WHITE PAPER

5 CRITERIA FOR SELECTING AN EFFECTIVE SSO SOLUTION FOR SHARED MOBILE DEVICES

BlueFletch

OVERVIEW

The frontline workers in sectors like retail, transportation, manufacturing, and warehousing face the increasing challenge of managing multiple applications on shared mobile devices. Single Sign-On (SSO) technology simplifies this complexity by enabling users to access all necessary applications with a single set of credentials.

This white paper explores the criteria for selecting an SSO solution that enhances productivity, reduces support calls, and ensures robust data security for Android apps in shared workforce environments.

> **Goal:**
>
> Understanding of how SSO can transform the efficiency and security of operations for businesses with shared mobile devices

WHAT IS SINGLE SIGN-ON (SSO)?

Single Sign-On (SSO) is a user authentication process that allows individuals to access multiple applications using one set of login credentials.

This technology eliminates the need for users to remember and enter separate usernames and passwords for each application used, streamlining the login process and enhancing the overall user experience.

> *Single Sign-on eliminates the need for users to remember and enter separate usernames and passwords for each application*

By providing a single point of entry, SSO simplifies access to a suite of tools and systems, making it an ideal solution for environments where frontline employees frequently switch between different applications, such as the retail floor or in the warehouse.

The concept of SSO is not new; it has evolved over the past two decades, initially serving as a convenience feature for IT environments with numerous standalone applications. As the digital landscape expanded and the number of applications required by users grew, the need for a more seamless and secure method of accessing these tools became apparent.

This led to the development of modern SSO solutions, which not only simplify the login process but also enhance security by reducing the number of attack surfaces—each additional password is a potential entry point for unauthorized access.

Early on, SSO systems were often proprietary and confined within organizational boundaries. As the internet and cloud computing grew, federated SSO emerged, allowing users to access resources across different domains and organizations using a single identity.

Technologies such as Security Assertion Markup Language (SAML), OpenID Connect, and OAuth played a significant role in this transition, enabling secure and standardized ways to manage identities across various web services.

SSO IN SHARED WORKFORCE DEVICE ENVIRONMENTS

In sectors like retail, transportation, and logistics, shared devices are an operational necessity. Employees often use the same handheld scanners, tablets, or smartphones to complete tasks such as inventory management, order fulfillment, and customer service.

This frequent device sharing introduces unique challenges, particularly in authentication methods. Efficient and secure authentication is crucial in these environments to maintain operational continuity and protect sensitive information.

> *Efficient and secure authentication is crucial in these environments to maintain operational continuity and protect sensitive information.*

Single Sign-On (SSO) emerged as a powerful solution to address these challenges by simplifying and securing the login process across multiple applications on shared devices.

Efficient Authentication

In fast-paced sectors, time is a critical factor. Workers often switch between tasks and devices, making traditional login processes cumbersome and time-consuming.

SSO reduces the need for employees to remember and enter different credentials for each application, thus speeding up the login process. For instance, a warehouse worker can access inventory, shipping, and employee communication apps without the need to log in separately to each one.

This efficiency not only saves valuable time but also minimizes disruptions in workflow, enhancing overall productivity.

Security Enhancement

Shared device environments are particularly vulnerable to security risks. Multiple users accessing the same device increase the likelihood of unauthorized access and data breaches.

SSO addresses these risks by centralizing the authentication process. This approach reduces the risk of compromised passwords and strengthens the overall security posture. Moreover, with SSO, IT departments can more easily enforce strong password policies and update access rights, ensuring that only current employees have access to the necessary applications.

Seamless User Experience

A significant challenge in shared device environments is maintaining a seamless user experience across different shifts and roles. SSO simplifies this by allowing users to access all their required apps through a single authentication event.

This consistency is crucial for reducing training time and minimizing errors, especially in high-turnover sectors like retail and transportation. Employees can transition smoothly between tasks without the frustration of multiple logins, leading to higher satisfaction and lower error rates.

Management of Multiple Credentials

In environments where employees need access to various applications, managing multiple credentials can lead to inefficiencies and security vulnerabilities.

SSO simplifies credential management by reducing the number of passwords each user needs to remember and maintain. This not only decreases the likelihood of password-related support calls but also streamlines the process of onboarding new employees and revoking access for those who leave the company.

FIVE CRITERIA FOR SELECTING AN EFFECTIVE SSO SOLUTION FOR SHARED MOBILE DEVICES

When selecting a Single Sign-On (SSO) solution for shared mobile devices, particularly in sectors like retail, transportation, and logistics, it is essential to choose a system that meets the specific needs of these environments.

Here are the five key criteria to consider when evaluating SSO solutions for shared mobile devices, particularly those running on Android:

1. **Compatibility with Android Apps**

   Android dominates the mobile operating system market, especially in rugged and shared devices used in shared environments. An ideal SSO solution should seamlessly support Android and web applications, ensuring that employees can access all necessary apps without compatibility issues.

   This involves basic login functionalities and deeper integrations with Android-specific features such as biometrics, NFC, and system-level permissions. The SSO system should be tested across different versions of Android to guarantee consistent performance on both older and newer devices, as frontline workforces often use a mix of device generations.

2. **Ease of Integration**

   The ability to integrate smoothly with existing systems and applications is critical for any SSO solution. This criterion is about minimizing the need for extensive custom development, which can be costly and time-consuming. Look for SSO solutions that offer standard integration protocols like SAML, OpenID Connect, or OAuth.

   These standards facilitate easier and more reliable integration with a wide-range of enterprise applications, from legacy systems to modern cloud-based services. Additionally, the SSO provider should offer APIs and SDKs that allow for flexible and scalable integrations, enabling businesses to adapt the solution to their evolving needs without major disruptions.

3. **Security Features**

   Security is paramount in any authentication solution, especially in shared device environments where the risk of unauthorized access is elevated. A robust SSO system should employ advanced encryption methods to protect user credentials and session data both in transit and at rest.

Security features like risk-based authentication, which adjusts security measures based on the user's behavior and context, can further enhance the protection of sensitive data.

Additionally, session security is important in shared environments. A solution should be able to clean cached data, sessions, logins and cookies when the shift is complete so the shared device is ready for the next user.

4. User Experience

The success of an SSO solution in a shared device environment heavily relies on its impact on the user experience. A seamless login experience that minimizes disruptions to the workflow is essential.

This means reducing login times and eliminating the need for multiple password entries throughout the workday. An effective SSO solution should provide a smooth transition between apps and services, maintaining session continuity even when switching between tasks or devices.

The design should be intuitive, with clear prompts and minimal steps required for authentication, ensuring that even less tech-savvy users can navigate the system effortlessly. Password-less authentication, such as using biometrics or near field communication (NFC) badges on the device is also a consideration, especially in situations where quick reauthentication is needed to reestablish a user session.

5. Support and Maintenance

Finally, the level of technical support and maintenance services provided by the SSO solution vendor is a crucial factor. In high-pressure industries, any downtime or technical issues can lead to significant operational disruptions.

Therefore, choose a vendor that offers reliable, responsive technical support and proactive maintenance services. This includes regular updates to address security vulnerabilities, compatibility patches for new Android versions, and quick responses to any emerging issues. A vendor with a strong track record of customer support and a comprehensive service level agreement (SLA) will ensure that the SSO system remains operational and effective over time.

Selecting the right SSO solution for shared mobile devices requires careful consideration of these five criteria. By focusing on compatibility with Android apps, ease of integration, robust security features, a seamless user experience, and reliable support and maintenance, businesses can ensure that their SSO system enhances operational efficiency and security in their shared device environments.

BENEFITS OF IMPLEMENTING SSO

Implementing Single Sign-On (SSO) in shared workforce environments offers numerous benefits that can transform the way organizations operate.

1. **Productivity and Efficiency**

   SSO significantly enhances productivity by streamlining the login process across multiple applications. In shared device environments, employees frequently switch between tasks and applications, and each login interruption can consume valuable time.

   By enabling a single authentication event to access all necessary applications, SSO reduces the time wasted on repetitive logins. This consolidation allows employees to focus more on their core tasks without the disruption of frequent password prompts.

   As a result, workflows become more efficient, and employees can handle their responsibilities faster and with fewer errors, leading to improved operational outcomes.

2. **Reduced Support Calls**

   One of the most immediate impacts of implementing SSO is the reduction in support calls related to password issues. Traditional setups, where employees must remember multiple passwords, often lead to frequent password resets and account lockouts, burdening IT support teams.

   With SSO, the complexity of managing multiple credentials is eliminated, drastically lowering the incidence of these problems. This not only reduces operational costs by freeing up IT resources from routine password reset requests but also enhances overall service quality as IT teams can focus on more strategic initiatives rather than routine support.

3. **Enhanced Security**

   While simplifying access, SSO also substantially improves security. By reducing the number of passwords that employees need to remember, SSO encourages the use of stronger, unique passwords for the initial login.

   Data and session clearing on the device prevents a shared device from carrying over operational data in environments users share devices.

4. **Cost Savings**

   The financial benefits of implementing SSO are substantial and multifaceted. The time saved on multiple logins across different applications translates directly into labor cost savings.

   For instance, reducing the average login time can save minutes per employee each day, which accumulates over thousands of employees and devices to represent significant annual savings. Moreover, as mentioned, the reduction in support calls also leads to operational cost savings. Organizations can reallocate these resources to more productive uses.

   According to industry studies, the implementation of SSO can lead to savings of hundreds of dollars per device per year through improved efficiency and reduced IT support costs.

SUMMARY

By choosing the right SSO solution for your shared mobile devices, you position your frontline workforce for success, ensuring a secure, efficient, and user-friendly operational environment.

For those ready to get started or seeking more guidance, BlueFletch offers expertise and support to ensure a smooth transition to a more efficient and secure authentication system. For more information and personalized assistance, we invite you to contact BlueFletch.

Effective organizations recognize that the investment in new mobile technology can be substantial.

ABOUT BLUEFLETCH

Based in Atlanta, BlueFletch is an award-winning innovator in the mobility industry, focused on helping enterprises secure, manage, and support their shared and rugged workforce devices.

The BlueFletch Enterprise platform is trusted by the Fortune 1000 in retail, transportation, healthcare, logistics, and warehousing as well as organizations worldwide.

Providing a customized launcher, SSO, Support/Analytics, and Device Tracking and management for Android workforce devices, BlueFletch Enterprise helps ensure an organization’s digital transformation or management initiatives are effective and secure.

Learn more at https://www.bluefletch.com