SSO vs MFA/2FA—and the cost of insecure logins

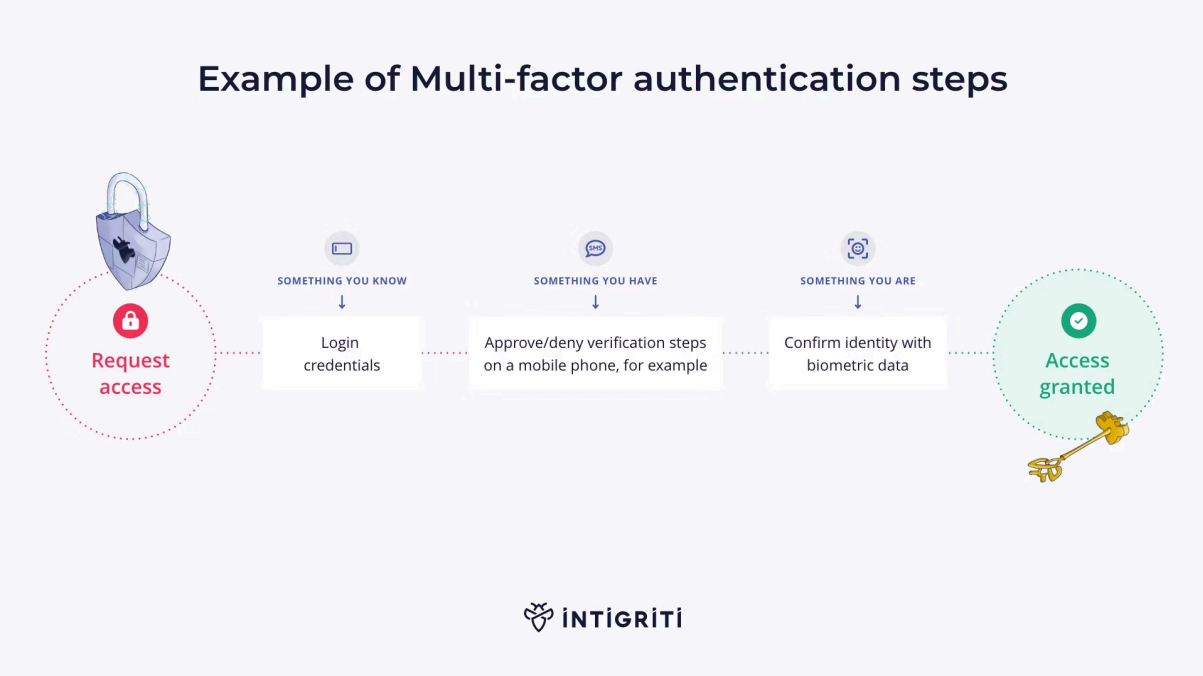
BY ANNA HAMMOND · SEPTEMBER 26, 2024 · LAST UPDATED ON MARCH 6, 2025

Between 2004 and 2024, passwords topped the list as the most frequently leaked type of data. It's safe to say that this security measure alone isn't enough to fend off cybercriminals. Fortunately, many businesses recognize this issue as an increasing number of organizations are adopting stronger authentication methods, such as single sign-on (SSO), multi-factor authentication (MFA), and two-factor authentication (2FA).

That may be a lot of acronyms to remember, but you needn't worry. This guide will help you understand the meaning of each solution, the benefits of combining them, and why doing nothing could come at a greater price.

What is SSO vs MFA vs 2FA?

In short, SSO allows users to login to multiple systems with a single set of credentials whereas 2FA and MFA focus on enhancing security through multiple verification steps.



Implementing MFA

Many in the IT community have expressed frustration that some SaaS vendors only offer SSO at an additional cost or with enterprise pricing. Further, Microsoft reports that its systems deflect over 1,000 password attacks every second, demonstrating the persistent threat of cyberattacks. Crucially, more than 99.9% of the accounts that have been successfully compromised do not have MFA enabled.

These instances highlight the criticality of strengthening weak login processes with more robust authentication methods. Let's discuss the pros and cons of each solution below.

SSO explained

SSO allows users to log in once and gain access to multiple applications or systems without needing to log in again. This streamlines the login process and reduces the need for multiple passwords, improving both security and user experience.

What are the benefits of SSO?

The key benefits of SSO include:

- **Improved user experience:** Users only need to remember one set of credentials, reducing the hassle of managing multiple usernames and passwords. This makes it easier to access various applications and services.
- **Increased security:** SSO reduces the risk of password fatigue, which can lead to users creating weak passwords or reusing them across different platforms. With SSO, users are less likely to write down passwords or use simple, easy-to-guess words or combinations.
- **Centralized control:** IT administrators can manage user access to multiple applications from a single, centralized point. This makes it easier to enforce security policies and monitor user activity.
- **Reduced IT costs:** With fewer password-related issues, the number of help desk requests decreases, freeing up IT resources for other tasks and reducing operational costs.
- **Streamlined access management:** SSO simplifies the process of granting or revoking access to applications. When a user leaves the organization, IT can disable a single account to cut off access to all connected systems.
- **Enhanced productivity:** Users can quickly switch between applications without having to log in each time, saving time and increasing productivity.
- **Better compliance:** SSO helps in tracking user activity across different applications, making it easier to meet regulatory compliance requirements and internal auditing standards.
- **Reduced phishing risks:** Since users only enter their credentials once, the risk of phishing attempts capturing login information is significantly reduced.

Overall, SSO provides a more secure, efficient, and user-friendly way to manage access to multiple applications and services.

Does SSO have security risks?

While single sign-on offers numerous benefits, it also comes with certain security risks, including:

- **Single point of failure:** If the SSO system goes down, users may lose access to all connected applications.

- **Potential vulnerability:** If an attacker gains access to SSO credentials, in theory, they could then access all connected systems.
- **Implementation complexity:** Properly implementing SSO can be technically challenging and time-consuming.

Given these risks, one might ask: is it better to have SSO or not? For most businesses, implementing SSO is beneficial over not having it. The advantages of improved user experience, enhanced security, and centralized control generally outweigh the risks.

What is 2FA/MFA?

2FA/MFA is a security process where users must provide two or more different forms of identification to access an account or service. Imagine you're at a party, and someone asks, "Why do you have both a lock and a deadbolt on your front door? Isn't one enough?" You reply, "Well, a lock is good, but a deadbolt adds an extra layer of security. If someone tries to pick the lock, the deadbolt makes it much harder for them to get in."

Multi-factor authentication works in much the same way. Think of your password as the lock—it's a good first line of defense, but it can sometimes be picked or compromised. 2FA/MFA acts like that deadbolt, providing an additional layer of security that makes it significantly harder for anyone to gain unauthorized access to your accounts.

2FA vs MFA: What’s the difference?

You may have noticed by now that throughout this guide we’ve grouped 2FA and MFA together—why is that? The methods are similar, but there is a small difference. Mainly, MFA can involve more than two factors, such as something you know (like a password), something you have (like a security token), and something you are (like biometric data). This additional layer enhances security by making it harder for unauthorized users to gain access.

What are the benefits of MFA?

There are several MFA benefits. For example, it provides:

- **Enhanced security:** By requiring multiple forms of identification, MFA adds an extra layer of security, making it much harder for unauthorized users to gain access to your accounts.
- **Protection against weak passwords:** Even if a user's password is compromised, having MFA in place can prevent unauthorized access, as the malicious actor would need the second factor to gain entry.
- **Reduced risk of identity theft:** By requiring additional verification, MFA helps protect users' personal information and reduces the likelihood of identity theft.
- **Compliance with regulations:** Many industries have regulations that require robust user authentication. Implementing MFA can help businesses meet these compliance requirements.
- **Improved user trust:** When users see that a service takes security seriously by implementing MFA, it can increase their trust and confidence in that service.

- **Early fraud detection:** In some cases, MFA can alert users to attempted fraud. For example, if a user receives a verification code via SMS without trying to log in, they know someone else is attempting to access their account.
- **Protection against common cyberattacks:** MFA can help protect against common cyberattacks like phishing, keylogging, and brute-force attacks, as simply obtaining a user's password is not enough to gain access.

These benefits are clearly being realized by businesses today. According to JumpCloud's 2024 IT Trends Report, 83% of organizations now require MFA in addition to password-based authentication.

Does MFA come with challenges?

While multi-factor authentication has many benefits, there are some challenges to consider. These include:

- User inconvenience due to additional authentication steps
- Complexity in setting up and managing the systems
- Potential costs
- The need for user education
- Recovery issues if users lose access to their second factor.

To overcome or mitigate these challenges, organizations can utilize user-friendly MFA solutions that minimize inconvenience. They can also invest in robust implementation and management tools to simplify the process, allocate resources for user education and support, and ensure there are reliable recovery options for users. By addressing these areas, businesses can maximize the benefits of MFA while minimizing the associated challenges.

The bottom line: Should you implement the double-lock system?

Like every system, SSO and MFA comes with advantages and disadvantages—but ultimately, these methods provide an extra layer of security for businesses that make it much harder for hackers to gain unauthorized access to user accounts.

Additionally, your employees will thank you. Instead of juggling multiple logins, users can access various applications with a single sign-on, reducing frustration and increasing efficiency. This centralized management also simplifies the enforcement of security policies and monitoring of user activity, ensuring consistent security measures across all platforms. Furthermore, with fewer password-related problems, IT support teams can focus on more critical tasks, leading to better resource allocation and overall operational efficiency.

Finally, many industries have regulations requiring robust authentication methods. Implementing MFA and SSO helps organizations meet these compliance requirements, avoiding potential legal issues and fines.

In summary, the long-term benefits make investing in these solutions well worth it. Have you already taken advantage of SSO and MFA, yet? Intigriti's platform includes these security features by default. Want to get a feel for what else you can do on our platform? Simply head to our demo page today for a free tour!

Frequently Asked Questions

How to enable two-factor authentication (2FA) on the Intigriti platform

For a detailed step-by-step guide on how to enable Two-Factor Authentication (2FA), please visit our knowledge base article here.

How to enable Single Sign-On (SSO) on the Intigriti platform

For a detailed step-by-step guide on how to set up Single Sign-On (SSO), please visit our knowledge base article here.

Can I enable Two-Factor Authentication (2FA) on the Intigriti platform if Single Sign-On (SSO) is already enabled?

SSO provides a secure login process for your Intigriti account, and 2FA is managed through your organization's existing security protocols. Therefore, you can't manage 2FA directly within the Intigriti platform.