Oracle Role Manager

An Oracle White Paper
Updated June 2009

ORACLE

INTRODUCTION

Oracle Role Manager is an enterprise-class application for managing business and organizational relationships, roles and resources. As the most comprehensive role management product on the market and the system of record for role lifecycle management, it also provides tools for role mining, organizational modeling and administration.

Businesses today must provide timely access to enterprise information systems while also ensuring that such access is compliant with government regulations and policies. However, in today's global business environment, managing data across users, organizations, locations and reporting structures quickly becomes a critical challenge. Often, the maintenance of this information remains a manual task, making it difficult to secure and costly to respond to business events in real time. As a result, the process for providing access is prone to errors, lags behind organizational changes, and lacks the necessary flexibility to represent the many complex and dynamic relationships in today's organizations.

Oracle Role Manager solves these challenges by providing a comprehensive feature set for role lifecycle management, business and organizational relationships and resources. Built using scalable J2EE architecture, Oracle Role Manager enables business users to define user access by abstracting resources and entitlements as roles. Organization data in existing applications can be managed within Oracle Role Manager to model complex relationship paths across business structures such as reporting organization hierarchies and locations. Business policies defined in Oracle Role Manager utilize organization and relationship data to drive role membership and ultimately access. Through seamless integration with Identity and Access Management (IAM) applications, Oracle Role Manager enables you to automate provisioning events, addressing governance and compliance needs across your existing information technology (IT) infrastructure.

With Oracle Role Manager, you will be able to:

- Enhance security by dramatically improving the timeliness and accuracy of provisioning and de-provisioning of resources as role membership changes
- Accelerate your role management implementation by mining for candidate roles
- Maintain a single authoritative source for roles and entitlements
- Strengthen regulatory compliance through detailed audits on who should have access to what, and why user was given access

In a June 2007 study on IAM technologies, the Gartner Group highlighted the importance of maintaining role and group information, stating that companies must enhance their IAM processes to establish and manage the enterprise role throughout its entire lifecycle. As one of the most advanced role management applications available on the market today, Oracle Role Manager enhances the value of your existing IT investment and lowers the overall cost of compliance.

KEY BENEFITS

Enhanced security

Oracle Role Manager dramatically improves the accuracy of resource provisioning based on policy. By responding in real-time to business events, such as a new hire or transfer,

automated role-based provisioning ensures that access and entitlements align with business policy. Oracle Role Manager also offers mining tools to identify rogue entitlements, uncover users with no entitlements (“orphaned” users), and discover candidate roles. Not only do these tools assist in analyzing and cleaning up your existing data, they quickly add value to your IAM investment and create a secure foundation for role lifecycle management.

Authoritative source for roles and entitlements

As the comprehensive source for role and role lifecycle management, Oracle Role Manager can provide contextual and policy based roles to a variety of enterprise applications, including Business Process Management (BPM) workflows and IAM applications. As an abstraction of entitlements, roles provide a mechanism for defining contextual policies that ultimately answer the question of 'Who should have access to what?'.

Authoritative modeling of business and operational data

Operational data such as employee white pages, reporting structures and even external data about partners or customers often lose value by being spread across disparate systems that remain unconnected to security policy. By bringing together diverse operational data into a single authoritative application Oracle Role Manager can easily model organizational structures and relationships. These business models form the foundation for building secure and accurate role policy. Oracle Role Manager also provides mining tools to assist in data cleansing and analysis, ensuring accurate modeling of operational data.

Enable scalable role management process

Automated provisioning events based on role membership and policy improves IT productivity, limits manual workarounds and prevents security violations. Business users can utilize Oracle Role Manager to define and manage roles and create business policy to drive automated provisioning events. The abstraction of entitlements as roles and the capturing of business context enable the business users to engage in the corporate security process. Business user involvement is critical toward deploying a scalable security process where role and policy data can be kept accurate and up-to-date.

Enable high level of service level and business continuation integrity

Role membership is updated automatically based on changes to organizations, people, and resources. Out-of-the-box integration with IAM systems means that as role membership changes, access and entitlements change. Integration with IAM combined with the authoritative repository for operational data makes Oracle Role Manager an ideal tool to plan and prepare for unforeseen events, such as disaster and emergency situations. Automating emergency access based on pre-configured business continuity model can enable core business operations to continue while minimizing the overall impacts to your organization and your clients during a catastrophic emergency.

Oracle Role Manager allows users across the enterprise to create and manage roles, define role membership according to business policy, map roles to resources and entitlements and change the state of roles to control access.

FEATURES

Enterprise Role Lifecycle Management

Oracle Role Manager provides comprehensive tools to support enterprise role lifecycle management (RLM). Utilizing a web-based user interface, users across the enterprise can create and manage roles, define role membership according to business policy, map roles to resources and entitlements and change the state of roles to control access. As business events occur and the organization changes, role membership is dynamically recalculated, ensuring appropriate access and preventing security holes and compliance violations.

Role and Rule Mining

Tools for role mining take existing enterprise data about users, entitlements and the relationships between them to discover candidate IT roles. This process, commonly referred to as "bottom-up" analysis, identifies patterns in existing entitlements and user memberships to suggest roles that can be exported and managed in Oracle Role Manager.

Adopting a role management solution can be a daunting task for businesses trying to sort through data across the enterprise. The process for role mining first leads the business through data analysis and validation, role mining and finally rule mining which can further refine candidate IT role membership.

Oracle Role Manager accelerates your role management implementation by providing tools and methodology around:

- Importing user, resource, and privilege information from diverse sources for analysis and validation. Data analysis tools assist in the process of cleansing data to delete orphaned user accounts and uncover existing violations of security policy.
- Allowing role mining parameters to be configured improves the accuracy of mined results. Changing the values of role mining parameters based on the unique characteristics of an imported dataset increases the probability of quality candidate roles.
- Discovering and structuring candidate roles as a role hierarchy allows users to easily review clusters of entitlements. Hierarchical structures streamline analysis and validation of mining results ensuring that roles contain the correct entitlements.
- Discovering potential rules and policies for mined roles. Rules are derived from user attributes and relationships and assist in refining role membership for more secure role definitions.
- Exporting role definitions for complete role lifecycle management. Desirable mined roles and rules that have undergone evaluation from the business can be selected for export into a role management system.

Context-Aware, Polyarchy Enabled Role Engine

Oracle Role Manager features powerful role engine that uses your business policy and traverses the relationships between users and organizations to derive accurate, real-time role membership. This contextually aware engine resolves complex relationships across business organizations to ensure that access is aligned with corporate strategy.

For example, you can specify:

- A cost center manager is a person who is in a manager relationship with an organization in a cost center hierarchy.
- A European account executive is a person who has a specific job code or team membership in the sales branch of the reporting hierarchy and who is located in the European branch of the location hierarchy.

Oracle Role Manager supports three main types of roles out of the box: Business, IT and Approver. Business roles, which can be policy based, rely on contextual business information to refine membership such as a job code attribute or membership in the engineering organization. To manage roles effectively, business owners should manage business role definitions and role memberships that reflect what a person does.

IT roles, which can be thought of as a collection of privileges or entitlements, are mapped to business roles, automating access to members of the role. The IT organization should manage IT role definitions and the entitlements to ensure that appropriate access is granted to role members.

Approver roles are defined contextually, and can resolve complex queries such as "Who is the cost center manager for Joe?".

Business roles that are policy based incorporate hierarchical information across the business to provide accurate scope, and context for the assignment. This allows people who understand and manage the organizational structure to define the structure and automate role membership.

Oracle Role Manager also supports the traditional, ad hoc way of managing business role memberships manually. This strategy may be employed when a business role should not be based on policy or when the complexity of the role and its supporting data are more easily managed statically.

Though Oracle Role Manager provides three types of roles out of the box, custom role types can be configured to meet the needs of today's dynamic enterprises.

Authoritative Role and Entitlement Repository

Oracle Role Manager aggregates and manages contextual business information such as organizational relationships into a comprehensive role repository. Serving as the central source of information for roles, these complex relationships supply authoritative entitlement data to enterprise systems.

Configurable and Extensible Role and Relationship Model

Organization structures, relationships and business operational models can be unique and diverse as businesses themselves. While one business may depend on a traditional reporting organization hierarchy, another business may have a more collaborative organization. Oracle Role Manager responds to this need by making it easy to model unique business structures and relationships and providing tools for customizing the user interface.

Role Delegation

Common business scenarios require the ability to delegate access and privileges to users. By providing delegated administration of roles, Oracle Role Manager enables business users to easily delegate access and privileges without violating existing business policy. Delegated administration provides business users the ability to manage access, a function normally centralized in IT departments. This feature of Oracle Role Manager highlights how identity and access management tasks quickly scale across the organization to lower IT costs.

Organization and Relationship Management

Organization and Relationship information in Oracle Role Manager can be used by role engineers to resolve role memberships without manual intervention.

The complexity of an individual's relationships in a dynamic organization poses a significant challenge for existing applications and directories, which lack the ability to capture and manage complex business relationships. At best, directories can describe one organizational hierarchy, leaving additional hierarchies and memberships to be represented as simple Boolean attributes. For example, with directories, you can indicate whether Jane is a manager, but you cannot capture the full context of her role, including what Jane manages, who she manages, what her span of control or authority is, and what entitlements she has across heterogeneous applications. To properly reflect organizational reality and to maintain data integrity among interdependent hierarchies, you need a model that maps the intersection of multiple, overlapping hierarchies or "polyarchies".

To understand how modeling the polyarchy enhances role lifecycle management, it helps to look at the business problems of a leading national grocery chain. The grocery chain was faced with managing retail stores that spanned multiple geographies, managing different supply chains for different products and adapting to high personnel turnover and routine changes in staff responsibility. By modeling each of these business structures as separate hierarchies and then building the relationships across them, the grocery chain was able to fix identity and access problems such as multiple retail clerks sharing one register account. Role policy for retail clerks could be written in terms that business users can understand by utilizing the hierarchies for employees and retail stores. Using the polyarchy to define role policy is crucial for operational efficiency and provides the foundation for business integrity.

Oracle Role Manager's web-based GUI accelerates role engineering and allows business users and administrators alike to define and manage complex business relationships.

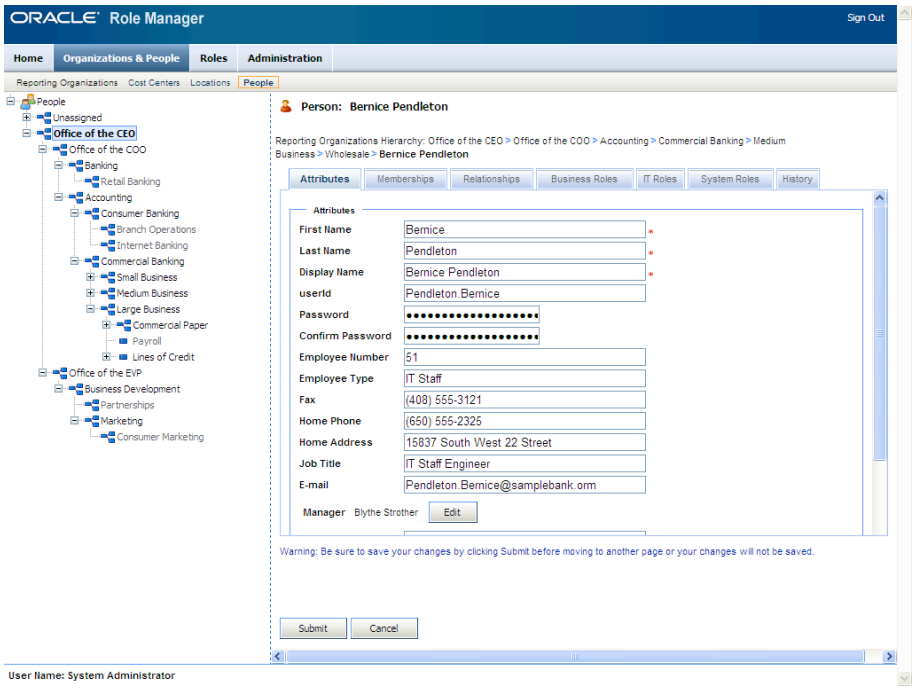

Figure 1. Oracle Role Manager can manage entities across multiple intersecting hierarchies, or polyarchies.

Oracle Role Manager integrates with existing business applications to model multiple organizational structures and the relationships between them as first-class objects. In addition to providing out of the box standard organization structures, Oracle Role Manager can easily be configured to support unique business operation models and relationships. The Oracle Role Manager graphical user interface (GUI) provides multiple views of intersecting business hierarchies and relationships. Examples of common organization models include reporting organization, locations, teams, customers or partners. Additionally, Oracle Role Manager can respond to organizational lifecycle events, ensuring that information updates occur in real-time. These complex relationships become a powerful store of data that role engineers can use to define policies for roles. As common business events occur, policy based role membership is re-calculated and entitlements are granted or revoked according to policy.

Integration Solutions

Oracle Role Manager serves as the role management repository for identity and access management (IAM) systems. It utilizes previous investments in IAM systems and synchronizes roles and polices with entitlements in target systems. For external task assignment integration, such as Business Process Management (BPM) or workflow, other systems can also leverage Oracle Role Manager's contextually derived roles for role resolution in approval workflows.

Oracle Role Manager application suite complements existing IAM infrastructure and fills the role management gap by equipping provisioning systems with role and role membership.

Integration with Identity Provisioning

Oracle Role Manager provides out of the box integration with Oracle Identity Manager (OIM) to initiate provisioning events. The provisioning system extracts user attributes including role and relationship data from Oracle Role Manager using application programming interfaces (APIs). A comprehensive, time-stamped audit trail is maintained of all user provisioning activities. This seamless integration uses role membership and policy to automate and enforce user access to information, applications and systems.

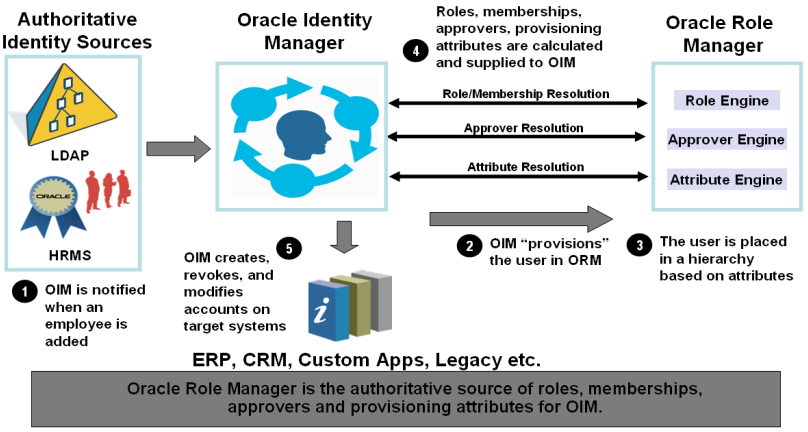

Figure 2. Oracle Role Manager is authoritative for roles while Oracle Identity Manager automates provisioning.

Based on roles and corporate policy, appropriate provisioning workflows can be triggered within OIM. OIM leverages Oracle Role Manager for dynamic provisioning approvals by mapping approver roles to user groups. When all required approvals are in place, OIM triggers provisioning workflows to complete the user provisioning process.

Oracle Role Manger's integration with OIM ensures that:

- Provisioning events occur when role membership changes
- Provisioning events occur when business role and IT role mappings change
- Business events, such as a new hire or transfer, trigger role membership changes and thus provisioning

Similar integration can be achieved with provisioning applications from other vendors as well.

Business Applications - ERP and HR

In addition to ensuring the proper role based access for business applications. Oracle Role Manager can also provide business applications rich role information to better automate transactions. Large enterprises often have complex rules when it comes to routing business transactions for both approval and processing. For example, the rules governing how a

purchase request should be routed through a global purchase organization may be based on the item being purchased, the organization affiliation of the requestor, the type of items and service being purchased, or the vendor of the product. The rules that determine which buyer should handle a particular purchase request and which approvers need to approve the request often rely on hard coded rules in the procurement application.

Oracle Role Manager can also provide extensibility for human resource applications. HR applications historically have limited ability to model complex hierarchies. Management of more advanced concepts such as job role and position may often require deployment of additional modules. Oracle Role Manager's powerful polyarchy and role capabilities can be an attractive option to extend the HR application, offering the additional benefit of providing out-of-the-box consistency between HR roles and IT entitlements.

Another common challenge with application management is granting of emergency access to ensure business continuity. Emergency access is often granted without proper level of control or audit in today's enterprise. Oracle Role Manager allows an organization to model its operational plan in case of emergencies. Employees can be granted roles and access automatically based on a pre-defined configuration during an emergency event.

Via its integration to Oracle Identity Manager, Oracle Role Manager offers out-of-the-box integration with leading business applications such as Oracle E-Business Suite, PeopleSoft, Siebel, SAP and JD Edward, as well as vertical applications such as Oracle Retail Suite and Oracle Clinical Solutions.

Governance, Risk and Compliance (GRC)

Role management should be a critical part of any enterprise GRC solution. Role management is the authoritative source for role and entitlement data and the natural enforcement point for Segregation of Duties (SOD). Since role management is also the authoritative source for "who should have what", the roles and policies in role management application also need to be tightly controlled and attested to on a periodic basis.

Oracle Role Manager captures auditable data for role configuration and role memberships. This data is readily available via the out-of-the-box reporting feature and can be exported to an audit platform such as Oracle GRC Manager as evidence of compliance. Using the attestation feature in Oracle Identity Manager, roles and entitlement memberships can also be re-certified per audit requirements.

Oracle Role Manager can also be integrated with enterprise application control (EAC) products from vendors such as LogicalApps/Oracle, Virsa/SAP and Approva. EAC products excel at deep SOD controls for specific ERP applications. Oracle Role Manage complements EAC application by adding enterprise-wide role SOD across heterogeneous systems, extending EAC coverage to critical IT infrastructure as well as legacy business applications such as mainframe based applications.

CONCLUSION

In today's security-conscious business environment, companies need a sound strategy for building a complete identity and access management infrastructure. Unfortunately, commonly

used applications like directories lack the architectural flexibility to capture and maintain information about people and complex organizational relationships.

Oracle Role Manager is an elegant solution based on standards and patented technology with solid architectural flexibility. Applications across the enterprise can leverage it to ensure accurate and timely management of information about roles, organizations and relationships and entitlements. Oracle Role Manager provides the necessary tools for comprehensive role lifecycle management, allowing users to effectively manage access and resources across the enterprise. The end result: simpler IT administration, lower costs, and reduced security risk.

Oracle Role Manager
Updated June 2009

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com