SelfMon

Virtualisation Module

Galaxy Flex, Flex+, Dimension, G3, Classic & G2 Control Panels

Installation &Setup Manual

Document Version V0.30 - Module Firmware V1.21.106 - SelfMon Ltd

Contents

Module description

The SelfMon Virtual Module is a low-cost bus-based RS485 module that combines multiple virtualised peripherals along with an HTTP server and MQTT clients. This enables two-way MQTT communication with the Honeywell Galaxy range of control panels. Table 1 provides an overview of the functionality. The module has an ARM Cortex-M4F processor with 512k flash, 256k of RAM and an NVRAM for settings storage. Connection to the control panel is achieved via onboard Molex 4-way header using a flying lead or via 4 screw terminals with standard alarm cable.

Table 1

Control Panel	Zone Status	Virtual Keypad (iii)	RSS (iv)	GX App (iv)	SelfMon App (iv)	SelfMon Reporting	Virtual RIO (v)	Virtual E080 (vi)	Virtual Printer	Virtual RF Portal
Galaxy Dimension	✓ (i)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Galaxy Flex+ (V3)	✓ (i)	✓	×	×	×	×	✓	×	✓	✓
Galaxy Flex (V3)	✓ (i)	✓	×	×	×	×	✓	×	✓	✓
Galaxy Flex (V1)	✓ (i)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Galaxy G3	✓ (i)	✓	✓	×	✓	✓	✓	✓	✓	✓
Galaxy Classic	✓ (ii)	✓	✓	×	✓	✓	✓	✓	✓	✓
Galaxy G2	✓ (ii)	✓	✓	×	✓	✓	✓	✓	✓	✓
Galaxy 8/16+	×	✓	×	×	×	×	×	×	✓	×

(i) The module will read zone status in any system setting state from any physical RIOs located on the RS485 bus enabled in read-only mode. Onboard zones, along with other zones may also be read using SIA4 in conjunction with a Honeywell Ethernet module - or for Dimension and G3 panels when the virtualised E080 is set to SIA zone and group mode.

(ii) Only zones from physical RIOs are located on the RS485 bus and enabled in read-only mode.

(iii) The virtual keypad is available via HTTP and MQTT. The MQTT keypad has a two-way topic path mechanism, where an input single or multi-key sequence may be submitted. Note that on the G2 series, the module must consume one of the 4 keypad slots.

(iv) Capability is available via port 10001 when E080 module emulation is enabled. It is recommended that Keypad 15 is enabled in conjunction with the E080 emulation, as Keypad 15 enables remote user access (default code 543210).

(v) Virtual RIOs may be enabled depending on the connected bus and panel capability. Each virtual RIO enables 8 inputs and 4 outputs. The inputs can then be set using MQTT. The output status is driven by the control panel and may be subscribed to in MQTT.

(vi) The virtualised E080 module enables the replacement of any existing E080 module, supporting encrypted RSS, GX and SelfMon apps as well as polled path self-monitoring with the SelfMon platform. SIA port 10005 is not provided, but SIA zone and group can be enabled for onboard zone and group status.

Module installation

The module must be installed on the RS485 Galaxy bus. The module may co-exist with existing Ethernet modules, RIOs and RF portals, but internal virtualised addresses must be disabled or set to read-only (using the settings page detailed in the ‘module configuration’ section) so that the virtual module does not attempt to write at the same time as the physical devices. The module PCB is keyed so that it can be fitted in the Flex plastic enclosure module slots. For metal enclosures, adhesive standoffs are supplied for surface mounting. Please ensure that a 15mm gap is maintained between the module edge and the enclosure, as the panel lid fits inside the metal casing.

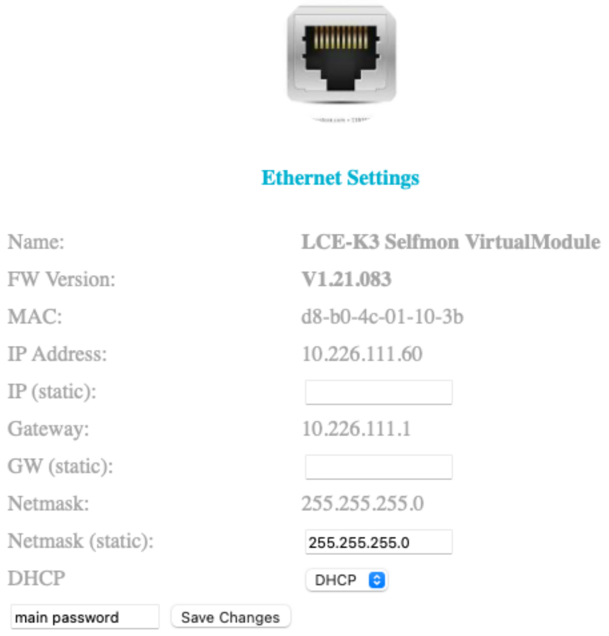
A flying lead is supplied to allow quick connection to the control panel. The connection may be made by inserting the stripped wire ends into the module and plugging them into the RS485 header on the control panel (The colour coding of the flying lead wires is shown on a label inside the module shipping packet). Where a control panel has multiple bus connections, the lowest number should be selected. If further expansion is required (Dimension 96, 264 and 520 panels), additional modules may be added to each bus. Where multiple modules are fitted, they may be subscribed individually using the unique 6-digit vmod address. In this case, each module will be assigned its own DHCP address and require configuration using the individual settings web page.

Module configuration

When the module boots, the virtual keypad is served from port 80. The module settings page is available at http://ip.addr/settings.shtm (where ip.addr is the module DHCP assigned address)

Network connection

When connected to your Ethernet network and control panel, the module will default to DHCP networking. This will require that a DHCP server is available on the network to assign an IP address to the module. It is advisable to set a permanent lease to the module MAC address. A future update will allow a static address to be assigned via menu or control panel Ethernet module settings. You can switch to a static address by modifying the DHCP option and manually entering addresses. Ensure that your router is not set to allocate any static address that you select.



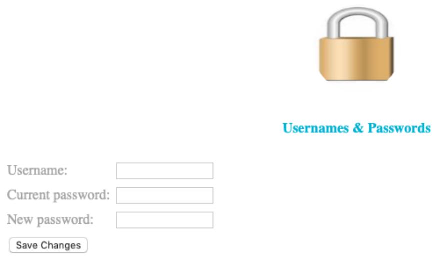
Ethernet Settings

Name:	**LCE-K3 Selfmon VirtualModule**
FW Version:	**V1.21.083**
MAC:	d8-b0-4c-01-10-3b
IP Address:	10.226.111.60
IP (static):	
Gateway:	10.226.111.1
GW (static):	
Netmask:	255.255.255.0
Netmask (static):	255.255.255.0
DHCP	DHCP

Figure 1 – Network settings

System password

The system user is “**admin**”, and the initial password is set to “**thisisatdefault**”. This should be changed as a first step when the module is connected to the local network. To change the password, the username and initial (current) password must be provided along with the new password.



Usernames & Passwords

Username:
Current password:
New password:

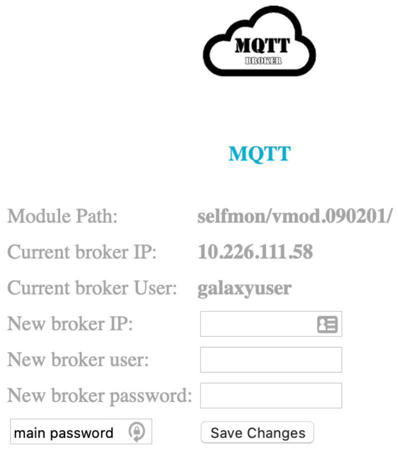
Figure 2 – Changing the default password

MQTT client

The module implements an MQTT client for connection to a compliant MQTT broker/server. The module settings page located at http://ip.addr/settings.shtm (where ip.addr is the DHCP assigned address) includes a section for configuration of the client username and password. The broker IP address, client username and client password should be entered along with the main module password (default '**thisisatdefault**')

Note that the MQTT client does not currently include TLS encryption, so the broker should remain local until an encrypted release is made available. The **user** and **broker password** fields **MUST** be populated for the MQTT client to initialise a connection. Note that the username requirement is between **4 and 15** characters in length, and the password is between **7 and 15** characters.

The main system password must be entered along with any updates in order that they are accepted and stored. The module will publish on the module path: *selfmon/vmod.AABBCC* where *AABBCC* is the last three octets of the unique module MAC address.

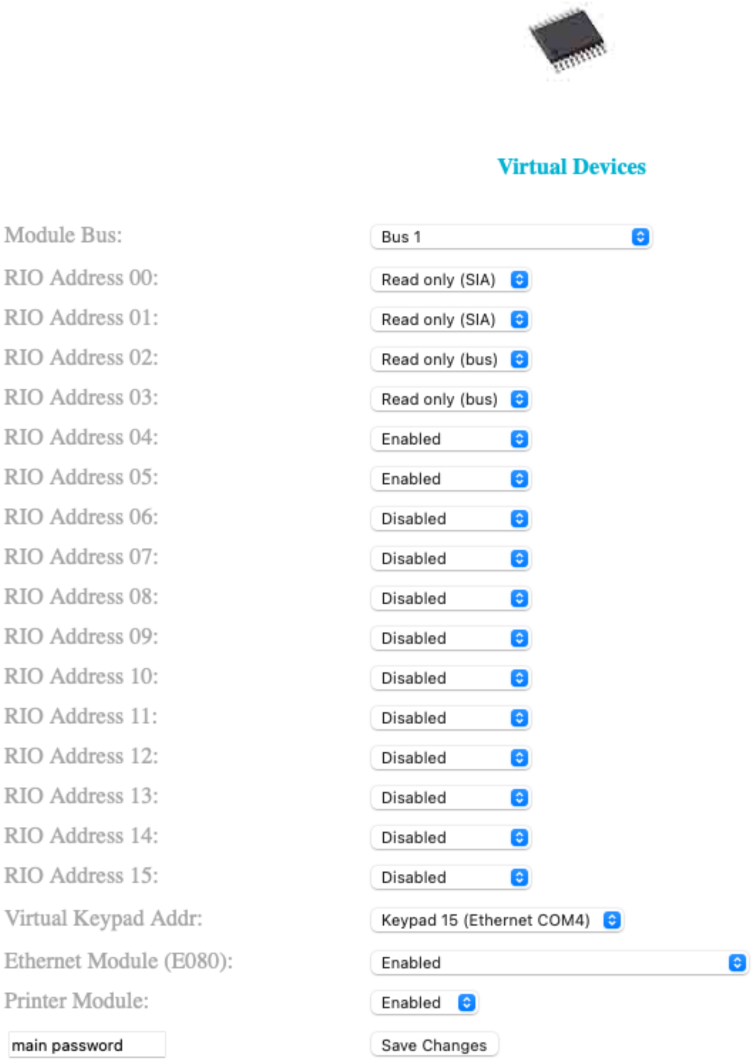


MQTT

Module Path: selfmon/vmod.090201/
Current broker IP: 10.226.111.58
Current broker User: galaxyuser
New broker IP:
New broker user:
New broker password:

Figure 3 - MQTT Settings

Virtual device state



Virtual Devices

Module Bus:	Bus 1
RIO Address 00:	Read only (SIA)
RIO Address 01:	Read only (SIA)
RIO Address 02:	Read only (bus)
RIO Address 03:	Read only (bus)
RIO Address 04:	Enabled
RIO Address 05:	Enabled
RIO Address 06:	Disabled
RIO Address 07:	Disabled
RIO Address 08:	Disabled
RIO Address 09:	Disabled
RIO Address 10:	Disabled
RIO Address 11:	Disabled
RIO Address 12:	Disabled
RIO Address 13:	Disabled
RIO Address 14:	Disabled
RIO Address 15:	Disabled
Virtual Keypad Addr:	Keypad 15 (Ethernet COM4)
Ethernet Module (E080):	Enabled
Printer Module:	Enabled
main password	Save Changes

Figure 4 – Virtual device state

WARNING: *If you have physical RIOs fitted to the same control panel bus as the module, you MUST ensure that the address of the physical device is set to Read Only in the virtual module. If you neglect this setting, the module will override the physical RIO zones to a permanent CLOSED state.*

The ‘Module Bus’ option changes the MQTT zone paths. If you fit the module, or multiple modules on Galaxy Dimension 96, 264 or 520 panels, this option will ensure that the zone numbers align with the bus that the module is attached to.

Each virtual device may be enabled, set to read-only (bus or SIA), or disabled.

The device states are explained as follows:

- **Enabled :** The device will consume an address on the RS485 bus and appear as a logical device when scanned during the Galaxy engineering escape sequence.
- **Read only (bus):** The device will not consume an address, but output and input

state information for any existing **external physical bus device** at that address will be forwarded to MQTT.

- **Read only (SIA):** The device will not consume an address, but output and input state information for any existing physical device at that address will be read using SIA4 and forwarded to MQTT. Note that this currently requires either a Honeywell Ethernet module to be fitted and configured for SIA4 commands (please see SIA4 integration for configuration requirements) or the virtualised E080 set to '*enabled with SIA zone and group*'.
- **Disabled :** The module will not read or respond to any traffic at that device address and no information will be forwarded to MQTT.

The virtual keypad address may be assigned based depending on the control panel connected. Engineering keypad 19 is always configured to the bus and as it's the module default, it will always appear on connection without bus scanning.

When E080 is fitted or E080 emulation is enabled, then Keypad 15 (Ethernet) enables the '**remote**' user to log in (default pin code 543210). This special user can log into the system without impacting the system set state. The user has engineer type privileges to reset faults and change system configuration. Keypad 3 is suggested for use with the G2 (where only keypad addresses 0 to 3 are available). Note that if you have a virtual keypad on the address, you cannot add a physical keypad on that same address.

MQTT publishing and callback

Note that green text denotes topics that are published for the module to process. All other topics are published by the module for MQTT topic subscribers.

Module version, heartbeat & last will

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/version	V1.XX.YYY	The module firmware version string will be published for the first ten heartbeat signals. YYY denotes beta releases.
selfmon/vmod.xxxxxx/heartbeat	disconnected or displaying counter / debug	The last will is set to enable the broker to display 'disconnected' if the client goes offline. The debug information displays a counter incrementing at around 5 second intervals concurrent with the green LED flash rate.
selfmon/vmod.xxxxxx/temperature	Temp Celsius	The core temp of the module. Spec max is 90.

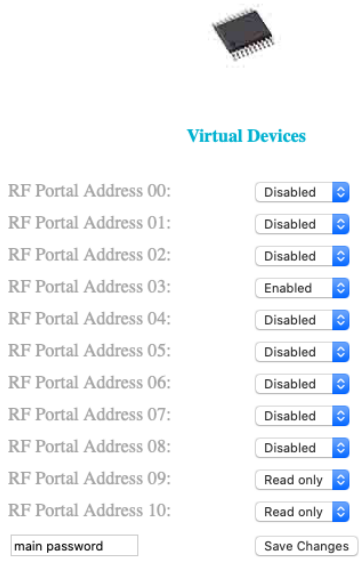
Administration commands

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/cmd/mac/00332211 where 33 is the last byte.	NA	Used in manufacturing one time MAC address programming – not for general use
selfmon/vmod.xxxxxx/cmd/setdefaults	NA	Set module defaults via MQTT

Virtual keypad control

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/vkp/display/line1 selfmon/vmod.xxxxxx/vkp/display/line2	Keypad display lines 1 & 2	Two strings of up to 16 characters that mimic the keypad display.
selfmon/vmod.xxxxxx/vkp/key	Comma separated key sequence	Raw payload can be input as each key individually or sequenced if separated by comma. The letter E is mapped for 'ent' and X is mapped to 'esc' keys. Multiple keys may be processed in sequence if separated by a comma. Eg. 1,1,2,2,3,3,E will enter with the default engineer code. 1,2,3,4,5,A will fully set the system. Keys 0,1,2,3,4,5,6,7,8,9,A,B,*,#,E,X are allowed.

Virtual RF portal control



Virtual Devices

RF Portal Address 00:	Disabled
RF Portal Address 01:	Disabled
RF Portal Address 02:	Disabled
RF Portal Address 03:	Enabled
RF Portal Address 04:	Disabled
RF Portal Address 05:	Disabled
RF Portal Address 06:	Disabled
RF Portal Address 07:	Disabled
RF Portal Address 08:	Disabled
RF Portal Address 09:	Read only
RF Portal Address 10:	Read only
main password	Save Changes

Figure 5 – RF Portal virtual device state

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/vportal/write/1YY Where devices are enabled in the module config page. Where YY is 00 to 10. ***Note that only one free vportal address needs to be enabled. Other addresses, where portals are fitted, can remain in read-only mode, or be left as disabled.*** ***Do not confuse RF portal addresses with the virtual RIO devices that RF portal devices support themselves. Control for these devices is at menu 51.60 and they may be disabled if vmod RIO address slots are required.***	12345,full 12345,unset 12345,part 12345,night	For virtualised RF portals, you can enter a fob serial number (add to menu 42.X.12). Then publish the serial number with comma, then command. Note that night set is available on Flex panels only. For bus 2, you can enter 205 Etc. The serial number must match the user number. After enabling the vportal, you may need to initially publish command two times to synchronise the serial number.
selfmon/vmod.xxxxxx/pportal/105/alpha/yyyyy selfmon/vmod.xxxxxx/pportal/105/v2/yyyyy Where RF portal devices are present in the system and read-only in the module config page. Devices transmitting in V2 or Alpha will publish on the relevant topic path.	Where yyyyy is the received serial number. The payload is the transmission word in decimal.	The physical RF portals enabled in read only mode will publish device data when RF devices transmit. Each device has a unique serial number. You will need to determine the payload meaning Eg. 6 = closed for a contact and 70 = open. Note that you may pick up your neighbours sensors if they have a Honeywell based Evohome or Galaxy wireless devices.

Zone status change

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/**prio**/inputs/read/XXXX	OPEN or CLOSED	The ‘prio’ physical RIO path will show any external RIO (on the same bus as the virtual module and programmed as read-only. If the RIO is in read only mode, this status will be the state of the hardware RIO being monitored. Note that onboard zones can only be read by enabling SIA4 (see SIA4 section).
selfmon/vmod.xxxxxx/**vrio**/inputs/read/XXXX	OPEN or CLOSED	Read the state of virtual ‘vrio’ zone XXXX where XXXX is the zone number Eg. 1021 to 1148.
selfmon/vmod.xxxxxx/**vrio**/inputs/write/XXXX	OPEN or CLOSED alternatively ON and OFF.	Change the state of a virtual zone. This state change will be picked up the control panel and may be programmed with a zone function.

Output status change

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/**prio**/outputs/YYYY	ON or OFF	Read the state of ‘prio’ physical RIO output YYYY where YYYY is the output number Eg. 1021 to 1124. Outputs are driven by the control panel and may be used to relay zone status or provide programmable output state. Only external RIO’s on the same bus as the virtual module may be read.
selfmon/vmod.xxxxxx/**vrio**/outputs/YYYY	ON or OFF	Read the state of ‘vrio’ vitual output YYYY where YYYY is the output number Eg. 1021 to 1124. Outputs are driven by the control panel and may be used to relay zone status or provide programmable output state.

Virtual printer

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/**vprinter**/log	Log strings	Setting panel menu 51.28/29 will output various panel events. If log output is disabled, other print menu functions can be used.

SIA4 Integration

The SIA4 protocol is supported by the Honeywell Ethernet modules and internally to the virtualised E080 device. The interface provides a limited set of commands, enabling a polled update of Zone and Group status. These are fixed for the virtualised E080 and modifiable using the SIA4 menu options for the external Honeywell Ethernet modules.

The virtualisation module implements a SIA4 client that can connect to the Honeywell Ethernet module where SIA4 is enabled in the configuration menus. If the option ***E080 enabled SIA zone + group*** is selected, the module will implement SIA4 without any requirement of the Honeywell module being fitted. There are separate settings depending on the module and panel combination:

Dimension / G3 panels

Menu 56.4.2 Alarm Report format needs to be set to SIA with level 4 enabled.
Menu 56.4.8 SIA Control needs to have the vmod IP address entered.

*Note that it is advised when using the VMOD in Dimension control panels to run the VMOD with emulated **E080 enabled SIA zone + group**, or **read-only other COM fitted**. In virtualised or read-only E080 mode, the module will send SIA zone and group requests internally and read event reports from the bus, then forward them to your SelfMon account (requires server IP addresses populated in the VMOD menu). With this option selected, the 'SIA Connections' menu section of the VMOD config page is ignored.*

*Note that if there is a requirement for both the Honeywell E080 / Third Party IP COM device and the VMOD modules to be fitted due to ARC signaling requirements, SelfMon reporting will only work if the **read-only other COM fitted** option is selected and the SelfMon Connection section server IPs are populated.*

Flex panels

Galaxy Flex control panels fitted with a VMOD can provide full zone status in one of two different ways. The first is in combination with an A083 fitted where the VMOD communicates with the A083 via the Ethernet network. The second is when the Flex V3 control panel has no Honeywell module fitted and is configured for ‘Galaxy RS485 bus mode’ with the module fitted on the same bus as the keypad.

Note that the VMOD config Virtual RIO section needs the RIOs set to ‘Read Only (SIA)’ before zone state changes will be published using the methods detailed below.

No Honeywell module fitted.

When no A083 module is fitted and SIA4 zone status is required, the Galaxy Flex V3 control panel must have the Ethernet bus select menu **56.3.3.8** set to **2-GALAXY**. The VMOD bus option menu should then be set to ‘Bus 1 (Flex3 COM4 Galaxy Bus)’. The E080 should then be set to enabled with SIA Zone and Group. After making these changes, ensure that menu 72 is entered to detect all newly enabled devices. The MQTT zone and group status will populate with zone status and system set status. Since firmware version 1.21.206 this option also supports the time and date SIA command XTD*YYYYMMDDhhmmss (see SIA Time & Date Setting for details).

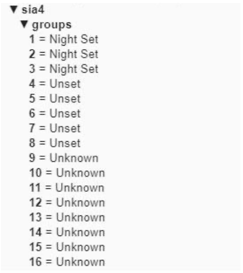
Honeywell module fitted.

Menu 56.5.1 set to any address or the VMOD IP address. ***Note that you need to press ‘ent’ and set any address to ENABLED.***

Menu 56.5.1.2.1 set path to Ethernet. ***Note that you need to press 'ent' and Set ethernet to ENABLED.***

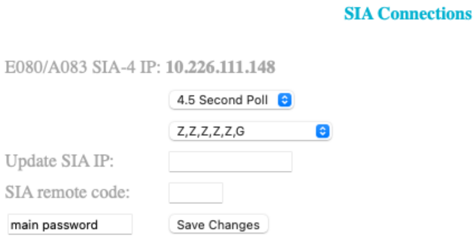
After enabling the SIA4 menu options at the control panel, you can enter the E080 or A083 Ethernet module IP address in the SIA-4 IP address section of the vmod configuration page. Where any RIO is set as read-only or enabled, the vmod.xxxxxx/prio/inputs/read paths will start to populate in blocks of 8 (including the onboard zones).

If group status is selected, the vmod.xxxxxx/sia4/groups topic path will be populated with the status of each group. Where a control panel does not support all 16 groups, unsupported groups will remain in an 'Unknown' state and should be ignored.



```
▼ sia4
  ▼ groups
     1 = Night Set
     2 = Night Set
     3 = Night Set
     4 = Unset
     5 = Unset
     6 = Unset
     7 = Unset
     8 = Unset
     9 = Unknown
     10 = Unknown
     11 = Unknown
     12 = Unknown
     13 = Unknown
     14 = Unknown
     15 = Unknown
     16 = Unknown
```

The polling rate is adjustable, with 1.5 seconds recommended for Dimension panels. Since the Dimension has a slower data bus, reduced poll intervals may cause the primary bus to slow, giving slower responses on keypad devices. The selector for zone and group status allows for different sequences to be selected. Where Z,Z,Z,G will update group status on the fourth poll and zones on all other polls. The default option alternates between zones and group status. The SIA Remote User code may be updated if the panel remote user code has been modified. If the panel remains at the default code of 543210, then you do not need to enter the code.



SIA Connections

E080/A083 SIA-4 IP: **10.226.111.148**

4.5 Second Poll

Z,Z,Z,Z,Z,G

Update SIA IP:

SIA remote code:

main password

Note: One benefit of using SIA4 for zone status over bus mode operation is that wireless zone state changes are picked up, negating the need to monitor RF portals in read-only mode and decoding the RF device payloads. The RF portal read-only mode can still be used to pick up devices that are not programmed to any panel zone if required.

SIA Time & Date Setting

The SIA interface allows for adjusting time and date by publishing the XTD command. It is expected that this be performed automatically at a convenient interval to keep the system clock aligned. For E080 and A083 modules, polling must be enabled to allow the clock adjustment command to be queued. The VMOD only requires that SIA 4 is enabled (see note below).

Note: If you are using the VMOD with emulated Ethernet on Dimension or G3 panels, this feature will work only if you set the panel menu to SIA 4 reporting (Menu 56.4.2 SIA level 4 - ENABLED). This is allowable with the VMOD secure MQTT reporting mechanism. There is no SIA support for the older G2 panels.

Path	Raw Payload	Description
selfmon/vmod.xxxxxx/cmd/sia	XTD*20210701122100	XTD*YYYYMMDDhhmmss Where YYYY is the year, MM month, DD day of month, hh hour, mm minute and ss second. The example raw payload provided will set the system clock to 12:21:00 on the 1st of July 2021.

Module LED indications

The module has two LED's which are located in the Ethernet jack assembly as follows:

- The right-side LED will illuminate constantly once powered and no Ethernet connection is available. Once the network is active, the LED will pulse with Ethernet packet activity.
- The left-side LED will be unlit if no network connection and will give a fast-blink rate when the network is not 'link up' or where no broker connection is achieved. If a broker login is achieved, the LED blink rate will slow to a ~5-second interval. Along with this interval, the module will publish a heartbeat diagnostic string.

Factory default settings

The module settings may be restored to factory defaults by momentarily connecting a jumper across pins 8 and 10 in the IDC header, as shown in figure 6 in yellow. The module must be powered and the application running when performing this operation. After the jumper has been momentarily connected and disconnected, the module power must be cycled to restore the default settings.

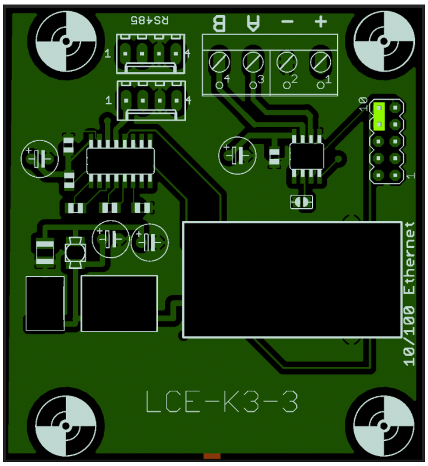


Figure 6 – Virtual module defaults pins

Firmware upgrade

The module application firmware may be upgraded via Ethernet. This requires that the 'lmflash' Windows application runs on a Windows system on the same subnetwork as the module. The 'lmflash' program should be configured with the module MAC address and a temporary IP address for the module to use. The 'lmflash' program will send a 'magic packet' to the module, switching it into Ethernet bootloader mode and then transferring the new firmware binary. Note that as long as the original application is running, there is no need to **force** the bootloader into recovery mode. To check that the module application code is running, remove the Ethernet connection, and the amber LED should illuminate. If both LEDs illuminate, then either the main program has been corrupted, or the bootloader recovery mode jumper is fitted.

Download the 'lmflash' program and follow the update instructions listed here: http://www.selfmon.uk/fw/lce-k3/

Bootloader recovery mode

In the event that the module application firmware becomes corrupted or crashes, the bootloader may be forced into recovery mode by connecting a jumper across pins 8 and 10 in the IDC header as shown in the previous figure 6 and powering on with the jumper in position. To double-check that you are in bootloader mode, unplug the Ethernet connection and confirm that both Green and Amber LEDs are illuminated. If only Amber is illuminated, then the module is not in bootloader recovery mode.

The ‘lmflash’ Windows program may then be used to re-install the application firmware via Ethernet. After the upgrade is complete, the jumper may be removed, and the module power cycled to boot the bootloader and, in turn, automatically run the newly installed application.

If the firmware upgrade fails, run a program like ‘WireShark’ to view network traffic. Start a capture on the local interface and then filter the traffic using ‘bootparams’ as the filter. When you power on the module, you should see ‘BOOTP’ requests from the module showing the MAC module address. If you don’t see these, then check your Ethernet cable connections to the module. If you see the ‘BOOTP’ requests, then you should see a ‘BOOTP’ reply from the host / IP address that is running the ‘lmflash’ program.

WARNING: If another host is replying to the BOOTP request, then this will cause a conflict and you need to isolate that host from the network while you perform the flash upgrade. If you don’t see any reply, then the ‘lmflash’ program is not configured with the correct MAC address or does not have permission to start a ‘BOOTP’ server on your Windows system.

When the module upgrade is complete, power down the module. Remove the jumper and Ethernet connections and power on the module. The module amber LED should be illuminated. Plugging in the Ethernet connection should result in both LEDs flashing as per normal operation.

SelfMon Reporting

The module can send encrypted SIA and heartbeat polling transmissions via a separate MQTT channel to the SelfMon platform. This requires that the control panel is configured to send events, and the E080 emulation and SelfMon Primary / Secondary IP addresses are configured in the module configuration menu. The control panel configuration may differ depending on the Galaxy variant.

Dimension / G3 / Classic / Flex V1 / G2 control panels or Flex V3 in virtual printer reporting mode

SelfMon Module Config Page:

Enable the E080 module.
SelfMon Primary - 34.242.137.208
SelfMon Secondary - 54.247.112.82

Enter and exit engineering mode to detect the virtualised E080 module.

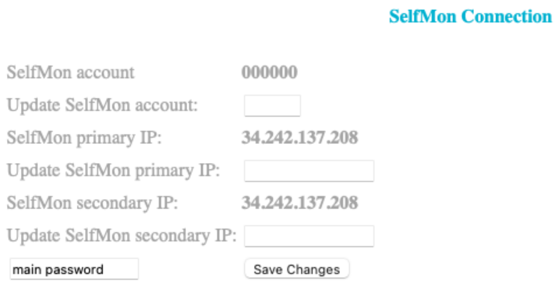
Panel Menu:

Please follow SelfMon ‘panel settings’ menu for your control panel.

Note:
The SelfMon account number in the selfmon connection comes from the panels programmed account code. It only needs to be populated in the module config when using either the **Virtual Printer to SelfMon** or when adding the VMOD module in ‘**E080 read-only mode’** in addition to an existing Honeywell E080 module or third party RS485 based COM4 Ethernet module where that module is set to report to a non-SelfMon account number.

Panel addresses and port values are not used, but they need to be populated in order that the panel transmits the event for the module to process.

Take care to enter the correct SelfMon account number, as the platform intrusion detection will blacklist your IP address if you send to an invalid or suspended account.



SelfMon Connection

SelfMon account	000000
Update SelfMon account:	
SelfMon primary IP:	34.242.137.208
Update SelfMon primary IP:	
SelfMon secondary IP:	34.242.137.208
Update SelfMon secondary IP:	
main password	Save Changes

Virtual Printer to SelfMon

There is an option for Flex control panels to forward printer output to your SelfMon account. To achieve this, you need to set the following

1. In the vmod virtual devices section, set the bus menu for 'Flex3 print to SelfMon'
2. In the vmod virtual devices section, set the printer module to 'enabled'
3. In the vmod SelfMon connection section, **enter your account number**, and SelfMon server addresses **34.242.137.208** and **54.247.112.82**.
4. In the control panel menu, modify menu 51.28 to enable the printer and 51.29 to set your level of print logging.

After modifying the settings above, the vmod will start sending the print log to your selfmon account. This is of benefit where there is no A083 module fitted. Note that there will be no remote keypad via port 10001 when the A083 module is not fitted to the Flex.

VMOD module secondary to Honeywell E080 or 3rd Party Module

1. The 3rd party module Eg. DualCom must be configured to send events to a 3rd party alarm receiving center, or the Honeywell RSS event receiving software.
2. Configure the VMOD to the primary bus.
3. Set the Virtual E080 menu option to ‘Read Only 3rd Party Communicator’ mode.]
4. In the vmod SelfMon connection section, **enter your account number**, and SelfMon server addresses **34.242.137.208** and **54.247.112.82**.

RSS & Apps

The module will provide a TCP/IP interface on port 10001. This port provides an encrypted interface for RSS and Android/iOS apps. The E080 option must be set to enabled for port 10001 communications. Note that the GX app is only compatible with the Dimension and Flex control panels. The G3, G2 and Classic panels are only supported with the SelfMon phone apps. You may install the SelfMon app to gain app-based event reporting and still use the Honeywell GX app to control your panel.

SelfMon Android & iOS Device Apps

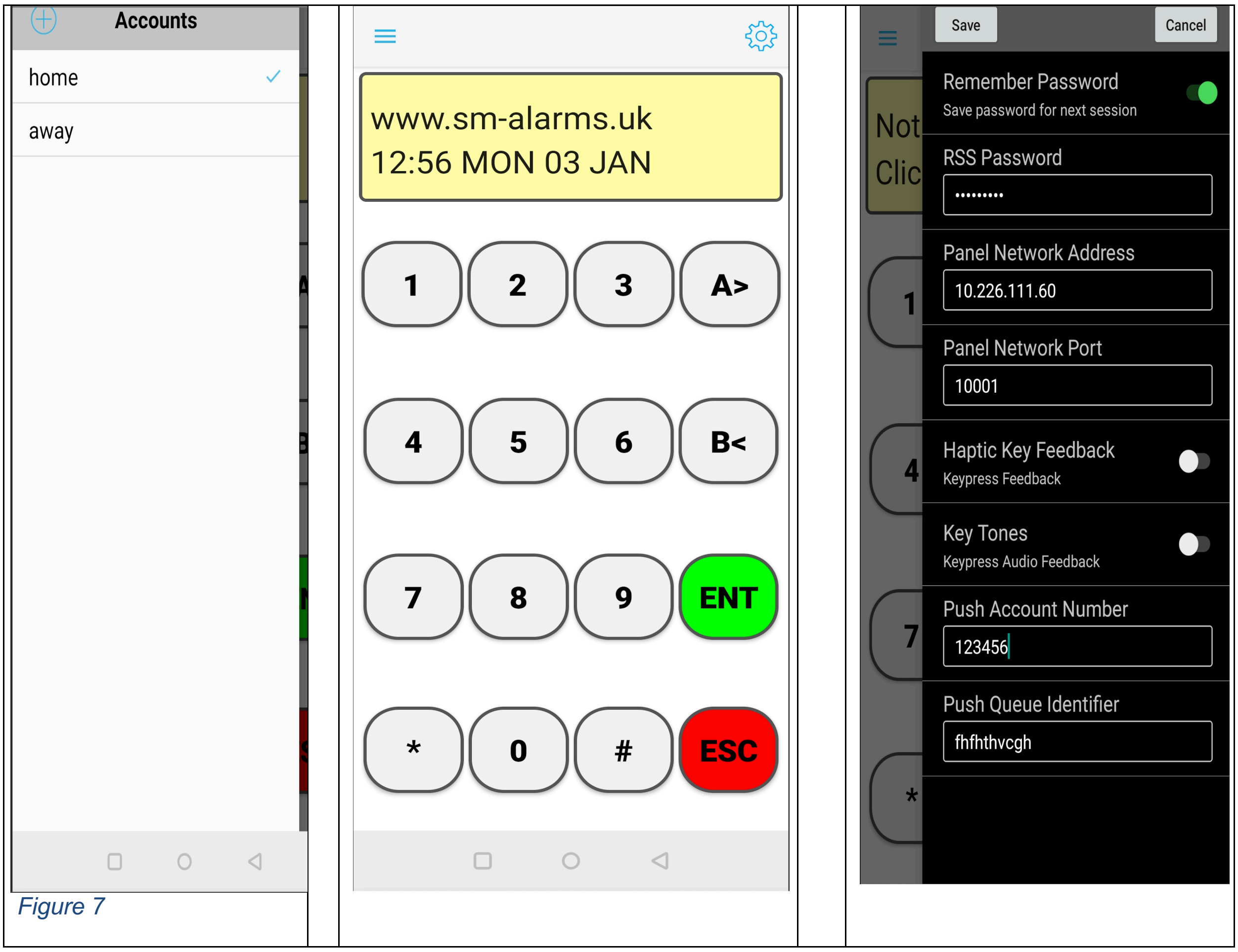
Remote access settings need to be set to enabled for app or RSS access.

For Dimension, the settings are:
56.4.3.1 - Access period - 'Any Time'
56.4.3.2 - Mode - 'Direct Access'

For Flex, the setting is:
56.4.1 - Access period - 'Any Time'
56.4.2.4 - Access via Ethernet - 'Enabled'

The SelfMon Android and iOS applications provide two functions. The first is a direct connection to the virtualised keypad when supported by the Ethernet module via TCP port 10001. The second is a push notification receiver for free SelfMon push notification transmissions.

You can add connections to your control panel using the ‘hamburger’ menu icon on the left. If your home router does not support NAT loopback, you may have to add a home account and an away account, as your router will not loop back on the external network DNS name to your internal panel address.



Accounts

home ✓

away

www.sm-alarms.uk
12:56 MON 03 JAN

Remember Password — Save password for next session: on

RSS Password: •••••••••

Panel Network Address: 10.226.111.60

Panel Network Port: 10001

Haptic Key Feedback — Keypress Feedback: off

Key Tones — Keypress Audio Feedback: off

Push Account Number: 123456

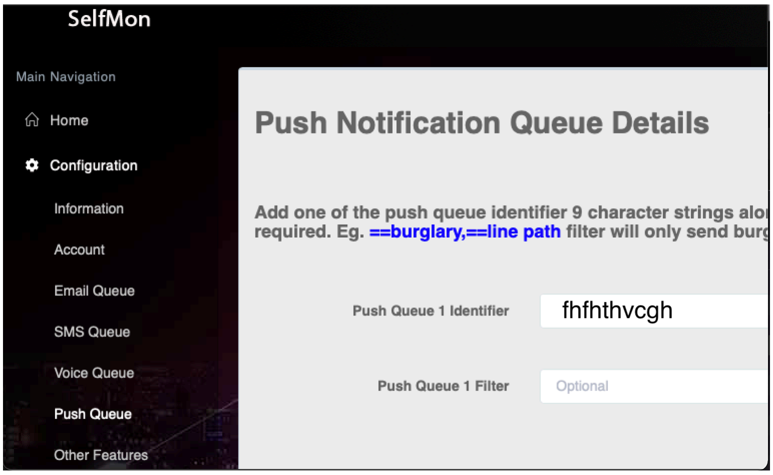
Push Queue Identifier: fhfhthvcgh

Figure 7

In figure 7, you can see that an account has been added for ‘home’ and information has been added for that account using the ‘gear’ icon. When this account is selected, the application running on the mobile device on local WiFi, will connect directly to the control panel. In the example, the internal address is 10.226.111.60.

To control the panel externally from the premises, you need to port forward TCP port 10001 from the internal control panel address. **(Port forwarding setup varies depending on your router and is outside the scope of this guide – search for your router guide and check that TCP port 10001 is open by using a service like https://portchecker.co)**
You can add an ‘away’ account for this if required. If using SelfMon, and you have hourly automatic tests enabled, you can also enable the SelfMon DNS service in the **‘Configuration -> Account -> Edit’** option. A DNS name will then be provided in **‘Configuration -> Information’** and this may be added as the panel network address. Each time your control panel sends an Event, the SelfMon platform will check and update the DNS record if required.

If you configure external access, it’s **important** to have an RSS password configured. Failing to do this will allow anyone to access your control panel from the internet. Unfortunately, the only way to set the RSS and UMS passwords at the moment is with Honeywell RSS software.



Push Notification Queue Details

Add one of the push queue identifier 9 character strings alo
required. Eg. ==burglary,==line path filter will only send burg

Push Queue 1 Identifier: fhfhthvcgh

Push Queue 1 Filter: Optional

Figure 8

To configure push notifications, you must first have set up SelfMon event reporting from your control panel. You can then navigate to **‘Configuration -> Push Queue’** and select one of the five push queues available. You will see that each queue has a nine-character identifier. If you add the identifier and your SelfMon account number to the phone app and **‘Save’** as in the example in figure 8, you will receive registration confirmation and the app will start to receive notifications each time your panel makes a transmission. You can add an optional filter to only receive desired events specific to the push queue. For example, saving a filter string: **==burglary,==tamper** will only allow push notifications for burglary and tamper events to the device subscribed to that queue.

Installation example 1

In this example, we consider a Galaxy Dimension 48 control panel. The panel has two keypads, an Ethernet module and two external RIO modules fitted.

First, enter engineering mode and select menu 61.1.3, stepping through and noting the external RIO addresses. You will see that internal RIO's are on addresses 0 and 1 as expected. The external RIO's addressed as 2 and 3 and that aligns with the physical rotary address selector on the devices.

That's a total of 32 physical zones. In this example, we note that only 10 zones are wired (used) in the control panel. With 4 RIO slots taken in the Dimension 48, this leaves a further two address slots for the virtual module.

Since the Dimension 48 has a single bus, you can connect the virtual module to the engineering header or to any dual connector device already connected to the header. To do this, wire the flying lead bare wire terminals into 0V +12 A B of the module. Place the standoff feet into the module and remove the backing tape. Select a suitable position in the control panel to place the module in order that the lead reaches the engineering header. Ensure that the module is not too close to the edge and that the Ethernet connector is facing inwards allowing insertion of the Ethernet cable. Fix the module in position and plug the 4-way connector onto the bus header.

Next, plug in the RJ45 Ethernet connector connected to the Ethernet network. Examine the module LED's and see that the power LED is red, and that the amber LED on the module is flashing with network activity. The green LED should be flashing at half second intervals - indicating that the module is not connected or logged into to an MQTT broker.

Log into your network router and determine the DHCP address that the module d8:b0:4c:xx:xx:xx has been allocated. Set the IP address as a fixed or permanent lease on your router. Use a PC web browser to load the module configuration page. Eg. http://129.159.0.200/settings.shtm In the configuration page, focus on the middle section and set the following options:

- Leave the bus selection as default 1 as the Dimension 48 only has one bus.
- Leave address 00 and 01 as disabled, as these devices cannot be read directly on a Dimension 48 panel.
- Enable read-only on modules 02 and 03, as these are external RIO addresses.
- Set addresses 04 and 05 as enabled as these are free RIO slots.
- If you have existing RF portals, set the addresses to 'read-only'. Set one unused address as 'enabled'.
- Leave the virtual keypad address at 19, which is the engineers keypad slot.

A new password has not yet been set on the module, so enter '**thisisatdefault**' into the box displaying 'main password' and select the 'save changes' button. The options selected should remain selected after saving. Note that if the settings jump back to the previous options, then you have used the wrong password.

Now that the bus devices have been configured, use the control panel keypad to exit engineering mode to scan for new devices. The enabled virtualised RIO modules should be recognised by the control panel and showing at 100% in the diagnostics menu.

Return to the module configuration page and enter the MQTT server details. Save the changes using the password as per the previous step. Note that the module currently connects to the broker with no TLS on port 1883. (a future update or alternative vmod hardware may implement TLS). After updating the broker information, the green module LED slows to a steady 5 second on / off interval. This indicates a successful login to the broker.

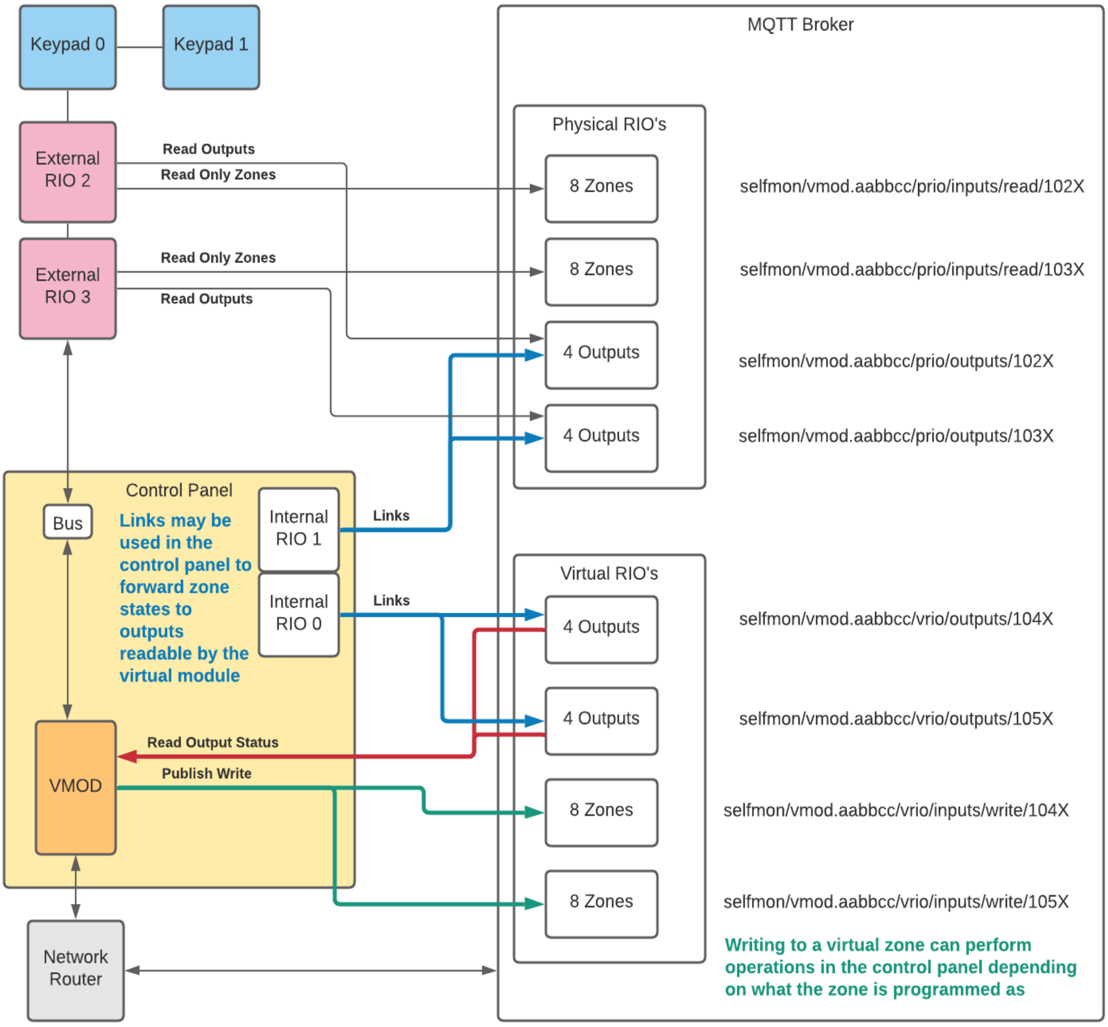
Next, use a tool like MQTT explorer to view the selfmon topic in your broker. You should see that the module has published on the topic selfmon/vmod.aabbcc/ where the example 'aabbcc' are the last three octets of the module Ethernet MAC address. This path is printed on the module label. ***Note that the paths are case sensitive***

At this point, you should see some topics being published by the module including a heartbeat and module core temperature. The topics may also be showing further sub-paths for **'vkp'** the virtualised keypad and **'vrio'** the virtualised remote I/O or RIO module. If you have enabled a 'read-only' physical RIO on the same bus as the virtual module, then any zones or output status changes on those RIOs will be published under the physical RIO **'prio/read'** topic path. In this example, devices 1021 to 1028 and 1031 to 1038 were set as 'read-only', so you will see the zones change state at the same time as any devices connected to the physical RIOs are triggered. These paths may be subscribed to by MQTT clients to determine zone and output status for the existing external RIOs.

For paths that are based on virtual RIO addresses, the zone states may be changed by clients who publish a payload of OPEN or ON and CLOSED or OFF on that **'vrio/write'** topic path.

The RIO outputs are also available. Outputs can only be read via MQTT. The state of the outputs is determined by the control panel programming. If an output is programmed as BELL, then during an activation, the topic path for that output will have a payload of ON published by the virtual module.

If you wish to determine the state of the internal control panel zones, then a programmed 'link' from the internal zone to a physical or virtual RIO output is required. For example, you can create a link in menu 54 from zone 1001 to virtualised or physical output addresses. In this example, 1041 to 1054 and 1021 to 1034 respectively. Unfortunately, you cannot link zones, as doing so will only set the destination zone to 'masked' status.



Keypad 0
Keypad 1
MQTT Broker
External RIO 2
Read Outputs
Read Only Zones
Physical RIO's
8 Zones
selfmon/vmod.aabbcc/prio/inputs/read/102X
External RIO 3
Read Only Zones
8 Zones
selfmon/vmod.aabbcc/prio/inputs/read/103X
Read Outputs
4 Outputs
selfmon/vmod.aabbcc/prio/outputs/102X
4 Outputs
selfmon/vmod.aabbcc/prio/outputs/103X
Control Panel
Bus
Links may be used in the control panel to forward zone states to outputs readable by the virtual module
Internal RIO 1
Links
Internal RIO 0
Links
Virtual RIO's
4 Outputs
selfmon/vmod.aabbcc/vrio/outputs/104X
4 Outputs
selfmon/vmod.aabbcc/vrio/outputs/105X
VMOD
Read Output Status
Publish Write
8 Zones
selfmon/vmod.aabbcc/vrio/inputs/write/104X
8 Zones
selfmon/vmod.aabbcc/vrio/inputs/write/105X
Writing to a virtual zone can perform operations in the control panel depending on what the zone is programmed as
Network Router

Figure 9 – VMOD Virtual RIO's, Physical RIO's and Broker Paths

In Figure 9, we can see that the external RIOs 2 + 3 are available in read-only mode, allowing the reading of zone and output states for those physical devices. When a zone changes state or output is driven by the panel, the status changes are published to the relevant **'prio'** topic paths. The physical RIO topic paths are read-only and cannot be written to. The virtual RIO **'vrio'** input write paths may be written to. Writing to one of these paths will change the state of the virtual zone in the control panel. An example would be a key switch zone, where writing an OPEN or ON followed by CLOSED or OFF to that zone topic path would flag the control panel to start setting the system. Care should be taken with this, as there may be someone in the premises or an open zone. A feedback loop of programming an output as 'set' would provide a clear indication that the system was successfully set as intended.

All output paths are driven by the control panel. If you program a reflex link from a control panel internal zone to one of the outputs, then the relevant topic path and payload for that output will be updated when the internal zone changes state.

For physical portal modules in read-only mode, pressing a fob button or activating a wireless sensor will publish on the V2 or Alpha path depending on the RF device configuration/type. Virtual portals will accept commands for setting and unsetting provided that the serial number passed with the command is included in a control panel user account. This is achieved using the menu for RF fob serial number in Alpha protocol 42.X.10 on Flex and 42.X.12 on Dimension control panels.

Engineering hardware builds

Engineer-only modules include the capability to unlock panel codes. If the module is labelled with a circled E on the label, it is an engineer-only build and not for sale to the DIY market. The special build includes a code unlock feature, where connecting the module to any Dimension, G3 or Classic panel bus 1 engineering header, power cycling and then grounding pin 5 in the IDC header for 10 seconds, the module will default the engineer code 112233 and remote code 543210. The authority code is also enabled and set to 999999. This allows the on-site engineer to authorise using the authority account, and then gain access with the default engineer code.

Electrical characteristics

Input voltage 12V DC
Input current 35mA

Troubleshooting

Keypad cursors are incorrect - Ensure that the bus selection is correct for your control panel and that vmod firmware is at the latest release. The character positioning was fixed in version 1.21.092

Flex keypad does not work after a reboot - The default keypad address on the vmod is set to 19 which is the engineer address. On Flex, if you reboot the system, you need to enter engineering mode once to enable the engineering keypad. You can always use any other free address slot for the virtual keypad and the non-engineering addresses do not require enabling like address 19. The Dimension and G3 control panels are not affected.

Firmware will not upgrade - Please see the separate troubleshooting ''VMOD bootloader upgrade debug' document in the firmware folder.

The module crashes after a long runtime and I have port 10001 forwarded - Please upgrade to the latest firmware as this issue was fixed in version 1.21.091

Known issues in current release

FW0009 – RF devices currently report a decimal payload. This will be updated at a future date with a payload detailing the actual state of the device.