



BARRIERS TO SINGLE SIGN-ON (SSO) ADOPTION FOR SMALL AND MEDIUM-SIZED BUSINESSES



Overview

To better understand barriers and catalysts of single sign-on (SSO) adoption, the Cybersecurity and Infrastructure Security Agency (CISA) engaged with various stakeholders involved with SSO. These include SSO vendors, experienced managed service providers, non-profit organizations dedicated to improving cybersecurity, and small and medium-sized businesses (SMBs) that have experience with adopting SSO and migrating across SSO platforms. Based on these discussions, CISA found that despite the benefits of SSO, the adoption of SSO capabilities for identity management remains low, particularly among SMBs. Numerous obstacles can hinder the successful implementation of a workable SSO solution. These include cost, technical hurdles, and a lack of awareness and resources.

ADVANTAGES OF SSO ADOPTION

SSO is a user authentication and access control system that allows users to access multiple applications, tools, and systems with just one set of credentials. By centralizing the authentication process, SSO streamlines identity management and simplifies the user experience by only needing to remember one username and password for all accounts. SSO can bolster security measures as it decreases the frequency of users having to input their login credentials. Furthermore, SSO can reduce password duplication across various platforms, consequently reducing the potential for password leakage.

SSO improves user experience relative to other access management solutions such as individual usernames and passwords, making it more likely that users will properly implement security measures. Users can easily enable and disable the capability to enter multiple systems, platforms, apps, and resources. Also, it may effectively resolve the problem of password-related downtime and reset expenses. When properly implemented and configured, SSO technology offers numerous advantages to SMBs in terms of improving cybersecurity.

SSO ADOPTION CHALLENGES FACED BY SMBS

Despite the benefits, the rate of SSO adoption by SMBs is limited for several reasons:

- Small enterprises often opt for manual passwords and hands-on approaches over an SSO option. These methods tend to be more cost-effective in terms of the purchasing cost, which does not include the hidden cost associated with administrative overhead. A primary reason for the difference in the purchasing cost is that SSO is often available only as a premium enterprise-level service. Such a service (a) can cost significantly more per user than a lower-tier service without SSO and (b) typically requires a minimum number of users. These can be substantial barriers for many organizations.
- A lack of technical know-how and awareness poses another significant barrier to SSO adoption. Vendors feel confident that they offer sufficient training materials and how-to guides to support customers in effectively deploying SSO technology. However, customers have different perceptions and user experiences. Customers see SSO as a complex solution with numerous moving parts that may impede its successful deployment. These implementation challenges need to be addressed before customers consider adopting SSO.
- Customers have varying degrees of satisfaction with the accuracy and completeness of support materials and instructions. Even some of the more experienced and technically savvy users have needed to submit numerous support tickets and engage in multiple interactions with their vendor's customer support staff to fill gaps or

resolve inaccuracies and omissions. For SMBs with limited resources, the opportunity cost of that time makes the pursuit of proper SSO implementation prohibitively expensive and results in a negative user experience.

- Regarding technological awareness, vendors often see SSO as a minimum standard security practice that all organizations should follow regardless of size or industry. They emphasize its benefits beyond security (e.g., potentially reducing cyber insurance costs for SMBs). However, customers have differing perspectives. Some see it as adding value that improves their security posture, while others view it as an unnecessary expense that does not deliver significant operational improvement and commensurate returns. The latter view may reflect a lack of awareness of all the benefits SSO may provide and highlights the need for clear messaging on its advantages.

RECOMMENDATIONS FOR SMBS

Implementing a systematic approach to SSO will facilitate SSO deployment in SMB environments. We recommend SMBs use an approach such as the following. Start by analyzing the organization's needs, such as the number of users, applications, and security requirements. This assessment will help determine the most suitable SSO solution. Look for affordable options (e.g., cloud-based solutions that do not require extensive infrastructure). Compare the features and compatibility of different SSO solutions provided by the many vendors in the market. Evaluate how well the solutions integrate with existing infrastructure and applications. Conduct a pilot project to minimize risks and test the solution's effectiveness before rolling it out to the entire organization. Train the staff and provide clear guidelines for password management and security practices. Continuously monitor the SSO solution to strengthen the overall security posture.

RECOMMENDATIONS FOR VENDORS

Based on user feedback, vendors can significantly improve their service offerings by implementing the following recommendations. Vendors should (a) gather customer requirements and offer tailored solutions that meet their needs, while eliminating unnecessary services; (b) offer more flexible seat thresholds or requirements; and (c) improve the accuracy and completeness of support materials for their essential set of services such as SSO.

First, basic and essential services such as SSO should be decoupled from bundles with premium services. Vendors should avoid upselling techniques, whereby they sell unnecessary services to SMBs. While product bundling is a recognized pricing strategy to extract maximum consumer surplus, the need for essential cyber services to protect and defend critical infrastructure and cyber-poor, target-rich organizations should not be leveraged to upsell premium services that may not have the same appeal or value-added. Instead, they should encourage customers to request additional services to improve their overall security standing when needed.

Second, vendors should provide a more flexible schedule of seat thresholds or requirements that would allow a meaningful service tailoring based on organization size. Specifically, for SMBs, special consideration should be given for pooling SSO licenses at the MSP level or SMB-group level rather than the individual subscriber organization level.

Third, it is crucial that vendors offer SMBs any necessary support and training. To reduce the number of call-ins and amount of technical support required by SMBs to properly implement and maintain SSO, the quality of the instructions given to users upfront should be significantly improved. In their user experience feedback, users consistently emphasized that instructions are incomplete, vague, and often inaccurate. The latter factor is a barrier not only to SSO adoption, but also manifests itself when the existing users attempt to migrate platforms. Jointly these three factors (i.e., the inclusion of SSO in bundles with premium services, inflexible seat thresholds and requirements, and inaccurate and incomplete instructions) result in a negative user experience, which negatively influences adoption decisions for potential SSO adopters.

CISA'S SSO STUDY

A detailed overview of the barriers and catalysts for SSO adoption is included in the CISA report, [Barriers to Single Sign-On \(SSO\) Adoption for Small and Medium-Sized Businesses: Identifying Challenges and Opportunities](#). The report summarizes views of vendors and customers and provides a set of recommendations for encouraging SSO adoption.