APPSIAN

SOLUTION BRIEF

PeopleSoft Single Sign-On

Bring native SAML compatibility into PeopleSoft for simplified and secure Single Sign-On

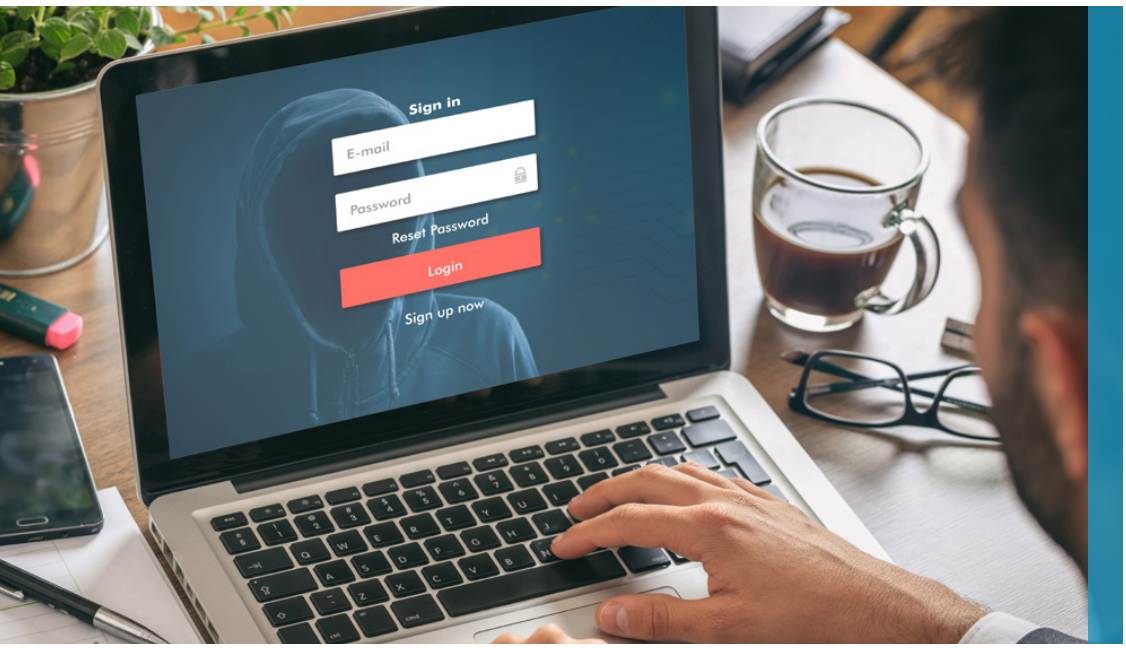
Abstract

SAML-based Single Sign-On solutions have become the go-to approach for delivering seamless access and improved security throughout an organization's application landscape. Today's most popular Identity Providers such as ADFS, Shibboleth, OKTA, Ping, and Azure all use the SAML standard – and SAML compatibility is a staple in the growing stack of modern enterprise applications.

However, this shift has left behind legacy ERP applications. Unfortunately for PeopleSoft customers, a lack of native SAML compatibility means that their PeopleSoft applications will require custom development to handle SAML assertions or end up being isolated from enterprise-wide SSO initiatives altogether.

Both scenarios have their downfalls. Custom development is costly and time consuming, requires specialized knowledge, and the resulting solution is often fragile with continuous maintenance costs that can grow into uncertainty. Isolation is worse. Without a centralized authentication system, organizations must add an extra step in user provisioning and often face increased password reset support costs specific to PeopleSoft. Application avoidance can happen as users see the manual login a hinderance, and poor password management practices can set in.

So, what other options are there? In this solution brief, we will discuss how organizations can leverage Appsian's turnkey PeopleSoft SSO Connector to ensure that their PeopleSoft applications are a part of a seamless enterprise environment that improves security, boosts user productivity, and enables efficient identity management.



Challenges

PeopleSoft does not support SAML

PeopleSoft lacks native support for SAML - the widely accepted identity federation standard. Most off-the-shelf SSO providers are unaware of this, and do not consider or address this critical challenge during implementation discussions. The inevitable roadblock of PeopleSoft lacking SAML support comes up during testing, thus compelling your SSO vendor to suggest a time-consuming and costly customized solution.

Custom developments are not ideal

Off-the-shelf SSO solutions need to be significantly modified in order to work with PeopleSoft. Organizations must build an extensive framework of additional customizations and hardware in order to simulate communication between PeopleSoft and their respective identity provider (ADFS, Shibboleth, etc.). In addition to prolonged implementation, customizations to SSO solutions are insecure, fragile, lack functionality for some transactions, and originate problems that are difficult to troubleshoot. They also require the procurement of extra infrastructure (reverse proxy server) resulting in possible project budget overruns.

Application isolation downfalls

Without SAML-compatibility, PeopleSoft applications are often left out of enterprise-wide SSO initiatives. The isolation of PeopleSoft applications from the rest of the enterprise application stack can have several negative effects:

- IT teams are faced with increased support costs associated with password resets
- Manual user provisioning and deprovisioning without a centralized identity management
- Lack of IdP-enforced governance policies (such as password strength & renewals)
- Reduced productivity due to downtime associated with password reset and recovery

Solution

Appsian's PeopleSoft SSO Connector is designed to create a simple, extensible, and easy-to-maintain approach to the implementation of modern authentication and SSO technologies. The PeopleSoft SSO Connector supports identity federation through the implementation of related rules capable of responding to assertions/claims from SAML based id providers.

Being the only turnkey solution for native SAML-compatibility in PeopleSoft, the module allows organizations to support SAML-based SSO technology without any customizations or additional infrastructure.

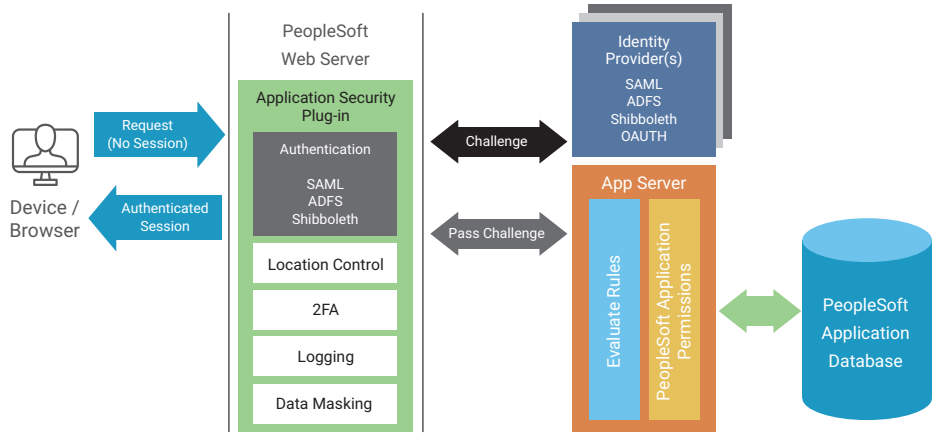
Enabling Single Sign-On in PeopleSoft eliminates the need for end-users to utilize multiple passwords and empowers them to seamlessly transition between PeopleSoft and other enterprise applications using a single, strong login credential. It also empowers IT teams to centralize authentication management and makes it easy for them to provision password databases as employees come and go in the organization.

With Appsian's PeopleSoft SSO Connector, organizations can:

- Leverage existing investment in SSO solutions to authenticate PeopleSoft sessions via SAML-based Identity Providers
- Access PeopleSoft via deep link navigation (sent by email or other communication channels)
- Support multiple IdPs concurrently for consolidated systems with separate user groups
- Deploy your IdP's SSO in PeopleSoft as quick at 7 days with no additional hardware or custom coding

How it Works

Appsian's PeopleSoft SSO Connector plugs directly into an existing PeopleSoft web server. Authentication requests are routed via an existing identity provider, and if accepted, applicable roles and permissions are applied to that individual user's ID. This enables access to be delegated to users only with authenticated PeopleSoft sessions (based on configurable rules.)



APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com