Oracle Access Governance

Oracle Access Governance is a cloud native identity governance and administration (IGA) service that provides customers a simple, easy-to-understand view of what resources individuals can access, whether they should have that access, and how they're using their access entitlements. Businesses are challenged every day to enforce appropriate, just-in-time user access rights to manage control of their information and address regulatory compliance requirements of least-privilege access. With immediate and prescriptive guidance about the types of access that users should have, Oracle Access Governance makes it easier for administrators to provision new users and deprovision departing users quickly. In addition, machine learning intelligence in Oracle Access Governance can monitor all types of access for anomalous behavior patterns and automate remediation actions as required. Instead of big, manual, periodic reviews, Oracle Access Governance allows continuous compliance with the proper access management and constantly evaluates and reports risks. Events and access at risk are reviewed regularly and informed by built-in intelligence. This continuous compliance model significantly reduces the cost and effort of audit response. Oracle Access Governance continuously adds support for orchestrated systems, providing strong insights into access controls across new applications that may span across cloud and on-premises environments.

Governance and Compliance
Identity Intelligence
Access Control
Identity Orchestration

Oracle Access Governance continuously discovers identities, monitors their privileges, learns usage patterns, and automates access review and compliance processes with prescriptive recommendations to provide greater visibility and compliance into access across an organization's entire cloud and on-premises environment.

"As we steer our path towards the adoption of a cloud native governance architecture, Oracle Access Governance rises as a critical player in this arena. Its strategic design, emphasizing intuitive user access review, prescriptive analytics powered by data insights, and automated remediation, echoes our commitment to fostering a secure IT environment. This cloud native service aligns perfectly with our forward-looking IT security strategy, and we are eager to explore its potential."

Chinna Subramaniam
Director, IAM & Directory Services, Department of Technology, City and County of San Francisco

Background

Traditionally, organizations of all sizes and across industries have encountered challenges in effectively managing access levels for users, devices, bots, and services, aiming to enhance productivity while minimizing potential risks. Additionally, maintaining visibility into who has access to which digital asset and verifying the validity of such access in accordance with company compliance guidelines is another significant challenge.

Organizations typically rely on manual processes to assign permissions to users and other identities. This often involves users reaching out to other individuals through email or collaboration tools to request access. However, manual processes pose challenges in terms of scalability and compliance verification. Organizations also depend on periodic manual reviews across access rules, entitlements, permissions, roles, and policies.

The global increase in cloud adoption and digital transformation has compelled organizations to be aware of security risks associated with access and entitlements. With the prevalence of multicloud and hybrid environments, organizations face challenges of effectively managing accurate and automated provisioning or deprovisioning of user access. Additionally, the complex and time-consuming nature of access reviews and the lack of necessary context make it difficult for reviewers to make informed decisions about an individual's access. The lack of clarity leads many organizations to take a "rubber-stamp approval" approach, providing blanket approvals that don't revoke overprivileged access. These issues make it hard for organizations to minimize or eliminate risks associated with identity access to digital assets, overprivileged access to critical data, prove compliance with corporate policies, and reduce governance costs.

Overview

To leverage advanced identity governance and administration capabilities, organizations should evaluate solutions that offer flexible access control measures to improve productivity. These solutions should incorporate real-time capabilities, such as prescriptive analytics, to identify anomalies and mitigate security risks effectively. By evaluating and implementing such solutions, organizations can bolster their security posture and streamline identity governance processes.

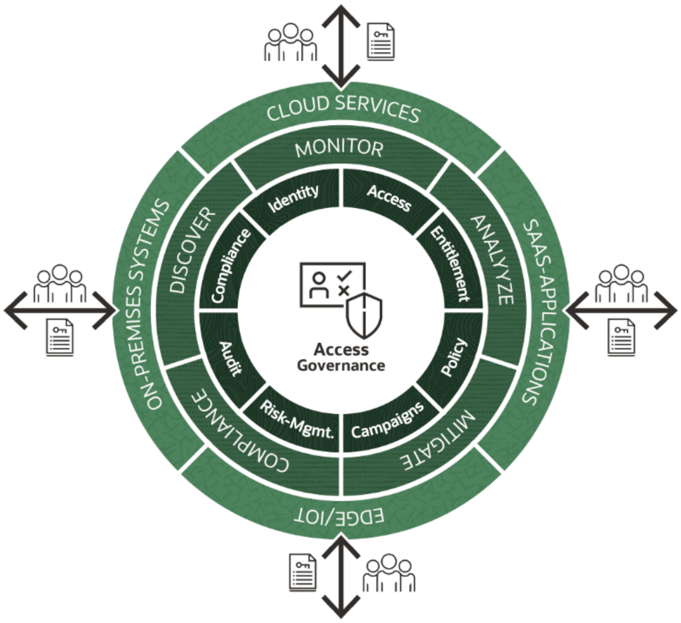


Figure 1. Oracle Access Governance—Governance that's always on

Oracle Access Governance delivers a comprehensive governance solution that encompasses various provisioning methods such as access request and approvals, role-based access control, attribute-based access control, and policy-based access control. This service features a conversation-style user experience, offering deep visibility into access permissions across the entire enterprise. It facilitates dynamic, periodic, and automated event-based micro-certifications, such as an access review triggered by a job code or manager change. Additionally, it enables near real-time access reviews, providing detailed recommendations with options for reviewers to accept or review an entitlement based on the identified level of risk.

Oracle Access Governance can also run with Oracle Identity Governance (OIG) in a hybrid deployment model. Organizations that opt for a hybrid model can take advantage of advanced capabilities available from cloud native services, while retaining parts of their on-premises Identity and Access Management Suite for compliance or data residency requirements.

"With our transition to a cloud-based governance solution, Oracle Access Governance presents an appealing option for streamlining user access reviews, providing enterprise-wide visibility into access permissions, ensuring zero migration effort, and offering insight-driven analytics. We believe it has the potential to enhance our IT security and efficiency, making it a worthwhile solution for organizations exploring cloud governance platforms."

Monica J. Field
IT Director, Identity and Access Management, Cummins Inc.

"We see tremendous value when leveraging identity-as-a-service solutions, such as Oracle Access Governance, to integrate more powerful, analytics-driven security for organizations moving to the Cloud. This solution enables Deloitte professionals to deliver enhanced security with agility, scale, and analytics, all while helping clients protect their existing investments in governance and supporting multicloud environments."

Kashif Dhatwani
Advisory Senior Manager
Cyber and Strategic Risk
Deloitte & Touche LLP

Key Benefits

- **Simplified self-service:** Oracle Access Governance provides self-service that empower users to request access bundles or roles for themselves or others. This streamlined process enhances efficiency and empowers users to actively participate in access governance activities.

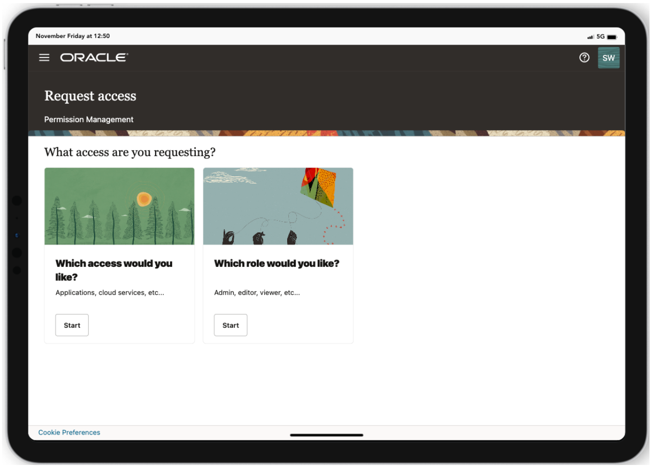

November Friday at 12:50
5G
ORACLE
SW
Request access
Permission Management
What access are you requesting?
Which access would you like?
Applications, cloud services, etc...
Start
Which role would you like?
Admin, editor, viewer, etc...
Start
Cookie Preferences

Figure 2. Simplified self-service

- **Automated provisioning:** Oracle Access Governance supports identity collections, which enables attribute-based access control (ABAC). This capability allows for fine-grained control over access bundles based on specific attributes associated with identities. Furthermore, Oracle Access Governance incorporates role-based access control (RBAC), a feature that enables access rights to be defined and managed based on specific roles. These identity collections and roles can be further used by policy-based access control (PBAC) for granting and managing access rights. Unmatched accounts help in detecting orphaned and rogue accounts in various governed systems.
- **Flexible delegated access control:** Oracle Access Governance facilitates delegated ownership, which allows businesses to manage identity collections while application owners oversee access bundles including accounts and entitlements. This delegation enables efficient and streamlined management of access rights within Oracle Access Governance, promoting collaboration and accountability among stakeholders.

Key features

Oracle Access Governance includes robust set of features and some of them are:

- **Cloud native service**: It's an OCI native subscription service.
- **Intuitive user experience**: It offers an intuitive user experience using a conversational approach.
- **Interactive dashboard**: It includes dashboards that offer valuable insights to enable users to focus on essential tasks.
- **Enterprise-Wide Browser**: It includes analytics driven dashboard for privileged users to get deep visibility of all access information.
- **Identity orchestration:** It supports rapid application onboarding with a low-code, wizard-based integration approach that includes correlation and transformation rules.
- **Easy integrations:** It offers a wide range of specialized and generic integrations connected through downloadable container-based agents, RESTful APIs, or flat-files.

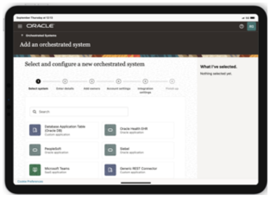
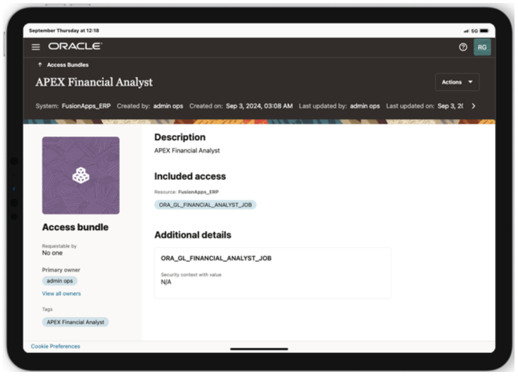


Figure 3. Application Catalog

- **Wide range of integrations:** It offers identity orchestration to various Oracle workloads such as Fusion Apps, EHR, Databases etc. and non-Oracle workloads such as Microsoft AD, Entra ID, MS SQL, IBM DB2 etc.
- **Simplified access request:** It provides a simple user experience for self-service-based requests.
- **Automated provisioning:** It provides multiple access



APEX Financial Analyst

System: FusionApps_ERP Created by: admin ops Created on: Sep 3, 2024, 03:08 AM Last updated by: admin ops Last updated on: Sep 3, 20

Requestable by: No one

Primary owner: admin ops

View all owners

Tags: APEX Financial Analyst

Description: APEX Financial Analyst

Included access

Resource: FusionApps_ERP

ORA_GL_FINANCIAL_ANALYST_JOB

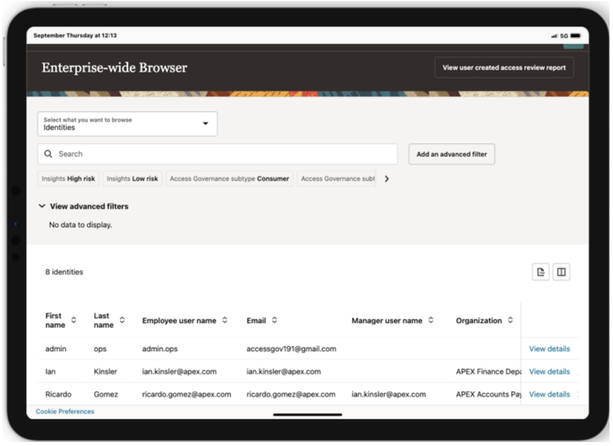
Additional details

ORA_GL_FINANCIAL_ANALYST_JOB

Security context with value: N/A

Figure 4. Configuring an access bundle with various permissions

- **Visibility into access map:** Oracle Access Governance offers visibility into user access across the entire organization, providing insights into which users have access to specific applications, resources, and services. Managers can review the access map of their teams, enabling them to understand and oversee the access privileges of their team members. Individual users can also view their own access permissions, giving them transparency into and awareness of their own access rights.



Enterprise-wide Browser

Select what you want to browse: Identities

No data to display.

8 identities

First name	Last name	Employee user name	Email	Manager user name	Organization	
admin	ops	admin.ops	accessgov191@gmail.com			View details
Ian	Kinsler	ian.kinsler@apex.com	ian.kinsler@apex.com		APEX Finance Depa	View details
Ricardo	Gomez	ricardo.gomez@apex.com	ricardo.gomez@apex.com	ian.kinsler@apex.com	APEX Accounts Pay	View details

Figure 5. Visibility into enterprise-wide access

- **Improve certification efficiency**: Oracle Access Governance empowers organizations with actionable insights and prescriptive analytics, facilitating a comprehensive understanding of the necessary access required to expedite user productivity. Organizations gain visibility triggered by event-based certifications, such as a job or organization change or timeline-based certifications, so access reviewers can quickly take the necessary actions to update access privileges. Policy and group reviews help to further enforce the principle of least-privilege.

control measures that can be leveraged to automate access provisioning in various scenarios.

- **Actionable access Reviews:** It simplifies the access review process and provides actionable insights based on prescriptive analytics so managers can make informed decisions.
- **Micro certifications:** It facilitates intelligent event-based access reviews triggered only when there are changes in the system of record. Timeline-based micro-certifications helps in timely reviews of accesses based on important milestones. Unmatched account certifications get triggered when orphaned and rogue accounts are detected.
- **Codeless workflows:** It provides lightweight codeless workflows for access control and governance.

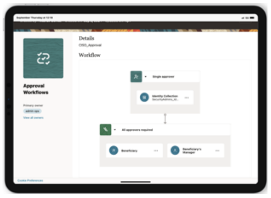
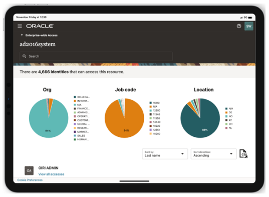


Figure 6. Workflow Editor

- **Configurable Notifications:** It includes customizable notifications that can be delivered either by native or any OCI notification delivery service.
- **Comprehensive IT audit, and reporting:** It includes simplified auditing, monitoring, and flexible reporting capabilities.



ad2016system

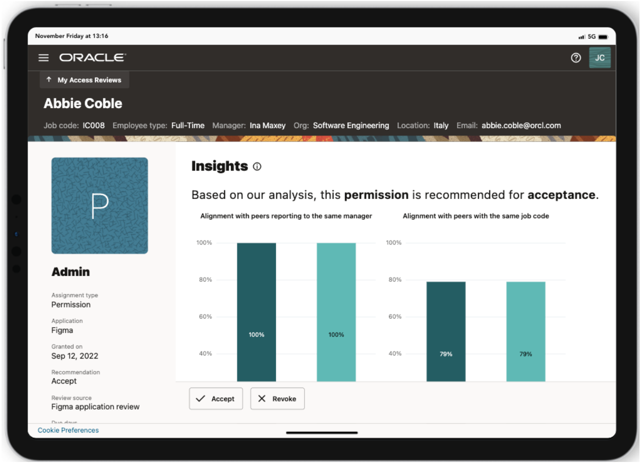
There are 4,666 identities that can access this resource.

Sort by: Last name

Sort direction: Ascending

OIRI ADMIN

Figure 7. Analytical Dashboard



November Friday at 13:16

Abbie Coble

Job code: IC008 Employee type: Full-Time Manager: Ina Maxey Org: Software Engineering Location: Italy Email: abbie.coble@orcl.com

Admin

Assignment type: Permission

Application: Figma

Granted on: Sep 12, 2022

Recommendation: Accept

Review source: Figma application review

Insights

Based on our analysis, this **permission** is recommended for **acceptance**.

5G
ORACLE
JC
My Access Reviews
P
Due days
Alignment with peers reporting to the same manager
Alignment with peers with the same job code
100%
80%
60%
40%
100%
100%
79%
79%
Accept
Revoke
Cookie Preferences

Figure 8. Enforce access controls with prescriptive analytics.

- **Governance anywhere:** Oracle Access Governance provides governance across enterprise applications, IaaS, PaaS, SaaS workloads including Oracle and non-Oracle Workloads.
- **Enhance regulatory compliance:** Oracle Access Governance helps enforce and attest to regulatory requirements, such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and GDPR – that are associated with identifying who has access privileges to sensitive, high-risk data.
- **Reduce costs:** Oracle Access Governance allows organizations to use a cloud native identity governance service that helps reduce IT costs and save time through efficient, user-friendly dashboards, code-less workflows, and wizard-based application onboarding.

Summary

Oracle Access Governance helps organizations to automate access control, gain visibility, make informed access decisions, and support their overall compliance objectives. Organizations can extend their current Identity Governance and Administration capabilities with a cloud native service to begin with deeper insights. For more information, review the Oracle Access Governance product documentation or visit the Oracle Access Governance webpage.

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