W-LOCK EXT

GSM Code Lock access control unit

USER MANUAL

Contents

Figures

Tables

1 FOR YOUR SAFETY

SWITCH ON SAFELY

Do not switch the unit on when use of wireless phone is prohibited or when it may cause interference or danger.

INTERFERENCE

All wireless phones and units may be susceptible to interference, which could affect performance.

SWITCH OFF IN HOSPITALS

Follow any restrictions. Switch the unit off near medical equipment.

SWITCH OFF IN AIRCRAFT

Follow any restrictions. Wireless devices can cause interference in aircraft.

SWITCH OFF WHEN REFUELING

Do not use the unit at a refueling point. Do not use near fuel or chemicals.

SWITCH OFF NEAR BLASTING

Follow any restrictions. Do not use the unit where blasting is in progress.

USE SENSIBLY

Use only in the normal position as explained in the product documentation. Do not touch the antenna unnecessarily.

2   INTRODUCTION

W-LOCK is a simple GSM switch system designed to ensure low-cost, simple to install/use, reliable and single box solution for remote managed switching application. It is designed for unlimited range, pin code access, caller ID control and Wiegand access support.

Optional W-LOCK supports alarm detection, stay-alive messages, credit detection etc…

3   W-LOCK FEATURES AND APPLICATIONS

Features:

⇒ Built-in 4 (2G) or 5 (3G) band GSM module

⇒ Keypad Access entry support (up-to 1000 PIN codes)

⇒ Caller ID numbers control (up-to 500 caller ID numbers)

⇒ Up to 100 temporary SPIN access codes

⇒ Up to 1000 PIN access codes

⇒ Input Wiegand receiver

⇒ 1 output (relay supported)

⇒ Programming with PC via "USB to Mini USB cable" connected to the unit

⇒ Programming by WEB server

⇒ Programming by SMS commands

Applications:

⇒ Remote gate opener – Caller ID number recognition

⇒ Simple (Wiegand) access system

4   START UP

W-LOCK unit accepts a standard GSM SIM cards from any network.

VERY IMPORTANT	USE A **MICRO SIM CARD**	

WARNING	DO NOT Insert or remove the SIM card while the unit is powered ON!!

IMPORTANT	Before inserting SIM card to unit make sure the PIN code is removed!!

⇒ Insert SIM card in W-LOCK unit.

⇒ Connect power cable to W-LOCK unit (YOU MUST POWER THE W-LOCK UNIT WITH THE POWER SUPPLY IF INCLUDED. Do not power with any other power supply).

⇒ Power up the unit.

⇒ Wait until LED1 (Green) starts flashing. This is set in around 30 – 45 seconds.

⇒ W-LOCK unit is now ready to operate.

5   LED INDICATION

Green LED (LED1)

- Indicates the level of the GSM signal from 1 to 5 LED flashes (1 is weak signal, 5 is excellent signal)

Yellow LED (LED3)

- Short flashing indicates that the GSM module is ON, but it is not yet connected on the GSM network. After connection, yellow led is flashing with short pulse (0,5s) ON and a long pulse OFF (5s).

6   CONNECTION DIAGRAM

Before connection the W-LOCK please take a look at connection diagram.
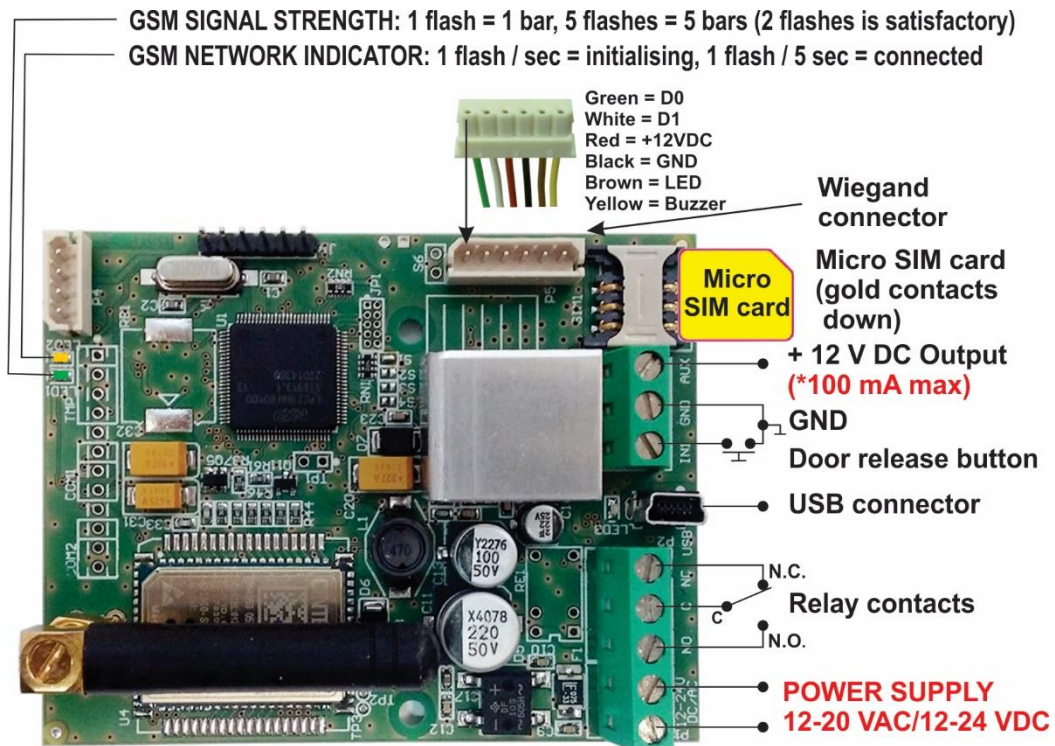
Figure 1: W-LOCK : Connection diagram

IMPORTANT	*DO NOT USE Power out (12V AUX) for electric lock driving! Use separate power source for door electric lock!*

7   W-LOCK UNIT MANAGEMENT

Unit supports different types of management (programming):

⇒ Unit can be programmed directly by USB connection, with the use of configuration software running on PC (EasySet).

⇒ Unit can be programmed remotely by using WEB server access.

⇒ Unit can be programmed remotely by SMS commands (Optional).

8 W-LOCK FUNCTIONS WITH PROGRAMMING INSTRUCTIONS

As mentioned in previous chapters W-LOCK unit can be programmed in various way, this document will focus on most common programming way: WEB programming.

IMPORTANT	SIM card in the W-LOCK unit **MUST have DATA PLAN** to be able to use WEB programming!

8.1 WEB SERVER - LOG IN

The web server can be find under the address: **http://www.easyset.eu/.**
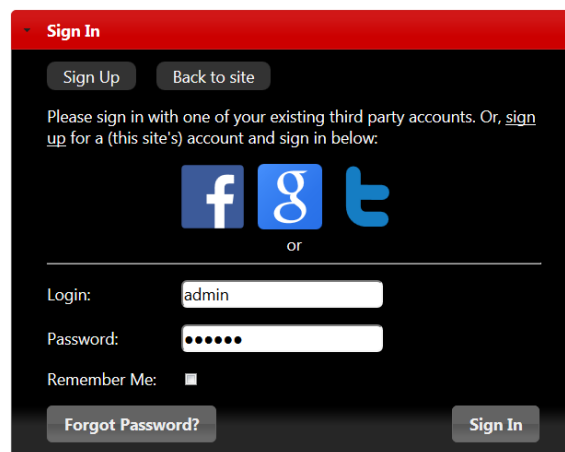
Figure 2: WEB Server-Sign In page

User must first use the Sign IN section to create working profile on the server. The profile can be created by using social login like Facebook, Google account or Twitter. The user lacks any of the social profile it can proceed to Sign UP page use standard user name and password entry.

NOTE	Server support Firefox, Google Chrome, Safari.

8.2 WEB SERVER – ADDING UNITS TO USER PROFILE

After login the user will be diverted to WEB server main window. This page is used to add/remove/search for W-LOCK units from the user's profile.

Select "+" sign to select ADD W-LOCK units to user's profile.
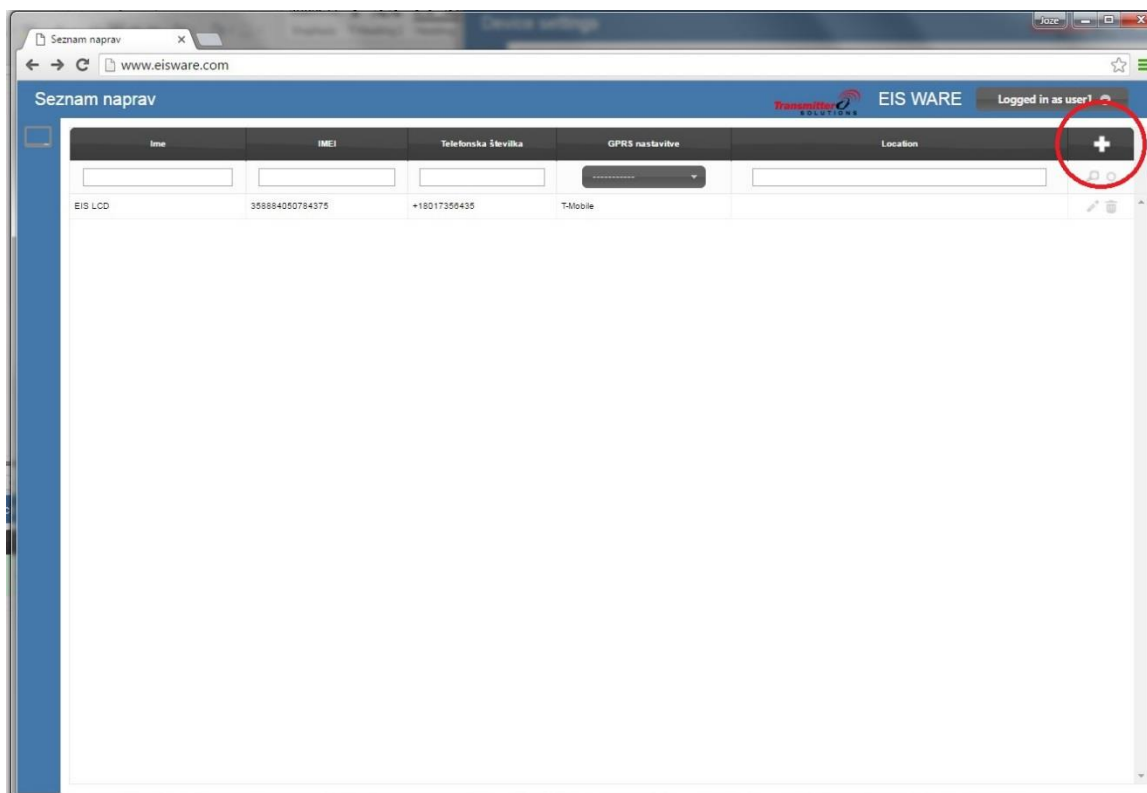
Figure 3: WEB Server-Main page select ADD mode
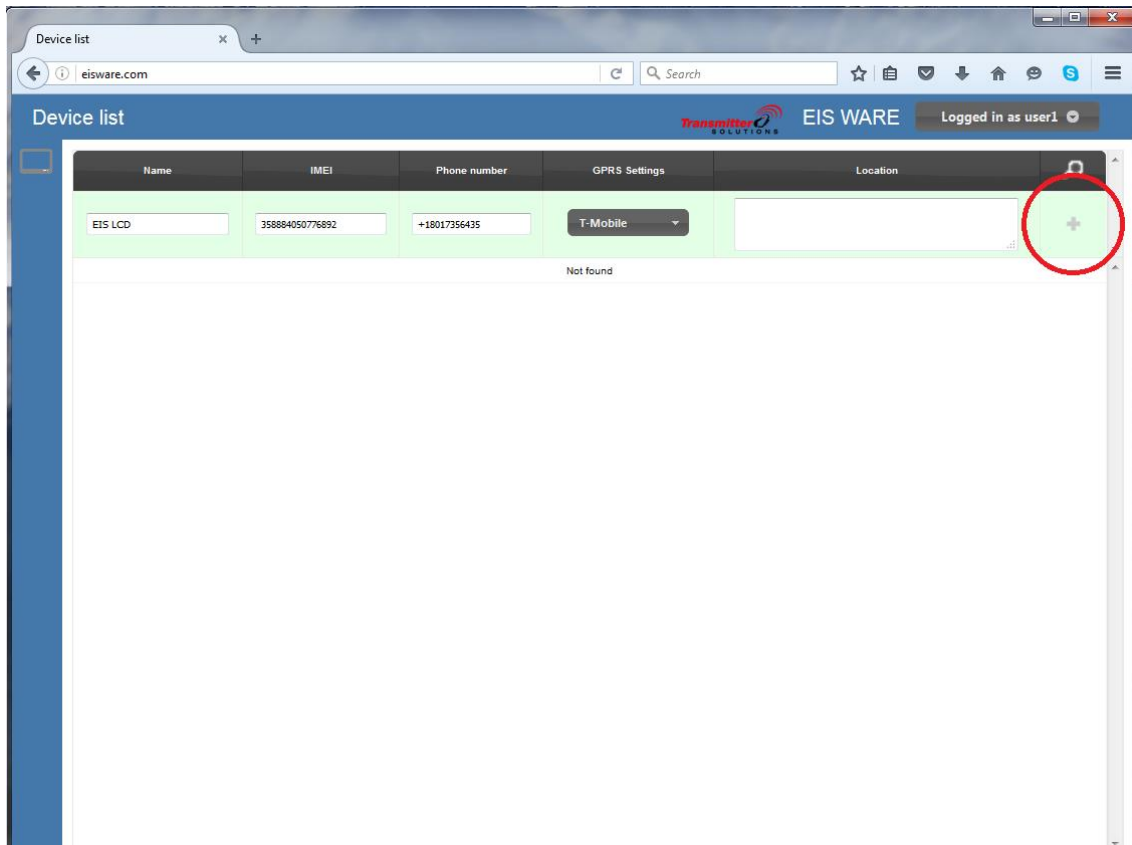
Figure 4: WEB Server-Main page adding W-LOCK units

User than provides required data:

- **Name**: Name for the added unit - mandatory information.
- **IMEI**: Identification number of the unit, can be found in the enclosure of the unit - mandatory information. The IMEI is located on the cellular chip and also should be on the card board box of the W-LOCK .
- **Phone Number:** The telephone number of the SIM card in the W-LOCK unit - mandatory data.
- **GPRS settings:** Information needed to enable data connection between the server and the unit. Selectable from the drop-down menu - mandatory data.
- **Location:** Notification field, used by the user to provide extra data for its own information - optional data.

By clicking the "+" (insert sign) after filling mandatory data, the unit will be added to the user profile.

First building of the unit data-base may take a few minutes.

8.3 WEB SERVER-UNIT MANAGEMENT

After the W-LOCK unit is added to user database, the user can change the configuration of the specific unit.

All changes made by the user are listed in the **Change Log** window. By clicking **Send to device** button ALL changes are send to the unit. User can revert all changes made, before sending, by clicking **Revert all** or select particular entry and revert it.

Figure 5: WEB Server-Unit management window

8.4 KEYPAD PIN ENTRY – ACCESS

Primary use of on-board keypad is access by entering PIN codes. Pin codes must be at least 4 digits. Pin codes can be defined in two sections. First section is permanent pin code and second is temporary pin codes which are limited by the consecutive time they are entered.

Permanent pin codes placed in **Pin access** tab.

Pin codes are placed in two tables. For each table user can define which output they will trigger.
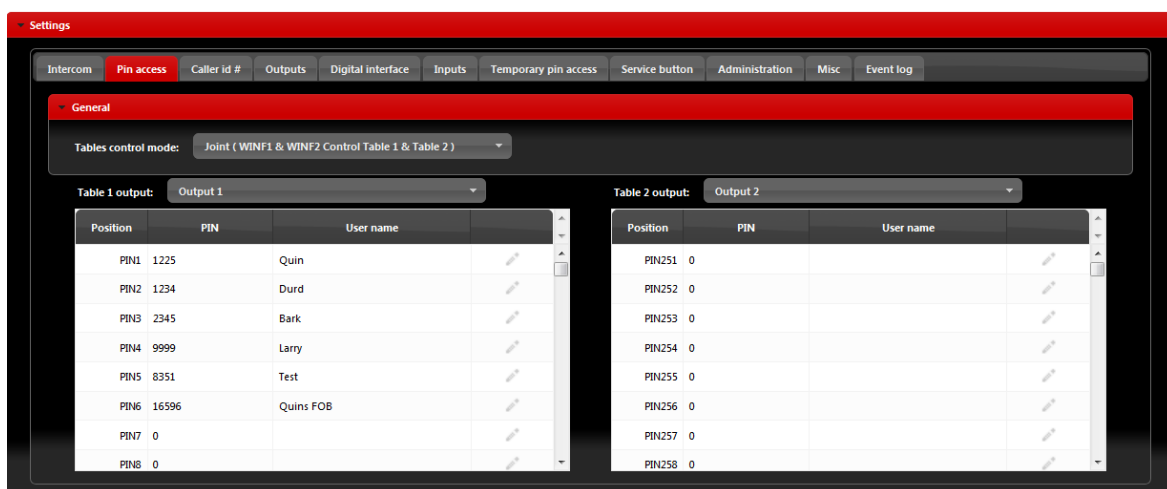
Figure 6: WEB Server-Keypad PIN Access: Permanent PIN codes.

Temporary pin codes are placed in **Temporary pin access** tab.
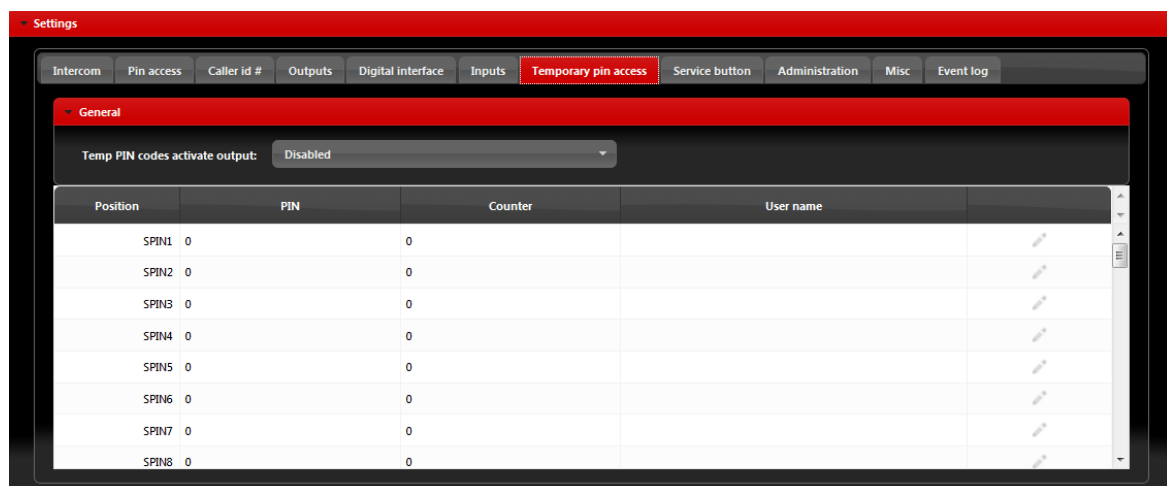
Figure 7: WEB Server-Keypad PIN Access: Temporary PIN codes

- **Temp PIN codes activate output:** Selecting the output that will be triggered in case of correct SPIN code.

- **SPIN entry:** For each SPIN entry user need to select PIN code value and Counter value which defines how many time the PIN code will be valid and optional a User name. Counter will be decreased each time SPIN code will be used

8.5 WIEGAND ACCESS

W-LOCK unit has onboard support for 1 Wiegand output based device. With the user of external replicator more Wiegand devices can be connected to the unit.

Configuration of Wiegand interface is found in **Digital interface** tab in the **Input** section. Wiegand interface can be found on board with a dedicated Wiegand connector and cables.
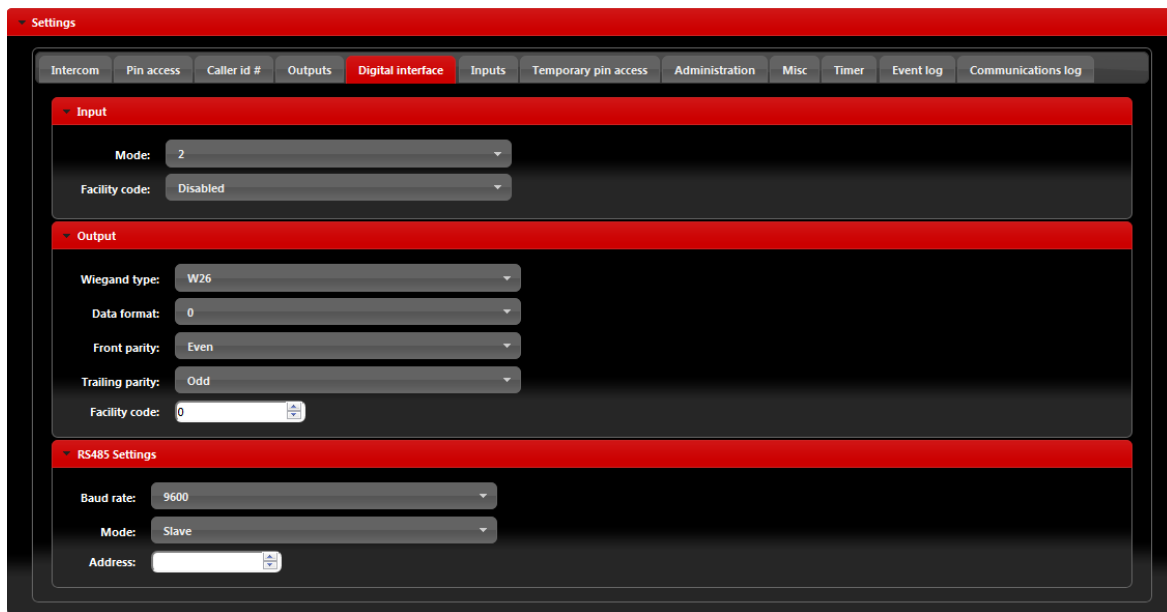
Figure 8: WEB Server-Wiegand interface support.

- **Mode:** Select appropriate data formatting (Advise unit provider for more info if needed, mode 2 is most common setting)
- **Facility code:** User can *Enable* or *Disable* facility code field.

Wiegand devices can be defined in two sections. First section is permanent pin codes and second is temporary pin codes - limited by the number of use.

NOTE	See Chapter 9-WIEGAND INPUT DATA FORMATS for detailed explanation of different data format options.

Permanent use: devices are added in **Pin access** tables.

They are placed in two tables. For each table user can define which output they will trigger.
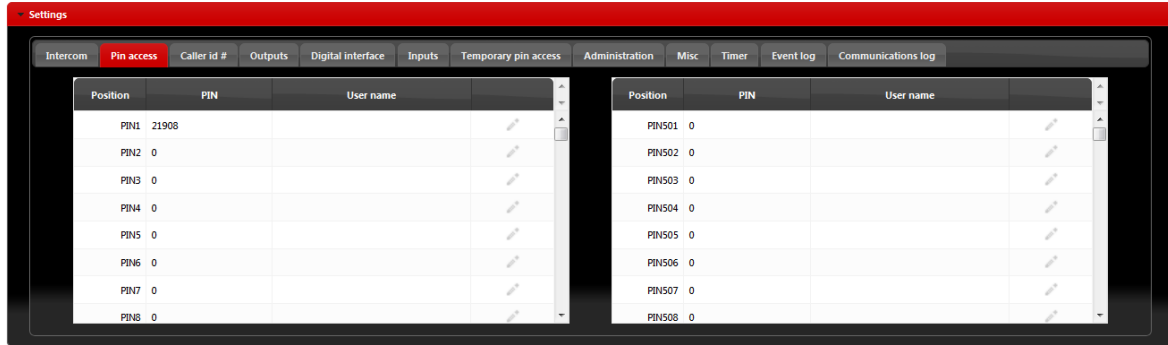
Figure 9: WEB Server-Adding Wiegand devices with permanent use.

- **PIN entry:** For each PIN entry user need to select PIN code value and optional User name.

Temporary pin codes are placed in **Temporary pin access** tab.
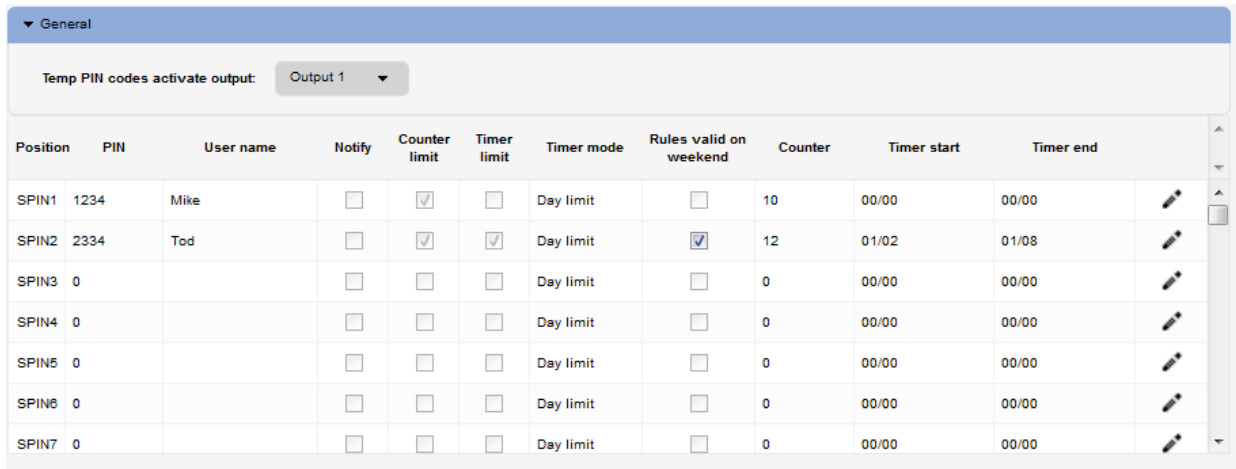
Figure 10: WEB Server-Adding Wiegand devices with temporary use.

- **Temp PIN codes activate output:** Selecting the output that will be triggered in case of correct SPIN code.

- **SPIN entry:** For each SPIN entry user need to select appropriate values.

SPIN options	Description
SPIN value	Temporary PIN code
User name	Name of the user
Notify	If SPIN code is used, administrator numbers CAN be notified
Counter limit	Enable/Disable counter limitation (consecutive use)
Timer limit	Enable/Disable timer limitation
Timer mode	Timer limit mode: Day limit (day limitation), Timer limit (hours of a day access limitation)
Rules valid on weekend	Enable/Disable timer limitation for weekend days
Counter	Number of allowed use of SPIN code
Timer start/Timer end	Bottom and Top timer limitation

Table 1: WEB Server - SPIN entry parameters.

8.6 CALLER ID ACCESS

Caller ID access is a very simple way to control relay output defined in **Caller ID output** setting. User will by calling in the W-LOCK unit trigger defined output.

Settings for this function are found in the **Caller id #** tab.
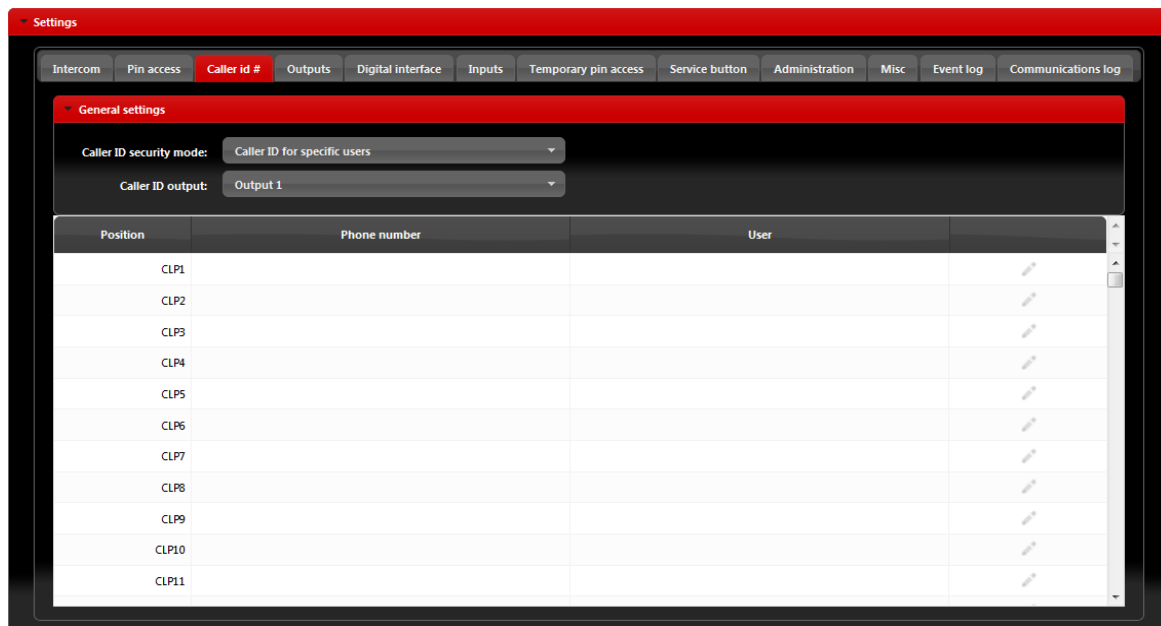
Figure 11: WEB Server-Caller ID Access

General settings:

- **Caller ID security mode:** Selecting *Caller ID Disabled* deactivates caller ID function – all numbers are restricted. Selecting *Caller ID for specific users* will limit the caller ID function only to the numbers on the list. Selecting *Caller ID always ON* will allow all user that know the number of the unit to open defined output. In last option the user doesn't need to be on the list to trigger the output

- **Caller ID output:** Selecting the output that will be triggered in Caller ID function.

NOTE	Selection *Caller ID always ON* will allow anybody with the knowledge of the unit number to trigger the output by calling the unit. Use this setting with caution.

8.7 OUTPUTS SETTINGS

The behavior on the outputs is defined in the **Output tab.**

Figure 12: WEB Server-Output setting

Output 1 - Settings for output 1:

- **Output (relay) mode:** User can select between 3 options

  Disable-Output is disabled.

  Latching-Output is in latching mode. First Caller ID or PIN entry will activate the output, second Caller ID or PIN entry will deactivate the output.

  Time Pulse-Output is time pulse mode. After output is triggered it will be activated for the time defined in **Output pulse duration**, after that time output will be restored.

- **Output pulse duration:** ON time for output in case of output mode *Timer pulse.*

- **Output is:** Output can work in normal or inverted (normally close) mode.

  Normally open-In idle mode output pins are in open position.

  Normally closed-In idle mode output connections are closed.

Additional output settings - Setting are used to link onboard actions with the outputs if needed:

- **Unauthorized call or SMS received:** If unauthorized call or SMS is received on the unit this event will activate output defined under this section.

- **Input 1 activate output:** If input 1 is actived this action will activate output defined under this section.

NOTE	Do to limitation of the outputs use additional outputs settings with care.

8.8 TIMER-TIMED CONTROLLED OUTPUT

W-LOCK unit features 2 timers that can be used to control the output on the unit. Timers can run in day or week mode depending on the selected setting.
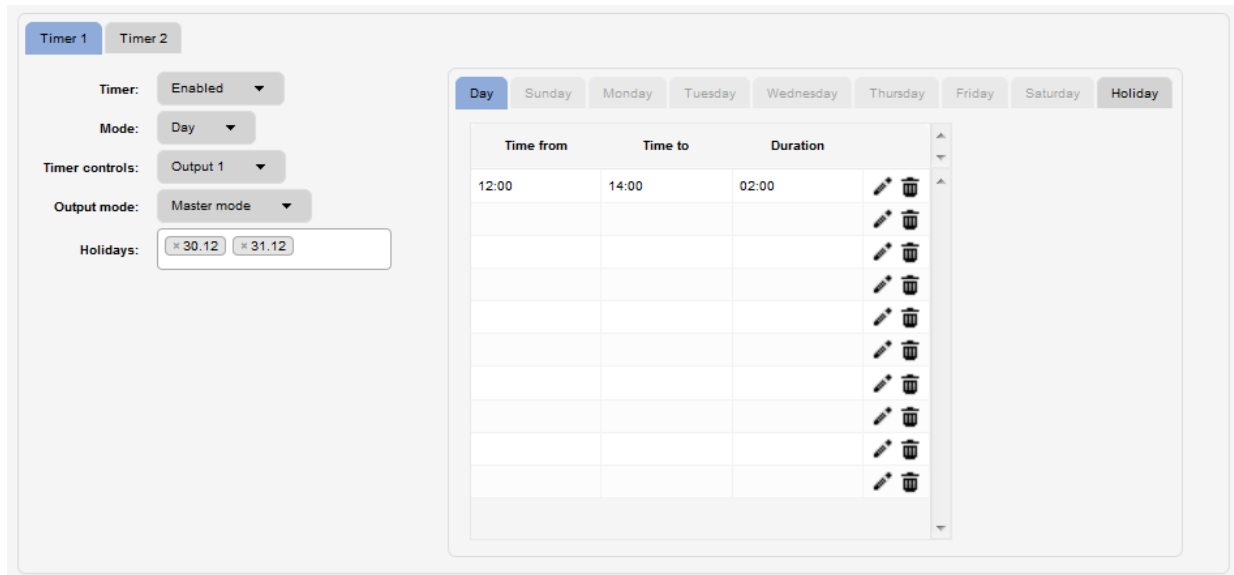
Figure 13: WEB Server-Timer setting →Day mode.
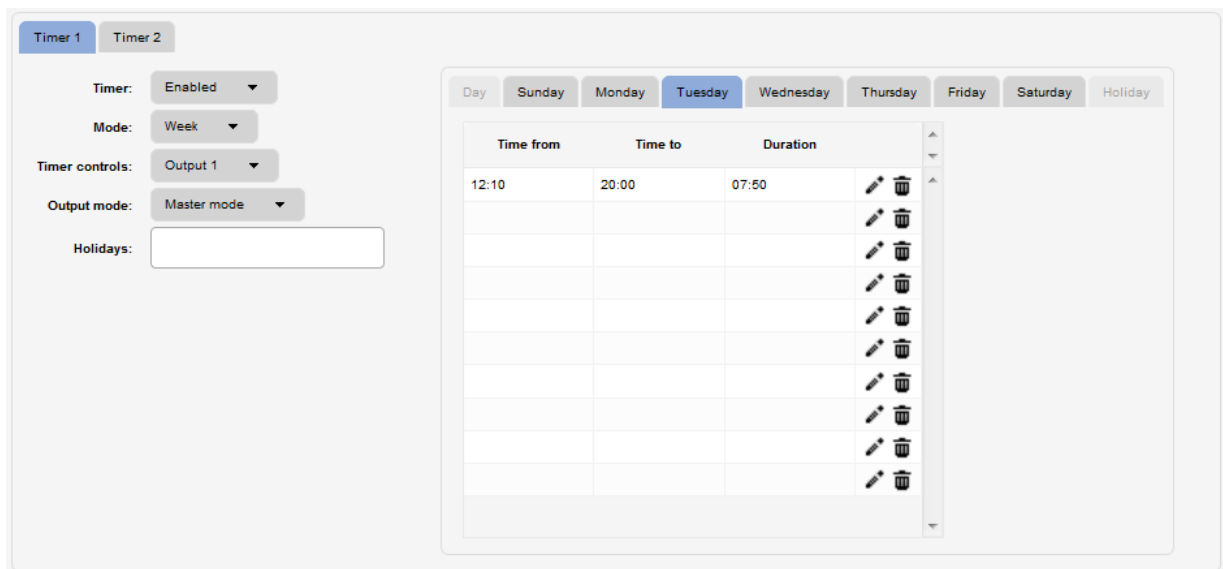
Figure 14: WEB Server-Timer setting →Week mode.

Timer settings:

- **Timer:** Parameter is used to enable and disable the timer function.
- **Mode:** User can select between day or week mode. In day mode the timer will control on the day table which is the same for all week. In week mode the user can define different setting for each day in the week.
- **Timer controls:** Output controlled by the timer function.
- **Output mode:** Output mode management definition.

OUTPUT mode options	Description
Slave mode	The behavior of the outputs (Time pulse or Latching mode) is defined in the **Output** tab.
Master mode:	When the output is driven by the timer (output is activated by the timer) the outputs are in latching mode regardless of the setting in **Output** tab. When the output is not activated by the timer, the outputs are working by the defined settings in **Output** tab.
Output precondition	In this mode Timer is used as PRECONDITION for output control used by other functions like PIN access or Called ID #.

Table 2: WEB Server-Timer setting, output mode options

- **Holidays:** With the definition of the holiday days (use day picker), user can define special behavior on the holiday days.

The described settings are the same for both timers.

NOTE	**Self-updating clock** (Misc tab) MUST be enabled for proper function of timer function!

8.9 ADMINISTRATION

Administration tab allows user to enable advanced settings: notification of unauthorized access, periodic test messages, lock down of the unit…
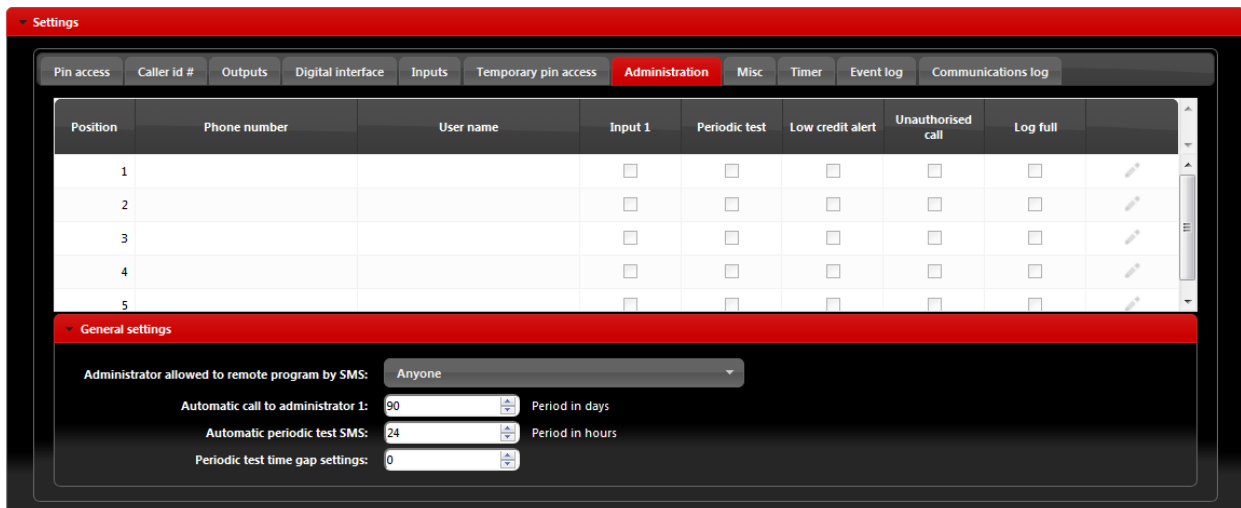
Figure 15: WEB Server-Notification numbers

- **Phone number**, **User name:** Phone number and user name of the user that will be receiving notification messages.
- **Input1:** If on input line 1 alarm condition is meet, users with check boxes will receive alarm notification SMS.
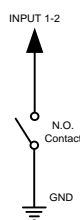
Figure 16: WEB Server-Input alarm configuration
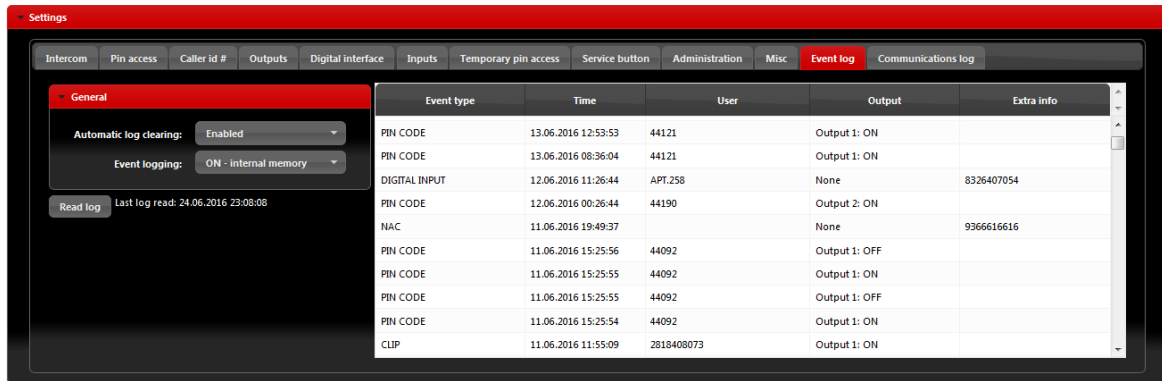
- **Periodic test:** User can receive periodic (keep-alive) SMS, tick the check box for the appropriate user. Timer period is defined under parameter **Automatic periodic test SMS**, it is definable in hours.
- **Low credit alert:** In case of prepaid SIM card the unit can notify the user if the credit on the SIM card is low. To enable notification SMS tick the check box in corresponding position. Note that additional input in the **Misc** tab is needed to fully enable credit checking function.

- **Unauthorized call:** In case of unauthorized call the unit can notify user. To enable notification SMS tick the check box in corresponding position.

- **Administration allowed to remote program by SMS:** By selection this option the user can "Lock down" the W-LOCK unit, preventing any unauthorized user to change any configuration on the unit.

- **Automatic call to administrator 1:** To prevent SIM card provider to lock out the SIM card from the network, user can define a periodic call out to telephone number under position 1. Parameter is defined in days (It is not mandatory to set this parameter).

8.10 EVENT LOGING

W-LOCK unit itself supports a 20000 log event entry. These log events can be pull up to the server by clicking **Read Log** button in the "Event Log" tab. Events are listed in the table.

Figure 17: WEB Server-Log event

Each event is equipped with the event type, time, output if triggered and the user name of the user responsible for the event.

If user names are available (Called ID #, PIN codes, Intercom user …) user name will be shown in the user column.

NOTE	After events are read and stored to the server, the local copy on the unit gets deleted.

8.11 MISCELLANEOUS

This tab is split into 2 sections.
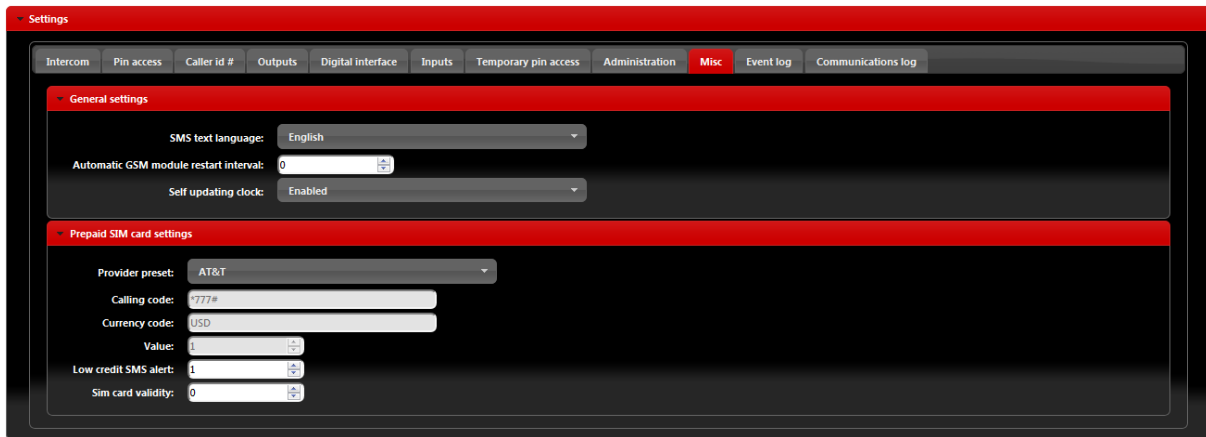
Figure 18: WEB Server-Misc

General settings can be found:

- **SMS text Language**: define the language of the SMS information send out. User can select appropriate language in drop-down menu.
- **Automatic GSM module restart interval:** User can select GSM module restart interval (hours) if needed (Not advisable to use this parameter if not advised otherwise).
- **Self-updating clock:** Parameter is used to allow unit to synchronize to real time. To have the correct time along in log event it is advisable to enable this function.

Prepaid SIM card setting is used the enable credit checking/parsing in case if prepaid SIM card is used. User can select the proper setting by selecting used SIM card provider in the drop down menu in **Provider preset.**

9   WIEGAND INPUT DATA FORMATs

W-LOCK unit support standard Wiegand interface, it will work with Wiegand 26bit and Wiegand 30bit protocol. On each Wiegand protocol W-LOCK unit support 4 different data formats, they all can be selected through all possible management systems.

Selecting the appropriate data format for Wiegand interface is done by connecting the WEB server, selecting the **Digital interface** and in **Input** section selecting proper **Mode** option.

Figure 19: WEB Server-First Wiegand interface support.

9.1 WIEGAND 26 BIT, DIFFERENT DATA FORMATS

Possible data format:

Mode 0: All 24bit of data are used a decimal representation, no option for facility code

P	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity											**24Bit card number**														**Parity**

	Limits
Card Number	0 - 16777215
Facility Number	None

Table 3: Wiegand 26: Mode 0.

Mode 1: 24bit of data is divided between facility code 8 bits and 16bits for card number

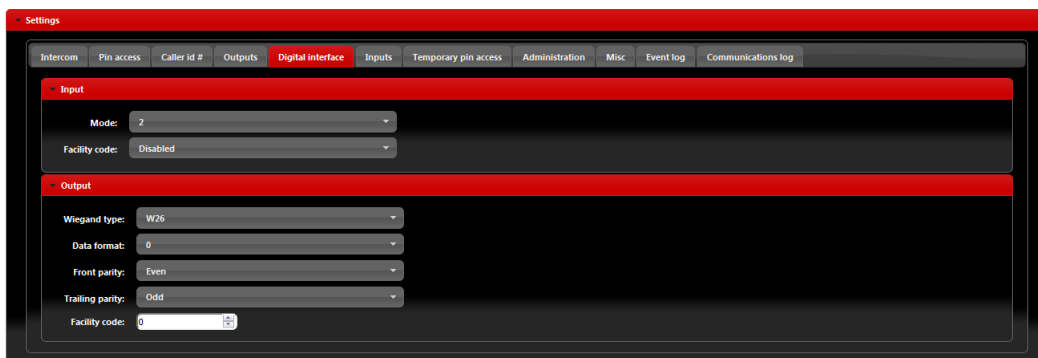	P	F	F	F	F	F	F	F	F	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity			**8Bit card facility number**										**16Bit card number**												**Parity**

	Limits
Card Number	0 - 16777215
Facility Number	NOT USED

Table 4: Wiegand 26: Mode 1.

Mode 2: 24bit of data is divided between facility code 8 bits and 16bits for card number

P	F	F	F	F	F	F	F	F	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity			**8Bit card facility number**										**16Bit card number**												**Parity**

	Limits
Card Number	0 - 16777215
Facility Number	0 - 255

Table 5: Wiegand 26: Mode 2.

Mode 3: Sections of 4bit data are used as decimals values for number

P	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity		**Dec. 6**			**Dec. 5**			**Dec. 4**			**Dec. 3**			**Dec. 2**			**Dec. 1**								**Parity**

	Limits
Card Number	0 - 99999
Facility Number	None

Table 6: Wiegand 26: Mode 3.

9.2 WIEGAND 30 BIT, DIFFERENT DATA FORMATS

Possible data format:

Mode 0: All 30bit of data are used a decimal representation, no option for facility code

P	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity													**28Bit card number**																**Parity**

	Limits
Card Number	0 - 268435455
Facility Number	None

Table 7: Wiegand 30: Mode 0.

Mode 1: 30bit of data is divided between facility code 8 bits, 16bits for card number and 4bits of unused data.

P	0	0	0	0	F	F	F	F	F	F	F	F	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity	**Not used**				**8Bit facility number**								**16Bit card number**																**Parity**

	Limits
Card Number	0 - 16777215
Facility Number	NOT USED

Table 8: Wiegand 30: Mode 1.

Mode 2: 28bit of data is divided between facility code 8 bits, 16bits for card number and 4bits of unused data.

P	0	0	0	0	F	F	F	F	F	F	F	F	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity	**Not used**				**8Bit facility number**								**16Bit card number**																**Parity**

	Limits
Card Number	0 - 16777215
Facility Number	0 - 255

Table 9: Wiegand 30: Mode 2.

Mode 3: Sections of 4bit data are used as decimals values for number

P	0	0	0	0	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	P
Parity	**Not Used**				**Dec. 6**				**Dec. 5**				**Dec. 4**				**Dec. 3**				**Dec. 2**				**Dec. 1**				**Parity**

	Limits
Card Number	0 - 99999
Facility Number	None

Table 10: Wiegand 30: Mode 3.

10 CONTACTS

MARS COMMERCE d.o.o.
MIRKA VADNOVA 19
4000 KRANJ
SLOVENIA

TEL: 00 386 4 280 74 00
E-MAIL: info@mars-commerce.com
WEB SITE: www.mars-commerce.com

TEHNICAL SUPPORT
Tomaz HRIBAR
Email: tomaz@mars-commerce.com

SALES
Uros STARE
Email: sales@mars-commerce.com