



Access Control as a Service (ACaaS)

Service Definition Document

G-Cloud 15



Crown
Commercial
Service

Contents

What is ACaaS?

Backup and disaster recovery

Support & managed service

Service constraints

Technical Requirements

Outage & Maintenance Management

Data Storage & Security

What is ACaaS?

ACAAS is a managed **cloud-based access control system** supporting single or multi-site businesses. User roles and permissions are centrally managed, with encrypted, 24/7 access from any approved device. Hardware is minimal (readers/keypads), and the platform is flexible, scalable, and integrates with alarms, video, and intrusion systems.

Alert Data provide Cloud Access Control as managed service, where we host your system and take care of it for you. It's all paid for by subscription, with no upfront costs or hidden fees.

Products we support:

Hosted

- Maxxess
- Paxton
- TDSI

Web ready

- TDSI Gardis Pro
- Avigilon ACM

Features & benefits

Hosting your Access Control in the Cloud provides your business with the following benefits:

- Secure & Safe – All data encrypted and stored offsite.
- Access Anytime, Anywhere – Web-based interface makes control simple.
- One Platform, Every Site – Centralised control for multiple locations.
- Right Access, Right People – Role-based permissions keep your team secure.
- Works with What You Have – Integrates with alarms, video, and intrusion systems.
- Grow Without Limits – Easily add new access points as you expand.
- Less Hardware, Less Hassle – Minimal on-site equipment required.
- Compatible & Flexible – Supports Maxxess, Paxton, TDSi (Gardis).
- Reduced IT burden – Let us take care of onboarding and managing your system health

Backup & Disaster Recovery

Our disaster recovery procedures ensure rapid restoration of service in the event of an outage, minimising downtime and maintaining operational continuity for all users. The plan covers immediate response, system restoration, and ongoing monitoring to prevent recurrence.

Response and Recovery Actions

- Immediate: On detection of an issue, senior management and IT teams are alerted, and the recovery process is mobilised. Critical services are prioritised.
- Within 3 Hours: Impacted users are notified; system performance is assessed; backup and restore processes are initiated; hardware and UPS status are checked.
- Within 8 Hours: Coordination with external service providers occurs, temporary or replacement hardware is installed if necessary, and telecommunications failover is implemented if required.
- Within 24 Hours: Systems are gradually restored to minimum operational capability, tested for integrity, and full support is provided to users.
- Ongoing: System performance is continuously monitored, user requests are addressed, and lessons learned are incorporated to improve future DR performance.

Backup Strategy

- Data and system configurations are backed up continuously to encrypted, geographically redundant locations.
- Backups are routinely tested for integrity and recovery capability.

Compliance & Security

- All data is protected in transit and at rest in accordance with GDPR, ISO 27001, and relevant NCSC Cloud Security Principles.
- Access to backups and recovery procedures is strictly controlled and monitored.

Support & Managed Service

ACaaS is fully managed service, providing end-to-end support throughout the customer journey. As it is a managed service, ACaaS is suitable for businesses with limited technical expertise or multi-site businesses with a stretched IT team.

Each customer is assigned a dedicated Account Manager to provide ongoing guidance and act as the primary point of contact. Our managed service and self-service support are included in the subscription, with optional enhanced services such as out-of-hours monitoring available at additional cost (get in touch for details).

Our proactive monitoring continuously checks system health, camera performance, and cloud infrastructure, resolving issues on behalf of the customer and only contacting them when necessary. Support is available via ticketing, email, phone, or by booking calls and reporting faults online.

Onboarding and offboarding support

We provide full onboarding support. We migrate your current on-premise system (single or multi-site) and move it to a host deployment. We handle setup and configuration, plus train the team on the system and workflows, to ensure rapid adoption of the platform, without costing IT time. If support is needed, customers can get in touch via their dedicated account manager by phone or email, or they can submit a ticket to report any faults online.

Our proactive support ensures the system is operational from day one, with any issues identified and resolved by our team. Users also have access to manufacturers guides, and online resources to reinforce training and enable self-service.

Should a customer choose to leave the service, we provide an electronic data extract for users and events at no additional cost.

Support response times

Response times based on priority of the incident raised. Initial response times based on priorities outlined below.

P1 – within 1 hour of case submission

P2 – within 4 hours of case submission

P3 – within 1 business day of case submission

P4 – within 2 business days of case submission

Service Definition – G-Cloud 15

Phone support is available 9-5 (UK time), Monday to Friday.

Service constraints

Specific constraints depend on the software product we are hosting for the customer.

Technical requirements

As a Cloud service, no application is required; ACaaS is designed to be accessible on any device, via an internet browser.

Supported browsers:

- Edge
- Firefox
- Chrome
- Safari
- Opera

Stable internet is required for a reliable experience. If a customer has a remote site or unstable connection, we can work with them to maximise bandwidth.

Outage & maintenance management

We offer a 99% guaranteed availability, subject to software patching and updates.

Our service is designed for high resilience, ensuring continuous availability and secure operation. The platform is hosted in UK-based cloud datacentres with redundant power, network, and storage systems. Core infrastructure and data are replicated across multiple nodes to prevent service disruption. Proactive system health monitoring identifies and mitigates potential issues before they impact users. Detailed information about our datacentre setup and resilience measures is available on request for procurement or security review purposes.

Service outage reporting is provided via email. If any devices go offline or experience issues, the system automatically generates alerts and notifies users by email. This ensures customers are promptly informed of outages and can take any necessary action.

Data Storage & Security

Alert Data take Cloud security seriously, following industry-leading guidance and standards.

All data is stored in a GDPR-compliant UK data centre. Penetration testing is undergone at least every 6 months by a CREST-approved service provider. Data is encrypted in-transit and at rest. Our data centre has physical access controls, complying with ISO27001, and 24/7 security including Cloud CCTV with off-site recording. We also protect data using obfuscating techniques and data storage sharding.

We are Cyber Essentials Plus Certified, demonstrating our commitment to top-tier security practices.