TEX MVP SERVER

USER'S MANUAL

for server version V5.3.469 or higher
Rev. 1.1 2010.07.05 Central

Table of contents

1 Characteristics of the GPRS network

The GPRS devices use the Global Packet Radio Service technology within the GSM communication network to communicate, send and receive information. Used protocol is TCP/IP.

1.1 Benefits and features of GPRS communication

- Continuous connection with the network:
  Connection between two communication points is being established much faster than at the GSM voice devices.
- Data quantity Invoicing:
  The provider of the network is invoicing the quantity of communication flow, not the time used for communication. Therefore, only the real sent and received data quantity is being invoiced.
- Higher speed of data flow than with the classical radio communication:
  The speed of communication on the receiver side can be up to 40kbit/s, and on the transmitting side up to 20kbit/s.

The available connection time and speed at the specific GPRS network depends on the used devices, number of users in the specific cell and the type of applications. There are no reserved sources in the GPRS network therefore the quality of service for data transmission can not be guaranteed.
In case of data transmission through GPRS network, it is possible to divide it in two parts: the wired and the wireless carrier part.
The characteristics of the wireless part is that the connection time is higher when establishing the connection for the first time, if there was no data flow for a longer period (more than 40 seconds), or if available communication channels count is low, because too many users are sharing (many GPRS users are connected to the same cell).

Therefore, the quality will be:

- The delay can vary from 0.6 – 3sec, for the reasons mentioned above
- The available speed can be 0 – 40kbit/s, depending on the number of users in the cell, i.e. the types of devices used.

Naturally, these parameters are affected with the radio circumstances (interference, signal strength), but we can accept for the basic rule the fact that where a good phone calls can be made with GSM voice communication, the GPRS should also have a good radio quality.
If you can not achieve good quality, an external antenna should be used, or it is necessary to change provider.

1.2 Public and dedicated APN

Characteristics of Public APN:

- The IP address of transmitters is dynamically changed:
  After the connection is broken or ended, the device will get a new one when reconnecting.
- For the authentication, the provider only checks if the Internet service is enabled for the specific SIM card i.e. for the phone number of the SIM card
- There is no guaranteed annual availability
- The provider does not have to inform users about maintenance of network (temporarily stopping the service), therefore a multitudinous break of the connections with GPRS devices is possible.

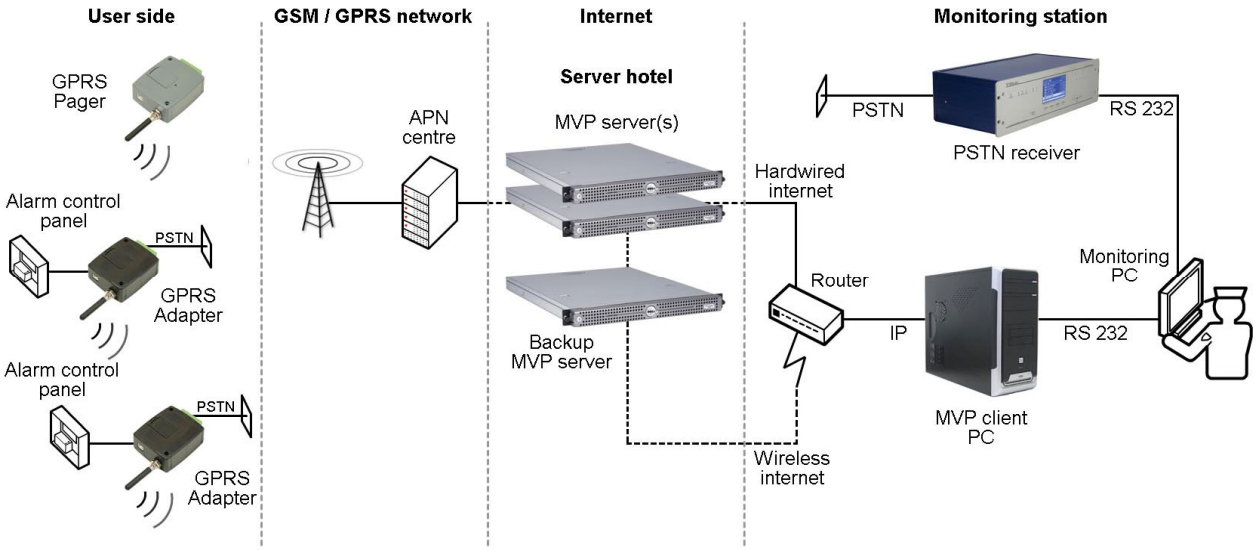
Characteristics of Dedicated APN:

The provider creates this APN specially for the customer who ordered it, therefore only those SIM cards that are dedicated to this customer can use it.
When creating the dedicated APN (internet VPN), provider will place a safe passthrough to every device in private network that needs to be connected to public network (Internet).
This means that every SIM card in the network will have a unique APN username and password. The passthrough are encrypting the package that leaves the private network and decrypting those that are coming from public network, thus creating an encrypted channel in the public network, Internet.

- Every SIM card (can) get a fix IP address, within the internal range of IP addresses
- In order to achieve a higher security, encryption is applied during the data transfer.
- The service can be used only with a special authentication (unique APN username and password checking by Gateway server, i.e. APN center)
- The whole communication works through a secured connection, therefore the owner of the APN who has a server with fix IP address should have a secured connection to the provider's APN server either through Internet, or directly, with leased line
- The provider should guarantee a high annual availability, more than 98% . Therefore, the service can not be stopped for a long time
- It is possible for the provider to monitor the user's network:
  If an error is detected, the recovery procedure can be started immediately, and the user can be notified about it.
- The provider must inform the user about the service stopping for maintenance reasons.
- The provider should provide a non-stop customer help service available
- The internal topology of this network is hidden for potential intruders

2 System operation

GPRS devices are using the GPRS communication as the primary option to forward the messages. In case that it is not possible to send the report to monitoring station through GPRS, they can switch to GSM voice channel, and in case of GPRS Adapter, the PSTN (phone line) can also be used to send the report to PSTN line receiver (e.g. Sur-Guard).



Using the GPRS network, GSM service provider's APN centre and then the internet, the GPRS devices communicate with the MVP server (with the first one available, in case of system with more servers). The MVP server forwards the incoming data packets to the MVP client(s) of the corresponding monitoring station(s), which then decrypts and forwards the data through serial port to the monitoring PC.
The serial communication between the MVP client software and the monitoring PC is realized with the same basic protocol which is used by conventional PSTN receivers, therefore any monitoring software can be used on the monitoring PC, even the existing one, if it handles Contact ID format (e.g. TMS, ComSys, Alarm-sys, etc.).
For maximum security it is recommended to use internet on two different lines from two different service providers, where the primary line can be a leased line internet or ADSL, and the secondary can be a wireless connection. This way, if the hardwired internet fails, the alarms can be received through the wireless connection.

2.1 Backup GPRS transmission

If the device is unable to connect through GPRS to any of the servers, then it communicates with the monitoring station's switched line receiver using GSM voice call or PSTN, depending on the configuration and settings.
In case of messages sending through GSM voice or when there is a GSM adapter on the receiver's side, an increased delay in communication is expectable.
More details can be found in chapter „**PSTN receiver settings**".

2.2 Server functions

The primary function of the MVP server is the realization, encryption and logging of the communication between the GPRS devices (GPRS Adapter, GPRS Pager) and the MVP client softwares.
The MVP server operates with Unix (SUN Solaris) operating system and it uses the internet to communicate with the GPRS devices and MVP client softwares.

2.2.1 MVP server client features

- Management of more than 4000 GPRS devices at the same time
- Encrypts all network traffic, uses unique encryption keys for each device
- Frequent encryption key change for maximum security
- Monitors active devices with test heartbeat signals, generates alarm event in case of heartbeat signal loss
- Monitors network connections (LAN, WAN), generates event on connection loss
- Automatic time synchronization over the Internet
- Multilevel server and client access
- Management of logical groups and company sites
- A single server can be used by more monitoring stations at the same time
- Possibility of realization of multiserver architecture
- Replication an synchronization between servers
- Management of 2 Ethernet ports (100/1000 Mbit/s)
- Management of 1 internet, and optional +1 private network (APN) at the same time
- Fast event transmission towards MVP clients
- Separation of GPRS device migration and connection loss event
- Continuous supervision of the connection of MVP clients
- WEB based event log
- Full configurability through Web interface
- Server update through encrypted remote connection

2.3 Requirements for monitoring central station security levels

High security level

- Two MVP servers operated in parallel, installed in two different server hotels
- Dedicated APN service
- Leased line internet connection, as primary internet connection
- ADSL connection, as reserve internet connection
- PSTN receiver for reserve reception
  (in case of GPRS or internet connection failure)
- Uninterruptible power supply

Normal security level

- One MVP server installed in server hotel
- Dedicated APN service
- ADSL connection, mint as primary internet connection
- Wireless internet connection, as reserve internet connection
- Use of T.E.L.L. Backup MVP server
- PSTN receiver for reserve reception
  (in case of GPRS or internet connection failure)
- Uninterruptible power supply

Minimum security level

- One MVP server installed in server hotel
- Public APN service
- ADSL internet connection
- Wireless internet connection, as reserve internet connection
- (Use of T.E.L.L. Backup MVP server)
- PSTN receiver for reserve reception
  (in case of GPRS or internet connection failure)
- Uninterruptible power supply

2.3.1 Types and characteristics of Internet connections

- **Leased line**

Leased line is a physical connection between the customer's site and the provider's network. This is the highest level of technical support, functional reliability and bandwidth. By this dedicated line the service provider provides permanent connection to its internet network. The monthly fee is higher but there is a guaranteed availability through the year. This guarantee means that the provider – according to the agreement - must pay penalty in case the service is out of order.
As an option the customer can buy or lease router from the service provider (for more information please contact the service provider).

- **ADSL connection**

This connection uses the service provider PSTN network through traditional telephone line, a pair of copper or optical wire. In case they fail the ADSL service is out of function. The bandwidth is guaranteed until the first server only.
If the low cost but unreliable ADSL internet connection is used instead of a leased line temporary connection outages should be taken into consideration.
The ADSL connection is established and maintained by external devices (e.g. ADSL router) in which user ID and password must be set to establish connection, and the an unlimited lease time must be set in the router.
When ADSL internet connection is used the TEX server must be in a separate network since viruses and spywares can infiltrate through the network and they slow down the capacity.

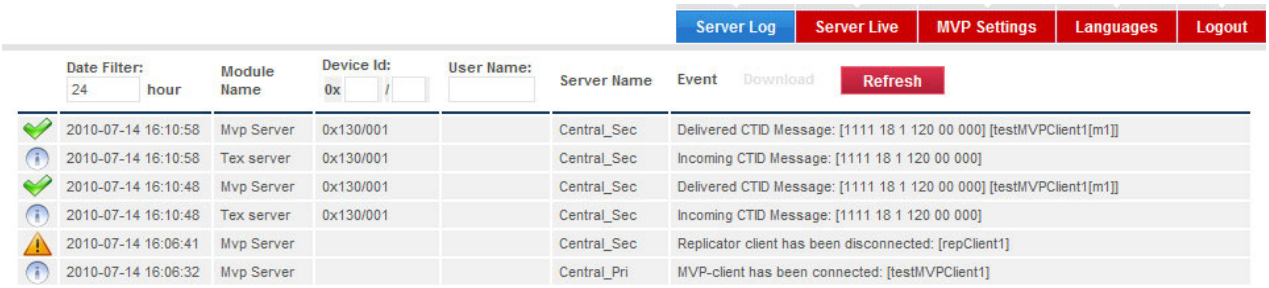
- **Other internet connections**

If you wish to purchase an internet service using cable modem or other connection, a router should be used because of the port forwarding and port enabling (even MAC address registration) functions.

3 The MVP server configuration web interface

The configuration page of the server can be opened with a web browser (Mozilla Firefox 3.0+, Internet Explorer 8.0+, Google Chrome 4.0+ are recommended) by entering the IP address and the web port. The default web port is 8080:
eg.: if the fixed IP of the server is 195.196.197.198, then the following address must be entered in the web browser: **http://195.196.197.198:8080**

3.1 Server Log



The „Server Log" menu makes possible to trace the events related to the concerned company and the events sent by the company's GPRS devices, in a contracted event log. The event log is refreshed automatically at every 10 seconds, however it can be refreshed at anytime by pressing "**Refresh**" button. In case of using more servers in the system, then the events of the certain servers are replicated in the server log, which means all events are available on all servers.

Elements of the event log:

Event category: displayed with icons, represents the type of the events

: **Info**: information (e.g. incoming Contact ID message)

: **Successful** event forwarding, the monitoring station confirmed the event

: **Failed**, no confirmation is received from the monitoring station

: **Warning**: e.g. GPRS test report timeout or restore

Date Filter: the length of the event log can be selected here by entering a number between 0-24 in the textbox, which is considered in hours and adjusts the log length retroactively for the entered period, but maximum only 500 lines can be displayed at the same time. By default, events of the last 24 hours are displayed. After entering the desired value, press "**Refresh**" button to validate. Filtering can be released by deleting the value from the textbox, then pressing "**Refresh**" button. Right below the textbox, the date and time of the events can be seen.

Module Name: name of the software module, which transmits the event

Device ID: this option makes possible to filter the event log by desired group ID and/or serial number. After entering the desired values in the textbox and pressing "**Refresh**" button, the event log will be filtered to the events of the given GPRS device(s). Filtering can be released by deleting the values from the textbox, then pressing "**Refresh**" button.

User Name: this option makes possible to filter the event log by desired user name. After entering the desired user name in the textbox and pressing "**Refresh**" button, the event log will be filtered to the activity events of the given user. Filtering can be released by deleting the name from the textbox, then pressing "**Refresh**" button.

Server name: the server's name on which the event occurred.

Event: this section contains the event details. The following messages may be displayed here (event details in square brackets, e.g. characters of the Contact ID message, IP address, etc.):

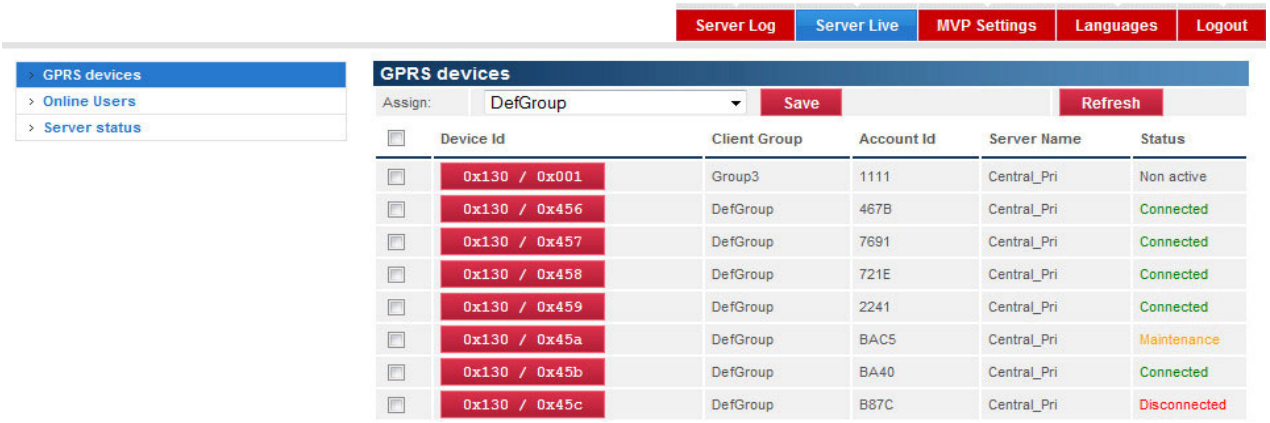
- **IP connection has been established: [...]**
  GPRS device (or IP client) successfully connected to the server (authentication, i.e. identification was also successful).
- **IP connection has been terminated: [...]**
  The previously successfully connected GPRS device or client disconnected from the server, the network connection is lost (e.g. GPRS connection error). If the device reconnects within the predefined interval (GPRS test report frequency + server timeout which is 3 minutes by default), then this process is not detected at the monitoring workstation, as no GPRS test report lost CTID message is generated.
- **IP connection has been closed: [...]**
  Unsuccessful connection attempt (possible attack or port scan attempt). The network connection is established, but authentication is unsuccessful. Connection without authentication is closed in a very short time.
- **IP connection closed, (re)connecting with the same device ID: […]**
  A GPRS device is reconnecting to the server but the server did not detect a lost connection earlier (e.g. GPRS network error). Wrong GPRS device programming may cause that two devices receive the same identifier. In this case if the second device also connects to the server, then the server – according to the logic above – detects this as if the same device would have connected again: so it closes the old network connection and replaces it with the new one. The other disconnected device, however, will soon reconnect, and the above process starts again. This process continues until one of the devices is turned off.
- **IP connection – 12 hour GPRS test is OK**
  For security reasons devices restart every 12 hours. This message notifies about the successful connection after the restarting. It is not detected at the monitoring workstation.
- **Incoming CTID message: […]**
  The server received a Contact ID message from a GPRS device.
- **Delivered CTID message: [...]**
  The Contact ID message received by the server was successfully delivered to the monitoring software.
- **GPRS test report lost, CTID message generated: […]**
  This CTID message is generated and sent to the monitoring program if the device did not send another GPRS test report (heartbeat), within the preconfigured time interval (GPRS test report frequency + server timeout, which is 3 minutes by default).
- **GPRS connection restored, CTID-R message generated: […]**
  This is the pair of the "GPRS test report lost, CTID message generated" message. It generates a CTID-R message and sends it to the monitoring program, if the connection of the given client is restored again after the previously sent "GPRS test report lost, CTID message generated" message. The GPRS device reconnects, authenticates and sends GPRS test report (heartbeat).
- **LAN network connection lost, CTID message generated: […]**
  If the server detects that the LAN network is unavailable, it generates this CTID message and sends it to the monitoring program. The LAN network is monitored according to the related IP addresses set in the configuration file: the server regularly checks whether the specified IP addresses are available.
- **LAN network connection restored, CTID-R message generated: […]**
  If the server generated and sent a "LAN network connection lost CTID" message previously, then it generates and sends this message after the connection has restored.

- **Internet1 (Internet2) network connection lost, CTID message generated: […]**
  If the server detects that the internet is unavailable, it generates and sends this CTID message to the monitoring program. The internet connection is monitored according to the related IP addresses set in the configuration file: the server regularly checks whether the specified IP addresses are available.
- **Internet1 (Internet2) network connection restored, CTID message generated: [...]**
  If the server generated an "Internet network connection lost" message previously, and it now detects that the internet is available, then it generates and sends this CTID message to the monitoring program.
- **Coordinator server: Replication sent to cohort**
  The main server has sent replication data (settings, log entries, status) towards the other servers (cohort). Cohort servers are the servers in the system on which modification of the settings is not available.
- **Cohort server: Replication received from the coordinator**
  The replication data sent by the main server was received by the cohort server. The name of the given cohort server is displayed in the „Server Name" column.
- **Replicator client has been disconnected**
  The replication (settings and log sharing) between the servers in the system is performed for each company account by a client software so-called "replicator", which runs in the background on the server. This event indicates that the replicator client was unable to connect to the server.
- **Relication config saving failed**
  The cohort server was unable to save the received replication.
- **Cohort server: Replication has been refused**
  The cohort server has refused the received replication because it was not trusted, did not have the right certificate.
- **Cohort server: Replication has been saved**
  The cohort server has saved the received replication successfully.
- **Replicator client has been connected**
  The replicator client has connected to the server.
- **Replicator client has been disconnected**
  The replicator client has disconnected from the server.

3.2 Server Live

In this menu server information and status of GPRS devices is displayed, and assignment of GPRS devices to client groups can be performed.

3.2.1 GPRS devices



In this menu the status of the registered GPRS devices is displayed, and assignment of GPRS devices to client groups can be also performed here.
Client groups are such logical groups, to which devices can be assigned and this way diverse configurations for monitoring stations can be realized, e.g. sharing clients between monitoring station divisions. At „MVP Clients" settings the client groups can be assigned selectively to the desired MVP client softwares, this way the given MVP client software receives only the messages of the assigned client group. In this manner can be created e.g. a regional client group, of which messages are received only by the monitoring station available on that specific region/district, but in case of e.g. internet connection failure, the reception point having the next lower priority can be the monitoring station of the neighboring region/district.
The logical client groups can be created in the „MVP Settings / Client Groups" menu.

Menu items:

Navigation: navigation between pages, if the number of GPRS devices is more than 30

Assign: the GPRS devices marked using the checkbox can be assigned to the client groups selectable from the drop-down menu

Save: finalizes the assignment of the marked GPRS devices to the selected client groups

Refresh: serves for refreshing manually the list of GPRS devices. The list is not refreshed automatically

Checkbox: the GPRS devices can be selected one by one, by clicking on their checkbox found to the left from the device ID's, or all the devices can be selected by clicking on the checkbox found in the header.

Device ID: the group ID and the serial number of the GPRS devices in hexadecimal format. By clicking on the desired device ID, the server log of the given device is displayed.

Client Group: the logical client group of the GPRS devices, to which they have been assigned

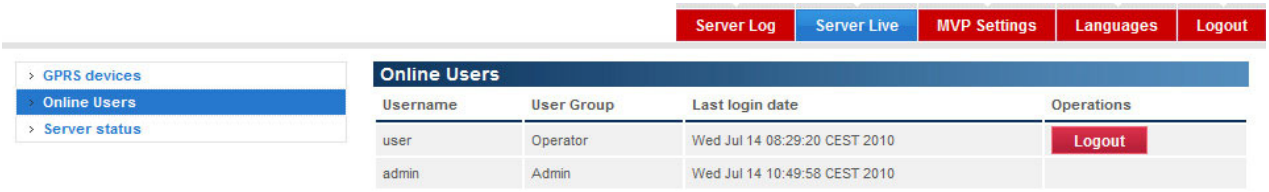
Server Name: the server's name to which the GPRS device connects

Account ID: the user account ID of the GPRS devices (or alarm control panels)

Status: the connection status of the GPRS devices
- **Connected**: the GPRS device is connected to the server
- **Disconnected**: the connection between the GPRS device and the server is lost
- **Non active**: there is no connection with the GPRS device for at least 3 minutes
- **Maintenance**: the GPRS device is restarting

The list contains only GPRS devices which have already connected to the server, therefore registration of a new GPRS device can be done by establishing its connection to the server. In csase of using more servers in the system, the status of the GPRS devices connected to the other servers is displayed on the recent server as well with a short delay.
A newly connected GPRS device is assigned automatically to the „Default" client group, which configuration can be modified as described above (Assign).

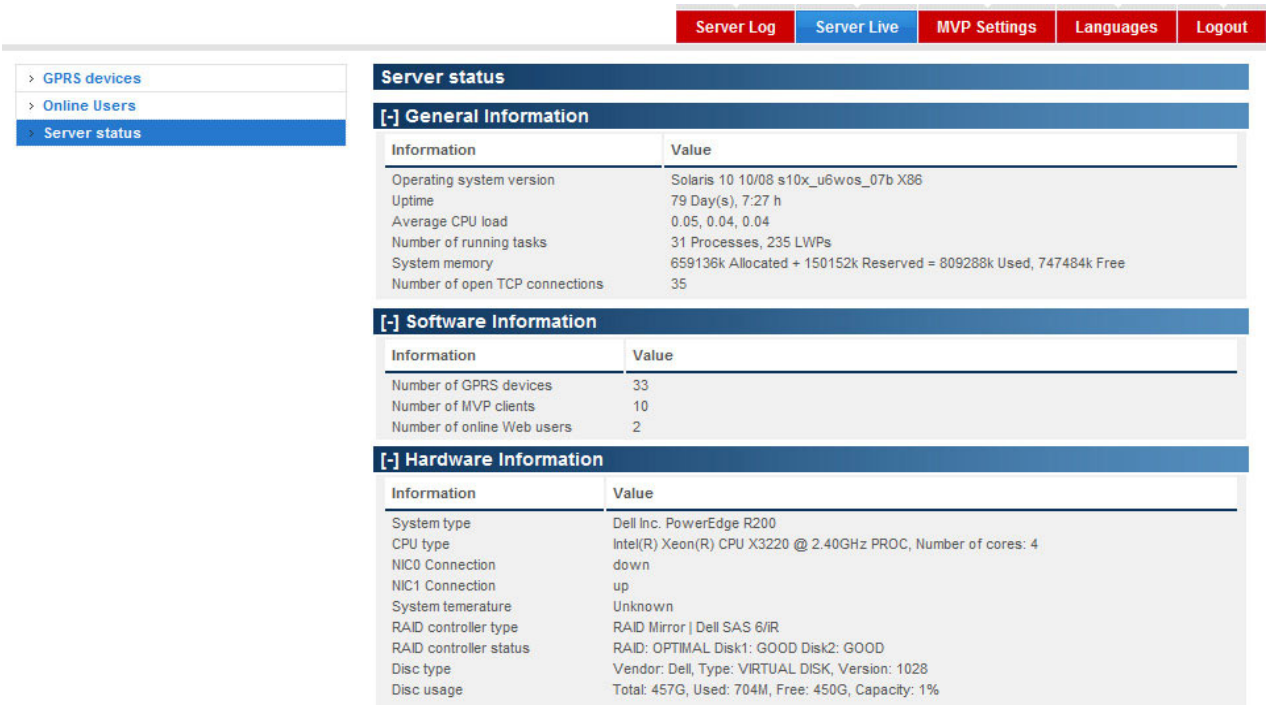
3.2.2 Online users



This menu shows the users recently logged in on the server's configuration web interface, as well as the date and time of the last login.

Logout: using this button, the admin user can perform forced user logout for any user.

3.2.3 Server status



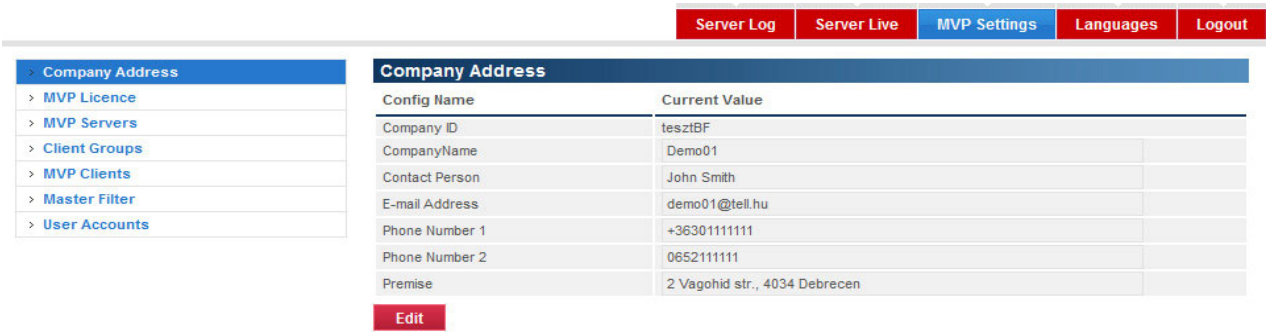
In the „Server status" menu general, software, and hardware information is displayed about the server. Information with importance for users:

General Information / Uptime: shows the time elapsed from the last server power up.
Software Information / Number of GPRS devices: shows the number of GPRS devices registered ever on the server.
Software Information / Number of MVP clients: shows the number of MVP clients registered ever on the server.
Software Information / Number of online web users: shows the number of users logged in on the server.
Hardware Information / NIC0-NIC1 connection: shows the status of the two network interfaces.

3.3 MVP Settings

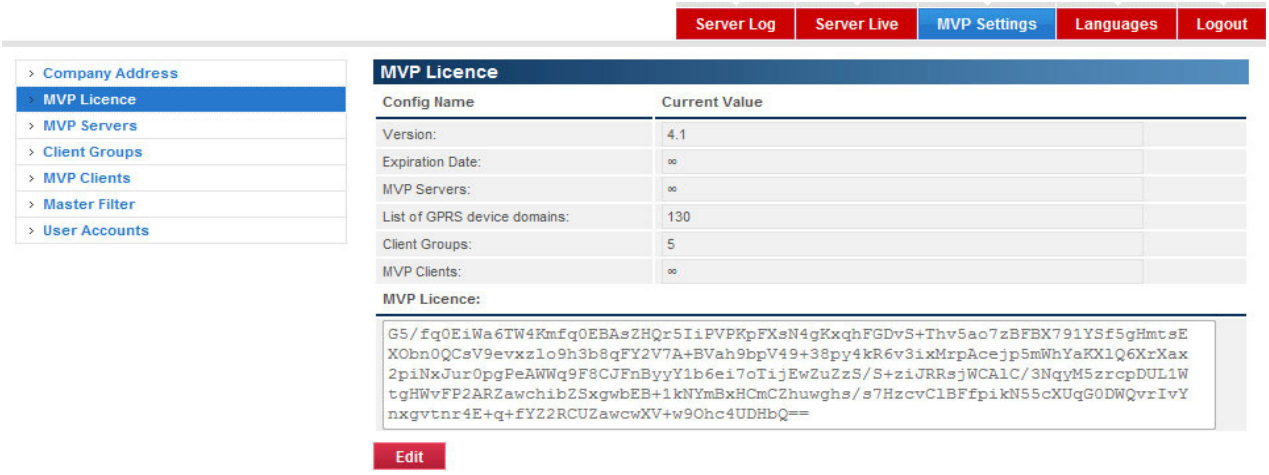
Any modification performed in this menu disconnects the MVP clients from the server which will reconnect afterwards, thus notifying the monitoring station as well that settings have been modified.

3.3.1 Company Address



In the „Company Address" menu there is possibility to enter or modify data after pressing „**Edit**" button. The **Company ID** cannot be modified, this is registered in the server by the manufacturer when ordering.

3.3.2 MVP licence

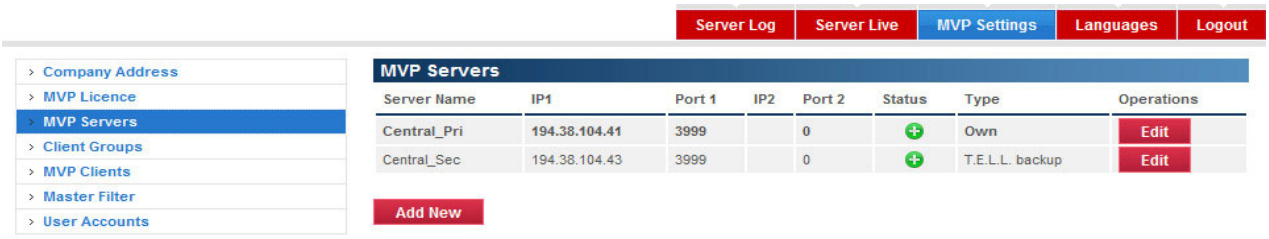


The „MVP licence" menu shows the services contained by the actual licence, and makes possible the registration of new licence as well.

To register a new licence press „**Edit**" button, then delete the actual licence code from the textbox, insert here the new licence code and press „**Save**" button.
By pressing „**Reset**" button, the last saved licence code can be restored in the textbox.

In case of registering an incorrect or faulty code, the server will continue to operate with default licence, which contains default services.

3.3.3 MVP servers



In this menu the connection availabilities of the present server and further MVP servers (e.g. backup server) can be set and modified, as well as their connection status can be traced.

The server on which tracing is recently in progress is highlighted with bold characters.
The existing server's data can be modified after pressing „**Edit**" button. Registration of a new server can be performed by pressing „**Add New**" button. To save the new or modified data, press „**Save**" button. By pressing „**Reset**" button, the last saved data can be restored.

Server ID: fixed server identifier, this cannot be modified within the server

Short name: a desired individual short name can be entered

Full name: a desired individual longer name can be entered

IP1-2: the server's external IP address(es)

Port1-2: the server's external communication port(s)

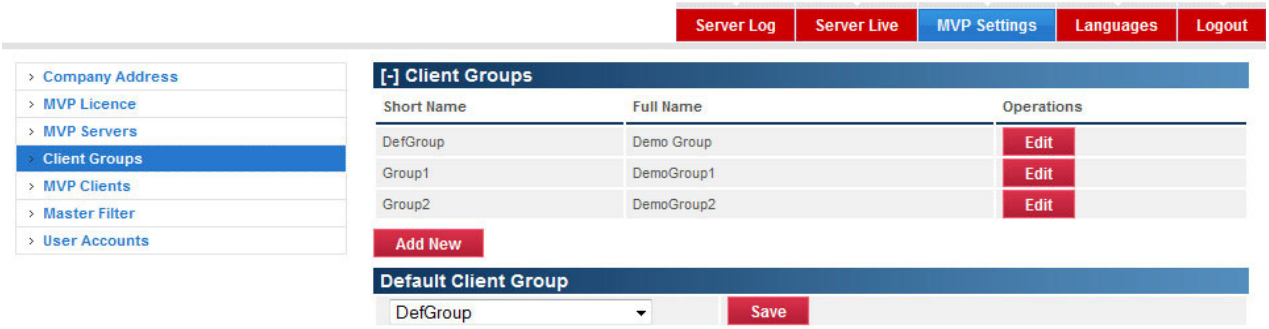
Local IP1-2: the server's local IP address(es)

Local Port 1-2: the server's local communication port(s)

Status: server status (green icon = available, red icon = unavailable)

Type: server type (fixed types can be selected from a drop-down menu when in edit mode)

3.3.4 Client Groups

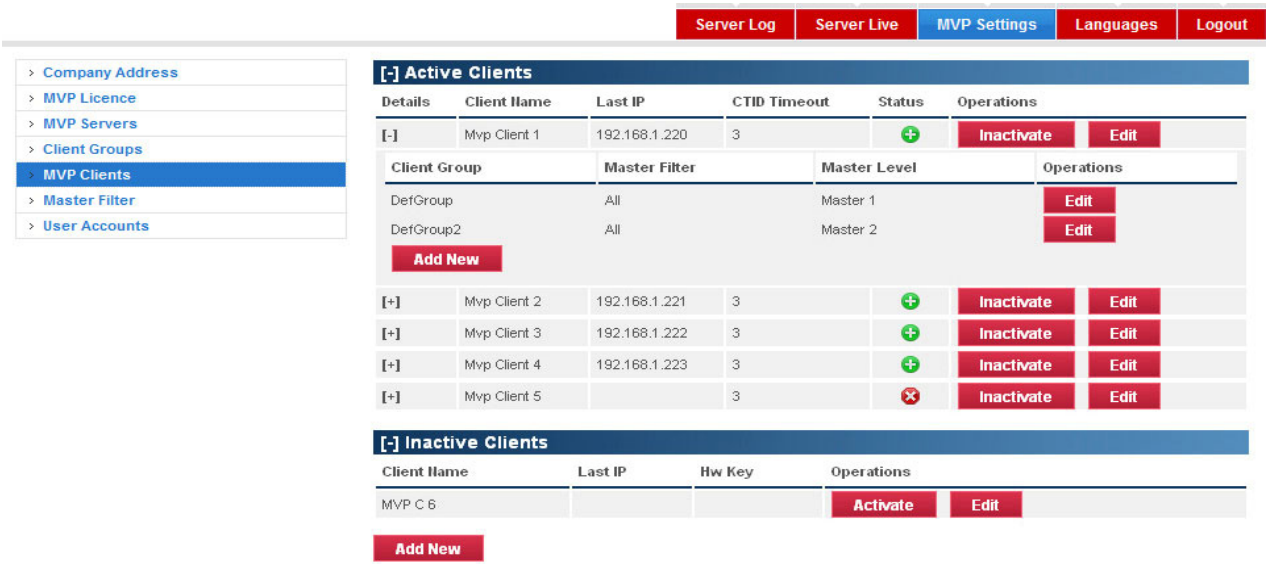


Client groups are sets that can be created freely, through which the GPRS devices registered on the server can be grouped (devided in smaller groups, or add into one group). One GPRS device can be strictly assigned only to one client group. One MVP server can manage by default maximum 4000 GPRS devices, which means one physical device group. This number can be increased by the four thousands (by physical device groups), altogether till 12000, depending on the licence.
The added client groups can be assigned to the MVP client softwares, this way the given client software will receive the signals of the GPRS devices which belong to the client group assigned to the software. In this manner, multi-site or backup monitoring system can be easily realized.

After pressing „**Edit**" button, the short and the full name of the selected client group can be modified. To save the modifications, press „**Save**" button. By pressing „**Reset**" button, the last saved data can be restored.
To add a new client group press „**Add New**" button, then fill in the textboxes and save.

Default Client Group: here the default client group can be modified, to which the newly registered GPRS devices are assigned automatically. To modify the setting, select the desired client group from the drop-down menu, then save the modification by pressing „**Save**" button.

3.3.5 MVP Clients



In this menu the registration and configuration of the MVP client softwares can be performed.

To register a new MVP client software, press „**Add New**” button, fill in the textboxes, then save the data using „**Save**” button.
To modify the data of a registered MVP client software, press „**Edit**” button, perform the desired modifications, then save the changes using „**Save**” button. By pressing „**Reset**” button, the last saved data can be restored.
After installation, the MVP client software dedicates itself to the computer, which means that it generates a hardware key from the given computer's hardware configuration, and sends this key to the server each time it connects to the server. In this manner the software will not operate if it is copied to another PC, because this will have a different harware key which will not be accepted by the server. The same happens if the hardware configuration of the computer is changed, e.g. in case of replacing the motherboard, processor, videocard, or other component. For such cases use the „**Save and Clear HwKey**” button. If pressed, the server deletes the registered hardware key and will register the new key which will be sent by the client software from the computer with the changed hardware configuration.

Explanation of the textboxes and header elements:

Client Name: desired name can be entered (e.g. given company site)

Username: the same user name, which is set in the given client software

Password and confirmation: the same password and its confirmation, which is set in the given client software

CTID Timeout: if the given client software does not respond for a Contact ID message within the interval entered here, then the server forwards the message to the client software which has the next priority level

Last IP: the IP address from which the given MVP client software has last connected

Status: shows the status of the given client software (green icon = available, red icon = unavailable). The status display is not refreshed automatically, it can only be refreshed by changing between menus.

Details: by pressing „+”, the client group, event filter and priority settings of the given client software appear.

The MVP client softwares can be rated in two groups: active and inactive. The active MVP clients are the ones which operate, the inactive ones are the unused ones, to which the server does not forward any events. If for example the use of an MVP client is temporarily unnecessary, this can be moved in the inactive group by pressing „**Inactivate**” button, later it can be reactivated with „**Activate**” button.

After opening the details, there is possibility to modify the given MVP client software's client group, event filter and priority level, and to add new client group.
To add a new clint group, press „**Add New**” button, perform the settings, then save using „**Save**” button.
To modify an assigned client group or its settings, press „**Edit**” button, perform the desired modifications, then save the changes using „**Save**” button. By pressing „**Reset**” button, the last saved data can be restored.

Settings of the client group edit menu:

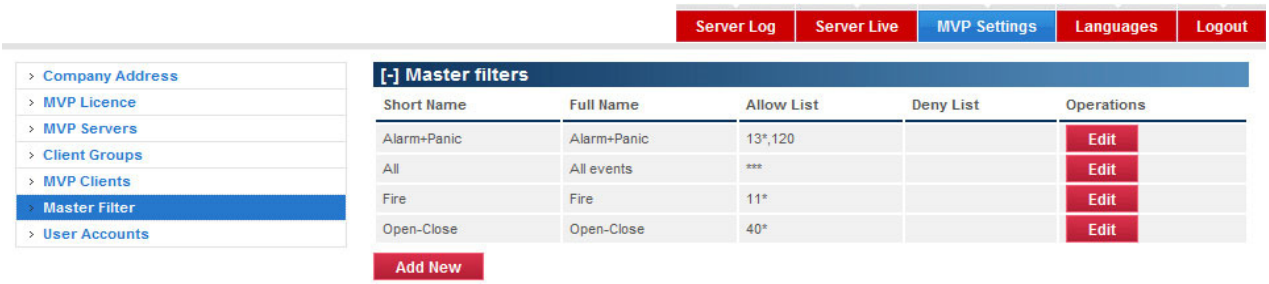
Client ID: fixed MVP client software identifier, this cannot be modified

Client Group: the client group, of which events you wish to forward to the given MVP client

Master Filter: the event filter created in „Master Filter" menu can be assigned here to the given client group, referring to the given MVP client software

Master Level: an event sending priority level (Master1 - Master9, Visitor) can be assigned to each client group, referring to the given MVP client software. The highest priority level is Master1, the lowest is Master9. The server forwards the events towards the MVP client softwares in this order, by taking in consideration the „Timeout" setting of the given MVP client software (the event is forwarded first to the client software which has Master1 priority level for the given client group, if this does not respond within the time set in „Timeout" section, then the event is forwarded to Master2, and so on). If „Visitor" priority level is selected, the given MVP client software receives always the given client group's events, but cannot confirm them (serves only for informative monitoring).

3.3.6 Master Filter



In „Master Filter" menu the event filters can be configured. The event filters provide possibility for separation, filtering and directed forwarding of events towards certain MVP client softwares (e.g. forwarding of alarm events only towards the alarm monitoring station(s), and service events only towards the technical monitoring station(s)).

To add a new filter press „**Add New**" button, enter the desired parameters, then save the data using „**Save**" button. To modify an existing filter peress „**Edit**" button, perform the desired modifications, then save the changes using „**Save**" button. By pressing „**Reset**" button, the last saved data can be restored.

Settings of the filter edit menu:

Short name: a desired short name can be entered for the given filter, which appears in the drop-down list when editing MVP clients

Full Name: a desired full name can be entered for the given filter

Allow list: permitted (3 digits) Contact ID codes, must be separated with comma

Deny list: denied (3 digits) Contact ID codes, must be separated with comma

In the allow and deny lists the certain Contact ID codes must consist of 3 digits, in case of enumeration they must be separated with comma (e.g. for test report and battery failure: 602,302).
There is also possibility to specify event groups using „*” character. This character substitutes any digit (e.g. 3** means all Contact ID codes which begin with 3).

The filter's operation principle:

- If the given Contact ID code exists in the deny list, then it is DENIED
- If the given Contact ID code does not exist in the deny list, but exists in the allow list, then it is PERMITTED
- If the given Contact ID code does not exist in the deny list nor in the allow list, then it is DENIED
- If the given Contact ID code exists both in the deny list and in the allow list, then it is DENIED

The deny list has the priority against the allow list.

3.3.7 User Accounts

Users can be configured in „User Accounts” menu. Basically two types of users can be registered: **Admin** and **Operator**. Admin users have maximum access on the server's web interface, while Operators cannot perform modifications, they can only view the data and the settings.
To add a new user press „**Add New**” button, fill in the textboxes, then save the data using „**Save**” button. To edit an existing user press „**Edit**” button, perform the desired modifications, then save the changes using „**Save**” button. By pressing „**Reset**” button, the last saved data can be restored.

Elements of the user edit menu:

User ID: fixed user identifier, this cannot be modified

Username: desired user name used to login on the server's configuration page. The user name is case sensitive.

Last login IP: the IP address from which the given user has last logged in (cannot be modified, is just informative data)

Last login date: the given user's last login date (cannot be modified, is just informative data)

Full Name: the user's full name

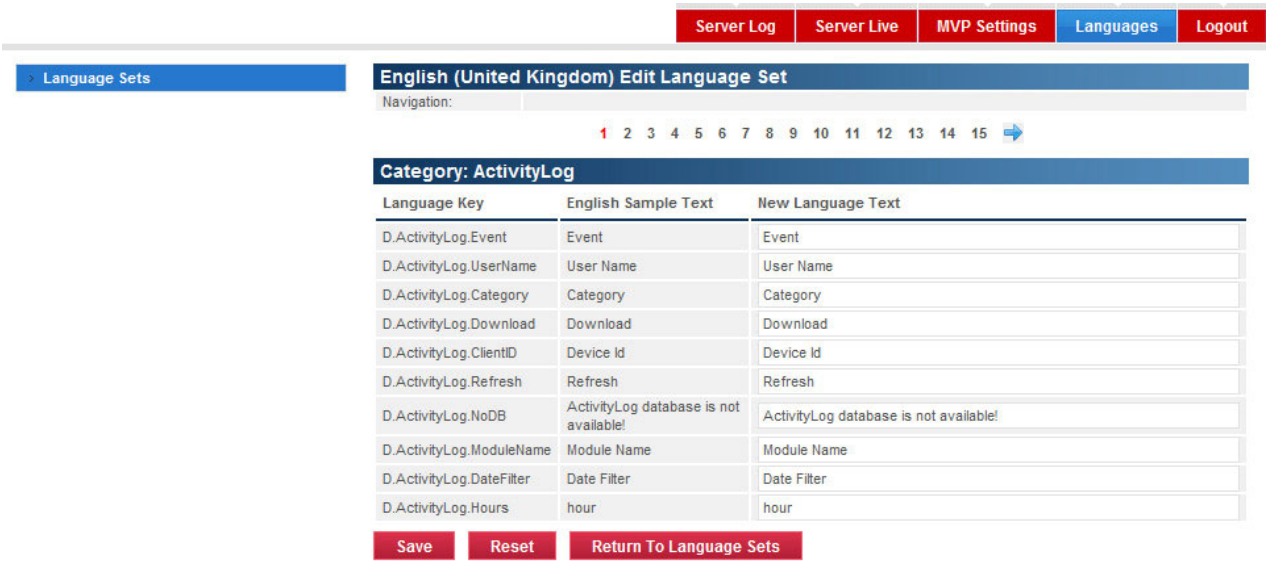
Password and Confirmation: the desired password used to login, and its confirmation. The password is case sensitive and must consist of at least 5 characters

User Group: the type of the user (access level), can be selected from drop-down list

When configuring users, take in consideration that at least one Admin user must exist in the system, therefore the system does not allow to modify all the user's access level to Operator. Operators can modify only their own names, user name and password.
The login access of certain users can be denied or permitted using „**Disable**"/"**Enable**" buttons.

3.4 Languages

The „**Language / Language Sets**" menu provides possibility to modify, customize and translate to other languages the texts and captions of the server's web interface. If using more servers in the system, the modifications are replicated to the other servers as well.
To modify an existing language set press the „**Edit**" button of the given language. In the language edit menu the texts and captions of the web interface are sorted by categories on more pages. Navigation between pages can be done by clicking on the page numbers or on the arrows. Perform the desired modifications in the „**New language text**" section, then save the changes using „**Save**" button. By pressing „**Reset**" button, the last saved data can be restored.



Default Language Set: it can be selected from the drop-down list by company, which language set to be used by default when accessing the web interface. To modify the setting, select the desired language from the drop-down list, then press „**Save**" button. In case the display is still necessary on a different language, there is possibility to select the desired language from the existing and enabled language sets using the drop-down menu when logging in.

Create New Language Set: to create a new language set, select the desired langage from the drop-down list, then press „**Add New**" button. Thereafter the selected language set is created and is opened automatically for editing, where you can do the translation as described above.

If necessary, the availability of certain language sets in the drop-down menu of the login page can be disabled/enabled using „**Disable/Enable**" buttons.

3.5 Logout

The „**Logout**" button serves for exiting the web interface. After pressing it, the server loggs out the user logged in, then the browser window is closed automatically.

4 MVP client software

The MVP client software is the application used to receive the events forwarded by the MVP server, and its role is also to forward the received events through serial port towards the alarm monitoring software. The serial data communication protocol of the MVP client software is similar to the protocol of PSTN alarm monitoring receiver devices.

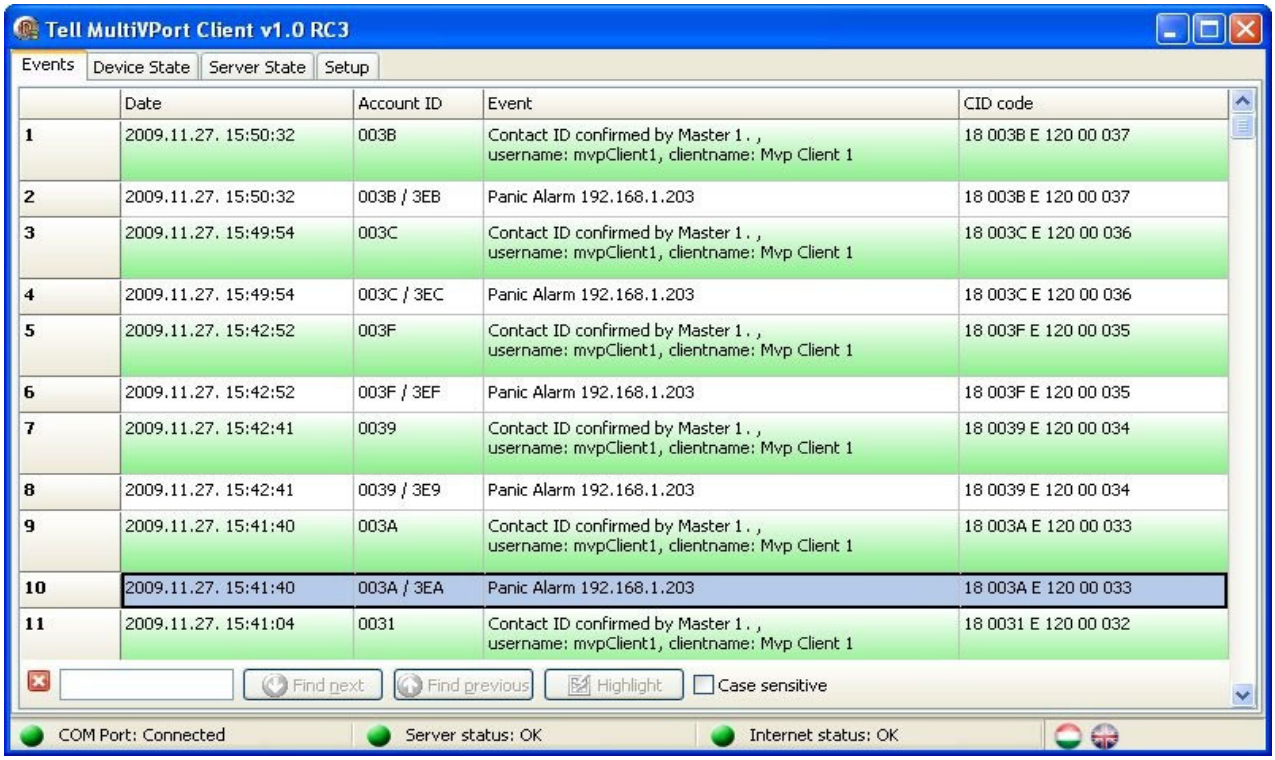
The language of the user interface can be selected using the language icons found in the lower right corner of the program window.

- **Operation principle, basic concepts**

When a GPRS device sends a Contact ID event, the server forwards this event to all authorized MVP client softwares (this is called broadcast), according to the set event filters. So the event os received by all MVP clients, to which the given GPRS device's client group is assigned, and for which the given Contact ID event is not denied in the event filter, i.e. the event filter lets it through. According to the priority levels (Master1-Master9, Visitor) of the MVP client softwares, the event is forwarded first through serial port towards the alarm monitoring software by the MVP client which has the highest priority level (Master1), the event is displayed in the other MVP clients only as an information, specifying the Contact ID code itself and indicating the client group and the priority level of the MVP client which should confirm the event. This informative message is qualified as „Info event" and the given MVP client will not confirm it towards the server. There is possibility to generate Contact ID from info event and to forward it once towards the monitoring software through serial port.
If for some reason the MVP client with the highest priority level does not confirm the event (e.g. it has lost the connection with the alarm monitoring software, or has no connection to the internet), then the MVP server resends the event to all concerned MVP clients, but this time the one with the next priority level (e.g. Master2) forwards the event to the alarm monitoring software and confirms it. At the other MVP clients this event is received as info message (confirmation is requested from Master2). If necessary, this procedure continues until one of the MVP clients confirms the Contact ID event, or until the event is resent. If an event is confirmed by an MVP client, or the server has forwarded the event to the connected Master1 – Master9 clients, but confirmation is not received from any of them, then an informative message is received by all MVP clients assigned to the given client group which indicates if the event reception was successful or not.
The server resends the Contact ID event towards the MVP clients by switching between priority levels until one of the clients confirms the event. If it has tried on all priority levels but no confirmation is received from any of the clients, then the server does not confirm the event towards the GPRS device. If thereafter the GPRS device resends (repeats) the Contact ID event, then the forwarding procedure starts from the beginning (the GPRS device resends the event until it reveives confirmation, or until the alarming time expires.)
If the GPRS device resends the Contact ID event several times during the server still waits for confirmation of this event from one of the MVP clients, then the server "rejects" the event repeated by the GPRS device, does not forward the repetitions again towards the MVP clients until it receives the confirmation.
When one of the MVP clients confirms the event successfully, the server sends a message to all concerned MVP clients which specifies the priority and the client group of the MVP client which performed the successful confirmation. This message is also qualified as „Info event". If no confirmation was received from any of the MVP clients for the broadcasted Contact ID event, the server indicates this too to all clients in the given client group by sending an „Unsuccessful Contact ID Broadcast" message.

Service events: the messages which indicate loss and restoration of connection, and 12h test reports sent by GPRS devices are qualified as service events.

4.1 Events



The events and messages received from the MVP server(s), as well as the intermal messages of the MVP client software are displayed in the „**Events**" menu.

Attention! The MVP client software does not store the received events, only displays and forwards them through serial port, therefore it does not substitute in any form an alarm monitoring software!

The software's event list is capable to display 2100 events, and when exceeding this number, last 300 events are automatically deleted from the list.

Columns of the event list:

Date: date and time of event reception

Account ID: user account ID of the device from which the event has been received

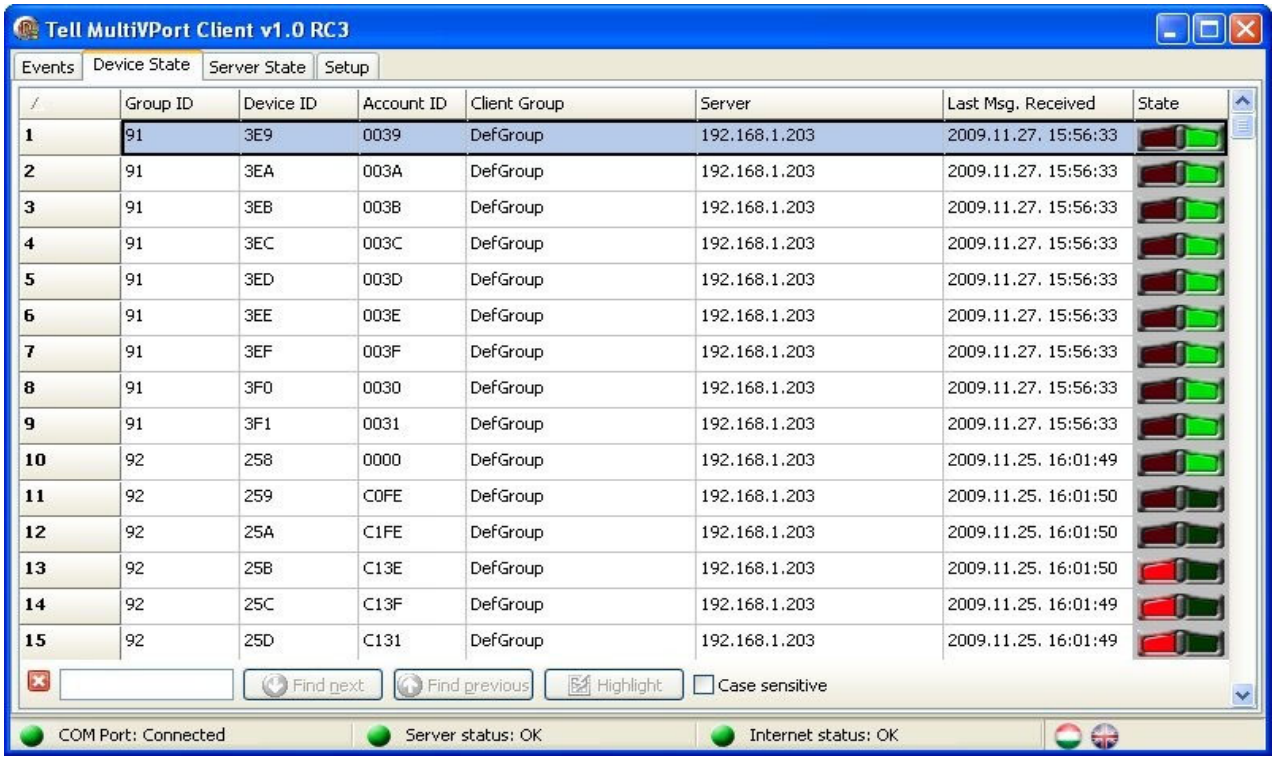
Event: event description, which can be customized by editing the **CID.ini** file found in the software's directory, where is possibility to modify the program's internal Contact ID codes and their names.

CID code: the event's Contact ID code

The incoming contact ID events which are to be confirmed are not highlighted with any colour in the list.
The info events which indicate successful confirmation are highlighted with green in the MVP client's event list, while the ones that indicate unsuccessful confirmation are highlighted with yellow (unsuccessful broadcast). The trouble messages (e.g. no confirmation is received from the alarm monitoring software for an event forwarded through serial port) are highlighted with red.

Searching for a desired text part is possible using the searching section found in the lower part of the program window. „**Find next**" and „**Find previous**" buttons can be used to jump on the next, respectively on the previous searched text part. „**Highlight**" button can be used to highlight all text parts in the list which match the searched text part. By enabling „**Case sensitive**" option, the searcher makes difference between upper and lower case letters.

4.2 Device State



/	Group ID	Device ID	Account ID	Client Group	Server	Last Msg. Received	State
1	91	3E9	0039	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
2	91	3EA	003A	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
3	91	3EB	003B	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
4	91	3EC	003C	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
5	91	3ED	003D	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
6	91	3EE	003E	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
7	91	3EF	003F	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
8	91	3F0	0030	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
9	91	3F1	0031	DefGroup	192.168.1.203	2009.11.27. 15:56:33	
10	92	258	0000	DefGroup	192.168.1.203	2009.11.25. 16:01:49	
11	92	259	C0FE	DefGroup	192.168.1.203	2009.11.25. 16:01:50	
12	92	25A	C1FE	DefGroup	192.168.1.203	2009.11.25. 16:01:50	
13	92	25B	C13E	DefGroup	192.168.1.203	2009.11.25. 16:01:50	
14	92	25C	C13F	DefGroup	192.168.1.203	2009.11.25. 16:01:49	
15	92	25D	C131	DefGroup	192.168.1.203	2009.11.25. 16:01:49	

The „**Device State**" menu provides information about the status of the GPRS devices which are assigned to the same client group as the MVP client software.

Columns of the table:

Group ID: the GPRS device's group identifier, this is individual for each company

Device ID: : the GPRS device's identifier (serial number)

Account ID: the GPRS device's user account ID for monitoring station

Client Group: th client group to which the GPRS device has been assigned on the server

Server: a server's IP address or domain name, to which the GPRS device is actually connected

Last Msg. Received: the date and time of reception of the event or test report sent last by the GPRS device

State: the connection status of the GPRS device

green is lit = connected to the server

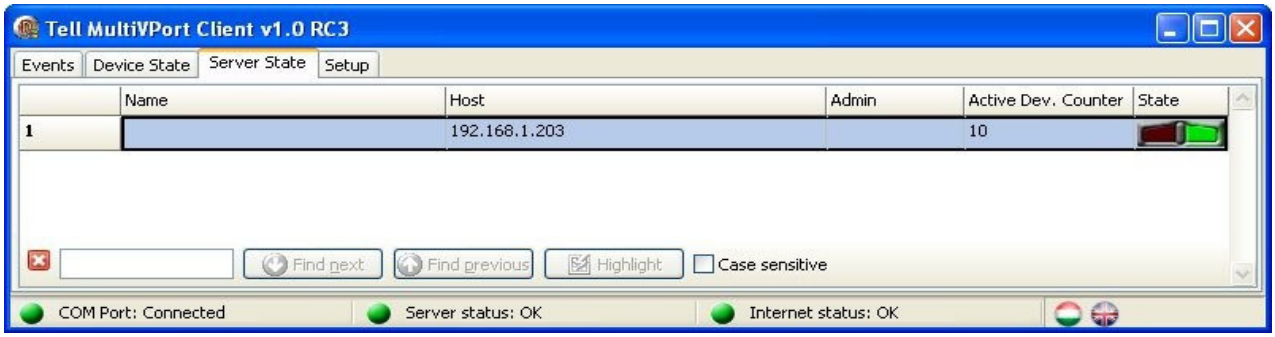
red is lit = not connected to the server

green and red blink together = there is no connection between the MVP client software and the given MVP server (the status of the GPRS device is uncertain, the "device connection timeout" has not expired yet, but it has also not connected to other server yet)

none of them are lit = there is no connection with the GPRS device for more than 168 hours

The indicators found in the „**State**" column are automatically refreshed each second, while refreshment of all other data in the table is performed in the time interval set at „**Setup / Server / IP HeartBeat Rate**" section.

4.3 Server State



The „**Server State**" menu provides information about the status of the server(s) which belong(s) to the system.

Columns of the menu:

Name: the MVP server's name

Host: the server's IP address or domain name

Admin: a gray tick indicates if the server is a master (admin) server

Active Dev. Counter: the number of GPRS devices which are actually connected to the server

State: connection status between the server and the MVP client software

green is lit = connection is established
red is lit = no connection
none of them are lit = connection establishing in progress

In case of losing the server connection, the MVP client attempts to reestablish the connection with the server(s) by 3 seconds.

The server status is displayed automatically and immediately on a change, while the number of active devices is refreshed each second.

Adding further servers: can be performed in the servers.ini file. Data format:
Must begin with [Servers] , then each server must be added in new line as follows:
IP1=ip0:port0
IP2=ip1:port1

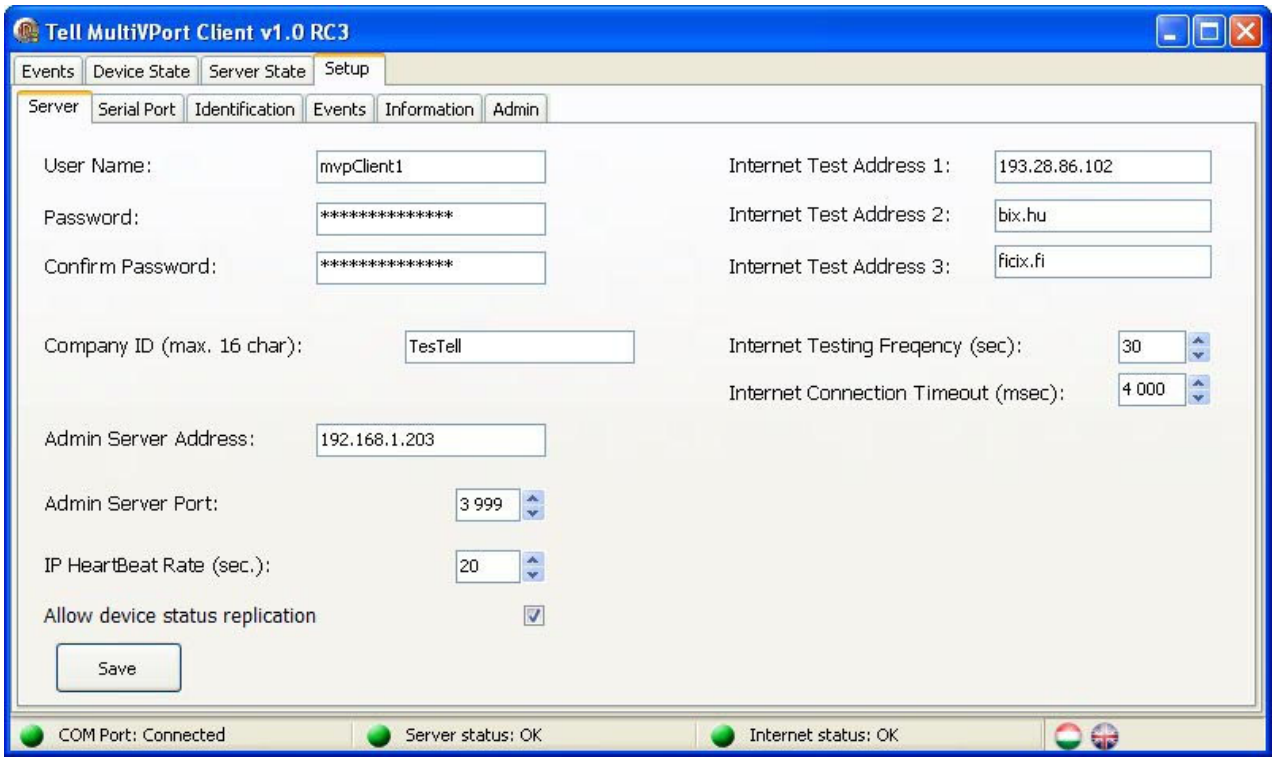
Example for adding one more server:
[Servers]
IP1=192.168.1.31:3999

For any modification performed in servers.ini file, the MVP client must be restarted in order to load the new settings. You can verify in the MVP client's „**Server State**" menu whether the new settings took effect.

4.4 Setup

The settings related to and necessary for the operation of the MVP client software can be configured in the „**Setup**" menu.
To view or modify the settings administrator password is requested. The default password is: ***admin***, which can be changed in the „**Admin***"* menu.

4.4.1 Server



The admin server settings and the settings necessary for internet connection testing can be configured in the „**Server**" menu.

Settings:

User Name: the user name which is set in the MVP server's „MVP Settings / MVP Clients" menu, regarding to the given MVP client software

Password, Confirm Password: the password which is set in the MVP server's „MVP Settings / MVP Clients" menu, regarding to the given MVP client software

Company ID: the fixed company ID which is set by the manufacturer in the MVP server's „MVP Settings / Company Address" menu

Admin Server Address: the IP address or domain name of the main MVP server

Admin Server Port: the communication port of the main MVP server (default: 3999)

IP HeartBeat Rate: it can be specified in seconds, how often the MVP client should send test signal towards the MVP server and synchronize date and time, respectively request GPRS device list from the server (changing this parameter requires technical expertise, since too rare requests may result loss of connection, while too frequent heartbeat sending may result network and computer overload)

Internet Test Address 1,2,3: three arbitrary IP addresses or domain names used for testing the internet connection

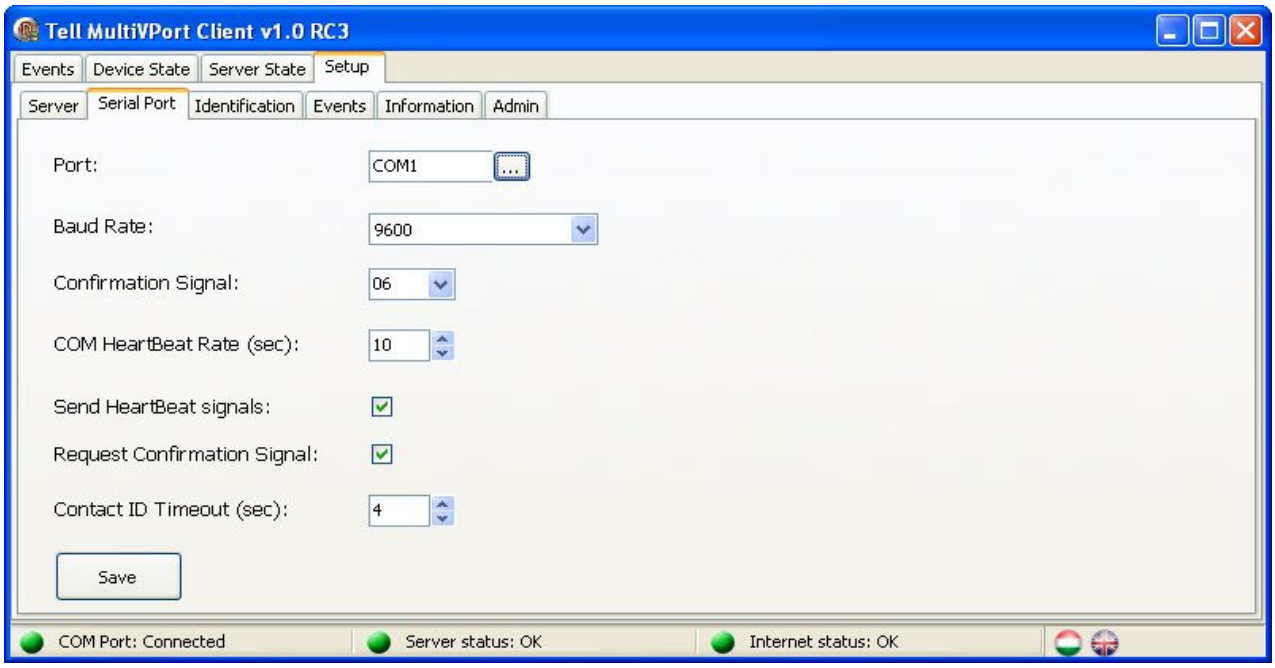
Internet Testing Frequency: it can be specified in seconds, how often the MVP client must check the existence of the internet connection. In case of internet connection loss, the program generates the trouble message within the time specified in this section, but at the latest when this time expires.

Internet Connection Timeout: it can be specified in milliseconds, how much the MVP client software should wait for answer when testing the internet connection, before it generates trouble message. Trouble message is only generated is none of the 3 test addresses can be accessed. If no test addresses are entered, the program generates connection failure message only a single time during its operation.

Allow device status replication: if enabled, the MVP client sends the GPRS device status information towards the other servers in the system, this way the status of the GPRS devices will be available on the web interface of these servers as well.

Press „**Save**" button to save the changes.

4.4.2 Serial Port



In the „**Serial Port**" menu, the communication performed through serial port between the MVP client software and the alarm monitoring software can be configured. The default serial settings are: **databit 8**, **parity 0**, **stopbit 1**, which can be modified in the setup.xml file found in the program's directory.

Settings:

Port: the port of the PC on which the MVP client software runs, that is connected to the alarm monitoring

Baud Rate: the baud rate of the communication between the MVP client software and the alarm monitoring software (default: 9600)

Confirmation Signal: the confirmation signal type of the alarm monitoring software (default: 06)

COM HeartBeat Rate: it can be specified in seconds, how often the MVP client software must send heartbeat signal towards the alarm monitoring software (this value must be lower than the alarm monitoring software's heartbeat setting, otherwise trouble messages of serial connection lost will be generated in the alarm monitoring software)

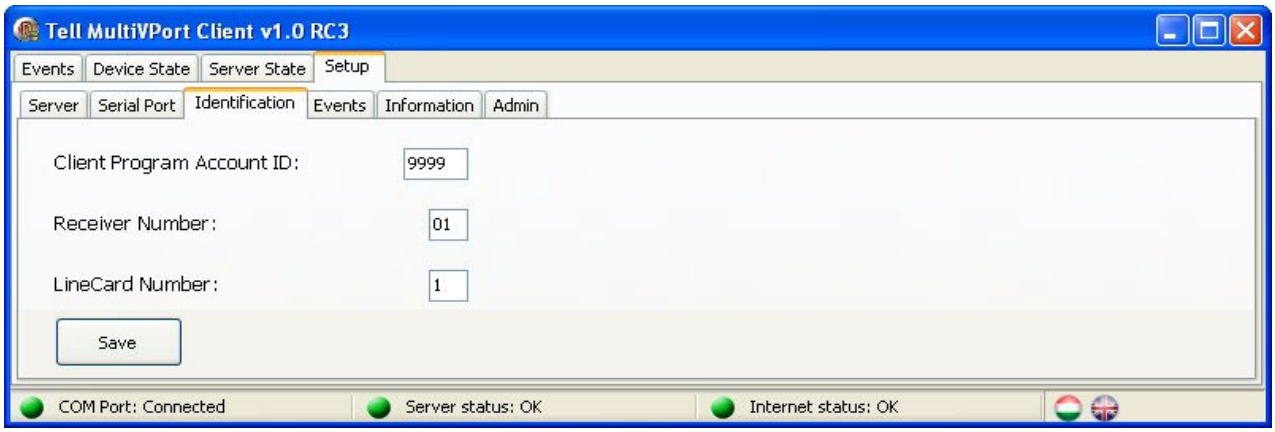
Send HeartBeat signals: if enabled, the MVP client software sends heartbeat signal towards the alarm monitoring software in the specified time interval

Request Confirmation Signal: if enabled, the MVP client software verifies if it receives the corresponding confirmation signal for the Contact ID events from the alarm monitoring software through serial port within the timeout

Contact ID timeout: it can be specified in seconds, how long the MVP client software should wait for the alarm monitoring software's confirmation signal after forwarding a Conatct ID event, before it generates trouble message

Press „**Save**" button to save the changes.

4.4.3 Identification



The „**Identification**" menu serves for configuration of the settings by which the alarm monitoring software identifies the MVP client software and its internal messages (just like a conventional PSTN alarm monitoring receiver device).

Settings:

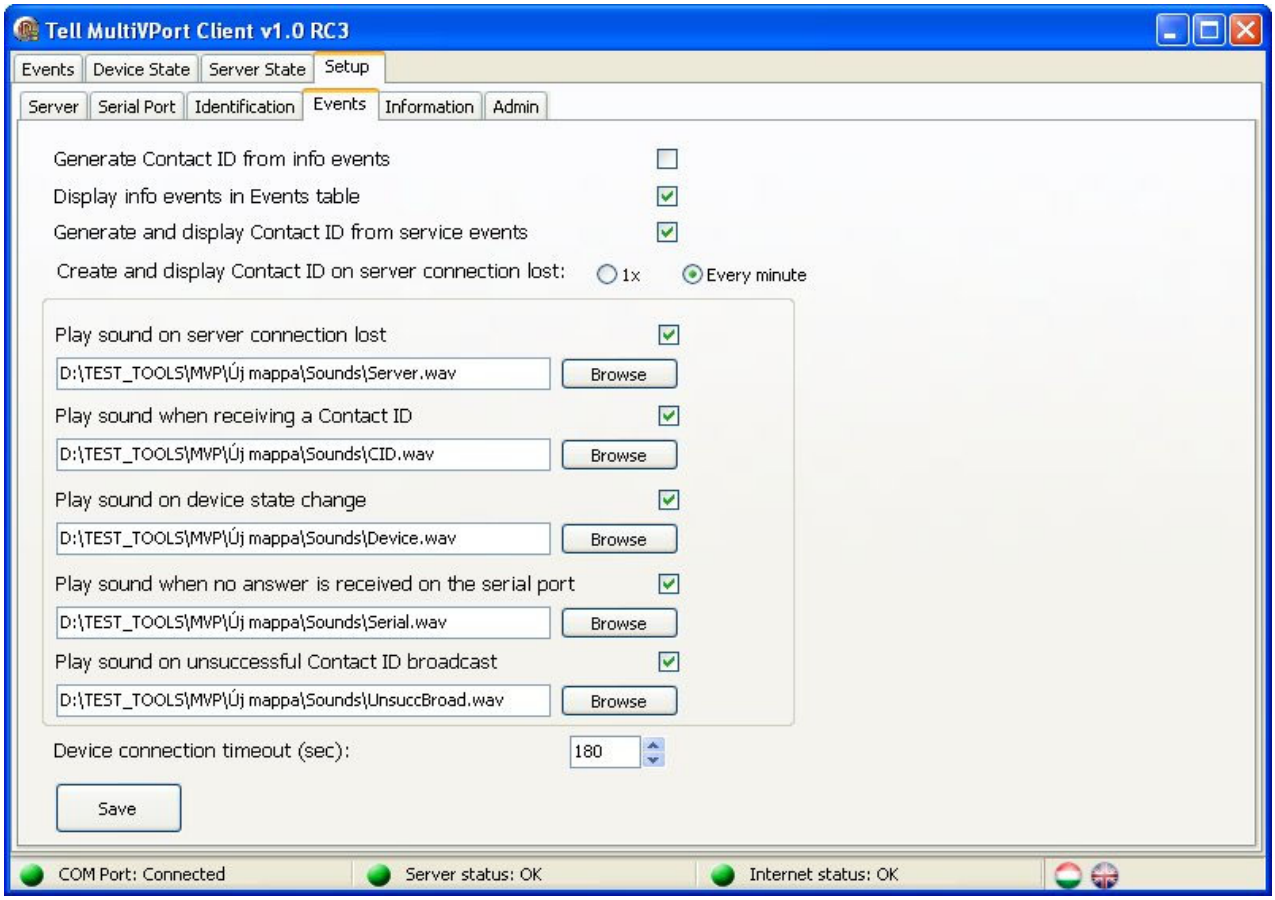
Client Program Account ID: the MVP client software sends its own internal messages (e.g. internet connection loss…) towards the alarm monitoring software using this account ID

Receiver Number: the MVP client software uses the receiver number specified here, when forwarding an event towards the alarm monitoring software

LineCart Number: the MVP client software uses the linecard number specified here, when forwarding an event towards the alarm monitoring software

Press „**Save**" button to save the changes.

4.4.4 Events



The „**Events**” menu serves for configuration of event and trouble message management.

Settings:

Generate Contact ID from info events: if enabled, the MVP client generates Contact ID events from incoming info events and sends them through serial port towards the alarm monitoring software. (the MVP client sends a certain event only once through serial port, except if no answer is received from the alarm monitoring software)

Display info events in Events table: if enabled, the MVP client displays the incoming info events in the “Events” menu. This option is fully independent from forwarding the info events through serial port, which can be disabled or enabled as described above.

Generate and display Contact ID from service events: if enabled, the MVP client displays the service events in the “Events” menu, as well as generates Contact ID event from them and forwards them through serial port towards the alarm monitoring software

Create and display Contact ID on server connection lost:

1x: if selected, the MVP client software notifies only once about the loss of the server connection, when the failure is detected

Every minute: if selected, the MVP client software notifies about the loss of the server connection when the failure is detected, then repeats the notification each minute until the failure ends

Play sound on server connection lost: if enabled, a desired „wav” audio file can be selected which will be played when the connection between the MVP client and the server is lost

Play sound when receiving a Contact ID: if enabled, a desired „wav” audio file can be selected which will be played when a Contact ID event is received

Play sound on device state change: if enabled, a desired „wav” audio file can be selected which will be played when the status of any of the connected GPRS devices is changed (conecction loss, connection restore)

Play sound when no answer is received on serial port: if enabled, a desired „wav” audio file can be selected which will be played when no answer is received from the alarm monitoring software after forwarding a Contact ID event or heartbeat signal through serial port

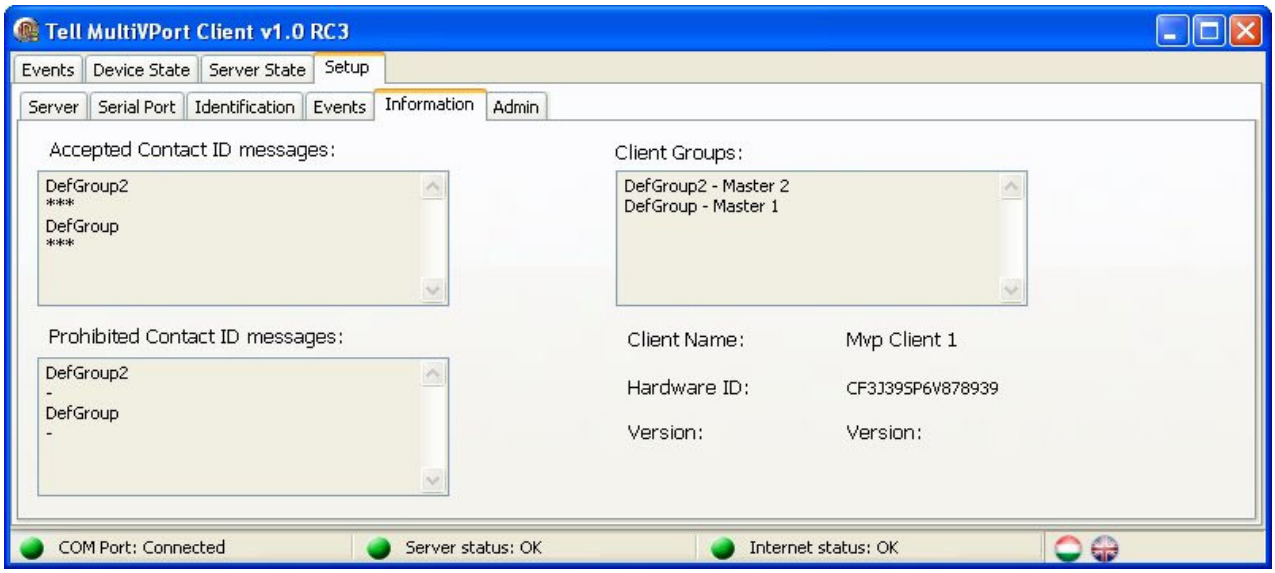
Play sound on unsuccessful Contact ID broadcast: if enabled, a desired „wav” audio file can be selected which will be played when no confirmation is received from any of the MVP clients for a Contact ID event forwarded by the server

Device connection timeout: it can be specified in seconds, how much time the MVP client software should wait before generating a trouble message after detecting that no periodic test report signal is received from a GPRS device. It is recommended to set this value a few seconds higher than the value of GPRS test report set in the GPRS device, to let one missed test report fit in the device connection timeout range, avoiding this way needless generation of trouble messages. The value of the test report frequency set in the GPRS device + the device connection timeout set here, must be higher than the IP heartbeat rate, to avoid unwanted message generation. It is recommended to set this value a bit higher than the test report frequency set in the GPRS device, e.g. 185 sec, if the value in the device is 3 min.

Example: if the GPRS device sends the periodic GPRS test report (heartbeat) by 180 seconds, and the “Device connection timeout” setting is 185 seconds, then the MVP client software waits 185 seconds after a periodic GPRS test report is missed. If the test report (or any Contact ID event from the GPRS device) is still not received during the 185 seconds, the MVP client generates trouble message about the loss of the connection with the GPRS device and changes the status of the device.

Press „**Save**” button to save the changes.

4.4.5 Information



The „**Information**” menu displays brief information about the server’s and the given MVP client’s settings. In this menu modification of the displayed settings is not possible.

Elements of the menu:

Accepted Contact ID messages: in this window the client groups assigned to the given MVP client are displayed, and the Contact ID event codes allowed for the given MVP client. The „*” character used in the Contact ID code means any character.

Prohibited Contact ID messages: in this window the client groups assigned to the given MVP client are displayed, and the Contact ID event codes denied for the given MVP client. The „*” character used in the Contact ID code means any character.

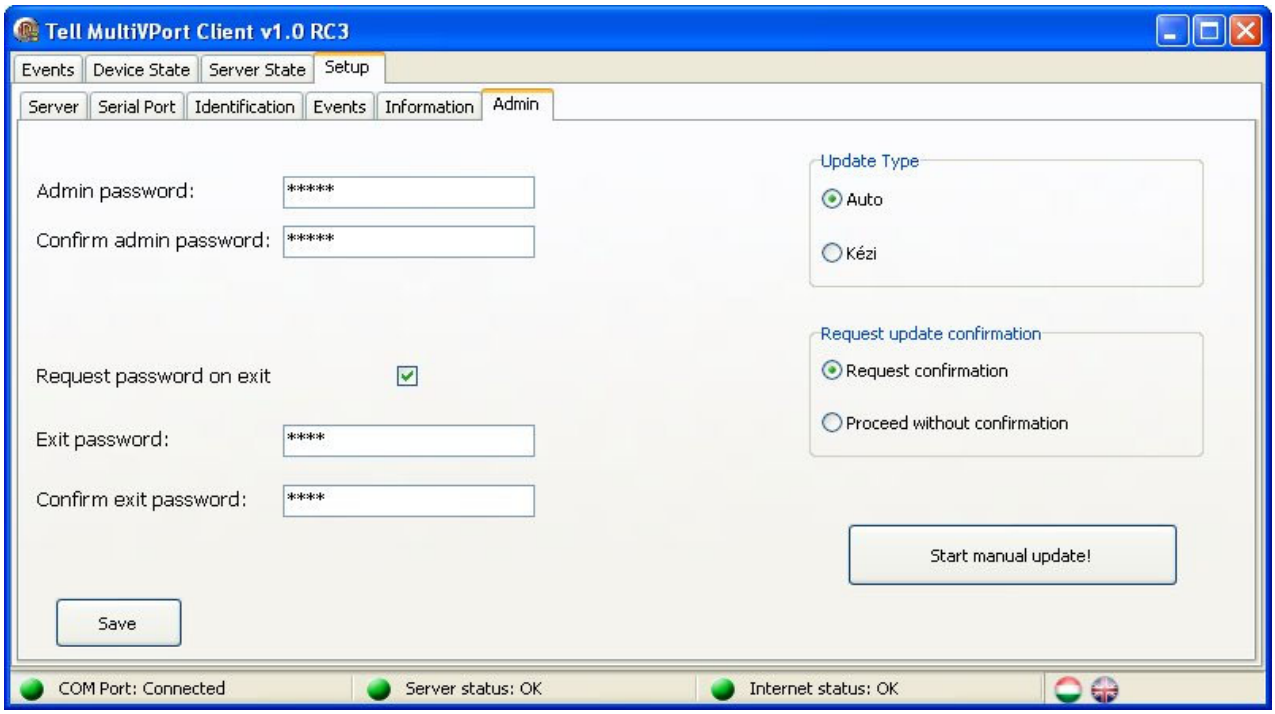
Client Groups: in this window the client groups assigned to the given MVP client are displayed, and the MVP client’s priority level in the given client group.

Client Name: the MVP client’s name, which is can be configured and modified through the server’s web interface

Hardware ID: the hardware key, by which the server allows the given MVP client software to connect to the system

Version: the MVP client’s software version

4.4.6 Admin



In the „**Admin**" menu the MVP client program's administrator and exit password can be changed, and software update settings can be configured.

Settings:

Admin password, Confirm admin password: the administrator password and its confirmation, which serves for accessing the setup menu.

Request password on exit: if enabled, the program requests password in case of closing the software, and does not allow closing until the right password is entered.

Exit passwort, Confirm exit password: the password and its confirmation necessary to close the program. The default exit password is: **exit**

Update Type:

- **Auto**: if selected, the program checks in 20 minutes intervals automatically if there is newer software version available on the internet or not
- **Manual**: if selected, the software update starts only by pressing „**Start manual update!**" button

Request update confirmation: if „**Request confirmation**" option is selected, the program will ask for confirmation before performing the software update, otherwise the update is performed without question and then the software is restarted automatically using the new version

Start manual update!: by pressing this button, the software update can be started manually.

Press „**Save**" button to save the changes.

4.5 Program status bar

In the program's status bar (the lower part of the program window) the actual status of the serial port connection, the server connection and the internet connection can be traced.

COM port connection status display:	
COM Port: Opened	COM port opened successfuly (is not busy)
COM Port: Closed	COM port opening failed (already busy)
COM Port: Connected	Connected to the alarm monitoring software
COM Port: Closed	Connection to the alarm monitoring software is lost

Server connection status display:	
Server status:	Establishing connection in progress
Server status: OK	Server connection established
Server status: ERROR	Connection to one of the servers is lost

Internet connection status display:	
Internet status:	Establishing connection in progress
Internet status: OK	Internet connection established
Internet status: ERROR	Internet connection lost

4.6 System requirements

System requirements of the PC on which the MVP client software runs:

- **Minimal requirements:**
  - Processor: 1Ghz
  - Memory: 512 MB
  - Internet bandwidth (download / upload): 1024 / 128 kbit/sec
  - Operating system: Windows 98
- **Recommended system configuration:**
  - Processor: Core 2 Duo 2.4GHz
  - Memory: 1024 MB
  - Internet bandwidth (download / upload): 4096 / 256 kbit/sec
  - Operating system: Windows XP / Vista / Windows7

5 Appendix

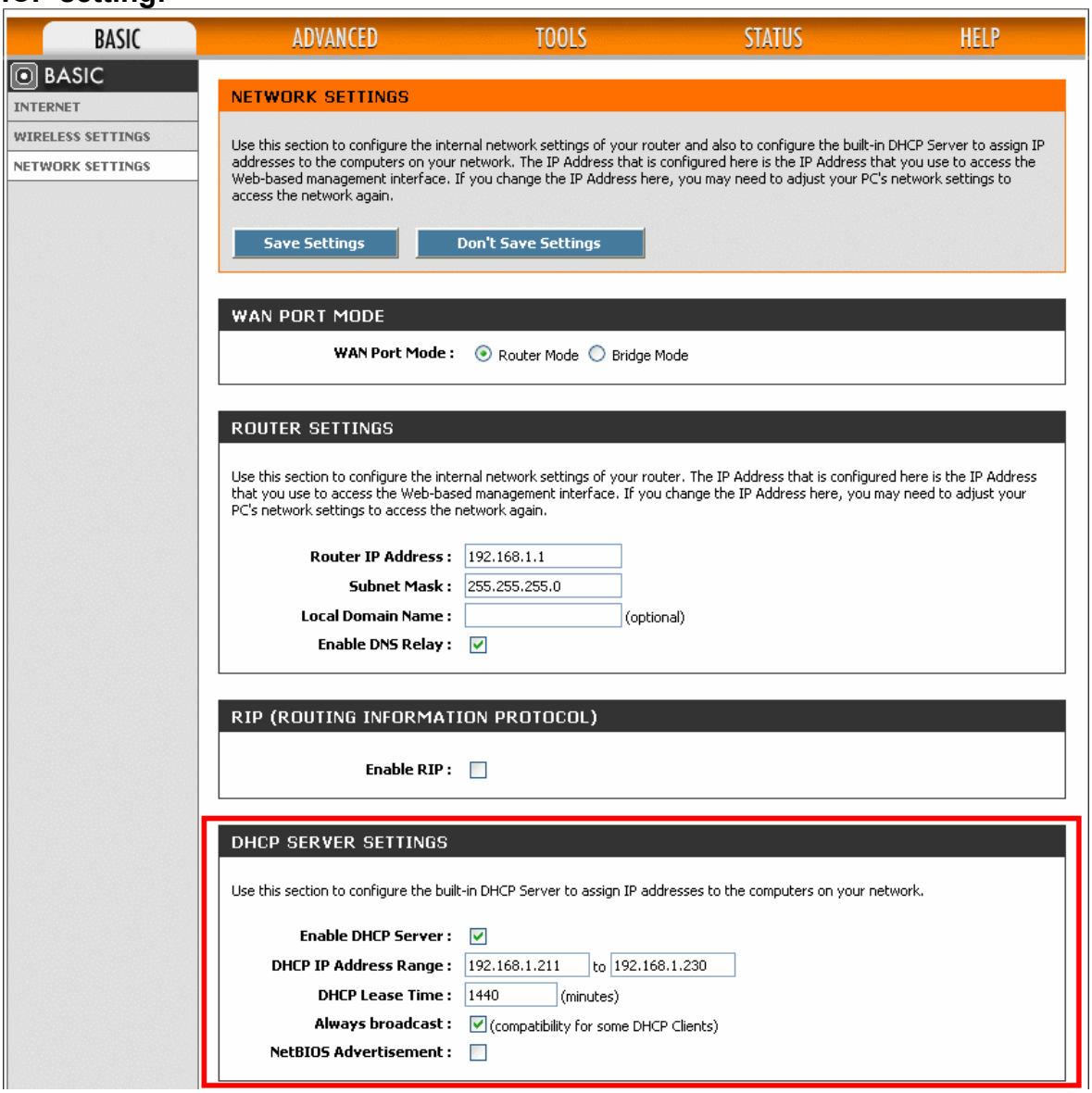
5.1 Router settings

According to the manufacturer's recommendation, the server has to be installed in a server hotel. Otherwise, in case the server is still installed elsewhere behind a router, then for the system's proper operation the following settings must be performed in the router:

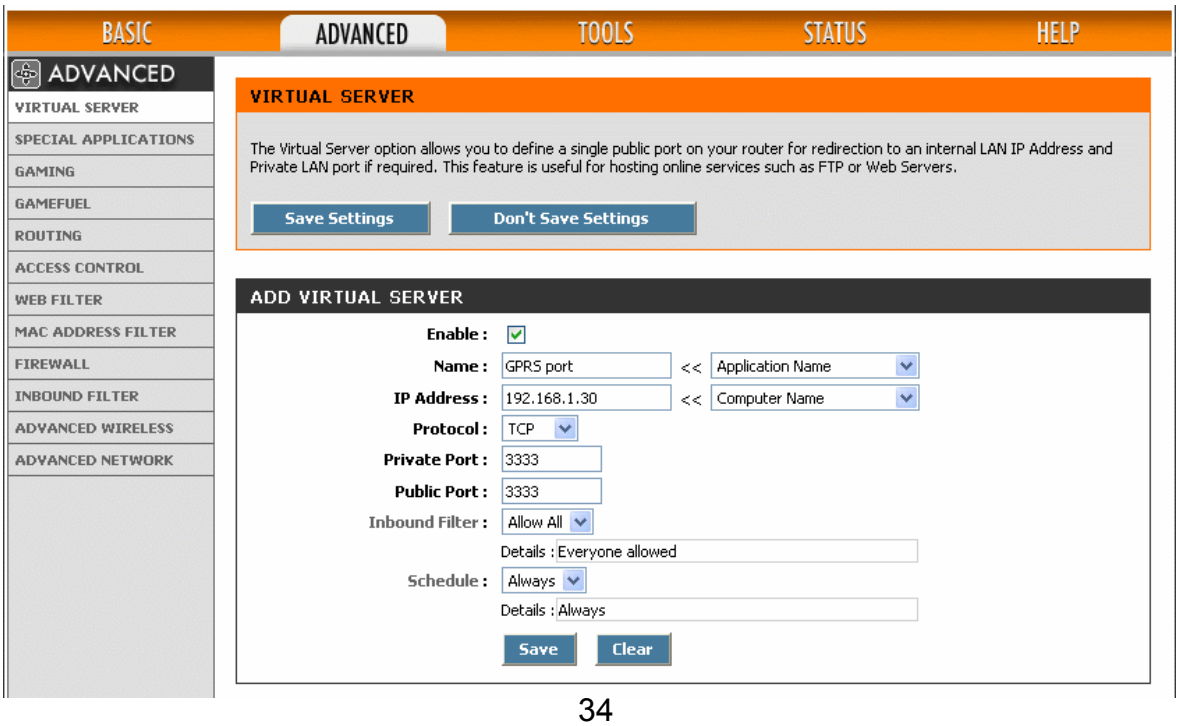
- In case of using DHCP, **make sure that the server's local IP address is not included in the DHCP range**.
- Forward the public communication port of the GPRS devices (default: 3333) to the server's local IP address, to port 3333 and make sure it is always enabled
- Forward the public communication port of the MVP clients (default: 3999) to the server's local IP address, to port 3999 and make sure it is always enabled
- Forward the communication port of the server's web interface (default: 8080) to the server's local IP address, to port 8080 and make sure it is always enabled, if you wish the web interface to be available from outside
- Forward the public service port (default: 22) to the server's local IP address, to port 22 but enable this only on the manufacturer's special request, for upgrade or remote diagnostics.

Example for router setting, if the server's IP address is e.g. 192.168.1.30: (The example is shown using a D-Link DGH 4300 router)

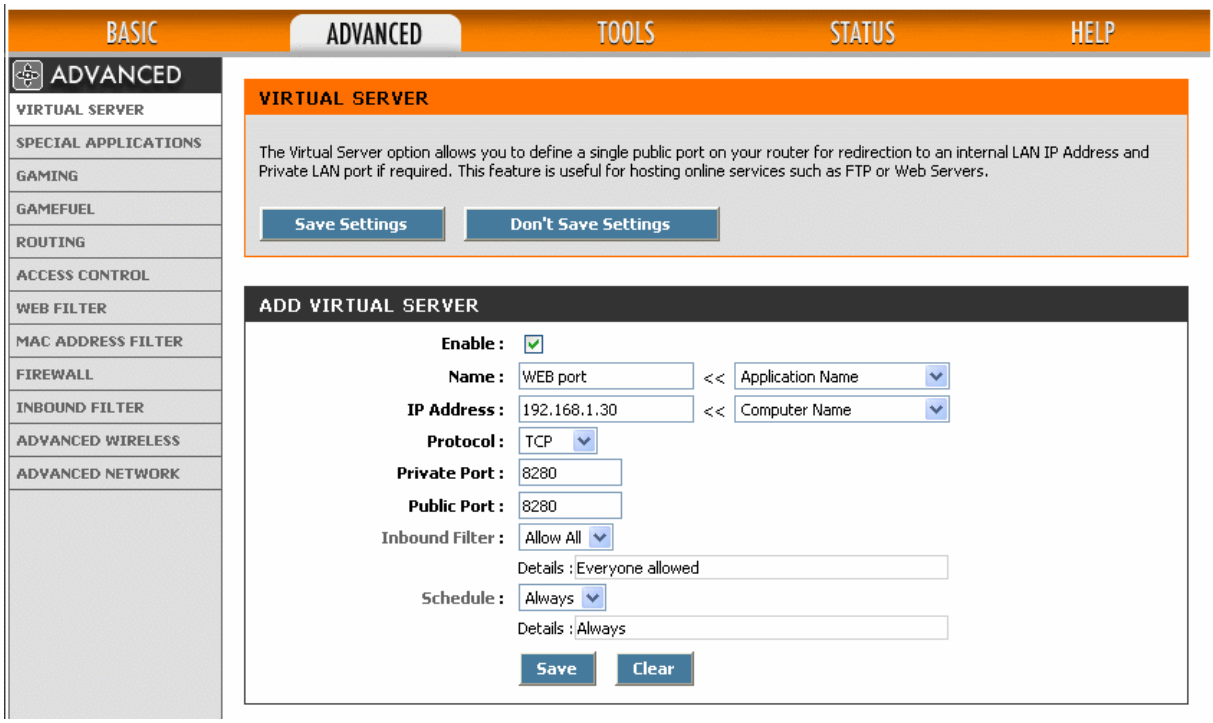
DHCP setting:



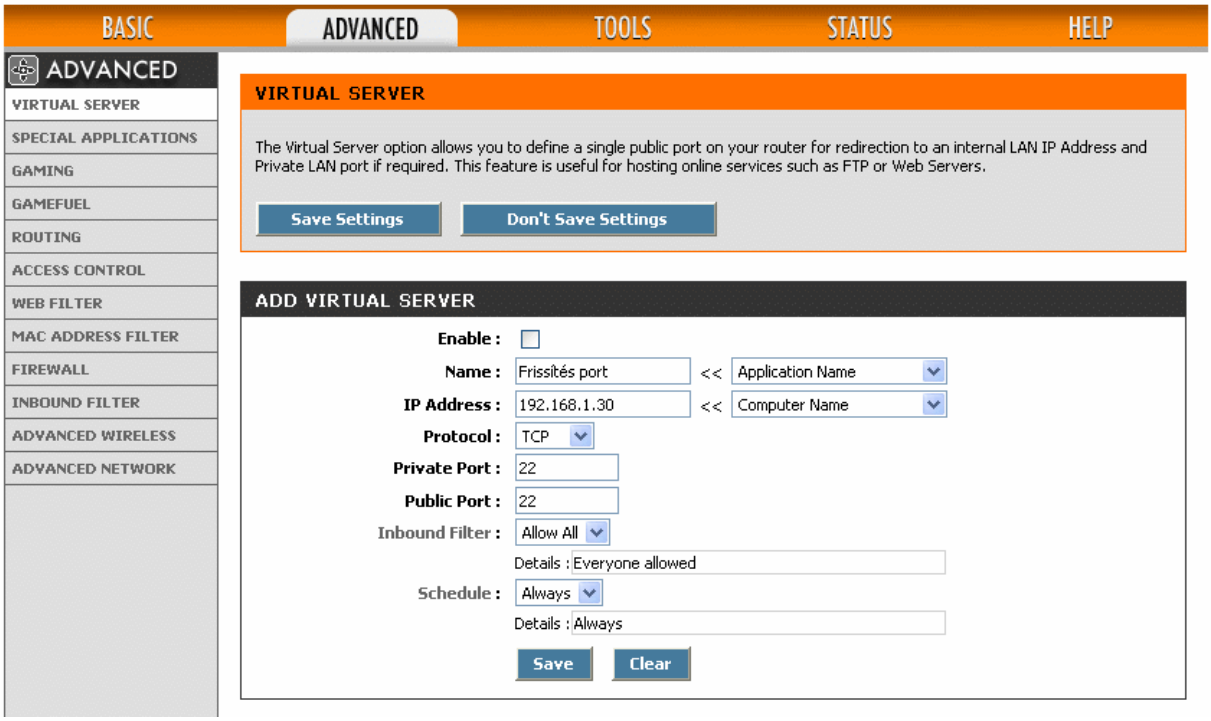
Enabling GPRS communication port forwarding:



Enabling server web interface port forwarding:



Service port forwarding:



5.2 Types and installation of GPRS devices

5.2.1 GPRS Adapter

Basic function of GPRS Adapter: forwarding the signals of the alarm panel to the monitoring station over a GSM / GPRS connection.

5.2.2 GPRS Pager

Basic function of GPRS Pager:
Can be used as an accessory to alarm centers, as a GPRS alarm transmitter, or as a 4 zone GPRS control panel that can be activated independently.
Further functions:

- SMS notification with custom text for all events
- Sending Contact ID for events occurring on the inputs and their restoration

5.2.3 Installation of the GPRS Adapter and GPRS Pager

A PC or laptop running Windows XP or Windows Vista operation systems is required for installing the tools (modules). In case of a laptop power supply over the USB port is not always enough for the device, so external power supply must be provided.
The software required for using the GPRS system have to be installed.
GPRS_Setup is used for GPRS settings (IP addresses, APNs, network test), USB and IP programming software are used for installation settings.
The module can be connected to the computer over an USB port. Settings can only be implemented this way when programming the module for the firs time. When there are GPRS settings in the module and it has already connected to the server, both GPRS and installation settings can be reprogrammed over the internet.

Do the following when installing the device:

- Before installation, measure the GSM signal strength at the mounting place of the GPRS device with your cell phone, or by connecting the module to the computer. If the measured signal strength values are not satisfactory (at least 17-20), change the mounting place of the module or you may have to install another type of antenna.
- Do not mount the unit at a place where it can be exposed to strong electromagnetic interferences, e.g. near electric motors
- Do not mount it at damp places or places with high degree of air humidity
- Antenna connection: the antenna can be fastened with an FME-M connector. The antenna supplied with the module provides good transmission under normal reception circumstances. In case of signal strength problems use another antenna with a higher gain, or look for a better mounting place for the product.

5.2.4 Setting the test report

Test report frequency is recommended to be set for 3 minutes for all modules. In case of longer test report frequency timing the GPRS provider may not detect traffic, and close connection with the module. This appears as a lost network connection in the system, which is detected by the module only after the expiration of the predefined period.
The longer this timing is, the more likely that the module cannot immediately send the signal to the server when an alarm event occurs, because it has to rebuild the lost network connection first. This results in sending a delayed signal. The 3 minutes test report accumulates to a mere 2-3 MB monthly traffic per device.

5.2.5 Setting IP addresses

“Primary server IP A” and “Secondary server IP A” addresses must be distinguished from among the 6 possible IP addresses that can be set. These will be the high priority addresses for the modules. The primary server address of the monitoring service has to be provided here.
The GPRS module will treat all other IP addresses as lower priority. This means that it disconnects from these addresses at intervals of 10 minutes, and will try to reconnect to one of the two high priority addresses mentioned before. Reconnection attempt may occasionally result in a lost connection message in the system.

5.2.6 GSM signal strength

Reliable operation later on is influenced by the displayed signal strength, the reception level of the GPRS module. If this is not acceptable, the GPRS network may close connection. The modules might keep losing the network, and they will be unable to send the network test report on time. As a recommendation from T-mobile, the service should only be used in areas with unexceptionable sound quality, or else using the GPRS service might present problems. Signal strength required for acceptable operation should reach at least level 17 on the scale of the diagnostic program, and it should not drop below level 15 during communication. In areas without unexceptionable quality (e.g. basement, outer areas, high, shielding buildings nearby), or if the device is on the cell border (contact your provider about this), the use of a directional antenna may be necessary.
Significant drop in signal strength may also occur if the antenna is not properly installed.
When locating an antenna, take into consideration that high quality transmission requires a ground potential for the antenna, which is provided by a metal case.

5.3 Mounting the GPRS devices, putting into operation

5.3.1 Mounting the GPRS Adapter

It is recommended to place the GPRS Adapter into the same metal case in which the alarm control panel is located. Drill a hole identical in size with the FME connector of the adapter, and fasten the connector into the metal case with the screw-nuts. Make sure the FME connector and the metal case get in galvanic contact. Connecting to the communication channel of the alarm panel is done by connecting the alarm control panel's phone line communicator output (RING – TIP) and the line input of the Adapter (GSM). If a PSTN line is also connected, it can be connected to the PSTN inputs of the Adapter.

Important: if the metal case of the alarm control panel is connectid to the protective ground, then also connect the Mini "V-" connector of the Adapter to this ground point!
In case of a plastic case and/or inadequate signal strength it may be necessary to install another antenna. Contact the manufacturer for more information.

5.3.2 Installing the GPRS Adapter

After performing the settings, mounting and connections, and inserting the SIM card, the device can be powered on (9-24 V DC on V+ and V- inputs). Before inserting it, make sure that the contact surfaces of the SIM card and the module's card case are clean, and free from contamination. It is significant to make sure that the power supply will be enough for the joint draw from the alarm panel and the GPRS adapter. Standby current consumption of the Adapter is 200 mA / 12 V DC, but during communication it can reach even 500 mA.
If the Adapter cannot draw the 500 mA from the output, it can result in communication problems and lost test signals. Read more about the programming and installation configuration in the product's operation and installation guide.

5.3.3 Mounting the GPRS Pager

If the module is mounted in a metal case, drill a hole identical in size with the FME connector into the metal case, and fasten the connector into the metal case. Make sure the connector and the metal case get in galvanic contact. In case of a plastic case the module can be placed entirely within the case.
A signal is initiated by a NC or NO contact between zone inputs Z1 – Z4 and input V-, depending on the settings. NO1 and NO2 are normally open relay contact outputs that can be controlled by events or by the phone depending on its programming. Their maximum load is 5A / 12 VDC each.

5.3.4 Installing the GPRS Pager

After performing the settings, mounting and connections, and inserting the SIM card, the device can be powered on (9-24 V DC on V+ and V- inputs). Before inserting it, make sure that the contact surfaces of the SIM card and the module's card case are clean and free of contamination.
The device can be powered on. Make sure that the power supply will be enough for the demand from module. Standby current consumption of the module is 100 mA, but during communication it can reach even 500 mA. Read more about the programming and installation configuration in the product's operation and installation guide.

5.4 Connecting GPRS devices to the server

A maximum of six connection IP addresses can be set up in the GPRS devices:

- 2 IP A (primary IP A and secondary IP A)
- 2 IP B (primary IP B and secondary IP B)
- 2 backups (1st backup and 2nd backup),

and it can be set for all configured IP addresses which APN connection to use from the two. With observing priorities, alarm transmission will be take place over one of these possibilities (including GSM voice call and the PSTN line as well in case of the GPRS Adapter).

If all the six available IP addresses are filled in, then after a successful connection to the GSM network, the module will attempt to reach the given IP addresses according to the following priority:

IP address	Number of connection attempts
Primary server IP A	2
Primary server IP B	1
Secondary server IP A	1
Secondary server IP B	1
Backup server IP 1	1
Backup server IP 2	1

and then it restarts the cycle.

Altering between two IP addresses takes an average 30 seconds.

Returning to the “Primary IP A” (or “Secondary IP A”) address:

GPRS devices must be primarily connected to “primary server IP A”, or “secondary server IP A”. If the devices connected to another configured server due to a lost connection, then they will try to return again to the “primary server IP A” address after a certain time.
The module is counting the time expired from the moment of connection, or from the last Contact ID signal, or from the moment the remote PC connection was lost. If it reaches 10 minutes, the device will try to return to “primary server IP A” address.
(10 minutes < return time < 10 minutes + GPRS test report frequency). The higher the GPRS test frequency, the longer it takes for the adapter to return to the primary IP address.
10 minutes are valid only if there is no event, but if a new event occurs, it restarts counting the 10 minutes.

After the GPRS device is powered on, it takes 35 seconds for the module to build the connection to the server. An alive connection between the module and the server can be verified in two methods:

- using the module's LED indicators
  Adapter:
  - pulsing green, red is off – connected to server;

  Pager:
  - pulsing green, red is off – connected to server and the module is not armed;
  - green and red are pulsing alternately – connected to server and the module is armed.
- using the module's programming software installed on a PC:
  start the "GPRS Adapter/Pager remoter" software installed on the computer, and prepare it for connecting to the module. Power on the module, connect it to the computer and establish the connection with the module. Click on "Module status / Communication details" and monitor the top left field of the newly opened window

Adapter: the meaning of fields appearing in the detailed communication window:

Right field	Displays the processes (AT commands) running in the Adapter
Upper left field	The communication of the Adapter and the server, and the main processes of the module
Middle left field	Summary of the Contact ID reports
Lower left field	DTMF based communication of the alarm control panel towards the Adapter (dialing, Contact ID reports)

Pager: the meaning of fields appearing in the detailed communication window:

Right field	Displays the processes (AT commands) running in the Pager
Upper left field	The communication of the Adapter and the server, and the main processes of the module
Middle left field	Displays switchings between operational modes
Lower left field	DTMF communication towards the Pager (e.g. controls from mobile phone)

5.4.1 Successful connection to the server

When server connection is established successfully, the following messages are displayed in the upper left field:

CONNECTING TO SERVER: Primary A	connecting to server Primary A in progress
G: Send(CONNECT)	
G: ACK_OK	connection established, confirmed
G: Auth.request	
G: Server Timeout=3	specifying the GPRS test report interval
CONNECTED TO SERVER	connecting successful
Version report sent.	

Then the GPRS test reports at the pre-configured intervals (default: 3 minutes):

G: Send(ALIVE)	sending the GPRS test report
G: ACK_OK	test report confirmed, connection OK

If reports have been generated in the meanwhile, they will be displayed as well.

5.4.2 Unsuccessful connection to the server

An unsuccessful connection to the server repeats the "**CONNECTING TO SERVER:**" message regularly, and displays the "**CONNECT FAIL**" message among the processes in the window on the right. If there is a problem with the inserted SIM card (contact, PIN code, not the correct card), the module will not get to display even these messages. Instead, "**!! SIM PIN CODE ERROR !!**" or "**!! SIM CARD ERROR !!**" are displayed.

If a SIM card or network connectivity error arises after installation, the **+CREG** value in the field on the right in the „communication details" window of the GPRS_remoter software will be other than **0.1**. In this case check SIM card connectivity. When **0.2**, the module is searching for GSM operator. If this value is **0.5**, then the card is in Roaming mode. This might happen at places close to the country border, if this service is enabled on the card. In this case disable the attempt to alter to Roaming mode with your provider, and use a directed antenna if this occurs because the device is at a cell border.

There might be several reasons for an unsuccessful connection:

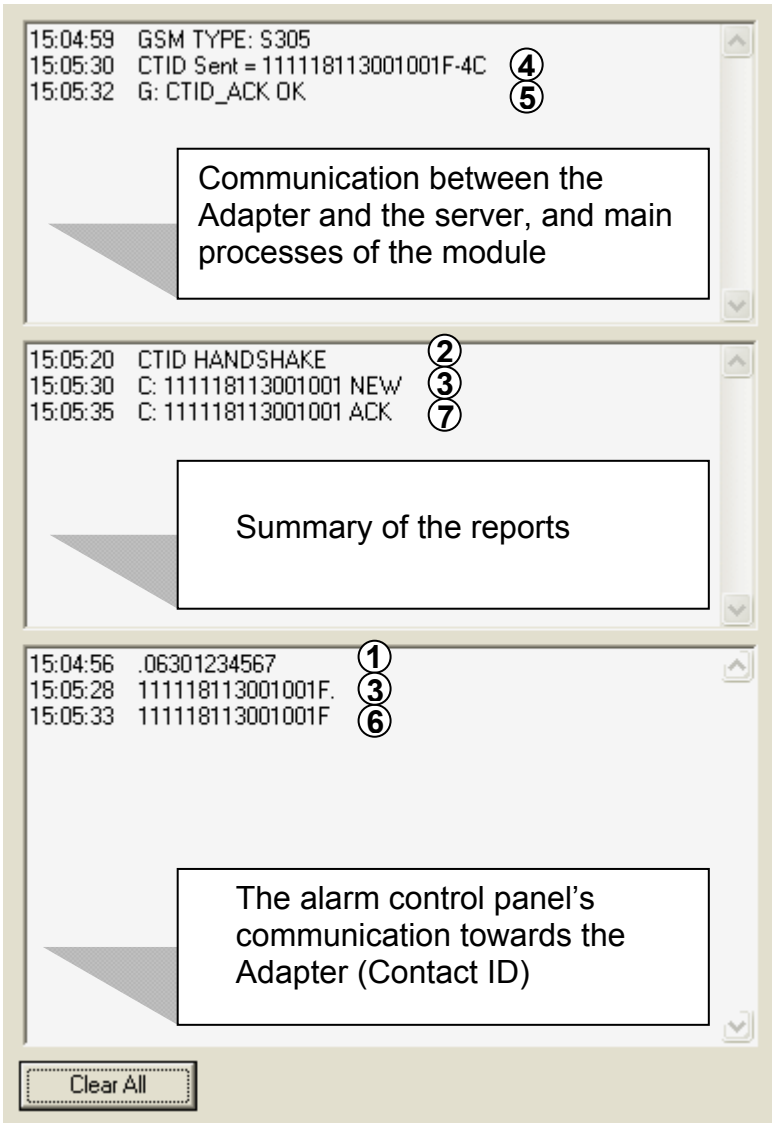
Possible reason for connection error	Troubleshooting
The configured IP address is incorrect	Check the IP addresses using the GPRS_setup software
The port set for the IP address is incorrect	Check the port(s) assigned to the IP address(es) using the GPRS_setup software
In case of public APN: the APN name is incorrect	Check the APN name using the GPRS_setup software
In case of a dedicated APN: the APN name and/or identifier is incorrect	Check the APN name, identifier, password using the GPRS_setup software
The selected APN is not the right one (APN1-2)	Check the selected APN using the GPRS_setup software
The GSM signal strength is not satisfactory at the mounting point of the device	Check the GSM signal strength using the GPRS_remoter software, and if it is not satisfactory, search for a better location for the module, or use a special antenna
PIN code request is enabled on the SIM card inserted into the module, and it was not or wrongly entered in the software when it was configured	Disable PIN code request on the SIM card, or if it is requred, set it using the GPRS_setup software
The module was previously installed with another SIM card, and the "FIX SIM" function was enabled in the software when it was configured	Check the status of the "FIX SIM" function using the GPRS_setup software. If it is enabled, disable it, then install the device with the correct SIM card. The function can be then enabled again if necessary
GPRS service is unavailable (there is a maintenance at the provider)	Ask your GSM provider
There is no internet connection on the server side	Check the router, the ADSL modem, and ask your internet provider

5.5 GPRS Adapter – reporting over GPRS connection

After the alarm panel has dialed the phone number, the Adapter transmits the handshake signal, and receives Contact ID events. They are forwarded to the server one by one, from where it receives the acknowledgement. The Adapter will not acknowledge the transmitted event towards the alarm panel until the acknowledgement arrives from the server. For this reason only at least every second attempt of the alarm panel will be acknowledged. This results from the GPRS network delay. **The system uses real acknowledgement**, which means that the acknowledgement towards the alarm panel is initiated by the acknowledgement of the monitoring station. This way the signal cannot be lost because the event will only be acknowledged if it really reaches the monitoring station and it acknowledged the signal.

The alarm panel waits approx. 1 second for the acknowledgement after the Contact ID signal, and then it repeats. This interval is usually not enough for the acknowledgement reply due to the GPRS network delay, so the alarm device receives an acknowledgement to the first repetition of the same Contact ID signal. For this reason it is important that the alarm panel is configured so that it repeats the same event until the acknowledgement.

Event transmission example:



1. The alarm control panel dials the monitoring station's phone number
2. The Adapter emits the handshake to the alarm control panel
3. The alarm control panel transmits the Contact ID event code to the Adapter, which receives it at the same time
4. The Adapter forwards the event code towards the server
5. The server confirms the reception of the event code (if the monitoring station received the report)
6. The alarm control panel repeats the Contact ID event code, because it has not received the confirmation
7. The Adapter confirms the event towards the alarm control panel

Report transmission when there is no GPRS connection
When there is no GPRS connection, the following three processes are executed regardless of the settings:

1. If the GSM network is not available, but there is a telephone line, it immediately switches to it
2. If the GSM network is available, but the module is still searching for an available server, and if there is a telephone line, it switches to the telephone line for the time of searching
3. If it has found a server, it hangs up PSTN connection at once (if there was one). (The call in progress might be aborted, but it will not result in loss of message, as the alarm control panel will repeat the event until it receives the confirmation signal.)

Depending on the settings, the module handles signals received during the absence of the GPRS network in one of the following ways.

Forward all events over GSM voice call
With this setting, the reports are transmitted to monitoring station in the following way:
If there is a GSM line and the module tried all the servers but none of them are available, then it switches to GSM voice call mode, i.e. it hangs up PSTN telephone connection, if there was one. (The call in progress might be closed, but it will not result in loss of message, as the alarm control panel will repeat the event until it receives the confirmation signal.)

- Switching to GSM voice call mode:

occurs 90 seconds after the received Contact ID, i.e. the alarm control panel is continuously attempting the alarm transmission because it does not receive the confirmation signal until the alarm transmission is successful, so it initiates the new call after the expiration of the 90 seconds over GSM voice call.

- Switching from GSM voice call mode back to GPRS:

Returning to GPRS mode occurs 120 seconds after the last transmitted event. Then the device attempts to connect to the server(s) according to the configured priorities.

Report only the following events over GSM voice call
With this setting, the reports are transmitted to monitoring station in the following way:
In the absence of GPRS connection the module only initiates sending reports over GSM voice call to the monitoring station if the event is specified on the list at the installation. “Less important” events not specified in this list will not generate GSM call costs.
Event codes must be specified as 4 hexadecimal digits in the list, where the first digit differentiates between the new event (“1”) and the restore event (“3”).
Use a “∗” character to define event groups when entering event codes. This means that any hexadecimal digits can arrive from the alarm panel at the place of “∗” character typed into the code, but if the other elements of the code match with the specified one, the event will be transmitted.

Switching to filtered GSM voice mode:
If the GSM network is available and the module tried to reach all the GPRS servers, but it cannot establish the connection or it received a Contact ID event and it could not transmit the report over GPRS within 90 seconds, then it switches to event filtering operation mode. In this case the module emits the “handshake” signal, receives the events of the alarm control panel, and confirms them (these will be lost), until it finds one that is specified on the list. If it finds an event that is on the list, it will not confirm it, and the report will be transmitted over GSM voice call at next dialing, beginning with the filtered event. The panel is continuously attempting the alarm transmission, which ensures that it will start a new dialing.

Events immediately following the filtered event will be transmitted within the same call, regardless if they are specified in the list or not, since the panel will not hang up the connection until it transmits all gathered events.

Switching from filtered GSM voice call mode back to GPRS:
The device returns to GPRS mode 120 seconds after it transmitted the last event. After this, the device attempts to connect to the server(s) again.

Do not use GSM voice call, alter to PSTN telephone line if available
If the GSM network is available and the module tried all GPRS servers, but could not establish the connection, or it received a Contact ID event and it could not transmit it over GPRS within 90 seconds, it switches to PSTN line and the next call will be accomplished over the PSTN connection. (Besides this, it will switch to PSTN line in the cases described earlier in this chapter.)

5.5.1 Configuring the alarm control panel

The adapter is suitable for connecting alarm control panels which use the Contact ID communication protocol, so panels not meeting the Contact ID standards should be avoided.

To ensure that transmission to the monitoring station will operate properly, the following communication settings should be applied in the alarm control panel used with the adapter:

- enable communication (dialing)
- set dialing to TONE operation method
- set communication protocol to Contact ID format
- set user account identifier
- set the monitoring station's telephone number (for reporting over GSM voice call); this must match the telephone number set in the GPRS Adapter, otherwise the module will not emit the handshake signal
- fill in the report codes (automatic or programmed Contact ID)
- set the number of dialing attempts (e.g. Paradox default setting is 8, possibilities are 1-15)
- set the time interval between repeating calls (e.g. Paradox max 255 seconds)
- set the number of repetitions for unacknowledged events within 1 call (e.g. Paradox 8 times)
- **The alarm control panel must repeat the same event until it is acknowledged! This is required by the Contact ID standard. Still, there are control panels that – even in case of unsuccessful transmission - attempt to send events circularly, by proceeding with the next event. Thus, the order of events arriving to the monitoring station will not match the real order, and the GPRS Adapter will not be able to acknowledge the event the way it should, if the repetition of the given event is preceded by several other events. This increases the time needed for transmitting the reports to the monitoring station, and endangers alarm transmission security! Do not use such an alarm control panel!** Certain alarm control panels offer the possibility to choose between the two operation methods. In such cases use the one complying with the standard.

Care must be taken about setting the multiple dialing attempts of the alarm panel. An unsuccessful signal transmission over the GPRS connection might even take 90 seconds – counted from the first unacknowledged event – for the GPRS adapter to alter to the network or to GSM voice call.

5.5.2 Testing communication

After installation, it is recommended to test the communication between the device and the alarm control panel by listening in, or with diagnostics software. Audio testing can be performed by connecting an active loudspeaker to the telephone line input of the alarm control panel, which makes the communication audible between the alarm control panel and the module. At the same time connect the module to the computer and start the GPRS_remoter software. Click on “Module Status / Communication details” button, and monitor the fields on the left in the newly opened window. Contact ID events sent by the alarm control panel and acknowledgements arriving to them can be monitored here. When the alarm control panel dials, the adapter automatically emits the “handshake” signal, so that the panel can start communication. The module forwards the received Contact ID report over GPRS channel, which will be confirmed by the module when it receives the acknowledgement reply from the monitoring station. By listening in the line it can be heard that – due to the GPRS network delay (as described previously in the chapter entitled “GPRS Adapter – reporting over GPRS connection”) – only every second transmission attempt to the monitoring station is acknowledged.

The meaning of the GPRS Adapter’s major messages:

CTID Sent ="*Contact ID event code*"	- forwarding of the Contact ID event over GPRS
G: CTID_ACK OK	- the monitoring station confirmed the event
!!GPRS SEND ERROR!!	- the report could not be forwarded over GPRS

By using an active loudspeaker it can be observed whether the Contact ID report codes issued by the alarm control panel are clearly audible, with proper volume, are free from discontinuity, and whether the adapter confirms them.

Possible errors:
- If communication is noisy, too low or occasionally the code is flagging and for this reason the adapter does not confirm it, the problem might be with the communicator of the alarm control panel.
- If the alarm control panel does not start communication after the “handshake” signal is emited, the problem might be with the settings of the alarm control panel or its communicator.
- If the module is in GPRS operation mode (logged on to the network, connected to the server) and the alarm control panel dials, but it does not receive the “handshake” signal from the Adapter, check the following parameters:
  - does the telephone number of the monitoring station’s PSTN receiver match the one set in the alarm control panel and in the Adapter,
  - if you do not use PSTN or GSM voice call signal transmission method, then set **0123** instead of the monitoring station’s phone number in the alarm control panel (in this case the adapter monitors the dialing of this number, and emits the “handshake” signal).

It is also recommended to generate report and listen to the transmission to the monitoring station over GSM voice call as well, and to make sure about noise free and successful communication. This can be done by changing the server’s IP address or the APN name in the module so that it cannot establish a connection with the server, and by selecting “Forward all events over GSM voice call” option. Thus the module will forward generated events over the GSM voice channel, as no server connection will be available.

5.6 GPRS Adapter – timings of connection switching

Event	Duration
Connecting to the primary IP address after a restart or powerup	≈ 35 sec
Switching between the certain IP addresses (counted from detecting the loss of the connection)	≈ 30 sec
Switching to GSM switched line – if there is no event but the server is unavailable (counted from detecting the loss of the connection)	120 sec
Switching to GSM switched line – if there is an event and the server is unavailable (counted from event reception)	max. 90 sec
Switching to GSM switched line – if there is an event and the server is available, but the module does not receive the confirmation (counted from event reception)	max. 90 sec
Switching back from GSM switched line to server (without event, or with event, counted from the last event reception)	120 sec
Switching from the backup server to primary server (without event, or with event, counted from the last event reception)	Between 10 minutes and 10 minutes + GPRS test report frequency interval
Switching to PSTN mode if GSM transfer is disabled and the server is unavailable (counted from detecting the loss of the connection or from event reception)	60 sec

5.7 GPRS Pager – timings of connection switching

Event	Duration
Connecting to the primary IP address after a restart or powerup	≈ 35 sec
Switching between the certain IP addresses (counted from detecting the loss of the connection)	≈ 30 sec
Switching to GSM switched line – if there is an event and the server is unavailable (counted from event reception)	max. 90 sec
Switching to GSM switched line – if there is an event and the server is available, but the module does not receive the confirmation (counted from event reception)	max. 90 sec
Switching back from GSM switched line to server (without event, or with event, counted from the last event reception)	120 sec
Switching from the backup server to primary server (without event, or with event, counted from the last event reception)	Between 10 minutes and 10 minutes + GPRS test report frequency interval

5.8 PSTN receiver settings

If reporting is performed through GSM voice calls, or if a GSM Adapter is used to receive the reports at the PSTN receiver side, expect even more increased signal delays.
This delay timing varies between 50-400 ms.
This means that the timings of the receiver unit designed for PSTN phone lines must probably be changed because of the GSM network delay. As a result, it might happen that e.g. after acknowledging a Contact ID code series, the monitoring receiver will wait for the next Contact ID code series only for the minimal time period as defined by the standard. In case of signal transmission over GSM, however, the acknowledgement sent for the Contact ID code series will arrive to the alarm control panel with the GSM network delay, and the next Contact ID code series started as a result of this will also arrive with a delay to the monitoring station.
In case of improper settings, or in case of an outdated monitoring receiver that cannot be configured with parameters, the receiver unit might hang up the line owing to a timeout before the newer signal would arrive.
In order to solve this possible technical problem contact the manufacturer of the specific receiver unit so as to adjust the necessary settings.

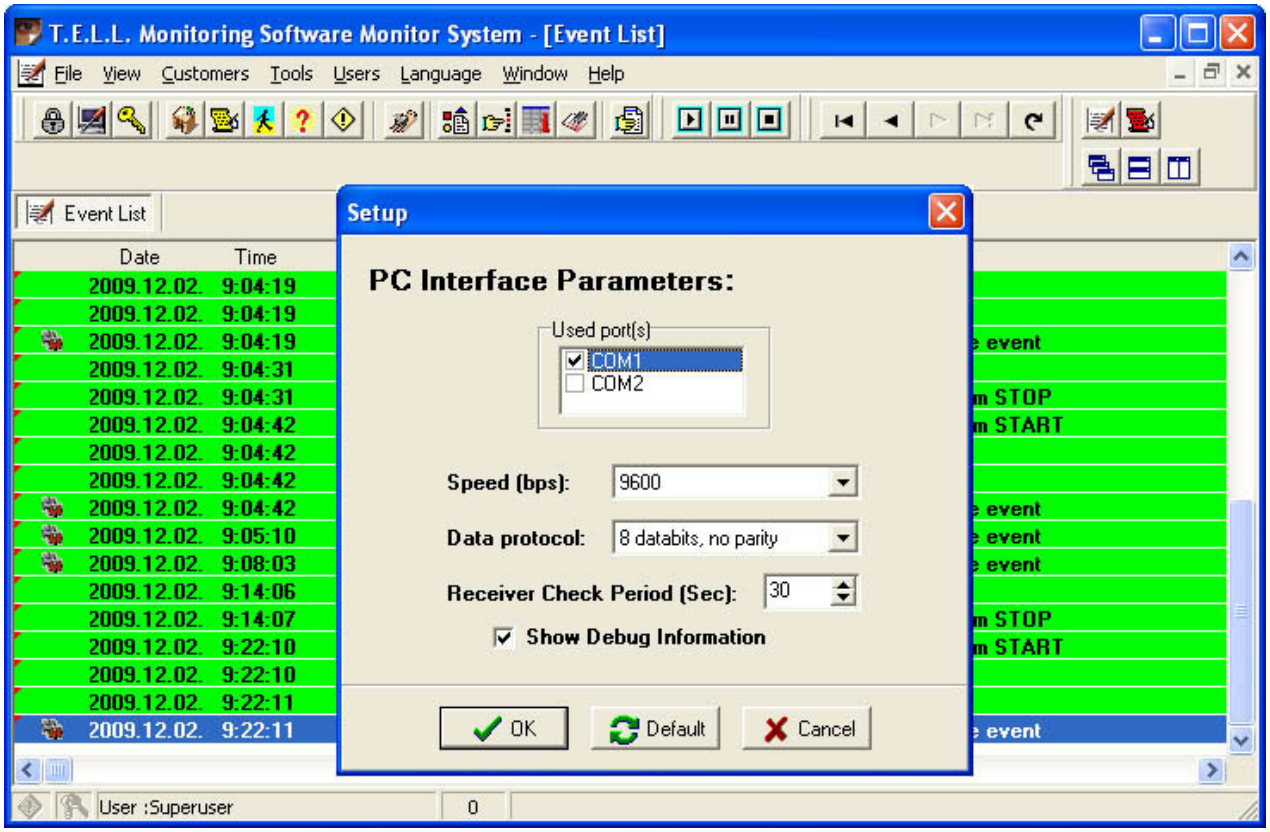
5.9 Alarm monitoring software settings

5.9.1 Serial connection settings

The serial connection should be set in the following way in the monitoring software:

- Baud Rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Heartbeat (connection checking) signal timeout: 30 seconds

An example for TMS alarm monitoring software:



Events generated by the **MVP client software** and their Contact ID codes:

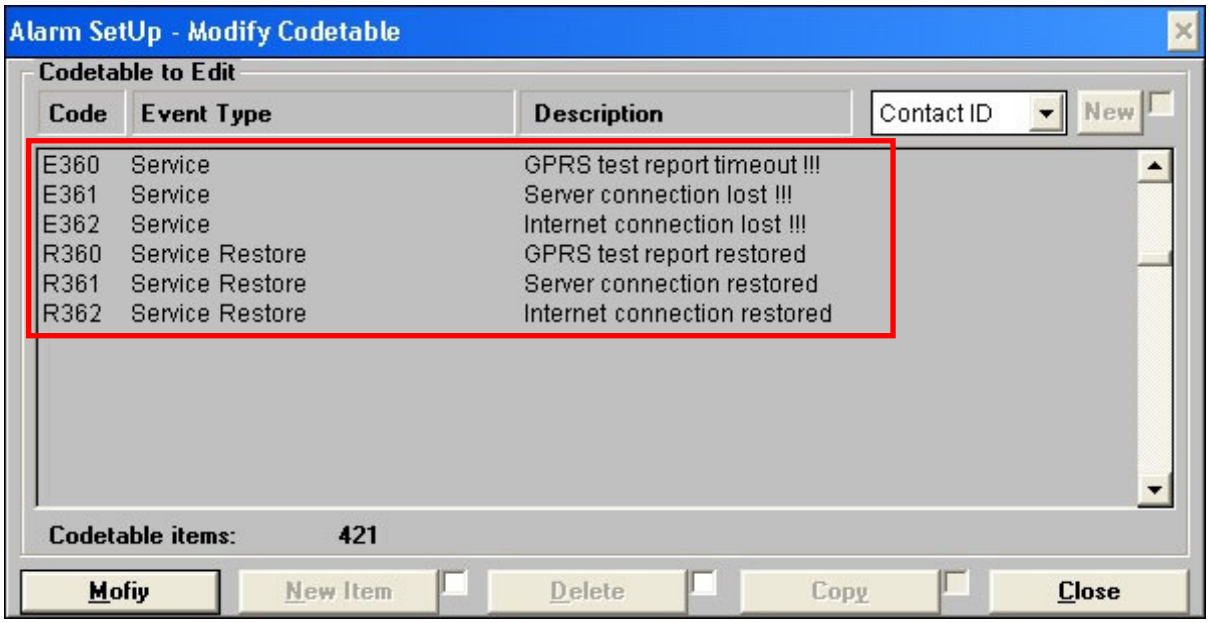
Contact ID code	Event
E361	Server connection lost
E362	Internet connection lost

The MVP client also sends the restoration of the Contact ID codes mentioned above.
Example: E361, when the server conection is lost, then R361 when the connection is reestablished.

The MVP client software's user account ID sent towards the alarm monitoring software is: **9999** by default.
Events and their Contact ID codes generated by the **MVP client software**, but sent towards the alarm monitoring software with the **user account ID set in the GPRS device**:

Contact ID code	Event
E360	GPRS test report timeout

After connecting to the server, the GPRS device informs the server about the GPRS test report frequency and the user account identifier, and it also sends the first GPRS test report (heartbeat signal).
When the MVP client detects that the time set for the GPRS test report frequency since the last test report has elapsed, then it waits for the time set at "device connection timeout" section, and if no test report arrives until that time, then the GPRS test report is considered lost, so the MVP client generates an E360 Contact ID message using the user account ID set in the related GPRS device. The TMS alarm monitoring software contains by default the events mentioned in the tables above. In case of using a different alarm monitoring software than TMS, then these events have to be registered in the given monitoring software's Contact ID codetable. For easier identification, these events can be named in the alarm monitoring software as shown in the tables above.
(e.g. in case of Alarm-Sys monitoring software):



5.10 Utility programs

The GPRS settings of the devices can be adjusted using the “GPRS Setup” software, while the installer settings can be programmed with the remoter programming software of the given GPRS device.

5.10.1 GPRS Setup

Using the GPRS setup software, the GPRS settings of the GPRS devices can be adjusted. The software is dedicated by being issued with individual monitoring station identifier, and it suports the following settings:

- SIM card PIN code
- Public and dedicated GPRS APN settings (identifier, password)
- Server IP addresses and port numbers
- GPRS test report frequency
- DNS server addresses (backup or secondary server for dynamic IP addresses)

GPRS devices can be connected to the software in two ways:

- Through USB port (the very first programming can be done only this way)
- Through the internet (devices which are connected to the server)

Details of the program’s usage can be found in the installation and user manual of the GPRS device.

5.10.2 GPRS Adapter programming software

The GPRS Adapter can be connected to its programming software through USB port or through the internet, through the server. The software can be used for the following tasks:

- Monitor the module status
- Display module version
- Set parameters:
    - Monitoring settings (operation modes on GPRS fault)
    - Individual Contact ID reports

Details of the program’s usage can be found in the installation and user manual of the GPRS device.

5.10.3 GPRS Pager programming software

The GPRS Pager can be connected to its programming software through USB port or through the internet, through the server. The software can be used for the following tasks:

- Monitor the module status
- Display module version
- Download event log
- Change installer password
- Set parameters:
    - Zones
    - Events
    - Relay outputs
    - Phone numbers
    - Alarm settings

Details of the program’s usage can be found in the installation and user manual of the GPRS device.

5.10.4 Serial number generator program

The serial number generator program is needed if you would like to expand your existing, operating T.E.L.L. GPRS system with new GPRS devices, and you purchase so called „blank" GPRS devices from the distributor which are not locked to a monitoring service by the manufacturer.

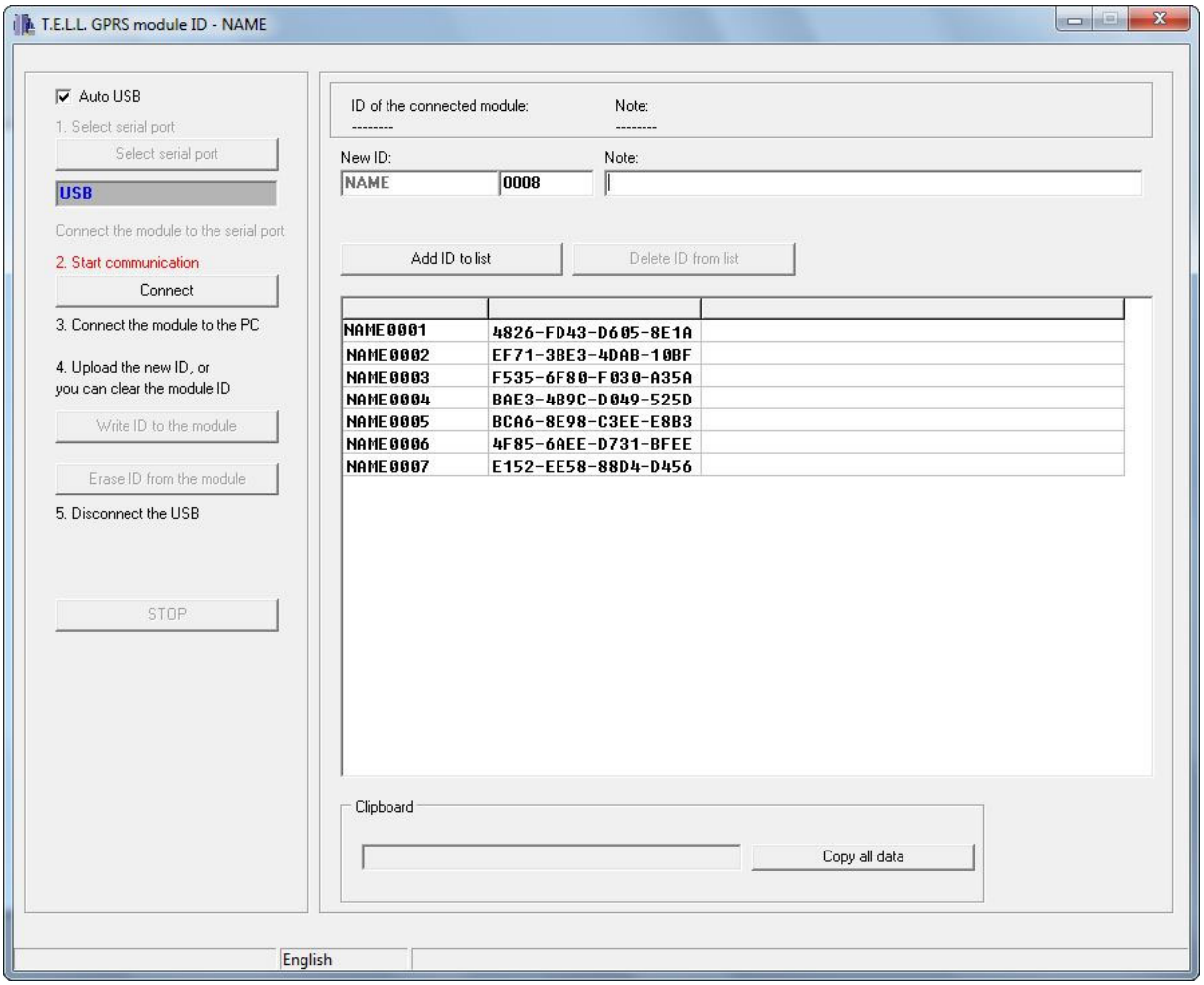
Blank devices ease the process of new installations as the distributor can serve the customer from stock, and the monitoring service can do the "naming" (programming the serial number) with their own serial number generator program, thus implanting the module into their own line of devices.
So after purchasing, generating the serial number, and doing the usual programming, the device can be immediatelly used with an activated SIM card.
If you do not have your own unique serial number generator program yet, ask the manufacturer, and you will shortly receive the program in e-mail.

Before starting to generate the new serial number with the program for the blank device, import the data of the existing devices into the program!
The description for this process can be found below.
Serial number generation can be accomplished using the serial number generator program. Serial numbers are needed for the server to identify the individual devices. Blank devices are assigned a "BIANCO" identifier. These modules can be freely numbered with the serial number generator program, according to the identifier of the monitoring service.

- Open the "**sernummerer.exe**" program
- Add all non-blank devices into the list (unless already done so):
  type in the serial number of the device into the "**New ID**" serial number field,
  type in the description, then click the "**Add ID to list**" button
- Power off the module (disconnect from power supply)
- Disconnect the module from USB, if earlier connected
- Select "**AUTO USB**" option, or select the USB port number after pressing "**Select serial port**" button
- Press "**Connect**" button
- Connect the module to USB
- The program will read in a few seconds the identifier set in the module and will display it in the program header
- Enter the serial number wished to be set in the module in the "**New ID**" field (at the very first programming it is recommended to start with serial 0001)
- A description can be also assigned to any identifier (e.g. the user's name, location, etc.)
- Press "**Write ID to the module**" button
  (the identifier will be automatically added to the list)
- Disconnect the module from USB

Identifiers can be added to the list by clicking the “**Add ID to list**” button even if there is no module connected to the software.

The identifier selected in the list is automatically copied to clipboard, and it is displayed in the “**Clipboard**” field. The whole content of the list can be copied to clipboard by clicking the “**Copy all data**” button, and then this can be pasted into a table as well.
Rows of the list can be deleted one by one. For this, select the row to be deleted and press “**Delete ID from list**” button.



The serial number generator program is unique for each monitoring station, so making sure that the GPRS device can only be used by the monitoring station which purchased it (or numbered it). These devices will be able to connect to their own servers only.
For this reason do not share your serial number generator program with unauthorized persons!

5.10.5 Bootloader program

The bootloader software can be used to update the firmware of GPRS devices through USB connection.

Remote update of operating devices, which are connected to the server can only be performed by the manufacturer. Contact the manufacturer if remote update is necessary.

The firmware of a GPRS device can be updated locally through USB port with the Bootloader program as follows:

- Start „Bootloader X22” software on Windows XP or Windows Vista operating system
- Power off the module (disconnect from power supply)
- Disconnect the module from USB, if earlier connected
- Select ”**AUTO USB**” option, or select the USB port number after pressing ”**COM port**” button
- Open the new firmware file using ”**Open Firmware File**” button (the file is provided by the manufacturer)
- The file description is displayed, check if it corresponds to your device
- Disconnect the module from USB, if earlier connected
- Start the upload by pressing ”**Start**” button
- Connect the device to USB
- Wait until upload is finished (the status bar reaches 100% and “Upload finished successfully!” message appears)
- If you do not wish to update further devices, close the program

5.11 List of common errors: GPRS modules

Error description	Possible reason	Solution
The LEDs of the module are off after installation	There is no supply voltage or its value is less than 9V DC	Check the supply voltage and the necessary current
The computer cannot detect the module over the USB cable	The USB cable is not plugged in the module or in the computer, or it has no proper contact	Check the USB cable connection
	USB serial port is not selected in the installed software, or the selected port is not the one to which the module is connected to	Select the correct USB serial port or enable “AUTO USB” option, then connect the module to the computer
	The specific USB port is used by another device	Check USB ports in use
	The USB cable is damaged	Try another USB cable
“**!! SIM PIN CODE ERROR !!**” message is displayed in the top left field of the “Communication details” window in GPRS_ remoter software	SIM card is not inserted	Check the SIM card
	No SIM card contact	Check the contacts of the SIM card and the card case. They should be free from contamination, and the case pins should not be bent
	SIM card PIN code request is enabled, and the PIN is not set in the module or it is wrong	Disable PIN code request on the SIM card using a mobile phone, or if this function is needed, set the PIN code in the module as well with the GPRS_setup software
“**!! SIM CARD ERROR !!**” message is displayed in the top left field of the “Communication details” window in GPRS_ remoter software	The inserted SIM card is not corresponding	Insert the corresponding SIM card
	The module was previously installed with another SIM card, and the “FIX SIM” function was enabled in the GPRS_setup software when it was configured	Check the status of the “FIX SIM” option with the GPRS_setup software. If it is enabled, disable it, and then install the device with the corresponding SIM card. You can then enable the option again if necessary.
There is no **OK** answer to the **AT** commands for a longer time (>2 minutes) in the right field of the “Communication details” window in GPRS_ remoter software	The module became faulty	Contact your dealer or the manufacturer

Error description	Possible reason	Solution
The **+CREG** value does not settle at **0.1** in the right field of the “Communication details” window in GPRS_remoter software	The module cannot connect to the network	Check the SIM card
The module does not establish connection to the server (The “**CONNECT FAIL**” message is seen among the processes in the right field of the “Communication details” window) in GPRS_remoter software	The server IP address is not configured properly	Check the IP address(es) with the GPRS_setup software
	The port is not configured properly for the IP address	Check the port(s) assigned to the IP address(es) with the GPRS_setup software
	In case of a public APN: the APN name is not configured properly	Check the APN name with the GPRS_setup software
	In case of a dedicated APN: the APN name and/or identifier, password is wrong	Check the APN name, identifier and password with the GPRS_setup software
	The APN selected is not the right one (APN1-2)	Check the selected APN with the GPRS_setup software
	The GSM signal strength is not satisfactory at the Module’s mounting location	Check the GSM signal with the GPRS_remoter software, and if it is not satisfactory, find a better place for the module, or use a special antenna
	PIN code request is enabled on the SIM card inserted into the module, and the PIN code was not, or not correctly entered into the software at configuration	Disable PIN code request on the SIM card, or if it is necessary, set it properly with the GPRS_setup software
	The module was previously installed with another SIM card, and the “FIX SIM” function was enabled in the GPRS_setup software when it was configured	Check the status of the “FIX SIM” option with the GPRS_setup software. If it is enabled, disable it, and then install the device with the corresponding SIM card. You can then enable the option again if necessary
	The GPRS service is unavailable (maintenance at the service provider)	Contact your provider for information
	There is no internet connection on server side	Check the router, the ADSL modem, ask your internet provider
	GPRS service unavailable on the SIM card inserted into the module	Insert the correct SIM card into the module, or ask your provider

6 Troubleshooting, repairing

6.1 Repairing the server file system

If the server halted abnormally, abruptly, or there was a power loss and no uninterruptible power supply was in use, the operating system might detect file system damage when it is restarted, so the service does not start on the server.
For this reason, always check the normal operation of the server after each power loss that might affect the server:

- Check if the alarm monitoring software reports losing the server as a receiver unit
- Check if the server event log is available from a browser

If none of the above conditions are met, then the file system is probably damaged, as mentioned above.

This error can be corrected on site, but definitely an IT professional should do it. Repair steps are the following:

- Connect a monitor and a keyboard to the server
- If the monitor displays the following messages, the server must be restarted in failsafe operation mode to use it again securely:

```
WARNING – The following files in / differ from the boot archive:
/etc/path_to_inst
cannot find: /etc/devices/mdi_ib_cache: No such file or directory
The recommended action is to reboot and select „Solaris failsafe”
option from the boot menu. Then follow prompts to update the
boot archive.
To continue booting at your own risk, clear the service:
# svcadm clear system/boot-archive

…    svc.start[7]:    svc:/system/boot-archive:default:    Method
“/lib/svc
/method/boot-archive” failed with exit status 95.
…   svc.start[7]:   system/boot-archive:default   failed   fatally:
transitioned tom maintenance (see ‘svcs –xv’ for details)
Requesting System Maintenance Mode
(See /lib/svc/share/README form more information.)
Console login service(s) cannot run

Root password for system maintenance (control-d to bypass):
```

- Restart the server (with the `reboot` command or by pressing the reset button)
- Select the “`Solaris failsafe`” menu item (if you cannot select the menu item and you use a USB keyboard, then change your keyboard to one that connects to the PS/2 port, or configure USB keyboard support in the BIOS)

- The operating system performs the maintenance, for which it asks a few questions. Answer yes to all of these questions by pressing the key “y” (“z” on Hungarian keyboards):

```
Searching for installed OS instances...

An out of sync boot archive was detected on /dev/dsk/c0d0s0.
The boot archive is a cache of files used during boot and
should be kept in sync to ensure proper system operation.

Do you wish to automatically update this boot archive? [y,n,?] y
Updating boot archive on /dev/dsk/c0d0s0.
The boot archive on /dev/dsk/c0d0s0 was updated successfully.

Solaris 10.1... X86 was found on /dev/dsk/c0d0s0.
Do you wish to have it mounted read-write on /a? [y,n,?] y
mounting /dev/dsk/c0d0s0 /a

Starting shell.
```

- If the `Starting shell.` message appears, the operating system completed the maintenance, and it has to be restarted with the `reboot` command or by pressing the reset button
- Select “`Solaris 10.1... X86`” from the menu appearing soon (this will be selected automatically as well after a few seconds)
- If the `Console login:` message appears, the system has started (this takes now more time than usually). Check the normal operation of the system again according to the above description, and if testing conditions are not met, contact the manufacturer.