EIS4G -1 DOOR ENTRY UNIT

USER MANUAL

Transmitter Solutions®

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.

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-1, EIS-2, and EIS-4 (collectively referred to as EIS units) are compact, 4G-based intercom systems engineered to provide a cost-effective, easy-to-install, and reliable all-in-one solution for access control and communication. These systems offer wireless 4G connectivity with unlimited range, support for PIN code access, caller ID- based entry, and compatibility with Wiegand access control devices.

Optional features include alarm detection, periodic status (heart-beat) messaging and more.

3. EIS-1 FEATURES AND APPLICATIONS

Key Features

- Integrated 5-band 4G module for global network compatibility
- Supports up to 4 intercom call buttons, with 5 programmable phone numbers per button
- Keypad access control with support for up to 1,000 permanent PIN codes
- Caller ID access control for up to 1,000 authorized phone numbers
- Wiegand input interfaces
- Two programmable relay outputs for access control and automation

Programming Options

- Remote programming through the web server interface
- SMS-based programming (optional feature)

Typical Applications

- Gated Community Access: Visitors communicate with residents to request entry.
- Apartment Buildings: Enables communication between visitors and individual units for secure entry.
- Private Homes: Front door intercoms for screening guests or deliveries.
- Warehouses & Loading Bays: Facilitates quick communication between drivers and warehouse staff.
- Reception Areas: Screen visitors before granting access.
- Gated Parking Access: Visitor verification and remote gate control.

4. START UP

The EIS 1 comes with a 4G SIM card

VERY IMPORTANT	**The EIS unit comes with a 4G SIM card which must be 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 INCLUDED POWER SUPPLY. Do not use 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 15s intervals until the unit reaches normal operation.**

5. LED INDICATION

Blue LED (LED1)

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

Red LED (LED2)

- 4G GSM module Activity

Yellow LED (LED3)

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

6. CONNECTION DIAGRAM

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

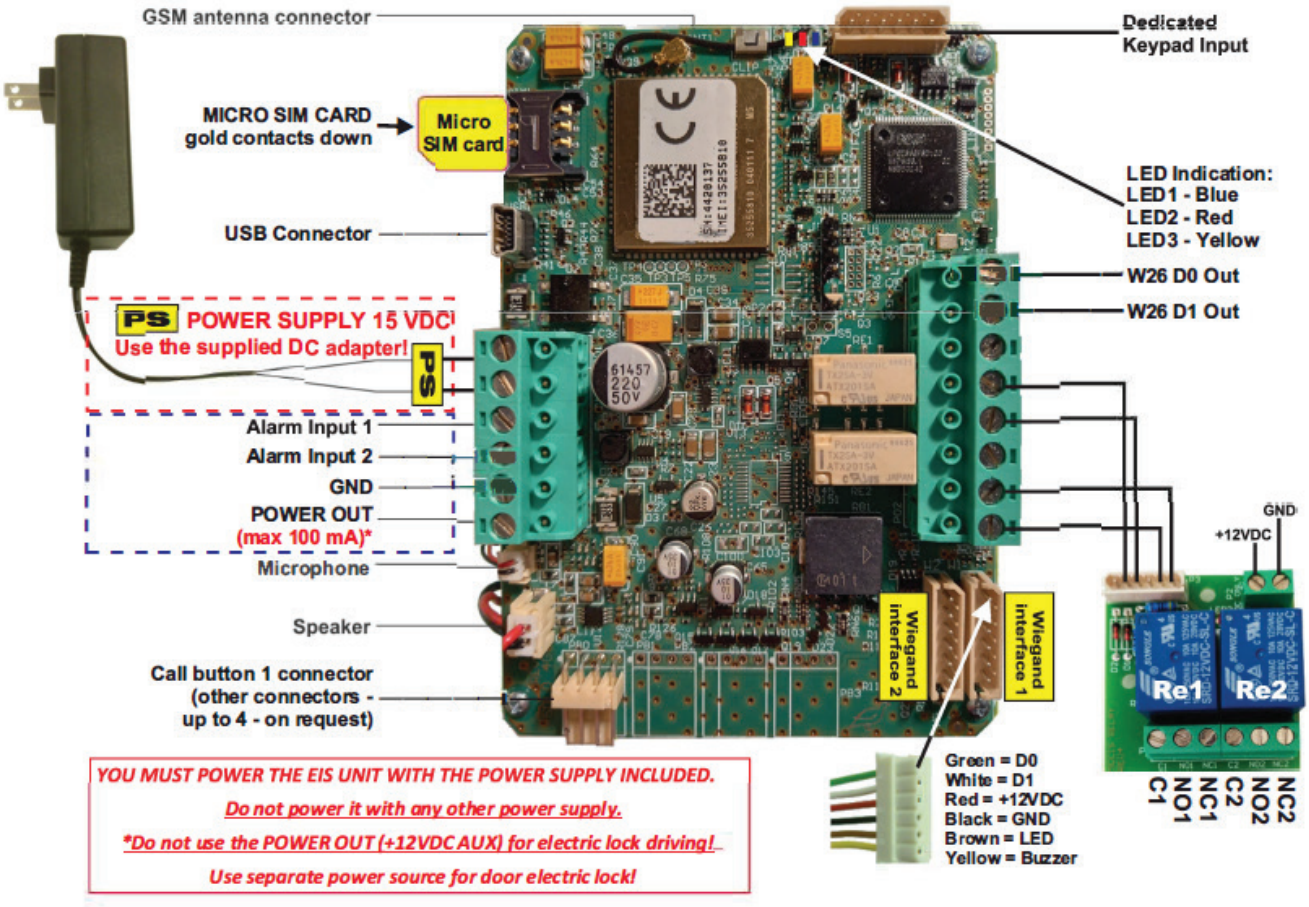


Figure 1: EIS Connection diagram

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

7. EIS MANAGEMENT

Unit supports different types of management (programming):

- 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 outlined in earlier sections, the EIS unit supports multiple programming methods. This document focuses on the most commonly used method:web-based programming via the online web server

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 support 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. To add a new unit, click the "+" icon and follow the prompts to register the device to your account.

Figure 3: WEB Server-Main page select ADD mode

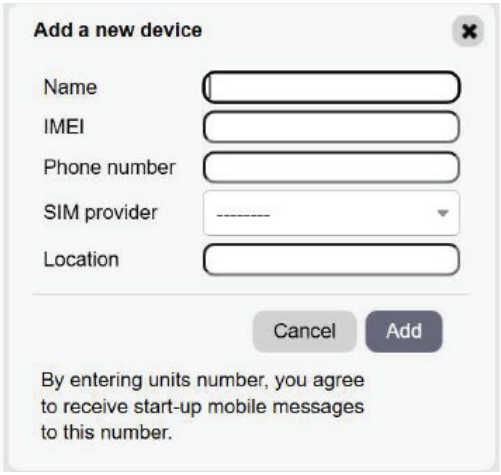


Figure 4: WEB Server-Main page adding EIS units

Mandatory 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.
- **SIM provider:** Select 4G from the dropdown list

Optional Data:

- **Location:** Notification field, can be populated by the user to provide extra data for their own information.

NOTE	**Building the unit database for the first time may take a few minutes.**

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.

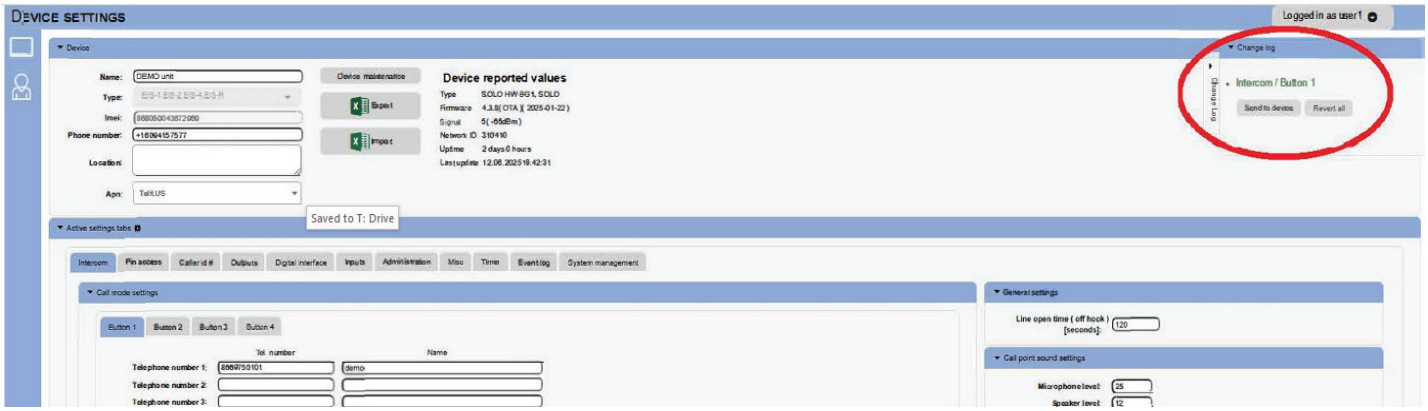


Figure 5: WEB Server-Unit management window

8.4 INTERCOM CONFIGURATION

The primary function of the EIS 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 stop calling the remaining numbers in the sequence.

Intercom settings and configuration can be managed via the **Intercom** tab in the web interface.

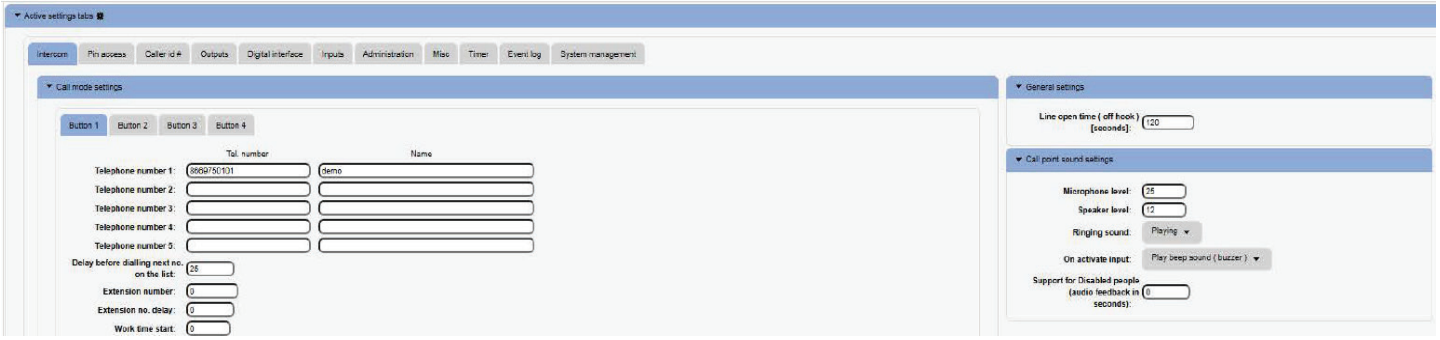


Figure 6: WEB Server-Intercom settings.

Intercom management parameters:

- **Telephone Number 1 to 5:** Defines the sequence of phone numbers the unit will call when a call button is pressed.
- **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.

NOTE	**EIS-1 has 1 CALL button.**

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

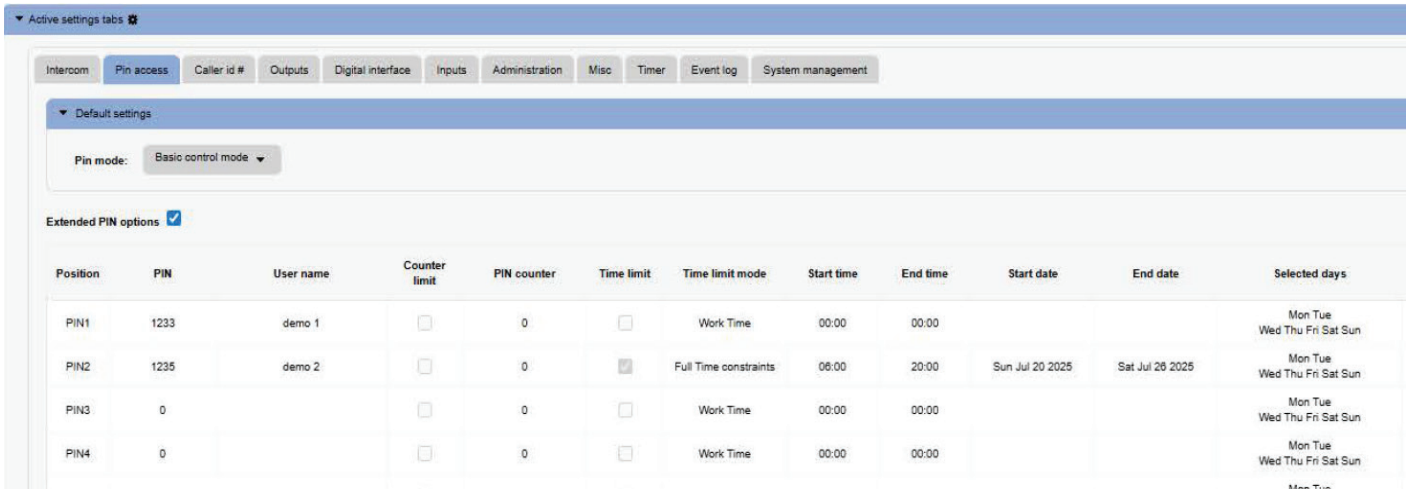


Figure 7: Web Server - PIN Access configuration

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.

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.

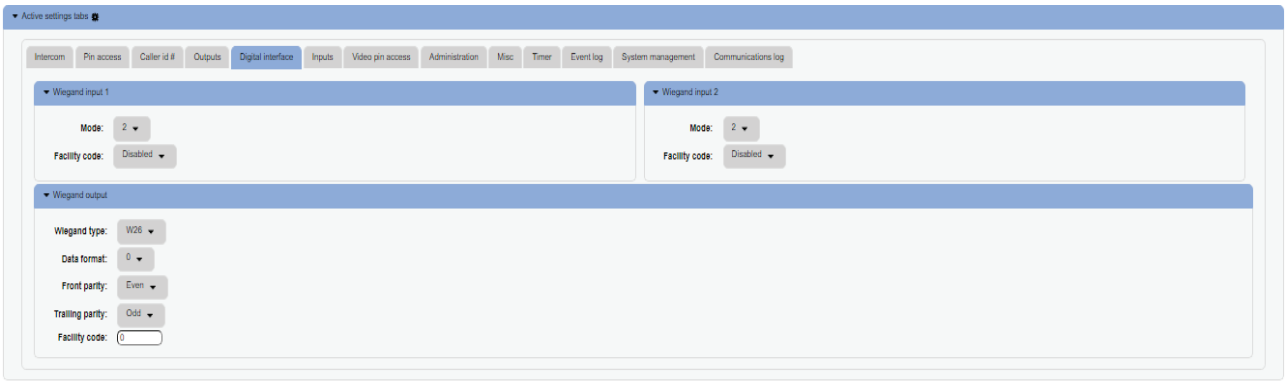


Figure 8: WEB Server-Wiegand interface support.

Wiegand Inputs (Input 1 and Input 2

- **Mode:** Select the appropriate Wiegand data format. Mode 2 is commonly used. For specific format details, consult your device provider.
- **Facility Code:** Option to enable or disable the use of a facility code in the input data.

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 INPUT DATA FORMATs for detailed explanation of different data 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.

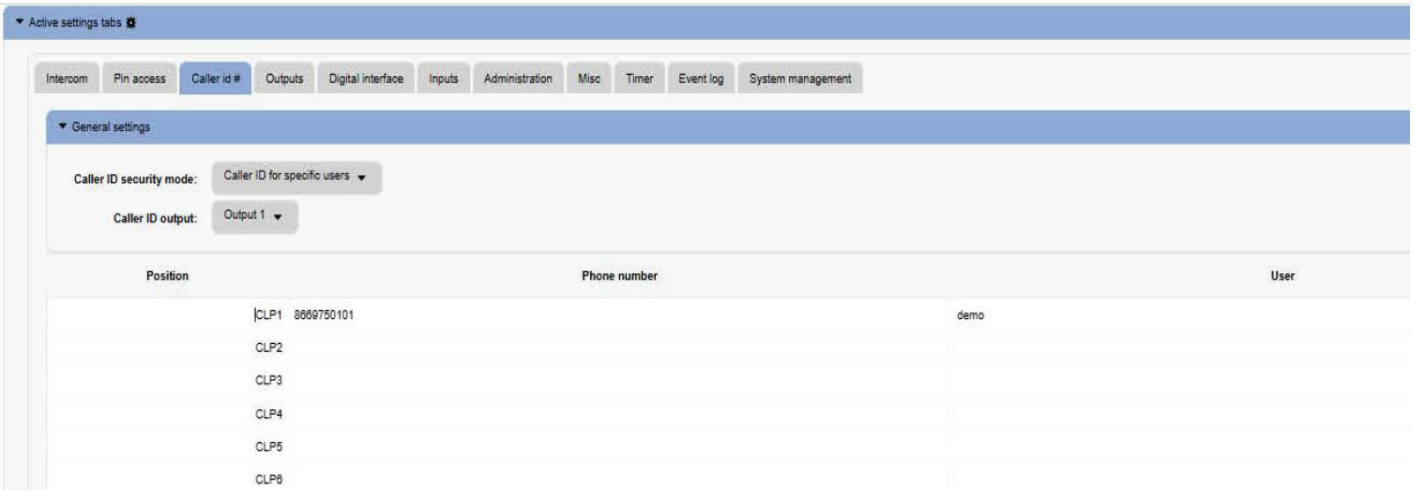


Figure 9: WEB Server-Caller ID Access

General Settings:

- **Caller ID Security Mode:** Defines how the system handles incoming calls for access control.
  The user can select from three modes:
  Caller ID Disabled – Deactivates the Caller ID function; no numbers are permitted.
  Caller ID for Specific Users – Only phone numbers listed in the system are allowed to trigger outputs.
  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

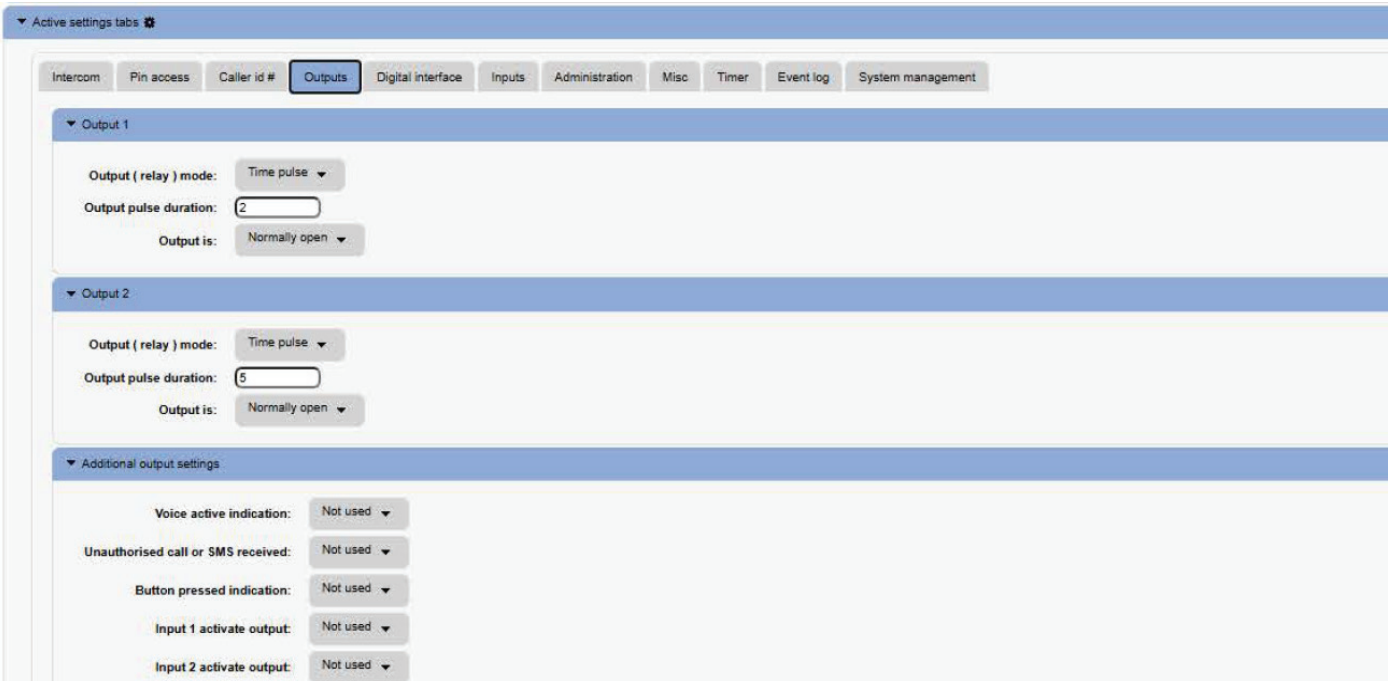


Figure 10: WEB Server-Output setting

Output 1- Settings for output 1:

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

- **Voice active indication:** Activates the assigned output when a voice connection (intercom call) is established.
- **Unauthorized call or SMS received:** Activates the assigned output when an unauthorized call or SMS is received by the unit.
- **Button pressed indication:** Activates the assigned output when the intercom call button is pressed.
- **Input 1 activate output:** An alarm event detected on Input 1 will activate the assigned output.
- **Input 2 activate output:** An alarm event detected on Input 2 will activate the assigned output.

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

The EIS unit is equipped with two independent timers that can be used to control the outputs of the device automatically, based on a predefined schedule.

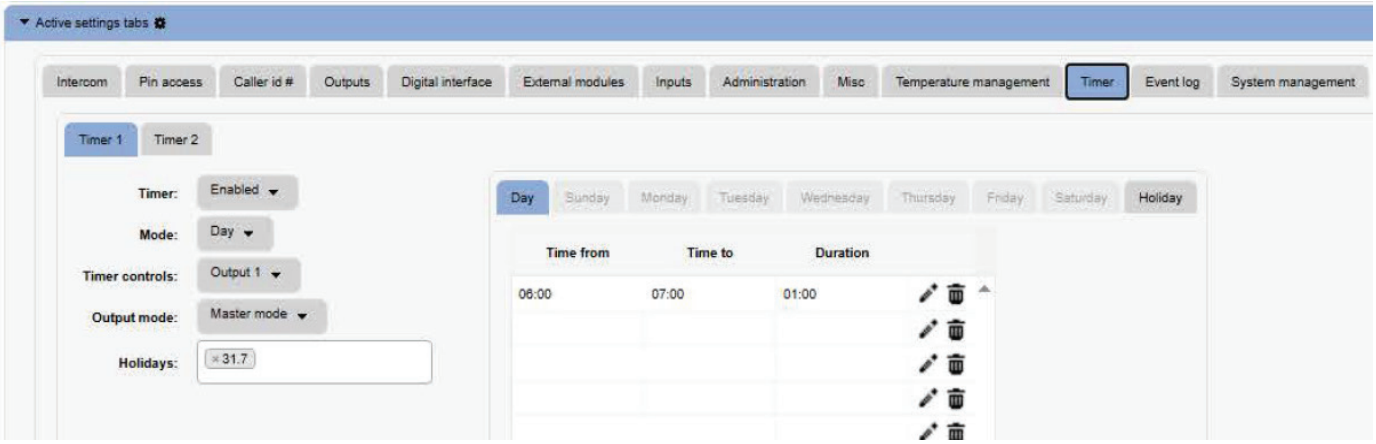


Figure 11: WEB Server-Timer setting →Day mode.

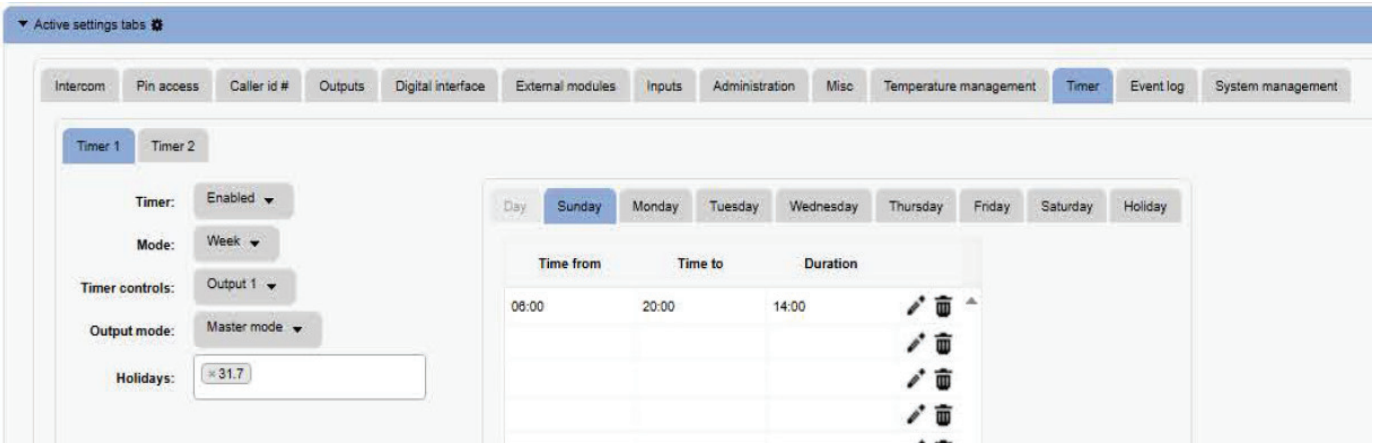


Figure 12: WEB Server-Timer setting →Week mode.

Timer settings:

- **Timer:** The parameter allows the user to enable or disable the timer function
- **Mode:** The user can select between Day Mode or Week Mode for the timer operation. In Day Mode, the timer operates based on a single day schedule (day table), which applies to all days of the week.
  In Week Mode, the user can configure a separate schedule for each individual day of the week, allowing different settings for every day.
- **Timer controls:** Output controlled by the timer function.
- **Output mode:** Output mode management definition.
- When the output is controlled by the timer (i.e., activated by the timer), it operates in Latching Mode regardless of the mode configured in the Output tab.
- When the timer is not active, the output operates according to the settings defined in the Output tab.

OUTPUT mode options	Description
Slave mode	The behavior of the outputs (Time Pulse or Latching Mode) is configured in the Output tab.
Master mode:	When the output is controlled by the timer (i.e., activated by the timer), it operates in Latching Mode regardless of the mode configured in the Output tab. When the timer is not active, the output operates according to the settings defined in the Output tab.
Output precondition:	In this mode, the Timer is used as a precondition for output control. This means the output can only be activated by other functions — such as PIN access or Caller ID — if the Timer condition is active..

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

- **Holidays:** Use the Day Picker to define holiday dates and set custom output behavior for holidays.

NOTE	The settings described are the same for both timers.

8.10 ADMINISTRATION

The Administration tab allows the user to enable advanced settings, such as: Notification of unauthorized access, Sending periodic test messages, Lockdown of the unit and other security or monitoring features.

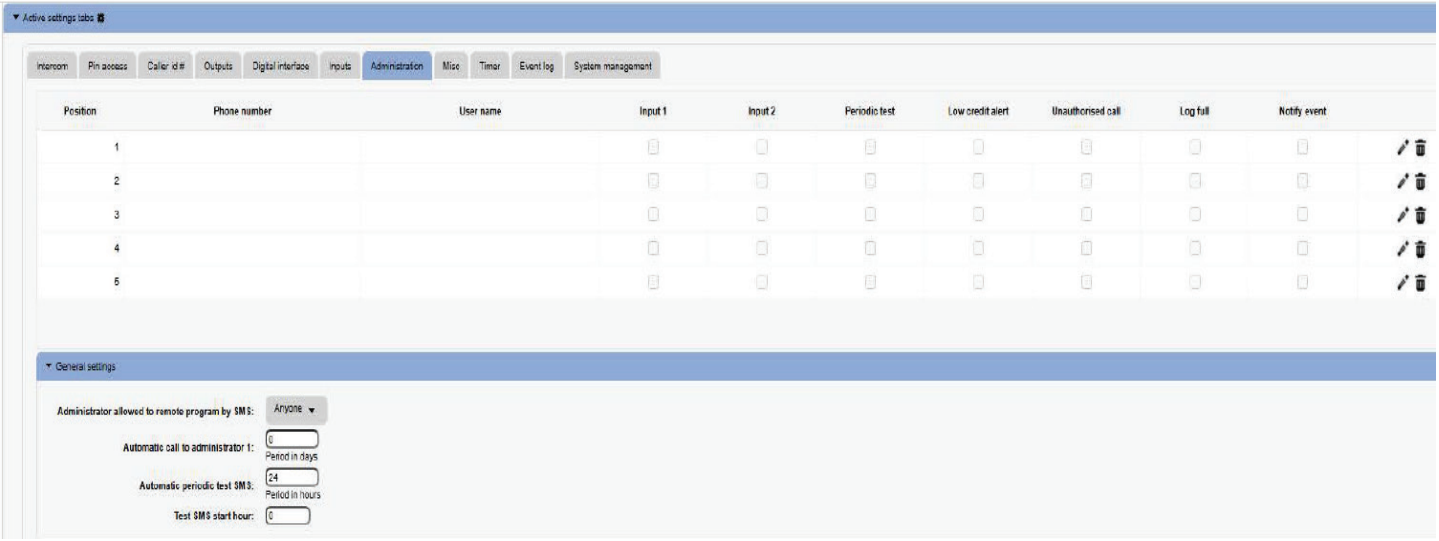
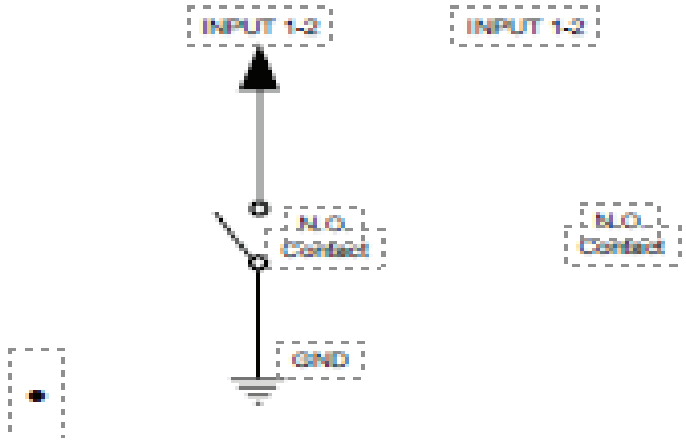


Figure 13: WEB Server-Notification numbers

- **Phone number, User name:** Specifies the phone number and user name of the user designated to receive notification messages.
- **Input1, Input2:** When an alarm condition is met, users with the checkbox selected will receive an alarm notification via SMS.

Figure 14: WEB Server-Input alarm configuration.



- **Periodic test:** To send periodic (heart-beat) SMS messages to a user, enable the checkbox next to the corresponding user. The sending interval is defined in hours under the parameter Automatic Periodic Test SMS
- **Unauthorized call:** In case of an unauthorized call, the unit can notify the user via SMS. To enable this notification, click the checkbox next to the corresponding user number.
- **Log full:** The administrator can receive an SMS notification when the event log buffer reaches a critical level of fullness.
- **Notify event:** Defines which administrators will be notified via SMS if the notification event is enabled in the PIN Access tab..
- **Administration allowed to remote program by SMS:** By selecting this option, the user can lock down the EIS unit, preventing any unauthorized user from making configuration changes to the device.
- **Automatic call to administrator 1:** To avoid the SIM card being locked by the provider due to inactivity, the unit can make a periodic outgoing call to the phone number set in position 1. The interval is configurable in days. This setting is optional and can be left unset if not required.
- **Automatic periodic test SMS:** Defines the time interval (timeout) for sending periodic SMS messages.
- **Test SMS start hour:** Defines the first hour when the periodic SMS message will be sent.

8.11 EVENT LOGING

The EIS unit supports storage of up to 20,000 log event entries. These log events can be retrieved and uploaded to the server by clicking the Read Log button located in the Event Log tab. Once retrieved, the events will be displayed in a table for review.

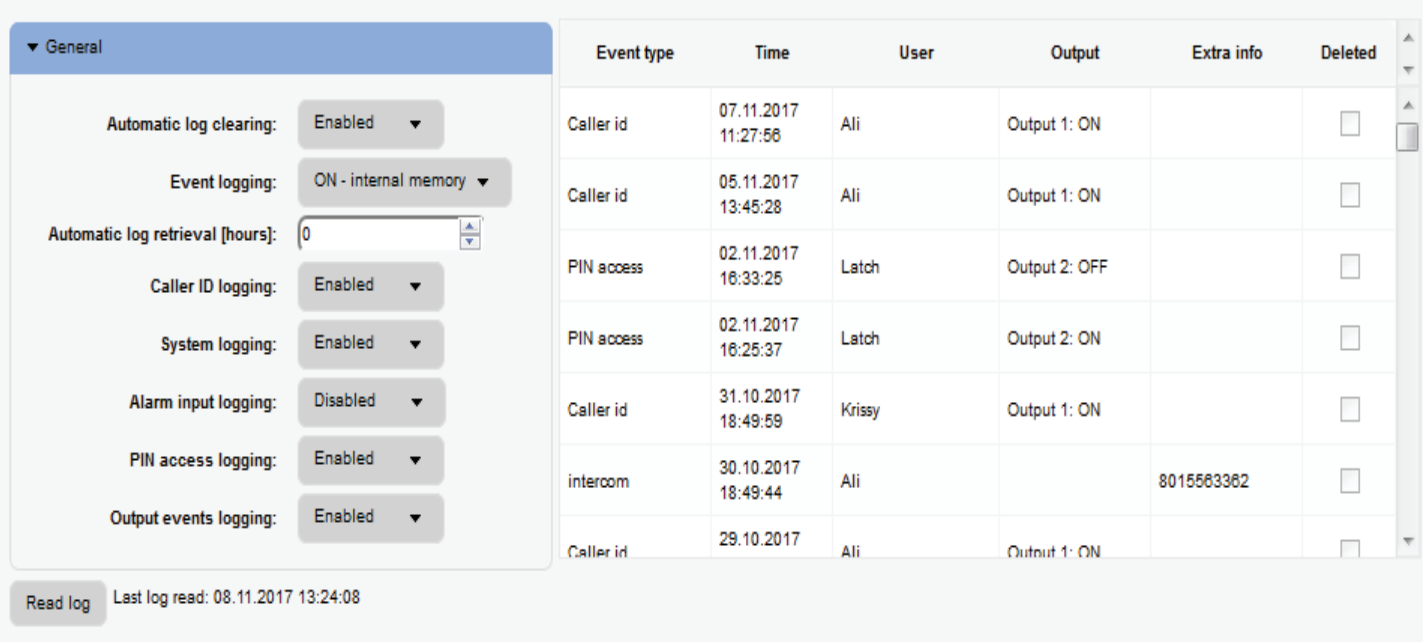


Figure 15: WEB Server-Log events.

Every event entry contains information about the event type, time of occurrence, triggered output (if any), and the user responsible for the event. If user identification is available (such as Caller ID, PIN code, or Intercom user), the user name will be displayed in the User column.

- **Automatic Log Clearing** Defines the behavior of the unit when the internal log buffer is full. The user can choose to either Clear old events automatically or Stop recording new events when the buffer limit is reached.
- **Event Logging** Specifies where event logs are stored. The user selects one of the following options: No Logging – Events will not be recorded.
  Logging to Internal Memory – Events are stored in the unit's internal memory.
  Logging via USB – Events are sent in real-time over the unit's USB connection to an external PC.
- **Automatic Log Retrieval** Defines the time interval (timeout period) for automatic uploading of log events from the unit to the web server

EIS-1

- **Caller ID Logging** Enable or disable the logging of events generated by Caller ID numbers.
- **System logging:** Enable or disable the logging of special system events (e.g., unit startup, configuration changes, errors).
- **Alarm input logging:** Enable or disable the logging of alarm events generated by the input lines.
- **Pin access logging:** Enable or disable the logging of both permanent and temporary PIN access events.
- **Output events logging:** Enable or disable the logging of output-triggering events (e.g., Timer activation, Intercom call, etc.).

NOTE	After event data is retrieved and saved to the server, the unit automatically deletes the local copy of the event log.

8.14 MISCELLANEOUS

This tab is split into 2 sections.

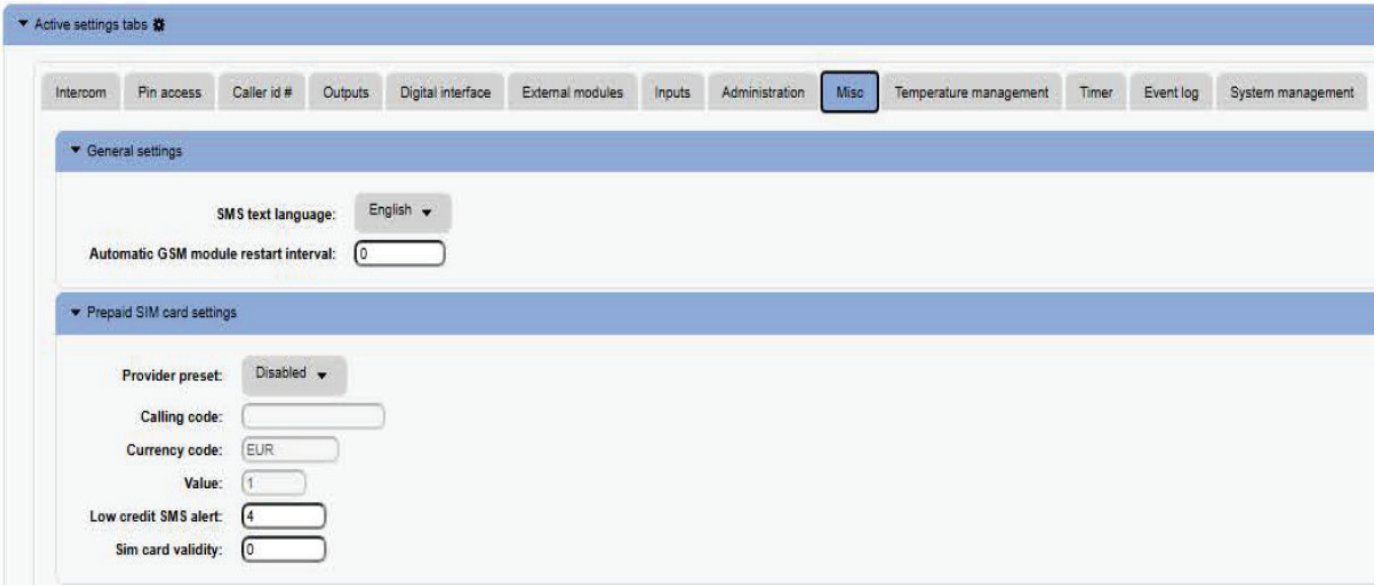


Figure 16: WEB Server-Misc

General settings:

The following parameters can be configured under General Settings:.

- **SMS text Language:** Defines the language used for all outgoing SMS messages. The user can select the preferred language from the drop-down men
- **Automatic GSM module restart interval:** Allows the user to set an automatic restart interval (in hours) for the GSM module, if necessary.
- **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.

Note: It is recommended to use this parameter only if specifically advised.

9 WIEGAND INTERFACE DATA FORMATS

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..