What is Single Sign-On (SSO)?

In today's busy workplace, the business of actually conducting business has become increasingly complicated. As companies integrate more and more applications and software systems into their business processes, the average employee finds themselves accumulating a veritable laundry list of usernames and passwords. In fact, according to a 2017 report from LastPass, the average office worker has to wrangle around **191 logins**, creating a potential data-based powderkeg for Information Technology (IT), Human Resources (HR), and entire companies. Small wonder, then, that identity management technologies such as Single Sign-On (SSO) have drawn so much interest.

By connecting diverse accounts via a single set of login credentials, Single Sign-On streamlines workflows and reduces stress on IT resources and greatly simplifies onboarding and user access control for HR. Like all technology, it has its limitations—but for those who need a secure and effective way to manage multiple accounts across their organisation, it has the potential to generate substantial value in the form of cost savings, reduction of waste and resource consumption, and improved worker productivity.

Single Sign-On Overview

Imagine a single key that unlocks all the doors you need to conduct your daily business. It's simple to use, secure, and can even unlock new doors added to your daily routine as needed. Single Sign-On

is a simple, powerful embodiment of this idea, turning a single *security token* (i.e., a username paired with a password) into a user-friendly tool to manage identity and access.

A New Way to Manage Identity

Traditionally, Web applications and software packages that without SSO user authentication work like this:

1. A user visits a website or opens an application.
2. The website or application consults its database to verify authentication. If the user has already been authenticated (using "remember me," "log me in automatically," etc.), the site or program grants them access at the appropriate level.
3. If the user is not already authenticated, the site or program requests a set of login credentials (i.e., username and password).
4. The user signs in with their login credentials.
5. The site or program verifies the submitted set of credentials against its database and grants the user access if they match.
6. Once the user is logged in, the site or application retains the authentication data during their active session, granting them appropriate access across pages on the website or different areas of the application.

Sites and programs that don't use SSO generally rely on cookies to maintain login credentials for the active sessions or tokens, which are similar but do not retain session information and process more quickly than cookies do.

The process works differently with Single Sign-On, which introduces third-party services for verification and leverages trust between websites, applications, and the verifying party.

IN SSO, the third party is known as an *identity provider* (IDP) or *identity service provider (IDSP).*

One familiar example is Google Sign-In, part of Google's Identity Platform used by millions of people to log into a growing range of social media, web applications, and websites. Business users may also be familiar with more corporate-oriented service providers such as Microsoft's Active Directory or the Linux-based Lightweight Directory Access Protocol (LDAP).

SSO verification works like this:

1. The user visits the website or opens the application.
2. The site or app contacts the SSO provider to verify authentication. If the user's been authenticated, user access is granted.
3. If the user hasn't been authenticated, they are routed to the SSO solution to log in.
4. The user logs in.
5. The SSO system contacts the identity service provider or authentication system to verify the

user's identity.
6. Once verified, the SSO solution sends the authentication data to the website or application and grants user access.
7. The site or application passes authentication information throughout the site or application as the user moves through them, verifying access as they go.

SSO uses tokens to maintain user credentials across websites and applications. As long as the user is logged in and authenticated with SSO, they won't need to login again for connected websites and applications that use the same system during their session.

Identifying True SSO Solutions

It's important to distinguish a true Single Sign-On system from similar technology known as *password vaulting,* which allows for access to multiple sites and applications with a single set of credentials, but requires users to log in each time they move to a new site or program.

Because they operate on user-established rulesets and protocols, SSO systems can grant user-specific access to company-specified websites and applications through a login portal without the need for multiple logins. SSO systems can be cloud-based or on-premises, and use what's known as *federation* to integrate with the company's identity provider of choice.

This federated SSO connects with Active Directory, LDAP, etc., which stores the user's credentials, including:

- Username and password
- Domains and applications the user is allowed to access
- Specific areas and activities permitted within the specified sites and programs (e.g., a user may have access to review legal documents but does not have editing capabilities).

SSO uses specific security protocols, such as Security Assertion Markup Language (SaML) or Open Authorisation (OAuth), to establish and secure the trust relationship between the company's systems, the SSO solution, and the IDP.

Another security protocol known as *multi-factor authentication* (MFA) is quickly becoming an essential part of the SSO authentication process as well; it enhances security by introducing an additional two-factor backup for passwords (such as verification from a mobile device) to protect accounts from unauthorised access.

> "An increasingly mobile workforce generates strong demand for access from not just multiple locations but multiple platforms and devices. IT teams can simultaneously provide an improved user experience and secure, real-time remote access using SSO—while still maintaining user identity and access control."

Major Benefits of SSO

With proper implementation, SSO offers powerful benefits. Higher productivity, simpler IT support and monitoring, and greater security are achieved through multiple process improvements.

Easier Onboarding

SSO solutions allow for HR to provide a single login for all company-related Web and application access, connected to IT policies for both the user and any groups they may be a part of within the organisation. User activity can be monitored and updated as required, without the need to update multiple accounts.

Streamlined IT Management

An increasingly mobile workforce generates strong demand for access from not just multiple locations but multiple platforms and devices. IT teams can simultaneously provide an improved user experience and secure, real-time remote access using SSO—while still maintaining user identity and access control.

Bringing together current and legacy applications (such as an on-premises Enterprise Resource Planning (ERP) system, a cloud-based procurement solution, and a marketing Web portal) using SSO makes it possible for users to access everything they need to do their jobs without having to switch to a different username for each task.

Flexible, scalable security makes it easy to provide contextual access for users to minimise risk while preserving convenience and functionality. For example, a certain employee may have full access to financial data and applications in the office, but limited access to high-value data and intellectual property when on a tablet or phone outside the company's intranet. IT spends less time resetting forgotten passwords and correcting human errors, and more time on high-value tasks.

On the other end, users struggling with password fatigue and a growing number of applications and websites in their daily workflows experience less stress, and have higher productivity, when they can login once to obtain access to everything they need (and none of the things they don't). They also present a far smaller security risk to the company, as forgotten, insecure, or (worst of all) shared passwords are eliminated.

Reduced Help Desk Costs

Given that large companies can spend up to **a million dollars each year** on password resets alone, making the switch to SSO can make an appreciable difference by slashing help desk calls from day one.

Tips for Implementing SSO

A successful implementation strategy for SSO requires some careful forethought and planning. You can increase the likelihood of success by:

- Identifying the applications and websites within the scope of SSO integration.
- Review and replacement, as necessary, for applications that don’t support SSO.
- Selecting a single identity provider for your entire user base (e.g., Active Directory, Google Identity, LDAP, etc.).
- Selecting the appropriate SSO security protocols, including MFA. Incorporate MFA with SSO implementation to avoid wasted time and work-hours integrating these services after the fact.
- Creating group-based access, password, and activity policies for the selected applications and websites within the SSO solution, with exceptions for individuals as warranted.
- Providing adequate training and review for users.
- Monitoring security protocols for vulnerabilities and updating as required.

SSO Helps You Combat Waste, Stress, and Inefficiency

Users don’t want to remember a forty-digit code with seven umlauts and an irrational number just to access their email. On the other hand, no one wants a phrase like “PWord1234” standing as the only barrier between corporate espionage or a major customer data breach. By enhancing user experience while simultaneously reducing IT costs and workload, SSO strikes the right balance for companies looking to modernise their approach to identity management.

About **PurchaseControl**

PurchaseControl is cloud based procurement software for business spend management. We empower businesses by providing greater transparency and oversight into the purchasing process. With PurchaseControl, you have the flexibility to manage how spend actually happens instead of how you wish it would happen.

The entire PurchaseControl team has experience within a range of businesses, and as such, we bring a practical, holistic approach to purchasing. We understand what it takes to run a business and apply that knowledge to make PurchaseControl as effective as possible for all users.

Learn more at www.purchasecontrol.com

Contacts

EU Office Information

UK: +44 845 591 27 24

Ireland: +353 1 513 4623

enquiry@purchasecontrol.com

US Office Information

US: 800 737 5605

inquiry@purchasecontrol.com

Connect With Us

Facebook: https://www.facebook.com/PurchaseControl/

Twitter: https://twitter.com/purchasecontrol/

LinkedIn: https://www.linkedin.com/company/purchasecontol/