Oracle Access Management 12.2.1.4.0

Modernized and Open Standard Based Platform

Oracle Access Management (OAM) 12c is part of the Oracle Fusion Middleware Identity and Access Management Suite 12c that includes Oracle Access Manager, microservices – Oracle Advanced Authentication (OAA) and Oracle RADIUS Agent (ORA), and extended support of legacy software Enterprise Single Sign On (ESSO). Collectively, these solutions can provide innovative, fully integrated services that complement traditional access management capabilities by extending security from on-premises to cloud in a scalable format. Adoption of open standards such as SAML, OAuth, OpenID Connect, and FIDO2 allows adaptive authentication, risk analysis, multifactor authentication (MFA) methods, federated single sign-on (SSO), and fine-grained authorization extended to mobile and cloud applications. The release of the OAM container image can simplify the upgrade experience, accelerate the move to cloud, and automate the deployment experience with high availability and disaster recovery on-premises or in the cloud.

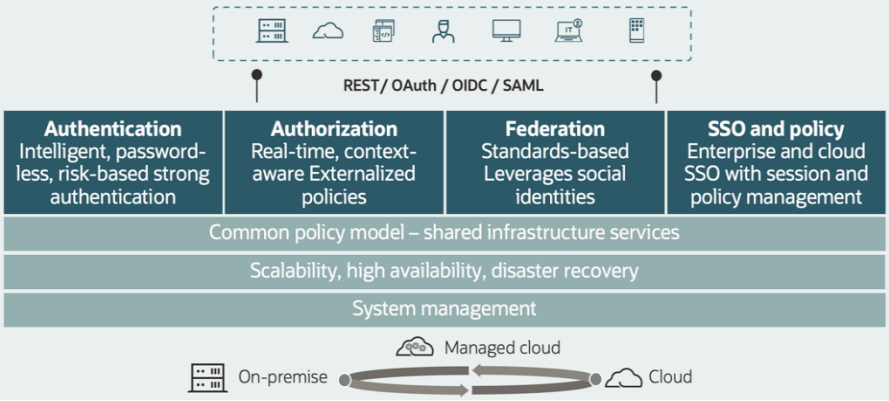

Figure 1. Oracle Access Management Deployment Options and Core Components

Core Functionalities

Oracle Access Management 12c provides the following functionalities, licensed and enabled as required:

- **Access Management Core Services**: Authentication, web SSO, coarse-grained authorization for enterprise applications deployed on-premises or in the cloud.
- **Identity Federation**: Cross-Internet-domain authentication and delegated authorization supporting industry standards such as SAML, OAuth, and OpenID Connect. Social logon using social network identities is supported.
- **Adaptive Access and Risk Analysis**: Using multifactor authentication and the heuristic fraud detection service, the Oracle Mobile Authenticator (OMA) provides soft-token TOTP solutions with one-touch notification services as well as passwordless access with OMA push notifications.

Key Features

Cores Services

- Multiple authentication schemes
- Web single sign-on (SSO) and Identity Federation
- Session management life cycle
- Coarse-grained authorization

Intelligent Access Management

- Context-aware (device context, geo-location, session context, transaction context)
- Content-aware (leveraging content classification)
- Risk-aware (real-time risk assessment based on context and policies)
- Context, content, and risk driven, dynamic, step-up authentication and fine-grained authorization

Adaptive Access

- MFA with FIDO2, YubiKey, One-time Password (OTP), Time-based One-time Password (TOTP), SMS, Email, or Oracle Mobile Authenticator (OMA) (a soft token OTP mobile app)
- Device fingerprinting
- Predictive auto-learning
- Knowledge-based authentication (KBA)
- Out of band TOTP for password resets
- Passwordless access with OMA push notification
- QR code-based OMA App registration

Fraud Detection and Investigation

- Real-time and batch analysis (heuristic behavior analysis)

- **Oracle Mobile Authenticator (OMA):** Supports new enhanced enrollment process for adding your accounts to the OMA app. Organizations can use the App Protection feature to help protect the OMA app with a fingerprint identity sensor such as Touch ID for iOS and Fingerprint for Android. Windows 10 platform is now also supported.
- **Oracle Advanced Authentication (OAA):** Customers can enhance their MFA solution with support of FIDO2 and YubiKey modern passwordless factors. Customers can extend this protection by pairing it with the new microservice Oracle RADIUS Agent (ORA) to help customers protect Oracle databases, VPN, and SSH sessions with a modern MFA user experience.
- **OAuth2 Dynamic Client Registration**: Dynamic Client Registration provides a way for native mobile apps to dynamically register as clients with the OAM OAuth Server.
- **OAP over REST**: Oracle Access Protocol (OAP) over REST enables the use of HTTPS infrastructure to route and load balance requests. Changing the transport mechanism between WebGate and server can have a beneficial impact on reducing operational cost for hybrid deployments. This is especially significant when some components are on-premises and others have moved to cloud.
- **Password Management**: OAM supports multiple password policies, enabling varied levels of password-based complexity protection for users belonging to different groups. The reset and forgot password capability can be supported with second factor authentication methods and Out-of-band TOTP.
- **OAM Snapshot Tool**: The OAM Snapshot tool helps administrators manage, migrate, and update OAM deployments. This tool enables management of OAM deployments across various infrastructures in a uniform manner, utilizing Oracle Database backup and cloning solutions.
- **Multi Data Center Lifecycle Simplification**: OAM simplifies the process of setting up and administering multi data center (MDC) topologies without using test to production tooling. New REST based APIs introduced for administrative and diagnostic purposes can significantly reduce the number of configuration steps performed in the MDC environment. OAuth Artifacts (such as Identity Domains, Clients, Resources, etc.) created in one data center are visible and seamlessly synchronized across other data centers.
- **OAuth Consent Management**: Consent Management can be enabled for each of the OAuth Identity Domains or all the OAuth Identity Domains in OAM. All OAuth tokens issued to a client can be revoked on demand by an administrator, in scenarios such as a user no longer using the relevant client application or the device is lost or stolen.
- **OAuth Just-In-Time (JIT) Provisioning**: JIT user provisioning enables a user identity to be provisioned dynamically when the user tries to login for the first time using any social identity providers. User account creation is done directly, without the need to provision users in the system, in advance.

- Universal risk snapshot

Standard-based Integration

- Support for SAML 2.0, OAuth 2.0, OpenID Connect, and FIDO2
- Integration with Oracle Cloud Infrastructure Identity and Access Management (OCI IAM)

Password Management

- User group specific password policies groups
- OTP based Forget Password and Out of band TOTP for password resets
- Admin driven forced password change

MDC Lifecycle Simplification

- MDC Admin REST APIs
- Support OAuth in Multi Data Center environment

Enhanced OAuth2 Supports

- OAuth consent management
- OAuth Just-in-time (JIT) provisioning
- OAuth dynamic client registration
- OAuth refresh token revocation

Simplified Installation, Configuration and Upgrade

- Production ready OAM container image with Kubernetes and OAM container Image in Oracle Cloud Infrastructure (OCI) marketplace for quick evaluation
- OAM SnapShot Tool
- OAP over REST
- Bootstrapping framework
- Stateless mid-tier with DB state persistence

- **OAM Stateless Mid-tier:** Database state persistence with stateless mid-tier can simplify the upgrade and cloud migration process. It enables new use cases including linking of sessions across web, API and device access and consolidated state across SSO, federation, and OAuth.
- **TLS1.3 and SHA2**: OAM 12c supports TLS1.3, , and IPV6 protocols and addresses FIPS 140-2 compliance requirements. All the simple mode certificates that are generated out-of-the-box for WebGate SSL communication are upgraded to SHA2.
- **Enterprise Single Sign-On (ESSO) release**: ESSO eliminates the need for users to remember and manage passwords for virtually any application. ESSO 11.1.2.4.0 is the latest release available for customers to deploy or upgrade to.
- **Standards Based Integration**: Adoption of open standards such as OAuth, OpenID Connect, SAML, and FIDO2 allows for heterogeneous environment coexistence. REST APIs are extended in 12c for federation management, multi data center, OAuth, password management, multifactor authentication, OTP, password policy, and session management.
- **New and Enhanced WebGates:** The 12c version of WebGates released for Apache HTTP Server and Internet Information Services web servers.
- **OAM Container Image:** Using the OAM Container Image, OAM can be deployed on-premises and in the cloud with Kubernetes container orchestration, allowing deployment and upgrade automation, auto-scale, and portability to multi cloud and on-premises environments.
- **Simplified Install and Upgrade Experience**: The installation footprint and time investment have been significantly reduced with fewer steps and less time using the bootstrap framework and configuration auto-discovery. OAM deployments can now be patched with the Stack Patch Bundle, which includes the bundle patches for each of the select identity management products and the patches for their respective underlying components.
- **Performance Improvements**: Session management has been enhanced using significant Database Optimizations in OAM 12c.
- **Integration with OCI Identity and Access Management:** OAM supports SSO between apps protected by OCI IAM and OAM using Federation.

To find out more information about OAM 12.2.1.4.0, please visit OAM Help Center- https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/index.html.

Key Benefits

- Scalability (support for up to 250 million user accounts)
- High availability with active-active multiple data center support
- Dynamic, proactive security posture, avoiding the common pitfalls of reactive, static security systems

Related Products

- Oracle Directory Services: All-in-one directory solution with storage, proxy, synchronization, and virtualization capabilities.
- Oracle Identity Governance: User administration (provisioning), privileged account management, identity intelligence and analytics.
- OCI Identity and Access Management: Cloud native, comprehensive, security and identity management platform.

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle