Leveraging Federated SSO Capabilities within Oracle E-Business Suite

Scalable security and streamlined user access for Oracle EBS
Table of Contents

Introduction 3
Oracle E-Business Suite 4
Today's Diverse Enterprise 5
Password Fatigue 6
More Flexibility, More Problems 7
Leveraging SSO within Oracle EBS 8
PingFederate Integration for Oracle EBS 9
PingFederate Integration with Oracle EBS Workflow 10
Conclusion 11

Sources

¹Forrester Research®, The Total Economic Impact of the Identity Management Platform from Ping Identity, July 2013
INTRODUCTION
The Oracle® E-Business Suite (EBS) is a fully integrated set of business applications that has helped transform the modern enterprise. From customer relationship management to financials to supply chain management, EBS provides a unified platform that gives organizations a consolidated view of resources in real time.

Like any large suite of applications, managing identity and passwords in EBS is often IT’s biggest challenge. Passwords inevitably fall out of sync or users forget them, and the cost of manual password resets by IT becomes measurable. In order to overcome these challenges, today’s most successful organizations are demanding single sign-on (SSO) capabilities for their EBS environments.

A federated single sign-on solution for EBS allows an existing token to be used for authentication, eliminating the need for multiple passwords while providing a secure and scalable platform that leverages your existing technology investments.

Working in partnership, LikeMinds Consulting and Ping Identity® provide Oracle E-Business Suite customers with secure SSO technology as well as consulting and integration services. With deep experience in Oracle EBS, LikeMinds makes it simple to streamline IT administration and provide secure access management for EBS environments.

In this eBook, you’ll learn recommendations for incorporating the Ping Identity PingFederate® solution to provide SSO capabilities for Oracle EBS.
Oracle EBS is comprised of a transformative set of applications that help organizations manage the complexities of global business environments and make better decisions, reduce costs and increase performance. The comprehensive suite includes applications for customer relationship management, human capital management, financials, value chain planning, supply chain and service management.

Not counting employees, Oracle EBS is the heart of many businesses. It utilizes a single, consolidated database to store the enterprise-wide data, which means organizations have a unified view of all of their resources in real time. Summary reports and other critical metrics can be accessed on a daily basis and viewed on customizable portals.
In addition to password management and policies, three primary issues are driving increased adoption of identity federation in organizations today.

**Diverse applications**
The adoption of cloud applications and software as a service (SaaS) is continuing at an accelerated rate. Additionally, partner websites and APIs not only have the ability to further exacerbate the password problem, but auditing access to these applications can be difficult or impossible. Enabling federated SSO into these applications helps resolve both of these issues.

**Diverse users and entry points**
Users are signing on to Oracle EBS from places other than the corporate network. The proliferation of mobile devices means that there is a high probability that employees are signing on to these applications from a local coffee shop, a customer site or the airport. Users want legacy applications, SaaS applications and other API-based applications available from mobile devices, and organizations have realized that the increased productivity and lower costs associated with bring your own device (BYOD) initiatives are worth the risks—especially when those risks are mitigated with secure identity federation.

**Multiple identity stores**
It’s important to keep in mind that user data could be stored anywhere. Identity data could be in Active Directory or an Oracle LDAP system. Users could also be granted access to applications through a web access management (WAM) system. A legacy identity management system could combine multiple corporate directories, adding to the number identity stores. Cloud identities are also being utilized to bring down costs and remove the burden of identity management for contractors and other part-time users.
Enterprises typically employ password change policies in order to comply with security mandates. With multiple identity stores and applications, passwords have to be reset on different cycles, and, inevitably, they fall out of sync. This means that users forget their constantly rotating passwords, or worse, write them down or put them in a spreadsheet. For administrators, this creates a painful, drawn-out process because they are constantly verifying that the right user accounts are in the right user stores and are manually resetting passwords.

**The true cost of password resets**
According to analysts, the two most frequent calls to the IT help desk are ‘how-to requests’, such as how to access or operate IT resources, and ‘password resets’. These requests account for 20 to 30 percent of all help desk interactions.
MORE FLEXIBILITY, MORE PROBLEMS

While the enterprise has become much more flexible and there are many more options for access and application types, managing and auditing access to these applications continues to be challenging. To unweave these complexities, today’s enterprises are looking to:

- Address access control requirements for web, mobile and APIs.
- Eliminate password fatigue and improve productivity.
- Integrate easily into existing architectures like Oracle EBS.

Enter a federated architecture

Enterprises have an alternative—a federated architecture. The Ping Identity PingFederate solution extends single sign-on (SSO) capabilities to Oracle EBS through simple adapters and agents (which will be covered in depth later in this eBook). This modular approach to identity federation also allows simple integrations with other disparate systems and SaaS applications as well. The PingFederate federation server provides a layer that standardizes interfaces and identity stores in your enterprise and enables you to do business securely. A federated architecture allows you to eliminate multiple passwords because it securely passes the user identity using standardized tokens or assertions instead of usernames and passwords.

A federation server is a connection point between the user stores and the resources that the users need to get work done.

A federation server allows you to:

- Authenticate across identity stores.
- Eliminate IT administrative overhead.
- Accelerate new relationships with customers and partners.
- Provide SSO and a better user experience.

Simplified administration

A federated architecture makes it possible to give users access to the resources they need while helping to streamline administration. With this approach, IT can also bridge external identities that come from partners or customers and connect them to the applications that they need to get work done. With this framework, administrators maintain control over users and scale as needed. They also have a central point of administration that leverages existing processes and policies instead of forcing new workflows or additional identity management systems and processes.

Extend access to customers and partners

A federated architecture also makes it easy to extend access to customers and partners, allowing companies to accelerate these relationships while providing a better user experience. This is important because it allows enterprises to reduce the friction that typically exists when trying to bring in a third-party and makes it easier to give partners and customers access to the systems that they need.

SSO means a better user experience

From a user perspective, federated SSO means they can securely connect to whatever resource they need to do their job—with a single identity. Sign on once, from anywhere on any device, and you’re in. It is a seamless experience for the end user, regardless if they are signing on to Oracle EBS, a SaaS system or a mobile application.
LEVERAGING SSO WITHIN ORACLE EBS

There are two pieces of the Oracle architecture that are needed to make any single sign-on solution work with Oracle EBS. These components are the Oracle EBS AccessGate and the Oracle Internet Directory (OID).

Oracle EBS AccessGate
Oracle EBS AccessGate is an application that is responsible for mapping a single sign-on user to an Oracle EBS user and then creating an EBS session for that user. Note that this application is not a component of Oracle Access Manager (OAM), and OAM is not required as part of this solution. When single sign-on is enabled, EBS delegates authentication to the EBS AccessGate, but authorization is still performed by EBS.

Oracle Internet Directory
The Oracle Directory Integration Platform (DIP) is used to synchronize users between the Oracle Internet Directory and the EBS database. This synchronization, which can be one-way or two-way, links externally managed users to EBS internally managed users. DIP can also be used to synchronize accounts from a corporate Active Directory, for example. PingFederate then integrates with OID in order to retrieve the globally unique identifier (GUID) for these externally managed users.
PINGFEDERATE INTEGRATION FOR ORACLE EBS

The PingFederate solution includes adapters and agents that make it simple to integrate with identity stores as well as applications. As an Identity Provider (IdP), these adapters are referred to as first mile connections, which allow an enterprise to connect to an identity store for authentication. A Service Provider (SP) will leverage a last mile connection into their own applications. Last mile adapters allow PingFederate to act as a broker, taking an existing session or token and converting it into a format that is consumable by the application.

The EBS solution uses both of these capabilities in order to enable SSO. User authentication is typically done through the HTML Form Adapter, which is used to gather the username and password. The user’s password is then validated against OID or some other authentication service, such as an LDAP server. PingFederate also includes an Integrated Windows Authentication (IWA) adapter that can be used for authentication via Kerberos or NTLM for browsers that support those protocols.

The last mile adapter is used to generate a standard, encrypted token that contains the attributes that are needed by the EBS AccessGate—namely the username and GUID. This token is sent to the PingFederate agent that runs on a Microsoft IIS or Apache web server. The agent is responsible for decrypting the token and providing the attributes to the web server, which makes the HTTP headers available to the AccessGate.

Once the AccessGate receives these headers, it communicates with the EBS database to confirm the GUID and match the user to their EBS account. The AccessGate then creates an EBS session for the user and redirects them to the requested application.
PINGFEDERATE INTEGRATION WITH ORACLE EBS WORKFLOW

1. The user requests an EBS resource
2. EBS redirects the user to the web server proxying for the AccessGate
3. The user is redirected to PingFederate for authentication
4. The credentials are validated and the GUID is retrieved
5. The user is redirected to the web server proxying for the AccessGate with an encrypted token
6. The Apache or IIS agent decrypts the token and provides HTTP headers to the AccessGate
7. AccessGate matches the GUID and creates an EBS session for the user
8. The user is redirected to the EBS resource with an EBS session
9. The session is validated and the user is authorized for the application
CONCLUSION

By integrating federated identity, enterprises can optimize their use of Oracle EBS through scalable security and streamlined user access. Federated SSO capabilities mitigate access management risks and unburden IT administrators from dealing with password resets and the fatigue of multiple passwords for end users.

The Ping Identity PingFederate solution enables SSO for the Oracle EBS environment and extends SSO to other internal applications, regardless of whether the user is on the corporate intranet or at their local coffee shop. This federated identity architecture also allows enterprises to combine identity data from employees, customers and partners to grant access to portals, SaaS applications and third-party systems with a single password, using any device. This federated, Next Gen Identity™ approach enables a more secure enterprise and provides streamlined access across the entire organization.

For more information on securing your Oracle EBS environment, please contact Ping Identity today at U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.