What is single sign-on authentication?

Get the full interactive view at
https://bitwarden.com/fr-fr/resources/what-is-single-sign-on-
authentication/

bitwarden

Single sign-on authentication enables users to access multiple applications with one set of credentials, for example, a username and password. For enterprises managing thousands of employees, SSO reduces credential tracking from potentially thousands of logins to just one per user. This creates faster, more secure access while balancing security with convenience.

Organizations that implement SSO authentication find that their employees experience less frustration with login processes and enjoy smoother daily operations. Consider an enterprise managing 1,000 employees, each needing access to four different systems — that's 4,000 credentials to track without single sign-on (SSO), but only 1,000 with it.

> For enterprises managing thousands of employees, SSO reduces credential tracking from potentially thousands of logins to just one per user.

Key SSO terminology

The single sign-on (SSO) ecosystem includes several important concepts. Authentication verifies a user's identity, while authorization determines what resources they can access. Tokenization uses digital tokens to manage access securely across multiple systems. An SSO gateway connects users with various applications through a central login mechanism. Identity Providers issue and manage user credentials, while Service Providers rely on them for authentication. Protocols like OpenID Connect (OIDC) and SAML 2.0 facilitate SSO functionality across diverse systems.

How SSO authentication works

SSO single sign-on centralizes the authentication process. Users sign in once, and the system authenticates them across all supported platforms. The process begins when a user logs in and the system verifies their identity. The system then issues a secure token, which is stored on the device. When accessing another application, the system validates the token without requiring additional login steps. This seamless verification process occurs behind the scenes, creating a frictionless experience for end users while maintaining security protocols. This token-based authentication is what makes single sign-on authentication particularly effective for enterprises with complex application ecosystems.

Common SSO solutions

Organizations can choose from several SSO authentication implementation options. Directory services like Active Directory and LDAP provide centralized user management for traditional enterprise environments. IAM systems manage both identities and permissions, offering granular control over user access across systems. SSO gateways such as Okta and OneLogin act as intermediaries, connecting users to multiple services through a central authentication portal.

Read more:

Integrating OneLogin with SAML

When evaluating single sign-on for their organization, IT leaders should consider these options based on their existing infrastructure and security requirements.

Business benefits of single sign-on

SSO enhances user experience by minimizing login steps and reducing password fatigue, resulting in more productive and satisfied teams. The centralized login system improves security by reducing vulnerable access points and simplifying monitoring efforts. Organizations reduce IT costs as fewer password-related help desk calls allow support teams to focus on more critical tasks.

Businesses meet regulatory standards more efficiently with centralized identity systems that streamline compliance requirements. The platform also enables secure access to resources on mobile devices, supporting today's distributed workforce.

> SSO enhances user experience by minimizing login steps and reducing password fatigue, resulting in more productive and satisfied teams.

Enterprise strategy and SSO authentication

Password fatigue creates more than user complaints — it generates operational issues. Multiple logins slow down employees and burden IT teams with support requests. When users struggle to access necessary tools, productivity declines. SSO minimizes these distractions, helping teams stay focused and efficient.

This fatigue often leads to risky behaviors, such as reusing passwords and creating weak passwords. Recent surveys highlight that 72% of Gen Z reuse passwords, and 35% rarely update passwords even after a data breach. This behavior stems partly from the overwhelming number of passwords people need to remember, with 7 in 10 Americans feeling overwhelmed by this task. To combat password fatigue, many organizations now turn to SSO authentication combined with password managers, which dramatically reduces the likelihood of password reuse and enhances security.

> Password fatigue often leads to risky behaviors, such as reusing passwords and creating weak passwords. Read more about generational cybersecurity trends in the World Password Day 2025 survey.

Even with SSO authentication in place, businesses still face password challenges. While SSO centralizes access to connected applications, employees still interact with numerous systems outside the SSO ecosystem that require separate credentials. These non-SSO applications — vendor portals, legacy systems, personal accounts used for work — create security gaps that password managers effectively close. Organizations implementing SSO without complementary password management often discover this critical vulnerability only after experiencing a security incident.

Implementation considerations for single sign-on (SSO)

Costs

SSO implementation can involve several expenses. Though some solutions like Bitwarden include SSO in the enterprise plan, many SaaS tools charge a premium for enabling SSO capabilities, sometimes referred to as the "SSO tax." Organizations often need to upgrade to higher-tier plans to access this functionality. Additional costs include configuration, maintenance, integration tools like SAML or SCIM, and staff training.

> Solutions like Bitwarden include SSO

These implementation challenges explain why many organizations deploy SSO incrementally, creating a hybrid environment where password managers remain essential for managing credentials across both SSO and non-SSO systems. Despite these upfront expenses, the long-

term savings in time, security improvements, and productivity gains typically justify the investment for most enterprises.

Best practices

Organizations can implement strong password policies and multi-factor authentication to protect against credential theft. Teams should optimize the login experience across all key applications and maintain regular system updates with the latest security patches. Choosing a scalable platform ensures the SSO solution grows with the business and handles increased authentication traffic. Adopting centralized Identity and Access Management streamlines permissions and simplifies oversight. Regular security audits help detect vulnerabilities early and maintain compliance standards. Monitoring system performance and user behavior supports ongoing reliability and security.

Getting started with SSO authentication

A phased rollout allows for controlled testing and refinement before full deployment. Organizations should begin with an established SSO single sign on solution like Microsoft Entra ID or Keycloak to ease implementation challenges. Thorough testing helps identify potential issues before they affect the entire organization. Comprehensive training for IT staff, developers, and end users ensures smooth adoption. Regular audits and updates maintain system performance and security over time. SSO authentication implementations succeed most often when organizations approach the project with realistic timelines and clear success metrics.

Get started with this practical guide to using single sign-on or see this FAQ for answers to common SSO queries.

Check out these guides for setting up SSO with Microsoft Entra ID or using Keycloak for streamlined SSO.

Business value of single sign-on

SSO enhances security by centralizing authentication, streamlines access across platforms, and supports business growth through scalability. It reduces IT overhead from password resets, boosts employee satisfaction through simplified access, and aligns technical infrastructure with long-term business goals. Organizations maximize their SSO investment by integrating solutions like password managers with SAML protocols and consulting with trusted providers for tailored deployment plans.

Read more:

Step-by-step SAML SSO configuration guide

SSO and password management

Businesses increasingly integrate SSO with password management capabilities, allowing users to authenticate through their existing SSO identity provider. This integration supports protocols such as SAML 2.0 and OpenID Connect, offering flexibility and security for enterprise environments. This implementation represents the ideal scenario where SSO authentication works in conjunction with other security tools to create a comprehensive authentication ecosystem that strikes a balance between security and user convenience.

Despite SSO's many benefits, it cannot completely eliminate password challenges. Most organizations find that many of their applications don't support SSO integration, leaving a substantial portion of their digital ecosystem requiring traditional password management.

Password managers fill this critical gap by securing credentials for both SSO and non-SSO applications while enforcing password complexity requirements. They also provide emergency access protocols, secure password sharing capabilities, and robust credential management for temporary vendors and contractors — all essential functions that SSO alone cannot deliver. The combination of SSO for streamlined authentication and password managers for comprehensive credential security creates the most resilient security posture.

> Businesses increasingly integrate SSO with password management capabilities, allowing users to authenticate through their existing SSO identity provider.

Conclusion

Single sign-on authentication represents a critical component in modern enterprise security architecture. As organizations expand, the need for streamlined, secure access management becomes increasingly important. SSO addresses both security concerns and user experience challenges by centralizing authentication processes and reducing password fatigue. However, security experts consistently recommend implementing SSO alongside robust password management solutions rather than viewing them as competing technologies.

Forward-thinking organizations implement SSO as part of a comprehensive identity management strategy that includes password management tools, recognizing that simplified access translates to improved productivity, reduced security risks, and lower operational costs. The reality of mixed cloud applications, legacy systems, and third-party platforms — demands this layered approach. Organizations achieve optimal security when SSO handles authentication for supported systems while password managers secure the remainder of the digital landscape. As remote work and cloud services continue to proliferate, this dual approach of SSO single sign-on with password management will remain essential for businesses aiming to balance security requirements with operational efficiency.

> Get started with enterprise-grade SSO solutions.