Enabling Single Sign-On from Desktop to Cloud for the Extended Enterprise

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Oracle
January 2011
Table of Contents

Executive Summary ........................................................................................................................................1
The Cloud Opportunity ................................................................................................................................1
Weighing the Risks ........................................................................................................................................2
  Single Sign-on From Anywhere, To Anywhere ..................................................................................3
  Simplifying User Management ............................................................................................................3
  Key Benefits ...........................................................................................................................................4
EMA Perspective ........................................................................................................................................4
About Oracle ................................................................................................................................................5
About Oracle Identity Management ........................................................................................................5
Enabling Single Sign-On from Desktop to Cloud for the Extended Enterprise

Executive Summary
With all the pressure on today’s IT not only to perform but to expand capability while containing costs, organizations are increasingly turning to third-party resources such as Cloud computing, SaaS and hosted technology services. Businesses will want access to these services to be as seamless as access to existing internal resources—but there are implications to this trend that the enterprise should be aware of in order to achieve this expansion safely. When access to external resources is in control of a third party, organizations may not be aware of the implications for their own sensitive information. Single sign-on is often adopted as a solution for making access to a wide range of disparate resources as seamless as possible, but not all Single Sign-On (SSO) solutions are created equal, and not all may give the enterprise the level of control it needs over issues such as changes in employee roles or terminations.

In this report, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts explore these issues and the value of enterprise single sign-on. With its recent acquisition of Passlogix, Oracle expands the range of identity management solutions into a realm that extends the flexibility of SSO throughout the enterprise. Today, this flexibility enables businesses to extend SSO just as readily to Cloud, SaaS and third-party resources, giving enterprises a tool for taking control of access to both internal and external IT assets, and adapting seamless authentication to the business, rather than forcing the business to adapt to external requirements that may be out of step with business priorities.

The Cloud Opportunity
Enterprises today are adopting Cloud-based and hosted solutions for a number of business priorities. Traditionally, fields such as Customer Relationship Management (CRM) dominated this approach, but today organizations are turning to hosted solutions and Software-as-a-Service (SaaS) for everything from personal productivity applications to business intelligence.

The advantages of the hosted approach are many. In exchange for an ongoing fee, hosted services relieve organizations of much of the burden of on-premise business systems management, including implementation, deployment and maintenance. They help shift IT expenses from the capital to the operational side of the balance sheet, freeing organizations to invest in capabilities more central to strategic priorities. Already, hosted SaaS alternatives have demonstrated aspects of the success that many expect from the promise of Cloud computing—arguably the “ultimate” hosted experience.

Ideally, enterprises would like the experience of SaaS and hosted technologies to be seamlessly identical to—or better than—internal resources.

This means an approach to single sign-on that extends from within the enterprise to third-party resources. The transparency of the approach has high appeal, but in order to make the right choice, businesses must understand the impact of third-party SaaS and Cloud computing alternatives on secure access management, and how these issues should influence their choice of an SSO solution.
Weighing the Risks

Hosted services connect with large numbers of customers. This means that the provider may be highly motivated to enforce a consistent policy across all customers, which may be difficult to adapt to individual needs. Organizations that have developed their own policy regarding the sharing of access credentials may find this problematic. They may be required to adapt their policy to that of the provider, rather than the other way around. This could create problems if, for example, the provider shares user information with partners or other resources. Without visibility into such a situation, would the customer know if their employees’ credentials had been shared?

This raises the issue of access audit. Organizations may be faced with regulatory or other requirements for maintaining auditable reporting of activity such as IT resource access. Not all third-party services may provide this capability. Fewer still may provide it in a way that truly supports compliance requirements.

Another complication of introducing hosted offerings and SaaS into the enterprise is that access to important third-party resources may be vulnerable to risks beyond enterprise control. Personnel may access sensitive SaaS-based resources such as customer records from a home computer that may be infected with malware such as spyware or keyloggers. Organizations may have little or no control over endpoint security measures outside the business that would reduce exposure to these risks.

User account lifecycle management poses another concern. When users of resources within the enterprise move, change roles or leave the company, the business often manages these changes internally—but are these changes also made in SaaS or third-party resources? If an employee is terminated for cause, how confident is the business that such an individual is unable to access SaaS-based customer account information from their home computer?

These are some of the risks that can be prevented by single sign-on tools that can be extended to SaaS, Cloud, or other third-party resources. Single sign-on technologies can help close these gaps while delivering a seamless experience that enables personnel to access third-party resources just as if they were any other enterprise resource to which the user has access at initial logon.

Many approaches to SSO, however, require a business to adapt to them. What about techniques that adapt to the business?

Oracle Enterprise Single Sign-On: Adapting Seamless Access Control to the Enterprise

Oracle Enterprise Single Sign-On Suite Plus or Oracle ESSO (formally Passlogix v-GO) centralizes the management of direct and granular control over access to a wide range of enterprise resources. Today, this capability can provide direct control over access to third-party, Cloud and SaaS environments tailored to the needs of the business, regardless where resources are hosted or how they are delivered.

When the Oracle ESSO agent is deployed on the desktop, it manages all of the user’s account names and passwords on their behalf. The user need only log initially into Windows. Applications are recognized when they are launched based on their unique attributes, and the correct access credentials are supplied.
to each as required, transparent to the user. SaaS and Web resources are handled as any other application, with the correct credentials supplied to each on recognition by the Oracle ESSO agent.

Oracle ESSO can be deployed into existing infrastructure without the need to integrate with target applications. It can accept authentication directly from the Windows logon or many strong authentication solutions. It can use existing directories and databases as central repositories for user management, including Microsoft Active Directory, LDAP directories, or any SQL database.

Oracle ESSO can handle the tasks of generating more secure random passwords for users, without the need to involve the user in password management. When users log into their personal Windows system, Passlogix transparently handles access to other resources as needed.

**Single Sign-on From Anywhere, To Anywhere**

This means that users no longer need to remember multiple passwords for multiple resources—but what about when they need access to third-party Cloud or SaaS applications from somewhere else? Business users may often find themselves needing to log into hosted applications from their home systems or other endpoints outside the business. If the Oracle ESSO agent is managing access to these resources from inside the enterprise, how will users be able to access them if they do not know their password?

Oracle ESSO answers this need with On-Demand functionality, which makes ESSO functionality available to users by clicking on a Web site link. ESSO users can download a transient version of the agent, enabling them to use their single sign-on password to access any resource, regardless where either the target or the user endpoint may be located. This also helps protect against users exposing passwords to threats that capture input directly from the keyboard. Oracle ESSO provides protection to access credentials whenever invoked, just as it does for the permanently installed agent inside the enterprise. When the agent is shut down, the On-Demand software enhances security by removing all traces of the ESSO application and the user’s application credentials.

**Simplifying User Management**

When personnel move, change their role within the business, or leave the organization, Oracle ESSO extends these changes to access via single sign-on. Because the software can use many enterprise directories and databases, it inherently applies the rights granted in them to end-user application access. Oracle ESSO integrates with user provisioning solutions to assure that user lifecycle management—the policy-defined management of user moves, adds, changes and terminations—is enforced directly in the solution in harmony with other identity and access management resources.

These capabilities help to assure consistency in policy-based access control from the data center to service providers as well as to the user endpoint. For example, Microsoft Windows users gain access to Oracle ESSO functionality through the Windows logon. If their access to the Windows environment is changed or terminated, their access to resources through ESSO is changed or terminated as well. While businesses will want to assure that third-party accounts are managed appropriately, Oracle helps simplify and centralize the management of access to those accounts, without direct reliance on third-party resources to enforce controls on individual users.
Key Benefits
The Oracle ESSO approach places control of access to any application, including hosted Cloud and SaaS resources, in the hands of the business. This avoids reliance on third-party policy or enforcement of secure practice. Oracle ESSO does this in a way that adapts these resources to the needs of the business, rather than forcing the business to adjust to the policies and practices of third parties that may not always align with those of the customer.

Oracle ESSO provides greater and more consistent assurance of privacy protection and security for usernames and passwords and the privileges they control, both inside and outside the organization. Users never need know the username and password for any third-party service, even when password changes are requested by the application, since Oracle ESSO handles the interface with the application or service. This simplifies password management for the user, who is relieved of the need to remember multiple passwords, as well as for the business, which can significantly reduce its support costs arising from password reset requests. Oracle ESSO’s automated password generation capabilities can assure that highly secure passwords can be generated to meet specific needs, providing greater security for password-based access. The ability to leverage two-factor authentication techniques when needed further strengthens the Oracle approach. The solution integrates with many strong authentication infrastructures, and can force re-authentication prior to providing applications with the user’s credentials.

These capabilities also support regulatory compliance requirements for enforced password policies and password changes. This helps to mitigate compliance violation risks while still enabling users to access SaaS and Cloud resources from any convenient location, both inside and outside the enterprise. Oracle ESSO further supports compliance with the logging of access to applications that regulatory policies often require.

The ability to manage user access to third-party resources through the management of user account changes or terminations in primary resources such as Active Directory expands the benefits of the Passlogix approach to single sign-on for mitigating a wide range of risks.

EMA Perspective
As the enterprise increasingly seeks to extend its boundaries to off-premises and third-party solutions, businesses will want access to be as seamless as possible. Customers must, however, take seriously the implications of this move, and the risks of controls on access to sensitive business resources in the hands of a third party. In order to mitigate those risks, organizations will want to seek out solutions that not only help keep them in control, but that adapt more secure authentication to the needs of the business, rather than the other way around.

Oracle ESSO delivers these values within the enterprise. The advantage it brings to assuring stronger authentication for Cloud, SaaS and other third-party services is that the flexibility of its approach can be just as readily applied to resources hosted outside the enterprise.

Inside the enterprise, the Oracle ESSO solution is compatible with a wide range of resources, from Windows to mainframe, Java and Web-based applications. It supports a number of line-of-business applications such as healthcare, human resources, accounting and financial systems, as well as widely

The advantage Oracle ESSO brings to assuring stronger authentication for Cloud, SaaS and other third party services is that the flexibility of its approach can be just as readily applied to resources hosted outside the enterprise.
adopted application platforms. Among third-party SaaS and hosted resources, Oracle ESSO extends single sign-on to customers of widely recognized brands such as Salesforce.com, GovTrip, NetSuite, major banking sites, and many others.

This may be more than customers get from solutions that extend single sign-on strictly to third-party or hosted resources. This highlights an important point that businesses should consider in evaluating their options for single sign-on for hosted environments: Prospective customers of a single sign-on solution should weigh not only the total value of an approach, but the ability of a solution to adapt flexibly to any environment, which may go far to “future-proofing” their solutions for seamless authentication across a number of disparate resources going forward.

About Oracle

Oracle (NASDAQ: ORCL) is one of the world’s largest enterprise software companies, with more than 300,000 customers. Oracle Fusion Middleware consolidates Oracle’s standards-based software to deliver “hot-pluggable” middleware with a comprehensive and seamlessly integrated software infrastructure. Oracle Fusion Middleware’s Identity Management capabilities enable customers and partners to decrease security threats across diverse IT environments while helping address governance, risk and compliance needs.

About Oracle Identity Management

Serving as the security backbone for Oracle Fusion Middleware, Oracle Identity Management is a leading suite of Identity Management products. Oracle Identity Management’s support of industry standards such as WS*, XACML, SAML and SPML helps enable customers and partners to more easily integrate applications with the framework. The family of software includes Oracle Identity Manager, Oracle Identity Analytics, Oracle Access Manager, Oracle Entitlements Server, Oracle Enterprise Single Sign-On Suite Plus, Oracle Identity Federation, Oracle Adaptive Access Manager, Oracle Directory Services, and Oracle Management Pack for Identity Management; all of which can be used in its entirety or as individual components.

To learn more, visit http://www.oracle.com/identity.

Trademark

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105, Boulder, CO 80301
Phone: +1 303.543.9500, Fax: +1 303.543.7687