

# Oracle Identity Governance Suite

## 12.2.1.3.0 Datasheet

**ORACLE**

**ENTERPRISE PERFORMANCE  
MANAGEMENT SYSTEM**

Organizations need to balance the requirements to provide users with quick access to the resources with the organization's risk and compliance obligation, ensuring that users only have access to the resources they need to perform their jobs effectively. To achieve this balance, organizations need to deliver intuitive ways for users to request access to systems and applications, manage appropriate policies and processes to approve such access, provide simple ways for managers to confirm that such access is appropriate and finally, monitoring tools for managers and administrators to periodically check and certify that access is properly assigned to employees. Further, these systems need to apply to both standard user accounts and high risk, privileged accounts that are often shared by multiple administrators. Oracle provides a simplified complete and comprehensive Identity Governance solution that enables organizations to efficiently balance the objectives of access, security, and compliance, while enabling user self-services to reduce total cost of ownership.

### KEY FEATURES

#### Oracle Identity Governance

##### 12.2.1.3.0

- Simplified, business friendly Self Service interface drives productivity and increases user satisfaction and operational efficiency
- Simplified, business friendly Application On-Boarding UI which enables business users to on-board an application in OIG
- Manage risk and reduce costs with a unified Identity Governance solution for both standard and privileged user access
- Choose a platform approach to Identity Management to see a 48%

### Oracle Identity Governance

Oracle Identity Governance reduces the total cost of ownership for organizations by empowering user self-service, simplifying application on boarding process, simplifying audit and compliance tasks and automating IT operations. By delivering a complete and comprehensive platform for access request, role lifecycle management, access certification, closed loop remediation and privileged account management, Oracle Identity Governance is a solution that address today's requirements and enables organizations to quickly adapt to emerging requirements. Oracle Identity Governance suite provides many benefits, including:

- Increased end user productivity – a business friendly and intuitive self-service experience that is both persona oriented(different UI and access level for Persona) and provides guided navigation, common business glossary for improved search, unified workflow orchestration and immediate access to key applications
- Increased IT productivity and automation of provisioning tasks, simplified application on-boarding, accelerated user- on-boarding and stringent controls over

**ORACLE**

lower operational cost and 33% fewer audit deficiencies

- Centralized and extensible access catalog to store and further define business friendly definitions for Roles, Applications & Entitlements
- Simplified Access Requests with intuitive and flexible approval workflows and policy-driven provisioning improves IT efficiency, enhances security and enables compliance
- Role based access control with Role Mining, Advanced Role Lifecycle Management and Role Analytics
- Risk-based, business user friendly Identity Certifications & closed loop remediation of access rights. Group and Custom group reviewers for the certifications
- Continuous IT Audit Monitoring and Reporting to determine and take action on toxic combinations of access privileges across the enterprise

**KEY BENEFITS**

**Oracle Identity Governance  
12.2.1.3.0**

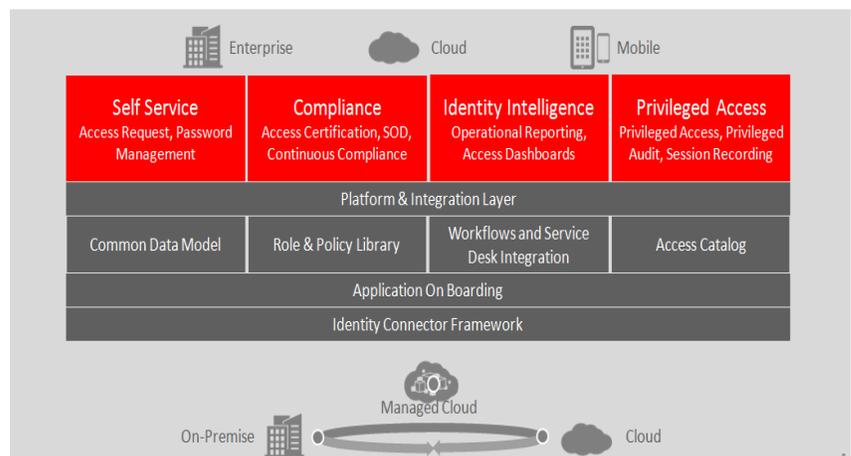
- Increased security: Enforce internal security audit policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges.
- Privileged Account Management: Allow authorized users to manage sensitive servers, applications and services in a controlled audited manner.
- Enhanced regulatory compliance: Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA and GDPR) associated with identifying who has access privileges to sensitive, high risk data
- Improved business responsiveness: Get users productive faster through

sensitive access to shared privileged accounts

- Reduced total cost – single vendor platform for identity governance, combines comprehensive out-of-the-box capabilities with a flexible and simplified customization framework and deployment manager. You can easily import export configurations from one environment to other i.e. three step import/export process
- Reduced risk – guaranteed access revocation, detection and management of orphaned accounts, proactive and reactive IT audit policies (detection and enforcement), fine grained authorization controls, preventive and detective access policies, continuous monitoring and role based access re-evaluation
- Increased efficiency – risk based identity certification on live data reduces overall time to certify access. Provisioning automation and closed-loop remediation ensure access is controlled and maintained.
- Simplified install and upgrade experience – Integrated quick start installer with SOA, webLogic and IDM. Installation footprint and time has been significantly reduced~ 20 minutes.
- Business Friendly Access Policies –Self Service Business user friendly access policies and directly link ups and multiple application instances with access policies. Access policies get enforcement during role inheritance.
- Simplified Application On-Boarding Process –Business user can easily on-board applications in OIG. It's simple, intuitive wizard base application configuration UI. Customization scripts space is available in wizard itself.
- SCIM and REST API security –KSS (key store service) and Support for various TLS1.2. SCIM interfaces are secured via OWSM JWT token and custom request headers. REST interfaces are secured via OWSM JWT token.

**Assembling the Blocks – Core Solution Components**

Oracle Identity Governance provides a number of core services, each of which solves a unique governance challenge faced by many enterprises.



immediate access to key applications and systems, while enforcing security policies

- Reduced costs: Reduce IT costs through efficient, business friendly self-service, application on boarding and platform-based architecture

#### ARCHITECTURE FEATURES

##### Oracle Identity Governance 12.2.1.3.0

- Converged Solutions: Oracle Identity Governance Suite solutions - Oracle Identity Governance, Oracle Identity Analytics & Oracle Privileged Account Manager work together to create a complete governance process for the enterprise
- Ease of Deployment: UI Customizations and integrations are durable and can survive patching and upgrades
- Flexible and Resilient: Oracle Identity Governance can be deployed in single or multiple server instances. Multiple server instances provide optimal configuration options, fault tolerance, redundancy, fail-over and system load balancing
- Maximum Reuse of Incumbent Infrastructure: Oracle Identity Governance is built on an open architecture to integrate with and leverage existing software and middleware already implemented within an organization's IT infrastructure
- Standards-based: Oracle Identity Governance incorporates leading industry standards, such as J2EE, BPEL and OASIS

## Business Friendly Self Service and Access Request

Organizations are eager to reduce costs and accelerate processes by empowering user self-service. Embracing this paradigm, Oracle Identity Governance solutions include out-of-the-box, business persona oriented self-service and guided navigation that enables end users to complete tasks seamlessly, while using a UI that is tablet friendly and pertains to the Identity Governance tasks they care about the most. In addition, Shopping cart style access request interfaces are designed to follow common practices popular on commercial e-commerce sites, such as “add to cart”, “review cart”, “checkout out” etc. Core to empowering end user self-service is the expressive and comprehensive Access Catalog: a glossary that includes user-friendly names for all systems and resources to simplify the user process of searching for the right system or business application. Further, this catalog also includes enterprise items such as sensitive, privileged accounts, roles and entitlements, necessary to drive roles-based provisioning.

## Simplified Application on Boarding

As the number of applications in any organization have increased to which to which employees have access. On boarding large numbers of application is bit challenging and time consuming process. But, with the help of OIG simplified application on boarding feature: - which enables business users to on board application in OIG makes its seamless and effortless. It has reduced the application on boarding significantly and you can easily on board any numbers of applications in OIG.

## Advanced Role Lifecycle Management

In an effort to effectively manage the proliferating number of users, many organizations are leveraging roles to assign and manage rights and privileges. To support this approach, Oracle Identity Governance includes innovative and robust role discovery and lifecycle management capabilities, which both harvest roles as they are created and manage approval processes for any changes to roles on an ongoing basis. In addition, robust Role Analytics enable role designers and approvers to evaluate the impact of role changes, with inline SoD violations checks, impacts to users and entitlements and metrics that help with role consolidation. All role activities are fully audited and changes can be rolled back if necessary.

## Streamlined Access Grants

While a business friendly interface simplifies the access request process, access grants must be approved by authorized entities, which may require various levels of information as justification for the request. Oracle Identity Governance leverages standards-based approval workflows, which include enterprise capabilities such as delegating approval and including supporting attachments on workflow requests to provide the additional detail required to make an approval decision.

## AVAILABLE CONNECTORS

### Oracle Identity Governance 12.2.1.3.0

- Business Applications: Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP
- LDAP stores: Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory
- Security systems: RSA, RACF, Top Secret, ACF2
- Collaboration Suites:  
Exchange/Domino and GroupWise
- Operating systems: OEL, Red Hat Linux, HP-UX, AIX, Solarix, AS/400 and Windows
- Ticket Management systems: BMC Remedy
- Cloud Connectors: Oracle CRM On-demand, Google Apps, Office365, Salesforce, ServiceNow, Concur, Box, DropBox, WebEx and SuccessFactors
- Databases: Oracle, MySQL, SQL Server, DB2, Sybase
- Technology Integrations: SSH, Telnet, Flat File, JDBC, LDAP V3, SOAP, Generic Scripting(Groovy, Beanshell and JS), RESTand SCIM

## Simplified Identity Certification

As the number of applications to which employees have access increases, certifying access becomes imperative, especially for larger enterprise organizations. In order to efficiently scale and sustain, these processes need to be both automated and resilient. With advanced, risk-based analytics and easy to navigate dashboards, Oracle Identity Governance offers a robust set of identity certification features that streamline the review and approval processes to effectively manage risk on an ongoing basis. Beyond understanding “who has access to what”, in depth analytics can provide detailed graphical and actionable business context, as well as 360-degree views on how such access was granted and highlights outliers for individuals versus their roles. In addition, Identity Certifications promote business user friendliness via innovative capabilities such as the ability for reviewers to complete certifications offline and ability to add customer reviewers and group reviewers for the certification. In addition, workflow capabilities that allows both Business and IT teams to collaborate on a single Identity. Workflow can be easily customizable based on the business process

## Simplified Test to Production Environment Movement

OIG Deployment Manager is a simple three steps process UI for exporting and importing Oracle Identity Governance configuration(s). Usually, you use the Deployment Manager to import/export configurations from one deployment to another, for example, from a test to a production deployment, or to create a backup of your system.

Certification campaign are also included. Finally, the solution offers closed loop remediation, which provides an automated way for reviewers to revoking improper access across target systems and includes alerts should remediation fail.

## Privileged Account Management

Within virtually every organization, there are sensitive, privileged accounts, such as Root Admin accounts. These accounts must be shared between multiple users and are frequently managed insecurely. Oracle identity Governance enables organizations to extend core identity management policies to these sensitive, privileged accounts. Administrators, or super users seeking access to these accounts can use the standard, access request interface and Access Catalogue to request access to these privileged accounts. Standard approval workflows and certifications apply and organizations can leverage their existing Oracle Identity Governance connectors to manage the privilege account passwords.

## IT Audit Monitoring & Reporting

Oracle identity Governance provides both policy-based audit monitoring and detailed and flexible reporting capabilities. Comprehensive dashboards enable both system administrators and delegated administrators to run reports on

virtually any artifact of a user's access rights, access grants and the genesis of each. The Oracle Identity Governance Suite offers the ability to define and enforce detailed security policies both within and across applications to enforce continuous Segregation of Duties analysis. This enables intelligent monitoring and to identify and remediate imminent violations typically caused by access grants following job changes or other HR events. Finally, decisions made to identify certification reports are always stored and archived for audit purposes.



#### CONTACT US

For more information about [insert product name], visit [oracle.com](http://oracle.com) or call +1.800.ORACLE1 to speak to an Oracle representative.

#### CONNECT WITH US

-  [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

#### Hardware and Software, Engineered to Work Together

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0817