

SOLO-NX EXT

COMPACT GSM DOOR ENTRY UNIT WITH 1, 2 or 4 CALL BUTTONS



USER MANUAL

Contents

1	FOR YOUR SAFETY	4
2	INTRODUCTION.....	5
3	SOLO-NX FEATURES AND APPLICATIONS.....	6
4	START UP.....	7
5	LED INDICATION.....	8
6	CONNECTION DIAGRAM	9
7	SOLO UNIT MANAGEMENT.....	10
8	SOLO FUNCTIONS WITH PROGRAMMING INSTRUCTIONS	11
8.1	WEB SERVER - LOG IN.....	11
8.2	WEB SERVER – ADDING UNITS TO USER PROFILE.....	12
8.3	WEB SERVER-UNIT MANAGEMENT	14
8.4	INTERCOM CONFIGURATION	15
8.5	WIEGAND ACCESS.....	17
8.6	CALLER ID ACCESS	21
8.7	OUTPUTS SETTINGS	22
8.8	SOLO WIEGAND OUTPUT INTEGRATION.....	24
8.9	TIMER-TIMED CONTROLLED OUTPUT.....	25
8.10	ADMINISTRATION	27
8.11	EVENT LOGGING	29
8.12	MISCELLANEOUS	30
8.13	PIN ACCESS NOTIFICATION FUNCTION	31
9	WIEGAND INPUT DATA FORMATS	33
9.1	WIEGAND 26 BIT, DIFFERENT DATA FORMATS	34
9.2	WIEGAND 30 BIT, DIFFERENT DATA FORMATS	35
10	CONTACTS	36

Figures

Figure 1: SOLO: Connection diagram	9
Figure 2: WEB Server-Sign In page	11
Figure 3: WEB Server-Main page select ADD mode.....	12
Figure 4: WEB Server-Main page adding SOLO units	13
Figure 5: WEB Server-Unit management window	14
Figure 6: WEB Server-Intercom settings.....	15
Figure 7: WEB Server-First Wiegand interface support.....	17
Figure 8: WEB Server-Wiegand interface support.....	18
Figure 9: WEB Server-Adding Wiegand devices with permanent use.....	19
Figure 10: WEB Server-Adding Wiegand devices with temporary use.	19
Figure 11: WEB Server-Caller ID Access	21
Figure 12: WEB Server-Output setting.....	22
Figure 13: WEB Server-Wiegand Output settings.....	24
Figure 14: WEB Server-Timer setting →Day mode.	25
Figure 15: WEB Server-Timer setting →Week mode.....	25
Figure 16: WEB Server-Notification numbers	27
Figure 17: WEB Server-Input alarm configuration	27
Figure 18: WEB Server-Log event	29
Figure 19: WEB Server-Misc	30
Figure 20: WEB Server-Global enabling of the notificaton function.	31
Figure 21: WEB Server-Selecting administrator numbers for notification.	32
Figure 22: WEB Server-First Wiegand interface support.....	33
Figure 23: WEB Server-Second Wiegand interface support.	33

Tables

Table 1: WEB Server-SPIN entry parameters.	20
Table 2: WEB Server-Timer setting, output mode options	26
Table 3: Wiegand 26: Mode 0.....	34
Table 4: Wiegand 26: Mode 1.....	34
Table 5: Wiegand 26: Mode 2.....	34
Table 6: Wiegand 26: Mode 3.....	34
Table 7: Wiegand 30: Mode 0.....	35
Table 8: Wiegand 30: Mode 1.....	35
Table 9: Wiegand 30: Mode 2.....	35
Table 10: Wiegand 30: Mode 3.....	35

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

SOLO-NX (SOLO) is a simple GSM intercom communication system designed to ensure low-cost, simple to install/use, reliable and single box solution for intercom application. It is designed for unlimited range, wire free GSM intercom, pin code access, caller ID control and Wiegand access support.

Optional SOLO supports alarm detection, stay-alive messages, credit detection etc...

3 SOLO-NX FEATURES and APPLICATIONS

Features:

- ⇒ Built-in 5 band GSM module
- ⇒ Up-to 4 intercom call button support (5 numbers each)
- ⇒ Caller ID numbers control (up-to 1000 caller ID numbers)
- ⇒ Up to 100 temporary SPIN access codes
- ⇒ Up to 1000 PIN access codes
- ⇒ 2 x Input Wiegand receiver
- ⇒ 2 outputs (relay supported)

- ⇒ Programming with PC via “USB to Mini USB cable” connected to the unit
- ⇒ Programming by WEB server
- ⇒ Programming by SMS commands

Applications:

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

4 START UP

SOLO unit accepts a standard GSM SIM card from any network.

**VERY
IMPORTANT**

USE A MICRO SIM CARD



WARNING

DO NOT Insert or remove the SIM card while the unit is powered ON!!

IMPORTANT

Before inserting SIM card to unit make sure the PIN code is removed!!

- ⇒ Insert SIM card in SOLO unit.
- ⇒ Connect power cable to SOLO unit (YOU MUST POWER THE SOLO 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.
- ⇒ SOLO unit is now ready to operate.

NOTE

SOLO device will “beep” in 15s interval until the device is not in normal operation.

5 LED INDICATION

Blue LED (LED1)

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

Red LED (LED2)

- GSM module Activity

Yellow LED (LED3)

- Short flashing indicates that the GSM module is ON, but it is not yet connected on the GSM network. After connection, yellow led is flashing with short pulse (0,5s) ON and a long pulse OFF (5s).

6 CONNECTION DIAGRAM

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

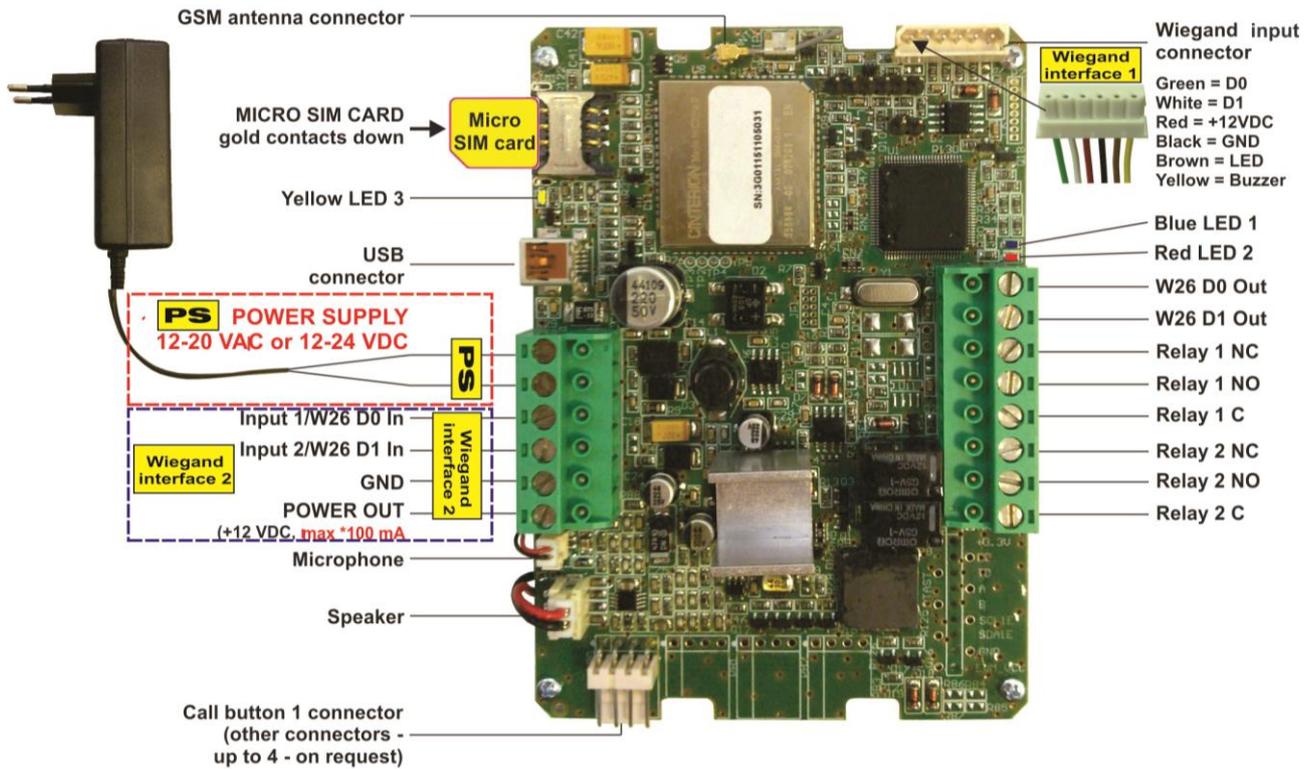


Figure 1: SOLO: Connection diagram

IMPORTANT

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

7 SOLO UNIT MANAGEMENT

Unit supports different types of management (programming):

- ⇒ Unit can be programmed directly by USB connection, with the use of configuration software running on PC (SOLO Ware).
- ⇒ Unit can be programmed remotely by using WEB server access.
- ⇒ Unit can be programmed remotely by SMS commands (Optional).

8 SOLO FUNCTIONS WITH PROGRAMMING INSTRUCTIONS

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

IMPORTANT

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

8.1 WEB SERVER - LOG IN

The web server can be find under the address: <https://www.easyset.eu/>.

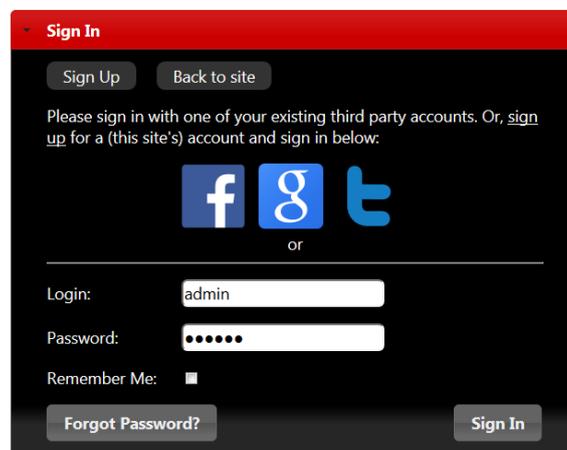


Figure 2: WEB Server-Sign In page

User must first use the Sign IN section to create working profile on the server. The profile can be created by using social login like Facebook, Google account or Twitter. If user lacks any of the social profile it can proceed to Sign UP page use standard user name and password entry.

NOTE

Server support Firefox, Google Chrome, Safari.

8.2 WEB SERVER – ADDING UNITS TO USER PROFILE

After login the user will be diverted to WEB server main window. This page is used to add/remove/search for SOLO units from the user's profile.

Select “+” sign to select ADD SOLO units to user's profile.

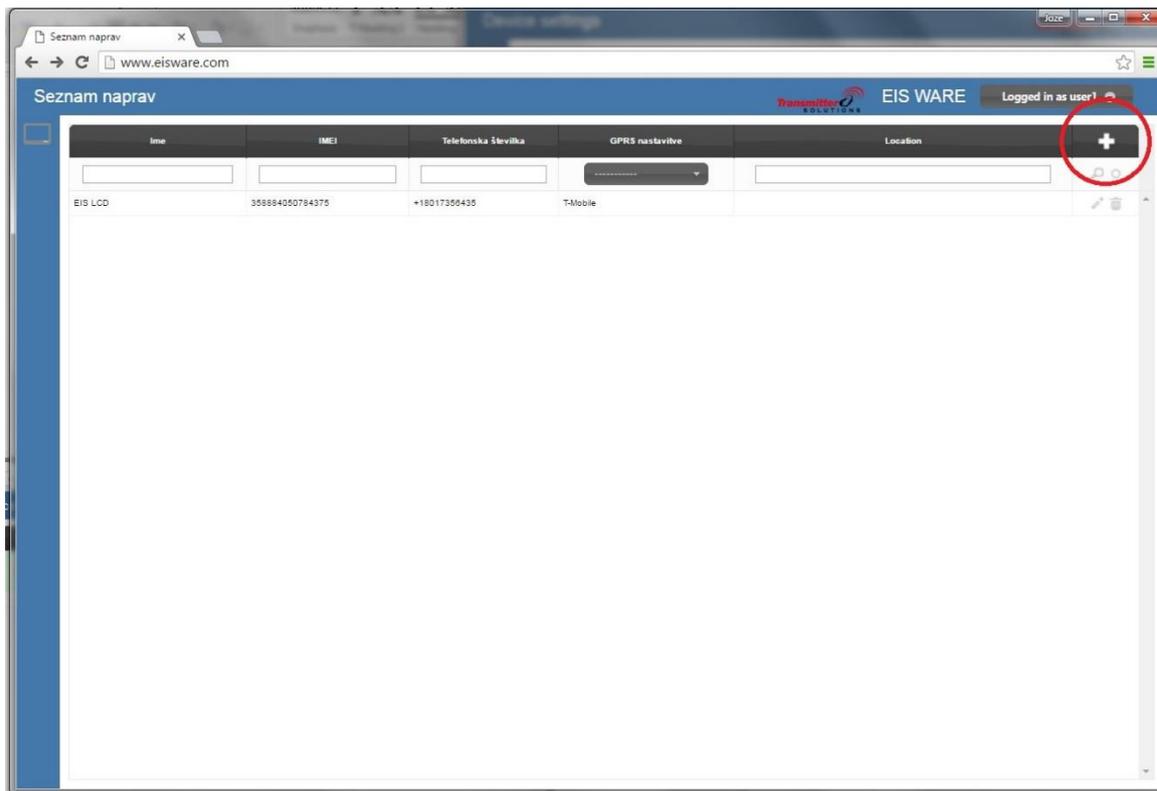


Figure 3: WEB Server-Main page select ADD mode

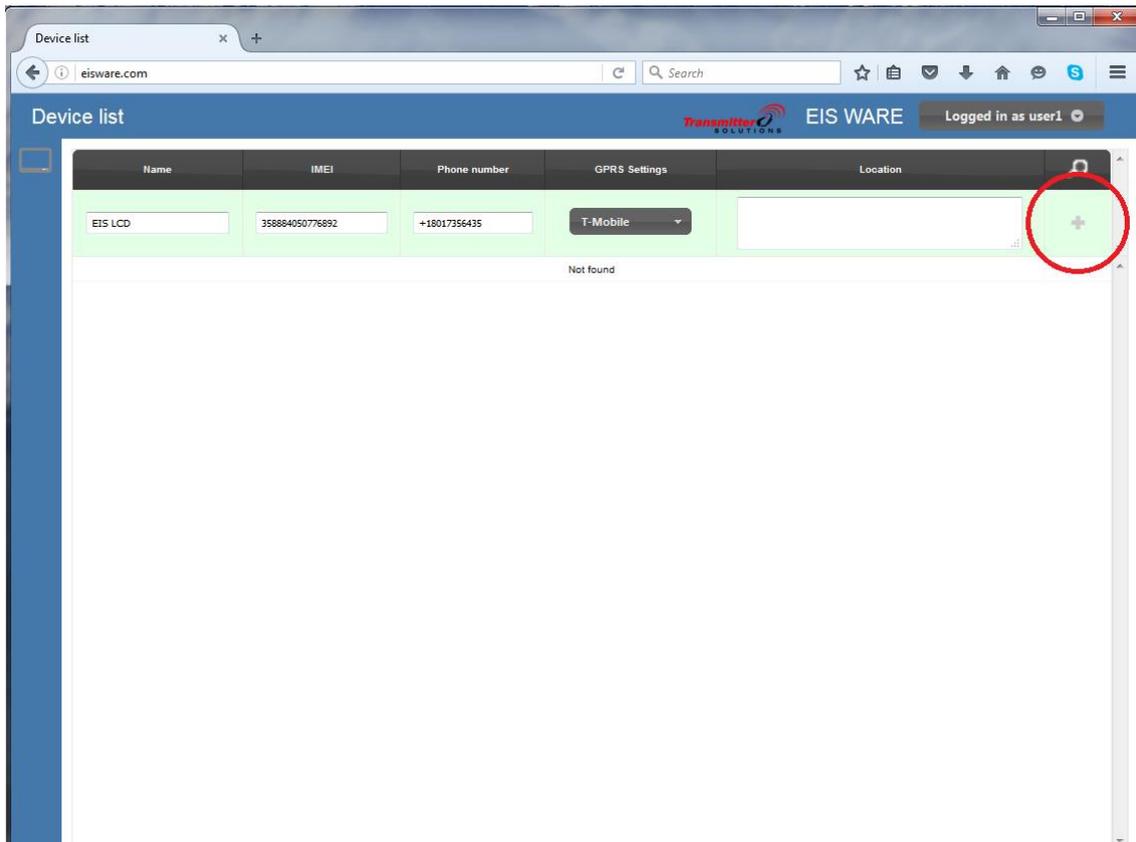


Figure 4: WEB Server-Main page adding SOLO units

User than provides required data:

- **Name:** Name for the added unit - mandatory information.
- **IMEI:** Identification number of the unit can be found in the enclosure of the unit - mandatory information. The IMEI is located on the cellular chip and also should be on the card board box of the SOLO.
- **Phone Number:** The telephone number of the SIM card in the SOLO unit - mandatory data.
- **GPRS settings:** Information needed to enable data connection between the server and the unit. Selectable from the drop-down menu - mandatory data.
- **Location:** Notification field, used by the user to provide extra data for its own information - optional data.

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

First building of the unit data-base may take a few minutes.

8.3 WEB SERVER-UNIT MANAGEMENT

After the SOLO unit is added to user database, the user can change the configuration of the specific unit.

All changes made by the user are listed in the **Change Log** window. **By clicking Send to device button ALL changes are sending to the unit.** User can revert all changes made, before sending, by clicking **Revert all** or select particular entry and revert it.

The screenshot displays the 'Device settings' interface for a device named 'EIS LCD'. The interface is divided into several sections:

- Device Section:** Contains input fields for Name, Type, Imei, and Phone number, along with a Location field. It also includes 'Save changes', 'Cancel changes', 'Export', and 'Import' buttons. A 'Device reported values' section shows firmware, signal, network ID, time, and uptime.
- Settings Section:** Features a 'Change log' window with a red border, listing 'Intercom / table' and 'Pin access / table' changes. Below it are 'Send to device' and 'Revert all' buttons.
- General Settings Section:** Includes tabs for 'Intercom', 'Pin access', 'Caller id #', 'Outputs', 'Digital interface', 'Inputs', 'Temporary pin access', 'Service button', 'Administration', 'Misc', and 'Event log'. The 'General' tab is active, showing 'Tables control mode' set to 'Joint (WINF1 & WINF2 Control Table 1 & Table 2)'.
- Table 1 output (Output 1):**

Position	PIN	User name
PIN1	2233	Mark
PIN2	0	
PIN3	0	
PIN4	0	
PIN5	0	
PIN6	0	
PIN7	0	
PIN8	0	
- Table 2 output (Output 2):**

Position	PIN	User name
PIN251	0	
PIN252	0	
PIN253	0	
PIN254	0	
PIN255	0	
PIN256	0	
PIN257	0	
PIN258	0	

Figure 5: WEB Server-Unit management window

8.4 INTERCOM CONFIGURATION

Primary function of the SOLO unit is intercom support. Selecting (calling) apartment number is achieved pressing the call button beside appropriate name plate.

This action will start a voice call procedure from **Phone number 1** till **Phone number 5**. After the call is answered the called user has the option to trigger the output by pressing “11” for opening *Output 1* or “21” for triggering Output 2.

If the call is answered the unit will stop dialing next numbers on the list.

Management of the intercom function is found under **Intercom** tab.

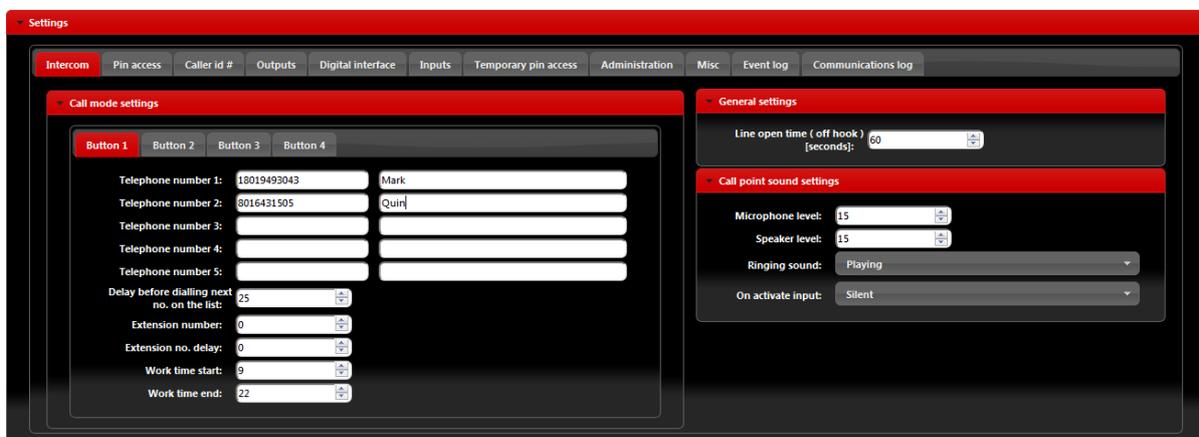


Figure 6: WEB Server-Intercom settings.

Intercom management parameters:

- **Telephone number 1...Telephone number 5:** Number that the unit will call when call button pressed.
- **Delay before dialling 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.

Voice call setting

- **Microphone level:** Increasing the level will increase the sensitivity of the unit microphone decreasing will decrease the sensitivity.
- **Speaker level:** Increasing the level will increase the volume of the unit speaker, decreasing will decrease the level of the speaker.
- **Ringing sound:** By selecting *Playing* the unit will play the dial tone in the connection phase of the call, by selecting *Muted* the unit will not play any sound in the connection phase of the call.
- **On activate input:** By selecting *Play beep sound (buzzer)* the unit will provide audio feed back (buzzer BEEP) when the apartment entry is selected, by selected *Muted* unit will provide no audio feedback when the apartment entry is selected.

8.5 WIEGAND ACCESS

SOLO unit has onboard support for 2 Wiegand output based device. With the user of external replicator more Wiegand devices can be connected to the unit.

Configuration of first Wiegand interface is found in **Digital interface** tab. First Wiegand interface can be found on board with a dedicated Wiegand connector and cables.

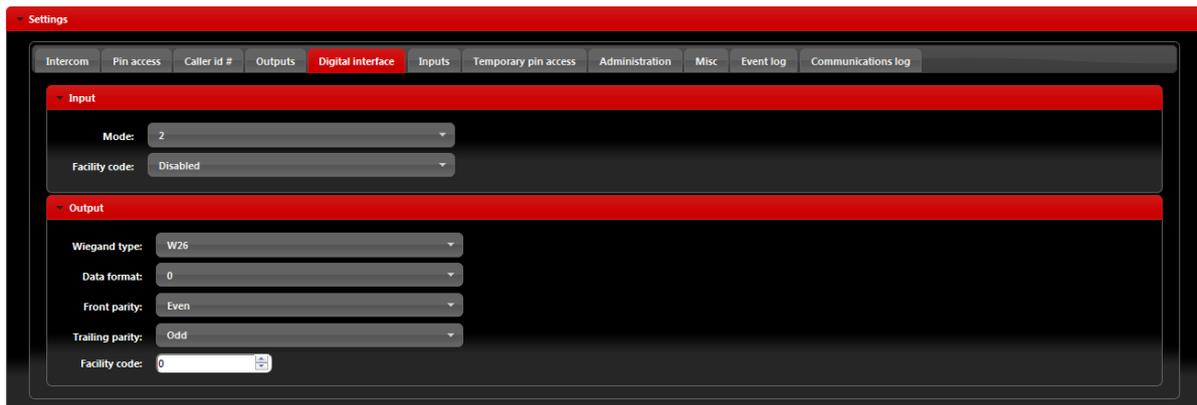


Figure 7: WEB Server-First Wiegand interface support.

- **Mode:** Select appropriate data formatting (Advise unit provider for more info if needed, mode 2 is most common setting)
- **Facility code:** User can *Enable* or *Disable* facility code field.

Second Wiegand interface is shared with alarm input lines; user must select *Wiegand* in **Input operation mode** found in the **Inputs** tab.

Additional settings for Wiegand interface input are found in **Wiegand input 2 configuration** section.

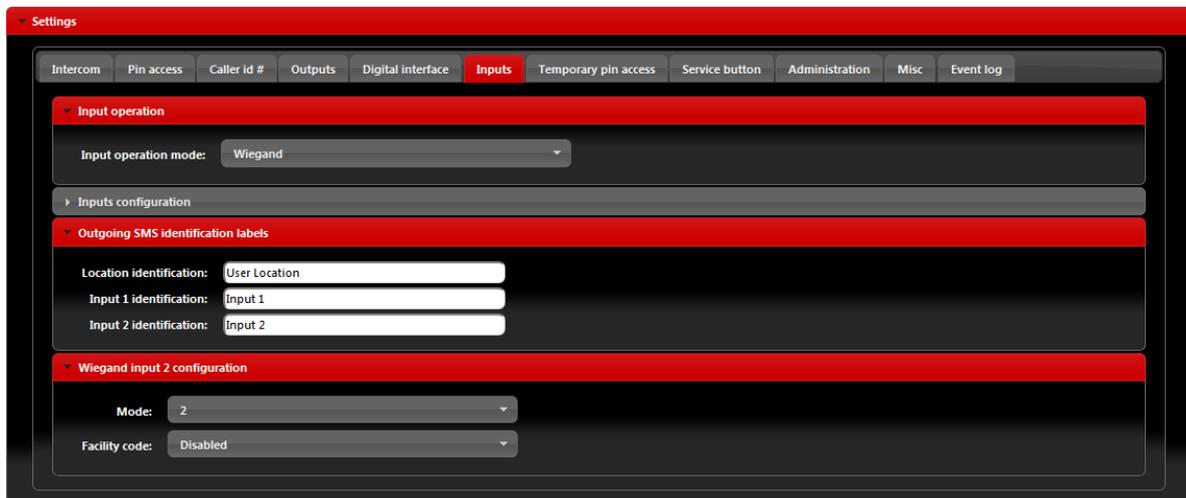


Figure 8: WEB Server-Wiegand interface support.

- **Mode:** Select appropriate data formatting (Advise unit provider for more info if needed, mode 2 is most common setting)
- **Facility code:** User can *Enable* or *Disable* facility code field.

Wiegand devices can be defined in two sections. First section is permanent pin codes and second is temporary pin codes - limited by the number of use.

NOTE

See [Chapter 9-WIEGAND INPUT DATA FORMATS](#) for detailed explanation of different data format options.

IMPORTANT

Unit **MUST** be restarted when switching between *Normal* and *Wiegand* mode in the **Input operation mode**.

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

They are placed in two tables. For each table user can define which output they will trigger.

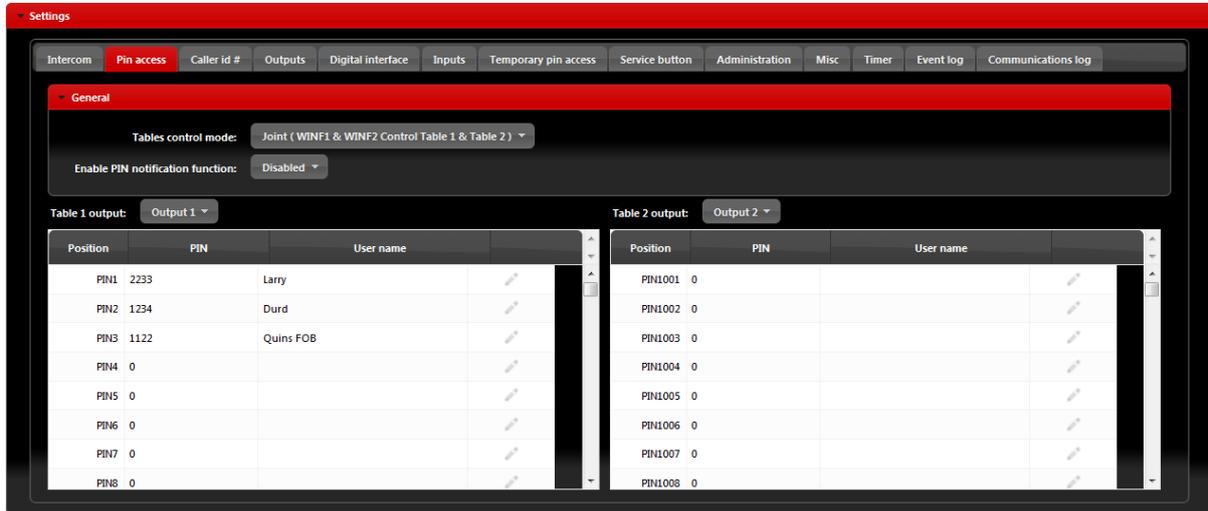


Figure 9: WEB Server-Adding Wiegand devices with permanent use.

- **PIN entry:** For each PIN entry user need to select PIN code value and optional User name.

Temporary pin codes are placed in **Temporary pin access** tab.

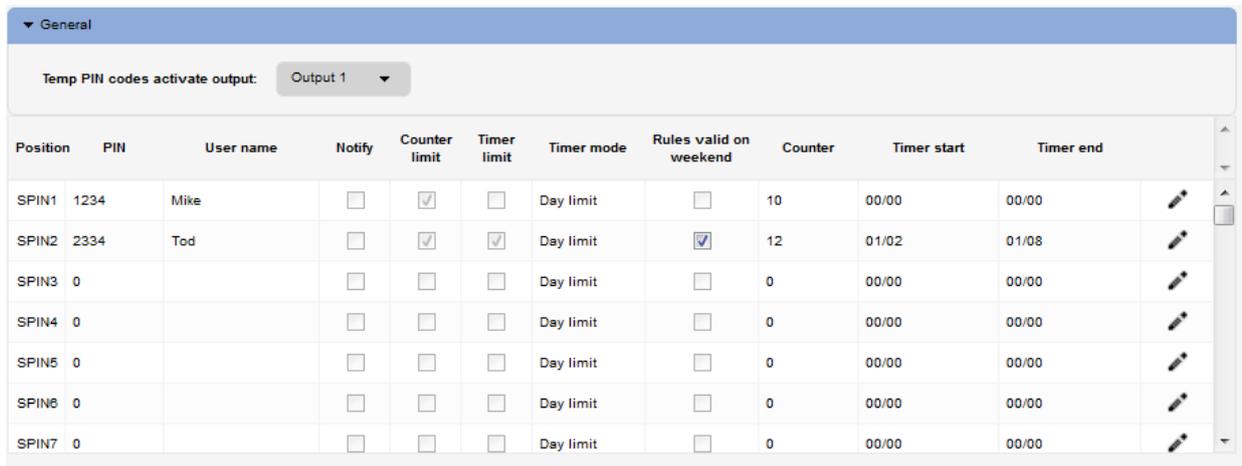


Figure 10: WEB Server-Adding Wiegand devices with temporary use.

- **Temp PIN codes activate output:** Selecting the output that will be triggered in case of correct SPIN code.

- **SPIN entry:** For each SPIN entry user need to select appropriate values.

SPIN options	Description
SPIN value	Temporary PIN code
User name	Name of the user
Notify	If SPIN code is used, administrator numbers CAN be notified
Counter limit	Enable/Disable counter limitation (consecutive use)
Timer limit	Enable/Disable timer limitation
Timer mode	Timer limit mode: Day limit (day limitation), Timer limit (hours of a day access limitation)
Rules valid on weekend	Enable/Disable timer limitation for weekend days
Counter	Number of allowed use of SPIN code
Timer start/Timer end	Bottom and Top timer limitation

Table 1: WEB Server-SPIN entry parameters.

8.6 CALLER ID ACCESS

Caller ID access is a very simple way to control relay output defined in **Caller ID output** setting.

User will by calling in the SOLO unit trigger defined output.

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

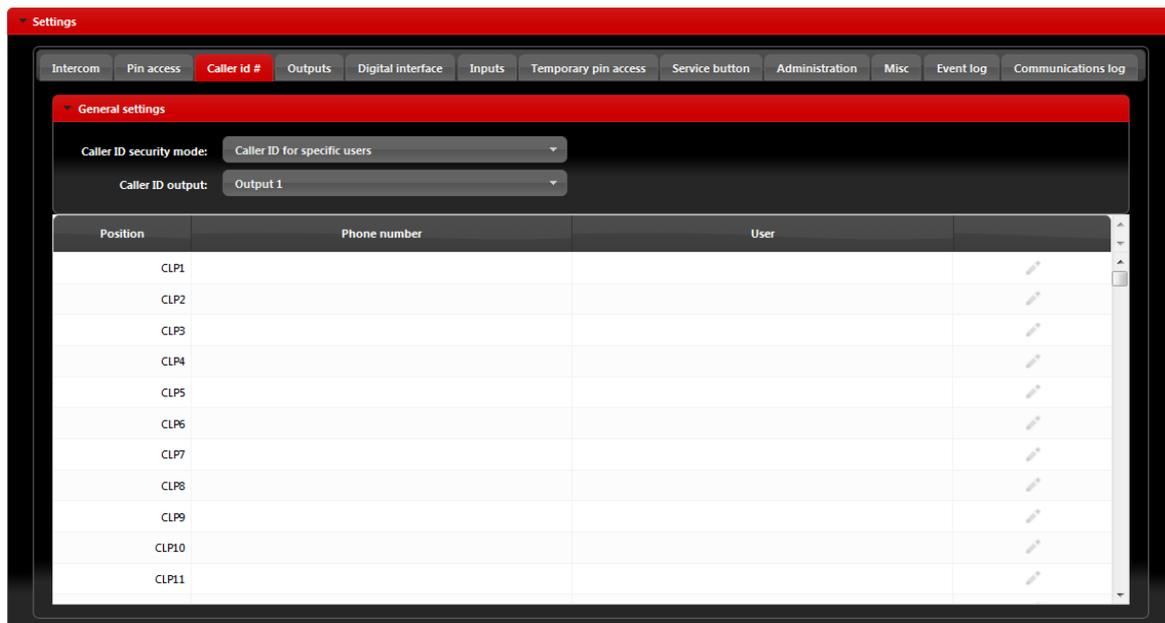


Figure 11: WEB Server-Caller ID Access

General settings:

- **Caller ID security mode:** User can select between 3 options:
Caller ID Disabled deactivates caller ID function – all numbers are restricted
Caller ID for specific users will limit the caller ID function only to the numbers on the list.
Caller ID always ON will allow all user that know the number of the unit to open defined output. In last option the user doesn't need to be on the list to trigger the output
- **Caller ID output:** Selecting the output that will be triggered in Caller ID function.

NOTE

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

8.7 OUTPUTS SETTINGS

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

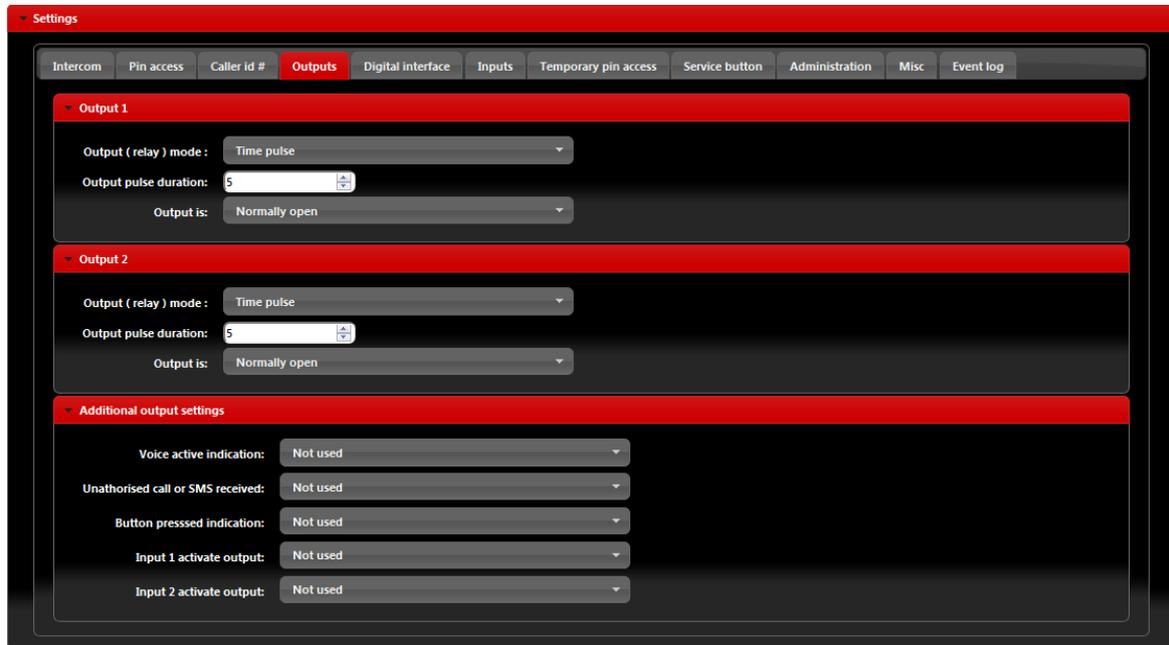


Figure 12: WEB Server-Output setting

Output 1 - Settings for output 1:

- **Output (relay) mode:** User can select between 3 options
Disable-Output is disabled.
Latching-Output is in latching mode. First Caller ID or PIN entry will activate the output, second Caller ID or PIN entry will deactivate the output.
Time Pulse-Output is time pulse mode. After output is triggered it will be activated for the time defined in **Output pulse duration**, after that time output will be restored.
- **Output pulse duration:** ON time for output in case of output mode *Timer pulse*.
- **Output is:** Output can work in normal or inverted (normally close) mode.
Normally open-In idle mode output pins are in open position.
Normally closed-In idle mode output connection are closed.

Output 2 - Settings for output 2:

- **Output (relay) mode:** User can select between 3 options
 - Disable*-Output is disabled
 - Latching*-Output is in latching mode. First Caller ID or PIN entry will activate the output, second Caller ID or PIN entry will deactivate the output.
 - Time Pulse*-Output is time pulse mode. After output is triggered it will be activated for the time defined in **Output pulse duration**, after that time output will be restored.
- **Output pulse duration:** ON time for output in case of output mode *Timer pulse*.
- **Output is:** Output can work in normal or inverted (normally close) mode.
 - Normally open*-In idle mode output pins are in open position.
 - Normally closed*-In idle mode output connections are closed.

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

- **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

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

8.8 SOLO WIEGAND OUTPUT INTEGRATION

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

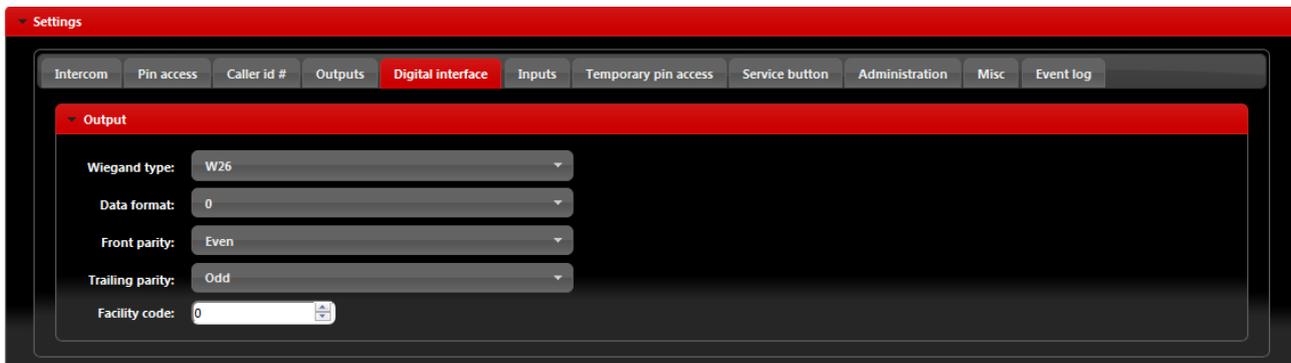


Figure 13: WEB Server-Wiegand Output settings.

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.

8.9 TIMER-TIMED CONTROLLED OUTPUT

SOLO 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.

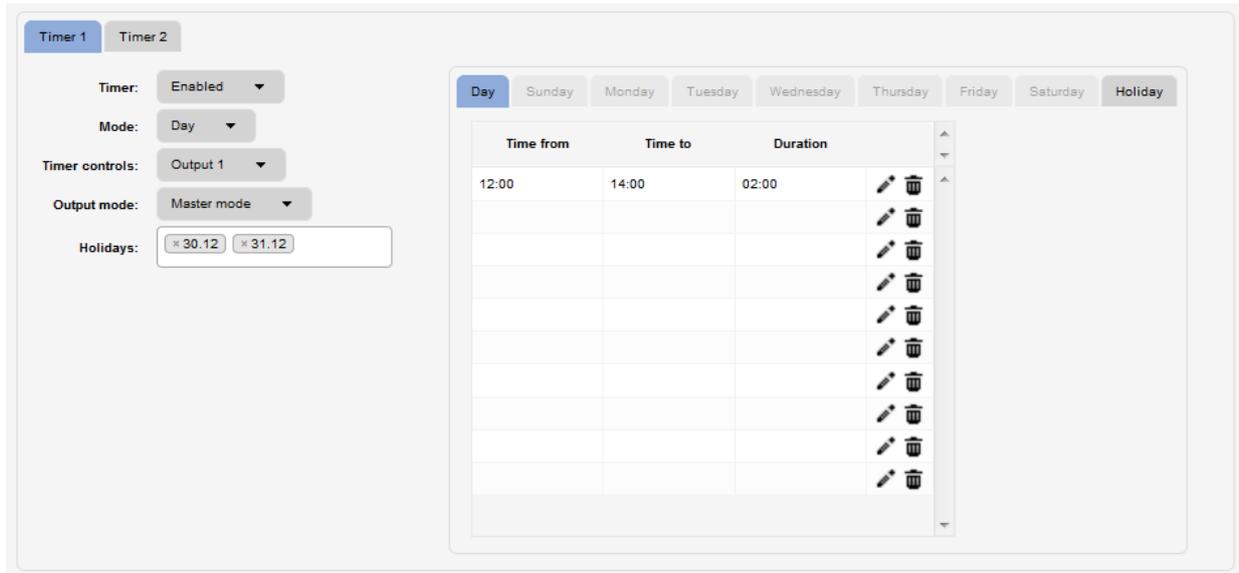


Figure 14: WEB Server-Timer setting →Day mode.

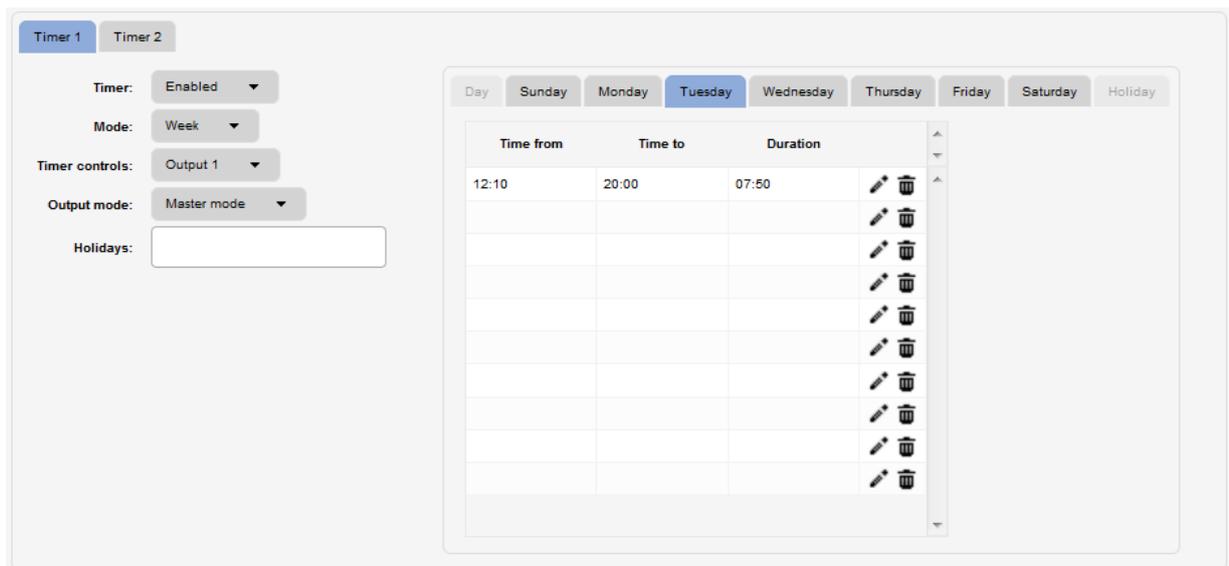


Figure 15: WEB Server-Timer setting →Week mode.

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 the timer will control on the day table which is the same for all week. In week mode the user can define diffent setting for each day in the week.
- **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 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.

8.10 ADMINISTRATION

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

Position	Phone number	User name	Input 1	Input 2	Periodic test	Low credit alert	Unauthorised call	Log full	Notify event	
1	8018285058		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
2			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

▼ General settings

Administrator allowed to remote program by SMS: Anyone

Automatic call to administrator 1: Period in days

Automatic periodic test SMS: Period in hours

Test SMS start hour:

Figure 16: WEB Server-Notification numbers

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



Figure 17: WEB Server-Input alarm configuration

- **Periodic test:** User can receive periodic (keep-alive) SMS, tick the check box for the appropriate user. Timer period is defined under parameter **Automatic periodic test SMS**, it is definable in hours.
- **Low credit alert:** In case of prepaid SIM card the unit can notify the user if the credit on the SIM card is low. To enable notification SMS tick the check box in corresponding position. Note that additional input in the **Misc** tab is needed to fully enable credit checking function.

- **Unauthorized call:** In case of unauthorized call the unit can notify user. To enable notification SMS tick the check box in corresponding position.
- **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 SOLO 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.

8.11 EVENT LOGGING

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

Event type	Time	User	Output	Extra info	Deleted
Caller id	07.11.2017 11:27:56	Ali	Output 1: ON		<input type="checkbox"/>
Caller id	05.11.2017 13:45:28	Ali	Output 1: ON		<input type="checkbox"/>
PIN access	02.11.2017 16:33:25	Latch	Output 2: OFF		<input type="checkbox"/>
PIN access	02.11.2017 16:25:37	Latch	Output 2: ON		<input type="checkbox"/>
Caller id	31.10.2017 18:49:59	Krissy	Output 1: ON		<input type="checkbox"/>
intercom	30.10.2017 18:49:44	Ali		8015563362	<input type="checkbox"/>
Caller id	29.10.2017	Ali	Output 1: ON		<input type="checkbox"/>

Figure 18: WEB Server-Log event

Each event is equipped with the event type, time, output if triggered and the user name of the user responsible for the event.

If user names are available (Called ID #, PIN codes, Intercom user ...) user name will be shown in the user column.

- **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 events.
- **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, Intercom, ...)

NOTE

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

8.12 MISCELLANEOUS

This tab is split into 2 sections.

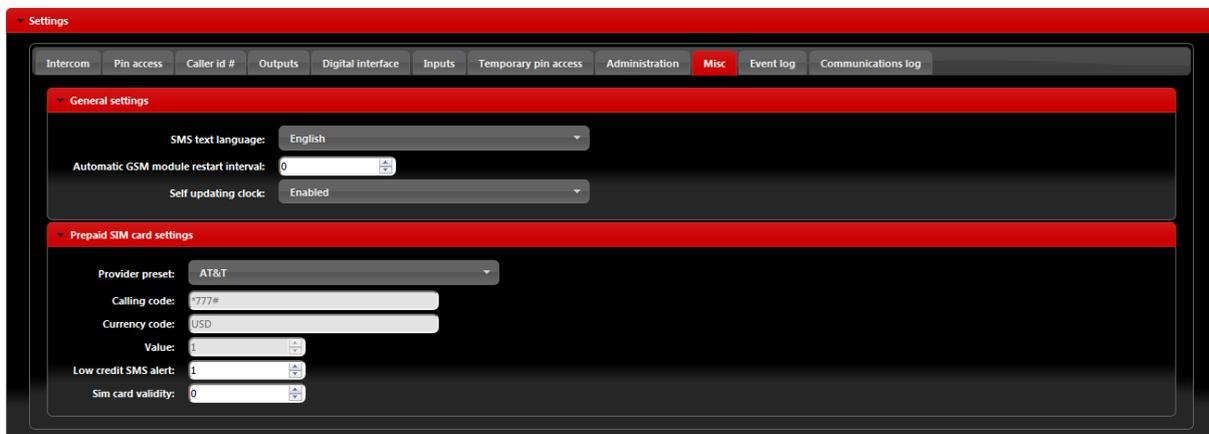


Figure 19: WEB Server-Misc

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**.

8.13 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.

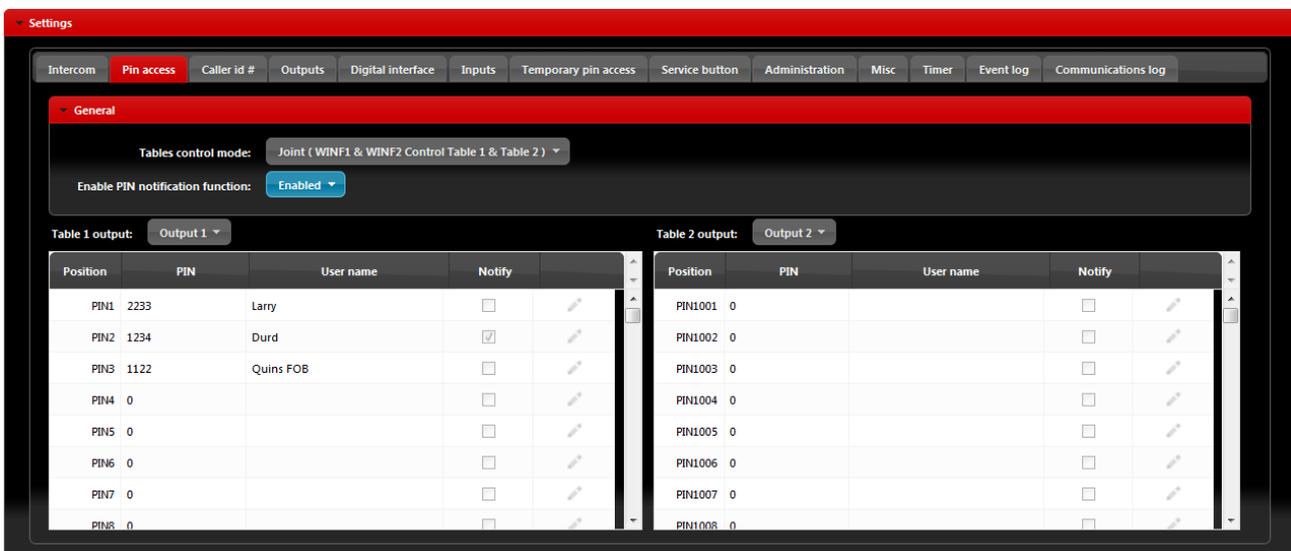


Figure 20: WEB Server-Global enabling of the notification function.

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.

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.

Position	Phone number	User name	Input 1	Input 2	Periodic test	Low credit alert	Unauthorised call	Log full	Notify event
1	8018285058		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
2			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

▼ General settings

Administrator allowed to remote program by SMS: Anyone ▼

Automatic call to administrator 1: Period in days

Automatic periodic test SMS: Period in hours

Test SMS start hour:

Figure 21: WEB Server-Selecting administrator numbers for notification.

9 WIEGAND INPUT DATA FORMATS

SOLO units support standard Wiegand interface, it will work with Wiegand 26bit and Wiegand 30bit protocol. On each Wiegand protocol SOLO 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.

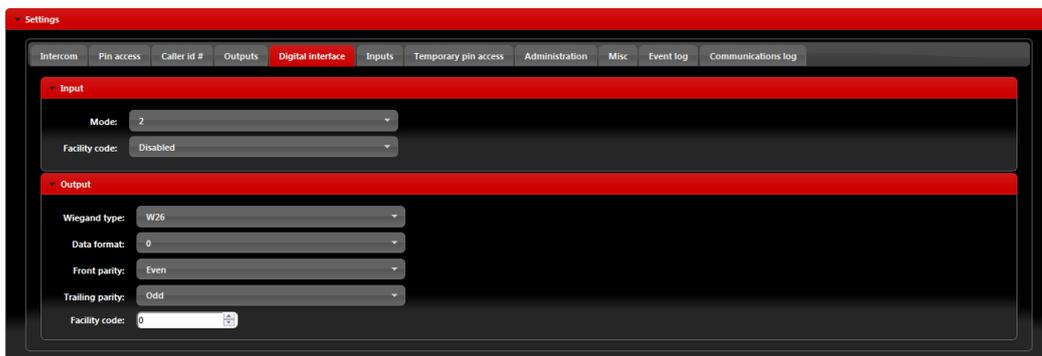


Figure 22: WEB Server-First Wiegand interface support.

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.

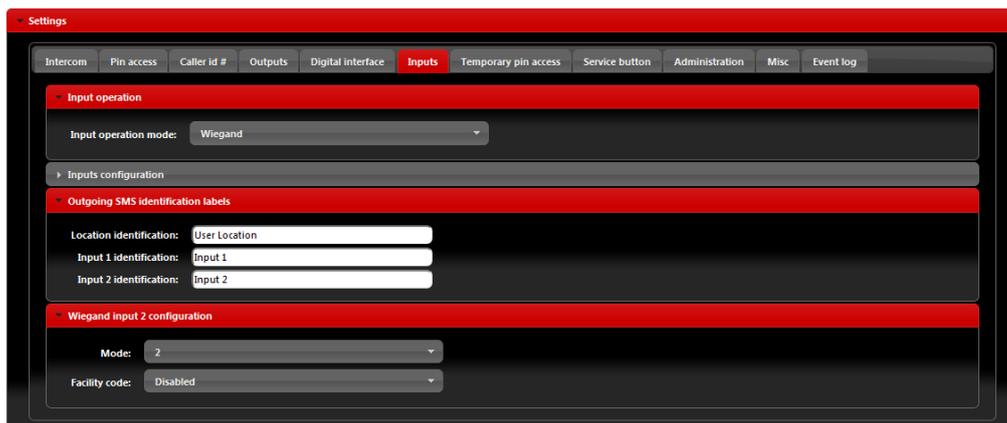


Figure 23: WEB Server-Second Wiegand interface support.

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	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	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	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	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	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	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	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	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	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	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.

10 CONTACTS

MARS COMMERCE d.o.o.

MIRKA VADNOVA 19
4000 KRANJ
SLOVENIA

TEL: 00 386 4 280 74 00

E-MAIL: info@mars-commerce.com

WEB SITE: www.mars-commerce.com

TEHNICAL SUPPORT

Tomaz HRIBAR

Email: tomaz@mars-commerce.com

SALES

Uros STARE

Email: sales@mars-commerce.com