



Service Definition Document

Avco SystemsAuthinity

Contents

Service Overview	3
Executive Summary	3
Service Overview	4
Security	5
System Requirements	6
High Level Operation	6
Features	6
Quality and Information Security Management System	9
Additional Service Options	10
Data Backup and Disaster Recovery	10
Business Continuity	10
Data Restoration	11
Onboarding and Offboarding Process	11
Onboarding.....	11
Offboarding	11
Data Migration.....	11
Service Levels and Constraints	12
Availability	12
Scheduled Maintenance	12
Severity Levels	12
Commercial	14
Ordering and Invoicing Process	14
Termination Terms.....	14

Service Overview

Executive Summary

Authinity is a modern identity management solution to aid organisations with complex compliance requirements. It achieves this by enabling organisations to become their own identity provider, so that their end users can sign in with their company and not rely on third-party providers, such as Google or Facebook. As an identity provider, Authinity allows you to define the policies around sign-ins and signups in a manner that is compliant with your own policies. By connecting your services to Authinity, they can immediately inherit the policies you have defined, ensuring that they too, are compliant. With just a single policy to maintain, Authinity greatly reduces sign-off time and ensures that all your applications are kept up to date with best practices and are always in line with your current policies. IT costs are also reduced, as there is no longer a need to store and secure your users' information, nor is there a need to pay for the development of individual login portals, as this is all provided.

Policy customisation lets you define how you need your users to sign up and sign in to your applications. For sign-ups, you are free to setup an invite-only system, only allow sign-ups from specified domains or allow users to 'self' sign up from any domain. Sign-in policy customisation gives you further control, letting you specify the rules around credential creation and management.

Authinity allows organisations to set custom branding for your landing page and automated communications, giving your users a consistent experience. Your organisation's logo will be included across the user interface and heading up all email communications initiated by the user.

Authinity has been implemented to be as simple as possible, letting organisations create their custom provider in seconds. Integrating with your newly made provider is just as simple and meets the OpenID Connect specification to enable your applications to integrate with your provider in a manner that is brief and well documented.

The Authinity service was designed and developed using a security first principle that implements a defence-in-depth architecture and follows our strict standards for quality and security.

Authinity is available immediately and we provide UK-based support for any of your enquiries.

Features	Benefits
✓ User management and support suite	✓ Reduce cost to user support with self-service features
✓ Single sign-on identity provider	✓ Reduce development cost with secure login for all your services
✓ Self-service password resets	✓ High availability
✓ Password blacklist	✓ Configure your authentication and sign-up policies easily
✓ Multi-factor authentication	✓ Always be in-line with current best practice guidelines
✓ Brute force protection	✓ UK-based support on hand
✓ OpenID connect integration	✓ No installations necessary
✓ Authentication and sign-in policy customisation	✓ Confidence that your users' data is always protected
✓ Accessible with any modern device or browser	✓ Never worry about improper encryption or hashing implementations again
✓ User interface branding customisation	✓ Regular security updates included

Service Overview

Each organisation has their own compliance and policy requirements when introducing new services, leading to added IT costs, as a bespoke solution is frequently required to meet those requirements. This cost is compounded by the need for many services and changes to policy and best practice recommendations. Enter Authnity, a cloud service designed to lift that burden from organisations with easy-to-use customisation options to quickly meet your organisation's requirements and establish your organisation as a secure identity provider to your users.

Past service models required each service to design, create and maintain their own authentication gateways, as well as shoulder the burden of keeping users' information secured. Identity providers solve this problem by offering a single vault to protect your user information and a single authentication gateway to maintain it, providing a seamless user experience when authenticating across many services. With Authnity,

we enable organisations to quickly become identity providers and to connect their users with the services they wish to offer them, freeing up your service providers to focus on providing the best service for your users.

Providing many services to your users brings with it the challenges of meeting the required sign off and compliance for each login portal or other authentication gateway. Moving this to a single solution significantly reduces this effort. With Authinity, you only need specify your compliance and policy needs once to ensure that all your services are compliant with your requirements.

With a centralised vault to protect your users' information, GDPR compliance is made easier by enabling you to respond to subject access requests quickly and efficiently, and, with our security standards, you can be sure that your users' private information remains that way.

Security

Security comes first for Authinity. From design to implementation, security has been at the forefront of our concerns. We make regular use of automated scanning tools (Figure 1) as well as manual simulated attacks as part of our development process to ensure that Authinity remains secure.

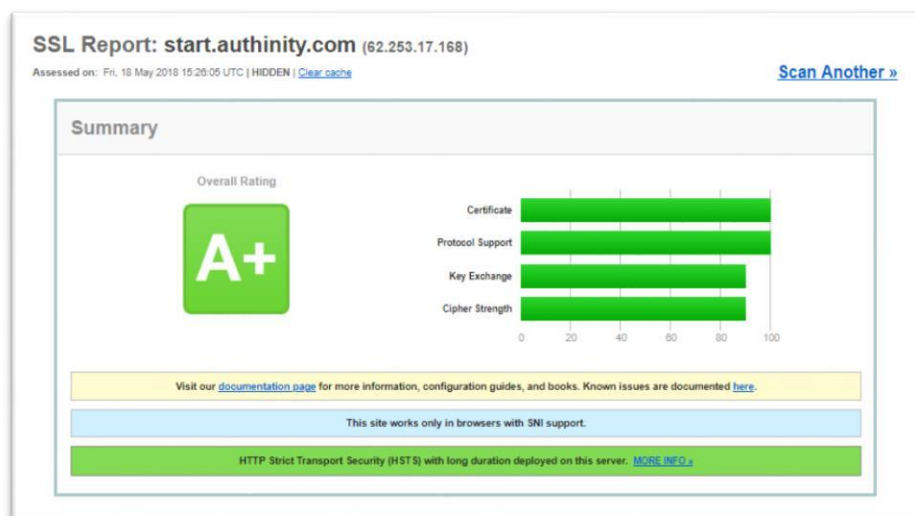


Figure 1 - Qualys SSL Labs scan results

Our key management policy employs a defence-in-depth approach to its implementation and follows the guidance of NIST and OWASP. The application secures data by use of a series of flexible Data Encryption Keys (DEKs). The DEKs are themselves encrypted by a much smaller number of Key Encryption Keys (KEKs), which are stored within a Hardware Security Module (HSM). The HSM performs the decryption routines, thereby eliminating the risk of the KEKs being exposed to the host machine. A single DEK is only ever used a

limited number of times to encrypt; these DEKs are regularly expired and the underlying data re-encrypted automatically.

System Requirements

Authinity is a modern, cloud-based service and therefore only requires a modern web browser to fully utilise the service.

High Level Operation

The first step is to establish your organisation as an identity provider so that your users can “Sign in with ‘Your Company’”. Our quick start will set this up for you in just a few clicks. Once you’ve entered your company name, you’ll be immediately redirected to your unique Authinity service (which we set up automatically) and ready to start configuring your policies. Once you’ve saved your policy settings, you’re ready to start adding the services that you wish to provide to your users. Again, we make this fast and intuitive to complete.

With your services added, they are now authorised to utilise Authinity as their sign-up and sign-in portals, which can be achieved by following the industry standard for integrating with an identity provider.

Once integrated, your service users will have the option to “Sign in with ‘Your Company’”, which will redirect them to your custom Authinity service, where they can sign up or sign in, before being redirected back to the service seamlessly.

Features

Authinity offers different features based on the assigned role for that user. For the majority of usecases, the user will be logging in, then being automatically redirected back to their service provider that initiated the log-in journey. But they are also given options to keep their account details up to date, manage their password and complete self-service operations to unlock their account or reset forgotten credentials. For an administrator, you are given additional permissions to manage your organisation settings and given access to tools that help you support your users.

Organisation Settings

Policies

By default, we set up your organisation to automatically follow best practice guidelines, but you can alter these settings to match your policy:

- **Password** - Here you can choose what rules to apply when users create their passwords. You can set a minimum length, the expiry, the complexity rules that must be met (e.g. at least one upper case, at least one digit, etc), and whether you’d like to prevent passwords contained in the blacklist of weak or breached passwords.

- **Sign up** - Define how you'd like your users to sign up. You can restrict sign-ups to specific domains or make it an invite-only system for more control.
- **Sign in** - If you'd like your users to pass an additional security challenge before logging in, you can do that here with a knowledge-based challenge (memorable word).

Branding and Customisation

Once your core policies are set up, you can go further with our user interface customisation options to personalise the user experience.

- **Logo** - Set your company's logo for all your users to see. Your logo is included on all user interface screens.
- **Landing background** - Customise the main landing page where your users will log in to bring them a user experience consistent with the rest of your services.
- **Secondary colours** - Select from a range of secondary colours and select the one that best suits your theme.

Self-Service Operations

All user accounts are given permission to perform self-service account operations, removing the support overhead of having dedicated personnel perform these operations:

Account Recovery

Users may lose access to their account for various reasons, be it a forgotten password or a lost device that holds their two-factor secret. Authinity provides means to automate the account recovery process:

- **Forgotten password** - A time-sensitive email is sent to the user on their request, containing a unique code to reset that account. Upon entering the correct code, the user may select a new password (that must pass the organisation's policy settings) and regain access to their account. If the organisation has enabled knowledge-based challenges (e.g. a memorable word), the user must also complete this challenge to reset.
- **Lost device** - For accounts that have two-factor enabled, Authinity generates one-time use codes that allow a user to input as if it were a one-time password that would otherwise be generated from their device.

Account Management

Users are free to update their account information and credentials at any time:

- **Two-factor** - Comes as standard and lets users connect an authenticator device (such as Google Authenticator).
- **Change password** - Users are challenged with their current password but are then free to update to a new password here (must be in line with your organisation's password policy).
- **Change memorable word** - Authenticated users can change their memorable word at any time and are challenged with their current password before doing so.

- **Profile** - Users are free to update their account information containing their name and address information.

Other Features

On top of the self-service and organisation settings, Authinity comes with:

Analytics

Authinity provides administrators with an up-to-date snapshot of user activity over the last 24 hours, giving them a quick view of usage metrics instantly:

- **Sign ins** - View the distribution of successful, failed, or abandoned logins over the last 24 hours.
- **Accounts** - An overview of all your users, how many are signed up, fully registered, or still pending.
- **Applications** - See the number of sign in redirects initiated by your connected services over the last 24 hours.

Built-in Logging / Auditing

Authinity has built-in functionality to capture user activity:

- **Logging** - We log all user interactions with the service so that enough information can be provided to see exactly who did what and when.
- **Auditing** - As a security measure, we make log files available on request.

Email

Emailing is an important part of the self-service features. That's why we include automated email services in our product at no additional cost:

- **Automated emails** - This includes password resets, sign-up invitations, account verification and notifications about account lock-outs.
- **Branded** - Your company logo is included as a branded header across all email communications.

Security Log

All users, upon logging in, will see a security log summary to help identify unauthorised accesses and access attempts:

- **Previously signed in at** - The date and time this account was last authenticated
- **Last failed sign in at** - The date and time a failed login happened for this user
- **Password last changed** - The date and time the user last changed their password

Account Notifications

We know that it can be frustrating to users who lock themselves out of their account. That's why we've added automated communication to users to assist them when this happens:

- **Account deactivated due to inactivity** - This automated email explains to a user that their account has been deactivated due to inactivity and the steps needed to resolve this issue, should they require it.
- **Lockout** - If an account is locked out due to too many failed login attempts, this email explains what has happened and the steps to resolve the issue.
- **Credentials updated** - This notification is triggered when credentials for an account are changed (e.g. the password) and serves as an alert that also provides steps on what to do if they did not make this change.
- **Already signed up** - Some users may forget that they have already signed up and attempt to reregister. For these users, we automatically notify them that they have already signed up and provide the steps necessary to regain access to their account, if required.

Quality and Information Security Management System

Quality is central to Avco Systems' philosophy and permeates all areas of the company's business, including its internal and external aspects and its dealings with interested parties. The company endeavours to satisfy or exceed expectations and is committed to a policy of continual improvement of its systems and working practices. In particular, it aims to ensure that its service quality satisfies the specific contractual obligations of its customers, together with the standards of quality in ISO 9001:2015, including the adherence to statutory and regulatory requirements.

Critical to the quality of the company's services is information security – protection of information from a wide range of threats to ensure business continuity, minimise business risk and maximise business opportunities and return on investment. Such security is essential in today's business environment because secure information sharing depends upon valuable assets in terms of data, equipment and personnel. The company is dedicated to safeguarding its information and that of its interested parties, to fulfil both its contractual obligations and the requirements of ISO 27001:2013.

The company has combined its quality and information security management systems in an Integrated Management System (IMS), which is subject to internal and external audits. The IMS aims to protect the company's reputation, the efficiency and effectiveness of its business operations, and the confidentiality, integrity and availability of all company and third-party information.

The framework for setting objectives and establishing an overall sense of direction and principles of action with regard to the IMS is provided by Management Review meetings at planned intervals. In addition, there is an ISMS Forum, which meets to initiate and co-ordinate the implementation of information security within the organisation.

The company has a strategy to mitigate information security risks as far as is practicable. This is supported by a formal methodology whereby risks are identified and either accepted according to documented criteria or reduced using control measures. Action taken will be adequate and proportionate to the

expected impact that the loss of confidentiality, integrity or availability may have on systems and their data.

The company is committed to staying up to date with information security best practices and will maintain contact with appropriate special interest groups for that purpose. All personnel share responsibility for the quality of the company's services and for information security.

Additional Service Options

Avco Systems has a strong reputation for providing high-quality, efficient and effective solutions for organisations for over 30 years. Avco Systems believes in building productive relationships with customers and can adapt to suit specific customer requirements. Please contact Avco Systems should additional services be required.

Data Backup and Disaster Recovery

Business Continuity

All services hosted in Avco Systems' infrastructure are subject to the company's certified ISO27001:2013 Business Continuity Plan and Business Continuity Process. The company verifies, reviews and evaluates the established and implemented information security continuity controls as part of regular disaster recovery and business continuity testing.

Backups will be performed to minimise data loss in the unlikely event of a disaster situation. Backups will be stored securely in Avco Systems' data centres.

Component	Frequency	Type	Retention
Database	Daily	Full	1 year

Avco Systems will coordinate with the customer to identify specific backup and disaster recovery requirements outside of the standard offering.

Data Restoration

Should a serious event occur, Avco Systems will liaise with the customer to authorise data restoration from backup media. Avco Systems will aim to restore data from the latest backups as swiftly as reasonably possible.

The restoration/migration of existing data from another provider can be requested separately at an additional cost, if required.

Onboarding and Offboarding Process

Onboarding

Avco Systems will provide a dedicated delivery and support team during the introductory stage of the service delivery. The friendly, UK-based support team will provide assistance during the initial configuration and installation of the service, as well as user documentation, if required. If applicable, onsite training can be supplied at an additional cost.

The customer will provide a dedicated contact during the onboarding process.

Offboarding

In the unlikely event that the customer does not wish to extend or renew the contract, Avco Systems will:

- Securely provide all customer data relevant to the service
- Decommission the existing service and ensure all customer data is securely destroyed

Data Migration

The migration of existing data from any other provider can be requested separately at an additional cost.

Service Levels and Constraints

Availability

The service has an Availability Target of 99.9% annually. This excludes scheduled maintenance activities, for which the customer will be notified in advanced, as described below. Customers can contact the dedicated, UK-based support staff by telephone and email from Monday to Friday, 08:30 – 18:00 (excluding public and bank holidays).

Scheduled Maintenance

Unless previously agreed with the customer, Avco Systems will perform service affecting maintenance operations outside of normal business hours (Monday to Friday, 08:30 – 18:00). Avco Systems will endeavour to:

- Provide customers with as much notice as reasonably possible ahead of any scheduled maintenance
- Minimise the length of maintenance windows and subsequent disruption to the customer

The customer will be responsible for notifying end users.

Severity Levels

The severity of any problem will be mutually agreed between Avco Systems and the customer according to these guidelines. All service levels defined apply during the standard working hours of Monday to Friday 08:30 – 18:00 (excluding public and bank holidays).

Priority/Severity	Severity Level Definition
Critical	A problem that must be resolved before the customer can continue normal business operations. Avco Systems support staff will use reasonable endeavours to respond to the customer with a workaround within two hours of receiving notice of a critical problem being reported. Avco Systems staff will work continuously on critical problems until the fault is permanently cleared or the system is operational.

Serious	A problem that significantly inhibits production but does not prevent operations. Avco Systems support staff will use best endeavours to respond to the customer with a workaround within four hours of receiving notice of a serious problem being reported.
Moderate	Requirements that do not impede productive use of the software. Avco Systems support staff will use best endeavours to respond to the customer with a workaround within seventy-two hours of a moderate problem being reported.
Minor	Cosmetic production problems and general test system problems that do not affect availability of the production system. This severity level will also be used to categorise general technical help desk calls. Avco Systems support staff will respond to the customer within one week of a minor problem being reported.

The resolution of problems, irrespective of their classification, will use the fastest and most effective means, including telephone support and software patches.

The support team will gather and record as much information as possible concerning the request and, if necessary, work with the development team to resolve the issue. The fault will be tracked and progressed until closure, with the team keeping the customer updated each step of the way.

Commercial

Ordering and Invoicing Process

Avco Systems will begin to deliver the service defined in this document upon receipt of:

- The completed G-Cloud framework 'call-off' contract and terms and conditions acceptance
- A purchase order from the customer

The customer will be invoiced for the charges monthly in arrears.

Termination Terms

Either party may terminate the service by giving the other at least 30 days written notice, terminating at the end of a month. The minimum contract period is twelve months.