

ORACLE ACCESS MANAGER INTEGRATION WITH LAYER 7 SECURESPAN

KEY FEATURES

- Enables Oracle Access Manager to seamlessly manage access control for both Web and Web services applications.
- Faster deployment: single-sign on deployed quickly to Web-services applications without costly and time consuming programming.
- Simplified management.: SecureSpan Gateway / Bridge completely and transparently automates flow of SSO token cookies between Oracle Access Manager and client applications.
- Consistent security: SecureSpan Gateway enforces fine-grained authorization rules, providing end to end protection of Web services.

Platform-independent XML/Web services is rapidly becoming the technology of choice for integrating applications. But many business processes traverse multiple back-end systems, presenting significant authentication challenges in a Web services environment. Oracle and Layer 7 Technologies provide a unique solution for addressing these issues by seamlessly and cost-effectively extending the benefits of Web single sign-on to Web services implementations.

Introduction

XML-based Web services provide powerful technology for reusing shared application logic across diverse business processes. Web services are based on a variety of specifications designed to ensure application-level interoperability regardless of differences in platforms, operating systems or development environments. This flexibility has helped fuel the rapid increase in Web services projects across a broad range of application integrations, business processes and industry verticals.

Like other existing applications, Web services leverage identity-based access control as a key component of an overall security process. However, unlike more traditional Web applications, Web services present some unique identity management challenges that can lead to both significant technical and deployment cost issues.

Access Control Challenges in Web Services

Business processes using Web services often need to traverse multiple departments, business units, and partners; each residing in separate security domains with independent preferences, capabilities, and requirements. This distributed and sometimes heterogeneous nature of Web service integration complicates access control significantly. The same client application may have to present distinct credentials to multiple services in a composite business process. Each time the client requests information from one of the services it has to re-authenticate, slowing performance and adding latency to the transactions.

In Web-based applications this is addressed using a Single Sign-On system (SSO) to streamline authentication across heterogeneous services and persist sessions to help avoid multiple authentications. However this approach relies on several built-in capabilities in Web browsers which can't deal with Web services environments, resulting in costly and complex custom software to replicate similar capabilities.

A Solution for Single Sign-On in Web Services

For human users accessing multiple back-end applications through a browser, SSO products work well for providing one-time login to backend systems. Using Single Sign-on, a user can avoid having to remember multiple passwords to re-authenticate to each application and is insulated from the complex interactions between Web browsers, SSO systems and servers required to facilitate SSO.

The secret to why single sign-on works well in Web applications is because Web browsers support both cookie caching and Web address redirects. Session tokens generated by an SSO product like Oracle Access Manager can be cached by a browser and presented to each back-end application exposed through the portal without the end user having to re-enter authentication credentials. The end user only needs to login one time to bootstrap the process. This same requirement exists for Web services where client applications also need to access multiple back-end Web services without re-authenticating. Ideally this would be accomplished using the same familiar SSO infrastructure organizations may have in place for their Web needs.

Layer 7's SecureSpan product line offers enterprises a first of its kind ability to reuse existing SSO infrastructure for Web services. The SecureSpan Gateway is an Web services firewall appliance designed to provide centralized protection between application servers exposing a Web service and client applications residing in different identity, security or middleware domains who request access to these services.

The SecureSpan Gateway implements run-time access control for Web services requests by forwarding client credentials to Oracle Access Manager for authentication, much like a standard Web application. This serves two purposes. First, it allows the SecureSpan Gateway to delegate identity and authentication decisions to access policies defined and managed in Oracle Access Manager. Secondly, it allows Oracle Access Manager authentication and session tokens (cookies or SAML assertions) to be passed using Web services protocols to a Web services client application. All identity management tasks (provisioning, revocation and profile management) are assumed by Oracle Access Manager for all transactions, both Web and Web services.

Addressing Client-Side Needs

However, delegating authentication to Oracle Access Manager is only the first step to provide client application access via SSO since, unlike the Web, Web services have no browsers to cache session tokens and provide address redirects. The SecureSpan Bridge fills this gap by performing a similar function to a Web browser in a Web services transaction: automatically negotiating cryptographic and security session parameters; packaging and transmitting client credentials in a WS* specification compliant format; signing messages and message parts using a digital certificate it provisions; and most critically for SSO, caching Oracle Access Manager session cookie tokens passed to it by the SecureSpan Gateway, embedding these tokens in SOAP messages, bypassing the need for subsequent re-

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Identity Management is an integrated, scalable and robust identity management infrastructure that includes LDAP V3 directory services, directory synchronization, access management and a certificate authority.

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

LAYER 7 WEB SERVICES FIREWALLING PRODUCTS

The SecureSpan™ Gateway is a Web services firewall appliance designed to protect interactions between client and services residing in different identity, security or middleware domains.

The SecureSpan™ Bridge is an XML VPN client for enabling fast and flexible partner or portal connectivity in XML and Web services environments.

authentication. The Bridge performs all of these tasks automatically without complex programming on either the client application or Web service.

This combination of Oracle Identity Management and Layer 7's SecureSpan product line provides a complete Web services SSO solution, addressing both services and clients in an easy to deploy, easy to manage fashion.

Key Features

Key features of the combined Layer 7 SecureSpan and Oracle Identity Management products include:

- **Rapid Deployment.** Single-sign on deployed quickly to Web-services applications using commercial off the shelf products with no programming required.
- **Centralized Control.** Oracle Access Manager used to seamlessly manage identity-based access control for both Web and Web services applications.
- **Simplified Management.** SecureSpan Gateway / Bridge completely and transparently automates flow of SSO token cookies between Oracle Access Manager and client applications.
- **Consistent Security.** SecureSpan Gateway enforces fine-grained run-time authorization rules on every message, providing end to end protection of Web services.

Joint Oracle Layer 7 Value Proposition

Oracle Access Manager provides the industry's most comprehensive solution with integrated identity administration, unified workflow, single sign-on, centralized policy management and a compliance-reporting framework. It is the industry's only solution, which provides seamless integration with Oracle Fusion family of products as well as a number of third-party products and platforms.

The combination of Layer 7's SecureSpan Gateway, SecureSpan Bridge and Oracle Access Manager offers a unique ability to deliver enterprises SSO for securing their Web services implementations. For Oracle Identity Management customers, SecureSpan delivers this value to enterprises using their existing Oracle Access Manager-based Web SSO infrastructure, saving them both implementation time and expense.

Contact Information

For more information contact Layer 7 Technologies by telephone at 1-800-681-9377 or by email at info@layer7tech.com. For more information on Oracle Identity Management solutions, visit www.oracle.com/identity

Disclaimer: When Oracle conducts partner integration and testing, we verify only that the software integration functions according to the partner's proposed integration plan, and that it makes appropriate use of Oracle components and integration technologies in the environment specified in the published Integration Datasheet. Customers are solely responsible for the selection of all third-party software, including any integration software, used in conjunction with Oracle Identity Management and for the results of such use.