EIS 4G MS-2025

Caller ID and Wiegand access control device

USER MANUAL

Transmitter SOLUTIONS®

CONTENTS

Contacts

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

Figures

Tables

1. FOR YOUR SAFETY

SWITCH ON SAFELY

Do not switch the unit on where use of wireless phone is prohibited or where 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 required 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 near 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 location as explained in the product documentation. Do not touch the antenna unnecessarily.

2. INTRODUCTION

EIS-MS is a compact, 4G-based access system designed to deliver a cost-effective, easy-to-install, and reliable all-in-one solution for access control.

These systems offer wireless GSM connectivity within cell coverage range and support multiple access methods, including PIN/Wiegand codes and caller ID-based entry. They are also compatible with Wiegand access control devices.

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

3. EIS-MS 4G FEATURES AND APPLICATIONS

Key Features

- Integrated 5-band GSM module for global network compatibility
- Access control with support for up to 1,000 PIN or Wiegand codes
- Caller ID access control for up to 500 authorized phone numbers
- Wiegand input interface
- Programmable relay output for access control and automation

Programming Options

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

Typical Applications

- Automated Gate Access – For residential, commercial, or community gates (e.g., apartment complexes or gated communities).
- Garage Door Control – Allowing homeowners to open/close garage doors remotely.
- Parking Barriers – Granting access to authorized vehicles in parking lots or garages.
- Remote Equipment Control – Powering on/off industrial machines, irrigation systems, or HVAC units.
- Storage Units – Managing access to individual storage lockers or storage facilities.
- Construction Sites – Temporary access control for workers or contractors on site

4. START UP

EIS-MS unit accepts a standard GSM SIM card provided with the Unit.

VERY IMPORTANT	**Use ONLY the Micro SIM card provided with the EIS-MS. No other Slm cards are supported** 
WARNING	**DO NOT insert or remove the SIM card while the unit is powered ON!!**
VERY IMPORTANT	**Connect power cable to EIS unit. YOU MUST POWER THE EIS UNIT WITH THE POWER SUPPLY INCLUDED! No other power supply can be used !**

- Power up the unit.
- Wait until LED1 (Green) starts flashing. This takes about 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 will flash with short pulse (0.5 sec.) ON and a long pulse (5 sec.) OFF .

6. CONNECTION DIAGRAM

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

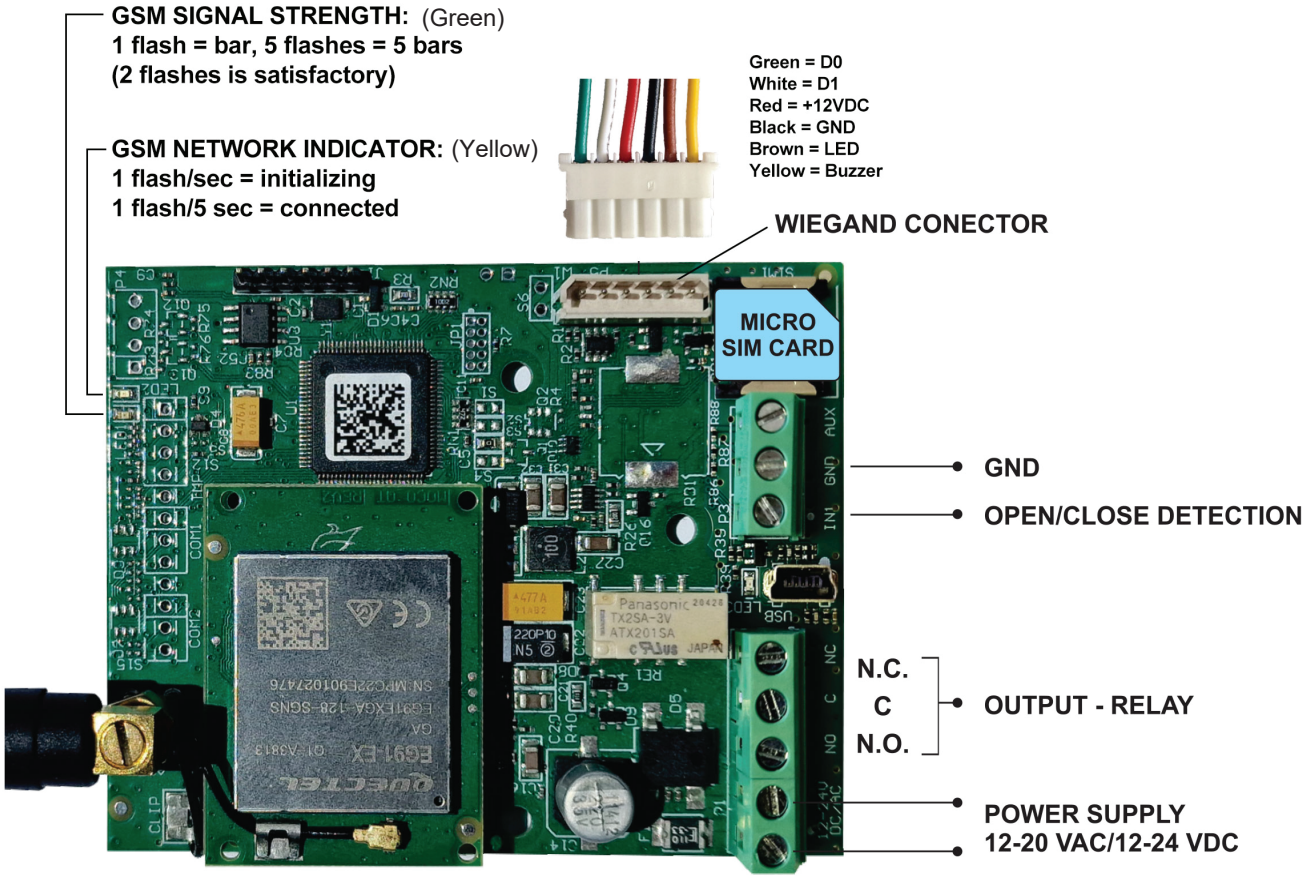


Figure 1: EIS-MS: Connection diagram

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

7. EIS-MS UNIT MANAGEMENT

This unit supports 3 different types of remote management (programming) as shown below:

- Web server access.
- Android or iOs apps.
- SMS commands (Optional).

8. EIS FUNCTIONS with PROGRAMMING INSTRUCTIONS

As outlined in the previous section, the EIS-MS unit supports multiple programming methods. This document focuses on the most commonly used method: web-based programming via the online browser interface.

IMPORTANT	**SIM card in the EIS-MS unit MUST have a DATA PLAN to be able to use 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

8.1 WEB SERVER - LOG IN - cont'd

Users can 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 one of these social media accounts, they can create a profile using a standard username and password.

NOTE	**Server supports the following browsers:** 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 (circled below) and follow the prompts to register a new device to your account as shown in Figure 4 below.

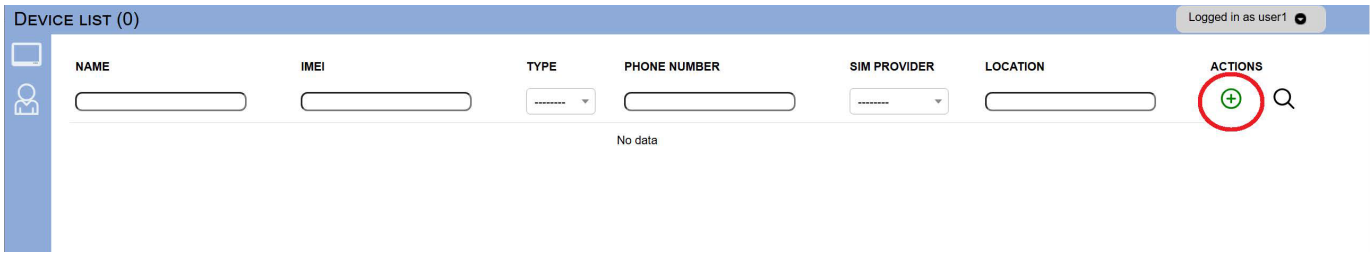


Figure 3: Web Server-Main page select ADD mode

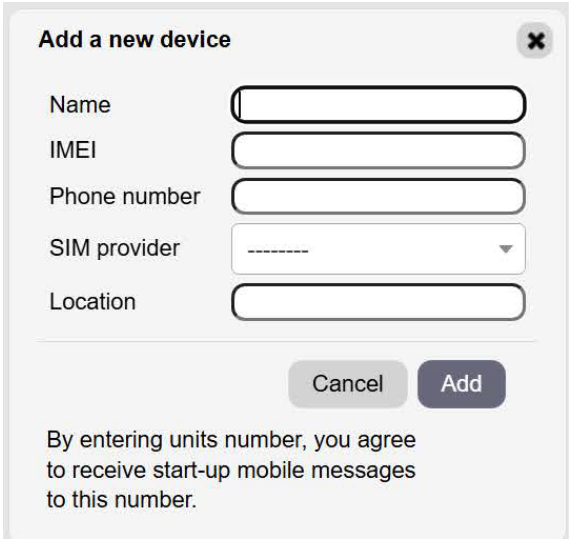


Figure 4: Web Server-Main page adding EIS units

8.2 WEB SERVER - ADDING UNITS TO USER PROFILE cont'd

User then provides required information:

RequiredInformation:

- **Name:** Name for the newly added unit.
- **IMEI:** Identification number of the unit. It can be found inside the enclosure of the unit. The IMEI is also located on the cellular chip and should be on the box containing the EIS unit.
- **Phone Number:** The telephone number of the SIM card in the EIS unit
- **SIM provider:** Information needed to enable data connection between the server and the unit. Selectable from the drop-down menu.

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.

8.3 WEB SERVER - UNIT MANAGEMENT

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

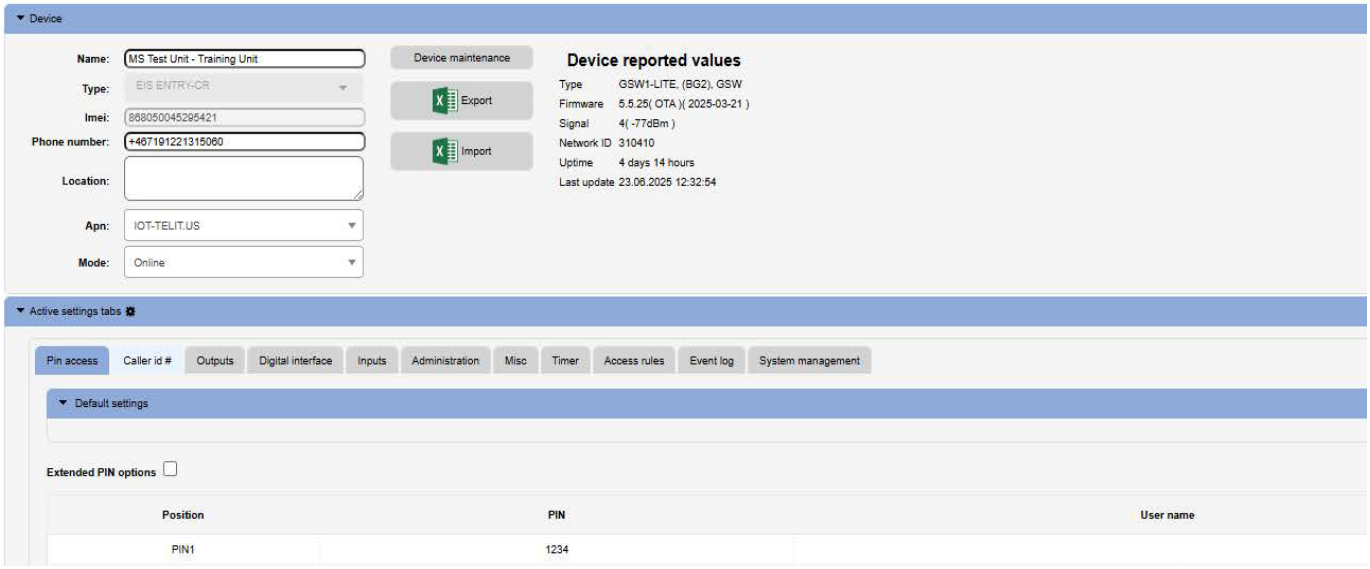


Figure 5: Web Server-Unit management window

IMPORTANT	**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.**

8.4 PIN/WIEGAND NUMBER ACCESS

External Wiegand devices enable secure access using PIN/Wiegand #, etc. 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.

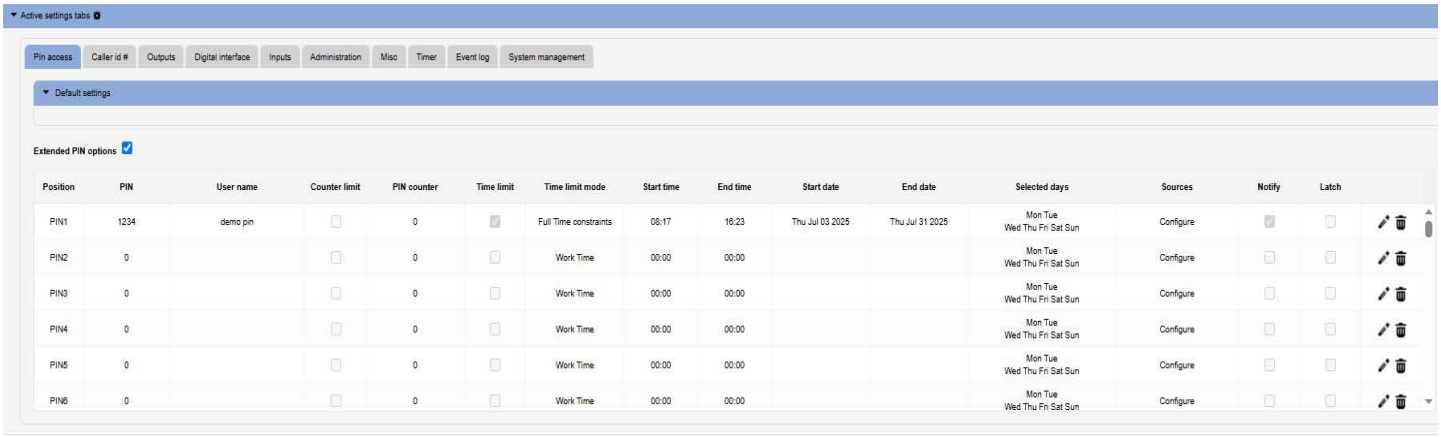


Figure 6: Web Server - PIN Access configuration

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 Zones	- *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 on which 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.

8.5 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.

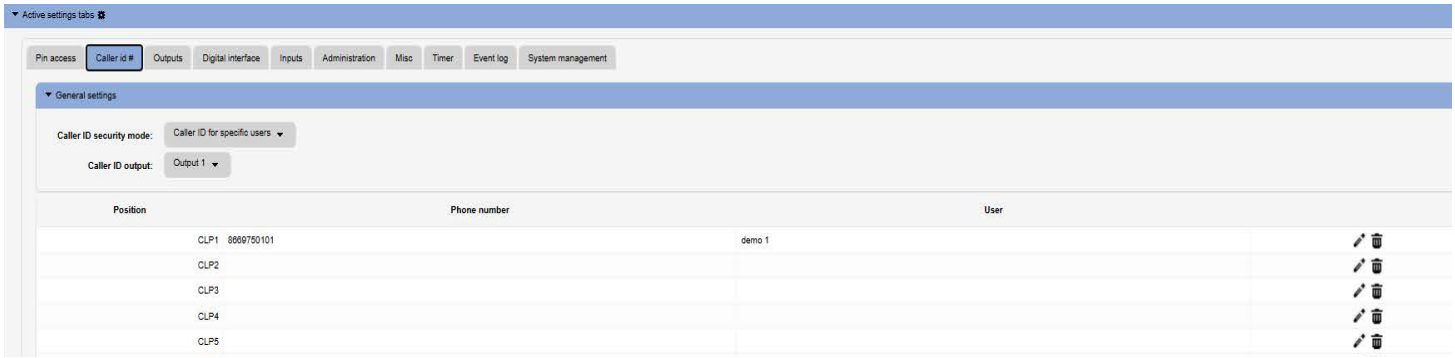


Figure 7: Web Server-Caller ID Access

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. Call to open feature is disabled
- ***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.*

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

- **Caller ID Output:** Specifies which output 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.

8.6 OUTPUTS SETTINGS

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

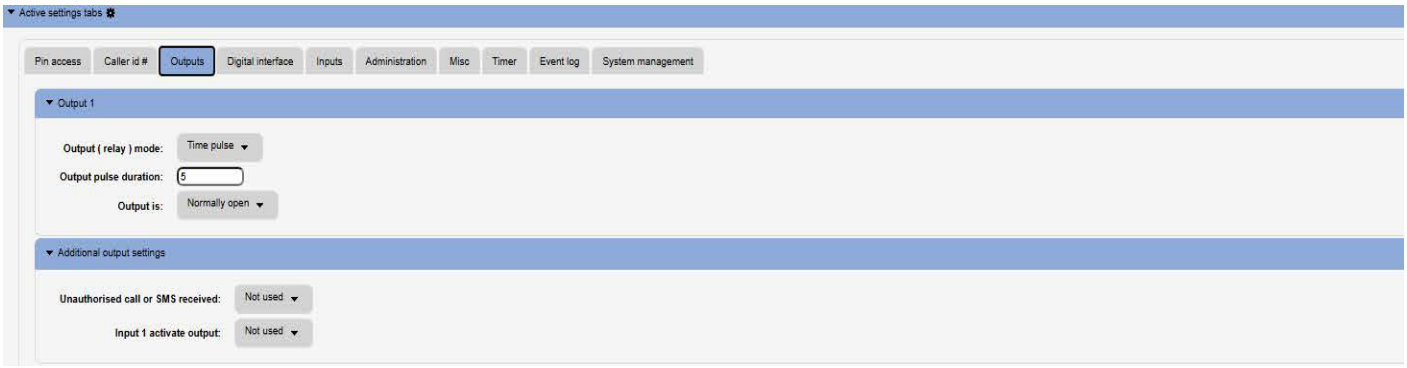


Figure 8: Web Server-Output setting

Output 1 - Settings:

- **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 - Used to link onboard actions with the outputs if needed:

- **Unauthorized call or SMS received** Activates the assigned output when an unauthorized call or SMS is received by the unit.
- **Input 1 activate output:** An alarm event detected on Input 1 will activate the assigned output.

NOTE	Due to functional limitation of these output settings, use additional outputs settings with care.

8.7 TIMER-TIMED CONTROLLED OUTPUT

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

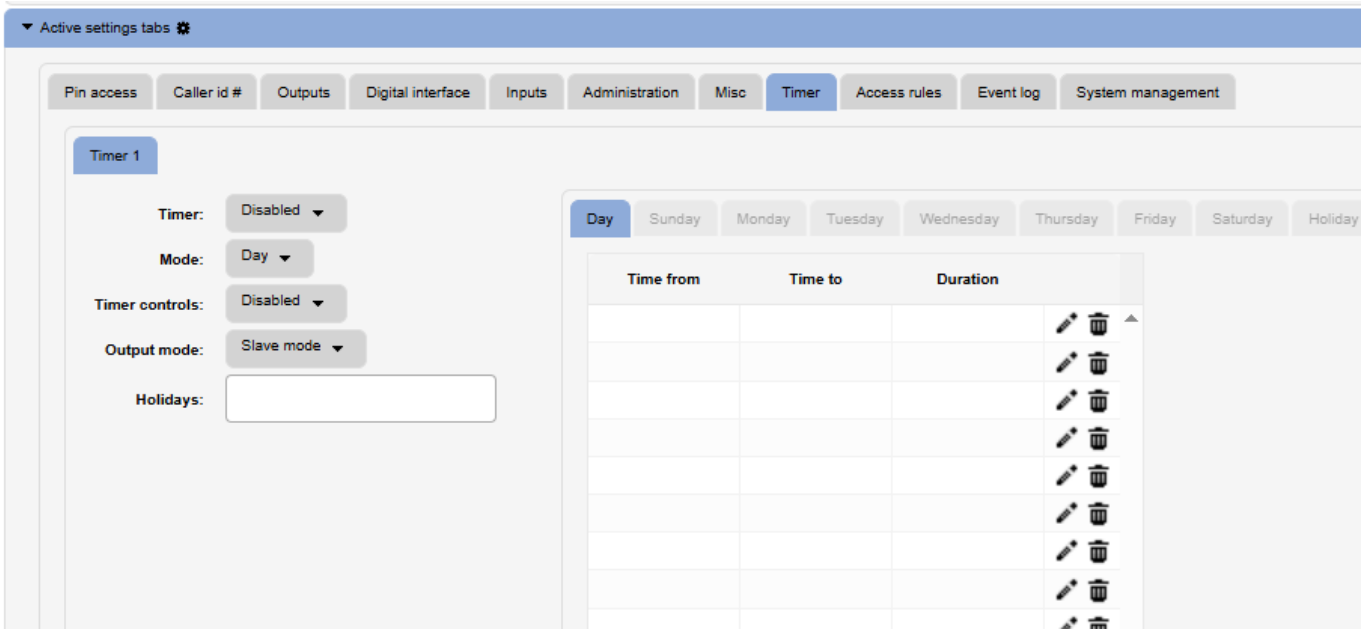


Figure 9: Web Server-Timer setting →Day mode.

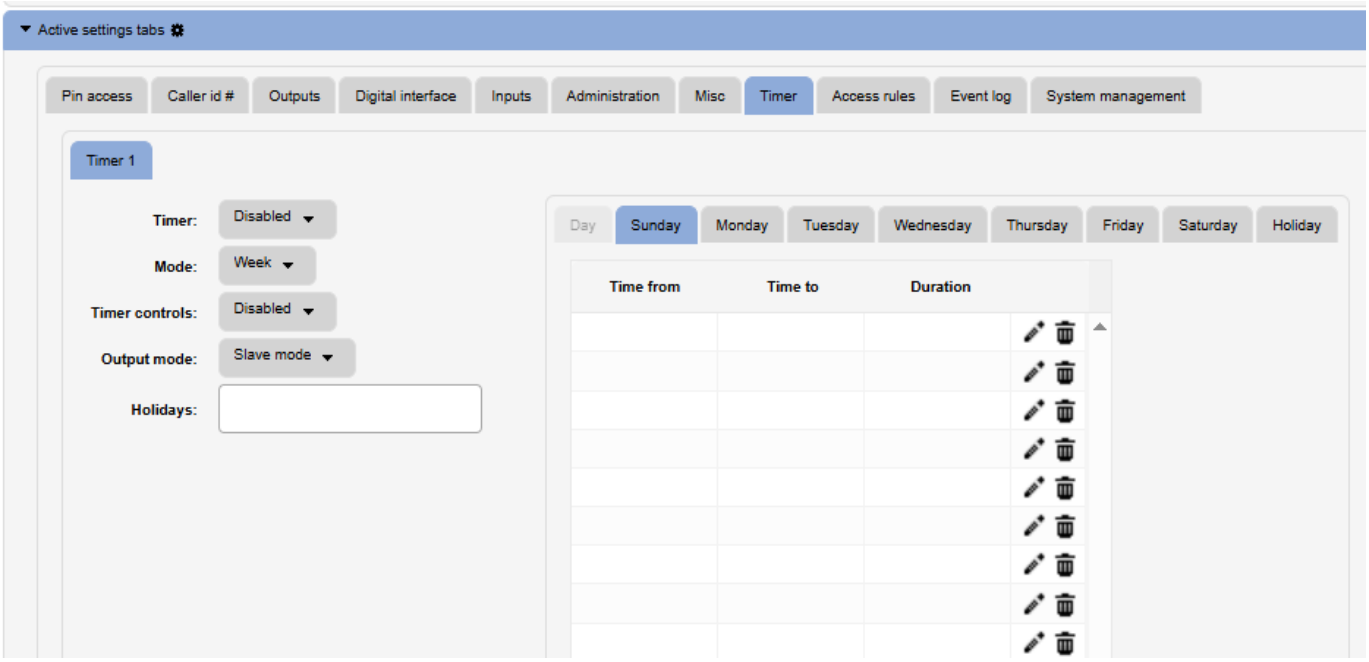


Figure 10: Web Server-Timer setting → Week mode.

8.7 TIMER - TIME CONTROLLED OUTPUT cont'd

Timer settings:

- **Timer:** The parameter allows the user to enable or disable the timer function as required
- **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.

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 functions as a precondition for output activation. This means the output can only be triggered by other access methods—such as PIN entry or Caller ID—if the Timer condition is currently active.

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

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

8.8 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.

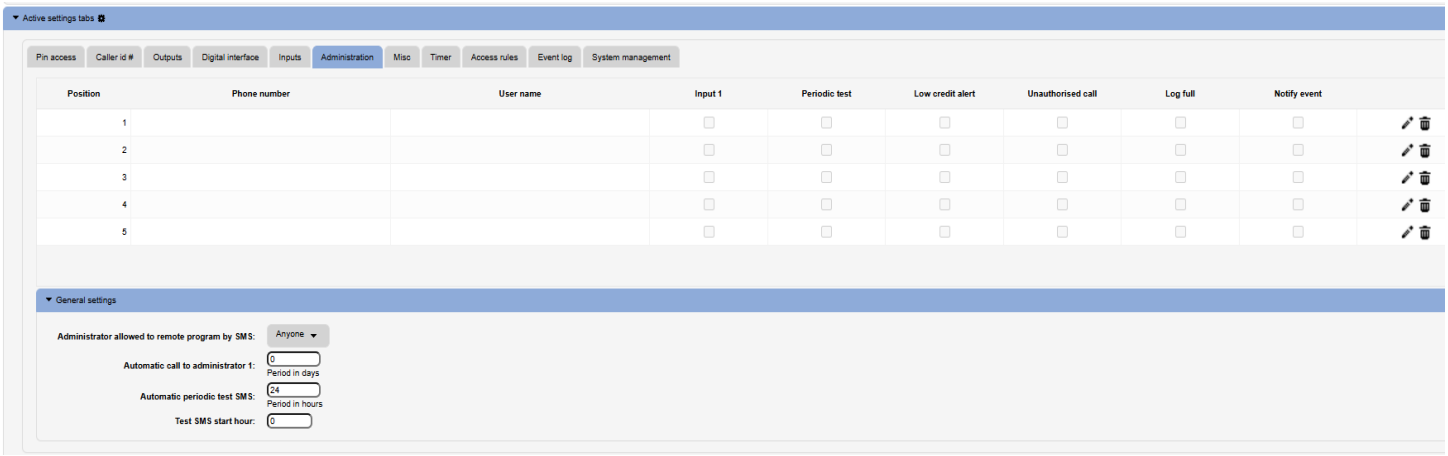
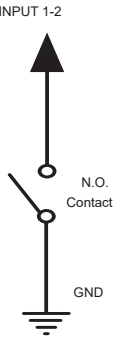


Figure 11: Web Server-Notification numbers

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

Figure 12: 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.**

8.8 ADMINISTRATION cont'd

- **Unauthorized call:** In case of an unauthorized call, the unit can notify the user via SMS. To enable this notification, tick the checkbox next to the corresponding user name.
- **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.

8.9 EVENT LOGGING

The event log is a record of events related to how the EIS unit is being used such as times and dates that users enter or exit a property. The EIS MS unit supports storage of up to 20,000 log event entries.

These logged 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.

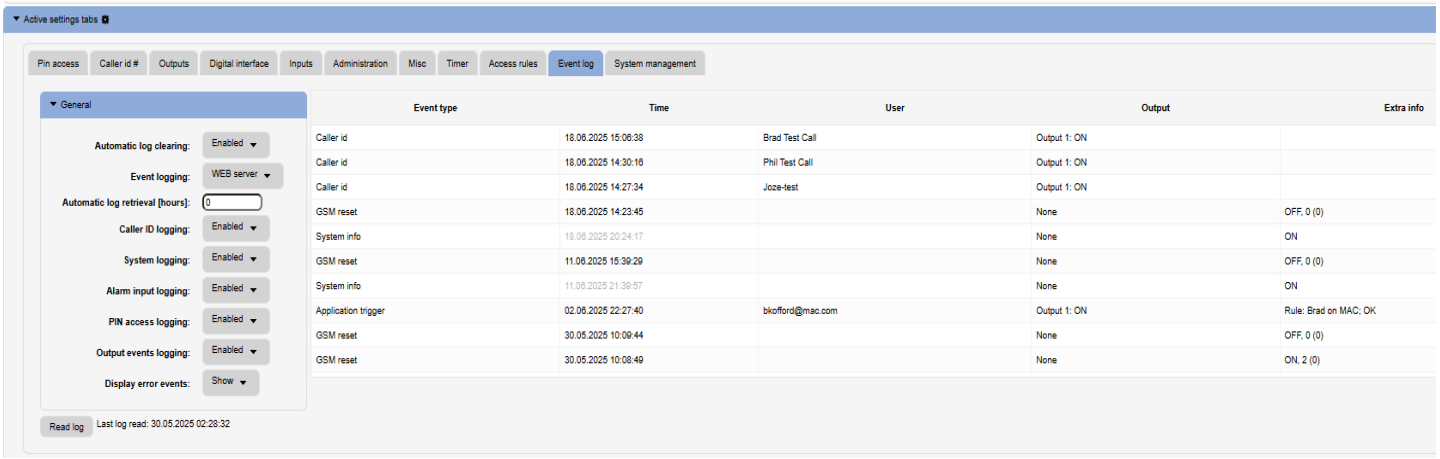


Figure 13: Web Server-Event Log

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.

8.9 EVENT LOGGING cont'd

- **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 will be stored. The user can select one of three following options:

  1- *No Logging* – Events will not be recorded.
  2- *Logging to Internal Memory* – Events are stored in the unit's internal memory.
  3- *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.

- **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.).

8.10 MISCELLANEOUS

This tab is split into 2 sections.

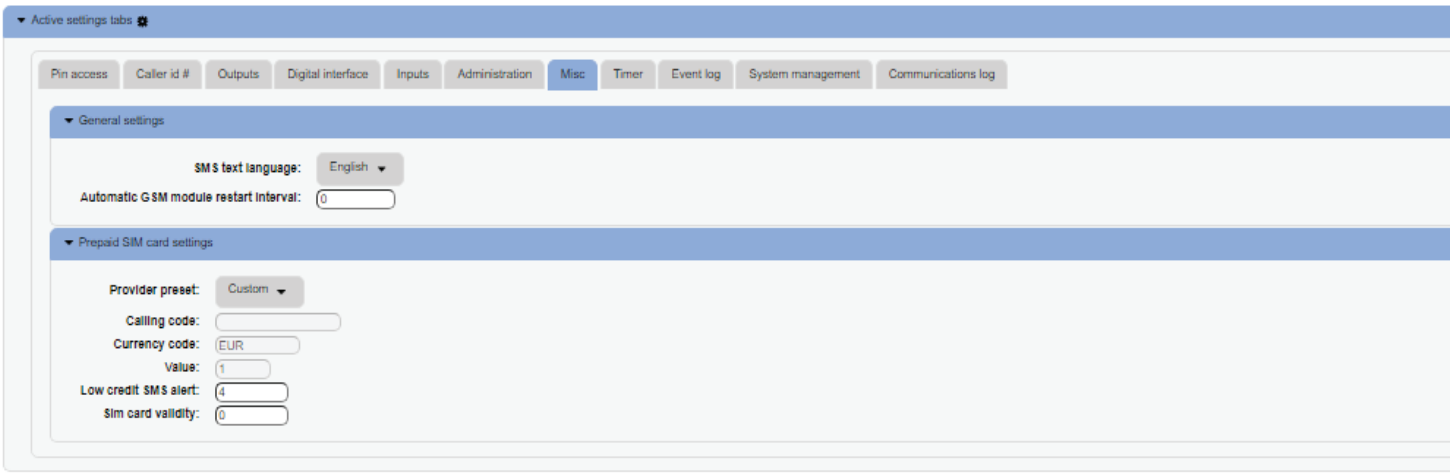


Figure 14: Web Server-Misc

General settings: The following parameters can be configured

- **SMS Text Language**
  Defines the language used for all outgoing SMS messages. The user can select the preferred language from the drop-down menu.

- **Automatic GSM Module Restart Interval**
  Allows the user to set an automatic restart interval (in hours) for the GSM module, if necessary.

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

9.WIEGAND INTERFACE DATA FORMATS

EIS-MS unit support standard Wiegand interface, it will work with Wiegand 26-bit and Wiegand 30-bit protocol and others.

9.1 WIEGAND 26 BIT, DIFFERENT DATA FORMATS

Possible data format:

Mode 0: All 24 bit 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: 24 bit of data is divided between facility code 8 bits and 16 bits 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. (Ignores Facility Code)

Mode 2: 24 bit of data is divided between facility code 8 bits and 16 bits 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. (Uses Facility Code)

Mode 3: Sections of 4 bit 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 30 bit 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: 30 bit of data is divided between facility code 8 bits, 16 bits for card number and 4 bits 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: 28 bit of data is divided between facility code 8 bits, 16 bits for card number and 4 bits 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 4 bit 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	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.