

Pacific Compensation Insurance, Co.

About Pacific Compensation Insurance, Co.

Pacific Compensation (PacComp) deploys PortalGuard as a secure, fully branded portal that uses PortalGuard's Single Sign-On as a gateway to expedite agent and customer access.

Specific Pain Point

Pacific Compensation Insurance, Co. (PacComp) wanted a fully integrated and secure portal that would also be able to provide access to data and applications for specific agents and customers.

PacComp needed a solution that would allow them to fully integrate their company logos, color schemes, and iconography while giving specific user groups easy access to areas that are of importance to them.

In addition, administrators required a solution with auditing capabilities so that reports could be generated on demand.

Existing Challenge

PacComp actively uses the ASP model for hosted services like Salesforce and had deployed an initial Single Sign-On (SSO) solution for some of their existing apps. However, this solution was not universally deployed across all applications and lacked the customizability that would allow them to seamlessly integrate into their company portal.

Relying on a solution that only met some of the necessary requirements placed more strain on the local IT department and lead to end-user frustration due to a lack of true SSO. Difficulties arose in providing end-users with access to ONLY the resources they required without any excess distractions.

The initial Single Sign-On solution that was in place did not have a full range of auditing features - further hampering PacComp's ability to address the various needs of their hybrid internal/external access portal.

PortalGuard Resolution

By deploying the PortalGuard Single Sign-On (SSO) solution PacComp was able to address and eliminate each of their various pain points while simultaneously addressing the need to give end users access to specific resources based on their login credentials.



Customer Profile

Industry:

Insurance

1,150+ Users

Location:

California

Top Applications Used:

AD, Salesforce, PCIC, SpringCM

PortalGuard SSO provides PacComp with a fully customizable platform that allows IT administrators to easily integrate it into their custom-built portal framework. By giving clients the ability to brand, customize and thoroughly control how PortalGuard looks, PacComp was able to easily integrate the login prompt onto their main login page.

With the ability to integrate with multiple types of directories such as AD, LDAP or a custom SQL repository, PortalGuard allows the IT team at PacComp to setup specific user groups and directory forests for their various employees, agents, and customers.

With the PortalGuard SSO integration, PacComp users login and are presented with only the applications and resources required by them – there are no additional distractions or unnecessary options available. Additionally, regardless of the application, users are no longer required to login again for each application or resources once they have successfully authenticated through the PacComp portal.

The Technical Approach

A particularly challenging pain point for PacComp was the need to provide SSO access to a wide range of applications – most SSO providers would only support a handful at most. PortalGuard natively supports a wide range of SSO protocols, which allowed PacComp to approach this particular need from a better foundation.

For those applications that were SAML enabled, PortalGuard's Identity Provider (IdP) acts as a SAML-based portal and uses a single set of credentials for the portal login itself. PortalGuard then grants access to their pre-registered web-based accounts automatically

In those instances where applications are not SAML enabled, PortalGuard provides a forms-based solution. In forms-based SSO, a user's web-application credentials are stored in a vault on the PortalGuard server where they are protected using AES-256 encryption and PistolStar's patent-awarded key-derivation technology. PortalGuard references the credentials within the vault whenever the end user attempts to login through the PortalGuard SSO Portal. In doing so, there is no need for the user to authenticate separately, and authentication is as seamless as it would be with true SAML SSO.

Finally PortalGuard includes a reporting interface that provides administrators with the ability to audit and monitor login attempts by user, location, time, and IP address (among others). This reporting capability relies on a SQL backend and the data can be exported and distributed on demand to adhere to a variety of auditing requirements.

Additional Resources

[SAML Single Sign On Tech Brief](#)

[Centralized Self-Service Password Reset Tech Brief](#)

[Get out of the Password Reset Business - Webinar](#)

PortalGuard is a cybersecurity authentication package that delivers a full set of features in a single, fully customizable solution. PortalGuard provides single sign-on (SSO), self-service password reset (SSPR), two-factor authentication (2FA), and over 130 other features to ensure that each campus is equipped with the tools needed to face any authentication challenge.