ORACLE ENTITLEMENTS SERVER

KEY FEATURES

FEATURES

- Rules defined for application access control, role mapping, and delegation
- Policies defined based on user, group, or resource attributes
- Entitlements defined for applications or resources
- Controlled access to software objects, data, and business objects
- Support for Simple Object Access Protocol, XACML policy export, and XACML request/response protocol
- Security Assertion Markup Language support for identity propagation
- Centralized or distributed PDPs
- Central administrative console (PAP)
- Single hierarchy displaying all application resources
- Incremental distribution of entitlements to PDPs
- Administrative policy analysis
- Detailed collection of runtime security metrics
- Pluggable security service provider interfaces
- Authentication, authorization, auditing, credential mapping, and identity propagation
- Broad platform support

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 standalone server or with a distributed approach that embeds information 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 in an application—for managing access. The process of managing a complex set of business entitlements for diverse applications and users can quickly become a challenging, if not impossible, ongoing 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 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.

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 and software components (for example, URLs, Enterprise JavaBeans, JavaServer Pages) and arbitrary business objects (for example, customer accounts, patient records). Policies can then be written to specify the users, groups, and roles that can access those resources.

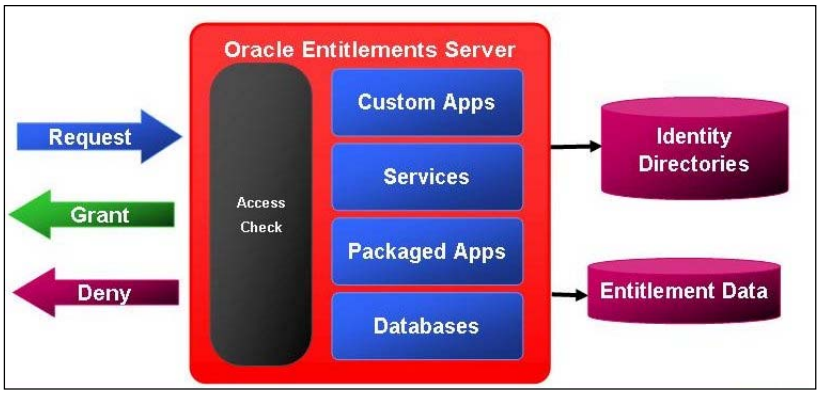

Figure 1: Oracle Entitlements Server externalizes security policy and centralizes its management.

Policy Decision Points

Oracle Entitlements Server is built on patented distributed-computing security architecture. Runtime enforcement of entitlements or policies is accomplished by a set of Security Services Modules (SSMs). The SSMs act as the Policy Decision Points (PDPs), with two deployment options. SSMs can be deployed as one of the following:

- **A central standalone entitlements server,** which can be invoked via Web services or by the Extensible Access Control Markup Language (XACML) 2.0 request/response protocol
- **A distributed set of embedded entitlement PDPs,** which plug into the application container itself, where policy is evaluated and enforced locally and application context can be included in the access decision

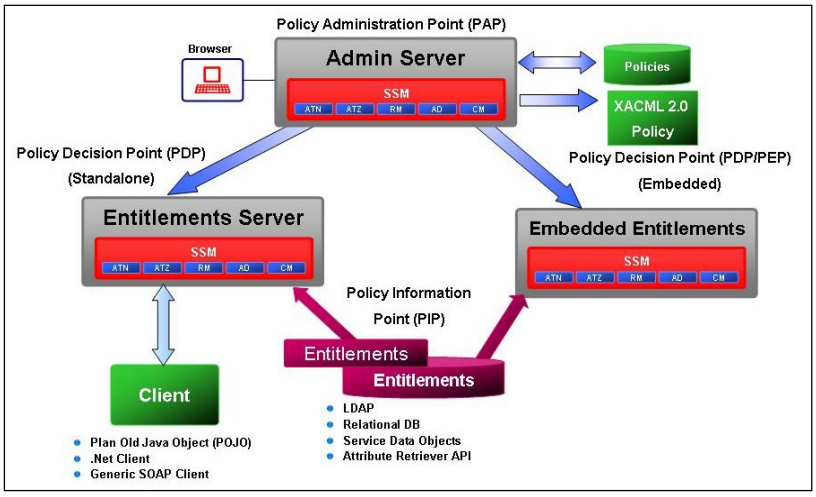

Figure 2: This illustrates the Oracle Entitlements Server functional architecture.

Policy Information Points

The SSMs 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 SSMs can retrieve static user data during user authentication, or

they can retrieve dynamic entitlements data during policy evaluation. The SSMs maintain a fully configurable cache to minimize data retrieval calls to the PIPs.

The SSMs within Oracle Entitlements Server contain a security framework that provides a set of standard security services, enabling them to authenticate, authorize, map roles and credentials, and audit. All runtime security services can be invoked directly through available Java or Web services APIs.

Administrative Server

Authorized administrators can easily define access control policies and security configurations at the Policy Administration Point (PAP) on the administrative server. They can manage policy centrally and delegate administration with the administrative server, which controls the distribution of security policies and configurations to the SSMs.

Administrators can view and centrally manage all security policies and configurations with a console on the administrative server. In addition, a Web-based console allows authorized users to manage entitlements based on user roles within a specific application.

The administrative server generates and issues 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 SSMs and to export Oracle Entitlements Server policies in XACML 2.0 format. Administrators can use the Java and Web services APIs provided to access and complete programming for all Oracle Entitlements Server administrative functions.

Integrating Policy Management across the Infrastructure

Today's applications can be spread across 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.

Supported Infrastructure Environments

Oracle Entitlements Server supports the following environments:

- Oracle WebLogic Server
- IBM WebSphere Application Server
- Microsoft .NET Framework
- Apache Tomcat HTTP Web server
- Java applications

KEY BENEFITS

BENEFITS

- Agility to respond to changing business needs
- Consistent security policy and management
- Transparency through entitlements reporting
- Traceability with integrated runtime access logs for easy auditing
- Improved efficiency for developers

- Documentum Content Server
- Oracle Database
- Microsoft Office SharePoint Server

Platform Support

Oracle Entitlements Server supports a variety of administrative browsers and server platforms, operating systems, and policy storage solutions, including the following:

Platforms and Requirements	
Administrative browser	• Microsoft Internet Explorer 6.0, 7.0
Administrative server platforms	• Oracle WebLogic Server 8.1.6, 9.2.2, 10.0.1 • Apache Tomcat 5.5.25, 5.5.9
Operating systems	• Sun Solaris 8, 9, 10 • IBM AIX 5.3 • Microsoft Windows 2000, 2003 • Red Hat Enterprise Linux 4.0 • Novell SUSE Linux Enterprise Server 9.2, 10
Policy storage solutions	• Oracle Database 9.2.0.5, 10.1.2, 10.2.0.1 • Sybase Adaptive Server Enterprise 12.5.2, 15 • Microsoft SQL Server 2000, 2005 • DataMirror PointBase 5.1 • IBM DB2 Enterprise Server 9.1

Contact Us

For more information about Oracle Entitlements Server, please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

ORACLE