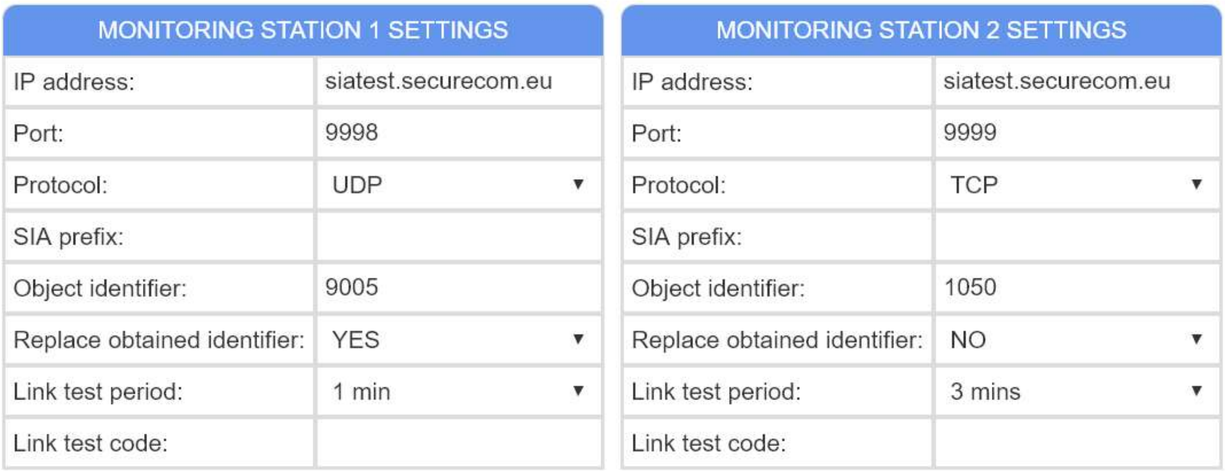


COMM. EVENT CODES	
Setup changed:	306
OUT controlled:	206

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 and OFF.

8.4. Monitoring station settings

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



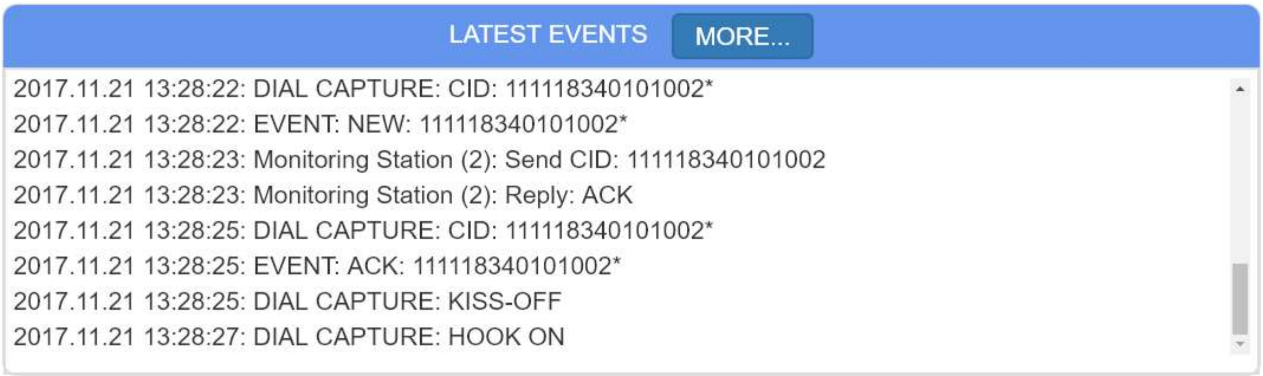
MONITORING STATION 1 SETTINGS	
IP address:	siatest.securecom.eu
Port:	9998
Protocol:	UDP ▼
SIA prefix:	
Object identifier:	9005
Replace obtained identifier:	YES ▼
Link test period:	1 min ▼
Link test code:	

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.

8.5. Communication details

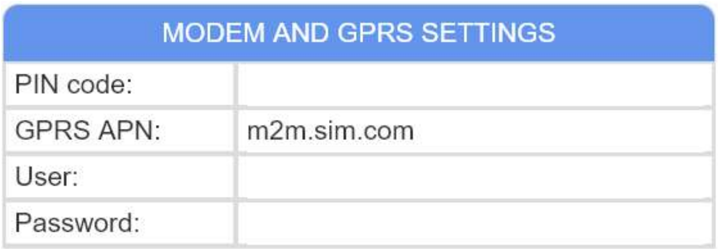
This area presents a detailed communication between the Alarm panel and monitoring receiver.
All messages and feedback data, as well as error messages are presented with a source and a time stamp (date, hour, minute, second), when was the signal received.



```
2017.11.21 13:28:22: DIAL CAPTURE: CID: 111118340101002*
2017.11.21 13:28:22: EVENT: NEW: 111118340101002*
2017.11.21 13:28:23: Monitoring Station (2): Send CID: 111118340101002
2017.11.21 13:28:23: Monitoring Station (2): Reply: ACK
2017.11.21 13:28:25: DIAL CAPTURE: CID: 111118340101002*
2017.11.21 13:28:25: EVENT: ACK: 111118340101002*
2017.11.21 13:28:25: DIAL CAPTURE: KISS-OFF
2017.11.21 13:28:27: DIAL CAPTURE: HOOK ON
```

8.6. Mobile data connectivity settings

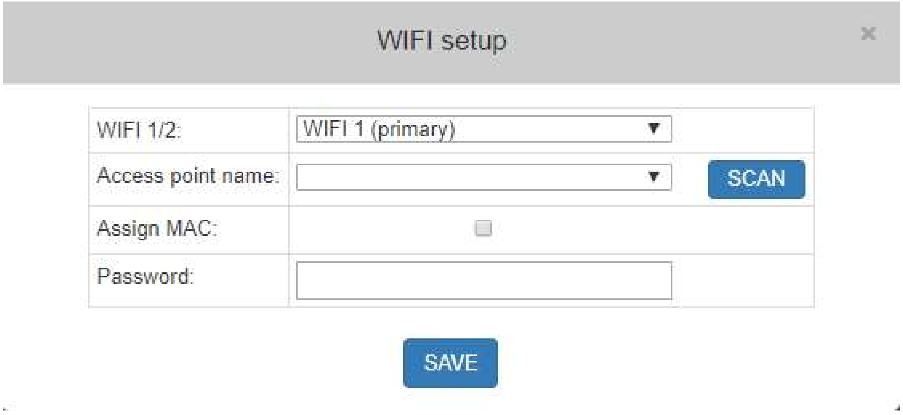
The *SINGULAR* device backup connection parameters can be remotely changed.



MODEM AND GPRS SETTINGS	
PIN code:	
GPRS APN:	m2m.sim.com
User:	
Password:	

8.7. Wifi network management

Using the ⚙ icon next to Wifi network name in "Module Status" area, you can open the dialog where the wifi network settings can be changed.



WIFI 1/2:	WIFI 1 (primary) ▼	
Access point name:	▼	SCAN
Assign MAC:	□	
Password:		

This dialog is not showing the valid settings in ***Securecom*** device. Fields are showing empty space, so after adding a new value and a click to "save button, the new values will be loaded to the device. Therefore, this dialog is used just to CHANGE (load new) settings for Wifi connection.

You can select which settings you want to change, the Primary or Secondary network. Clicking on "scan" button, you will get a list of available networks, with the signal strength. Select one network and enter the appropriate Password for that network. Clicking on "Save" button, the settings woll be loaded to the device and it will restart with these new settings.

In case when device can not connect to the Wifi network with the new settings, it will restart with restored previous settings for Wifi network.

The “Assign MAC “ option will lock the connection to the selected access point. This should be used in case when the device is installed in a position where multiple SSID with same names are visible. This way the device will always connect to same access point (node) after every restart.

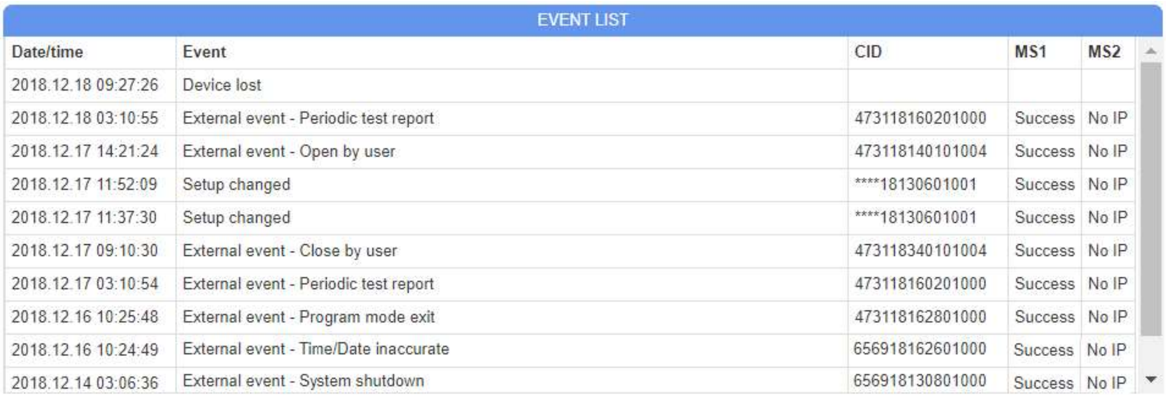
8.8. Special Se DANGER

In case of wrong settings of fields explained in this chapter, you can cut-off the connection of device to server or monitoring station. Please be sure that this area is handled extremely carefully, changed data is surely correct. In case that some detail in this chapter is not clearly explained, please turn to technical support.

The special dialog on Puloware web site is opened with a “gearbox” icon, next to “Module Status” header. In these two fields, you can limit the path for communication to Puloware server, and to monitoring station receivers. Both fields provide options “Wifi + Mobile data” (default value) and “Mobile data only”, while the connection to server also shows the “wifi only” option.
Changing the value in the server connection field to “mobile data only” or “ wifi only” will prevent the device to use the other connection method. This means there will be no redundant connection to server, so if the selected connection is faulty (for example internet connection of the wifi network is lost), the device will be disconnected from the server (offline),until the selected connection method is fixed.
Changing the default value in the “connection to monitoring” field to “ mobile data only” will result that device will be sending all reports to monitoring station through the data network, it will never use the Wifi for reporting to MS1 or MS2. This option is useful if the receiver in monitoring station is working ina VPN, and can not be accessed from Internet.
If some event fits to more than one filterin the table, it will be displayed with the first event name in the table where the settings fit the occured event. Events are checked in the table from the top to bottom, and when a match is found, the comparation is finished and the event is displayed with that name.

8.9. Event list

This table shows last 10 events that happened in system, and you can scroll the table down for some older events. It contains all events that were reported by alarm panel (marked as „External events”) and the events that happened with communicator itself, regardles if they are being reported or not (Device lost, output controlled, setup changed,...).



EVENT LIST

Date/time	Event	CID	MS1	MS2
2018.12.18 09:27:26	Device lost			
2018.12.18 03:10:55	External event - Periodic test report	473118160201000	Success	No IP
2018.12.17 14:21:24	External event - Open by user	473118140101004	Success	No IP
2018.12.17 11:52:09	Setup changed	****18130601001	Success	No IP
2018.12.17 11:37:30	Setup changed	****18130601001	Success	No IP
2018.12.17 09:10:30	External event - Close by user	473118340101004	Success	No IP
2018.12.17 03:10:54	External event - Periodic test report	473118160201000	Success	No IP
2018.12.16 10:25:48	External event - Program mode exit	473118162801000	Success	No IP
2018.12.16 10:24:49	External event - Time/Date inaccurate	656918162601000	Success	No IP
2018.12.14 03:06:36	External event - System shutdown	656918130801000	Success	No IP

Besides the Time/date of event and it’s name (as it is defined in „Event filter” table), table also shows the complete CID message in it’s raw format, and the status of reporting to MS1 and MS2 receivers. If reporting to one Monitoring Station receiver was sucessfull, reporting to the other will show „Ignore”. This means that since message was delivered to one receiver, communicator will not continue transmiting it.

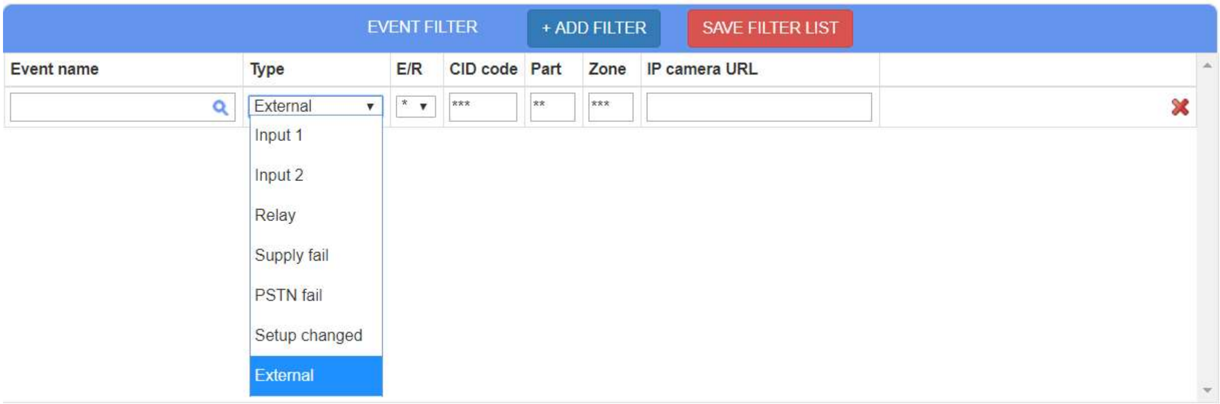
As the MS2 is the Backup receiver, all messages will be sent to MS1 first, and if the acknowledge fails, they will be sent to MS2. If both acknoledges fail, the status will be „stored" or „timeout", depending on the source of event.

Best way to check if the communicator is connected and the alarm panel is set properly, is to generate a specific event in alarm system (for example, Alarm in zone 002). When the desired event has occured, Alarm panel should „report the event" to the communicator, and the occured event should appear on the top of the Event list with a default name.

If you generate a specific event in the alarm system and it does not appear in the event list. Settings of alarm panel (communication settings) are wrong, or the connection on „Ring" and „ Tip" terminals are bad.

8.10. Event filter

Using this table, you can personalise the messages on your smartphone application. All events named in this table will also affect the event names shown in „Event list" table.
With „ADD Filter" button you can open a new line to add a new filter.



Event name	Type	E/R	CID code	Part	Zone	IP camera URL
	External	*	***	**	***	

Select the event that you want to rename or select „External" if you want to rename a event that is comming from an alarm system. In that case you must also enter values in the other fields, to fit the Contact ID string that is sent from the alarm panel when the required event has occured:

- The field „E/R" represents the „Event/restore" field of the Contact ID messagr (sometimes it is sent as number 1 or 3).
- „CID code" field must fit the 3-figure event code from sent Conact ID message (in „Standard Event code table" it is 130 for Burglary, 401 for Arming/disarming, 300 for system trouble...).
- „Part" Field should fit the PARTITION NUMBER in the sent Contact ID message
- „ZONE" field should fit the User/zone field of the sent Contact ID message
- „Event name" is the field where the new name of the selected event should be put. This label will show in both event list (puloware web site) and in the application.
- The „Camera URL field is attended for a future functions. For now, it wil just add link in a form of small camera next to the corresponding event in the event list. Clicking on the camera will cause opening a new browser page, with URL that was enterd in this field.

A „star" for value means „any figure". For example, a value „13*" for CID code will result that any CID code from 130 to 139 will"fit" this filter. Therefore, if you do not want to „ filter by zone" (for example, name all burglary events „ ALARM", put the stars in „zone" field. If you want to name the zone, you have to make one filter for each zone with the event that you want to name („Burglary in kitchen" for CID 130 and zone 001, „Motion detected in sleeping room” for CID 130 in zone 003, „detector in kitchen tampered” for code 137 with zone 001, etc.)

Most accurate way to rename some specific event from your alarm system is to create the required event in the alarm panel. And rename it with Puloware server, following these instructions:

1. *Create a new line in event filter table (with „add filter” button), and Select the „external” in „type” field*
2. *Put in the „event name” field he text that you want to be displayed when the selected event occures*
3. *Find the desired event in the event list*
4. *Select the 15 character long number next to the event, in the „CID” coloumn*
5. *From the 15 characters, check the 7th figure. If it is „1”, select the „E” in „E/R” field. If the figure is 3, select the „R”*
6. *Copy the next 3 figures to the „CID code” field*
7. *Copy the next two figures to the „Part” field*
8. *Copy the last 3 figures to the „Zone” field*

If the procedure was made correctly, the name of the event should immediatelly change to the desired name (that was put in the „Event name” field) in the event list table (Web page of the device), and also in the event list presented on Smartphone application.

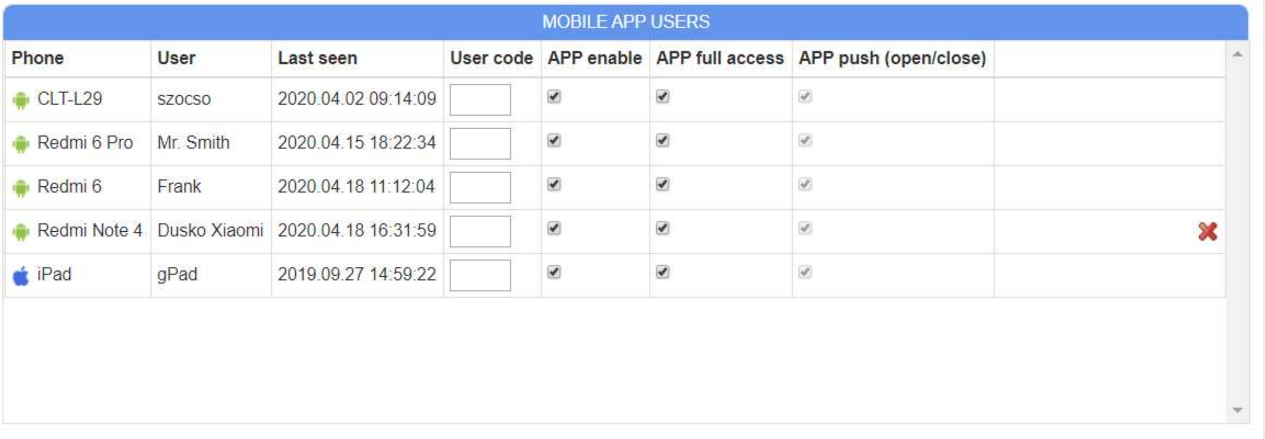
8.11. Handling Alarm panel users

A „User codes” table is used to identify the users of the alarm system. This way, if some operation was made on the alarm system keypad (for example armed the area) the **User number** oin the alarm system can be assigned to a name in the Puloware system. For example, if John is „user 3” in the alarm system, entering this name with number 003 in this table will result that on puloware platform all operations made with this code will be displayed with name John. (Area armed user John)

With „add code” button a new line is opened in the table, where you can enter a new name and it’s user number in the alarm system. Entered data will be saved only after you click the „Save code list”. If the page was leaved without saving, all data that was entered without saving will be lost

8.12. Handling smartphone users

When a specific device from device list is selected and thus the site that prents settings of that device is shown, all smartphones with „Puloware client” application where this device was added will be listed in this table. This table presents the type of the device and a „operator name” that was put during the application instalation on that phone. Besides that, you can see the time (with date) when was a last time when a specific device used to controll or monitor that communicator.
Also, a „User code” field is there in each smartphone line, where a 3 figure number can beentered. This number will be added az „zone number” in the Contact id report code that is sent to monitoring station when „Output controlled” event occures (as defined in section 6.3 of this manual). This way, the operator of the arm/disarm command to the alarm system wih smartphone application can also be identified to the monitoring station- in case that authentification is required later („ who disarmed the system with smartphone ?”) , it can be easilly traced.



MOBILE APP USERS

Phone	User	Last seen	User code	APP enable	APP full access	APP push (open/close)	
CLT-L29	szocso	2020.04.02 09:14:09		☑	☑	☑	
Redmi 6 Pro	Mr. Smith	2020.04.15 18:22:34		☑	☑	☑	
Redmi 6	Frank	2020.04.18 11:12:04		☑	☑	☑	
Redmi Note 4	Dusko Xiaomi	2020.04.18 16:31:59		☑	☑	☑	✖
iPad	gPad	2019.09.27 14:59:22		☑	☑	☑	

This table also alows the limitation of rights fora specific operator (smartphone), and clicking on the small red cross at the right end of each line (it appears when a mouse is bringed to that line) the communicator can be removed from that smartphone application. Naturally , the application restart is required for change to take effect.

The three checkboxes that are visible in each smartphone's line can be used to limt the rights of that smartphone, i.e that operator:

- „App enable" allows the operator to controll the output from his smartphone app. If the checkbox is selected, „arming" or „disarming" can be performed with the application in that smartphone
- „App full access" option allows the operator's access to the event list
- „App push" enables the sending of push notifications to that device. Naturally, in order to receive and signal the push notification, it must be also enabled in the apllication, for the particular type of event (under „settings"). In order for phone to handle push notifications, all requirements and authorisations in smartphone must be set properly and services running.

8.13. Upgrading device software

The botom of device web page provides two buttons that are used for device firmware upgrade. If you need to upgrade the device software, it is recomended to use the button on the bottom of the page, with a label „ Click here to beginthe device firmware update to the latest version in background". This will start the download of the latest available software version for this device type from Puloware server to the device. The process will be shown in the „Latest events" window, where the downloaded block number will be displayed. You can stop the download using the „stop" button. After the download is finished, the device will restart with the new software and the version number in the status area will show the new version number . If the downloaded file is corrupted (due to errors during download) or the downloaded version is same as the current version of the device, the download file will be dropped and device will restart with the old software. The download procedure can be started again with the same button.

If you have a special version of a firmware for your device (OEM device), you can use the „Select one from your disk" button, to select the appropriate file and start the file download. The flow of download will be displayed next to the button and when it is finished, the device will restart and try to use the downloaded file as it's software. In case of error, the downloaded file will be dropped and device will restart with software that it had before download.

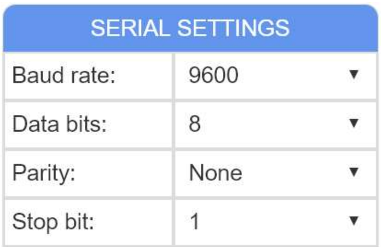
Avoid communication (commands, events from alarm panel,...) with the device during the firmware download. Any interference can defect the download matherial, and it will result with error in downloaded file on the end.

9. TRANSPARENT FORWARDING OF SERIAL PORT

Using this feature, you can remotely program any alarm panel from any place, you only need an internet connection to your laptop.
This way the remote connection oveffjfjr Mobile data network and Internet is replacing a physical “Serial cable”. So you can use the programming software same way as if the alarm panel was physically attached to the COM port. All signals (every bit) that come in on the *SINGULAR* physical serial port, goes out on the virtual com, and vice-versa. This „ tunnel connection” is going through the WiFi network and internet, and it is provided by the PULOWARE IoT server.

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 should 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.

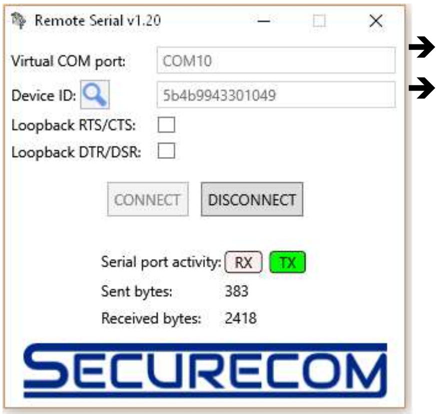


SERIAL SETTINGS	
Baud rate:	9600 ▾
Data bits:	8 ▾
Parity:	None ▾
Stop bit:	1 ▾

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. Download the setup for the remote serial software from the following link and install it on your machine : http://puloware.com/public/RemoteSerialSetup.exe

4. Run the software, select a free (not used) COM port for your machine, and enter the device ID of the Securecom device that is connected with the serial port of the alarm panel that you want to program remotely. Click “Connect”, and the COM port will be generated (you can also see it in a Windows device manager)



Remote Serial v1.20

Virtual COM port: COM10

Device ID: 5b4b9943301049

Loopback RTS/CTS: □

Loopback DTR/DSR: □

CONNECT DISCONNECT

Serial port activity: RX TX

Sent bytes: 383

Received bytes: 2418

➔ Serial port that is set for „ cable connection” in alarm panel software

➔ Communicator Serial number (written on sticker, on device backside)

5. Run the Alarm panel programming software (eg. WINLOAD, Babyware, DLS, Proste, ...). Select the COM port generated by “remote serial” software, and start the connection like if the panel was connected directly with programming cable to that COM port. As soon as the data is being transferred, the “serial port activity” will show the blinking that bytes were received, and sent.

10.TECHNICAL DATA

1. Supply Voltage	10.5 to 30V DC
2. Current consumption, idle	120mA
3. Current consumption, max.	500mA
4. Operating temperature	-20°C to +70°C

11.INSTALLATION AND PROGRAMMING 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 must be enabled and protocol must be set to Contact ID
- All events must be set for reporting (disarming without alarm, zone bypassing, ...)
- Alarm panel Inputs connected to communicator outputs must be set as “keyswitch inputs”, and appropriate resistors should be applied in the zone loop wiring.

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