Galaxy Gateway manual rev 1.4

1. Introduction

Galaxy Gateway produces an interface between Honeywell Galaxy line of intruder alarm panels. Since the panels do not expose all data over SIA4 control or RS485, a combination is needed to get all functionality.

A list of capabilities:

	RS485	SIA4
Zone states	X	X
Zone alarm states		X
Zone omit		X
Output states	X	X
Output control		X
RF detector states (RF portal)	X	
RF key fob states (RF portal)	X	
Group states		X
Group control		X
Group alarm states		X
Virtual keypad	X	
Virtual rio’s	X	
NTP time synchronisation		X
Device tampers	X	X
SIA3 reports		X
DCM and Max door states	X	
Card number	X	

States being retrieved over RS485 is limited to the bus line the module is connected to.

2. Compatibility

- Galaxy G3 series (V5.xx)
  - Control via onboard RS232 or E080
  - RS485 listening and emulation

- Galaxy Flex series (V1.xx)
  - Control via A080
  - RS485 listening and emulation

- Galaxy Flex (+) series (V3.xx)
  - Control via A083
  - RS485 listening and emulation

- Galaxy Dimension (V6.xx / V7.xx)
  - Control via onboard RS232 or E080
  - RS485 listening and emulation

- Galaxy G2 series
  - No control possible
  - RS485 listening and emulation

Panels	Int RS232	Eth	RF Portal	RF Rio	VKpd	VRio	Sia Control
Dimension	V	E080	V	V	V	V	V
Flex V3		A083	V		V	V	V
Flex V1		E080	V		V	V	V
G3	V	E080		V	V	V	V
G2			V		V	V	

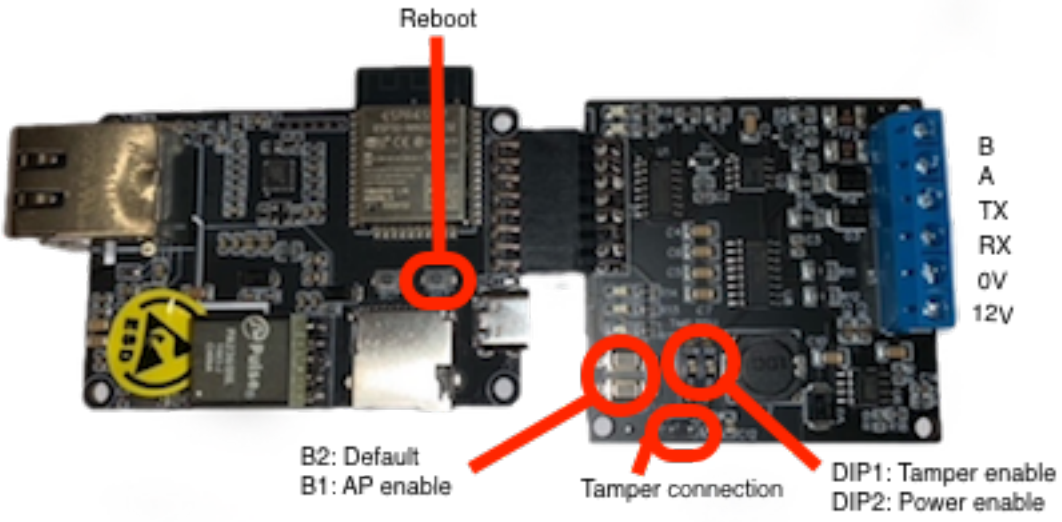
3. Installation

The module can be powered from either POE or from the Panel over a 12V supply next to the AB or AUX3 when available.

In order to use the onboard PSU to power the module set DIP2 to ON.

RS485 -> connect A on the module to A on the Galaxy
connect B on the module to B on the Galaxy

RS232 -> connect TX on the module to RX on the Galaxy
connect RX on the module to TX on the Galaxy



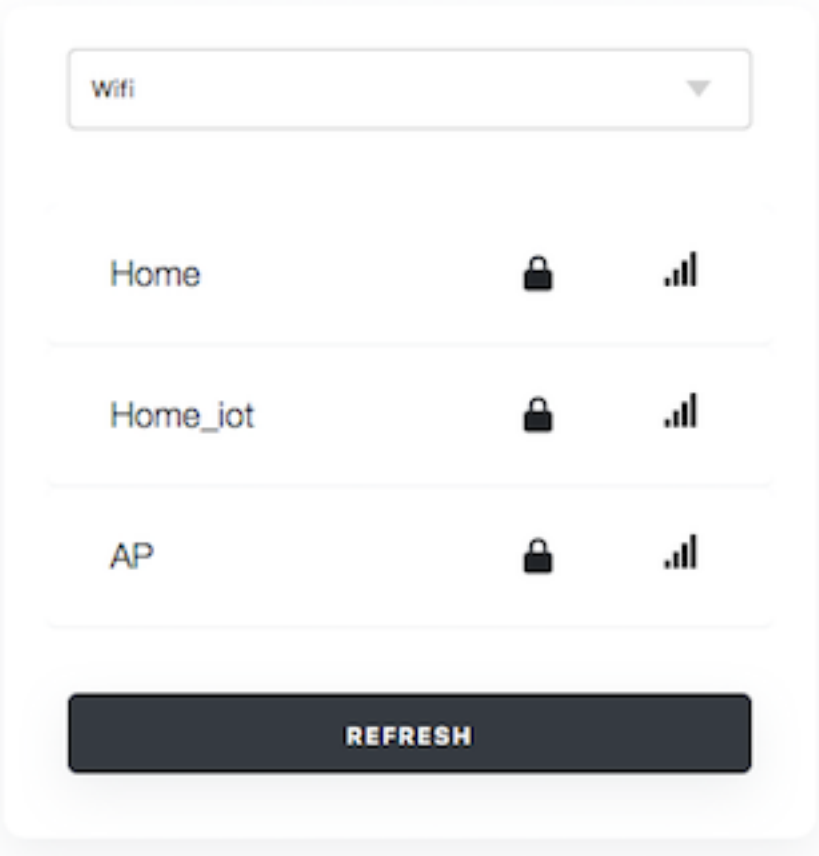
The onboard tamper connection can be enabled by disabling DIP1. This will enable the header pins and allow connection for an external tamper switch. The activation of the tamper switch results in the triggering of the tamper of a virtual keypad and is sent back to the panel and over MQTT as a device tamper.

POE is **not** recommended as when using RS485 virtual keypad or virtual rio emulation, if the module looses power, the panel will report missing components. **2 missing components results in a confirmed alarm!**

4. Configuration

On first bootup, the module opens up an access point (AP) to connect to for the initial configuration. This is a so-called Captive Portal. As soon as the wifi connection is established, the AP will close. To bring up the AP again, press the AP button on the module or connect to the telnet server and command the AP to be started from there.

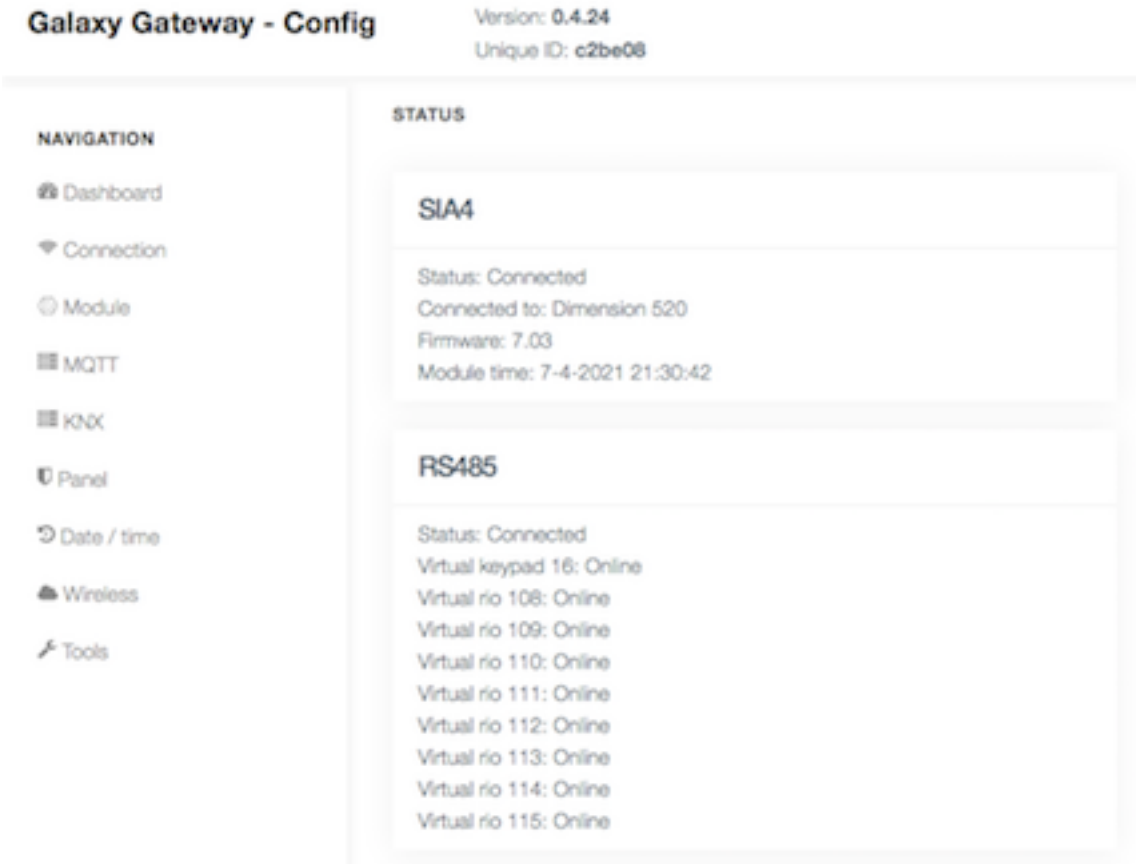
-> telnet “module ip”
-> ap start



The Captive Portal allows for primary setup of either Wifi or Lan connection. Upon selection of the interface, a choice for DHCP or Static IP assignment is presented. After saving the settings, the portal will close. Manually restart the module to start the actual configuration. A web interface is presented to do this on the IP address the module has received from DHCP or the Statically assigned IP address.

When Wifi is enabled, Lan is disabled and visa versa.

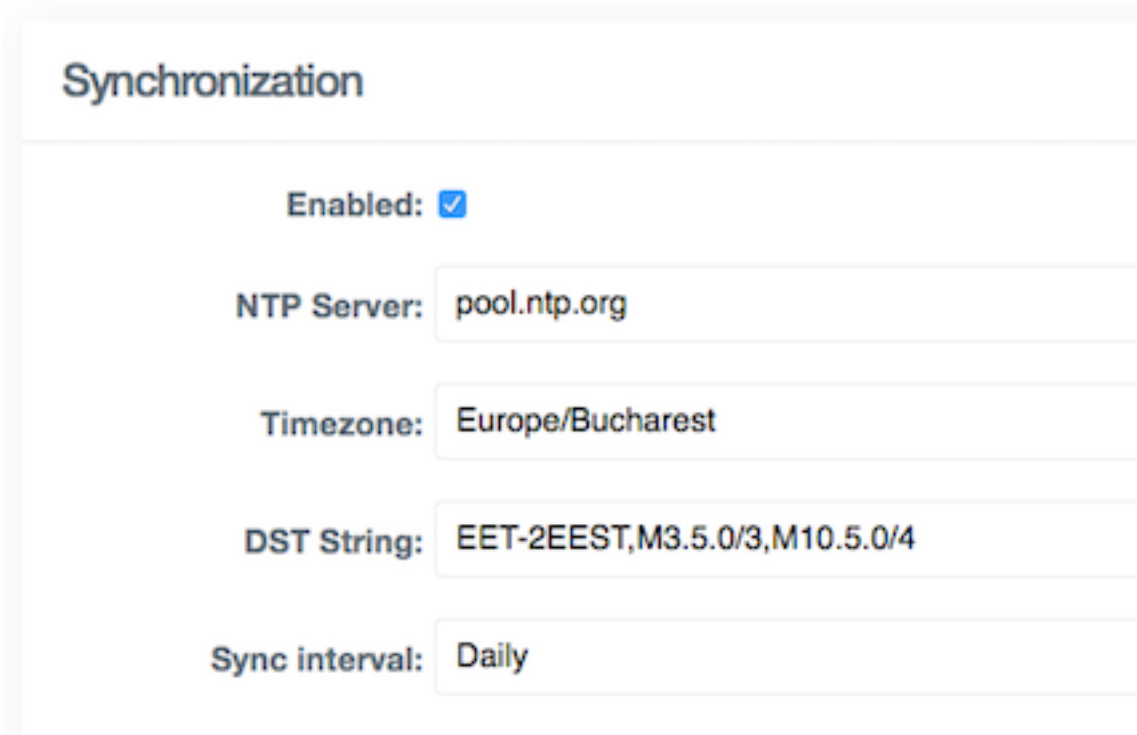
WARNING: BEFORE MAKING ADJUSTMENTS, IT IS ADVISED TO PUT THE PANEL IN ENGINEERING MODE



Since allot of the communication relies upon a unique id, both the firmware version and unique id is displayed in the web interface.

Various status columns display the status of the different connections and automatically update every 15 seconds together with the SIA3 Log.

- NTP
  When using SIA4 control with the panel, the option for NTP time synchronisation becomes available.



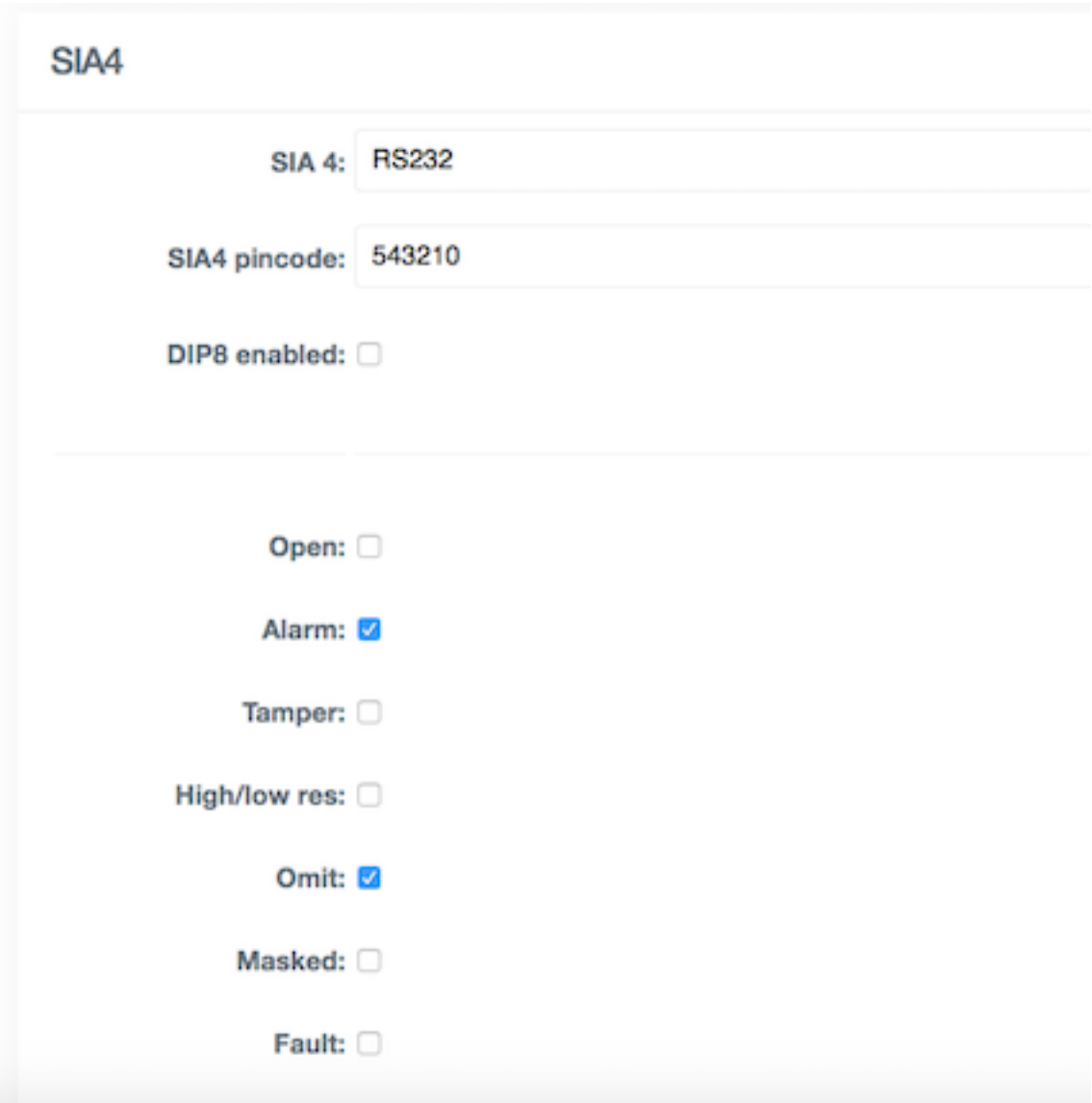
In order for the NTP server from the internet to work, a DNS IP address has to be configured. When using a local NTP server, the IP address for that can also be directly entered.

Choosing your timezone will automatically update the DST settings. Keep in mind that the DST settings will only be applied on the next synchronisation, not when the actual time has changed.

The sync interval allows control over how often the panel needs to be updated. The option “Forced” will not automatically do it, but instead needs to be manually executed via the telnet command “ntp”.

- SIA4 Control

  This allows the module to be setup to control the panel and retrieve bulk status updates for zones, outputs and groups.



The method allows you to switch between RS232 and IP. The SIA4 pincode is the “remote pin” setting for the galaxy panels. By default this is 543210 and can only be changed by using Remote Servicing Suite.

The DIP8 setting is only valid when the panel is a 264 or 520. Dipswitch 8 on main board allows for moving Rio1 on the main board to a virtual rio 0. If this is enabled, the data being pulled is different so if you have a 264 or 520, make sure the tick box is set accordingly.

Below that, you can control the amount of data that will be retrieved over SIA4. There is however a penalty to be paid, the more enabled, the slower the refreshes. Each tick box represents an additional query that needs to be sent.

The default should be good enough, but enable more / less as desired. By default a compound feedback is requested when “open” is not selected:

- 0 = closed / low res / high res
- 1 = open / tamper / masked / fault

When “open” is selected, it retrieves the true open
and closed state. Tampers, masked etc are not processed unless the extra options are selected.

By default only “alarms” and “omit” are ticked.

- RS485 enable
  When RS485 is enabled and connected, it allows for listening in events on the galaxy bus for increased speed of zone detection but also to emulate rio's and a keypad.

The DIP8 setting corresponds to the same DIP8 setting at SIA4 control. If the module was setup to connect over SIA4 to the panel and made a successful connection, it will pull the panel details and adjust the options available automatically.

Debounce is possible when both SIA4 and RS485 is enabled. In order to avoid duplicate openings and closings of zones, RS485 is given priority over SIA4 for zones that are available on both given the higher speed.

When SIA4 is not used, the panel type and size need to be set manually.

Selecting a keypad address will allow for a virtual keypad. Same as for the rio's. Multiple can be selected by holding the shift key.

Once selected, exit engineer mode on the panel for the additional modules to be recognised.

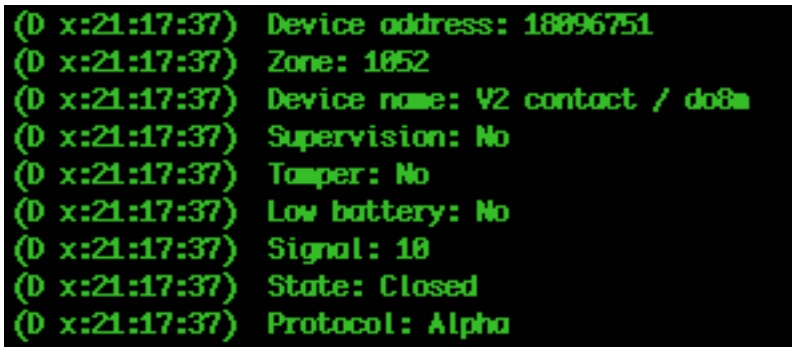
- RF Map

When the module is connected to RS485, it also exposed RF devices. By default, the RF statuses only get shown in the debugger over telnet. Because there's no relationship between a RF detector and a zone, we need to create one.

The serial numbers can either be filled in from the panel together with the zone number, or activate the detector and watch the debug output. Without a mapping, the detector status won't be used.

A mapping is not needed for RF key fobs. Those will automatically be added and sent over MQTT together with which button has been activated.

Below you can see an example of what it looks like in the telnet server.



Once mapped, all info is exposed over MQTT including attributes.

5. Panel configuration

Default ethernet sia control port is 10005 TCP
Default ethernet sia3 report port is 10002 TCP

G3 / Dimension - SIA4 control setup

- Internal RS232
  - 56.6.1 -> set the mode to direct
  - 56.6.2 -> set the format to SIA level 4
  - 56.6.4.1 -> set the baudrate to 57600
  - 56.6.4.2 -> set the databits to 8
  - 56.6.4.3 -> set the stopbits to 1
  - 56.6.4.4 -> set the parity to none

  in order to receive SIA3 reports as well:

  - 56.6.3 -> set the account to a 6 digit number

- Ethernet
  - 56.4.1 -> set the local ip details
  - 56.4.2.1 -> set the format to SIA level 4
  - 56.4.8.1 -> set the ip address of the module
  - 56.4.9.3 -> set the encryption for sia control to off

  in order to receive SIA3 reports as well:

  - 56.4.2.1 -> set the format to SIA level 3
  - 56.4.2.2 -> set the IP address of the module
  - 56.4.2.4 -> set the account to a 6 digit number
  - 56.4.2.8 -> set the protocol to tcp
  - 56.4.9.1 -> set the encryption for alarm report to off

  Or by using the alarm monitor

  - 56.4.2.1 -> set the format to SIA level 3
  - 56.4.2.8 -> set the protocol to tcp
  - 56.4.6.1 -> set the IP address of the module
  - 56.4.6.2 -> set the account to a 6 digit number
  - 56.4.9.1 -> set the encryption for alarm report to off

Flex V3 - SIA4 control setup

- Ethernet
  - 56.3.3 -> set the local ip details
  - 56.5.1.1.1.1 -> enable SIA4 IP any
  - 56.5.1.2.1.1 -> enable SIA4 Ethernet

  in order to receive SIA3 reports as well:

  - 56.1.1.1.4.1 -> set the IP address of the module
  - 56.1.1.1.4.2 -> set the format to SIA level 3
  - 56.1.2.1.1 -> set the account to a 6 digit number
  - 56.1.2.1.3 -> set the receiver order to 1
  - 56.3.3.5.1 -> set the encryption to off

Flex V1 - SIA4 control setup

- Ethernet
  - 56.4.1 -> set the local ip details
  - 56.4.2.1 -> set the format to SIA level 4
  - 56.4.8.1 -> set the IP address of the module

  in order to receive SIA3 reports as well:

  - 56.4.2.1 -> set the format to SIA level 3
  - 56.4.2.2 -> set the IP address of the module
  - 56.4.2.4 -> set the account to a 6 digit number
  - 56.4.2.8 -> set the protocol to tcp
  - 56.4.9.1 -> set the encryption for alarm report to off

  Or by using the alarm monitor

  - 56.4.2.1 -> set the format to SIA level 3
  - 56.4.2.8 -> set the protocol to tcp
  - 56.4.6.1 -> set the IP address of the module
  - 56.4.6.2 -> set the account to a 6 digit number
  - 56.4.9.1 -> set the encryption for alarm report to off

6. Telnet

By default, a telnet server is running on port 23 on the module allowing for debugging and remote control. Typing “?” will bring up the help menu.

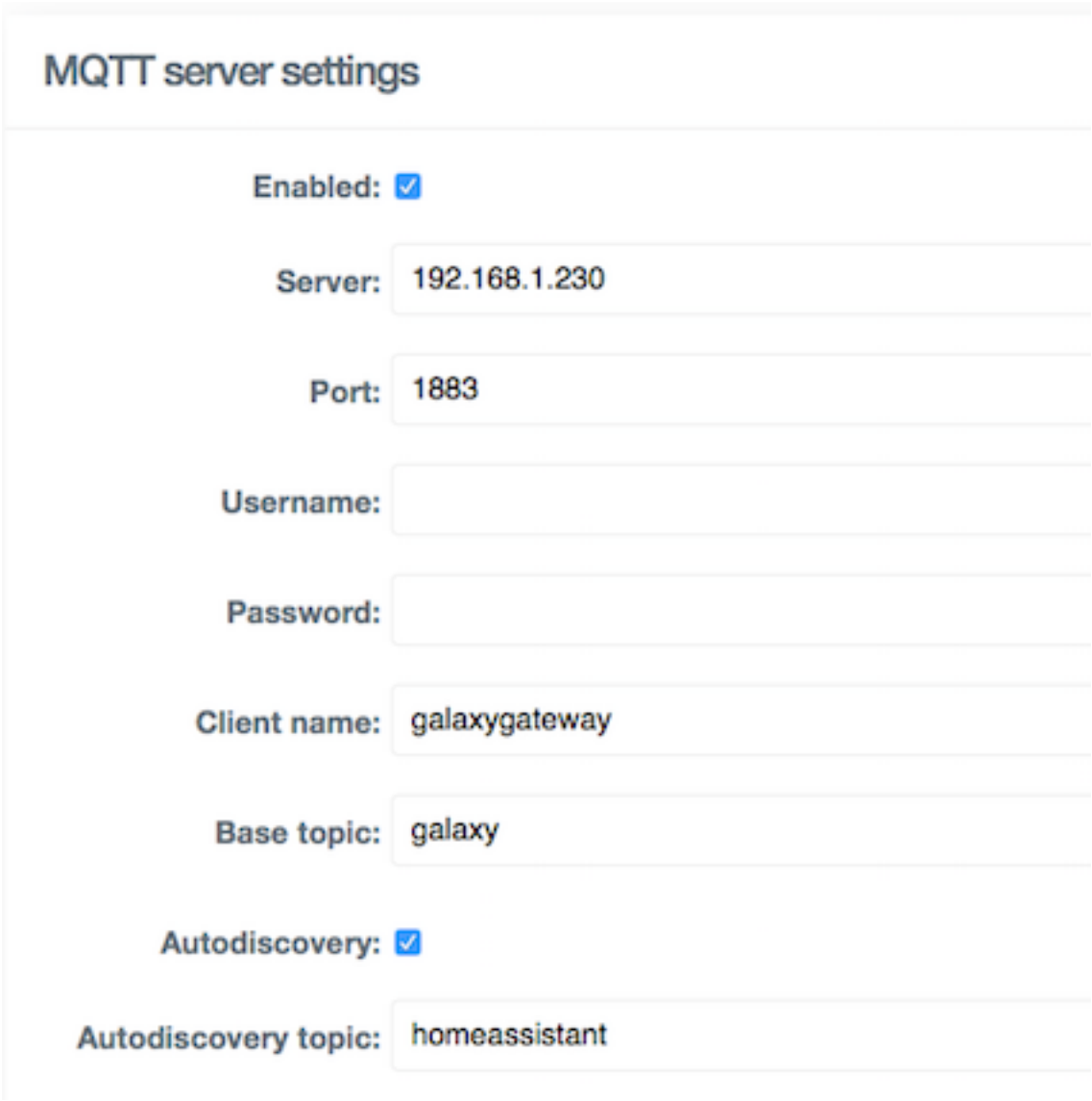
-> telnet “module ip”
    -> ?

Commands available:

- ver (displays module software version and unique id)
- flush (clears the registers)
- reload (bring stored configuration active)
- ntp (force nap update sync)
- sia (bring up latest 15 SIA3 reports received)
- ap (start / stop)
- autodiscovery (on / off)
- proxmax (convert prox number to max number)
- maxprox (convert max number to prox number)

7. MQTT

When MQTT is enabled, all gathered information is sent to a series of MQTT topics. In order to allow for multiple modules, a unique id is used which is automatically generated and visible in the AP portal and through telnet.



The client name is the name used to connect to a MQTT broker. Make sure this name is unique along the clients.

Autodiscovery is a feature that allows Home Assistant for example to automatically discover entities with all their properties. The Autodiscovery topic needs to be set to the topic where HA is listening to. See manual option 9 for more information about the integration.

The base topic by default is “galaxy” and the structure is as follows:

- galaxy/_UNIQUEID_/
  - device
    - state (online / offline)
    - version (version nr)
    - sia4 (online / offline)
    - rs485 (online / offline)
    - tamper (on / off)

  - zone/_ZONENR_/
    - state
      - 0 = closed
      - 1 = open
    - attr *(json string)*
      - tamper / masked / low-high res / fault / omit / alarm
    - **cmd**/omit
      - 0 = omit off
      - 1 = omit on
    - **cmd**/soak
      - 0 = soak off
      - 1 = soak on

  - output/_OUTPUTNR_/
    - state
      - 0 = off
      - 1 = on
    - **cmd**/set
      - 0 = off
      - 1 = on

- outputs/_OUTPUTFUNCTIONNR_/_GROUP_/
    - **cmd**/set
        - 0 = off
        - 1 = on

- group/_GROUP_/
    - state
        - 0 = unset,
        - 1 = full set
        - 2 = part set
        - 3 = ready to set
        - 4 = time locked
    - alarm
        - 0 = normal
        - 1 = alarm
        - 2 = reset required
    - **cmd**/set
        - 0 = unset
        - 1 = full set
        - 2 = part set
        - 3 = reset
        - 4 = abort set
        - 5 = forced set

- event/
    - state
        - timestamp
    - attr *(json string)*
        - date / time / event type / account / userid / text / device / code / area / nr

- keypad/
    - **cmd**/key
        - 0-9 and A-F
    - beep
    - setting
    - line1
    - line2

- rf/_SERIALNR_/
    - state
        - 0 = closed
        - 1 = open
    - attr *(json string)*
        - low batt / protocol / tamper / supervision / temperature / signal strength / rf button / pressed

- dcm/_DCMNR_/
    - state
        - 0 = closed
        - 1 = open
    - attr *(json string)*
        - cardnumber

- max/_MAXNR_/
    - state
        - 0 = closed
        - 1 = open
    - attr *(json string)*
        - cardnumber

To watch the MQTT topics, it's advised to use MQTT Explorer to connect to the broker.

Examples with abcdef as unique id:

To toggle output 1002 on:
galaxy/abcdef/output/1002/cmd/set = 1

To toggle all outputs in group A1 on:
galaxy/abcdef/outputs/0/A1/cmd/set = 1

To toggle PA outputs in group A1 off:
galaxy/abcdef/outputs/3/A1/cmd/set = 0

To send a full set command for A1 directly without exit time:
galaxy/abcdef/group/3/A1/cmd/set = 2

To send a full set command for A1 directly with exit time mimicking:
galaxy/abcdef/keypad/cmd/key = 1234A (pincode followed by A)

Group command possibilities:
At alarm state 0 and:
- state 0 -> cmd 5
- state 1 -> cmd 0
- state 2 -> cmd 0
- state 3 -> cmd 1 / 2
- state 4 -> No cmd possible

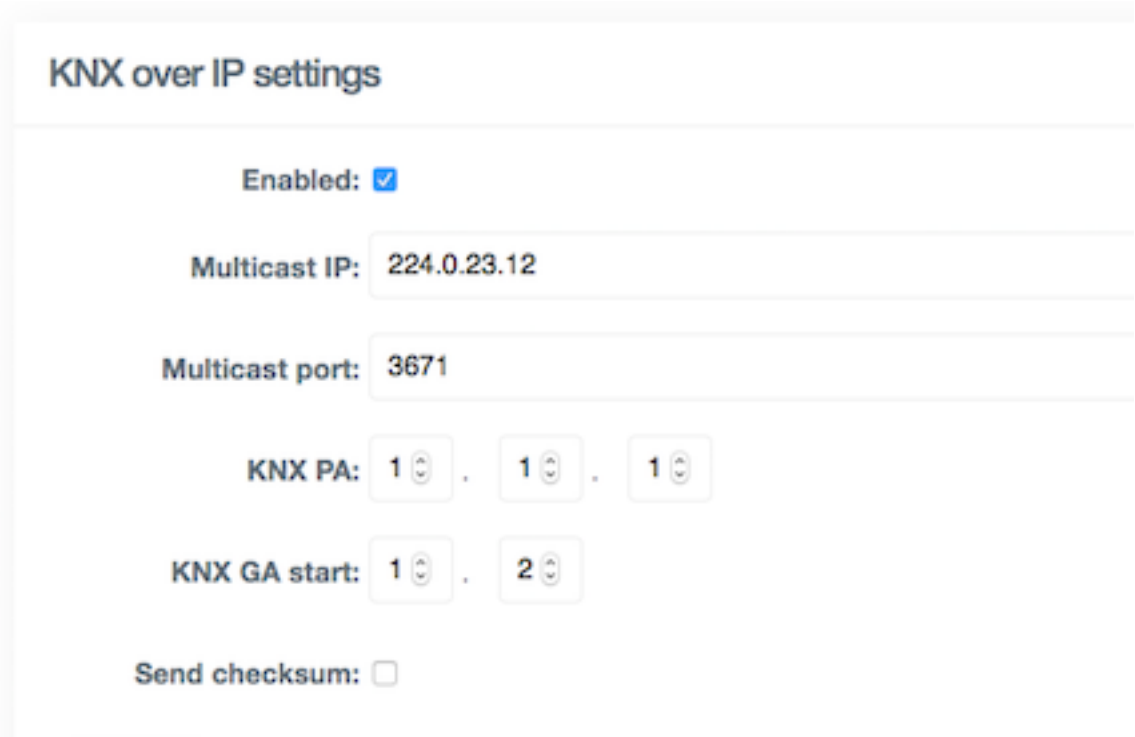
At alarm state 1 and:
- state 0 -> cmd 5
- state 1 -> cmd 0
- state 2 -> cmd 0
- state 3 -> cmd 1 / 2
- state 4 -> cmd 0

At alarm state 2 and:
- state 0 -> cmd 3 / 5
- state 1 -> cmd 3 / 0
- state 2 -> cmd 3 / 0
- state 3 -> cmd 3 / 1 / 2
- state 4 -> cmd 3

8. KNX

The module offers KNX status events to be sent via IP over UDP. The broadcast IP and port can be changed if needed.

The PA and GA can be set in the web interface. Based on the GA selected, zone, output and group addresses are set automatically like this with a GA set to 1.2:



The GA is used to construct the below table:

	KNX addr	*DPT*	*R/W*	*Description*
				Module status
1	a/b/ 0	DPT 1	R	0 = offline, 1 = online
				Panel status
2	a/b/ 1	DPT 1	R	0 = offline, 1 = online
				Group status / toggle
3	a/b/ 16-47	DPT 5	R/W	Read: 0 = Unset 1 = Set 2 = Part set 3 = Ready to set 4 = Time lock Write: 0 = Unset 1 = Set 2 = Part set 3 = Force set 4 = Reset
				Group alarm status
4	a/b/ 48-71	DPT 5	R	0 = Normal 1 = Alarm 2 = Reset required
				DCM door status
5	a/b/ 72-135	DPT 1	R	0 = closed, 1 = open
				MAX door status
6	a/b/ 136-167	DPT 1	R	0 = closed, 1 = open
				Header outputs
7	a/b/ 168-173	DPT 1	R/W	0 = off, 1 = on
				DIP8 ON - Outputs 0011 - 0014
8	a/b/ 174-179	DPT 1	R/W	0 = off, 1 = on
				DIP8 ON - Zones 0011 - 0014
9	a/b/ 180-187	DPT 5	R	Bit 1 = Closed / Open Bit 2 = Alarm Bit 3 = Tamper Bit 4 = Omit Bit 5 = Masked Bit 6 = Fault Bit 7 = High / low res

				Rio outputs
10	a/b +1/ 0-255	DPT 1	R/W	0 = off, 1 = on
				Rio zones 1001 - 2158
11	a/b +2/ 0-255	DPT 5	R	Bit 1 = Closed / Open Bit 2 = Alarm Bit 3 = Tamper Bit 4 = Omit Bit 5 = Masked Bit 6 = Fault Bit 7 = High / low res
				Rio zones 3001 - 4158
12	a/b +3/ 0-255	DPT 5	R	Bit 1 = Closed / Open Bit 2 = Alarm Bit 3 = Tamper Bit 4 = Omit Bit 5 = Masked Bit 6 = Fault Bit 7 = High / low res

9. Modbus

Modbus is currently under development. Both TCP and RTU are supported. RTU wil disable the Galaxy RS485.

			uint16_t	
FC01	Output nr	1-266	0/1	R
FC03	Group	1-32	0-4	R
	Group alarm	33-64	0-2	R
FC04	Zone open	1-520	0/1	R
	Zone alarm	521-1040	0/1	R
	Zone tamper	1041-1560	0/1	R
	Zone omit	1561-2080	0/1	R
	Zone mask	2081-2600	0/1	R
	Zone fault	2601-3120	0/1	R
	Zone res	3121-3640	0/1	R
	Max status	3641-3648	0/1	R
	Dcm status	3649-4664	0/1	R

FC05	Output nr	1-266	0/1	W
FC06	Group	1-32	0-5	W
	Output func 0	33-64	0-96	W
	Output func 1	65-96	0-96	W

FC06 output func is used to set all outputs configured as the specified function number. See the galaxy installation manual for a list of output functions and their corresponding number. 33-64 indicates the group to which the outputs belong.

For example: FC06 : 33 : 1 will turn on all bells outputs in group A1.
FC06 : 41 : 16 will turn on all fire outputs in group B1.
FC06 : 65 : 1 will turn off all bells outputs in group A1.

10. Integration

Currently a full integration with Home Assistant has been realised. The easiest way is to enable MQTT auto discovery. This will push all available topics to the discovery topic “homeassistant”. Make sure HA is setup to use the discovery topic.

```yaml
mqtt:
  broker: 127.0.0.1
  birth_message:
    topic: 'homeassistant/status'
    payload: 'online'
  will_message:
    topic: 'homeassistant/status'
    payload: 'offline'
  discovery: true
  discovery_prefix: homeassistant
```

Once done, enable the MQTT auto discovery through the telnet or web interface.

-> telnet “module ip”
    -> auto discovery on

Once it finishes, you should see all entities available in the entity registry of HA.

The module is also subscribing to the last will message so that when HA comes online, the registers are flushed and new statuses will be pushed.

RF buttons and detectors will be pushed as soon as they are seen based on their serial number.

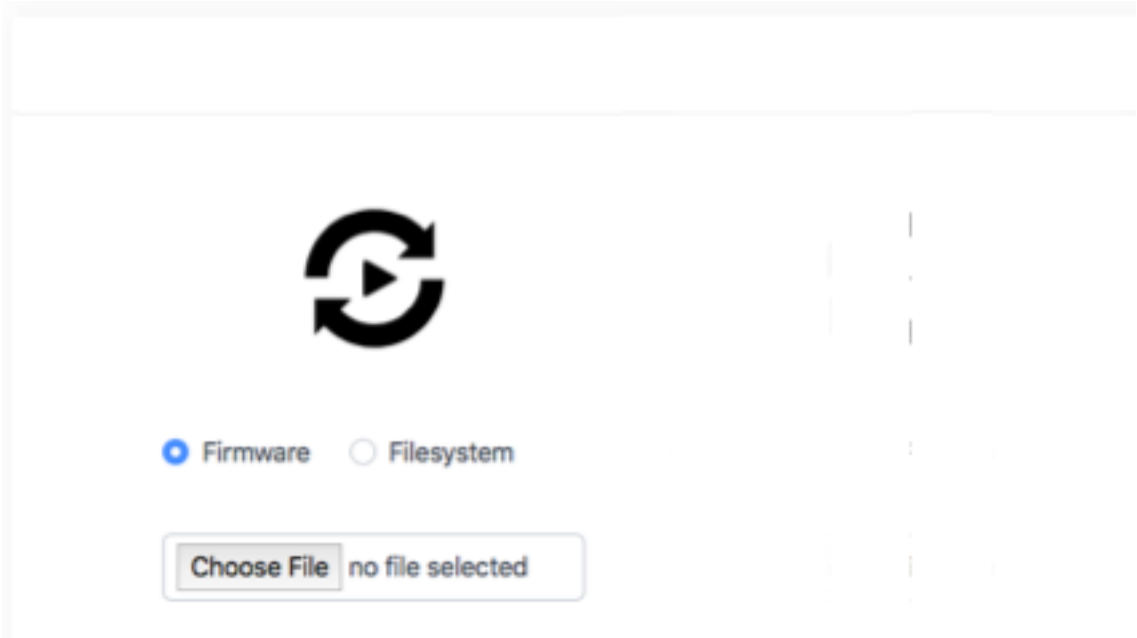
A card is available for both the virtual keypad and group management from https://seasoft.nl/downloads

11. Updating

To update the firmware of the module it is advisable to put the panel in engineer mode prior to doing so. The firmware consists of 2 parts, a bin file which is the actual firmware and a littlefs.bin file which contains the filesystem.

- Through the web interface -> Tools

WARNING: BEFORE UPDATING, YOU MUST PUT THE PANEL IN ENGINEERING MODE, THE UPDATE PROCESS WILL INTERFERE WITH RS485 WHEN USING A VIRTUAL KEYPAD OR RIO.



12. Resetting the module

In the event the module becomes unresponsive or otherwise doesn't do what it should do, there are 2 options to bring it back to life:

1. Pressing the reset switch for 2 seconds on the extension module while the module is powered up will flush the stored settings and upon reboot, fires up the Captive Portal for a new network configuration. When done, the web interface will come back for further configuration.

2. Pressing the reset switch while powering up the module will do a more critical erase of all settings and wipe the filesystem. To a factory default. This will do a reboot as well and bring up the Captive portal. However when done with the network configuration, because the filesystem is wiped, there is no web interface yet. Open up http://moduleip/update to upload the littlefs.bin file again. Once done, the web interface is back up and running allowing the rest of the configuration.

13. Worth knowing

Since the module exposes functionality that allows for remote arming / disarming of the panel, be careful with MQTT access to the outside world and it strongly advised to use a username / password and to remove anonymous access. Check your MQTT broker documentation on how to do this.

Driving outputs on the panel requires some attention. The galaxy panels offer a way to change the output polarity of an output in menu 53 from the default POS to NEG. The outputs can handle more current when pulling the output to negative then they can when feeding a positive 12+. Normal driving setup is by taking a fixed +12V from a feed (RS485 / AUX3 / +12V connection next to zones) and a negative from a rio output. When the default polarity is set to POS, when the output activate and pulls the output to 0V allowing whatever it is connected to be driven. There is no way to detect for the module what the polarity setting on the panel is! Which means that those outputs that are configured with a default polarity as NEG, need to be driven in reverse order for proper operation. For example:

To ACTIVATE output 1011 with polarity set to POS you would send:
galaxy/abcdef/output/1011/cmd/set = 1

To ACTIVATE output 1011 with polarity set to NEG you would send:
galaxy/abcdef/output/1011/cmd/set = 0

If your panel is being monitored and or is certified,
consult your alarm installation company!

14. Technical details

Input voltage range: 5V - 26V DC

Current draw powered @ 13.8V:
Peak: 210mA
AP mode: 44mA
Wifi connected: 21mA

Dimensions: 14cm x 6cm