



ORACLE[®] ACCESS MANAGER

LEGACY-TO-OAM ZERO-DOWNTIME SSO MIGRATION

BY OTECIA INTERNATIONAL

Content

1. Solution Overview	3
1.1. Challenges	3
1.2. Objectives	4
1.3. Scope	4
1.4. Results	4
2. About Otecia International	5

1. Solution Overview

Otecia International, a leading global provider of Identity Management solutions, has developed a proven methodology to let customers quickly, easily, and safely migrate from legacy SSO to the Oracle Access Manager (OAM) SSO with *zero-downtime* without disruption in service or availability. With the *zero-downtime migration* capability, Otecia International brings the advantages of rapid enterprise SSO deployment to a wider range of organizations by making it easier to configure and administer highly available industry standards-based enterprise SSO infrastructure.

Upon initial user authentication, the solution authentication and authorization plug-ins intercept and migrate user credentials to OAM format. On subsequent user authentication requests, the solution validates successful credential migration and transparently allows users to proceed accessing OAM-protected applications, without negatively affecting end-users experience.

The solution requires minimal or no modifications to existing applications that are part of the legacy SSO.

1.1. Challenges

In today's world of compliance regulations, organizations are required to protect sensitive data within enterprise applications. Over time, various security policies have been enacted to protect applications. For example, login processes have been put in place to secure the user access, yet access control to the applications has often been integrated within the application logic and separate data stored have been put in place to store credentials. Users have been required to regularly update passwords for each application, yet accommodating such requirements have resulted in the proliferation of insecure practices (writing down passwords, reuse easy-to-guess password combinations, or sharing passwords among users).

In a typical scenario, legacy SSO solutions rely on custom-built code to be integrated within each application to enable reduced sign-on capabilities. Other implementations of legacy SSO rely on client-server software to allow users to launch non-SSO enabled applications via a centralized SSO infrastructure, acting as a repository for application-specific user credentials.

The following challenges have been identified with the continued use of legacy SSO systems:

- Climbing maintenance cost for non-standard custom-built Single Sign-On framework
- Increased security risk from storing user account passwords in decryptable format.
- High deployment and integration cost for new applications
- Lack of high-availability with legacy SSO implementations

1.2. Objectives

- Migrate users and customers to a more secure industry-standard SSO platform such as Oracle Access Manager
- Spare customers and employees the hassle of establishing new credentials
- Zero migration down-time for customers and employees
- Save costs by reducing help desk support calls
- Scalable solution supporting over one million customers and employees
- Built-in high-availability solution

1.3. Scope

The solution is built around the Oracle Access Manager foundation to enable web single sign-on across all internet and intranet applications. It includes OAM plug-ins to migrate credentials from a legacy SSO to OAM.

The solution serves as an enterprise authentication framework that will work for all applications, including legacy reduced sign-on applications, providing unified authentication processes (including form-based credentials and PKI/digital certificates).

The enterprise security framework can optionally accommodate advanced authentication features such as:

- Concurrent login detection enforcement, allowing one session per user with grace period notification
- Federated Access
- Persistent cookie-based authentication

The solution will ensure that existing users with legacy authentication credentials will find the transition to the OAM SSO environment transparent. Legacy persistent cookie-based credentials will continue to work and will be automatically replaced with SSO credentials.

1.4. Results

The operating cost of the migrated infrastructure is significantly lower than the original legacy SSO infrastructure. Existing customers have commented on the reliability of the solution.

End user satisfaction and productivity is greatly improved, while enacting more stringent enterprise security policies to minimize wild-spread insecure practices. Migration to an enterprise single sign-on such as the industry standards-based OAM solution provides for providing centralized management of application authentication, authorization, and auditing to meet compliance regulations requirements. Support costs are reduced by eliminating requirements to track and change multiple user passwords and troubleshooting password management related issues.

2. About Otecia International

Otecia International is a leading provider of expert consulting services for Identity and Security E-Business enterprise software solutions. Founded in 2004 and headquartered in Washington, DC, Otecia International excels in helping clients across the globe with strengthening enterprise security, lowering operating costs, and improving user productivity. Its team of experts brings exceptional understanding of the technology, adhering to the best industry practices.

For more information about our services, please visit our website at <http://www.otecia.com>
Otecia International and Otecia Consulting are trademarks of Otecia International, Inc.

© 2008 Otecia International, Inc. All rights reserved.