ORSUS
ACCESS MANAGER

ORSUS ACCESS MANAGER

Experience One Login to Multiple Apps with OAM

Due to the rise of numerous target applications each of which requires its own authentication mechanism; the passwords must be remembered, leading to a good number of identities and passwords to remember, leading to a point of concern for end-users and IT Staff. As digital transformation continues to reshape organizations and evolve businesses around the globe, secure application access from anywhere, any device, and any time is imperative.

ORSUS Access Manager (OAM) is a secure platform as a solution to enable one time sign-in across multiple applications. OAM provides secure authentication services to applications and single sign-on capabilities based on renowned standards such as SAML 2.0, OpenID Connect and OAuth 2.0. Applications can authenticate with OAM using these protocols with minimal configuration.

OAM aids users with a single pane of glass to access all their authorized applications without having to re-authenticate and perform self-service operations. It supports Kerberos and Adaptive authentication based of network, device, and location along with 2FA services via Email, SMS, Voice & Google Authenticator.

“ Experience One Login to Multiple Apps with OAM

OAM FUNCTIONS

- A single interface to access all authorized applications integrated with the OAM solution for productivity and ease of use
- User federation by connecting & integrating with existing enterprise user registries seamlessly
- Act as a standalone SAML/OpenID Connect Identity Provider along with advanced features such as Identity brokering & Social login
- Clustering for scalability & high availability
- Multi tenancy support
- Easy to use Administration interface to manage realms & resources
- Can be deployed as a web application running on bare metal with OpenJDK or even as a Container image on Docker or Kubernetes
- Multi-factor authentication via SMS, Voice, Email & Google Authenticator
- Kerberos authentication
- Risk based/ Adaptive authentication for Device detection, Location detection & Network detection

OAM **Features**

Admin console

Centrally manage all aspects of the OAM server, configure single sign-on, identity brokering, user federation and social login. Create and manage applications and define fine-grained authorization policies across users, groups, permissions, and sessions.

Databas

OAM Server database stores all realm users, groups, policies, permissions, etc. As OAM supports federation, replicating user information in the OAM database is optional.

User console

A single interface to access all authorized applications integrated with the OAM solution and a portal to perform self-service operations.

Ingress controller

Leveraged for traffic routing between the Admin & User console running as pods within the Kubernetes cluster.

OAM ARCHITECTURE