ORACLE IDENTITY MANAGER 11*g*

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. It manages the entire identity and role lifecycle to meet changing business and regulatory requirements and provides essential reporting and compliance functionalities. By applying the business rules, roles, and audit policies, it ensures consistent enforcement of identity based controls and reduces ongoing operational and compliance costs.

KEY FEATURES

- Self-service identity management drives user productivity, increases user satisfaction and optimizes IT efficiency
- Universal delegated administration enhances security and reduces costs
- Requests with approval workflows and policy-driven provisioning improves IT efficiency, enhances security and enables compliance
- Password management reduces IT help desk costs, and improves service levels
- Integration solutions featuring Adapter Factory and pre-configured connectors enables quick and low cost system integration

KEY BENEFITS

- **Increased security:** Enforce internal security policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges.
- **Enhanced regulatory compliance:** Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA) associated with identifying who has access privileges to sensitive data
- **Streamlined operations:** Reduce inefficiency and improve service levels by automating repeatable user administration tasks
- **Improved business responsiveness:** Get users productive faster through immediate access to key applications and systems
- **Reduced costs:** Reduce IT costs through efficient staff usage and common security infrastructure

Introduction

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that is designed to administer user access privileges across a company's resources throughout the entire identity management life cycle, from initial on-boarding to final de-provisioning of an identity. Oracle Identity Manager is built on a state-of-the-art Java EE architecture. Java EE is a standard, robust, scalable, and secure platform that forms the basis for many of today's enterprise applications. Additionally, Oracle Identity Manager's flexible architecture can handle the most complex IT and business requirements without requiring changes to existing infrastructure, policies or procedures. Its architecture elegantly abstracts core identity administration and provisioning functions into discrete layers. This hallmark flexibility also enables Oracle Identity Manager to excel at handling the constant flow of business changes that impact real-world identity management deployments.

User Self Service

Registration & Profile Management

Using Oracle Identity Manager's self-service interface, end users can create self registration requests. They can additionally view, manage and update their own profile data. This reduces administrative overhead and provides users with control over their identity profiles. The user forms for registration and profile management are extensible. Oracle Identity Manager leverages Oracle Metadata Services (MDS) that allows the structural and behavioral aspects of the configuration to be declaratively described using XML based metadata. This separation of configuration metadata from core UI results into significant reduction in customizations and also provides a simplified development, configuration and deployment experience for self service features.

Password Management

Using Oracle Identity Manager's self-service interface, end users can manage their enterprise

ARCHITECTURE OVERVIEW

- **Ease of Deployment:** Deployment Manager assists in the migration of integration and configuration between environments.
- **Flexible and Resilient:** Oracle Identity Manager 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 Manager is built on an open architecture to integrate with and leverage existing software and middleware already implemented within an organization's IT infrastructure.
- **Modular Architecture:** Oracle Identity Manager is made up of abstraction layers, which allows the execution logic to be changed and refined without affecting logic or definitions that still apply.
- **Standards-based:** Oracle Identity Manager incorporates leading industry standards, such as J2EE and Organization for the Advancement of Structured Information Standards (OASIS).

password that is used in Single Sign-On and gets synchronized or mapped to passwords across managed resources. Oracle Identity Manager enforces compliance of this password with enterprise password policies as well. For the recovery of forgotten passwords, Oracle Identity Manager employs the security challenge questions. This self-service capability easily pays for itself many times over through reduced help desk calls. Oracle Identity Manager also provides random password generation capabilities that may be invoked during registration or administrator-based password reset. Additionally, Oracle Identity Manager's password management features are out-of-box, pre-integrated with all login and password related flows in Oracle Access Manager and Oracle Adaptive Access Manager. Integration with Oracle Adaptive Access Manager includes password recovery mechanism using KBA or OTP based challenge questions and responses. The integration thus serves as a pre-integrated platform for advanced user and administrator authentication scenarios that provide stronger security control.

User Interface

Oracle Identity Manager provides a multi-tab, desktop-like, dynamic Web 2.0 user experience based on Oracle's ADF technology. In addition to great usability, it also provides high performance architecture, such as real-time scrolling and transparent paging. This UI framework allows high level of meta-data driven customization such as branding changes, label changes or changes in default sorting schemes etc. It also includes built-in globalization support. It provides very advanced browse, keyword based search and advanced search capabilities. It also tailors the user experiences for different user groups for example a task-oriented desktop-application-like UI model for administrators and guided wizards for business end-users.

Request Management

Request Service

Oracle Identity Manager allows users to create requests for business & IT roles, new application accounts, modifications to existing application accounts and application entitlements or privileges. It provides a very flexible, simplified, business-centric, and context sensitive request creation wizard that allows users to create these requests in context of their current views. As an example, the users may create requests for additional roles while viewing their existing role assignments, create request for additional accounts or modification to existing accounts while viewing the provisioned resource lists, or create a complex request including multiple roles & resources for self or others from their home page. By placing the request and approval process closer to the business, enterprises realize better service levels and reduced costs.

Approval Orchestration

Oracle Identity Manager relies on the Oracle BPEL Process Manager, an integral component of Oracle SOA Suite for its approval workflow and routing engine. Developers can use Oracle JDeveloper as their Integrated Development Environment that offers a rich visual design paradigm for creating and deploying BPEL based processes. Additionally developers can also leverage Oracle BPEL Process Manager's advanced approval features like email based approvals, serial or parallel approval orchestrations or voting based approval etc. This not only results into significantly faster deployment time, but also provides the architecture agility to adjust workflows quickly when business processes and enterprise policies change for the approval needs.

Request Templates

Request Management allows administrators to create job or role specific request templates. The template is a simplified overlay on top of a request model that allows the person defining that template to control how a request gets created, and add additional layers of approval, authorization and data restrictions over those already defined in the model. Once configured by the administrators, the request templates provide the much-desired request catalog services to the end users. This results into significantly enhanced usability experience for the end users while creating access requests by providing them with a narrowing down the list of roles, resources and entitlements specific to their job functions.

Identity & Role Administration

Universal Delegated Administration

Delegated administration plays an increasingly important role as the already extended enterprise becomes increasingly virtualized and the service provider delivery model becomes increasingly prevalent. Oracle Identity Manager's Universal Delegated Administration provides highly flexible authorization model without compromising corporate security policies by moving administration points as close to the user as possible. This ensures that the enterprise can achieve tighter control and better security, all the while increasing productivity of their users. Oracle Identity Manager embeds a fine-grained authorization service based on Oracle Entitlement Server (OES). Using this authorization service, Oracle Identity Manager provides advanced, attribute level delegated administration policies using dynamic & declarative constructs. For example, administrators can configure a policy stating that the helpdesk can only change the password of the users in certain organizations, or an organization administrator can unlock a locked out user only in her organization.

Role & Policy Administration

Oracle Identity Manager enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators may specify access levels for each resource to be provisioned, granting each user only the exact level of access required to perform his job, no more and no less. These policies can be driven by user roles or attributes, enabling implementation of role based access control (RBAC), as well as attribute based access control. Effective blending of role and attribute based policies is key to a scalable and manageable enterprise provisioning solution. Oracle Identity Manager also ensures that any entitlements granted to a user based on policy get revoked when that policy no longer applies to that user (due to role or context changing).

Oracle Identity Manager provides advanced role administration features that allow administrators to browse and search roles, define role hierarchies, manage role membership rules and existing memberships etc. Additionally role administration capabilities include a role category service that provides a navigation catalog for roles while browsing, searching, administering or requesting roles enhancing the user experience for the end users, line managers as well as delegated administrators.

Oracle Identity Manager also provides out of box integration with Oracle Identity Analytics to provide end to end role lifecycle management, integrated role engineering and closed loop remediation services.

Guaranteed De-provisioning

When a user leaves the organization or her access is no longer required or valid due to a job change, Oracle Identity Manager revokes access on demand or automatically, as dictated by role or attribute based policies. This ensures that a user's access is promptly terminated across all no-longer-required resources to minimize security risks, as well as to prevent paying for access to costly resources, such as data services.

Audit & Compliance

Reconciliation Services

Oracle Identity Manager's Reconciliation Engine component ensures consistency between Oracle Identity Manager's provisioning environment and Oracle Identity Manager's managed resources within the enterprise. The Reconciliation Engine discovers directly managed or unauthorized accounts or entitlements provisioned outside of Oracle Identity Manager. It also provides bulk load utilities to support day-one bootstrap scenarios for on-boarding a new identity store or a new target system under Oracle Identity Manager management. This engine is specifically architected to provide high performance & internet-grade scalability in multi-million user populations. For extranet and enterprise deployments with such high volume scenarios, more than 10x performance gains have been observed when compared with previous releases.

Oracle Identity Manager also provides web based reconciliation event management UI capabilities that allow application as well as IT administrators to view the current state of all reconciliation jobs, tasks and events. They may also perform additional operations like retrying events etc. Administrators can also perform manual linking for orphan accounts in this easy to use, intuitive event manager UI. An orphan account is an operational account without a valid user.

Oracle Identity Manager can also manage the lifecycle of special service accounts, also known as administrator accounts, which have special life cycle requirements that extend beyond the lifecycle of an assigned user and across the lifecycles of multiple assigned users. Proper management of service accounts can help to eliminate another source of potential orphan accounts.

Policy Enforcement & Compliant Provisioning

Oracle Identity Manager ensures that all provisioning triggered from it is compliant to various enterprise-IT Audit policies defined in Oracle Identity Analytics. It also integrates with ERP Segregation of Duty (SoD) policy engines like such as Oracle Application Access Controls Governor and SAP BusinessObjects GRC Access Control for ERP level SoD enforcement. This ensures that policy violations are caught while provisioning rather than "after the fact" in the detective controls.

Reporting

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. The system captures all necessary data to answer the question "Who has access to What, When, How, and Why?" and make this data available in reports through 30+ out-of-the-box reports. Some of the identity data captured includes user identity profile history, user group membership history, user resource access and fine-grained entitlement history. When combined with the transaction data generated and captured by Oracle Identity Manager's workflow, policy, and reconciliation engines, an enterprise has all the required data to address

any identity and access related audit inquiry. Oracle Identity Manager's reporting and auditing capabilities enable an enterprise to cost effectively cope with ever increasingly stringent regulatory requirements, such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and HSPD-12.

Integration Solutions

Connector Framework

Oracle Identity Manager's Connector Framework eliminates the complexity associated with creating and maintaining connections to the proprietary interfaces in business applications. Connector Framework provides rapid integration to commercial or custom systems. The connector framework separates connector code (integration libraries specific and optimized for the target system) from connector meta-data (data models, forms, connectivity information and process). This separation makes extending, maintaining and upgrading connectors a manageable and straightforward process. This also enables custom logic to be more easily pluggable in through custom extensions that do not prevent customers from upgrading to the improved versions of the connector code. Oracle Identity Manager provides the following integration technologies for the connector development:

1. Adapter Factory: Oracle Identity Manager's Adapter Factory® technology eliminates the complexity associated with creating and maintaining the connections to target systems. Users can create new or modify existing integrations using Adapter Factory's graphical user interface, without programming or scripting. Once connectors have been created, their definitions are maintained within the Oracle Identity Manager repository, creating self-documenting views. These views make extending, maintaining and upgrading connectors a manageable and straightforward process.

2. Generic Technology Connector: The Generic Technology Connector framework provides a complimentary solution for identity repository based data flows. It is a framework with basic building blocks that allows system administrators to design custom connectors quickly and easily. Generic Technology Connector may communicate with any target resource by using standard protocols such as HTTP, SMTP, FTP, and Web Services combined with generic message formats such as CSV, SPML, and LDIF.

Pre-Configured, Out-of-the-Box Connectors

For the most popular commercial applications and interface technologies, Oracle Identity Manager offers an extensive and rapidly expanding library of pre-configured connectors. With these connectors, an enterprise can get a head start on application integration. Each connector supports a wide range of identity management functions and uses the most appropriate integration technology recommended for the target resource, whether it's proprietary or based on open standards. These connectors enable out-of-the-box integration, but can be enhanced to work with each enterprise's unique integration requirements.

Applications Integration

Service Oriented Security

Oracle Identity Manager enables Oracle Fusion Middleware & Applications as well as custom applications that customers may have to externalize their identity administration services through its XSD profile SPML web service. This service defines the interfaces for applications to interact with Oracle Identity Manager. Additionally, Oracle Identity Manager supports a LDAP identity repository for managing users, roles and role assignments. The

SPML web service can thus be used by applications to achieve LDAP integration. Oracle Identity Manager also provides identity services for example, generating a username or a random password for the user, reserving username in LDAP while user registration is going through approval etc. Applications leveraging such a service oriented security strategy are able to benefit from the innovation in Oracle Identity Manager on day 1. Additionally, applications customers looking for enterprise provisioning solutions face a much shorter & smoother learning curve given that they are already well versed with provisioning technology powering their applications such as those from Oracle Fusion Middleware & Applications.

Simplified Identity Administration for Oracle Applications Unlimited Products

Oracle Identity Manager provides simplified identity administration for all Oracle Applications Unlimited products including Oracle E-Business Suite, PeopleSoft, Siebel and JD Edwards products. These applications typically are deployed in an identity ecosystem involving SSO solutions, LDAP directories, GRC SoD application, and one or more internal user repositories. For example, Oracle E-Business Suite is usually deployed with Oracle SSO, Oracle Internet Directory, Oracle Application Access Controls Governor, and FND, TCA, HRMS store. Oracle Identity Manager abstracts the identity administration challenges of managing user accounts and entitlements in such a deployment by providing provisioning orchestration across the entire ecosystem. Customer's total cost of ownership associated with securing their Applications Unlimited products is greatly reduced.

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

SOFTWARE. HARDWARE. COMPLETE.

ORACLE