Gallagher Command Centre

Mobile App – Security

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

Contents

1 Background 4

2 Network Security 5

3 Command Centre Mobile App Identification and Authentication 6
- 3.1 User Authentication 6
- 3.2 Device Authentication 6
- 3.3 Connection Security and Identification (Client) 7
- 3.4 Connection Security and Identification (Server) 7

4 Data Security – Command Centre Mobile App 8
- 4.1 Data in Transit 8
- 4.2 Data at Rest 8

5 Privileges and Restrictions 8

6 Auditing and Logging 8

7 Mobile Alarm Notifications and Cloud Services 10
- 7.1 Mobile Notifications Architecture 10
- 7.2 Cloud Services Technical Details 11
- 7.3 Firewall Recommendations: 11
- 7.4 Cloud Services Data Storage and Retention 11
- 7.5 Cloud Services Data Transmission 12
- 7.6 Cloud Services Security Controls 12
- 7.7 Cloud Services Monitoring and Response 12
- 7.8 Security and Penetration Testing 13

1 Background

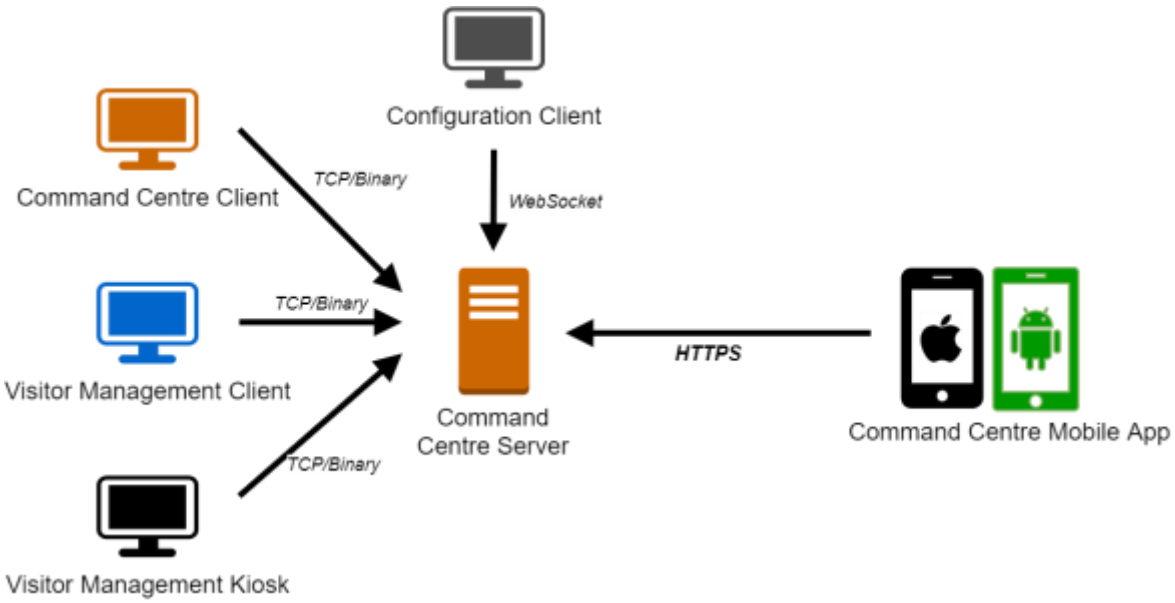
This document references version 8.30 of Command Centre. If you are working with a newer version of Command Centre, please contact your Gallagher representative to confirm if this document is still relevant.

For guidance deploying older versions of Command Centre, please refer to the previous version of this document provided with that Command Centre version.

The Command Centre system provides physical access control, intruder alarms and perimeter security functionality. It is deployed as a service on a Windows server and has a number of clients which can connect to it to perform various tasks:

- Command Centre Client: The main client for operational management of a site. Includes functionality for alarms management, cardholder management, site monitoring, access administration and reporting. Available for Windows only.
- Configuration Client: The main client for system configuration.
- Visitor Management Client: Provides reception functionality to manage visitors to site.
- Visitor Management Kiosk: A self-service kiosk to allow visitors to register themselves onsite.
- **Command Centre Mobile App: An Application for iOS and Android which enables security staff to perform tasks while away from the other Command Centre clients. It communicates over HTTPS using a REST based protocol.**

The following diagram illustrates how these clients connect back to the Command Centre Server.



The app does not provide access to the full functionality of Command Centre. The 8.30 release includes the following features - available on both iOS and Android unless otherwise specified:

- Alarm Management: The ability to view and action alarms.

- Mobile Push Notifications: Can be used to notify operators of alarms in a more secure, functional and cost effective way than SMS or Email.
- Status and Overrides: The ability to find items, view their current status, and perform overrides on them. The types of items this functionality is available for are: Doors, Access Zones, Alarm Zones, and Fence Zones.
- Macros can be run remotely from the Mobile App.
- Manual Cardholder lookup: The ability to search for and view Cardholder details (including photo, access groups, competencies, personal data fields); based on a variety of configurable search criteria.
- Cardholder lookup using a Barcode or QR code: A code can be assigned to a Cardholder, and the camera on a mobile device can be used to scan it to quickly look up the corresponding Cardholder record.
- Cardholder lookup by reading an Access Card.*
- Cardholder Spot Check: The ability to record an encounter with a Cardholder for auditing purposes.
- Calibration of Bluetooth settings for Gallagher Bluetooth® Low-Energy enabled readers.
- Mobile Access Reader: Access Cards* and Mobile Credentials can be read, and Cardholders can be placed into access zones with full access decision rules and auditing employed in the same way as a traditional Gallagher hardware reader.
- Mobile Evacuation: Operators can view the list of cardholders whose location is recorded as being in specific areas, and can update their location manually, or by reading their Access Card*/Mobile Credential

*Note regarding Access card and Mobile Credential reading:
As of March 2020, these features require an iPhone.
Mobile Credentials can be read using the built-in Bluetooth® Low-Energy on the iPhone.
MIFARE DESFire access cards or PIV cards can be read using the built-in NFC capabilities of the iPhone.
MIFARE Classic, MIFARE Plus and 125khz access cards can be read using the Gallagher Mobile Reader hardware attachment.

2 Network Security

Due to its nature, the app will connect over a Wi-Fi or cellular network and therefore has a lower level of base security. I.e. the system can be accessed from anywhere and does not require a physical connection.

The network must be configured to allow connections to the Command Centre Server on two ports to successfully set up and use the app. The first port (hereafter 'the data port') will be for the main connection between the app and the server; the second will be to support enrolment of new devices (hereafter 'the enrolment port'). The data port default is **8901** but can be configured on the Command Centre Server. The enrolment port is always the main port plus one, i.e. the default is **8902**.

The enrolment port is not enabled unless there are active devices pending enrolment.

You can use the Mobile App with a variety of different network configurations depending on your security requirements and existing infrastructure – such as:

- Secure (Corporate) local WiFi Network
- VPN over cellular internet connection
- Direct connection over cellular internet connection

All the above methods can be configured either with or without an external reverse proxy server such as IIS, Apache or Nginx.

The technical information paper titled **Command Centre Mobile Client Network Deployment Options TIP** accompanies this document and discusses the pros/cons and details of the various options in greater detail.

3 Command Centre Mobile App Identification and Authentication

To ensure only authorised users can connect, the app requires both device and user authentication.

3.1 User Authentication

Command Centre provides options to log on using Command Centre-specific credentials or via a windows username and password (validated in Active Directory). Both of these options are supported by the app.

The app will remember the username that was last entered but will not save the password; this must be re-entered on subsequent logons.

3.2 Device Authentication

The Command Centre Client provides a Device Management screen to allow the customer to configure which devices are allowed to connect to the system. This is achieved by the following process:

- The Command Centre Server will generate a self-signed server certificate on installation which will be used in establishing secure connections from the mobile devices. It is possible for the customer to replace this certificate with their own one that has been signed by a trusted authority.
- A Command Centre administrator must enter a mobile device into the Device Management screen before it is able to connect. This will generate a random one-time-use enrolment code which is valid for 24 hours.
- When an operator attempts to connect the app to the Command Centre Server, they will need to enter a valid enrolment code which has not been used previously and is still valid. If they enter a valid enrolment code the app and the server will then exchange keys over an encrypted link so that the device can be authenticated by the server for future connections.
- At this stage the app will now be able to complete a login with a valid username and password and access Command Centre functionality.
- If a device is lost or compromised it can be deleted from the Device Management screen which will prevent it being able to connect in the future. An operator could also just generate a new enrolment code to force the device to go back through the enrolment process.

3.3 Connection Security and Identification (Client)

The Mobile Application will pin the server's TLS certificate as part of the enrolment process. This prevents an attacker from tricking a Mobile Device to accidentally connecting to the wrong server, or otherwise impersonating an enrolled server.

A side effect of this is that changing the certificate will cause all enrolled devices to distrust the server, and they will have to be re-enrolled.

3.4 Connection Security and Identification (Server)

The Command Centre Server can be configured to use one of two methods to identify client devices. Both involve the certificate and RSA 2048-bit key pair which is issued to the device during enrolment: TLS Client Certificate, and Signed Token.

3.4.1 TLS Client Certificate

This is the default option. The device certificate is used as TLS client certificate, which provides cryptographically strong identification of the device to the server each time it opens a network connection. TLS client certificates are an industry standard and widely used part of the TLS protocol, and represent the strongest form of client device identification and security.

The security provided by TLS client certificates is such that it is not possible to insert a server between the mobile device and the Command Centre Server (man-in-the-middle).

More information is available on Wikipedia: https://en.wikipedia.org/wiki/Client_certificate

3.4.2 Signed Token

As mentioned above, TLS client certificates prevent a man-in-the-middle server from operating (This is generally good as man-in-the-middle may represent an attacker), however it is common IT best practice to insert a man-in-the-middle HTTPS reverse proxy to act as a barrier between an internal server and the internet.

This is not possible with TLS client certificates, so the Signed Token mode exists an alternative which allows traffic to be sent through an HTTPS reverse proxy. The Signed Token mode performs similar cryptographic operations using the device certificate, however it does so at the application protocol level, thus can be passed through a reverse proxy.

Technically this involves the server issuing a challenge that the client device signs with its private key (which never leaves the device) as part of the logon process. The server verifies the signature, thus cryptographically proving it is the correct device.

4 Data Security – Command Centre Mobile App

4.1 Data in Transit

The communication channel used by the App follows best practice for secure internet connections using SSL/TLS. By default, the Command Centre Server will provide certificates with a 2048-bit key to use for the initial RSA encryption. The symmetric encryption strength, as well as which version of TLS and which hashes/algorithms to accept, will be whatever the Windows server is configured to use. These can be changed by configuring the server. For Windows Server 2012 R2 this defaults to TLS1.2 and AES128.

Important: By default, Windows may allow a number of older encryption algorithms and ciphers, including TLS1.0, SHA1 and other less secure options. The Mobile devices will not use these older options, so Gallagher recommend you alter the Windows security settings to only allow modern algorithms and ciphers and reduce the attack service against other third parties.

Please refer to the Server Hardening guide for more information.

4.2 Data at Rest

The Command Centre Mobile App is designed to store as close to zero data as possible, relying on the Command Centre Server to provide secure storage. Stored data includes the following:

- Key material (the Certificate and Keys used to identify the device to the server).
  This is stored in operating-system provided secure storage as allowed by the device (usually some form of hardware-backed secure storage).
- Non-sensitive data, such as user preferences.
  This is stored on the device file system.

The iOS operating system prevents applications from accessing each other's data and always encrypts all contents of the file system. This is deemed enough to protect the limited data that the App will store locally.

The Android operating system also prevents applications from accessing each other's data and may optionally encrypt data stored on the device if the device has this feature enabled.

Mobile Device Management software can be installed if a customer wishes to be able to remotely wipe a device and clear data off it.

5 Privileges and Restrictions

As with the Command Centre Client and Configuration Client, Operator Privileges and Workstation Restrictions will be applied in the app to restrict what an operator can view on the device.

6 Auditing and Logging

The logging policy for mobile devices is similar to that of Command Centre workstations.

- Users logging on and off will generate an event in Command Centre which can be reported on.

- Any action that might modify the state of the system (editing an item, opening a door, locking down a zone, running a macro, etc.) will be reportable (usually this is in the form of logging an Event in Command Centre).
- Spot check pass/fail events are reportable.
- All access actions performed by the Mobile Reader are fully reportable and can be grouped with other access events from wired readers, or viewed separately as desired.
- Operators' viewing data is not reportable (except viewing alarm details, which adds an entry to the Alarm History).

For all reportable actions, the specific mobile device that performed the action and the user who was logged on at the time will be linked to the event.

The Command Centre Server does not capture any information about the network or remote IP addresses used when logging mobile events.

Examples:

As mentioned above, each device must be enrolled into Command Centre with a unique identifier before it can be used. Users could then, for example, report on:

- mobile logins and logouts across the system on any phone,
- alarms processed by a guard on their personal phone,
- actions the Security Manager performed on their iPad, but not their iPhone, and vice versa,
- actions performed on a shared phone over the last two days,
- all Cardholders granted into a specific zone via the Mobile Reader,
- actions performed on a specific phone after a specific time (e.g. after a duress alarm has been raised).

7 Mobile Alarm Notifications and Cloud Services

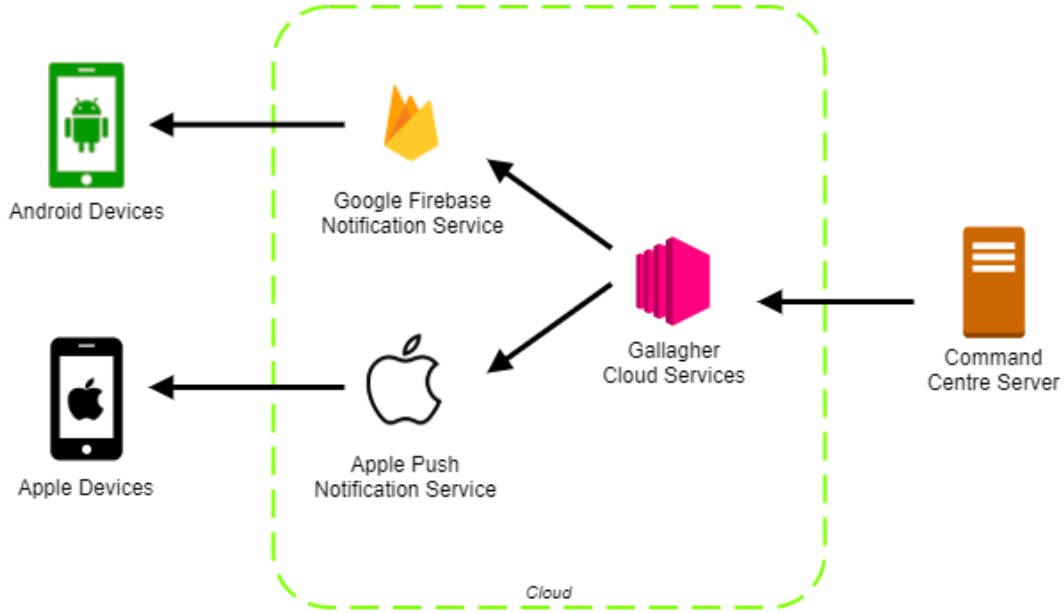
Command Centre can be configured to notify of alarms using the push notification systems built into iOS and Android. This offers several improvements over the pre-existing SMS notification option.

1. Mobile notifications often arrive more quickly and reliably than SMS notifications.
2. Mobile notifications can present information more clearly and with more flexibility.
3. Mobile notifications are integrated with the App. If you tap on a mobile alarm notification, the App will be automatically opened, taking you directly to the details of the selected alarm, at which point you can acknowledge, process or add notes to the alarm directly.

In order to use mobile alarm notifications, you must allow your Command Centre Server to connect to the Gallagher Cloud services, and send alarm details.

Note: The same Gallagher Cloud Services also provide Mobile Connect credential registration functionality. For more information please refer to the document titled "**Mobile Connect Cloud and App Security**"

7.1 Mobile Notifications Architecture



In order to send notifications to Apple devices, we must use Apple's Push Notification Service.

In order to send notifications to Android Devices, we must use Google's Firebase Notification Service.

We have elected to send messages through Gallagher's Cloud Services, so that:

- Individual Command Centre Servers need not connect to Firebase or Apple directly, and thus need not manage the security and accounts associated with those connections.
- IT departments can allow the Command Centre Server to only connect specifically to the Gallagher Cloud Services, improving the security profile of the server.

7.2 Cloud Services Technical Details

Currently, there is a single logical endpoint, located in Sydney, Australia.
Internally we employ multiple redundant servers for failover and scalability.

It has the DNS address **commandcentre-ap-southeast-2.security.gallagher.cloud**

It has two static IP addresses: **52.62.211.7** and **54.79.91.203**

Communications with cloud services take place solely using HTTPS over the standard port **443**.

Gallagher cloud services use TLS client certificates to securely and uniquely identify each individual Command Centre Server. The client certificates are issued by the cloud to each Command Centre Server the first time it connects.

Note: The same Gallagher Cloud Services also provide Mobile Push Notifications functionality for the Command Centre Mobile Application. For more information, please refer to the document titled **"Gallagher Mobile Connect Cloud and App Security Technical Information Paper"**.

7.3 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 ports or traffic to the Command Centre Server.

7.4 Cloud Services Data Storage and Retention

Gallagher Cloud Services do not apply at-rest encryption to any data relevant to the Command Centre Mobile App because none of it is sensitive enough to require encryption.

For each Command Centre Server that connects to the cloud, the cloud retains the following:

- Server licensed serial number
- TLS client certificate used to authenticate connections from that server
- Non-identifiable aggregate information such as counters of notifications sent
- Device mapping information required to send Alarm Notifications to mobile devices. This mapping information consists of randomized identifiers which cannot be traced to any individual device without access to the customer's on-premise Command Centre database
- Information related to the Mobile Connect app, if you use it. For details of this information please refer to the separate **Mobile Connect Cloud and App Security** document.

This information is the minimum required for the solution to function, and it is retained until you choose to delete it.
You may completely remove this information from the Gallagher Cloud Services by deleting the Cloud Server Item from within Command Centre using the explicit **Delete Cloud and Purge Data** function.
You must do this while your Command Centre Server has an active internet connection or it will not be able to inform the cloud of the deletion request.

7.5 Cloud Services Data Transmission

All data transfer with the cloud takes place over encrypted HTTPS.

Communication with Command Centre Servers is authenticated and secured using TLS client certificates (2048-bit RSA.)

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

For each alarm that has been configured to cause a notification, the Command Centre Server will send the following information to the cloud:

- a UUID which identifies the Operator,
- the alarm source name (e.g. "East Wing Door"),
- the alarm type name (e.g. "Door Open Too Long"),
- whether the alarm is escalated,
- the site display name.

The cloud will in turn, send this information to Google Firebase or Apple Push Notification Service which sends it to the operator's phone.

The Gallagher Cloud Services do not retain any of this notification information.

7.6 Cloud Services Security Controls

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.

The cloud services themselves are not exposed directly to the internet, all traffic is routed through a dedicated Security Gateway component, which employs OWASP standard rules and techniques for mitigating attacks, as well as application-specific URL allow-listing and appropriate rate limiting.

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.

7.7 Cloud Services Monitoring and Response

We employ automated analysis of both application and database logs, continuous monitoring of CPU, disk, 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.

7.8 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 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.