EIS: GSM CARD READER

EIS ENTRY-CR

USER MANUAL

Contents

Figures

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

EIS ENTRY-CR (EIS) 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 EIS supports alarm detection, stay-alive messages, credit detection etc…

3 EIS ENTRY-CR FEATURES and APPLICATIONS

Features:

⇒ Built-in 5 band GSM module

⇒ Caller ID numbers control (up-to 100 caller ID numbers)

⇒ Up to 50 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

EIS unit accepts a standard GSM SIM (T-Mobile or AT&T)
card 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 EIS unit.

⇒ Connect power cable to EIS unit (YOU MUST POWER THE EIS UNIT WITH THE POWER SUPPLY 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.

⇒ EIS 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 EIS please take a look at connection diagram.

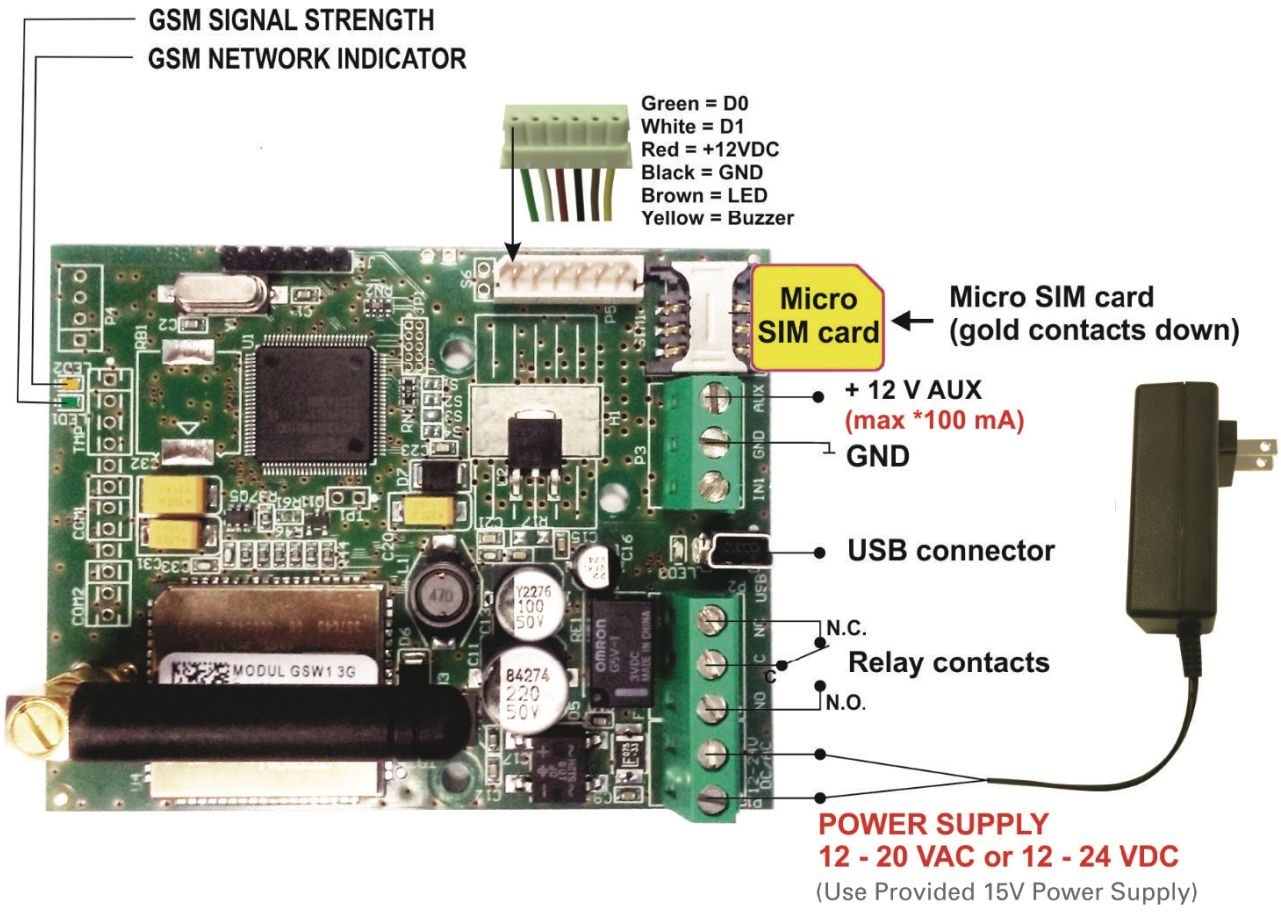

Figure 1: EIS: Connection diagram

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

7 EIS 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 (EIS Ware).

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

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

8 EIS FUNCTIONs with PROGRAMMING INSTRUCTIONs

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

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

8.1 WEB SERVER - LOG IN

The web server can be found under the address: **http://www.eisware.com/.**

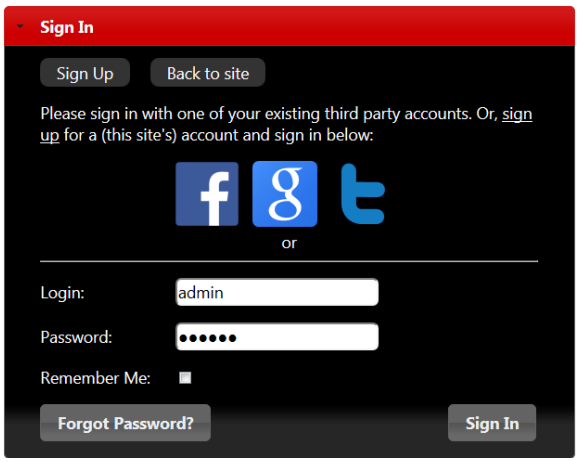

Figure 2: WEB Server-Sign In page

User must first use the Sign IN section to create working profile on the server. Create a new profile using the Sign UP button. If desired, you may sign in using your social media login.

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 EIS units from the user's profile.

Select "+" sign to select ADD EIS units to user's profile.

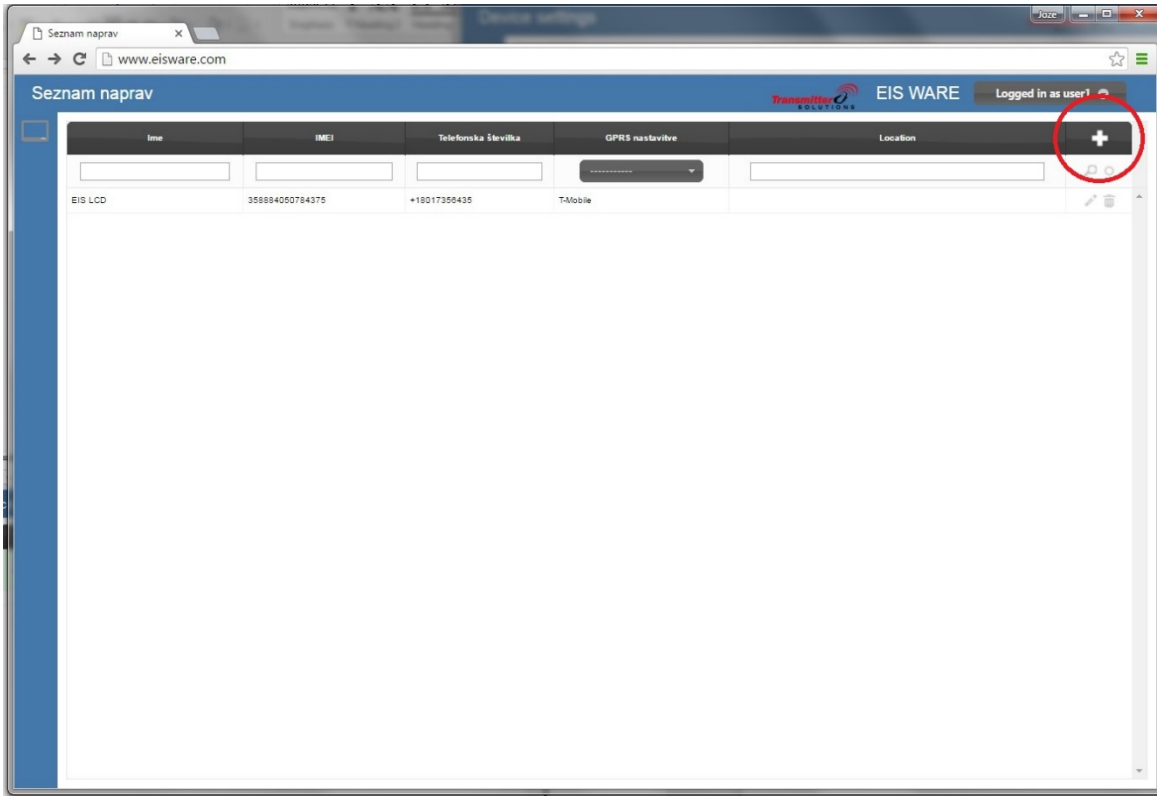

Figure 3: WEB Server-Main page select ADD mode

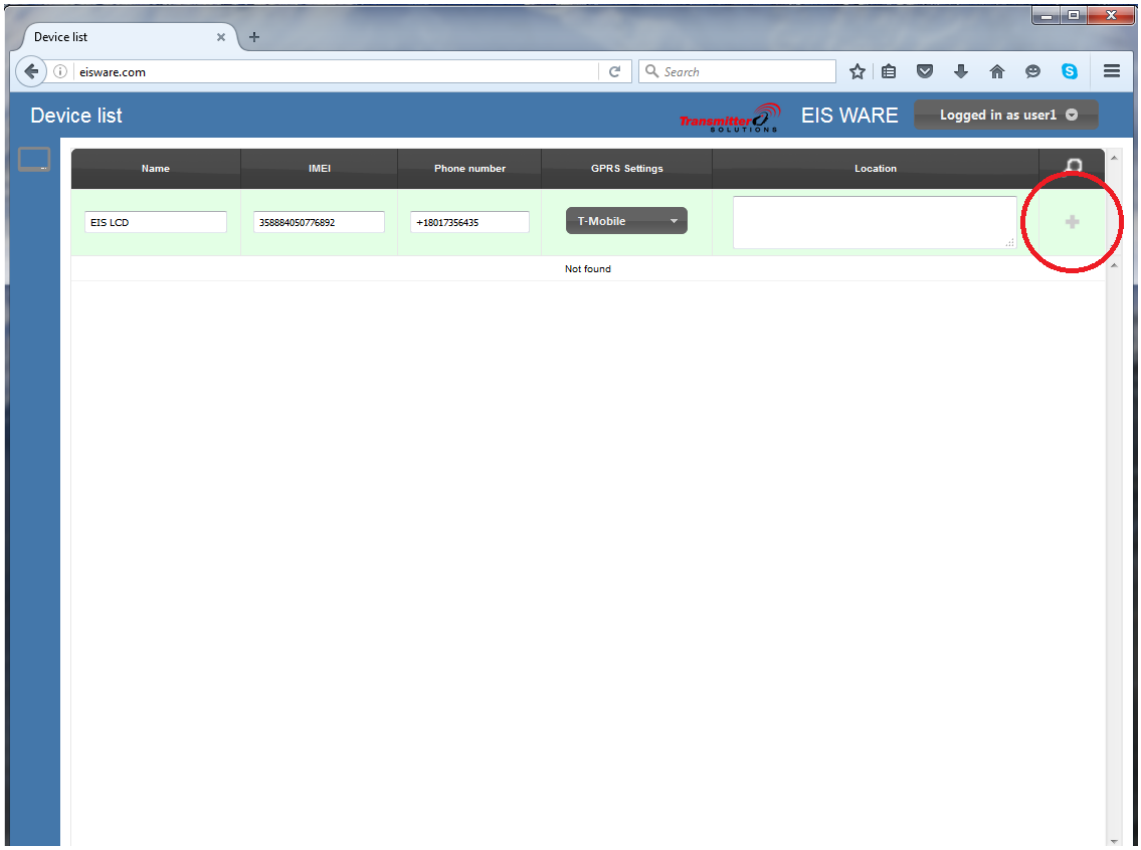

Figure 4: WEB Server-Main page adding EIS units

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 cardboard box of the EIS.
- **Phone Number:** The telephone number of the SIM card in the EIS 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 database may take a few minutes.

8.3 WEB SERVER-UNIT MANAGEMENT

After the EIS 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.

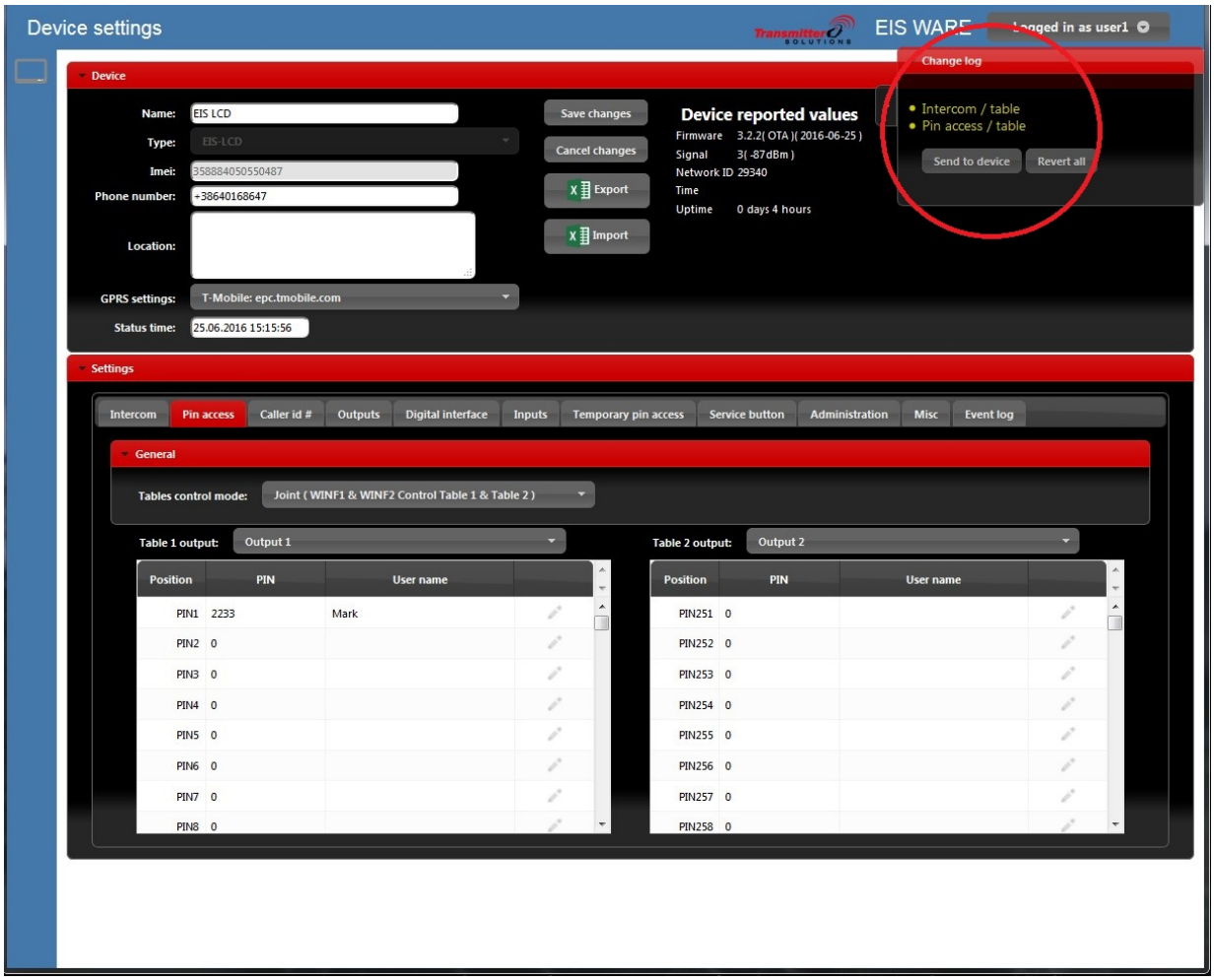

Figure 5: WEB Server-Unit management window

8.4 WIEGAND ACCESS

EIS 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. Wiegand interface can be found on board with a dedicated Wiegand connector and cables.

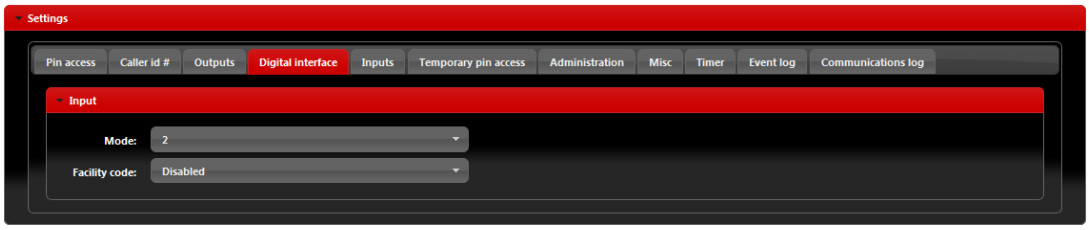

Figure 6: WEB Server-Wiegand interface support.

- **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.

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

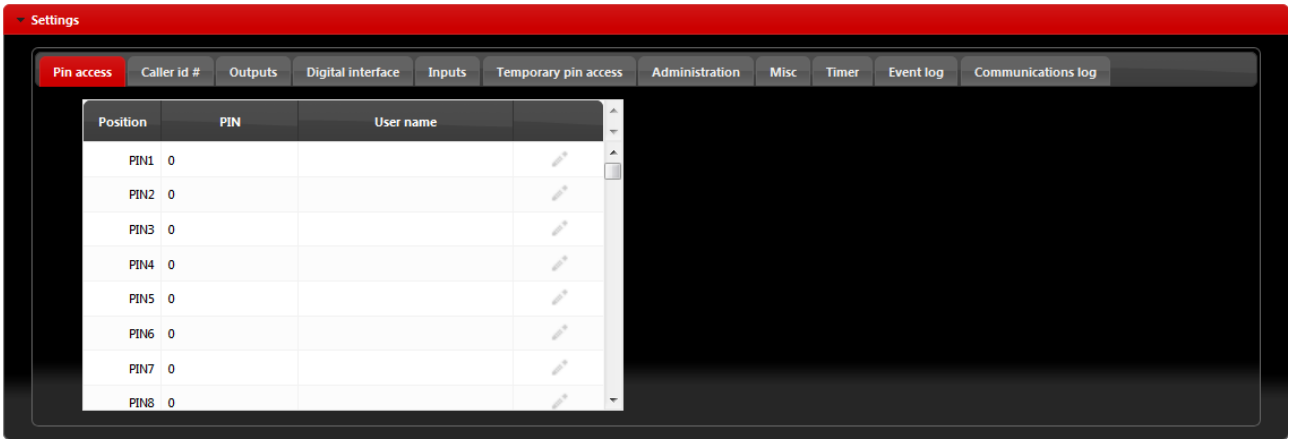

Figure 7: WEB Server-Adding Wiegand devices with permanent use.

- **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.

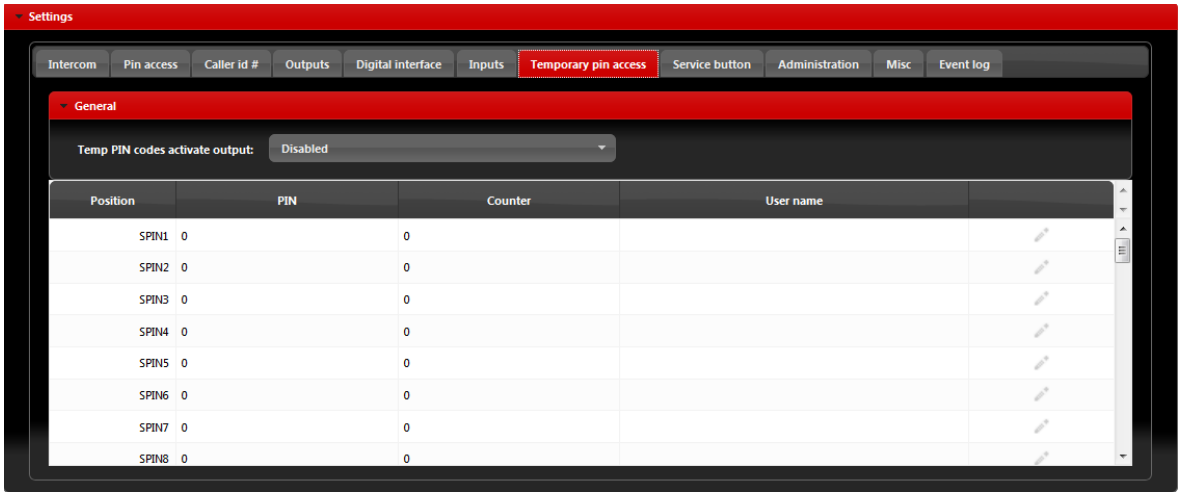

Figure 8: WEB Server-Adding Wiegand devices with temporary use.

- **Temp PIN codes activate output:** Selecting the output that will be triggered in case of correct SPIN code.
- **SPIN entry:** For each SPIN entry the user needs to select a PIN code value, 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 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 EIS unit trigger defined output.

Settings for this function are found in the **Caller id #** tab.

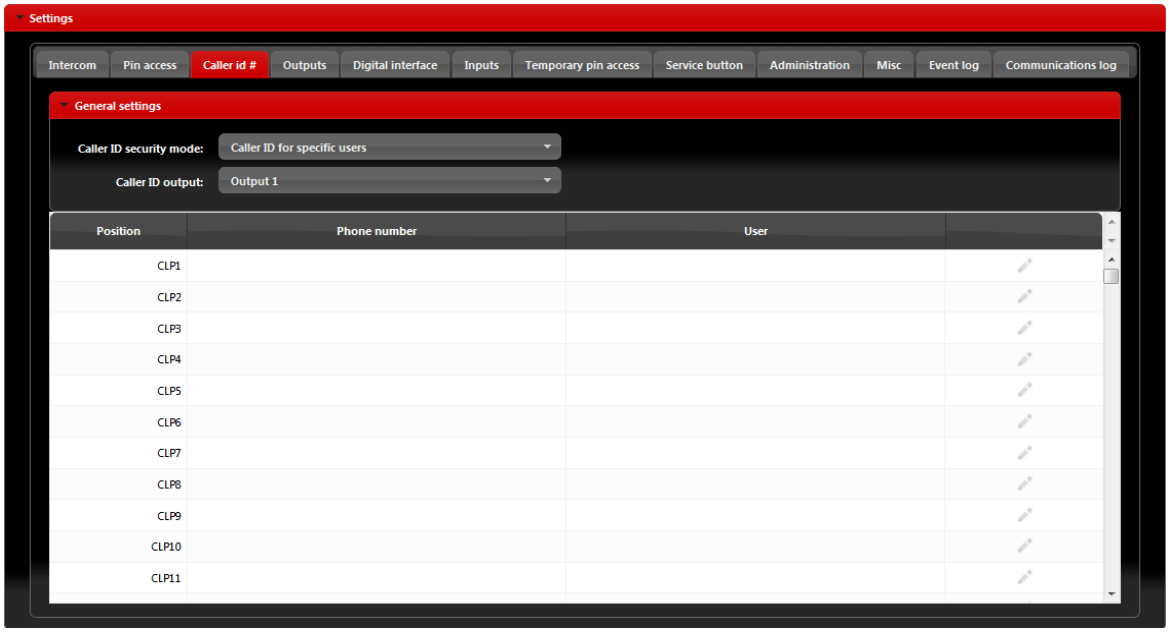

Figure 9: WEB Server-Caller ID Access

General settings:

- **Caller ID security mode:** User can select between 3 options:

  Caller ID Disabled deactivates caller ID function – all numbers are restricted

  Caller ID for specific users will limit the caller ID function only to the numbers on the list.

  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.

8.6 OUTPUTS SETTINGS

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

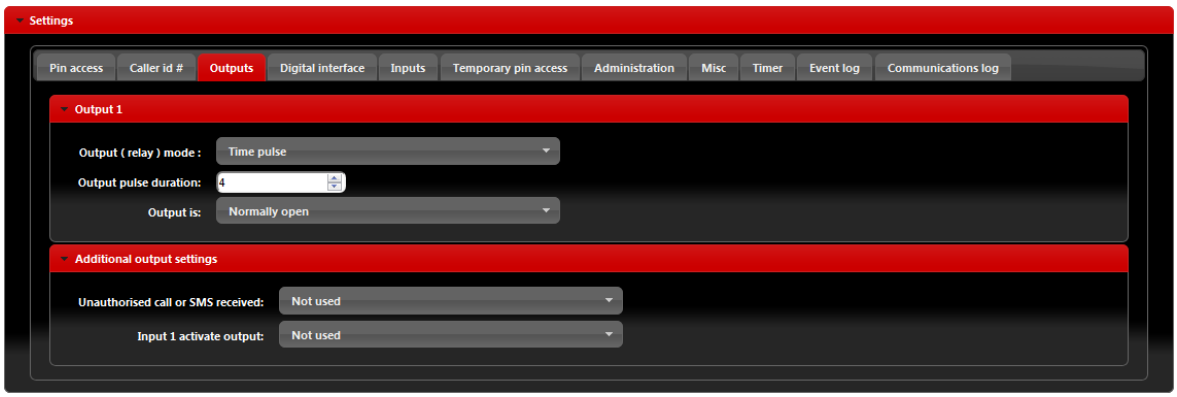

Figure 10: WEB Server-Output setting

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 activated this action will activate output defined under this section.

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

8.7 TIMER-TIMED CONTROLED OUTPUT

EIS unit features 1 timer that can be used to control the output on the unit. Timer can run in day or week mode depending on the selected setting. The behavior of the output (Time pulse or Latching mode) is defined in the **Output** tab.

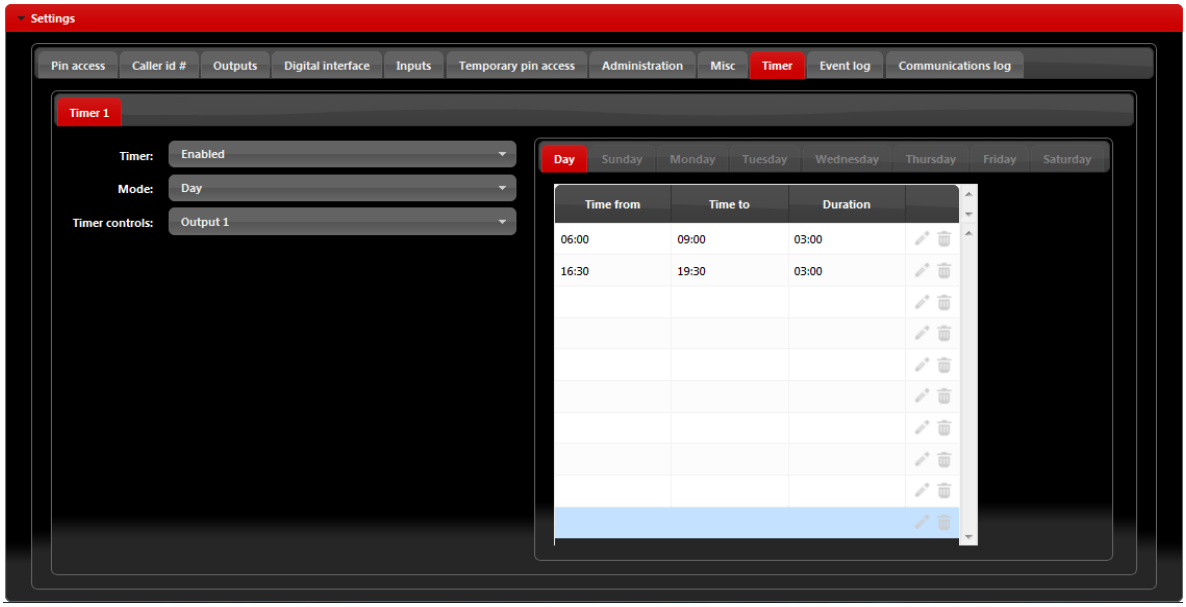

Figure 11: WEB Server-Timer setting →Day mode.

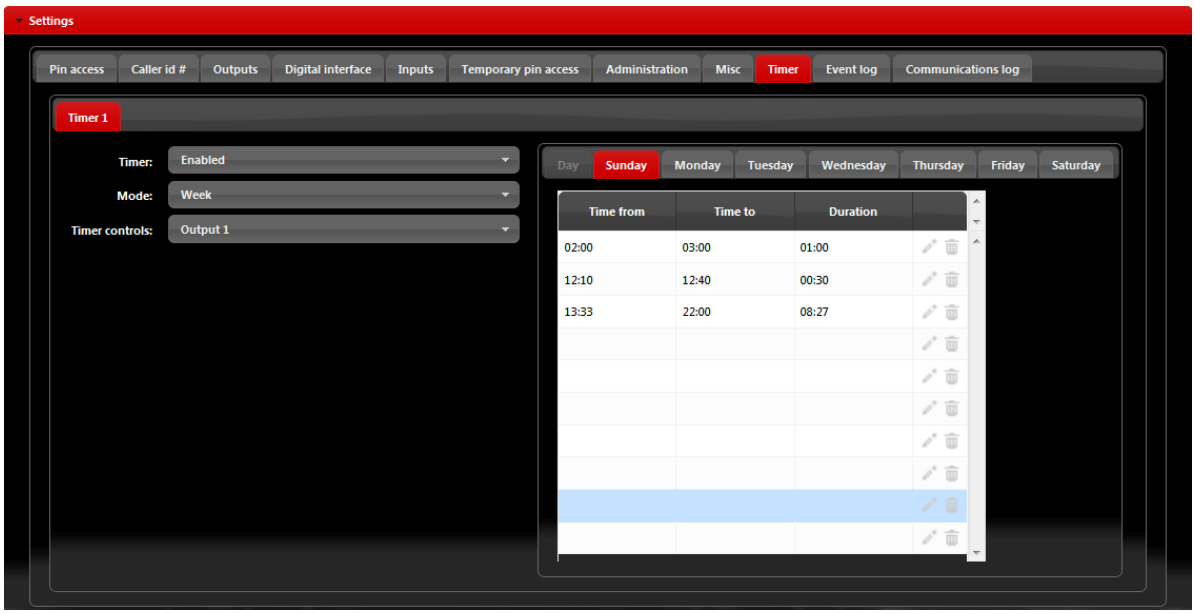

Figure 12: WEB Server-Timer setting →Week mode.

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.

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

8.8 ADMINISTRATION

Administration tab allows user to enable advanced settings: notification of unauthorized access, periodic test messages, lock down of the unit…

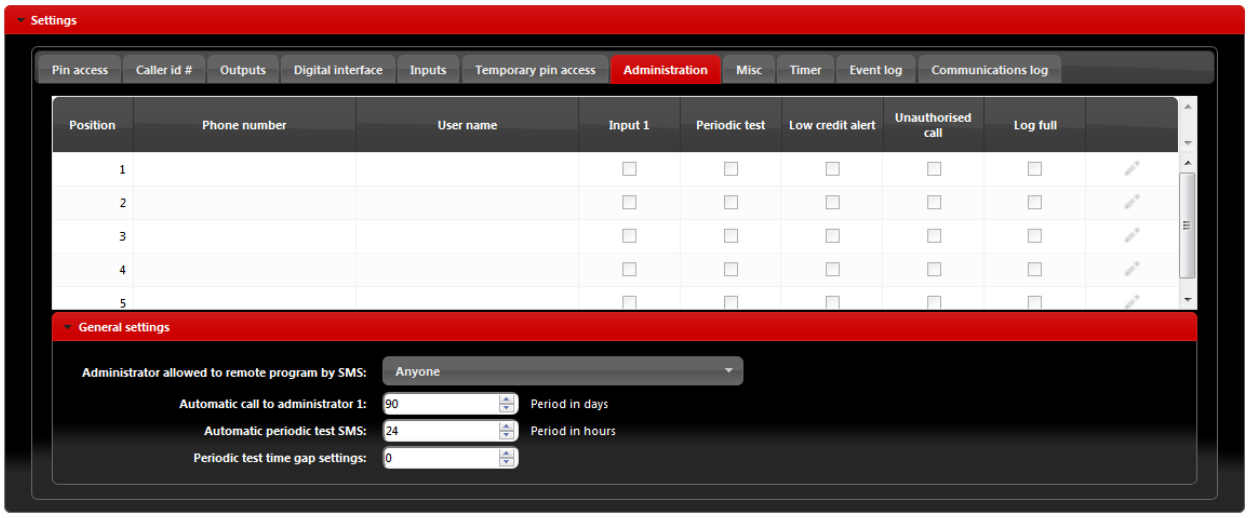

Figure 13: WEB Server-Notification numbers

- **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.

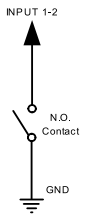

Figure 14: WEB Server-Input alarm configuration

- **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 EIS 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).

8.9 EVENT LOGING

EIS 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.

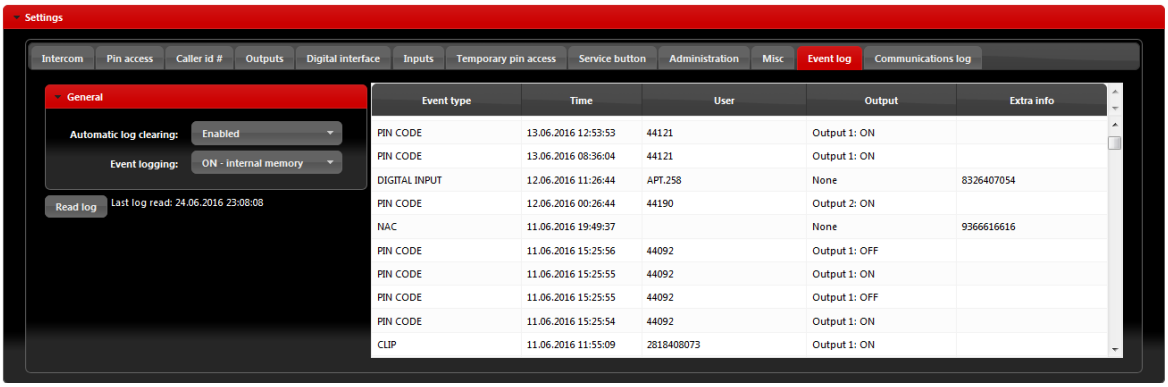

Figure 15: WEB Server-Log event

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.

8.10 MISCELLANEOUS

This tab is split into 2 sections.

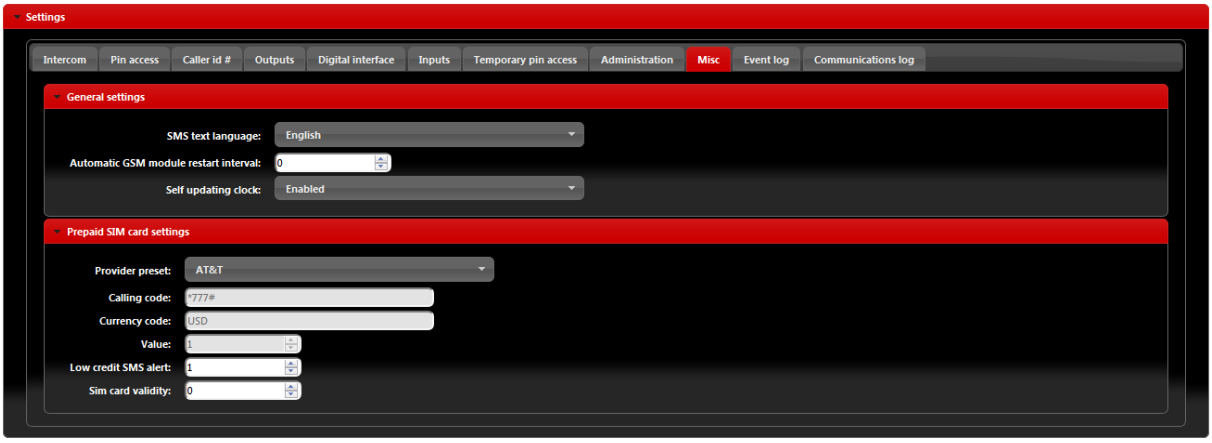

Figure 16: WEB Server-Misc

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.**

TRANSMITTER SOLUTIONS WARRANTY

The warranty period of this Transmitter Solutions product is twenty-four (24) months. This warranty shall begin on the date the product is manufactured. During the warranty period, the product will be repaired or replaced (at the sole discretion of Transmitter Solutions) if the product does not operate correctly due to a defective component. This warranty does not extend to (a) the product case, which can be damaged by conditions outside the control of Transmitter Solutions, or (b) battery life of the product. This warranty is further limited by the following disclaimer of warranty and liability:

EXCEPT AS SET FORTH ABOVE, TRANSMITTER SOLUTIONS MAKES NO WARRANTIES REGARDING THE GOODS, EXPRESS OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. BUYER MAKES NO RELIANCE ON ANY REPRESENTATION OF TRANSMITTER SOLUTIONS, EXPRESS OR IMPLIED, WITH REGARD TO THE GOODS AND ACCEPTS THEM "AS-IS/WHERE-IS". TRANSMITTER SOLUTIONS SELLS THE GOODS TO BUYER ON CONDITION THAT TRANSMITTER SOLUTIONS WILL HAVE NO LIABILITY OF ANY KIND AS A RESULT OF THE SALE. BUYER AGREES THAT TRANSMITTER SOLUTIONS SHALL HAVE NO LIABILITY FOR DAMAGES OF ANY KIND, WHETHER DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING INJURIES TO PERSONS OR PROPERTY, TO BUYER, ITS EMPLOYEES OR AGENTS, AS A RESULT OF THE SALE. BUYER ALSO AGREES TO HOLD TRANSMITTER SOLUTIONS HARMLESS FROM ANY CLAIMS BUYER, OR ANY THIRD PARTY, MAY HAVE AS A RESULT OF BUYER'S USE OR DISPOSAL OF THE GOODS. BUYER HAS READ THIS DISCLAIMER AND AGREES WITH ITS TERMS IN CONSIDERATION OF RECEIVING THE GOODS.

Transmitter SOLUTIONS®

2480 SOUTH 3850 WEST, SUITE B
SALT LAKE CITY, UT 84120
(866) 975-0101 • (866) 975-0404 FAX
WWW.TRANSMITTERSOLUTIONS.COM