



Gallagher Command Centre

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

Copyright © Gallagher Group Ltd 2025. 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received this document along with your Command Centre installation media, or via another similar channel then it may be out of date with respect to the functionality/behaviour of the Gallagher Cloud, and of the Mobile Connect Apps, which are distributed through platform App Stores and may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/mobileconnect-cloud-and-app-security>

Contents

1	Background	5
1.1	Target Audience for the Mobile Connect App	5
2	Mobile Credentials	6
2.1	Mobile Access Overview	6
2.2	Mobile Credential Registration Process	7
2.3	Mobile Credential Registration Technical Details	8
2.4	Mobile Credential Invalidation Scenarios	9
2.5	Mobile Credential Sharing	10
2.6	Mobile Credential Updates	12
3	Broadcast Push Notifications	14
3.1	Broadcast Notification Process	14
4	SALTO Mobile Access Integration	15
4.1	SALTO Key Issuing and Delivery	16
4.2	SALTO Key Encryption	16
4.3	SALTO Key Refresh	16
4.4	SALTO Key Revocation	17
4.5	SALTO Encoding Performance Management	17
4.6	SALTO Mobile Cardholder Access Events	17
5	Digital ID	18
5.1	Digital ID Security and Verification	18
5.2	Digital ID Issuing and Delivery	19
5.3	Digital ID Encryption	19
5.4	Digital ID Expiry and Revocation	20
6	Aperio BLE	21
6.1	Aperio Key Issuing and Delivery	21
6.2	Aperio Key Encryption	22
6.3	Authentication Over BLE	22
7	Mobile Wallet	23
7.1	Mobile Wallet Enablement	23
7.2	Mobile Wallet Access Badge Provisioning	23
7.3	Mobile Wallet Encryption	24
7.4	Mobile Wallet Access Badge Revocation	25
8	Gallagher Cloud Services Technical Details	26
8.1	Firewall Recommendations	26
9	Data Storage and Retention	27
9.1	Mobile Devices	27
9.2	Cloud Services	28
10	Data Transmission	31
11	Security Controls	31
11.1	Mobile Devices	31
11.2	Cloud Services	31
12	Monitoring and Response	32
13	Security and Penetration Testing	32
14	FIDO and Public Key Cryptography Based Security	33

14.1	FIDO	33
14.2	Public Key Cryptography	33
14.3	Cryptography Principles Applied by Gallagher Mobile Connect	34
15	Related Resources	34

1 Background

The Gallagher Mobile Connect app for iOS and Android lets people use their mobile devices instead of, or in addition to a traditional MIFARE or similar access card.

The app has several significant features:

- Opening Gallagher Doors or performing Bluetooth Actions such as arming an Alarm Zone. The app uses Bluetooth® Low Energy (or NFC (Near Field Communications) on supported Android devices) to communicate with Gallagher T-Series readers to accomplish this.
- Receiving broadcast notification messages via in-app Push Notifications. Notifications are delivered via the Gallagher Cloud.
- Opening BLE-capable SALTO and Aperio Doors.
- Displaying Digital ID cards.
- Provisioning Mobile Wallet Access Badges (Apple Wallet only).

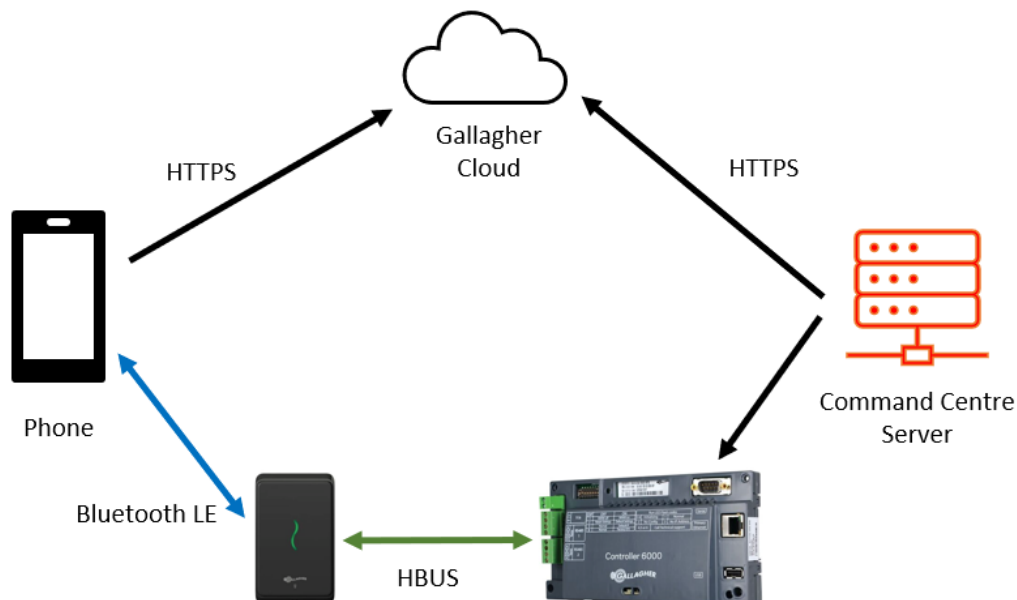
1.1 Target Audience for the Mobile Connect App

The target end user for the Mobile Connect application is anyone who might have an Access Card, including "partially-trusted" individuals such as students, contract employees, etc.

Phones are likely to be a mix of corporate and personally owned devices. Personal devices will probably not be monitored or controlled, and are unlikely to have access to corporate Wi-Fi, VPNs or other secure networks.

2 Mobile Credentials

2.1 Mobile Access Overview



In order for secure access attempts to be made via Bluetooth or NFC, the Controller first needs to know how to identify the phone.

This means we need to get some information from the phone, back to the Command Centre Server, and then down to the Controller. This is why we need the credential Registration process.

Mobile Connect registration is carried out by sending credential data through the Gallagher Cloud.

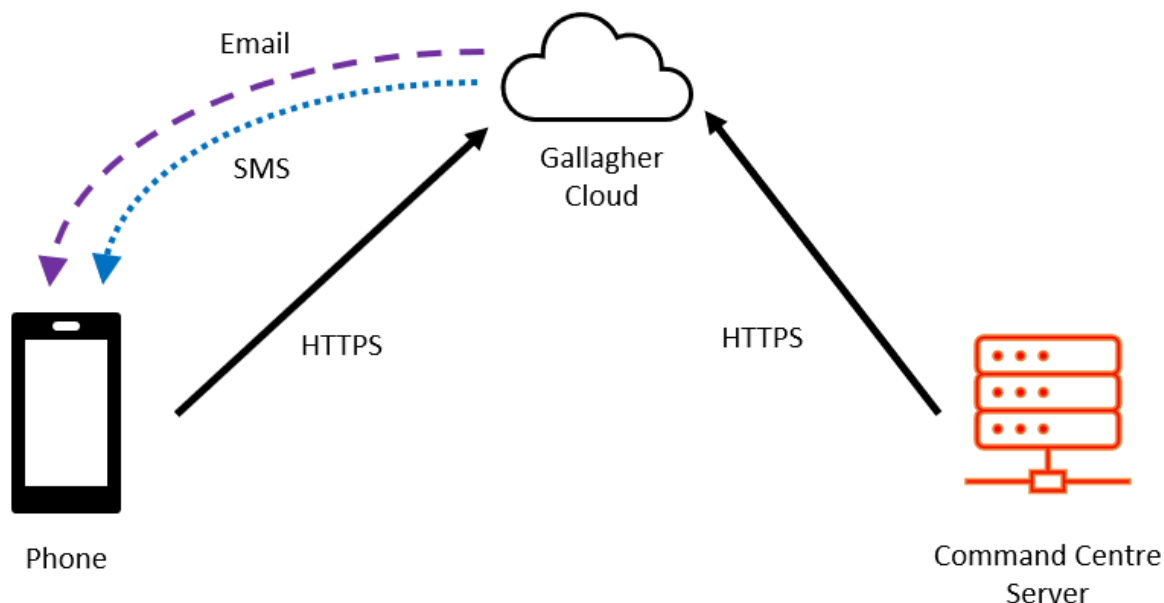
Why use the Gallagher Cloud for Mobile Credential Registration?

The Gallagher Cloud can act as a secure relay between phones and the Command Centre server. If we did not relay via the Gallagher Cloud, then registration would require phones to connect directly to the Command Centre itself. A key consideration is that users of Mobile Connect are unlikely to be carrying secure, authorized company devices on secure networks – instead they are members of the general public using their personal phones on the general internet.

It would not be responsible to require customers to expose Command Centre servers to network traffic from such a wide variety of potentially malicious sources. As such, most IT departments are not willing to allow this kind of network traffic through company firewalls.

Using the Gallagher Cloud as a relay for this information enables your Command Centre server to remain secure and protected on your internal network.

2.2 Mobile Credential Registration Process



1. A Command Centre operator adds a Mobile Credential to a Cardholder.
2. The Command Centre server connects to the Gallagher Cloud registration server and sends through the minimum information needed to complete the registration.
3. The Gallagher Cloud sends an Email to the Cardholder which contains a unique one-time-use registration code.
4. The user responds to the email, launching the Mobile Connect app. The app connects to the Gallagher Cloud and acknowledges the registration code.
5. The Gallagher Cloud sends an SMS (Short Message Service) message to the Cardholder which contains a one-time-use 6-digit confirmation code.
Note: SMS is only supported by the Gallagher Mobile Connect App. It is an optional step based on the Mobile Credential Type configuration in the Command Centre Server.
6. The user inputs this 6-digit code into the Mobile Connect app. The app connects to the Gallagher Cloud and acknowledges the confirmation code.
7. The app on the phone proceeds with registering the FIDO credential and sends the credential information to the Gallagher Cloud when complete.
8. The Command Centre server fetches this complete FIDO credential from the Gallagher Cloud, after which point it can make it available to controllers and it can be used for access.

2.3 Mobile Credential Registration Technical Details

Registration emails by default use a standard template; it is possible to customize this template, but this must be configured outside of your Command Centre software. For more information, please contact your Gallagher representative.

Registration emails are sent with a from address of: **no-reply@security.gallagher.cloud**.

This is not configurable.

Email Protocols Configuration for no-reply@security.gallagher.cloud:

Our product's outbound email system is secured using all three major authentication protocols: **SPF**, **DKIM**, and **DMARC**.

- **SPF (Sender Policy Framework)**: Configured to authorise only verified services (e.g. AWS SES and Microsoft 365) to send email on behalf of our domain.
- **DKIM (DomainKeys Identified Mail)**: Enabled to cryptographically sign outgoing messages, helping validate sender authenticity and message integrity.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**: Configured with a policy set to monitoring mode (p=none) to provide visibility into domain usage across receiving mail systems.

Together, these protocols help protect our domain from spoofing, improve deliverability, and align with email security best practices.

Note: If you employ a spam filter, you may need to configure it to allow messages from this address. Spam filters may also validate against the **smtp.mailfrom** header either in place of or in addition to the **from** header. Registration emails will have an smtp.mailfrom value of **<random id>@mailsender.security.gallagher.cloud**, so you may need to allow ***@mailsender.security.gallagher.cloud**.
E.g. smtp.mailfrom=01000171e6fd47ea-2cd6a766-3cf2-47dd-b207-189f0d368bf0-000000@mailsender.security.gallagher.cloud

Data sent from Command Centre to the Gallagher Cloud Services during registration consists of:

- The registration code (to uniquely identify the registration).
- The Cardholder's email address (to send them the registration email message).
- The Cardholder's mobile phone number (to send them the SMS confirmation code).
- Policy information such as how long the registration code should be valid before expiring.

The registration code consists of cryptographically strong random data.

It expires after 7 days (by default) if not used. This expiry period is configurable individually for each site.

An SMS confirmation code expires 1 hour after being issued.

If a user enters the SMS confirmation code incorrectly more than 5 times, the invitation will be cancelled.

If the SMS confirmation code is not correctly entered within the hour, it will be reset and a second, then third confirmation code will be sent if the user re-tries the registration process.

If the user attempts to retry after the third SMS message has been sent-but-not-completed, the invitation will be cancelled.

2.4 Mobile Credential Invalidation Scenarios

There are several scenarios where a user can invalidate their credential by changing settings on their device. This only affects access where two-factor authentication is required by the reader.

- Android Mobile Connect: when a user is enrolled using a fingerprint for two-factor authentication and an additional fingerprint is added to the device.
- iOS Mobile Connect: when a user removes their device passcode after enrollment.

Both these scenarios require re-enrollment of the Mobile Credential.

There are also two rare scenarios in iOS Mobile Connect on Face ID capable phones, where credentials can be invalidated by revoking permission to use Face ID.

- When a user selects Face ID as their authentication method, then denies permission to the app when prompted during enrollment.
- When a user enrolls with Face ID, then disables permission to the app in the phone's settings.

When a credential is broken in this way, the app must be reinstalled before a new credential can be enrolled.

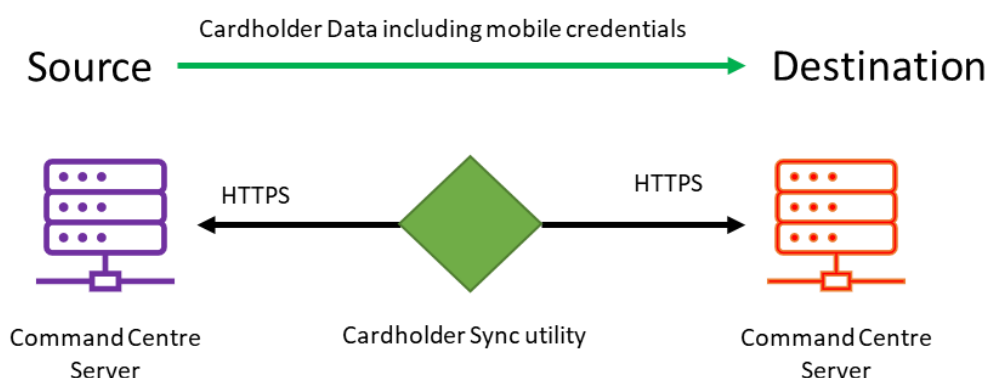
2.5 Mobile Credential Sharing

If multiple Command Centre servers are joined together using Command Centre's multi-server feature, then credentials added by one server will automatically be synchronized across all other servers in the group. This has been the case since the initial release of Mobile Credentials with Command Centre version 7.60.

Command Centre version 8.50 adds the ability to export and import Mobile Credentials between Command Centre servers without requiring the servers to be joined in a multi-server group.

To enable this, Cardholders must be using the Mobile Connect app (or incorporating Mobile Connect SDK inside their own app) of version **15** or greater. The systems must be configured as follows:

1. Use the Cardholder Sync utility to Synchronize Cardholder Data Between the Two Servers



The Cardholder sync utility will connect to both servers using their respective REST APIs, will read data from the source server, and import it into the destination server.

Once this has been configured, the destination server will contain a copy of all the Mobile Credential data including FIDO public keys. These will be distributed to Controllers attached to the destination server to enable Access on their respective Readers.

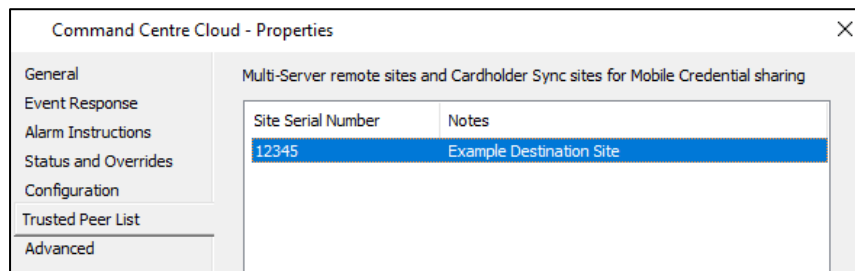
Licensing Note: Credential licensing is allocated against the server which originally issues the Mobile Credential (the "source"). Credentials imported into a destination server do not count towards the Mobile Credential license allocation for that server.

Important: Using the sync tool to copy Mobile Credential data in versions prior to Command Centre 8.50 is not supported. It may result in duplicate credentials - rather than sharing of the existing credential – and may cause unexpected outcomes such as access errors and consume excess licenses.

2. Configure Cloud Trust Between the Source and Destination Servers

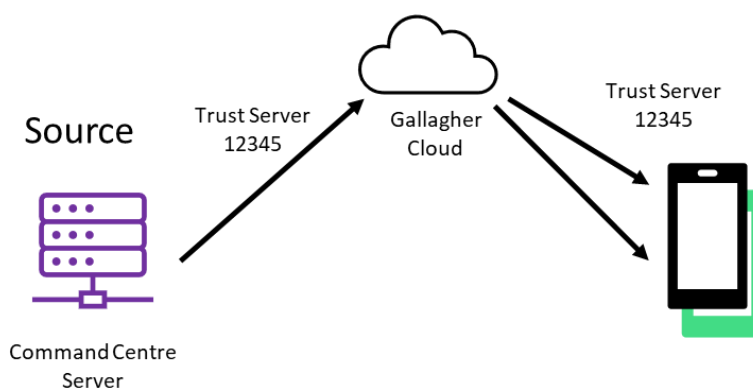
While the Cardholder sync utility will copy the raw credential data, the Gallagher Cloud, as well as connected Mobile Apps / SDK's will not trust the destination server, and thus the credentials will not work on the destination, unless explicitly configured to do so.

On the source server, modify the Cloud Item's Trusted Peer List, and add the license serial number of the destination server



Upon doing this, a message will be sent from the source Command Centre server, telling it that the destination server is now trusted by the source. This allows the destination server to broadcast notifications, SALTO keys and Digital ID cards to credentials that were issued by the source.

The Gallagher Cloud will then also send a message to each phone with a Mobile Credential issued by the source, instructing that phone to trust the destination site's readers.



Revoking Trust

The site which initially issues the credential is considered to "own" it and has authority over which other sites are allowed to use it. To revoke trust from a destination site, remove the destination site's entry from the Trusted Peer List. This results in a message being sent to the Cloud and Phones, telling them to de-trust the given server.

Mobile Credential data exported by the sync tool will not be deleted/updated or modified as part of a de-trust operation, as an automated process may not have enough information to do this safely. The destination server will need to manually clean these up.

The public-key nature of FIDO ensures that even if credentials should remain on the destination server after a de-trust operation, there is no security risk to the source server, it is merely wasteful.

2.6 Mobile Credential Updates

2.6.1 Updates Issuing and Delivery

A Mobile Credential once registered can receive data as updates from the issuing Command Centre server via the Gallagher Cloud. Updates are normally triggered by a related system configuration change, access change, or credential specific change.

Mobile Credential updates include SALTO keys, Digital ID, Aperio Keys, Mobile Wallet provisioning data.

When Gallagher Cloud Services receives the credential update, it will send a "background" push notification to your phone. When your phone receives this push notification, the Mobile Connect app launches invisibly in the background to retrieve the credential updates.

The Mobile Connect app uses the user's FIDO credential to securely authenticate to the Gallagher Cloud and download the updates. Once the credential updates are successfully retrieved, the data is deleted from the Gallagher Cloud database.

Delivery Considerations

- If the Command Centre server does not have an active internet connection, or if the connection is slow, then it will not be able to send Mobile Credential updates, or updates may be delayed.
- If the end user's phone does not have an active internet connection, or the connection is slow, then it will not be able to receive updates, or updates may be delayed.
- Google and Apple can drop notifications. Dropping notifications is rare, and will generally only occur if the user has had their device powered off for a long period of time or has **disabled** notifications using their system settings.
- Google and Apple do not guarantee instant or reliable delivery of "background" push notifications.

Note: While background notifications are not guaranteed, in practice we find that in almost all cases the background notification is delivered, and the phone receives the credential update (i.e. SALTO key, Digital ID, Aperio Key, ...etc.) within 5-10 seconds after the Gallagher Cloud sends the push notification.

Note: Whenever the Mobile Connect app is opened, it will connect to the Gallagher Cloud and check for Mobile Credential updates that might have been dropped or not delivered by Google and Apple.

2.6.2 Updates Encryption

In transit/cloud:

Mobile Credential update data is **always** protected by End-to-End encryption where the issuing Command Centre server is running version 8.40 or higher. For more information on End-to-End encryption, please refer to the technical Information paper “Mobile End to End Encryption TIP” (**REF1**).

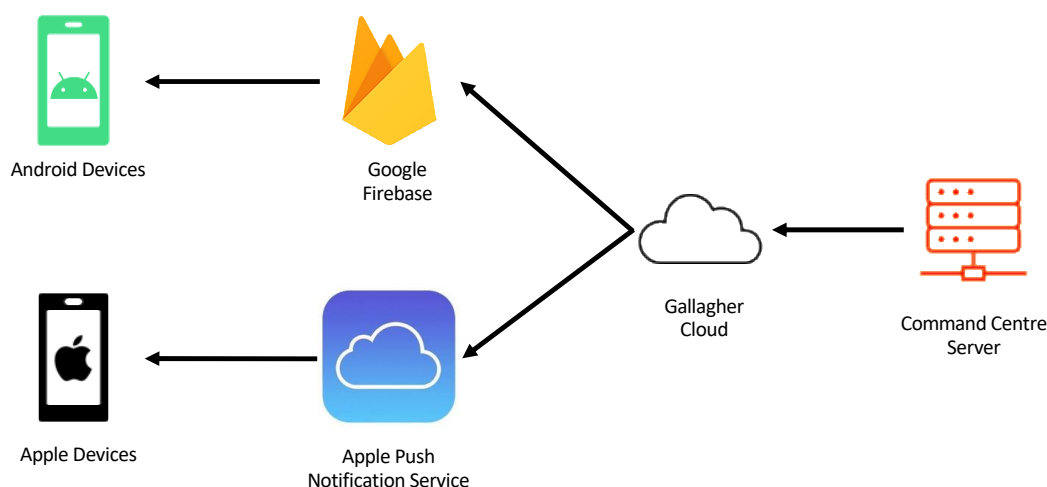
Note: End-to-End encryption is applied to all credential update types. Extra notes will be stated in the individual update “Encryption” section where this differs.

At rest on the mobile device:

Encrypting credential update data at rest is evaluated individually by type.

- Mobile Connect app versions 14 or higher will use Elliptic Curve Integrated Encrypted Scheme (ECIES) with AES-128 to encrypt sensitive data such as SALTO and Aperio access keys at rest on the mobile devices. This will happen regardless of the Command Centre version.
- Low risk data is stored unencrypted at rest in the filesystem on Android, and in the app's private database on iOS. Mobile operating systems provide sandboxing which prevents other applications and most casual attackers from reading it.

3 Broadcast Push Notifications



Android and iOS require that broadcast push notifications are sent via the respective cloud platforms controlled by Google and Apple.

Why send broadcast messages via the Gallagher Cloud?

Command Centre servers could communicate directly with Google and Apple, but in practice this would have major drawbacks

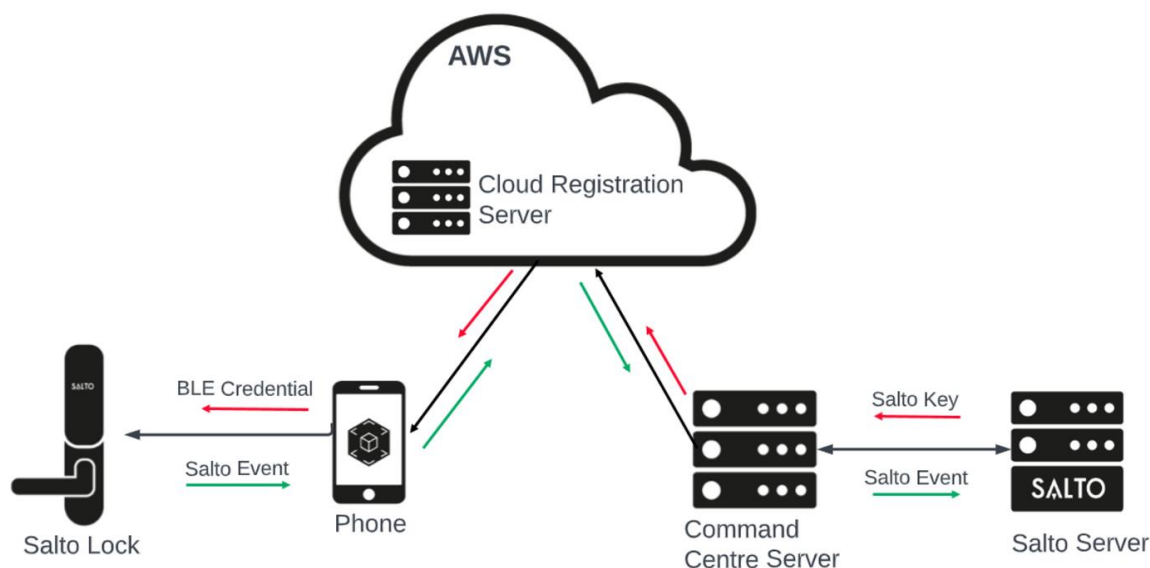
- Google/Apple push notification services require security keys and a development account for their respective platforms. It would be a significant burden to require each individual Command Centre customer to create and manage these things
- Google/Apple cloud services have a huge range of dynamic IP addresses, which makes controlling outbound access through corporate firewalls very difficult.
- Mobile push notifications are not guaranteed to be reliable. If (for example) multiple messages are sent while a phone is powered off, Google/Apple reserve the right to drop some messages and only send the most recent one. By sending messages through the Gallagher cloud, we can ensure that no data is lost as our cloud can buffer messages.

3.1 Broadcast Notification Process

1. Command Centre sends broadcast notifications to the target Cardholders.
2. Command Centre queues these messages internally and delivers them to the Gallagher Cloud as quickly as it can (determined by network speed).
3. The Gallagher Cloud forwards the messages to either Google Firebase (for Android devices), or Apple (for iOS devices).
4. The user receives a notification on their phone containing a summary of the message.
5. When the user opens the notification, they will be taken to the Notification List screen in Mobile Connect.
6. The full message details, along with any other messages are downloaded as a Mobile Credential update. For more information, refer to Mobile Credential “*Updates Issuing and Delivery*” section.

Note: Notification details are encrypted using AES-256 at rest when they are held temporarily in the Gallagher Cloud's database.

4 SALTO Mobile Access Integration



If your site has SALTO Bluetooth-capable wired or wireless locks, and you have integrated your SALTO server with Command Centre, then you can use the Gallagher Mobile Connect App to open Bluetooth-capable SALTO doors. This requires Command Centre version 8.10 or newer.

In order to communicate with SALTO hardware, the Gallagher Mobile Connect App incorporates SALTO's JustIN Mobile SDK. The JustIN Mobile SDK handles Bluetooth communication with SALTO locks, but it does not account for delivery and maintenance of SALTO access keys used to open those locks.

Mobile Connect solves this by attaching the SALTO key to Gallagher's existing Mobile Credential. We use the Mobile Credential to securely deliver the SALTO key to the correct phone. As such, Gallagher Mobile Credentials are a pre-requisite for using SALTO BLE locks with the Mobile Connect app.

As of Command Centre version 9.00, Cardholder access events audit trails will also be sent back from Mobile Connect users if the site has mobile events enabled. This means that offline doors will receive the access events from users with a Mobile Credential as well as standard card types. There is no additional setup required for this if Cardholders already have Mobile Credentials. The additional configuration will be sent along with the next SALTO key update.

If you do not have any SALTO integration, this part of Command Centre and the Mobile Connect App is deactivated.

Licensing Note: While no additional license is required by Command Centre, SALTO may require an additional Salto BLE (Bluetooth Low Energy) site license in addition to the purchase of Salto BLE hardware.

Security Note: SALTO keys are less secure than FIDO-based Gallagher Mobile Credentials.

It is also not possible to use SALTO locks in PINs or Two-factor mode.

It is recommended that you use Mobile/FIDO credentials for security-sensitive areas.

4.1 SALTO Key Issuing and Delivery

When your SALTO access changes, the following occurs:

1. Command Centre asks the SALTO server to encode a new key, containing your new access.
2. Command Centre associates the new key with your Mobile Credential and sends it to the Gallagher Cloud.
3. The Gallagher Cloud Services store the key until the Mobile Connect app on your phone connects and retrieves the new key.
Note: If the key is not retrieved within 7 days, it will be deleted from the Gallagher Cloud.
4. The SALTO key is delivered to the phone similarly to other Mobile Credential updates via the Gallagher Cloud using “background” push notification. For more information, refer to the Mobile Credential “*Updates Issuing and Delivery*” section.

4.2 SALTO Key Encryption

In transit/cloud:

SALTO keys are protected using End-to-End encryption, as well as being encrypted using AES-256 at rest. For more information, refer to the Mobile Credential “*Updates Encryption*” section.

At rest on the mobile device:

SALTO keys are encrypted at rest. For more information, refer to the Mobile Credential “*Updates Encryption*” section.

4.3 SALTO Key Refresh

SALTO keys (as issued by your SALTO server) are valid for up to 7 days, at which point your key must be refreshed. This is the behavior of SALTO's system and is not under the control of Gallagher.

If you are familiar with SALTO's traditional access-card based system, this is analogous to the situation where you must badge on a wired update point periodically to refresh your card.

Command Centre and Mobile Connect transparently manage this refresh process for you. Six days (possibly earlier, see below) after issuing a SALTO key, Command Centre will ask the SALTO server for a refreshed key, and silently send this through the Gallagher Cloud and to the target mobile phone(s)

If, for some reason the refreshed key cannot be delivered to the phone (for example if the phone has no internet connection) then, after the key has expired, the Mobile Connect App will show a warning in the user interface and ask you to connect your phone to the internet to receive a refreshed key.

4.4 SALTO Key Revocation

If you make a change in Command Centre to remove SALTO access from a Cardholder (for example you remove all their SALTO access groups), Command Centre will send a message via the Gallagher Cloud to the target phone(s) to instruct them to immediately delete their SALTO keys.

4.5 SALTO Encoding Performance Management

If you make a large number of SALTO access changes at once - for example, you assign 5,000 Cardholders to a SALTO access group that they did not previously have - this will cause Command Centre to immediately ask the SALTO server for 5,000 new keys so that they can be sent to the Gallagher Cloud and delivered to phones.

This may cause the SALTO server to be busy while it encodes all these new keys. Command Centre does not attempt to delay or spread this load *when you make an access change* as the priority is making sure the Cardholders have their correct access as soon as possible

SALTO key refresh happens in the background and thus may not be anticipated. To reduce the performance impact on the SALTO server, when Command Centre is refreshing keys, it will deliberately spread out the process, such that the key refreshes for those 5,000 Cardholders do not all occur at the same time.

To spread the load, Command Centre will refresh some credentials earlier than strictly required. It spreads them out across the entire 6-day period so some credentials may get refreshed after 1 or 2 days. Because the refresh process is transparent to the user this should not affect access or performance for any individual user. Command Centre will never delay the refresh of a credential past the 6-day point as that could affect the user's access.

4.6 SALTO Mobile Cardholder Access Events

As of Command Centre version 9.00, the audit trail event is the only supported event on the SALTO JustIN Mobile SDK.

Mobile events from SALTO will be delivered to Command Centre server via the existing cloud connection that is used to transport SALTO keys. These events will surface in the same way as standard card badging events.

When SALTO events are generated, they are encrypted with the appropriate site key (End-to-End encrypted) and buffered for sending to the Command Centre Cloud. When a cloud connection can be established, stored events are sent in batches. The Gallagher Cloud will buffer these encrypted events. The Command Centre server periodically checks its connected cloud for updates. If there are stored events, they will be sent to the server in one of these updates.

Once the encrypted SALTO events received by Command Centre server they are decrypted and sent off to the SALTO server for processing.

5 Digital ID

Command Centre version 8.40 adds the ability to send Digital ID cards to Mobile Connect app and SDK users.

Digital ID cards are created on the Command Centre server, encrypted using End-to-End encryption, and then sent to the Gallagher Cloud in a similar fashion to SALTO keys.

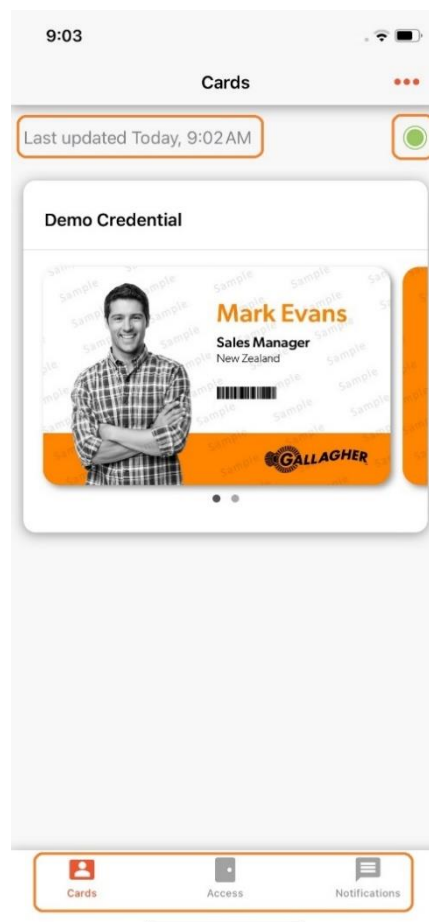
The Mobile Credential provides a secure connection between the phone and cloud which is used to deliver the ID data, and as such, a Mobile Credential is a pre-requisite for Digital ID.

5.1 Digital ID Security and Verification

A Digital ID card is meant to provide a customer-branded visual identification for the Cardholder.

Practically, a Digital ID consists of images and text, and it is not possible to stop an attacker from either copying the ID with a screenshot or fabricating their own images.

The Mobile Connect app adds several "liveness indicators" around the context of the Digital ID in order to stop a would-be attacker from showing a static screenshot when a security guard asks to inspect their Digital ID:



-
1. The app shows a "Last updated" time showing the last time the app synchronized data with the Gallagher Cloud. The app should synchronize every time it is opened, so a guard can verify that this time is relatively current.
The time is important because if a Digital ID card is revoked, this will propagate down to the phone, which will show "Revoked" over the ID card. A user can stop this propagation by preventing the Mobile Connect app from using cellular data, and thus it won't be able to synchronize. If a guard sees a last updated time that is far in the past, it is an indicator that something may need further investigation.
 2. The app displays a pulsing animated circle. A guard can verify that this is animating correctly and thus the app is not a static screenshot
 3. The rest of the app is functional, and a guard can request that the Cardholder taps around through other parts, demonstrating that they are not showing a low-fidelity mockup.

Due to the nature of Digital ID images, it is not possible to stop a skilled and motivated attacker from building a fully functioning fake version of the entire Mobile Connect app.

Sites should consider their security threat model; if a higher level of authentication is required, they should provision their security staff with the separate Gallagher Command Centre Mobile app so they can securely verify Cardholder credentials when needed.

The Command Centre Mobile app has a Mobile Reader function, which can use Bluetooth Low Energy to communicate with the Mobile Connect app on the Cardholder's phone and perform a secure FIDO authentication operation. This will establish with a very high level of security that the Cardholder's credential is legitimate and that the Mobile Connect app is genuine.

5.2 Digital ID Issuing and Delivery

When a Digital ID card is added to a Cardholder, or updated:

1. The Command Centre server rebuilds the Digital ID card image.
2. Command Centre associates the updated data with your Mobile Credential and sends it to the Gallagher Cloud Services.
3. The Gallagher Cloud Services store the Digital ID until the Mobile Connect app on your phone connects and retrieves the new ID.
Note: The Digital ID is deleted from the Gallagher Cloud after it is retrieved.
4. The Digital ID is delivered to the phone similarly to other Mobile Credential updates via the Gallagher Cloud using "background" push notification. For more information, refer to the Mobile Credential "Updates Issuing and Delivery" section.

5.3 Digital ID Encryption

In transit/cloud:

Digital IDs are protected using End-to-End encryption. For more information, refer to the Mobile Credential "Updates Encryption" section.

At rest on the mobile device:

Digital IDs are not encrypted at rest on the mobile device. They are stored in the filesystem on Android, and in the app's private database on iOS.

While this may appear problematic at first glance, practically a Digital ID consists of images and text; Anyone in a position to extract this low-level data from the device's filesystem is already able to simply copy the ID data using a screenshot or could rebuild it themselves using an image manipulation program. At-rest encryption of ID images on the device itself would not provide any meaningful security improvement.

5.4 Digital ID Expiry and Revocation

Digital ID cards share the same infrastructure within Command Centre as other cards. As such, they can be marked as Active, Expired, Pending, or Disabled. This can be set individually per Digital ID (for example a user can have two Digital ID cards, one Active and one Expired).

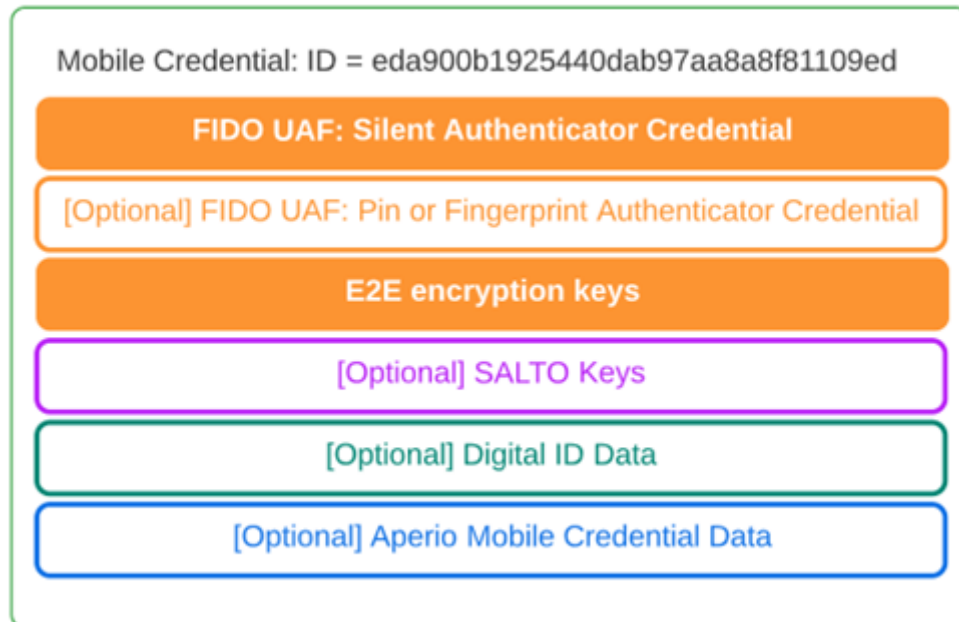
Mobile Connect will draw a gray overlay over any non-active Digital ID cards, and overlay appropriate text, such as "Expired", such that it will be immediately clear if a card is not active.

Changes are updated live on devices. In most cases, if you manually mark a Digital ID as expired, this will be visible on the end-user's phone within a few seconds.

Note: If a large number of Digital ID updates are generated at once (for example, changing a card layout that is used across many cards), then it may take some time for the server to re-generate all the ID images and send them to the Gallagher Cloud.

6 Aperio BLE

Command Centre version 9.00 adds the Aperio BLE functionality to Mobile Connect. This requires BLE capable Aperio readers upgraded with compatible firmware and the Aperio PAP tool to load in Gallagher Mobile Credentials.



The Aperio portion of a Mobile Credential is referred to specifically as the Aperio key as it allows access to an Aperio door when carried by the user. For secure delivery, it is attached to a Mobile Credential, so this is a prerequisite for using Mobile Connect with Aperio BLE enabled doors.

This key contains a diversified version of the site's Aperio site key, along with an encrypted copy of the user's Mobile Credential ID. This data together is required by the Aperio door to identify the user and let the Gallagher system make an access decision.

This key exists for all Mobile Credential users if the site key has been generated. It can also be removed for all Mobile Credential users if the site key is removed. This key does not expire but can be deactivated in Command Centre as part of the Mobile Credential.

6.1 Aperio Key Issuing and Delivery

When the Aperio site key is first generated on the Command Centre server:

-
1. An Aperio key is generated for all active Mobile Credentials.
 2. The Aperio key is End-to-End encrypted for each Mobile Credential and sent to the Gallagher Cloud for delivery.
 3. The Gallagher Cloud Services store the Aperio key until the Mobile Connect app on your phone connects and retrieves it.
Note: The Aperio key is deleted from the Gallagher Cloud once retrieved.
 4. The Aperio Key is delivered to the phone similarly to other Mobile Credential updates via the Gallagher Cloud using “background” push notification. For more information, refer to the Mobile Credential “*Updates Issuing and Delivery*” section.

When a Mobile Credential is created on the Command Centre server after the key is generated, the above process is followed similarly.

When the Aperio site key is removed from the Command Centre server, the above process is followed for all active Mobile Credentials, but a delete message is sent instead. The Aperio key will be removed from Mobile Connect when this message is received.

6.2 Aperio Key Encryption

In transit/cloud:

Aperio Keys are protected using End-to-End encryption. For more information, refer to the Mobile Credential “*Updates Encryption*” section for more information.

At rest on the mobile device:

Aperio Keys are encrypted at rest. For more information, refer to the Mobile Credential “*Updates Encryption*” section for more information.

6.3 Authentication Over BLE

Mobile Connect communicates over Bluetooth LE technology with compatible Aperio doors for requesting access. This communication emulates the DESFire card protocol with AES-128 encryption on protected data similar to physical DESFire cards.

To prevent tampering of the virtual DESFire card data at any stage, the payload – Mobile Credential ID, is generated on the Command Centre server and encrypted (AES-128) with the site key. This encrypted payload is what is received by the controller, such that any tampering of the payload results in unusable data.

On Aperio doors with two factor authentication (2FA) enabled, during the authentication process, the user will be prompted with their mobile device’s screen lock for the second factor. Users that have not set a screen lock will have an error message and will not be able to meet the 2FA requirement.

7 Mobile Wallet

Command Centre version 9.10 adds the ability to provision Wallet Employee Access Badge for Mobile Connect app and SDK users.

Note: Mobile Wallet is only supported for Apple Wallet on iOS devices.

7.1 Mobile Wallet Enablement

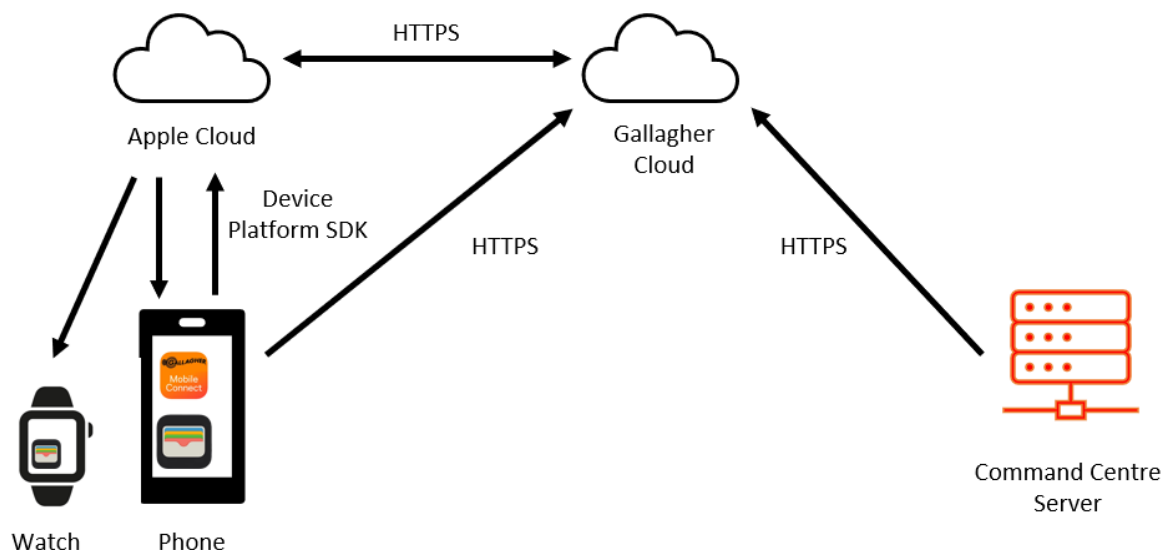
Mobile Wallet Employee Access Badge provisioning requires the following:

- The Command Centre server must be licensed to use the Mobile Wallet feature.
- Active connection to the Command Centre Cloud and the Gallagher API Gateway.
- TCI value and badge template identifier to use with Apple Employee Badge Type assigned and authorized by Gallagher.
Note: Authorizing TCI values and approving artwork templates identifier offers an additional layer of protection, ensuring that these are not shared between customers without explicit mutual consent.
- A Mobile Credential is a pre-requisite for the provisioning of a Wallet Access Badge solution as it provides a secure connection between the phone and the Gallagher Cloud Services which is used to deliver the Wallet provisioning data.

Note: The Mobile Credential is not required once the Wallet Access Badge has been provisioned.

7.2 Mobile Wallet Access Badge Provisioning

When a Mobile Credential Type is linked to an Apple Employee Badge Type, all Mobile Credentials of the given type are sent a Wallet provisioning update:



-
1. The Command Centre server associates the Wallet provisioning data with your Mobile Credential and sends provisioning data as an update to Gallagher Cloud Services. The update is used by the Mobile Connect app to display an “Add to Wallet” button and enable the Cardholder to provision the Wallet Access Badge.
 2. Gallagher Cloud Services store the Wallet provisioning update until the Mobile Connect app on your phone connects and retrieves the data.
Note: The Wallet provisioning data is deleted from the Gallagher Cloud after it is retrieved.
 3. The Mobile Wallet provisioning data is delivered to the phone similarly to other Mobile Credential updates via the Gallagher Cloud using “background” push notification. For more information, refer to the Mobile Credential “*Updates Issuing and Delivery*” section.
 4. When the Mobile Connect user clicks the “Add to Wallet” button, the Mobile Credential is used to authenticate to the Gallagher Cloud Services and requests a Wallet Access Badge provisioning invitation and an account identifier.
 5. The Mobile Connect app forwards the provisioning information to the Apple Access Platform using iOS PassKit SDK to start the provisioning process. For more information on Mobile Wallet integration refer to the technical Information paper “Mobile Wallet Access Badge TIP” (**REF2**).
Note: The timing and the order in which badges are added to phones and paired watches is not guaranteed as the continuation of the provisioning process is dependent on Apple Access Platform.
 6. Once the Wallet Access Badge is added successfully to the Wallet app, Mobile Connect app hides the “Add to Wallet” button so that only one pass per device can be added.
Note: One Wallet Access Badge per phone and one per paired watch are allowed. Provisioning the badge on the paired watch is triggered automatically by Apple with the same “Add to Wallet” button.
 7. If you remove your Access Badge from the Wallet app on the phone or the paired watch that was provisioned with your Mobile Credential, then the “Add to Wallet” button in the Mobile Connect app will be enabled again allowing the user to re-provision a new badge if the credential is still allowed to provision Wallet Access Badges.

7.3 Mobile Wallet Encryption

In transit/cloud:

Mobile Wallet provisioning data is protected using End-to-End encryption. For more information, refer to the Mobile Credential “*Updates Encryption*” section.

Provisioned Wallet Access Badges data such as badge number, Cardholder name and Wallet maintenance identifiers are retained and encrypted at rest. For more information, please refer to the technical Information paper “Mobile Wallet Access Badge TIP” (**REF2**).

At rest on the mobile device:

Mobile Wallet provisioning data is not encrypted at rest on the mobile device. However, it is stored in the app's private database on iOS and protected by the mobile operating system sandboxing.

The Wallet Access Badge is stored on the Secure Element of the device by Apple.

The Secure Element (**SE**) is a tamper-resistant chip designed to securely store sensitive information. It ensures that no sensitive data is shared during transactions. The SE is isolated from the main operating system, adding an additional layer of security.

7.4 Mobile Wallet Access Badge Revocation

Mobile Connect has no control over the Wallet Access Badges once provisioning is completed. However, at provisioning time the Cardholder and the Mobile Credential status are used to determine if the badge provisioning is still allowed.

Mobile Wallet Access Badges are access credentials which share the same infrastructure within Command Centre as other credentials. As such, they can be marked as Active, Expired, Pending, or Disabled. This can be set individually per badge (for example a Cardholder can have two Wallet Access Badges one Active for the phone and one Disabled for the paired watch).

Wallet Access Badges are provisioned as Active from Apple by default. Passes state updates can be performed by either the device user via the Wallet app or iCloud account or by the Command Centre operator. Access Badge state updates include disabling, re-activating, and removing the badge.

Note: A Wallet Access Badge that is disabled by a Command Centre operator cannot be reactivated by the Cardholder Wallet app or iCloud account. However, a Cardholder can remove the badge and re-provision it again. It is recommended to de-authorize the Cardholder or delete the provisioning Mobile Credential to revoke access.

8 Gallagher Cloud Services Technical Details

Currently, the Gallagher Cloud service that maintain communications with Mobile Connect app is a single (logical) endpoint, located in Sydney, Australia. However, internally we employ multiple redundant servers for failover and scalability.

The Gallagher Cloud service maintaining Mobile Credentials has the DNS (Domain Name Server) address **commandcentre-ap-southeast-2.security.gallagher.cloud**, and the following static IP addresses: **52.62.211.7** and **54.79.91.203**

Communications with the Gallagher Cloud service take place solely using HTTPS over the standard port **443**.

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

Note: If the Mobile Wallet feature is enabled for a site, a different cloud service is used to maintain the provisioned Wallet Access Badges. For more information, please refer to the technical Information paper “Mobile Wallet Access Badge TIP” (**REF2**).

8.1 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.

9 Data Storage and Retention

9.1 Mobile Devices

The Mobile Connect app stored information is not encrypted at rest unless otherwise stated. However, Mobile operating systems provide sandboxing which prevents other applications and most casual attackers from reading it.

The following data stored locally on the phone:

1. Mobile Credential Display/Diagnostic Information:
 - The name of the site a Cardholder has registered against.
Note: The displayed site name is configurable. It can be altered or left blank if a site does not wish this information to be shown or saved.
 - The date they registered.
 - The authentication method they selected for second factor.
2. Secure Mobile Credential Information, which consists of the FIDO credential information and private keys.
Note: This information is stored by FIDO certified authenticator components. It is stored using hardware secure storage and encryption on devices which support this, or otherwise the best available encryption and storage option for a given device.
3. Received Broadcast notification messages:
 - The notification message text.
 - The date and time the notification was received.
 - The name of the site which sent the notification.
Note: The displayed site name is configurable. It can be altered or left blank if a site does not wish this information to be shown or saved.
4. SALTO Key data if configured. (**Encrypted**, Mobile Connect app versions 14 or higher using (ECIES) with AES-128).
5. Digital ID card data if configured.
6. Aperio Key data if configured. (**Encrypted**, Mobile Connect app using (ECIES) with AES-128).
7. Provisioning Mobile Wallet data if feature enabled and configured (only available on iOS devices).
 - Cardholder First and Last names.
 - Cardholder global identifier unique within a Command Centre system (UUID).
8. The linked Apple Employee Badge Type global identifier unique within a Command Centre system (UUID).

Deleting Device Stored Information

Data is retained on the mobile device until the Cardholder deletes it.

To delete Mobile Credential data, a Cardholder can use the Settings screen in the app to delete a credential for a specific site, or they can uninstall the entire app.

To delete broadcast notification messages, a Cardholder can delete the messages by swiping them on the notifications list screen within the app, or they can uninstall the entire app.

Note: Deleting a Mobile Credential does not delete the broadcast notification messages that were received while the credential was active. The Cardholder may delete these manually.

9.2 Cloud Services

Gallagher Cloud Services retains some data for Mobile Credentials, connecting Command Centre sites and Mobile Wallet data.

9.2.1 Mobile Credential Data

For each Mobile Credential the following data persisted by the Gallagher Cloud Services:

- The credential FIDO information pertaining to registrations does not require encryption due to FIDO's use of public key cryptography (refer to the FIDO section for more information on this).
- Any un-downloaded Mobile Credential updates (including broadcast notification messages, SALTO keys, Digital ID, Aperio keys, and Mobile Wallet provisioning data).
Note: Mobile Credential updates are End-to-End encrypted where the issuing Command Centre server is running version 8.40 or higher, so this is never readable by Gallagher or any other party. For more information on End-to-End encryption, please refer to the technical Information paper "Mobile End to End Encryption TIP" (*REF1*).
- The Mobile Connect app downloads associated Mobile Credential updates silently when the app receives "background" push notification and every time the app is launched. Once downloaded, this data is removed from the Gallagher Cloud.
- If the Mobile Connect app is not launched, un-downloaded broadcast notifications and SALTO key updates will be removed after 7 days.
- The most recent un-downloaded Digital ID update is always retained. However, Digital ID data is always End-to-End encrypted.
- Minimum data such as device platform, platform version, SDK version and app name, are collected for diagnostic purposes. This data is not encrypted at rest.

Removing Individual Mobile Credential Data from Gallagher Cloud Services

When you use Command Centre to remove a Mobile Credential from a Cardholder, the Command Centre server will queue a request to instruct the Gallagher Cloud to delete the credential, and anything associated with it (FIDO public keys, and any un-downloaded Mobile Credential updates).

Your Command Centre server must have an active internet connection for this delete request to be delivered to the Gallagher Cloud, otherwise it will be queued until an internet connection is available.

When a Cardholder deletes their Mobile Credential using the settings screen in the Mobile Connect app, their phone will tell the Gallagher Cloud to also delete the corresponding credential and associated data. The delete

function requires an internet connection.

Note: If you uninstall the Mobile Connect app, it is not given the opportunity by the mobile operating systems to contact our cloud. As such you will need to remove the credential through Command Centre if you are concerned about this.

Cardholder Personal Information

Cardholder email addresses are never persisted by the Gallagher Cloud. It receives them from Command Centre and immediately discards them after sending an email.

Cardholder mobile phone numbers are stored for the minimum amount of time to allow for registration.

- When a Cardholder completes the registration process using the Mobile Connect app, the Gallagher Cloud immediately deletes the corresponding mobile number.
- When a registration expires, the Gallagher Cloud immediately deletes the corresponding mobile number.
- When a registration is cancelled, the Gallagher Cloud immediately deletes the corresponding mobile number.

Note: The above is the deletion policy for the active database. However, mobile numbers may be persisted in database backups for longer periods than this.

9.2.2 Command Centre Site Data

For each Command Centre server that connects to the Gallagher Cloud, the Gallagher Cloud retains the following:

- Server serial number.
Note: the server name is NOT retained.
- Server licensing information.
- A TLS client certificate used to authenticate connections from that server.
- Information about any in-progress or successful mobile device registrations, consisting of:
 - Random credential identifier UUIDs.
 - FIDO Public Key(s).
 - **Note:** *Expired or failed mobile device registration information is deleted after the configurable expiry period.*

Note: *Registered Mobile Credential data is retained until it is requested to be deleted by either the Mobile Connect app, or the Command Centre server. It needs to be stored to enable broadcast notifications to work securely.*
- Command Centre also periodically sends a count of active Mobile Credentials for licensing purposes.
Note: This information is the minimum required for the solution to function, and it is retained until you no longer wish to use the Gallagher Cloud Services.

Removing All Information About Your site from Gallagher Cloud Services

It was previously the case that deleting the Cloud FT Item from within the Command Centre configuration client would request the Gallagher Cloud services to remove all data related to the site. After July 2018, this is no longer the case – regardless of the Command Centre server version installed on a given site.

Deleting the Cloud FT Item within Command Centre will now send a message informing the Gallagher Cloud to release the license serial number (to allow for server migrations and upgrades) however all other data is retained.

Command Centre 8.00 adds a "Delete Cloud and Purge Data" feature, accessible on the "Advanced" tab of the Cloud FT Item configuration dialog. You can use this to request that all information referred to by this document about the site is removed from Gallagher Cloud Services. The purge data feature does not work if the Command Centre server does not have an active internet connection.

Important Note: If you use the purge data feature to remove the Gallagher Cloud connection, and then later re-establish a connection to the Gallagher Cloud, then any Mobile Credentials issued before the purge will not be known to the Gallagher Cloud. **This means those credentials will fail to receive any updates.** If you wish to correct this, you must re-issue those credentials.

Note for older sites: The purge data feature is available in version 8.00 or newer of the Command Centre software. If you have not or are not able to upgrade your server to version 8.00 or newer but would still like your data to be deleted from the Gallagher Cloud Services, please contact privacy@gallagher.com or by using any of the methods listed on the Gallagher website at <https://www.gallagher.com/privacy>. If you email, please use a subject line containing the terms "Mobile Connect Cloud Services" in order to help us process your request more quickly.

9.2.3 Mobile Wallet Data

If a Command Centre is enabled to use the Mobile Wallet feature, then extra data is retained and encrypted at rest by the Gallagher Cloud Services. For more information about the stored data, please refer to the technical Information paper "Mobile Wallet Access Badge TIP" (**REF2**).

10 Data Transmission

Data transfer between Mobile devices and Reader hardware is not encrypted as no private information is sent. Authentication is secured by FIDO.

All other data transfer between Command Centre, the Cloud and Mobile devices uses encrypted HTTPS. We support TLS 1.2 and TLS 1.3; Older protocols are disallowed which mitigates most encryption-related security risks.

You can view the SSL Labs industry standard report here:

<https://www.ssllabs.com/ssltest/analyze.html?d=commandcentre%2dap%2dsoutheast%2d2.security.gallagher.cloud&latest>

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

Communication between Mobile devices and the Gallagher Cloud is authenticated using FIDO (P256 Elliptic Curve).

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

11 Security Controls

11.1 Mobile Devices

Security, Access Controls, and Isolation are provided by mobile operating systems and hardware.

11.2 Cloud Services

Our cloud services are securely hosted using Amazon Web Services. They are isolated from other Gallagher or external services using an AWS (Amazon Web Services) 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 Gallagher Cloud environment are only allowed access to the minimum set of resources they require to function (for example: they are only allowed to connect to the specific database / key storage they require and cannot access resources for any other services).

Platform security updates are applied daily as 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.

Regular external penetration tests, system hardening, and audit logging are all in place to provide verification and assurance.

12 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 Gallagher Cloud Services status page (<https://status.gallagher.com/>), Channel Partners, or a direct email alert system, which customers may sign up to by contacting their Channel Partner.

13 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 is engaged to do a comprehensive review annually, or more frequently with each major release as required. 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.

14 FIDO and Public Key Cryptography Based Security

In order to provide a secure solution:

- Phones must be able to identify themselves to Controllers (via a reader)
- Controllers must be able to prove that the phone's identity is legitimate
- Controllers must be able to prove that data sent from the phone has not been tampered or misused.

14.1 FIDO

Gallagher Mobile Connect uses the FIDO UAF protocol for identification and authentication to provide security when access is attempted by a Cardholder using their mobile device.

FIDO is an acronym for **Fast IDentity Online**. It represents a set of open, interoperable and secure specifications for online authentication. It is managed by the FIDO alliance (<https://fidoalliance.org/>) which is an open group consisting of companies including Microsoft, Google, Intel, MasterCard, Visa and many others.

UAF is an acronym for **Universal Authentication Framework**, and is a FIDO protocol designed to authenticate users to services using public key cryptography instead of traditional methods such as passwords. It aims to provide improved security and usability through support for biometric, PIN and other convenient forms of authentication.

The FIDO UAF protocol has gained wide acceptance as being secure, reliable and resistant to many forms of attack. As an open protocol, the specifications are publicly available, and as such have been scrutinised and reviewed in great detail by many parties.

14.2 Public Key Cryptography

The full details of public key cryptography are outside the scope of this document, but it can be summarised roughly as follows.

- To identify something, a pair of large numbers is generated which are mathematically linked together. These are called **keys**.
- Each of the keys can be used to encrypt, or generate a signature for a set of data, which the other key can be used to decrypt or verify.
- The mathematics is such that given one key, it is not practically possible to discover the other, so one key is safe to distribute without requiring additional encryption.
- Given this property, one key is designated as the **private key** and kept safe. The other is designated as the **public key**. Copies of the public key are sent to other parties we wish to communicate with.
- The private key can be used to generate a signature for a piece of data, which is sent along with that data. The public key can be used to verify the data. The mathematics formally prove that the data originated with the private key, and that it has not been tampered with.
- Encryption can also be performed, but this is not needed by FIDO, so does not warrant further explanation.

Public Key Cryptography is also known as asymmetric cryptography, referring to the two sides of the conversation both holding different keys.

14.3 Cryptography Principles Applied by Gallagher Mobile Connect

The FIDO UAF protocol applies these principles as follows:

At registration time:

- The phone generates a public and private key pair (Elliptic Curve P-256).
- The public key is sent from the phone to Command Centre, which saves it, and makes it available to controllers for later use.

Sending the public key to the controller is the primary reason for having a registration process.

At access time:

- The phone signs some data with its private key and sends the data and the signature.
- The Controller uses the corresponding public key (which it obtained during registration) to verify the signature and the data. This securely proves that the phone is the correct one and the data is legitimate.

A number of points arise from this approach:

1. An attacker being able to clone the credential depends on their obtaining a copy of the private key. It is important to keep it safe.
2. The public key can only verify the phone, not impersonate it. As such, it is not considered sensitive information, and if it happens to get copied, intercepted or otherwise made available to malicious third parties, the credential still remains secure.
3. Only the public key needs to be transmitted. The private key can remain securely on the device. This greatly reduces the ability for any malicious third parties to intercept or gain access to it.
4. If hardware secure storage is available, the private key can be stored in this secure hardware. In these situations, the private key never leaves this secure hardware chip for any reason.
5. For an attacker to clone or compromise a credential, they must:
 - a. At bare minimum have physical access to your phone
 - b. Modify its operating system to circumvent the phone's built in security defenses.
 - c. If hardware secure storage is used, even this will not reveal the private key. An attacker must resort to physical attack methods such as removing the secure hardware chip and physically opening it, which may destroy the chip entirely.

15 Related Resources

ID	Document Title	Location
REF1	Mobile End to End Encryption TIP	https://gallaghersecurity.github.io/r/mobileconnect-End-to-End-encryption
REF2	Mobile Wallet Access Badge TIP	https://gallaghersecurity.github.io/r/mobile-wallet-access-badge