



Gallagher Command Centre

AccessNow

Technical Information Paper

Disclaimer

This document gives certain information about products and 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The information is indicative only and is subject to change without notice, meaning it may be out of date at any given time.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 of 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 2026. All rights reserved.

Table of Contents

1	Background.....	3
2	Cloud Service Terms	4
3	Overview.....	4
	3.1 Service Architecture	4
	3.2 Deployment.....	4
	3.3 User Authentication	4
4	Network Requirements	5
	4.1 White Label URL - Customer Domain Support	6
	4.2 Email Service	6
5	Integrations	6
	5.1 Command Centre	6
	5.2 Identity Providers.....	6
	5.2.1 Identity Provider: User Group Mapping	6
6	Data Security	6
	6.1 Data in Transit	7
	6.2 Data at Rest.....	7
7	Data Processing Terms	7
	7.1 Data processing by AWS	7
	7.2 EU and UK Customers Data Processing	8
8	Security Controls	8
	8.1 Certifications	8
	8.2 Penetration Testing.....	8
9	Monitoring and Response	9
10	Service Terms	9

1 Background

This document outlines **AccessNow**, a PIAM (Physical Identity and Access Mangement) service that extends Command Centre's identity management. AccessNow manages physical identity lifecycles and access, improving security, compliance, and user experience. Cloud-native automation enables efficient requests, approvals, and provisioning.

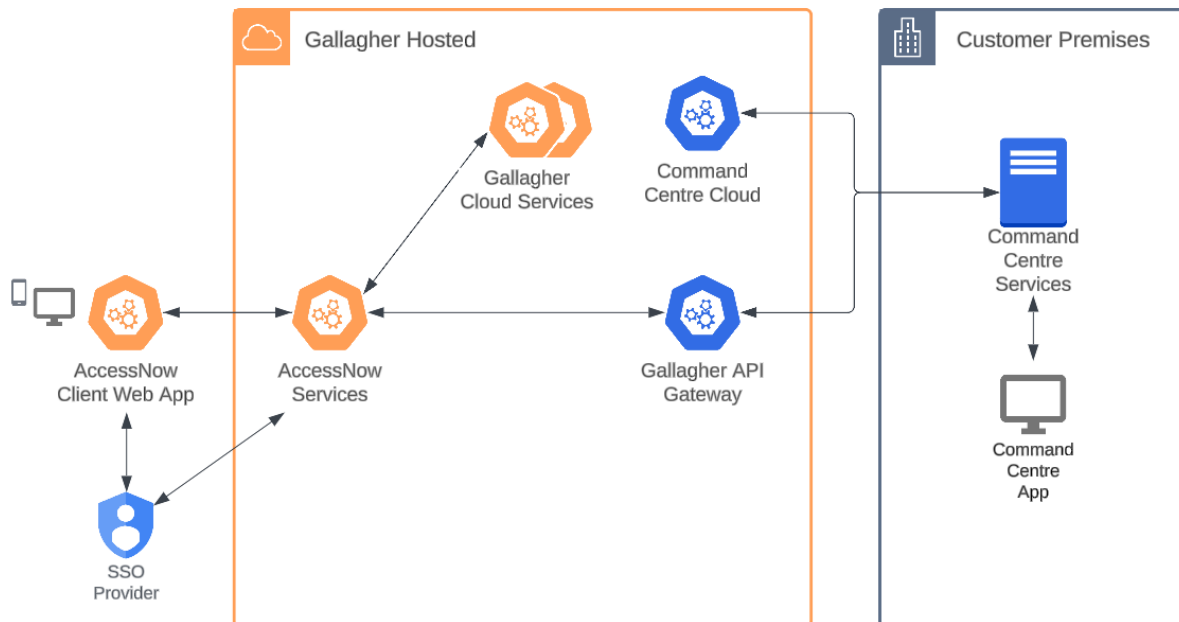
2 Cloud Service Terms

The [Gallagher Cloud Services – General Terms](#) outline how customers can use Gallagher's cloud services, including AccessNow, under a binding agreement with Gallagher Group Limited. The document covers subscriptions, service delivery, data handling, liability limits, customer responsibilities, and provider obligations.

3 Overview

3.1 Service Architecture

Access Now is a cloud service operated by Gallagher. It is available through a publicly accessible web application, which communicates with a dedicated backend. The backend connects to on-premises Command Centre servers using the Gallagher API Gateway.



3.2 Deployment

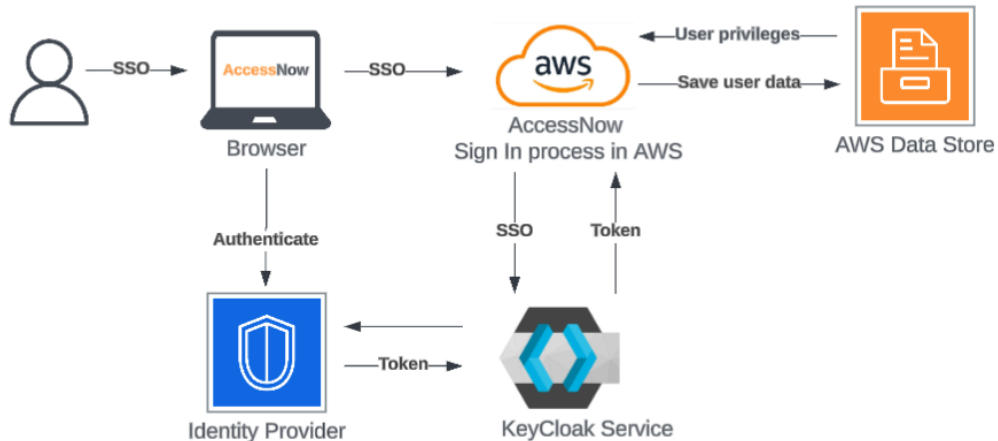
The AccessNow workflow solution is located in **Sydney, Australia**. Several redundant servers are used within the region to support scalability and fault tolerance.

3.3 User Authentication

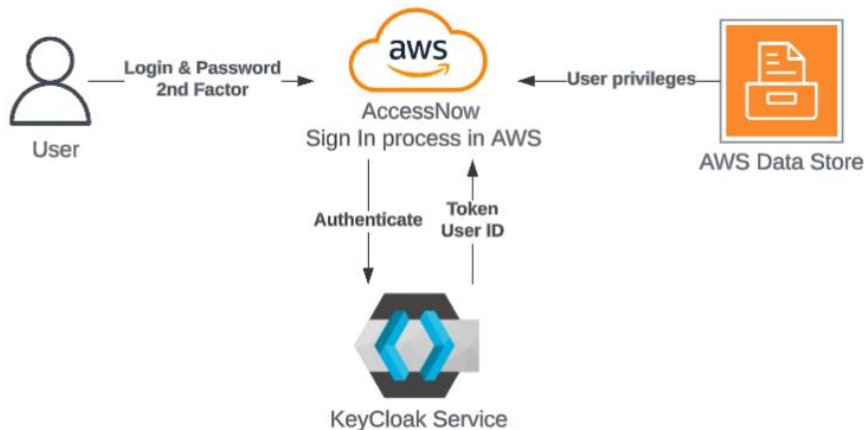
AccessNow primarily uses customer Single Sign-On (SSO) for authentication. Gallagher also offers an Authentication Service for users without SSO, such as Channel Partner users.

Supported authentication and authorization protocols include OpenID Connect, OAuth 2.0, and SAML.

Login with Single-Sign-On (SSO)



Login with username & password



4 Network Requirements

The AccessNow workflow solution depends on the Command Centre server being connected to the Command Centre Cloud via Gallagher API Gateway. Please refer to the technical information paper on the Gallagher API Gateway to ensure that network requirements for those services are met.

The main interaction point of the AccessNow is a web application hosted by Gallagher. Gallagher publicly hosts this application at an address under the following:

DNS:

<https://<customer>-sa-ap-southeast-2.security.gallagher.cloud>

<https://<customer>-an-ap-southeast-2.security.gallagher.cloud>

Authentication DNS:

<https://auth-sa-ap-southeast-2.security.gallagher.cloud>

<https://auth-access-now-ap-southeast-2.security.gallagher.cloud>

AccessNow supports also custom domains.

4.1 White Label URL - Customer Domain Support

AccessNow supports white-label URLs, allowing the web application to be accessed on the customer's domain.

To set this up, the URL must be configured in AccessNow. Details for a CNAME record will be returned. These details should be used to create a CNAME record at the customer's domain provider.

Completing this configuration starts a process for validating the domain and generating an SSL certificate. This process takes some time to complete, after which the URL will be usable.

4.2 Email Service

Customers can use the Gallagher email service. No Setup required.

5 Integrations

5.1 Command Centre

AccessNow connects to the Command Centre using a REST API Client. Both systems require configuration, which is detailed in the AccessNow user guide.

5.2 Identity Providers

AccessNow enables integration with common Identity Providers, such as Microsoft EntraID, allowing users to utilise SSO login and access user information on these platforms.

AccessNow requires a unique link between its users and Command Centre cardholders for management purposes. For cardholders to be managed from Accessnow, a distinct Personal Data Field must exist and be filled in Command Centre. This unique identifier field is determined during SSO set-up.

To enable SSO, you must register AccessNow as an application in the Identity Provider. Then, add the configuration in AccessNow to include the Client ID, Secret, OpenID Connect authorize and token URLs. AccessNow provides a redirect URI, which must also be added to the Identity Provider settings.

5.2.1 Identity Provider: User Group Mapping

AccessNow supports user groups that can be mapped to multiple Identity Provider groups.

When this feature is enabled, the Identity Provider configuration for AccessNow should add a claim to the token that includes the user's groups.

In AccessNow, it is necessary to configure the name of this claim. Mapped Groups can then be established, referencing Identity Provider groups by their ID.

6 Data Security

6.1 Data in Transit

All data transfer between Gallagher Command Centre, Gallagher API Gateway, Gallagher AccessNow, Gallagher Cloud Services, and clients uses encrypted HTTPS.

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

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

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

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

6.2 Data at Rest

The AccessNow solution persists data in AWS datastores, using industry-standard AES-256 encryption for data and metadata at rest.

Data retained by the AccessNow solution includes:

- User Id, Name and Email.
- Other user and cardholder data entered or retrieved from Command Centre that is required as part of a request, including actions taken to complete the request as configured in workflows.
- Data specific to managing the request to allow auditing.
- Customer defined lists of data that can be used in workflows.

7 Data Processing Terms

[Gallagher's Data Processing Addendum \(DPA\)](#) forms part of the [Gallagher Cloud Services General Terms](#) and applies to **all Gallagher cloud customers worldwide**, regardless of location. The DPA sets out Gallagher's obligations as a data processor and the customer's role as data controller (or equivalent under local law), and it ensures compliance with all applicable global data-protection regulations.

The agreement ensures compliance with major privacy laws, governs international transfers, outlines security measures, defines the use of AWS as sub-processor, covers breach notification duties, retention and deletion rules, and incorporates required GDPR-style annexes for lawful processing and transfers.

7.1 Data processing by AWS

AccessNow SaaS is deployed on **Amazon Web Services (AWS)**. Data is hosted in AWS **Australia**, so primary processing occurs in Australia.

[AWS Data Processing Addendum](#) adds to the Gallagher-AWS Agreement, detailing AWS's terms for handling Customer Data as a sub-processor. This DPA ensures compliance with data protection laws, outlines roles and

responsibilities, and establishes security measures for handling Customer Data within the AWS Network. It also includes **2021 EU Standard Contractual Clauses**, processor obligations, security measures, and sub-processor terms.

7.2 EU and UK Customers Data Processing

Where required, both Gallagher's and AWS's DPA agreements incorporate the European Union Standard Contractual Clauses (SCCs) and the UK International Data Transfer Addendum (IDTA) to support lawful international transfers of personal data. These transfer mechanisms apply automatically when EU or UK data is involved and do not affect customers whose data is not subject to those jurisdictions.

[AWS UK GDPR Addendum to AWS Data Processing Addendum](#) serves as a supplement to the AWS Data Processing Addendum (DPA) and is applicable when the processing of UK Customer Data during the use of AWS services is subject to the UK GDPR. This document clearly specifies that it augments the AWS DPA and implements the UK Standard Contractual Clauses (SCCs) with the UK Addendum for data transfers from the United Kingdom to AWS regions such as Australia.

8 Security Controls

Our cloud services are hosted on Amazon Web Services and are separated from external networks through an AWS Virtual Private Cloud.

Strict firewall and access controls secure all administrative functions and endpoints.

All administrative users of our cloud systems must have a Security Technician Certificate of Approval from the New Zealand Private Security Personnel Licensing Authority.

Cloud services are restricted to accessing only the specific resources they need, such as their designated database or key storage, and cannot access resources for other services.

Platform updates, including Operating System security patches, are implemented daily as necessary. We utilise automated scanning tools that provide alerts if any third-party software components in use are referenced in a vulnerability database, such as the public CVE database or similar sources.

8.1 Certifications

Gallagher maintains data security and privacy standards. Its cloud-hosted solutions are SOC 2 Type 2 certified, and Gallagher also holds certifications such as ISO27001, CAPSS CPNI 2021, and EN50131-4.

8.2 Penetration Testing

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

Our internal security staff hold a key role in the development of our cloud services, providing expertise, security reviews and internal penetration testing.

An external specialist security company will be engaged to conduct a comprehensive review when major changes are made, as determined by our internal security review process. External penetration tests are not conducted on a fixed annual schedule, but rather in response to significant updates or as required by

internal assessments. Prior reviews have been conducted by CyberCX (previously Insomnia Security), and executive summaries of the findings are available by request.

We are open to customer or otherwise externally arranged penetration testing, however we require advance notice and approval from Gallagher to avoid disruption of our services which may impact other customers.

9 Monitoring and Response

We automatically analyse application and database logs, monitor system resources, and track application health.

Alerts are generated and sent to Gallagher, with 24/7 monitoring of service status. Customers are notified of incidents or outages through Channel Partners or our [Status Page](#). Subscribe for updates [here](#).

10 Service Terms

Review the service level provided in the [Cloud Service Level Agreement](#) and check the details of [Cloud Services Terms and Privacy](#).