CloudClevr

Clevr360 Security Guide

PUBLIC DOCUMENT

CloudClevr

Table of Contents

1 Introduction

Clevr360 has been designed and built with an inherent level of security controls and principles. It leverages the latest technologies available from Microsoft Azure to allow for the most stringent of security controls to be implemented.

CloudClevr selected the use of the Microsoft Azure platform given it is designed to host millions of customers and applications simultaneously, supporting the same technologies millions of developers and IT professionals already rely on and trust. It thereby provides a trustworthy foundation upon which Clevr360 can meet its security requirements. Azure in this context provides a wide array of configurable security options that are customised by Clevr360 to deliver against its security strategy.

The system architecture and operating methods adopted as part of the delivery programme are also secure in design to ensure data integrity and to minimise risk of any security breach or security related impact. These methods and technologies collectively ensure a highly secure application is delivered.

The main security aspects implemented and leveraged by Clevr360 are summarised in this document.

This is a living document which is subject to periodic updates as the security landscape evolves.

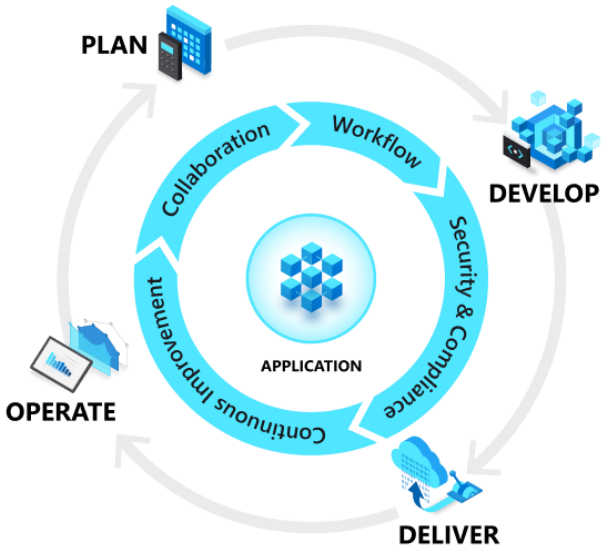
2 Development Programme

The following aspects are implemented as part of the Clerv360 development programme:

Coding Practices - secure and best-practice coding principles are followed by the software development team. Code is stored in a version control system that has strong authentication controls regulating who can review and accept code changes. Input validation is performed along with appropriate error handling. Regular code reviews and analysis tooling are used to identify potential security issues in the code as part of the overall software development lifecycle.

Security Updates - the technology chosen for the implementation of the Clevr360 software application is efficient, mature, mainstream, and reliable which also provides long-term security updates and available support. This primarily includes the use of C# & .NET framework for backend services along with React 18v framework for frontend services. Updates to these technology stacks form part of the product review & planning sessions.

Software Development Lifecycle - the development methodology and overall Clevr360 development programme is based on agile principles with an iterative delivery approach. CloudClevr has invested heavily in automated testing along with continuous integration & continuous delivery practices.



Code changes are frequently merged into a central repository, triggering an automated build and test process. This approach can quickly identify any security vulnerabilities or concerns, enabling them to be addressed as part of each software iteration. This activity also continuously deploys software to a testing

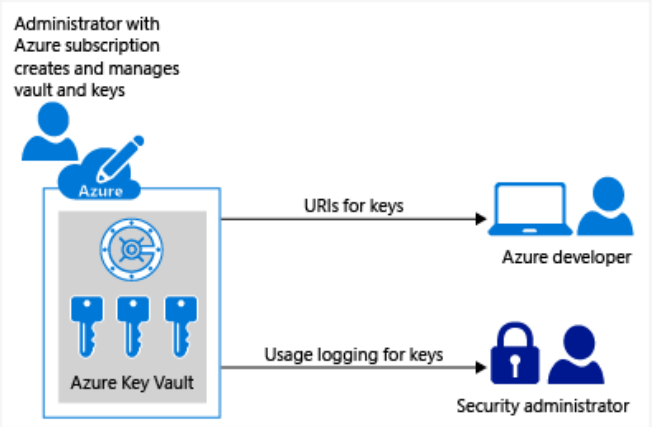
environment once code has been built and tested. Following this, tooling is used to automatically deploy the code into the production environment once it has been built, acceptance test completed, and ready as part of our internal release process. This removes any risk of human error which can result in potential security gaps being introduced.

3 Service Architecture

The following aspects are implemented as part of the Clevr360 service architecture:

Data Isolation - the Clevr360 service architecture is multi-tenanted in design & operation, and as such provides full isolation of associated users and associated data between each organisation.

Centralised Management – the Clevr360 service architecture implements the use of a secured and centralised storage approach for application configuration and key management; in this context Azure Key Vault is leveraged by the Clevr360 application. Azure Key Vault is a cloud service for securely storing and accessing secrets. It encrypts keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). A key vault is in place for CloudClevr with the Clevr360 application provided with URIs to call for keys.



This approach enables full control over stored keys where permission is granted for applications such as Clevr360 to use them as needed. In this context Microsoft doesn't see or extract keys and applications never have direct access to keys. This approach ensures that data is separate from the software code itself ensuring improved security and overall resilience.

Disaster Recovery & Business Continuity – Clevr360 places emphasis on business continuity through a disaster recovery plan. Our disaster recovery strategy is designed to ensure a quick resolution of operations in the face of unforeseen disruptions. This minimises downtime and safeguards the integrity of our services.

Back-up Procedure - Critical data is automatically backed up to a geographically separate location using Microsoft Azure Backup.

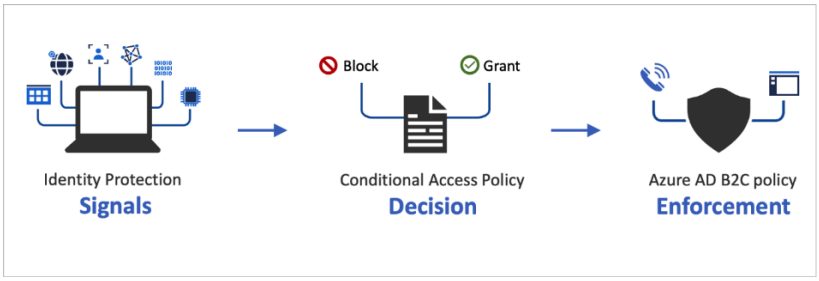
4 Service Access

The following aspects are implemented as part of the Clevr360 service access:

Authentication - all users that access the Clevr360 application or any associated infrastructure are securely authenticated, with all application access and actions performed audited. Clevr360 leverages the use of Azure Active Directory B2C technology which provides business-to-customer identity as a service.

Azure AD B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks. Clevr360 leverages these capabilities implementing custom policies to deliver the required user flows and experience.

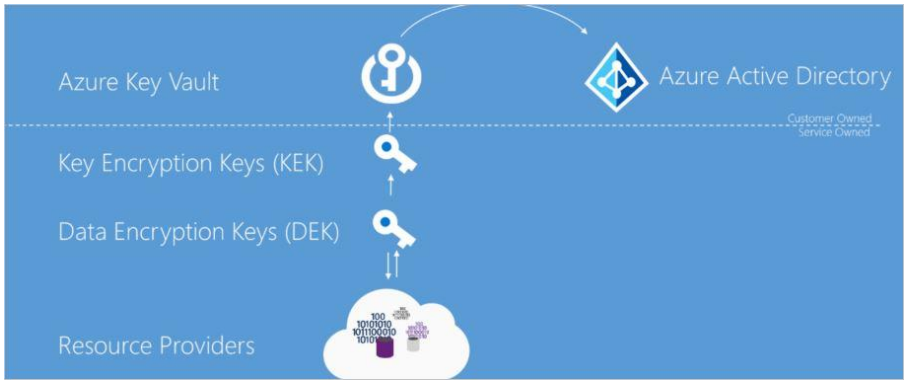
Multi-Factor Authentication (MFA) – all users that access the Clevr360 application must do so with MFA. This is enforced by Clevr360 which leverages Azure Active Directory B2C capabilities which integrate directly with Microsoft Entra MFA to add a second layer of security when accessing the Clevr360 application. Clevr360 leverages Microsoft Authenticator along with password as the two authentication methods.



5 Service Data

The following aspects are implemented as part of the Clevr360 service data:

Encryption at Rest - data encryption at rest is a mandatory step towards data privacy, compliance, and data sovereignty. Clevr360 leverage Azure cloud storage environments and requests that the storage service automatically encrypt data when writing it to Azure Storage. Clevr360 leverages a strong bit key length (minimum 256-bit) and cipher suite. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly. The storage location of the encryption keys and access control to those keys leverages Azure Key Vault.



Encryption in Transit - encryption in transit is a mechanism of protecting data when it is transmitted across networks. Clevr360 leverages a strong bit key length (minimum 256-bit) and cipher suite. Clevr360 leverages Transport Layer Security (TLS) protocol to protect data when it's traveling between the application and customer devices. Microsoft datacentres negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

CloudClevr ICO Registration– CloudClevr is registered with the ICO as per the below table.

CloudClevr Holdings Ltd	ZB640354
CloudClevr Ltd	Z5688672

Data Location and Usage – all data associated with the Clevr360 platform is hosted entirely within the United Kingdom. This applies to every environment in our delivery pipeline including development, testing, and production. Keeping all our data within the United Kingdom helps us follow strict rules and gives users peace of mind about where their information is kept.

To further protect customer information, no live or identifiable customer data is ever used in development or testing activities. Instead, these environments operate using anonymised datasets to uphold data privacy and minimise any associated risks. This approach is a core component of our commitment to safeguarding user trust and ensuring compliance with UK GDPR.

Data Isolation in a Multi-Tenant Environment – Clevr360 operates as a multi-tenant platform, meaning multiple organisations' data may be hosted on the same physical infrastructure. However, strict security controls are in place to keep each customer's information completely separate. Access credentials are limited to a single tenant, so no organisation can access another's data.

Data Retention and Return - information about your organisation and associated account details is stored for as long as you use the Clevr360 service. Data from your connected services, such as Microsoft 365, is refreshed daily and kept to support comparative insights, analytics and reporting features within Clevr360. We don't store any additional data beyond what is collected from your connected services. Because of this, we don't normally provide a copy of that data back to you as it remains available through the connected services themselves.

6 Web Interface and Access Requirements

Clevr360 is accessed through a secure web interface, using HTTPS with a minimum of TLS 1.2 encryption and support for forward secrecy. This ensures that all data in transit is protected using industry-standard security protocols.

The application is compatible with recent versions of all major web browsers. While we don't publish a definitive compatibility list, our security design is browser-independent and does not rely on any specific browser features to remain secure.

There are no facilities for uploading files into the platform. Similarly, downloads are only possible through the main web interface using secure, encrypted connections.

Clevr360 communicates over port TCP/443, which is standard for secure HTTPS traffic. In most environments, no firewall changes are required. However, depending on your organisation's security policies, you may need to whitelist https://app.clevr360.com to allow access.

7 Logical Access Security

Each user within Clevr360 is issued a unique ID, which ensures individual accountability and traceability within the platform.

User Password Requirements – the following requirements are set by the Clevr360 application for all users:

- At least eight characters long
- Include a combination of at least three of the following;
    - lowercase letters
    - uppercase letters
    - numbers
    - special symbols

Sessions - sessions remain active for up to one hour but can be refreshed if the user remains active.

User Roles - Clevr360 supports three user roles with varying levels of access:

- **User**: Can view insights on utilisation, adoption, and productivity, and access general reports.
- **Admin**: Has all User permissions, plus access to assurance insights, full reporting, and user management.
- **Super Admin**: Has full access, including permissions to manage service integrations and metadata.

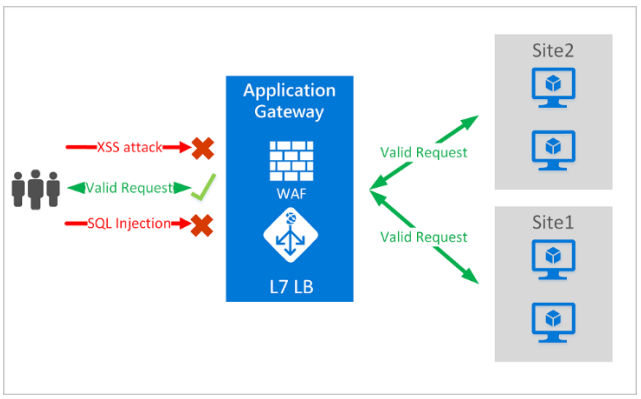
Permissions are controlled by Super Admin users within your organisation and CloudClevr support staff. All user logins are recorded through Microsoft Active Directory B2C for audit purposes.

User Authentication - authentication is handled through local accounts using Microsoft Active Directory B2C. Single sign-on (SSO) is not currently supported. However, all users are required to use time-based one-time password (TOTP) multi-factor authentication (MFA) to enhance account security.

8 Service Infrastructure

The following aspects are implemented as part of the Clevr360 service infrastructure:

Web Application Firewall (WAF) – is a feature of Azure Application Gateway leveraged by Clevr360 to help protect the application from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacking. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as the top 10 common vulnerabilities. The use of a centralized web application firewall to protect against web attacks makes security management much simpler and gives better assurance to the application against the threats of intrusions.



Secure Access - all backend services and infrastructure are deployed within a private and secured network in the Azure environment, with controlled access, and a layer of abstraction implemented between the publicly accessible front end web application and all backend services. This provides an isolated runtime environment deployed into an Azure Virtual Network, with a layered security architecture providing differing levels of network access for each application tier.

Application Insights - is an extensible Application Performance Management (APM) service provided by Azure that is leveraged by the Clevr360 application. This is used to monitor services and automatically detect performance anomalies. If there are crashes, failures or performance issues, our support teams can search through the telemetry data in detail to diagnose the cause. Application Insight thus becomes a valuable security tool because it helps with the availability in the confidentiality, integrity, and availability security triad.

9 Azure Platform

As referenced Clevr360 leverages the latest technologies available from Microsoft Azure to allow for the most stringent of security controls to be implemented.

Microsoft Azure runs in datacentres managed and operated by Microsoft. These geographically dispersed datacentres comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability.

The datacentres are fully managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity.

Microsoft publish a series of articles which provides information about what they do to secure the Azure infrastructure; this information can be accessed here.

10 Security Validation

Clevr360 has undergone comprehensive penetration testing conducted by a trusted third-party provider to validate the security posture. This has enabled the Clevr360 product team to ensure there are no critical or high-risk vulnerabilities present within the solution, demonstrating our commitment to proactive security measures.

Any identified lower risk vulnerabilities will be remediated as part of the on-going product development lifecycle. This approach ensures the security posture of Clevr360 is robust in operation and ensures the integrity and confidentiality of user data is upheld.

Continued vigilance and proactive measures, such as regular penetration testing, are integral components of our security strategy. We remain dedicated to staying ahead of potential threats and ensuring the highest standards of security for our platform and its users.

11 General Data Protection Regulation (GDPR)

CloudClevr and Clevr360 acknowledges the importance of data privacy and compliance with the General Data Protection Regulation (GDPR). As a European Union regulation on information privacy, GDPR sets stringent standards for the protection of personal data within the European Union and the European Economic Area. In alignment with GDPR principles, CloudClevr has implemented robust measures to safeguard user data and ensure compliance with the regulation within Clevr360.

Key GDPR Compliance Measures

Data Minimisation - CloudClevr follows the principle of data minimisation, ensuring that only the necessary personal data required for specific purposes is processed. Unnecessary data collection is avoided to uphold user privacy.

User Consent - prior and explicit consent is obtained from users before collecting and processing their personal information. CloudClevr employs transparent and user-friendly mechanisms for obtaining and managing consent.

Data Subject Rights - CloudClevr and Clevr360 respects the rights of data subjects as outlined in GDPR. Users of Clevr360 have the right to access their data, rectify inaccuracies, and request the deletion of their information. CloudClevr has processes to facilitate these rights.

Data Security - to ensure the security of personal data, Clevr360 employs encryption at rest and in transit. Strong encryption standards are applied to protect data integrity and confidentiality.

Incident Response and Reporting - in the event of a data breach, CloudClevr has a defined incident response plan to promptly identify, contain, and mitigate the impact. Additionally, CloudClevr complies with GDPR reporting requirements, notifying relevant authorities, and affected individuals when necessary.

Data Protection Impact Assessment (DPIA) - CloudClevr conducts regular DPIAs on Clevr360 to assess and mitigate the risks associated with processing personal data. This approach ensures ongoing compliance with GDPR requirements.

By adhering to these GDPR compliance measures, CloudClevr demonstrates its commitment to upholding the highest standards of data protection and privacy for its users.

CloudClevr

CloudClevr as a Data Controller for Clevr360

As a data controller under the General Data Protection Regulation (GDPR), Clevr360 assumes responsibility for determining the purposes and means of processing personal data. Clevr360 is committed to upholding the highest standards of data protection
and privacy.

Key Aspects of Clevr360's Role as a Data Controller

Purpose Limitation - CloudClevr clearly defines and communicates the specific purposes for which personal data is processed within Clevr360. CloudClevr ensures that data processing is limited to what is necessary for the intended purposes.

Legal Basis for Processing - Clevr360 identifies and communicates the legal basis for processing personal data. Whether based on user consent, contractual necessity, legal obligations, or other legitimate interests, Clevr360 ensures that data processing is conducted lawfully.

Data Protection by Design and Default - Clevr360 integrates data protection principles into its systems and processes from the outset. CloudClevr follows privacy-by-design and privacy-by-default principles to minimize data risks and enhance user privacy.

Accountability - CloudClevr acknowledges its accountability as a data controller. The company maintains comprehensive records of its data processing activities, conducts regular internal audits, and cooperates with relevant data protection authorities.

Data Transfer Considerations – in general if personal data is transferred outside the European Union or the European Economic Area, CloudClevr ensures compliance with GDPR requirements for such transfers. Adequate safeguards, such as Standard Contractual Clauses or other approved mechanisms, are implemented to protect the data. However it should be noted that Clevr360 is exclusively hosted within the UK region of the Microsoft Azure platform, as such personal data processed by Clevr360 will not be transferred outside the European Union or the European Economic Area.

By fulfilling its role as a data controller with Clevr360 in accordance with GDPR principles, CloudClevr aims to instil trust and confidence in users regarding the responsible handling of their personal information.

CloudClevr

Data Capture and User Association

To create an account on Clevr360, we collect basic details from both the organisation and individual users.

For the organisation, only the organisation name is required.

For each user, the following information is captured:

- First name
- Last name
- Email address
- Phone number (optional)

All user information is indexed against both the individual user and the associated organisation, allowing for clear relationships between users and their organisation within the system.

CloudClevr

12 Version

Version	Date	Comments
1.0	24/02/2024	Initial release
1.1	03/10/2024	Updated release
1.2	2606/2025	Updated release