



Gallagher Command Centre

OneLink

Technical Information Paper

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group, and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2026. All rights reserved.

Important: If you received this document along with your Command Centre installation media, or via another similar channel then it may be out of date with respect to the functionality/behaviour of the cloud, and of Gallagher Mobile Apps, which are distributed through platform App Stores and may be more recent than your Command Centre installation.

It is recommended you refer to the latest revision of this document, which can be found here:

https://resources.security.gallagher.com/Technical_Resources/Technical_Information_Papers

Contents

1	Background	4
2	Architecture	4
2.1	Architecture Overview	4
2.2	Cloud Security	5
2.3	Messaging	5
3	Controller Registration	7
3.1	Overview	7
3.2	Registration process	7
3.3	Technical information	7
4	Supported Hardware	8
5	OneLink Deployment Considerations	8
5.1	Inter-controller communications	8
5.2	Internet connectivity	8
5.3	Data usage	8
5.4	OneLink performance	9
6	Regions	9
7	Network Configuration Details	10
7.1	On Premises	10
7.2	Controller	10
8	Data Storage and Retention	11
9	Data Transmission	11
9.1	Data Visibility	11
10	Controller Authentication	12
11	Security Controls	12
11.1	Cloud Services	12
12	Monitoring and Response	13
13	Security and Penetration Testing	13

1 Background

OneLink utilises Gallagher Cloud Services to enable controllers to connect to the on-premises Command Centre Server over the internet. This enables a secure but simplified connection in scenarios that would otherwise require complex networking solutions, such as:

- When the controller is located at a site that is remote, mobile, or has limited networking infrastructure
- When only a mobile data connection is available
- When restrictive networking policies are in place

The OneLink solution described in this document depends upon the Gallagher Cloud API Gateway. The technical information paper for the Gallagher Cloud API Gateway can be found at:

<https://gallaghersecurity.github.io/r/commandcentre-cloud-api-gateway>

2 Architecture

2.1 Architecture Overview

The OneLink solution encompasses a cloud-hosted instance of the Controller Service, and associated services and configuration options necessary to connect the Controller and Command Centre to the cloud service.

The Controller Service is the component of Command Centre responsible for managing network connections with controllers and dispatching incoming and outgoing messages. It implements message queuing, handling, and routing of messages between Controllers and Command Centre Server but does little processing of its own. The Controller Service maintains a secure WebSocket connection with each controller, and interfaces with Command Centre Server via the Web API. Typically, the Controller Service is deployed as a service running on Windows Server alongside Command Centre (on the same machine), but when it is deployed to the cloud it is referred to as the Controller Gateway. A site may use both the Controller Service (for controllers on the local network) and the Controller Gateway (for controllers connected via OneLink over the internet) at the same time.

In essence, the Controller Gateway is a cloud-deployed version of the regular on-premises Controller Service, hosted on Amazon Web Services (AWS). It maintains a secure WebSocket connection with each connected controller and routes messages from those controllers to the on-premises Command Centre Server Web API via the [Gallagher Cloud API Gateway](#). This differs from the on-premises Controller Service, which sends requests directly to the Command Centre Web API without using the Gallagher Cloud API Gateway as a proxy. The Controller Gateway periodically polls Command Centre to pull any new messages that need to be delivered to a controller. The flow of messages between the controller and Command Centre is explained in more detail in Section 2.2.

Each controller connected to Command Centre may be communicating via a different instance of the Controller Gateway, particularly if the controllers are spread across multiple geographic regions. There is no current limit to the number of Controller Gateway instances that Command Centre can accept simultaneously. Likewise, a Controller Gateway can manage connections from any number of controllers at once. A controller may only be connected to a single Controller Gateway at a time.

The Controller Registration Service is part of the OneLink solution but runs as a separate cloud microservice. It maintains a repository of mappings between controllers and Command Centre sites, which is accessed by the Controller Gateway to determine which site each controller should be connected to. A controller becomes associated with a particular site when Command Centre Server sends a registration request to the Controller Registration Service – this occurs whenever a controller is configured as a cloud controller in Command Centre. The controller registration process is explained in greater detail in section 3.

Another part of the OneLink solution is the Trusted Issuer Service, this is a separate cloud microservice that provides the controller with signed lists of trusted certificate issuers, certificate revocations, and revoked signing certificates. This allows the controller to establish a chain of trust for authenticating communications with the Controller Gateway and the Controller Registration Service. More details about controller authentication can be found in section 10.

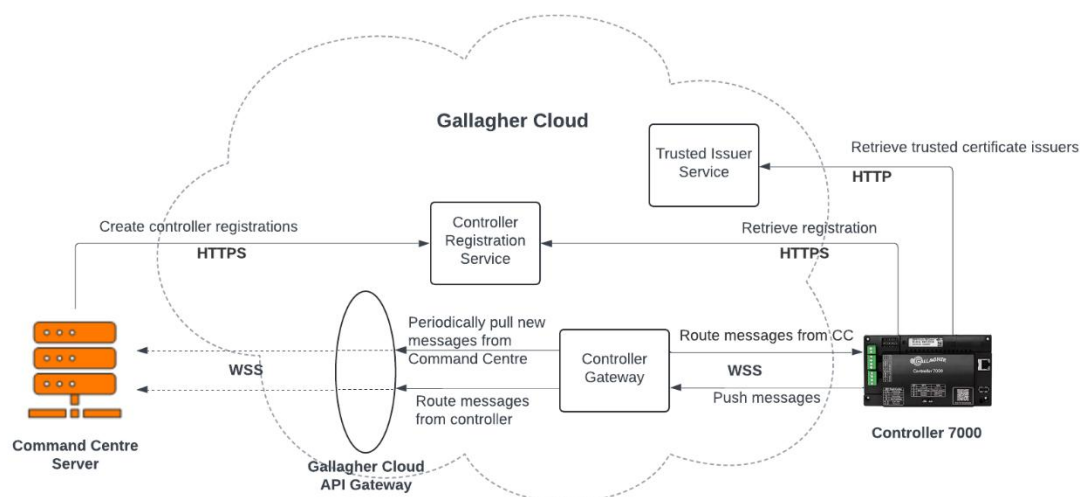


Figure 1: OneLink architecture overview

2.2 Cloud Security

To ensure the resilience and integrity of the OneLink platform, our cloud architecture incorporates multiple layers of AWS-native security controls. These services work together to provide protection against network-level threats, web-based attack vectors, and software vulnerabilities:

- AWS Shield – Provides managed, always-on protection against the most common network and transport-layer DDoS attacks. This helps maintain service availability even during high-volume or malicious traffic events.
- AWS AF (Web Application Firewall) – Enforces customizable rule sets to block common web exploits (such as injection attacks, malicious payloads, or unauthorized access attempts). In addition to rule-based filtering, WAF automatically identifies and mitigates anomalous or suspicious request patterns, adding an intelligent layer of defence against unexpected client behaviour and potential DDoS-style traffic spikes.
- AWS API Gateway - Adds an authenticated and encrypted entry point with IAM/Cognito/Lambda-based access control, integrated WAF inspection, request validation, and built-in throttling to prevent abuse and traffic spikes.
- Amazon ECR Image Scanning – Continuously scans container images used by the Controller Gateway application, identifying known CVEs and software vulnerabilities early in the deployment pipeline. This strengthens supply-chain security and supports proactive remediation before code is promoted to production.

2.3 Messaging

The primary role of the Controller Gateway is to facilitate the transfer of messages between a controller and Command Centre Server. This section describes the flow of messages in each direction.

2.3.1 Controller to Command Centre Server

A secure WebSocket connection is maintained between each connected controller and the Controller Gateway. A single instance of the Controller Gateway may manage connections from many different controllers. Controllers generate messages and push them to the Controller Gateway via the secure WebSocket connection. Incoming messages from any given controller are associated with a particular Command Centre Server by the controller registration. The Controller Gateway routes the messages to the appropriate Command Centre Server via the Gallagher Cloud API Gateway.

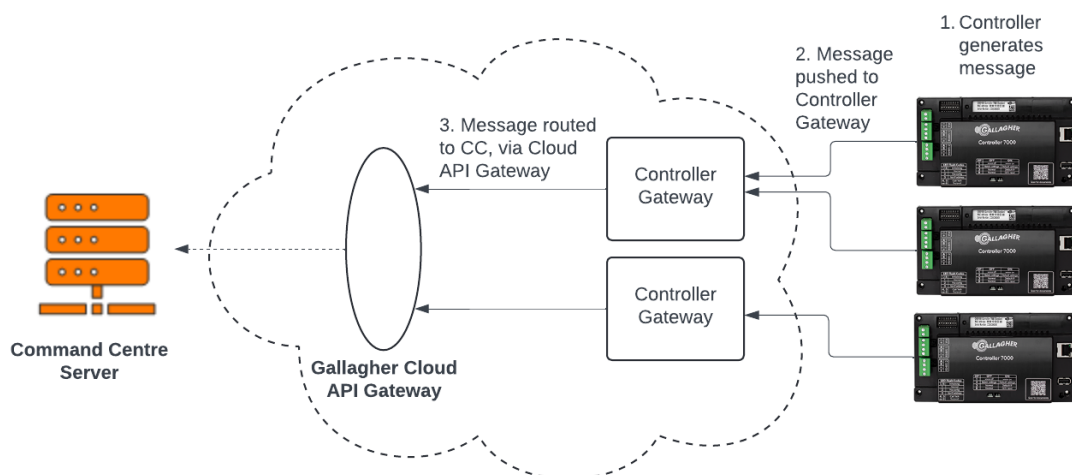


Figure 2: Flow of messages from controllers to Command Centre via OneLink

2.3.2 Command Centre to Controller

Messages generated by Command Centre are added to a local message queue. Unlike the controller, Command Centre Server never pushes messages to the Controller Gateway. Instead, the Controller Gateway (via the Gallagher Cloud API Gateway) periodically polls Command Centre for any queued messages that have not yet been delivered. When messages are available, Controller Gateway retrieves them and delivers them each to the appropriate controller over the secure WebSocket connection. This design ensures that Command Centre does not make any outgoing requests to Controller Gateway, providing two important advantages:

1. **Security:** no additional network configuration (e.g. opening ports) beyond what is necessary for the Gallagher Cloud API Gateway.
2. **Performance:** the Controller Gateway can manage message throughput and batching of large messages according to the bandwidth of each controller.

Note that Command Centre supports connections from multiple Controller Gateways at once, and each Controller Gateway is only permitted to retrieve messages bound for controllers that are connected via that same Controller Gateway.

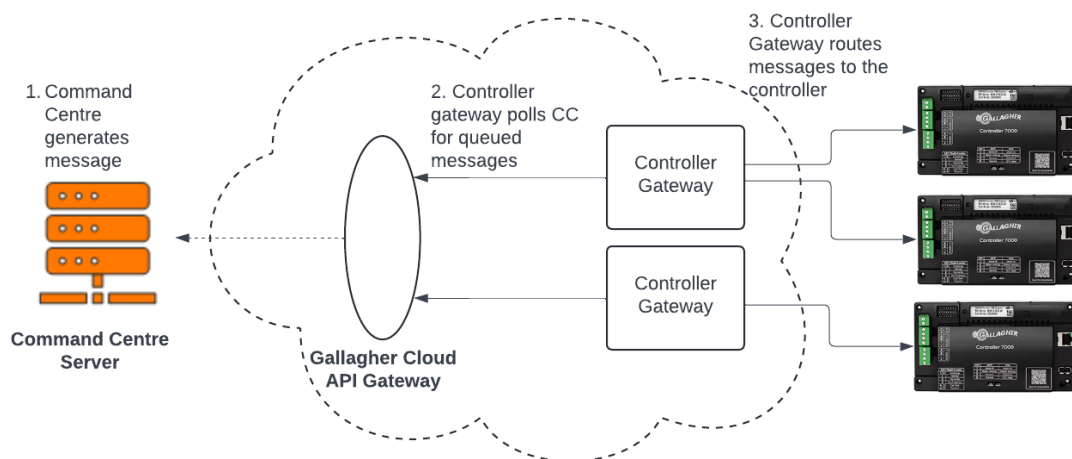


Figure 3: Flow of messages from Command Centre to controllers via OneLink

3 Controller Registration

3.1 Overview

The Controller Registration Service is part of the OneLink solution but runs as a separate cloud microservice. It maintains a repository of mappings between controllers and Command Centre sites, which is used to:

- Inform the Controller Gateway which site each controller should connect to. If a controller has not been registered against a site, then it cannot connect via OneLink
- Inform a controller that it has been configured for OneLink, and provide the URL of the Controller Gateway for the controller to connect to

Registrations are added to the repository whenever a controller is configured as a cloud controller in Command Centre. A registration request, containing the MAC address and serial number of the controller, is sent from Command Centre to the Controller Registration Service. These controller details are then stored in the cloud along with the ID of the site that initiated the registration. When the controller later requests a connection with the Controller Gateway, it can be routed to the correct site.

3.2 Registration process

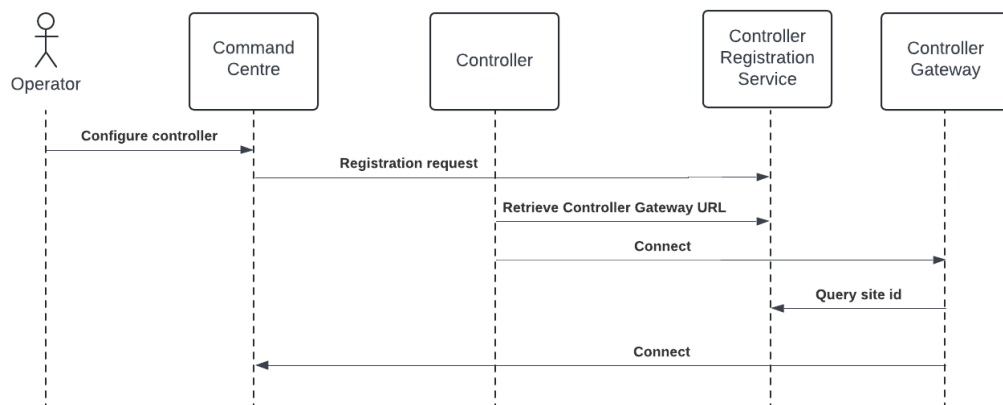


Figure 4: Sequence diagram of the controller registration process

1. A Command Centre operator creates a controller item in Command Centre and checks the “OneLink” option
2. Command Centre Server sends a registration request to the Cloud Controller Registration Service, which adds the registration to the cloud database, linking the controller MAC address and the site.
3. The unconfigured controller is powered on with DIP Switches 2 and 7 on
4. The controller retrieves the Controller Gateway URL from the Controller Registration Service
5. The controller attempts to connect to Controller Gateway using the provided URL
6. The Controller Gateway queries the Controller Registration Service to determine which site the controller should connect to
7. The Controller Gateway forwards the connection request to the site via Gallagher Cloud API Gateway
8. Command Centre authenticates the controller, and a connection is established. Communication between the Controller and Command Centre Server continues through the Controller Gateway.

3.3 Technical information

In order to create a controller registration both the MAC address and serial number of the controller must be configured in Command Centre. Although the MAC address alone is enough to uniquely identify the controller, the serial number is also required to reduce the risk of registering the wrong MAC address. The serial number and MAC address are cross-checked against a database of Gallagher controllers, and if they do not both correspond to the same controller then the registration request is rejected.

It is possible that two sites may both attempt to register the same controller, whether accidentally or maliciously. In this scenario, the site that made the registration first is given precedence, and the second site will be notified that the controller has been previously registered to another site. If your controller has been registered to another site, contact customer support to resolve the issue.

A registration is automatically deleted if the controller has not connected via OneLink within 14 days of the registration being created. If the controller does connect within that time, the registration is retained until the controller item is deleted in Command Centre.

4 Supported Hardware

OneLink is supported on all C7000 series controllers.

5 OneLink Deployment Considerations

As previously described, as the Controller Gateway is essentially a replication of the Controller Service, Controllers connected via OneLink will operate with the same functionality as those connected via the local network.

That said, careful consideration should be given to the Controller application when choosing an appropriate connection method and data plan. Controllers deployed to remote sites with little activity will have a different requirement to very busy sites.

5.1 Inter-controller communications

OneLink Controllers that require inter-controller communication, need to be able to talk to one another on a local network. There is no provision for OneLink connected controllers to communicate with each other via the cloud.

5.2 Internet connectivity

The controller requires a stable internet connection and access to DHCP and DNS services.

If a firewall is in place, it must allow TCP outbound traffic from the controller to:

- Controller Registration Service: <https://controller-onboarding.security.gallagher.cloud:443>
- Controller Gateway: <wss://controller-gateway.security.gallagher.cloud:443>
- Trusted Issuer Service: <http://controller-onboarding.security.gallagher.cloud:80>

Users should consider the specific application requirements when choosing the connection method.

High security or areas with strict performance needs may be best placed to consider standard connectivity methods utilising the local network.

OneLink's advantage is flexibility. Controllers may connect to OneLink in a variety of ways; via basic cellular routers, via an office internet connection (see section 7 Network Configuration Details) or other (such as Starlink).

However, whilst Controllers retain the ability to operate in an "offline" mode, overall system operation and performance may be impacted if a stable and performant internet connection commiserate to the application is not provided.

5.3 Data usage

Whilst Controller-Server communications are generally modest in bandwidth, certain actions/configurations could result in larger data usage.

The usage and update profile of the controller should be considered when deciding on an appropriate data plan.

As a guide:

- Basic operation (based on a single software update, 300 badging events and general background comms) – approx. 200MB per month per controller.
- Set up an access zone with 100 cardholders and assigned access to the door on the controller – approx. 0.3MB of data.
- Set up an access zone with 1000 cardholders and assigned access to the door on the controller – approx. 3.0MB of data
- Controller software update – approx. 40MB (additional device software updates would increase this).

5.4 OneLink performance

Whilst every effort is made to ensure that the OneLink system itself is performant, as a cloud service there may be, on occasion, an increased latency in periods of extended high load.

6 Regions

OneLink (specifically the Controller Gateway) is deployed in both the Australian and US AWS regions. Controllers connect to OneLink through a single, fixed URL, and OneLink intelligently routes each connection to the Controller Gateway instance closest to the controller's geographic location.

When a controller and its associated Command Centre server are located in the same region (for example, both in the US), the OneLink data-transport pipeline remains entirely within that region under normal operating conditions. This provides a clear data-residency path, which can be important for customers who prefer their data to remain within a specific geographic boundary during transmission. OneLink does not store customer data.

OneLink also supports deployments where controllers and Command Centre servers are located in different regions. In these cases, OneLink routes messages from the Controller Gateway in the controller's region to the Gallagher Cloud API Gateway in the region where the Command Centre server is hosted. Command Centre can simultaneously support connections from multiple Controller Gateway instances across regions.

From a resilience perspective, OneLink includes disaster-recovery (DR) capabilities that allow connections to be temporarily rerouted through an alternative region (e.g., via Australia if the US region becomes unavailable). This ensures service continuity but may result in data being processed outside the controller's or Command Centre's usual region during DR events. This behaviour aligns with common cloud patterns for multi-region failover and high availability and occurs only in exceptional circumstances.

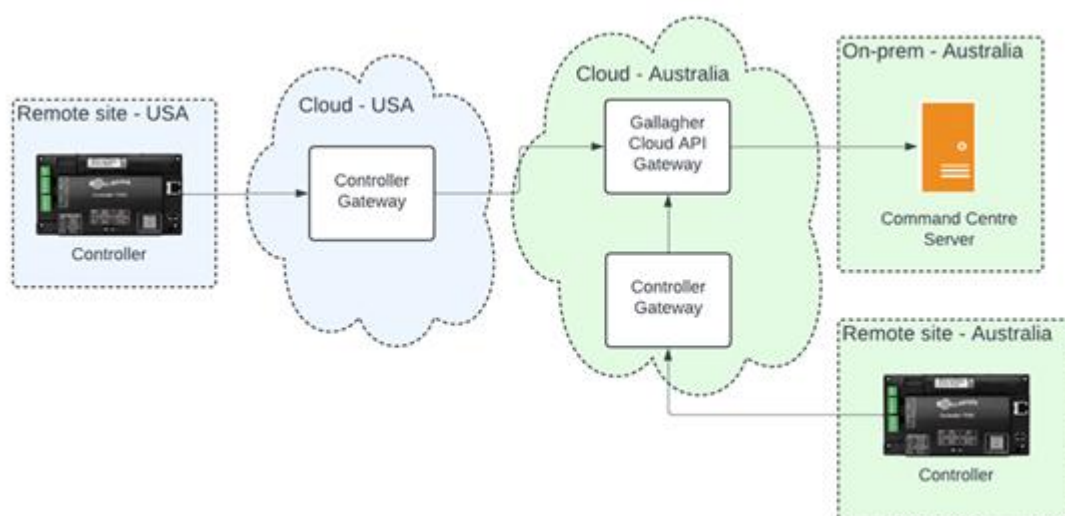


Figure 5: Cross-regional support. A controller in one region can connect to a Command Centre Server in another region. Messages are forwarded from the Controller Gateway hosted in the region local to the controller to the Gallagher Cloud API Gateway hosted in the region local to Command Centre Server.

7 Network Configuration Details

7.1 On Premises

All communication between the Controller Gateway and Command Centre uses the Gallagher Cloud API Gateway as a proxy. No additional network configuration is required beyond what is outlined in the [Gallagher Cloud API Gateway Technical Information Paper](#). Similarly, the Controller Registration Service can be accessed by Command Centre if Command Centre Cloud is configured and connected.

7.1.1 Firewall Recommendations

Configure your firewall to allow TCP outbound traffic on port 443 with a source of your internal Command Centre server, and destination of the following DNS or IP addresses.

Note: There is no need to allow any inbound traffic to your Command Centre server.

If you are configuring firewall rules based on IP address, please allow the following static IP addresses:

Australian Command Centre Cloud:

DNS address: **commandcentre-ap-southeast-2.security.gallagher.cloud**

IP addresses: **52.62.211.7 and 54.79.91.203**

Australian Gallagher Gateway Region:

DNS address: **commandcentre-api-au.security.gallagher.cloud**

IP addresses: **3.106.1.6 and 3.106.100.112**

United States Gallagher Gateway Region:

DNS address: **commandcentre-api-us.security.gallagher.cloud**

IP addresses: **44.193.42.111 and 3.209.194.103**

Global Cloud Services API Gateway:

DNS address: **services.security.gallagher.cloud**

IP addresses: **15.197.141.103 and 76.223.78.39**

7.2 Controller

The controller does not require any direct connection to the on-premises Command Centre server because all communications are routed via the cloud-hosted Controller Gateway. The controller requires a stable internet connection and access to DHCP and DNS services. If a firewall is in place, it must allow TCP outbound traffic from the controller to:

- Controller Registration Service: <https://controller-onboarding.security.gallagher.cloud:443>
- Controller Gateway: <wss://controller-gateway.security.gallagher.cloud:443>
- Trusted Issuer Service: <http://controller-onboarding.security.gallagher.cloud:80>

Although the Trusted Issuer Service is communicating on HTTP port 80, the trusted issuer data is publicly available and cryptographically signed to allow the controller to authenticate it as genuine and untampered with.

8 Data Storage and Retention

Certain site data is retained in the cloud for any site that uses Gallagher Cloud Services. To read more about data retention for Gallagher Cloud Services in general, refer to the [Gallagher Cloud API Gateway Technical Information Paper](#). This section will cover only the data specifically relevant to OneLink.

For each controller that uses OneLink, the following data is retained in persistent storage:

- Controller MAC address
- Controller Serial number
- The identifier for the site the controller is associated with

This data is necessary for the Controller Gateway to determine which site a controller should be connected to. It is held in an AWS DynamoDB database, which employs encryption-at-rest and is accessible only by processes running within the Gallagher Cloud VPC. The data can be deleted from the cloud by deleting the controller item in Command Centre.

We may temporarily log message metadata for diagnostic purposes. We will never log the content of messages, nor will we save message content to persistent storage. Logs may include the following data:

- The message type
- Date and time a message was received
- Whether a message was successfully delivered
- Reason for failure of delivery of a message
- The MAC addresses of controllers that connect via OneLink

We may also collect anonymised aggregate statistical information (e.g. the number of messages processed) for performance analysis purposes.

9 Data Transmission

All controller communications with the Controller Gateway and the Controller Registration Service are authenticated using mutual TLS certificates (384-bit ECDSA). We support TLS 1.3; older protocols are disallowed, which mitigates most encryption related security risks. The controller communicates with the following cloud services:

- **The Controller Registration Service:** data transfer between the controller and the Controller Registration Service uses encrypted HTTPS.
- **The Controller Gateway:** data transfer between the controller and the Controller Gateway uses encrypted WSS.
- **The Trusted Issuer Service:** the data provided by the trusted issuer service is signed by an edge signing key with a root of trust to a root key stored securely offline. The controller uses a Gallagher Production Root certificate to trust this data and ensure it has not been tampered with.

All communication between Command Centre and the Controller Gateway is routed via the Gallagher Cloud API Gateway. Communication between Command Centre and the Gallagher Cloud API Gateway is described in the [Gallagher Cloud API Gateway Technical Information Paper](#).

9.1 Data Visibility

It is important to note that the Controller Gateway has visibility into messages that transit through it.

The Controller Gateway may inspect the contents of a message in order to route it to the correct Command Centre Web API endpoint. Messages are held in an in-memory queue and are deleted once they have been delivered. We will never modify or extract message content, nor will we save message content to persistent storage.

Messages may contain any of the following:

- Site-specific information such as the names of doors and zones
- Item configuration such as schedule times

- Alarms
- Events, including the ID numbers of relevant cardholders and cards
- Cardholder names
- Override commands, such as instructions to open a door

10 Controller Authentication

All controller communications with the Controller Gateway and the Controller Registration Service are secured using mutual TLS (384-bit ECDSA).

Controllers periodically query the Trusted Issuer Service to retrieve signed lists of trusted certificate issuers, certificate revocations, and revoked signing certificates. Although the publicly available information provided by the Trusted Issuer Service is sent over HTTP, the controller authenticates the attached signature using a Gallagher Production Root certificate stored on the C7000 Edgelock. This ensures the trusted issuer information is genuinely Gallagher provided and has not been altered or otherwise tampered with. The controller uses the signed trusted issuer information to authenticate the Controller Gateway and the Controller Registration Service.

The first time a controller connects to Command Centre, it must authenticate by demonstrating possession of a genuine Gallagher Factory Key (ECDSA-384) signed by a trusted CA. Command Centre then pins the controller's TLS certificate. For any subsequent connections from the same controller the controller's TLS certificate is compared to the pinned certificate, and the connection is rejected if the certificates do not match. It is important to understand that the TLS handshake and the Gallagher Factory Key authentication are carried out by the Controller Gateway cloud service; Command Centre delegates trust to the Controller Gateway to execute this aspect of controller authentication.

11 Security Controls

11.1 Cloud Services

Our cloud services are securely hosted using Amazon Web Services. They are isolated from other Gallagher or external services using an AWS Virtual Private Cloud (VPC). Databases are segregated and provisioned according to the needs of each application, maintaining clear system boundaries to ensure data protection.

Users and services within our cloud environment are granted only the minimum permissions necessary for their tasks. This approach ensures that access is limited and controlled, reducing the risk of unauthorised actions.

Platform updates are applied frequently to ensure we consistently use the most up-to-date operating systems with the latest security patches. We employ an automated vulnerability management process which alerts if any third-party software components we use are identified in a vulnerability database such as (but not limited to) the public CVE database.

All administrative users accessing our cloud infrastructure require a current Security Certificate of Approval from the NZ Government Private Security Personnel Licensing Authority (PSPLA). Two-factor authentication and strong password policies are enforced for all access to cloud infrastructure. We also employ automatic rotation of user access keys and automatic deletion of inactive accounts.

12 Monitoring and Response

A 24/7 DevOps support team is available to address any critical system events or escalations that are raised. These events may come to the attention of the support team by the following channels:

- Customer reports
- Our automated monitoring systems
- Identified by the support team themselves

We employ automated analysis of both application and database logs, continuous monitoring of CPU, disk and network resource usage and application-specific health monitoring, with notifications to keep our support teams informed of any issues. We also employ monitoring tools to detect malicious activity and unusual behaviour.

We run simulated user interactions against our cloud systems to help identify availability and performance issues and ensure services meet the expected standard.

Notice of any incidents or outages that may affect customers will be provided via our Channel Partners.

13 Security and Penetration Testing

Gallagher employ internal security and penetration testing staff. Our internal security staff hold a key role in the development of our cloud services, providing expertise, security reviews and internal penetration testing.

An external specialist security company will be engaged to do a comprehensive review annually, or more frequently with each major release as required. Prior reviews have been conducted by CyberCX (previously Insomnia Security), and executive summaries of the findings are available by request.

We are open to customer or otherwise externally arranged penetration testing, however we require advance notice and approval from Gallagher to avoid disruption of our services which may impact other customers.