EIS 4G -CONTROLLER

Caller ID and Wiegand access control device

USER MANUAL

Transmitter SOLUTIONS®

EIS-CONTROLLER

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 a 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 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 WISELY

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

2. INTRODUCTION

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

These systems offer wireless GSM connectivity with unlimited range and support multiple access methods, including PIN 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-CONTROLLER FEATURES AND APPLICATIONS

Key Features

- Integrated 4G – LTE module for USA network compatibility
- Access control with support for up to 1,000 PIN codes
- Caller ID access control for up to 1000 authorized phone numbers
- 2 Wiegand input interfaces + 16 additional Wiegand inputs via extension modules
- (2 + 16) Programmable relay outputs 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 – Allows 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

The EIS unit comes with a 4GIM 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 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.

5. LED INDICATION

Blue LED (LED1)

- Indicates the level of the GSM signal from 1 to 5 LED flashes (1 is a weak signal, 5 is an 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 flashes with a short pulse (0,5s) ON and a long pulse OFF (5s).

EIS-CONTROLLER

6. CONNECTION DIAGRAM

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

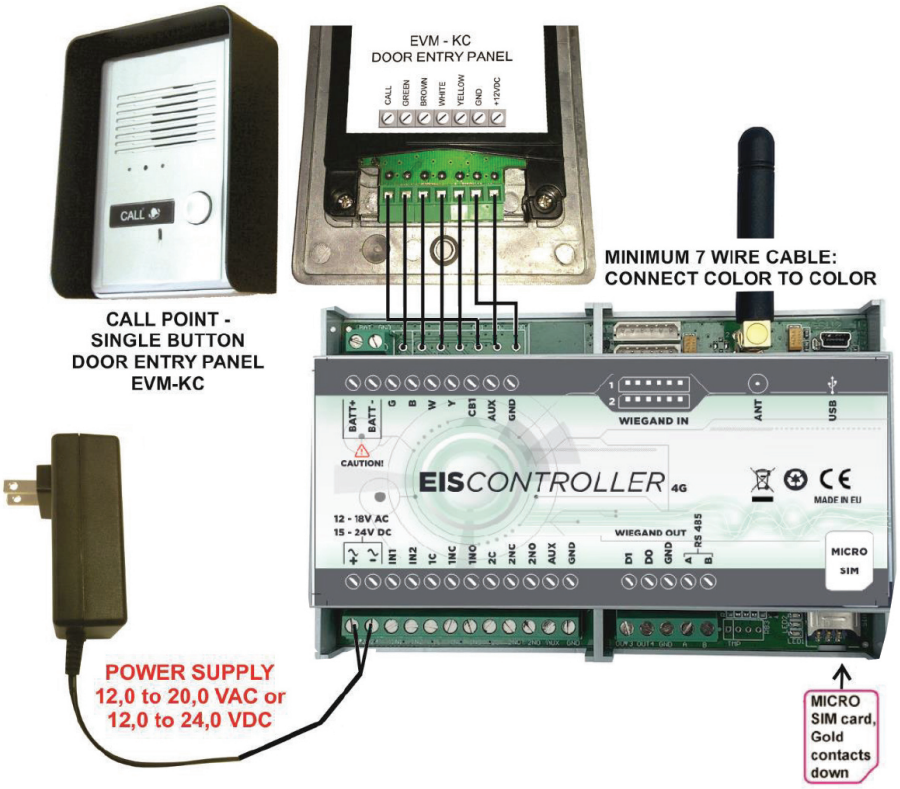


Figure 1: EIS-CONTROLLER: Connection diagram

PS	Power supply	**BATT+**	Back-up Battery connection
PS		**BATT-**	
IN1	Alarm input 1 / Call button 1	**G**	GSM Intercom – Call point connections
IN2	Alarm input 2 / Call button 1	**B**	
1C	Relay output 1 – Common	**W**	
1NC	Relay output 1 – Normal Close	**Y**	
1NO	Relay output 1 – Normal Open	**CB1**	
2C	Relay output 2 – Common	**AUX**	
2NC	Relay output 2 – Normal Close	**GND**	
2NO	Relay output 2 – Normal Open	**WIEGAND**	Wiegand input connector
AUX	+12V AUX max. 100 mA in total!	**ANT**	GSM Antenna
GND	Ground	**USB**	USB conn. for programming with PC
OUT 3	Wiegand output D0		
OUT 4	Wiegand output D1		
GND	Ground		
A	RS485 A		
B	RS485 B		

Figure 2: GSW2 EXIO: Connection table

IMPORTANT	**DO NOT USE Power out (12 V AUX) to operate electric locks! A separate power source must be used for electric door locks.**

7. EIS-CONTROLLER UNIT MANAGEMENT

Unit supports different types of management (programming):

- Unit can be programmed remotely by using WEB server access.
- Unit can be programmed remotely using Android or iOS apps.
- Unit can be programmed remotely by SMS commands (Optional).

8. EIS CONTROLLER FUNCTIONS with PROGRAMMING INSTRUCTIONS

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

8.1 WEB SERVER - LOG IN

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

Figure 3: 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.

To add a new unit, click the “+” icon and follow the prompts to register the device to your account

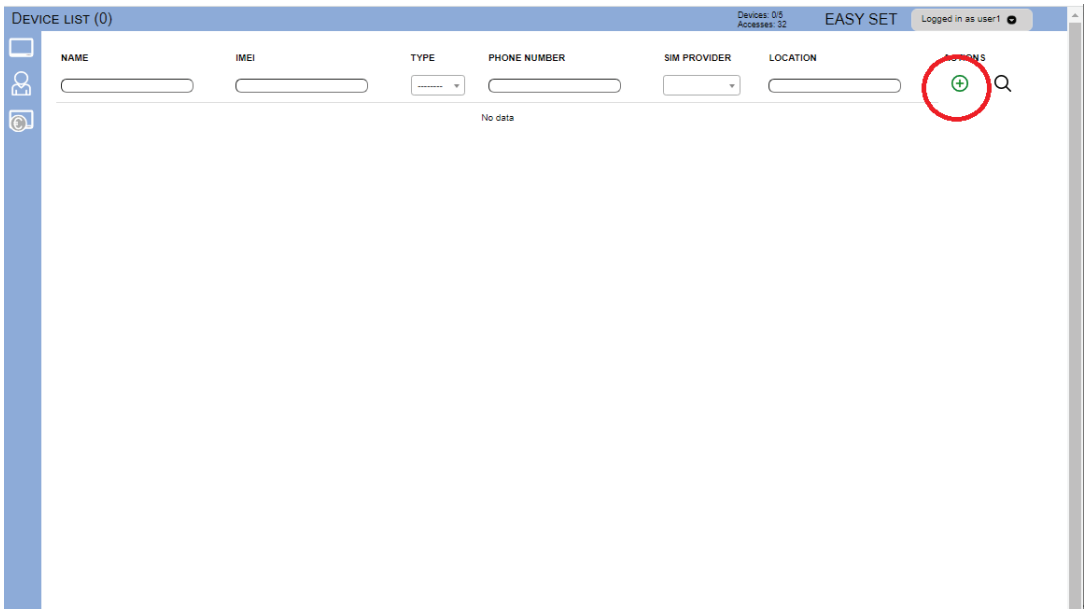


Figure 4: Web Server-Main page select ADD mode

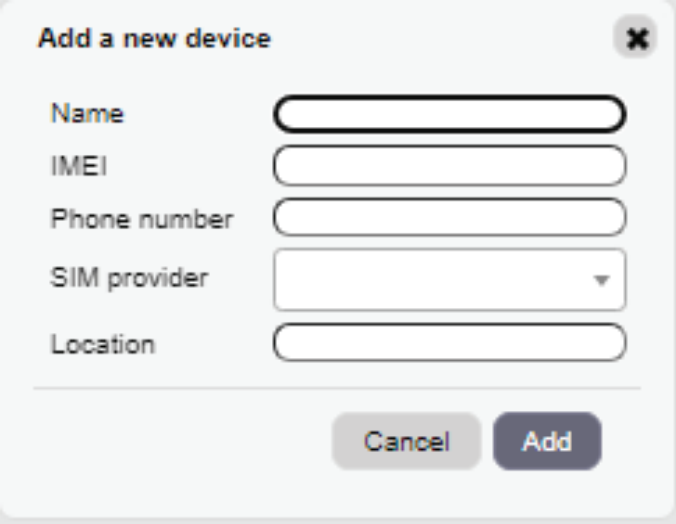


Figure 5: Web Server-Main page adding EIS units

User then provides required data:

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 provision:** A SIM card is inthe EIS Unit when it is shipped to the customer. ONLY that SIM card should be used in the EIS Unit. DO nouse any other SIM card.

Optional Data:

- **Location:** Notification field, used by the user to provide extra data for its own information - optional data.

NOTE: First building of the unit data-base 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.

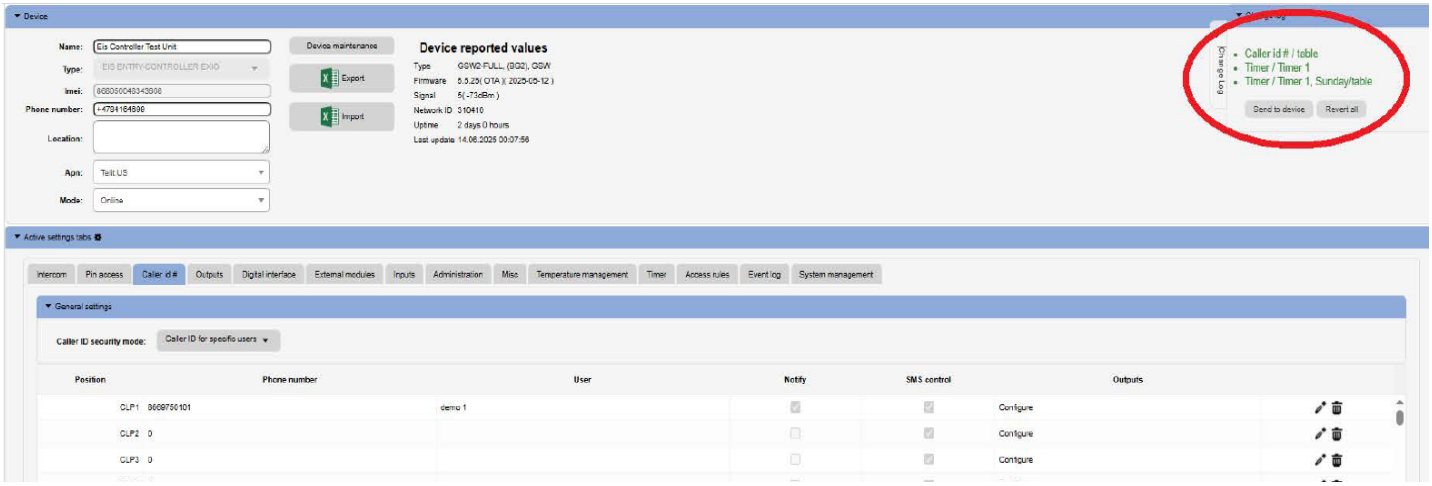


Figure 6: Web Server-Unit management window

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

8.4 PIN ACCESS

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:

PIN codes can operate in three distinct modes, each 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.

EIS-CONTROLLER

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.

Hotel Access Mode:

This mode is the same as Restricted Access mode, but with added support for MASTER codes.

PIN code configuration options

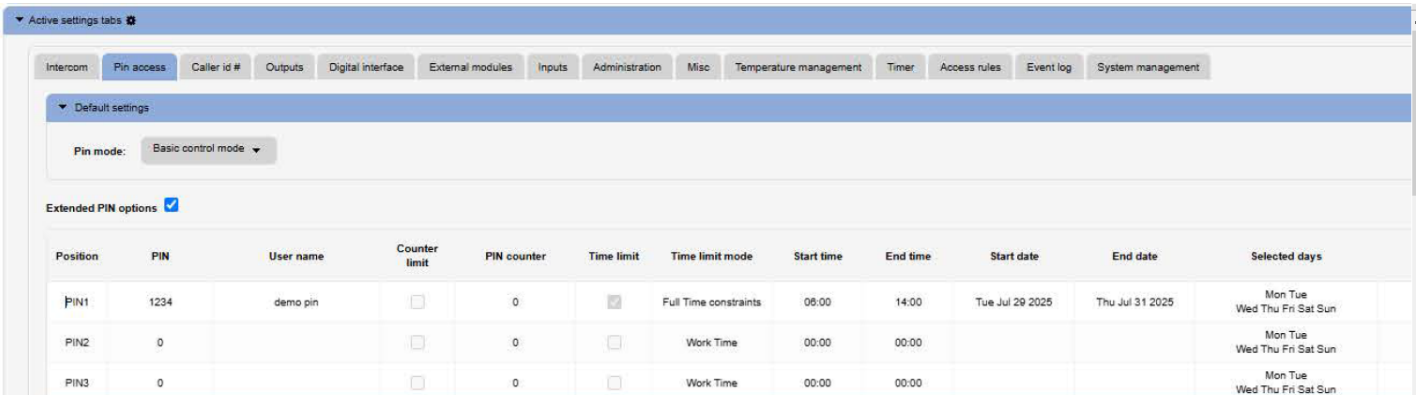


Figure 7: Web Server - PIN Access configuration

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.

8.5 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.

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

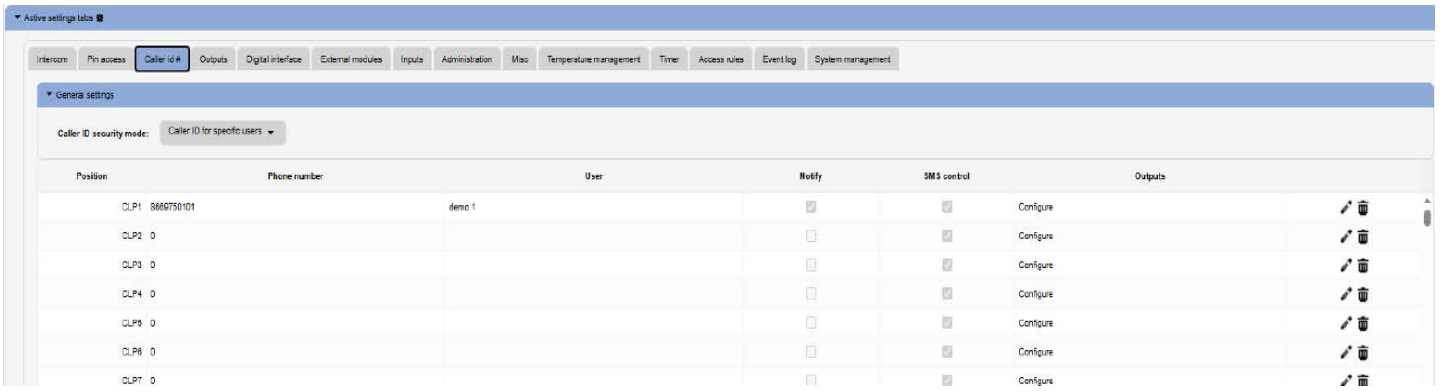


Figure 8: Web Server-Caller ID Access

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 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.
- **Notify:** If enabled, sends an SMS notification to administrators when the CLIP is used.

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.**

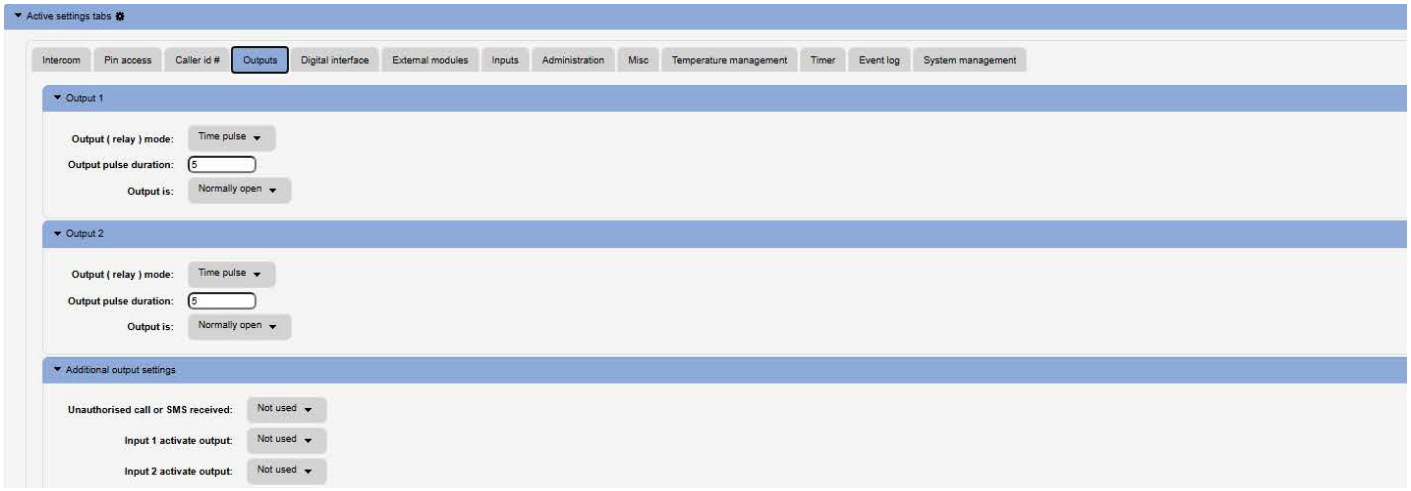


Figure 9: Web Server-Output setting

Settings for Output 1:

- **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 - Setting are 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.
- **Input 2 activate output:** An alarm event detected on Input 2 will activate the assigned output.

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

8.7 TIMER/TIMED CONTROLLED OUTPUT

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

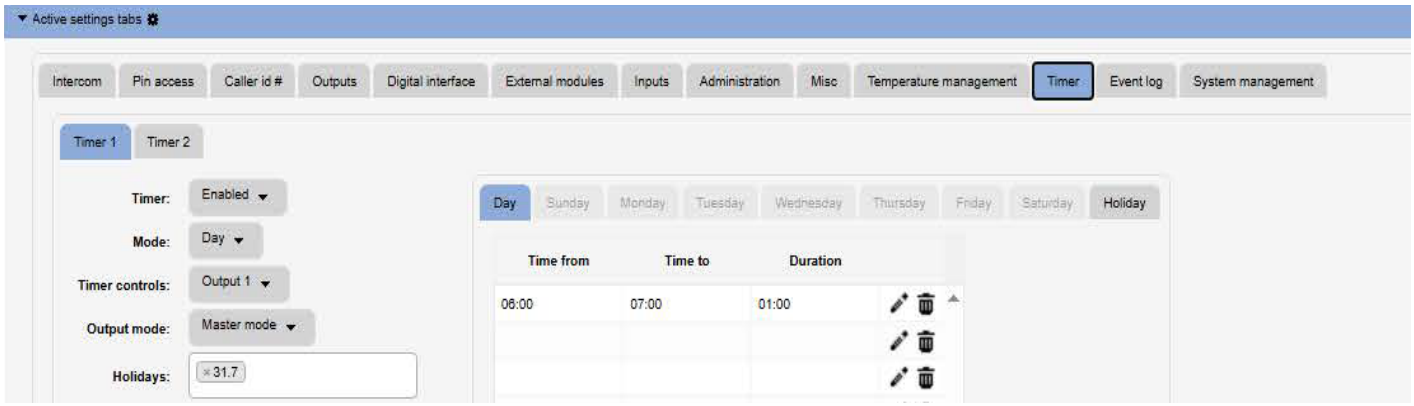


Figure 10: Web Server-Timer setting →Day mode.

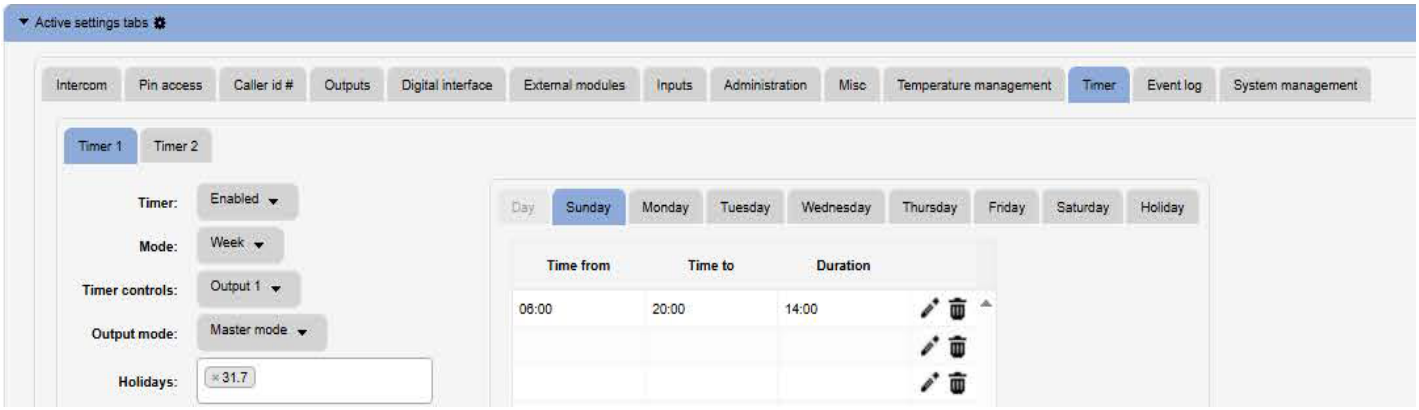


Figure 11: Web Server-Timer setting →Week mode.

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
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.
Slave mode	The behavior of the outputs (Time Pulse or Latching Mode) is configured 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 to define holiday dates and set custom output behavior for holidays.

8.8 INTERCOM CONFIGURATION

One of the features of the EIS unit is the secure integration of intercom functionality. The intercom function is enabled by connecting an external audio module. Apartment selection (calling) is performed by pressing the call button located next to the corresponding nameplate.

This action initiates a voice call sequence, starting with Phone Number 1 and continuing up to Phone Number 5, if necessary. Once the call is answered, the recipient has the option to activate outputs by entering specific codes:

- Pressing **“11** will trigger **Output 1** (e.g. door opening).
- Pressing **“12”:** will trigger **Output 2.**

When the call is successfully answered, the unit stops dialing the remaining numbers on the list.

The intercom function settings can be configured under the Intercom tab.

General Settings:

- **Enable intercom button 1:** User has to enable intercom button 1 before using it as a call button 1.
- **Enable intercom button 2**: User has to enable intercom button 2 before using it as a call button 2.
- **Line open time:** Defines the maximum in-call time in seconds before the unit automatically disconnects the call.

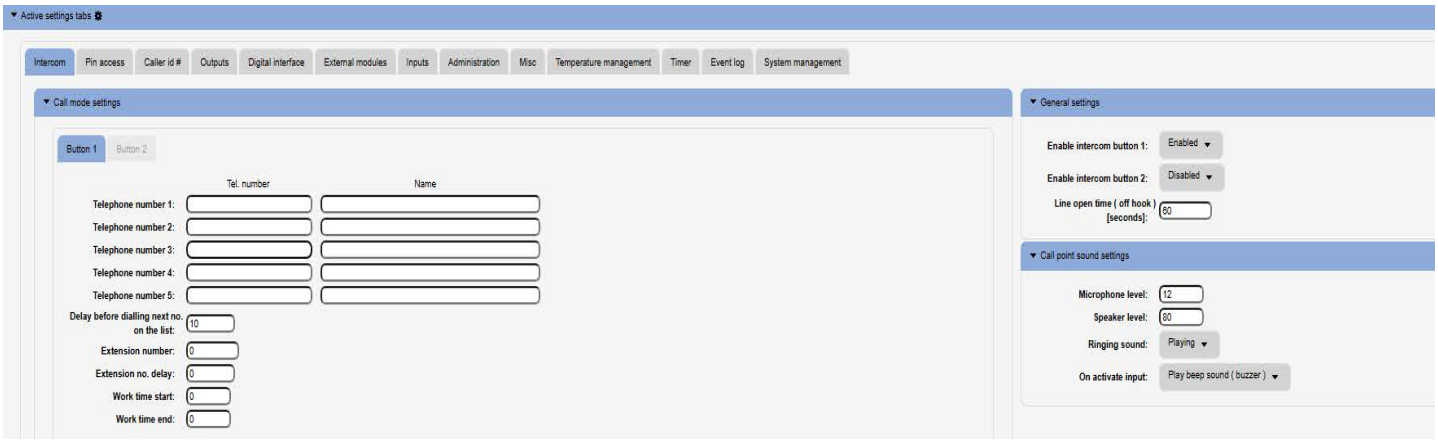


Figure 12: Web Server-Intercom Settings

Call mode settings:

- **Telephone number 1…Telephone number 5:** The numbers the unit will call when the call button is pressed.

  Delay before dialing next no. on the list: Time delay in seconds before the next number on the list is dialed if the previous call is not answered.

  Extension number: Parameter used to set the DTMF number for the auto self-select function.
- **Extension no. delay:** Parameter used to set the delay (in seconds) for sending the DTMF number in the auto self-select function.
- **Work time start, Work time end:** Parameters used to define the work time schedule. During this period, numbers in positions 1 to 4 will be dialed; outside this period, the number in position 5 will be dialed.

Call point sound settings:

- **Microphone level:** Increasing the level increases the microphone's sensitivity; decreasing it lowers the sensitivity.
- **Speaker level:** Increasing the level raises the speaker volume; decreasing it lowers the volume.
- **Ringing sound:** If *Playing* is selected, the unit will play a dial tone during the call connection phase; if *Muted* is selected, no sound will be played during the connection phase.
- **On activate input:** If *Play beep sound (buzzer)* is selected, the unit will provide audio feedback (buzzer BEEP) when an apartment entry is selected; if *Muted* is selected, no audio feedback will be provided.

8.9 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.

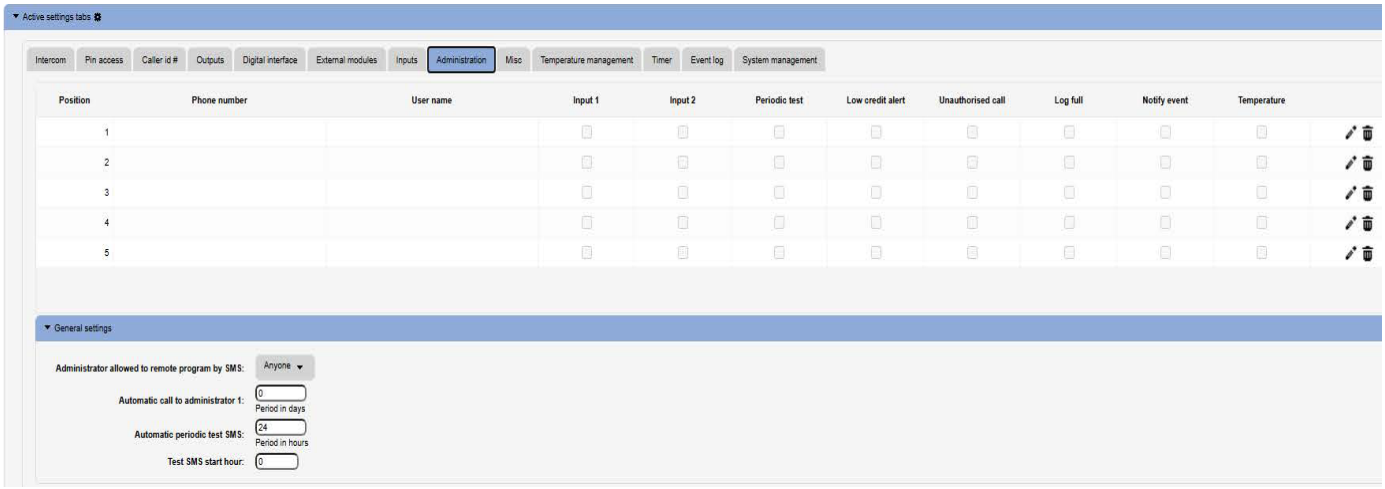
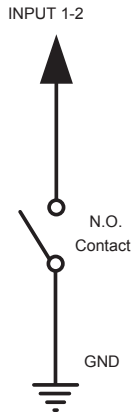


Figure 13: Web Server-Notification numbers

- **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, tick the checkbox next to the corresponding user n.
- **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.

8.10 EVENT LOGGING

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.

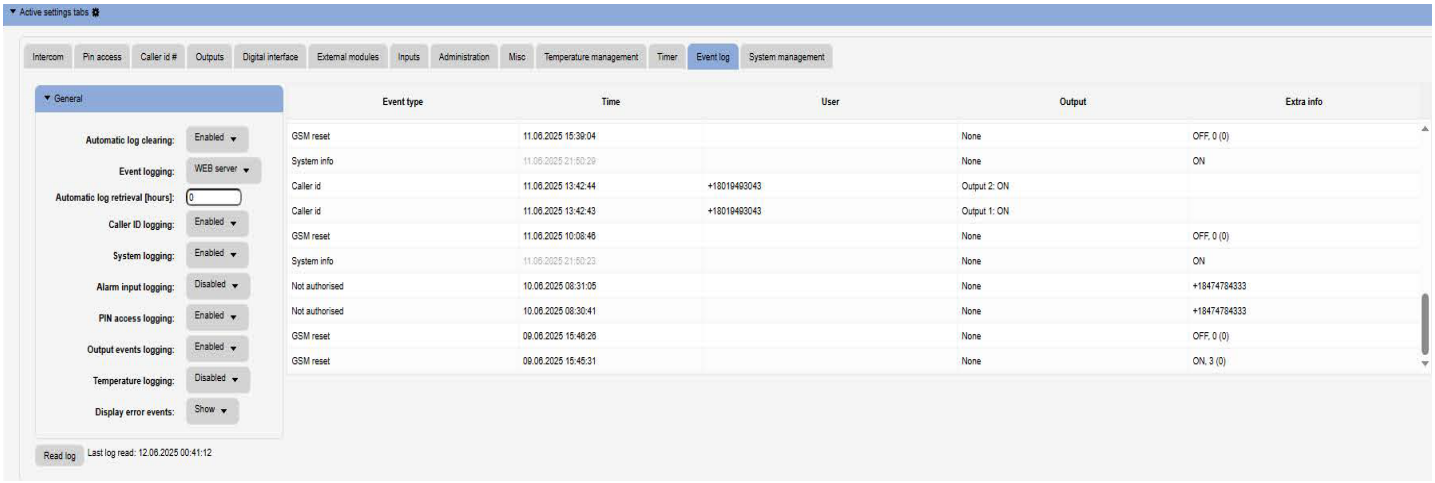


Figure 15: Web Server-Log event

EIS-CONTROLLER

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 will be stored. The user can select 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.

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

8.11 MISCELLANEOUS

This tab is split into 2 sections.

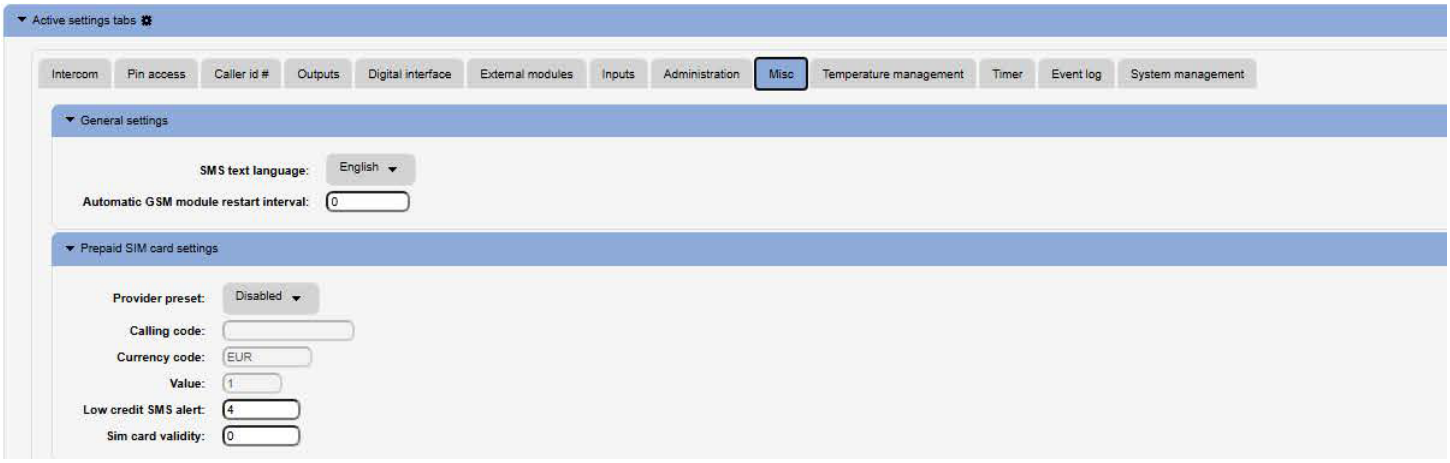


Figure 16: Web Server-Misc

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 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.*

9.WIEGAND INTERFACE DATA FORMATS

The EIS-CONTROLLER unit supports standard Wiegand 26-bit Wiegand 30-bit protocols and others.

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	B	P
Parity	28Bit card number																											Parity

	Limits
Card Number	0 - 268435455
Facility Number	None

Table 7: Wiegand 30: Mode 0.

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

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

	Limits
Card Number	0 - 16777215
Facility Number	NOT USED

Table 8: Wiegand 30: Mode 1.

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

P	0	0	0	0	F	F	F	F	F	F	F	F	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	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	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.