

Securing SharePoint with Oracle Entitlements Server

Oracle Entitlements Server, an industry-leading fine-grained authorization solution, enables enterprises to efficiently and securely manage SharePoint portal environments, thereby reducing administrative costs, managing compliance risks, and providing more and better services to employees, partners, and customers.

Introduction

Due to its ease of initial setup and low cost, Microsoft Office SharePoint Server has rapidly moved beyond its intended purpose as a departmental collaboration tool to become a critical business application for many enterprises. As its use and influence spread across a company, content that represents business-sensitive or regulated data is bound to find its way to an ever-widening audience.

IT organizations are now facing intense pressure to control and secure SharePoint deployments across their infrastructures. However, the SharePoint product does not provide comprehensive or efficient ways to ensure that only the right people have access to the right content. The result is that many IT organizations are the victims of SharePoint's success in the business as administrative costs rise, security risks proliferate, and exposure to compliance violations widens. In order to meet these challenges and continue to use SharePoint as a business collaboration platform, enterprises must adopt more powerful tools to protect sensitive content.

SharePoint Challenges

There are three major challenges that companies face in securing SharePoint environments:

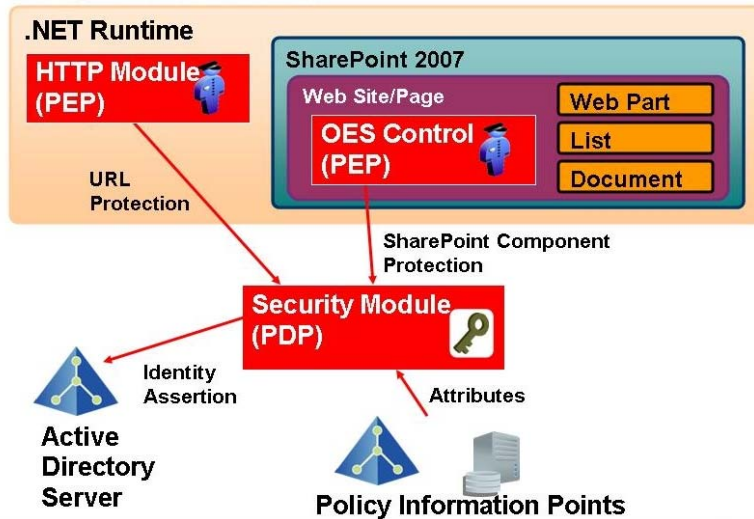
1. **Managing Enterprise deployments.** In SharePoint, each site is typically administered as a separate island, making it difficult to put in place policy to support company or regulatory requirements. Individual site administrators end up making independent decisions about who should have access to sensitive content. The result is that there is no way to provide consistent enforcement of enterprise controls or risk management policies. When it comes time to audit who has access to what for purposes of compliance reporting, this work must be done manually.
2. **Managing the access rights of large numbers of users.** As SharePoint portals grow in importance to the business, so grows the user population that requires access. SharePoint native security requires assigning permissions directly to users or groups, which quickly becomes time-consuming and error-prone for large numbers of users. The group management function in SharePoint is not a robust enterprise role management capability, and therefore cannot enforce least-privilege access based upon the business role of users. The result is that users are more likely to be given access to pre-set groups of permissions, leading to security and compliance risks.
3. **Enforcing access at a granular level.** SharePoint sets permissions in broad buckets, which is fine, for example, when all of the documents in a site are of the same type and importance. But when documents, specific transactions, custom content, or data from external sources need to be protected individually – a requirement for any enterprise information portal – SharePoint is simply not up to the task.

Oracle Entitlements Server

Oracle Entitlements Server (OES) is a **Fine-Grained Entitlements Management Solution** that provides centralized policy management and distributed runtime policy enforcement for applications. Oracle Entitlements Server is made up of two major components. The administration application acts as the policy administration point (PAP) and is used to manage policy, configuration, roles, and entitlements. The second component comprises one or more Security Modules (SM), which evaluate

fine-grained access control policies at the policy decision point (PDP) and enforce them at the policy enforcement point (PEP).

OES delivers a dedicated Policy Enforcement Point and Security Module for SharePoint out-of-the-box, which is shown in the below diagram. Each time a SharePoint resource is requested – be it a web page, document, transaction, list item, or Web part – the PEP intercepts the request and lets the Security Module determine whether the specific user in question is authorized to make that request.



This pluggable service framework inside the Security Module provides a powerful integration platform for connecting Oracle Entitlements Server to Web SSO, identity management, user provisioning, and other security products in the business.

Meeting SharePoint Challenges with Oracle Entitlements Server

Oracle Entitlement Server enables you to:

1. **Protect SharePoint in-depth.** OES provides fine-grained control over SharePoint resources down to the document, transaction, and data levels. OES enforces complex policies that are based on user and resource context, ensuring access is granted according to business rules.
2. **Enforce policy across multiple SharePoint portals.** OES serves as a centralized “traffic cop” in real-time by runtime evaluation and enforcement of policy. Consistency and adherence to enterprise security, risk management, and compliance policies are pro-actively managed.
3. **Establish a centrally managed repository.** SharePoint Security Administrators can quickly manage policy across all sites and sub-sites within the SharePoint environment, and delegate those responsibilities when appropriate.
4. **Secure SharePoint for all users.** OES integrates with your current identity, role, and entitlements data sources to ensure the right content goes to the right user, whether an employee, a contractor, a partner, or a customer.

How to Learn More

Oracle Entitlements Server is a part of Oracle’s industry-leading Identity Management suite of best-of-breed products. Please visit www.oracle.com/identity for more information.

Copyright 2008, Oracle. 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.