ORACLE

Oracle Cloud Infrastructure Identity and Access Management

Oracle provides end users with a seamless user experience while enforcing strong security.

Organizations need to securely manage access and entitlements to a wide range of applications across cloud and on-premises. The solution should be easy to use, centrally managed, and aligned with a zero trust approach to security. Oracle provides a cloud-native, identity-as-a-service (IDaaS) platform to address these needs.

OCI Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) is a cloud-native IDaaS service providing broad coverage of identity and access use cases for employees, partners, and consumers. It helps manage access and entitlements across a wide range of cloud and on-premises applications. OCI IAM's zero trust strategy positions identity as the security control mechanism for expanding IT landscapes.

Sign-On with flexible authentication options

Enable flexible sign-on with support for federated, social, and delegated sign-on as well as passwordless authentication, robust risk-aware adaptive security (based on device, network, time, etc.), and numerous options for multi-factor authentication (MFA) (mobile app, SMS, email, phone call, FIDO2, etc.)

Seamless user experience and self-service

Provide an experience that's intuitive and easy with self-service registration and profile management. A dashboard view offers quick access to applications with the ability to select favorites, like bookmarks, to enable faster movement in environments with numerous applications. Users can request access directly from the user console to help make it quick and easy to get productive.

Easy administration of users, groups, and access

Create and manage users, groups, and apps in the admin console via step-by-step wizards. Access can be assigned to users through group memberships which are then assigned access to applications. This eases management efforts and allows for repeatable onboarding and certification processes.

Developer friendly APIs and sample code

All available functionality is exposed programmatically via APIs. Sample code and SDKs make it easy for developers to include IAM functions into custom or commercial apps. App consumers are provided profile self-service, seamless social and passwordless logon, and terms-of-use consent management.

"We are seeing a lot of value with Oracle's OCI IAM service. It is more secure, cost effective, and resilient, allowing us to provide a highly available identity platform with improved user experience."

Chinna Subramaniam
Technical Director, IAM & Directory Services
City and County of San Francisco, CA

Identity Standards

In addition to a broad set of REST APIs, OCI IAM supports numerous standards and protocols including:

- OpenID Connect
- SAML 2.0
- OAuth 2.0
- OATH
- FIDO2
- SCIM 2.0
- RADIUS

Broad and flexible application coverage

In addition to a catalog of pre-integrated apps and support for open standards (SAML, OIDC, OAuth, SCIM), OCI IAM supports a wide variety of apps via proxies, bridges, and gateways that offer single sign-on and identity lifecycle management to on-premises or cloud-hosted applications and platforms.

Built-in reporting and auditing on activity and risk

Included reporting provides broad visibility into access activity. A system log captures activities such as logon attempts and user or group changes. An application access report shows which apps are being accessed by which users. Use this information to identify potentially malicious attempts and enforce the principle of least privilege by reducing unnecessary permissions.

Customize and configure to meet your specific requirements

Numerous configuration options enable a customized experience. From company branding to allowed MFA factors, administrators have full control over the end-user experience based on their own organization's needs. Each application can even have unique sign-on or terms-of-use policies.

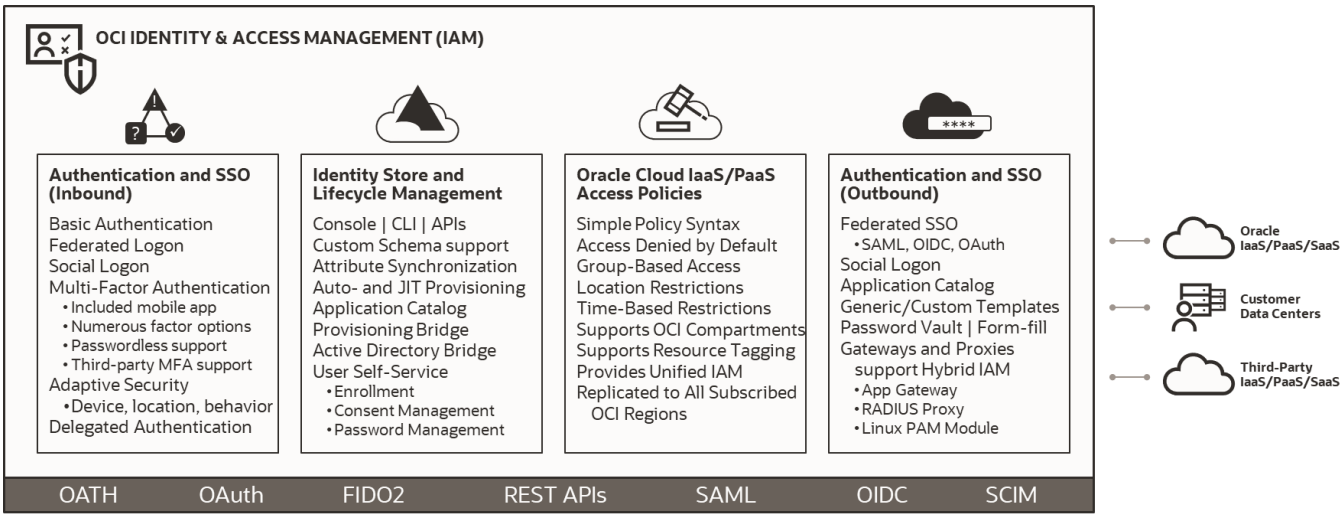
Authentication Methods

OCI IAM supports numerous authentication methods including:

- Username + Password
- Certificate X.509
- MFA: Security Questions Mobile App (passcode, push notification), Email, SMS, Phone Call, FIDO2 Authenticators
- Passwordless Logon
- Trusted Devices
- Adaptive Security: Device (managed, trusted, secure), Network, Location, User Behavior (failed attempts, velocity)

Manage access and entitlements across hybrid IT environments

OCI IAM helps make it easy to manage access and entitlements across hybrid-cloud environments with flexible authentication options, a seamless user experience, easy administration, and the ability to customize and accommodate unique requirements. OCI IAM is a service with broad global coverage, support for local data residency requirements, and high scale and performance. To learn more, visit oracle.com/cloudidentity.



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