



Cellular communicator G16

Installation manual

March, 2019

Contents

1	DESCRIPTION	4
1.1	List of compatible control panels	5
1.2	Communicator model types	5
1.3	Specifications	5
1.4	Communicator elements	6
1.5	Purpose of terminals	6
1.6	LED indication of operation	6
1.7	Structural schematic with G16 usage	7
2	QUICK CONFIGURATION WITH TRIKDISCONFIG SOFTWARE	8
2.1	Settings for connection with Protegus app	8
2.2	Settings for connection with Central Monitoring Station	9
3	INSTALLATION AND WIRING	11
3.1	Physical installation process	11
3.2	Schematics for wiring the communicator to a security control panel	12
3.3	Schematic for connecting to panel keyswitch zone	13
3.4	Schematics for input connection	14
3.5	Schematics for wiring a relay	14
3.6	Schematics for connecting iO series expansion modules	14
3.7	Schematic for connecting the W17u WiFi communicator	15
3.8	Turn on the communicator	15
4	PROGRAMMING THE CONTROL PANEL	16
5	REMOTE CONTROL	18
5.1	Adding the security system to Protegus app	18
5.2	Additional settings to arm/disarm the system using the control panel's keyswitch zone	18
5.3	Arming/disarming the alarm system with Protegus	19
5.4	Configuration and control with SMS messages	20
6	TRIKDISCONFIG WINDOW DESCRIPTION	21
6.1	TrikdisConfig status bar description	21
6.2	"System settings" window	22
6.3	"CMS reporting" window	23
6.4	"User reporting" window	25
6.5	"SIM card" window	27
6.6	"RS485 modules" window	27
6.7	"Event summary" window	30
6.8	Restoring factory settings	30
7	REMOTE CONFIGURATION	31
8	TEST COMMUNICATOR PERFORMANCE	31
9	FIRMWARE UPDATE	31

Safety requirements

The communicator should be installed and maintained by qualified personnel.

Prior to installation, please read this manual carefully in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

Disconnect the power supply before making any electrical connections.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.



Please act according to your local rules and do not dispose of your unusable alarm system or its components with other household waste.

1 Description

Cellular communicator **G16** directly connects to supported DSC, Paradox, UTC Interlogix (CADDX), Innerrange, Texecom, Honeywell, Crow and Pyronix alarm panels.

Communicator transmits full event information to the Central Monitoring Station.

Communicator also works with **Protegeus** application. With **Protegeus** users can control their alarm system remotely and get notifications about security system events. **Protegeus** app is compatible with all security alarm panels from various manufacturers that are supported by the **G16** communicator. Communicator can transmit event notifications to the Central Monitoring Station and work with **Protegeus** simultaneously.

Communicator **G16** can connect directly to DSC®, Paradox®, UTC Interlogix® (CADDX), Innerrange®, Texecom®, Honeywell®, Crow® and Pyronix® control panels. For panels from other manufacturers use the **G16T** communicator.

Features

Sends events to monitoring station receiver:

- Sends events to TRIKDIS software or hardware receivers that work with any monitoring software.
- Can send event messages to SIA DC-09 receivers.
- Connection supervision by polling to IP receiver every 30 seconds (or by user defined period).
- Backup channel, that will be used if connection with the primary channel is lost.
- Events can be reported to CMS with SMS messages. SMS will be sent even if data connection stops working in the mobile operator network.
- With parallel communication channels events can be sent to two receivers at same time.
- When Protegeus service is enabled, events are first delivered to CMS, and only then are sent to app users.

Works with Protegeus app:

- “Push” and special sound notifications informing about events.
- Remote system Arm/Disarm.
- Remote control of connected devices (lights, gates, ventilation systems, heating, sprinklers, etc.).
- Remote temperature monitoring (with iO or iO-WL expanders).
- Different user rights for administrator, installer and user.
- Users can also be informed about events with SMS messages and phone calls.

Notifies users:

- Users can be notified about events not only with Protegeus app, but also with SMS messages and a call.



Controllable outputs and inputs:

- 1 output, controlled via:
 - Protegeus app.
 - SMS message.
- 2 inputs, selectable type: NC; NO; NC/EOL; NO/EOL; NC/DEOL; NO/DEOL.
- Add additional inputs and controllable outputs with wired and wireless iO expanders.

Quick setup:

- Settings can be saved to file and quickly written to other communicators.
- Two access levels for configuring the device for CMS administrator and for installer.
- Remote configuration and firmware updates.

1.1 List of compatible control panels

Manufacturer	Model
DSC®	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020
PARADOX®	SPECTRA SP4000, SP5500, SP6000, SP7000, SP65
	MAGELLAN MG5000, MG5050, MG5050E
	DIGIPLEX EVO48, EVO192, EVOHD, NE96, EVO96
	SPECTRA 1727, 1728, 1738
	ESPRIT E55, 728ULT, 738ULT
UTC Interlogix®	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom®	Premier 24, 48, 88, 168
	Premier Elite 12, 24, 48, 64, 88, 168
Pyronix®	MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6, MATRIX 816
Innerrange®	Inception
Honeywell®	Ademco Vista-5, Ademco Vista-20, Ademco Vista-48
Crow®	Runner 4/8, Runner 8/16

*Connect control panels from other manufacturers to the **G16T** communicator.

1.2 Communicator model types

This manual applies to these **G16** models:

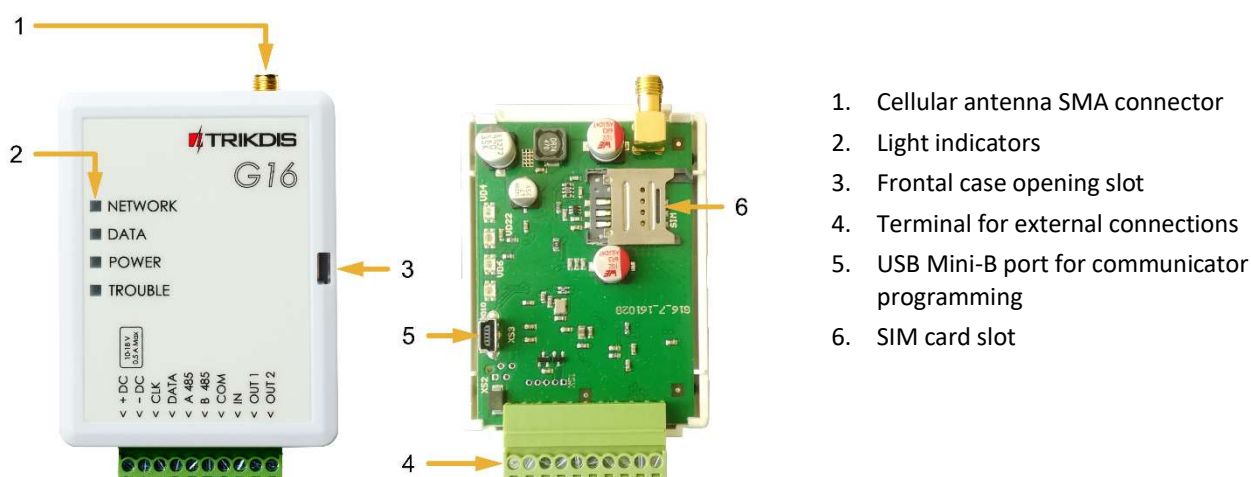
- G16_321x – 3 version, 1 SIM, 2G modem
- G16_331x – 3 version, 1 SIM, 3G modem
- G16_341x – 3 version, 1 SIM, 4G modem
- G16_3M10 – 3 version, 1 SIM, LTE CatM1 & EGPRS modem.

1.3 Specifications

Parameter	Description
Inputs	1 selectable type input: NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL. Expandable with iO series expanders.
Output	2, OC type, commutating up to 0,15 A, 30 VDC max. Expandable with iO series expanders.
2G modem frequencies	850 / 900 / 1800 / 1900 MHz
3G modem frequencies	800 / 850 / 900 / 1900 / 2100 MHz
4G modem frequencies	Depends on region
Power supply voltage	10-18 V DC
Current consumption	60-100 mA (on standby) Up to 250 mA (while sending data)
Transmission protocols	TRK, DC-09_2007, DC-09_2012
Message encryption	AES 128
Changing settings	With TrikdisConfig computer program remotely or locally via USB Mini-B port Remotely with SMS messages

Parameter	Description
Operating environment	Temperature from -10 °C to 50 °C, relative humidity - up to 80% at +20 °C
Communicator dimensions	92 x 65 x 26 mm
Weight	80 g

1.4 Communicator elements



1.5 Purpose of terminals

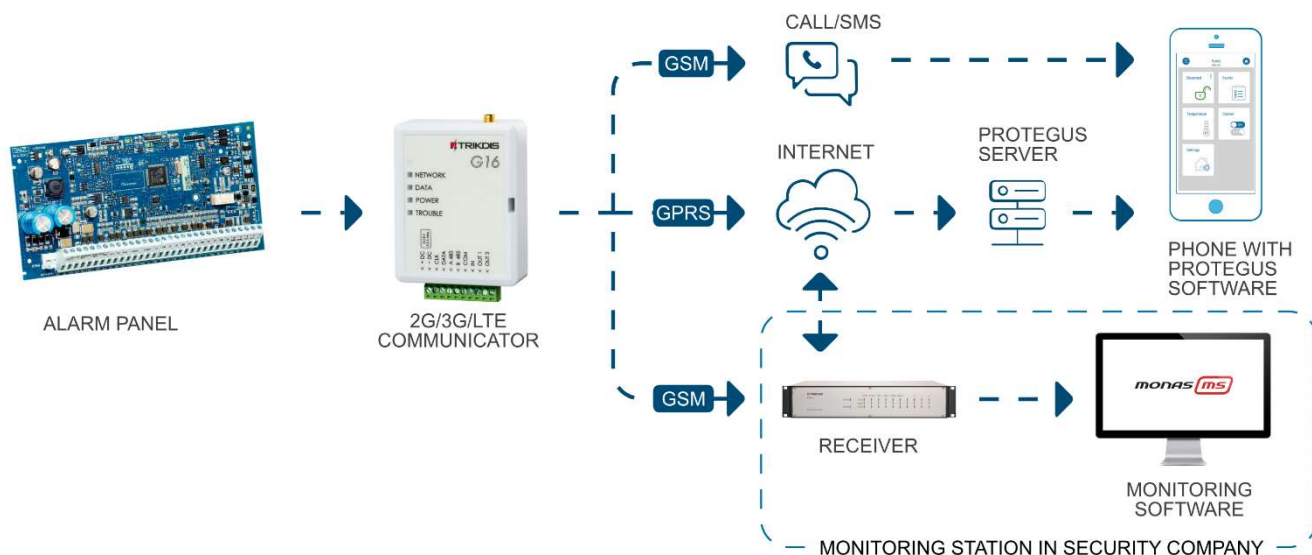
Terminal	Description
+DC	+10 V/+18 V power supply
-DC	+10 V/+18 V power supply
CLK	Serial bus terminals for direct connection to control panel
DATA	
A 485	RS485 bus A contact
B 485	RS485 bus B contact
COM	Common (negative) terminal
IN	Input
OUT1	1 st open-collector output
OUT2	2 nd open-collector output

1.6 LED indication of operation

Indicator	Light status	Description
NETWORK	Off	No connection to cellular network
	Yellow blinking	Connecting to cellular network
	Green solid with yellow blinking	Communicator is connected to cellular network. Sufficient cellular signal strength for 2G is level 5 (five yellow flashes) and for 3G level 3 (three yellow flashes)
DATA	Off	No unsent events

Indicator	Light status	Description
POWER	Green solid	Unsent events are stored in buffer
	Green blinking	(Configuration mode) Data is being transferred to/from communicator
	Off	Power supply is off or disconnected
	Green solid	Power supply is on with sufficient voltage
	Yellow solid	Power supply voltage is insufficient ($\leq 11.5V$)
	Green solid and yellow blinking	(Configuration mode) Communicator is ready for configuration
	Yellow solid	(Configuration mode) No connection with computer
TROUBLE	OFF	No operation problems
	1 red blink	SIM card not found
	2 red blinks	SIM card PIN code problem (incorrect PIN code)
	3 red blinks	Programming problem (No APN)
	4 red blinks	Registration to GSM network problem
	5 red blinks	Registration to GPRS/UMTS network problem
	6 red blinks	No connection with the receiver
	7 red blinks	Lost connection with control panel
	Red blinking	(Configuration mode) Memory fault
	Red solid	(Configuration mode) Firmware is corrupted

1.7 Structural schematic with G16 usage



Note:

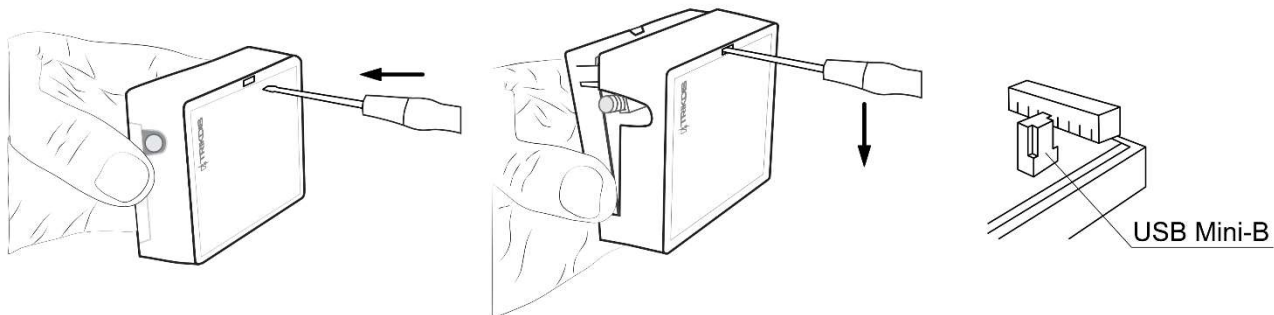
Before you begin, make sure that you have the necessary:

- 1) USB cable (Mini-B type) for configuration.
- 2) At least 4-wire cable for connecting communicator to control panel.
- 3) CRP2 cable for connecting to Paradox panel's serial port.
- 4) Flat-head 2,5 mm screwdriver.
- 5) Sufficient gain cellular antenna if network coverage in the area is poor.

- 6) Activated SIM card (PIN code request can be turned off).
 - 7) Particular security control panel's installation manual.
- Order the necessary components separately from your local distributor.

2 Quick configuration with *TrikdisConfig* software

1. Download **TrikdisConfig** configuration software from www.trikdis.com (type "TrikdisConfig" in the search field) and install it.
2. Open the casing of the **G16** with a flat-head screwdriver as shown below:

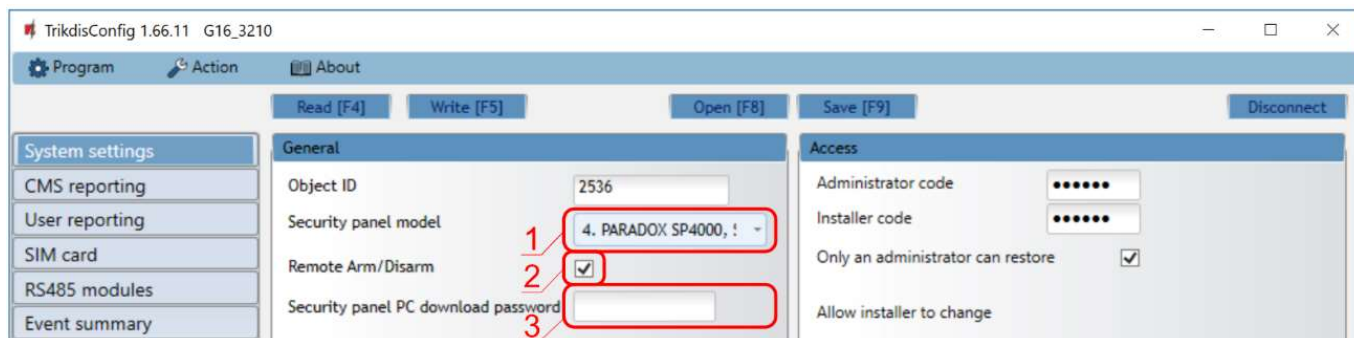


3. Using a USB Mini-B cable connect the **G16** to the computer.
4. Run **TrikdisConfig**. The software will automatically recognize the connected communicator and will open a window for configuration.
5. Click **Read [F4]** to read the communicator's settings. If requested, enter the Administrator or Installer 6-digit code in the pop-up window.

Below we describe what settings need to be set for the communicator to begin sending events to the Alarm Receiving Center and to allow the security system to be controlled with the **Protegeus** app.

2.1 Settings for connection with Protegeus app

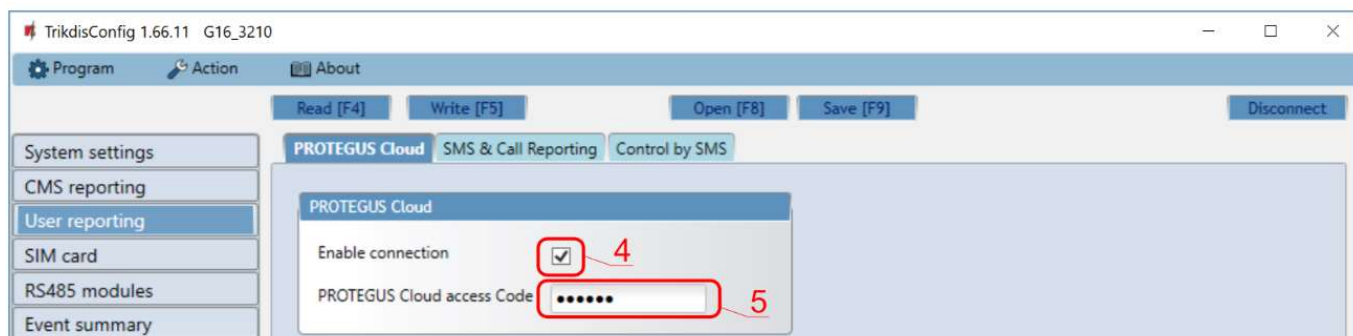
In "System settings" window:



- 1) Select **Panel type** that will be connected to the communicator.
- 2) Select **Remote Arm/Disarm** if you want users to be able to control the panel in **Protegeus** app with their keypad code. This setting is only shown for directly controlled panels.
- 3) For the direct control of Paradox and Texecom panels enter **Panel PC download password**. It must match the password that is entered in the control panel.

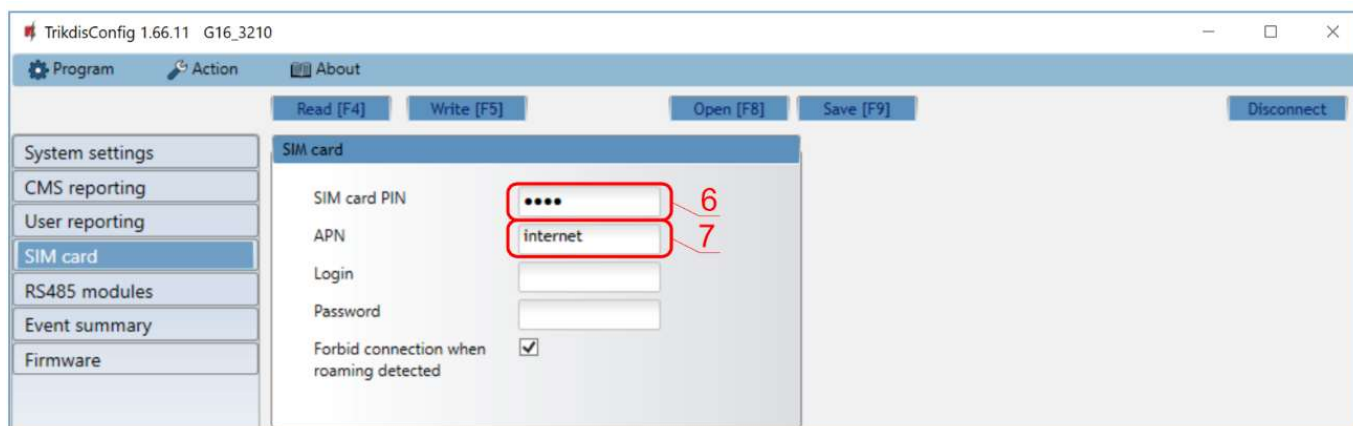
Note: For the direct panel control to work, you will need to change the panel settings. How to do this is described in chapter 4 "Programming the control panel". In this section you will find information on how to change the PC download/UDL password.

In “User reporting” window, “PROTEGUS Cloud” tab:



- 4) Tick the checkbox **Enable connection** to the **Protegeus** Cloud.
- 5) Change the **Cloud access Code** for logging in to **Protegeus** if you want users to be asked to enter it when adding the system to **Protegeus** app (default password – 123456).

In “SIM card” window:



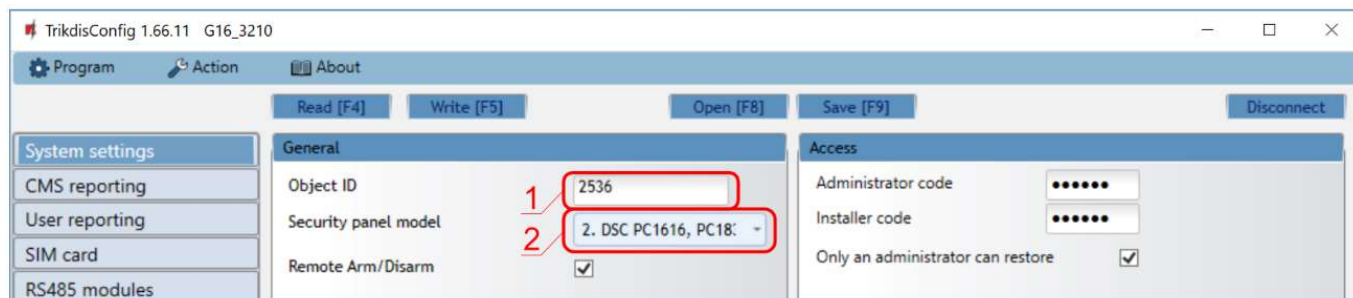
- 6) Enter **SIM card PIN** code.
- 7) Change **APN** name. **APN** can be found on the website of the SIM card operator (“internet” is universal and works in many operator networks).

After finishing configuration, click the button **Write [F5]** and disconnect the USB cable.

Note: For more information about other **G16** settings in **TrikdisConfig**, see chapter 6 “TrikdisConfig window description”.

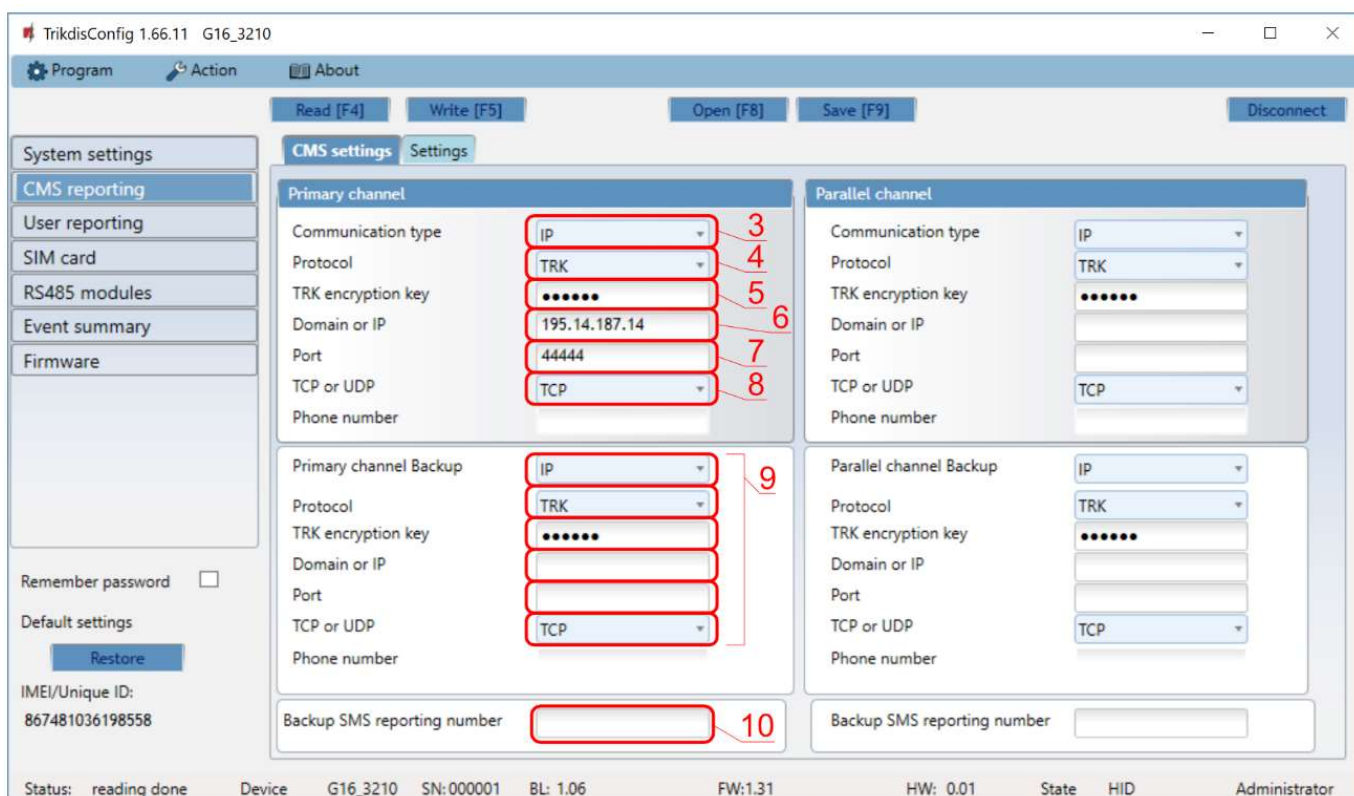
2.2 Settings for connection with Central Monitoring Station

In “System settings” window:



- 1) Enter **Object ID** (account) number provided by the Central Monitoring Station (4 characters, 0-9, A-F).
- 2) Select **Panel type** that will be connected to the communicator.

In “CMS reporting” window settings for “Primary channel”:



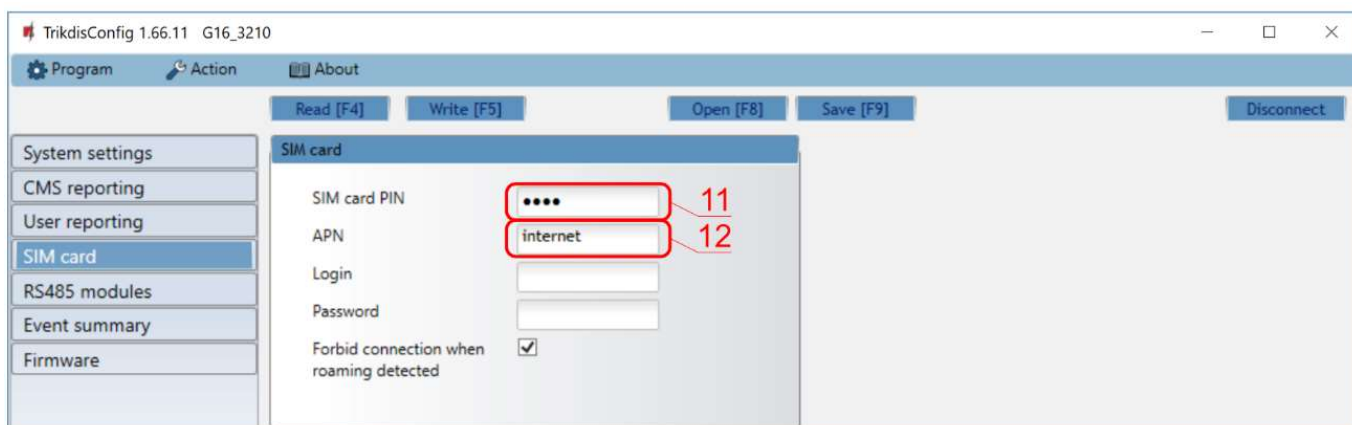
- 3) **Communication type** - select the **IP** connection method (We do not recommend SMS as the primary channel).
- 4) **Protocol** - select the protocol type for event messages: **TRK** (to TRIKDIS receivers), **DC-09_2007** or **DC-09_2012** (to universal receivers).
- 5) **TRK encryption key** - enter the encryption key that is set in the receiver.
- 6) **Domain or IP** - enter the receiver's Domain or IP address.
- 7) **Port** - enter receiver's network port number.
- 8) **TCP or UDP** - choose event transmission protocol (**TCP** or **UDP**) in which events should be sent.

Note: If you want to set communication with CMS via **SMS** messages, you only need to set **Encryption key** and **Phone number**. SMS messages can be received only by TRIKDIS receivers: IP/SMS receiver RL14, multichannel receiver RM14 and SMS receiver GM14.

If you selected the **DC-09** protocol, additionally enter object, line and receiver numbers in the **Settings** tab of the **CMS reporting** window.

- 9) (Recommended) Configure **Primary channel Backup** settings.
- 10) (Recommended) Enter **Backup SMS reporting number**.

In “SIM card” window:



11) Enter **SIM card PIN** code.

12) Change the **APN** name. **APN** can be found on the website of the SIM card operator (“internet” is universal and works in many operator networks).

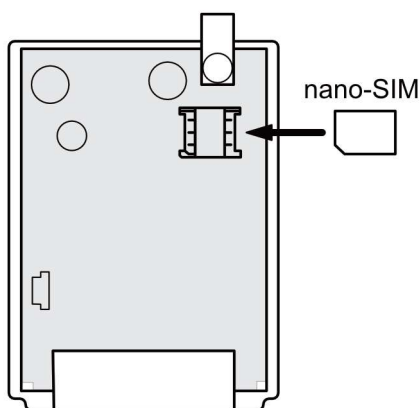
After finishing configuration, click **Write [F5]** and disconnect the USB cable.

Note: For more information about other **G16** settings in **TrikdisConfig**, see chapter 6 “TrikdisConfig window description”.

3 Installation and wiring

3.1 Physical installation process

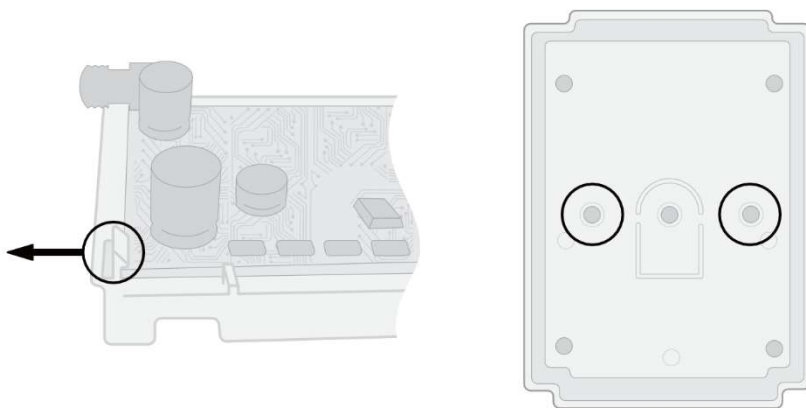
- 1) Remove the top cover and pull out the contact terminal.
- 2) Insert SIM card into the holder:



Note:

- Ensure that the SIM card is activated.
- Ensure that mobile internet service (mobile data) is enabled if connected via IP channel.
- To avoid entering the PIN code in **TrikdisConfig**, insert the SIM card into your mobile phone and turn off the PIN request function.

- 3) Remove the PCB board from the bottom part of the case.
- 4) Fix the bottom part to a suitable place with screws.



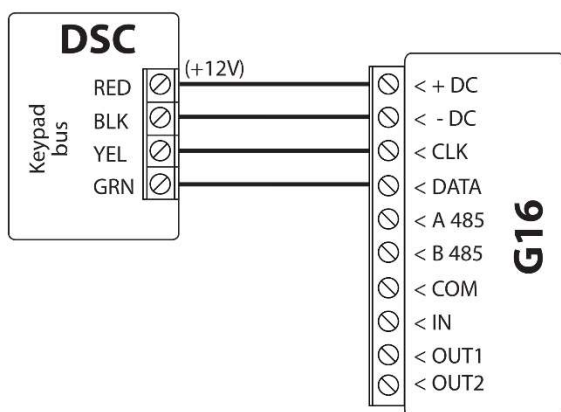
- 5) Place the PCB board back into case, insert contact terminal.
- 6) Screw cellular antenna on.
- 7) Close the top cover.

3.2 Schematics for wiring the communicator to a security control panel

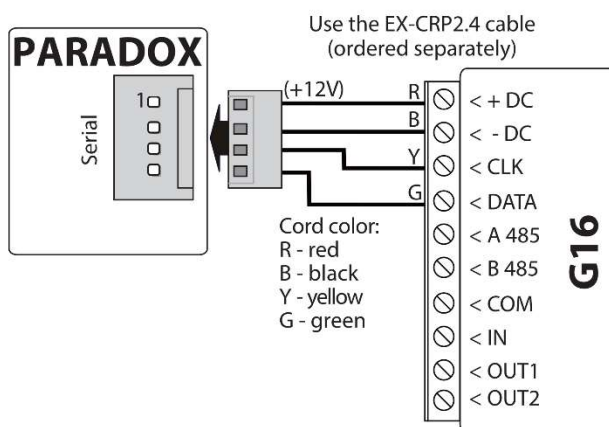
Following one of the schematics provided below, connect communicator to the control panel.

1. Schemes for connecting to the security control panels:

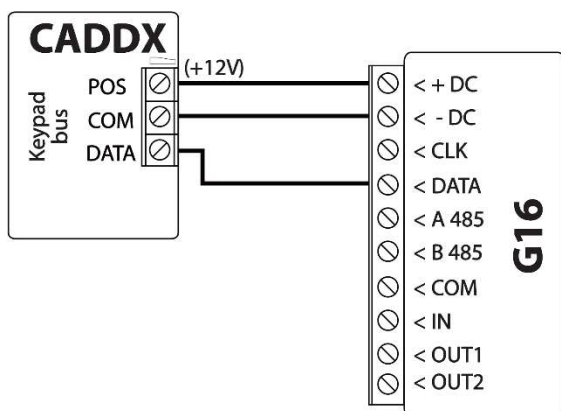
DSC panel connection diagram



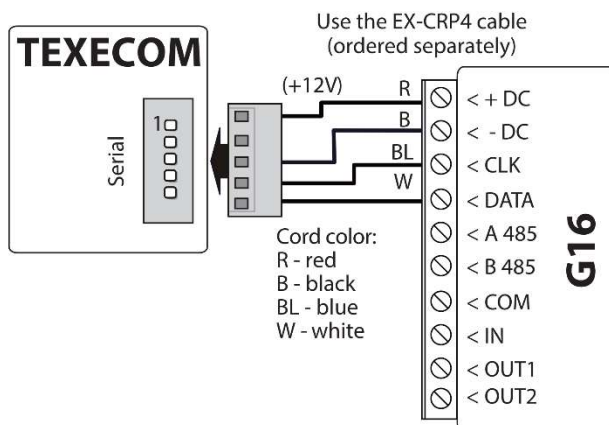
PARADOX panel connection diagram

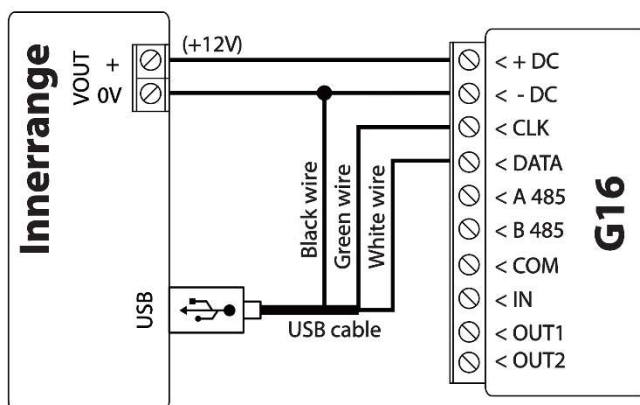
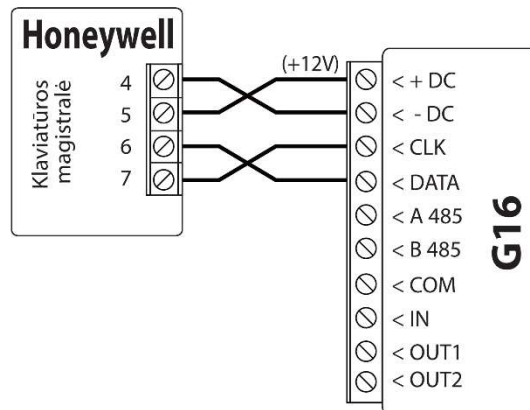
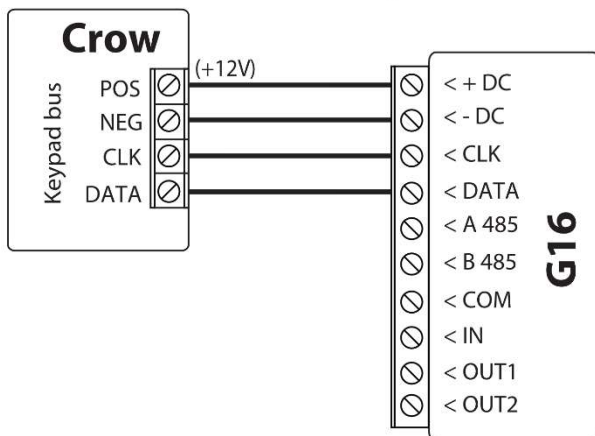
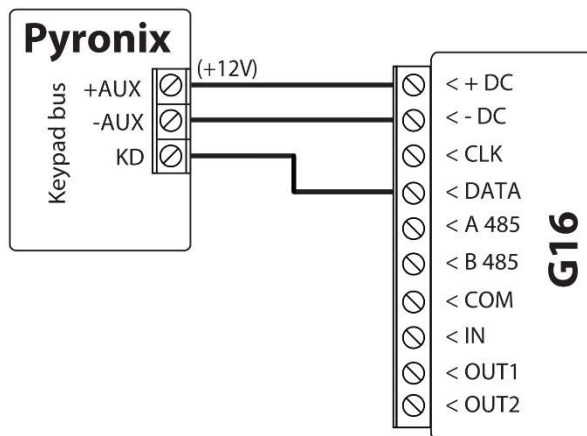


CADDX panel connection diagram



TEXECOM panel connection diagram

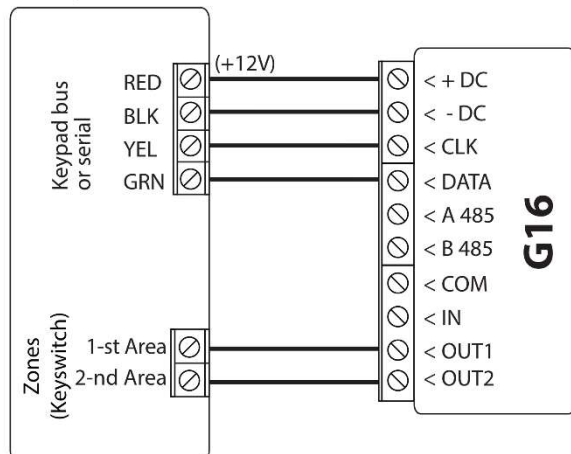


INNERRANGE INCEPTION panel connection diagram

Honeywell Vista-20, Vista-48 panel connection diagram

Crow Runner 4/8, Runner 8/16 panel connection diagram

Pyronix panel connection diagram


3.3 Schematic for connecting to panel keyswitch zone

Follow this schematic if the control panel will be armed/disarmed with a **G16** PGM output turning on/off the panel's keyswitch zone.

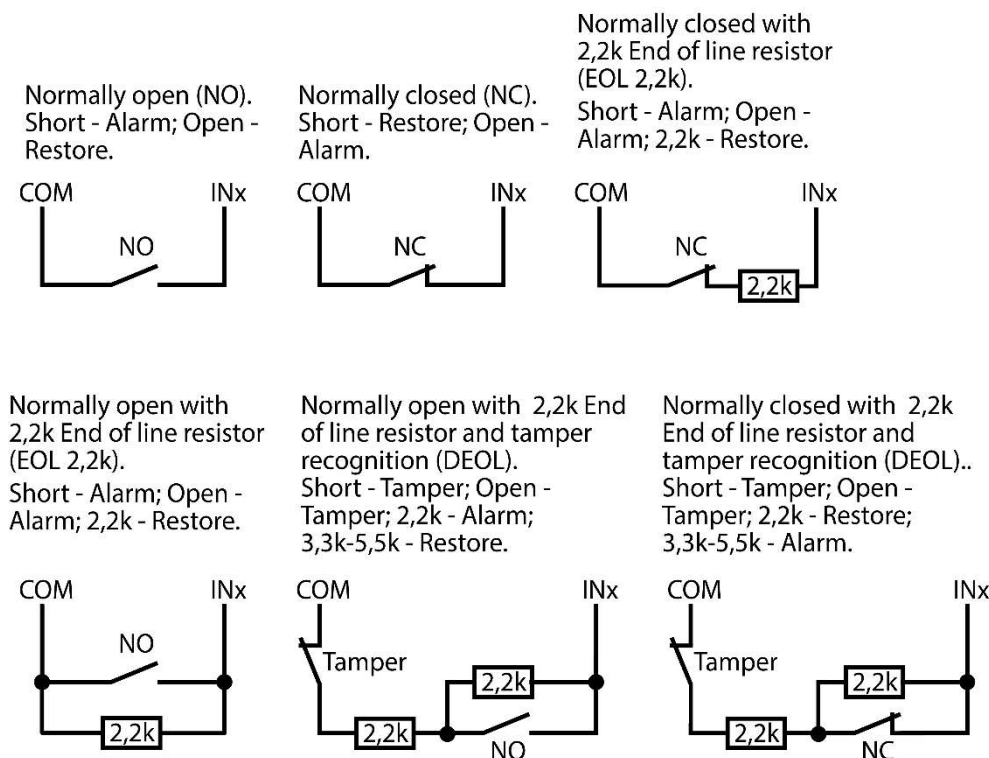
Note: **G16** communicator has two programmable outputs OUT (PGM) that can control two areas of the security system. If you want to control the system in this way, **Output OUT1 & OUT2 mode** needs to be set to **Remote control** (default setting) in the **TrikdísConfig** window "**System settings**". Also, do not select the **Remote Arm/Disarm** box.

Control panel terminals


3.4 Schematics for input connection

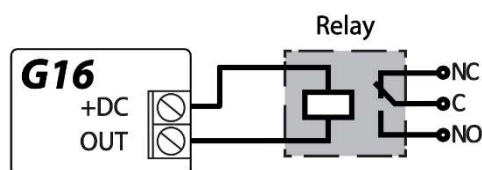
The communicator has one input terminal (IN1) for connecting NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL type circuits. Default input setting - NO. The input type can be changed in the **TrikdísConfig** window **System settings -> Input IN1 type**.

Connect the input according to the selected input type (NO, NC, NC/EOL, NO/EOL, NO/DEOL, NC/DEOL), as shown in the schemes below:



Note: If more inputs or outputs need to be connected to the communicator, connect the TRIKDIS iO series wired or wireless output expander. Connection method is described in the iO manual and chapter 3.6 “Schematics for connecting iO series expansion modules”.

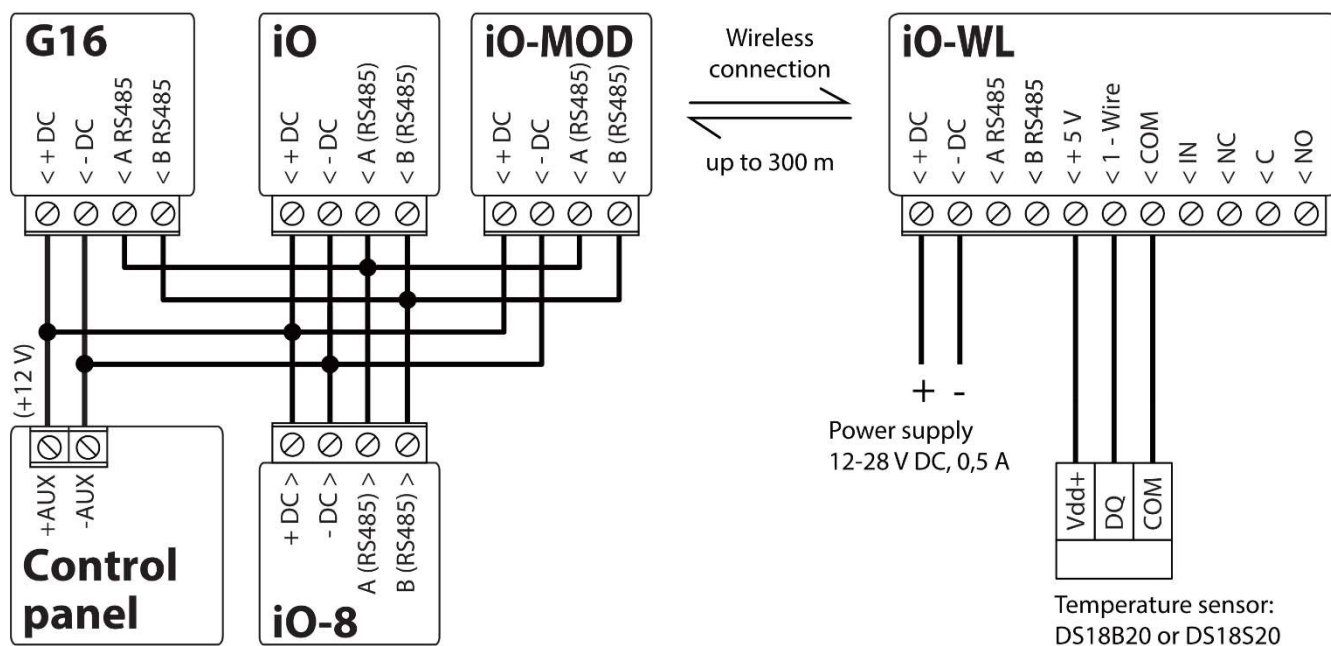
3.5 Schematics for wiring a relay



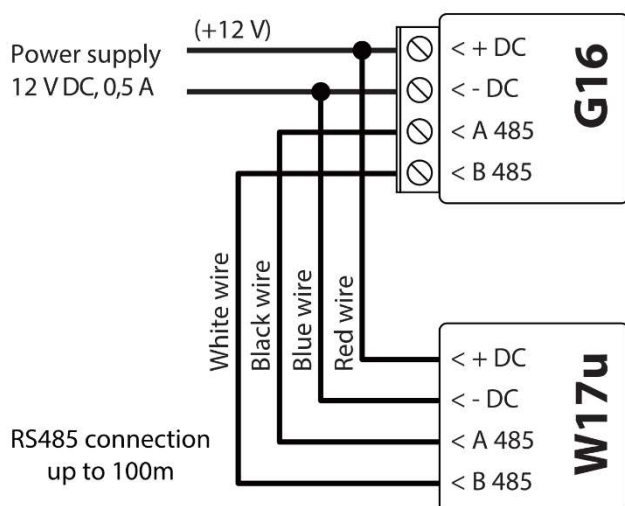
With relay contacts you can control (turn on/off) various electronic appliances.

3.6 Schematics for connecting iO series expansion modules

If more inputs or outputs need to be connected to the communicator, or if you want to connect a temperature sensor, connect the TRIKDIS iO series wired or wireless output expander. Configuration of expander modules connected to the G16 is described in chapter 6.6. “RS485 modules” window”.



3.7 Schematic for connecting the **W17u** WiFi communicator



The **W17u** communicator sends messages to the CMS (Central Monitoring Station) and to **Protegius** using a WiFi internet router. When WiFi connectivity is available, the **G16** sends event messages via the **W17u** communicator. When WiFi connectivity is disrupted, the **G16** sends messages via GPRS. When WiFi connectivity is re-established, the **G16** returns to sending messages via **W17u**.

Configuration of the **W17u** WiFi communicator to work with the G16 is described in chapter 6.6. “RS485 modules” window”.

3.8 Turn on the communicator

To start the communicator, turn on the security control panel’s power supply. This LED indication on the **G16** communicator must show:

- “POWER” LED illuminates green when the power is on;
- “NETWORK” LED illuminates green and blinks yellow when the communicator is registered to the network.

Note:

Sufficient strength of 2G cellular signal is level five (five “NETWORK” indicator flashes in yellow color). Sufficient strength of 3G/4G signal is level three (three “NETWORK” indicator flashes in yellow color).

If you count less yellow “NETWORK” LED flashes, the network signal strength is insufficient. We recommend to select a different place to install the communicator, or to use a more sensitive cellular antenna.

If you see a different LED indication, it indicates a certain malfunction. Diagnose it by following the LED indication table in chapter 1.6 “LED indication of operation”.

If the **G16** indication does not illuminate at all, check the power supply and connections.

4 Programming the control panel

Below it is described how to program the security control panel so that the **G16** communicator could read events from the panel and control it remotely.

To enable remote control of the security panel, make sure that the checkbox **Remote Arm/Disarm** is selected in the *TrikdisConfig* window “**System settings**”.

DSC

DSC panels do not need to be programmed.

PARADOX

Paradox control panels need to be programmed only for direct control with *Proteagus*. You do not need to program Paradox panels for reading events.

For remote control of Paradox panels, you need to set up a PC download password. This password must match the password which was set in the *TrikdisConfig* window “**System settings**”, when the checkbox next to **Remote Arm/Disarm** was selected.

To set this password, with the keyboard connected to the security control panel:

- For MAGELLAN, SPECTRA series: go to cell 911 and enter 4-digit PC download password.
- For DIGIPLEX EVO series: go to cell 3012 and enter 4-digit PC download password.

TEXECOM

Texecom control panels need to be programmed for both reading events and remote control.

You need to set the Texecom panel’s **UDL passcode**. This password must match the password which was set in the *TrikdisConfig* window “**System settings**”, when the box next to **Remote Arm/Disarm** was selected.

The security control panel can be programmed with Texecom software - Wintex. Enter **UDL passcode** (4-digit code) in the **Communication Options** window, **Options** tab.

Also, you can program with a keypad connected to the security control panel:

- 1) Enter the 4-digit installer’s code and press the [Menu] button to enter the programming menu.
- 2) Press the [9] key immediately afterwards.
- 3) Press [7][6], and then [2]. Enter the 4-digit **UDL passcode** (**UDL passcode** must match the **G16** communicator’s **PC login password**).
- 4) Press [Yes] and leave the programming mode by pressing [Menu].

UTC INTERLOGIX (CADDX)

With the keyboard connected to the security control panel:

- 1) Press [*][8] and enter the installer’s code (default - 9713).
- 2) Enter the device number assigned to the connected communicator (default - 0).
- 3) Set the settings below for each row. In sequence, enter the position, segment number and the required setting. Clicking [*] (asterisk) will return you to the local input field.

Position	Segment	Setting
23	3	12345678
37 (not necessary)	3	12345678
	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678

Position	Segment	Setting
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

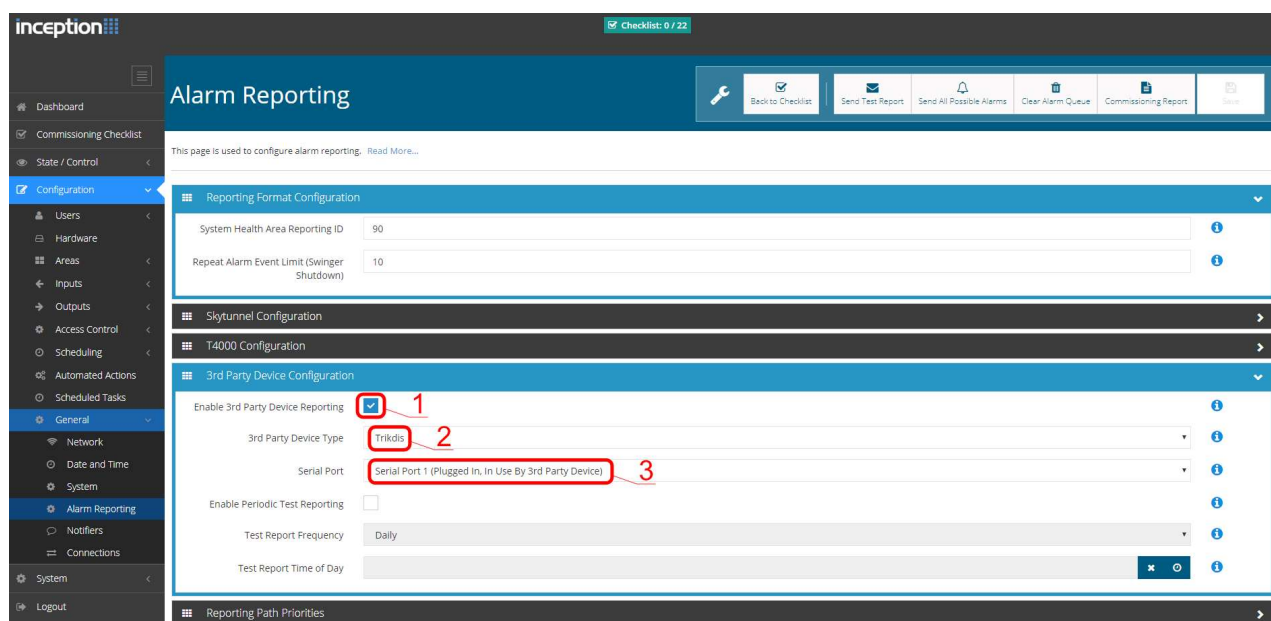
After having programmed all the fields listed, press [Exit] twice to exit the programming mode.

INNERRANGE

Innerrange Inception security control panel version must be **2.3.0.3507-r0** or higher.

The control panel must be connected to the internet. Connect to **Innerrange Inception** by entering: <https://skytunnel.com.au/inception/SERIALNUMBER>, where SERIALNUMBER is the number of the controller that you can find on the panel's enclosure.

Open **Configuration > General > Alarm Reporting**. In the **3rd Party Device Configuration** settings group you need to enter:



1. **Enable 3rd Party Device Reporting** - select this checkbox.
2. **3rd Party Device Type** - set "Trikdis".
3. **Serial port** - set "Serial Port 1 (Plugged In, In Use By 3rd Party Device)".
4. Save settings and exit the application.

Honeywell Ademco Vista

Follow these steps for **Honeywell Ademco Vista-20** and **Honeywell Ademco Vista-48** panels. **The panel's firmware version must be V5.3 or higher.** With a keypad that is connected to the panel:

1. Enter the programming mode. Enter the installer code 4)[1][1][2] and after that [8][0][0] . Alternatively, turn on the panel's power supply. In 50 seconds after the power supply is turned on, press the buttons [*] and [#] at the same time (this method can be used when programming mode was exited by pressing in keypad [*][9][8]).
2. Turn on the sending of Contact ID events via LRR. Press [*][2][9][1][#] in keypad.
3. When using the „Remote Arm/Disarm“ function, allow to use the 2nd AUI address. In keypad press [*][1][8][9][1][1][#] .

Exit the programming mode. In keypad press [*][9][9]

Crow

There is no need to program Crow Runner 4/8 and Runner 8/16 panels.

5 Remote control

5.1 Adding the security system to Protegus app

With **Protegus** users will be able to control their alarm system remotely. They will see the status of the system and receive notifications about system events.

- 1) Download and launch the **Protegus** application or use the browser version: www.protegus.eu/login.

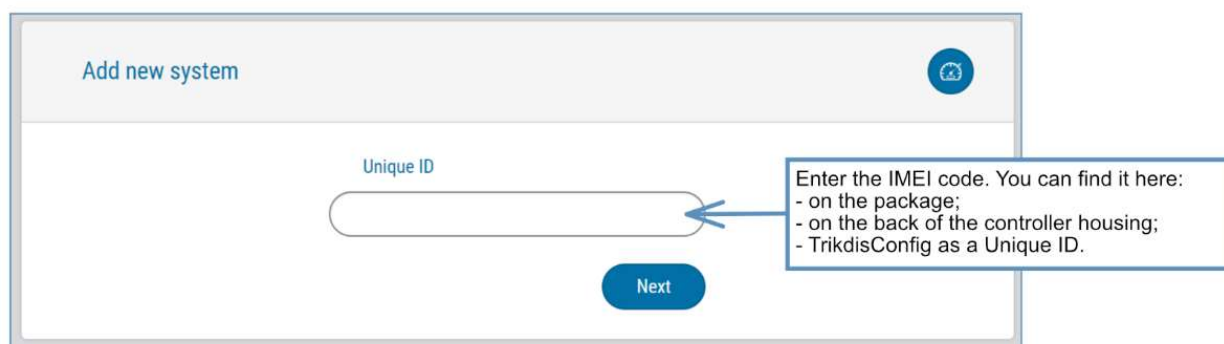


- 2) Log in with your user name and password or register and create new account.

Important: When adding the **G16** to **Protegus** check if:

1. The inserted SIM card is activated and the PIN code is either entered or disabled;
2. **Protegus cloud** is enabled. See chapter 6.4 “User reporting” window;
3. Power supply is connected (“POWER” LED illuminates green);
4. Registered to the network (“NETWORK” LED illuminates green and blinks yellow).

- 3) Click **Add new system** and enter the **G16**’s “IMEI/Unique ID” number. This number can be found on the device and the packaging sticker. Click **Next**.

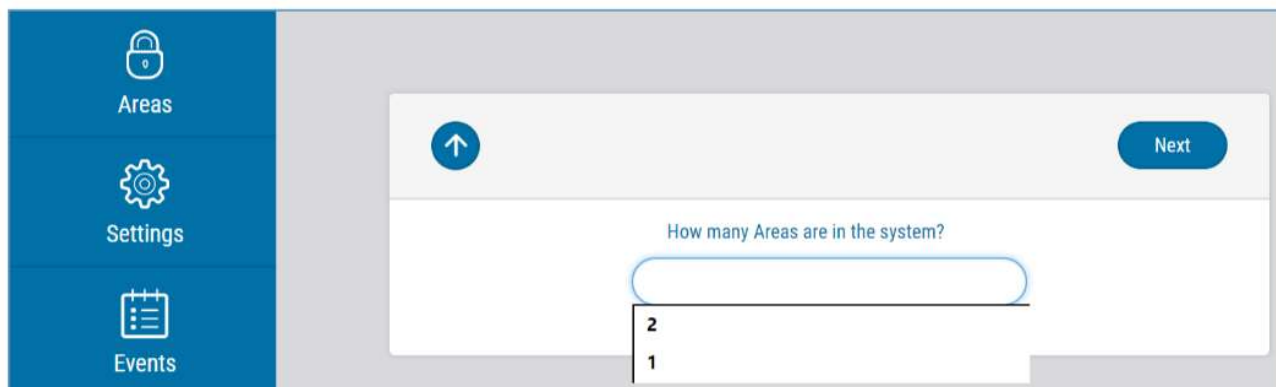


5.2 Additional settings to arm/disarm the system using the control panel’s keyswitch zone

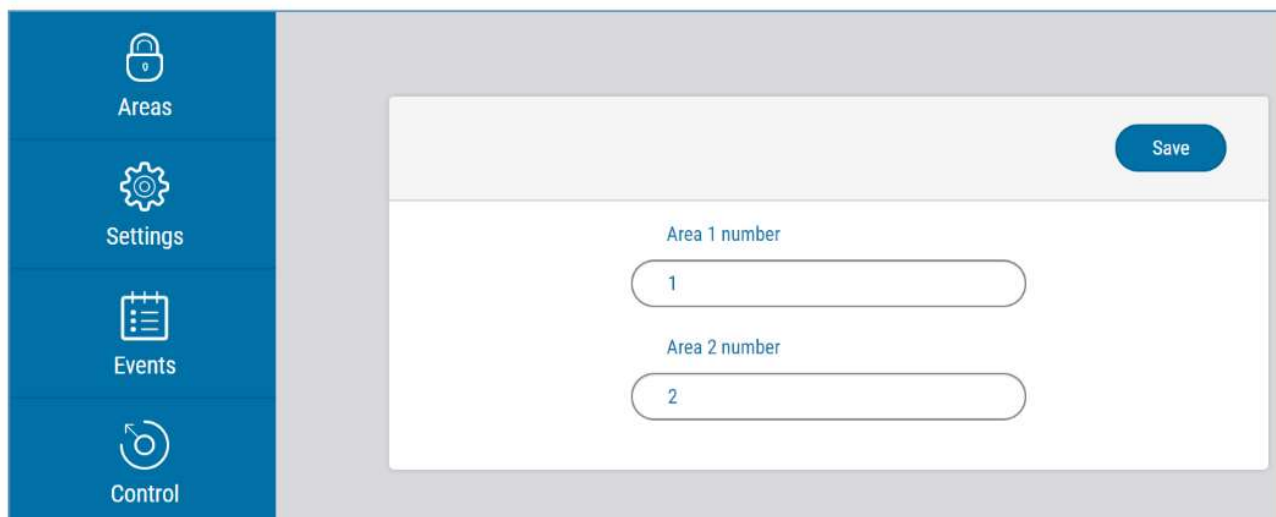
Important: The control panel zone to which the **G16** output OUT is connected to has to be set to keyswitch mode.

Follow the instructions below if the security control panel will be controlled with a **G16** PGM output, turning on/off the control panel keyswitch zone.

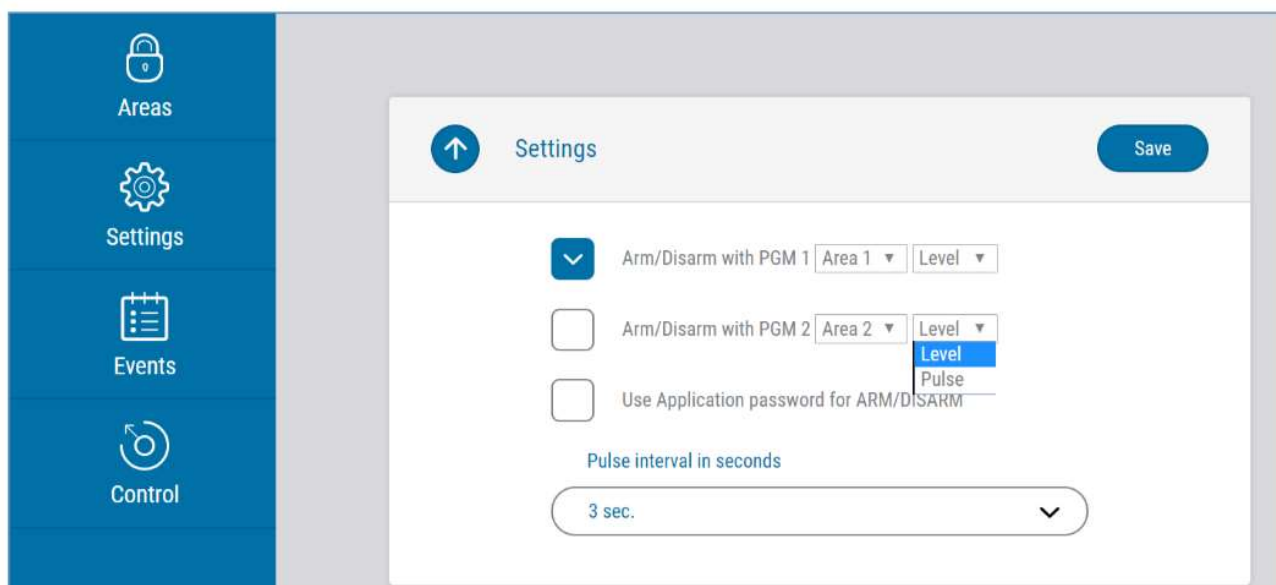
- 1) In the new window, click **Areas** in the side menu. In the next window, specify how many alarm system areas (1 or 2) are in the system and press **Next**.



- 2) In the new window, identify what is the number for each of the specified areas in the security system and press **Save**.



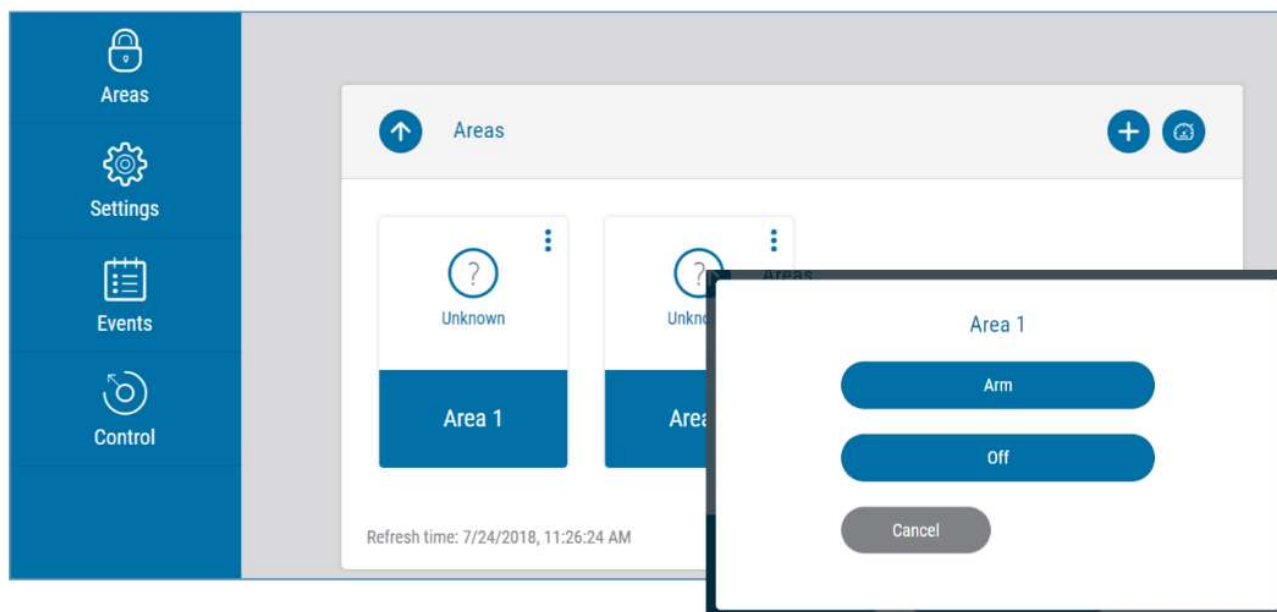
- 3) In the side menu press **Settings** and in the newly opened window press **Settings**. Select the box **Arm/Disarm with PGM** and specify which area the output will control. One PGM output can control only one area.



- 4) Select **Level** or **Pulse**, depending on the type of control panel keyswitch zone. You can also change the duration of the pulse interval if it is required for the connected control panel.
- 5) For additional security, you can select **Use Application password for ARM/DISARM**. Then after pressing the button to arm/disarm the alarm system, a window for entering the app password will open.

5.3 Arming/disarming the alarm system with Protegus

- 1) To control the system, open the **Areas** window.
- 2) In the **Areas** window click the Area button. In the pop-up window select the action (arm or disarm the security system area).
- 3) If requested, enter the user code or **Protegus** password.



5.4 Configuration and control with SMS messages

You can remotely configure and control the communicator with SMS messages.

Message structure is: Password _{space} Command _{space} Data

For password use the **Administrator code** for *INFO*, *RESET*, *OUTPUTx*, *CONNECT* commands, and **Installer code** for *INFO*, *RESET*, *OUTPUTx* commands.

SMS command list

Command	Data	Description
<i>INFO</i>		Request information about the device. Response will be: communicator type, IMEI number, serial number and firmware version. E.g.: 123456 INFO
<i>RESET</i>		Restart the device. E.g.: 123456 RESET
<i>OUTPUTx</i>	<i>ON</i>	Turn on an output. x is the output number (1 or 2). E.g.: 123456 OUTPUT1 ON
	<i>OFF</i>	Turn off an output. x is the output number (1 or 2). E.g.: 123456 OUTPUT1 OFF
	<i>PULSE=tttt</i>	Turn on the output in impulse mode, for the specified time interval (sec). "tttt" is the time duration of impulse in seconds, described in four digits. E.g.: 123456 OUTPUT2 PULSE=0002
<i>CONNECT</i>	<i>Protegeus=ON</i>	Enable access to Protegeus service. E.g.: 123456 CONNECT PROTEGEUS=ON
	<i>Protegeus=OFF</i>	Disable access to Protegeus service E.g.: 123456 CONNECT PROTEGEUS=OFF
	<i>IP=0.0.0.0:8000</i>	Set primary channel IP address and Port number. E.g.: 123456 CONNECT IP=192.120.120.255:8000
	<i>ENC=123456</i>	Set TRK encryption key. E.g.: 123456 CONNECT ENC=123456
	<i>APN=Internet</i>	Set APN name. E.g.: 123456 CONNECT APN=INTERNET
	<i>USER=user</i>	Set APN user. E.g.: 123456 CONNECT USER=User
	<i>PASS=password</i>	Set APN password. E.g.: 123456 CONNECT PASS=Password
	<i>CP=</i>	Select security control panel from a list. E.g. (assign control panel Paradox SP6000 that is number 4 on the list to the G16): 123456 CONNECT CP=4

Command	Data	Description
	<i>DIR=</i>	Direct control 4-digit password or OFF to disable it. E.g. (enter the direct control 4-digit password 1122): 123456 CONNECT DIR=1122

You can restrict the phone numbers from which the communicator will accept the commands. See chapter Klaida! Nerastas nuorodos šaltinis.4 “User reporting” window, “Control by SMS” tab.

6 TrikdisConfig window description

6.1 TrikdisConfig status bar description

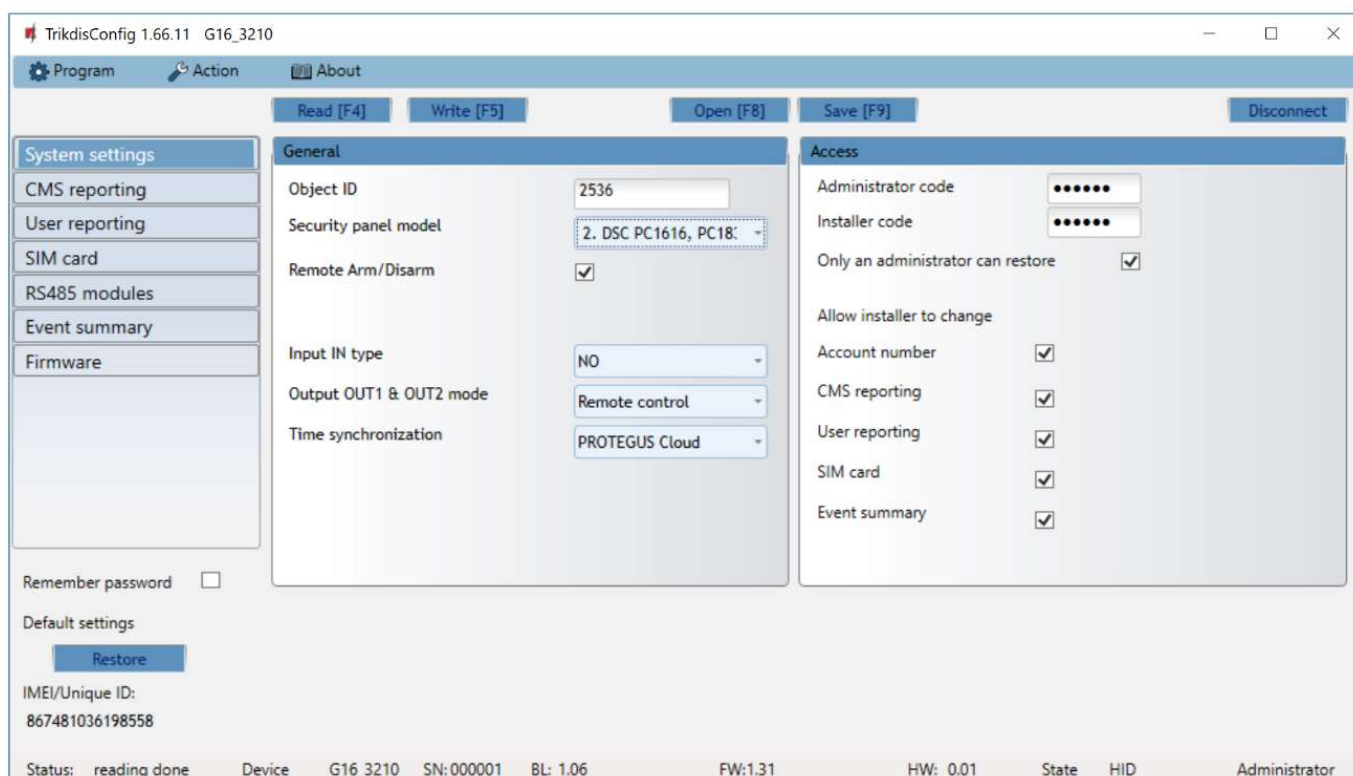
After connecting the **G16** and clicking **Read [F4]**, **TrikdisConfig** will provide information about the connected device in the status bar:

IMEI/Unique ID: 867481036198558	
Status: reading done	Device G16_3210 SN:000001 BL: 1.06 FW:1.31 HW: 0.01 State HID Administrator

Object	Description
Unique ID	Device IMEI number
Status	Operating condition
Device	Device type (G16 should be shown)
SN	Device serial number
BL	Browser version
FW	Device firmware version
HW	Device hardware version
Status	Connection to program type (via USB or remote)
Administrator	Access level (shown after access code is approved)

After pressing **Read [F4]**, the program will read and show the settings which are set in the **G16**. Set the necessary settings according to the **TrikdisConfig** window descriptions given below.

6.2 “System settings” window



“General” settings group

- **Object ID** – if the events will be sent to the CMS (Central Monitoring Station), enter the account number provided by the CMS (4 characters hexadecimal number, 0-9, A-F).
- Select the **Panel type** that will be connected to the communicator.
- **Remote Arm/Disarm** - when the checkbox is selected, the **G16** will directly control the control panel remotely. This setting will be visible only for directly controlled panels. For direct control of the control panels you need to change the panel settings, as described in section 4 “**Programming the control panel**”.
- **Control panel PC download/UDL password** - for the direct control of Paradox and Texecom control panels you need to enter the PC/UDL password. It must match the password that was entered in the control panel. How to change this password is described in section 4 “**Programming the control panel**”.
- **Input IN type** - select the input type from the list (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).
- **Output OUT1 & OUT2 mode** - select the output operation mode from the list.
- **Time synchronization** - select which server to use for time synchronization.

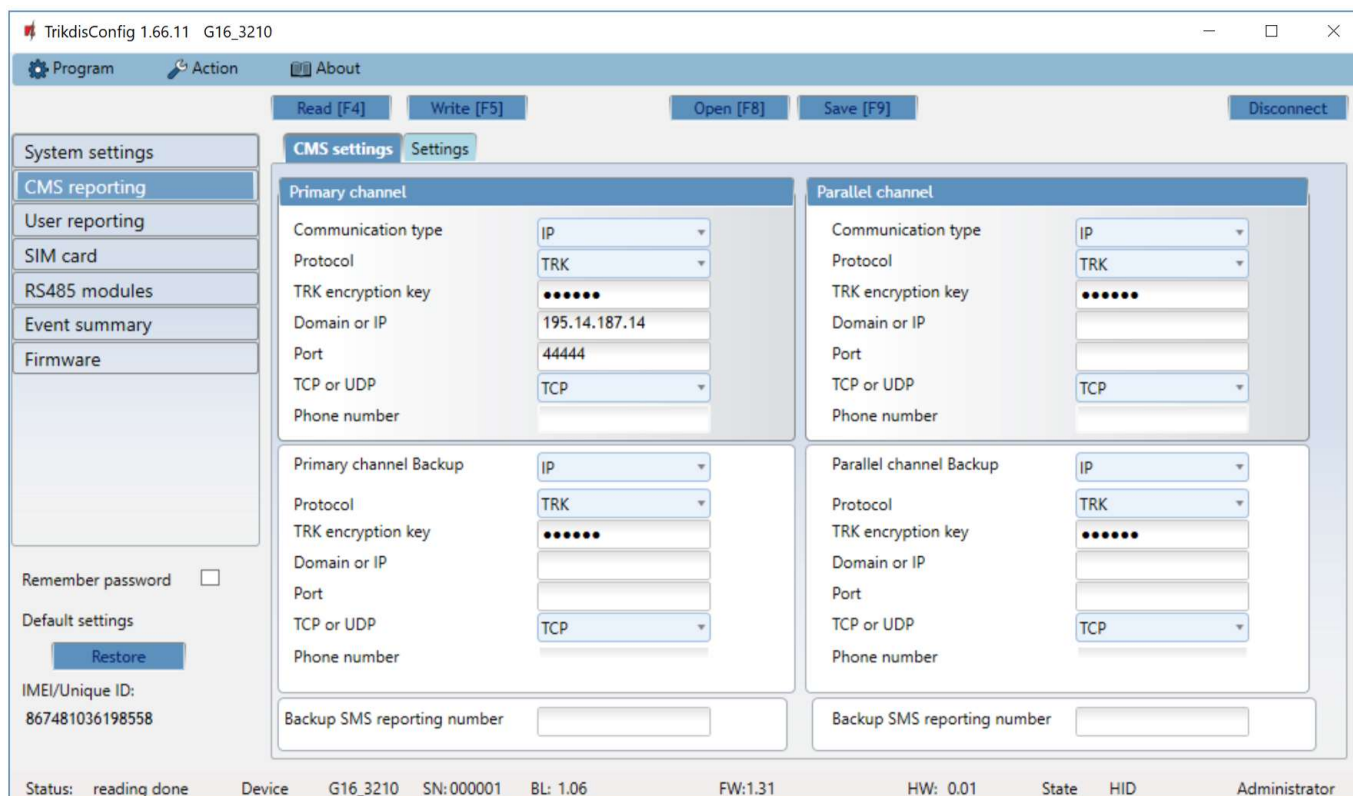
“Access” settings group

When setting up the communicator **G16** there are two levels of access for, the administrator and the installer:

- **Administrator code** - allows you to access all configuration fields (default code - 123456).
- **Installer code** - limited access for configuring the communicator (default code - 654321).
- **Only an administrator can restore** - if the box is checked, factory settings can be restored only by entering the administrator code.
- **Allow installer to change** – the administrator can specify which settings can be changed by the installer.

6.3 “CMS reporting” window

“CMS settings” tab



The communicator sends events to the monitoring station via cellular internet (IP) or with SMS messages.

Events can be sent over several channels of communication. The primary and parallel communication channels can operate simultaneously, this way the communicator can send events to two receivers at the same time. Backup channels can be assigned for both primary and parallel channels, which will be used when the connection via the primary or parallel channel is interrupted.

Communication is encoded and password protected. A TRIKDIS receiver is required for receiving and sending event information to the monitoring programs:

- For connection over IP - software receiver IPcom Windows/Linux, hardware IP/SMS receiver RL14 or multichannel receiver RM14.
- To receive SMS messages - hardware IP/SMS receiver RL14, multichannel receiver RM14 or SMS receiver GM14.

SMS communication is particularly useful as a backup channel, because it works even when there is no mobile internet connection. We do not recommend SMS as a primary channel.

“Primary channel” settings group

- **Communication type** - select which method for connecting to the monitoring station receiver will be used: **IP** or **SMS**.
- **Protocol** - select in which coding the events should be sent: **TRK** (to TRIKDIS receivers), **DC-09_2007** or **DC-09_2012** (to universal receivers).
- **TRK encryption key** - 6-digit message encryption key. The key written to the communicator must match the receiver’s key.
- **Domain or IP** - enter the domain or IP address of the receiver.
- **Port** - enter the network port number of the receiver.
- **TCP or UDP** - select in which protocol (TCP or UDP) the events should be sent.
- **Phone number** (only for SMS messages) - enter the telephone number of a TRIKDIS SMS receiver. The phone number must begin with the country code (e.g., 370xxxxxxx).

“Primary channel Backup” settings group

Enable the backup channel mode to send events via backup channel if connection via primary channel is lost. Backup channel settings are same as described above.

“Parallel channel” settings group

Events are transmitted in parallel with the first channel through this channel. When the second channel is enabled, events can be sent simultaneously to two receivers (e.g., local and centralized monitoring stations). Parallel channel settings are the same as described above.

Backup SMS reporting number

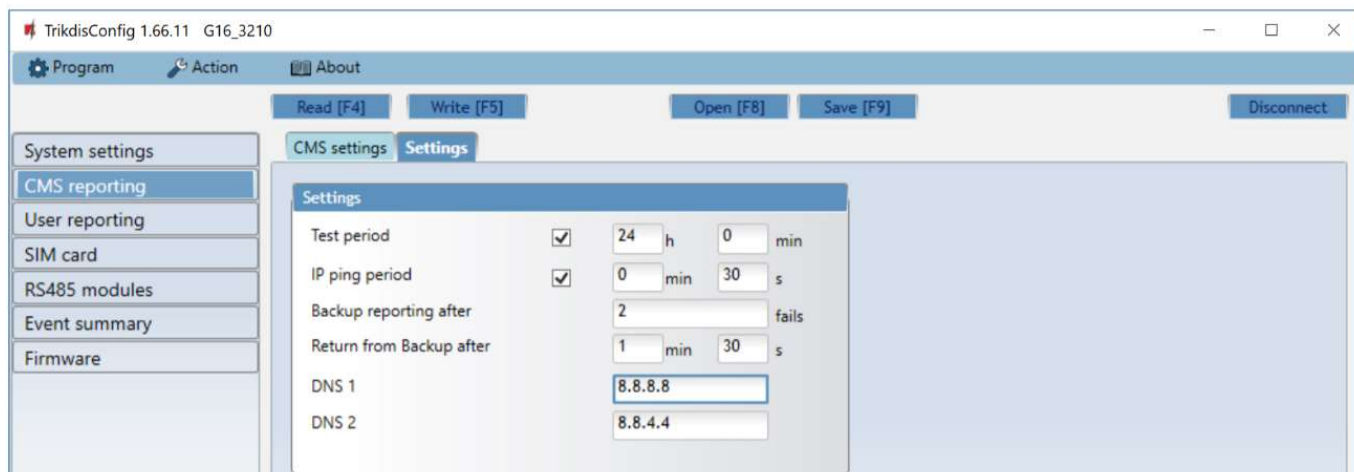
Backup SMS messages are sent when they cannot be transmitted via the primary, parallel and backup channels. It is especially useful because it works even when there is no IP connection in the mobile operator network.

This channel is operational only when IP mode is set for the first channel and its backup channel.

SMS notifications will be sent to the Central Monitoring Station SMS receiver: 1) immediately after the first time when communicator starts operating; and 2) if the TCP / IP or UDP / IP connection is interrupted in the first channel and its backup channel.

- **Backup SMS reporting number** - enter the phone number for TRIKDIS alarm receiving center’s SMS receiver. Phone number must begin with the country code (e.g., 370xxxxxxx).

“Settings” tab



“Settings” settings group

- **Test period** - TEST event period for testing the connection. Test events are sent as Contact ID messages and forwarded to the monitoring software.
- **IP ping period** – period for sending internal PING heartbeats. These messages are only sent via IP channel. The receiver will not forward PING messages to the monitoring software to avoid overloading it. Notifications will only be sent to the monitoring software if the receiver fails to receive PING messages from the device within the set time.

By default, the “Connection lost” notification will be transmitted to the monitoring software if the PING message is not received by the receiver over a time period three times longer than set in the device. E.g. if the PING period is set for 3 minutes, the receiver will transfer the “Connection lost” notification if a PING message is not received within 9 minutes.

PING heartbeats keep the active communication session between the device and the receiver. An active session is required for remote connection, control and configuration of the device. We recommend setting the PING period for no more than 5 minutes.

- **Backup reporting after** - indicates the number of unsuccessful attempts to send the message via Primary channel. If device fails to transmit specified number of times, the device will connect to transmit the messages via Backup channel.
- **Return from backup after** - time after which the G16 will attempt to reconnect and transmit messages via the Primary channel.
- **DNS1, DNS2** - (Domain Name System) identifies the server that specifies the IP address of the domain. Used when domain is set in the communication channel **Domain or IP** field (not IP address). Google DNS server is set by default.

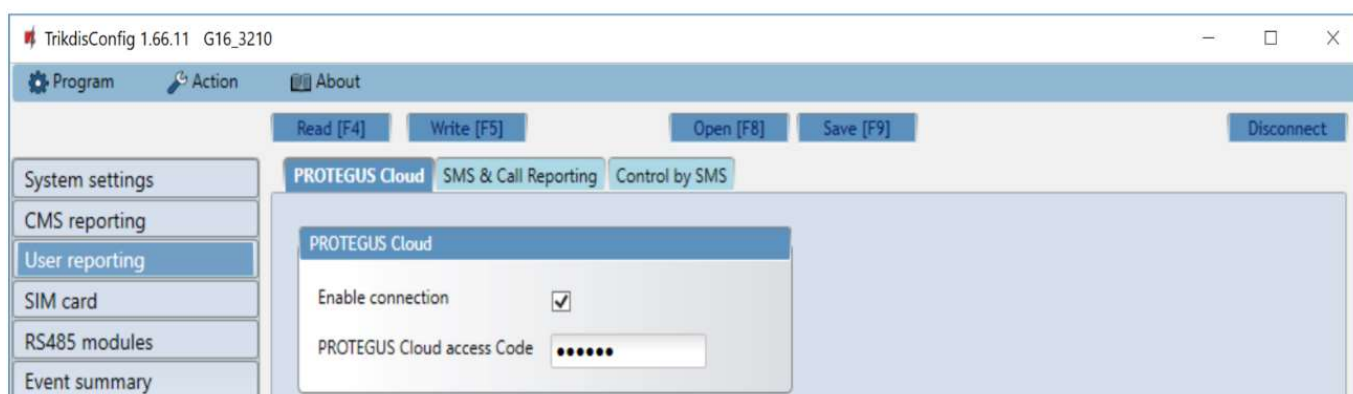
“DC-09 parameters” settings group

The settings are displayed when the **DC-09_2007** or **DC-09_2012** protocol is set in the communication channel **Protocol** field for sending events to universal receivers.

- **Object ID in DC-09** - enter the object number. The object number entered in this field will be used if DC-09 encoding is selected. A hexadecimal number from 3 to 16 characters can be entered. This Number is provided by the Alarm Receiving Center.
- **DC-09-line No.** - enter line number of the receiver.
- **DC-09 receiver No.** - enter the receiver number.

6.4 “User reporting” window

“PROTEGUS cloud” tab

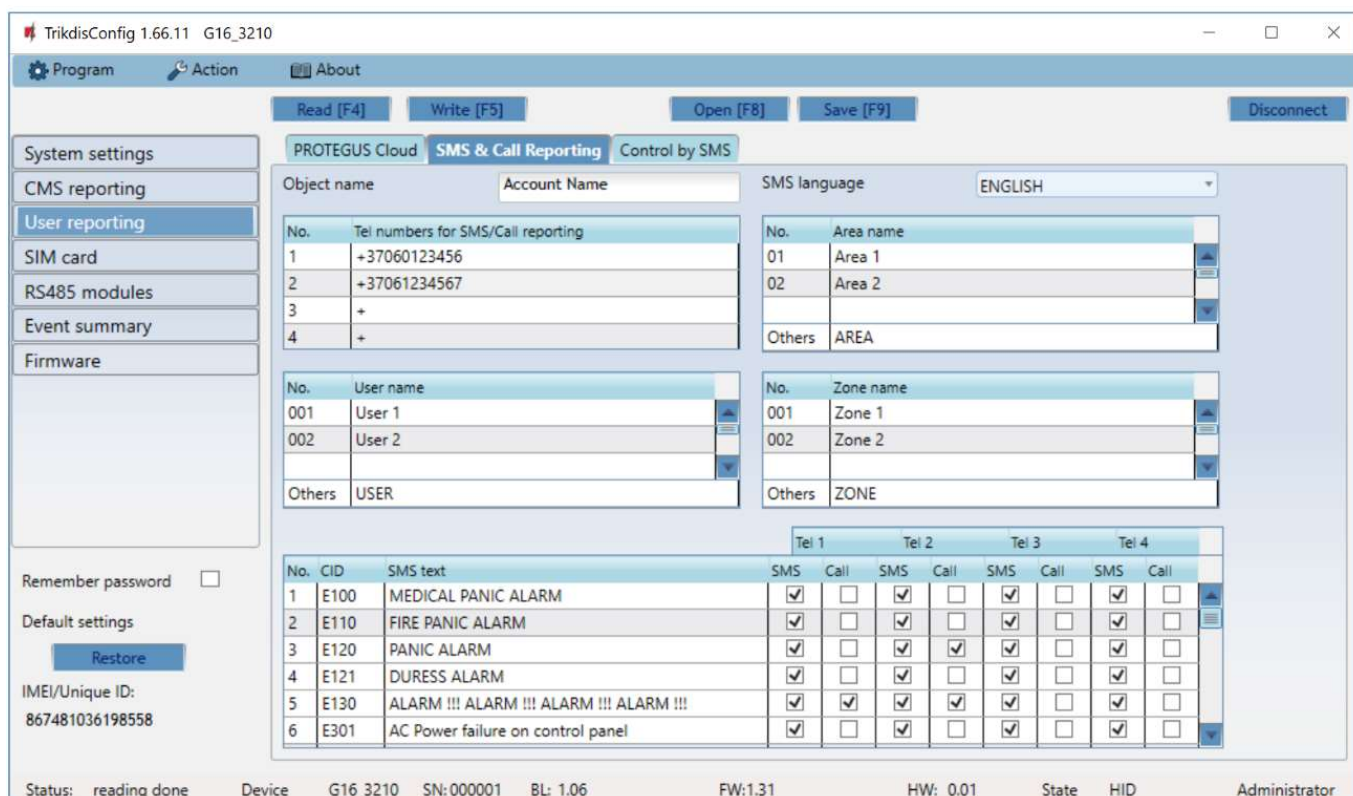


Protegeus service allows users to remotely monitor and control the communicator. For more information about **Protegeus** service, visit www.protegeus.eu.

“Protegeus Cloud” settings group

- **Enable connection** – enable the **Protegeus** service, the **G16** will be able to exchange data with **Protegeus** app and to be remotely configured via **TrikdisConfig**.
- **Cloud access Code** - 6-digit code for connecting to the **Protegeus** app (default - 123456).

“SMS & Call Reporting” tab



TrikdisConfig 1.66.11 G16_3210

Program Action About

Read [F4] Write [F5] Open [F8] Save [F9] Disconnect

System settings
CMS reporting
User reporting
SIM card
RS485 modules
Event summary
Firmware

PROTEGUS Cloud SMS & Call Reporting Control by SMS

Object name Account Name SMS language ENGLISH

No.	Tel numbers for SMS/Call reporting
1	+37060123456
2	+37061234567
3	+
4	+

No.	Area name
01	Area 1
02	Area 2
Others	AREA

No.	User name
001	User 1
002	User 2
Others	USER

No.	Zone name
001	Zone 1
002	Zone 2
Others	ZONE

No.	CID	SMS text	SMS	Call	SMS	Call	SMS	Call	SMS	Call
1	E100	MEDICAL PANIC ALARM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	E110	FIRE PANIC ALARM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	E120	PANIC ALARM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	E121	DURESS ALARM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	E130	ALARM !!! ALARM !!! ALARM !!! ALARM !!!	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	E301	AC Power failure on control panel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Remember password ☐

Default settings
Restore

IMEI/Unique ID:
867481036198558

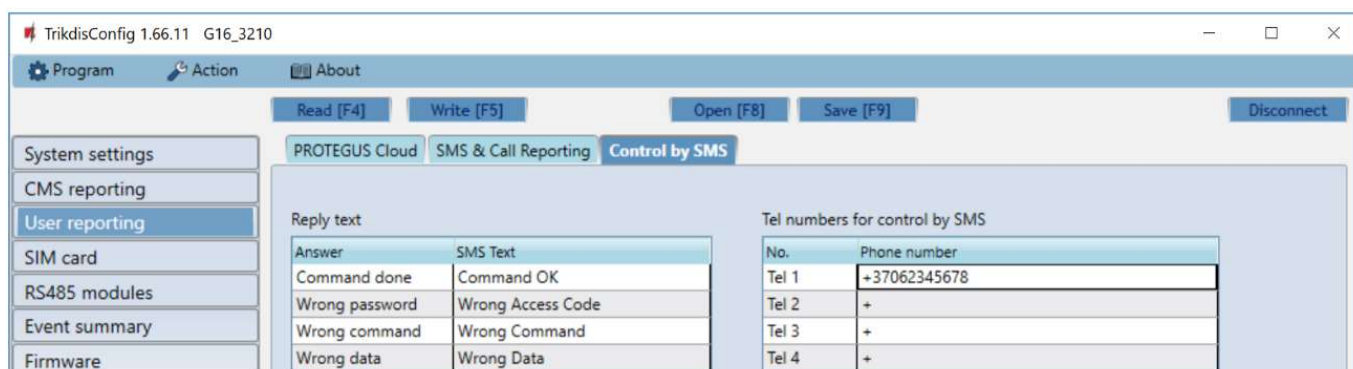
Status: reading done Device G16_3210 SN:000001 BL: 1.06 FW:1.31 HW: 0.01 State HID Administrator

Notifications about system events can be transmitted to users' mobile phones via SMS messages or phone calls.

- **Object name** - name the system to which the communicator is connected. Every SMS notification will include the name of the object.
- **SMS language** - choose the language for SMS messages (SMS messages can be sent with language-specific characters).
- **Tel numbers for SMS/Call reporting** - enter up to 4 user phone numbers that will receive event SMS messages or calls. Phone numbers must begin with the country code, for example +370xxxxxxx, 00370xxxxxxx or 370xxxxxxx.
- **Area name, User name, Zone name tables** - each area, user and zone may have a name that will be used in SMS event messages. Enter the area, user or zone number in the appropriate table and enter the name next to the number.
- **CID event table** - you can change which phone numbers receive SMS messages or phone calls notifying about the events on the list.

You can change the texts for SMS messages of default events, change the contact ID (CID) codes and enter new events with descriptions.

“Control by SMS” tab



TrikdisConfig 1.66.11 G16_3210

Program Action About

Read [F4] Write [F5] Open [F8] Save [F9] Disconnect

System settings
CMS reporting
User reporting
SIM card
RS485 modules
Event summary
Firmware

PROTEGUS Cloud SMS & Call Reporting Control by SMS

Reply text

Answer	SMS Text
Command done	Command OK
Wrong password	Wrong Access Code
Wrong command	Wrong Command
Wrong data	Wrong Data

Tel numbers for control by SMS

No.	Phone number
Tel 1	+37062345678
Tel 2	+
Tel 3	+
Tel 4	+

You can send SMS commands to the communicator that will control the basic functions of the device. Find the control commands in chapter 5.4 Configuration and control with SMS messages.

- **Reply text** - SMS text that the user receives after sending an SMS command. SMS text can be edited.

- **Tel numbers for control by SMS** - you can enter phone numbers from which the communicator will accept commands.

Note: If no phone number is entered, the device will accept commands from any phone number. In any case, security is guaranteed by the requirement to enter administrator or installer password in the SMS command.

6.5 “SIM card” window

- Important:**
1. Ensure that the SIM card is activated and working before using it.
 2. If mobile internet connection will be used for sending events via IP channel or to **Protegas**, ensure that mobile data service is enabled.



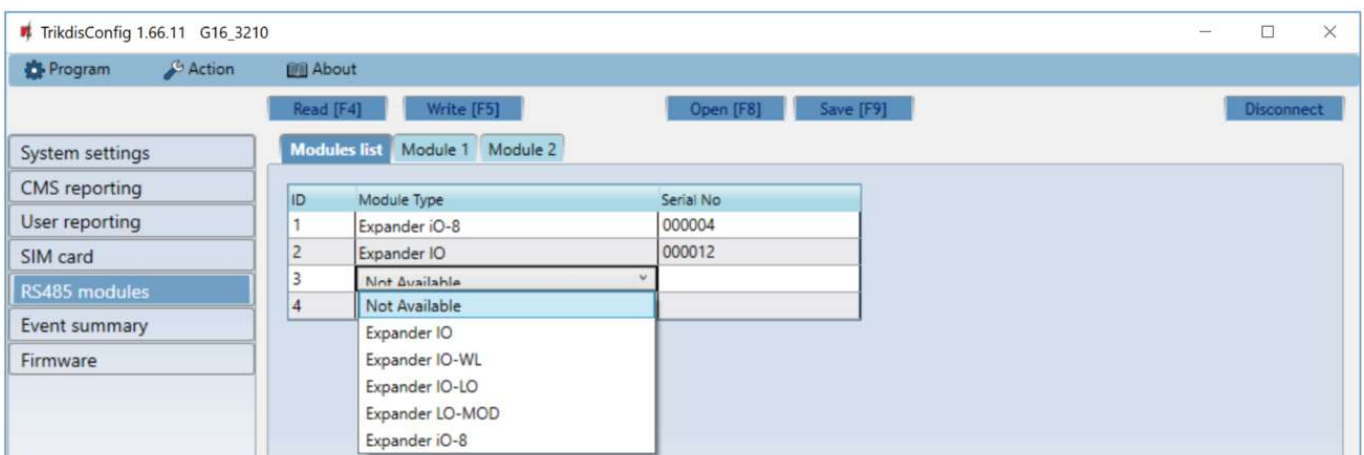
“SIM card” settings group

- **SIM card PIN** - enter the SIM card PIN code. This code can be disabled by inserting the SIM card into a mobile phone and disabling the request. If you disabled the SIM card PIN request, leave the default value in this field.
- **APN** - enter APN (Access Point Name). It is required for connecting the communicator to the internet. APN can be found on the website of the SIM card operator (“internet” is universal and works in the networks of many operators).
- **Login, Password** - if required, enter the user name (login) and password for connection to the internet.
- **Forbid connection when roaming detected** - you can use this function when the security system is installed near the country border. This function prevents the communicator from operating in the other country’s mobile network.

6.6 “RS485 modules” window

“Modules list” tab

IO series expanders can be connected to the communicator to add additional inputs, outputs and serial buses for temperature sensors. Connected expanders must be added to the **Modules list** table.



ID	Module Type	Serial No
1	Expander iO-8	000004
2	Expander IO	000012
3	Not Available	
4	Not Available	

- **Module type** – select the module that is connected to the communicator via RS485 from the list.

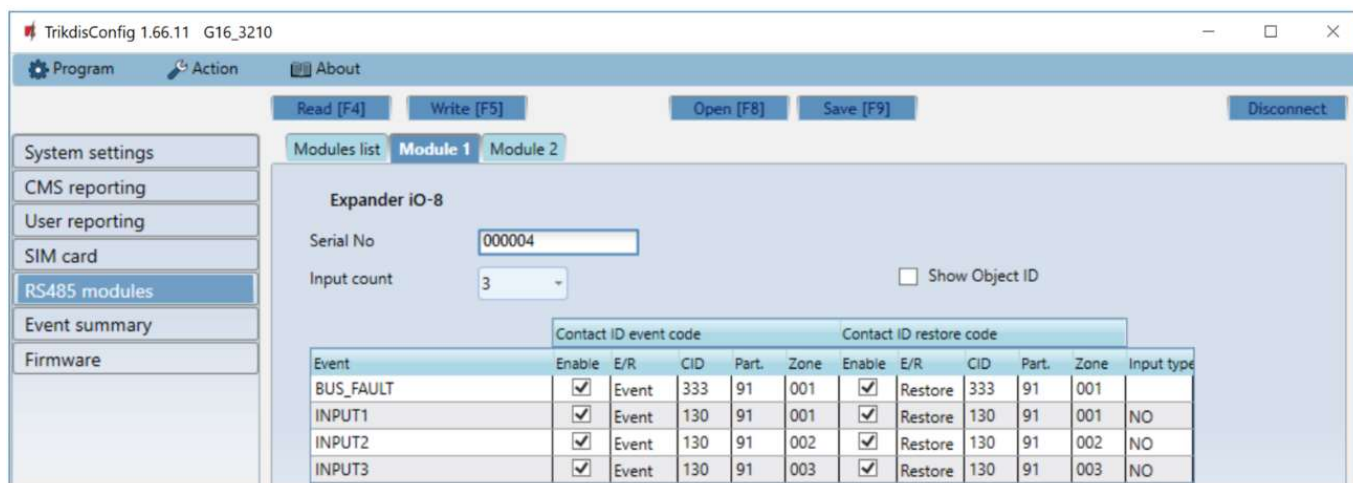
- **Serial No** – enter the module serial number (6 digits), which is indicated on stickers on the module's case and packaging.

After selecting the connected module and entering its serial number, press the **Write [F5]** button. When the change is written, disconnect the USB Mini-B cable from the communicator. Wait one minute (the communicator has to register the connected module). Connect the USB Mini-B cable to the communicator. Click the **Read [F4]** button. Go to **RS485 modules** → **Module**.

“Module” tabs

After adding the expander to the communicator as described above, in the **RS485 modules** window a new tab will appear with this module's settings. The tab will be given a number. Bellow we describe the settings for **iO-8** and **iO** series expanders and for the WiFi communicator **W17u**.

iO-8 expander settings window



Contact ID event code						Contact ID restore code					
Event	Enable	E/R	CID	Part.	Zone	Enable	E/R	CID	Part.	Zone	Input type
BUS_FAULT	<input checked="" type="checkbox"/>	Event	333	91	001	<input checked="" type="checkbox"/>	Restore	333	91	001	
INPUT1	<input checked="" type="checkbox"/>	Event	130	91	001	<input checked="" type="checkbox"/>	Restore	130	91	001	NO
INPUT2	<input checked="" type="checkbox"/>	Event	130	91	002	<input checked="" type="checkbox"/>	Restore	130	91	002	NO
INPUT3	<input checked="" type="checkbox"/>	Event	130	91	003	<input checked="" type="checkbox"/>	Restore	130	91	003	NO

Expander **iO-8** has 8 universal (input/output) terminal contacts. Up to four **iO-8** expanders can be connected.

- **Input Count** – select what number of terminal contacts should be set to input (IN) mode. The rest of the terminal contacts will become outputs (OUT).

Settings for controllable outputs are set directly in Protegus app. There you can assign an output for arming/disarming the alarm system or for remote control of devices.

In the table inputs can be assigned Contact ID event and restore codes. After input is triggered, the communicator will send an event with set event code to monitoring station receiver, Protegus app and SMS (to user telephone number).

Contact ID event code:

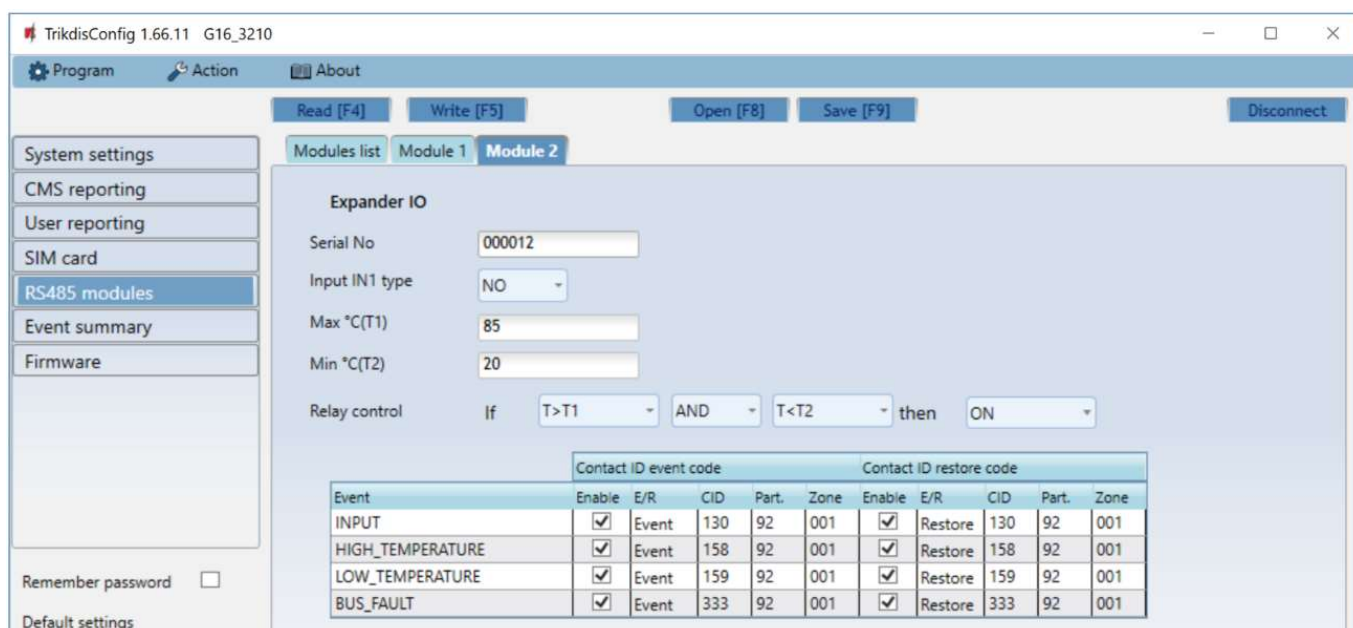
- **Enable** – allow message transmission, when the input is triggered.
- **E/R** – choose what type of event will be sent when input is triggered – **Event** or **Restore**.
- **CID** – assign a Contact ID event code to the input.
- **Part.** – assign the partition (area) to the input. It is set automatically: if the module no. is 1, then the area is 91; if the module no. is 4, then the area is 94.
- **Zone** – set the zone number for the input.

Contact ID restore code:

- **Enable** – allow message transmission when the input is restored.
- **E/R** – choose what type of event will be sent when input is restored – **Restore** or **Event**.
- **CID** – assign the Contact ID restore code to the input.
- **Part.** – assign the partition (area) to the input. It is set automatically: if the module no. is 1, then the area is 91; if the module no. is 4, then the area is 94.
- **Zone** – set the zone number for the input.
- **Input type** – select the type of the input (NO or NC).

For customers to receive SMS messages or calls about input triggers, enter the Contact ID event code that is assigned to the input to the table in “**SMS & Call Reporting**” tab.

iO expander settings window



TrikidisConfig 1.66.11 G16_3210

Program Action About

Read [F4] Write [F5] Open [F8] Save [F9] Disconnect

Modules list Module 1 Module 2

Expander IO

Serial No: 000012

Input IN1 type: NO

Max °C(T1): 85

Min °C(T2): 20

Relay control: If T>T1 AND T<T2 then ON

Contact ID event code						Contact ID restore code					
Event	Enable	E/R	CID	Part.	Zone	Event	Enable	E/R	CID	Part.	Zone
INPUT	<input checked="" type="checkbox"/>	Event	130	92	001	Restore	<input checked="" type="checkbox"/>	Restore	130	92	001
HIGH_TEMPERATURE	<input checked="" type="checkbox"/>	Event	158	92	001	Restore	<input checked="" type="checkbox"/>	Restore	158	92	001
LOW_TEMPERATURE	<input checked="" type="checkbox"/>	Event	159	92	001	Restore	<input checked="" type="checkbox"/>	Restore	159	92	001
BUS_FAULT	<input checked="" type="checkbox"/>	Event	333	92	001	Restore	<input checked="" type="checkbox"/>	Restore	333	92	001

Remember password ☐

Default settings

Expander **iO** has: terminals for 1 input, 1 output (relay contacts) and 1-Wire serial bus for connecting temperature sensors.

Relay output can be controlled according to logical (IF, THEN) conditions.

Input IN1 type – set the input type (NO or NC).

Max °C(T1) – when the temperature is higher than this setting, an event message will be generated. For an event message to be generated, it must be enabled in the table.

Max °C(T2) – when the temperature is lower than this setting, an event message will be generated. For an event message to be generated, it must be enabled in the table.

Relay control – set logical (IF, OR) conditions, upon which the relay output will be controlled.

In the table inputs can be assigned Contact ID event and restore codes. After an input is triggered, the communicator will send an event with the set event code to the monitoring station receiver and to **Protegeus** app. Set as described in the previous page about **iO-8 expander settings window**.

W17u WiFi communicator settings window



TrikidisConfig 1.66.11 G16_3210

Program Action About

Read [F4] Write [F5] Open [F8] Save [F9] Disconnect

Modules list Module 1

W17u

Serial No: 000004

DHCP mode: DHCP

Static IP: 192.168.1.27

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.254

Wifi SSID name: Trikidis2

Wifi SSID password: 56DsD96

Contact ID event code						Contact ID restore code					
Event	Enable	E/R	CID	Part.	Zone	Event	Enable	E/R	CID	Part.	Zone
BUS_FAULT	<input checked="" type="checkbox"/>	Event	333	91	001	Restore	<input checked="" type="checkbox"/>	Restore	333	91	001

Remember password ☐

- **DHCP mode** – WiFi module's mode for registering to network (manual or automatic).
- **Static IP** – static IP address for when manual registering mode is set.

- **Subnet mask** – subnet mask for when manual registering mode is set.
- **Default gateway** – gateway address for when manual registering mode is set.
- **Wifi SSID name** – name of the WiFi network that the **W17u** will connect to.
- **Wifi SSID password** - WiFi network password.

In the table, you can assign Contact ID event and restore codes to the RS485 data bus fault event. When connection between the **W17u** and **G16** is disrupted or re-established, the **G16** will send a message with the assigned CID code to the CMS and **Protegeus** app.

Note: You must configure the **G16** to send messages to CMS and **Protegeus**, see chapters 2.2 “Settings for connection with Central Monitoring Station” and 2.1 “Settings for connection with Protegeus app”.

6.7 “Event summary” window

This window allows you to turn on, off, and modify internal messages sent by your device. Disabling an internal message in this window will prevent it from being sent regardless of other settings.



In this window, you can turn on, turn off or change the internal event messages sent by the device. After turning off the internal event in this window, it will not be sent irrespective of other settings.

- **COMMUNICATION** – message about connection error between the control panel and **G16**.
- **IN_ALARM** – message about input (IN) circuit trigger.
- **IN_TAMPER** – message about input (IN) circuit tamper trigger.
- **PING** – PING heartbeat signal.
- **POWER** – message about low power supply voltage.
- **REMOTE_STARTED** – message about remote connection to configure **G16** with **TrikdisConfig**.
- **REMOTE_FINISHED** – message about disconnection from remote configuration with **TrikdisConfig**.
- **START** – message about **G16** connecting to the network.
- **TEST** – periodic test message.

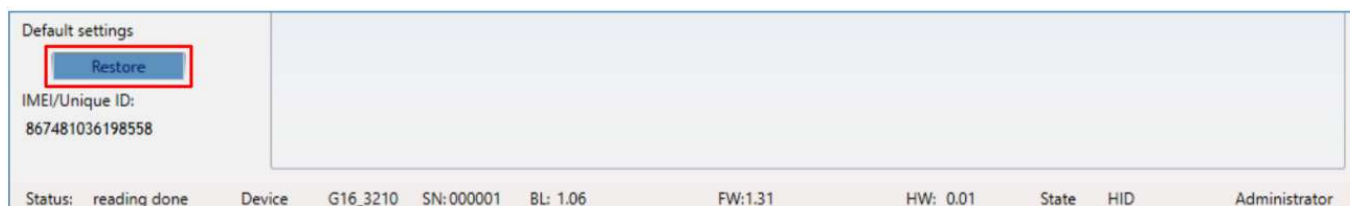
Note: To enable periodic TEST messages and set their period, go to **CMS reporting -> Settings -> Test period**.

- **Enable** – when selected, the sending of messages is enabled.

You can change the Contact ID code for each event, and also the zone and partition number.

6.8 Restoring factory settings

To restore the communicator's factory settings, you need to click the **Restore** button in the **TrikdisConfig** window.

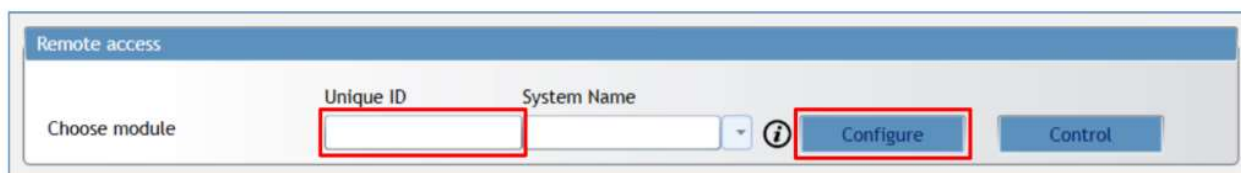


7 Remote configuration

Important: Remote configuration will work only if:

1. The inserted SIM card is activated and the PIN code is either entered or disabled;
2. **Protegeus cloud** is enabled. How to enable cloud is described in section 6.4 “User reporting” window;
3. Power supply is connected (“POWER” LED illuminates green);
4. Registered to the network (“NETWORK” LED illuminates green and blinks yellow).

1. Start the configuration program **TrikdisConfig**.
2. In the **Remote access** section enter the communicator’s **IMEI/Unique ID** number. This number can be found on the device and the packaging sticker.



3. (Optional) in the **System name** field, enter the desired name for the **G16** with this Unique ID.
4. Press **Configure**.
5. In the newly opened window click **Read [F4]**. If required, enter the administrator or installer code. To save the password, select “**Remember password**”.
6. Set the necessary settings and when finished, click **Write [F5]**.

8 Test communicator performance

When the configuration and installation is complete, perform a system check:

- 1) Generate an event:
 - by arming/disarming the system with the control panel’s keypad;
 - by triggering a zone alarm when the security system is armed.
- 2) Make sure that the event arrives to the alarm receiving center and/or is received in the **Protegeus** application.
- 3) To test communicator input, trigger it and make sure to receive the correct event.
- 4) To test the communicator outputs, activate them remotely and check their operation.
- 5) If the security control panel will be controlled remotely, arm/disarm the security system remotely by using the **Protegeus** app.

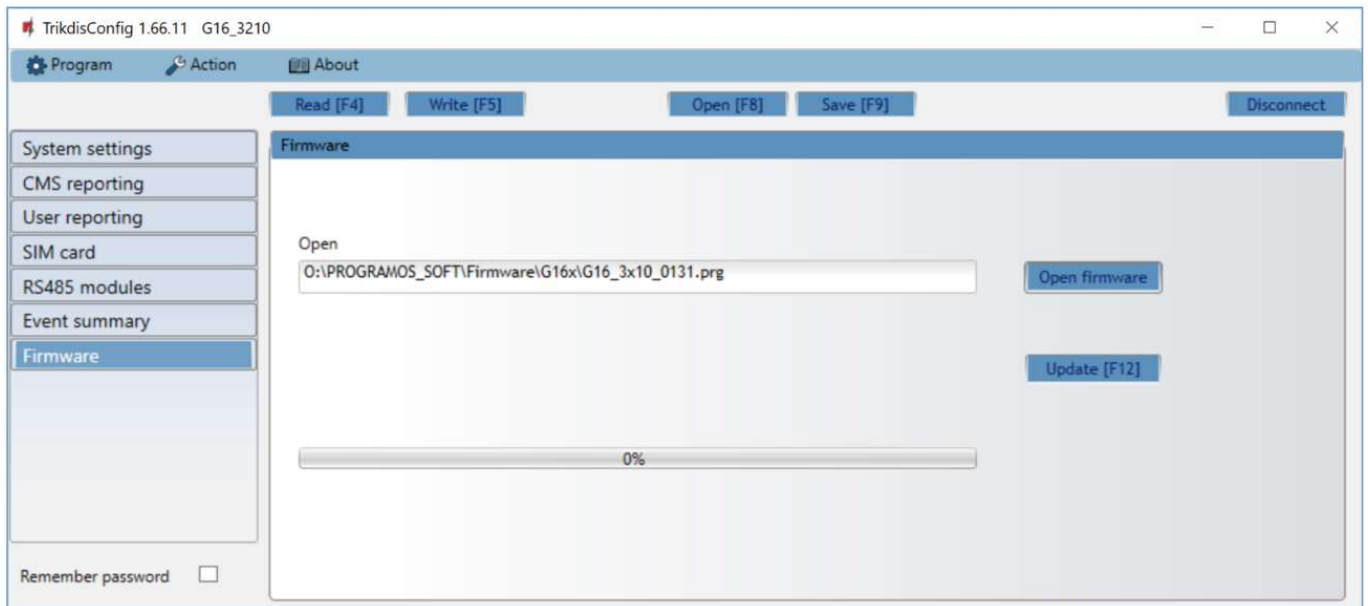
9 Firmware update

Note: When the communicator is connected to **TrikdisConfig**, the program will automatically offer to update the device’s firmware if updates are present. Updates require an internet connection. Antivirus software, firewall or strict access to internet settings can block the automatic firmware updates.

The communicator’s firmware can also be updated or changed manually. After an update, all previously set settings will remain unchanged. When writing firmware manually, it can be changed to a newer or older version. To update:

1. Run **TrikdisConfig**.
2. Connect the communicator via USB cable to the computer or connect to the communicator remotely.

- If a newer firmware version exists, the software will offer to download the newer firmware version file.
3. Select the menu branch **Firmware**.



4. Press **Open firmware** and select the required firmware file. If you do not have the file, the newest firmware file can be downloaded by registered users from www.trikdis.com , under the download section of the **G16** communicator.
5. Press **Update [F12]**.
6. Wait for the update to complete.