Gallagher Command Centre

Command Centre Web

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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.

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this document along with your Command Centre installation media, or via another similar channel then it may be out of date with respect to the functionality/behaviour of the cloud, and of Gallagher Mobile Apps, which are distributed through platform App Stores and may be more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

Contents

1 Background

Command Centre Web is a browser based client for Command Centre, allowing sites to access their cardholder data from anywhere with an internet connection. This provides flexibility and removes the need to set up and maintain a full Command Centre Workstation.

The current iteration of the client is focused on cardholder management, and has several features, including:

- Create cardholders
- Viewing and editing cardholder detail
- Assigning and maintaining access for cardholders
- Assigning and maintaining a cardholders credentials (cards)
- Viewing a cardholders history and activity

1.1 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 Command Centre Web 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/commandcentre-cloud-api-gateway.html

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

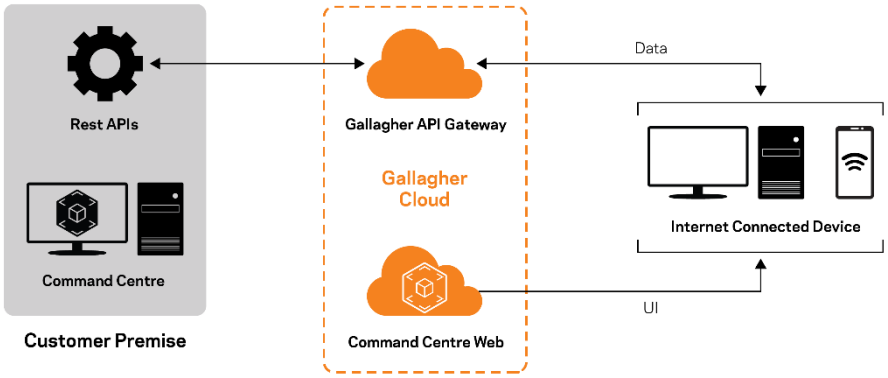
https://gallaghersecurity.github.io/r/commandcentremobile-app-security

https://gallaghersecurity.github.io/r/cloud-licensing-service

2 Architecture

2.1 Overview

Command Centre Web is a single page app that uses the existing Gallagher API Gateway infrastructure to read and write data to Command Centre using REST APIs. The REST API requests and responses are sent and handled in the user's browser running on the user's device.



3 Regions

Command Centre Web is both hosted in Australia and United States. The region you use should be the same region of the Command Centre API Gateway configured for your Command Centre server.

Note:

- If you change the configured Gateway region, then you must use the new Command Centre Web URL.

4 Network Configuration Details

Each Gateway region has a corresponding Command Centre Web endpoint.
Internally we employ multiple redundant servers for failover and scalability.

Australian Command Centre Web:

DNS address: **commandcentre1.security.gallagher.cloud**

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

United States Command Centre Web:

DNS address: **commandcentre2.security.gallagher.cloud**

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

Communications with Command Centre Web take place solely using HTTPS over port 443.

4.1 Firewall Recommendations

Firewall Recommendations for Command Centre API Gateway applies.

Configure your firewall to allow TCP outbound traffic on port 443 with a source of the devices used to access Command Centre Web, and destination of the above DNS addresses.

5 Data Storage and Retention

All the data displayed in Command Centre Web is retrieved from Command Centre server through the Command Centre API Gateway. No data is saved in the cloud. Some data may be cached locally by the browser, such as:

- Cardholder data, including names, personal data fields and related items.

6 Data Transmission

All data transfer between the Command Centre server and Command Centre Web is done via the Gallagher API Gateway and uses encrypted HTTPS.

We support only TLS 1.2 and TLS 1.3; older protocols are disallowed which mitigates most encryption-related security risks.

Refer to the Gallagher API TIP for more information on this https://gallaghersecurity.github.io/commandcentre-cloud-api-gateway.html.

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.

Security Controls

6.2 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 that 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.

6.3 Multi-factor authentication

A time-based one-time password (TOTP) is required to login to Command Centre Web. Command Centre server will validate the TOTP code in addition to the operator's login name and password.

The TOTP is generated using SHA256 and is only valid for 30 seconds. Operators can get the TOTP using the Command Centre Mobile Connect app.

7 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.

8 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.

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.

9 Anonymized Usage data/Telemetry

While we strictly do not capture any identifiable information from Command Centre, we may capture product analytics for the purpose of understand how the product is being used.

Data is captured and processed in accordance with our Gallagher Privacy Policy, which can be found here: https://security.gallagher.com/en/Legal/Command-Centre-Web-Privacy-policy

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

All such data is anonymized.

For example, if user in the web 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.

Gallagher may gather non-identifiable usage information such as:

- The cardholder search, view, and save features were each 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 web client / operator performed any specific actions.