ORACLE
FUSION MIDDLEWARE

An Oracle White Paper
July 2014

# Oracle Entitlements Server and Oracle WebCenter Content

ORACLE

# Protecting Unstructured Data

Content management systems such as Oracle WebCenter, Microsoft Sharepoint, etc., are deployed in many organizations to store a variety of documents and other sensitive content. These systems typically provide basic access control mechanisms, often limited to basic authentication schemes, heavy reliance on AD (in the case of SharePoint), and coarse-grained authorization capabilities that typically rely on folders being mapped to LDAP groups and/or roles (with the typical RBAC role explosion problem).

The below content is mainly based on WebCenter Content; the same set of capabilities is possible across both systems.

## Oracle WebCenter Content (WCC)

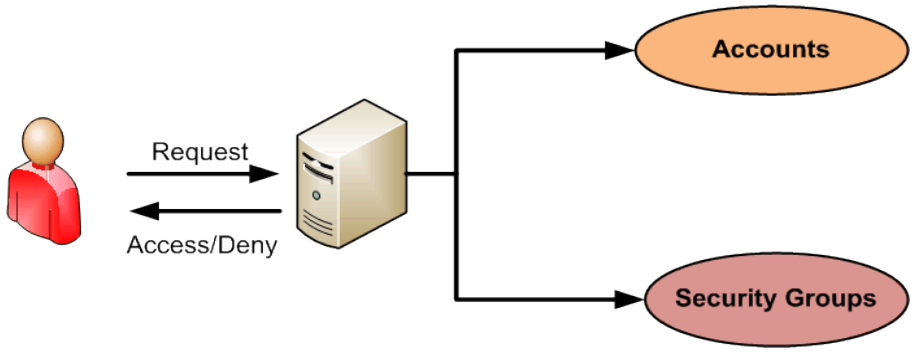
Oracle WebCenter Content (WCC) provides a unified application for delivering document management, web content management, digital asset management, and records and retention management. The suite of products offers a flexible, robust and scalable content management solution that allows employees, customers, and partners to collaborate, contribute and access business content anywhere worldwide. Oracle WebCenter Content helps companies fully maximize the value of their information and intellectual assets by bringing content such as spreadsheets, contracts, marketing materials, CAD drawings, digital assets, records, and catalogs to the Web where they can be efficiently managed.

### WebCenter Access Control

Oracle WebCenter Content helps minimize risk by allowing organizations to control access to content and automate the retention and disposition based on consistent policies. While authenticators (primarily LDAP and RDBMS) play an important role in identifying which groups (or roles) a user belongs to, different strategies are employed by different systems to identify who can access a piece of

content.

The Security framework in Oracle WebCenter Content allows administrators to configure access control strategies to documents by creating




**Security Group(s)**: A classification of files, controlled by permissions (Read, Write, Delete, and Admin) and assigned to roles which in turn are assigned to users and groups

**Accounts**: Specific account permissions assigned to user logins. Accounts provide greater flexibility and granularity in your security structure than security groups alone provide.

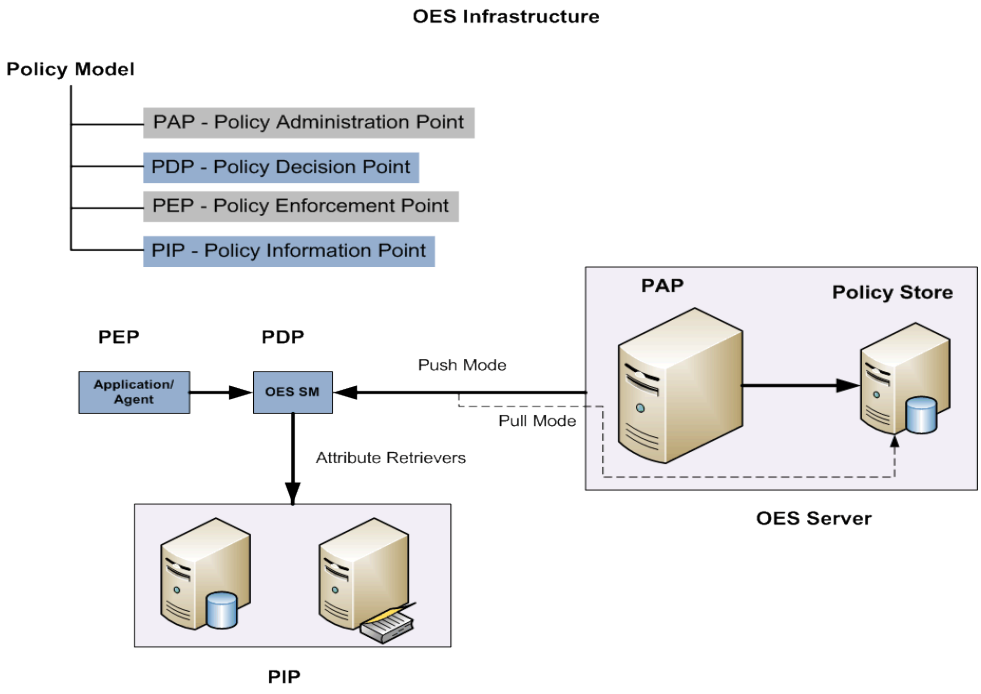
**Note**: When accounts are used, the account becomes the primary permission to satisfy before security group permissions are applied.

## The Problem

1. WebCenter security cannot handle fine-grained authorization models where authorization decision could be on the basis of a combination of document attributes.
2. No authorization provision in Oracle WebCenter Content based on the authentication scheme, environmental factors (e.g., if the jail broken mobile device was used), geographic location, or user performing a particular operation.
3. Doesn't handle complex entitlements-based authorization models. For example, in Oracle WebCenter Content, a document can be tagged as part of a security group "Sensitive" and blanket rules can be created to authorize Read/Edit/Delete privilege on documents tagged with the "Sensitive" security group.
4. The Oracle WebCenter Content security group doesn't address fine-grained access control requirements, for example, allow only "Senior Management Employees" with at least "3" years in the company to READ a "Sensitive"' document tagged with category (via a custom metadata) "Future Product Line-up."
5. They also do not provide a full gamut of entitlements management features including auditing, administration, review, and a comprehensive reusable policy model.
6. Oracle WebCenter Content's native security model is based on group membership, i.e., RBAC (Role Based Access Control) and is not aligned with the growing ABAC (Attribute Based Access Control) model. This results in the need to create security groups to address extensive permutations leading to even greater complexity and administrative burdens.

## The Solution

This section outlines a potential Oracle WebCenter Content implementation, in accordance with the requirements discussed in the previous section. Three essential components are needed to fulfill these requirements: OES connector aka OES Security Module (SM) /OES Client, Oracle Entitlements Server (OES), and Oracle Database.




### OES Defined

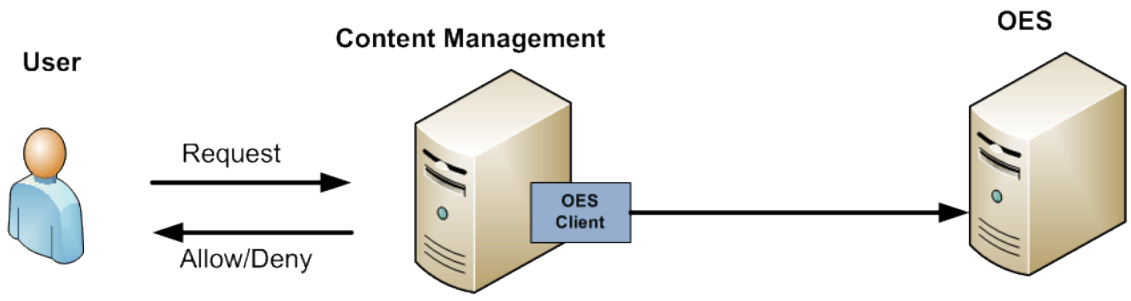
1. OES is a fine-grained entitlements management solution that provides centralized policy management and distributed runtime policy enforcement for applications.

2. OES is made up of two major components and includes the **Entitlements Server** which is a policy administration point and the **Security Modules** (SMs) which are agents that act as a policy enforcement point or a policy decision point or both.
3. OES can serve as the authorization engine for all the content managed by Oracle WebCenter Content using RBAC and ABAC policies.
4. OES can leverage an existing user attribute repository to enforce these policies by supplying user attributes, role membership, group membership, and other relevant attributes to drive coarse-grained and fine-grained access to content in Oracle WebCenter Content.

## Benefits Of OES And WebCenter

The simplified version of deployment architecture diagram is as shown below.

1. The Content Management is integrated with OES infrastructure
2. The OES client, also called the Security Module (SM), is embedded inside the Content Management; this SM provides both
    - Policy Decision Point (PDP) and
    - Policy Enforcement Point (PEP)




3. Corporations would no longer require creating extensive permutations and management of complex Security groups and Accounts in Oracle WebCenter Content.
4. This approach will allow corporations to leverage rich policies that incorporate user, resource, and content metadata attributes in lieu of Oracle WebCenter Content's native model based solely on Security groups and Accounts.
5. WebCenter OES Security Module (SM) is available out of the box to function as "PEP" or as "PDP" or both that provides fine-grained authorization capabilities to resources/content within the native Oracle WebCenter Content environment.
6. The SM can function as a Policy Information Point (PIP) to obtain user attributes from Identity store, any LDAP compliant directory, database, etc.

7. Distributes policies from the Administration Server to the decision endpoints and separates security decision making from application logic.
8. Updates security policies at run time and audits all access decisions and management operations.

## Document Access Control

There are a variety of content types managed by Oracle WebCenter Content including sensitive documents, spreadsheets, contracts, marketing materials, CAD drawings, digital assets, records, and catalogs.

Access rights to various documents should be determined based on:

1. The document classifications
2. End user operations such as search, view, check-in, check-out, delete, etc.
3. Information about the user stored in the corporate identity store
4. How the user authenticated to the Content Management system
5. Any other environmental information

The following are some of the scenarios that corporations may encounter:

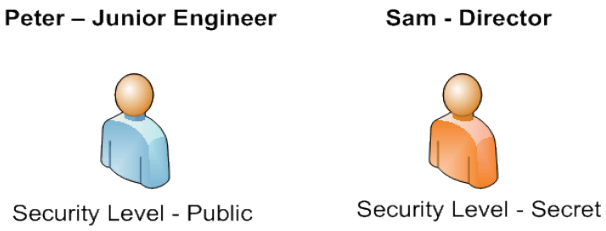
1. Documents marked "Sensitive" (Sensitivity Level) can be viewed / edited only by users in the specific business unit satisfying the clearance level, authentication scheme used, region, department, and a combination of other criterions. This configuration is part of the said document's metadata.
2. Sensitive medical documents like "Healthcare Plans" can only be viewed by users who have subscribed to a given healthcare plan offered by the enterprise.
3. A member of the "Human Resource" business unit cannot access any document in the "Legal" business unit unless authorized by policies.

4. Restrict viewing of content to internal users within the enterprise, only allowing some sensitive pages to non-employees, targeting documents to a geographic location, and with limitations imposed on the extranet content for some customers and suppliers.

## Use Cases

The following is an example of an end-to-end flow of users performing operations on content managed by Oracle WebCenter Content, and access is controlled to the content by authorization enforced by OES. OES Java SM caches the authorization policies received in non-controlled pull mode from the OES Administration server for enhanced performance.

Let's consider company Acme Corporation with the following users:




The documents are tagged with sensitivity/security/ clearance level.

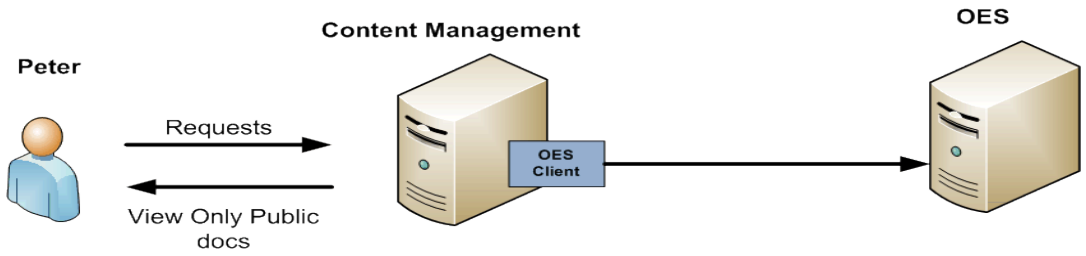
1. Secret - can access "Secret" and "Public" documents
2. Public - can access only "Public" documents
3. Top Secret - can access "Top Secret," "Secret," and "Public" documents

Document Classification:

1. The cost analysis spreadsheet is tagged with the security level "Secret"
2. Technical overview is tagged with security level "Public"
3. New Acquisition - Detailed plan documents are tagged with "Top Secret"

## Use Case 1:

Peter is a junior engineer who works in the Engineering department and is entitled to view only "Public" documents. He is able to perform a search and view only on documents that are marked as "Public." Any documents tagged as not "Public" are hidden.

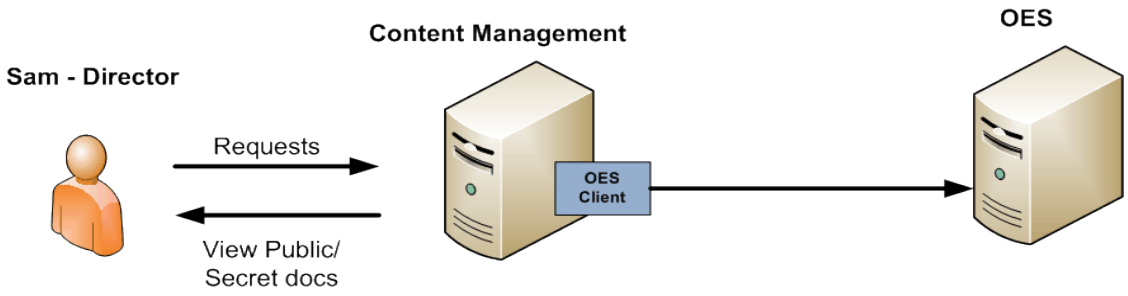



1. Peter requests a search operation to view the list of documents.
2. He logs in to the content system.
3. He is authenticated against an LDAP.
4. In Post authentication, his role is retrieved and passed on to the OES client /Security Module (SM).
5. The OES client applies authorization policies for the request and checks them against Peter's security clearance.
6. Only technical documents are displayed which are marked as "Public."
7. Now, Peter selects a specific document to view.

8. The request is handed over to the OES client which in turn validates and fulfills the request to view documents marked as "Public."

## Use Case 2:

Sam is a director in the Engineering department and is entitled to view documents that are tagged as "Secret." He is able to perform a search, view, check-in, and check-out on documents that are marked both as "Secret" and "Public."

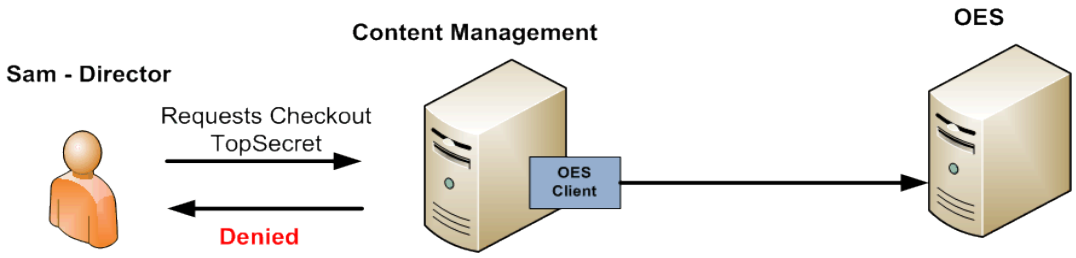



1. Sam requests to perform a check-out operation of a "Secret" document and is authenticated against an LDAP.
2. In Post authentication, the user subject is populated with the required principals including any roles, groups, or user attributes required to perform authorization. This particular user belongs to the "Director" role in LDAP.
3. The request to check-out the content/object type is handed over to the OES client. The requests also consist of user attributes, roles (i.e., Director role), and the requested content/object type.
4. The OES client applies authorization policies for this request and checks whether check-out is allowed or not for Sam.
5. A predefined policy in OES allows the check-out operation to any user who belongs to the "Director" role on the target resource.

6. Based on the authorization decision, which in this case is ALLOW, Sam is granted permission to perform the check-in operation.

## Use Case 3:

Let's take another scenario where Sam tries to access content that is based on enforcing Attribute Based Access Control (ABAC). The steps are as follows:




1. Sam requests to perform a check-out operation on a document tagged as "Top Secret." He is first authenticated against an LDAP.
2. The check-out operation is restricted to users having the "Vice-President" role with a security clearance level of "Top Secret" (tagged via custom metadata) and at least "10" years service in the organization department. Note that, the Content Administrators can tag a document with rules to create a complex policy to target a specific user's population.
3. In Post authentication, the user subject is populated with the required principals including any roles, groups, or user attributes required to perform authorization. Sam belongs to the "Director" role in LDAP.
4. The request to check-out the content/object type is handed over to the OES client. The requests also consist of user attributes, roles (i.e., Director role), and the requested content/object type.
5. The OES client applies authorization policies for this request. User profile attributes (SecurityClearance="Secret", YearsOfService=9) are dynamically retrieved at runtime.

6. A predefined policy in OES allows the check-out operation to any user who has the "Vice President" role and a condition on SecurityClearance="TopSecret" and years of service >=10 on the target resource (content/object type).
7. Based on the authorization decision, which in this case is DENY, due to lack of required years of service, Sam is denied permission to perform the check-out operation on the given content/object type.

## Conclusion

By integrating Oracle WebCenter Content with OES, corporations can provide high performance fine-grained or coarse-grained access control for enterprise content using a consistent approach. Since corporations are able to natively leverage their existing LDAP directories and custom attribute repositories, this integration reduces administrative complexity and development expenses. Using the OES Java SM, corporations can easily employ rich ABAC policies, constructed within XACML, to enforce access to all types of WCC resources. Instead of applying the default Oracle WebCenter Content security model that is rigidly based on Security groups and Accounts, OES will allow administrators to craft intricate access policies that incorporate subject, resource, and environmental attributes without having to provision any new Security groups or Accounts.

OES facilitates security enablement of heterogeneous applications by providing Security Modules that serve as a PEP, PDP, or both. Authorization policy management and runtime enforcement are provided for sensitive applications, databases, containers (such as Java™, .NET), portals, and content management systems (such as Oracle WebCenter and SharePoint), development frameworks, object relational mapping technologies, intermediaries (such as XML gateways and ESB's), web services, and SOA infrastructure. Understanding that an enterprise can be comprised of varying skill sets, development languages, protocols, and frameworks, OES provides out-of-the-box SMs tailored for different environments. Using industry protocols such as SOAP, REST, and XACML, Oracle SMs can seamlessly operate with Java and .NET applications, and be deployed within popular containers such as

Tomcat, JBoss, or WebLogic. Oracle SMs enable security logic that evaluates access to be abstracted from applications and allow developers to focus on business logic expediting policy enforcement and reducing customizations. With SMs that can act as a PEP, PDP, or both, corporations have greater flexibility in their architectural approach to balance reusability, performance, and failover.

With OES and Oracle WebCenter Content integration, corporations can reduce development costs, make use of their existing identity infrastructure, and service unprovisioned consumers without system redesign or revision to current administrative practices. Additionally, companies can now enforce access control to resources based on "Is user ‘U’ allowed to perform action ‘A’ on content ‘C’ under the condition(s) "T" ”.

OES and WebCenter Content
July 2014
Author: Derick Leo
Contributors: Anant Kadam, Priscilla Lee

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

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



**Hardware and Software, Engineered to Work Together**