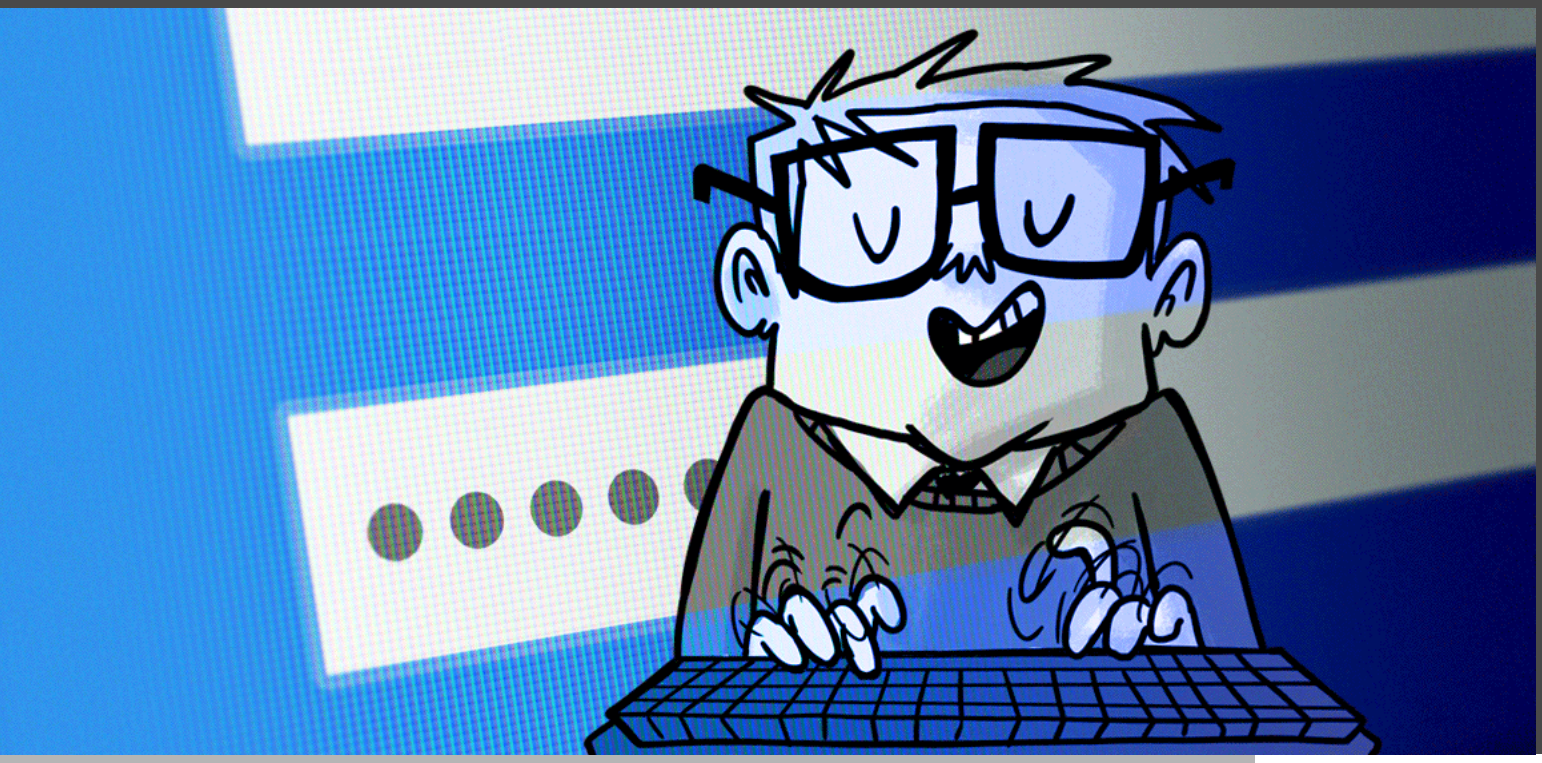
Devolutions

10 Reasons to Strengthen Identity Security with Single Sign-On (SSO)

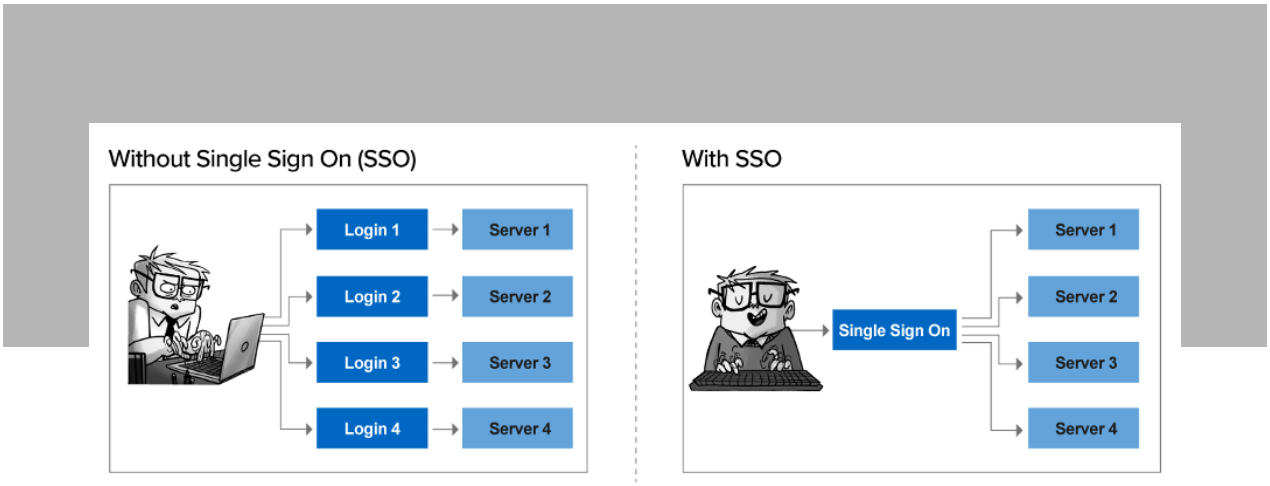


WE ARE LIVING THROUGH HISTORIC TIMES

We are living through historic times. I can't believe that one day we will tell our kids: "I remember when people fought for toilet paper during the COVID-19 pandemic." Or actually, our kids may be even more shocked when we say: "I remember when some companies didn't use SSO to strengthen identity security."

What Is SSO?

Every time a user logs in to an application, it opens a door for hackers. Single sign-on (SSO) enables users to log in one time with a single set of credentials, and then access all of the apps, data, and websites for which they have permission. For example, Devolutions Account supports SSO, and with a single login, users have access to all of Devolutions' web services, including Customer Portal, Online Database, Online Drive, Online Backup, Installer Service, Forum, and our Affiliate Program.



Here are 10 reasons to strengthen security identity with SSO:

1. Increase overall security

SSO uses various identity standards (e.g., SAML 2.0, OAuth, SCIM, and OpenID Connect) to securely transmit user access and provisioning information. Using SSO with role-based access control (RBAC) and two-factor authentication/multifactor authentication (2FA/MFA) greatly enhances an organization's identity security.

2. Enforce strong password policies

Passwords continue to be one of the weakest links in the cybersecurity chain. For example, 80% of hacking-related breaches involve compromised and weak credentials, 59% of people use the same password for multiple accounts (and most use the same password for as long as possible), and 34% of employees share passwords at work. SSO helps reduce the risk of poor password management practices by eliminating the need for multiple passwords, and at the same time forcing end users to only choose suitable complex passwords or passphrases.

3. Reduce password fatigue

The average end user must keep track of a whopping 191 passwords. SSO reduces password fatigue by allowing end users to choose and remember a single password (provided, of course, it is suitably strong as discussed

above). Having to remember that many passwords is an almost impossible task which increases the risk of reusing the same password. It also increases the risk of passwords being leaked by storing them in unsecured locations that aren't managed by IT, such as text files or post-it notes.

4. Enhance user experience

The average business user must input their credentials for various websites and apps 154 times per month (and for some business users the number is much higher and can run into the thousands per month). SSO eliminates this tedious and time-consuming task, which makes users more productive and happier.

5. Accelerate the adoption of desired apps

SSO makes resources readily available in a single location, which increases end user adoption of organization-promoted apps.

6. Reduce IT workload

Today's IT teams are stretched thin and forced to constantly do more and more, but with less and less budget and resources. SSO reduces IT workloads, since end users don't need to keep opening help desk tickets because they forgot their password (yet again). This also saves money. Research has found that a single password reset costs companies an average of $70, and that 20%-50% of all help desk calls are for password resets.

7. Deprovision ex-users

With SSO, end users — including workers, contractors, partners, and others who are no longer with the organization — can be deprovisioned quickly, or even automatically.

8. Increase speed

SSO is particularly helpful for organizations where large numbers of departments and people demand quick and unrestricted access to the same applications (e.g., emergency services and hospitals).

9. Prevent shadow IT.

With SSO, Sysadmins can monitor the cloud-based apps end users are accessing and prevent unauthorized downloads.

10. Support compliance

Deploying SSO can help organizations meet specific criteria associated with various regulations, such as SOX (IT controls must be documented data controls), HIPAA (users who access electronic records or require audit control must be authenticated), and PCI DSS (integrated with Active Directory to ensure a proper user identification mechanism for users).

SSO: The Drawbacks

There are challenges with every solution, and SSO is no exception. Some of its drawbacks include:

1. One ring (or password) to rule them all

If an SSO account is hacked, other accounts under the same authentication are also vulnerable. To fortify this single point of failure, it is essential to use strong, unique passwords or passphrases, and to use a 2FA or an MFA.

2. When SSO is down, access to connected sites is also down

An SSO system must be highly reliable, and there must be a solid backup plan for dealing with breakdowns.

3. SSO can take longer than expected to set up

Implementing SSO is like IKEA furniture — it can look simple, but once you start putting all the pieces together, you realize that it's quite complicated (though unlike IKEA furniture, organizations that implement SSO don't have to solve every problem with an Allen Key!). SMBs that do not have in-house expertise in this area should work with an MSP to make sure their SSO is implemented and managed correctly.

The Bottom Line

While SSO is not flawless, the benefits far outweigh the drawbacks, and as such all organizations — including SMBs, who are increasingly under attack — should make this a top priority.