

ORACLE IDENTITY MANAGER 11g R2 PS2

WHATS NEW IN A NUTSHELL?

- Access Policy Harvesting for reconciled accounts
- Additional APIs to retrieve Provisioned Objects details for applications
- Dynamic Organization membership
- Hierarchical Entitlements
- Catalog Auditing
- Out-of-box archiving/purge support for Tasks, Requests, Recon and Orchestration
- Draft Request support
- Additional Information in Request
- Account/Entitlements dependency handling
- Entitlement form support
- Sunrise/Sunset of accounts and entitlements
- Migration of in-flight provisioning related requests
- Flexible Certification
- Improved diagnostics console via Oracle Enterprise Manager
- Certification migration from prior versions
- Enable OIM Taskflows for Customization uptake
- FVC Utility simplification and performance enhancements
- BI Publisher certification for WebSphere Application Server

OVERALL FEATURES

- Feature-rich user interface that supports durable customizations
- Self-service identity management with personalized, business user friendly experience
- Accelerated application on-boarding
- Advanced delegated administration and password management
- Requests with approval workflows and policy-driven provisioning
- Identity Certifications
- Integration solutions featuring

Oracle Identity Manager is a highly flexible and scalable enterprise identity administration system that provides operational and business efficiency by providing centralized administration & complete automation of identity and user provisioning events across enterprise as well as extranet applications. Part of the Oracle Identity Governance Suite, it provides role lifecycle management and privileged account management, ensuring consistent enforcement of identity based controls thereby reducing ongoing operational and compliance costs. This white paper highlights key new features introduced in Oracle Identity Manager 11gR2 PS2.

Dynamic Organization Membership

In a typical enterprise or extranet use case scenario, a user will be associated to their home organization but would require membership to other organization entities to perform related functions. For example, a global help desk user who belongs to the Support organization would require access to view and perform certain functions (like password reset) on other organizations like Finance, Sales etc. OIM has the capability to manually assign the help desk user to an Organization Viewer admin role, which is restrictive and more applicable to permission grants. Dynamic Organization Membership provides a way to specify a rule that would drive the membership of the user to one or more organizations based on their user attributes. The feature introduces the ability to specify a membership rule for organizations similar to how roles are handled. Once the user is dynamically associated to other organizations, they get implicit viewer privileges to view users, roles and privileges made available to those organizations as well. If certain users are needed to perform certain functions, like the help desk example above, they can still be associated to the corresponding admin role manually. Note that this is dynamic rule based organization membership (not virtual organization) that has to be associated with a physical organization in OIM.

Simplified Request Management

Oracle Identity Manager provides a centralized catalog of access rights, including enterprise and application roles, standard and privileged accounts (OOTB integration with Oracle Privileged Access Manager) and entitlements. OIM enables customers to create multiple views of the centralized catalog, like catalog by location, by department or a hierarchical catalog showing all applications along with associated entitlements etc, tailored to their needs. A list of beneficiaries can also be programmatically sent to the catalog enabling customers to integrate with other request initiating systems like a ticketing system.

OIM provides a business user friendly catalog to request account entitlements. However it required the business user to know any entitlement related dependencies. For example, the user needed to know that they needed an e-Business account before they can request for an entitlement that grants them privileges to raise a purchase order in e-Business. OIM can now automatically request the account for a user when a related entitlement is requested, thereby reducing the burden of the business users to know the account-entitlement relationship.

Business users, requesters, approvers or access certifiers, often require detailed information on what a particular entitlement maps to in the target system. For example, granting an e-Business role or responsibility would grant a user a set of menu/button privileges. OIM now supports such

What's New in Oracle Identity Manager 11gR2 PS2?

Adapter Factory and pre-configured connectors for enterprise applications, LDAP & DB repositories.

- Comprehensive auditing and reporting

critical hierarchical entitlement metadata to be imported and made available during request, approval and certification processes.

Users typically would have more than one account in a target system and OIM supported multiple accounts to be associated with a user. OIM now supports specifying to which account a specific entitlement in a request needs to be associated with during the request checkout process.

In many cases, requesters are required to provide additional information during access request for each item requested. For example, in a request that involves multiple entitlements, the requester might be required to specify the start date and end date for each of the entitlements requested. OIM enables requesters to provide such information during request that can be carried all the way to approval and provisioning processes. OIM also provides an out-of-the-box scheduled task for entitlement grant and revoke based on the start and end dates specified.

OIM also enables requesters to save the request cart enabling them to validate and submit requests at a later time.

Collaborative Certification Process

OIM introduces the capability of specifying additional levels of reviews in the certification workflow process. For example, OIM can now launch a certification review process whereby the business manager reviews the users that report to him/her, but is then followed by the managers' manager also reviewing the same access rights, while viewing the decisions made by their subordinate.

Improved Diagnostics

OIM introduces a new operational console in Oracle Enterprise Manager that enables administrators a complete view of all the defined OIM operations, out-of-the-box and customer defined event handlers, child processes, workflow processes their state and error information without requiring to mine different server logs. This tool does not replace the larger IDM management pack in Enterprise Manager that provides a suite wide monitoring capability but serves as a useful diagnostic tool specifically for OIM.

Contact Us

For more information about Oracle Identity Management, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



Oracle is committed to developing practices and products that help protect the environment

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.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. 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. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together