

# ORACLE ENTITLEMENTS SERVER

## KEY FEATURES

### FEATURES

- Controlled access to software objects, data, and business objects
- Authorization policies to control access to application resources based on user, group, or resource attributes
- Centralized or distributed policy decision points (PDPs)
- Central administrative console (PAP)
- Policy Simulation for "What-if?" type scenarios
- Administrative policy analysis and detailed collection of runtime security metrics
- Incremental distribution of entitlements to PDPs
- Industry leading performance and stability
- Standards support- SOAP, XACML policy export, and XACML request/response protocol, SAML support for identity propagation
- Broad platform support and flexible integration options

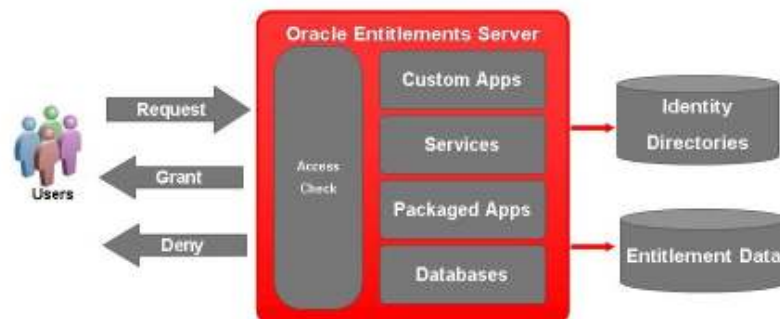
*Oracle Entitlements Server simplifies and externalizes application-level security management by removing security decisions from the applications and creating a unified policy administration system. The solution can manage complex entitlement policies with a stand-alone server or with a distributed approach that enforces policies at the application level. Oracle Entitlements Server enhances business agility, improves IT efficiency, and ensures consistent, transparent, and traceable security policy management.*

### Simplifying Application-Level Security Management

Maintaining application-level security has never been more of a challenge. Applications are more complex, and user communities continue to expand. As the security focus evolves from keeping the bad guys out to letting the good guys in, effective application security is increasingly recognized as essential for improving business efficiency. But each application has its own entitlements—sets of privileges that govern what a user is authorized to do or see. The process of managing a complex set of business entitlements for a diverse ecosystem of applications and users can quickly become a challenging, if not impossible, task.

So how do you ensure secure user access to enterprise applications and resources? How do you manage security policy across multiple application environments throughout the enterprise? How quickly can you respond to pressures to protect privacy and to comply with more regulations regarding information access?

Application security logic is typically hard-coded and maintained by developers within individual applications—an approach that is expensive to manage and difficult to adapt to changing business needs.



**Figure 1. Oracle Entitlements Server externalizes security policy and centralizes its management**

## Oracle Entitlements Server

Oracle Entitlements Server is a fine-grained Entitlements Management solution that externalizes entitlements, removing security decisions from the application. It secures access to application resources, software components, and arbitrary business objects such as customer accounts and patient records. Policies can then be written to specify the users, groups, and roles that can access those resources.

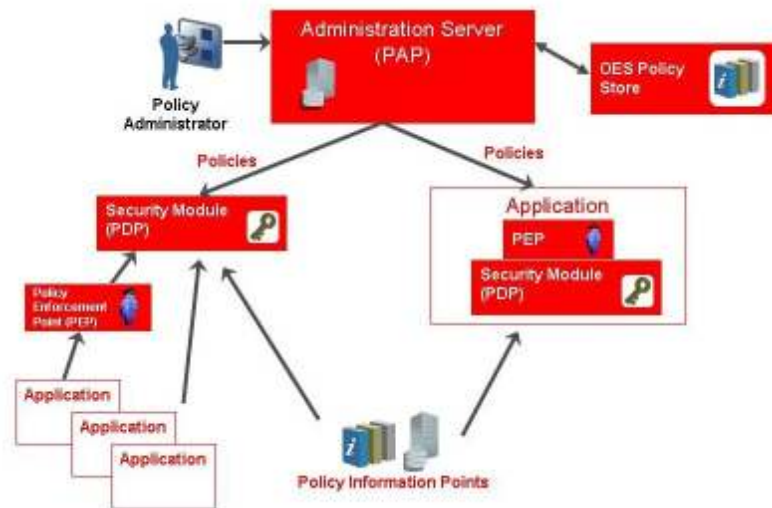


Figure 2. Oracle Entitlements Server architecture

### Policy Administration Point

Authorized administrators can easily define access control policies and security configurations at the Policy Administration Point (PAP). Using a web-based administration console, entitlement policies for all applications can be managed in a single location. The OES policy store can scale to meet the needs of extremely large policy sets required by large cross-organization authorization needs. OES provides the ability to segregate policies according to different applications and organizations and has a delegated administration facility to ensure that administrators can only view or change their authorized policies.

OES can describe any sort of access control policy. For example, “Only salespersons and sales executives can view the monthly revenue reports for their region”. It is also possible to incorporate advanced conditions and external information into an OES policy. For example, “Equity Traders with less than six months of tenure may only trade 85% of their daily limit when the market risk indicators are over 73%”.

The PAP also generates detailed reports on security policies, configurations, and user entitlements across a distributed applications environment. It offers the infrastructure support to distribute policies incrementally through transactions to the Policy Decision Points, and to export Oracle Entitlements Server policies in XACML 2.0 format.

Developers can use Java and Web services APIs to access all Oracle Entitlements

## ORACLE IDENTITY MANAGEMENT PRODUCTS

**Oracle Access Manager** delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

**Oracle Identity Manager** is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

**Oracle Identity Federation** enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

**Oracle Internet Directory** is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

**Oracle Virtual Directory** provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

**Oracle Web Services Manager** is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services.

**Oracle Enterprise Single Sign-On** provides users with unified sign-on and authentication across all their enterprise resources, including desktops, client-server, custom and host-based mainframe applications.

**Oracle Adaptive Access Manager** provides web access real-time fraud detection and multifactor online authentication security for the enterprise.

**Oracle Role Manager** is an authoritative source for role lifecycle management that leverages business policy and organizational data to automate role based provisioning and access control.

**Oracle Entitlements Server** externalizes and centralizes fine-grained authorization policies for enterprise applications and web services.

Server administrative functions.

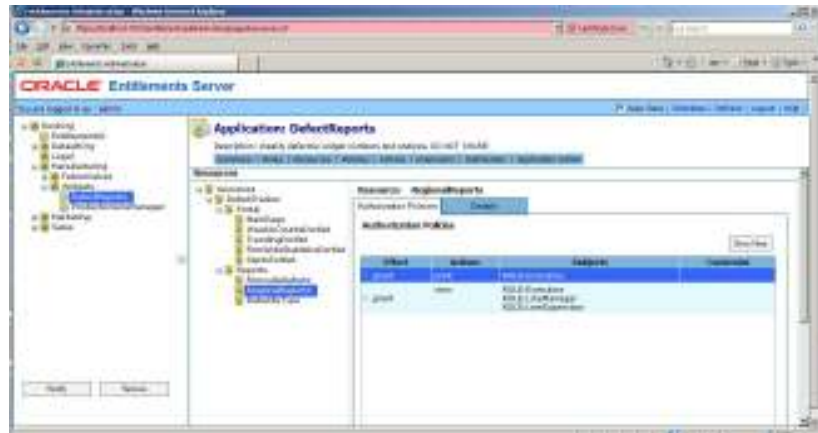


Figure 3. Oracle Entitlements Server administration console

### Policy Decision Points

Oracle Entitlements Server is built on a patented distributed-computing security architecture. Runtime enforcement of entitlements or policies is accomplished by a set of Security Modules (SMs) which act as policy decision points (PDPs). Policy Decision Points are the runtime “engines” for OES which provide the “Grant” or “Deny” decisions on behalf on an application. SMs may be deployed in either of two options:

- **A centralized stand-alone PDP** that can be invoked via standard Web Services, Java RMI or via the Extensible Access Control Markup Language (XACML) 2.0 request/response protocol.
- **A distributed embedded PDP** that plugs into the application container itself where policy is evaluated and enforced locally.

Applications can easily switch between a centralized and distributed strategy by simply changing their configuration. For example, an application may initially use a centralized PDP using web services and eventually embed its own PDP if performance requirements rule out such an architecture.

Security Modules receive their policies via a “push” from the PAP and store a local lightweight cache of policy. This allows them to operate even when the PAP is unavailable. The Security Modules are lightweight in nature and since they must operate in numerous application environments, they require no complex infrastructure such as a database or message queue.

### Policy Information Points

OES Security Modules can integrate with a number of Policy Information Points (PIPs) to retrieve user and group attributes or any entitlements data they require to make an access decision. The SMs can retrieve static user data during user authentication, or they can retrieve dynamic entitlements data during policy evaluation. Dynamic attribute retrieval from relational databases or LDAP stores can be configured by an administrator. In addition, a complete attribute retrieval API is

available for custom needs. The SMs also maintain a fully configurable cache to minimize data retrieval calls to the PIPs.

### **Integrating Policy Management Across the Infrastructure**

Today's applications are spread across various software and service environments, packaged solutions, and a variety of other infrastructure components. It can be difficult and time-consuming to develop and maintain access control policies across a complex network of applications if each environment within the infrastructure has to be individually protected. Oracle Entitlements Server allows you to manage security policy for a wide variety of infrastructure components, integrating them into a single set of centrally managed policies.

### **Contact Us**

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

Copyright © 2008, 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 is it 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. 0408