Gallagher SMB

System and Application Cyber Security

Technical Information Paper

Gallagher SMB System and Application Cyber Security | Edition 1.1 | July 2023

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

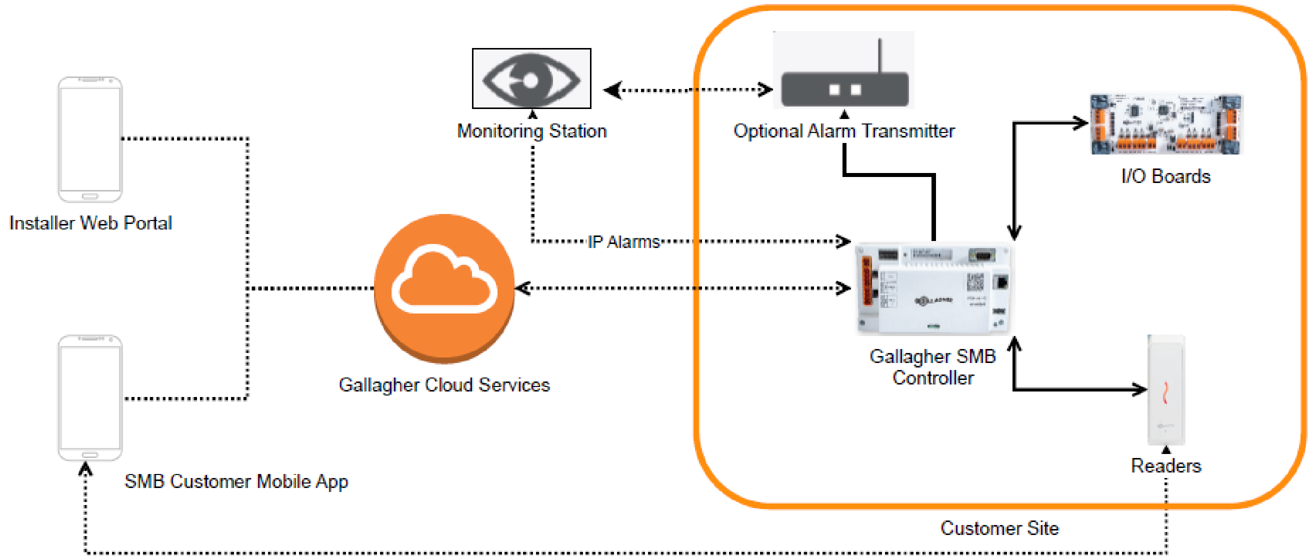
Except where stated otherwise, the information is subject to copyright owned by Gallagher Group, and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Important: Technical details are subject to change. It is recommended you refer to the latest revision of this document, which can be found here: Gallagher SMB Installation and Training

Contents

1 Background

System Overview



Gallagher Cloud Services

Gallagher SMB is a cloud-based solution that allows control of business security from anywhere, at any time.

The Gallagher SMB system is hosted by Amazon's AWS cloud computing platform requiring no server to be installed on-site.

Gallagher SMB Controller 6000

The Gallagher SMB Controller 6000 can manage localised access control, intruder alarms, and site management tasks, to ensure the site operates safely and efficiently. The controller connects to Gallagher's cloud infrastructure via a secure internet connection to allow remote functionality such as alarm management. If the internet connection is lost, the controller will continue to function allowing local access control and local arming/disarming via readers.

Gallagher SMB Installer Portal

Each Gallagher SMB site is configured using the Gallagher SMB Installer Portal web application.

The Gallagher SMB Installer Portal app has been designed as a one-stop portal for technicians to add, configure, monitor, manage customer sites, and manage technician accounts that can access the Installer Portal for their organisation.

A site can be configured using a computer, tablet, or smartphone and provides remote management, monitoring, and configuration of customer sites. Technicians can view item status and events in real-time and resolve site issues remotely.

Gallagher SMB Mobile App

Gallagher SMB is a mobile-first security solution. Mobile credentials offer convenience for both administrator and other users. Utilising a mobile device that the user already has, an administrator need not order, purchase, or distribute physical access credentials ever again.

The Gallagher SMB app for iOS and Android lets people use their mobile devices instead of, or in addition to a traditional access tag/card.

The target end user for the Mobile application is anyone who might need to access doors or arm and disarm areas, including "partially-trusted" individuals such as contract employees, etc.

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 on supported Android Devices) to communicate with Gallagher T-Series readers to accomplish this.
- Receiving notification messages via in-app Push Notifications. Notifications are sent via the cloud.

Gallagher SMB mobile credentials come from Gallagher's award-winning Mobile Connect credentialing solution. Mobile credentials are provisioned using the Gallagher SMB app, meaning an administrator can invite a user into the system. from anywhere, at any time. There is no limit to the number of mobile credentials that can be provisioned per site. The user will receive an email invitation, download the Gallagher SMB app, and register their credential. Administrators can verify which user credentials are active and revoke them at any time using the Gallagher SMB app.

Gallagher SMB Key Tags

SMB Key Tags provide an alternative credential to using the mobile credential in the SMB app. Local interactions with the security system can be performed without the Mobile app using uniquely encoded, Gallagher approved Key Tags. SMB Key Tags can be used for access control, and alarm management.

Specific areas can be configured to be more secure than others by specifying if single factor authentication or two-factor authentication is required to disarm the area. An area in two-factor, requires the user to authenticate themselves before the area will disarm.

User Codes

Unique User Codes can be created using the SMB app for each site user. Each code is ready for instant use as an access credential and can be revoked should a user leave, or it becomes compromised.

2 Gallagher Cloud Services

Currently, there is a single (logical) AWS endpoint. Internally we employ multiple AWS services for failover and scalability. Communications with Gallagher Cloud services take place solely using HTTPS over the standard port 443.

The Gallagher Cloud uses RSA with 1024-bit keys to identify each individual Gallagher SMB site's Controller securely and uniquely. These certificates are securely loaded into the Gallagher Cloud as part of the manufacturing process.

2.1 Maintenance and Upgrades

No downtime is expected as cloud services are deployed across multiple AWS Availability Zones and employ database replication (AWS RDS). Although software updates are regular and frequent, these are deployed using a rolling-deployment strategy to virtually eliminate any disruption experienced by users.

There may be short outages for things like a database engine upgrades/maintenance, but these are infrequent and will be clearly notified to Install Partners and/or customers prior to the outage via our status page and via email if necessary.

3 Gallagher SMB Controller 6000

The Gallagher SMB Controller 6000 communicates with the Gallagher Cloud services and monitored devices, allowing users to manage intruder alarms, access control, and site management tasks from their mobile device.

Once powered on, the Controller will:

- automatically request an IP address using DHCP
- perform a time sync using NTP (default NTP server is time.google.com)
- authenticate with the Gallagher Cloud
- establish a secure WebSocket connection (WSS) to the Gallagher Cloud services
- download a default configuration
- download and update itself with the latest firmware and security updates.

If the Controller loses its connection to the cloud, it will continue to operate locally, keeping the site secure. During this time, the customer will be able to arm and disarm their site at the reader, and request access through doors using Bluetooth or NFC. Events/Alarms generated when the Controller is offline will be retained and uploaded to the cloud when the Controller reconnects.

The controller is authenticated and authorised with the Gallagher Cloud using unique RSA keys securely generated and pre-loaded in the Gallagher factory.

All communication with the cloud is over a secure, encrypted network connection using industry best practice encryption protocols (TLS 1.2 or later / AES-256). The WebSocket is dropped, and the AES keys are periodically refreshed at a randomised frequency at least once per day to minimise the time they are in use.

The Controller and connected HBUS devices are updated automatically with the latest firmware when released, including new functionality and any necessary cyber security updates via Gallagher Cloud services.

The Controller includes many security features including:

- Self-monitoring capabilities, allowing users to receive alarm notifications and action intruder alarms.
- Secure WebSocket (WSS) with a connection encrypted by Transport Layer Security (TLS) is used for secure network communication between the controller and the Gallagher Cloud services.
- Controller data is safely stored and backed up in the cloud.
- High speed encrypted (HBUS) RS-485 connectivity and software updates to field devices.
- Remote configuration support through the Installer Portal.
- Support for multiple wiring topologies, allowing easy connectivity of existing field devices without re-wiring.
- Up to approximately 80,000 system events.
- Alarms are generated when high rates of network traffic are detected – e.g., a Denial-of-Service attack.

3.1 Firewall Recommendations

To allow the Gallagher Controller to connect to the Gallagher Cloud and time sync (NTP) services, the customer's network must allow these outgoing connections:

Port	Protocol	Details
67	UDP	DHCP to internal router
53	UDP	DNS to internal router
123	UDP	NTP to time.google.com
443	TCP	Gallagher Cloud *

* Gallagher Cloud services operate in a dynamic and scalable manner, and Gallagher do not provide a static IP address range for firewall inclusion.

3.2 Using a Proxy Server

If the site's network connects to the internet using a proxy server, the proxy server's connection details will need to be entered into the Gallagher Controller's configuration web pages using a web browser.

Refer to the **Gallagher SMB Kit Installation Note** for instructions to configure the proxy server connection for the Gallagher Controller:

https://media.gallagher.com/web/45a366228fc59ae9/installation-and-training/

4 Gallagher SMB Installer Portal - Configuration Web App

The Gallagher SMB Installer Portal is a web application for configuring SMB sites that communicates to the Gallagher Cloud from the technician's device via a web browser.

The Installer Portal web app supports desktop and mobile views. It is compatible with Chrome, Safari, and Edge browsers.

The Installer Portal only allows access to approved Technician users via HTTPS to Gallagher Cloud services. The Installer Portal can only be used as part of the SMB solution.

Regular updates are made to the Installer Portal as new software features and security enhancements become available.

When an organisation is approved as a Gallagher SMB Install Partner, the Install Partner's organisation entity is created in the Gallagher SMB cloud and an invitation email is sent to the Main Contact (Install Manager) of the organisation which will allow them to set a secure password to gain access to the Gallagher SMB Installer Portal.

To allow access to the Install Partner's Technicians to the organisation's Installer Portal, the Install Manager can create an account for each Technician from within the Installer Portal. Creating a new Technician account will automatically send an invitation email to allow the Technician to configure a secure password before they can log into the Installer Portal.

Only users that have the Install Manager privilege can create/edit/delete other Technician accounts to manage access to their organisation's sites via the Installer Portal.

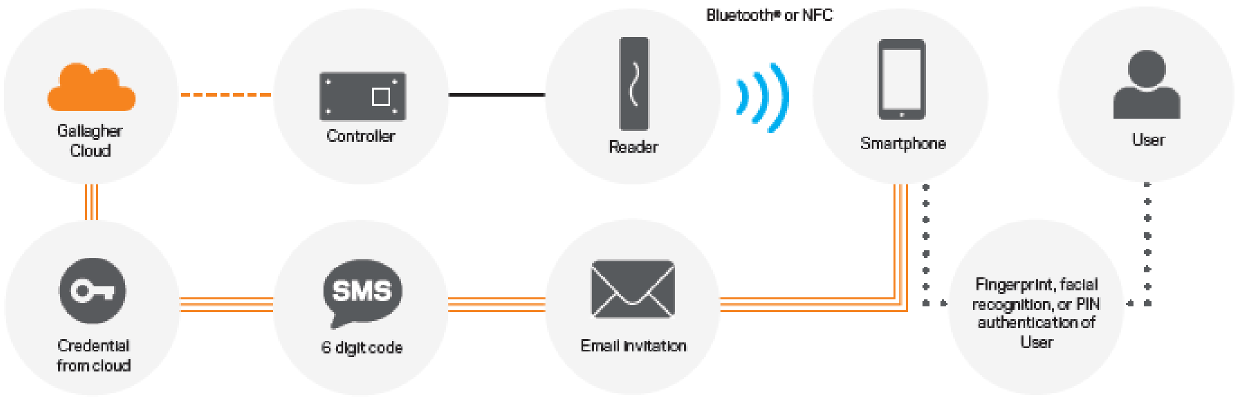
The Installer Portal only allows the user to access sites that have been created under that user's Install Partner organisation. Install Technicians can only make configuration changes to a site when 'Installer Mode' has been enabled by a suitably authorised Site Manager (customer). The customer can prevent changes to site configuration by disabling Installer Mode.

It is recommended that Installer Portal users configure two-factor authentication (2FA) for their Installer Portal account to add another level of security. 2FA is implemented using the industry-standard TOTP algorithm supported by most third-party authentication apps such as Google Authenticator.

5 Gallagher SMB Mobile App

5.1 Mobile Credentials

5.1.1 Mobile Access Overview



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 Gallagher Cloud, and then down to the Controller. This is the credential Registration process.

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

5.1.2 Mobile Credential Registration Process

1. A Site Manager creates a new user from the Customer app.
2. The Gallagher Cloud sends an email to the cardholder which contains a unique one-time-use registration code.
3. The user responds to the email by installing and launching the Gallagher SMB Mobile app. The app connects to the cloud and acknowledges the registration code.
4. The Gallagher Cloud sends an SMS message to the cardholder which contains a one-time-use 6-digit confirmation code.
5. The user inputs this 6-digit code into the Mobile app. The app connects to the cloud and acknowledges the confirmation code.
6. The app on the phone proceeds with registering the FIDO credential and sends the credential information to the cloud when complete.
7. The sends the complete FIDO credential to the Controller to be used for access.

5.1.3 Mobile Credential Registration Technical Details

Registration emails are sent with a from address of: **no-reply@security.gallagher.cloud**. This is not configurable.

If customers employ a spam filter, they 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*

The registration code consists of cryptographically strong random data. It expires after **5 days** if not used.

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.

5.1.4 Mobile Credential Invalidation Scenarios

There are several scenarios where a user can invalidate their credential by changing settings on their device.

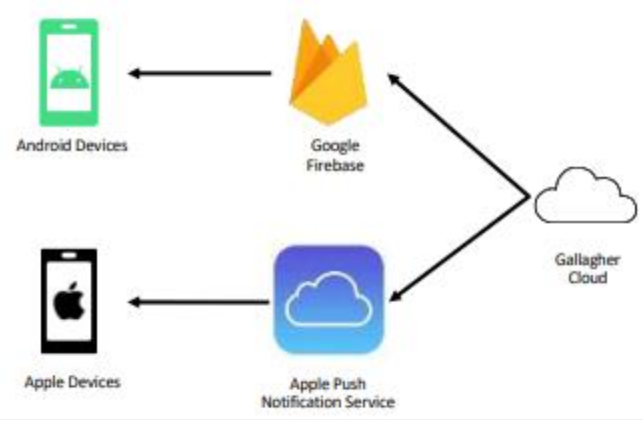
- Android Mobile App: when a user removes their device credential type (PIN, fingerprint etc) after enrolment for the Gallagher SMB app. The credential type can be re-added to restore app access.
- iOS Mobile App: when a user removes their device passcode off after enrolment. This scenario requires re-enrolment of the Mobile Credential.

There are also two rare scenarios in the iOS Mobile App 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 enrolment.
- When a user enrols 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.

5.2 Push Notifications



Android and iOS require that Push Notifications be sent via the respective cloud platforms controlled by Google and Apple.

5.2.1 Notification Process

1. The Gallagher Cloud services generate Push Notifications for target users when important incidents occur.
2. The Gallagher Cloud forwards the messages to either Google Firebase (for Android devices), or Apple (for iOS devices).
3. The Mobile app user receives a notification on their phone containing a summary of the message.
4. When the user opens the notification, they will be taken to the incident in the Mobile app for alarm incident notifications, or the Mobile app will open for other incidents.
5. Google/Apple may occasionally drop notification messages. Dropped messages are rare, and 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.

6 FIDO and public key cryptography-based security

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.

6.1 FIDO

The Gallagher SMB Mobile App 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.

6.2 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.

6.3 Cryptography principles applied by the Gallagher SMB Mobile App

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 mobile credential (public key) is sent from the phone to the Gallagher Cloud, 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.

Several points arise from this approach:

- 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.
- 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 remains secure.
- 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.
- 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.
- For an attacker to clone or compromise a credential, they must:
  - At bare minimum have physical access to the phone.
  - Modify the phone’s operating system to circumvent the phone's built in security defences.
  - 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.

7 Gallagher SMB Key Tags

Gallagher SMB Key Tags are encoded using an NFC enabled smartphone, running the Gallagher SMB Mobile app. A user with elevated privileges must authenticate themselves prior to encoding a tag. When encoded, a site-specific application is stored securely on the tag, meaning the tag can only be used on the site(s) it was encoded for.

Site applications are protected by site specific diversified keys stored securely in AWS. Multiple layers of security prevent tag cloning.

The tag's unique serial number is available for use by third-party systems.

The Gallagher SMB site applications encoded on the Key Tag can only be read by Gallagher readers installed at the site corresponding to the encoded application.

- Customers can encode and allocate tags to users via the SMB Mobile app.
- Key Tags provide an alternative option to using a smartphone for accessing a site.
- SMB Tags can be used across multiple sites.
- The Key Tags are MIFARE DESFire EV2/EV3 4k key fobs.
- SMB Key Tags contain a cryptographic signature issued by Gallagher, which ensures authenticity and prevents tag cloning.
- Up to 27 site applets can be stored on an SMB Tag.

NOTE – the default setting for each area on an SMB site requires two-factor authentication for local disarming. For convenience, each area on a site can be configured to allow single factor authentication to disarm an area. However, single factor authentication lowers the security level of the area as a single credential can be used to disarm the area – meaning a phone user with a valid mobile credential will be able to locally disarm the area without needing to authenticate themselves.
This should be a conscious decision made by the installer in consultation with the customer. The customer must request from their installer, that users be able to disarm using a tag. A phone user will still need to unlock their phone, before presenting it at the reader.

8 User Codes

The Gallagher SMB security system supports the use of User Codes to allow Area arming/disarming and Door access. To allow an Area to be disarm via a User Code, the Area needs to be configured for single-factor authentication – refer Note below. A site must also have at least one T30 Keypad Reader configured before User Codes can be issued and used.

Currently only 6-digit system generated user codes are supported. Only Site Managers can generate User Codes. Generated user codes are encrypted and stored securely in the SMB Cloud Services database.

Generated User Codes can be viewed from the Gallagher SMB Mobile app (by Site Managers) or, User Codes can be sent via an SMS message to individual users. User Codes that are sent via SMS cannot be viewed by any site user (or Technician) – only the receiving user will be able to view the code in the SMS message. When a User Code is viewed in the SMB Mobile App, the code is sent using secure HTTPS encrypted communication from the SMB Cloud Services to the SMB App. User Codes that are generated To Send, are sent using SMS to only the user's phone number that the User Code has been generated for.

User Codes can only be changed by deleting the previous User Code and generating a new User Code.

NOTE – the default setting for each area on an SMB site requires two-factor authentication for local disarming. For convenience, each area on a site can be configured to allow single factor authentication to disarm an area. However, single factor authentication lowers the security level of the area as a single credential can be used to disarm the area – meaning a phone user with a valid mobile credential will be able to locally disarm the area without needing to authenticate themselves.
This should be a conscious decision made by the installer in consultation with the customer. The customer must request from their installer, that users be able to disarm using user codes. A phone user will still need to unlock their phone, before presenting it at the reader.

9 Data Storage and Retention

9.1 Gallagher Cloud Services

Gallagher Cloud Services encrypts all SMB data at rest using AES-256 or better. Customer data (site data) is replicated across multiple AWS data centres. Customer data is backed up nightly, and the backups replicated across the data centres.

The registration process for the Gallagher SMB Mobile app will require user's details to be sent to the Gallagher Cloud Services. The Gallagher Cloud services then uses these details to send Mobile app invitations to users. Refer to the Gallagher SMB Privacy Policy for more information about user data storage and retention:
https://security.gallagher.com/Solutions/SMB/Policies

9.2 Removing all information about your site from Gallagher Cloud Services

To remove all your site information from Gallagher Cloud Services, please contact your Install Partner who will need to contact Gallagher Technical Support.

9.2.1 Personal Information

Refer to the Gallagher SMB Privacy Policy for your region: Gallagher SMB Policies

9.3 Mobile Devices

The Mobile app stores the following data locally on the phone:

- Mobile Credential Display/Diagnostic Information:
    - The name of the site a cardholder has registered against.
    - The date they registered.
    - The authentication method they selected for second factor.

  This information is not encrypted at rest. Mobile operating systems provide sandboxing which prevents other applications and most casual attackers from reading it.

- Secure Mobile Credential Information, which consists of the FIDO credential information and private keys. This information 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.

To delete mobile credential data from a mobile device, a user can uninstall the Mobile app.

9.3.1 Removing individual mobile credential data from Gallagher Cloud Services

When a Site Manager uses the Gallagher SMB Customer app to remove a mobile device from another user, the credentials are deleted from the Gallagher Cloud, and anything associated with it (e.g. FIDO public keys).

When a user removes a mobile device using the My Account screen in the Customer app, the corresponding credential and associated data is removed from the Gallagher cloud.

These functions require an internet connection.

10 Data Transmission

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

All other data transfer between the Gallagher Cloud and Mobile devices uses encrypted HTTPS.

Only TLS 1.2 or later is supported. Older protocols are disallowed which mitigates most encryption-related security risks.

Mobile App authentication is secured by FIDO.

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

Data transfer between the Gallagher Controller and the Gallagher Cloud is encrypted – refer to the Gallagher SMB Controller 6000 section above.

11 Security Controls

11.1 Gallagher Cloud Services

The Gallagher Cloud services are securely hosted using Amazon Web Services (AWS). 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 Load Balancer and Security Gateway component, which employs 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 daily where required.

Automated scanning tools are employed 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.

11.2 Mobile Devices

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

12 Monitoring and Response

Gallagher 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.

13 Security and Penetration Testing

Gallagher employ internal security focused staff, who hold several 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 when required.

An external specialist security company are engaged to do comprehensive reviews annually, or more frequently as required. Prior reviews have been conducted by CyberCX, and confirmation of these reviews is available on request.

Important: Technical details are subject to change. It is recommended you refer to the latest revision of this document, which can be found here: Gallagher SMB Installation and Training