FERMILAB-POSTER-23-239-V.

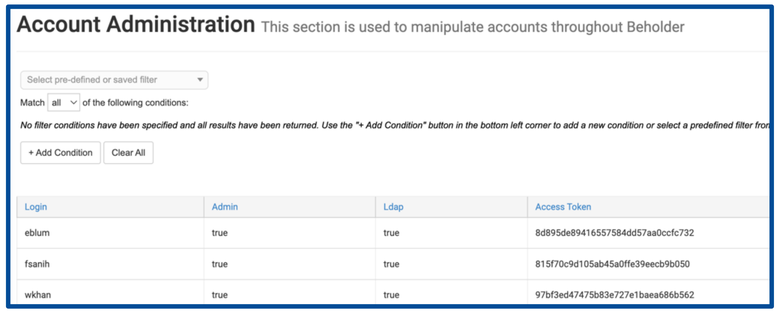
Unlocking Seamless Access: Enabling Single Sign On (SSO) for Beholder

Fatima Sanih, *The City College of New York*, Under the Mentorship of Jeny Teheran and Jason E. Ormes
Security and Emergency Management Division, Cybersecurity Team, Fermi National Accelerator Laboratory, Batavia, Illinois 60510

Introduction

Beholder is the central engine behind Fermilab's robust cybersecurity defenses. Due to its seamless integrations of detectors, vulnerability scanners, and blocking mechanisms, it stands as a formidable guardian against diverse cyber threats. Beholder uses the data produced by various sensors to direct the proper responses to defend the network against current threats and to deploy automatic responses as necessary. This provides a strong cyber security defense against fast-evolving cyber threats.

However, a challenge remains - account provisioning is manual and time-consuming during personnel onboarding and off boarding for Cybersecurity Operations. So, we explored the potential of integrating Single Sign-On (SSO) within Beholder, envisioning a future where streamlined user authentication enhances efficiency, strengthens security, and delivers a seamless user experience. This transformation will unlock the power of beholder's might through the realm of SSO.

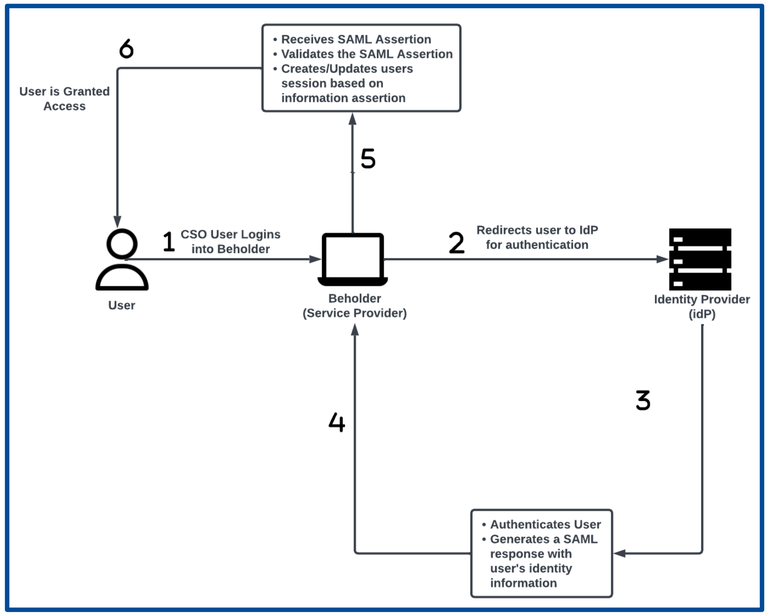


The process of the Cybersecurity Operations Team's manual provisioning of Beholder Accounts.

Benefit of SSO

Incorporating Single Sign-On (SSO) into the cybersecurity framework serves multiple crucial purposes. Firstly, it significantly enhances security by consolidating authentication processes, thereby reducing the number of potential attack surfaces. Moreover, SSO offers unmatched convenience to users, allowing them to access various applications and systems effortlessly using a single set of credentials. This streamlined approach boosts productivity by freeing users from repetitive authentication tasks, empowering them to focus on their primary responsibilities. Implementing SSO not only improves the overall usability of the system but also contributes to heightened employee satisfaction and engagement.

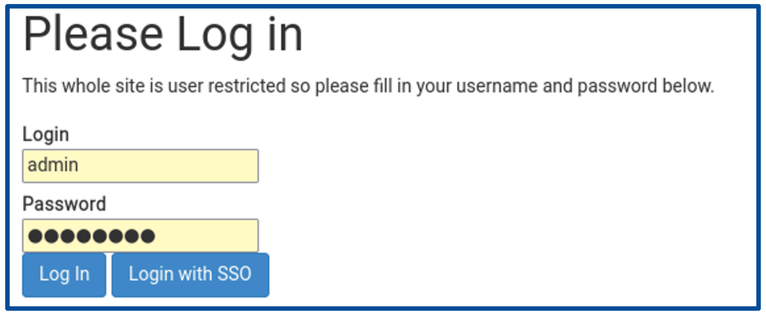
SSO Authentication Workflow



The flow chart describing the process of SSO authentication for Beholder.

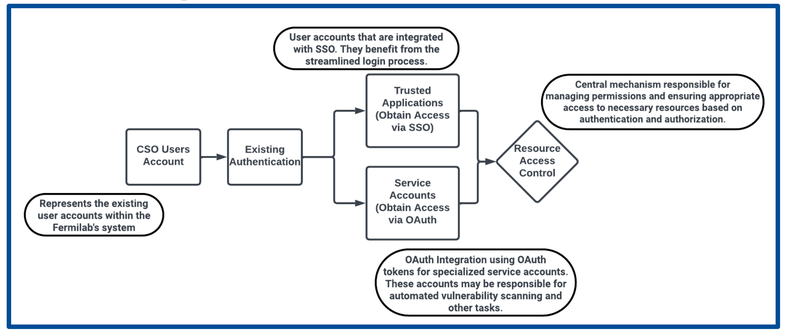
As illustrated in the flow chart above, the user initially attempts to access a protected resource. The service provider detects that the user is not authenticated and redirects them to the identity provider for authentication. The user then authenticates with the idP by providing their credentials.

Once authenticated, the idP generates a SAML response containing the user's identity information, such as their email or username. The SAML response is sent back to the service provider, which receives and validates it. If the SAML response is valid, the service provider creates or updates the user's session based on the identity information provided. Finally, the service provider grants access to the requested protected resource, and the user can access it.



User interface for the login screen with the SSO button

Future Improvements



The flow chart describing the future enhancements to Beholder's authentication process.

As Fermilab's cybersecurity landscape continues to evolve, there are several avenues for further improving the authentication process and enhancing the overall security posture. While the current SSO implementation provides a seamless login experience for users, OAuth can offer a standardized and secure way to enable third-party applications to access resources programmatically. This enhancement would streamline the process of granting permissions to trusted applications while maintaining strong security controls. By continually seeking to improve and adapt to emerging security challenges, Fermilab can ensure that its authentication mechanisms align with industry best practices and safeguard critical resources effectively.

Conclusions

The successful implementation of Single Sign On (SSO) authentication on Beholder required a comprehensive approach, from configuring SAML settings to updating the user model. Enabling SSO has brought numerous benefits, including heightened security by reducing attack surfaces, increased productivity for users through a single set of credentials for multiple applications, and improved usability and employee satisfaction. With SSO in place, the Cybersecurity Operations team at Fermilab can focus on ensuring a strong defense against fast-evolving cyber threats while efficiently managing account provisions through the onboarding and off boarding procedures. The adoption of SSO has been a crucial step in strengthening Beholder's overall cybersecurity posture and streamlining user access, contributing to a more secure and productive digital environment.

This research was supported in part by the U.S. Department of Energy (DOE), Omni Technology Alliance Internship Program. The program is championed by the DOE's Office of Chief Information Officer (OCIO) and represents a partnership with the leadership of the Office of Economic Impact and Diversity, the Office of Science, the Office of Nuclear Energy, and the National Nuclear Security Agency. The program is administered by the Oak Ridge Institute for Science and Education

This work was produced by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy. Publisher acknowledges the U.S. Government license to provide public access under the DOE Public Access Plan DOE Public Access Plan