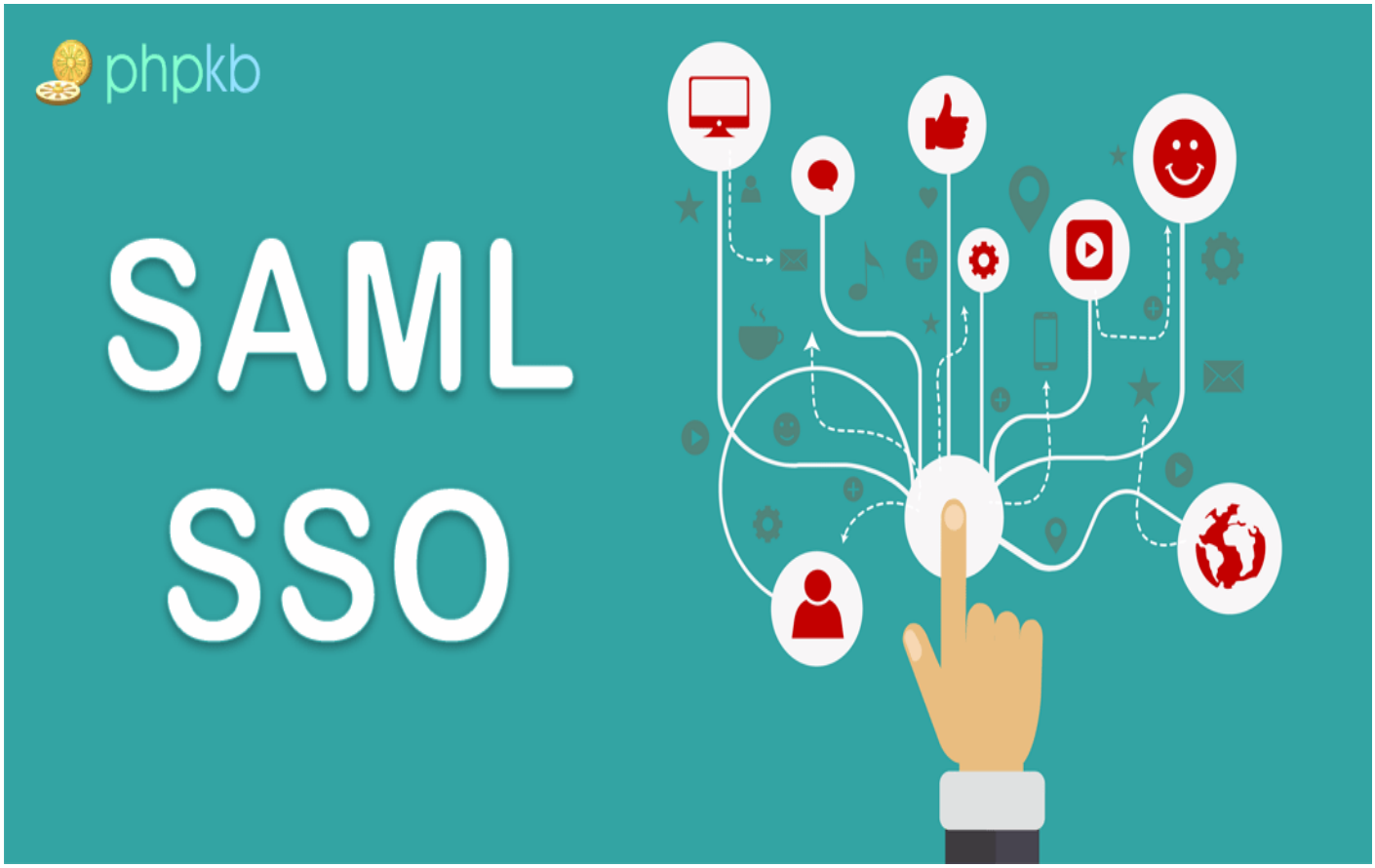
Knowledge Base Software with SAML SSO

309 Ajay Chadha January 20, 2023 Blog 4256 0

SAML (Security Assertion Markup Language) SSO (Single Sign-On) is a way to authenticate users for different systems, applications, and services. It allows users to log in once to access multiple systems, eliminating the need to remember multiple usernames and passwords.

What is SSO?

As the name suggests, Single Sign-On or SSO allows users to easily access multiple applications with a single login event. A user logging into an application with SSO enabled will also be able to log on to other applications seamlessly without having to enter the login credentials each time they want to access any of those applications.



How does it work?

Most applications (also called Service Providers) have a dedicated secure database where user information and their login credentials are stored. But for services that provide SSO, an external entity – the Identity Provider (IdP) is brought in to ease the user experience.

The IdP is essentially a third-party application that will perform user authentication for your application. Here is how it works:

1. You visit the required application or service provider sign-in page.
2. Redirection takes place to the IdP login page.
3. You enter and log in with your credentials.
4. User validation is initiated.
5. A trust relationship is established between the IdP and your service once the login is successful.

Once the authentication is successful, you can access all SSO-enabled applications within the service provider domain without signing in for each instance.

The IdP

The Identity Provider handles and authenticates credentials that users use to log in to an application, file server, or service. The IdP facilitates Single Sign-On with two standard protocols adopted by the service providers.

SSO Standards

1.SAML 2.0

The SAML is an open standard protocol that enables SSO for applications like PHPKB knowledge base software. Authentication via the SAML involves three entities:

1. Identity Provider – IdP
2. Service Provider (PHPKB Knowledge Base Software)
3. End User

Once the users are authenticated via the IdP, the IdP generates a SAML Assertion which is sent to the Service Provider. As the Service Provider holds a trust relationship with the IdP, the user is authenticated to log in, and SSO is achieved.

2.OpenID Connect

OpenID Connect (OIDC) is an open standard that is built on the OAuth2.0 protocol. This gives OpenID an additional layer of security. OpenID also involves the same three entities as mentioned above:

1. Identity Provider – IdP
2. Service Provider (PHPKB Knowledge Base Software)
3. End User

The IdP authenticates the end-user, then sends an access token back to the PHPKB knowledge base software. Now, PHPKB retrieves user info from the token passed on, and an SSO session is established between the knowledge base software and the Identity Provider.

Now that the credentials are verified and authentication complete, the user gains access to knowledge base software and other apps without providing credentials for each instance.

What is SAML SSO?

SAML is an XML-based standard for web browser single sign-on and is defined by the OASIS Security Services Technical Committee. The standard has been around since 2002, but lately, it is becoming popular due to its advantages:

Usability - One-click access from portals or intranets, deep linking, password elimination and automatically renewing sessions make life easier for the user.
Security - Based on strong digital signatures for authentication and integrity, SAML is a secure single sign-on protocol that the largest and most security-conscious enterprises in the world rely on.
Speed - SAML is fast. One browser redirect is all it takes to securely sign a user into an application.
Phishing Prevention - If you don't have a password for an app, you can't be tricked into entering it on a fake login page.
IT Friendly - SAML simplifies life for IT because it centralizes authentication, provides greater visibility, and makes directory integration easier.
Opportunity - B2B knowledge base software vendors should support SAML to facilitate the integration of their product.

Benefits of SAML SSO (Single Sign-On)

Implementing SAML SSO for your knowledge base can provide several benefits, including:

Improved security: SAML SSO allows for secure and encrypted communication between systems, which can help to protect sensitive information and reduce the risk of data breaches.

Increased productivity: By eliminating the need for users to remember multiple usernames and passwords, SSO can improve productivity and reduce the amount of time spent on login and password management.

Improved user experience: SSO provides a seamless and consistent user experience across different systems and applications, making it easier for users to access the information they need.

Centralized authentication and authorization: SAML SSO allows for centralized authentication and authorization, which can help to improve the overall security of your organization.

Better compliance: SSO can help organizations meet compliance requirements, such as HIPAA and SOC 2, by providing secure and controlled access to sensitive information.

Scalability: SAML SSO is a scalable solution, that can accommodate a large number of users and systems, making it suitable for organizations of all sizes.

Integration: SAML SSO can be integrated with a wide range of systems, applications, and services, allowing organizations to easily add new systems and services to their SSO infrastructure.

Cost-effective: SSO can help organizations to reduce costs by eliminating the need for multiple login systems, and by reducing the need for password resets and other support-related activities.

Better control: SAML SSO allows organizations to have better control over access to their systems and applications, by providing a central point of control for authentication and authorization.

By implementing SAML SSO for your knowledge base, organizations can improve the security and efficiency of their knowledge base, while providing a better user experience for their customers and employees. It can help to streamline the login process and provide secure access to critical information, while also reducing the costs associated with password management and support. Overall, SAML SSO can help organizations to better protect their knowledge base and the sensitive information it contains, while also improving the user experience for their customers and employees.

User Benefits:

Convenience: Users need to remember only one set of credentials. Connecting your site to Google user login is an excellent way to ensure that even sporadic users can remember their credentials; they can log in to Google to access all business applications via SSO.

Speed: With SSO, users don’t have to type in their credentials each time they want to access an application/service. New users can also sign up quickly as Google would already have done the email verification and data collection.

Business Benefits:

More sign-ups: SSO is easy and convenient and offers the least resistance path. This enables new customers to sign up quickly without much of a hassle by relying on a known brand like Google to authenticate and store their details. This way, they won’t have to worry about providing their information to your unknown brand, and hence trust is increased, leading to more conversions.

Reduced backend work: Having to remember multiple login credentials may lead to users forgetting them. In this case, the backend operations team has to reset the password and set new credentials. While reducing hack risk is essential, not having to reset user passwords is a whole lot of burden reduced. With SSO, all the authentication is taken care of by the IdP, and users only have to remember one password.

Better security: Without multiple login credentials hosted on your site, hackers have a much lower chance of hitting your application. You’re also less likely to have a handful of users with weak passwords poking holes in your overall security system.

Conclusion

Adopting SSO can make life easier for you and your clients. We have SSO enabled in the enterprise editions (both SaaS and Self-Hosted licenses) of PHPKB knowledge base software, and you can configure multiple user logins via the SSO by opting for the SAML SSO Plugin or OpenID Plugin.

Online URL: https://www.phpkb.com/kb/article/knowledge-base-software-with-saml-sso-309.html