

IP Bridge / IP Bridge 3G/4G

Remote monitoring IP interface and transmission module

USER MANUAL

for module version V2.1 and newer
Document version: 1.7 17.02.2021



Table of contents

1	Main function of IP Bridge	3
2	System operation	4
3	Wiring	5
4	Setup the alarm control panel	7
5	Installation, setup	8
5.1	Service ports	9
5.2	Router settings.....	9
5.3	Network configuration	9
6	Web based interface of IP Bridge.....	11
6.1	Module status	12
6.2	General settings.....	17
6.3	Servers	22
6.4	Mobile application	25
6.5	Event settings	26
6.6	Remote modules.....	33
6.7	Outputs	34
6.8	Report.....	35
6.9	S.M.A.R.T	35
7	Stopping the module properly	36
8	Restoring factory default settings	36
9	General LED signals	36
10	Technical specification	36
10.1	Generated telephone line specification	36
11	Appendix	37
11.1	Remote programming of alarm control panels	37
11.1.1	Paradox control panel.....	37
11.1.2	DSC alarm control panel.....	41
11.1.3	Premier and Premier Elit alarm control panel	44
11.1.4	Bentel alarm control panel.....	47
11.1.5	Inim alarm control panel	51

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.

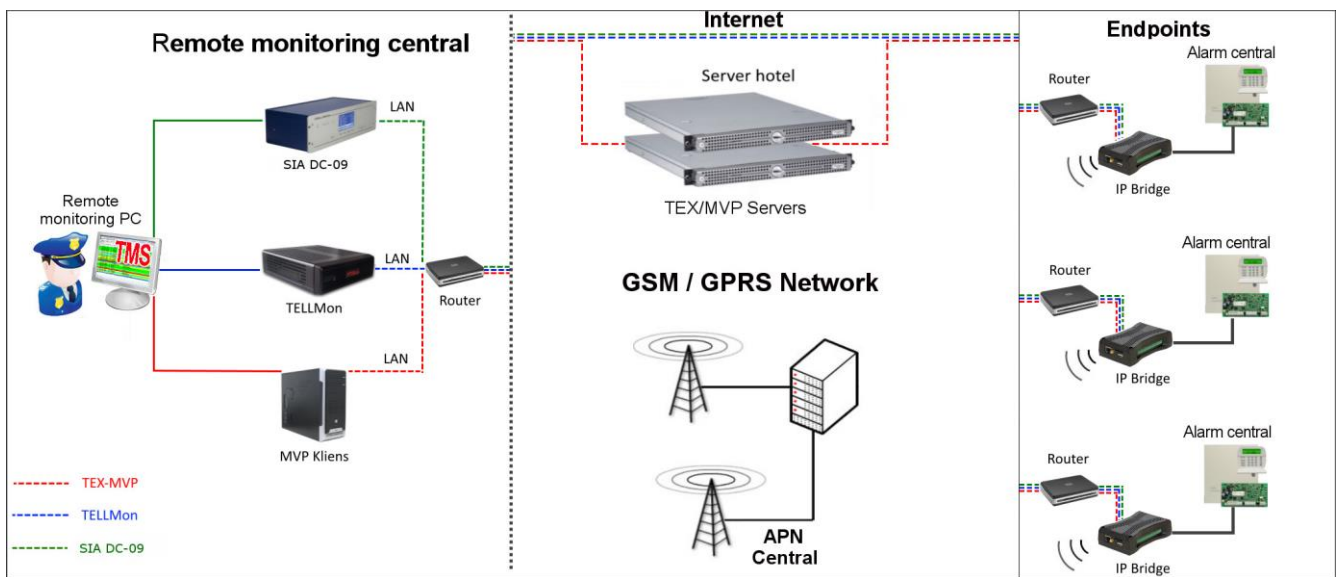
Third party services

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

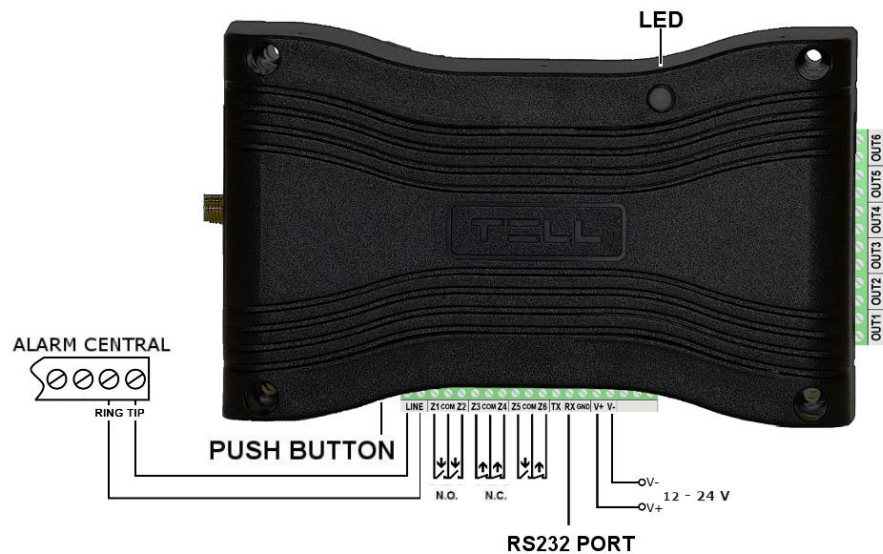
- **Connection with servers/receivers**

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**

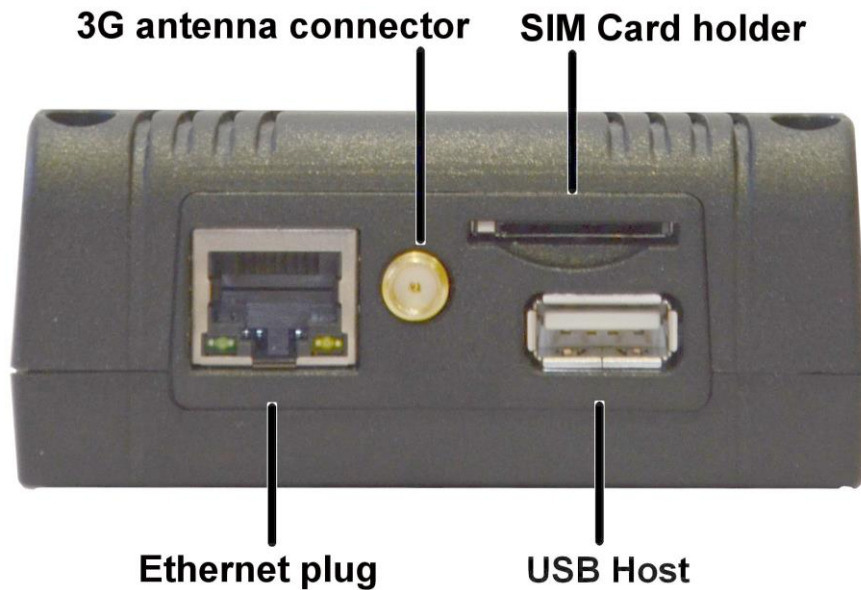
Connect the alarm central's telephone line input to the module's „LINE” terminals.

- **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 figure 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.



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.

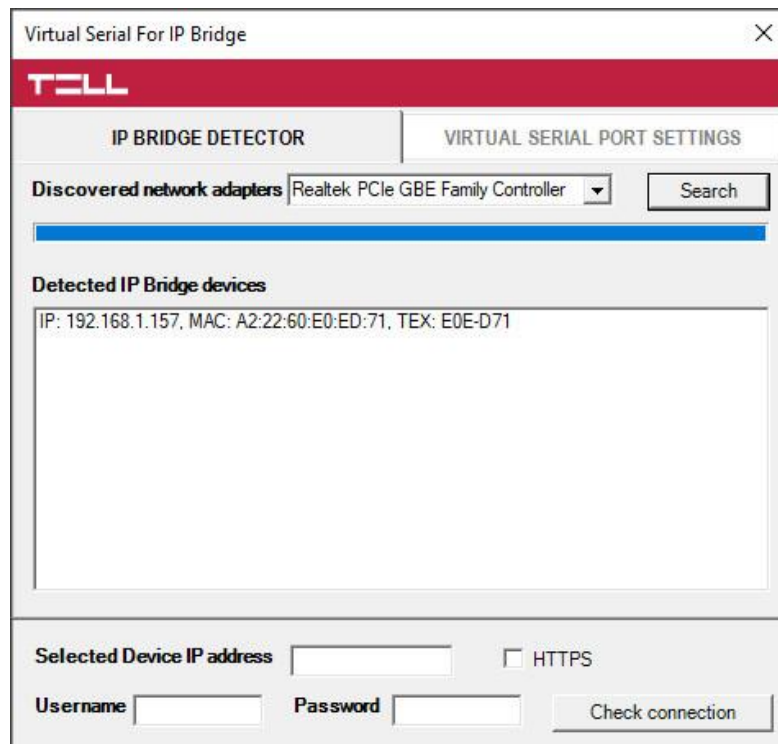
5 Installation, setup

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:



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.

The screenshot shows a web interface for configuring LAN IPv4 settings. On the left, there is a dark blue sidebar with the text "LAN IPv4:". The main area is light blue and contains several configuration fields:

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

At the bottom of the configuration area is a blue button labeled "Set configuration". A small blue question mark icon is visible on the right side of the configuration area.

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.).

Configuration sample:

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

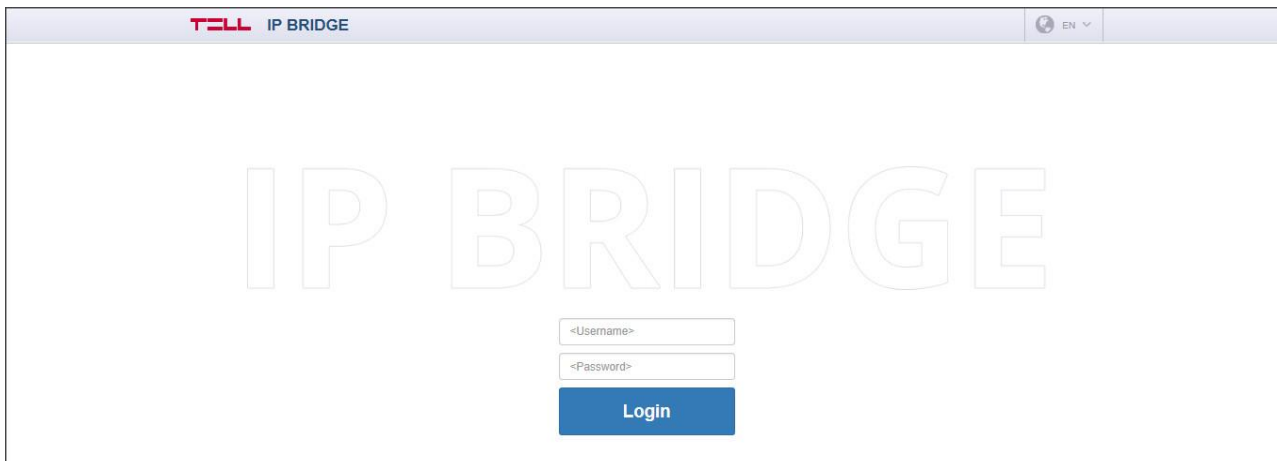
If you want the module to use 192.168.1.115 static IP, the 255.255.255.0 netmask, the 192.168.1.0 subnet, the 192.168.1.1 gateway, the 8.8.8.8 DNS1, the 208.67.220.220 DNS2, the content of the textfile must be as follows:

```
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 interface (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






The screenshot displays the 'Module status' page. At the top, there is a header with system information: Date (3/4/2019, 12:19:09 PM), LAN IP (192.168.2.103), Text ID (7D8-060), Mobilenet signal (Unknown), Line status (OnHook), Mobilenet IP, Supply voltage (23.66 V), External address (-), IMEI (865789023510250), SIM ID, and MAC (A2:22:5C:7D:80:60). Below the header, there are two tabs: 'STATUS' (active) and 'SETTINGS'. The main content area is divided into several sections:


- INPUTS:** Six input cards (INPUT 1 to INPUT 6) are shown, each with a green checkmark and the status 'Idle'.
- OUTPUTS:** Six output cards (OUTPUT 1 to OUTPUT 6) are shown, each with a red minus sign and the status 'Inactive'. Each card has 'Activate' and 'Deactivate' buttons.
- SERVERS:** Six server cards (SERVER 1 to SERVER 6) are shown. SERVER 1 is 'Offline', SERVER 2 is 'Online', and SERVERS 3-6 are 'Not Configured'.
- EVENT LOG:** A table with columns for #, Date, CID, and Cam. Name. It lists 10 events, including connection restores and losses, and periodic tests.

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:

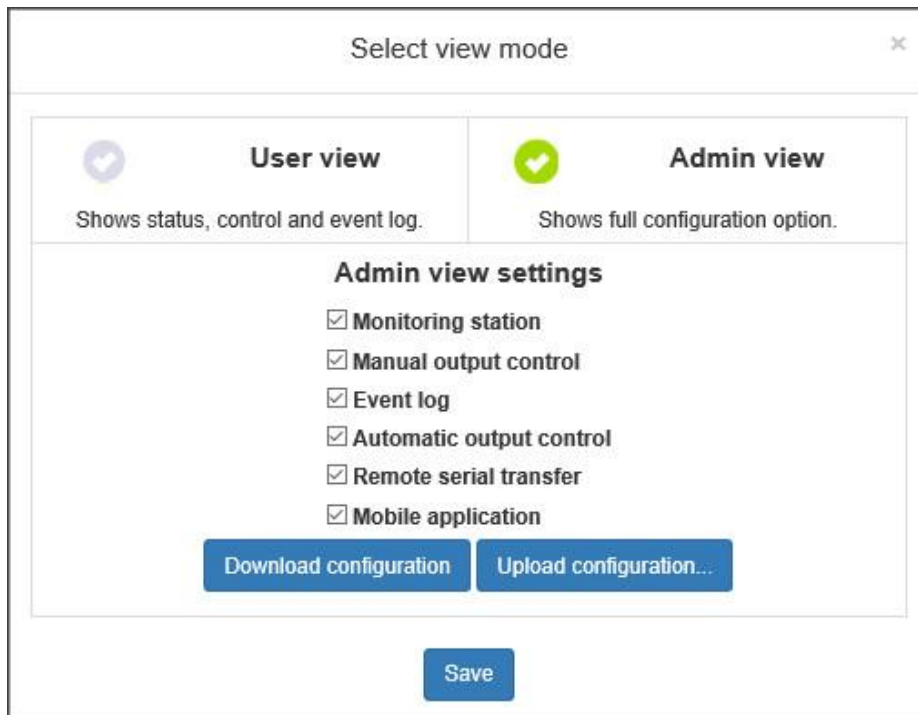
 **Internet connection is OK.** This icon is displayed if the module has a mobile internet IP but no Ping server is set or if there's a Ping server set in the Settings to verify the internet connection and the module can reach it.

 **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



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.



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.

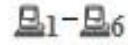
If the module is continuously trying to authenticate, it is likely that bad but existing IP address/port is set or the receiver on the IP address is incompatible with the IP Bridge module.


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

 : indicates whether there was notification sent to the IP address of S1...S6 server/receiver

 : the status of sending emails associated with the event

 : the status of relay control associated with the event

 : indicates whether push message was sent to A1-A4 smart device

#	Date	CID	S1	S2	S3	S4	S5	S6	@	Relay	Q1	Q2	Q3	Q4	Name
1	2017. 11. 27. 12:53:22	2000313001001	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	Input 2 restore
2	2017. 11. 27. 12:53:22	2000113001001	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-	Input 2 alarm
3	2017. 11. 27. 12:53:20	2000313001000	✓	✓	✓	✓	✓	✓	-	-	-	-	-	-	Input 1 restore
4	2017. 11. 27. 12:53:19	2000113001000	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-	Input 1 alarm
5	2017. 11. 27. 12:27:43	1234160200000	-	-	-	-	-	-	-	-	-	-	-	-	Periodic test report
6	2017. 11. 27. 11:57:43	1234160200000	-	-	-	-	-	-	-	-	-	-	-	-	Periodic test report
7	2017. 11. 27. 11:48:42	1234362800000	-	-	-	-	-	-	-	-	-	-	-	-	Program mode exit
8	2017. 11. 27. 11:26:53	1234162700000	-	-	-	-	-	-	-	-	-	-	-	-	Program mode entry
9	2017. 11. 27. 11:26:26	1234362800000	-	-	-	-	-	-	-	-	-	-	-	-	Program mode exit
10	2017. 11. 27. 11:24:55	1234162700000	-	-	-	-	-	-	-	-	-	-	-	-	Program mode entry

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
accountId	2000	9999

Setting changes

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... <input type="checkbox"/> 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 1.

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

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't 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 settings 2.

Allow redirect 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 a monitoring station, email sending or remote serial data transfer. 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.

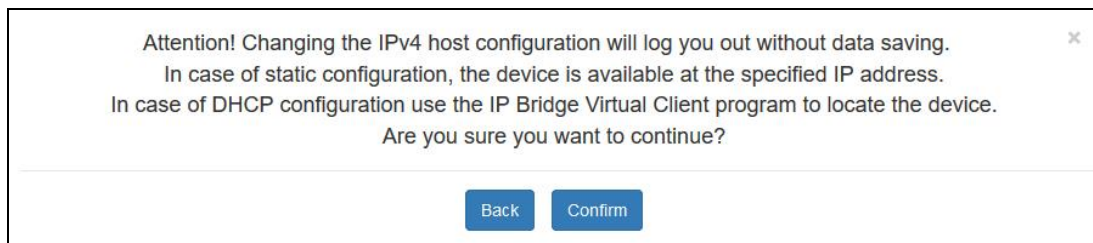
Network mask: The device's subnet mask.

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.



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 out without data saving.



Web server settings

General				
Ping servers:	Server selector:	Internet: Google DNS	Intranet: Custom	Mobile internet: 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 (pos):	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.

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 at all 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 alarm 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.

The screenshot shows the 'General' settings page with a 'Mobile network' section. It includes fields for 'Network selection' (Automatic), 'Connection type' (3G), 'Selected network' (Telenor HU), and a checked 'Roaming' option. Below these is a 'Select mobile network' button. The 'Update server' section has a text input field containing '<https://54.75.242.103:2035>', a 'Default' dropdown, and a 'Test settings' button. The 'Firmware update' section features an 'E-mail addresses for firmware update related notifications:' label, a text input field with '<E-mail addresses>', a dropdown menu set to 'Check and notify updates. (manually download and install)', and 'Hour' and 'Minute' spinners both set to 0. There are also 'Available updates' dropdown, 'Release notes', and 'Update now' buttons. The 'Default settings' section has a 'Factory reset' button.

General settings 3.

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.

The dialog box has a title bar with a close button (X). The main text reads: 'Attention! Factory reset will restart your device. Are you sure you want to continue?'. At the bottom, there are two buttons: 'Back' and 'Confirm'.

Factory reset

6.3 Servers

#	Server name	Server IP	Port	Network	Receiver	Enable test	Test interval
1:	SERVER 1	192.168.1.101	3535	LAN + WAN	TELLMon (TCP)	<input checked="" type="checkbox"/>	90 sec
2:	SERVER 2	192.168.1.102	3545	WAN + LAN	TELLMon (UDP)	<input checked="" type="checkbox"/>	90 sec
3:	SERVER 3	192.168.1.103	3333	LAN	TEX/MVP (TCP)	<input checked="" type="checkbox"/>	90 sec
4:	SERVER 4	192.168.1.104	3537	LAN	TEX/MVP (TCP)	<input checked="" type="checkbox"/>	90 sec
5:	SERVER 5	192.168.1.105	9999	LAN	SIA IP (TCP)	<input checked="" type="checkbox"/>	90 sec
6:	SERVER 6	192.168.1.106	9999	LAN	SIA IP (UDP)	<input checked="" type="checkbox"/>	90 sec

1. Riasztás 2. Servergroup 3. Servergroup 4. Servergroup 5. Servergroup 6. Servergroup

1. servergroup name: Alarm

#	Server	Primary server
1:	1: SERVER 1	<input checked="" type="checkbox"/>
2:	2: SERVER 2	<input type="checkbox"/>

+ ADD MORE

CANCEL SAVE

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:	<input type="text" value="2140"/>	
Account prefix (0-6 hexa):	<input type="text"/>	
Receiver number (0-6 hexa):	<input type="text"/>	
Response timeout (5-60 sec):	<input type="text" value="20"/>	
Max transmission attempt count (1-3 pcs):	<input type="text" value="3"/>	
Connection control period (at least 20 sec):	<input type="text" value="60"/>	
Encryption key (128 bits):	<input type="radio"/> Text format <input checked="" type="radio"/> Hexa format	<input type="password" value="<Password>"/> <input type="password" value="<Password>"/>
<input type="button" value="Save"/>		

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. Alarm 2. Fault 3. Servergroup 4. Servergroup 5. Servergroup 6. Riasztás ?

1. servergroup name:

#	Server	Primary server	
1:	<input type="text" value="1: SERVER 1"/>	<input checked="" type="checkbox"/>	
2:	<input type="text" value="2: SERVER 2"/>	<input type="checkbox"/>	

[+ ADD MORE](#)

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 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 Mobile application

Mobil application

Mobile application server settings

Enable:	<input checked="" type="checkbox"/>	?
Server IP:	<input type="text" value="54.75.242.103"/>	?
Port:	<input type="text" value="2020"/>	?
Network:	<input type="text" value="Default"/> Connection ready	?

?

#	User name	Mobile application ID	Mobile device name	
1:	<input type="text" value="admin"/>	<input type="text" value="530980EB4369A446B13318CF164130B991BC6476"/>	<input type="text" value="samsung SM-A510F"/>	<input type="button" value="QR code"/>
2:	<input type="text" value="<User name>"/>	<input type="text" value="<Mobile application ID>"/>	<input type="text" value="<Mobile device name>"/>	<input type="button" value="QR code"/>
3:	<input type="text" value="<User name>"/>	<input type="text" value="<Mobile application ID>"/>	<input type="text" value="<Mobile device name>"/>	<input type="button" value="QR code"/>
4:	<input type="text" value="<User name>"/>	<input type="text" value="<Mobile application ID>"/>	<input type="text" value="<Mobile device name>"/>	<input type="button" value="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 unique 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.

6.5 Event settings

Events		INPUT PROPERTIES ?				
Event name	Event custom name	INPUT TYPE	EOL	SENSITIVITY (MS)	BYPASS	NOTIFY NEXT
Input 1 alarm	<Input 1>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 1 restore	<Input 1>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 2 alarm	<Input 2>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 2 restore	<Input 2>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 3 alarm	<Input 3>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 3 restore	<Input 3>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
External event: *****	<input type="text"/>				<input type="checkbox"/>	<input checked="" type="checkbox"/> ↓
External event: *401*****	<input type="text"/>				<input type="checkbox"/>	<input checked="" type="checkbox"/> ↓ ↑
External event: *130*****	<input type="text"/>				<input type="checkbox"/>	<input checked="" type="checkbox"/> ↓ ↑
External event: *602*****	<input type="text"/>				<input type="checkbox"/>	<input checked="" type="checkbox"/> ↑
+ 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.

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.

Periodic test report

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 extension 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.

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

<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Type + Code</div> <div style="display: flex; justify-content: space-between;"> Type <input type="text" value="*"/> </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Event name</div> <div style="display: flex; justify-content: space-between;"> Code <input type="text" value="***"/> </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Partition</div> <div style="text-align: center;"><input type="text" value="**"/></div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Zone</div> <div style="text-align: center;"><input type="text" value="***"/></div> </div>
---	--	---	---

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

i

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 Save

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):

<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Type + Code</div> <div style="display: flex; justify-content: space-between;"> Type <input type="text" value="*"/> </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="text-align: center; font-weight: bold; font-size: small;">Event name</div> <div style="display: flex; justify-content: space-between;"> Code <input type="text" value="60*"/> </div> </div>
---	--

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/delete 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:

Events		INPUT PROPERTIES ?				
Event name	Event custom name	INPUT TYPE	EOL	SENSITIVITY (MS)	BYPASS	NOTIFY NEXT
Input 1 alarm	<Input 1>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 1 restore	<Input 1>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 2 alarm	<Input 2>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 2 restore	<Input 2>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 3 alarm	<Input 3>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	
Input 3 restore	<Input 3>	NO	<input type="checkbox"/>	200	<input type="checkbox"/>	

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 occurred.

Notify 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.

Configuration example:

We'd like to receive notification about open, close and burglary 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*****	<input type="checkbox"/>	<input checked="" type="checkbox"/>	↓
External event: †130*****	<input type="checkbox"/>	<input checked="" type="checkbox"/>	↓ ↑
External event: *****	<input type="checkbox"/>	<input checked="" type="checkbox"/>	↑

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:

Event name	Event custom name	CID CODE	PARTITION	ZONE
Input 1 alarm	IN1 alarm	130	01	001
Input 1 restore	IN1 restore	130	01	001
Input 2 alarm	IN2 alarm	130	01	002
Input 2 restore	IN2 restore	130	01	002
Input 3 alarm	IN3 alarm	130	01	003
Input 3 restore	IN3 restore	130	01	003

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:

Event name	Event custom name	ENABLE REPORTING	SERVER GROUP
IN1 alarm		<input checked="" type="checkbox"/>	1. Alarm
IN1 restore		<input checked="" type="checkbox"/>	1. Alarm
IN2 alarm		<input checked="" type="checkbox"/>	1. Alarm
IN2 restore		<input checked="" type="checkbox"/>	1. Alarm
IN3 alarm		<input checked="" type="checkbox"/>	1. Alarm
IN3 restore		<input checked="" type="checkbox"/>	1. Alarm

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 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 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.



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>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Zone 1. in alarm!	
Input 1 restore	<Input 1>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Input 2 alarm	<Input 2>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Zone 2. in alarm!	
Input 2 restore	<Input 2>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Input 3 alarm	<Input 3>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Zone 3. in alarm!	
Input 3 restore	<Input 3>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

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.

6.6 Remote modules

Remote module settings

In this module version, transparent serial data transmission can be executed, but only between the module and the IP Bridge Virtual Client program. The serial port settings can be modified here.

Remote module: The 'Receive only' is the only option to choose. In this case the module can communicate only with the IP Bridge Virtual Client to execute the transparent serial data transmission.

Serial port settings: In this section the serial port settings can be modified according to the connection type.

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

6.7 Outputs

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: In this module version, you can control the module's local outputs.

Output: Select the output's 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 control 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.

6.8 Report

Report

Report frequency: Daily Hour: 0 Minute: 0 Send report now

E-mail addresses: <E-mail addresses> Test e-mail address(es)

Events: Custom: New event: Restore: External: New event: Restore:

CANCEL SAVE

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.

6.9 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 data

Displays the SD card's S.M.A.R.T data. 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 microswitch 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 occurred / 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:	-20°C - +70°C
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

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:	[Network Icon] ▾ ?
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.

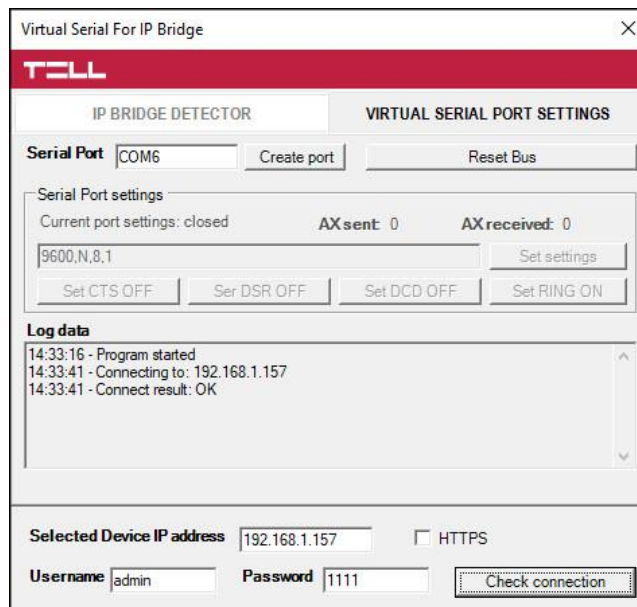
Maximum data delay: Recommended setting is 500 ms.

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:



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.

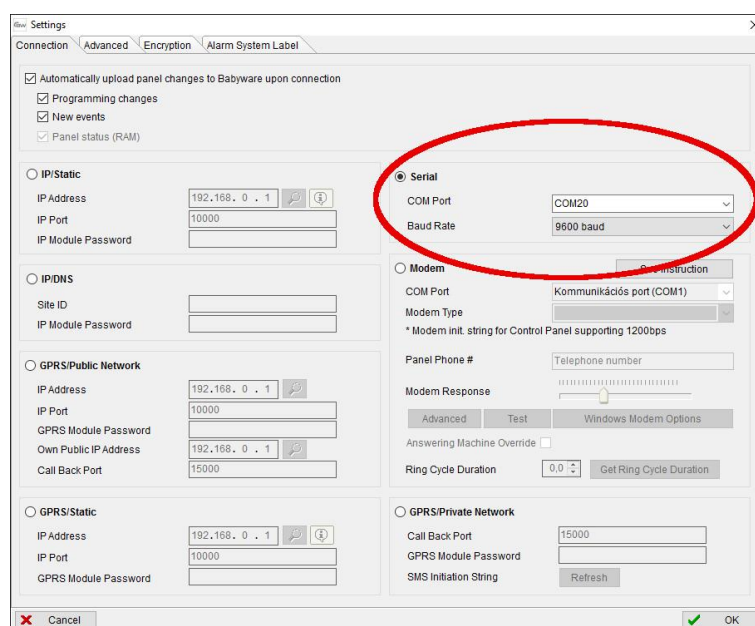
Check connection: Checks the module's address you set.

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

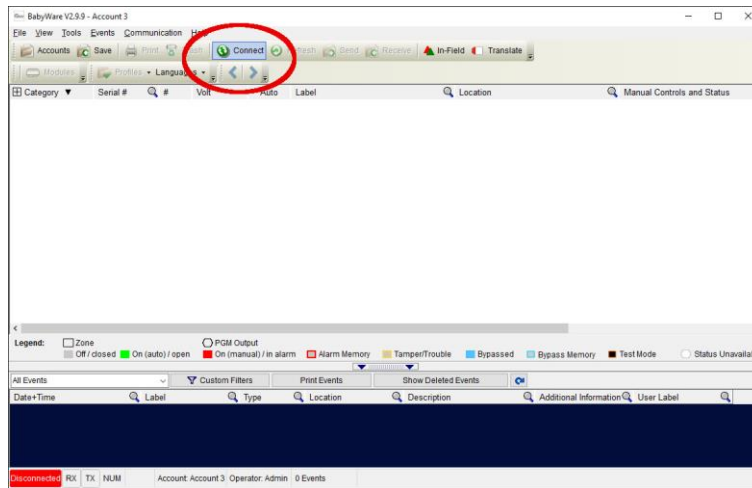
Create port: Creates the virtual port according to the settings.

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).

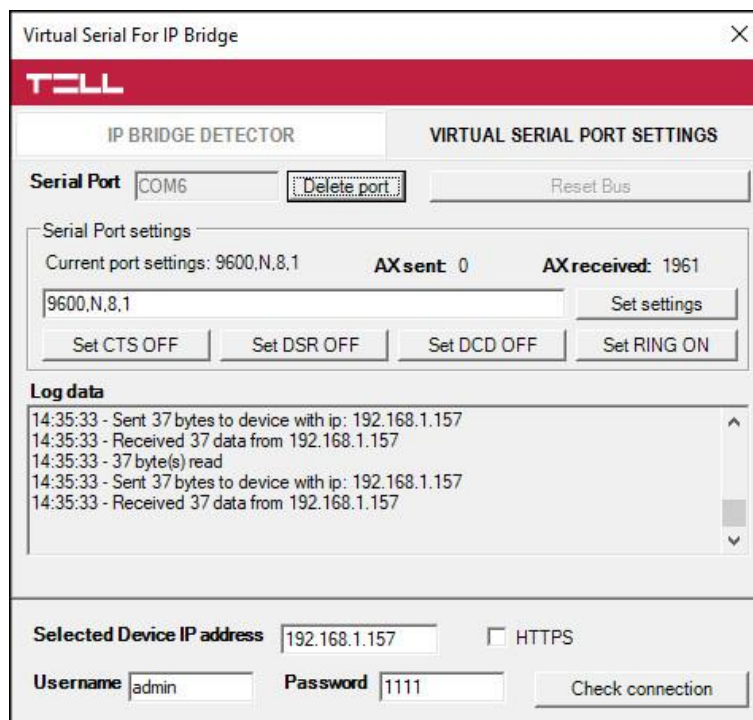


Select serial port



Connecting

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

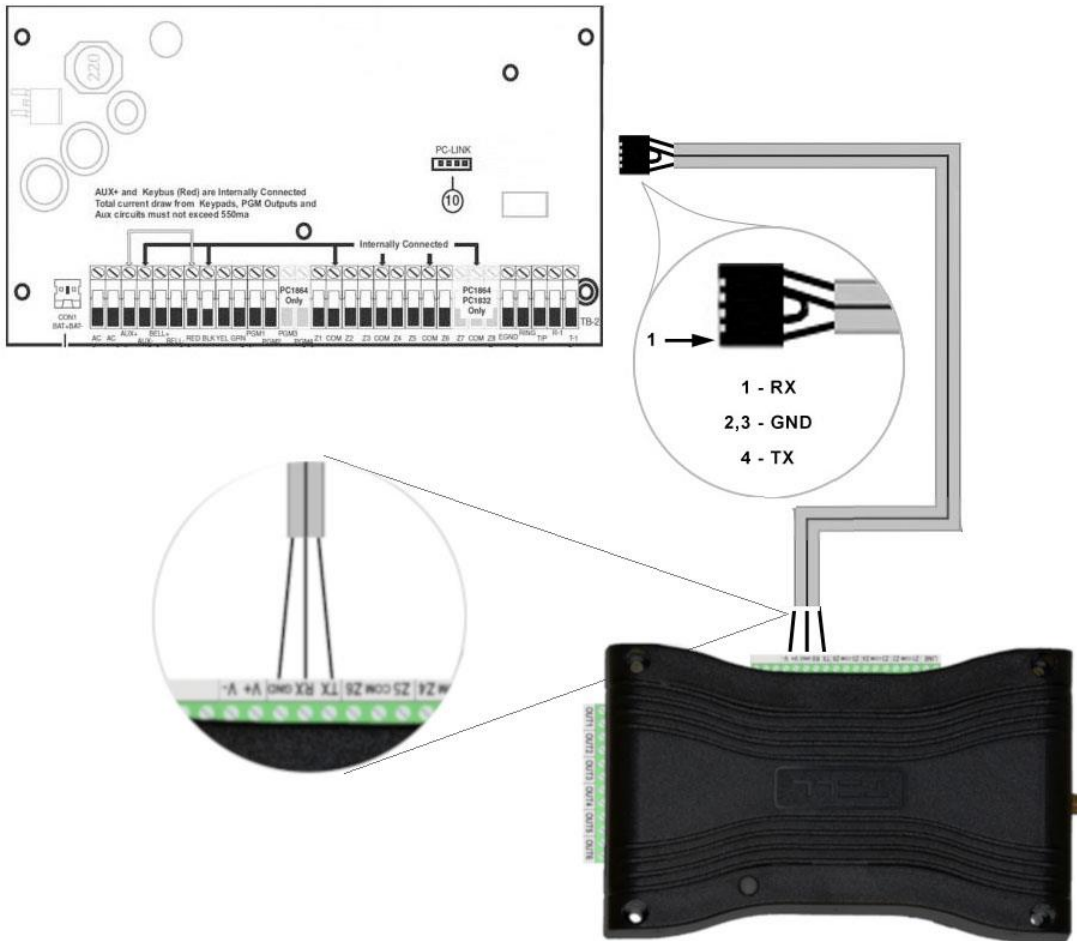


Connection established

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:



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.

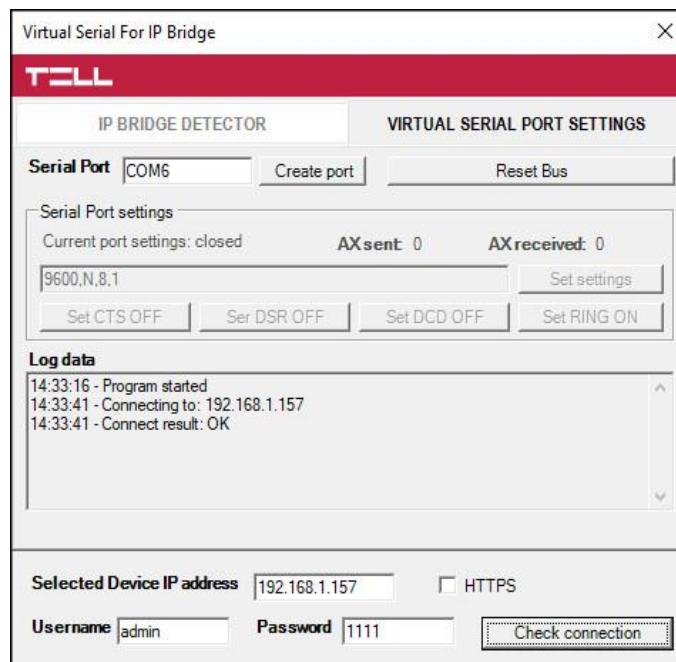
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

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:



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.

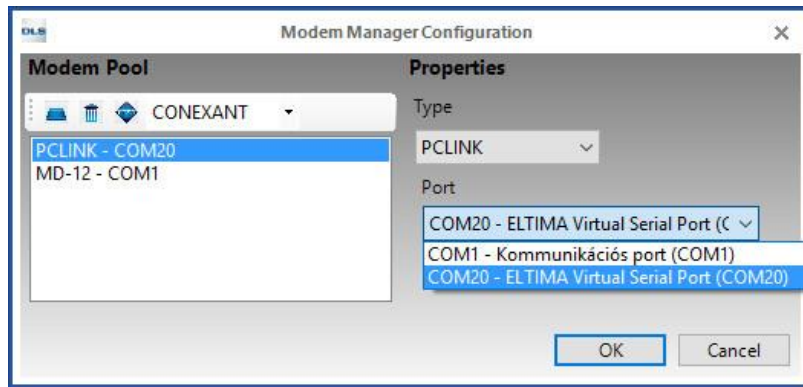
Password: The password of the user.

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

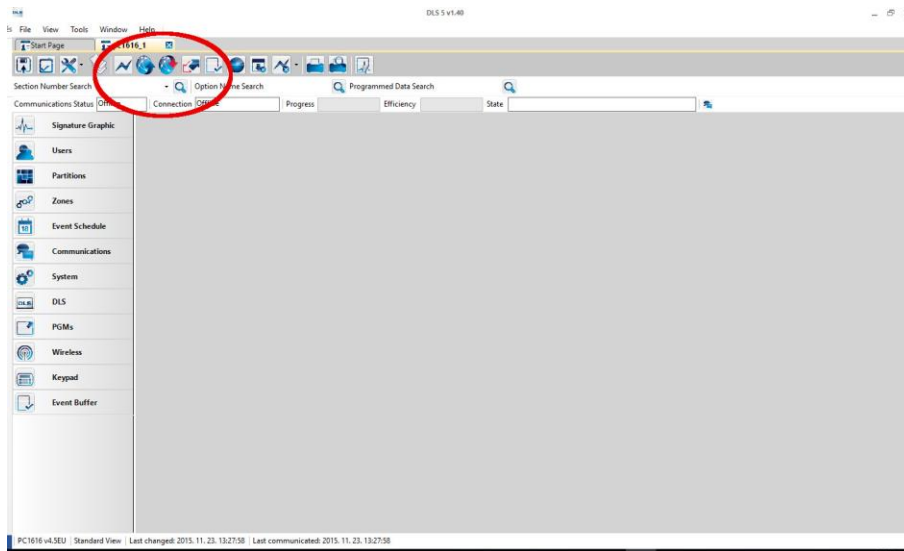
Serial Port: Set the virtual serial port’s address that you need to select in the alarm system’s programming software.

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).

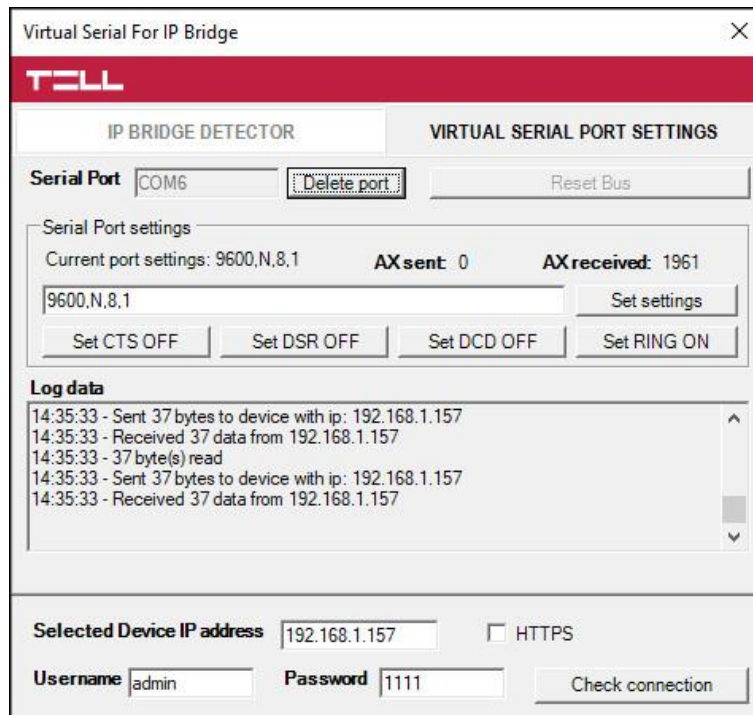


Select serial port



Connecting

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

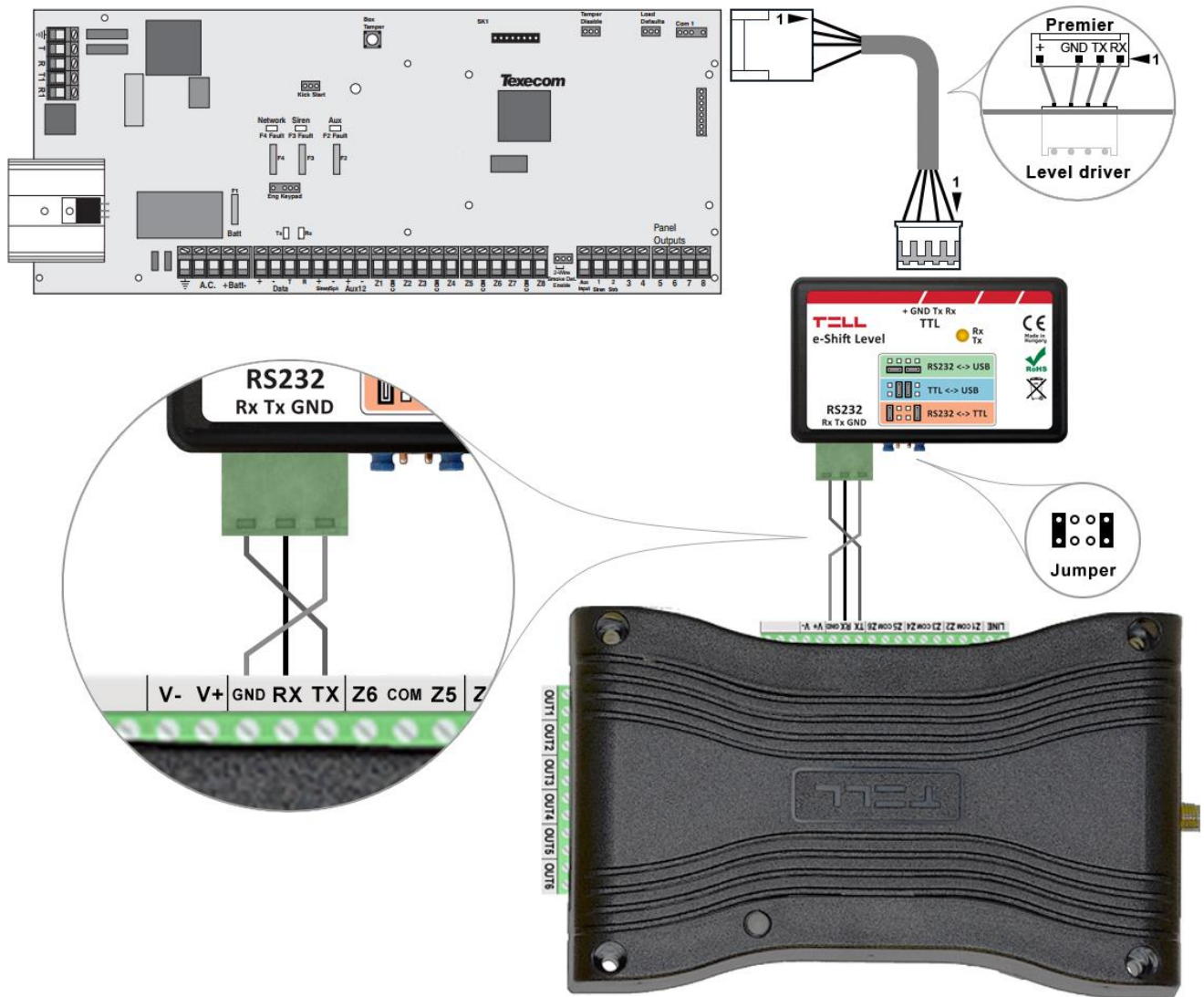


Connection established

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.

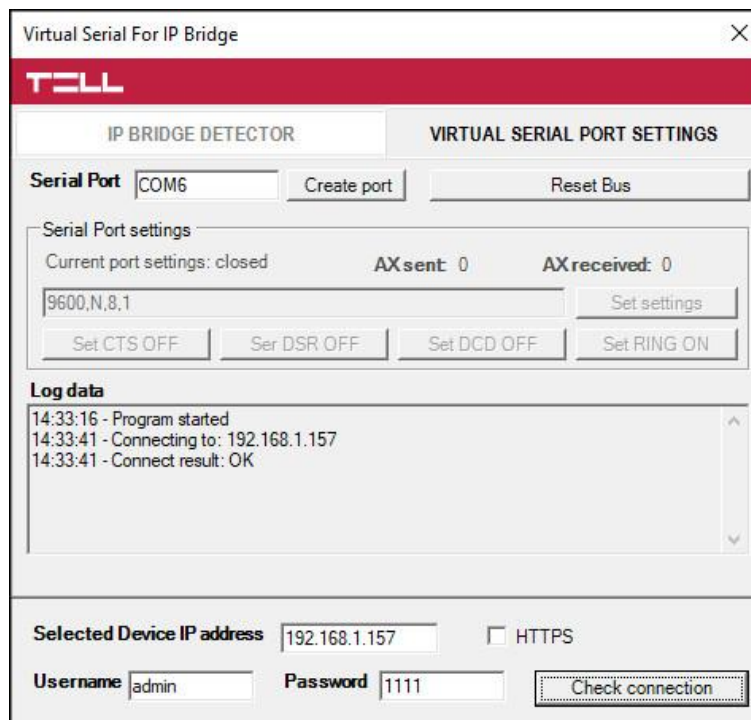
Attention! Serial data transfer may result high data traffic, so please consider this before selecting 3G/4G network as communication channel.

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:



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.

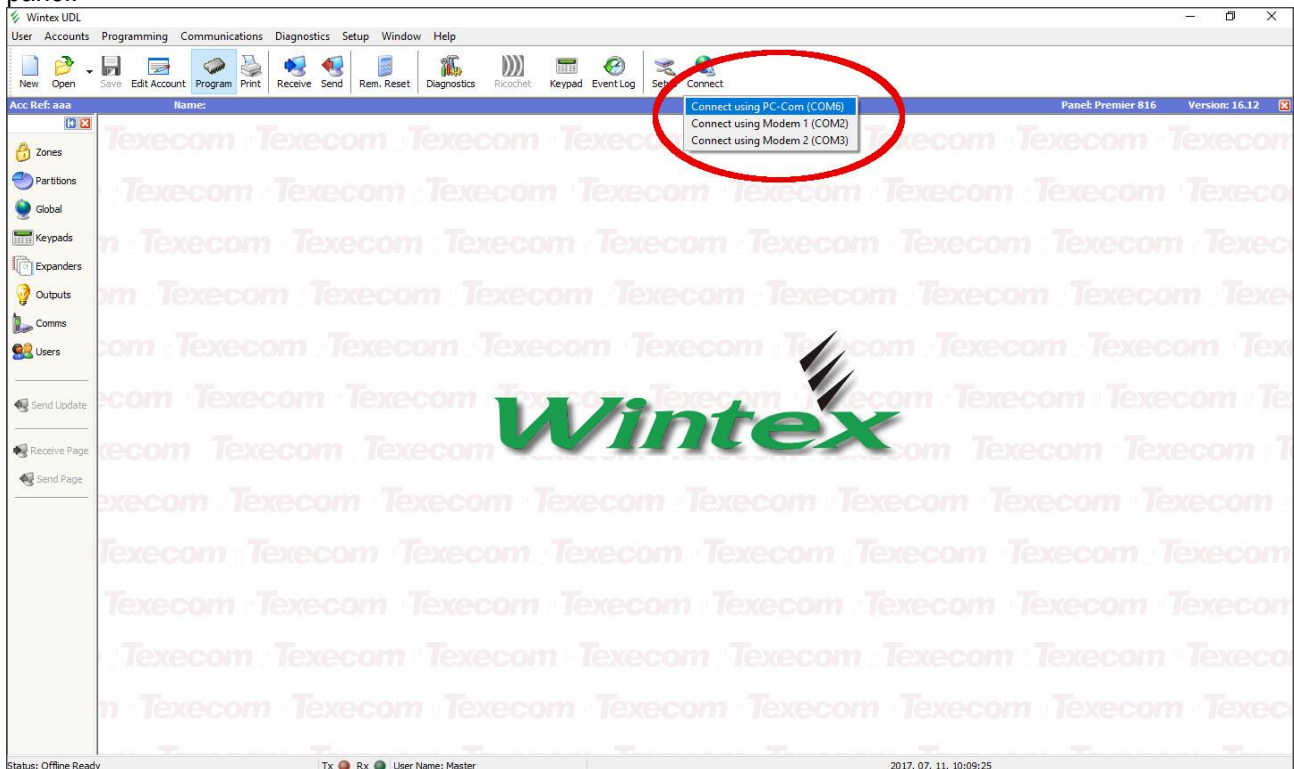
Check connection: Checks the module’s address you set.

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.

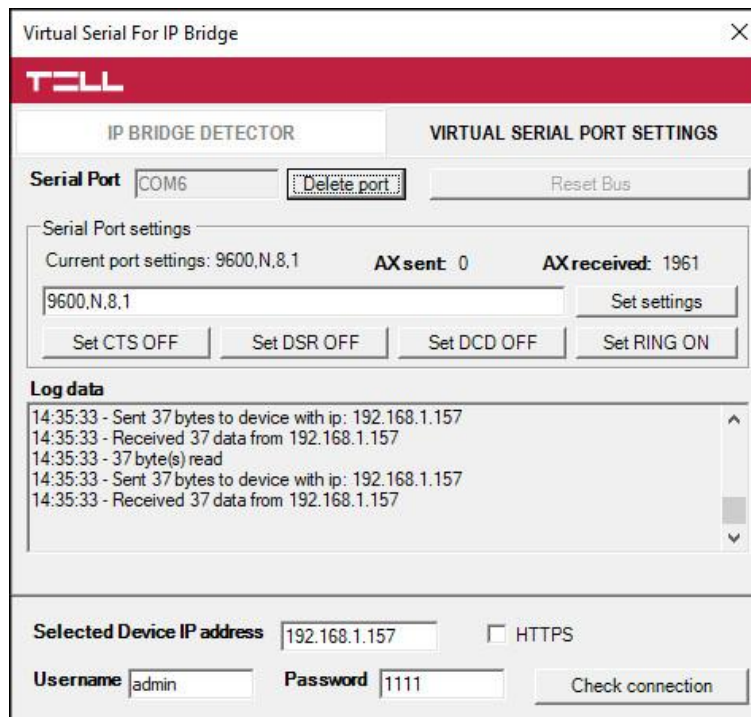
Log data: It provides information on the operation of the program, and displays data received on the serial port.

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



Select serial port

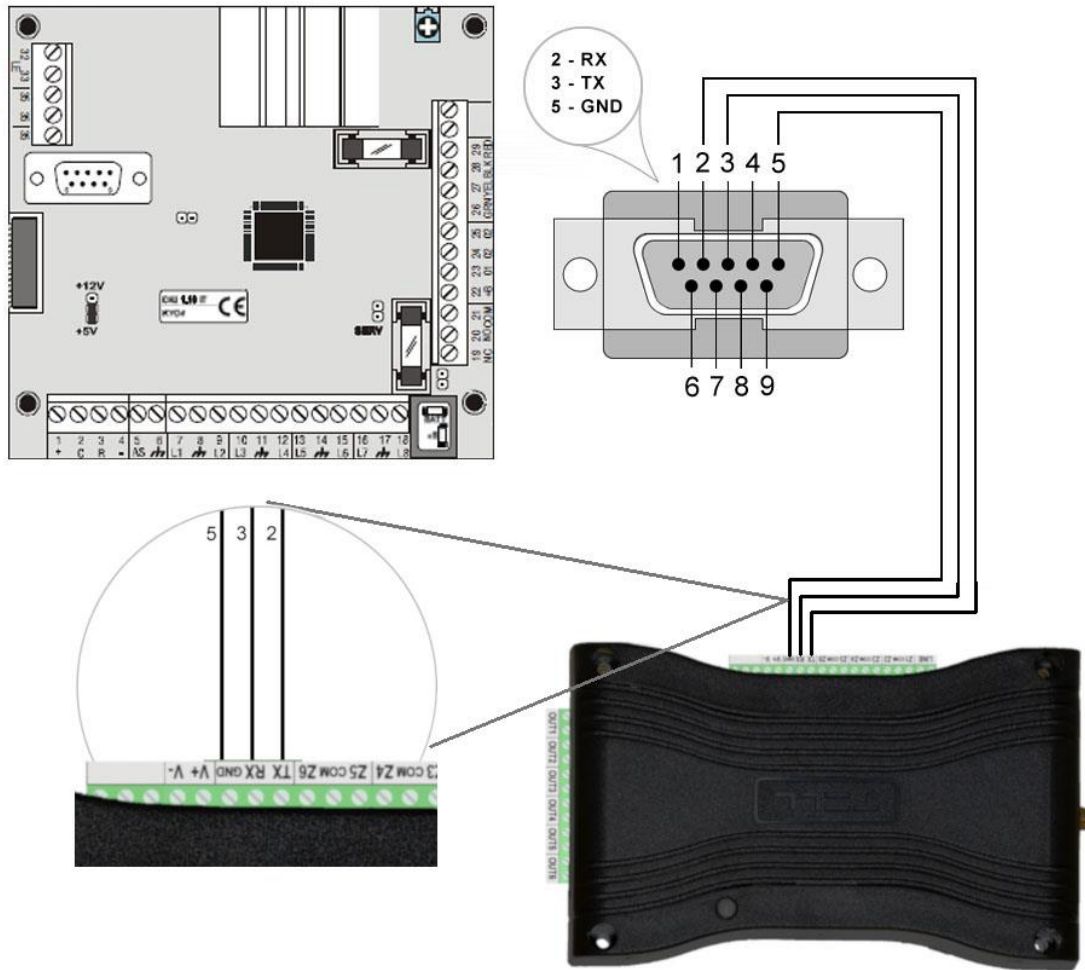
The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



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:

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.

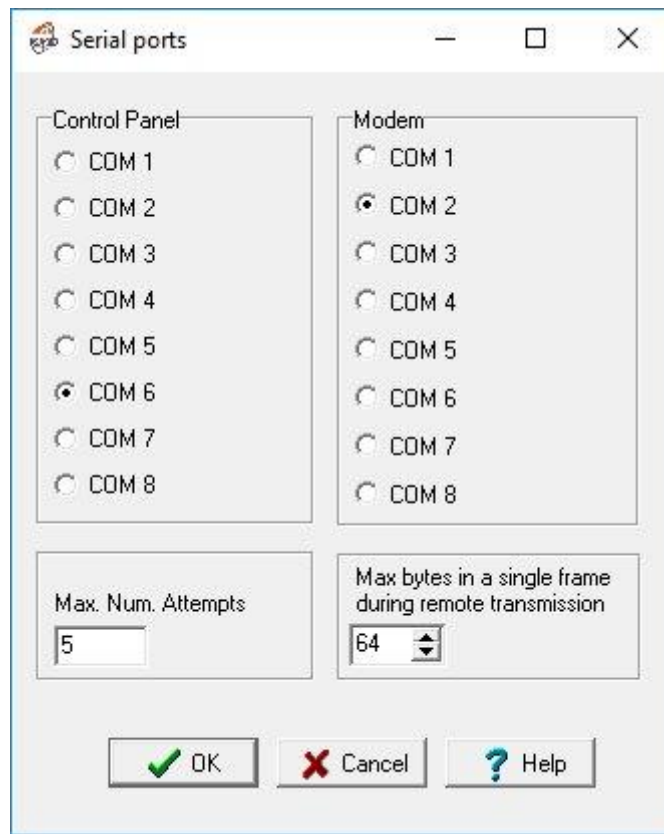
Check connection: Checks the module’s address you set.

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

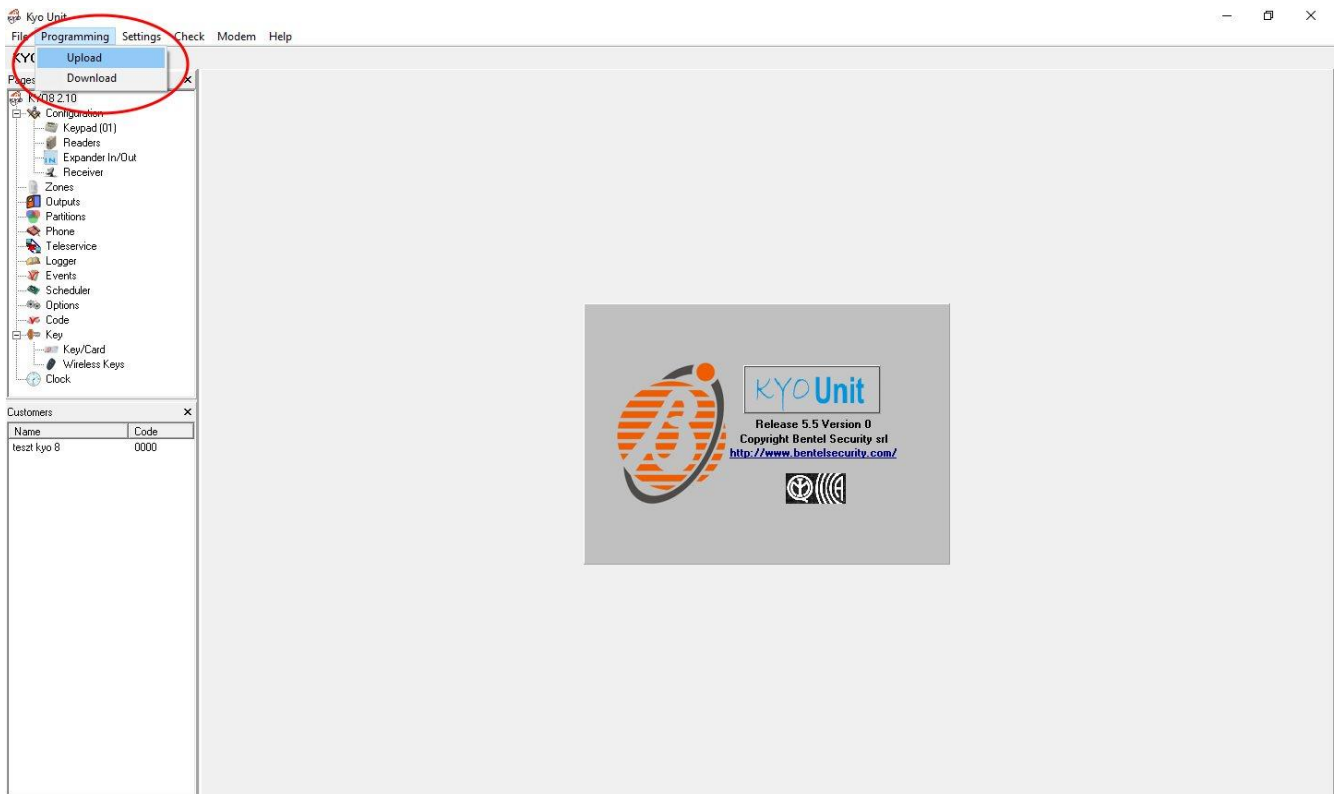
Create port: Creates the virtual port according to the settings.

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).

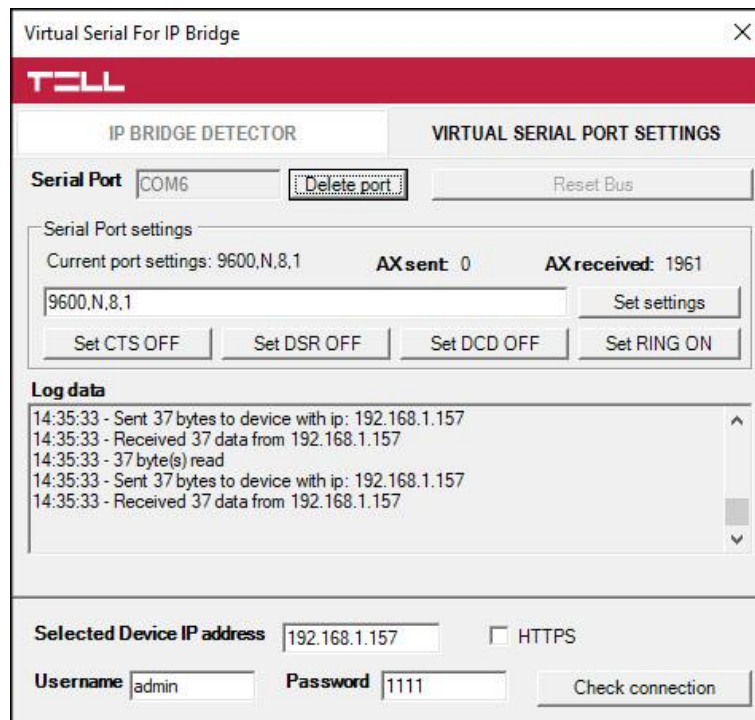


Select serial port



Connecting

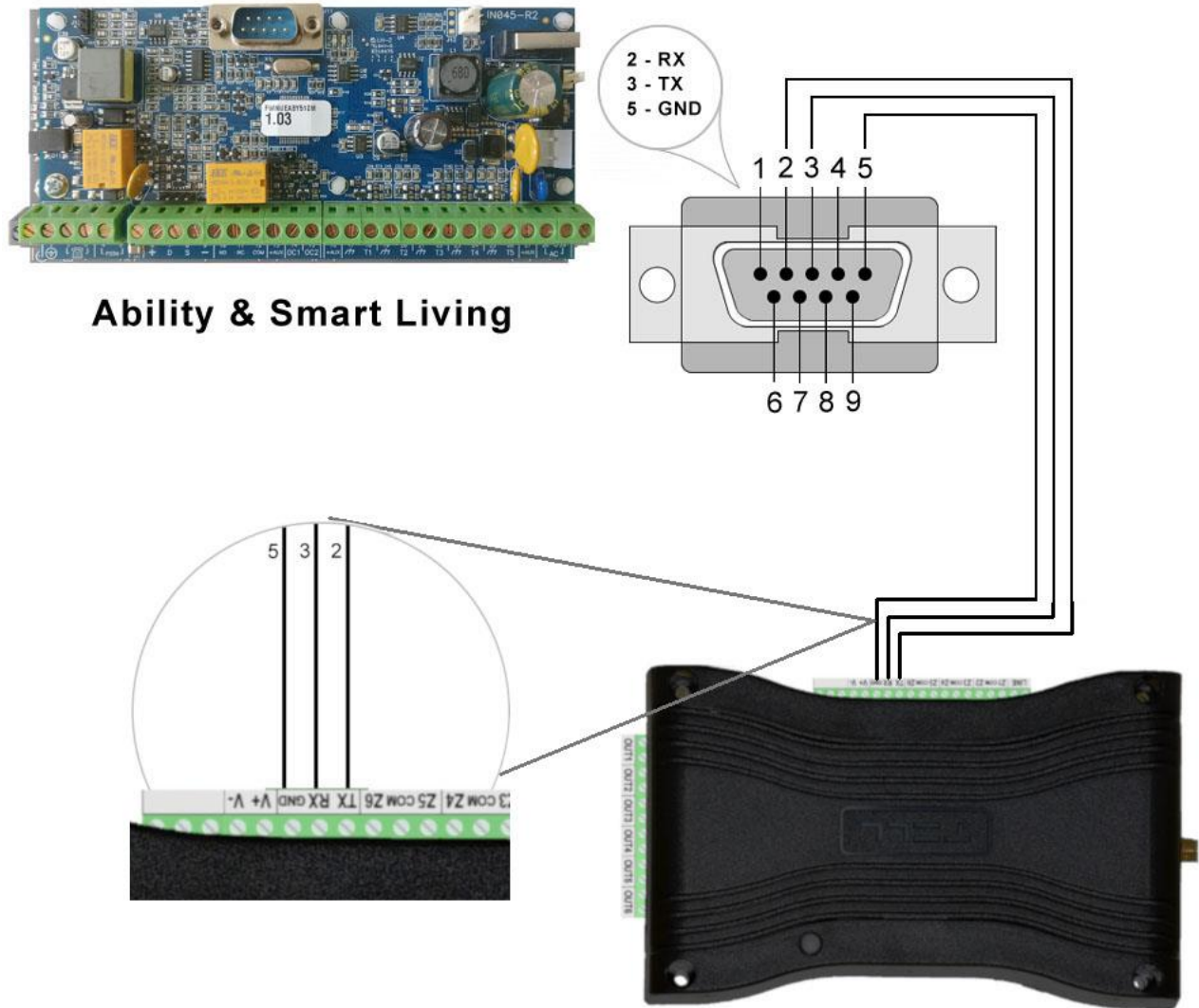
The programming software opens the serial port and establishes the connection with the alarm control panel (figure below).



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



Ability & Smart Living

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:

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.

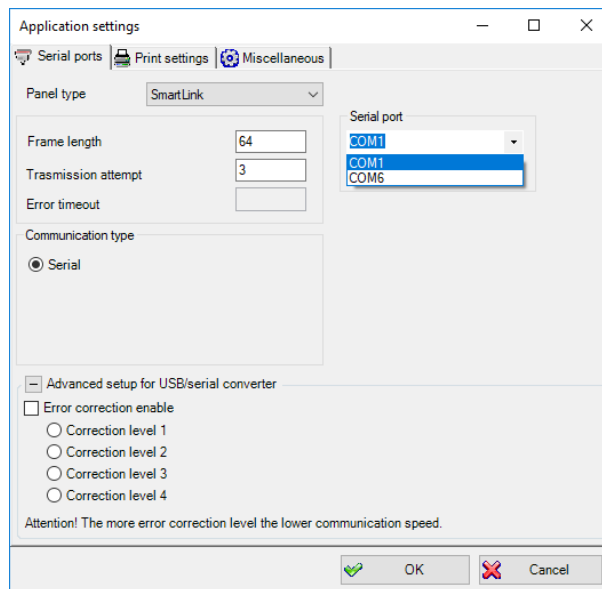
Check connection: Checks the module's address you set.

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.

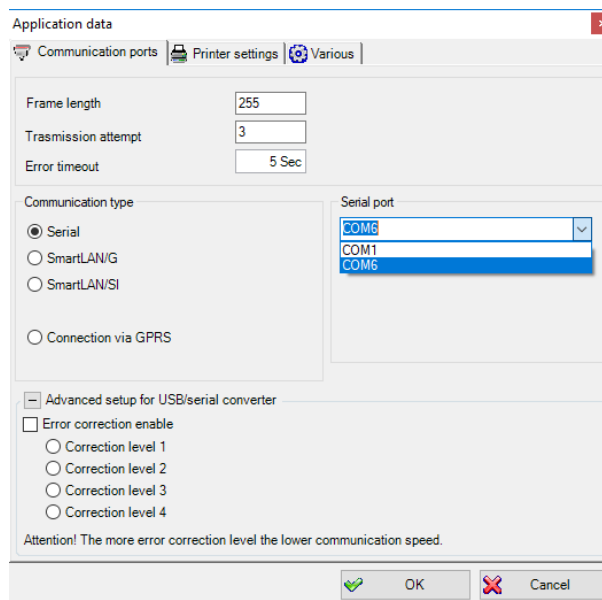
Log data: It provides information on the operation of the program, and displays data received on the serial port.

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).



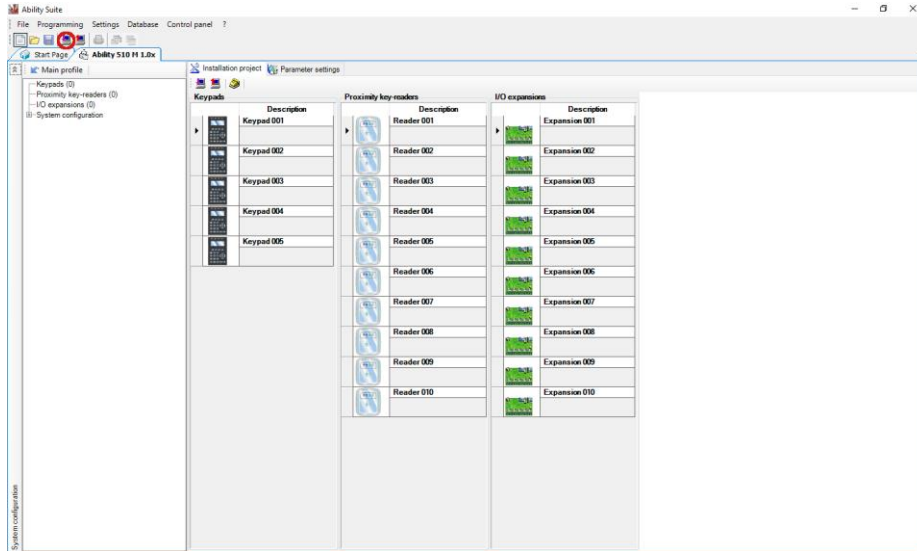
Select serial port

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



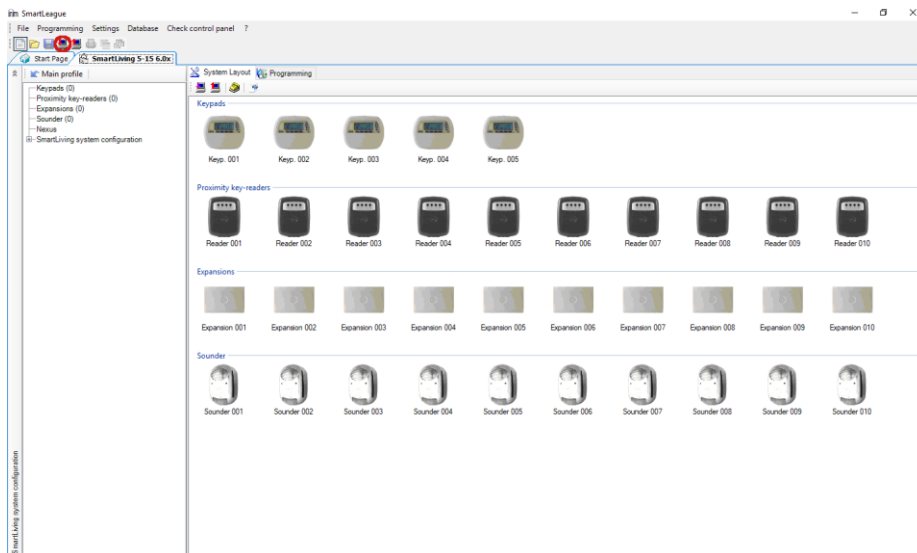
Select serial port

Connecting with Ability Suite programming software:



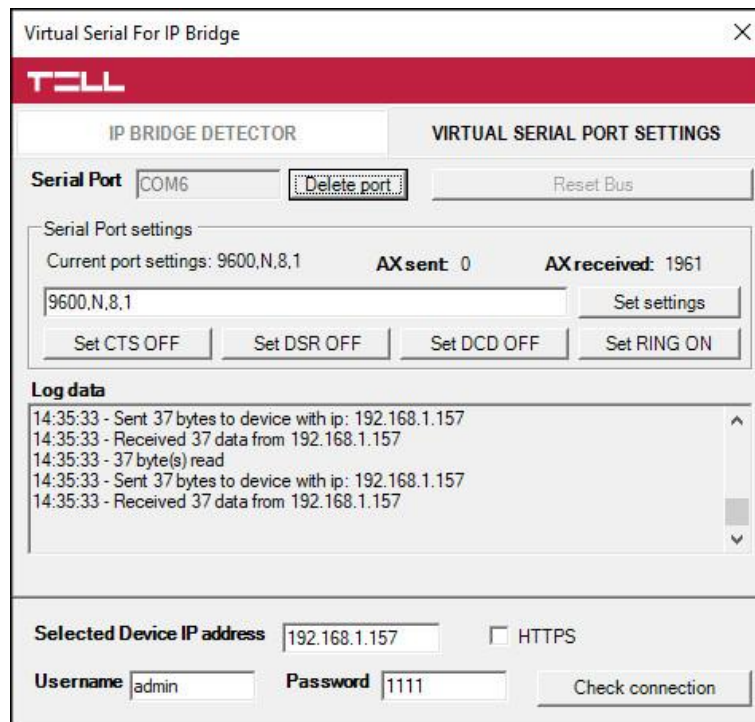
Connecting with Ability Suite

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).



Connection established

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