OpenIAM

About the OpenIAM Solution

OpenIAM is a fully integrated platform consisting of Identity Governance, Web Access Single Sign-On and Multi-Factor Authentication (MFA). Our solution is currently in production at enterprises in a variety of industries such as financial services, healthcare, energy & natural resources and construction.

Our platform has been developed leveraging a singular unified architecture. Regardless of the number of OpenIAM products deployed, customers see & manage a single, central identity solution and not a patchwork of disparate components that are glued together.

Enabling this functionality is a modern architecture that leverages containers, Elasticsearch, distributed caching and a responsive & user-friendly UI. For customers, this translates into low total cost of ownership and a platform that adapts to your ever-changing needs.

Identity Governance

Automates the task of managing identities

OpenIAM provides a comprehensive set of tools to enable automated provisioning and de-provisioning of users, resulting in zero day start and stops for both on-premise and cloud applications.

These controls are defined through policies which can leverage a combination of RBAC, attributes or rules. This can be further extended using workflow and delegation functionality.

Features

- User life cycle management
- Self-service portal
- Access request with workflow
- User access certification
- Password reset
- Audit and compliance
- Reports
- Workflow
- Rich integration API

Web Access Management

Allows you to take control of access to your systems

Comprehensive Single Sign-On (SSO) solution that includes identity federation using SAML 2, oAuth2 and OpenID Connect. OpenIAM also includes a reverse proxy to enable SSO to legacy applications that do not support a modern federation standard. Scalable to support millions of users.

Features

- Authentication
- SSO and federation
- Reverse proxy
- Session management
- Authorization (RBAC)
- Rich integration API

Strong Authentication

Intelligent authentication option that extends the core framework to include:

- Adaptive authentication plus risk-based authentication
- One-Time Password (OTP) via SMS
- OTP via mobile app for iOS and Android

www.openiam.com
sales@openiam.com
+1-858-935-7561

Self-Service Portal

Common end-user interface shared across the OpenIAM solution suite; accessible to both internal and external users based on the organizational requirements. Provides end-user with a centralized console for SSO, access request, profile management and many more features.

Self-Service Password Reset

Configurable options in Self-Service that end-users can use to reset their passwords securely – significantly reducing helpdesk and operational costs:

- Challenge response questions
- One-time link via email
- One-time token via SMS

Access Request

Workflow-driven access request solution allowing authorized users to create requests from:

- Service catalog
- Access profile
- Existing user profiles

Users can select multiple items in the same request by adding them to a “shopping cart”. Once a request is submitted, each component is forwarded to an appropriate approver. Requests can be delegated either manually or through automated rules. Once appropriate approvals are in place, the access right is granted or revoked.

Audit and Compliance

Account discovery and reconciliation
Automated tools to detect and repair accounts in managed systems based on policies. Helps eliminate dormant and orphaned accounts.

Access Certification
Access certification tools to streamline the review and approval processes to effectively manage risk on an ongoing basis.

Reporting (GDPR and CFR)
Out-of-the-box reports to monitor the IAM solution as well as aid with regulatory mandates such as GDPR and CFR.

Flexible Multi-Factor Authentication

Policy-driven authentication solution includes:

- Password-based authentication
- Option to select the identity store (such as RDBMS or LDAP)
- Certificate-based authentication
- Social authentication
- SMS-based OTP
- Mobile OTP

Authentication options are combined with step-up authentication. Future versions will include risk/adaptive authentication.

Role-Based Access Control

RBAC model that can be used by applications, reverse proxy, API security and more. New object types can be dynamically introduced into the RBAC model.

Mobile Security

Use of industry standards such as oAuth in mobile, cloud and social networks to access resources securely. Fully audited to ensure traceability and compliance. Authentication options are combined with step-up authentication. Future versions will include risk/adaptive authentication.

REST and SOAP API

All operations available on the user interface can be implemented via the API which is offered as both SOAP and REST.

OpenIAM

www.openiam.com
sales@openiam.com
+1-858-935-7561