IP Bridge Pro / Pro 3G/4G
Remote monitoring IP interface and transmission module

USER MANUAL

for module version V2.1 and newer
Document version: 1.7 18.02.2021

Table of contents

1 Main function of IP Bridge

The basic function of IP Bridge is to transmit the signals generated on the connected alarm system and its contact inputs towards a monitoring station via wired internet or in case it has an extension panel via mobile internet (GPRS, 3G, 4G). For signal transmission, the alarm system must be set to use Contact ID based communication.

Features:

- event sending through IP channel using TEX, TELLMon or SIA IP protocol
- phone line emulation
- 6 configurable server/receiver IP addresses
- built-in web server for configuration and control

Characteristics:

- 1 emulated phone line
- 6 NO/NC (configurable) contact inputs
- 6 NO (normally open) relay outputs
- 1 RS232 input
- 1 Ethernet connector
- 1 USB host

Information on the SD card used in this product

The IP Bridge is an operating system-based device that uses an SD card to store data. Depending on the use the device can execute hundreds of write operations per minute to the SD card (e.g. recording IP camera images). The number of write operations is closely related to the expected lifetime of the SD card.
Considering that the SD card's lifetime may be different depending on the use, the manufacturer **gives 1 year warranty for the SD card delivered with the device**.
Since the SD card is required for the device to work properly, it is recommended to make a backup of the SD card after the device is set. Ask TELL Technical Support for help to make a backup.

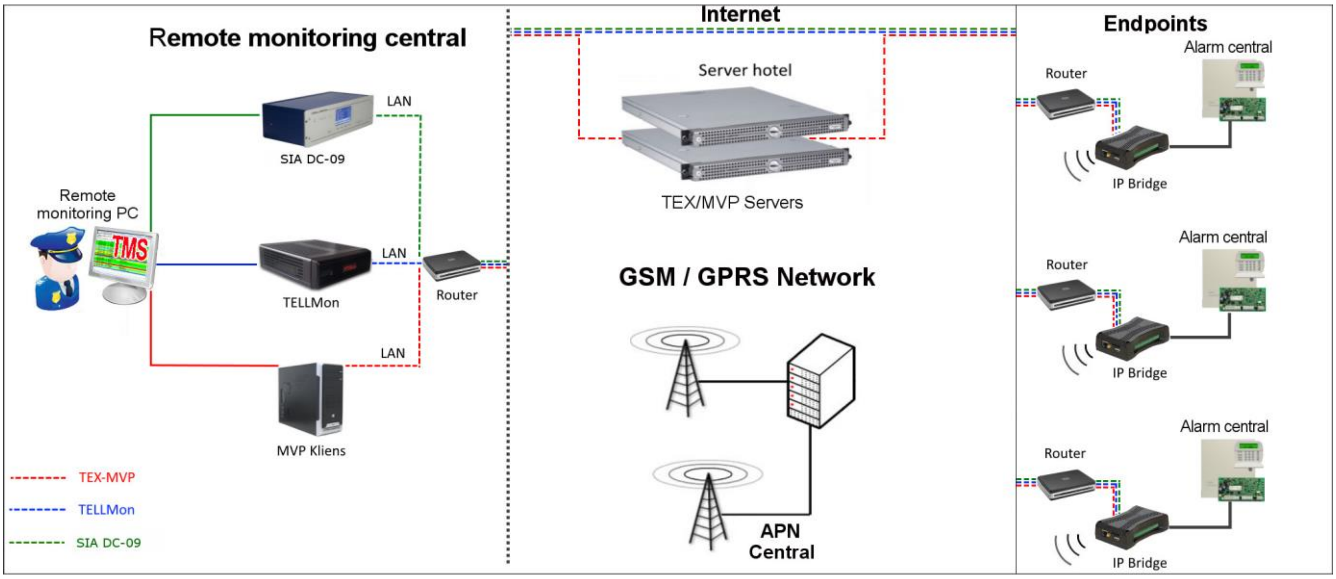
Third party services

Certain features of the IP Bridge are based on third-party services and devices. The flawless operation of third party service is required for the proper functioning of these features. These features and devices are as follows: VOIP service, NTP server, mobile service, FTP / SFTP server, router, alarm center and IP camera.

Since the correct functioning of these IP Bridge features depends on the faultless operation of the third-party service, the manufacturer can not guarantee any defects resulting from failure or malfunction of the third party service.

2 System operation

The **IP Bridge** transmits the signals of the alarm system connected to its simulated phone output and signals generated on its inputs towards a TEX-MVP remote monitoring server, TELLMon or SIA DC-09 receivers via wired internet. The route of the signals is illustrated in the following overview of the system.



Route of the signals

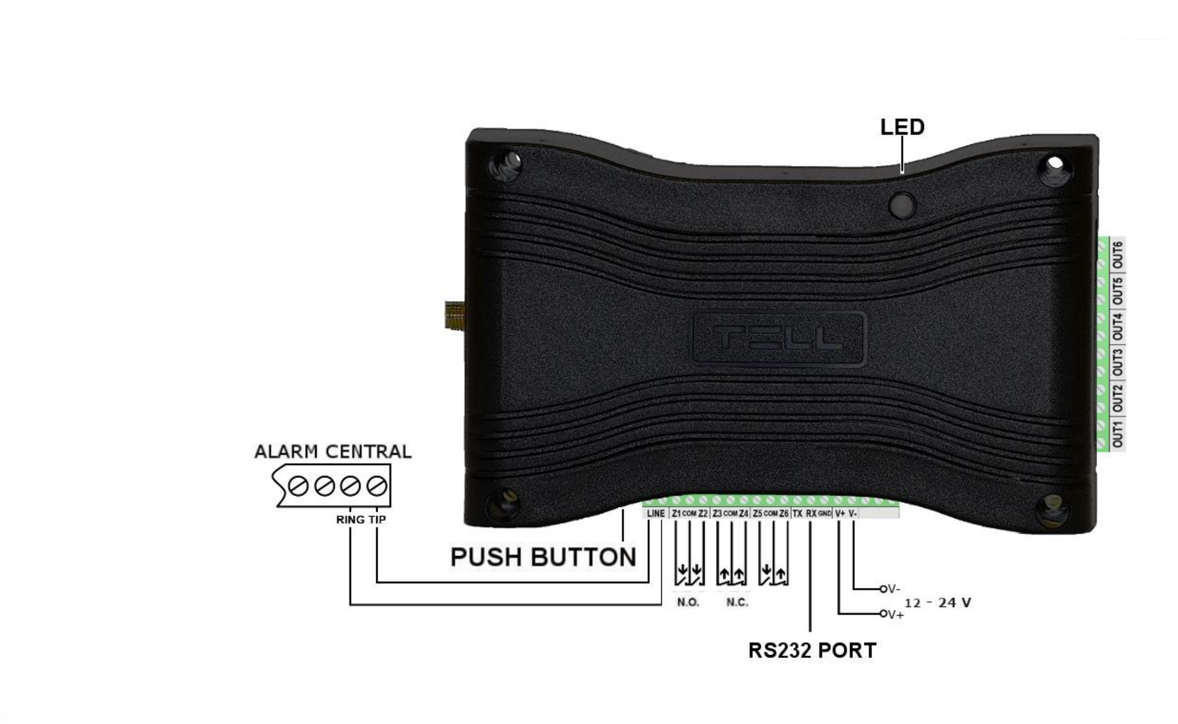
- **Connection with servers/receivers**

The module keeps alive the connection with the servers/receivers by sending periodic signals to their IP addresses. If the connection with any of the IP addresses is lost the device attempts to reconnect at least once per minute.

- **Event sending/Acknowledgement**

Events are sent to all preset IP addresses at the same time. The module acknowledges the event towards the monitoring station if it receives at least one ACK from any of the preset IP addresses. The same rule is applied to the module's internal events. Regardless the acknowledgement it continues to report the event to the rest of the IP addresses. If it doesn't receive an ACK from an IP address it attempts to report the event in every 10 seconds via LAN or in every 20 seconds via mobile internet for up to 10 minutes. If the event couldn't be reported for 10 minutes for all the preset IP addresses, the module stops trying. This event won't be reported again, but it will be in the module's event log. If any of the inputs is activated when a power failure occurs, an event will be generated again when the power comes back.

3 Wiring



Wiring diagram

- **Wiring alarm central**

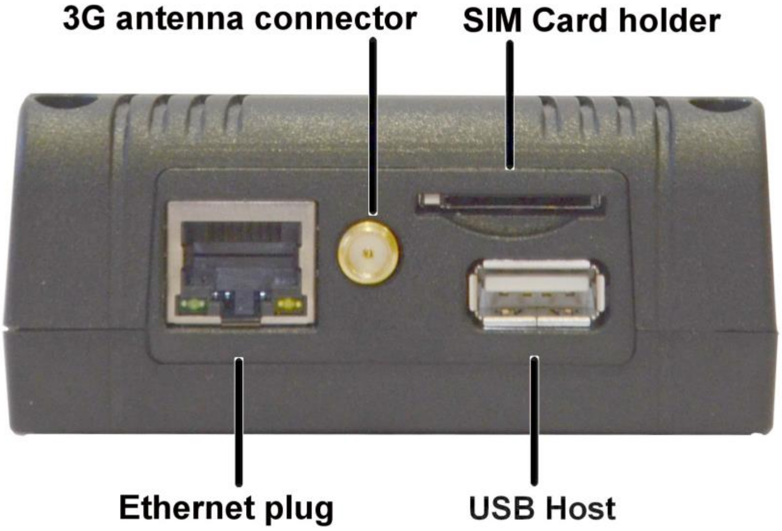
Connect the alarm central's telephone line input to the module's „LINE" terminals.

- **Wiring contact inputs**

Connect the inputs accordingly to the configured control mode, normally open (N.O.) or normally closed (N.C.).

- **Wiring outputs**

The outputs provide potential free, normally open (N. O.) contacts, please use them accordingly. Pay attention to the maximum loads supported by the outputs, which is 1A @ 12V DC by output! In case of higher load or higher voltage please use an external relay!



- **Connecting Internet**

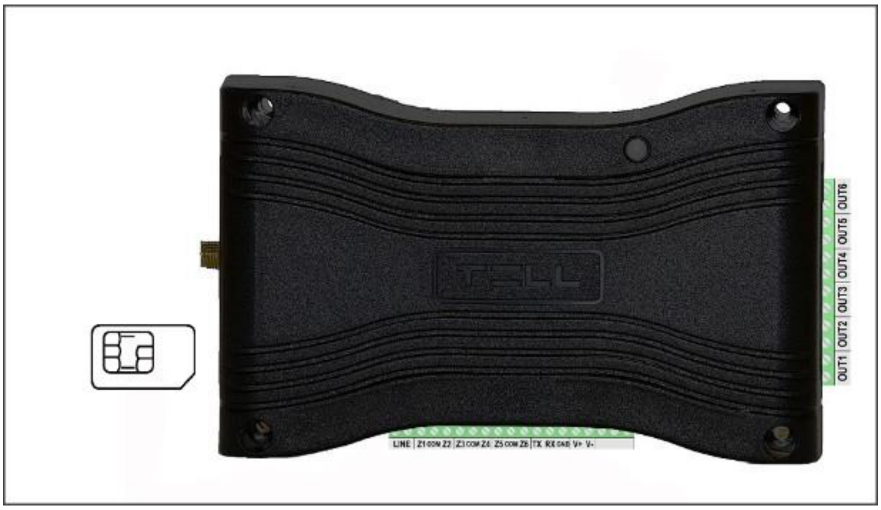
Connect the local internet network cable (LAN) coming from the router to the Ethernet connector of the IP Bridge.

- **Wiring antenna**

If the module has a 3G/4G modem, use the 3G/4G antenna connector to wire the antenna.

- **SIM card holder**

If the module has 3G/4G modem, insert the SIM card into the card holder according to the below and push it until it clicks. If you want to remove the SIM card, just push the card again. Due to the design of the SIM card holder it is recommended to use a mini ("normal") SIM card. 3FF ("multi-cut") SIM card may cause contact problems. When using a micro or nano SIM card, an adapter can be a solution for converting to mini ("normal") SIM card.


OUT1 OUT2 OUT3 OUT4 OUT5 OUT6
LINE Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 TX RX GND V+ V-

Inserting SIM card

- **Network configuration**

The module's network is configurable through the USB Host with a pendrive.

The connectors on IP Bridge panel	
LINE	Simulated telephone line for connecting alarm panel
Z1	1. contact input (considered between Z1 and COM)
COM	Common terminal between Z1 and Z2 contact inputs
Z2	2. contact input (considered between Z2 and COM)
Z3	3. contact input (considered between Z3 and COM)
COM	Common terminal between Z3 and Z4 contact inputs
Z4	4. contact input (considered between Z4 and COM)
Z5	5. contact input (considered between Z5 and COM)
COM	Common terminal between Z5 and Z6 contact inputs
Z6	6. contact input (considered between Z6 and COM)
TX	RS232 serial port TX
RX	RS232 serial port RX
GND	RS232 serial port GND
V+	Supply voltage 12-24V DC
V-	Supply voltage negative polarity (GND)
Outputs	
OUT1	1. relay contact output, normally open (N. O.)
OUT2	2. relay contact output, normally open (N. O.)
OUT3	3. relay contact output, normally open (N. O.)
OUT4	4. relay contact output, normally open (N. O.)
OUT5	5. relay contact output, normally open (N. O.)
OUT6	6. relay contact output, normally open (N. O.)

4 Setup the alarm control panel

Check the followings on the alarm control panel you connected the IP Bridge module to:

- Contact-ID communication format has to be set in the alarm control panel.
- The alarm control panel must be configured for communication to monitoring station as it were using a wired phone line.
- Set the dialing to TONE mode.
- Regardless the dialed phone number the IP Bridge emits the handshake signal and receives the Contact ID events.

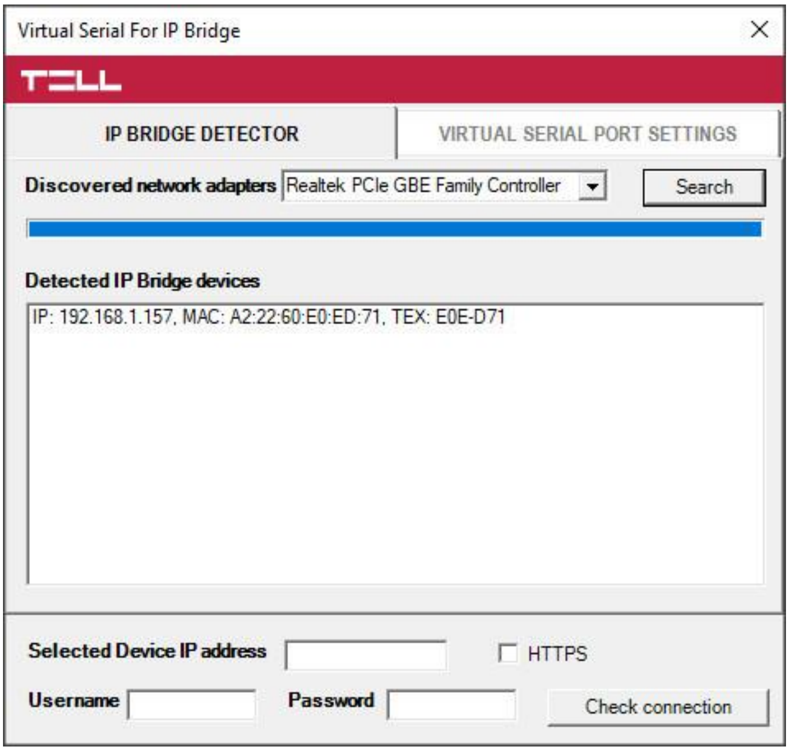
5 Installation, setup

Attention! Do not mount the device in places where it can be affected by strong electromagnetic interference! Do not mount the device in wet places or places with high degree of humidity!

After mounting and connecting the local internet the device can be powered up. Setting up the module can be done through an internet browser from any computer that is connected to the same local network as the device is. By default, the module is set to use DHCP, so IP address will be assigned to it by the local router.

Use the **IP Bridge Virtual Client** program, which can be downloaded from www.tell.hu website, to find the modules' IP Addresses. In this case you need to enter into your browser the IP address of the device you'd like to manage (e.g. pl.: 192.168.1.198). The web based interface uses port 80.

Using **IP Bridge Virtual Client** program


Virtual Serial For IP Bridge
TELL
IP BRIDGE DETECTOR
VIRTUAL SERIAL PORT SETTINGS
Search
Detected IP Bridge devices
Selected Device IP address
□ HTTPS
Username
Password
Check connection

Discovered network adapters: Realtek PCIe GBE Family Controller

IP: 192.168.1.157, MAC: A2:22:60:E0:ED:71, TEX: E0E-D71

IP Bridge Virtual Client

- Launch the program on a computer that is connected to the local network
- select the adapter from the **Discovered network adapters** list (It is important to select an adapter that is located on the same network as the IP Bridge.)
- click the Search button
- the program detects the IP Bridge devices connected to the network and lists them (see figure above)
- enter the found IP address into your browser

The displayed device list contains the following details:

IP:	the module's IP address
MAC:	the module's MAC address
TEX:	the module's TEX group code and also the device's ID (this can be modified later in the settings)

If the IP Bridge Virtual Client is unable to detect the module on the network, the UDP Broadcast service is disabled on the router. Since the IP Bridge uses DHCP by default, in this case, you can find the module's IP address in the DHCP list of the router.

Getting the module's network address using a pendrive:

Insert a pendrive into the module’s USB Host connector. The module creates the export folder and adds the macaddress.cfg file (e.g.: "export/A2225C7D806B.cfg") that contains the network settings. Once the file has been copied, the LED turns red and the pendrive can be removed.
The USB drive can be 2.0 or 3.0 and the file system can be NTFS, FAT32, ext2 or ext4.

The file content has the following details:

```
PLUGGED=1                        // the module is connected to the network
TYPE=dhcp                        // the network type is DHCP
MAC=A2:22:60:E0:ED:79            // MAC address of the module
IP=192.168.1.91                  // IP address of the module
GATEWAY=192.168.1.1
NETWORK=192.168.1.0
SUBNETMASK=255.255.255.0
DNS1=tellsofthun.local
DNS2=192.168.1.2
DNS3=8.8.8.8
```

5.1 Service ports

The following ports are used by IP Bridge module:

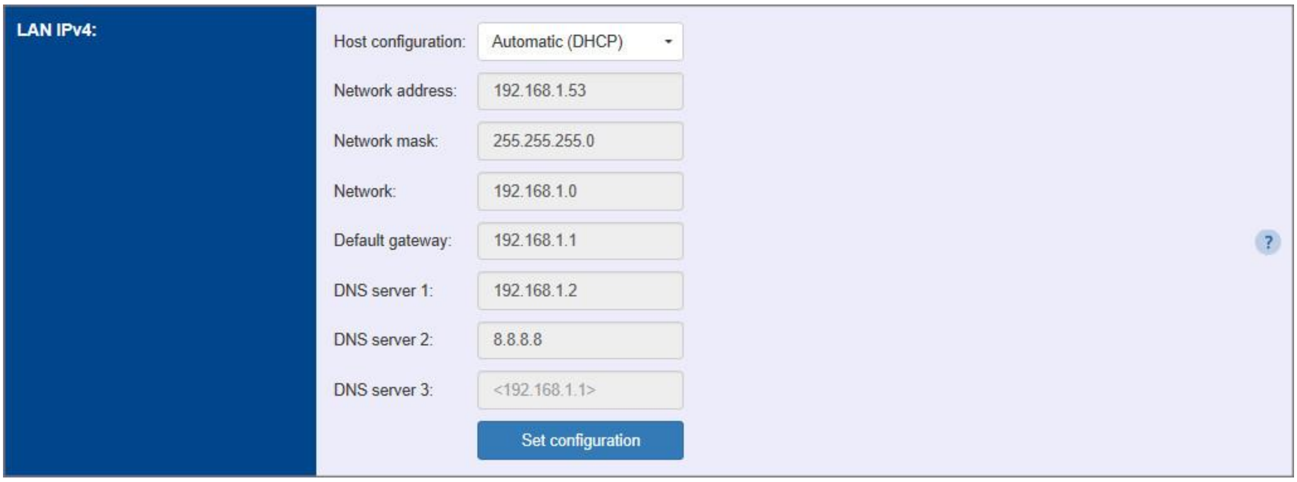
80	http web based interface
443	https web based interface
22	SSH – technical support

5.2 Router settings

If you’d also like to use the module’s web interface through the internet, set up on your router the port forwarding of port no. 80 and port no. 443 at the module’s IP address. If it is enabled in the module settings, then loading the web interface through port no. 80 (http://192.168.1.110) redirects to port no. 443 (https://192.168.1.110). In case the port no. 443 is already taken or forwarding of this port is not possible, you can also use a different one, but in this case open the page directly through https protocol (e.g.: https://192.168.1.110:8443). If you need the technical support’s help to solve any issue, you’ll need to open and forward port no. 22.

5.3 Network configuration

Network settings can be edited on the “General" tab of web interface. Here you can also update the IP configuration manually, if necessary.



LAN IPv4:

Host configuration: Automatic (DHCP)
Network address: 192.168.1.53
Network mask: 255.255.255.0
Network: 192.168.1.0
Default gateway: 192.168.1.1
DNS server 1: 192.168.1.2
DNS server 2: 8.8.8.8
DNS server 3: <192.168.1.1>

The network configuration can be set and modified with a pendrive as well. You can use USB 2.0 or USB 3.0 pendrives with NTFS, FAT32, ext2 or ext4 file system on it. To modify the network settings create the import/macaddress folder (pl.: import/A2225C7D806B) on the pendrive. Within this folder create the ipbridge.dnr file, that contains the settings.

The following settings can be added to the config textfile (the values and IP addresses below are only samples!):

ADDRESS="192.168.1.198"	: to set the static IP address
NETMASK="255.255.255.0"	: to set the netmask for the IP address
NETWORK="192.168.1.0"	: to set the default subnet
GATEWAY="192.168.1.1"	: to set the gateway for the static IP address
DNS1="8.8.8.8"	: to set DNS1 for the static IP address
DNS2="208.67.220.220"	: to set DNS2 for the static IP address
ADDRESS="dhcp"	: to restore DHCP mode

You can leave the unused settings in the configuration file, in this case mark them with a **#** character at the beginning of the line, so that the module ignores them (e.g.: **#ADDRESS="dhcp"**).
Important! In the created file add an ENTER at the end of each line and make sure that it doesn't contain any further whitespaces (tab, space, etc.).

<u>Configuration sample:</u>

If the A2225C7D806B MAC address was read from the module the path is the following: import/A2225C7D806B/ipbridge.dnr

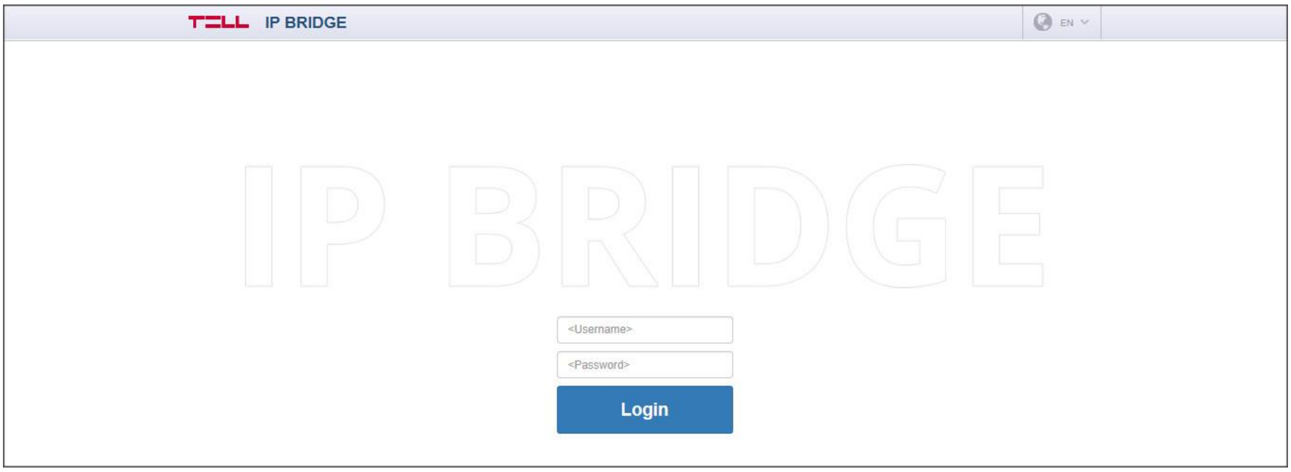
If you want the module to use 192.168.1.115 static IP, the 255.255.255.0 netmask, the 192.168.1.0 subnet, the 192.168.1.1 gateway, the 8.8.8.8 DNS1, the 208.67.220.220 DNS2, the content of the textfile must be as follows:

```
ADDRESS="192.168.1.115"
NETMASK="255.255.255.0"
NETWORK="192.168.1.0"
GATEWAY="192.168.1.1"
DNS1="8.8.8.8"
DNS2="208.67.220.220"
```

To apply the settings in the configuration file insert the pendrive into the module's USB Host connector. The module reads the settings from the file. The pendrive can be removed, when LED turns red. After removal LED turns green, the module applies the new settings then reboots. After restarting the LED is green.

6 Web based interface of IP Bridge

Enter the module's IP address into your browser to open the web intarface (e.g.: 192.168.1.198) and enter the username and password for login (see figure below). To access the interface via Internet, enter into your browser the router's external IP address followed by the port number you've forwarded (e.g.: 93.189.143.72:8181). In case the https redirect is enabled in the module, after connecting through http (port no. 80) automatically redirects to https (port no. 443).



Login

The default login credentials are:

Username:	**admin**
Password	**admin**

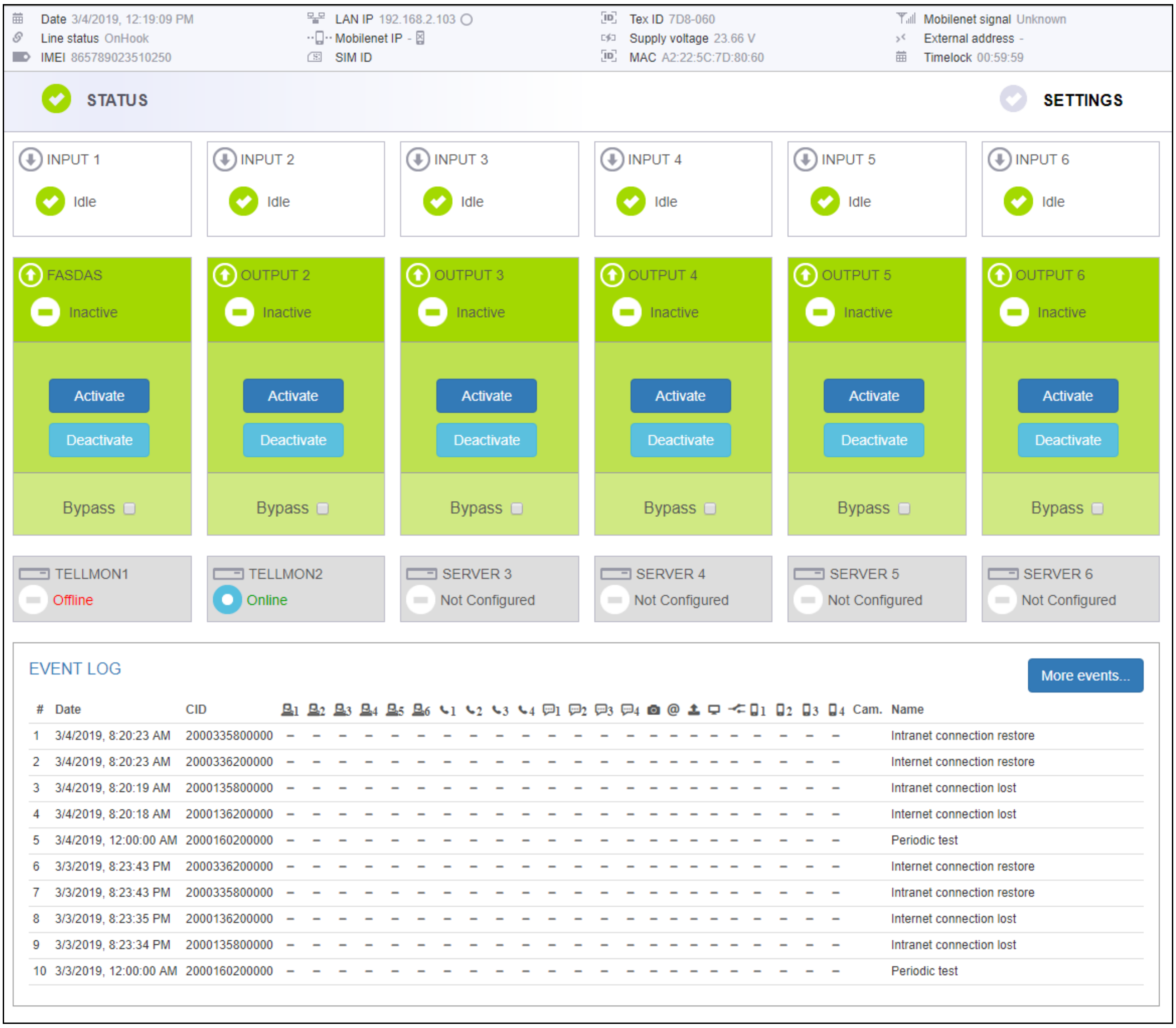
After the first login change the default passwords.

To add and manage additional users, the module has RADIUS server support that can be set in the „**RADIUS server**" section of the „**Settings**" menu.

If you enter incorrect username or password several times, the module will block the login from your IP address for the duration that is set in the settings. The default setting blocks the login for an hour after 5 incorrect login attempts.

After signing in, when you modify any module setting a red bar at the top of the page warns you to save the changes. There is no functional difference between the Save and Cancel buttons at the bottom of the page and on the warning bar.

6.1 Module status



Date 3/4/2019, 12:19:09 PM
Line status OnHook
IMEI 865789023510250

LAN IP 192.168.2.103 ○
Mobilenet IP -
SIM ID

Tex ID 7D8-060
Supply voltage 23.66 V
MAC A2:22:5C:7D:80:60

Mobilenet signal Unknown
External address -
Timelock 00:59:59

STATUS   SETTINGS

INPUT 1 Idle	INPUT 2 Idle	INPUT 3 Idle	INPUT 4 Idle	INPUT 5 Idle	INPUT 6 Idle
FASDAS Inactive Activate Deactivate Bypass □	OUTPUT 2 Inactive Activate Deactivate Bypass □	OUTPUT 3 Inactive Activate Deactivate Bypass □	OUTPUT 4 Inactive Activate Deactivate Bypass □	OUTPUT 5 Inactive Activate Deactivate Bypass □	OUTPUT 6 Inactive Activate Deactivate Bypass □
TELLMON1 Offline	TELLMON2 Online	SERVER 3 Not Configured	SERVER 4 Not Configured	SERVER 5 Not Configured	SERVER 6 Not Configured

EVENT LOG

More events...

#	Date	CID	👤1	👤2	👤3	👤4	👤5	👤6	📞1	📞2	📞3	📞4	💬1	💬2	💬3	💬4	📷	@	⬆	🖥	⭠	▯1	▯2	▯3	▯4	Cam.	Name
1	3/4/2019, 8:20:23 AM	2000335800000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Intranet connection restore
2	3/4/2019, 8:20:23 AM	2000336200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Internet connection restore
3	3/4/2019, 8:20:19 AM	2000135800000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Intranet connection lost
4	3/4/2019, 8:20:18 AM	2000136200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Internet connection lost
5	3/4/2019, 12:00:00 AM	2000160200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Periodic test
6	3/3/2019, 8:23:43 PM	2000336200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Internet connection restore
7	3/3/2019, 8:23:43 PM	2000335800000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Intranet connection restore
8	3/3/2019, 8:23:35 PM	2000136200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Internet connection lost
9	3/3/2019, 8:23:34 PM	2000135800000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Intranet connection lost
10	3/3/2019, 12:00:00 AM	2000160200000	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Periodic test

Module status

The module displays the module status page after login (see figure above). In the header the basic status information is displayed: the module's date/time, current LAN IP address, supply voltage, the module's remote monitoring group ID and device ID and the simulated phone line status. In addition, if the IP Bridge has an extension panel, the mobile internet's IP address, the signal strength with icon, the IMEI number and the SIM ID are also here.

The icon next to the IP address indicates the status of the connection:

🌐 **Internet connection is OK**. There's a Ping server set in the Settings to verify the internet connection and the module reaches it.

⊕ **Intranet connection is OK**. There's a Ping server set in the Settings to verify the intranet and it can be reached by the module. (This icon is displayed, even if there's also set a ping server to verify the internet, but that one can't be reached by the module.)

⊗ **There's no Internet connection.** There's a Ping server set in the Settings to verify the internet connection, but the module can't reach it.

○ **Network connected.** LAN cable is connected to the module, there is an IP address, but there's no ping server set.

? **Unknown network.** LAN cable is connected, there's ping server set (internet, intranet or both), but none of them can be reached.

No connection. This icon indicates that the module is starting or there's no LAN cable connected.

If the device has an extension module, the following icons can be displayed next to the Mobileinternet IP Address:

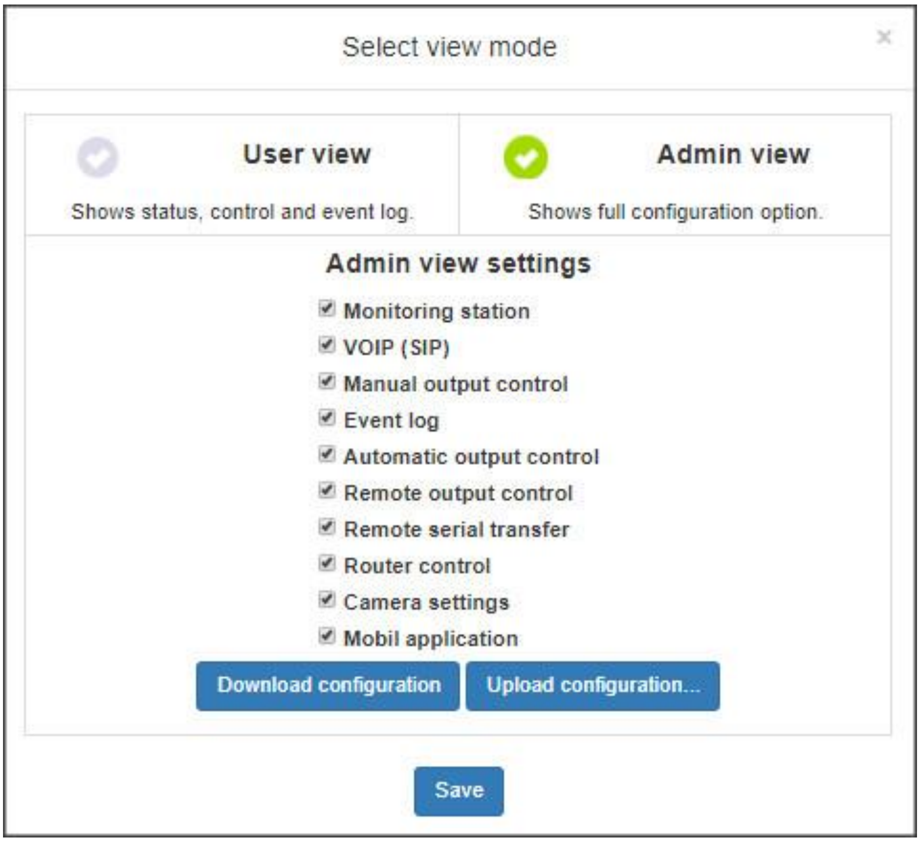
Internet connection is OK. This icon is displayed if the module has a mobile internet IP, but no Ping server is set or if there's a Ping server set in the Settings to verify the internet connection and the module can reach it.

There's no mobile internet connection: Also, this icon will be displayed, if the module can't connect to the mobile network, or if a Ping server is set in the Settings, but it can't be reached by the module.

The language of IP Bridge's web interface can be set with the language icon on the right side of the header.

The „gear" icon opens the view mode selector window (figure below) where you can also customize the selected view, to display only those menu items that are needed. Here you can also download the configuration to make a backup of your settings, or you can also upload a previously saved one.

Attention! The saved configuration file contains sensitive data. Please store it accordingly.



Select view mode

○ User view

Shows status, control and event log.

● Admin view

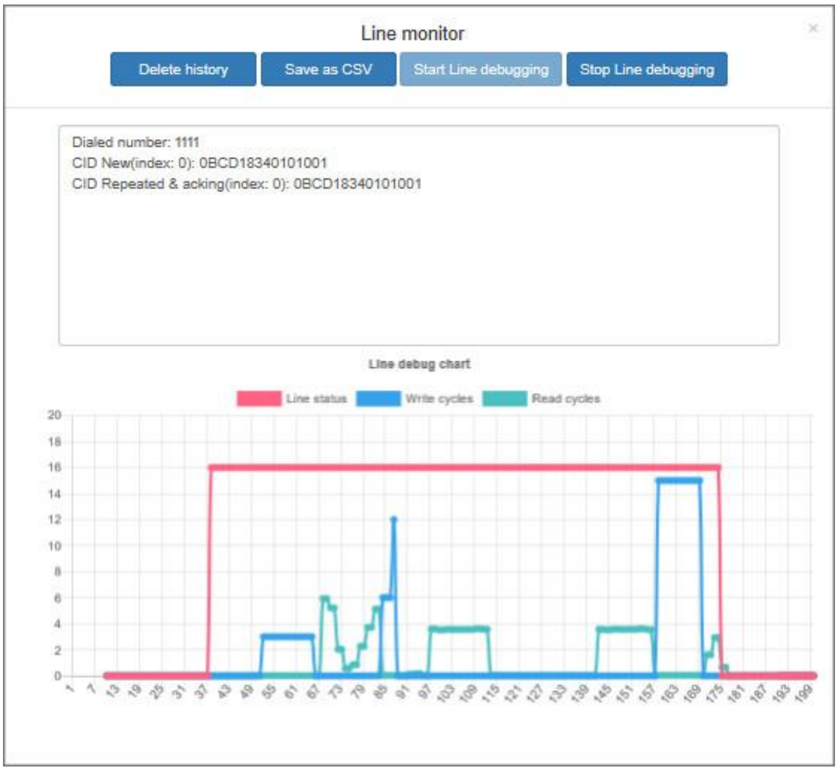
Shows full configuration option.

Admin view settings

- ☑ Monitoring station
- ☑ VOIP (SIP)
- ☑ Manual output control
- ☑ Event log
- ☑ Automatic output control
- ☑ Remote output control
- ☑ Remote serial transfer
- ☑ Router control
- ☑ Camera settings
- ☑ Mobil application

Select view mode

Line log: By clicking the icon next to the „Line status" opens the Line log window (figure below), which allows you to monitor the alarm control panel's communication. To graphically monitor the communication on the simulated phone line click the "Start Line debugging" button. Here you can export the incoming data into a csv file.



```
Dialed number: 1111
CID New(index: 0): 0BCD18340101001
CID Repeated & acking(index: 0): 0BCD18340101001
```

Line log

Input section: you can check the current state of the module's zone inputs: Idle / Active / Sabotage

Output section: you can check the current state of the outputs and also remote control them

Output status: Inactive/Active

Output control: outputs can be remote controlled with the Activate/Deactivate buttons.

Control with events: the automatic control of an output can be enabled or disabled with the bypass checkbox (e.g.: because of a malfunctioning sensor the output can be disabled.)

Servers section: you can check the connection with servers/receivers here. The connection status can be:

Not configured: the IP address and/or port is not set
Checking…: booting, checking in progress
Connecting…: connection is in progress
Authenticating…: authentication is in progress
Online: successful connection
Offline: the server/receiver is unavailable.

If the module is continuously trying to authenticate, it is likely that bad but existing IP address/port is set or the receiver on the IP address is incompatible with the IP Bridge module.

Event log: The Event Log (figure below) shows the events received from the alarm control panel through the simulated telephone line and also the internal events of the module. The module stores the past 500 events. The list always contains the last 10 events.

Date/time: date and time of the event
CID: the event’s Contact ID code

🖳1–🖳6 **:** indicates whether there was notification sent to the IP address of S1…S6 server/receiver

📞1–📞4: indicates whether there was V1-V4 phone number notified via VOIP voice call

💬1–💬4: indicates whether there was M1-M4 phone number notified via SMS

📷: the status of saving the camera images associated with the event

@: the status of sending emails associated with the event

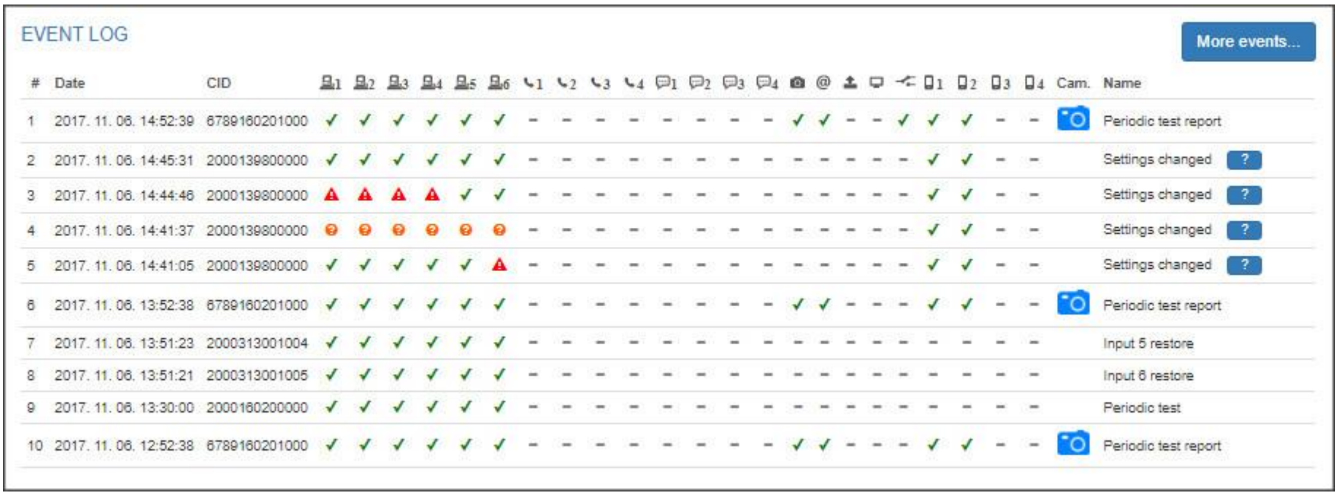
⭱: the status of uploading camera images to an FTP server

🖵: the status of displaying event in TMS

⇄: the status of relay control associated with the event

▯1–▯4: indicates whether push message was sent to A1-A4 smart device

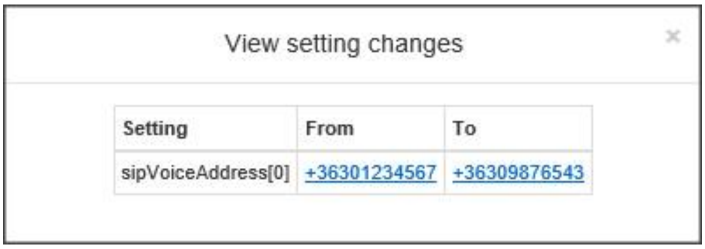
Cam.: If a camera image is associated with the event a camera icon appears in this column. By clicking on the icon the camera images can be viewed in a popup window.


EVENT LOG

#	Date	CID	🖳1	🖳2	🖳3	🖳4	🖳5	🖳6	📞1	📞2	📞3	📞4	💬1	💬2	💬3	💬4	📷	@	⭱	🖵	⇄	▯1	▯2	▯3	▯4	Cam.	Name
1	2017. 11. 06. 14:52:39	6789160201000	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	✓	–	–	✓	✓	✓	–	–	📷	Periodic test report
2	2017. 11. 06. 14:45:31	2000139800000	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–		Settings changed ?
3	2017. 11. 06. 14:44:46	2000139800000	⚠	⚠	⚠	⚠	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–		Settings changed ?
4	2017. 11. 06. 14:41:37	2000139800000	?	?	?	?	?	?	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–		Settings changed ?
5	2017. 11. 06. 14:41:05	2000139800000	✓	✓	✓	✓	✓	⚠	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–		Settings changed ?
6	2017. 11. 06. 13:52:38	6789160201000	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	✓	–	–	–	✓	✓	–	–	📷	Periodic test report
7	2017. 11. 06. 13:51:23	2000313001004	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Input 5 restore
8	2017. 11. 06. 13:51:21	2000313001005	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Input 6 restore
9	2017. 11. 06. 13:30:00	2000160200000	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Periodic test
10	2017. 11. 06. 12:52:38	6789160201000	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	✓	–	–	–	✓	✓	–	–	📷	Periodic test report

Short event log

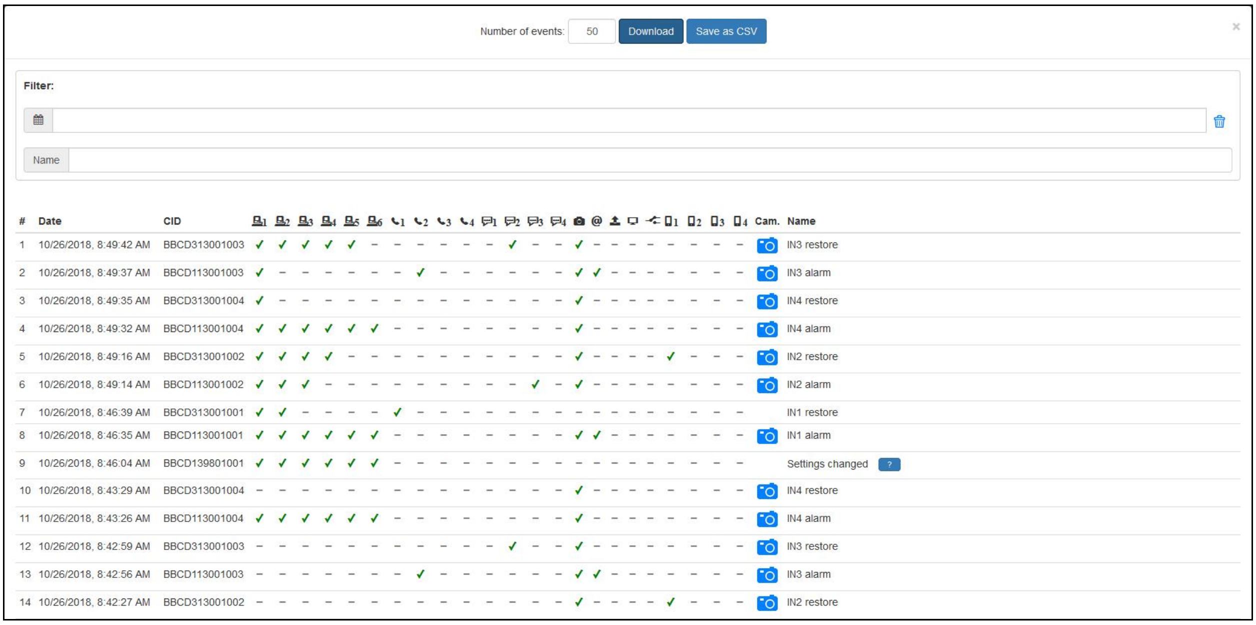
Name: This is the name of internal events or events received on telephone line. There’s a „?” icon next to the „Settings changed” events, which are generated when any of the settings are updated. Clicking on this icon you can check which setting was changed and what were the old and new values. (see figure below). If any sensitive information (e.g. password) has changed, it will not appear in the list of changes. If only sensitive data has been changed, the question mark icon will not be displayed.


View setting changes

Setting	From	To
sipVoiceAddress[0]	+36301234567	+36309876543

Setting changes

More events: The button opens a popup window where you can filter the events stored on the module (figure below).



#	Date	CID	🖥1	🖥2	🖥3	🖥4	🖥5	🖥6	📞1	📞2	📞3	📞4	💬1	💬2	💬3	💬4	📷	@	⬆	🖵	🔌	▯1	▯2	▯3	▯4	Cam.	Name
1	10/26/2018, 8:49:42 AM	BBCD313001003	✓	✓	✓	✓	✓	–	–	–	–	–	–	✓	–	–	✓	–	–	–	–	–	–	–	–	📷	IN3 restore
2	10/26/2018, 8:49:37 AM	BBCD113001003	✓	–	–	–	–	–	–	✓	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	📷	IN3 alarm
3	10/26/2018, 8:49:35 AM	BBCD313001004	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	📷	IN4 restore
4	10/26/2018, 8:49:32 AM	BBCD113001004	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	📷	IN4 alarm
5	10/26/2018, 8:49:16 AM	BBCD313001002	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	✓	–	–	–	📷	IN2 restore
6	10/26/2018, 8:49:14 AM	BBCD113001002	✓	✓	✓	–	–	–	–	–	–	–	–	–	✓	–	✓	–	–	–	–	–	–	–	–	📷	IN2 alarm
7	10/26/2018, 8:46:39 AM	BBCD313001001	✓	✓	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		IN1 restore
8	10/26/2018, 8:46:35 AM	BBCD113001001	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	📷	IN1 alarm
9	10/26/2018, 8:46:04 AM	BBCD139801001	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		Settings changed ?
10	10/26/2018, 8:43:29 AM	BBCD313001004	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	📷	IN4 restore
11	10/26/2018, 8:43:26 AM	BBCD113001004	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	📷	IN4 alarm
12	10/26/2018, 8:42:59 AM	BBCD313001003	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	✓	–	–	–	–	–	–	–	–	📷	IN3 restore
13	10/26/2018, 8:42:56 AM	BBCD113001003	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	📷	IN3 alarm
14	10/26/2018, 8:42:27 AM	BBCD313001002	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	✓	–	–	–	📷	IN2 restore

More events

Download: Downloads the set number of events stored in the module.

Save as CSV: The downloaded list can be saved in CSV format.

Filter: Events can be filtered by date range and event name.

The meaning of signs in the columns:

⇔ : new event was created and added to the notification queue

❓ : event sending in progress

✓ : successful event sending

– : server/receiver IP address is not set

⚠ : the signal couldn't be sent (e.g.: server is not available)

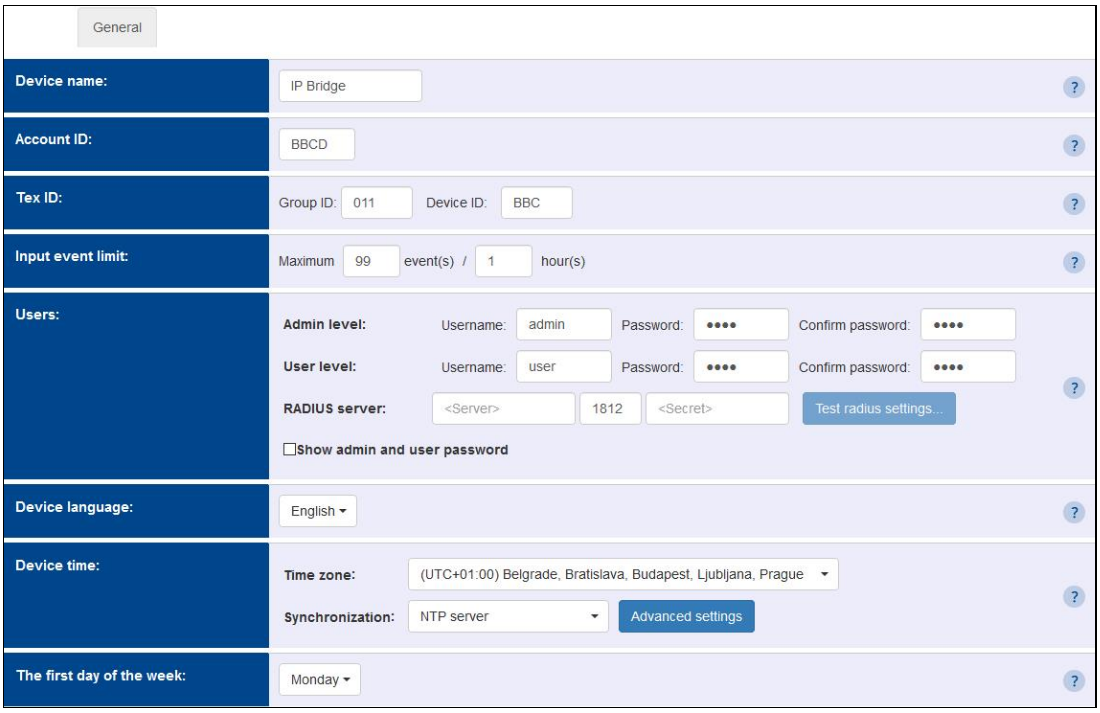
S : server connection ok, but no receipt was received

(serial port or connection failure at the monitoring station)

⏲ : Time out, event couldn't be sent within 10 minutes.

In the „More events…" window camera images and details of setting changes associated with the events are available just like in the short event list:

6.2 General settings



General

Device name:	IP Bridge
Account ID:	BBCD
Tex ID:	Group ID: 011 Device ID: BBC
Input event limit:	Maximum 99 event(s) / 1 hour(s)
Users:	Admin level: Username: admin Password: •••• Confirm password: •••• User level: Username: user Password: •••• Confirm password: •••• RADIUS server: <Server> 1812 <Secret> Test radius settings... □Show admin and user password
Device language:	English ▾
Device time:	Time zone: (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague ▾ Synchronization: NTP server ▾ Advanced settings
The first day of the week:	Monday ▾

General settings

You can configure the communication and operation settings on the „General” tab within „Settings” (figure above).

Device name: This is the unique name of the device that is displayed in the website’s header.

Account ID: The client identifier used for remote monitoring. This ID is used only for transmitting the module’s internal events. The external module events are forwarded with the ID that is received from the alarm system.

TEX ID:

Group ID: This is the monitoring station's ID in hexa format. If you don't have a Group ID, please contact your reseller.

Device ID: This is the module's 3 characters long ID in hexa format. The valid characters are 0...9, A, B, C, D, E, F.

Input event limit: This setting limits the number of events being taken into consideration in the selected period of time. The limitation will be applied by input but will affect all the inputs. After the limitation period has elapsed, the event becomes again enabled and can generate an alarm. The limitation period can be set between 1 and 99 hours. With this setting the repeating alarm caused by malfunctioning sensor can be avoided. In this case the output controlled by the event won’t work either.

Users: In default there’s one user with administrator level rights and one user with user level rights. Their username and password can be modified.

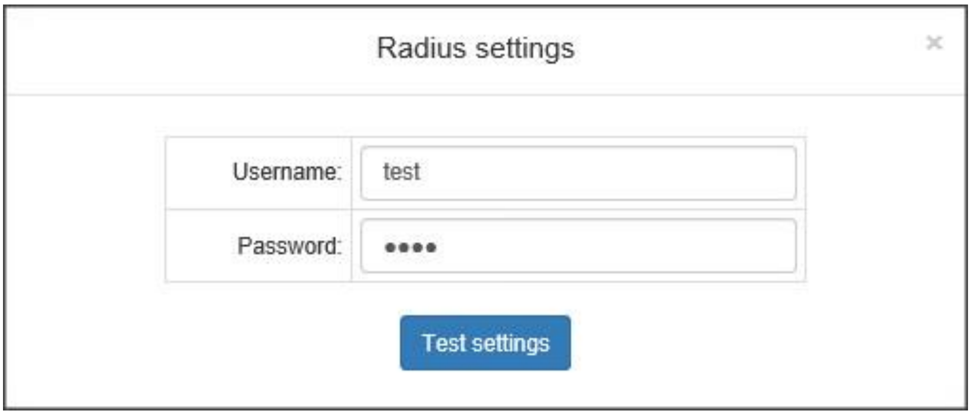
RADIUS server: Server access settings for adding and managing additional users.

Server: The IP address of the radius server.

Port: The port of the server. The default port is 1812.

Secret key: Encryption key for authentication.

Modify radius settings: In the popup window (see figure below) you can update the settings for Radius server connection. The connection data can be saved only after a successful test, so you can’t lock yourself out of the module.



Radius settings

Username: test

Password: ●●●●

Radius settings

Show admin and user password: Passwords will appear but will be hidden again after saving your changes.

Device language: Language of report sending.

Device time:

Device timezone: The proper time zone setting is necessary for the scheduled report sending via email and for creating periodic test reports.

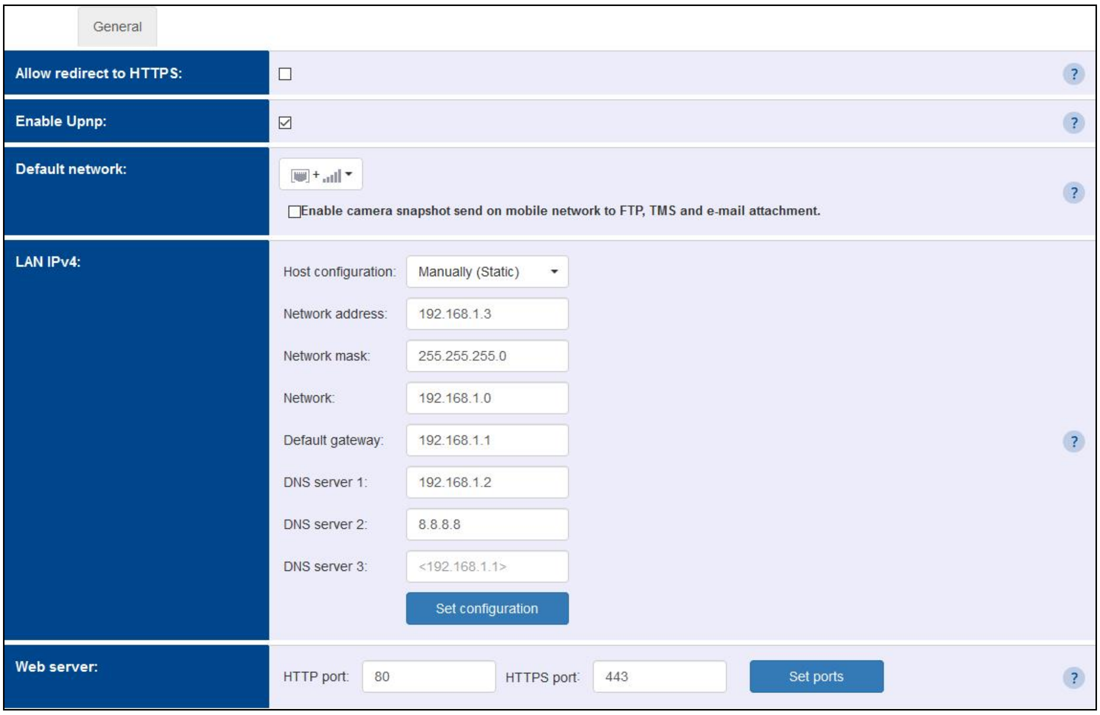
Synchronization:

NTP server: In the popup window you can enter and test 2 NTP servers.

Mobile application server: Time can also be synchronized through the TELL server. If you chose this option, you must enable the server connection. If it is not yet enabled, press the Advanced Settings button to be redirected to the appropriate settings.

Manual: If you do not have access to the Internet or you can not access the NTP or the TELL server through the network, you can manually enter the date and time.

The first day of the week: Setting up the first weekday is needed for the scheduled email sending.



General

Allow redirect to HTTPS:	□
Enable Upnp:	☑
Default network:	□Enable camera snapshot send on mobile network to FTP, TMS and e-mail attachment.
LAN IPv4:	Host configuration: Manually (Static) Network address: 192.168.1.3 Network mask: 255.255.255.0 Network: 192.168.1.0 Default gateway: 192.168.1.1 DNS server 1: 192.168.1.2 DNS server 2: 8.8.8.8 DNS server 3: <192.168.1.1>
Web server:	HTTP port: 80 HTTPS port: 443

General settings 2.

Allow access through HTTPS: It can be enabled that the module redirect the requests to a secure HTTPS connection.

Enable UPnP: The module can be enabled to use UPnP protocol. The UPnP service must be enabled in the network's router to work properly.

Default network: You can select default network for the services of the module, e.g. reporting towards monitoring station, email sending, remote serial data transfer or VOIP calls. If the selected option includes the mobile network communication, you can enable with the checkbox the image uploading via mobile internet as well. If the module doesn't have an extension panel LAN will be the default network and this field is hidden.

LAN IPv4: You can set up the device's IPv4 host configuration.

Host configuration: Assign automatically or manually.

Network address: The device's IP address.

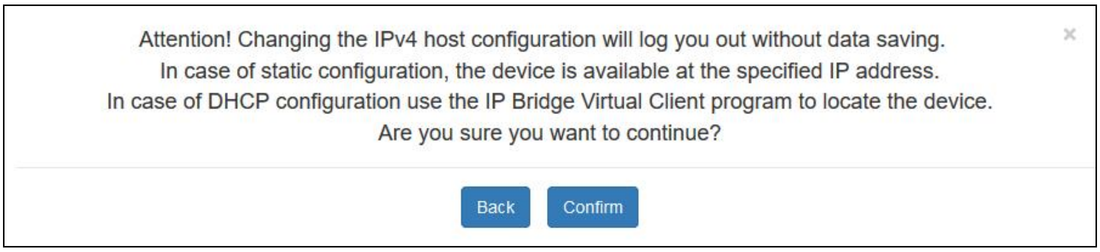
Network mask: The device's subnet mask.

Network: The device's subnet.

Default gateway: The device's default gateway. The device reaches the internet via this gateway.

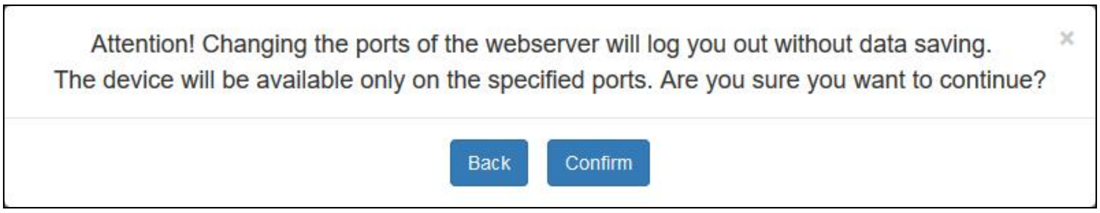
DNS server 1/2/3: The device's default DNS servers. The device resolves the domain names via these servers. If it is not set the device will use the Google DNS server (8.8.8.8) automatically.

Set configuration: The device tries to set the selected network settings. Changing the configuration will automatically log you out without data saving.

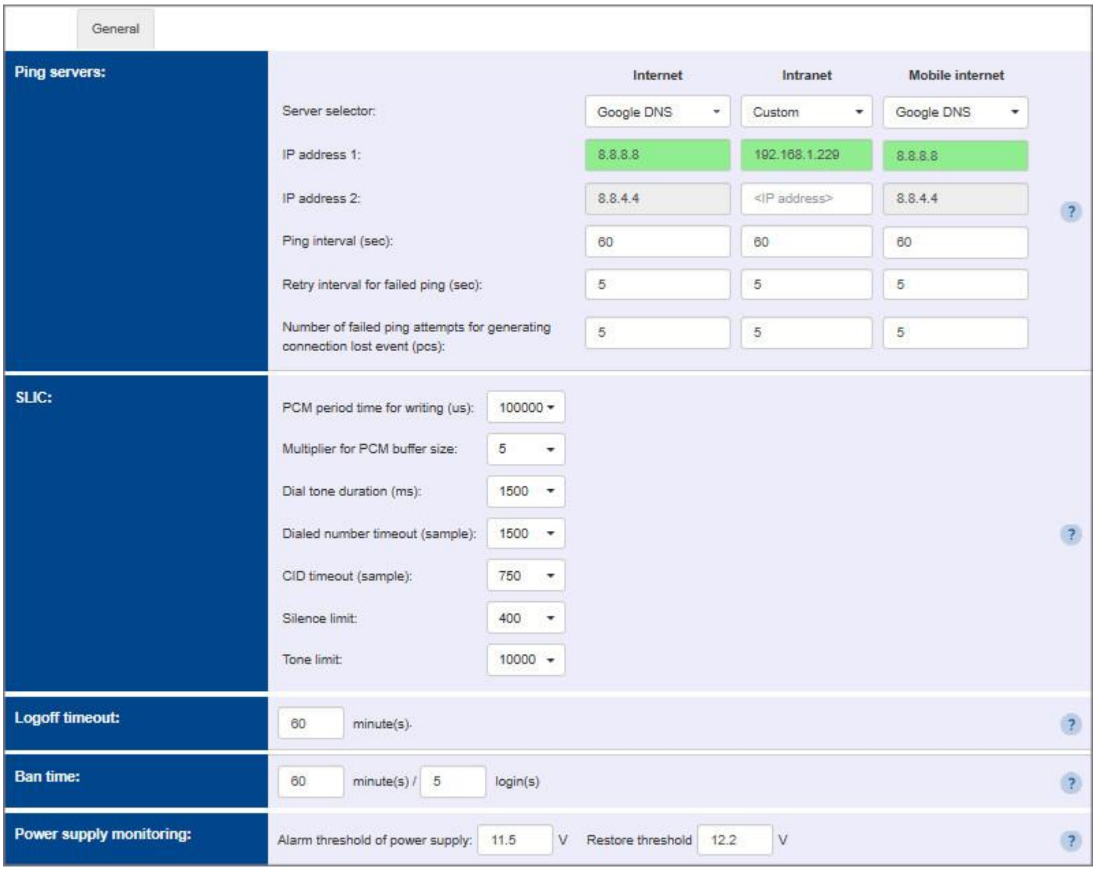

Attention! Changing the IPv4 host configuration will log you out without data saving.
In case of static configuration, the device is available at the specified IP address.
In case of DHCP configuration use the IP Bridge Virtual Client program to locate the device.
Are you sure you want to continue?

LAN IPv4 settings

Web server: The web server's HTTP and HTTPS ports can be set. Changing the ports of the webserver will log you aout without data saving.


Attention! Changing the ports of the webserver will log you out without data saving.
The device will be available only on the specified ports. Are you sure you want to continue?

Web server settings



Ping servers:

	Internet	Intranet	Mobile internet
Server selector:	Google DNS	Custom	Google DNS
IP address 1:	8.8.8.8	192.168.1.229	8.8.8.8
IP address 2:	8.8.4.4	<IP address>	8.8.4.4
Ping interval (sec):	60	60	60
Retry interval for failed ping (sec):	5	5	5
Number of failed ping attempts for generating connection lost event (pcs):	5	5	5

SLIC:

PCM period time for writing (us):	100000
Multiplier for PCM buffer size:	5
Dial tone duration (ms):	1500
Dialed number timeout (sample):	1500
CID timeout (sample):	750
Silence limit:	400
Tone limit:	10000

Logoff timeout: 60 minute(s).

Ban time: 60 minute(s) / 5 login(s)

Power supply monitoring: Alarm threshold of power supply: 11.5 V Restore threshold 12.2 V

General settings 3.

Ping servers: Ping servers can be set for checking internet and intranet. If the module has an extension panel, monitoring the mobile internet connection is also possible. Two IP addresses can be set for each network type.

Server selector: You can select predefined servers from the drop-down list, or you can also specify „Custom„ servers, in which case IP address 1 and 2 fields become editable.

Ping interval: sending frequency in seconds

Retry interval for failed ping: ping attempt frequency if ping failed

Number of failed ping attempts for generating connection lost event: After the specified number of failed ping and external event is generated about the failure.

SLIC: The parameters of the simulated phone line can be edited, if the device cannot or cannot safely recognize the CID signals of the connected alarm panel. ATTENTION! DO NOT CHANGE THE FACTORY DEFAULT VALUES UNLESS IT IS NECESSARY.

PCM period time for waiting/Multiplier for PCM buffer size: This related value pair influences the writing to the simulated phone line. The higher this value is, the more stable the writing is but also the slower the response towards the alarm central is. Because of the late acknowledgement the alarm central will repeat the CID events.

Dial tone duration: The module provides dial tone for the time set here. This value is related to the PCM sampling time.

Dialed number timeout: After the value specified here exits the reading and the value received so far will be the dialed phone number.

CID timeout: After the value specified here exits the reading and the signals received so far will be the CID codes.

Silence limit: This parameter can be used for noise reduction. The higher the silence limit, the better the noise reduction.

Tone limit: This parameter is suitable for filtering out the unwanted noises and the sounds of the device’s own writing. If the silence limit is modified, the tone limit also must be adjusted.

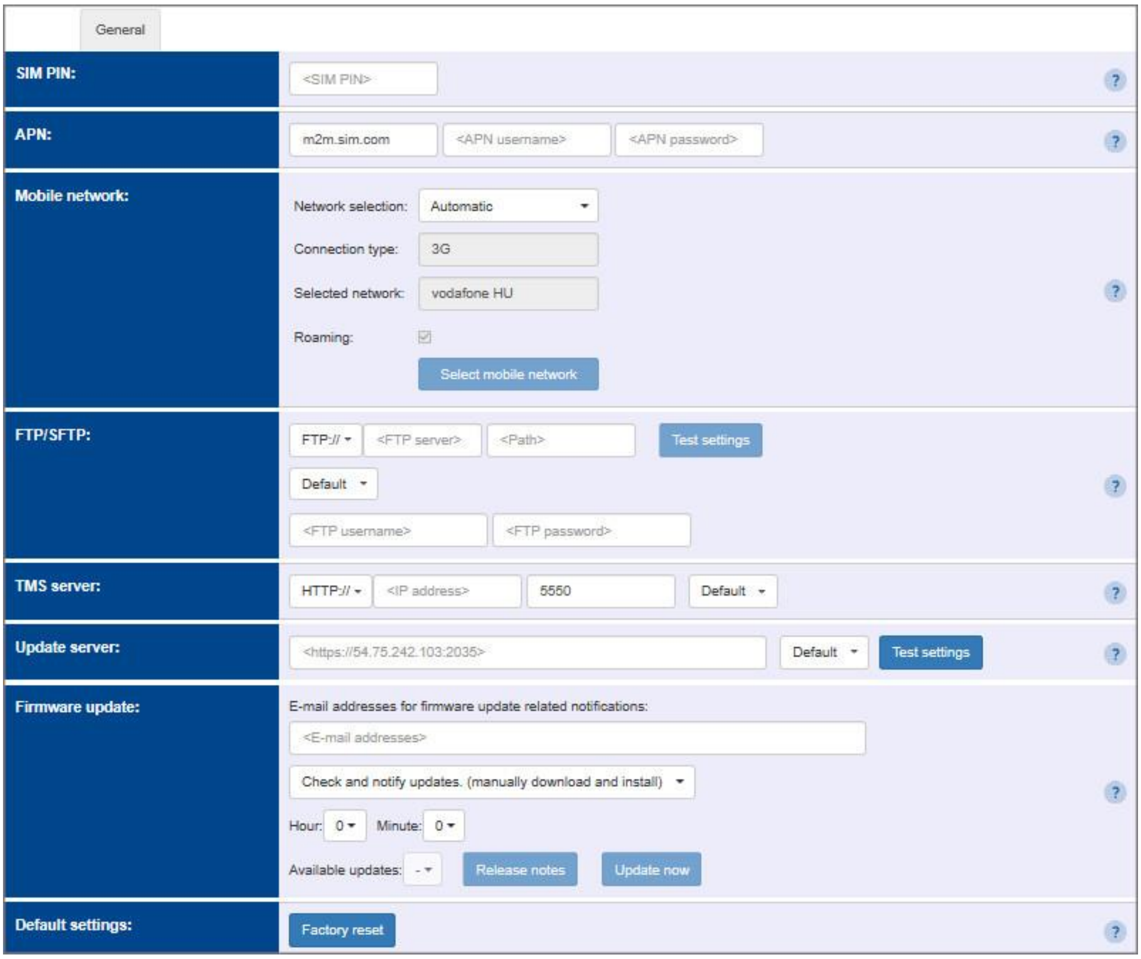
Logoff timeout: If there’s no activity for the time set here in minutes, the website will automatically log off.

Ban time: The user won't be able to login from an IP address for the time set here, if there was specified amount of failed login from the same IP address within the specified period of time. If 0 minute is set, the user won't be banned for failed login.

Battery: If the supply voltage falls below the alarm threshold and remains there for at least 30 seconds a „Battery fault" internal event is generated. If the supply voltage returns above the restore threshold and remains there for at least 30 seconds a „Battery restore" internal event is generated.

SIM PIN: If the module has an extension panel you can enter the SIM PIN here. If the SIM PIN is switched off, the module ignores the content of this field. The module tries a PIN code once if there are still 3 attempts. If there was a failed attempt before, a „Wrong SIM PIN" event is generated and you need to remove the SIM card from the module and unlock it by inserting it into a mobile phone and entering the correct PIN code.

APN: If the module has an extension panel, enter the Internet access point name (belongs to the SIM card, it is provided by the mobile service provider). In the case of a closed APN, the IP address of the servers must be authorized.



General

SIM PIN: <SIM PIN>

APN: m2m.sim.com <APN username> <APN password>

Mobile network:
Network selection: Automatic
Connection type: 3G
Selected network: vodafone HU
Roaming: ☑
Select mobile network

FTP/SFTP: FTP:// <FTP server> <Path> Test settings
Default
<FTP username> <FTP password>

TMS server: HTTP:// <IP address> 5550 Default

Update server: <https://54.75.242.103:2035> Default Test settings

Firmware update:
E-mail addresses for firmware update related notifications:
<E-mail addresses>
Check and notify updates. (manually download and install)
Hour: 0 Minute: 0
Available updates: - Release notes Update now

Default settings: Factory reset

General settings 4.

Mobile network: Network selection can be automatic, but you can also choose manual selection. In this case, in the Network selection field select the Manually option, then start the network searching with the Select mobile network button. After the network list is displayed, choose the provider and network type then push the Select mobile network button. These settings are available only for modules with extension panel.

FTP/SFTP: The module is able to upload the camera images captured during an alarm to an FTP server.

Select the protocol type from the dropdown list (FTP/SFTP)

Enter the IP address of the FTP Server and also the port number if necessary, separated by a colon (e.g.: 192.168.1.1:8181)

The path of the image folder can be also set.

The last 2 fields are for the username and password required for the connection.

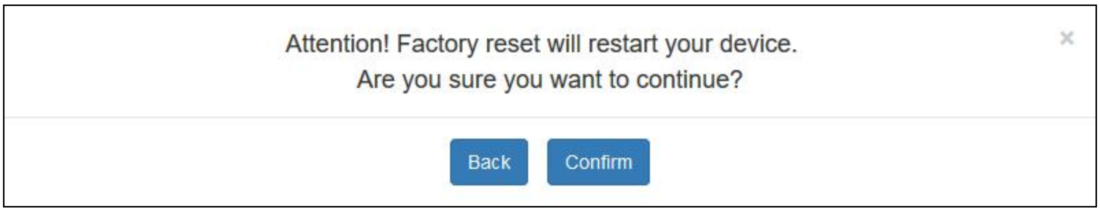
TMS server: The module is able to send not only the Contact ID code to the TMS user monitoring station but also the captured camera images and the live stream URL of the cameras. To set this enter the protocol, the server's IP address, the port number and select your network preferences. In case of an alarm, if the TMS is enabled for the event, the module automatically sends the necessary details to the TMS server set up here. If there's a camera assigned with the event, also the images captured by the camera will be sent to the TMS server.

Update server: If the Firmware update server is not set, in default the module downloads the firmware update from the server provided by the manufacturer.

Firmware update: To get a notification about the updates, enter your email address. You can select from the dropdown, whether you only want to get the notification about the update, or you also want the update to be automatically downloaded. And if so, you can also decide to allow downloading on mobile internet as well, or only on LAN. The time of update checking also can be edited. Select from the available updates and then you can get info about it with „Release notes" button or start the firmware update with „Update now" button.

⚠ **Attention!** The firmware of the device cannot be downgraded to an older version. Only versions that are newer than the current firmware are listed in the dropdown list.

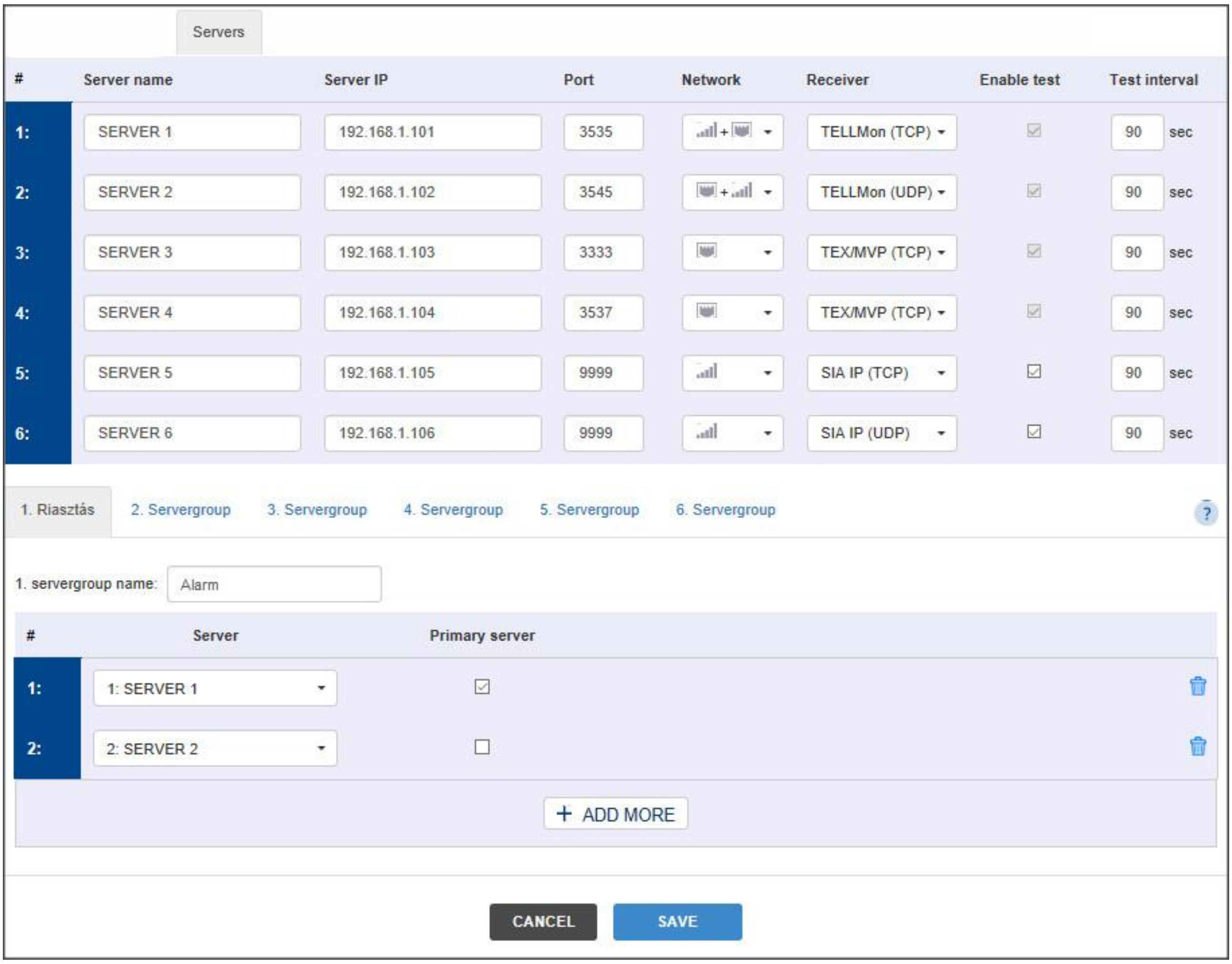
Default settings: The device settings will reset to the factory settings, but the current firmware version won't change.



Attention! Factory reset will restart your device.
Are you sure you want to continue?

Factory reset

6.3 Servers



Servers

#	Server name	Server IP	Port	Network	Receiver	Enable test	Test interval
1:	SERVER 1	192.168.1.101	3535	📶+🖧	TELLMon (TCP)	☑	90 sec
2:	SERVER 2	192.168.1.102	3545	🖧+📶	TELLMon (UDP)	☑	90 sec
3:	SERVER 3	192.168.1.103	3333	🖧	TEX/MVP (TCP)	☑	90 sec
4:	SERVER 4	192.168.1.104	3537	🖧	TEX/MVP (TCP)	☑	90 sec
5:	SERVER 5	192.168.1.105	9999	📶	SIA IP (TCP)	☑	90 sec
6:	SERVER 6	192.168.1.106	9999	📶	SIA IP (UDP)	☑	90 sec

1. servergroup name: Alarm

#	Server	Primary server
1:	1: SERVER 1	☑
2:	2: SERVER 2	□

Servers

In the Servers menu item (figure above) you can configure the data needed for the connection to remote monitoring servers. The module can send signals to 6 different servers simultaneously.

#: the index of the server

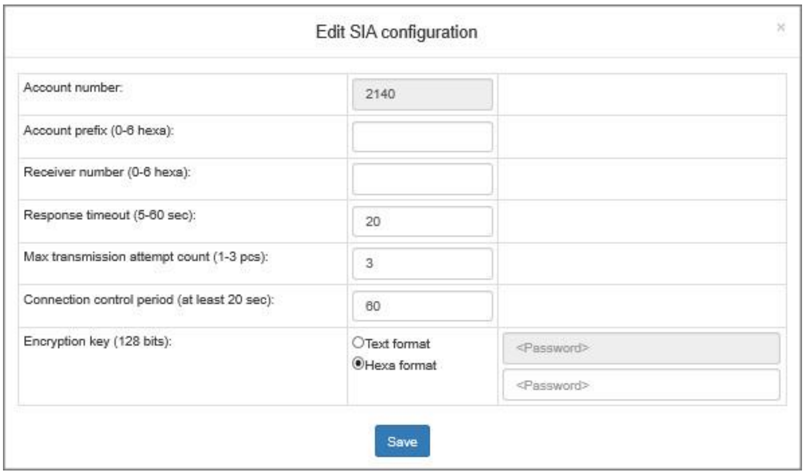
Server name: You can name the receiver

Server IP: The receiver's IP address or domain name

Port: Port number for the IP address

Network: Use the dropdown menu to set the communication channel for the device to access the remote monitoring receiver, and also select the backup communication channel. (If the module doesn't have an extension panel the only option is LAN and the selector is not displayed.)

Receiver: The receiver's type can be selected from the dropdown which also fills the port number with the default value. (If not the default port is used by the receiver, it can be manually updated). The selectable receiver types are: TEX/MVP (TCP), TELLMon (TCP), TELLMon (UDP), SIA IP (TCP), SIA IP (UDP). In case of a SIA IP receiver the configuration is editable.



Edit SIA configuration

Account number:	2140	
Account prefix (0-6 hexa):		
Receiver number (0-6 hexa):		
Response timeout (5-60 sec):	20	
Max transmission attempt count (1-3 pcs):	3	
Connection control period (at least 20 sec):	60	
Encryption key (128 bits):	○Text format ●Hexa format	<Password> <Password>

Edit SIA configuration

Edit SIA configuration:

Account number: This is the client's 1-6 characters long hexadecimal ID used for remote monitoring. It is only displayed here and can be edited on the General tab.

Account prefix (0-6 hexa): This up to 6 hexadecimal digits long prefix is optional. It depends on your remote monitoring company whether they use it or not.

Receiver number (0-6 hexa): Up to 6 hexadecimal digits to identify the receiver at the monitoring station. This is optional, it depends on your remote monitoring company whether they use it or not.

Response timeout (5-60 sec): This is the waiting time for a response between two sending attempts.

Max transmission attempt count (1-3 pcs): The number of attempts per data sending cycle.

Connection control period (at least 20sec): This is how much the device waits between two data sending cycles, that is, after the number of attempts specified in the "Max transmission attempt count" field.

Encryption key (128 bits): If the communication is encrypted, here you can enter the required 128-bit AES encryption key. The key can be entered in text format (up to 16 arbitrary characters) or in hexa format (up to 32 hexadecimal numbers).

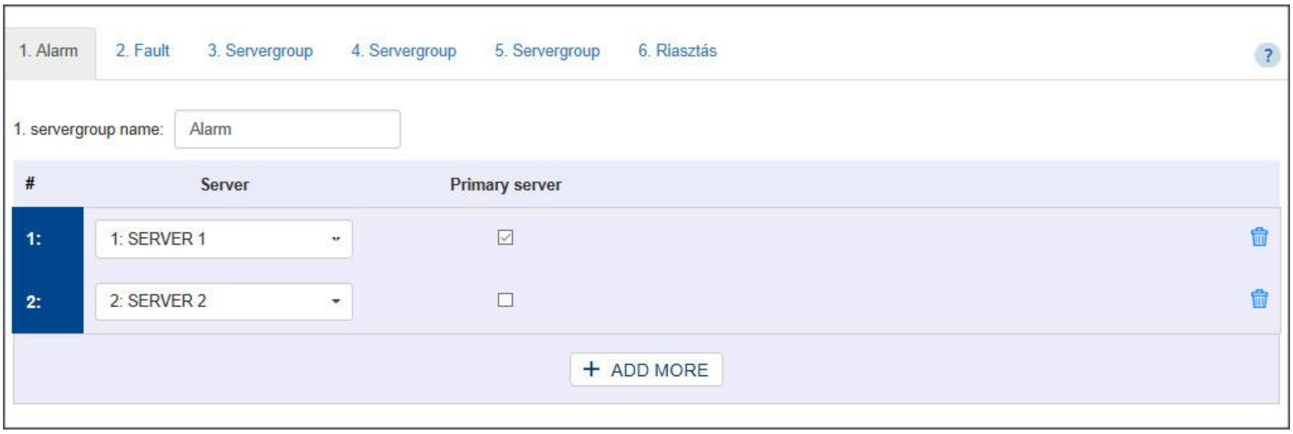
Enable test: Test report sending towards the given server can be enabled or disabled.

Test interval: Test report sending frequency in seconds. The module sends test report with the frequency set here to check the connection with the receiver at the given IP address.

Attention! Make sure you do not specify the same server with external and local IP as well, because in this case the transmission will not work properly.

Configuration example

From the servers up to 6 server groups can be created, which can be assigned with events later. By creating groups, you can separate alarm events from technical events for example. In each server group you can set which servers are primary and which are backup.



1. servergroup name: Alarm

#	Server	Primary server
1:	1: SERVER 1	☑
2:	2: SERVER 2	□

Server groups

Servergroup name: You can give a name to each server group. (e.g..: Alarm, Technical issues)

#: Index number within the group

Server: You can assign a server to a group by selecting it from the dropdown menu.

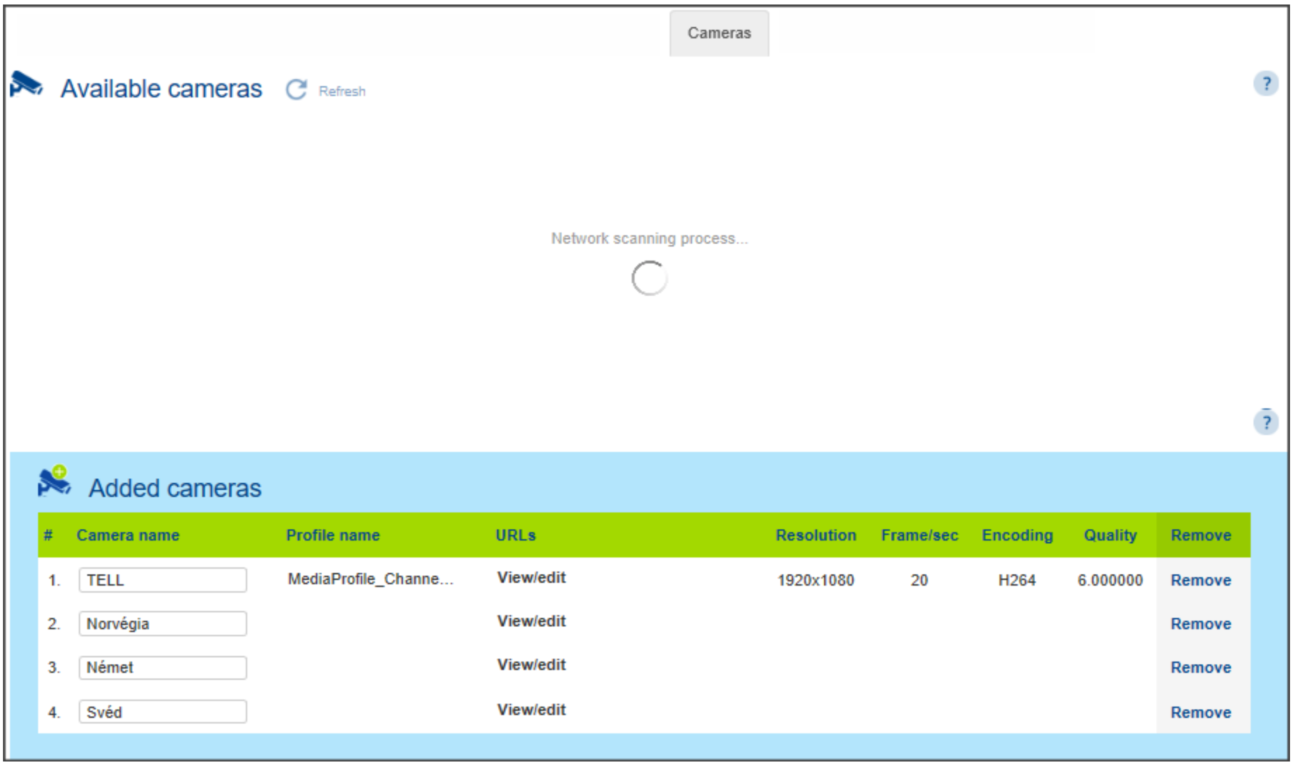
Primary server: Set with the checkbox which server is primary and which is backup. There can be more than one primary server. The signal will be sent simultaneously to each of them. The signal will be sent to the backup servers only if none of the primary servers were available. If there are multiple backup servers, the module sends the signal to them in order.

+ ADD MORE

Add server: You can add server to a group by selecting the servergroup and pressing the „ADD MORE" button at the bottom of Servers page.

Delete server: Use the dust bin icon next to the server to delete it from the group.

6.4 Cameras



Cameras

Available cameras Refresh

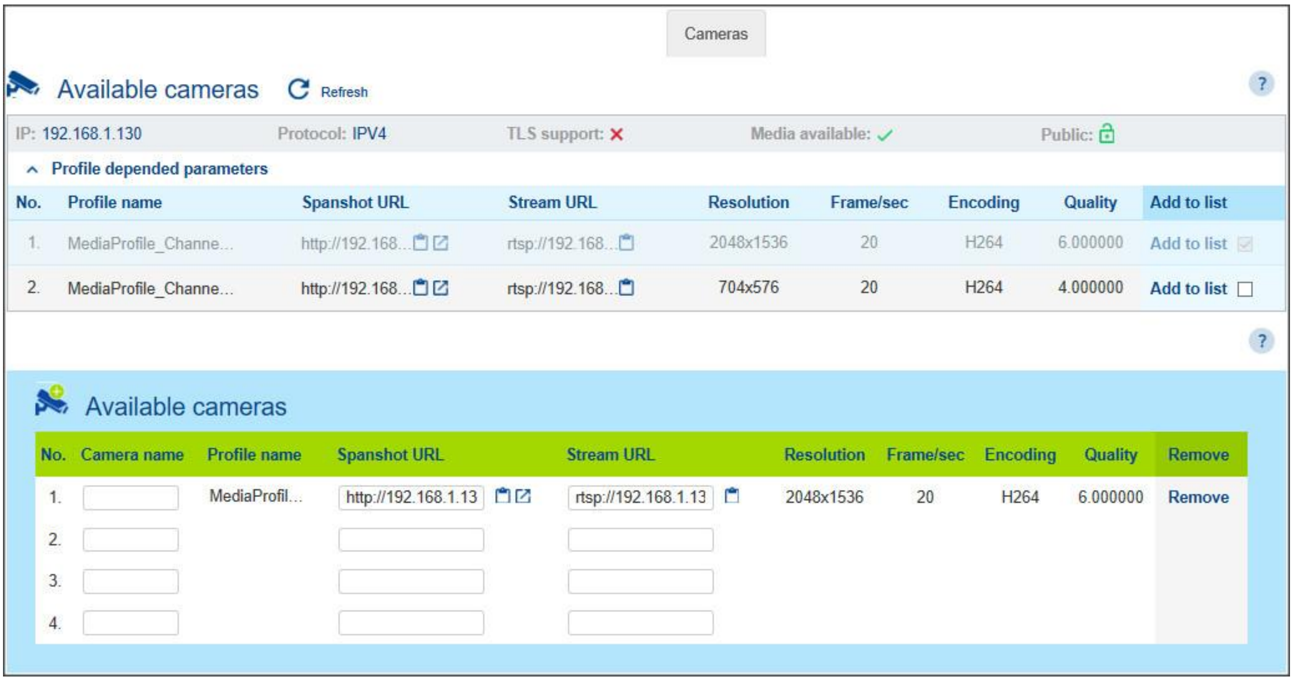
Network scanning process...

Added cameras

#	Camera name	Profile name	URLs	Resolution	Frame/sec	Encoding	Quality	Remove
1.	TELL	MediaProfile_Channe...	View/edit	1920x1080	20	H264	6.000000	Remove
2.	Norvégia		View/edit					Remove
3.	Német		View/edit					Remove
4.	Svéd		View/edit					Remove

Cameras

After you first turn on the device or restore the factory settings, you need to accept the privacy policy to access this feature. By clicking the Cameras menu, IP Bridge automatically finds and lists IP cameras that support the ONVIF recommendation and are connected to the same network (figure above).



Cameras

Available cameras Refresh

IP: 192.168.1.130 Protocol: IPV4 TLS support: ✗ Media available: ✓ Public: 🔓

Profile depended parameters

No.	Profile name	Spanshot URL	Stream URL	Resolution	Frame/sec	Encoding	Quality	Add to list
1.	MediaProfile_Channe...	http://192.168...	rtsp://192.168...	2048x1536	20	H264	6.000000	Add to list ☑
2.	MediaProfile_Channe...	http://192.168...	rtsp://192.168...	704x576	20	H264	4.000000	Add to list □

Available cameras

No.	Camera name	Profile name	Spanshot URL	Stream URL	Resolution	Frame/sec	Encoding	Quality	Remove
1.		MediaProfil...	http://192.168.1.13	rtsp://192.168.1.13	2048x1536	20	H264	6.000000	Remove
2.									
3.									
4.									

IP Camera settings

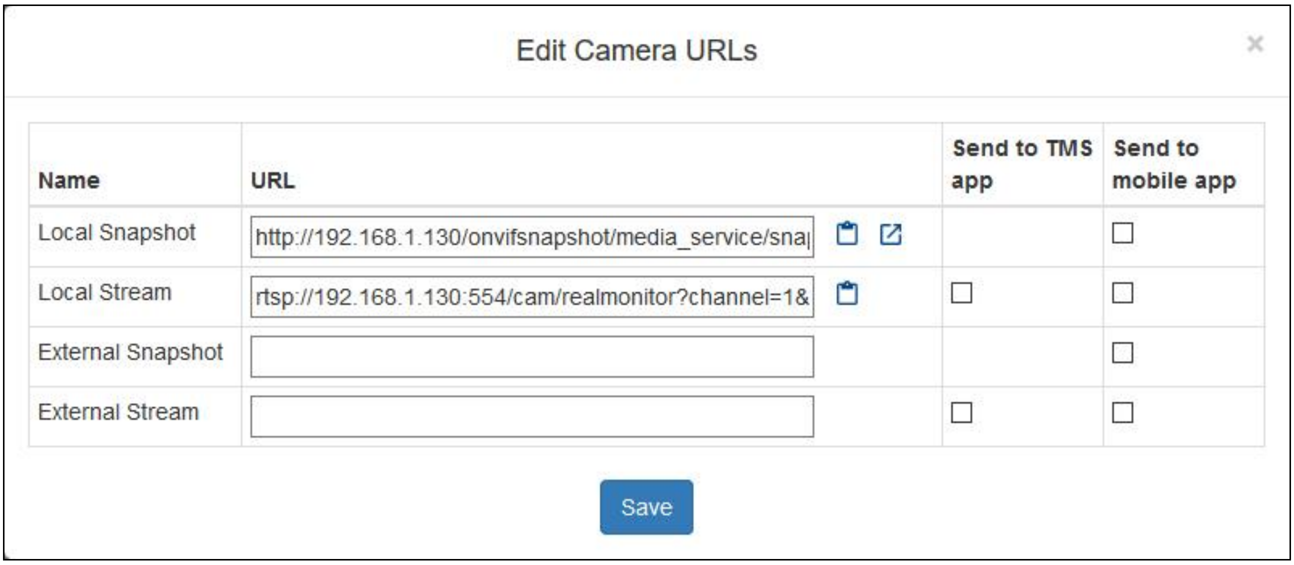
Clicking the „Profile dependent parameters” IP Bridge lists the profiles that are set in the camera (figure above). Usually, the difference between these profiles is the resolution.

The links of the found profiles (both the Snapshot URL and Stream URL) can be copied and tested.

Pressing this button displays in a popup window a snapshot of the camera using the profile settings. This makes easier to identify and select the profile.

If the IP camera doesn’t have the password-free connection enabled, IP Bridge can’t automatically sign in to get the configured profiles. In this case, the „Profile dependent parameters” button allows you to enter the username, password and the ONVIF port on which the IP Bridge can communicate with the camera.

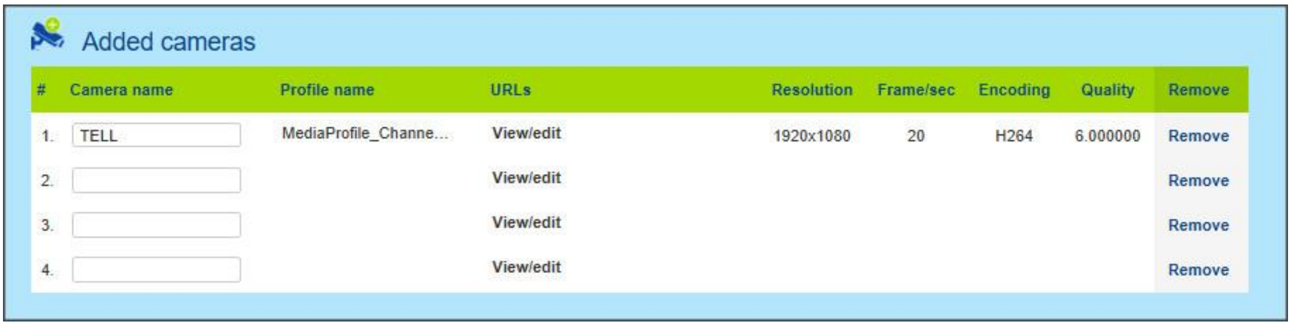
The „Add to list” button adds the given camera to the camera list of the IP Bridge and fills the required parameters (figure below). When you press this button, a popup window appears where you can edit the existing URL, manually add a new camera URL, or display the images of those cameras that you already added. You can also set up a URL to be sent to the TMS application and the mobile app. When you are auto-filling, you can enter a unique name for the camera which will be displayed in the Events menu item. Up to 4 cameras can be added to the device.



Edit Camera URLs

Name	URL	Send to TMS app	Send to mobile app
Local Snapshot	http://192.168.1.130/onvifsnapshot/media_service/sna|		□
Local Stream	rtsp://192.168.1.130:554/cam/realmonitor?channel=1&	□	□
External Snapshot			□
External Stream		□	□

Edit Camera URLs



Added cameras

#	Camera name	Profile name	URLs	Resolution	Frame/sec	Encoding	Quality	Remove
1.	TELL	MediaProfile_Channe...	View/edit	1920x1080	20	H264	6.000000	Remove
2.			View/edit					Remove
3.			View/edit					Remove
4.			View/edit					Remove

ONVIF IP camera URL

To edit the URL click the **“View/Edit”** button. This opens the same pop-up window (figure above) that appears when you add a new camera to the list.

Local Snapshot and Stream URL:

The module saves snapshots of configured IP cameras, so if an event occurs, it sends these saved images as attachments by email, uploads it to an FTP server, or sends it to the TMS system.

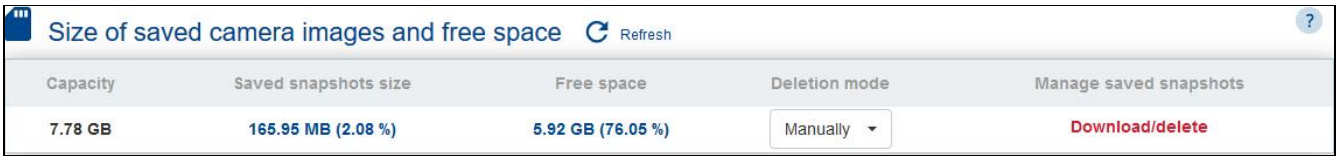
External Snapshot and Stream URL:

The module is able not only to store the images, but also to send the camera links in a Push message for the smartphone application. So in case of an event, even the live image can be viewed in the application. In this case, you need add your camera with its external link.

⚠ **Attention!** Depending on the camera resolution, the SD card may be full after 5-10 thousand events for which camera recording is required. In this case, the device can not store additional camera images until the previously recorded images are deleted. You can do this in the Cameras menu.

Managed saved snapshots:

The module stores the camera images recorded during the events on the SD card. This menu item provides information about the total size of the saved images (figure below) The images can be archived, downloaded or permanently deleted from the module.



Size of saved camera images and free space

Capacity	Saved snapshots size	Free space	Deletion mode	Manage saved snapshots
7.78 GB	165.95 MB (2.08 %)	5.92 GB (76.05 %)	Manually	Download/delete

Saved camera images

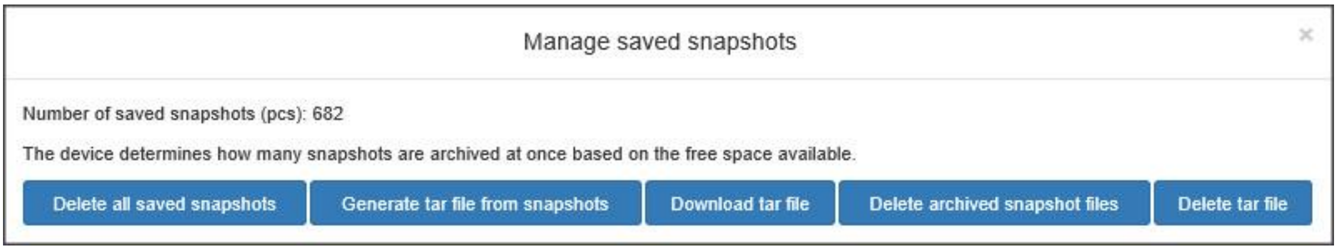
Capacity: Size of the SD card inserted into the module

Saved snapshots' size: The size of the saved images in MB and the percentage of the used space.

Free space: The free space on the SD card in MB and in percent.

Deletion mode: You can specify the storage time for the camera images (10 minutes, 3 days, manual)

Manage saved snapshots: The images can be deleted, archived or downloaded here. These buttons open a popup window.



Manage saved snapshots

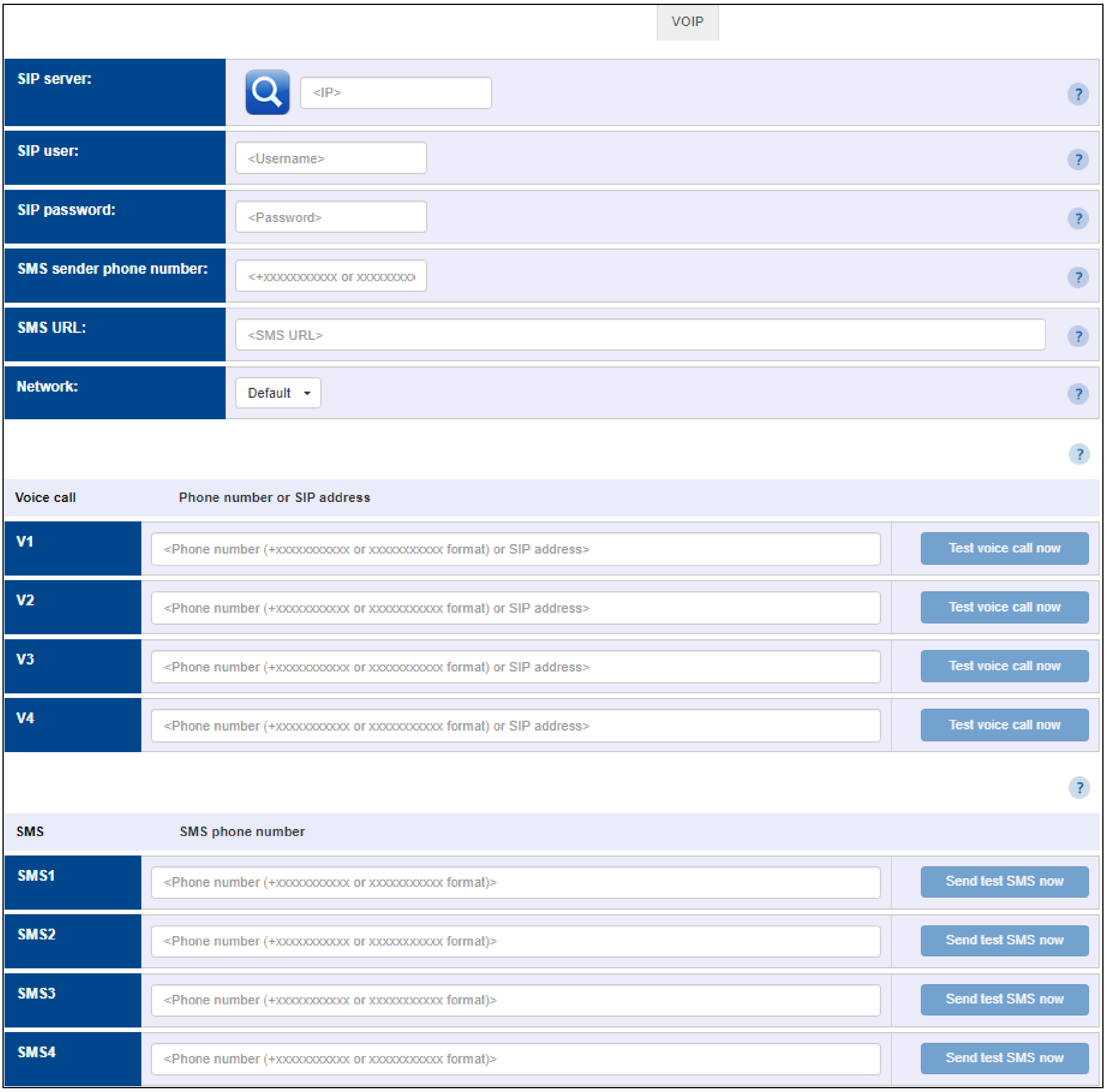
Number of saved snapshots (pcs): 682

The device determines how many snapshots are archived at once based on the free space available.

×
Delete all saved snapshots
Generate tar file from snapshots
Download tar file
Delete archived snapshot files
Delete tar file

Manage saved snapshots

6.5 VOIP



VOIP

SIP server:	<IP>
SIP user:	<Username>
SIP password:	<Password>
SMS sender phone number:	<+xxxxxxxxxxx or xxxxxxxxx
SMS URL:	<SMS URL>
Network:	Default

Voice call	Phone number or SIP address	
V1	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format) or SIP address>	Test voice call now
V2	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format) or SIP address>	Test voice call now
V3	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format) or SIP address>	Test voice call now
V4	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format) or SIP address>	Test voice call now

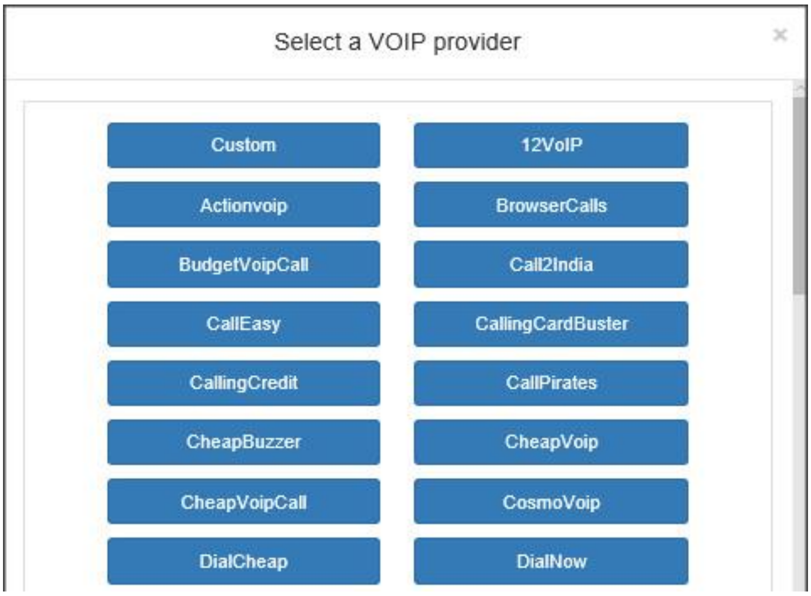
SMS	SMS phone number	
SMS1	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format)>	Send test SMS now
SMS2	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format)>	Send test SMS now
SMS3	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format)>	Send test SMS now
SMS4	<Phone number (+xxxxxxxxxxx or xxxxxxxxxxx format)>	Send test SMS now

Setting VOIP phone numbers

The device can report events to the configured **V1**…**V4**, and **SMS1**…**SMS4** phone numbers via voice call and SMS, using VoIP service through the Internet. For VoIP based notification it is necessary to register a user account at a VoIP service provider, and top-up your account balance as needed. After that, configure the service provider's SIP server IP address, the registered username and password, and the phone numbers to be notified, in the device settings.

The magnifier icon opens a popup window (see the figure below), where you can select your VoIP service provider.

Attention! The VoIP service in the device cannot be used to make transparent voice calls via the simulated telephone line output!
The device implements the SIP protocol using the PJSIP multimedia library. Please make sure that PJSIP supports the SIP provider you want to use.



VoIP providers

By selecting the service provider, the device automatically fills out all necessary information, you just need to add the username, password and SMS sender phonenumber.

If you can't find your provider in the list, select the 'Custom' option. In this case you need to add manually all the details.

SIP server: The SIP server's IP address.

SIP user: The username that belongs to your VoIP subscription.

SIP password: The password that belongs to your VoIP subscription.

SMS sender: This phone number will be displayed as SMS sender.

SMS URL: The provider's SMS URL

Voice call V1-V4: 4 phone numbers can be added, which (according to the event settings) can be reached via voice call if an event occurs.

Phone number or SIP address: In this field, you can set the phone number or SIP address for internet call. If the SIP server is set up and the account has credit, so it is topped up with money, the module can call phone numbers as well, else it can start only internet call and in this case only the SIP address is needed.

SMS 1-4: 4 phone numbers can be added. The preset SMS messages can be sent to these numbers if an event occurs (according to the event settings).

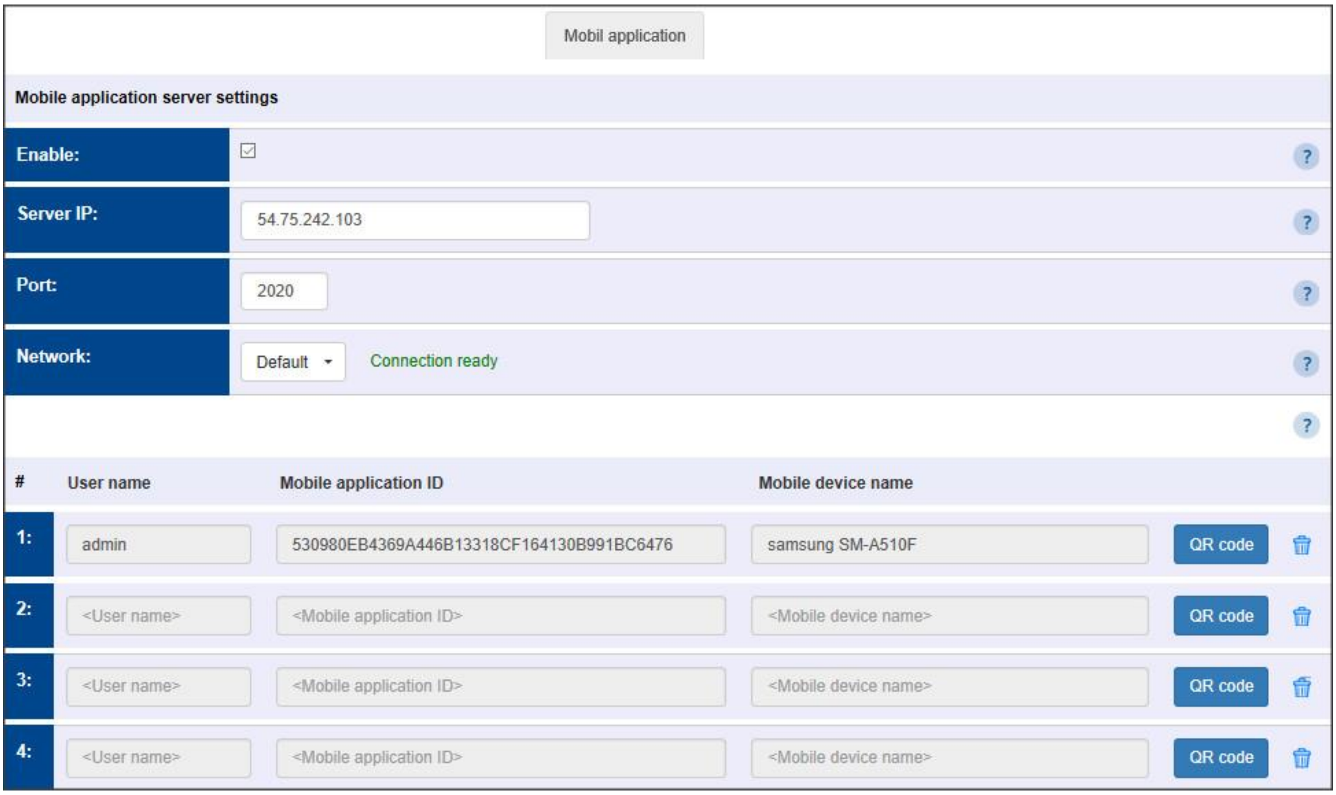
Test voice call now: If a SIP account is set, you can start a test voice call to the given number.

Send Test SMS now: If a SIP account is set, you can send test SMS to the given number.

Note:

Voice over Internet Protocol – commonly known as VoIP, Voice over IP or IP telephony – is a methodology and group of technologies for the delivery of voice communications over Internet Protocol (IP) networks, such as the Internet. Since the IP network doesn't guarantee that data packets are not lost, are delivered in sequential order or any other Quality of Service (QoS) criteria, VoIP implementations may face problems like the data packets' basic delay and the delay resultant from packet reordering and also data loss. The basic data delay depends on the distance of the partners within the network, the route of packets and the load on the network. The reordering of data packets depends on the VoIP service provider too. If you are experiencing bad voice quality during the call, it is advisable to try a voice call with a different VoIP service provider.

6.6 Mobile application



Mobil application

Mobile application server settings

Enable: ☑

Server IP: 54.75.242.103

Port: 2020

Network: Default ▾ Connection ready

#	User name	Mobile application ID	Mobile device name		
1:	admin	530980EB4369A446B13318CF164130B991BC6476	samsung SM-A510F	QR code	🗑
2:	<User name>	<Mobile application ID>	<Mobile device name>	QR code	🗑
3:	<User name>	<Mobile application ID>	<Mobile device name>	QR code	🗑
4:	<User name>	<Mobile application ID>	<Mobile device name>	QR code	🗑

Mobile application settings

In the „Mobile application” menu item you can set the server data required for Push message sending and also the devices that can be assigned with the module.

Enable: this service can be enabled/disabled here.

In default the server setting fields are filled with the data of manufacturer's server reserved for this purpose, which are the followings:

Server IP: 54.75.242.103

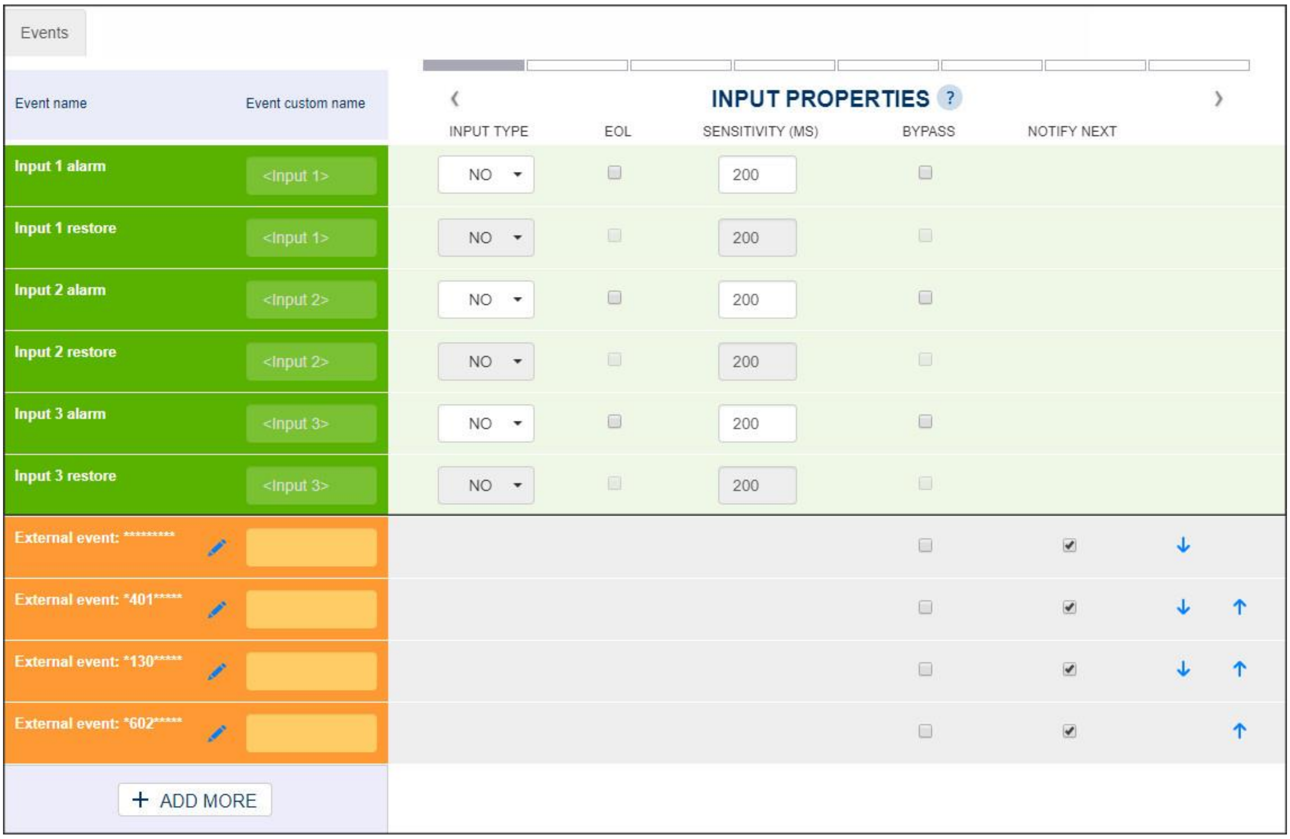
Port: 2020

Network: The drop-down menu allows you to set the communication channel for the device to access the server and whether it has a backup communication channel. (If the module doesn’t have an extension panel the only option is LAN and the selector is not displayed.)

⟳ When adding an application, clicking the update button displays application data.

4 mobile devices can be registered for the module. Each slot has a uniqe identifier that can be displayed by clicking the QR code button at the end of the line. In the mobile application you can register a device into the module by scanning the QR code of the given slot. After the registration the mobile application’s ID and the mobile device’s name are listed here.

6.7 Event settings



Events

‹ INPUT PROPERTIES ? ›

Event name	Event custom name	INPUT TYPE	EOL	SENSITIVITY (MS)	BYPASS	NOTIFY NEXT		
Input 1 alarm	<Input 1>	NO	□	200	□			
Input 1 restore	<Input 1>	NO	□	200	□			
Input 2 alarm	<Input 2>	NO	□	200	□			
Input 2 restore	<Input 2>	NO	□	200	□			
Input 3 alarm	<Input 3>	NO	□	200	□			
Input 3 restore	<Input 3>	NO	□	200	□			
External event: *********					□	☑	↓	
External event: *401*****					□	☑	↓	↑
External event: *130*****					□	☑	↓	↑
External event: *602*****					□	☑		↑

+ ADD MORE

Event settings

The module internal and external events can be configured on the **Events** tab of **Settings** menu item.

Event name:

IN1… IN6 alarm: new alarm events generated by external contact on input IN1… IN6 according to the (NO/NC) input settings (alarms)

Sabotage alarm/ Sabotage restore: The sabotage (tamper) setting is applied to each input specified with EOL option. The module will automatically enter the number of the violated zone (001...006) into the zone section of Contact ID code. The module does not send tamper signals from non-EOL inputs.

Battery fault/ Battery restore: The module has a power monitoring function. A battery fault event is generated if the supply voltage drops below 11.5V (or 23.0V) for at least 30 seconds. A battery restore event is generated if the module’s supply voltage restores above 12.4V (or 24.4V) for at least 30 seconds. The thresholds are configurable in the settings.

The following two internal events are generated depending on the settings. If there’s no Ping server set under the **Settings** tab, regarding both the internet and intranet the connection lost and connection restore events are generated when the IP Bridge gets an IP address on the network it is connected to. In this case the connection lost or connection restore events are generated simultaneously for both the intranet and internet. If Ping servers are configured to monitor the internet and intranet, the events are generated according to whether or not the module has accessed server.

Internet connection lost / Internet connection restore: The connection lost event is generated when the module is unable to connect to the network or if a Ping server is set up to monitor the internet but it can’t be accessed. The restore event is generated when the module successfully connects to the network or it is able to access the Ping server. If the connection error takes more than 10 minutes the notification time of the error event expires, and only the restore event will be transmitted, but the module’s event log will list the error event as well.

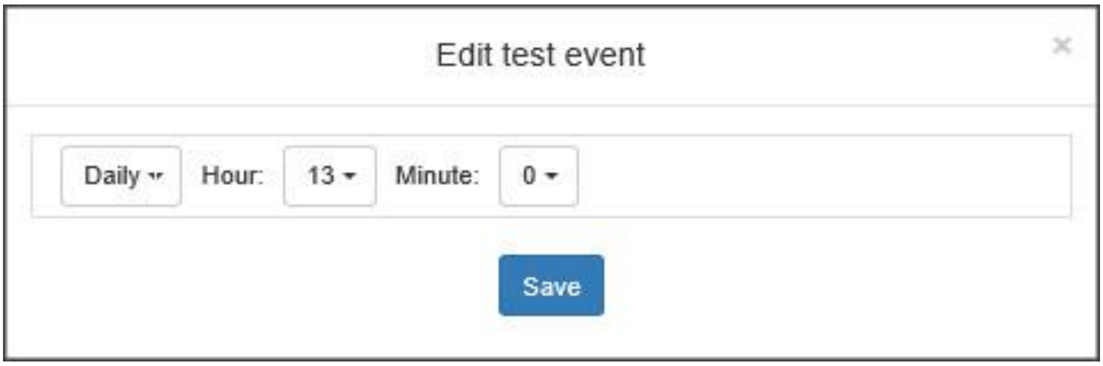
Intranet connection lost / Intranet connection restore: The connection lost event is generated when the module is unable to connect to the network or if a Ping server is set up to monitor the intranet, but it can't be accessed. The restore event is generated when the module successfully connects to the network or it is able to access the Ping server. If the connection error takes more than 10 minutes the notification time of the error event expires, and only the restore event will be transmitted, but the module's event log will list the error event as well.

Router warm restart: The module is able to warm restart certain type of routers on the same network the IP Bridge is connected to (see Router control menu item). This event is generated when there's no response to the ping set on the Router control tab and the module restarts the router.

Router cold restart: The module is able to warm and cold restart certain type of routers on the same network the IP Bridge is connected to (see Router control menu item). This event is generated if the warm restart set on the Router control tab wasn't successful and the module cold restarts the router.

Periodic test: The module is able to send periodic test reports towards the monitoring station.

The pencil icon next to the name opens a popup window (see figure below) where you can set the time of sending periodic test report.



Edit test event

Daily

Hour: 13

Minute: 0

Periodic test report

FTP backup failed: The module can upload the images from the cameras assigned with it to an FTP server, which can be set on the General tab of Settings (FTP/SFTP section). This event is generated when the module was unable to upload the images.

Not enough space: This event is generated when only 200 MB free space remains to store the images. If the size of the images has reached the maximum, the module will not delete images and will not record new images if an event occurs.

Settings changed: This internal event is generated when the settings are changed.

Mobil connection lost / Mobil connection restore: The connection lost event is generated when the module has 3G / 4G extenstion module, but it is unable to connect the mobile internet or if a Ping server is set to monitor the mobile network, but it can't be accessed. The restore event is generated when the module successfully connects to the network or it is able to access the Ping server. If the connection error takes more than 10 minutes the notification time of the error event expires, and only the restore event will be transmitted, but the module's event log will list the error event as well.

Only 2G network available: This event is generated when the device has a 3G/4G module, but 3G/4G network is unavailable at the location, so it can only connect to the 2G network. In this case the camera snapshot sending won't work, even if this option is enabled on the General tab.

3G/4G network available: This event is generated when the device has a 3G/4G module and the 3G/4G mobile network is available at the location.

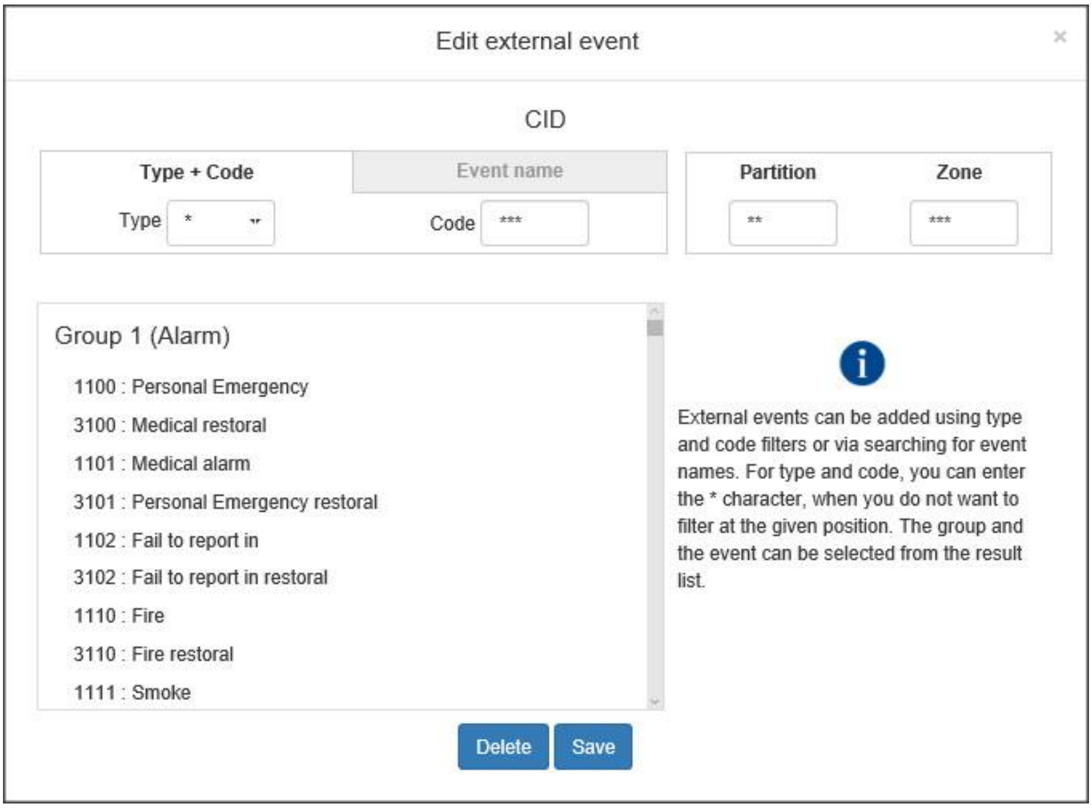
SIM card removed: This event is generated when the device has a 3G/4G module and the SIM card is removed from the module.

SIM card changed: This event is generated when the device has a 3G/4G module and the SIM card is replaced with another one. The module stores the last SIM ID and when a new card is inserted it compares its SIM ID with the stored value and if those are different this internal event is generated.

Wrong SIM PIN: This event is generated if the device has a 3G/4G module and PIN code is required to unlock the SIM card, but the PIN code set on the General tab is wrong. The module tries a PIN code once if there are still 3 attempts. If there was a failed attempt before a „Wrong SIM PIN" event is generated and you need to remove the SIM card from the module and unlock it by inserting in mobile phone and entering the correct PIN code.

External event: You can also set up to 20 external events in the module, which are Contact ID events received on the simulated phone line. The event codes expected from the alarm center can be added to the event list and for each code you can set the notification scheme based on which the module needs to report to a monitoring station, send email, send SMS, etc.

You can add external events with the „Add more" button at the bottom of the Events page. The button opens a popup window (see figure below).


Edit external event

CID

Type + Code	Event name	Partition	Zone
Type * Code ***		**	***

Group 1 (Alarm)

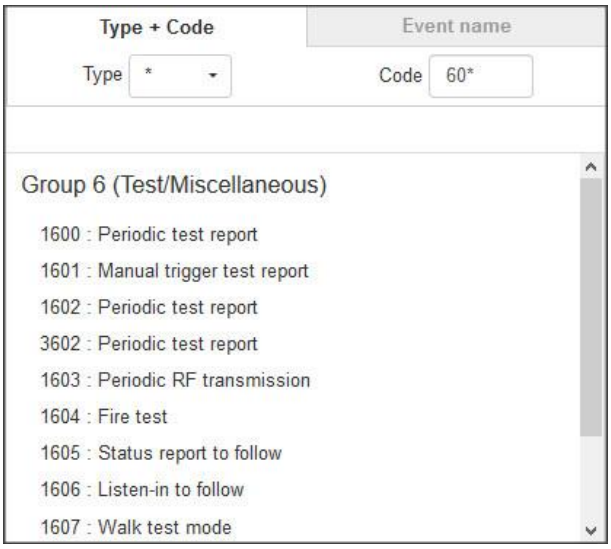
- 1100 : Personal Emergency
- 3100 : Medical restoral
- 1101 : Medical alarm
- 3101 : Personal Emergency restoral
- 1102 : Fail to report in
- 3102 : Fail to report in restoral
- 1110 : Fire
- 3110 : Fire restoral
- 1111 : Smoke

External events can be added using type and code filters or via searching for event names. For type and code, you can enter the * character, when you do not want to filter at the given position. The group and the event can be selected from the result list.

External event

When entering the event code, partition and zone, it is also possible to define an event group by using the „*" character. If any hexadecimal digit is received from the alarm center instead of „*", but the rest of the code is the same as the one you entered, the given event will be reported. The module compares the event received from the alarm center with the external events recorded in the table, and if there's a match, reports the received event according to the settings of the event found. The module checks the event by type, then by event code and finally by partition and zone number. When adding an external event, it is possible to add all the Contact ID codes, which is the default setting. In this case * must be left in each field and all the CID codes received on the simulated phone line will be transmitted according to the settings.

When adding an event you can select the event code from the predefined list. There are several options to filter event codes (figure below):



Type + Code | Event name

Type * Code 60*

Group 6 (Test/Miscellaneous)

1600 : Periodic test report
1601 : Manual trigger test report
1602 : Periodic test report
3602 : Periodic test report
1603 : Periodic RF transmission
1604 : Fire test
1605 : Status report to follow
1606 : Listen-in to follow
1607 : Walk test mode

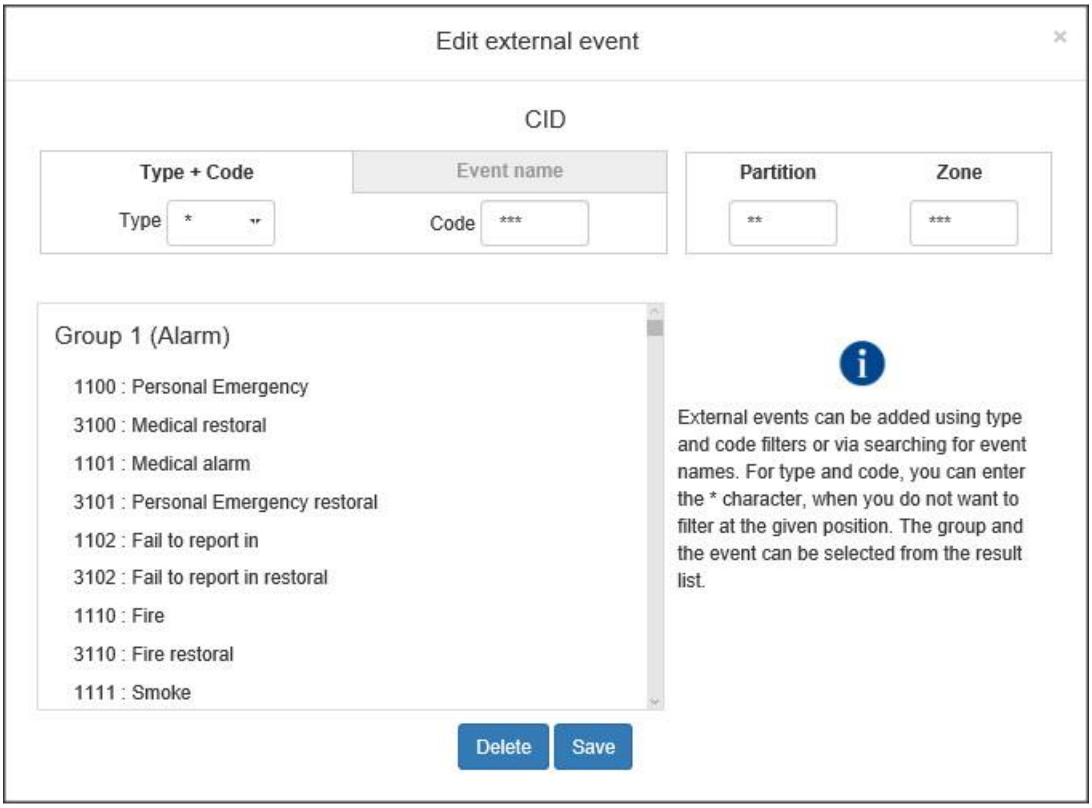
Filtering external events

Type: From the dropdown you can select New event (1), Restore (3) or Any (*).

Code: When you enter the 3 digits long CID code the result list is displayed. The „*" character can be used also here.

Event name: The event list can be filtered also by the event name. You don't need to add the full name, the list is automatically filtered when you type.

You can delete an external event you have added by clicking the edit button next to the event. The pop-up window appears (see figure below) and you can find the delete button next to the save button.



Edit external event

CID

Type + Code | Event name | Partition | Zone

Type * Code *** Partition ** Zone ***

Group 1 (Alarm)

1100 : Personal Emergency
3100 : Medical restoral
1101 : Medical alarm
3101 : Personal Emergency restoral
1102 : Fail to report in
3102 : Fail to report in restoral
1110 : Fire
3110 : Fire restoral
1111 : Smoke

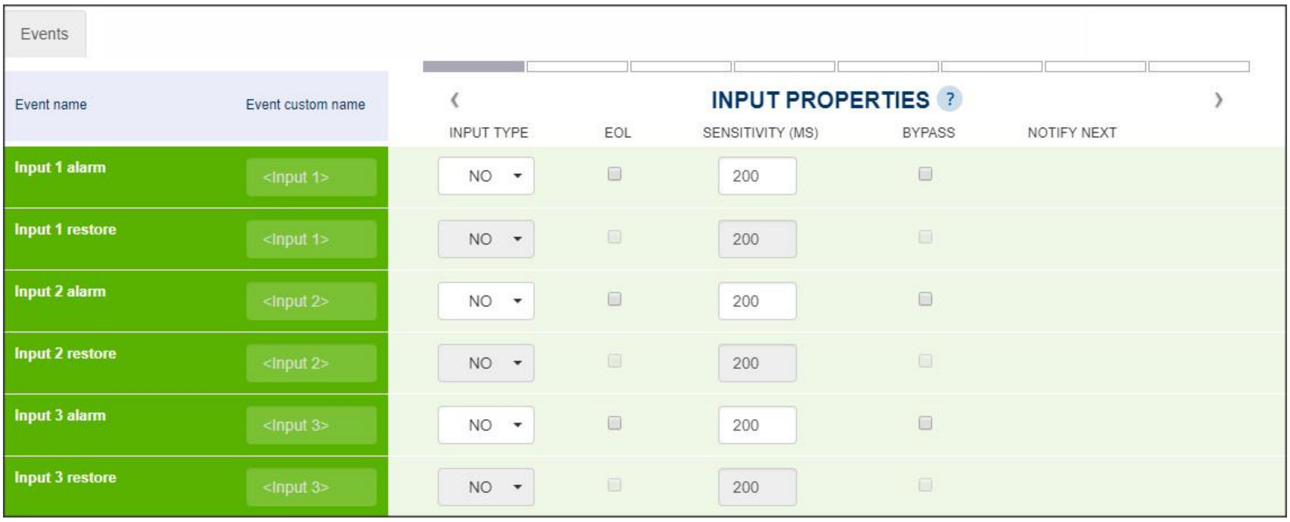
External events can be added using type and code filters or via searching for event names. For type and code, you can enter the * character, when you do not want to filter at the given position. The group and the event can be selected from the result list.

Delete/edit external event

Event custom name: Both the internal and external events can have a custom name, which is displayed in the event log, email report and also on the Status page. The default name will be used if the event doesn't have a custom name. The module automatically uses the default meaning of their CID codes.

There are several setting options for events, that can be found on the **Events** tab. All settings are grouped, and you can switch between them by arrows. The settings are the followings:

Input properties:



Event name	Event custom name	INPUT TYPE	EOL	SENSITIVITY (MS)	BYPASS	NOTIFY NEXT
Input 1 alarm	<Input 1>	NO	□	200	□	
Input 1 restore	<Input 1>	NO	□	200	□	
Input 2 alarm	<Input 2>	NO	□	200	□	
Input 2 restore	<Input 2>	NO	□	200	□	
Input 3 alarm	<Input 3>	NO	□	200	□	
Input 3 restore	<Input 3>	NO	□	200	□	

Input properties

Input type: select the default state of the input

- **NO**: normally open (To generate an alarm event the „Z1… Z6" input has to be shorted to the „COM" common terminal. The restore event is generated when opening this contact.)
- **NC**: normally closed (The „Z1… Z6" input has to be shorted to „COM" common terminal by default. Alarm event is generated when opening this contact. Alarm event is generated when the input is shorted to „COM" again.)

EOL: if enabled, tamper protection function is automatically activated for the given input. In this case the given input must be provided with a 1kΩ end-of-line resistor at the end of the loop, directly at the controlling contact

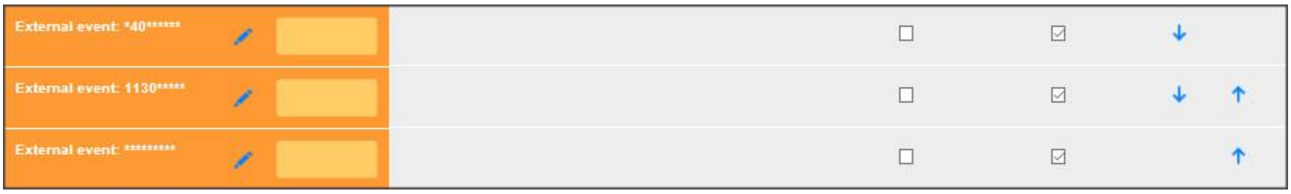
Sensitivity: The status change of the given zone input is ignored if it is shorter than the value set here. Unit of measure: millisecond (10… 99999)

Bypass: Both the internal and external events can be eliminated one by one if it is not needed or a failure has occured.

Notifiy next: If the CID codes of multiple external events are overlapping each other but you want to send notification about all of them independently, by selecting this checkbox the next event will be generated even if the CID code corresponds to this event.

<u>Configuration example:</u>

> We'd like to receive notification about open, close and bulglary events while we want all signals to be sent to the monitoring station (see figure below) as well. If we check bypass option and an open or close event is coming from the alarm system, the module communicates the first event (e.g: email notification with camera image and SMS sending) and also checks the next event code. If it doesn't fit, the module checks the next one. If it fits, the module executes the necessary actions. The module continues this as long as there's another external event or the „notify next" option is not checked.

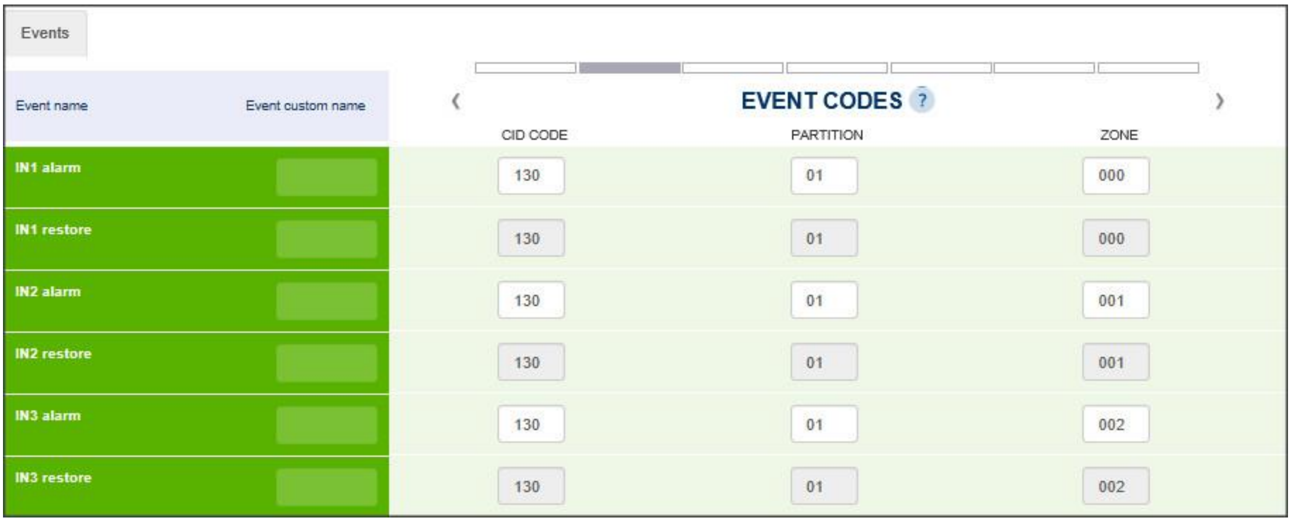


External event: *40******		□	☑	↓	
External event: 1130*****		□	☑	↓	↑
External event: *********		□	☑		↑

Adding multiple external events

↓↑ Use the arrows to modify the sort order of CID codes. The module always begins to evaluate the CID code filtering in the given order.

Event codes:



Events

EVENT CODES ?

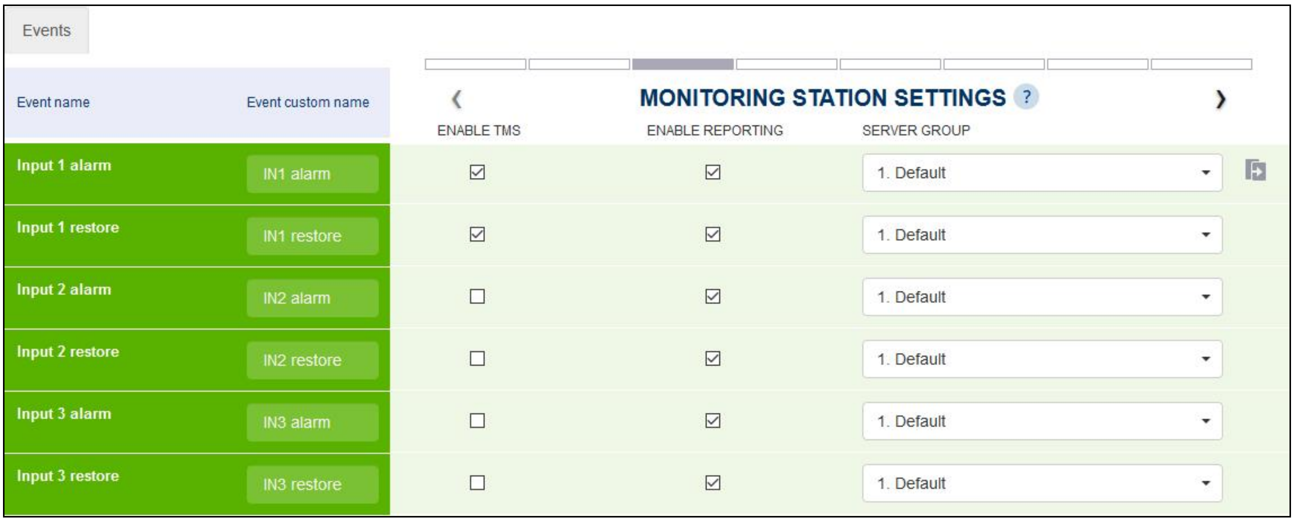
Event name	Event custom name	CID CODE	PARTITION	ZONE
IN1 alarm		130	01	000
IN1 restore		130	01	000
IN2 alarm		130	01	001
IN2 restore		130	01	001
IN3 alarm		130	01	002
IN3 restore		130	01	002

Event codes

Each internal event can be associated with a Contact ID code. Each one of them has a default Contact ID code, but it can be modified (see figure above).

CID code: 3 characters (0…9, A, B, C, D, E, F) long event code used for reporting to a monitoring station. (e.g. 130 = burglary; the restore event is reported with the same code)
Partition: the event's partition number (01… 99)
Zone: the event's zone number (001… 999)

Monitoring station settings:



Events

MONITORING STATION SETTINGS ?

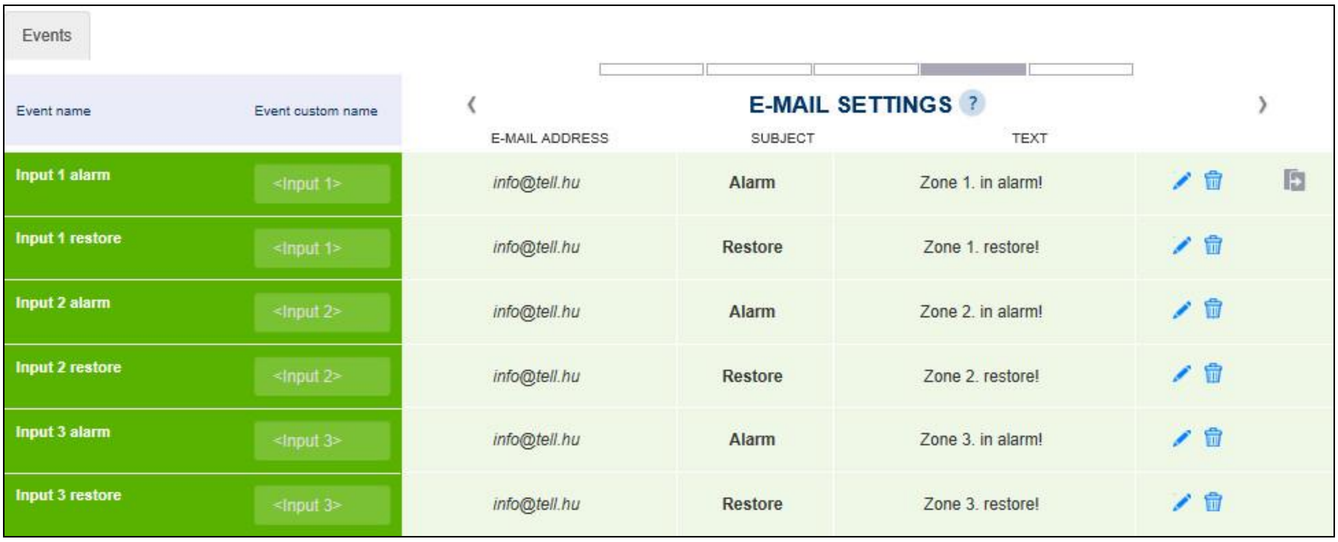
Event name	Event custom name	ENABLE TMS	ENABLE REPORTING	SERVER GROUP
Input 1 alarm	IN1 alarm	☑	☑	1. Default
Input 1 restore	IN1 restore	☑	☑	1. Default
Input 2 alarm	IN2 alarm	□	☑	1. Default
Input 2 restore	IN2 restore	□	☑	1. Default
Input 3 alarm	IN3 alarm	□	☑	1. Default
Input 3 restore	IN3 restore	□	☑	1. Default

Monitoring station settings

Server groups configured on the Servers tab can be associated with the events. It is also possible to assign different server groups to the alarm and restore events.

Check the **ENABLE TMS** option to start reporting to TMS.
Check the **ENABLE REPORTING** option to start reporting to a monitoring station.

Email settings:

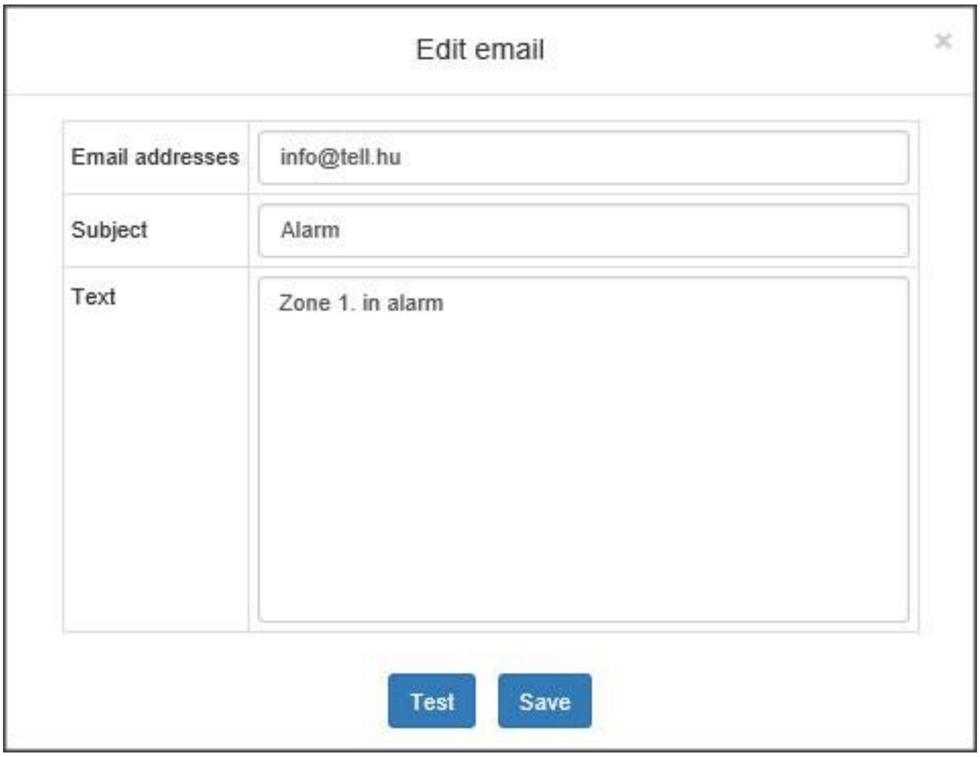


Event name	Event custom name	E-MAIL ADDRESS	SUBJECT	TEXT
Input 1 alarm	<Input 1>	info@tell.hu	Alarm	Zone 1. in alarm!
Input 1 restore	<Input 1>	info@tell.hu	Restore	Zone 1. restore!
Input 2 alarm	<Input 2>	info@tell.hu	Alarm	Zone 2. in alarm!
Input 2 restore	<Input 2>	info@tell.hu	Restore	Zone 2. restore!
Input 3 alarm	<Input 3>	info@tell.hu	Alarm	Zone 3. in alarm!
Input 3 restore	<Input 3>	info@tell.hu	Restore	Zone 3. restore!

Email settings

The module is able to send email notifications about events. Just like the monitoring station settings, the email settings also can be set up by events.

The edit icon opens a popup window (see figure below) where you can set the email address, subject and email body.


Edit email

Email addresses	info@tell.hu
Subject	Alarm
Text	Zone 1. in alarm

Edit email message

Enter the addresses into the **Email addresses** field. To add multiple addresses separate them by comma.

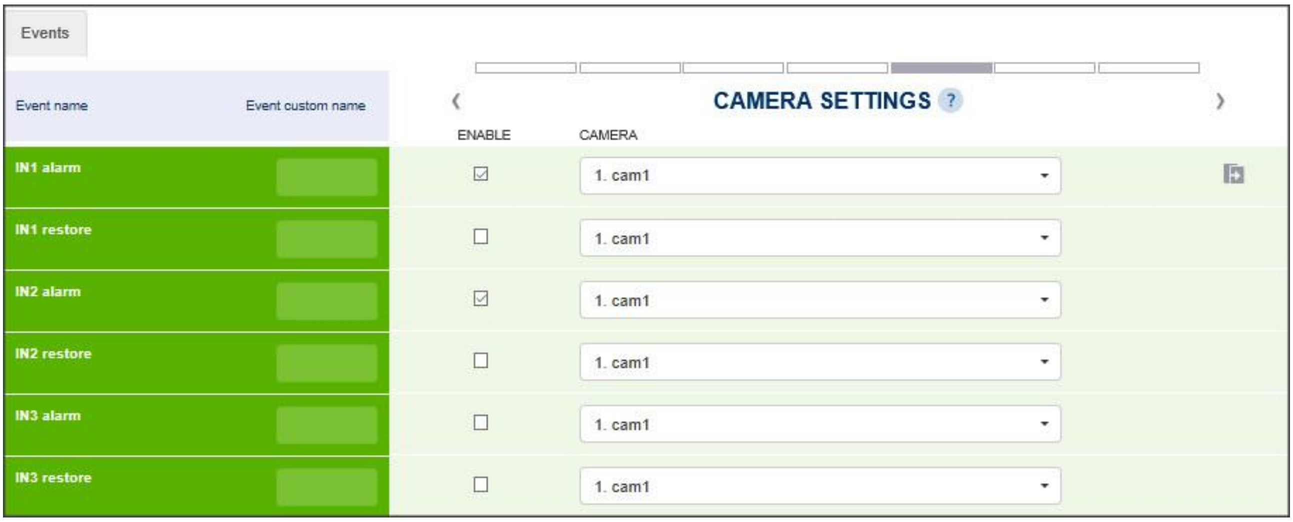
The **Subject** field is for the email subject.

Enter the email body into the **Text** field.

By pressing the **Test** button it is possible to send a test message to the entered addresses to verify that they are correct.
The **Save** button saves the email settings then the fields next to the event will be refreshed.

The delete button deletes all the email settings of the given event.

Camera settings:



Event name	Event custom name	ENABLE	CAMERA
IN1 alarm		☑	1. cam1
IN1 restore		□	1. cam1
IN2 alarm		☑	1. cam1
IN2 restore		□	1. cam1
IN3 alarm		□	1. cam1
IN3 restore		□	1. cam1

Camera settings

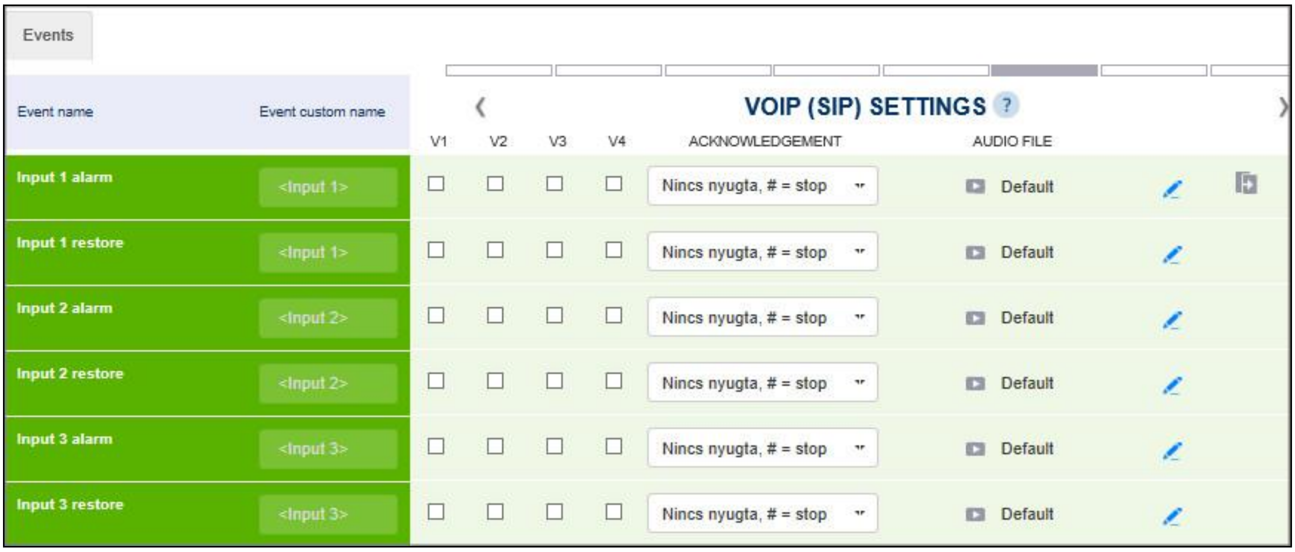
The cameras configured on the Cameras tab can be assigned to the events. If the event occurs, the module sends the last 5 images of the assigned camera to the corresponding e-mail address or uploads it to an FTP / SFTP server or sends it to the TMS server.

Enable: the camera assignment can be enabled with a checkbox.

Camera: You can assign camera to the event by selecting it from a dropdown list which lists the camera names you've set in the Camera name field of the Cameras tab.

Next to the camera dropdown menu, the email address is displayed that was assigned to the event in the E-mail settings. Image uploading to FTP / SFTP or TMS does not need to be enabled, it is sufficient if they are configured in **General** settings.

VOIP (SIP) settings:



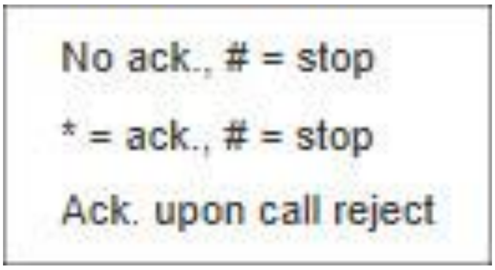
Event name	Event custom name	V1	V2	V3	V4	ACKNOWLEDGEMENT	AUDIO FILE
Input 1 alarm	<Input 1>	□	□	□	□	Nincs nyugta, # = stop	Default
Input 1 restore	<Input 1>	□	□	□	□	Nincs nyugta, # = stop	Default
Input 2 alarm	<Input 2>	□	□	□	□	Nincs nyugta, # = stop	Default
Input 2 restore	<Input 2>	□	□	□	□	Nincs nyugta, # = stop	Default
Input 3 alarm	<Input 3>	□	□	□	□	Nincs nyugta, # = stop	Default
Input 3 restore	<Input 3>	□	□	□	□	Nincs nyugta, # = stop	Default

VOIP SIP settings

You can also set up a voice call notification for the events. The phone numbers can be specified in the VOIP menu.

V1-V4 select the phone number you want to be notified about the event occurance.

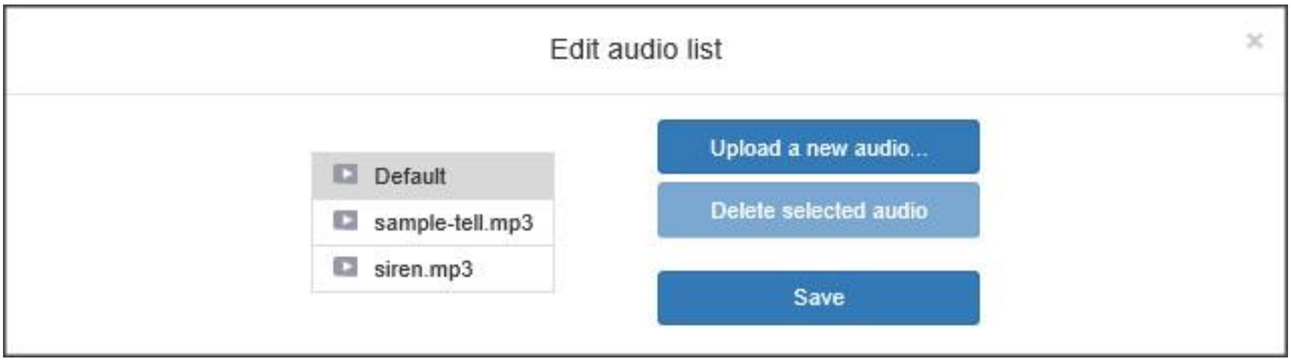
Acknowledgement: Select from the dropdown (see figure below):


No ack., # = stop
* = ack., # = stop
Ack. upon call reject

Acknowledgement

No ack, #=stop: accepting the call confirms the alarm event automatically; by pressing the # key on the phone stops reporting to the further phone numbers.
***= ack, #=stop**: the user must confirm the event by pressing the * key on the phone, otherwise the module recalls the number until the user confirms the alarm event. Pressing the # key on the phone stops reporting to the further phone numbers and confirms the event at the same time.
Ack. upon call reject: the alarm event can be confirmed by rejecting the call. In case of accepting the call, this also confirms the event automatically and reporting to the further phone numbers can be stopped by pressing the # key on the phone.

Audio file: Select the audio file you want to be played during the voice call.
To configure press the edit button in the event's row, which opens a popup window (see figure below).



Edit audio list

Upload a new audio: It is possible to upload audio files with mp3 extension which are not longer than 1 minute. Pressing the button opens a file browser window so you can select the file you want to upload.

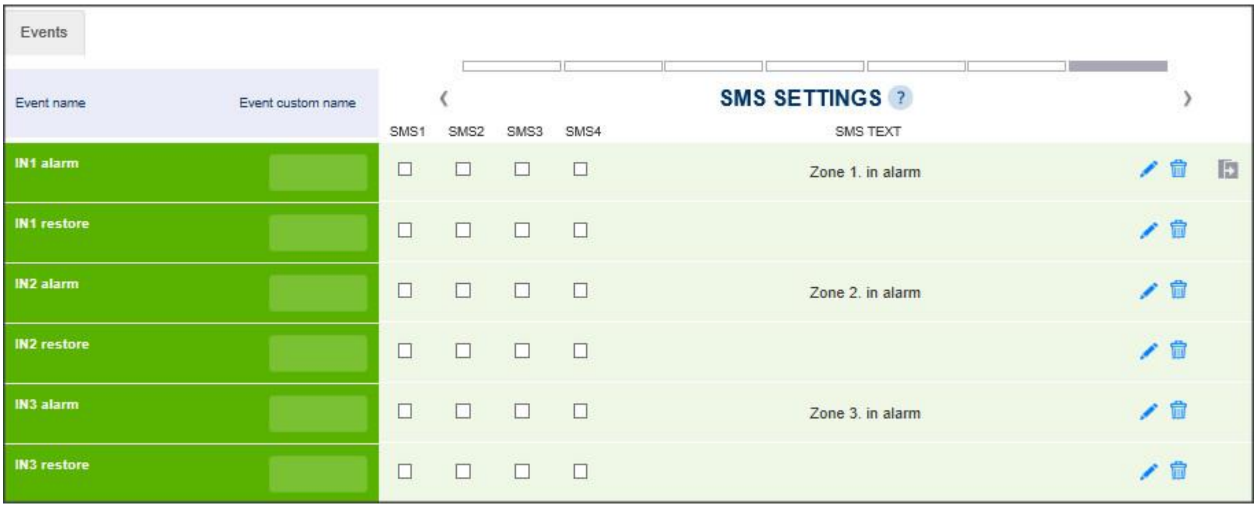
Delete selected audio: To remove a previously uploaded audio select it and press the „Delete selected audio" button.

Save: Select the audio file to be played during the voice call then save it.

Network: You can set the communication channel of VoIP calls for each event. It is possible to set for each kind of events a different network than the default network selected on the **General** tab.

Setting up the first event you can choose to fill all the other rows with the same settings.

SMS settings:



Events

SMS SETTINGS ?

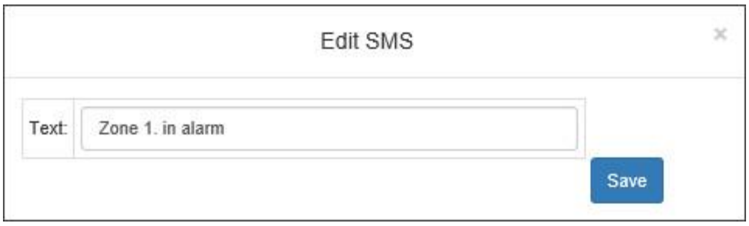
Event name	Event custom name	SMS1	SMS2	SMS3	SMS4	SMS TEXT
IN1 alarm		□	□	□	□	Zone 1. in alarm
IN1 restore		□	□	□	□	
IN2 alarm		□	□	□	□	Zone 2. in alarm
IN2 restore		□	□	□	□	
IN3 alarm		□	□	□	□	Zone 3. in alarm
IN3 restore		□	□	□	□	

SMS settings

It is possible to add SMS notification to the events. The phone numbers can be edited on the VoIP tab.

SMS1-SMS4: Select which phone numbers you want to be notified about the event.

The pencil icon opens a popup window (figure below) in which you can edit the SMS message. The maximal length of the SMS can be 70 characters.



Edit SMS

Text: Zone 1. in alarm

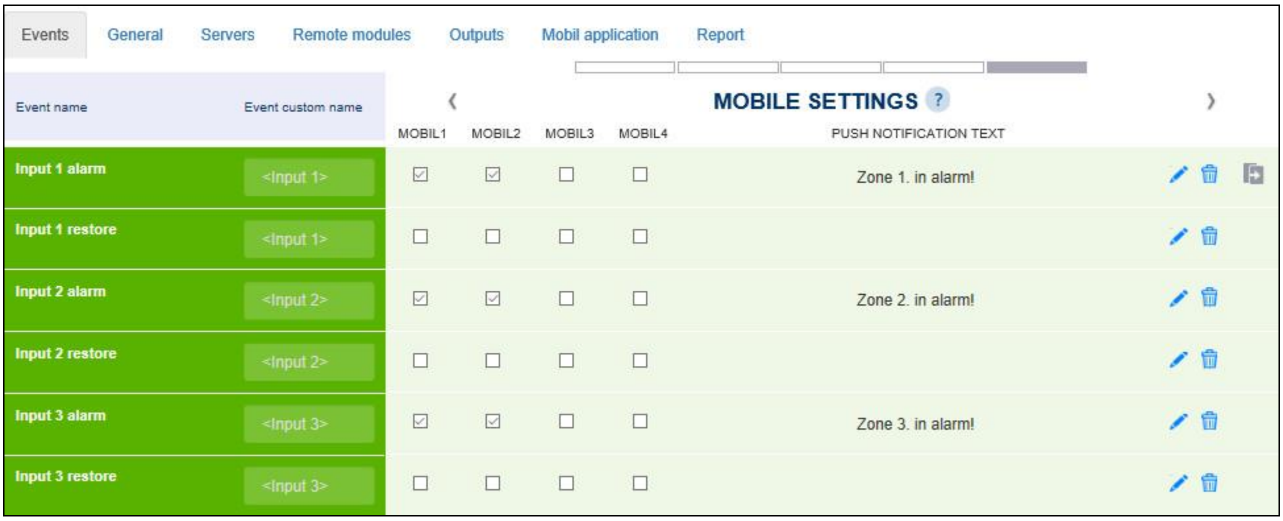
Edit SMS text

Save button saves the text for the event.

The delete button removes all the notifications set for the event.

Setting up the first event you can choose to fill all the other rows with the same settings.

Push notification settings:



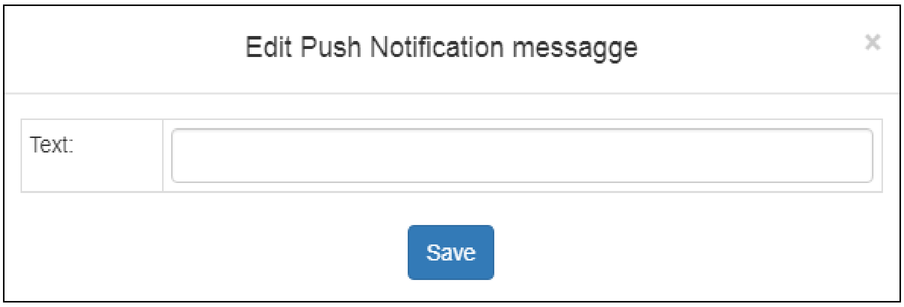
Event name	Event custom name	MOBIL1	MOBIL2	MOBIL3	MOBIL4	PUSH NOTIFICATION TEXT
Input 1 alarm	<Input 1>	☑	☑	□	□	Zone 1. in alarm!
Input 1 restore	<Input 1>	□	□	□	□	
Input 2 alarm	<Input 2>	☑	☑	□	□	Zone 2. in alarm!
Input 2 restore	<Input 2>	□	□	□	□	
Input 3 alarm	<Input 3>	☑	☑	□	□	Zone 3. in alarm!
Input 3 restore	<Input 3>	□	□	□	□	

Push notification settings

You can set Push message sending for the events. The devices can be added in the **Mobile application** menu.

MOBIL1 – MOBIL4: Select which devices you want to be notified via Push message about the event.

The pencil icon opens a popup window (figure below) in which you can edit the Push message. The maximal length of the message can be 70 characters.



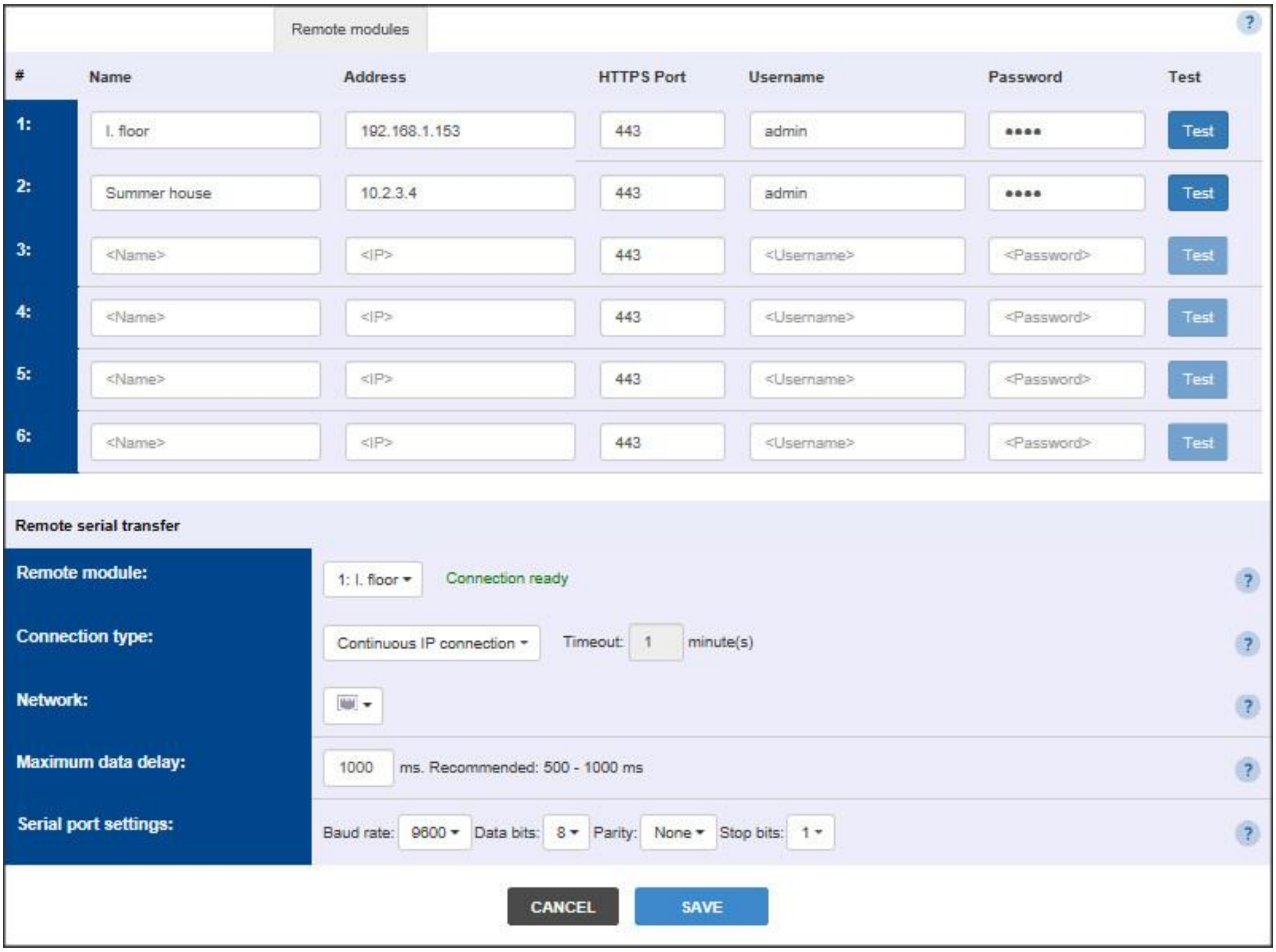
Edit push message

Save button saves the text for the event.

The delete button removes all the notifications set for the event.

Setting up the first event you can choose to fill all the other rows with the same settings.

6.8 Remote modules



Remote modules

#	Name	Address	HTTPS Port	Username	Password	Test
1:	I. floor	192.168.1.153	443	admin	●●●●	Test
2:	Summer house	10.2.3.4	443	admin	●●●●	Test
3:	<Name>	<IP>	443	<Username>	<Password>	Test
4:	<Name>	<IP>	443	<Username>	<Password>	Test
5:	<Name>	<IP>	443	<Username>	<Password>	Test
6:	<Name>	<IP>	443	<Username>	<Password>	Test

Remote serial transfer

Remote module:	1: I. floor ▾ Connection ready
Connection type:	Continuous IP connection ▾ Timeout: 1 minute(s)
Network:	▾
Maximum data delay:	1000 ms. Recommended: 500 - 1000 ms
Serial port settings:	Baud rate: 9600 ▾ Data bits: 8 ▾ Parity: None ▾ Stop bits: 1 ▾

Remote module settings

You can add up to 6 remote IP Bridge modules to your device. You can use them for transparent serial data transfer or for controlling the remote devices' output as an effect of a local event. The settings are the followings (figure below):

#: The module's index number

Name: Unique name can be set for each module.

IP: the module's IP address (If the remote module is not on the same network enter the router's IP address and the external port. It is also possible to add DNS instead of IP address. You need to configure the port forward in the router!)

Port: The device's https port

Username: The username of device administrator.

Password: The password of device administrator.

Test: You can check your settings by clicking the test button.

Remote serial data transfer:

The following settings are required for the transparent serial data transfer.

Remote module: Use the dropdown to select the remote module you'd like to associate with the device to use it for serial data transfer. Besides the six modules, you can also select the „**Receive only"** option. In this case the device only forwards data received from remote modules to its serial port. This can work with any number of remote modules and they don't even need to be among the associated remote modules. Also, this option must be selected if you use the module to program an alarm system through the IP Bridge Client program. If you select from the six associated remote modules the device indicates the connection status.

Connection type: You can select from the following two connection types:

> **Continuous IP connection:** The devices are continuously connected to each other.
>
> **Connect, if necessary:** The modules connect each other only for sending data. After the data is sent they close the connection.
>
> **Timeout:** In case of temporary connection this is the time the module waits after the last data was sent or received before closing the connection.

Network: Use the dropdown menu to set the communication channel for the device to access the remote module, and also select the backup communication channel. (If the module doesn't have an extension panel the only option is LAN and the selector is not displayed.)

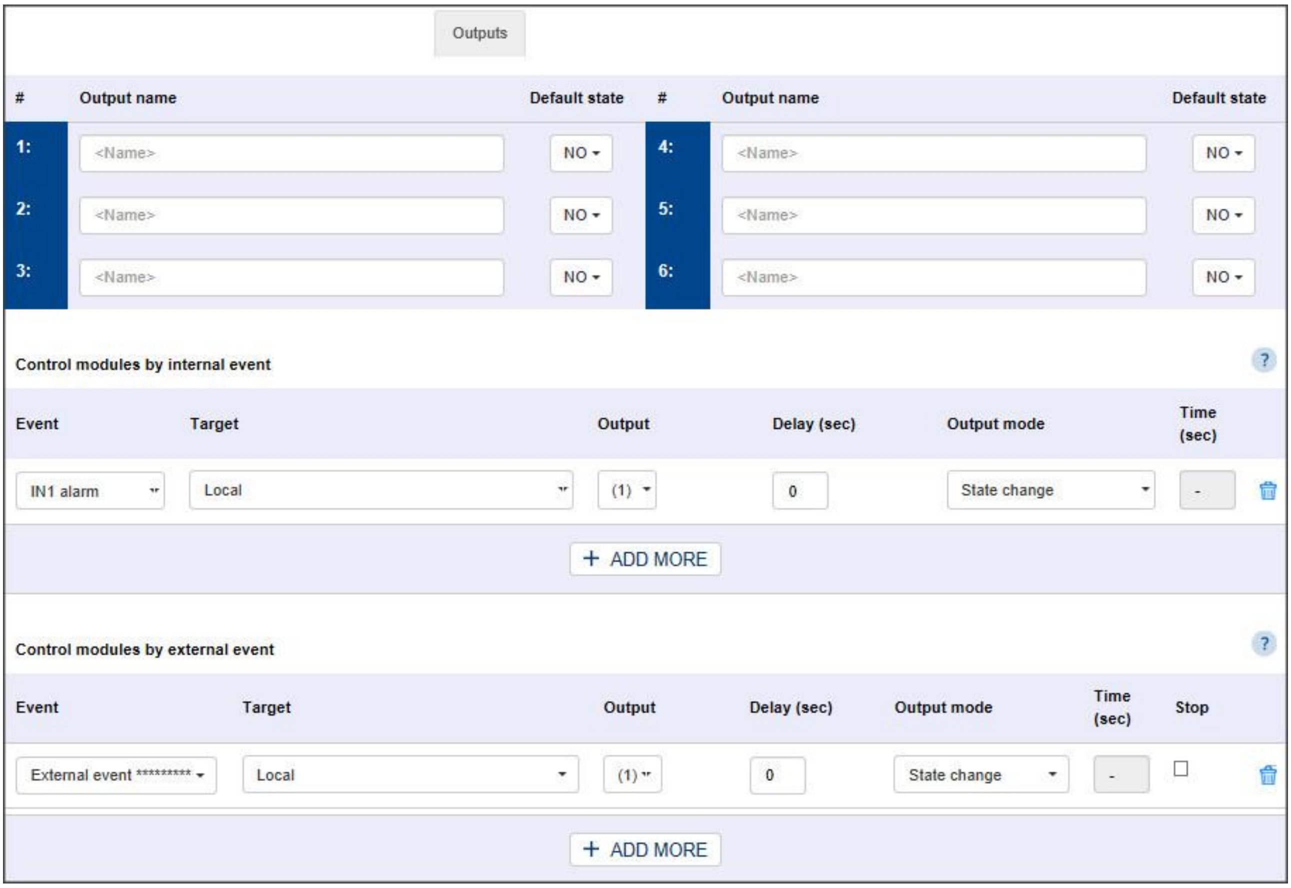
Maximum data delay: The module collects the data received on its serial port. If there's no delay in receiving data, after the amount of time set in this field the module sends the previously collected data to the remote module.

With these values the response times can be adjusted according to the established serial connection. If the maximum data delay is smaller, the device waits for fewer data and sends the packet to the remote module sooner, so the device on the remote module's serial port receives a quicker response.

Serial port settings: You can configure the serial port's settings to meet the requirements of the selected connection type.

For more detailed information on the remote programming of alarm systems, please see the Appendix.

6.9 Outputs



#	Output name	Default state	#	Output name	Default state
1:	<Name>	NO	4:	<Name>	NO
2:	<Name>	NO	5:	<Name>	NO
3:	<Name>	NO	6:	<Name>	NO

Control modules by internal event

Event	Target	Output	Delay (sec)	Output mode	Time (sec)
IN1 alarm	Local	(1)	0	State change	-

Control modules by external event

Event	Target	Output	Delay (sec)	Output mode	Time (sec)	Stop
External event *********	Local	(1)	0	State change	-	□

Output configuration

On the **Outputs** tab you can configure the outputs (figure above) and assign automatic control to them. The options are:

#: Index of the output

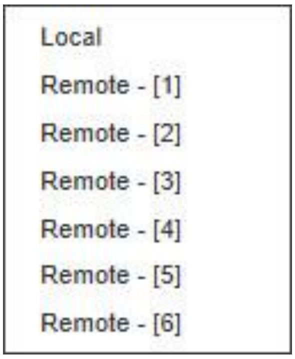
Output name: Unique name of the output which is displayed in the Status menu next to the index number.

Default state: Select the output's default state from the dropdown list. The module has 2 terminals for each output. If you configure the output to NC the relay status changes to closed and it remains closed.

Adding control modules by internal event:

Use the „Add more" button to add new control module. In the new row you can configure the output.

Event: The event can be selected from a dropdown, that lists all the internal and external events configured on the **Events** page.

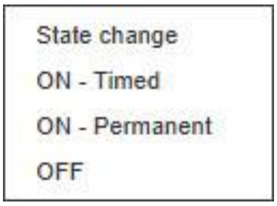


Target: You can select which module's output to activate due to the specific event. By selecting the „Local" option, you can control the module's local outputs. The **Remote 1-6** options referring to the modules added on **Remote modules** page.

Output: The target module's output. In case it has a unique name, it is also displayed in the dropdown, else it is listed by its sequence number.

Delay (sec): The delay of activating the output can be defined in seconds.

Output mode:



Output mode

State change: the event will cause a relay status change.
ON - Timed: the event activates the relay output for the time set in Time field in seconds. When the time is up the output becomes inactive again.
ON - Permanent: the event activates the relay output permanently (the relay output remains active until switching off or receiving status change command).
OFF: the event deactivates the relay output.

Time: If the selected output mode is ON-Timed you need to add how long the relay needs to stay switched ON.

Delete control module:

🗑 To delete a contol module use the dust-bin icon at the end of the row.

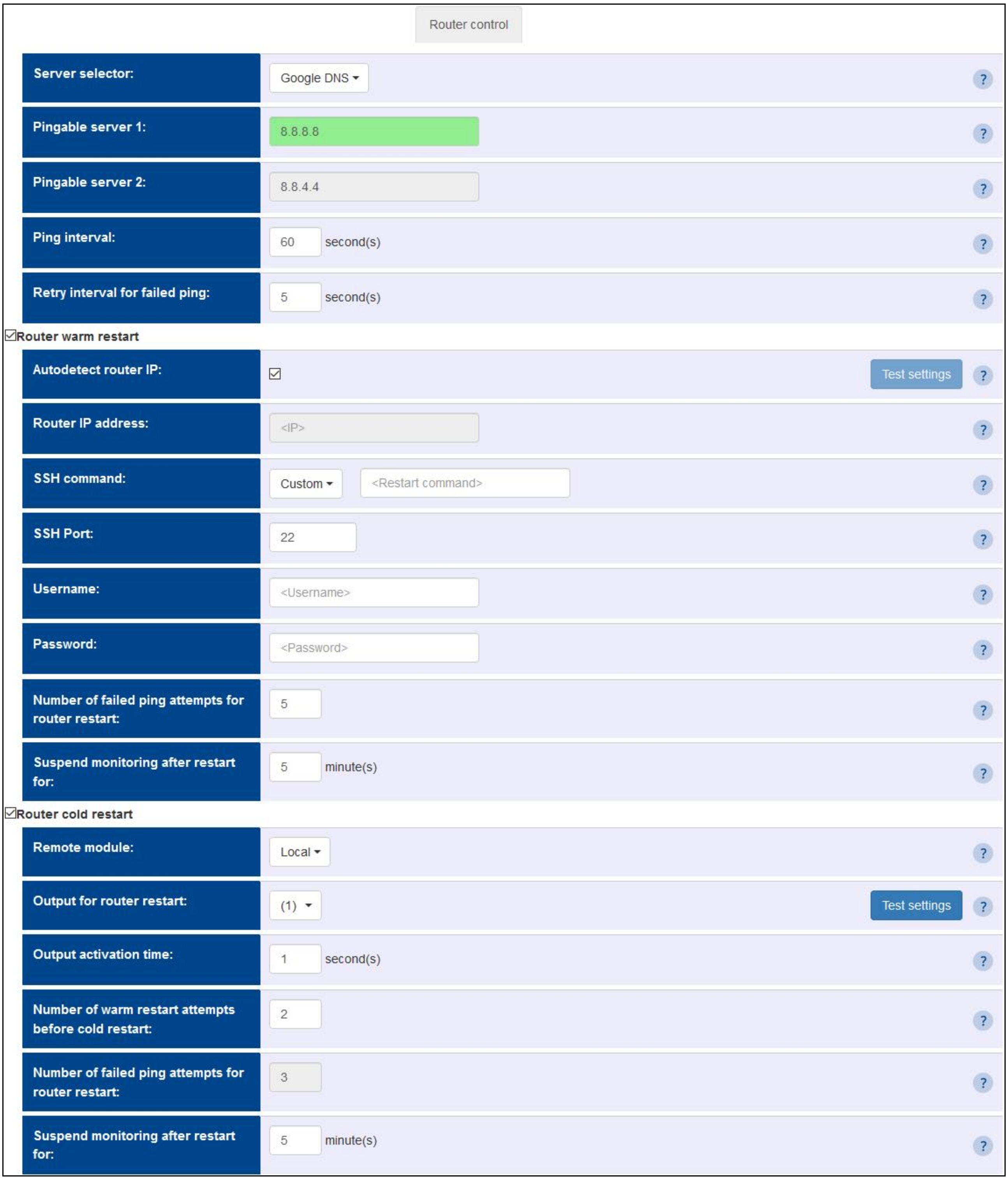
Control modules by external event:

Adding and configuring is the same as described above, but here only the external events added on Events page can be selected to control an output.

Stop: You can add multiple overlapping external events in the Events menu to control an output. If you select the „Stop" option for an event, the external events that is specified below will not be evaluated.

6.10 Router control:

The module is capable of router monitoring, so it can warm and cold restart routers on the same network the IP Bridge is connected to, if it doesn't receive answer from a configured Ping server. It is possible to enable only warm restart, only cold restart or both of them (figure below).



Server selector:	Google DNS ▾
Pingable server 1:	8.8.8.8
Pingable server 2:	8.8.4.4
Ping interval:	60 second(s)
Retry interval for failed ping:	5 second(s)

☑Router warm restart

Autodetect router IP:	☑
Router IP address:	<IP>
SSH command:	Custom ▾ <Restart command>
SSH Port:	22
Username:	<Username>
Password:	<Password>
Number of failed ping attempts for router restart:	5
Suspend monitoring after restart for:	5 minute(s)

☑Router cold restart

Remote module:	Local ▾
Output for router restart:	(1) ▾
Output activation time:	1 second(s)
Number of warm restart attempts before cold restart:	2
Number of failed ping attempts for router restart:	3
Suspend monitoring after restart for:	5 minute(s)

Router monitoring options

Server selector: You can select predefined servers from the drop-down list, or you can also specify „Custom" servers, in which case Pingable server 1 and 2 fields become editable.

Pingable server 1-2: Add the IP address of a server which can be accessed only through the router. These fields are editable only if you select "Custom" option from the dropdown. The field's background color indicates whether the IP address is reachable. It turns green if the IP was available, otherwise red.

Ping interval: The ping attempts' frequency can be set in seconds.

Retry interval for failed ping: The ping frequency can be increased if no response was received.

Router's warm restart:

Autodetect router IP: The module automatically detects the router on the same network and fills the "Router IP address" field.

Router IP address: If the automatic router detection is not enabled, you can manually enter the router's IP address.

SSH command: Certain router types support commands received through SSH connection. By selecting SSH mode, you can choose a restart command from the drop-down list, or you can specify a custom command.

SSH port: This is the router's authentication port. Also the IP Bridge can log into the router through this port.

Username: Add the username for logging into the router.

Password: Enter the password for logging into the router.

Number of failed ping attempts for warm restart: You can set the number of attempts before the module restarts the router.

Suspend monitoring after restart: This is the time the module waits before the next ping attempt after the router was restarted. This value can be modified depending on the time the router restart takes.

Router's cold restart:

Remote module: You can select which module output you want to be activated when the given event occurs. By selecting the Local option you can control the outputs of the given device. The Remote 1-6 options allow you to select from the modules specified in the Remote Modules menu.

Output for router restart: The router restart event will trigger the status change of the selected output. The selected output will be displayed in the Outputs menu. It can't be deleted and you can't use it for automatic output control.

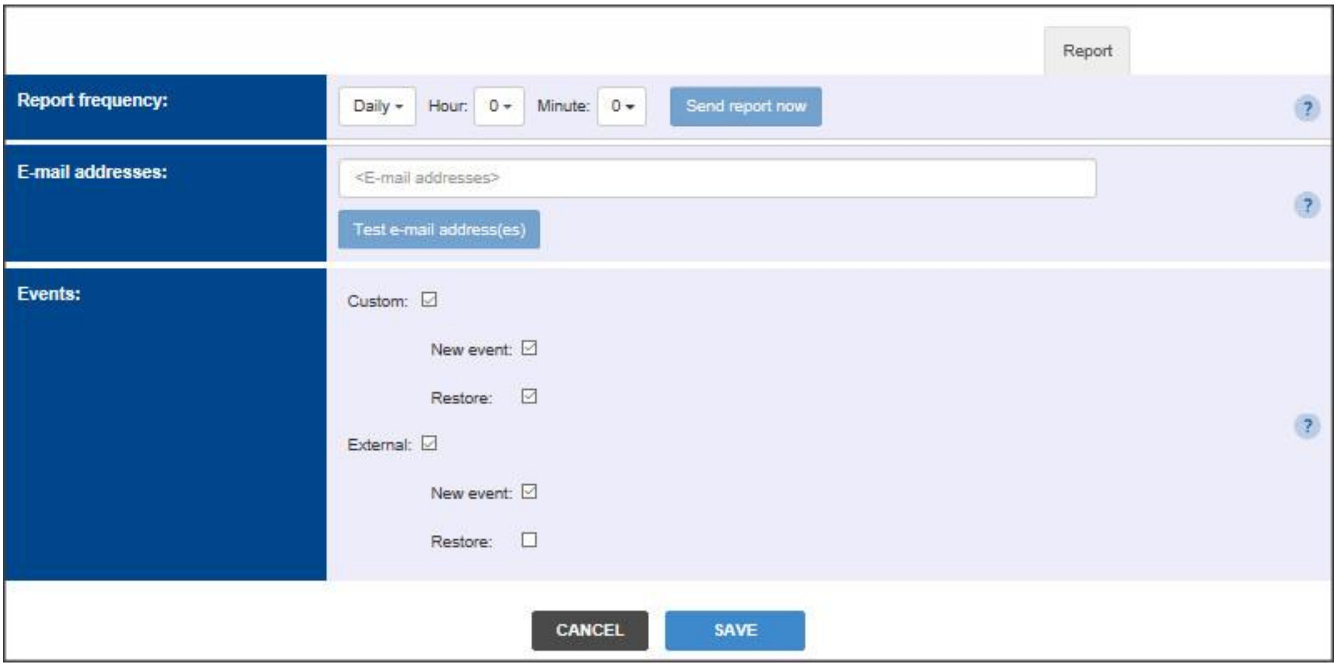
Output activation time: In this field you can set how long the output status change should take.

Number of warm restart attempts before cold restart: If the router's warm restart is also set, in this field you can add how many times to try to warm restart the router before cold restarting it.

Number of failed ping attempts for router restart: If the warm restart is not enabled, you can add the maximum number of failed ping attempts before power off and on the router. For cold restart option, you also need to fill the fields in warm restart section. Cold restart without attempting warm restart is enabled only if the module doesn't support the router's warm restart.

Suspend monitoring after restart: This is the time the module waits before the next ping attempt after the router was restarted. This value can be modified depending on the time the router restart takes.

6.11 Report



Report frequency: Daily Hour: 0 Minute: 0

E-mail addresses: <E-mail addresses>

Events:

Custom: ☑

New event: ☑

Restore: ☑

External: ☑

New event: ☑

Restore: □

Edit report sending

In the system, it is possible to send regular reports about the events. The reports can be configured as follows (figure above):

Report frequency: The frequency can be selected from the dropdown list.
Daily: The module sends a report every day. You can set the time of sending.
Weekly: The module sends a report every week. You can set the day and time of sending.
Monthly: The module sends a report every month. You can set the day and time of sending.

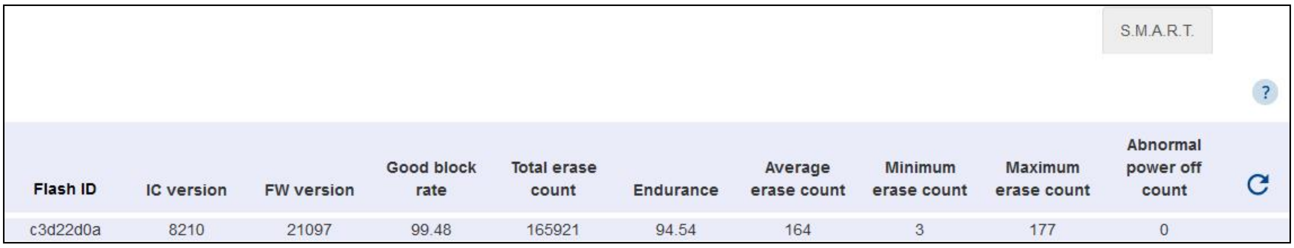
If the number of events reaches 250, the module sends the event report regardless the frequency.

Email addresses: Set the email address you want the report to be sent to. To add multiple addresses separate them with comma.

Events: You can select which kind of events you want to be listed in the report.

Test email address(es): This button is for testing the report settings. It sends a report according to the settings to the specified email address(es) if there's any.

6.12 S.M.A.R.T



Flash ID	IC version	FW version	Good block rate	Total erase count	Endurance	Average erase count	Minimum erase count	Maximum erase count	Abnormal power off count
c3d22d0a	8210	21097	99.48	165921	94.54	164	3	177	0

S.M.A.R.T info

Displays the SD card's S.M.A.R.T info. Works properly only with APACER cards.

7 Stopping the module properly

If you'd like to normally switch off the IP Bridge module, keep the microswitch on the module pressed. After the LED turns orange wait 3 seconds and then release the button. LED turns red then goes out. When LED doesn't lit anymore, you can disconnect the power supply.

8 Restoring factory default settings

There are two options to reset the factory settings. It can be done with the Factory reset button in the General Settings menu or with the button on the module. To reset the factory default settings with the button on the module, keep the microswittch on the module pressed. After the LED turns red wait 3 seconds and then release the button. The LED is lit orange first then turns red. The module restores the factory default settings then restarts automatically. Attention! During restore, also the network setting will be reset to the default DHCP.

9 General LED signals

Color	LED
Red	Booting / shutdown in progress
Green	The system is ready
Orange	An error occured / On/Off is in progress

10 Technical specification

Supply voltage:	12-24V DC
Nominal current consumption:	520mA @ 12V DC
Maximum current consumption:	700mA @ 12V DC
Operation temperature:	-20ºC - +70ºC
Maximum relay output load:	1A @ 12V DC
Dimensions:	130 x 69 x 19 mm
Weight:	200g (packed: 300g)

10.1 Generated telephone line specification

Line voltage:	48 V
Line current:	20 mA
Line impedance:	600 Ohm
Ringing voltage:	±50V (20 Hz)
Dial tone:	425 Hz

11 Appendix

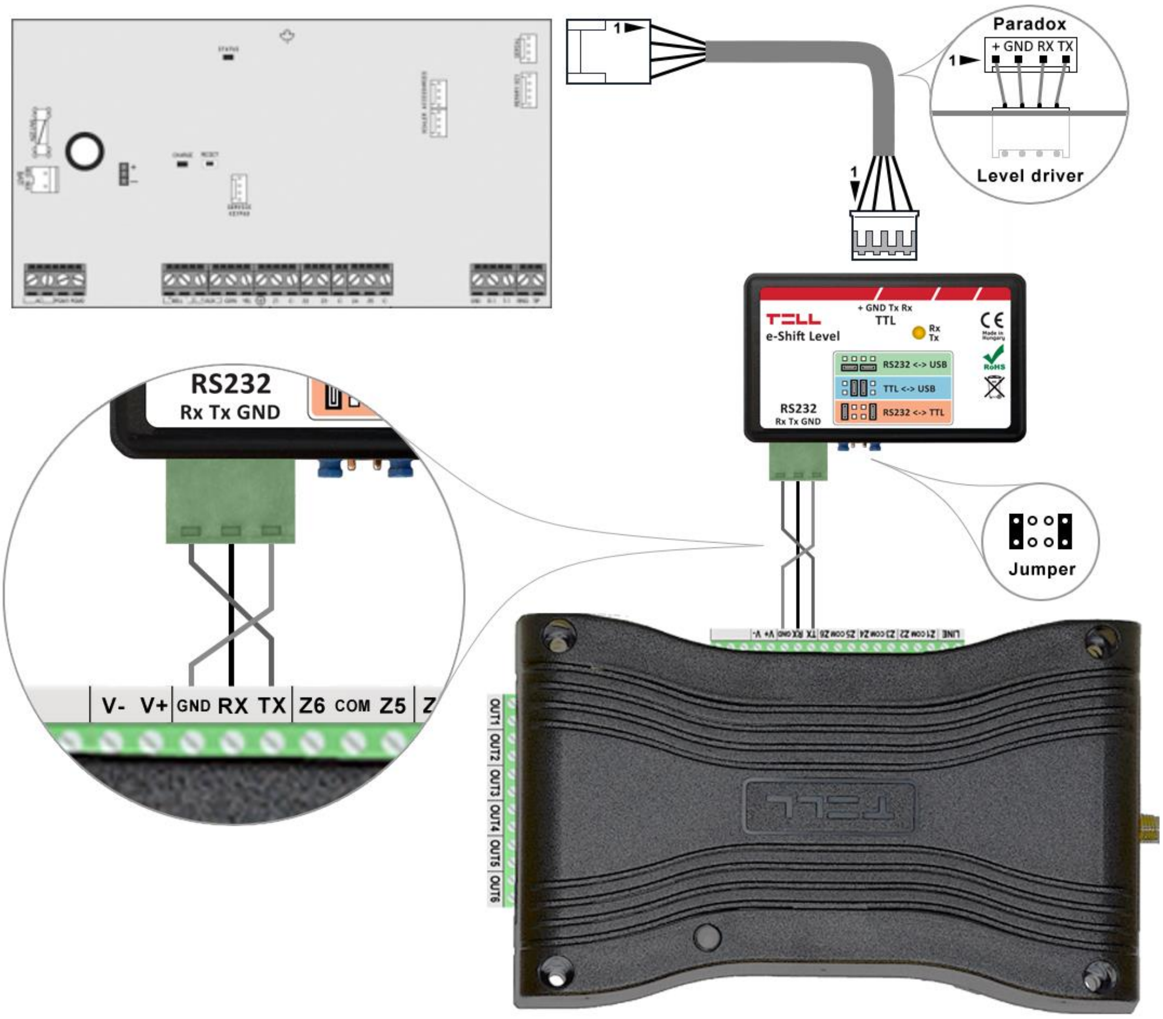
11.1 Remote programming of alarm control panels

In this case, the module performs transparent serial data communication over IP connection. The connection between the programming software and the alarm control panel is provided by the module and an IP Bridge Virtual Client program. The module's serial port is connecting to the alarm control panel while the programming software is connecting to the virtual serial port created by the client program.

Important! If you want to access the module via mobile internet, you need to make sure that the APN used by the computer running the programming software and the APN used by the module are accessible to each other. If it is possible, the devices have to be connected to the same APN or the mobile network's APN have to be the part of the computer's network.

11.1.1 Paradox control panel

Installation settings:

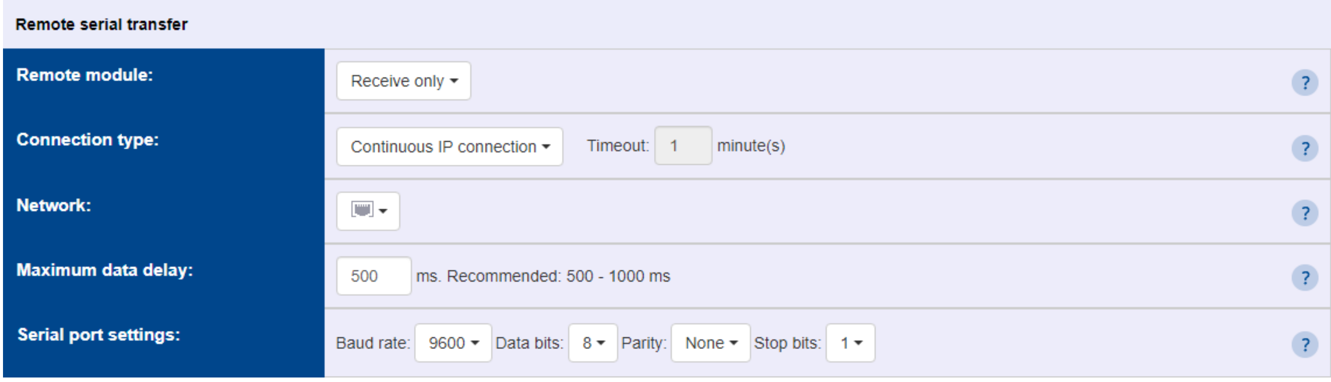


Wiring diagram for Paradox alarm systems

Connect a logic level converter (e-Shift Level) to the alarm control panel, then connect its serial port output with the module (see figure above). Only RX, TX and GND wires will be used, please connect these to the module in the order shown in the figure above.

Software settings:

Open the module's web interface, set the data for the serial port operation in the **Remote Modules** menu as shown below:



Remote serial transfer

Remote module: Receive only

Connection type: Continuous IP connection Timeout: 1 minute(s)

Network:

Maximum data delay: 500 ms. Recommended: 500 - 1000 ms

Serial port settings: Baud rate: 9600 Data bits: 8 Parity: None Stop bits: 1

Remote serial transfer

Remote module: Select the „Receive only” option from the dropdown list.

Connection type: Select the „Continuous IP connection” option from the dropdown list. By this setting, the connection between the programming software and the alarm control panel will be continuous.

Network: In case the module has a 3G/4G extension panel, the communication channel for transmitting serial data also can be selected here.

Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

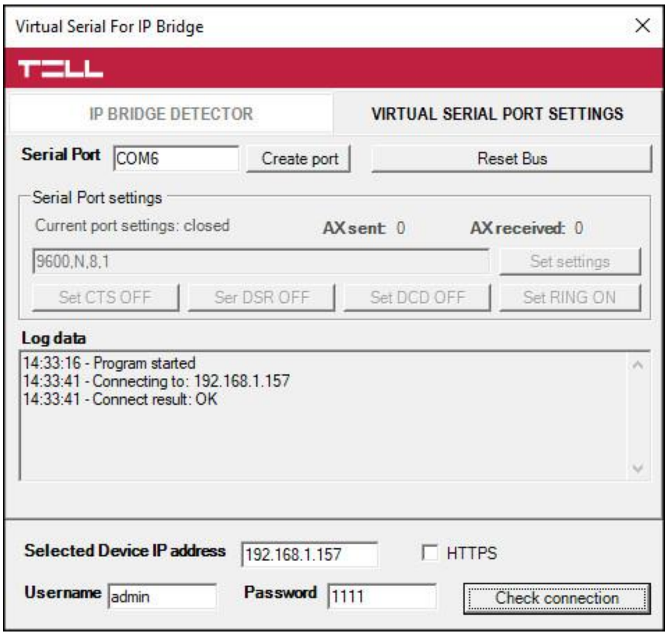
Maximum data delay: Recommended setting is 500 ms.

Serial port settings: Recommended settings for Spectra alarm control panels:Baud rate: 9600, Data bits: 8, Parity: None, Stop bits: 1.

Recommended settings for EVO alarm control panels:Baud rate: 57600, Data bits: 8, Parity: None, Stop bits: 1.

For connecting the alarm control panel and programming software install the IP Bridge Virtual Client software. This software connects the computer and the module and establishes a virtual serial data port that you need to select in the programming software.

After starting the program, the following setting options are available:



Virtual Serial For IP Bridge

Serial Port COM6

Serial Port settings

Current port settings: closed AX sent: 0 AX received: 0

9600,N,8,1

Log data

```
14:33:16 - Program started
14:33:41 - Connecting to: 192.168.1.157
14:33:41 - Connect result: OK
```

Selected Device IP address 192.168.1.157 □ HTTPS

Username admin Password 1111

Selected Device IP address: The module's IP address. If it is not in the same network with the module, it is also possible to add the DNS name with the necessary parameters. If you want to connect through mobile internet, enter the mobile internet IP address that you can find on the module's web-based interface.

Username: The username of the module administrator.

Password: The password of the user.

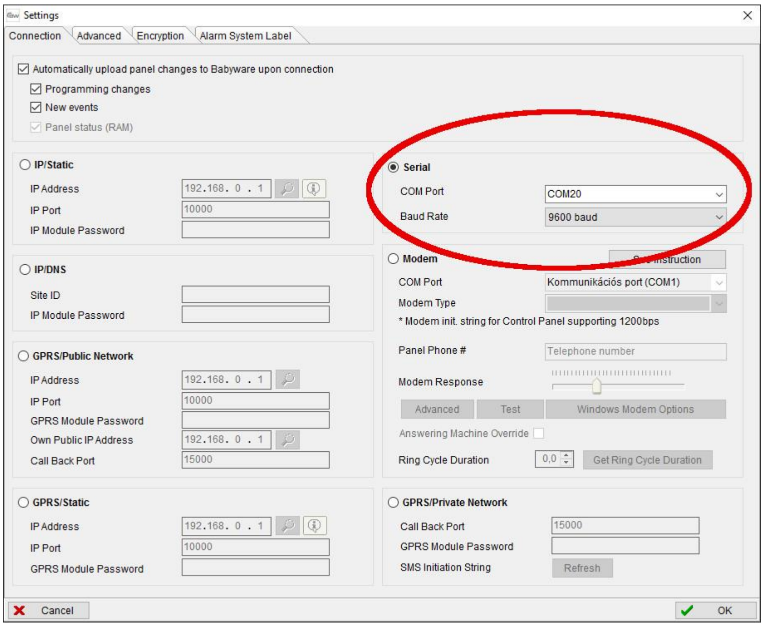
Check connection: Checks the module's address you set.

Serial Port: Set the virtual serial port's address that you need to select in the alarm system's programming software.

Create port: Creates the virtual port according to the settings.

Log data: It provides information on the operation of the program, and displays data received on the serial port.

In the Babyware programming software, select the virtual serial port, then connect it to the control panel (figures below).



Settings

Connection | Advanced | Encryption | Alarm System Label

☑ Automatically upload panel changes to Babyware upon connection
☑ Programming changes
☑ New events
☑ Panel status (RAM)

○ IP/Static
IP Address: 192.168. 0 . 1
IP Port: 10000
IP Module Password:

○ IP/DNS
Site ID:
IP Module Password:

○ GPRS/Public Network
IP Address: 192.168. 0 . 1
IP Port: 10000
GPRS Module Password:
Own Public IP Address: 192.168. 0 . 1
Call Back Port: 15000

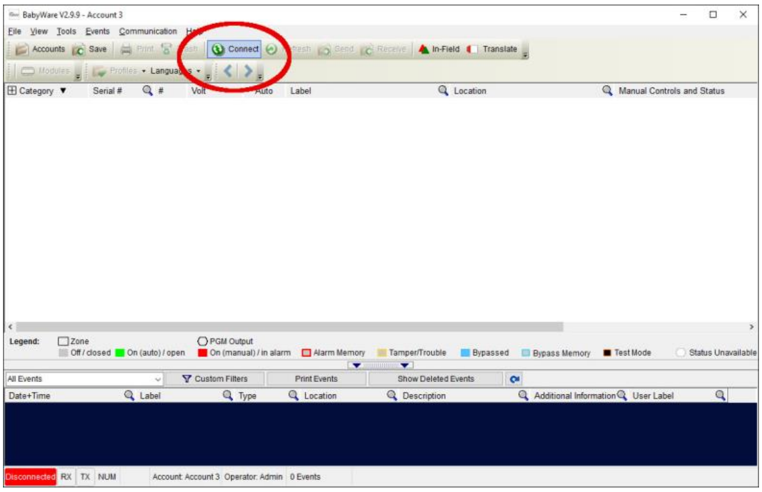
○ GPRS/Static
IP Address: 192.168. 0 . 1
IP Port: 10000
GPRS Module Password:

● Serial
COM Port: COM20
Baud Rate: 9600 baud

○ Modem
COM Port: Kommunikációs port (COM1)
Modem Type:
* Modem init. string for Control Panel supporting 1200bps
Panel Phone #: Telephone number
Modem Response
Answering Machine Override □
Ring Cycle Duration: 0,0

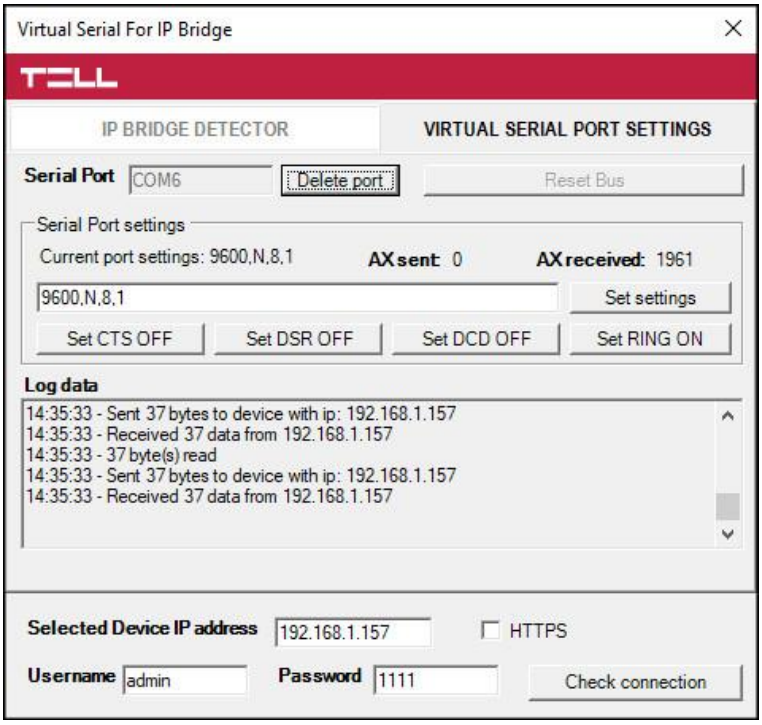
○ GPRS/Private Network
Call Back Port: 15000
GPRS Module Password:
SMS Initiation String

Select serial port



Connecting

The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



Serial Port COM6

Current port settings: 9600,N,8,1 AX sent: 0 AX received: 1961

9600,N,8,1

```
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
14:35:33 - 37 byte(s) read
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
```

Selected Device IP address 192.168.1.157

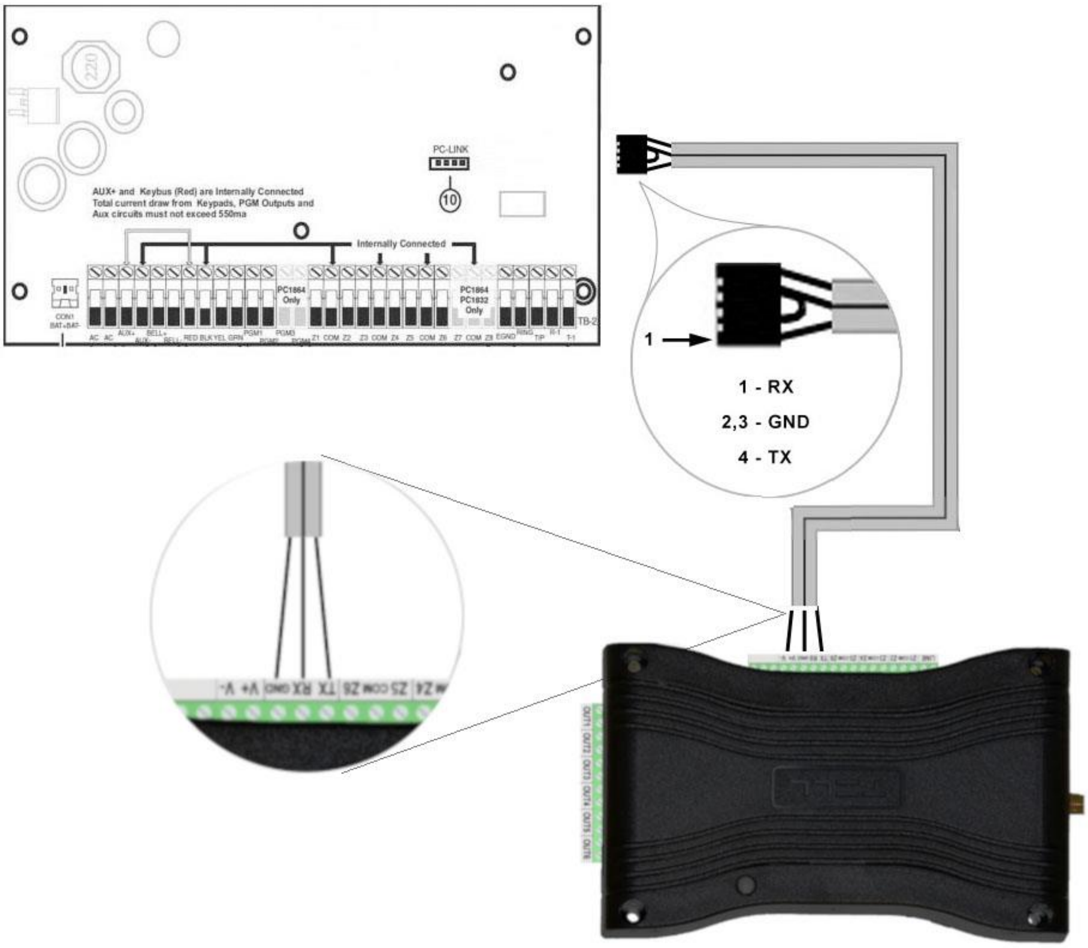
Username admin Password 1111

Connection established

When you finished with programming, press the **Delete port** button to close the connection and the virtual serial port.

11.1.2 DSC alarm control panel

Installation settings:

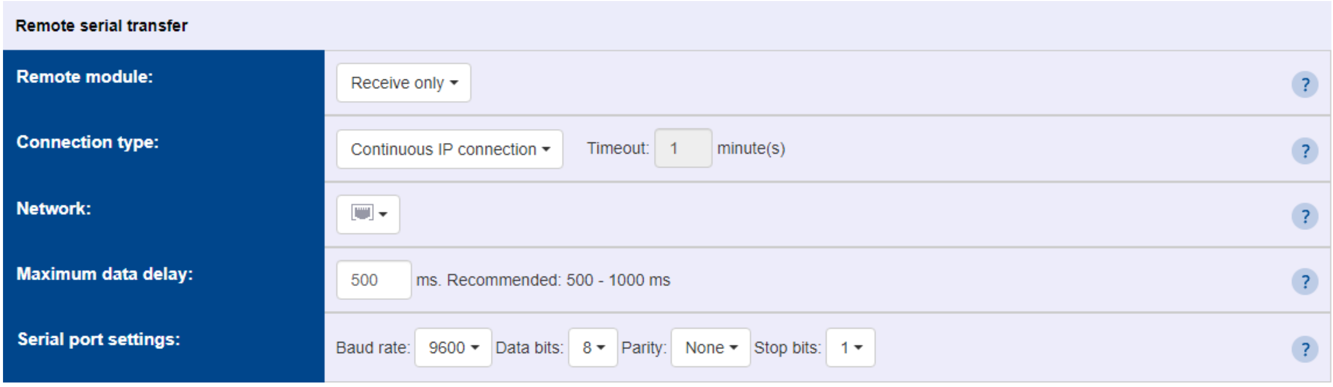

PC-LINK
AUX+ and Keybus (Red) are Internally Connected
Total current draw from Keypads, PGM Outputs and
Aux circuits must not exceed 550ma
Internally Connected
PC1864 Only
PC1864 PC1832 Only
1
1 - RX
2,3 - GND
4 - TX

Wiring diagram for DSC alarm systems

Connect a programming cable to the alarm control panel, then connect its serial port output with the module (see figure above). Only RX, TX and GND wires will be used, please connect these to the module in the order shown in the figure above.

Software settings:

Open the module's web interface, set the data for the serial port operation in the **Remote Modules** menu as shown below:



Remote serial transfer

Remote module:	Receive only ▾
Connection type:	Continuous IP connection ▾ Timeout: 1 minute(s)
Network:	▾
Maximum data delay:	500 ms. Recommended: 500 - 1000 ms
Serial port settings:	Baud rate: 9600 ▾ Data bits: 8 ▾ Parity: None ▾ Stop bits: 1 ▾

Remote serial transfer

Remote module: Select the „Receive only” option from the dropdown list.

Connection type: Select the „Continuous IP connection” option from the dropdown list. By this setting, the connection between the programming software and the alarm control panel will be continuous.

Network: In case the module has a 3G/4G extension panel, the communication channel for transmitting serial data also can be selected here.

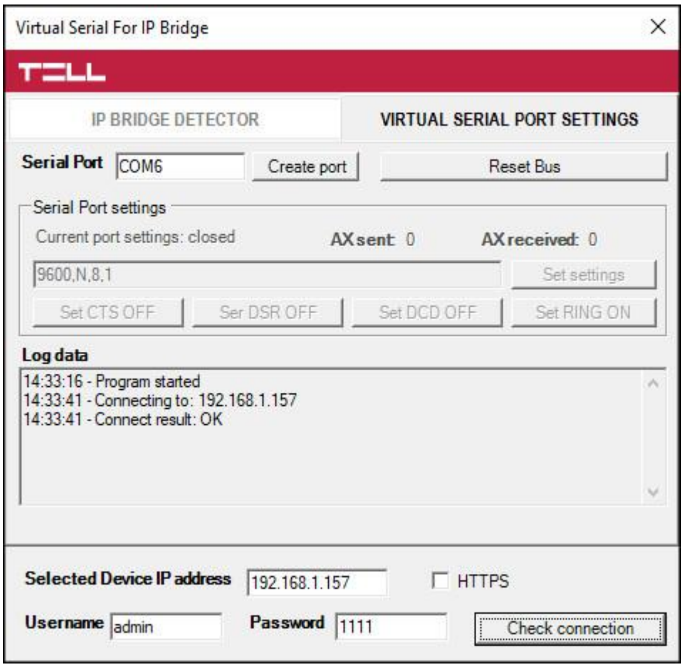
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

Maximum data delay: Recommended setting is 500 ms.

Serial port settings: Recommended settings: Baud rate: 9600, Data bits: 8, Parity: None, Stop bits: 1.

For connecting the alarm control panel and programming software install the IP Bridge Virtual Client software. This software connects the computer and the module and establishes a virtual serial data port that you need to select in the programming software.

After starting the program, the following setting options are available:



Virtual Serial For IP Bridge

Serial Port: COM6

Serial Port settings

Current port settings: closed   AX sent: 0   AX received: 0

9600,N,8,1

Log data

```
14:33:16 - Program started
14:33:41 - Connecting to: 192.168.1.157
14:33:41 - Connect result: OK
```

Selected Device IP address: 192.168.1.157   ☐ HTTPS

Username: admin   Password: 1111

Selected Device IP address: The module’s IP address. If it is not in the same network with the module, it is also possible to add the DNS name with the necessary parameters. If you want to connect through mobile internet, enter the mobile internet IP address that you can find on the module’s web-based interface.

Username: The username of the module administrator.

Password: The password of the user.

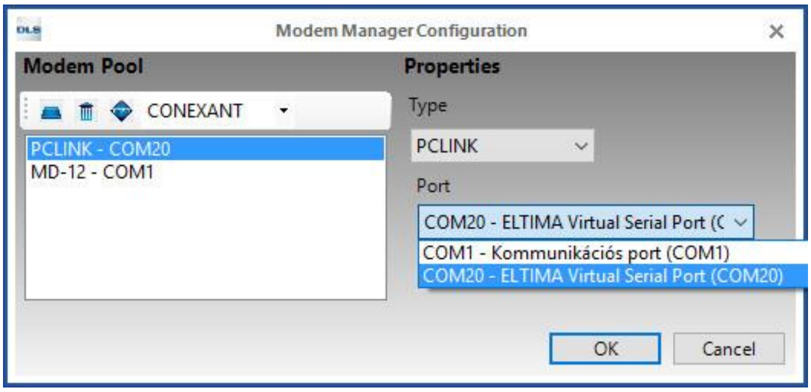
Check connection: Checks the module’s address you set.

Serial Port: Set the virtual serial port’s address that you need to select in the alarm system’s programming software.

Create port: Creates the virtual port according to the settings.

Log data: It provides information on the operation of the program, and displays data received on the serial port.

In the DLS 5 programming software, select the virtual serial port, then connect to the control panel (see below).



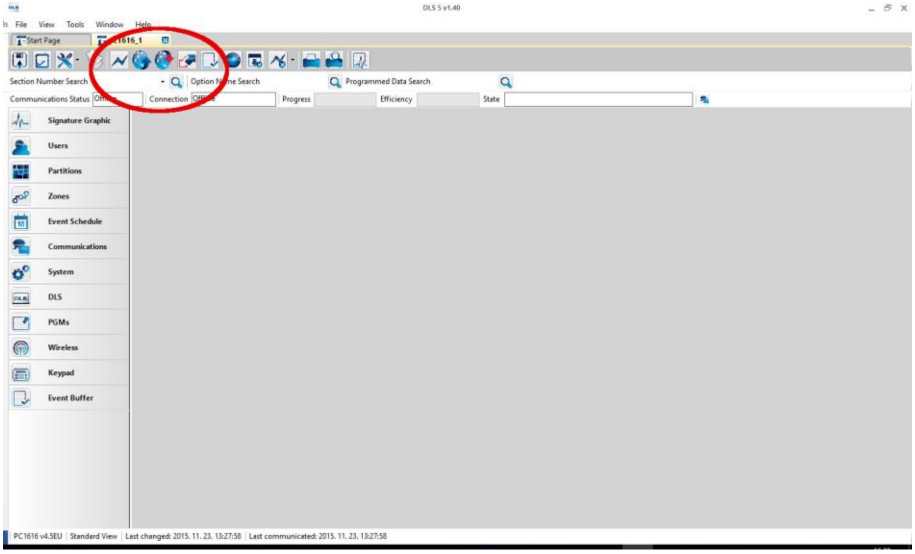
PCLINK - COM20
MD-12 - COM1

Type: PCLINK

Port: COM20 - ELTIMA Virtual Serial Port (C

COM1 - Kommunikációs port (COM1)
COM20 - ELTIMA Virtual Serial Port (COM20)

Select serial port

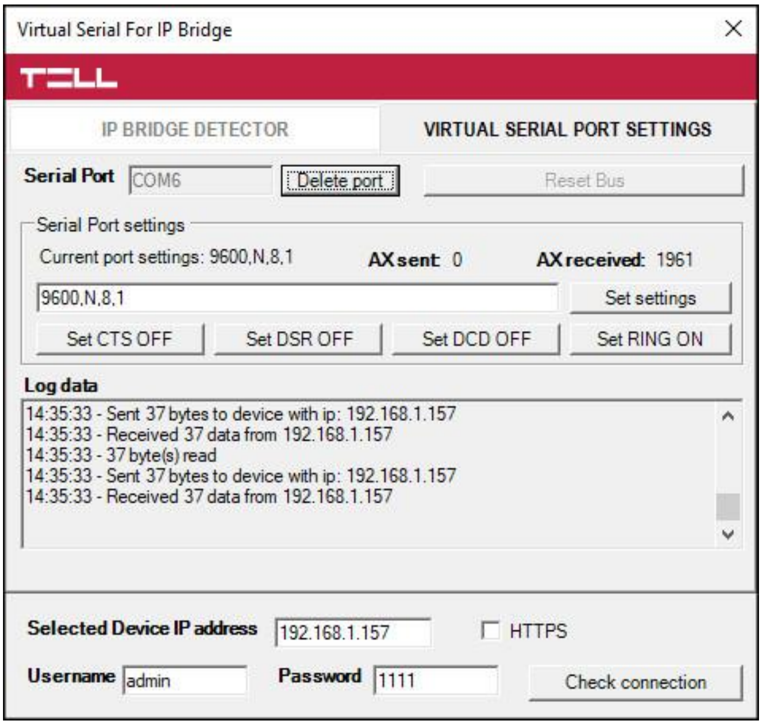


Communications Status: Offline
Connection: Offline

PC1616 v4.5EU | Standard View | Last changed: 2015. 11. 23. 13:27:58 | Last communicated: 2015. 11. 23. 13:27:58

Connecting

The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



Serial Port: COM6

Serial Port settings

Current port settings: 9600,N,8,1 AX sent: 0 AX received: 1961

9600,N,8,1

Log data

```
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
14:35:33 - 37 byte(s) read
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
```

Selected Device IP address: 192.168.1.157 ☐ HTTPS

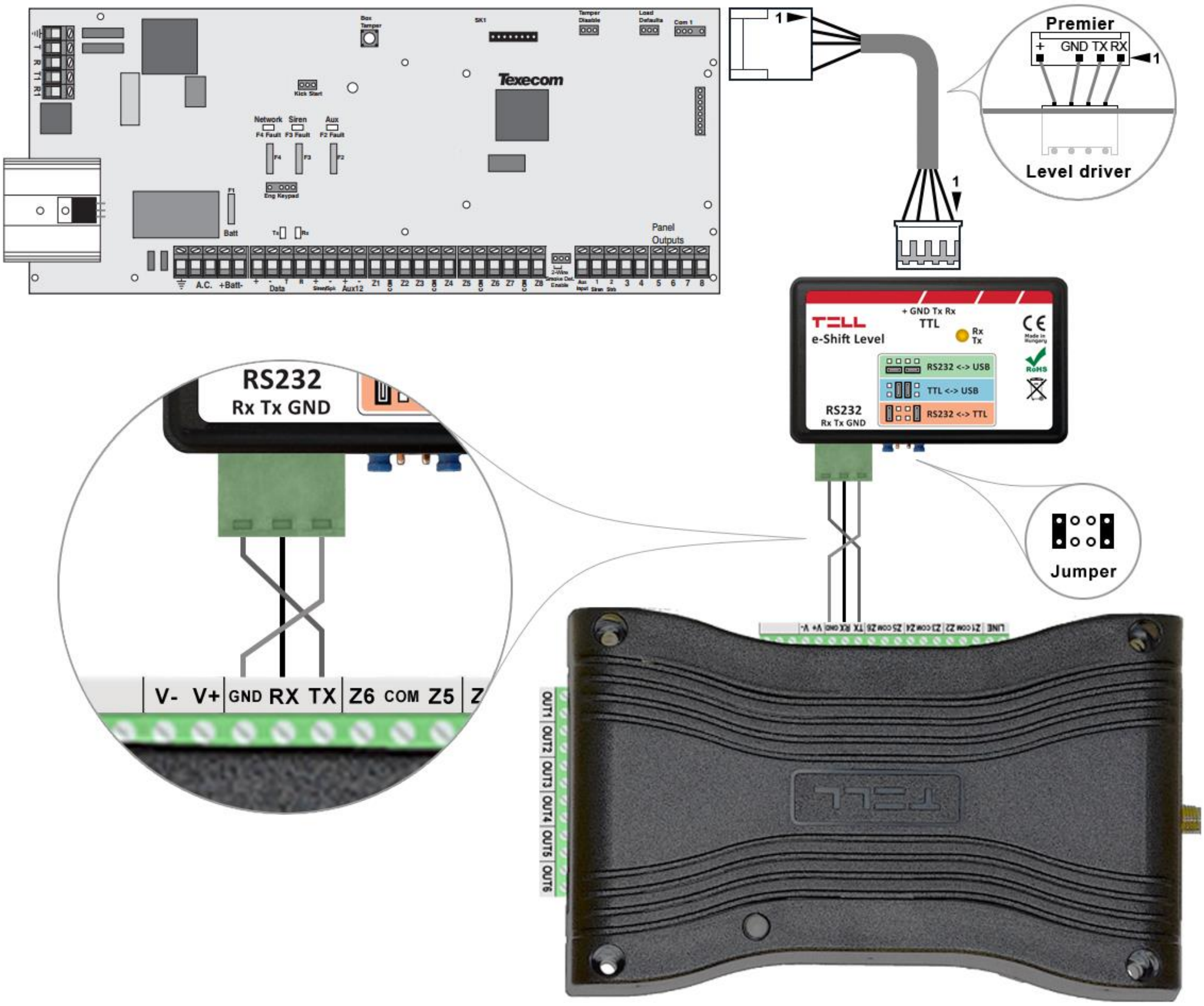
Username: admin Password: 1111

Connection established

When you finished with programming, press the **Delete port** button to close the connection and the virtual serial port.

11.1.3 Premier and Premier Elit alarm control panel

Installation settings:

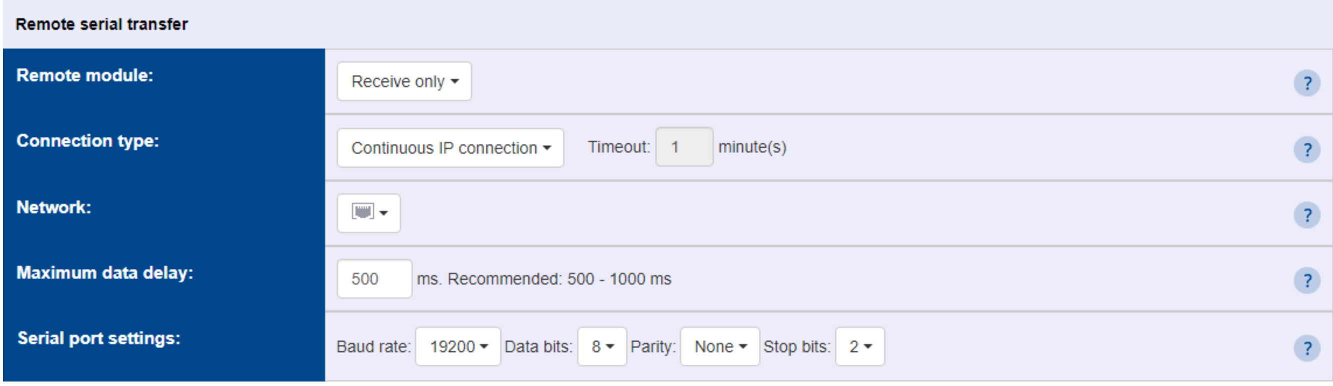


Wiring diagram for Premier alarm systems

Connect a programming cable to the alarm control panel, then connect its serial port output with the module (see figure above). Only RX, TX and GND wires will be used, please connect these to the module in the order shown in the figure above.

Software settings:

Open the module's web interface, set the data for the serial port operation in the **Remote Modules** menu as shown below:



Remote serial transfer

Remote module:	Receive only ▾	?
Connection type:	Continuous IP connection ▾ Timeout: 1 minute(s)	?
Network:	▾	?
Maximum data delay:	500 ms. Recommended: 500 - 1000 ms	?
Serial port settings:	Baud rate: 19200 ▾ Data bits: 8 ▾ Parity: None ▾ Stop bits: 2 ▾	?

Remote serial transfer

Remote module: Select the „Receive only" option from the dropdown list.

Connection type: Select the „Continuous IP connection" option from the dropdown list. By this setting, the connection between the programming software and the alarm control panel will be continuous.

Network: In case the module has a 3G/4G extension panel, the communication channel for transmitting serial data also can be selected here.

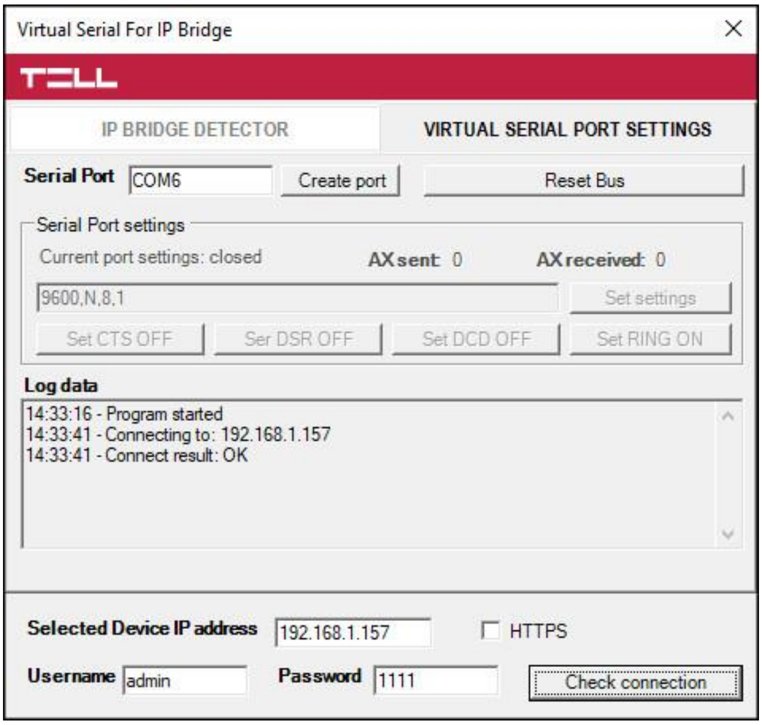
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

Maximum data delay: Recommended setting is 500 ms.

Serial port settings: Recommended settings: Baud rate: 19200, Data bits: 8, Parity: None, Stop bits: 2.

For connecting the alarm control panel and programming software install the IP Bridge Virtual Client software. This software connects the computer and the module and establishes a virtual serial data port that you need to select in the programming software.

After starting the program, the following setting options are available:



Serial Port: COM6

Serial Port settings

Current port settings: closed

AX sent: 0

AX received: 0

9600,N,8,1

Log data

```
14:33:16 - Program started
14:33:41 - Connecting to: 192.168.1.157
14:33:41 - Connect result: OK
```

Selected Device IP address: 192.168.1.157

□ HTTPS

Username: admin

Password: 1111

Selected Device IP address: The module's IP address. If it is not in the same network with the module, it is also possible to add the DNS name with the necessary parameters. If you want to connect through mobile internet, enter the mobile internet IP address that you can find on the module's web-based interface.

Username: The username of the module administrator.

Password: The password of the user.

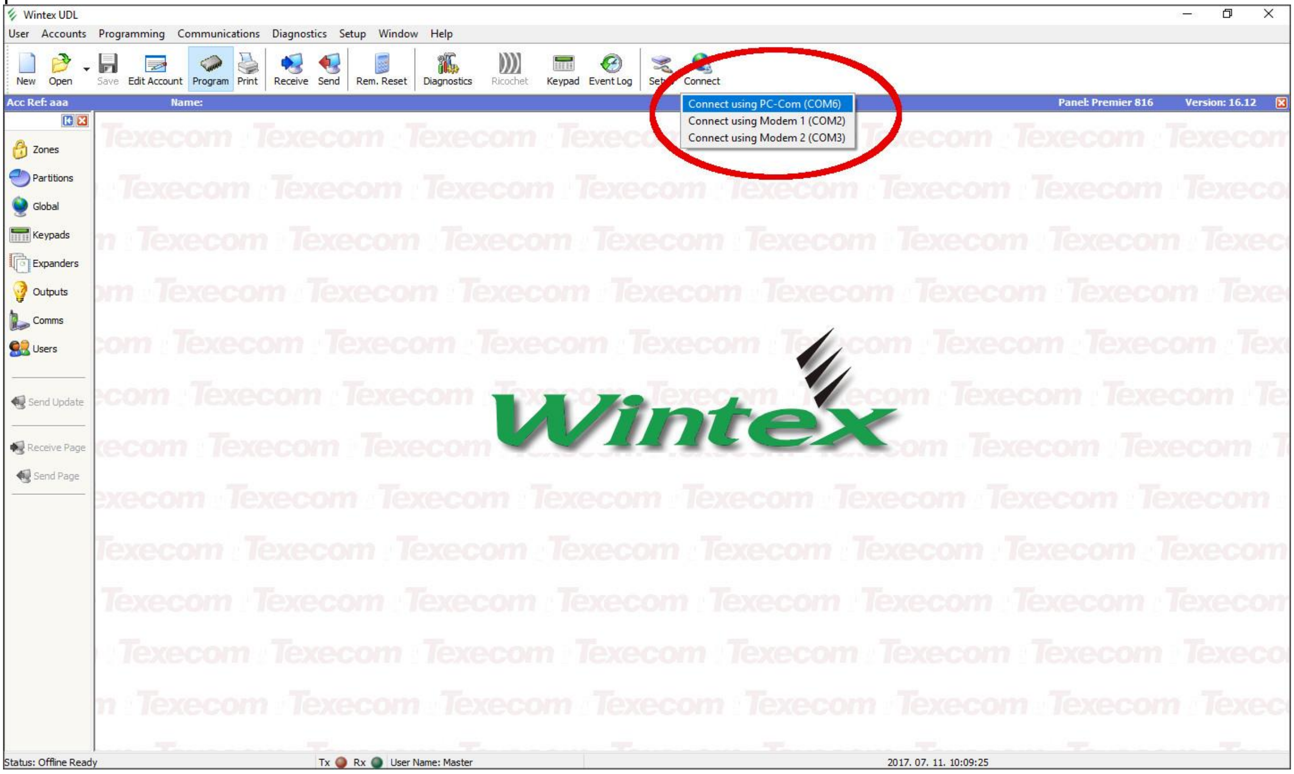
Check connection: Checks the module's address you set.

Serial Port: Set the virtual serial port's address that you need to select in the alarm system's programming software.

Create port: Creates the virtual port according to the settings.

Log data: It provides information on the operation of the program, and displays data received on the serial port.

In the Wintex programming software, select the virtual serial port (figure below), then connect to the control panel.



Acc Ref: aaa Name:

Panel: Premier 816 Version: 16.12

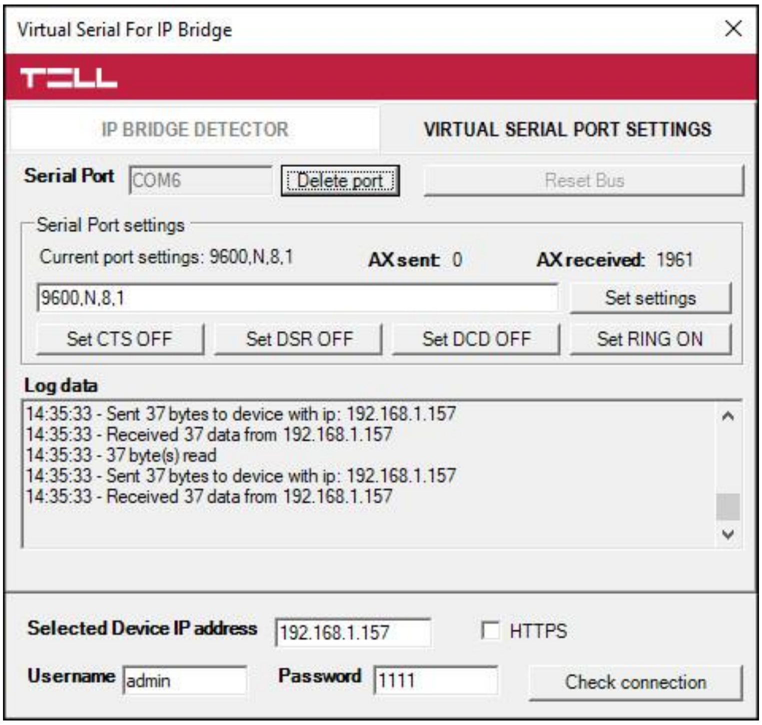
Status: Offline Ready

User Name: Master

2017. 07. 11. 10:09:25

Select serial port

The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



Serial Port: COM6

Current port settings: 9600,N,8,1 AX sent: 0 AX received: 1961

9600,N,8,1

Log data

```
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
14:35:33 - 37 byte(s) read
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
```

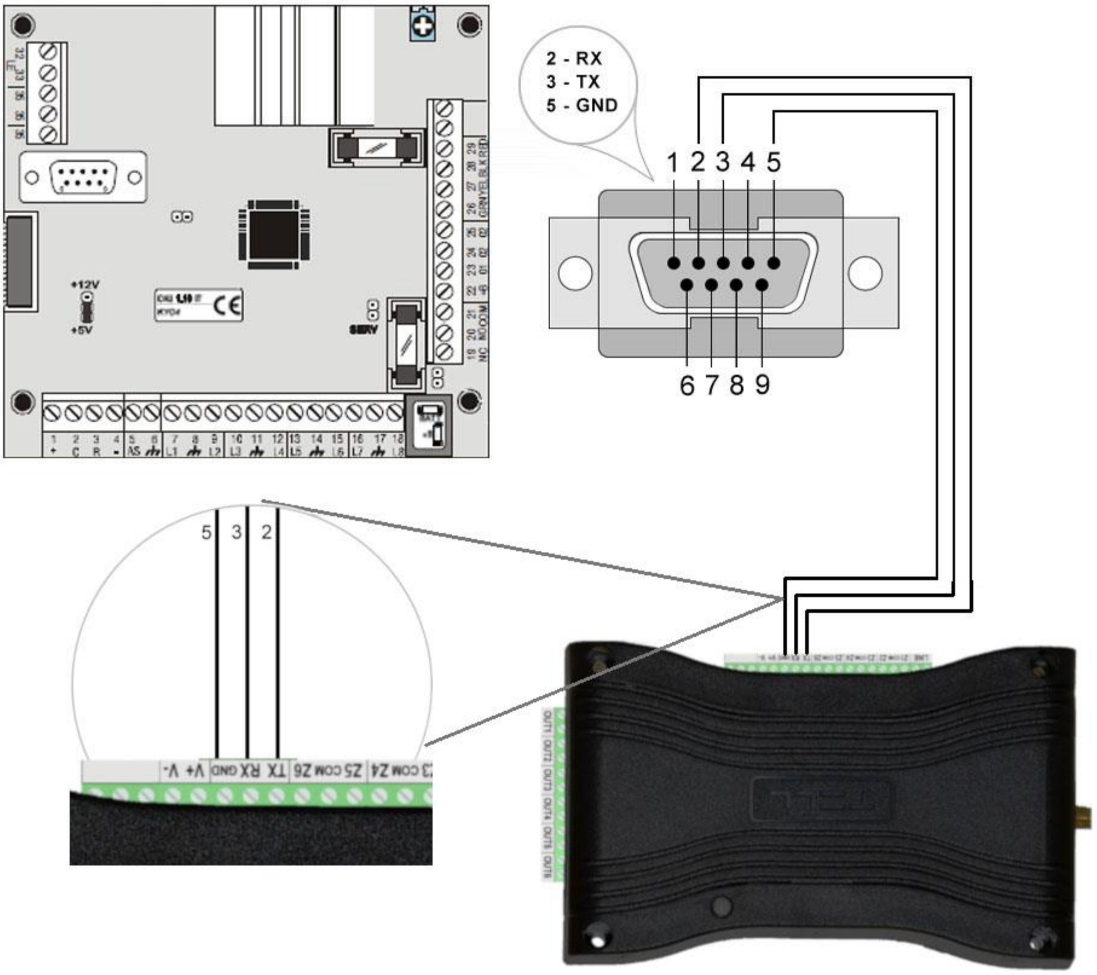
Selected Device IP address: 192.168.1.157 ☐ HTTPS

Username: admin Password: 1111

Connection established

When you finished with programming, press the **Delete port** button to close the connection and the virtual serial port.

11.1.4 Bentel alarm control panel

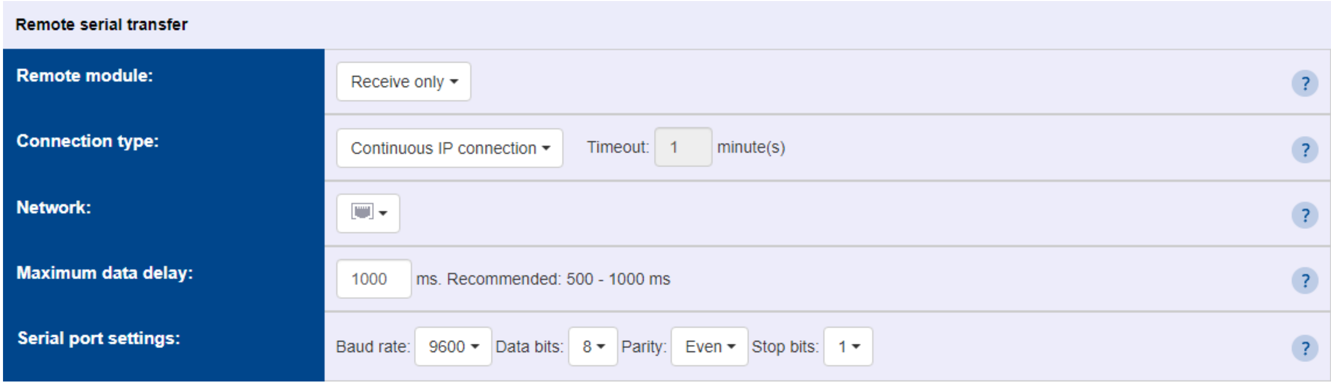


Wiring diagram for Bentel alarm systems

Connect a programming cable to the alarm control panel, then connect its serial port output with the module (see figure above). Only RX, TX and GND wires will be used, please connect these to the module in the order shown in the figure above.

Software settings:

Open the module's web interface, set the data for the serial port operation in the **Remote Modules** menu as shown below:



Remote serial transfer

Remote module:	Receive only
Connection type:	Continuous IP connection; Timeout: 1 minute(s)
Network:	
Maximum data delay:	1000 ms. Recommended: 500 - 1000 ms
Serial port settings:	Baud rate: 9600; Data bits: 8; Parity: Even; Stop bits: 1

Remote serial transfer

Remote module: Select the „Receive only" option from the dropdown list.

Connection type: Select the „Continuous IP connection" option from the dropdown list. By this setting, the connection between the programming software and the alarm control panel will be continuous.

Network: In case the module has a 3G/4G extension panel, the communication channel for transmitting serial data also can be selected here.

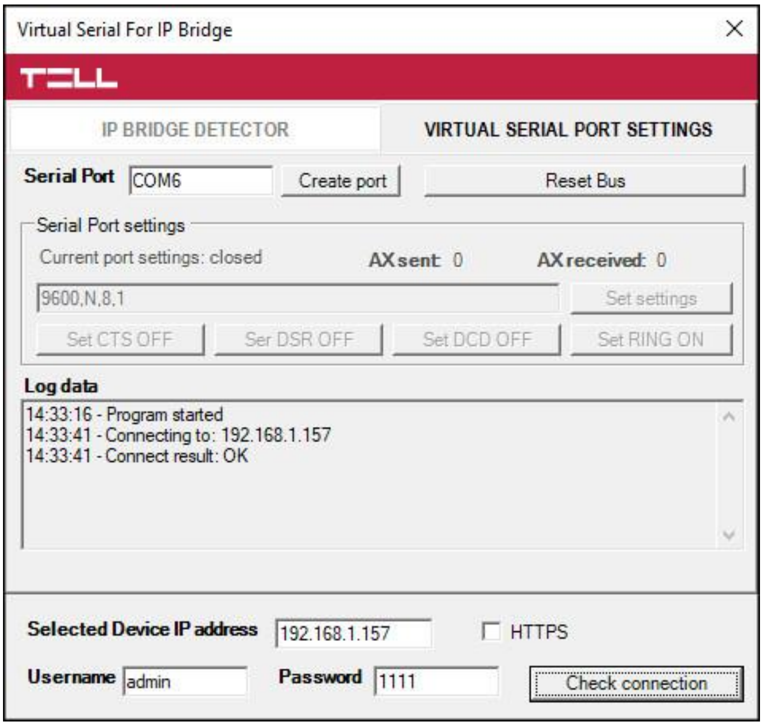
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

Maximum data delay: Recommended setting is 1000 ms.

Serial port settings: Recommended settings: Baud rate: 9600, Data bits: 8, Parity: Even, Stop bits: 1.

For connecting the alarm control panel and programming software install the IP Bridge Virtual Client software. This software connects the computer and the module and establishes a virtual serial data port that you need to select in the programming software.

After starting the program, the following setting options are available:



Virtual Serial For IP Bridge

Serial Port: COM6

Serial Port settings

Current port settings: closed

AX sent: 0

AX received: 0

9600,N,8,1

Log data

```
14:33:16 - Program started
14:33:41 - Connecting to: 192.168.1.157
14:33:41 - Connect result: OK
```

Selected Device IP address: 192.168.1.157

□ HTTPS

Username: admin

Password: 1111

Selected Device IP address: The module's IP address. If it is not in the same network with the module, it is also possible to add the DNS name with the necessary parameters. If you want to connect through mobile internet, enter the mobile internet IP address that you can find on the module's web-based interface.

Username: The username of the module administrator.

Password: The password of the user.

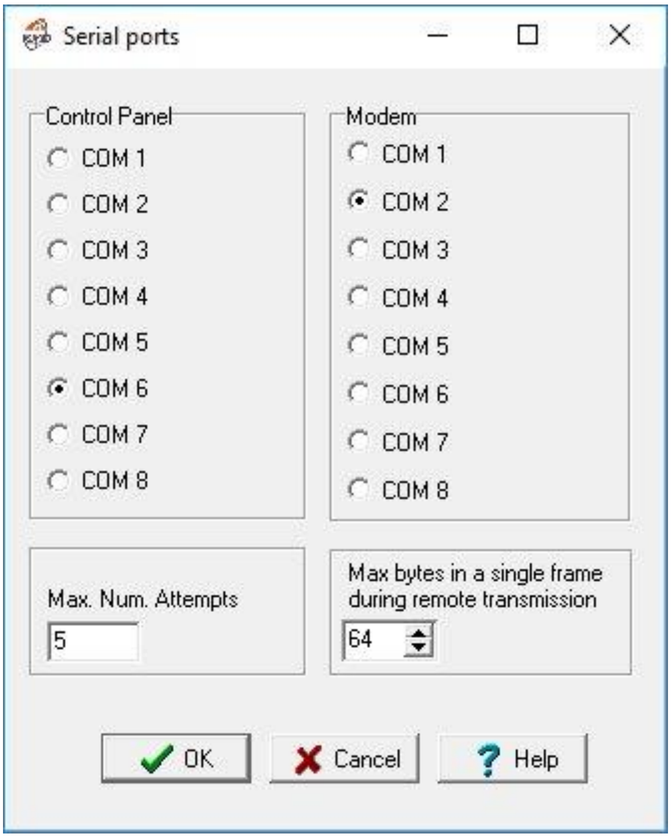
Check connection: Checks the module's address you set.

Serial Port: Set the virtual serial port's address that you need to select in the alarm system's programming software.

Create port: Creates the virtual port according to the settings.

Log data: It provides information on the operation of the program, and displays data received on the serial port.

In the Bentel Security Suite programming software, select the virtual serial port, then connect it to the control panel (figures below).



Control Panel

○ COM 1
○ COM 2
○ COM 3
○ COM 4
○ COM 5
● COM 6
○ COM 7
○ COM 8

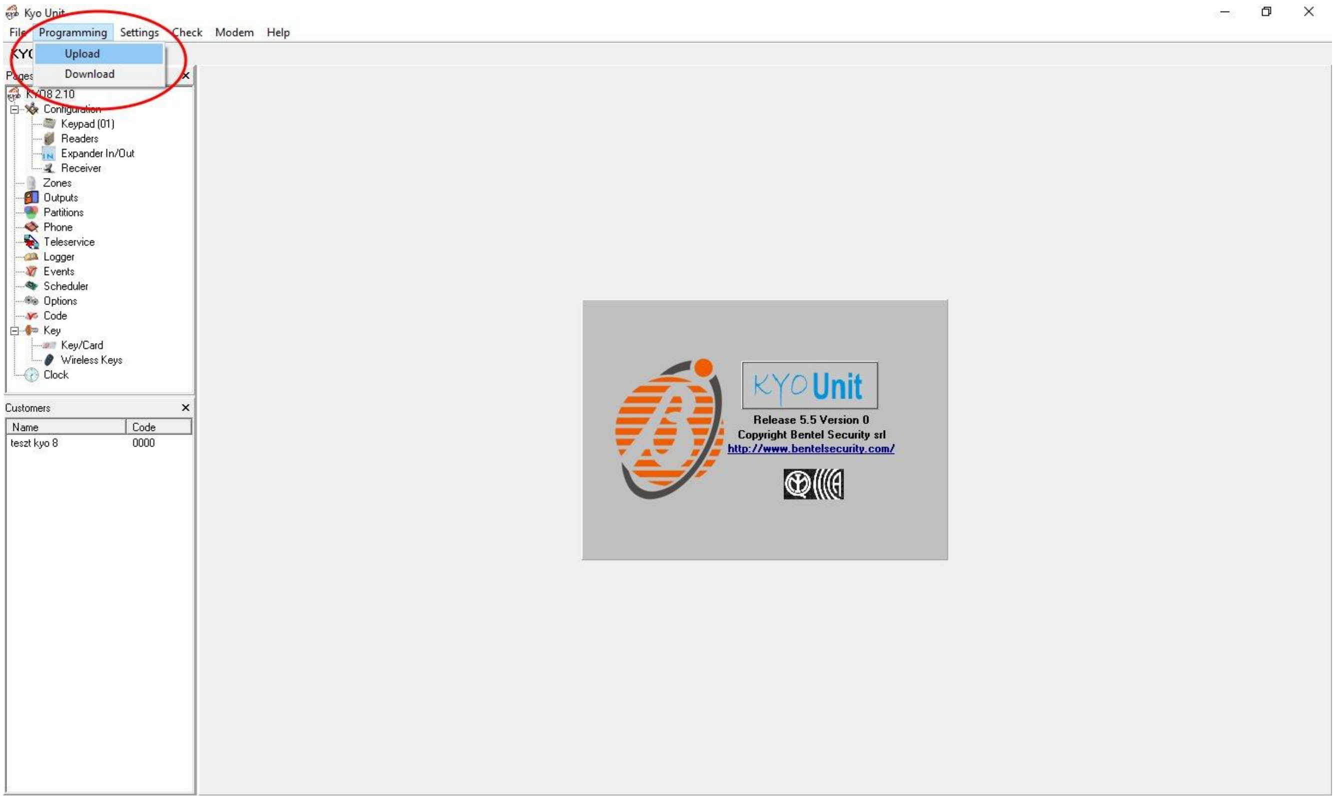
Modem

○ COM 1
● COM 2
○ COM 3
○ COM 4
○ COM 5
○ COM 6
○ COM 7
○ COM 8

Max. Num. Attempts: 5

Max bytes in a single frame during remote transmission: 64

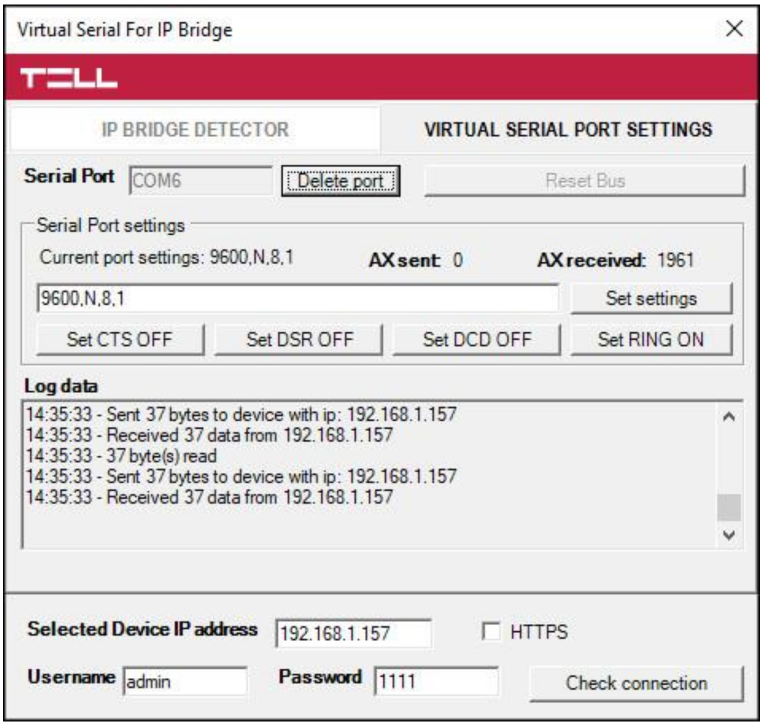
Select serial port



Name	Code
teszt kyo 8	0000

Connecting

The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



Serial Port COM6

Current port settings: 9600,N,8,1 AX sent: 0 AX received: 1961

9600,N,8,1

Log data

```
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
14:35:33 - 37 byte(s) read
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
```

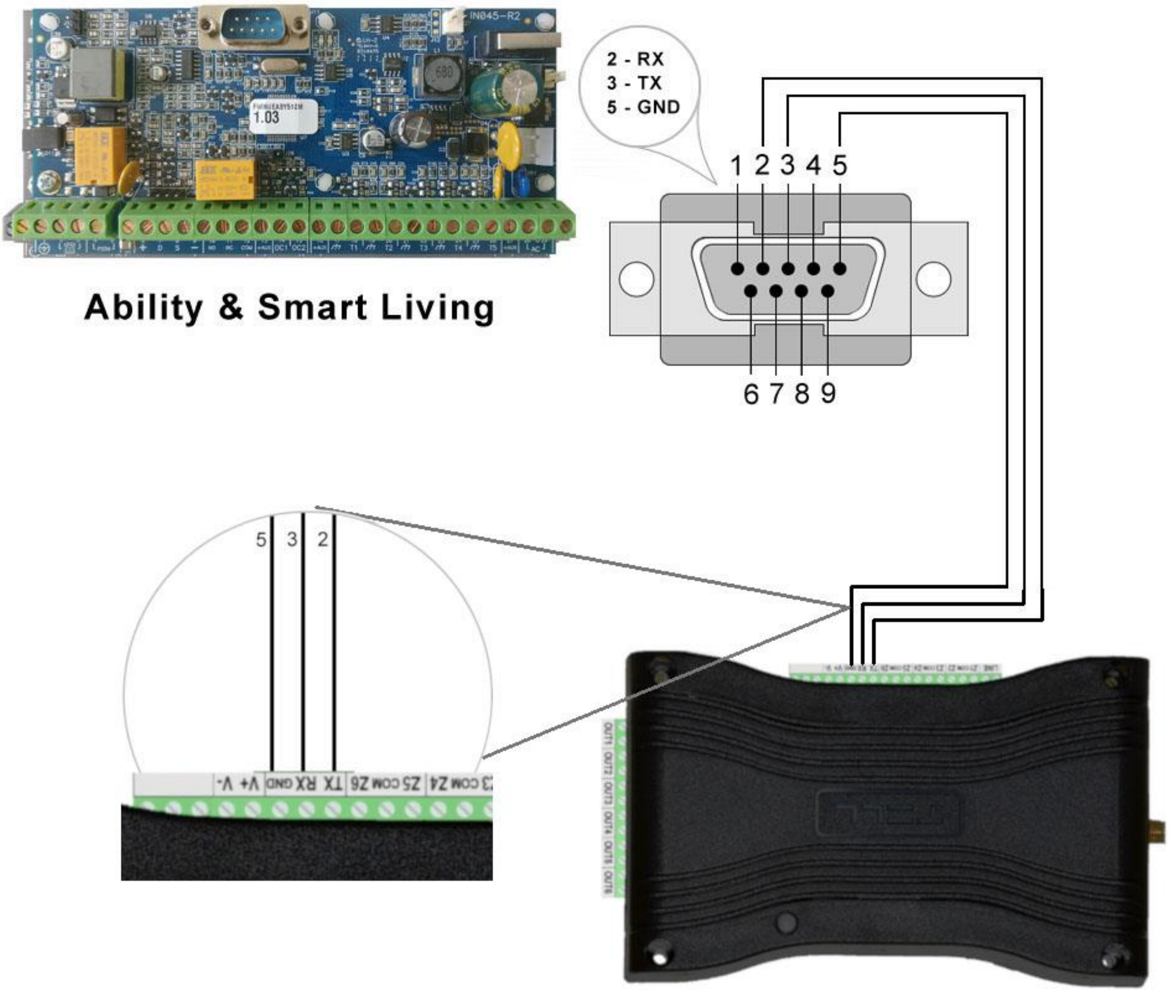
Selected Device IP address 192.168.1.157 ☐ HTTPS

Username admin Password 1111

Connection established

When you finished with programming, press the **Delete port** button to close the connection and the virtual serial port.

11.1.5 Inim alarm control panel

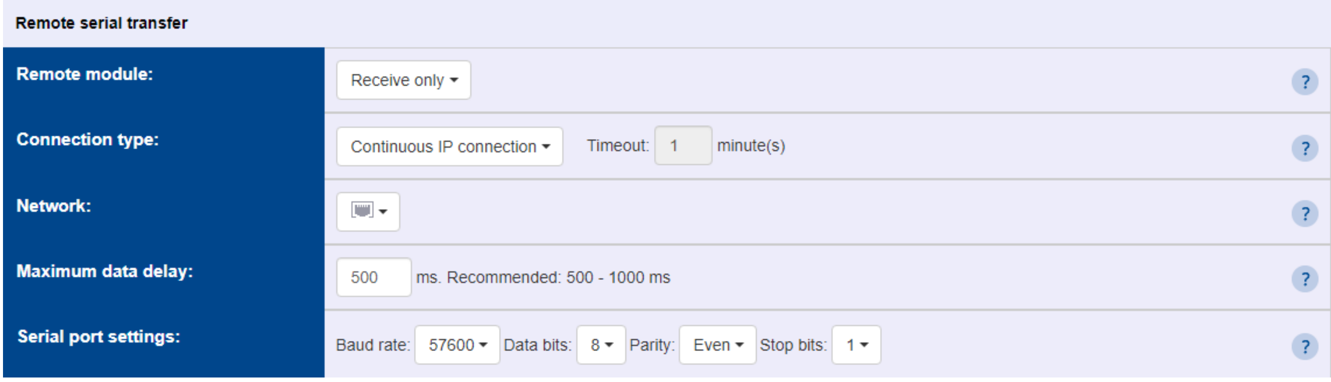


Wiring diagram for Inim alarm systems

Connect a programming cable to the alarm control panel, then connect its serial port output with the module (see figure above). Only RX, TX and GND wires will be used, please connect these to the module in the order shown in the figure above.

Software settings:

Open the module's web interface, set the data for the serial port operation in the **Remote Modules** menu as shown below:



Remote serial transfer

Remote module:	Receive only ▾
Connection type:	Continuous IP connection ▾ Timeout: 1 minute(s)
Network:	▾
Maximum data delay:	500 ms. Recommended: 500 - 1000 ms
Serial port settings:	Baud rate: 57600 ▾ Data bits: 8 ▾ Parity: Even ▾ Stop bits: 1 ▾

Remote serial transfer

Remote module: Select the „Receive only" option from the dropdown list.

Connection type: Select the „Continuous IP connection" option from the dropdown list. By this setting, the connection between the programming software and the alarm control panel will be continuous.

Network: In case the module has a 3G/4G extension panel, the communication channel for transmitting serial data also can be selected here.

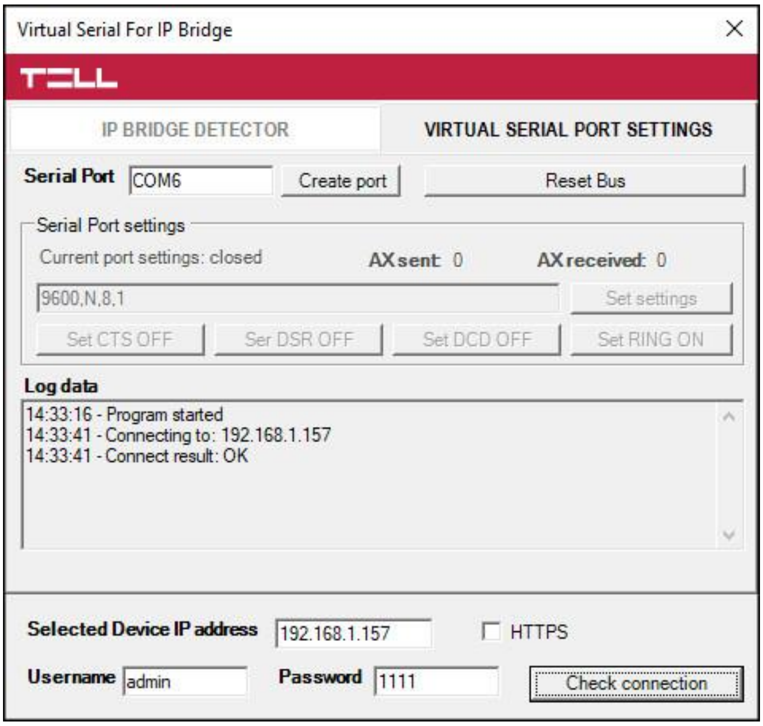
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

Maximum data delay: Recommended setting is 500 ms.

Serial port settings: Recommended settings: Baud rate: 57600, Data bits: 8, Parity: Even, Stop bits: 1.

For connecting the alarm control panel and programming software install the IP Bridge Virtual Client software. This software connects the computer and the module and establishes a virtual serial data port that you need to select in the programming software.

After starting the program, the following setting options are available:



Serial Port: COM6

Serial Port settings

Current port settings: closed AXsent: 0 AXreceived: 0

9600,N,8,1

Log data

```
14:33:16 - Program started
14:33:41 - Connecting to: 192.168.1.157
14:33:41 - Connect result: OK
```

Selected Device IP address: 192.168.1.157 □ HTTPS

Username: admin Password: 1111

Selected Device IP address: The module's IP address. If it is not in the same network with the module, it is also possible to add the DNS name with the necessary parameters. If you want to connect through mobile internet, enter the mobile internet IP address that you can find on the module's web-based interface.

Username: The username of the module administrator.

Password: The password of the user.

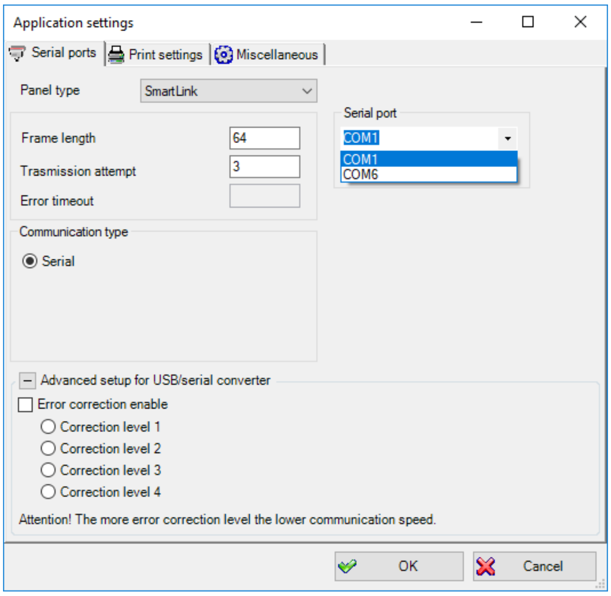
Check connection: Checks the module's address you set.

Serial Port: Set the virtual serial port's address that you need to select in the alarm system's programming software.

Create port: Creates the virtual port according to the settings.

Log data: It provides information on the operation of the program, and displays data received on the serial port.

In the Ability Suite programming software select the virtual serial port within the „Settings/Application settings” menu, then connect to the control panel (see below).



Panel type: SmartLink

Frame length: 64

Trasmission attempt: 3

Error timeout

Serial port: COM1

COM1
COM6

Communication type

● Serial

Advanced setup for USB/serial converter

□ Error correction enable

○ Correction level 1

○ Correction level 2

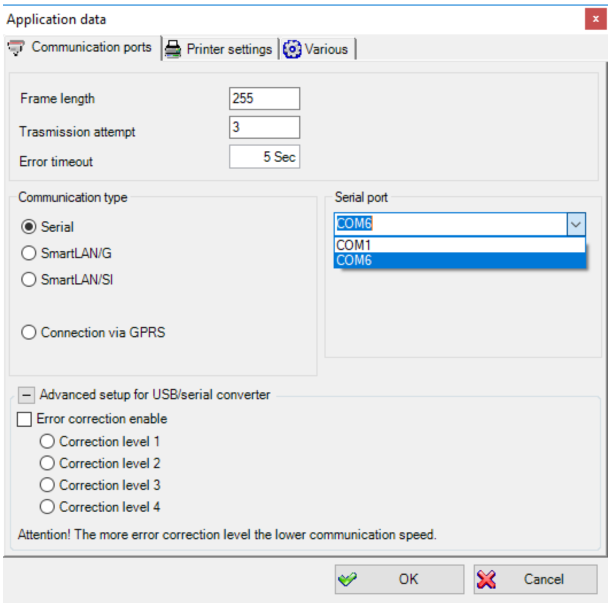
○ Correction level 3

○ Correction level 4

Attention! The more error correction level the lower communication speed.

Select serial port

Example of selecting virtual serial port in Smart League programming software within the „Settings/Application settings” menu (see figure below).



Frame length: 255

Trasmission attempt: 3

Error timeout: 5 Sec

Communication type

● Serial

○ SmartLAN/G

○ SmartLAN/SI

○ Connection via GPRS

Serial port: COM6

COM1
COM6

Advanced setup for USB/serial converter

□ Error correction enable

○ Correction level 1

○ Correction level 2

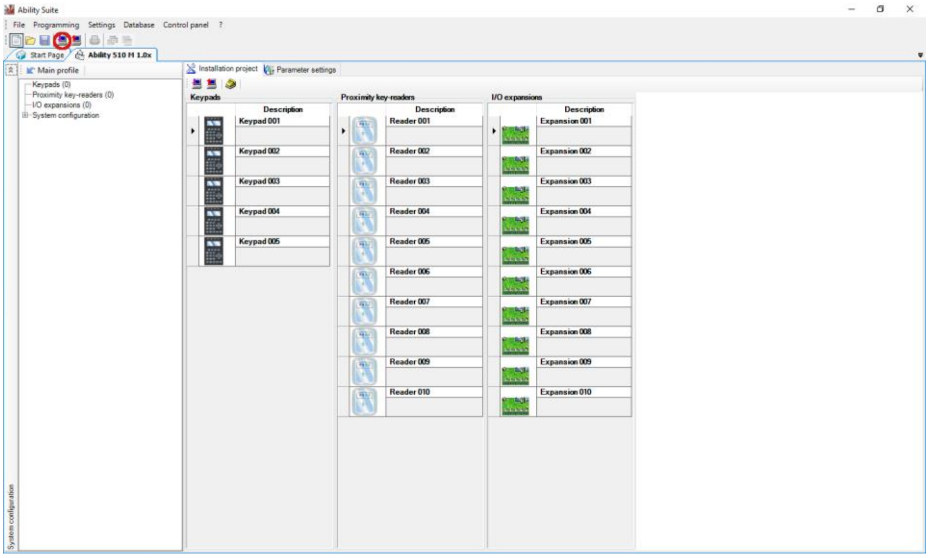
○ Correction level 3

○ Correction level 4

Attention! The more error correction level the lower communication speed.

Select serial port

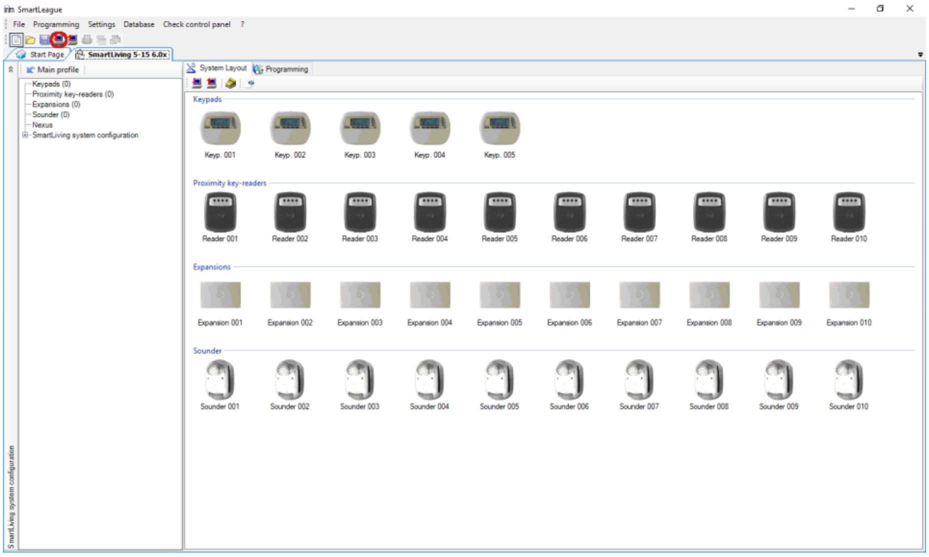
Connecting with Ability Suite programming software:



Keypads	Proximity key-readers	I/O expansions
Description	Description	Description
Keypad 001	Reader 001	Expansion 001
Keypad 002	Reader 002	Expansion 002
Keypad 003	Reader 003	Expansion 003
Keypad 004	Reader 004	Expansion 004
Keypad 005	Reader 005	Expansion 005
	Reader 006	Expansion 006
	Reader 007	Expansion 007
	Reader 008	Expansion 008
	Reader 009	Expansion 009
	Reader 010	Expansion 010

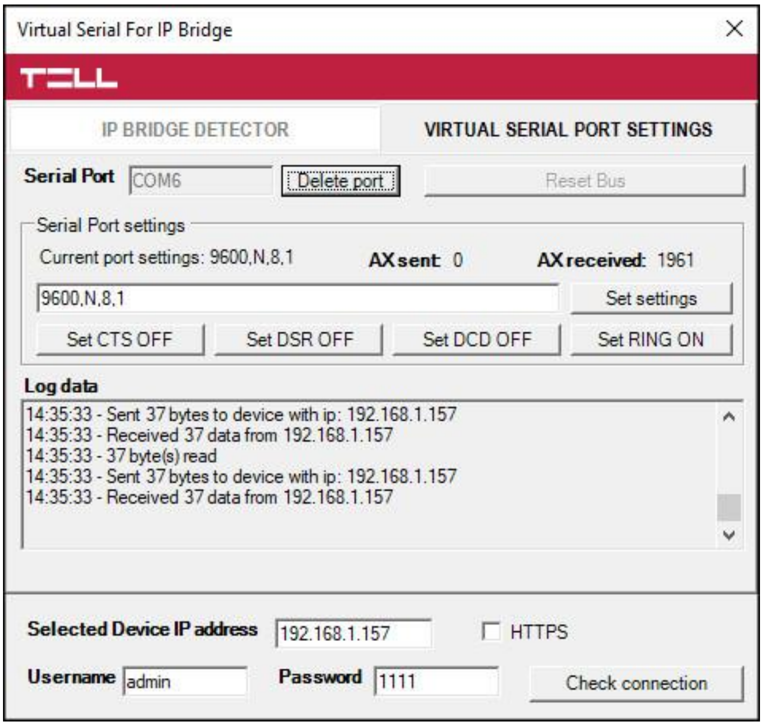
Connecting with Ability Suite

Connecting with Smart League programming software:



Connecting with Smart League

The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



Serial Port: COM6

Current port settings: 9600,N,8,1 AX sent: 0 AX received: 1961

9600,N,8,1

```
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
14:35:33 - 37 byte(s) read
14:35:33 - Sent 37 bytes to device with ip: 192.168.1.157
14:35:33 - Received 37 data from 192.168.1.157
```

Selected Device IP address: 192.168.1.157

Username: admin Password: 1111

Connection established

When you finished with programming, press the **Delete port** button to close the connection and the virtual serial port.

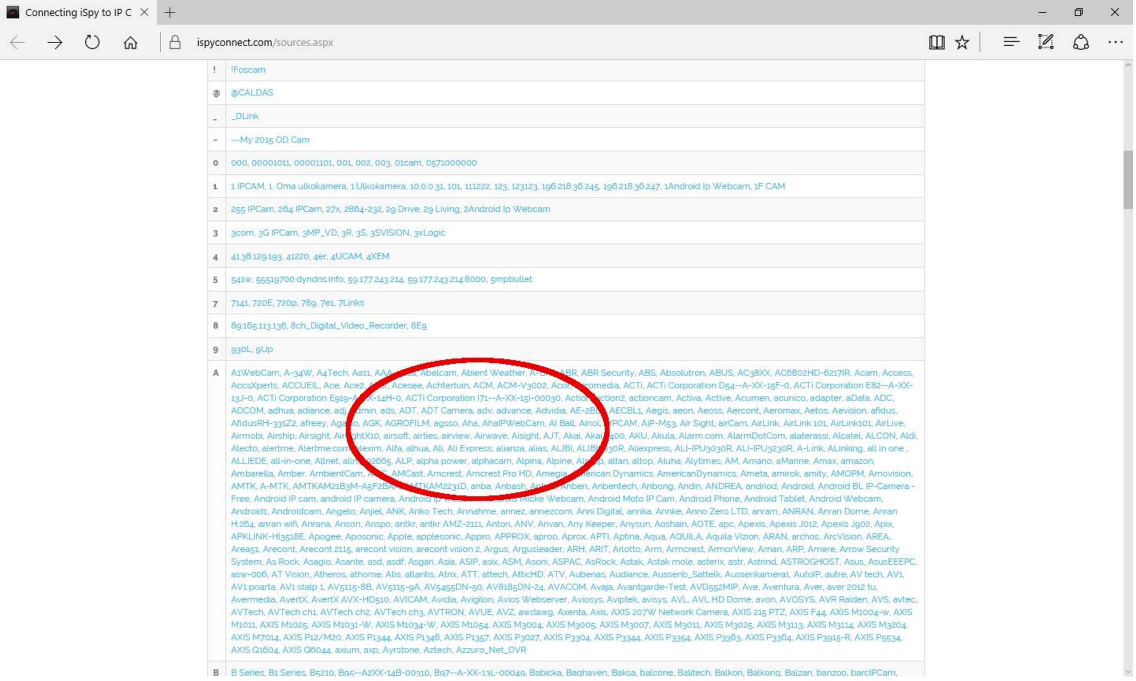
11.2 Camera image and video URL settings

If the camera doesn’t support ONVIF standard or the search tool can’t find it, the image and video URLs need to be set manually. If you do not find this information in the camera description, the following page may help you find the required URLs.

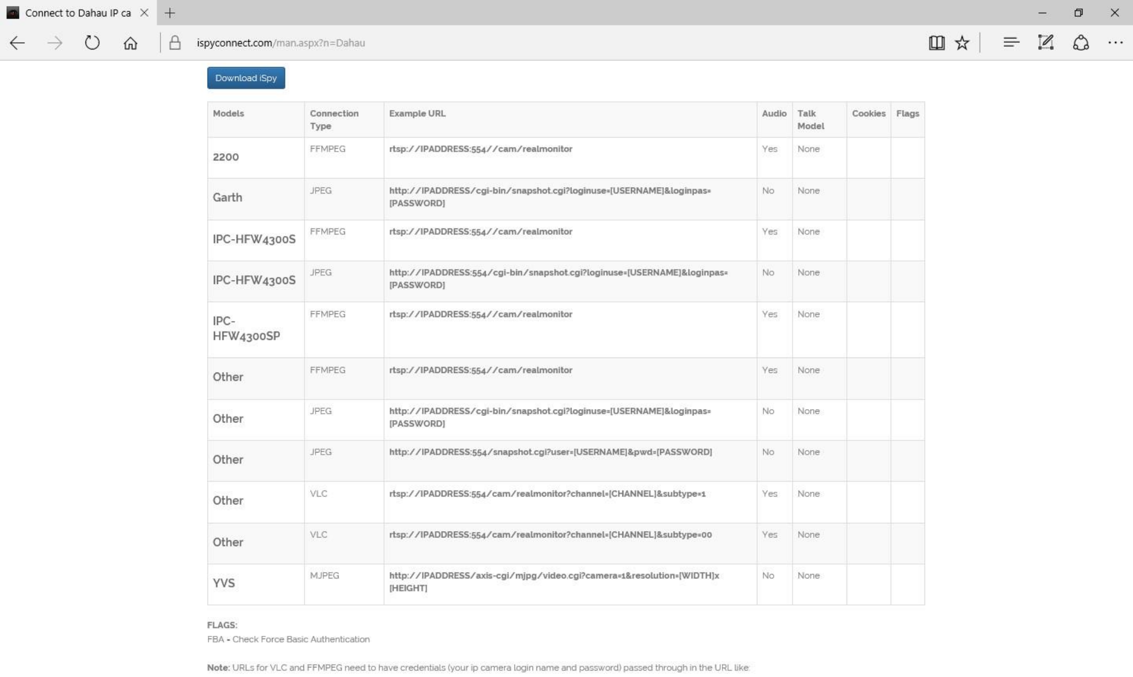
https://www.ispyconnect.com/sources.aspx

Configuration example:

Selecting the manufacturer on the website gives you a list of camera types (figures below). The type is located next to the image and if there’s a stream (rtsp) the sample link is also there.



!	!Foscam
@	@CALDAS
_	_DLink
-	--My 2015 OD Cam
0	000, 00001011, 00001101, 001, 002, 003, 01cam, 0571000000
1	1 IPCAM, 1. Oma ulkokamera, 1.Ulkokamera, 10.0.0.31, 101, 111222, 123, 123123, 196.218.36.245, 196.218.36.247, 1Android Ip Webcam, 1F CAM
2	255 IPCam, 264 IPCam, 27x, 2864-232, 29 Drive, 29 Living, 2Android Ip Webcam
3	3com, 3G IPCam, 3MP_VD, 3R, 3S, 3SVISION, 3xLogic
4	41.38.129.193, 41220, 4er, 4UCAM, 4XEM
5	541w, 55519700.dyndns.info, 59.177.243.214, 59.177.243.214:8000, 5mpbullet
7	7141, 720E, 720p, 789, 7e1, 7Links
8	89.165.113.136, 8ch_Digital_Video_Recorder, 8E9
9	930L, 9Up
A	A1WebCam, A-34W, A4Tech, Aa11, AAA [illegible], Abelcam, Abient Weather, A-[illegible] ABR, ABR Security, ABS, Absolutron, ABUS, AC38XX, AC6802HD-6217IR, Acam, Access, AccsXperts, ACCUEIL, Ace, Ace2, [illegible], Acesee, Achtertuin, ACM, ACM-V3002, Acor [illegible]romedia, ACTi, ACTi Corporation D54--A-XX-15F-0, ACTi Corporation E82--A-XX-13J-0, ACTi Corporation E919-A[illegible]X-14H-0, ACTi Corporation I71--A-XX-15I-00030, Actio[illegible]ction2, actioncam, Activa, Active, Acumen, acunico, adapter, aData, ADC, ADCOM, adhua, adiance, adj[illegible]dmin, ads, ADT, ADT Camera, adv, advance, Advidia, AE-2B[illegible] AECBL1, Aegis, aeon, Aeoss, Aercont, Aeromax, Aetos, Aevision, afidus, AfidusRH-331Z2, afreey, Aga[illegible]o, AGK, AGROFILM, agsso, Aha, AhalPWebCam, AI Ball, Ainol, [illegible]IPCAM, AiP-M53, Air Sight, airCam, AirLink, AirLink 101, AirLink101, AirLive, Airmobi, Airship, Airsight, Air[illegible]ghtX10, airsoft, airties, airview, Airwave, Aisight, AJT, Akai, Akai [illegible]400, AKU, Akula, Alarm.com, AlarmDotCom, alaterassi, Alcatel, ALCON, Aldi, Alecto, alertme, Alertme.com [illegible]lexim, Alfa, alhua, Ali, Ali Express, alianza, alias, ALIBI, ALIBI [illegible]30R, Aliexpress, ALI-IPU3030R, ALI-IPU3230R, A-Link, ALinking, all in one , ALLIEDE, all-in-one, Allnet, alln[illegible]02665, ALP, alpha power, alphacam, Alpina, Alpine, Al[illegible]p, altan, altop, Aluha, Alytimes, AM, Amano, aMarine, Amax, amazon, Ambarella, Amber, AmbientCam, [illegible], AMCast, Amcrest, Amcrest Pro HD, Amegia, [illegible]erican Dynamics, AmericanDynamics, Ameta, amirok, amity, AMOPM, Amovision, AMTK, A-MTK, AMTKAM21B3M-A5F2BA[illegible] AMTKAM2231D, anba, Anbash, [illegible], Anben, Anbentech, Anbong, Andin, ANDREA, andriod, Android, Android BL IP-Camera - Free, Android IP cam, android IP camera, Android Ip [illegible] Micke Webcam, Android Moto IP Cam, Android Phone, Android Tablet, Android Webcam, Android1, Androidcam, Angelo, Anjiel, ANK, Anko Tech, Annahme, annez, annezcom, Anni Digital, annka, Annke, Anno Zero LTD, anram, ANRAN, Anran Dome, Anran H.264, anran wifi, Anrana, Anson, Anspo, antkr, antkr AMZ-2111, Anton, ANV, Anvan, Any Keeper, Anysun, Aoshain, AOTE, apc, Apexis, Apexis J012, Apexis J902, Apix, APKLINK-HI3518E, Apogee, Aposonic, Apple, applesonic, Appro, APPROX, aproo, Aprox, APTI, Aptina, Aqua, AQUILA, Aquila Vizion, ARAN, archos, ArcVision, AREA, Area51, Arecont, Arecont 2115, arecont vision, arecont vision 2, Argus, Argusleader, ARH, ARIT, Arlotto, Arm, Armcrest, ArmorView, Arnan, ARP, Arriere, Arrow Security System, As Rock, Asagio, Asante, asd, asdf, Asgari, Asia, ASIP, asix, ASM, Asoni, ASPAC, AsRock, Astak, Astak mole, asterix, astr, Astrind, ASTROGHOST, Asus, AsusEEEPC, asw-006, AT Vision, Atheros, athome, Atis, atlantis, Atrix, ATT, attech, AtticHD, ATV, Aubenas, Audiance, Aussenb_Sattelk, Aussenkamera1, AutoIP, autre, AV tech, AV1, AV1 poarta, AV1 stalp 1, AV5115-8B, AV5115-9A, AV5455DN-50, AV8185DN-24, AVACOM, Avaja, Avantgarde-Test, AVD552MIP, Ave, Aventura, Aver, aver 2012 tu, Avermedia, AvertX, AvertX AVX-HD510, AVICAM, Avidia, Avigilon, Avios Webserver, Aviosys, Aviptek, avisys, AVL, AVL HD Dome, avon, AVOSYS, AVR Raiden, AVS, avtec, AVTech, AVTech ch1, AVTech ch2, AVTech ch3, AVTRON, AVUE, AVZ, awdawg, Axenta, Axis, AXIS 207W Network Camera, AXIS 215 PTZ, AXIS F44, AXIS M1004-w, AXIS M1011, AXIS M1025, AXIS M1031-W, AXIS M1034-W, AXIS M1054, AXIS M3004, AXIS M3005, AXIS M3007, AXIS M3011, AXIS M3025, AXIS M3113, AXIS M3114, AXIS M3204, AXIS M7014, AXIS P12/M20, AXIS P1344, AXIS P1346, AXIS P1357, AXIS P3027, AXIS P3304, AXIS P3344, AXIS P3354, AXIS P3363, AXIS P3364, AXIS P3915-R, AXIS P5534, AXIS Q1604, AXIS Q6044, axium, axp, Ayrstone, Aztech, Azzuro_Net_DVR
B	B Series, B1 Series, B5210, B95--A2XX-14B-00310, B97--A-XX-13L-00049, Babicka, Baghaven, Baksa, balcone, Balitech, Balkon, Balkong, Balzan, banzoo, barcIPCam,



Models	Connection Type	Example URL	Audio	Talk Model	Cookies	Flags
2200	FFMPEG	rtsp://IPADDRESS:554//cam/realmonitor	Yes	None		
Garth	JPEG	http://IPADDRESS/cgi-bin/snapshot.cgi?loginuse=[USERNAME]&loginpas=[PASSWORD]	No	None		
IPC-HFW4300S	FFMPEG	rtsp://IPADDRESS:554//cam/realmonitor	Yes	None		
IPC-HFW4300S	JPEG	http://IPADDRESS:554/cgi-bin/snapshot.cgi?loginuse=[USERNAME]&loginpas=[PASSWORD]	No	None		
IPC-HFW4300SP	FFMPEG	rtsp://IPADDRESS:554//cam/realmonitor	Yes	None		
Other	FFMPEG	rtsp://IPADDRESS:554//cam/realmonitor	Yes	None		
Other	JPEG	http://IPADDRESS/cgi-bin/snapshot.cgi?loginuse=[USERNAME]&loginpas=[PASSWORD]	No	None		
Other	JPEG	http://IPADDRESS:554/snapshot.cgi?user=[USERNAME]&pwd=[PASSWORD]	No	None		
Other	VLC	rtsp://IPADDRESS:554/cam/realmonitor?channel=[CHANNEL]&subtype=1	Yes	None		
Other	VLC	rtsp://IPADDRESS:554/cam/realmonitor?channel=[CHANNEL]&subtype=00	Yes	None		
YVS	MJPEG	http://IPADDRESS/axis-cgi/mjpg/video.cgi?camera=1&resolution=[WIDTH]x[HEIGHT]	No	None		

FLAGS:
FBA - Check Force Basic Authentication

Note: URLs for VLC and FFMPEG need to have credentials (your ip camera login name and password) passed through in the URL like:

You can substitute the following parameters in the sample link found on this page:

JPEG: http://IPADDRESS/cgi-bin/snapshot.cgi?loginuse=[USERNAME]&loginpas=[PASSWORD]

IPADDRESS: The device's IP address or the DNS name with the necessary parameters

[USERNAME]: The username for login

[PASSWORD]: The password of the user

It's important to note that the module supports Basic authentication, so you can only sign in to those devices that allow this.

Example:

http://192.168.1.240/cgi-bin/snapshot.cgi?loginuse=admin&loginpas=admin

Video: rtsp://IPADDRESS:554//cam/realmonitor

IPADDRESS: The device's IP address or the DNS name with the necessary parameters

Example:

rtsp://192.168.1.240:554//cam/realmonitor

In case of video recorders, it is possible to set in the URL which camera's snapshot or video URL you need.

JPEG: http://IPADDRESS/cgi-bin/snapshot.cgi?chn=[CHANNEL]&u=[USERNAME]&p=[PASSWORD]

IPADDRESS: The device's IP address or the DNS name with the necessary parameters

[CHANNEL]: The index number of the camera

[USERNAME]: The username for login

[PASSWORD]: The password of the user

Example:

http://192.168.1.240/cgi-bin/snapshot.cgi?chn=5&loginuse=admin&loginpas=admin