The growing number of business applications and services that end users need to access creates confusion and lost productivity from having to remember many usernames and passwords. IT staff are challenged to securely set up and authenticate users as the number of users and sites they need to provision continues to increase exponentially. These issues are exacerbated when applications are outsourced to many different service providers, each with their own proprietary identity management solutions. Often implementing and running identity federation software to manage identities across organizational domains requires specialized knowledge and skills that an organization may not have.

Oracle Managed Cloud Services - Identity Federation Service is designed to solve these problems by providing an efficient, cost effective, managed cloud based, federated, single sign-on service.

Identity Federation Service Overview

The use of Oracle Managed Cloud Services - Identity Federation Service improves usability, reduces support costs, and facilitates security and compliance. Usability is enhanced by reducing proliferation and dissemination of user identities and passwords, which, in turn, reduces user confusion, lost productivity, and support costs. This federated single sign-on service enables an organization to retain control over sensitive user credentials and authentication mechanisms. Last but not least, the service gives centralized visibility into authentication activities. As a result, the Oracle Managed Cloud Services - Identity Federation Service helps improve the usability and effectiveness of security mechanisms and aids compliance with security policies and visibility.

Powered by Oracle Identity Federation and Oracle Access Manager, the Identity Federation Service allows managed cloud based web applications to participate in cross-domain federated single sign-on circles of trust that span multiple sites. This allows users to log in once and access integrated applications across the managed cloud and other federated sites, without having to log into each application individually. The Identity Federation Service can optionally be integrated with your legacy directory in a variety of ways to leverage existing identity information. Oracle Managed Cloud Services takes care of integrating the Identity Federation Service with your applications based in managed cloud environments, resulting in rapid deployment, ease of use, and low cost to support end-users. This relieves your organization from having to develop the expertise to securely install, integrate, and run a federated single sign-on system.

Reduce Identity Proliferation and Reduce Support Costs

By reducing confusion about usernames and passwords, the Oracle Managed Cloud Services – Identity Federation Service can reduce help desk call volume for forgotten usernames and passwords. Furthermore, when users are educated to recognize one single sign-on login screen and only enter login credentials to that screen, the risk of stolen passwords from
phishing is reduced. The Oracle Managed Cloud Services - Identity Federation Service thus improves user experience and reduces end-user support costs.

Support for Industry Standards
The Oracle Managed Cloud Services - Identity Federation Service supports the Security Assertion Markup Language 2.0 (SAML 2) industry standard. For SAML2 implementations, the service can serve in an Identity Provider (IDP) role, authenticating users and issuing assertions, or in a Service Provider (SP) role, consuming assertions that indicate a user has already logged in to a trusted IDP. The Identity Federation service thus provides a cross-domain single sign-on solution that uses industry-standards for interoperability across a variety of cloud and internet services.

Support for Entire Identity Management Lifecycle
The Managed Cloud Services - Identity Federation Service is designed to facilitate an organization’s end-to-end identity management lifecycle. The service can leverage user profile information from an authoritative source to facilitate on-boarding of new hires with pre-federated accounts. Termination of accounts at the identity provider level immediately removes the ability of users to log into any application in the federated circle of trust. De-provisioning of accounts for terminated users can be implemented to remove orphaned accounts at the service providers so they don’t become a future security liability. The Identity Federation Service can also be integrated with other Managed Cloud security services such as the Identity Provisioning Service and Strong Authentication Service. In this way, the Managed Cloud Services - Identity Federation Service can benefit from an integrated flow of user profile information and support the identity management lifecycle of your user base.

Centralized Control over Authentication
Oracle Managed Cloud Services - Identity Federation Service provides several benefits for IT and security departments. The service supports the centralization of control over authentication mechanisms and policies across applications at multiple sites. The service also improves security by reducing the exposure of widely used, static credentials because users only enter their credentials to the identity provider in the federated circle of trust. The Identity Federation Service promotes centralized visibility for login activity. Use of the Identity Federation Service results in greater consistency in authentication procedures and policy, greater visibility, better security and less user confusion.

Managed Identity Federation Service
The Oracle Managed Cloud Services - Identity Federation Service alleviates your organization of the burden of installing and running many specialized identity management components and integrating them with your many business applications and potentially with other service providers.

The Oracle Identity Federation service is installed, configured, and integrated with Oracle business applications based in a managed cloud environment. The service is also configured to interact with your chosen Identity Provider or Service Providers via the SAML2 protocol. The service is configured to comply with your security policy for requirements such as session time out and log data retention periods. If Oracle serves as the identity provider, the Federated Single Sign-On login screen is customized to include your organization’s branding information. The service can optionally include integration with your existing directory
service for provisioning of pre-federated accounts.

As an industry-standard solution, no special software needs to be installed on end-user client devices. The service is also easy for end users to adopt. This service requires little ongoing attention from your IT organization because Oracle Managed Cloud Services takes care of running, patching, maintaining and monitoring of the service. In short, when the service is turned over to your organization, cross-domain federated single sign-on capability across your applications is ready to go.

Conclusion

In summary, in addressing the issues of supporting multiple applications, for both employee and partner/customer facing environments, Oracle Managed Cloud Services - Identity Federation Service, powered by Oracle Identity Federation and Oracle Access Manager, provides simplified, secure, cross-domain single sign-on authentication protection for Oracle applications based in managed cloud environments. The solution can serve as either a SAML2 Identity Provider (IDP) or a SAML2 service provider (SP) and can be easily integrated with other identity management solutions such as provisioning. This service includes integration with Oracle business applications to speed application deployment projects. This service solves critical identity management challenges and speeds up application deployment while still providing control with centralized visibility for authentication policy and logging.

Contact Us

For more information about Oracle Managed Cloud Services –Identity Federation Service, visit oracle.com/managedcloudservices or call +1.800.ORACLE1 to speak to an Oracle representative.