EIS4G -LCD Door Entry Unit

EISWARE
Programming Software

USER MANUAL

Transmitter Solutions®

EIS LCD

CONTENTS

Contacts

For technical questions, please call Transmitter Solutions Technical Support at 866-975-0101 ext. 2

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. Follow any restrictions.

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 WISELY

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

EIS LCD

2. INTRODUCTION

EIS-LCD, is a simple but powerful 4G intercom communication system designed to ensure low-cost, simple to install/use, a reliable, single-box solution for intercom application. It is designed for unlimited range, wire free 4G GSM intercom, pin code access, caller ID control and Wiegand access support.

EIS-LCD units are built for multi apartment applications.

Optional EIS supports alarm detection, heart-beat messages, and more.

3. EIS LCD FEATURES AND APPLICATIONS

Key Features

- Simple installation and setup
- Back lit for easy visibility
- Up to 200 apartments *(by model)
- 2 phone numbers per apartment
- Easy access: Up to 1000 additional caller ID numbers and 2000 (4 digit) PIN codes
- 2 relay outputs / 2 alarm inputs
- Up to 20,000 log event

- Supports 4G wireless carrier

Programming Options

- Programming by SMS commands
- Programming by Web server (EISWARE.com)

Typical Applications

- Single box, wire free intercom solution
- Remote gate opener – Caller ID number recognition
- Simple (Wiegand) access system

EIS LCD

4. START UP

EIS LCD, unit accepts a standard micro 4G GSM SIM card.

VERY IMPORTANT	**The EIS unit comes with a 4G GSM SIM card which mustbe used. No other SIM card can be used in the 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 (Blue) starts flashing. This is set in around 30 – 45 seconds.
- EIS unit is now ready to operate.

NOTE	**EIS device will “beep” in 15 sec. intervals until the unit begins normal operation.**

5. LED INDICATION

Blue LED (LED1)

- Indicates the level of the 4G signal from 1 to 5 LED flashes (1 is weak signal, 5 is excellent signal)

Red LED (LED2)

- 4G module Activity

Yellow LED (LED3)

- Short flashing indicates that the 4G module is ON, but it is not yet connected on the 4G GSM network. After connection, yellow led flashes with short pulse (0.5 s) ON and a long pulse OFF (5s)

EIS LCD

6. CONNECTION DIAGRAM

Before connection the EIS please take a look at connection diagram.

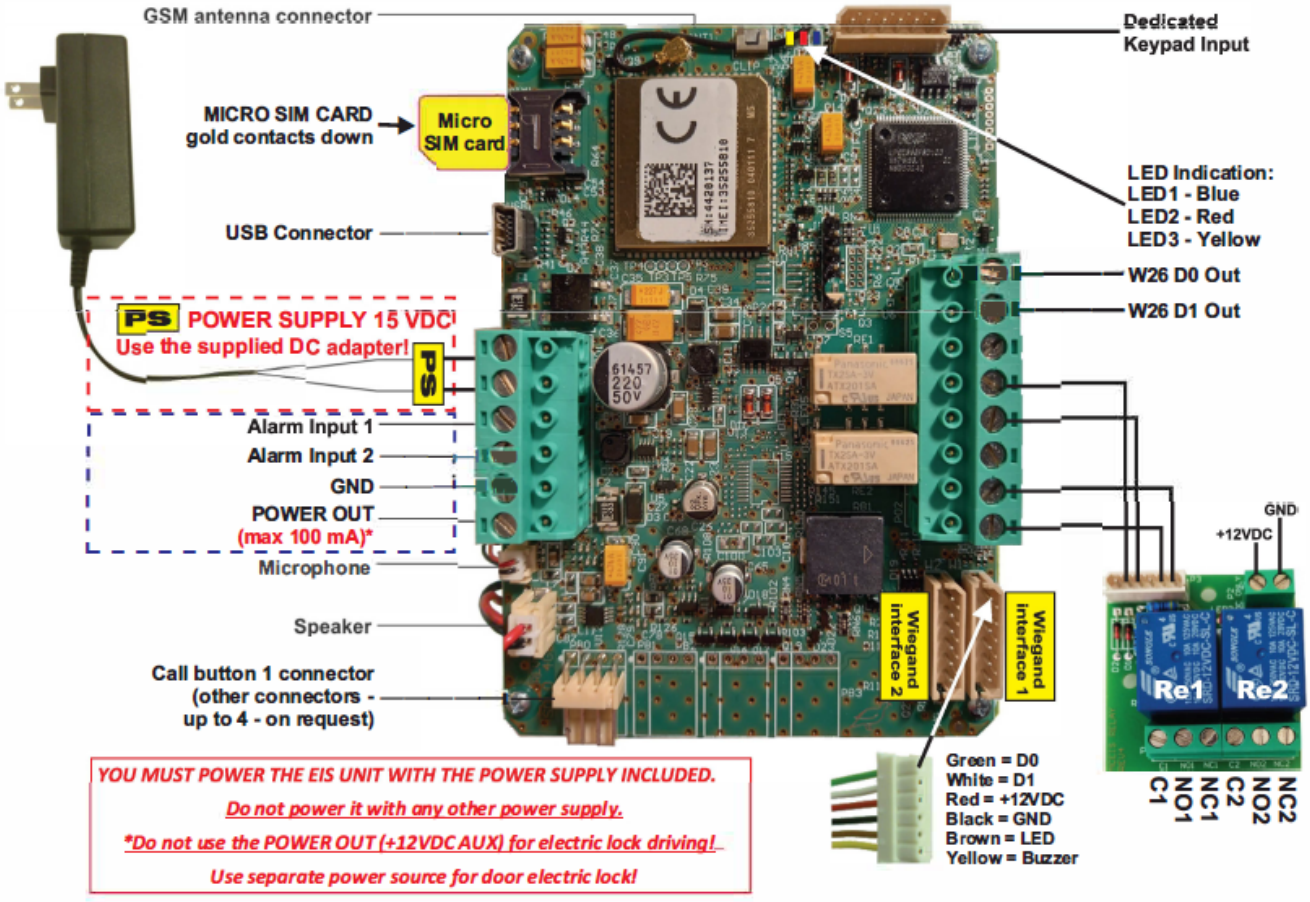

Figure 1: EIS Connection diagram

IMPORTANT	DO NOT USE Power out (12V AUX) to power electric locks! Use a separate power source for electric door locks!

7. EIS MANAGEMENT

Unit supports different types of management (programming):

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

  Access it by EISWARE.com

- EISWARE APP on IPHONE or ANDROID

  Must have data plan enabled to get data transfer on either method.

These are alternative solutions to accomplish the programming.
.

- 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.

8.1 WEB SERVER - LOG IN

Visit https://www.eisware.com/ to access the web server.

Figure 2: Web Server-Sign In page

Users must first use the Sign In section to create a working profile on the server. A profile can be created using social login options such as Facebook, Google, or Twitter. If the user does not have a social media account, they can proceed to the Sign Up page and create a profile using a standard username and password.

NOTE	**Server supports: Firefox, Google Chrome, Safari.**

8.2 Web SERVER – ADDING UNITS TO USER PROFILE

After logging in, the user will be redirected to the main web server dashboard. From this page, users can add, remove, or search for EIS units linked to their profile.

Select “+” sign to select ADD EIS units to user’s profile.

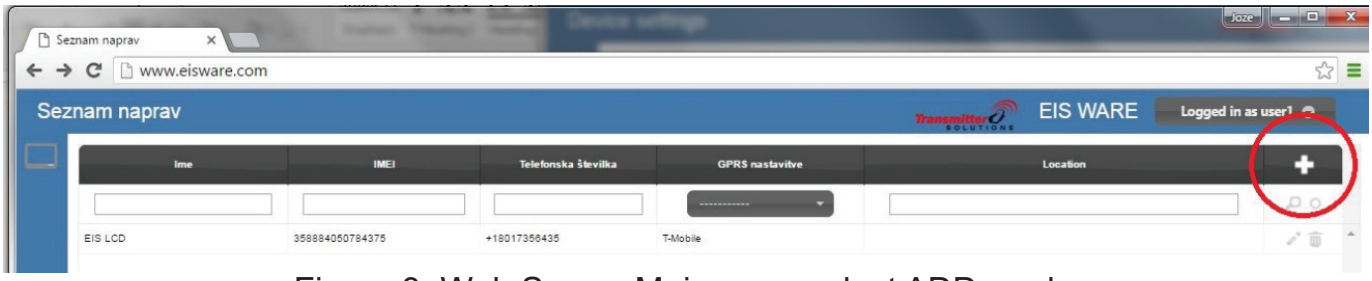

Figure 3: Web Server-Main page select ADD mode

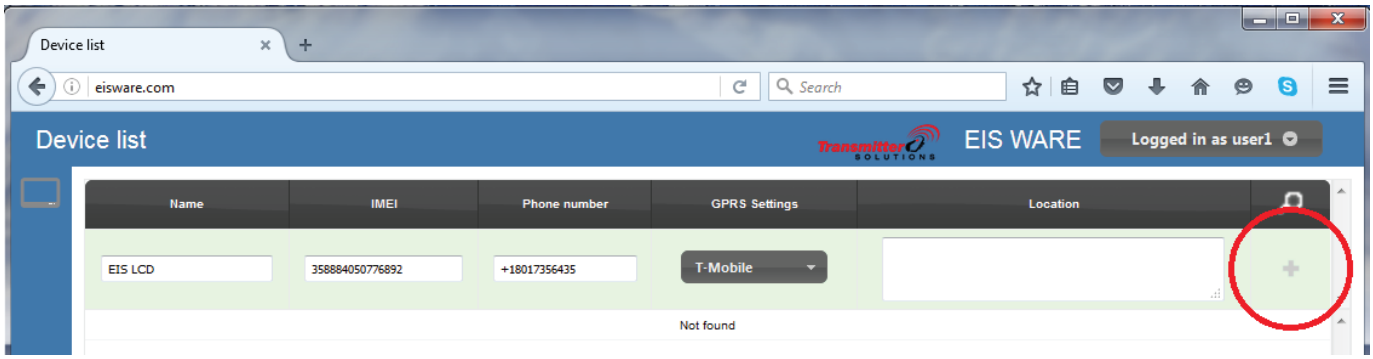

Figure 4: WEB Server-Main page adding EIS units

User then 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 EIS.
- **Phone Number:** The telephone number of the SIM card in the EIS unit - mandatory data.

Optional Information:

Location: Extra notification field available for the user for their own information

Please note: First-time build of the database may take a few minutes.

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

First building of the unit data-base may take a few minutes. It will show a progress window.

8.3 WEB SERVER-UNIT MANAGEMENT

Once the EIS unit has been added to the user’s database, the configuration settings can be modified as needed.

All changes are tracked in the **Change Log** window. To apply the updates, click the **Send to Device** button—this will transmit all pending changes to the unit. User can (Revert) the changes made, before sending, by clicking (Revert all) or select particular entry and revert it.

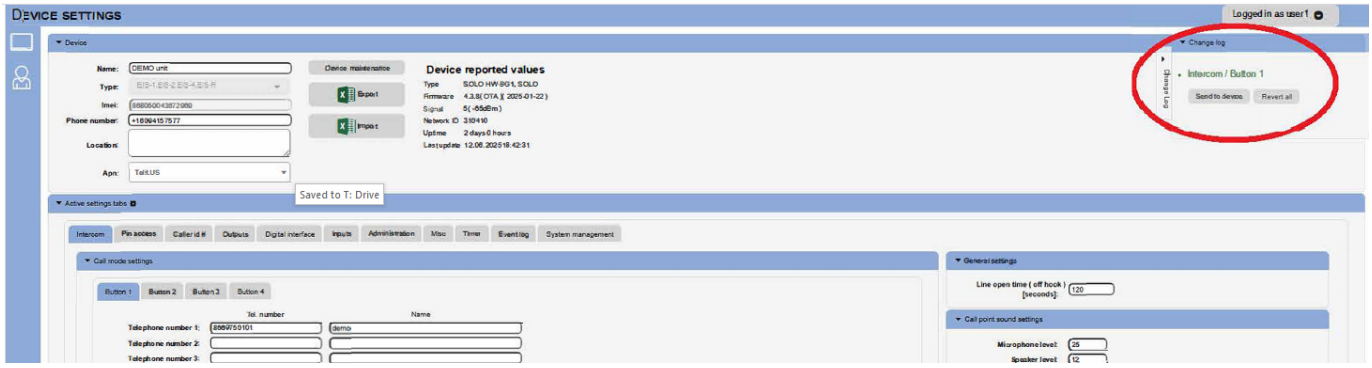

Figure 5: WEB Server-Unit management window

8.4 INTERCOM CONFIGURATION

The primary function of the EIS LCD unit is to provide intercom support. To initiate a call, the visitor presses the call button located next to the appropriate nameplate, corresponding to the intended apartment or user.

This action triggers a sequential voice call process, starting with **Phone Number 1** and continuing through to **Phone Number 5**, if necessary. Once the call is answered, the recipient can remotely activate one of the outputs by pressing:

- **"11"** to open **Output 1**
- **"21"** to activate **Output 2**

If the call is successfully answered, the system will not call remaining numbers in the sequence. Intercom settings and configuration can be managed via the **Intercom** tab in the web interface.

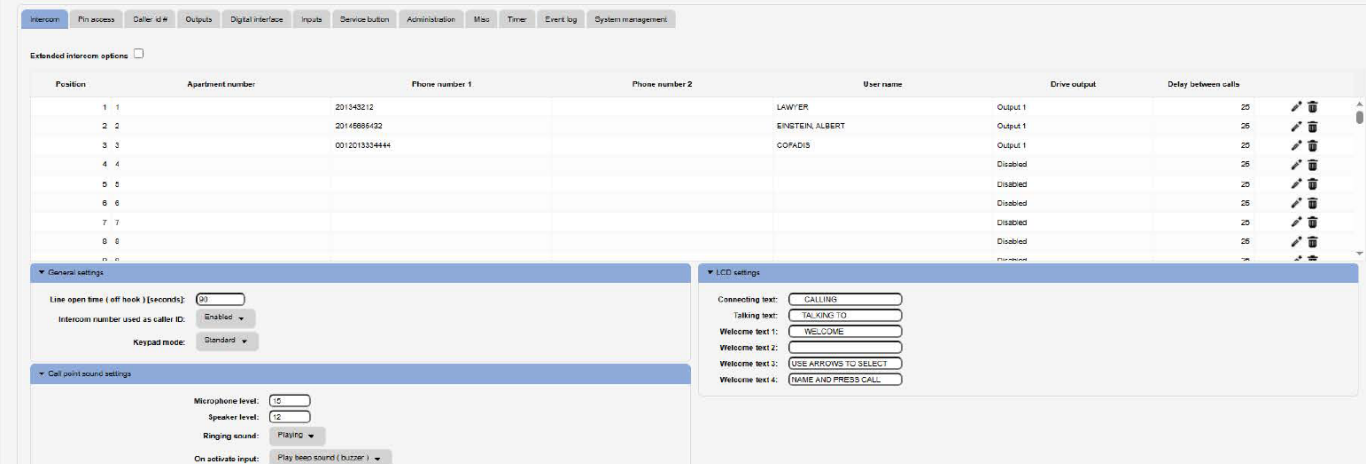

Figure 6: Web Server-Intercom settings.

Intercom management parameters:

- **Delay Before Dialing Next Number**: Sets the time delay (in seconds) before moving to the next number in the list if the previous call is not answered.
- **Extension Number**: Specifies the DTMF number used for automatic self-selection.
- **Extension Number Delay**: Sets the delay (in seconds) before sending the DTMF tone during auto-selection.
- **Work Time Start / End**: Defines the working hours during which Phone Numbers 1–4 are dialed. Outside of this time range, only Phone Number 5 will be called.

Voice call setting:

- **Line Open Time (Off-Hook) [seconds]**: Defines the maximum allowed call duration. Once this time limit is reached, the call will automatically disconnect.
- **Microphone Level**: Adjusts the microphone sensitivity. Increasing the level enhances pickup sensitivity; decreasing it reduces sensitivity.
- **Speaker Level**: Controls the speaker volume. Higher values increase output volume; lower values reduce it.
- **Ringing Sound**: When set to *Playing*, the unit emits a dial tone during the call connection phase. When set to *Muted*, no tone is played.
- **On Activate Input**: When *Play Beep Sound* is selected, the unit provides audible feedback (a beep) when a call button is pressed. When *Muted* is selected, no feedback sound is generated.

8.5 PIN ACCESS

The onboard keypad and external Wiegand devices enable secure access through PIN code entry. PIN code management is performed via the web server, which offers both simplified and advanced configuration views:

- **Simplified View**: Allows basic setup and management of PIN codes.
- **Advanced View**: Provides detailed configuration options, including usage restrictions and output assignments.

PIN codes can operate in three distinct modes, each is tailored to different access control needs:

Basic Control Mode:

A single PIN code can activate up to four predefined outputs. This mode supports full restriction options, including usage counters and time-based access limits.

Access Mode:

Each Wiegand input is assigned to a specific output:

- A PIN code entered via Wiegand Input 1 will trigger Output 1.
- A PIN code entered via Wiegand Input 2 will trigger Output 2.

All standard restriction parameters (usage counter and time limits) apply.

Restricted Access Mode:
This mode functions similarly to Access Mode but allows the user to assign a specific output to each PIN code manually, regardless of the Wiegand input used. Full restriction controls are also available in this mode.

The available configuration options on the web server interface will automatically adjust based on the selected PIN code mode.

PIN code configuration options

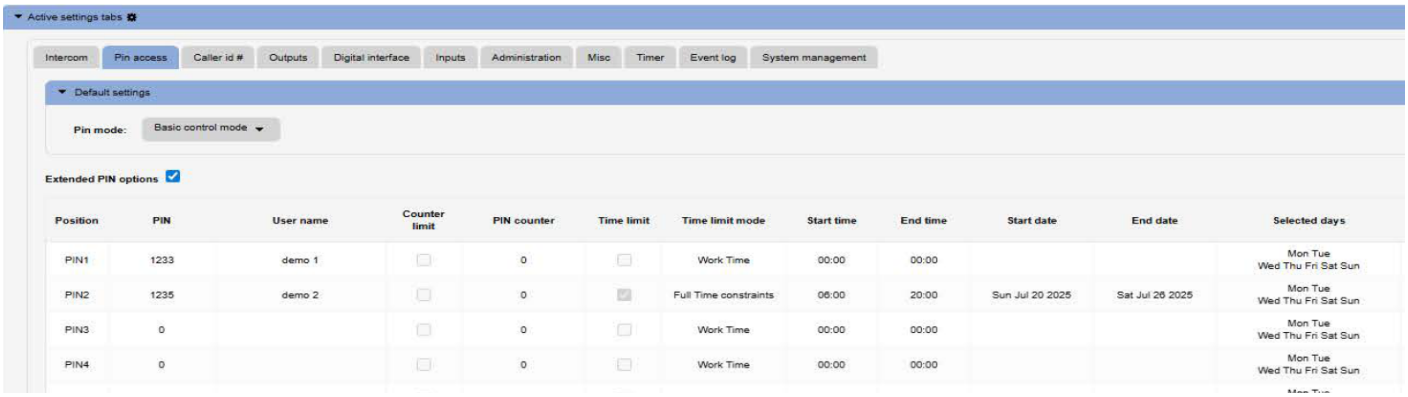

Figure 7: Web Server - PIN Access configuration

Configuration options	Description
PIN	The numeric value of the PIN code.
User name	Name or label assigned to the user associated with the PIN
Counter limit	Enables or disables a restriction on the number of times the PIN can be used.
Pin counter	Defines the maximum number of allowed uses when the counter limit is enabled.
Timer limit	Enables or disables time-based access restrictions.
Timer mode	- *Work Time*: Limits access by hours only (daily schedule, no calendar). - *Full Time Constraint*: Applies both time and calendar-based restrictions.
Start Time	Specifies the daily start time (in hours and minutes) when the PIN is valid.
End Time	Specifies the daily end time (in hours and minutes) for PIN validity.
Start date	Defines the calendar start date for PIN validity.
End date	Defines the calendar end date for PIN validity.
Selected days	Specifies which days of the week the PIN code is valid.
Outputs	Selects the output(s) that will be triggered by the PIN code.
Sources	Specifies the allowed input source (e.g., keypad, Wiegand device) for the PIN.
Notify	If enabled, sends an SMS notification to administrators when the PIN is used.
Latch	Forces the output into latching mode when activated by the PIN code.

Table 1: WEB Server-PIN entry parameters.

EIS LCD

8.6 DIGITAL INTERFACE

The EIS unit includes onboard support for two Wiegand-based input devices. In addition to receiving input from external Wiegand devices, the unit itself can also function as a Wiegand output device, allowing it to integrate seamlessly into larger access control systems.

In this configuration, incoming calls to the EIS unit can be forwarded through the Wiegand interface to the connected access control system for further processing.

Configuration settings for the primary Wiegand interface can be found under the **Digital Interface** tab in the web server.

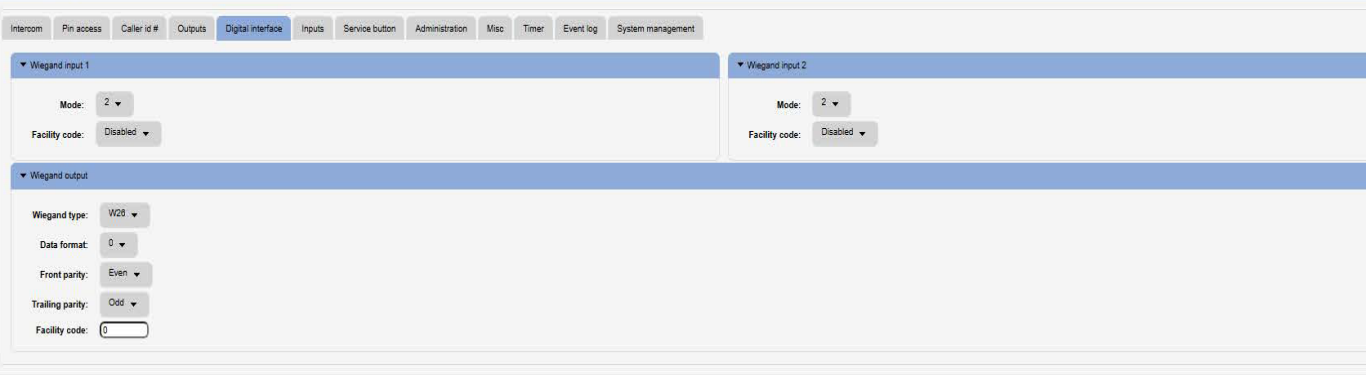

Figure 8: Web Server - Wiegand interface support.

Wiegand Inputs (Input 1 and Input 2)

- **Mode:** Select appropriate data formatting (See advance settings section if needed, mode 2 is most common setting)
- **Facility code:** User can Enable or Disable facility code field.

Wiegand Output

- **Wiegand Type**: Defines the bit length of the output data. *W26* (26-bit) is the most commonly used, and the default setting.
- **Data Format**: Choose the appropriate data format for the selected Wiegand type. Contact your provider for guidance if needed.
- **Front Parity**: Sets the type of parity used at the beginning of the Wiegand data stream.
- **Trailing Parity**: Sets the type of parity used at the end of the Wiegand data stream.
- **Facility Code**: Specifies the facility code to be included in the output data transmission.

NOTE	See Chapter 9 WIEGAND INTERFACE DATA FORMATS for a detailed explanation of different format options

8.7 CALLER ID ACCESS

Caller ID access offers a simple and convenient method for triggering relay outputs. When an authorized user places a call to the EIS unit, the system automatically recognizes the number and activates the designated output.

Configuration settings for this feature can be found under the Caller ID # tab in the web interface.

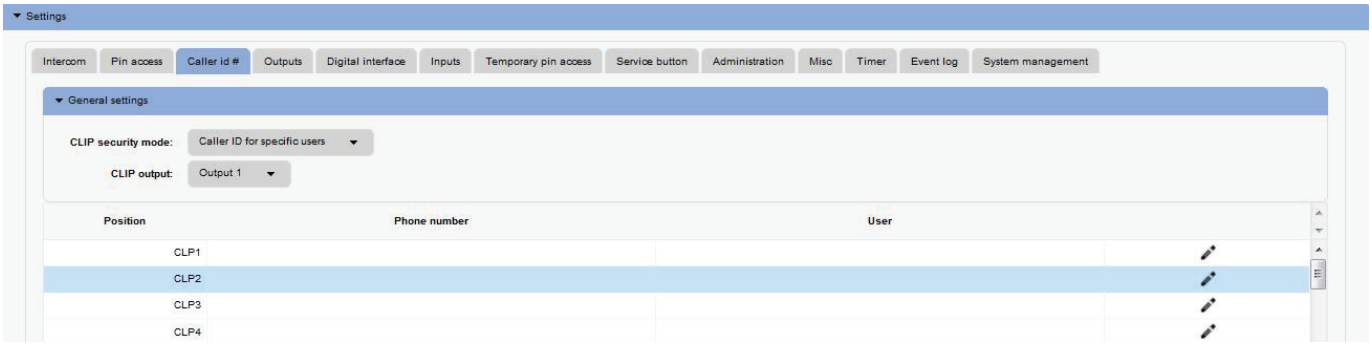

Figure 11: WEB Server-Caller ID Access.

General settings:

- **Caller ID Security Mode**: Defines how the system handles incoming calls for access control. The user can select from three modes:
  1 - ***Caller ID Disabled*** – Deactivates the Caller ID function; no numbers are permitted.
  2 - ***Caller ID for Specific Users*** – Only phone numbers listed in the system are allowed to trigger outputs.
  3 - ***Caller ID Always ON*** – Any caller who knows the unit's number can trigger the output, regardless of whether they are listed. **Use this setting with caution.**
- **Caller ID Output:** Specifies which output (e.g., Relay 1 or Relay 2) is activated when a valid call is received.
- **Phone Number:** The phone number associated with the authorized user.
- **User:** The name or identifier of the person assigned to the corresponding phone number.

NOTE	Enabling **Caller ID Always ON** allows *anyone* who knows the unit's phone number to activate the configured output by simply placing a call. This setting bypasses the user list and should be used with caution in unsecured installations.

8.8 OUTPUTS SETTINGS

The behavior on the outputs is defined in the Output tab

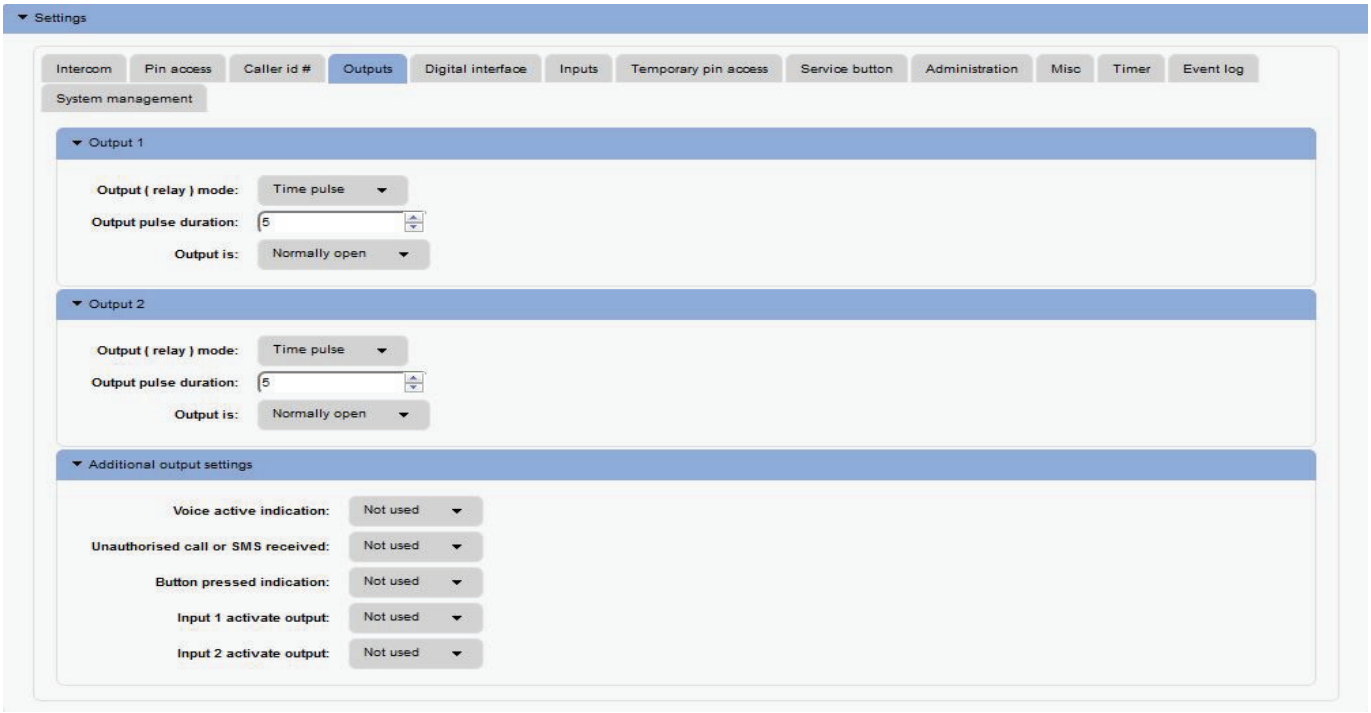

Figure 12: WEB Server-Output setting

Output 1 and **Output 2**

- **Output (Relay) Mode:** The user can select from three available options:
  Disable – The output remains deactivated at all times.
  Latching – The output operates in latching mode. The first valid Caller ID or PIN entry activates the output, and the second valid Caller ID or PIN entry deactivates it. *Time Pulse* – The output operates in pulse mode. Once triggered, the output remains active for a duration defined in the
- ***Output Pulse Duration* setting**: After this time elapses, the output automatically returns to its idle state.
- **Output pulse duration:** Defines the activation time (ON time) for the output when ***Time Pulse*** mode is selected.
- **Output is:** The output can operate in either normal or inverted (normally closed) mode. *Normally Open* – In idle state, the output contacts are open (disconnected). *Normally Closed* – In idle state, the output contacts are closed (connected).

Additional output settings - Settings used to link specific onboard events to output activation, if required:

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

- **Voice active indication:** When unit reaches voice connection (intercom call) output defined under this section gets activated.
- **Unauthorized call or SMS received:** If unauthorized call or SMS is received on the unit this event will activate output defined under this section.
- **Button pressed indication:** When intercom call button is pressed output defined under this section gets activated.
- **Input 1 activate output:** If input 1 is in alarm mode (**Input operation mode:** Normal mode selected) alarm input event on the input will activate output defined under this section.
- **Input 2 activate output:** If input 2 is in alarm mode (Input operation mode: Normal mode selected) alarm input event on the input will activate output defined under this section.

NOTE	Due to the limited number of available outputs, use the additional output settings carefully **and only when necessary.**

8.9 EIS WIEGAND OUTPUT INTEGRATION

EIS unit can be integrated into a bigger access system using a Wiegand interface. In this case numbers calling the unit will be transferred, over Wiegand interface, to access system.

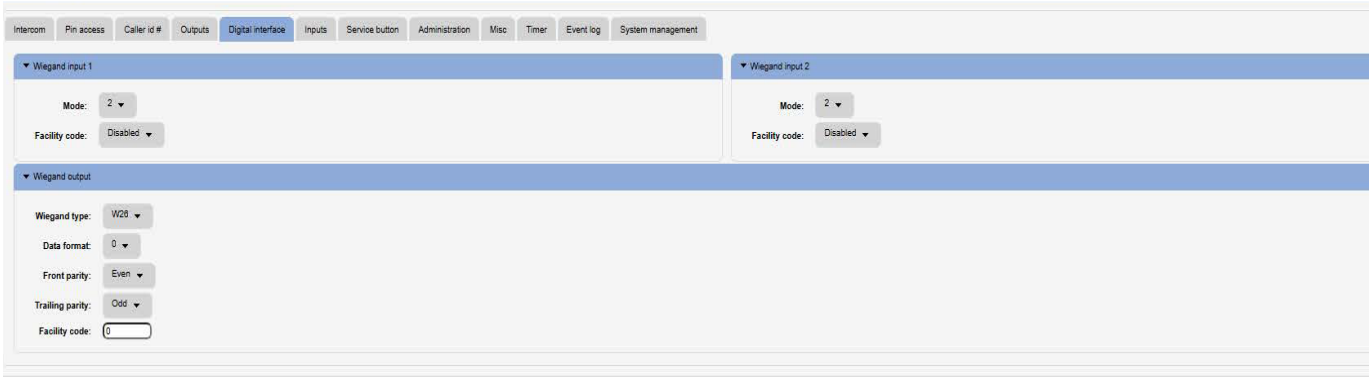

Figure 13: WEB Server-Wiegand Output settings.

Configuration of the Wiegand output interface

- **Wiegand Type:** Type of the Wiegand used (W26 is most common setting)
- **Data format:** Format of data set on the selected Wiegand type.
- **Front parity, trailing parity:** Selection of the proper parity in selected Wiegand type.
- **Facility code:** Is required, user can define facility code to Wiegand data.

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

8.10 TIMER-TIMED CONTROLLED OUTPUT

EIS unit features 2 timers that can be used to control the outputs on the unit. Timers can run in day or week mode depending on the selected setting. For each timer user can select which output it will control.

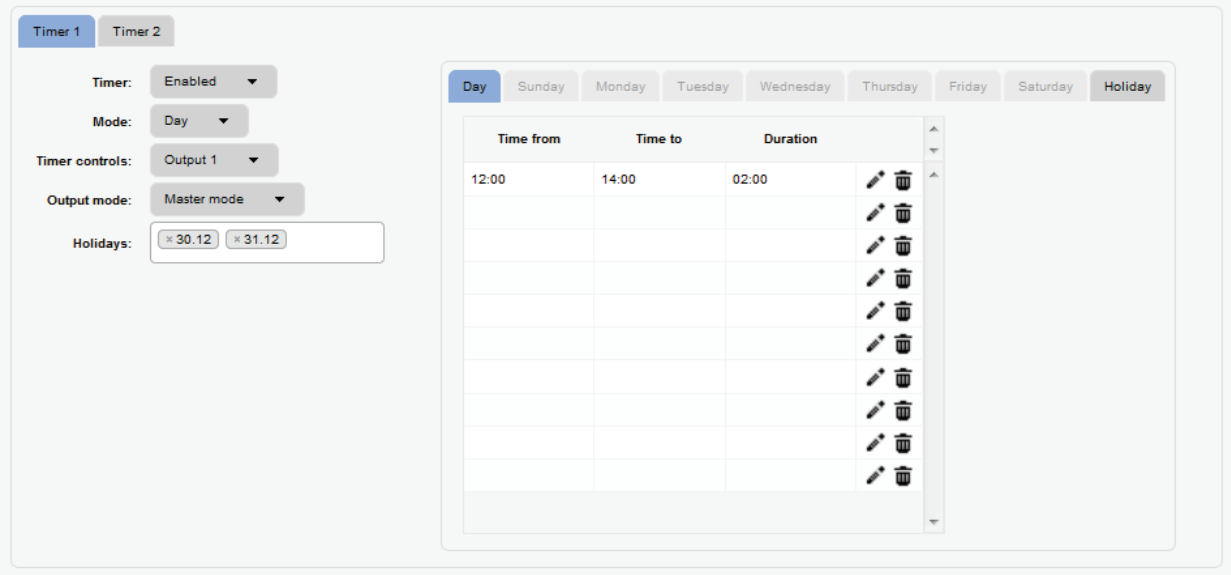

Figure 14: WEB Server-Timer setting →Day mode.

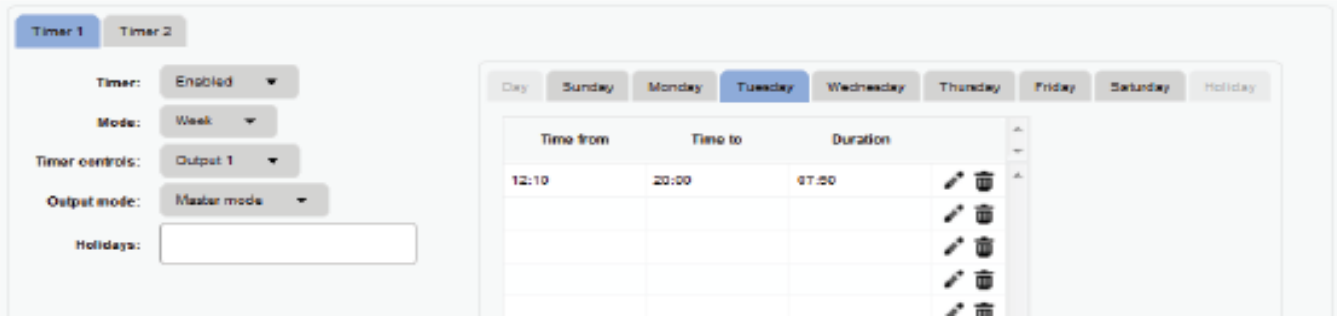

Figure 15: WEB Server-Timer setting →Week mode.

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.
  Output1 or Output2
- **Output mode:** Output mode management definition.

OUTPUT mode	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.

8.11 OUTPUTS SETTINGS

Service button is a dedicated button that is used to directly call numbers or directly trigger defined output on the EIS unit. It typically is mounted outside of the EIS Unit and is an additional component not included.

If the Call mode is selected in the Service button mode, unit will call number defined. If needed it is possible to define work hour schedule. In working time limits, unit will call first 4 number defined, out of working time limits unit will call 5th number defined.

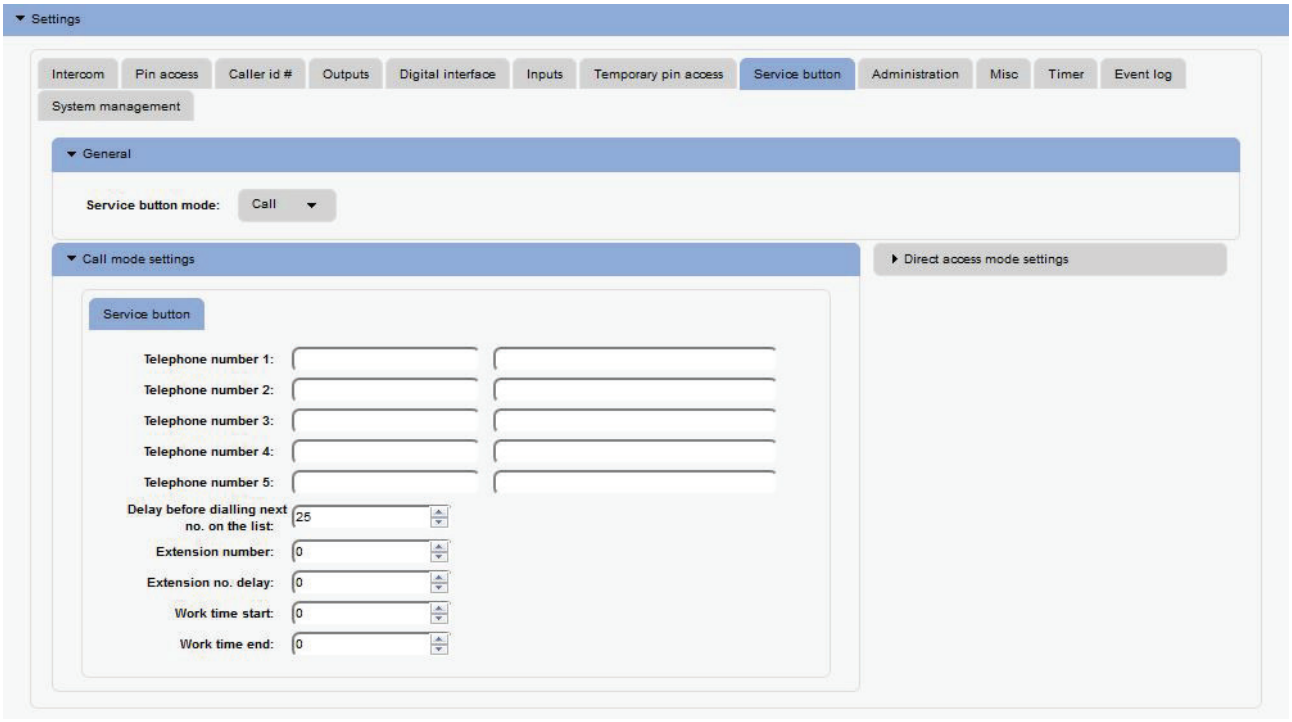

Figure 16: WEB Server-Service button settings (Call mode).

Call mode settings

- **Telephone number 1...Telephone number 5:** Number that the unit will call if button pressed.
- **Delay before dialing next no. on the list:** Time delay in second before next user on the list gets dialed if the call to the previous user is not answered.
- **Extension number:** Parameter is used to set the DTMF number in auto self-select function
- **Extension no. delay:** Parameter is used to set the delay (in sec.) for sending DTMF number in auto self-select function.
- **Work time start, Work time end:** Parameters are used to define work time schedule. Inside this limits number under position 1 to 4 will be dialed, outside this limits number under position 5 will be dialed.

If the *direct access* mode is selected in the **Service button mode**, service button press will activate output defined.

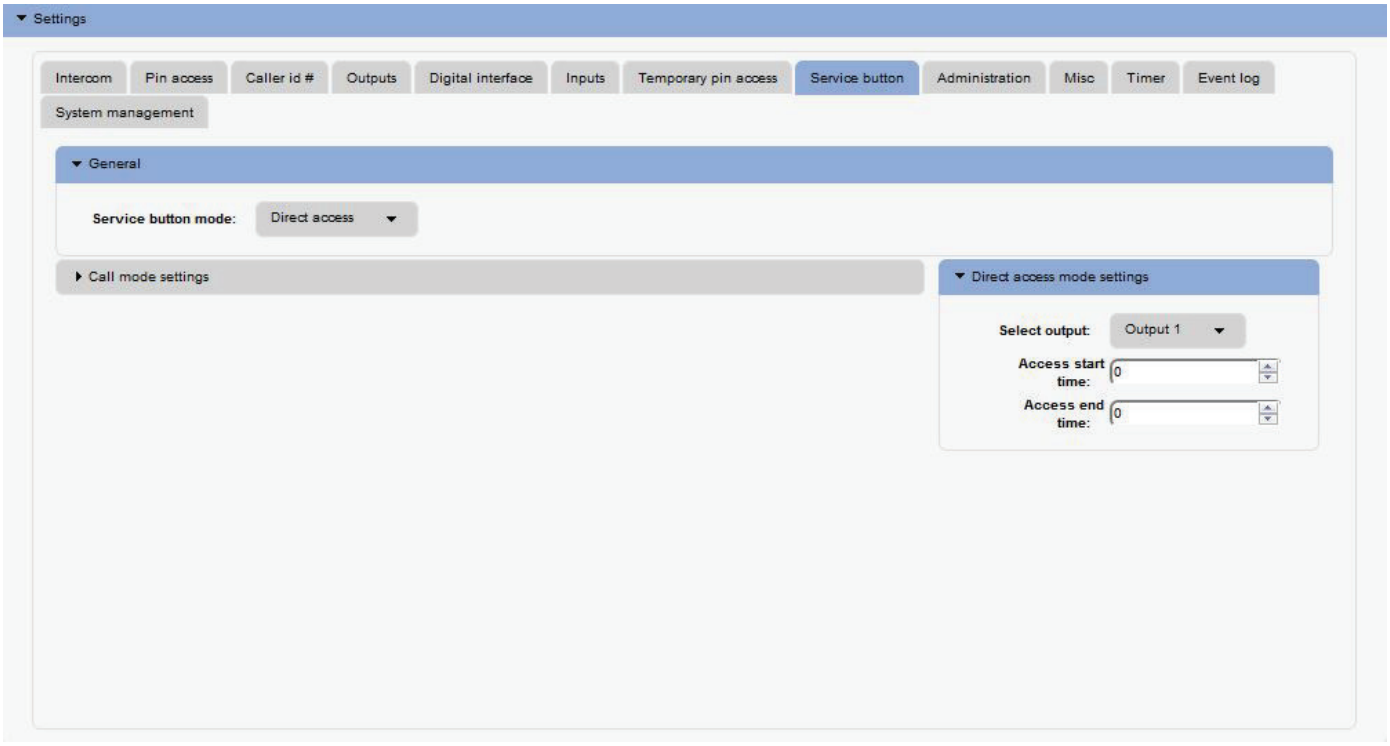

Figure 17: WEB Server-Service button settings (Direct access).

Call mode settings

- **Select output:** The output that will be triggered if service button is pressed
- **Access start time, Access end time:** Parameters are used to define work time schedule. If limits defined than only inside this limits the output defined gets triggered. If 24h access is needed don't use this limits.

NOTE	Service button is a special button that may/or may not be a part of the EIS unit. Please advise your installer if this function is needed.

8.12 ADMINISTRATION

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

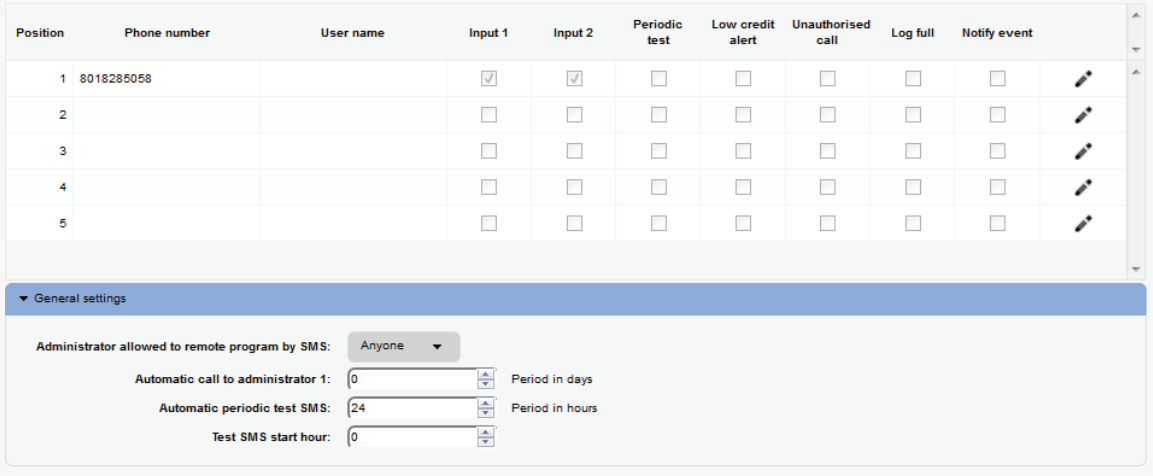

Figure 18: WEB Server-Notification numbers

- **Phone number, User name:** Specifies the phone number and user name of the user designated to receive notification messages.
- **Input1, Input2:** If input lines 1 & 2 are defined in alarm mode (Input operation mode: Normal mode) and if alarm condition is met, users with check boxes will receive alarm notification SMS.

Figure 19: Web Server-Input alarm configuration.

- **Periodic test:** User can receive periodic (heart-beat) SMS, tick the check box for the appropriate user. Timer period is defined under parameter Automatic periodic test SMS, and is definable in hours.

EIS LCD

- **Unauthorized call:** In case of unauthorized call the unit can notify user. To enable notification SMS tick the check box in corresponding position.
- **Log full:** Administrator can receive a SMS when LOG event buffer gets at a critical full level.
- **Notify event:** Selection of administrators that will be notified if the notification event is enabled in Temporary pin access tab or Pin access tab.
- **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).
- **Automatic periodic test SMS:** Definition of Time Out for periodic SMS sending.
- **Test SMS start hour:** Periodic SMS, first send-out hour..

8.13 EVENT LOGING

EIS unit itself supports a 20000 log event entry. These log events can be pulled up to the server by clicking **Read Log** button in the “Event Log” tab. Events are listed in the table.

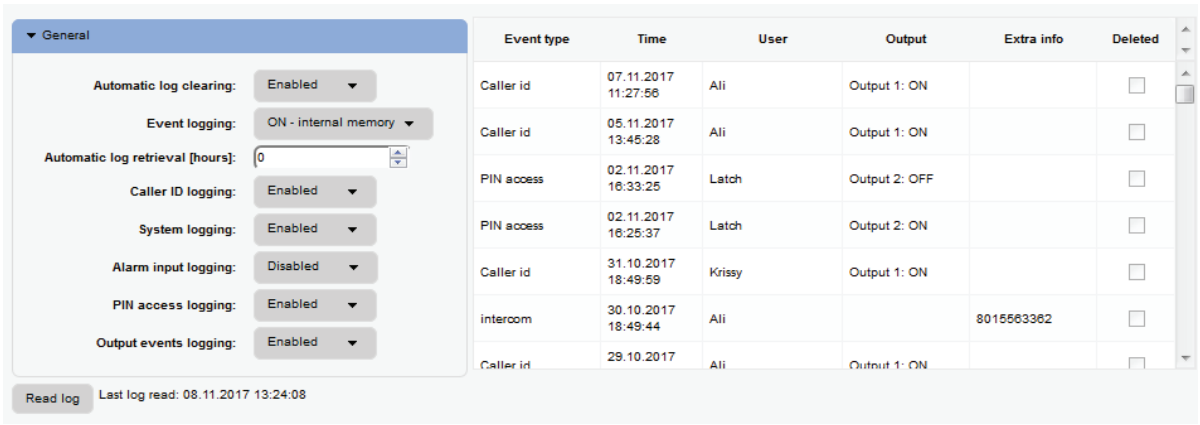

Figure 20: WEB Server-Log events.

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.

- **Automatic Log Clearing** Behavior if the internal LOG buffer on the unit is FULL of events, unit can CLEAR events or STOP recording new events.
- **Event Logging** User can select between, not logging, logging to internal memory (unit) or optional sending events over units USB connection to the external PC.
- **Automatic Log Retrieval** Definition of Time Out period for unit to upload LOG events to the WEB server.
- **Caller ID Logging** Enable/Disable logging of the Caller ID # events.
- **System logging:** Enable/Disable logging of special system evens.
- **Alarm input logging:** Enable/Disable logging for input alarm events.
- **Pin access logging:** Enable/Disable of the Pin access and Temporary pin access events.
- **Output events logging:** Enable/Disable of the events triggering the outputs (Timer,

8.14 MISCELLANEOUS

This tab is split into 2 sections.

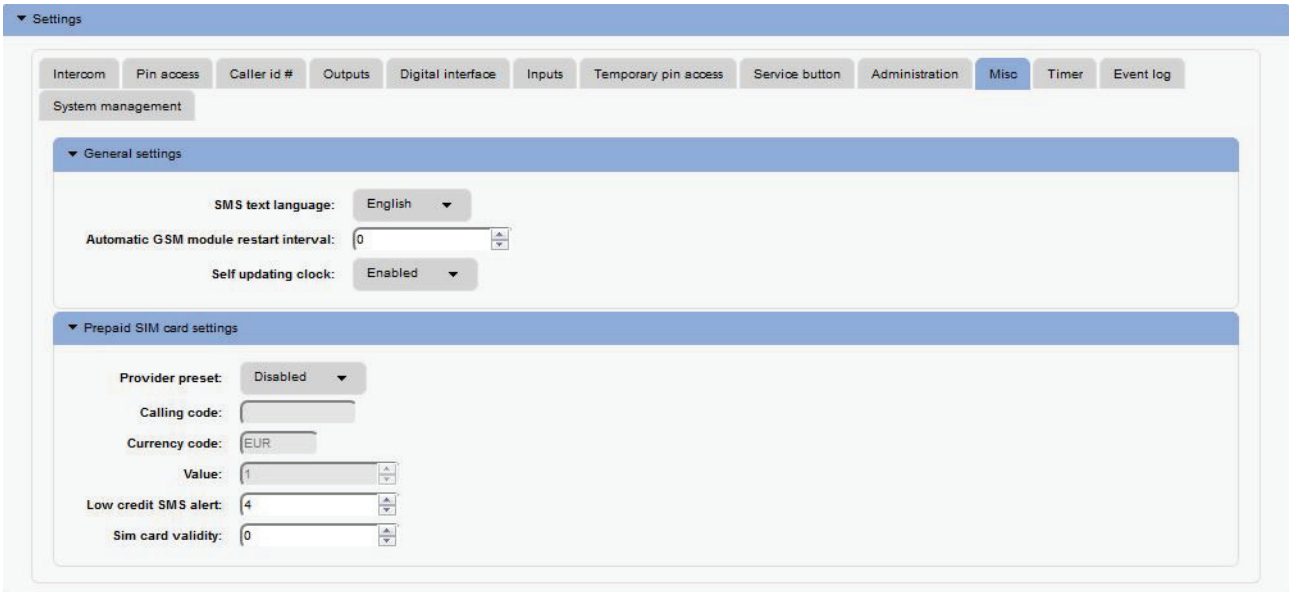

Figure 21: WEB Server-Misc.

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.**

8.15 PIN ACCESS NOTIFICATION FUNCTION

This function is used to notify administrator when a selected pin code is being used. Notification is done by SMS send to the selected administrator numbers.

Global enabling of the notification function is done in 2. Steps.
STEP 1: User has to select **Enable** option in the **Enable Pin Notification function.** STEP 2: Send the configuration to the device!!

This procedure is ONLY done 1 time when enabling this function.

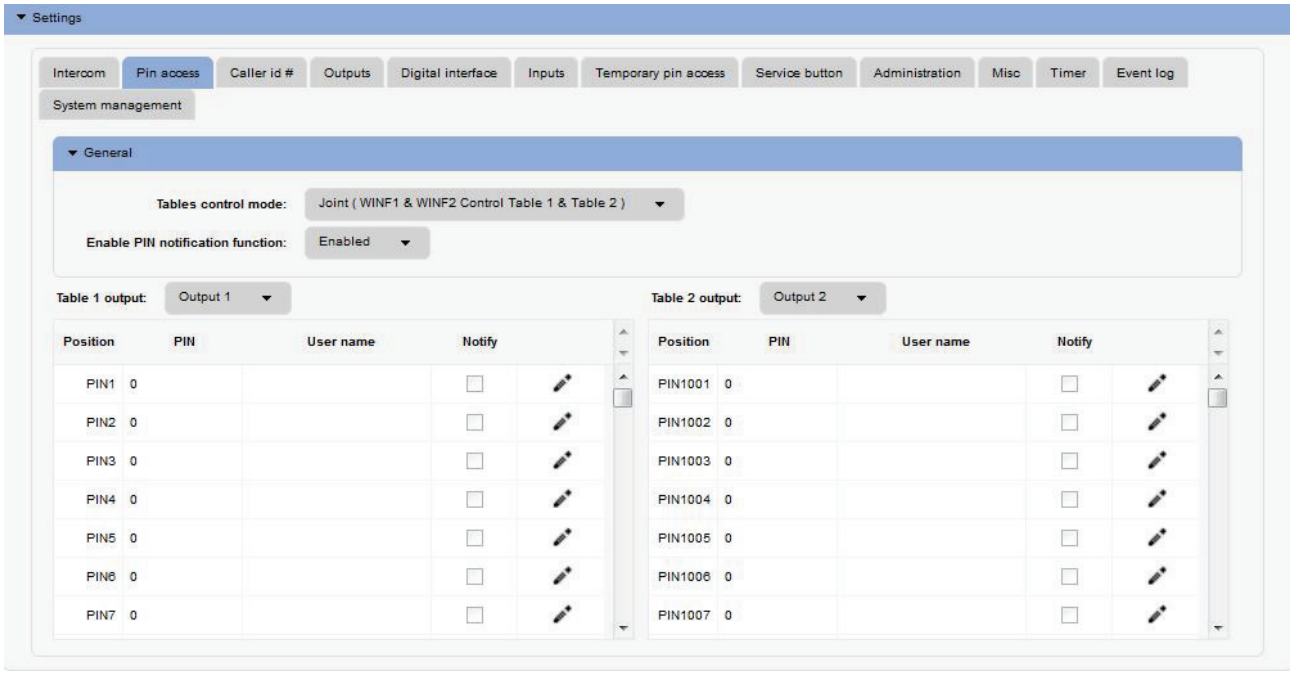

Figure 22: WEB Server-Global enabling of the notification function.

After the notification function is enabled, user can select which pin code will send the notification SMS. This is done by placing a tick in the check box of the pin code notify field.

EIS LCD

The last step is selecting a number that will be receiving the notification SMS. Selecting is done in the **Administration** tab. In the **Notify PIN** column put a tick in the check box for the appropriate phone number, multiple choices are possible.

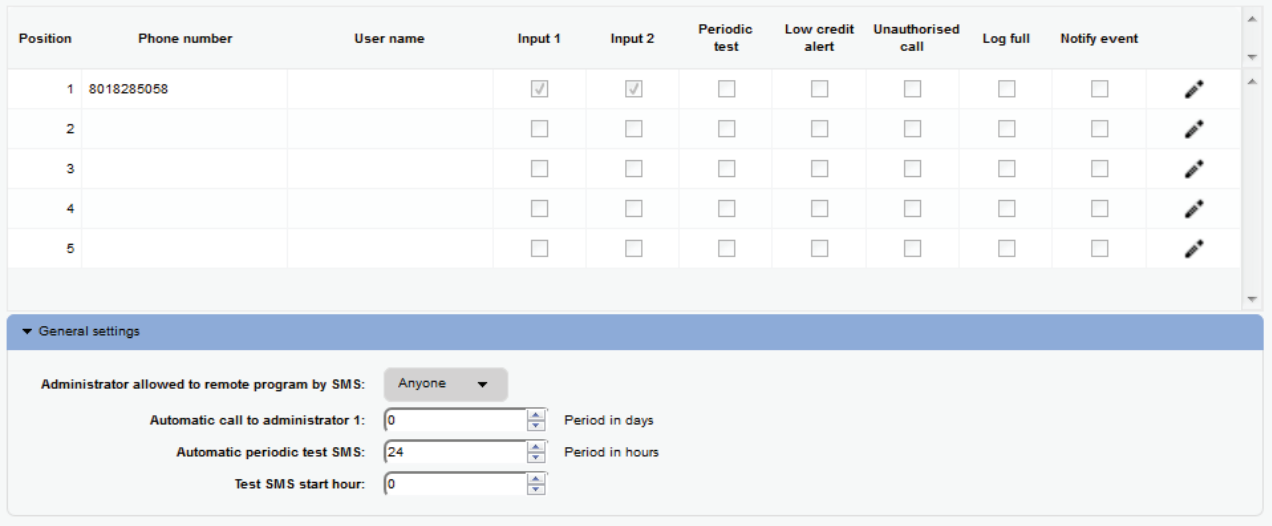

Figure 23: WEB Server-Selecting administrator numbers for notification.

9 WIEGAND INPUT DATA FORMATs

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

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

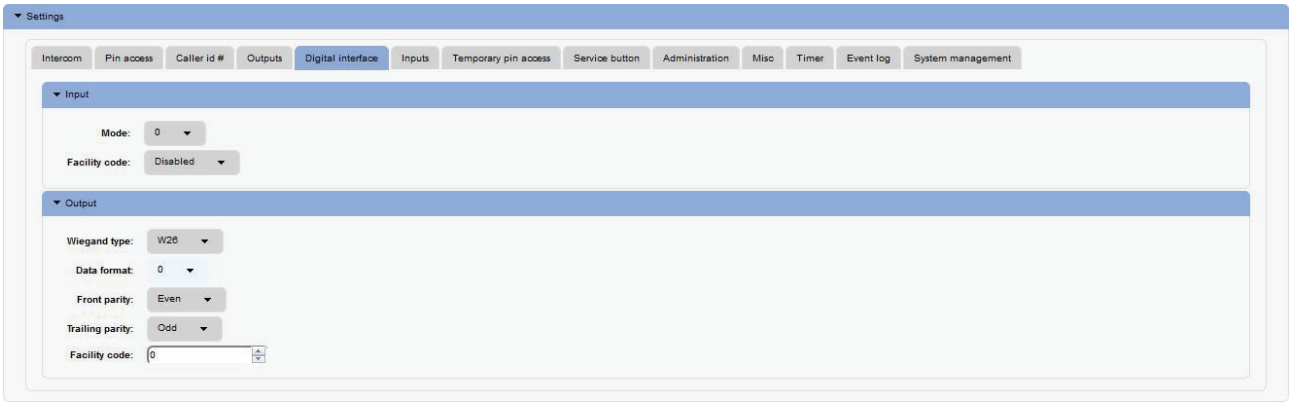

Figure 24: WEB Server-First Wiegand interface support.

Selecting the appropriate data format for SECOND Wiegand interface is done by connecting to the WEB server, selecting the **Input** tab and in **Wiegand input 2 configuration** section selecting proper **Mode** option..

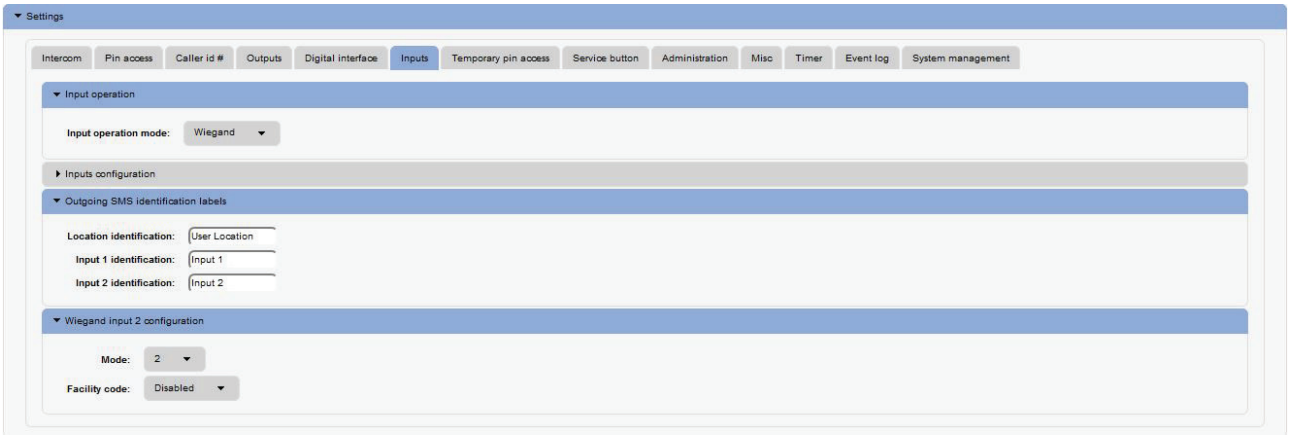

Figure 25: WEB Server-Second Wiegand interface support.

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	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	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	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	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	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	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	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.

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.