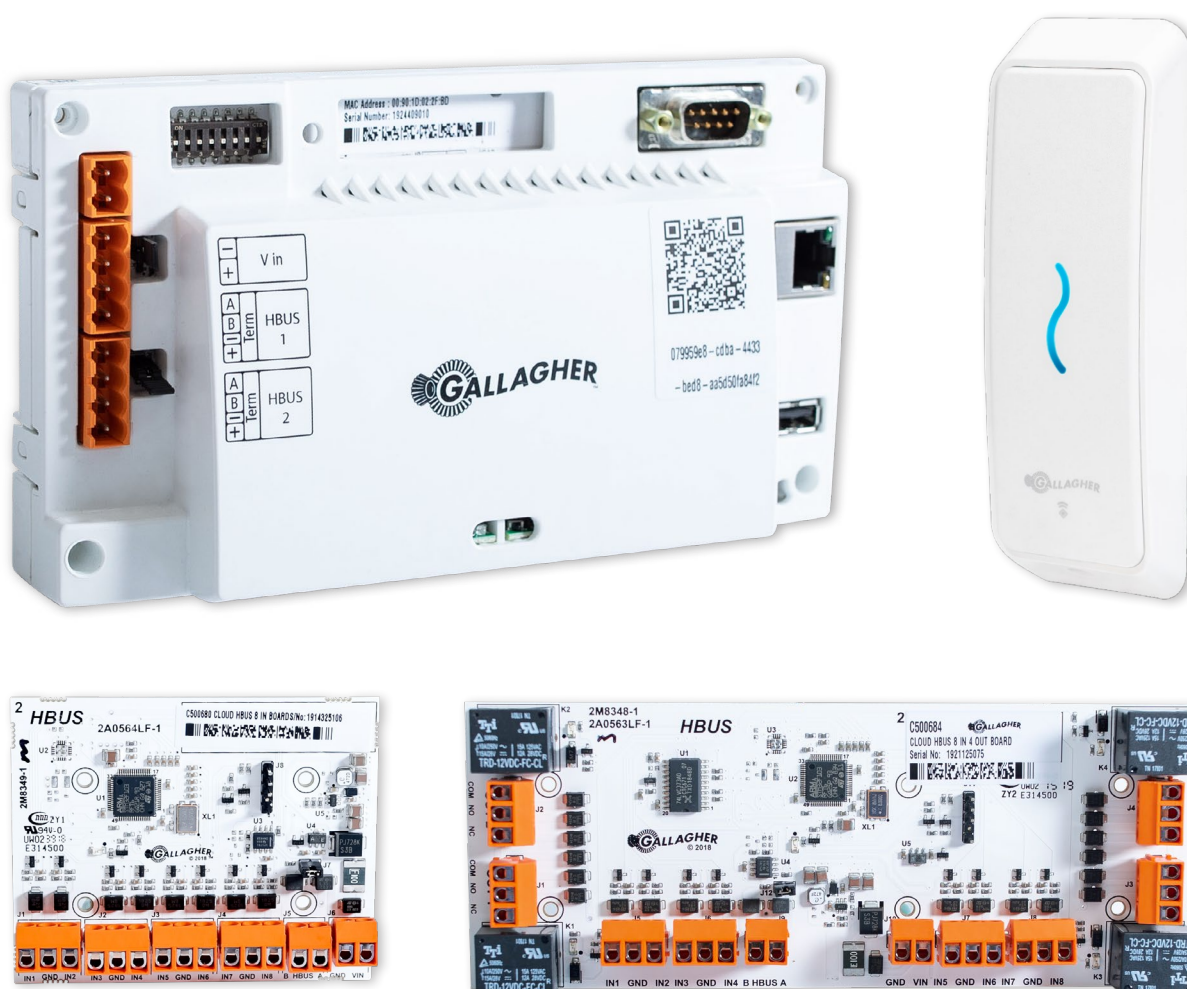




Gallagher SMB Kit

Installation Note

Gallagher SMB Component Kit: C500200



Introduction

Thank you for choosing Gallagher.

The Gallagher SMB security solution has been designed to meet the security of businesses with less complex security requirements. It is a fully integrated cloud-based security system that offers intruder alarm, access control, and user management all within one mobile app.

Kit contents

Check the cabinet contains the following items:

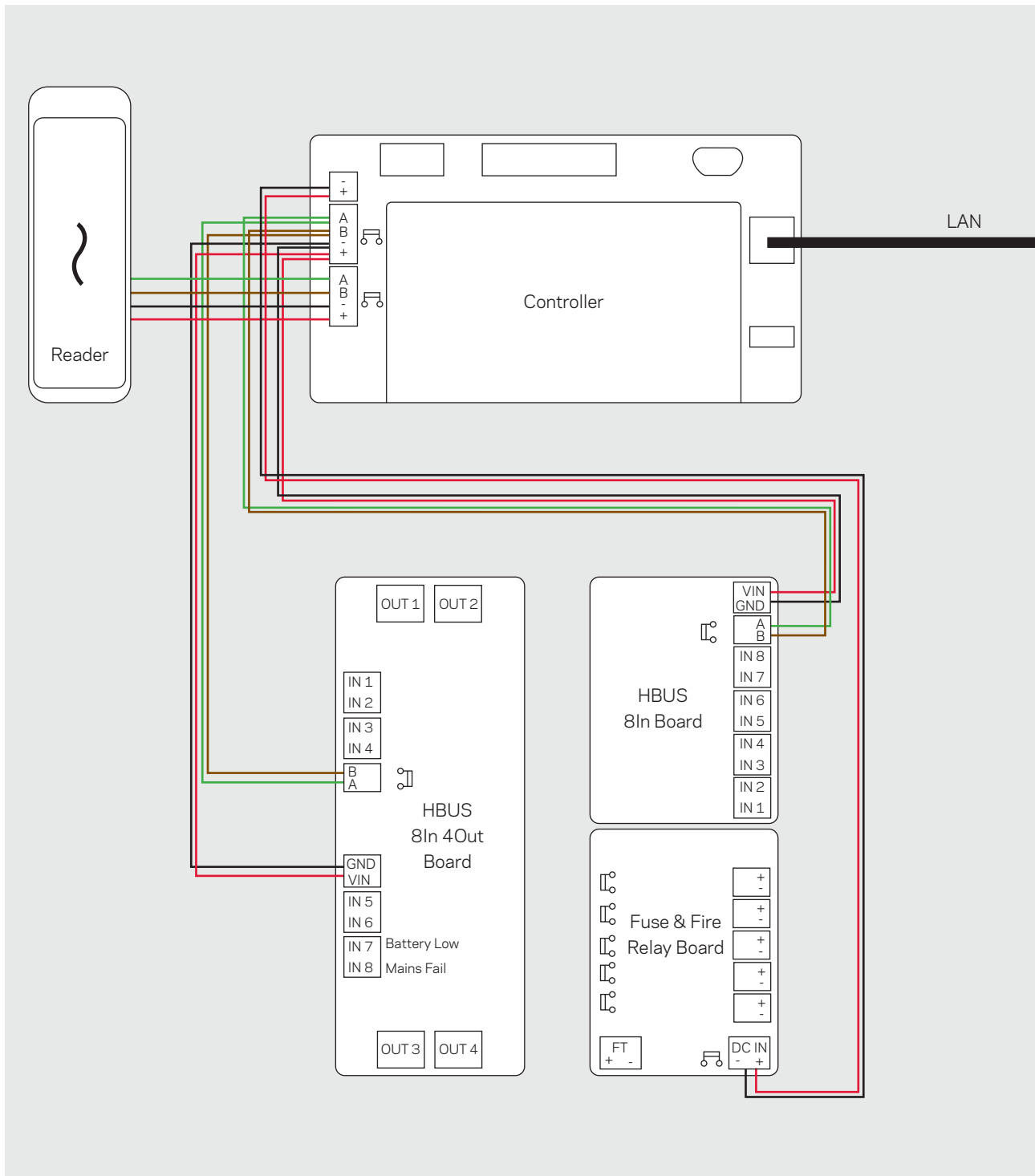
- 1 x SMB Controller (C500100)
- 1 x HBUS 8In Board (C300680)
- 1 x HBUS 8In 4Out Board (C300684)
- 1 x Gallagher SMB T15 Reader (C300480)

Additional items are:

- SMB Readers (C300430, C300431, C300480, C300481, C300490, C300491)
- SMB Dual Cabinet with 8 A power supply (C200105)
- HBUS 8In Board (C300680)
- HBUS 8In 4Out Board (C300684)
- HBUS 16In 16Out Board (C300688)
- HBUS 8 Port Hub (C300698)

Wiring the system

The hardware components in the kit can be wired together to support the site's default software configuration.



Installation

The installation of this kit must be carried out by a Gallagher trained technician. Complete the instructions in this document to install the kit.



ATTENTION: This equipment contains components that can be damaged by electrostatic discharge. Ensure both you and the equipment are earthed before beginning any servicing.

1. Install a cabinet

Before you begin

- **Location**
Choose an installation location for the cabinet. The cabinet should be installed in a cool, dry, and secured location such as a server room. The location must provide environmental and extreme temperature protection, AC mains power availability, and building cable availability for the external connections. Ensure the cabinet is accessible to the site's wired network.
- **Earthing**
Ensure there is an earth wire connected to the cabinet door and power supply unit. If the wire is disconnected during installation, please ensure it is reconnected.

2. Install readers

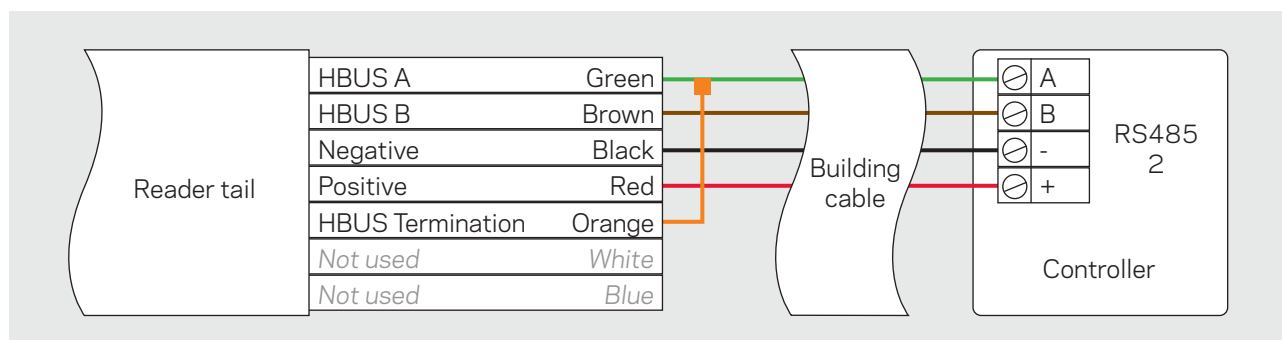
The default configuration provides allocation for one reader. It is recommended at least one reader be configured to a site. This allows a user to arm or disarm locally using their smartphone, in the event that the site loses internet connectivity. The smartphone uses Bluetooth to communicate with the reader.

Doors can be configured without a reader, if required.

The HBUS communications protocol allows a single reader to communicate over a distance of up to 500 m (1640 ft) from the controller, when using data only in a single CAT5E cable. Cabling should be a minimum size of 0.2 mm² (24 AWG).

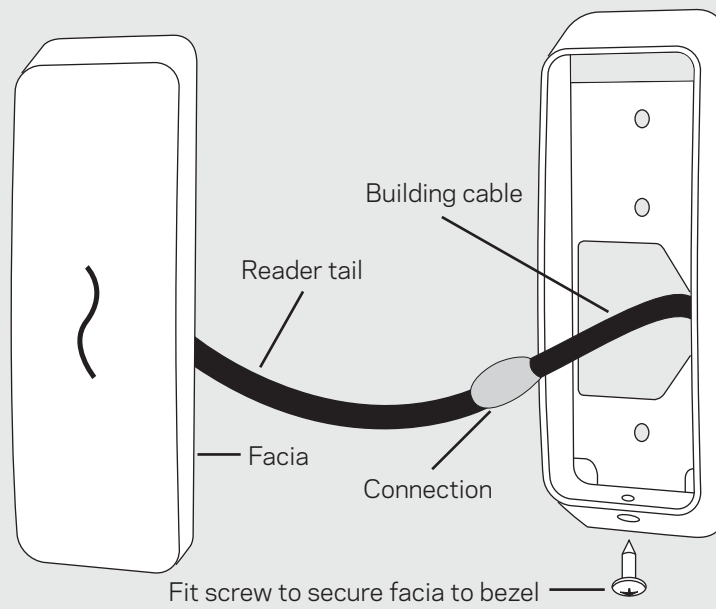
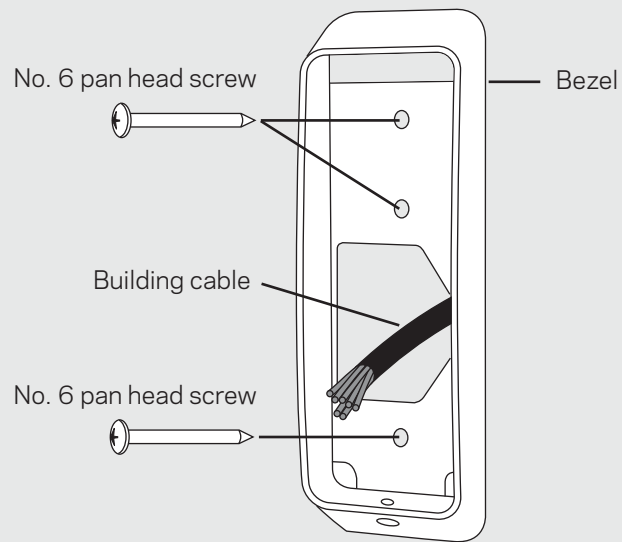
Connect the reader tail to the building cable. All cabling between HBUS devices should use 'daisy chain' wiring. This allows you to have multiple devices on the same cabling run. The end devices on the HBUS run must be terminated. To terminate a reader, connect the orange wire to the green wire.

Should you require multiple doors, the HBUS 8 Port Hub (C300698) can be utilized. This hub supports the star wiring of eight HBUS devices to the hub's eight ports. Note that you will still need to provide power to the door.



The reader is designed to be mounted on any solid flat surface. However, installation on metal surfaces, particularly those with a large surface area will reduce read range. The extent to which the range is reduced will depend upon the type of metal surface.

The recommended mounting height for the reader is 1.1 m (3.6 ft) from the floor level to the centre of the reader. However, this may vary in some countries, and you should check local regulations for variations to this height. If using conduit, the reader can be mounted on a mounting block (C300951).



3. Connect inputs and outputs

Two I/O boards are provided with the component kit; the 8In Board, and the 8In 4Out Board.

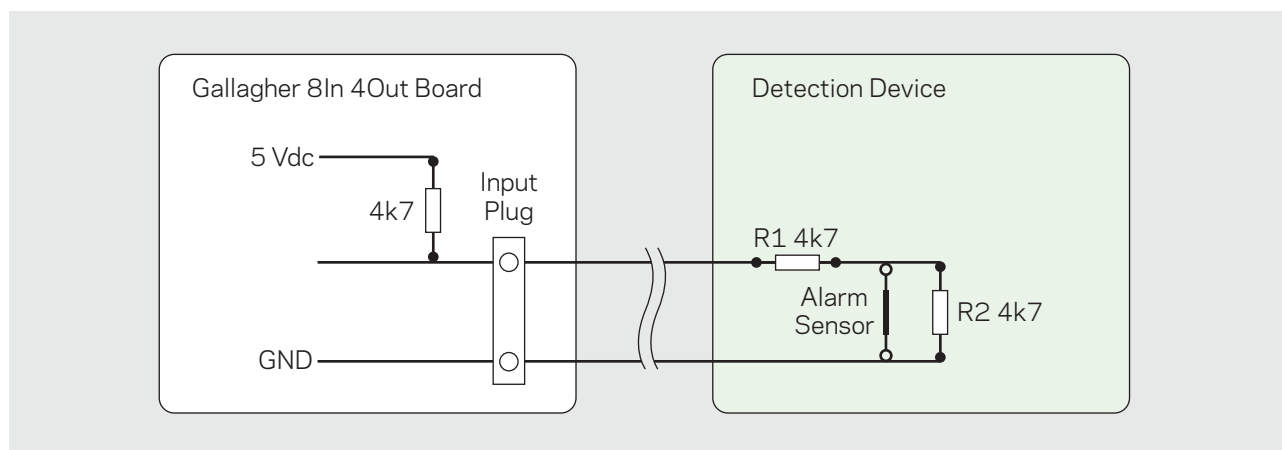
The boards provide connection for a total of 16 inputs and 4 outputs. Two of the 16 inputs are used for monitoring mains power failure and battery low. The remaining 14 inputs can be used to connect sensors.

The HBUS 16In 16Out Board (C300688) can be utilized with the SMB Kit to expand the solution.

Balanced inputs

Cabling should be a minimum size of 24 AWG (0.2 mm²) for all balanced inputs.

For tamper detection, the balanced inputs require resistors to be connected as close as possible to the device being monitored. When the monitored device incorporates a normally-closed tamper switch, it can be wired in series with resistor R1.



| Condition | Resistance | Voltage at 'X' |
|----------------------|---------------------|----------------|
| Short circuit tamper | 0 | 0 V |
| Normal | 1 (4k7) | 2.5 V |
| Alarm | 2 (4k7 + 4k7 = 9k4) | 3.3 V |
| Open circuit tamper | 0 (no resistance) | 5 V |

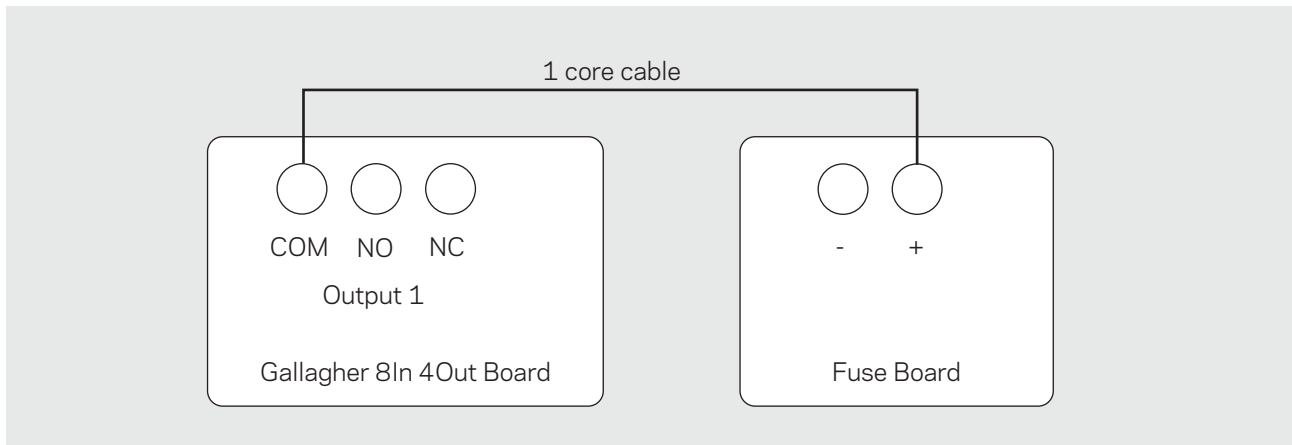
All devices connected to a single I/O board must share the same physical resistor value, (i.e. individual devices cannot have different resistors, unless assigned to different boards). You can change the resistance value for an I/O board within the SMB Installer Portal. Additional boards can be added to the system.

Power can be drawn from a Fuse & Fire Relay Board. This board can provide power distribution and enables a fire panel to control power to a site's doors. It can be used to control power to sensors and sirens, whilst maintaining circuit protection.

Output relays

Relays are provided as 'dry' contacts or 'electromagnetically switched' contacts. Each relay is rated 3 A at 24 Vdc for a resistive load, or 1 A at 24 Vdc for an inductive load.

The relay is controlled by the assigned output in the SMB Installer Portal. To utilize the relay, terminate the positive constant supply to the common termination of the relay and nominate either Normally Open (N/O) or Normally Closed (N/C) termination to operate the external device. Refer to the image below.



4. Connect power to the controller

A power supply is required to power the SMB components and should will provide two alarm outputs for monitoring battery low voltage and mains failure alarms. Both the alarm outputs have on-board 4k7 EOL resistors fitted as standard.

Note: Do not apply voltage directly to the Battery Low or Mains Failure outputs, as this will damage the monitoring circuitry, rendering the power supply unusable.

1. Connect the earth wire from the power supply to the cabinet door.
2. Using a battery lead, connect one or two 7 Ah 12 V batteries to the power supply. The batteries must be connected in parallel. The red wire connects to the red/positive battery terminal. The black wire connects to the black/negative battery terminal. The batteries are not provided. The batteries are used as standby batteries, should the mains power supply fail.
3. Connect an IEC power lead from the mains wall socket to the power supply unit. The IEC power lead is not provided with the kit.
4. Ensure all equipment operates correctly, both with mains power ON/batteries ON, and with mains power OFF/batteries ON.

Calculating battery life

To know how long your batteries will support your cabinet, calculate the following:

$(\text{combined battery capacity}^*) \div (\text{total current draw in amps}^{**}) = (\text{battery life in hours})$

*To find the combined battery capacity, add the Ah values of all your batteries.

**To find the total current draw, add the current draw of the individual units in your cabinet.

Refer to the end of this installation note and separate hardware installation notes for current draw values.

Battery Low alarm

The Battery Low system alarm will be triggered when the battery charge falls below 10.8 V. If no battery is connected the Battery Low alarm will not activate. This output is connected to Input 15 in the default configuration.

Mains Failure alarm

The Mains Failure system alarm will be triggered when the mains voltage falls below approximately 90 V or when the mains voltage rises above approximately 250 V. This output is connected to Input 16 in the default configuration.

5. Connect the controller to the cloud

The controller connects to the site's wired network. If the site's network is unreliable, an external router can be used to provide a 4G connection to the cloud or connection to the site's Wi-Fi.

1. Power on the controller. Connect an ethernet cable from the site's network to the controller's ethernet port. If using an external router refer to the products installation notes.
2. Does the site's network use a proxy server to access the internet?
If **no**, continue to step 4.
If **yes**, you will need to supply the proxy server's hostname, port, and logon credentials to the controller. Refer to the topic "*7. Controller web browser configuration*" later in this document, to access the proxy settings.
3. Log into the [SMB Installer Portal](#) and assign the controller to a site. If you have no login details, please refer to the Technician Onboarding Guide. Note: The SMB Installer Portal is a web-based portal and does not require you to download an app from the iOS or Google Play Store.
Refer to the topic "*6. Assign the controller to a site*" later in this document.
4. Once assigned to a site, the controller will come online and connect to the cloud. An IP address is automatically assigned to the controller via DHCP. There is no MAC address or IP addressing required.

The controller will download the latest firmware and its default configuration from the cloud. The download will take approximately 5 minutes. It may take longer if the download occurs over cellular. The controller will restart after the download completes. Configuration changes should not be published to the controller at this time.

If the controller doesn't come online, check the site has an internet connection. Plug your laptop into the network and test the connection. Ensure the following ports are open on the site's network for the controller:

| Port | Protocol | Details |
|------|----------|-------------------------|
| 67 | UDP | DHCP to internal router |
| 53 | UDP | DNS to internal router |
| 123 | UDP | NTP to time.google.com |
| 443 | TCP | SMB Cloud HTTPS |

6. Assign the controller to a site

1. Log into the [SMB Installer Portal](#).

Note: Login details can be requested from Gallagher Technical Support.

2. Has the site been created?

If **no**, continue to step 3.

If **yes**, go to step 6.

3. Select the **+ADD NEW SITE** located at the top of the screen.

The 'New Site' lightbox displays.

4. Enter a name for the site and complete all fields.

The key account holder will be the first person from your customer's site to download the Gallagher SMB App. The Key Account holder performs a similar role to a facility manager and is the person who will invite other users, to the site.

Select the **Site uses tags** checkbox if the site will be issuing key tags to users. Selecting this checkbox will enable tag assigning functionality within the Gallagher SMB App.

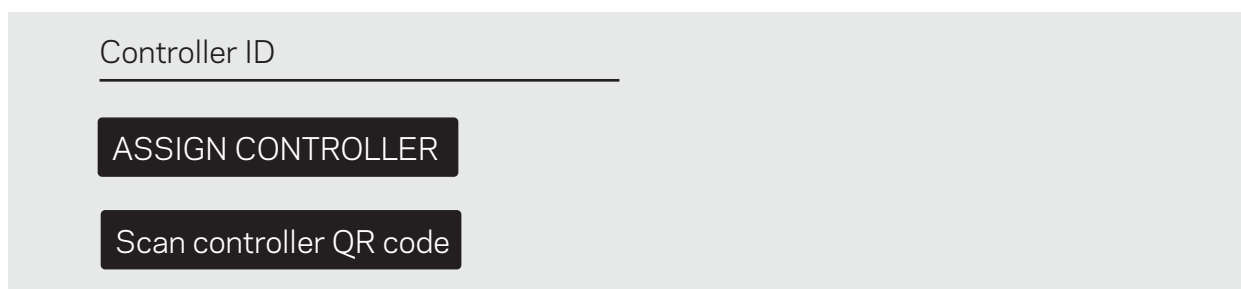
Note: If using tags, cards, or user codes to arm & disarm an area, change the **Locally disarm area** to **Single Factor** within the **Area** lightbox.

Select the Billing Frequency for the ongoing subscription – monthly or annual.

5. Select the **Save** button.

The site is created, and the default configuration is displayed.

6. Navigate to the site, click the **Scan controller QR code** button, scan the QR code printed on the controller, then click the **ASSIGN CONTROLLER** button. If using a laptop, take a photo of the QR code using your phone and present it to the laptop.



Controller ID

ASSIGN CONTROLLER

Scan controller QR code

Note: If you're unable to scan the controller's QR code, you can enter the controller's ID in the **Controller ID** field, then click the **ASSIGN CONTROLLER** button. The controller's ID is printed on the controller, below the QR code.

The controller will download the latest firmware and its default configuration from the cloud. If the message **Cannot assign controller** displays, it has already been assigned to a site.

7. Controller web browser configuration

The Controller's cloud configuration web pages allow configuration of specific Controller settings, including the Controller's date/time and NTP server if needed.

To connect to the Controller's cloud configuration web pages, there are two methods:

| Method | Procedure |
|--|---|
| Navigate to the Controller's IP address | <ol style="list-style-type: none">1. Find the IP address that has been assigned to the Controller by the local DHCP server.2. Set DIP switch 1 to ON.3. Connect a laptop/PC to the same network as the Controller.4. Using a web browser, go to the Controller's cloud configuration web page, replacing <code><ip_address></code> with the assigned IP address for the Controller: <code>http://<ip_address>/cloud/</code> The Sign In dialog displays.5. Enter cloud for the username, then GGLcloud for the password and press Enter. The Gallagher Cloud Controller Configuration web page displays.6. Select the required link to configure the Controller as needed.7. When finished, set DIP switch 1 to OFF. |
| Reset the Controller's IP address, then navigate to it | <p>If you cannot find the Controller's DHCP IP address, the Controller can use the default IP address by powering it on with DIP switches 1, 2, and 3 ON. The Controller then uses the following default addresses:</p> <ul style="list-style-type: none">▪ Controller IP: 192.168.1.199▪ Gateway: 192.168.1.198▪ Subnet: 255.255.255.0 <ol style="list-style-type: none">1. Connect the Controller to your PC via the Controller's Ethernet port.2. Set DIP switches 1, 2 and 3 to ON.3. Power cycle the Controller.4. Using a web browser from a PC on the same subnet as the Controller, enter the default IP address of the Controller as follows: <code>http://192.168.1.199/cloud/</code> The Sign In dialog displays.5. Enter cloud for the username, then GGLcloud for the password and press Enter. The Gallagher Cloud Controller Configuration web page displays.6. Select the required link to configure the Controller as needed.7. When finished, set DIP switches 1, 2 and 3 to OFF. |

8. Configure the site

Configure the site using the [SMB Installer Portal](#). Configure Areas, Inputs, Outputs, Doors, then click **PUBLISH** to download the configuration changes to the controller.

Note: the default configuration within the Installer Portal – might have components that are not required for your site set up. If you are not using these components delete them from the configuration.

For configuration instructions, refer to the [Help Centre for Installers](#).

9. Test the site

Test Mode allows technicians to install, configure, and test an SMB site without alarming others by setting off sirens or other devices activated in response to an alarm. Test mode also prevents Site Managers, guards, and monitoring services from responding to alarms generated while the system is being tested.

1. Click **Enable Test Mode** from the **Site Actions**
2. Test Mode can only be enabled for a period – set the time for Test Mode to expire
3. If Guarding or Monitoring is enabled, a warning will display advising the Technician to inform the Monitoring station or Guarding company.
4. Test buttons will appear next to the Outputs. Alarm Relays are bypassed, Technicians can 'chirp' test outputs from this screen.
5. Click the **Test button** next to each Output
6. Once testing is complete click **Disable Test Mode** to disable it immediately, or it will automatically disable at the set expiry time.

Note: Once a site is activated, Test mode can only be entered when Installer Mode is enabled.

10. Initialise tampers

The SMB controller has two tamper detectors. The front optical tamper detector will sense when the cabinet door has been opened. The rear optical tamper detector will sense when the cabinet is removed from its mounting surface.

When you have finished wiring the devices and no longer need to access the cabinet:

1. Close and lock the cabinet door using the key provided.
2. Within the [SMB Installer Portal](#), click the controller at the top of the hardware tree.
3. Within the site's controller lightbox, select **Restart**.

Note: If the cabinet you are using does not support the use of these optical tampers, this can be disabled.

11. Activate the site

When the site is activated, it will become operational and billing will commence. A site can be activated as soon as the system is operational, allowing the Key Account Holder to start using the system before you have fully completed the installation.

Select **Activate Site**. This will send an 'Account Activation' email to the Key Account Holder. The Key Account Holder will need to follow the instructions in the email to download the Gallagher SMB App and accept their credentials.

Note: If you are unable to onboard the Key Account Holder, ensure they have a PIN or pattern set on their phone.

The site has now been handed over to the customer. The SMB Installer Portal changes to 'read-only' for the site. If you need to make additional configuration changes, the customer must enable **Installer Mode** within the **Settings** of the SMB App.

Controller Run LED flash patterns

| Flash | Pattern | Meaning |
|------------------------------------|---|---|
| Short flash Long flash (1 s cycle) | 100 ms on, 250 ms off 400 ms on, 250 ms off | Boot code monitor running, network unplugged |
| Half flash | 450 ms on, 50 ms off (2Hz flash) | Controller resetting |
| Fast | 130 ms on, 130 ms off (4Hz flash) | Initialising |
| 1 flash | 500 ms on, 500 ms off (1Hz flash) | Normal running |
| 2 flashes | 2 flashes - pause (each flash is 50 ms on, 400 ms off, 1.2 s pause) | Controller is operating, connected to the cloud but has no configuration |
| 3 flashes | 3 flashes - pause (each flash is 50 ms on, 400 ms off, 1.2 s pause) | Controller has a valid set of keys but has not connected to the cloud |
| 4 flashes | 4 flashes - pause (each flash is 50 ms on, 400 ms off, 1.2 s pause) | No private keys or certificate loaded, so will be unable to authenticate with the cloud. Contact Gallagher Technical Support. |
| 5 flashes | 5 flashes - pause (each flash is 50 ms on, 400 ms off, 1.2 s pause) | Controller has a connection to the cloud but either the cloud has failed to authenticate the controller, or the controller has failed to authenticate the cloud. Contact Gallagher Technical Support. |
| 6 flashes | 6 flashes - pause (each flash is 50 ms on, 400 ms off, 1.2 s pause) | Controller does not have runnable firmware. Contact Gallagher Technical Support. |

Technical specifications

| Controller | Value |
|-----------------------------------|-----------------------------------|
| Voltage | 9 Vdc - 16 Vdc |
| Current without devices connected | 110 mA |
| Maximum current per RS485 port | 750 mA |
| Temperature range | -10 °C to 70 °C (14 °F to 158 °F) |
| Humidity | 0 - 95% non-condensing |
| 10/100BaseT Ethernet port | 1 x 10 Mbs/100 Mbs |

| I/O boards | Value |
|----------------------------------|---|
| 8In Board operating current | 50 mA DC (all inputs terminated with 4k7 resistors) |
| 8In Board power rating | 0.68 W |
| 8In 4Out Board operating current | 45 mA DC (relays OFF) 200 mA DC (relays ON) |
| 8In 4 Out Board power rating | 0.61 W (relays OFF) 2.72 W (relays ON) |
| Fuse | Onboard 1 A resettable polyfuse |

| Reader | Value | | |
|--------------------------|--|-------------------|----------------------|
| Voltage | 9 Vdc - 16 Vdc | | |
| Current | | Idle ¹ | Maximum ² |
| | T11 at 9 Vdc | 106 mA | 176 mA |
| | T11 at 13.6 Vdc | 80 mA | 142 mA |
| | T15 at 9 Vdc | 110 mA | 168 mA |
| | T15 at 13.6 Vdc | 81 mA | 136 mA |
| | T30 at 9 Vdc | 130 mA | 241 mA |
| | T30 at 13.6 Vdc | 87 mA | 160 mA |
| Temperature range | -35 °C to +70 °C Direct sunlight may increase the internal reader temperature above the ambient temperature level | | |
| Humidity | 0 - 95% non-condensing | | |
| Environmental protection | IP68 ³ | | |
| Impact rating | IK07 ³ | | |

| | |
|---|--|
| Unit dimensions | T11 Reader: Height 115 mm (4.5 inches) Width 70 mm (2.8 inches) Depth 12 mm (0.5 inches) |
| | T15 Reader: Height 139 mm (5.47 inches) Width 44 mm (1.73 inches) Depth 23 mm (0.9 inches) |
| | T30 Keypad Reader: Height 118.0mm (4.65 in) Width 86.0 mm (3.39 in) Depth 26.7 mm (1.05 in) |
| Maximum number of access controlled doors on one SMB controller | 10 |
| Standards and compliance | FCC, RCM, CE, RoHS |

¹ The reader is idle

² Maximum reader current during credential read

³ Environmental protection and impact ratings are independently verified