Access controller
GSM2WIEGAND v1.1

Installation and usage manual

Lviv 2022

Contents

Features

- Cellular network signal strength indication.
- Supported operating along with another access control system (U-Prox IP400 or similar).
- External RFID reader supported.
- Analog input for the force open access control equipment (button).
- Automatic network time synchronization.
- Built-in database with 1000 users.
- Supported operating with GGate access control server.
- Supported autonomous operating with user interaction only via mobile application/SMS.
- Built-in event buffer with 500 events, available from GGate access control server.
- Programmable “open” pulse signal duration.
- Automatic supply voltage measurement and SIM card account balance check.
- Over-The-Air (OTA) firmware update.
- Error indication while programming.

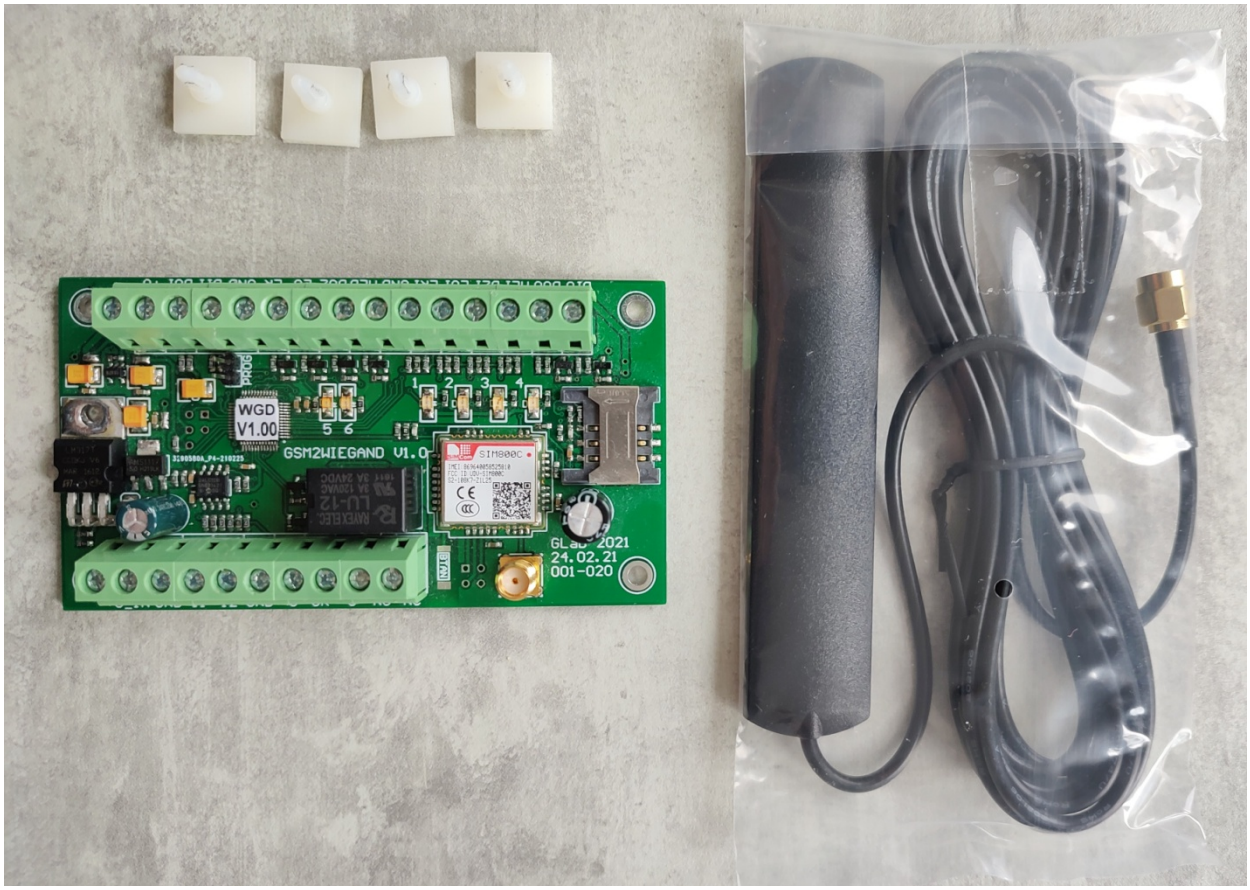


Figure 1. Top view of the device.

Technical characteristics

Device

Parameter	*Symbol*	*Unit*	*Value*
Power supply voltage	U_{pwrdc}	**V**	**+10…+15**
Maximal operating current	I_{pwrmax}	**mA**	**1000**
Average operating current in idle mode	I_{pwravg}	**mA**	**50**
Maximal log. «1» voltage on inputs D0I, D1I	$U1_{maxd}$	**V**	**5.75**
Maximal log. «1» voltage on other inputs	$U1_{max}$	**V**	U_{pwrdc}**+1**
Minimal log. «1» voltage on inputs D0I, D1I	$U1_{mind}$	**V**	**3.75**
Minimal log. «1» voltage on other inputs	$U1_{min}$	**V**	U_{pwrdc}***0.75**
Maximal log. «0» voltage on inputs D0I, D1I	$U0_{maxd}$	**V**	**1.25**
Maximal log. «0» voltage on other inputs	$U0_{max}$	**V**	U_{pwrdc}***0.25**
Minimal log. «0» voltage on inputs	$U0_{min}$	**V**	**0**
Maximal voltage on C, NO, NC	U_{relmax}	**V**	**120 AC, 24 DC**
Maximal load current on NO, NC	I_{relmax}	**mA**	**1000**
Maximal load current on other outputs (not protected)	I_{okmax}	**mA**	**200**
Maximal voltage on D0O and D1O outputs	U_{okmaxd}	**V**	**5.75**
Maximal voltage on other outputs	U_{okmax}	**V**	**15**
Maximal operating temperature	t_{max}	**°C**	**+65**
Minimal operating temperature	t_{min}	**°C**	**-20**

GSM module

Frequency range	**GSM 850/EGSM 900/ DCS 1800/ PCS1900, auto selection**
GSM class	**Small MS**
Transmitter power	**Class 4 (2W) at EGSM900/GSM850** **Class 1 (1W) at DCS1800/PCS1900**
SIM interface	**Support SIM card: 1,8V, 3V**

Inputs/outputs definition

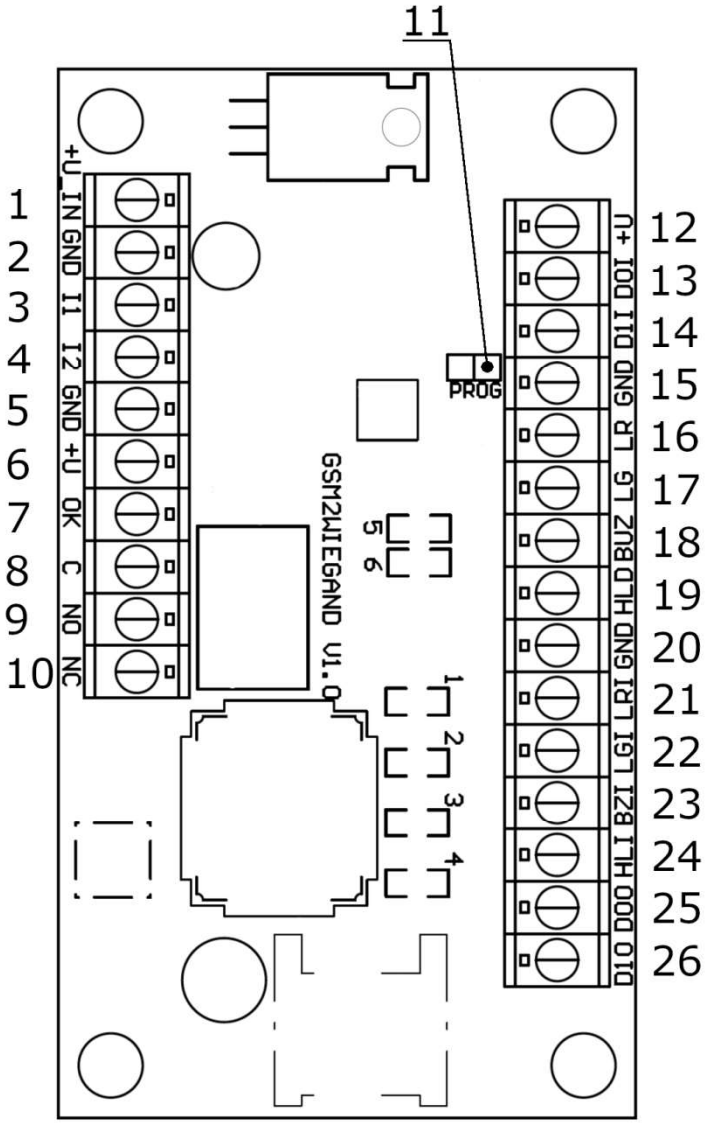


Figure 2. List of inputs and outputs of the device.

Table 1. List of inputs/outputs.

№	*Name*	*Description*	*Usage*
1	**+U_IN**	**Power supply «+», DC +12 V**	**DC power supply connectors**
2	**GND**	**Power supply ground**	
3	**I1**	**Analog input 1**	**Analog inputs, the first one is used to force open the controlled access equipment, the second is not used**
4	**I2**	**Analog input 2**	
5	**GND**	**Ground for analog inputs**	
6	**+U**	**Power output for the additional equipment**	**Outputs for managing the additional controlled access equipment**
7	**OK**	**«Open collector» output, repeats the relay signal**	
8	**C**	**Relay Common**	**Relay connectors for the controlled access equipment**
9	**NO**	**Relay Normal Open**	
10	**NC**	**Relay Normal Closed**	
11	**PROG**	**Configuration mode jumper**	**Jumper for configuring the device**

12	**+U**	**RFID reader power output**	**RFID reader connectors**
13	**D0I**	**Wiegand protocol data input (low level signal)**	
14	**D1I**	**Wiegand protocol data input (high level signal)**	
15	**GND**	**RFID reader ground**	
16	**LR**	**Red LED control output**	
17	**LG**	**Green LED control output**	
18	**BUZ**	**Buzzer control output**	
19	**HLD**	**RFID reader block output**	
20	**GND**	**Access control system ground**	**External access control system connectors**
21	**LRI**	**Red LED control input**	
22	**LGI**	**Green LED control input**	
23	**BZI**	**Buzzer control input**	
24	**HLI**	**RFID reader block input**	
25	**D0O**	**Wiegand protocol data output (low level signal)**	
26	**D1O**	**Wiegand protocol data output (high level signal)**	

Installation

SIM card requirements.

The device supports GSM Phase1, GSM Phase2+ standard SIM cards with 1.8 and 3.3 V supply voltage. This means that any SIM card manufactured past 2004 should work.

The SIM card must be activated and the PIN code request on boot must be disabled.

SIM card installation.

Attach the antenna to the device's golden SMA connector.

ATTENTION!

Turning on the device without the GSM antenna attached causes the GSM module to malfunction. Note that the manufacturer's warranty does not apply to the GSM module.

Insert the SIM card into the device as shown on **figure 2**.

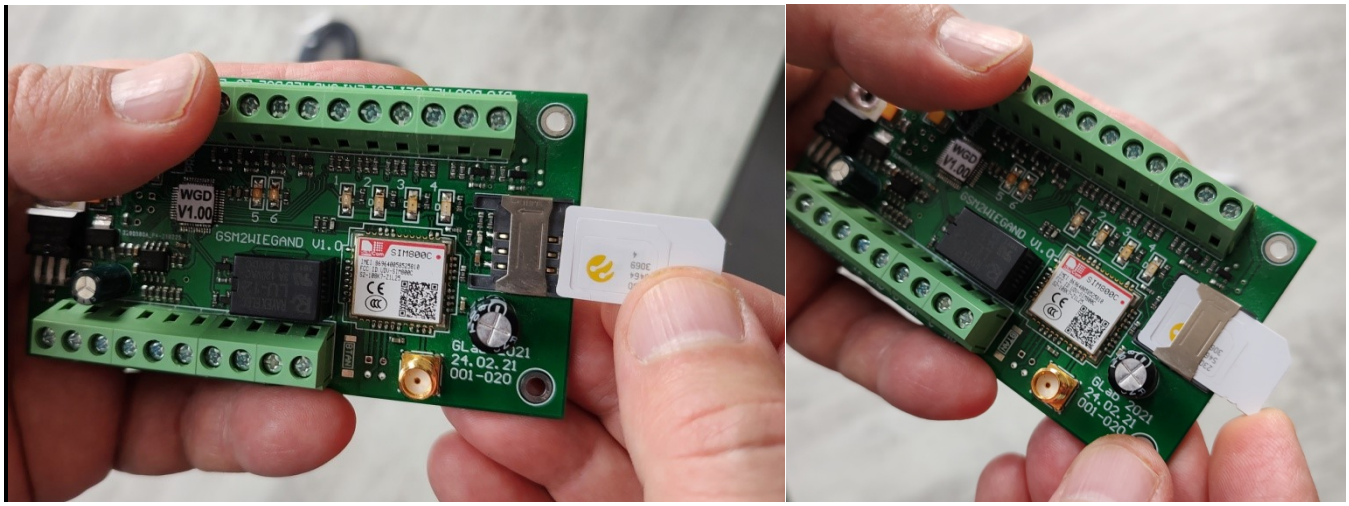


Figure 2. SIM card installation.

Connecting the power supply and the controlled access equipment.

Connect the power supply and at least one of the controlled access equipment as shown on **figure 3**. The access equipment can be controlled either with the «OK» output signal (transistor is open during active level), or with the NO, NC signals from the relay. Both OK and relay signals are similar and can be used simultaneously. Output to use depends on the specific controlled access equipment type. Input I1 can be used to connect arbitrary equipment for force opening the controlled access equipment, for instance a button (low signal level is active).

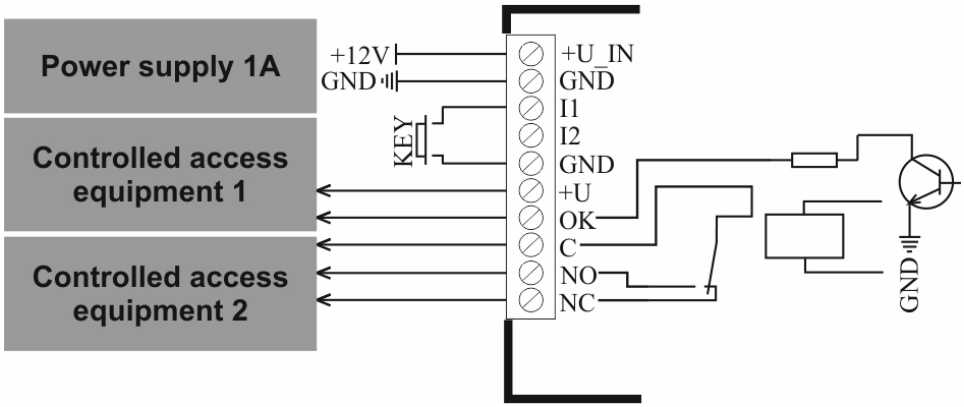


Figure 3. Connection schematic for power supply and controlled access equipment.

Connecting the RFID reader.

The device is capable of processing RFID tags. An external RFID tag reader is needed for that, a typical reader (e. g. U-Prox SL mini) connection example is depicted on **figure 4**.

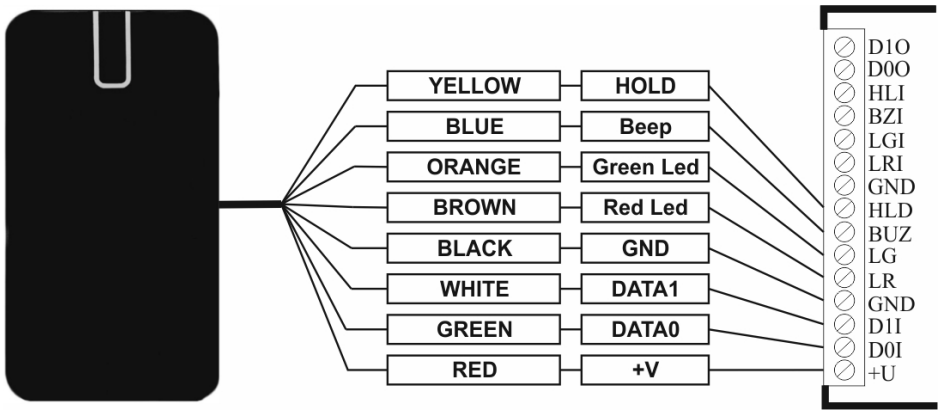


Figure 4. Connection schematic for an RFID reader

ATTENTION!

If the device is used along with an RFID reader, make sure that the Wiegand protocol types in the device settings (see* Mobile application and settings*) and in the reader settings are the same.

Connecting the external access control system.

The device can also act as an intermediary between the GSM module and/or RFID reader on one side and an external access control system on the other. In such case connecting the controlled access equipment is optional, provided that the whole database and the same access equipment are handled by the external access control system. A typical connection schematic for an external access control system is (e. g. U-Prox IP400) is shown on **figure 5**.

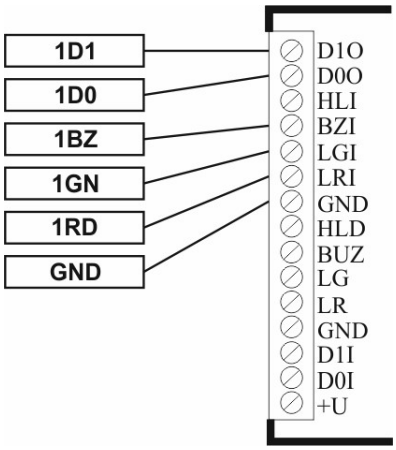


Figure 5. Connection schematic for an external access control system.

ATTENTION!

If the device is used along with an external access control system, make sure that the Wiegand protocol types in the device settings and in the access control system settings are the same. Also activate the «transparent mode» in the device settings (see* Mobile application and settings*).

Configuration

After installing the device and connecting all the needed equipment set the PROG jumper and switch on the power. The device will initialize and enter configuration mode if no errors were detected (more in **Initialization** subsection), after this the PROG jumper can be unset. When in configuration mode the device solely awaits an SMS message with the settings (the sender mobile number does not matter in this case) and does not accept calls or RFID tags. After the settings were received the device saves them and reboots, initializing and entering operation mode.

To re-enter configuration mode with an already configured device, reboot it and keep the PROG jumper set while the device is initializing. Alternatively the administrator (SMS message from the phone number marked as "administrator") can change the settings of an operating device without the need to reboot it manually. See section **Mobile application and settings** for detailed description of all settings and tips on how to add and configure the device using either the mobile application or manually via SMS.

Operating modes and LED indication

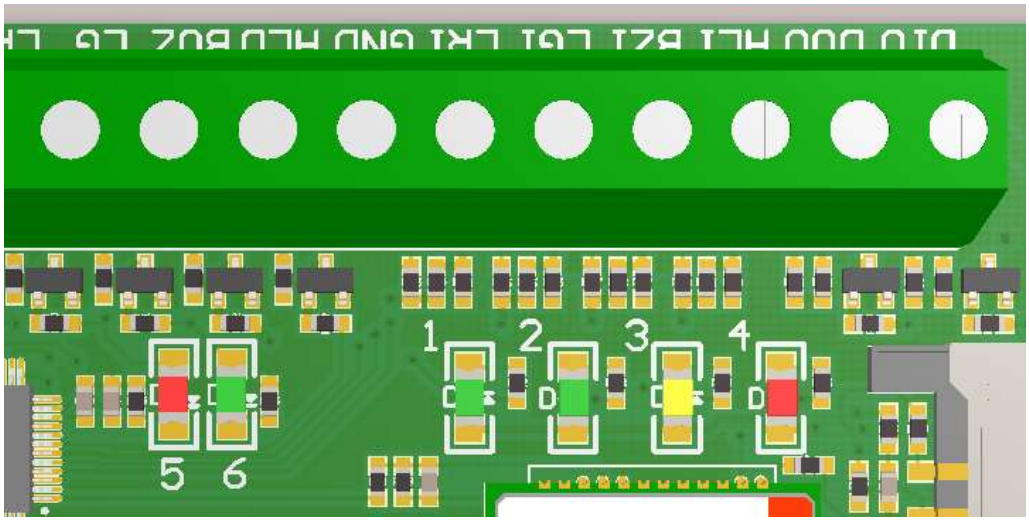


Figure 6. Indicating LEDs on the device.

LED indication.

All the device LEDs are shown on **figure 6**, more specifically green LEDs 1, 2 and 6, yellow LED 3 and red LEDs 4, 5. LEDs 1 and 2 indicate the signal level, LED 3 shows the current network processes or the exact error type, LED 4 indicates if there are any errors or problems with the network. LEDs 5 and 6 repeat the state of the outputs LR and LG (accordingly red and green LEDs of the RFID reader), also they blink alternately when the device is in configuration mode.

If one of the predicted critical errors occurs during initialization, red LED 4 starts to glow constantly while yellow LED 3 indicates the error type (see **Table 2**).

Table 2. Error codes of the device.

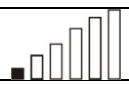
LED 3, number of pulses	***Error description***
2	**SIM card error. Clear all the SIM card contacts or replace the card.**
3	**PIN code error. Turn off the PIN code request in the security settings.**
4	**No response from the GSM module. Contact the manufacturer's service.**

ATTENTION!

The device indicates errors only for 30 seconds. Then the device will reboot the GSM module and try to initialize again.

If red LED 4 does not glow continuously, then the group of LEDs 1-4 indicates the mobile network status in any operating mode. In that case red LED 4 blinks if the cellular network coverage (or registration) is missing or insufficient for normal operation of the device. Yellow LED 3 is used to indicate the GSM module operation. If LED 3 blinks once per second, the GSM module is registering on the mobile network. LED 3 blinks once per 3 seconds when the GSM module has successfully registered on the network. If LED 3 glows and fades for 0.3 seconds then the connection to the access control server is established. Also LED 3 blinks rapidly when a network data transmission is in progress. Green LEDs 2, 1 and red LED 4 are used to indicate the cellular network signal level. Approximate signal level values are displayed in **Table 3**.

Table 3. Approximate values of the cellular network signal level.

LED			***Level***	***Note***
2	***1***	***4***		
On	**On**	**Off**		**Maximal signal level.**
Off	**On**	**Off**		**Signal level at about 50%. Enough for normal device operation.**
Off	**Blinks**	**Off**		**Signal level is not enough for normal device operation. External antenna is needed.**
Off	**Off**	**Blinks**		**The device is not operational. External antenna is needed.**

Initialization.

The device enters this mode after being powered. During initialization the device loads, configures the GSM module, tries to register on the mobile network and reads its own settings from memory. Initialization takes about 30 seconds, depending on the signal level and network response time. If booted for the first time (no settings in memory) or if the PROG jumper is set, the device then enters configuration mode, otherwise – operation mode. Also the device can re-enter initialization from any other mode in case of recurring GSM module malfunction in order to reboot the module.

During initialization red LED 4 blinks until GSM module is registered on the mobile network. If LED 4 starts glowing continuously, that means an error has occurred (see subsection **LED indication**). Additionally the BUZ output (RFID reader buzzer, if connected) is activated for several seconds at the beginning of initialization to notify the user.

Configuration mode.

Configuration mode is entered via PROG jumper staying set while initializing or the device settings being empty (first boot). Configuration mode is indicated by red and green LEDs 5 and 6, blinking alternately once per second.

The device will stay in this mode until it receives an SMS message with settings in a correct format or until the device is rebooted. Unlike in operation mode, the sender's phone number is not checked, therefore the device can be programmed not only by the administrator. Also when in configuration mode all the incoming calls are declined and RFID tags (if an RFID reader is connected) are ignored. After the settings are received and saved successfully, the device reboots automatically.

Operation mode.

When in operation mode, the device monitors all the incoming phone calls, SMS messages and RFID tags (if an RFID reader is connected), tries to maintain the connection to the access control server and communicates with it every minute (if configured, see **Mobile application and settings** and the GGate server interactive manual for more information).

The controlled access equipment can be opened in three ways:

1. Mobile call to the device's SIM card phone number.

   In that case the device checks if the caller's phone number is present in the database, is not blacklisted and if it has at least one opening attempt left. If the phone number meets the conditions, the device declines the call, opens the controlled access equipment and decrements the opening attempts for the calling user. Otherwise the controlled access equipment remains closed and if the «Play audio» setting is active, the device answers the call and plays the appropriate audio recording: one for when the caller's number is unknown and another if the number is present in the database but has no opening attempts left or is blocked. With the

«Play audio» setting inactive all the calls are declined and the calling user is not notified of why the access was denied.

2. RFID tag via an RFID reader (if connected).

   RFID tag number is handled similarly to the mobile phone number, except that the only feedback to the user is via RFID reader LEDs and LEDs 5, 6 on the device. The device turns on the green LED LG / LED 6 for the «Open duration» time (specified in the settings) if the access is allowed or the red LED LR / LED 5 if the access is denied. Note that such access indication is not exclusive to RFID tags and also works for phone calls and force open button.

3. Low level signal on I1 input (button / other equipment connected).

   In this case the device does no checks and acts as if an allowed phone number or RFID tag was received, the so called force open mode. For instance, it is useful for opening the door from inside the building.

Note that if «Transparent mode» is active in the settings, all the incoming calls and RFID tags, whether present in the internal database or not, are resent to the external access control system using the chosen Wiegand protocol. In «Transparent mode» the control of all RFID reader connectors is also delegated to the external access control system. Everything else works the same; therefore a part of the database (for example users' phone numbers) can be handled directly by the device and the other part (for example RFID tags or vice versa) can be handled on the side of external access control system and be treated as unknown numbers by the device. Controlled access equipment can also be different for each side.

Internal database is managed either with SMS messages from the administrator (see **Mobile application and settings**) or with the access control server (see the GGate server interactive manual). Also the administrator can change the device settings without having to switch to configuration mode.

When working with RFID reader, there is a separate method of adding RFID tags to the database for special cases when the tag number is unknown and difficult to check. To add the RFID tag that way, keep the PROG jumper set while reading the tag. Then the device will automatically add a new user with this tag into the first vacant database entry (if the database is not full and if this tag is not already present there). The opening attempts will be set to default (999) and can be later changed with the access control server. Alternatively, to avoid opening the access equipment case, the set PROG jumper for the next RFID tag can be replaced with the appropriate SMS command from the administrator (see **Mobile application and settings**).

Additionally the device tracks system time so that when date change is detected, the device tries to synchronize time with the Internet (NTP server) using the configured time zone, check the SIM card account balance (if configured in the settings) and synchronize the entire database with the access control server (if in server work mode). Note that completely powering off the device resets system time so the device will attempt all of the above during the first couple of minutes on reboot.

If the «Life pulse» setting is active, every day at 12:00 system time the device will send an SMS message containing SIM card account balance, current supply voltage, date and time to the administrator's phone number.

The database with the device users.

The device's internal database contains 1000 users, one database entry consists of:

- Index – the number of entry in the database;
- Phone number or RFID tag number – a 10 digit (hexadecimal numbers are accepted for RFID) user identifier that is checked to grant access;
- Daily opening attempts – how many times per day the user can request access, 999 max;
- Opening attempts left – how many times left for the current day. Cannot exceed daily opening attempts, is automatically set to daily opening attempts when date changes;
- Allow – a binary value, set to «1» by default, setting this to «0» will blacklist the current user.

The GGate access control server is the main database management tool. Also the mobile application or manual SMS messaging (not recommended) can be used, but only the access control server has full access to all the features and fine control of the database. For instance, editing the Opening attempts left and blacklisting the device, as well as setting up complex access routines is unavailable in mobile application.

Programming the settings.

Both the GSM Wiegand mobile application (recommended) and manual SMS messaging can be used to program the settings.

In the mobile application, select the «List of devices» to manage all the saved devices, then press «+» to add a new device. You will see a window with all the device settings like on the left of **figure 7**.

List of the settings:

- Device name – a name for the current device configuration, only for display in the application;
- Device phone number – the full device's SIM card phone number;
- Admin phone number – a full phone number, marked as «administrator» (your own phone number in most cases). Only this phone number can later be used to manage the internal database and change the device settings when in operation mode;
- Work mode – choosing the Server option in the dropdown menu involves working with GGate access control server, choosing the Autonomous option deactivates the access control server support. Choose the latter if you do not intend to use the GGate server, otherwise the next 2 fields also need to be filled;
- Server IP/Domain name – access control server network address or a domain name, 40 symbols max. Empty field or an IP address filled with zeros is equivalent to selecting the autonomous work mode and deactivates the server features;

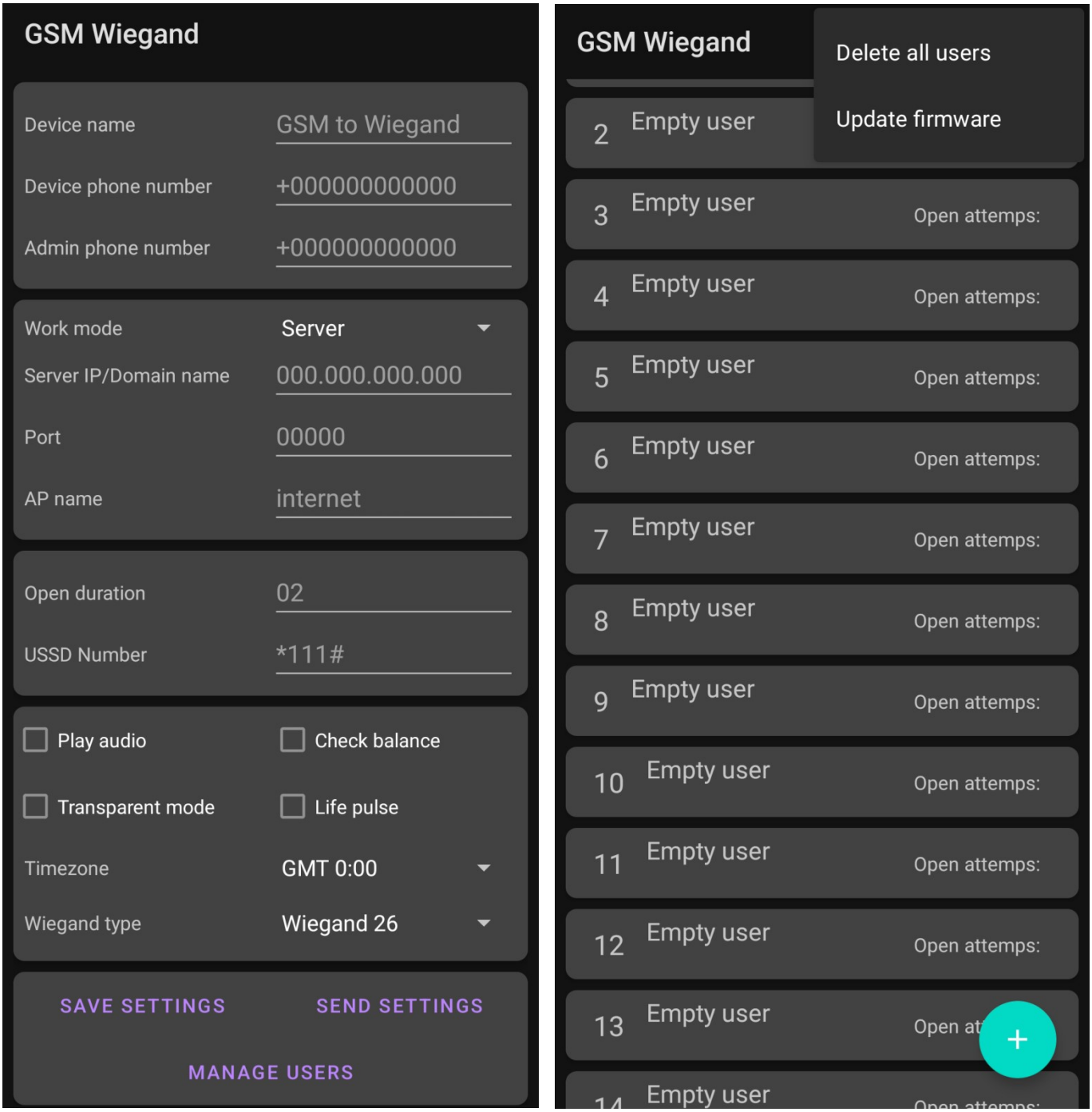


Figure 7. The device settings and list of users

- Port – a network port number that is being routed to the access control server;

- AP name – name of the mobile operator network access point, 20 symbols max. Depends on the specific mobile operator, «internet» for Ukrainian mobile operators;

- Open duration – duration in seconds of an active pulse signal to open the controlled access equipment, 2 digits max;

- USSD number – mobile number for USSD request to check the device mobile account balance. «*111#» for Ukrainian mobile operators;

- Play audio – selecting this option makes the device answer the incoming calls if access was denied and notify the calling user by playing short audio recordings;

- Check balance – whether the device should check the remaining money on the mobile account using the USSD number specified above when the date changes;

- Transparent mode – in this mode the device resends all the calling phone numbers and the inbound RFID tag numbers to the external access control system using the configured Wiegand protocol. Also LEDs 5, 6 and outputs HLD, BUZ, LG, LR repeat inputs HLI, BZI, LGI, LRI accordingly (see **Operation mode** for more details);

- Life pulse – the device will send an SMS message containing SIM card account balance, current supply voltage, date and time to the administrator phone number every day at 12:00 system time;

- Time zone – local Greenwich time zone (GMT), for automatic network time synchronization, from -12 to 12;

- Wiegand type – Wiegand protocol type, used for transferring data between the device, RFID reader and external access control system (if connected). It must match on all devices for correct operation;

The current device configuration can be then saved by pressing «Save settings» and the «Send settings» button sends an SMS message with the current settings to the device.

Programming the settings without the mobile application.

Although not recommended, the device can also be programmed without using the mobile application. Instead an SMS message of the following structure containing all the settings needs to be formed:

$SET%ADMINISTRATOR_PHONE_NUMBER%SERVER_IP/DOMAIN_NAME%PORT%AP_NAME%OPEN_DURATION%PLAY_AUDIO%CHECK_BALANCE%USSD_NUMBER%TRANSPARENT_MODE%LIFE_PULSE%TIME_ZONE%WIEGAND_TYPE

The field names, described in the previous subsection, are replaced with the field values in the correct order, separated by «%» symbol. To disable the access control server support (enable autonomous mode), you need to set the SERVER_IP/DOMAIN_NAME field to «000.000.000.000»; the PORT field is irrelevant then. The fields represented by checkboxes in the application (e. g. LIFE_PULSE) can have only «0» and «1» values, where 0 – inactive / unchecked, 1 – active / checked. The OPEN_DURATION field must consist of 2 digits, even if the opening pulse duration is less than 10 sec, the first «0» digit cannot be omitted. The TIME_ZONE field is an integer ranging from «-12» to «12». The WIEGAND_TYPE field is also an integer which corresponds to the specific Wiegand protocol type, see **table 4**.

A full example of an SMS message with the settings:

$SET%+280344598235%example.domain.com%8002%internet%02%1%1%*111#%0%1%4%5

Table 4. The corresponding Wiegand protocol types and the Wiegand type field values.

Wiegand type	Wiegand 26	Wiegand 32	Wiegand 34	Wiegand 37	Wiegand 40	Wiegand 42	Wiegand 56	Wiegand 60	Wiegand 64
Field value	0	1	2	3	4	5	6	7	8

Managing the database.

The mobile application can also be used to add / delete / edit users in the device's internal database via SMS messages instead of / along with the access control server. Note that only the administrator can do that.

To view the database management menu, select the specific device configuration and press «Manage users». In the next window all the device users are displayed and in the separate submenu above (**figure 7** on the right) there are commands to delete the whole database and update the device firmware. Using both commands is not recommended unless absolutely necessary.

To add a new user, press any empty database entry (the «+» button will instead add a user to the first vacant entry). To edit the user select the according existing entry. In any case the user management window is shown on **figure 8**.

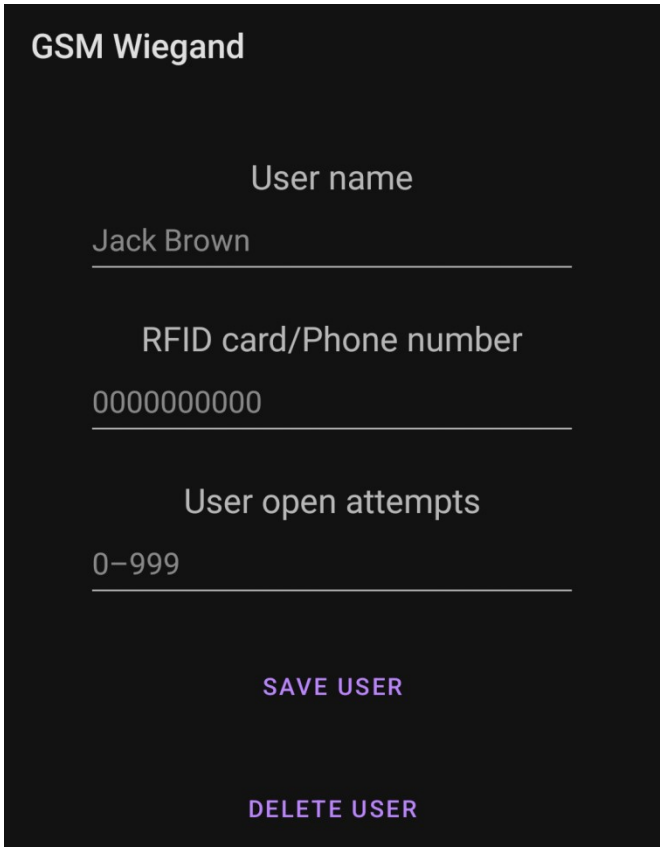


Figure 8. Managing a device user.

List of available settings:

- User name – the name of the user, only used for display in the application;

- RFID card / Phone number – either the user's mobile phone number or RFID tag number (hexadecimal, uppercase letters), 10 digits;

- User open attempts – number of controlled access equipment opening attempts per day for the current user, 0-999;

To add or edit the current user, press «Save user». Instead «Delete user» button removes the user entry from the database. Note that adding an existing user will remove the previous entry with the same user, so that there are no duplicates in the database. Removing a non-existent user has no effect.

ATTENTION!

In order to not deplete the account balance with excessive SMS traffic, the mobile application does not synchronize the database with the device. Meaning that any changes to the database made either by the access control server or by another updated administrator will not appear in the application! Therefore GGate access control server is the only main database editing tool with full access to all features.

Just like with the settings, it is possible to manage users manually via SMS (not recommended). To add / modify the user, send an SMS message in the following format to the device's phone number:

$WRI%USER_INDEX%RFID_TAG/PHONE_NUMBER%OPEN_ATTEMPTS

The USER_INDEX field determines the number of user entry in the database and must consist of 3 digits. Counting starts with 0, so that user number «000» is the first, «012» - thirteenth and so on.

The OPEN_ATTEMPTS field also must contain 3 digits.

Example:

$WRI%013%041B00016C%008

An SMS message to remove the user entry is similar to the previous one:

$DEL%USER_INDEX

Example:

$DEL%005

An SMS command to delete the entire database:

$DELA

An SMS command to update the device firmware:

$UPD

An SMS command to add the next scanned RFID tag to the database (equivalent to setting the PROG jumper while scanning):

$ADD

GGate access control server

The access control server is a main (although optional) instrument for interaction with the GSM2WIEGAND device. The GGate software is distributed freely and is designed for computers running Windows operating system. Note that in order to successfully connect the device to the server, the server must have a static IP address (or a domain name) on the network and an open port, accessible from the Internet and configured in the device settings.

The access control server has its own interactive manual, which describes many of the device features, including those only accessible from the server (for instance the event buffer, the commands). The manual is accessible directly via the help menu in the GGate server interface.

Warranty

ATTENTION! The manufacturer of this product is liable only within the limits of the warranty obligation for the operation of the device itself and is not responsible for the device installation quality, the cellular network coverage and service of the GSM operator, the quality of radio signal, etc.

The manufacturer is not responsible for any accident, caused by using the device by either the owner or the third party.

All responsibility for using the device is on the user.

The manufacturer is liable for warranty repair of the device during 12 months since the product was sold.

The warranty does not apply to devices that are out of order because of the user's fault, in particular due to violations of the exploitation and installation rules, damaged warranty seals, mechanical damage, as well as malfunctions, caused by a lightning strike, short circuit in the electric network and so on.

Also the warranty does not apply to the SIM800C module which is part of the device.

Scope of delivery

1. GSM2WIEGAND Access Controller	– 1 pcs.
2. ADA0068 Antenna	– 1 pcs.
3. Jumper	– 1 pcs.
4. Plastic mounting racks	– 4 pcs.