TEXUNA

IDENTITY AND ACCESS MANAGEMENT SERVICE (IAMS)

tender@texunatech.com / +44 (0) 203 393 4670 / www.texuna.com

TEXUNA

IDENTITY AND ACCESS MANAGEMENT SERVICE (IAMS)

Identity Provider (IdP) with Role-Based Access Control (RBAC) Lifecycle for enterprise authentication and authorisation.

Secure API-driven access to any application with centralised IAM policies. Integrate identity information across user journey lifecycle for joiners, movers and leavers.

OAuth and SAML-based Single Sign-On for behaviour tracking and attribute exchange between integrated systems.

Features

- Manage Identity Lifecycle Accounts and Credentials for joiners, movers, leavers.
- Application Access Management via central or remote permissions and groups.
- Dramatically cut helpdesk password reset support costs via Fido2.0 devices.
- Federation and social sign-on via SAML, JWT, OAuth2.0, OpenID Connect.
- Active Directory, OpenLDAP, ReSTful web services integration, secured via HTTPS/TLS/SHA2/AES256.
- Monitor privileged users, event statistics, behaviour and intrusion patterns.
- EAV extensible data model supporting Shibboleth SAML2 attribute exchange hub.
- Multi-Factor and biometric Authentication (2FA, TOTP, U2F, UAF, CTAP, WebAuthn).
- Account Administration Delegation, plus manage permissions / user groups centrally.
- Strong password policy configuration and enforcement (Salt and Hash) .

Benefits

- Enforce directory services, user management processes and security policy.
- Enhanced User Experience - single approach to access credentials.
- Self-Sovereign asynchronous cryptography (U2F PKI authentication and digital signature).
- Centralise GDPR compliance, secure storage of personal data with audit-trail.
- High Performance and High Availability via cluster or elastic service
- User self-service features and customisable user journey with homepage personalisation.

Registered Office: Texuna Technologies Ltd, 9 Disraeli Road, Putney, UK, SW15 2DR. Company №: 04003804
Contact: tender@texunatech.com / +44 (0) 203 393 4670 / www.texuna.com

- Devolved access control to simplify management of a huge user base.
- Open source software implementation with optional blockchain audit trail.
- Data encryption at rest gives data protection and privacy guarantees.
- Ability to independently assure individual identities through auxiliary KYC services.

Detailed service definition

Texuna Identity Assurance and Access Management (IAM) is an enterprise-class Identity Management (IdM) solution supporting mission-critical authentication and authorisation services for private and public cloud applications. Texuna Identity Assurance and Access Management also enables organisations to quickly and easily implement a secure Single Sign-On (SSO) experience for employees, customers, partners and contacts.

Texuna's IAM can be deployed on in-house, third-party or Texuna-provided hosting services. In all cases, web-based access to the administration component is provided, enabling the import of data (e.g. users and organisations), the connection of existing public or private cloud-based applications and the management of user access. Texuna IAM is effectively an electronic Identity as a Service (eIDaaS) that you can use to integrate and consolidate your in-house and cloud application presence for stakeholders and customers alike.

Built using open source technologies, IAM has been packaged by Texuna into a secure, robust and scalable (clustered) enterprise-level application, using industry standard protocols and open standards such as SAML via Shibboleth, OpenLDAP, Active Directory and OAuth. Texuna's IAM is a cloud agnostic service, operable within a public, private or hybrid cloud environment that can scale to tens of millions of users. It is also extensible with the ability to meet bespoke data capture requirements and accept custom RESTful integration services. It can therefore act as a secure message integration hub between integrated systems.

Operational Benefits of deploying IAM

- Increased security:
    - Secure user management policy and processes;
    - Automated password/account expiry;
    - Enforced password strength, with added Salt and Hash (SHA2) stored as shared secret on server side;
    - Apply multifactor authentication, with support for PKI asynchronous cryptography.
- Enhanced user experience:
    - Single set of credentials to access all connected systems;

  - Centralised user registration;
  - Ability to support Fido Alliance Universal 2nd Factor (U2F) devices to reduce reliance on shared secrets / passwords.
- Increased time efficiency for service desk and end users:
  - SSO reduces password amnesia;
  - Self-service and delegation features;
  - Devolved access control;
  - U2F has been demonstrated to significantly reduce helpdesk support requirements as it requires less password resets, and it doesn't involve the same complexity as TOTP devices that need batteries and network clock synchronisation.

- Centralised user and access management:
  - Reduced user management and administration costs;
  - Complete control over access management solution and policies.
- Practical and adaptable solution:
  - Ability to integrate seamlessly with compliant applications that support SAML, LDAP, OAuth2.0, and OpenID protocols;
  - Runs out of the box;
  - Open source implementation, avoiding expense of bespoke IdM systems;
  - Confidence in a tried-and-tested secure solution using open standards.

Core Features

- Account management:
  - Single Sign-On;
  - Account self-service;
  - Workflows:
    - Account activation;
    - Forgotten username/password;
    - Password reset.
  - Account administration delegation;

  - Single authoritative source of user information;
  - Registration and sign-in with social media accounts via OpenID Connect.
- Application management:
  - Self-service application integration – connect SAML-compliant systems;
  - Application access control via group management.
- Maintenance tools:
  - User/organisation import and export scripts;
  - Bulk user/organisation update scripts;
  - Searchable logs of SAML requests and audit events;
  - Ability to schedule automated tasks.
- Security features:
  - Strong password policy – customisable to your requirement;
  - Password salting and hashing algorithms;
  - Activity-based account locking/archiving;
  - Multi-factor authentication support;
  - Independently conducted penetration testing;
  - Option to push audit trail link to a distributed ledger blockchain.

Access Management

Texuna's IAM approach to application access management is to centralise permissions in a single location, ensuring ease of use for application support and IT service desk staff.

Texuna's IAM allows the creation of groups governing access to applications. Users are associated with groups via highly flexible administrator-defined rules that grant application access based on the attributes of the user and/or their associated organisation. Furthermore, IAM allows the creation of sub-groups for each application, replicating an application's granular permission structure and thereby enabling the control of both access and authorisation from a single location.

Texuna's IAM also supports a hierarchy of user types, facilitating the inheritance of permission and control over access management. This allows the delegation of permission and access management to appropriately authorised users.

Single Sign On and Open Standards

SAML2.0 is the most widely adopted existing SSO standard. It is a well-established, mainstream open standard. Many applications support SAML natively, including Google Apps, Dropbox and Office 365. Integration with social networks can be achieved via OAuth2.0 as defined by OpenID Connect. Support is also available for U2F / UFA with CTAP and WebAuthn. Other open standards in our service include; XML, HTTPS, Java Web Token, SOAP, AES256, SHA2, TLS2, etc.

Users log in with a single set of credentials for authentication and are automatically logged into all applications to which they have been granted access. Texuna's IAM user and group management interfaces give administrative users full control over application access management with granular level permissions.

Texuna also supports OpenLDAP integration to work with legacy web applications, and has an LDAP based integration with Microsoft Active Directory to allow identity management data synchronisation. This allows existing enterprise credentials only available within the internal Windows domain to be used for authentication across external web services. Other federated services such as Eduroam are also supported.

Using IAM eliminates the need to have specialist open-source technicians or authentication security experts on site, yet avoids the expense of bespoke IdM systems. Once installed, application developers, suppliers and SaaS partners have the option to use the SAML2 or OAuth2.0 web standards to authenticate users into your applications and services using Texuna's IAM. Shibboleth is the world's leading open source SAML implementation for authentication and authorisation.

Fully Managed Software Service

Texuna's IAM is a cloud agnostic service: it can be deployed within a private cloud, made available via a secure network in a public cloud, or deployed in a hybrid of the two. The default service is based on Texuna's AWS private network. Texuna's IAM is based around a core User Directory Manager (UDiMan) which sits within Texuna's Virtual Private Network on the AWS public cloud (SaaS version - see diagram). It is available for immediate delivery and use.

The platform can be deployed on any public or private cloud or on in-house infrastructure. Texuna will provide a temporary online link with the self-installing IAM with comprehensive guidance. Self-installing RPM packages are provided for this purpose.

Each RPM package is bundled with its own operating system (a minimal install of the CentOS Linux platform). This makes it quick and easy to deploy and maintain multiple IAM servers as virtual machines on the host server. The system will automatically find parallel installations to create a high availability, load-balanced, scalable cluster. Each RPM package includes the application server and a database server, and can be configured to be one, the other or both.

This means customers only need to provision a physical or virtual machine for IAM to run out of the box, removing all infrastructure environment (OS, web-servers etc.) setup and configuration effort. After

installation is complete an administrative account allows the customer to undertake user and integration configuration via an intuitive user interface. Guidance is provided for the initial configuration process, application integration, user import, and launch.

Recommended Infrastructure

Typical installations will include two IAM environments: one for testing and development, and one for live production. This setup not only provides greater access to pre-production Identity Assurance and Access Management features for customer testing but also facilitates integration testing between IAM and connected applications

Application Integration

Identity Assurance and Access Management allows administrators to configure the integration of new applications directly from the user interface. Applications must be SAML-compliant, and can be integrated in three simple steps:

- Add the new application to Identity Assurance and Access Management, and configure SAML settings.
- Add any groups required to define the permission structure required for the application.
- Assign users to those groups.

Following these steps, the appropriate users are able to access the new application.

Scalability, Availability and Resilience

Regardless of the size of the user base, Identity Assurance and Access Management is a highly scalable solution capable of meeting authentication needs. It is designed to accommodate rapid upscaling, primarily achieved by increasing the number of machines used in the installation.

Identity Assurance and Access Management can be deployed using a clustered approach, ensuring high availability and reliability of the application. If your user base will not access Identity Assurance and Access Management frequently, or if the availability of the system is not a priority, Texuna offers a single machine option.

A clustered approach is recommended within high load environments for the following reasons:

- Capacity:
    - The more machines running Identity Assurance and Access Management, the more simultaneous users it can support with low latency.

  - Scalability of data exchange will be limited with a single machine configuration.
- Maintenance of performance under load:
  - Spikes in user authentication activity can cause drops in performance.
  - Clustered systems are able to balance the load across multiple machines.
- Resilience:
  - Identity Assurance and Access Management is built from several core components. Clustering duplicates components over multiple machines.
  - A hardware failure on one machine does not impact service availability, since other machines automatically assume its responsibilities.
- Availability:
  - High availability is expected of organisations' core services.
  - A clustered system is more likely to be accessible and operable.
  - The SaaS cluster has 99.9% uptime guaranteed by service-level agreement. versus 99% for a comparable non-clustered package. In practice Identity Assurance and Access Management has achieved greater than 99.999% uptime.

A single-machine installation does not preclude opportunities to upgrade to a clustered approach at a later date as the service can be purchased on a per server basis.

General Terms

Information Assurance and ISO 27001

Texuna have a strong focus on high quality delivery and implement rigorous Quality Assurance processes and procedures:

- ISO 9001 certified with BSI as external auditors.
- Cyber Essentials and IASME Cyber Assurance Level 1 compliant.
- ISO 27001 certified with BSI as external auditors.
- We are a registered data controller with the Information Commissioners Office and have GDPR compliance in our approach to solutions, data management and deliveries.
- We adhere to ITIL and ISO 20000 standards for first, second and third level helpdesk support.
- We are an Amazon Web Services (AWS) cloud hosting certified partner.

Government Classification Scheme (GCS)

Texuna solutions are in use for 'official' level data systems. We ensure that your personal and sensitive data items are identified, encrypted and shown only to those users who have a need to see them. All sensitive and personal data is protected by stringent access control mechanisms. Data in transit and at rest is also encrypted as are all data backup files.

Comprehensive support of good data governance will often underpin data migration as well as best practice data warehouse management. We have a strong track record in migrating legacy systems to create a unified datastore while improving the quality and integrity of the data held (as well as in reducing duplication). This can also be done during data migration.

- Texuna can deliver a metadata rich data warehouse which incorporates best practice design, so that management and maintenance is cost effective and efficient.
- Texuna will ensure that client data, and especially any personal and sensitive data is:
    - Protected by encryption in transit and at rest;
    - Protected by stringent access control;
    - Guarded from improper use through sophisticated access and authentication controls;
    - Tracked using a comprehensive audit trail that can be reported on.

Backup and Maintenance

The Fully Managed Service includes support for backups, maintenance, monitoring, disaster recovery and upgrades. Hosting is always provided in zones physically located in the U.K. and/or EEA so that your data is fully protected. Texuna offers Business Continuity and Disaster Recovery options upon request.

Detailed maintenance guidance is provided for internal / in-house hosted implementations, including all disaster recovery instructions and scripts necessary to restore the application in case of failure. In addition, Texuna provides information on backups and monitoring that can be implemented using existing infrastructure, along with step-by-step guides to install upgrades.

Invoicing

Charges are invoiced monthly in advance. Payment terms are 30 days with a purchase order or immediate via credit card.

Contract Term

Minimum contract term is 1 year.

On-Boarding

The on-boarding steps are as follows:

- Contact Texuna with a draft order form, or submit online request;
- If required, a dialogue is opened to discuss the options most suited to your requirement;
- When options are agreed, the order form is finalised and formally accepted by both parties;
- Within agreed timelines, technical information related to install PaaS will be provided to Texuna;
- For SaaS the live environments and credentials will be sent to the Customer;
- For PaaS, Texuna provides time-limited administration account credentials, ready for user configuration.

Off-Boarding

On deciding to end a subscription, the off-boarding steps are as follows:

- Provide notice of termination at least 30 days;
- All relevant data is extracted in .csv format and sent to the customer via secure file transfer service. On confirmation of receipt, data is purged and destroyed from servers;
- For PaaS: Texuna provides a data export script. Customer confirms removal of the Texuna application from all relevant machines. Process must be completed within 30 days of contract expiry. PaaS administrator credentials will be automatically locked after this period.

Time to Provision/Deprovision

Dependent on customer requirements and options selected, time to provision is from 12 hours of order form acceptance. Time to de-provision can be from 24 hours of expiry of contract.

Service Constraints

Texuna applications may be subject to routine maintenance and this will be agreed in advance with our client so that disruption is minimised. Routine maintenance is never scheduled during the normal working day and does not typically result in noticeable downtime.

Customisation can be achieved via our Cloud Support services. No features will be deprecated without advance agreement with the customer. New features may become available from time to time.

Service Level Agreements

All user account information is encrypted to prevent unauthorised use. The SLA guarantees a monthly uptime percentage of at least 99.9% for SaaS. Different support level options are available as per the detailed pricing schedule. Severity level definitions and response times as well as financial recompense are only available under an enterprise support package.

Texuna Technologies Ltd,
9 Disraeli Road, London,
UK, SW15 2DR.
Company No.: 04003804

+44 (0) 203 393 4670

tender@texunatech.com

www.texuna.com

THANK YOU