Gallagher Command Centre

Cloud API Gateway

Technical Information Paper

Copyright © Gallagher Group Limited

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2022. 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received this document along with your Command Centre installation media, or via another similar channel then it may be out of date with respect to the functionality/behaviour of the cloud, and of Gallagher Mobile Apps, which are distributed through platform App Stores and may be more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://gallaghersecurity.github.io/r/commandcentre-cloud-api-gateway

Contents

Copyright © Gallagher Group Limited

1 Background

The preferred way for third party developers and integrations to communicate with a Gallagher Command Centre server is using the REST API. This API is also used by Gallagher's Command Centre Mobile App for iOS and Android, and other Gallagher-developed utilities such as the Contact Tracing Report.

Technical documentation for the REST API can be found at https://gallaghersecurity.github.io/

1.1 Objective

Connectivity is a recurring problem that customers encounter when using the REST API.

The Command Centre server software is designed to run on a Windows Server machine, and is architected to be deployed on-premises, on a customer's internal corporate network. Most installations are deployed this way.

If client software connecting to the REST API is also on-premises, on the same corporate network, then this typically works well. However, increasingly REST API clients are represented by cloud-based, or other remote sources. Deployments where the client is remote can be difficult and costly to configure, often requiring approval from corporate IT, firewall reconfiguration, and other tasks.

The Gallagher Cloud API Gateway is designed to solve this connectivity problem.

1.2 Reference: Other Gallagher Cloud Services

The API Gateway is an additional service, which has different characteristics from Gallagher's other cloud services (such as used for Mobile Credential enrolment).

This document specifically discusses the API Gateway service and does not cover these other cloud services. Please refer to the following document for technical, security and privacy information regarding Gallagher's other cloud services:

https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security

https://gallaghersecurity.github.io/r/commandcentremobile-app-security

Copyright © Gallagher Group Limited

2 Architecture

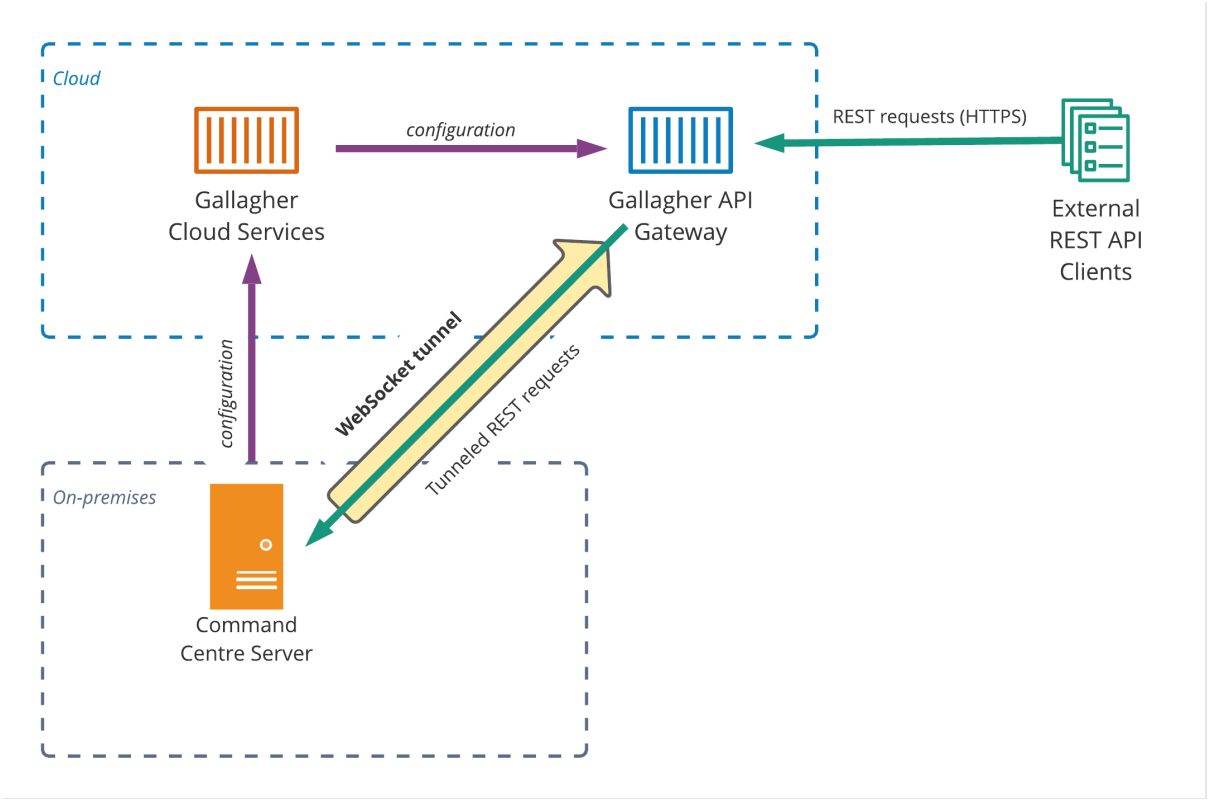
2.1 Overview

The Gateway tunnels REST API requests through to an on-premises Command Centre server.

It can accept requests from anywhere on the internet, allowing other cloud services or non-local clients to easily connect to the REST API.

Conceptually it fills a similar role to an HTTP reverse proxy such as Azure Application Gateway, AWS API gateway, HAProxy, or many web-server products that can act in such a role (Nginx, IIS, Apache).

The logical / network architecture of a Command Centre server using the Gateway is as follows:



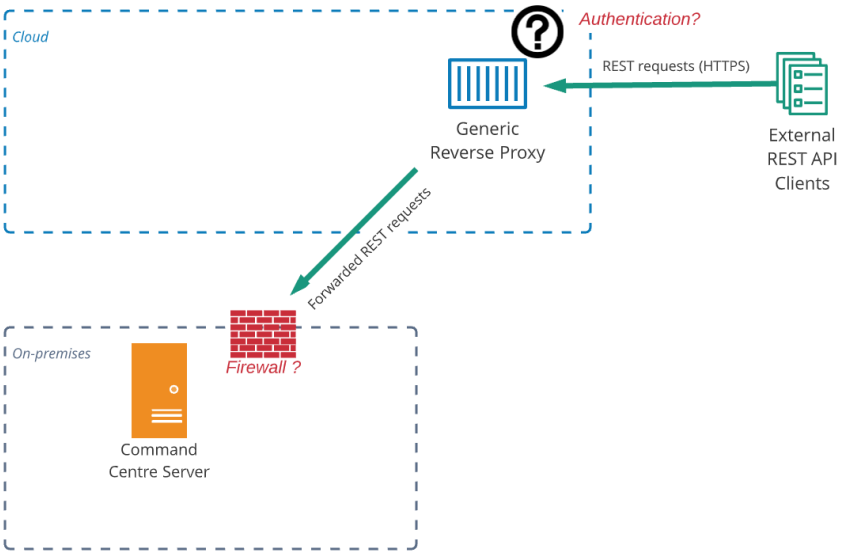
Copyright © Gallagher Group Limited

2.2 Differences between the Gateway and other reverse proxy solutions

It has always been possible to configure gateway-like services using other reverse proxy solutions, such as Azure Application Gateway, Nginx, HAProxy, etc.

Deploying such a solution requires you to solve several significant problems yourself.

Logical/network architecture of a generic reverse proxy solution:



Because the Gallagher API Gateway is purpose built for Command Centre, it has many significant advantages over a generic reverse proxy solution.

1. With other reverse proxy solutions, external REST API clients cannot use TLS client certificates for authentication in a way that is visible to the Command Centre server. This reduces the security of client connections.
   The Gallagher API Gateway has full support for TLS client certificates for REST and Mobile clients.
2. Other reverse proxy solutions need to connect directly to the Command Centre server to forward messages to it. This requires you either to open inbound firewall ports into your local network (which is a security risk) or configure a VPN to bridge your on-premises network with your cloud network (which can be difficult and costly). Local network reconfiguration also may break any firewall or VPN configuration, which may be difficult to track down and fix.
   The Gallagher API Gateway establishes a tunnel over an outbound HTTPS WebSocket connection to Gallagher's cloud services, which removes these problems.
3. Other reverse proxy solutions can be very complex to set up. Establishing that you have configured them correctly and securely can be a difficult task and may require external audit.
   The Gallagher API Gateway can be enabled by simply checking some boxes in Command Centre. Gallagher manage the technical details and ensure things are always secure and up to date.
4. Some other proxy solutions are not cloud-native (for example a custom deployment of Nginx or HAProxy). If you are using such a solution, then you may have service outages when you need to upgrade/reconfigure your proxy or experience a fault.
   The Gallagher API Gateway is built for the cloud. It uses multiple redundant services internally, allowing for zero-downtime upgrades, hardware and software fault tolerance, and scalability.

Copyright © Gallagher Group Limited

5. Other cloud-native solutions (such as AWS API Gateway) are fault tolerant and scalable, however they also may come with significant cost to operate and may require skill to administer.
   The Gallagher API Gateway has no direct cost and does not require any specialized cloud knowledge or skills.
   Note that the normal licensing cost associated with the on-premises REST APIs (or integrations that may use them) is still incurred, whether those APIs are accessed locally, or through the Gateway.

6. If you have a non-production Command Centre system (for example a test/staging server), then any generic reverse proxy must be deployed multiple times, using different URLs, which can be confused and misconfigured.
   The Gallagher API Gateway provides a single URL that your clients can connect to, and will intelligently route requests to the right system, based on authentication details such as client certificates and API keys.

7. Other reverse proxy solutions are not able to fully authenticate REST or Mobile clients, and so must forward all potentially valid traffic down to your Command Centre server.
   This may pose a security risk, as attackers may be able to send you malicious requests, or perform a Denial-of-Service attack, and does not allow you to have fine grained control over which REST or Mobile clients can use your proxy.
   The Gallagher API Gateway performs full authentication of both REST and Mobile clients itself, before sending anything to your Command Centre server. This allows device-specific control over Gateway usage and will block all unauthenticated requests at the Gateway, shielding your server from DoS-style attacks.

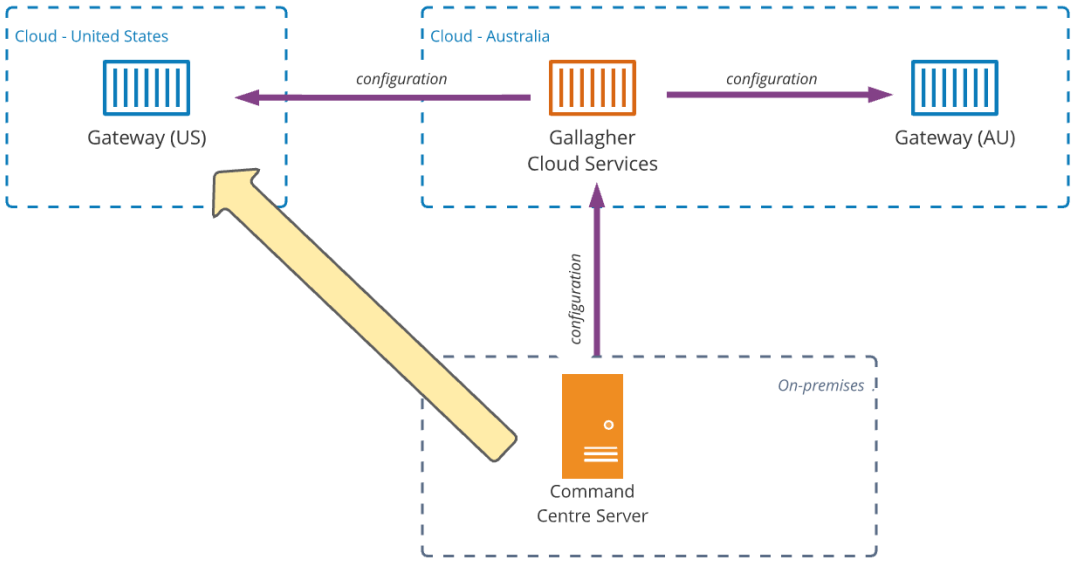
8. The Command Centre Mobile app can employ End-to-End encryption to fully protect requests that are sent through the Gallagher API Gateway. E2EE is a specialized technology that works in co-operation with the Gateway and could not be deployed as securely with a generic reverse proxy solution.

3 Regions

While Gallagher's other cloud services remain hosted in Sydney, Australia, the Gateway is designed to allow deployment of multiple instances in different regions. These are configured by the Australia-based cloud services, but once configured, run independently.

Gallagher will initially launch with a Gateway region in Australia, and a second in the United States of America.

Copyright © Gallagher Group Limited



You can configure your Command Centre server to connect to either region, so you can choose the one closest to reduce network latency and have control over where your data transits through.

We will add additional regions over time, depending on customer demand and other factors.
If you would like to use the Gateway, but there is a reason why you cannot use an existing region, please contact your regional Gallagher representative to discuss further.

Note:

- Each region has a different external URL for clients to connect to so you can ensure data is being sent to where you expect it.
- Gateway instances in one region will never send data to other regions. When you select a region, you are assured that your data will only transit through that region, and never to any others.
- A Command Centre server can only connect to a single region at a time.
- If you change the configured Gateway region, then you must reconfigure all your clients to match the new region.

Copyright © Gallagher Group Limited

4 Network Configuration Details

Each Gateway region has a single (logical) endpoint.
Internally we employ multiple redundant servers for failover and scalability.

Australian Gateway Region:

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

It has two static IP addresses: **3.106.1.6** and **3.106.100.112**

United States Gateway Region:

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

It has two static IP addresses: **44.193.42.111** and **3.209.194.103**

Communications with the Gateway take place solely using HTTPS over port 443.

Gallagher cloud services use TLS client certificates to identify each individual Command Centre server securely and uniquely. These client certificates are issued by the cloud to each Command Centre server the first time it connects. The Gateway uses the same TLS client certificate as our other cloud services to identify each Command Centre server.

4.1 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 above DNS or IP addresses. If you are configuring firewall rules based on IP address, please allow **both** static IP addresses.

You do not need to allow any inbound traffic to your Command Centre server.

4.2 Connectivity and Error handling.

The Gateway is designed to be transparent to end-users of the REST API. When making requests, you do not need to alter the payload, HTTP headers or client certificates that you use; these should all be the same as if you were connecting directly to the server's REST API via a local network connection. The only thing that you need change would be to replace the local URL with the cloud Gateway one.

For example, Local request:

```
<client certificate thumbprint e89ef121958c675c736efd3fdcd87ca31d502fde>
GET https://servername.yourcompany.local:8904/api/cardholders
Authorization: GGL-API-KEY F6F0-C8F0-60AF-7501-AFB9-C523-B2D3-1D3E
```

Equivalent Gateway request:

```
<client certificate thumbprint e89ef121958c675c736efd3fdcd87ca31d502fde>
GET https:// commandcentre-api-au.security.gallagher.cloud/api/cardholders
Authorization: GGL-API-KEY F6F0-C8F0-60AF-7501-AFB9-C523-B2D3-1D3E
```

When a REST or Mobile client makes a request to a Gateway, the gateway will authenticate the request to determine which Command Centre server to route it to. Requests which are not authenticated correctly will receive an HTTP 401 (Unauthorized) response.

Once authenticated, the Gateway will forward the request to that server, and hold the client request, waiting for the server's response. When the server replies, the Gateway will forward the response back to the external client.

Copyright © Gallagher Group Limited

If there is no open WebSocket tunnel for the configured server, the Gateway will respond with an HTTP 503 (Service Unavailable). Common causes of this response may include:

- Configuration information may take a few seconds to propagate from the Command Centre server out to all Gateway instances. If you receive a 503 error after changing configuration, wait 30 seconds and then try again.
- The client is connecting to a different Gateway region than the Command Centre server. Check that both are configured to use the same region.
- The Command Centre server is temporarily offline or disconnected from the Gateway. Check the status/overrides page of the Cloud Item in Command Centre for possible network errors.

5 Data Storage and Retention

To authenticate Servers, Clients, and route traffic correctly, Gallagher Cloud Services must hold the following information. This authentication information is replicated to all Gateway instances, which hold it in-memory. Gateway instances do not write this data to disk, log, or any other form of persistent storage.

- SHA256 hash of the Command Centre server's TLS client certificate public key, to authenticate the server.
- SHA256 hash of each configured Mobile App's TLS client certificate public key, to authenticate the mobile device.
- SHA256 hash of any pending mobile enrolment codes, to onboard new mobile devices.
- SHA256 hash of each configured REST Client's API Key, to authenticate the client.
- Additionally (if configured per REST client)
    - IP address filtering information
    - SHA1 thumbprint of the REST client's TLS client certificate

To reiterate: No REST API key, mobile enrolment code, or other sensitive information is ever held in Gateway instances, or other Cloud Services.

Gateway instances have no persistent storage. Configuration (the list of allowed clients, and their authentication information) is kept in-memory, and when new Gateway instances are deployed this is fetched anew from the central Cloud Services.

Central cloud services hold this information in a non-encrypted form at the application level; we employ full-disk encryption at the database level.

Copyright © Gallagher Group Limited

6 Data Transmission

All data transfer between Command Centre, the Cloud Services, Gateway Instance, Mobile Devices and REST API clients uses encrypted HTTPS.
We support only TLS 1.2 and TLS 1.3; older protocols are disallowed which mitigates most encryption-related security risks.

As of September 2021, the SSL Labs industry standard SSL Report scores an "A" when run against the Australian Gateway region. You can view the detailed report here:

https://www.ssllabs.com/ssltest/analyze.html?d=commandcentre%2dapi%2dau.security.gallagher.cloud&hideResults=on&latest

Communication between Command Centre and central Cloud services is authenticated using TLS client certificates (2048-bit RSA).

Communication between Command Centre and Gateway instances is authenticated using TLS client certificates (2048-bit RSA).

Inter-service communication between Gallagher Cloud Services and Gateway instances uses HTTPS / TLS 1.3 with certificate pinning.

6.1 Data Visibility

It is important to note that the Gateway has visibility into REST API requests that transit through it. This is inherent to the nature of the any reverse proxy/gateway solution; for example, if you configured an Azure Application Gateway, then Microsoft would have visibility of any traffic that was sent via that gateway as well.

REST API requests may contain any of the following, depending on how the external clients are using it:

- REST API Keys.
- Cardholder Personal Information such as names, phone numbers, photos, and last known location.
- Site-specific information such as names of doors, zones.
- Item configuration such as schedule times.
- Alarms.
- Override commands such as an instruction to open a door.

Gallagher policy is to never inspect, modify, save, log, or extract any sensitive or request-specific data such as the above.

We are aware that use of the Gateway requires customers to place significant trust in Gallagher, and we aim to fulfil that trust by employing strict security controls, and external audits, as per section 7, and additionally by implementing technical measures such as end-to-end encryption to further protect your data where possible.

6.2 End-to-End Encryption

Data transmitted using the Gallagher Command Centre Mobile app is protected by End-to-End encryption (E2EE) and is not subject to the above data visibility section. The Gateway does not have visibility into any of the data sent or received by the Mobile app and it is not possible for Gallagher, nor any other potential attacker to observe or modify it.

The Mobile app, when using the Gateway, employs the same ECIES encryption technology as our Mobile Connect app. E2EE is always enabled for Gateway connections and cannot be switched off. It remains disabled for direct (non-gateway) connections.

Copyright © Gallagher Group Limited

E2EE is not currently available for third party integrations using the REST API due to the significant technical challenges involved in implementing ECIES correctly. Please contact your Gallagher representative if you would like to discuss further.

For more detailed information on end-to-end encryption, please refer to the following Technical Information Paper: https://gallaghersecurity.github.io/r/mobileconnect-end-to-end-encryption

7 Security Controls

7.1 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.

Strict firewall and access control rules are in place protecting all administrative functions and other endpoints.

All administrative users accessing our cloud infrastructure require two-factor authentication and strong passwords.

Services within the cloud environment are only allowed access to the minimum set of resources they require to function (e.g., they are only allowed to fetch and connect to the sole database / key storage they require and cannot access resources for any other services).

Platform updates (for example Operating System security patches) are applied on a daily basis where required. We employ automated scanning tools which alert if any third-party software components we use are identified in a vulnerability database such as (but not limited to) the public CVE database.

8 Monitoring and Response

We employ automated analysis of both application and database logs, continuous monitoring of CPU, disk and network resource usage and application-specific health monitoring.

Alerts are automatically generated and immediately sent to Gallagher. These alerts, along with service status, are monitored 24 hours per day.

Notice of any incidents or outages that may affect customers will be provided via our Channel Partners, or a direct email alert system, which customers may sign up to by contacting their Channel Partner.

9 Security and Penetration Testing

Gallagher employ internal security and penetration testing staff, who hold a number of security certifications.

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.

Copyright © Gallagher Group Limited

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.

10 Anonymized Usage data/Telemetry

While we strictly do not capture any identifiable information from requests that pass through the Gateway, we may capture aggregated usage statistics, related to the generic purpose of Gateway requests, as well as request volumes and response times.

Data is captured and processed in accordance with our Gallagher Privacy Policy, which can be found here: https://security.gallagher.com/en-NZ/Legal/Cloud-API-Gateway-privacy-policy

We do this to improve the performance and reliability of our services and improve future product features.

All such data is anonymized and aggregated.

For example, if an external REST client does the following:

- Search for cardholders named "bob", returning 6 results.
- Load details of the first found cardholder, returning all information such as emails, phone numbers.
- Update the cardholder, editing their date of birth.
- View the current alarms in the system, returning 20 results.
- Add notes to three of them and then process all 20 in a bulk operation.

Gallagher may gather non-identifiable usage information such as:

- The cardholder search, view, and save features were each used once
- The alarm viewing feature was used once.
- The alarm-note feature was used three times.
- The bulk-process alarms feature was used once.

At no point will we capture what the search terms were, details/contents of the cardholders, alarms, notes, or request details such as how many alarms were bulk processed.

This information is then further anonymized, such that it is not possible to trace which REST Client / Operator or Mobile device performed any specific actions.

Usage information is aggregated into time periods, such that while it will be possible to see that N requests were performed within a time period, it is not possible to determine what specific time any of those requests occurred. The duration of a time period may vary depending on the specific data but will always be at least one hour.

Copyright © Gallagher Group Limited