ORACLE

FUSION MIDDLEWARE
IDENTITY AND ACCESS
MANAGEMENT SUITE

An Oracle White Paper
June 2012

Securing Microsoft Office SharePoint Server (MOSS) with Oracle Entitlements Server 11gr2

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Introduction

The widespread use of SharePoint within the organization has led to increasing demands to incorporate it into an enterprise wide access management environment. This provides both user and administrator efficiencies while enforcing a consistent level of web access security. The Oracle Entitlements Server (OES) 11gr2 Microsoft Office SharePoint Server (MOSS) Security Module (SM) extends native SharePoint authorization capabilities by providing standards based fine grained authorization to sensitive SharePoint documents and content while providing a robust framework for regulated access.

Benefits and Features of the OES MOSS SM 11g2

- Extends support for standards based Attribute Based Access Control (ABAC) and dynamic Role Based Access Control (RBAC) policies for fine grained access to SharePoint resources
- Easily allows usage of both user identity information and SharePoint document metadata in a rules based, constraint driven framework while supporting the notion of XACML style effects (Deny/Permit) and obligations for fine grained access decisions to SharePoint documents and content
- Allows retrieval of user identity and profile information from multiple stores and user repositories allowing extending of fine grained access to SharePoint resources to additional non Active Directory based employee groups as well as users such as customers, contractors or partners
- Provides tooling for discovery of SharePoint resources in a hierarchal fashion for modeling and enforcement of fine grained access decisions
- Consolidates access tracking and reporting for audit and compliance efforts
- Seamlessly integrates with Oracle Access Manager to provide enterprise wide user experience and efficiency via SSO and password services
- Supports both MOSS 2007 as well as MOSS 2010 deployments

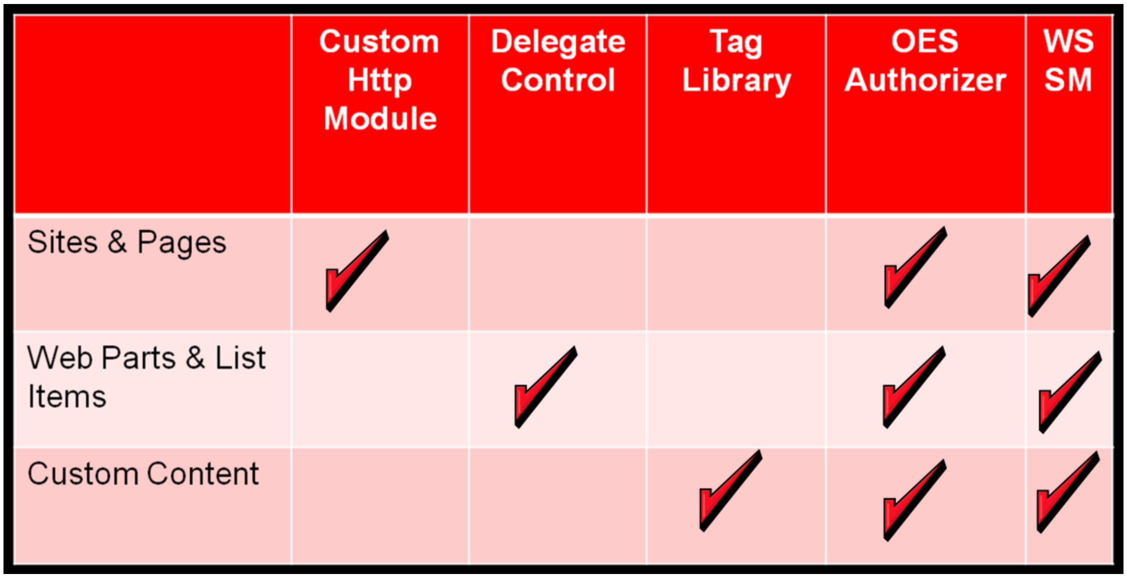
How it works

The Oracle Entitlements Server (OES) 11gr2 Microsoft Office Sharepoint Server (MOSS) Security Module (SM) provides fine-grained authorization capabilities to MOSS resources by leveraging the basic design provided by ASP.NET in intercepting requests and delegating control over various events that get triggered when different MOSS components are accessed.

The OES 11gr2 MOSS SM consists of the following components:

- CustomHTTPModule: Access requests to MOSS web sites and web pages are intercepted by this component which enforces OES access control by page redirection.
- OES Delegate Control: Access requests to MOSS list items, web parts and the navigation bar are protected by this_component which enforces OES access control by page reloading.
- OES Custom Tag Library : Sensitive content on MOSS web pages is wrapped within OES Custom tags. Access requests to protected content trigger the tags and OES access control is subsequently enforced by page reloading.
- OES Authorizer: The_OES Authorizer is the single point of contact with the OES Web Services Security Module (WS SM) for fetching all authorization decisions from it. The OES Authorizer fetches the configuration parameters from the MOSS web application settings and

creates authorization service requests using these parameters. All MOSS SM components hold a reference to the shared instance of this authorizer and use it to get individual as well as bulk decisions from it



	Custom Http Module	Delegate Control	Tag Library	OES Authorizer	WS SM
Sites & Pages	✓			✓	✓
Web Parts & List Items		✓		✓	✓
Custom Content			✓	✓	✓

Figure 1: Protecting MOSS Components with the OES 11gr2 MOSS SM

All OES MOSS SM components rely on the OES Web Services SM which acts as the Policy Decision Point (PDP). The OES Authorizer serves as the shared conduit between the OES MOSS SM components and the OES Web Services SM PDP. The OES Web Services SM makes the authorization decision and sends the decision back to the MOSS SM components based on a centrally configured, hierarchal and standards based policy framework available in the OES Administration Server. These policies are rules based, identity centric and constraints driven and can subscribe to ABAC, RBAC, dynamic RBAC and XACML style standards providing fine grained access to MOSS resources.

Protecting MOSS Resources using the OES MOSS SM

Web Sites & Web Pages

Microsoft Office SharePoint Server comes with a main MOSS Web Site within which Administrators can create sub sites. These sub sites can appear on the top navigation bar or on the side navigation bar or as links on any other pages in MOSS. All these web sites have their own unique URLs. As an example the MOSS SM can be used to secure web sites in MOSS denoting each department in the company such that contractors (whose identities are not stored in the corporate Active Directory) working temporarily for development projects in the company are given access to this portal but should not see web sites like those for the Management and Finance departments. However they can access other sites like Development and QA.

All the MOSS web sites are composed of one or more pages. For each web site there is a default page which can be customized by the user. There could be additional pages with different content in the web sites. For example if the Sales Team in an organization publishes quarterly sales information on a specific page in the Sales sub site on the company portal then the MOSS SM can ensure that this information should only be shown to the Management team and select groups within the Sales department.

The Custom HTTP module component of the MOSS SM is used to protect web sites & web pages. It is registered with one of the event handlers (BeginRequest or PreRequestHandlerExecute) such that any request for MOSS web sites or web pages will go through the Custom HTTP module and be passed to the OESAuthorizer. The OES Authorizer invokes the OES Web Services SM and gets an authorization decision from it. The authorization decision is based on a centrally configured OES policy. Based on the authorization decision, access is then permitted or denied to the user.

Web Parts & List Items

Web Parts in MOSS are like portlets that display content within pages. A user defined MOSS Page can be divided into multiple sections, each containing different content. So a web page can contain one or more web parts. As an example if the Admin Secretary in the department creates events and agenda for the management offsite in the management group's website in a specific web part then the MOSS SM can ensure that this web part should only be displayed to the management team and a user should be only be able to see those web parts for which the user is granted view access.

Lists in MOSS display a collection of items within a web part on a page. There are different types of lists in MOSS – Document Libraries, Task Lists, Announcement Lists etc. These lists can be seen via the Site Content and Structure page for the main site or sub sites or via menu items in the left or top navigation. Each list consists of individual list items. For example in an organization if the management team maintains all project documents that they work within a document list then the MOSS SM can ensure that certain sensitive documents will not be displayed to all users. So when such users view the list then those documents will not be shown to them.

The protection of web parts and list items is done via the OES Delegate Control component. When a page containing list items is to be displayed then the OES control on the page sends the request to OES via the OES Authorizer and gets bulk access decisions from OES for the user for each of the list items. In this case there are two sets of access decisions on the list items- from MOSS and the other from OES. Based on a comparison, the OES Delegate control toggles the MOSS permissions on list items to be consistent with OES decision. Upon page reload, only the list items that the user has been granted permission from OES are shown on the page. This is also the case where the OES access decision overwrites the MOSS permission.

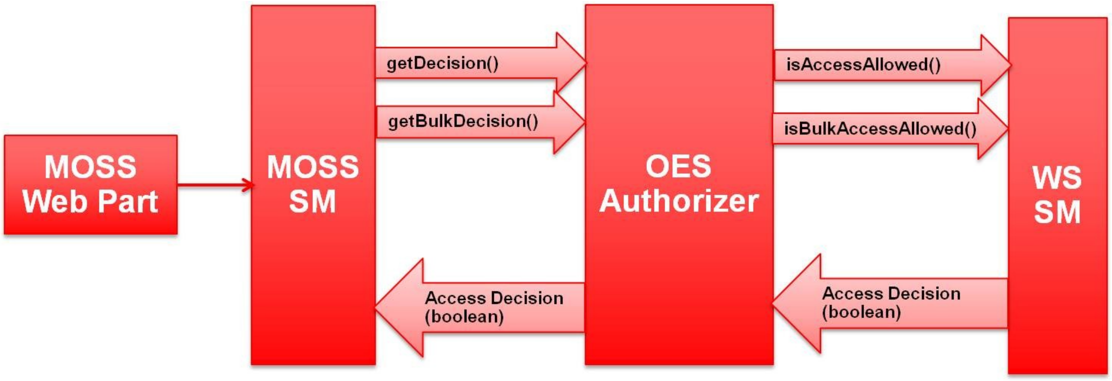


Figure 2: Protecting MOSS Web Parts with OES SM 11gr2

Custom Content Pages

MOSS allows admin users to publish custom content pages (which may not include any of the existing web parts) in any web/list. The custom content pages (which are essentially ASPX pages) may have some sensitive information published on them which has to be hidden from a certain set of users. For example an organization has published its financial statistics for the last quarter on a custom content page and wants only people with managerial rights to see some of the finer details of the report. Sensitive information that needs to be protected can be enclosed within custom ASP tags corresponding to the OES custom tag library. The tag library invokes OES Authorizer and fetches the access decision for the current user based on which that content will be shown only to users granted access by OES.

Navigation Bar Items

The Navigation Bar on MOSS site pages can be used to navigate to different pages or content of a MOSS site. Some sub sites, pages and content may not be allowed to be accessed by certain set of users. For example let's say that an organization has created a sub site to publish HR processes and status which should be accessible to the HR department only. The OES MOSS SM components can be configured such that based on policy the navigation element to this sub site on the Navigation Bar will only appear if the current login user works in the HR department and all other users will not see this element leading to this sub site on the Navigation Bar at all.

Conclusion

The Oracle Entitlements Server 11gr2 Microsoft Office SharePoint Server (MOSS) Security Module (SM) extends native SharePoint authorization capabilities by providing an enterprise wide standards based solution for fine grained authorization to sensitive SharePoint documents and content. It seamlessly integrates with the broad and comprehensive suite of Oracle Identity and Access Management products to further provide enterprise wide user experience and efficiency while meeting an organization's internal and external compliance needs.

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

Securing Microsoft Office SharePoint Server
(MOSS) with Oracle Entitlements Server 11gr2
June 2012
Author: Kanishk Mahajan

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

Hardware and Software, Engineered to Work Together