OpenAthens Security Guide 2.2

Introduction

OpenAthens is a cloud-hosted Identity and Access Management tool that utilizes the SAML 2.0 protocol to provide a single sign-on user experience for library patrons. OpenAthens can be configured to connect to an institution's own LDAP directory or other Identity Provider (e.g., ADFS, Okta, etc.) or, it can act as an Identity Provider itself.

As a provider of sensitive IT Services, OpenAthens takes security extremely seriously and utilizes a range of measures to secure its applications and data. OpenAthens is part of Jisc which provides a range of services to UK higher education and research communities. Jisc has a long history of implementing a strong security culture and cyber security is one of the services it provides to its customers. Good security practices are embedded across the organization.

This document provides an overview of OpenAthens approach to security. It provides information useful to customers and prospective customers carrying out due diligence on OpenAthens as a supplier.

Jisc

Security management

Jisc's Information Security Team maintains the organization's information security management system (ISMS). The ISMS is continuously monitored and improved to conform with or exceed the standards required by ISO 27001. Regular, mandatory training is delivered through an online learning platform to ensure all staff are familiar with their responsibilities and up to date with policies and procedures. Clear processes are in place to manage security related incidents and to liaise with law enforcement if required.

Business continuity

Jisc operates a business continuity plan designed to minimize disruptive incidents and to ensure the fastest possible return to normal operations. The plan consists of comprehensive policies, procedures, and technologies to manage a wide range of potential incidents. It is based on the plan-do-check-act methodology and the ISO22301 standard. The business continuity plan is reviewed annually.

Recruitment

Jisc's HR team ensure that all new employees are background checked through references and make sure they have attained the qualifications they claim to. Contracts for new staff and the induction process emphasize individual responsibilities for information security and the potential penalties for misuse. Staff resignations trigger a leaver process to ensure access rights to Jisc systems are revoked in a timely fashion.

Acceptable use

The Secure Working Practices Policy provides guidance and policies covering the acceptable use of Jisc's information assets. It is issued to both permanent and contract staff and forms part of the induction for new starters.

Security awareness

Security awareness training is delivered through Jisc's online training platform. It is delivered at least annually and is mandatory for all employees.

Risk management

An organization-wide risk management system is in place to identify, track, and manage risks that threaten Jisc's ability to achieve its objectives. As well as managing risks at board level, Risk Champions are assigned to each directorate in the organization. Their responsibility is to identify and manage directorate level risks and ensure they are reviewed in line with the risk cycle and also to coordinate risk management with other directorates.

Google Cloud Platform (GCP)

Almost all of the OpenAthens applications and data are hosted with Google's public cloud platform (GCP.) Google's approach to security was a major factor in the selection of GCP as the hosting platform for OpenAthens. As a public cloud provider, Google is able to invest significantly more resources in building a secure infrastructure internally.

GCP security overview

Google's security approach for GCP is outlined in its security white paper which should be made available to you along with this document, however it is also available from the GCP website **https://cloud.google.com/security/overview/whitepaper**. We recommended that customers read the document as GCP is a key part of the overall security stance for OpenAthens.

GCP physical data centre security

Google's data centers include a range of measures to ensure only authorized personnel can access the sites. These include custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. The data center floor features laser beam intrusion detection and access is gained via a security corridor that uses multi-factor access control. All sites are monitored 24/7 and are patrolled by security guards. Less than 1% of Google's staff has access to the data center floor.

GCP network and infrastructure

Google's IP data network uses its own fiber, public fiber, and undersea cables, see **https://cloud.google.com/blog/products/networking/google-cloud-networking-in-depth-cloud-cdn** for a recent map. Transfer of data across the public internet is limited to reduce opportunities for data to be intercepted. Only approved protocols and services are allowed to traverse the Google network with non-approved traffic automatically dropped. All incoming traffic is routed through front end servers that detect and drop malicious requests and DDoS attacks.

GCP hardware

Google uses its own custom-built processors, servers, and network components that do not include unnecessary components that could be a source of vulnerabilities. Servers run a custom operating system (COS) that is a stripped down and hardened version of Linux. The location and status of all hardware components are tracked using barcodes and asset tags with metal detectors and surveillance cameras used to prevent unauthorized removal. A robust disposal process ensures all data is wiped at the end of a component's life.

GCP operational security

Google uses a wide range of measures to scan and identify vulnerabilities and has a dedicated vulnerability management team responsible for tracking and resolving issues. It continuously monitors traffic to identify security issues and suspicious behaviour using both automated and manual inspections. Incident management procedures cover courses of action, notification processes, escalation, mitigation and are structured around the NIST guidance for incident handling.

OpenAthens

Infrastructure

With the exception of the EU portion of the OpenAthens Managed Proxy Service, all OpenAthens applications run on the Google Cloud Platform.

OpenAthens production, test, and development environments are run in separate projects within GCP each with their own dedicated Firewall. This ensures separation of traffic and data between projects and from other GCP customers.

Applications either run in Docker containers, primarily clustered and orchestrated by Kubernetes or use GCP's serverless technology, AppEngine. This approach minimizes the amount of server administration required by the OpenAthens team and therefore helps to reduce security risks. Google provides robust management of the underlying hardware infrastructure, and the latest, most secure updates are readily available and deployed. OpenAthens follows the GCP recommendations for configuring and hardening AppEngine instances and the Kubernetes cluster.

The data storage tier is a combination of GCPs managed SQL database and Apache Cassandra.

The OpenAthens Managed Proxy Service provides access to resources that are not available in a SAML access management federation. This service is not yet fully 'cloud-ready' so the EU part of that service currently runs on physical hardware in a UK data center due to its unique networking requirements. The Managed Proxy Service does not contain or transfer any personally identifiable information.

Data

What data is stored and why?

OpenAthens stores personally identifiable information but by default, it does not contain information that would be considered sensitive. A key principle is to minimize the data attributes required to only those needed to perform its basic function as a single sign-on service and then to allow its customers to extend the minimum default data set if required.

OpenAthens can be run by identity providers in either of two main modes: In the first mode, it can act as an organization's account directory, i.e., its store of usernames and passwords. In this mode, a username, e-mail address, first name, and surname are required to create a user account. The second mode is where a customer has an existing directory or authentication system. In this mode, OpenAthens can then be connected to that directory or authentication system and customers can map whichever data attributes they want to transfer into OpenAthens. By default, only a unique identifier needs to be mapped.

In both modes, customers can configure OpenAthens to add additional data attributes, for example, to provide richer reporting capabilities or to enhance personalization features on some publisher websites.

Data exchange with Service Providers

For a Service Provider to authorize access to its online content OpenAthens needs to pass a limited set of data attributes when a user authenticates. By default, only a unique identifier for a user is required together with the organization the user belongs to. The identifier is unique to each Service Provider and is anonymous,

Service Providers cannot identify an individual from this information and therefore cannot provide personalization services such as alerts.

Customers can configure OpenAthens to send additional information to Service Providers if required.

Data is exchanged using the SAML 2.0 standard and messages passed to Service Providers are encrypted and signed using XML cryptography and TLS.

Where data is stored

All live OpenAthens data is stored with the Google Cloud Platform and all personally identifiable data is stored within the Europe West region which is in London UK. The data storage is a combination of Google's fully managed relational database, (Cloud SQL), and Apache Cassandra.

Backups and recovery

To ensure data can be recovered in the event of a failure we take daily backups and store them in Google Cloud and separately within the DigitalOcean cloud service for additional redundancy. Backups are AES-256 encrypted and are retained for a maximum of 30 days.

Who can access data?

A small number of the OpenAthens Team with responsibilities for administering and supporting the system has access to the production environment and databases. This is strictly controlled by role and requires strong, two-factor authentication to gain access.

Customer access to user data is only possible through the OpenAthens applications using an administrator account. The data model defines a hierarchy of organizations which is the basis for the security model. At the highest level of each customers hierarchy, there is a unique domain administrator account that provides a logical separation between OpenAthens customers. Where a customer has multiple organizations, each organization has a separate administrator account below the domain level account which provides logical separation of organizations within a customer domain. This model enforces the security boundaries by ensuring any domain or organization administrator is only able to access data for their own organization and those below them in the hierarchy. There is no access permitted to higher levels of the hierarchy and there is no access permitted between domains.

OpenAthens logs all end-user and administrator activity and provides visibility through its administration tools.

Applications

The core of OpenAthens is the authentication service which performs the actual authentication operations that provide end-users with access to online content, and administrators with access to applications. However, OpenAthens is made up of a series of applications that provide a range of supporting functions required to run the service.

Data in transit

All data is encrypted in transit using TLS, both from the users' browser to the applications in Google Cloud and data moving between front end applications and databases over Google's network. For more information see: **https://cloud.google.com/security/encryption-in-transit/**

Data at rest

All data stored in Google Cloud is encrypted at the storage level using AES256. For more information see: **https://cloud.google.com/docs/security/encryption/default-encryption**

User account security

Misuse

OpenAthens monitors user activity to detect potential misuse of accounts, for example signing in from OpenAthens from different countries within a set time period. If suspected misuse is detected the user account moves to a blocked status which prevents further use. The administrator for the account receives an alert to investigate and unblock the account.

Account lifecycle

It is vital that personal data stored within OpenAthens meets the requirements for data privacy and protection and part of that is ensuring personal data is not retained beyond what is necessary for the defined purpose.

Lifecycle when using OpenAthens as a directory

Customers using OpenAthens as their account directory can have administrators create accounts or have them created directly by the user if a self-registration scheme is being used. When creating new accounts an activation process can be used to ensure the user's e-mail address is confirmed as valid. All accounts are created with an expiry date which determines the point at which an account can no longer be used unless renewed. Accounts in an expired state are deleted from OpenAthens a set period after the expiry date which can be configured by organization administrators.

Lifecycle for customer directories

When a customer is using their own account directory or is using their own authentication service, an OpenAthens account is created when the users first sign in. When the account expires in the source directory or authentication system, the user can no longer use their OpenAthens account. The account is deleted a set period after their last login date. This process ensures that OpenAthens remains in synch with the customer's account directory.

Contract termination

On termination of an OpenAthens subscription, the customer's access is revoked via a status change at the level of the customer domain. All customer administrators and user accounts within the domain are effectively suspended and a 6-month cooling off period is put in place. At the end of this period, all data is deleted from the OpenAthens database. Within 1 month of deletion, all data is also removed from back-ups and logs.

Password policy

Customers using OpenAthens as their account directory need to assign a username and password to each individual account. Length and complexity restrictions are enforced, and passwords are checked against a banned list to prevent use of common words or phrases. The nature of the service means that passwords do not expire. Requests to reset forgotten passwords result in a new activation link being sent to the accounts registered email address. Our current password policies can be viewed here: **https://docs.openathens.net/display/public/MD/About+usernames%2C+passwords+and+expiry+dates**.
*The minimum length will be increasing to 10 characters in Q2 2022.

Product development and releases

OpenAthens aims to minimize the security risks associated with development of its products and services. As part of this, product development is the responsibility of a dedicated, in-house development team. Where contract staff are used, they work within the OpenAthens team and follow its internal standards and processes.

The Teams work to Agile principles and processes to achieve regular releases of new features and resolution of issues. Development sprints are currently every two weeks.

Security is a major consideration when developing new features. The impact on security and privacy is assessed as part of the planning process for each individual piece of development work. When developing, team members

develop in line with a defined architectural pattern, and all code is subjected to peer review assisted with static code analysis tools to highlight security issues as well as code quality.

Testers are integrated into the team ensuring all individual features and bug fixes are tested as soon as development is complete. When features and bug fixes are combined into a release, the release is tested in a dedicated testing environment using a mix of automated and manual methods. Security tools are used as part of this testing phase to identify issues against the OWASP top 10 security vulnerabilities.

When a release is ready it is passed through a formal change control process to provide appropriate levels of authorization. All releases are communicated to customers via the OpenAthens status page (**https://status.openathens.net/**) with additional communications where there is a material impact on customers. Release notes are published in the OpenAthens documentation site to detail new features and issues resolution.

Post-release, applications are carefully monitored for any unexpected changes in behavior. This enables a rapid response to any issues.

Operational security

The day-to-day operation of OpenAthens is the responsibility of a dedicated in-house team supported by Jisc's extensive operational policies and procedures. Using the Google Cloud Platform, Google focusses considerable resource and expertise in maintaining and securing the underlying infrastructure. This enables the OpenAthens operations team to focus its efforts on managing the service itself.

OpenAthens is continuously monitored 24/7 for service availability using both uptime and transaction-based checking. In addition to the protection provided by GCP, the OpenAthens team monitors for suspicious activity or unexpected patterns of traffic using manual and automated methods.

Patching

To ensure the infrastructure is up to date with the most secure versions available all core applications are patched on a monthly cycle. The exception to this rule is if a security vulnerability is discovered that dictates an immediate response, in this scenario emergency patching is carried out as soon as is practical. Much of OpenAthens runs in a container-based architecture where a restart automatically triggers an update to the latest available image. This enables rapid response to situations requiring immediate patching.

High availability

All applications and data are distributed across multiple nodes and the nodes are distributed across multiple availability zones within Googles cloud platform to ensure high availability of the service. The use of a container-based architecture further helps to ensure high availability of the service. For example, applications automatically restart if they encounter issues and if a specific node fails it is removed from service and traffic is directed to the remaining 'healthy' nodes. Where appropriate, nodes are set to automatically scale to handle unexpected spikes in traffic.

Regular service management meetings review the performance and future capacity needs of the service. The infrastructure enables horizontal and vertical scaling to be implemented with significantly reduced lead times compared to a physical infrastructure.

OpenAthens continuously monitors its service availability against a service level agreement (SLA) of 99.95% for core services. For more details see the OpenAthens SLA document.

Penetration testing

OpenAthens undergoes penetration testing at least annually. Testing is carried out by an independent third party and any vulnerabilities found are added to the development backlog and addressed according to their severity classification. The service then undergoes a retest to check vulnerabilities have been cleared. Major

product releases or releases introducing significant new functionality may be additionally penetration tested prior to release.

Incident management

OpenAthens has a dedicated service desk that handles all incoming incidents. Out of hours, a dedicated on-call team is on hand to cover service incidents, so there is cover 24 hours a day and 7 days a week, 365 days a year. All incoming incidents are classified and assessed for impact and escalated accordingly. When a major incident occurs, an Incident Manager is assigned and takes responsibility for managing the incident through to resolution. All major incidents are followed up with a full report that details the incident, follow up actions, and an action plan. Service impacting incidents are communicated to customers via the OpenAthens status page.

Any incident related to information security or data privacy is additionally reported to the Jisc Information Security Team. The Information Security Team provides support and operates additional specific processes required for management of security incidents including communications with external agencies where required.

Relevant documentation

OpenAthens Service Level Agreement - Available on request from your point of contact if not already provided.

Google Security White Paper

****End of Document****