SSOJet

WHITEPAPER

SSO - BUILD VS BUY: MAKING THE RIGHT CHOICE FOR YOUR BUSINESS

www.ssojet.com

Introduction

Single Sign-On (SSO) - Build vs. Buy is the decision-making process businesses undergo to determine whether to create a custom solution or purchase a ready-made one. This article explores the benefits and drawbacks of each approach, as well as key factors to consider when making this decision.

Single Sign-On (SSO) is a popular authentication mechanism that enables users to access multiple applications with a single set of login credentials. SSO solutions have become increasingly popular in recent years, as they offer several benefits, including improved security, increased user convenience, and reduced costs.

When it comes to implementing an SSO solution, organizations have two main options: building an SSO solution in-house or buying an SSO solution from a third-party vendor. Both options have their advantages and disadvantages, and organizations need to carefully evaluate their requirements, resources, and expertise before deciding which approach to take.

In this blog post, we will explore the advantages of buying an SSO solution over building an SSO solution in-house. We will examine how buying an SSO solution can offer faster time-to-market, lower costs, expertise, scalability, and integration.
Let's dive in and explore the benefits of buying an SSO solution in more detail.

What is SSO?

SSO stands for Single Sign-On, which is an authentication mechanism that enables users to access multiple applications or systems using a single set of login credentials. With SSO, users do not need to remember multiple login credentials for different applications, which improves user convenience and productivity.

In an SSO setup, a user's login credentials are verified by a central authentication server, which then grants access to all the authorized applications or systems. This eliminates the need for users to log in separately to each application or system, saving time and reducing the risk of password fatigue, which can lead to weak or compromised passwords.

SSO can be implemented using various authentication protocols such as OAuth, OpenID Connect, SAML, and Kerberos. These protocols enable secure communication between the authentication server and the application or system, ensuring that only authorized users can access the resources.

SSO solutions have become increasingly popular in recent years, as they offer several benefits, including improved security, increased user convenience, and reduced costs. Organizations can either build an SSO solution in-house or buy an SSO solution from a third-party vendor, depending on their requirements and resources.

SSO : Build vs Buy

Single Sign-On (SSO) is a popular method of authentication that allows users to access multiple applications with a single set of credentials. It eliminates the need for users to remember multiple passwords and improves security by reducing the risk of credential theft. When it comes to implementing SSO, organizations have two options: build it in-house or buy a third-party solution. In this blog, we will explore the pros and cons of each approach to help you decide which option is right for your organization.

Build SSO In-House

Building an SSO solution in-house requires a significant investment of time, resources, and expertise. The process involves developing custom code, designing authentication protocols, and integrating with existing applications. Here are some of the pros and cons of building SSO in-house:

Pros:

- **Customization:** Building an SSO solution in-house allows organizations to tailor the solution to their specific needs. They can design the authentication protocols, user interface, and integration points based on their unique requirements.
- **Control:** Organizations have complete control over the SSO solution when they build it in-house. They can modify and update the solution as needed without relying on third-party vendors.
- **Flexibility:** An in-house SSO solution can be updated and modified as needed to meet changing business needs or to accommodate new applications or systems. This flexibility can be particularly valuable for organizations that are experiencing rapid growth or change.

- **Security:** An in-house SSO solution can be designed with security as a top priority. By controlling the design and implementation of the solution, the organization can ensure that the solution is as secure as possible, minimizing the risk of data breaches or other security incidents.

Cons:

- **Expertise:** Building an SSO solution requires specialized expertise in security, authentication protocols, and application integration. Organizations may need to hire or train staff with these skills.
- **Time:** Developing an SSO solution in-house can take months or even years, depending on the complexity of the solution and the resources available.
- **Maintenance:** Once the SSO solution is built, organizations are responsible for maintaining it, including updates, bug fixes, and security patches.
- **Cost:** While building an SSO solution in-house requires a significant upfront investment, it can require more investment in the long run.

Buy a Third-Party SSO Solution

Alternatively, organizations can buy a third-party SSO solution. These solutions are typically cloud-based and offer a range of features and integrations. Here are some of the pros and cons of buying a third-party SSO solution:

Pros:

- **Time-to-Market:** Buying a third-party SSO solution can significantly reduce the time-to-market compared to building a solution in-house. These solutions are typically pre-built and ready to integrate with existing applications.
- **Expertise:** Third-party SSO vendors have expertise in security, authentication protocols, and application integration. Organizations can rely on their expertise instead of building it in-house.
- **Maintenance:** Third-party SSO vendors are responsible for maintaining the solution, including updates, bug fixes, and security patches.
- **Saves time and resources:** Implementing a third-party SSO solution can save an organization time and resources as it eliminates the need to develop and maintain a custom-built SSO system.
- **Improved security:** Third-party SSO solutions are usually designed to provide a high level of security, such as encryption and multi-factor authentication, which can enhance security and reduce the risk of data breaches.
- **Integration with multiple applications:** A third-party SSO solution can integrate with a wide range of applications, including cloud-based and on-premises applications.

Cons:

- **Limited Customization:** While third-party SSO solutions offer a range of features, organizations may be limited in their ability to customize the solution to their specific needs.
- **Dependence on the third-party vendor:** When using a third-party SSO solution, organizations are reliant on the vendor for ongoing support, maintenance, and upgrades.
- **Data privacy concerns:** When using a third-party SSO solution, an organization's sensitive data may be stored in a third-party system, leading to potential data privacy concerns.

Advantages of buying SSO solution over building SSO in-house

Buying a Single Sign-On (SSO) solution from a third-party vendor can offer several advantages over building an SSO solution in-house. Here are some of the key advantages of buying an SSO solution:

- **Faster Time-to-Market:** Implementing an SSO solution can be a time-consuming process, requiring specialized skills and expertise. Building an SSO solution in-house can take several months or even years, depending on the complexity of the solution and the resources available. On the other hand, buying an SSO solution from a third-party vendor can significantly reduce the time to market. These solutions are typically pre-built and ready to integrate with existing applications, which means that organizations can implement SSO more quickly and efficiently.

- **Lower Costs:** Building an SSO solution in-house can be expensive, requiring significant investment in resources, expertise, and infrastructure. Organizations need to hire or train staff with specialized skills, purchase software and hardware, and invest in ongoing maintenance and support. In contrast, buying an SSO solution from a third-party vendor can be more cost-effective in the long run. These solutions typically offer a subscription-based pricing model, which means that organizations can avoid upfront costs and only pay for what they use. They can also avoid ongoing licensing fees and vendor lock-in.

- **Expertise:** Implementing an SSO solution requires specialized expertise in security, authentication protocols, and application integration. Building an SSO solution in-house can be challenging, particularly for organizations without this expertise. On the other hand, third-party SSO vendors have expertise in these areas and can provide organizations with the support and guidance they need. They can help organizations choose the right authentication protocols, ensure compliance with industry regulations, and provide ongoing maintenance and support.

- **Scalability:** SSO solutions need to be scalable to meet the changing needs of organizations. Building an SSO solution in-house can be challenging to scale, particularly for organizations with limited resources. Third-party SSO vendors, on the other hand, have the infrastructure and resources to scale SSO solutions quickly and efficiently. They can provide organizations with the scalability they need to meet their changing requirements.

- **Integration:** Implementing an SSO solution requires integration with existing applications, which can be a complex and time-consuming process. Building an SSO solution in-house requires expertise in application integration, and organizations need to ensure that their SSO solution integrates seamlessly with their existing applications. On the other hand, third-party SSO vendors have experience in integrating with a wide range of applications, and their solutions are typically pre-built to integrate with popular applications. This means that organizations can implement SSO more quickly and efficiently.

Conclusion

Both building an SSO solution in-house and buying a third-party solution have their pros and cons. Organizations need to evaluate their specific requirements, resources, and expertise before deciding which approach to take. In general, building an SSO solution in-house is best suited for organizations with specialized requirements and the resources and expertise to develop and maintain the solution. Buying a third-party SSO solution is best suited for organizations that require a fast time-to-market and a range of pre-built features and integrations. Whatever approach you choose, implementing an SSO solution can significantly improve security and user experience.

SSO With SSOJet

Integrating SSOJets into your B2B SaaS product can provide your customers with a simplified and personalized Single Sign-On (SSO) experience. With just a few lines of code, your customers can configure their SSO solution on their own, without requiring extensive technical knowledge or additional support from your team.

SSOJets supports commonly-used authentication protocols like OIDC and SAML, which allows for easy integration with Identity Providers (IDPs). In addition, SSOJets also enables social login SSOs, which allows users to authenticate using their social media credentials. To provide a seamless SSO experience, SSOJets offers customizable login boxes that can be embedded into your SaaS offering. These login boxes are designed to reduce in-app friction and enable users to authenticate smoothly, gaining quick access to your application.

By leveraging SSOJet's SSO components, you can customize the login box's appearance, making it consistent with your brand's identity and providing a personalized user experience. SSOJet's end-to-end SSO solution also ensures the security of user data by supporting multi-factor authentication and single logout, and adaptive authentication. This comprehensive solution minimizes IT overhead by enabling centralized user management and access control.

Overall, integrating SSOJets into your B2B SaaS product can help streamline the user authentication process, enhance user experience, and ensure the security of user data. With a customizable login box and a comprehensive SSO solution, SSOJets provides a complete end-to-end SSO solution for modern SaaS applications.

WHITEPAPER

Top 5 Auth0 Alternatives for SSO

SSOJET.COM

In this document, we will explore the top five Auth0 alternatives for SSO, and discuss the key features that these solutions offer. We will look at the benefits of each solution and help you understand which one is best for your needs.

Are you looking for an alternative to Auth0 for your Single Sign-On (SSO) needs? Look no further! While Auth0 is a popular choice for managing user authentication and authorization, there are other SSO providers that may better suit your business needs.
In this blog, we'll explore the top 5 Auth0 alternatives for SSO. Each of these providers offers unique features and benefits, so you can choose the one that best fits your requirements. From ease of use to customization options, we've got you covered. So let's dive in and explore the SSO along with top Auth0 alternatives for SSO!

What is Auth0?

Auth0 is a powerful platform that offers authentication and authorization services for SaaS applications, making it easier for developers to authenticate and authorize users using various methods. These include single sign-on (SSO), multi-factor authentication (MFA), and social logins, which can be integrated into both web and mobile applications.
This platform provides identity access management (IAM) capabilities, which ensures secure configurations for every authorization request and workflow. With Auth0, you can easily configure login behavior and create a seamless authentication experience for your users.

Auth0 also offers a comprehensive management dashboard, which can be used to administer user accounts and permissions. This platform comes with a host of features including passwordless authentication, user management, user profile storage, and token-based authentication, which can all be used to secure and manage access to applications and APIs.

One of the biggest advantages of Auth0 is its ability to support various types of applications and frameworks, making it highly versatile and customizable. With its flexible pricing options, Auth0 can easily fit into any budget, making it accessible to both small and large organizations.

Problem with Auth0

Like any other platform, Auth0 also has its limitations. For instance, while it provides robust security features, it can be challenging to set up and use for beginners. Moreover, customization options are limited, which may not meet the needs of highly complex projects.

Another major issue that customers have reported with Auth0 is its lack of pricing transparency. Many users have experienced unexpected and significant price increases, particularly when requesting essential B2B features such as custom domains, RBAC, and organizations, or when their businesses start to grow.

This lack of transparency can be especially challenging for early-stage B2B companies, which may not have the financial resources to allocate a large portion of their runway toward a single contract.

What are the best alternatives?

As we have discussed earlier in this article, Auth0 is a popular Identity and Access Management (IAM) solution that provides a range of authentication and authorization features for applications and services. However, it may not be the right fit for every organization or use case.

Fortunately, there are several alternatives to Auth0 that offer similar capabilities, as well as unique features and benefits. In this blog post, we will explore some of the best alternatives to Auth0 and compare their pros and cons to help you make an informed decision. We'll explore the top 5 competitors of Auth0 for SSO, namely workOS, Frontegg, KeyCloak, Fusion Auth, and SSOJet.

Each of these providers offers unique features and benefits, so you can choose the one that best fits your requirements. We'll provide a brief description of each provider, the pricing offered, and the pros and cons. You can also check out the list of popular SSO solutions and their details for B2B saas. Now let's dive in and explore the top competitors of Auth0 for SSO!

• WorkOS

Despite being founded just three years ago in 2018, WorkOS has already become a favorite among developers and companies seeking to enhance their applications with enterprise-level features. Although online reviews and updates are limited at this point, the company already boasts an impressive list of clients, including WebFlow, Eden, and AirBase.

The WorkOS API platform offers a range of building blocks to help developers quickly add enterprise features to their applications. These building blocks include an admin portal, SAML integration, and a directory sync feature. One of the standout features of WorkOS is the ability for clients to access automatically created audit trails (SIEM) with SCIM provisioning and HRIS integration with popular platforms such as Workday and Gusto. This provides businesses with a comprehensive suite of tools to manage user information and access, ensuring optimal security and compliance.

Pricing
WorkOS pricing starts from $125 without branding customization, IT Admin portal, and Support. Contact their sales for Pricing details.

Pros of WorkOS:

- Versatile API platform: WorkOS offers a collection of building blocks to help developers quickly add enterprise features to their applications.
- Secure and customizable admin portal: WorkOS's admin portal provides a secure and customizable onboarding UI, allowing users to programmatically generate onboarding links.
- SAML and directory sync feature: The stack includes APIs with RESTful endpoints, JSON responses, and normalized objects for SAML, enabling single sign-on (SSO) for any identity provider using SAML or Open ID Connect.
- Audit trails and HRIS integration: WorkOS provides automatically created audit trails (SIEM) with SCIM provisioning and HRIS integration with platforms like Workday and Gusto.

Cons of WorkOS:

- Limited online reviews and updates: As WorkOS is a relatively new player in the market, there are limited online reviews and updates available.
- Limited integrations with identity providers: While WorkOS supports SAML and Open ID Connect for SSO, it may not integrate with all identity providers, potentially limiting its compatibility with certain applications.
- Pricing: WorkOS does not provide transparent pricing, which can be a concern for some businesses looking to use the platform.

• Frontegg

Frontegg is a comprehensive platform designed to help companies optimize their customer engagement, product-led growth initiatives, and digital transformation. It provides a range of pre-built, customizable, and self-served components to assist in building and deploying web and mobile applications. Frontegg offers granular role and permission management and supports popular authentication methods such as single sign-on and passwordless (magic links and speedy logins).

The platform's main focus is to provide developers with easy-to-use tools to implement common user management features like onboarding flows, billing management, and analytics. It offers integrations with popular services such as Salesforce, Slack, and Twilio. Frontegg also provides features to manage and secure access to applications and APIs, and its plugin ecosystem enables customers to extend the platform with custom functionality.

Pricing

$99 Starter Package for up to 10 tenants and Growth package up to 50 tenants for $799/month and SSO connections are available only in $799 package only.

Pros of Frontegg:

- Frontegg provides a set of pre-built, customizable, and self-served components for building and deploying web and mobile applications, making it easier and faster for developers to implement user management features.
- The platform offers granular role and permission management, supporting popular authentication methods like single sign-on and passwordless, which can enhance the security and user experience of applications.
- Frontegg offers important integrations with popular services such as Salesforce, Slack, and Twilio, allowing customers to easily leverage these tools within their applications.
- The platform provides a set of features to manage and secure access to applications and APIs, which can help companies ensure the safety of their data and assets.
- Frontegg's plugin ecosystem enables customers to easily extend the platform with custom functionality, which can help meet specific business needs.

Cons of Frontegg:

- The pricing for Frontegg is not transparent and may be a concern for some customers.
- Some users have reported that the UI/UX of the platform could be improved, which may affect the overall user experience.
- The documentation for the platform can be more comprehensive and easier to navigate, which may be a challenge for developers who are new to the platform.

• KeyCloak

Keycloak is an open-source identity and access management (IAM) solution that provides authentication and authorization services for applications and services. It's a standalone server that supports various protocols such as SAML, OAuth 2.0, and OpenID Connect, making it easy to integrate with both cloud-based and on-premises applications and services.

Keycloak comes equipped with several features including user and group management, single sign-on, multi-factor authentication, and identity brokering. The identity brokering feature enables users to authenticate through external providers such as social networks and identity providers. It also has a web-based management console that simplifies managing and configuring the server, along with a set of APIs and libraries that can be used to integrate Keycloak with other applications.

Keycloak is free, open-source software, which means that companies can customize it to suit their specific needs. However, the lack of official support and documentation can make it challenging to use for those without technical expertise. Additionally, it may require additional resources to properly maintain and secure the server.

Pricing
Keyclock is an open source solution, you can host and use.

Pros of Keycloak:

- Keycloak is a powerful open-source solution that provides a wide range of authentication and authorization features.
- It can be easily integrated with a variety of applications and services, both on-premises and cloud-based.
- Keycloak supports multiple protocols, making it a flexible solution for managing user identities across different systems.
- Keycloak offers a web-based management console, which makes it easy to manage and configure the server.
- Keycloak has a large and active community, which means there are plenty of resources and support available.

Cons of Keycloak:

- While Keycloak is free to use, it requires some technical expertise to set up and configure.
- The user interface of Keycloak can be overwhelming for some users.
- The documentation and support for Keycloak can be limited compared to commercial solutions.
- Keycloak may not be suitable for small businesses with limited IT resources.

• Fusion Auth

FusionAuth is an identity and access management (IAM) platform designed to provide authentication and authorization services for web and mobile SaaS applications. It offers flexible deployment options, including cloud-based, on-premises, or hybrid models. The platform is user-friendly and can be easily integrated with other applications.

FusionAuth provides various essential features such as user registration, login, passwordless authentication, single sign-on, multi-factor authentication, and social login. It also includes user management and user profile storage. With its event-based architecture, FusionAuth enables the creation of custom workflows effortlessly.

FusionAuth's API-first architecture makes it easy for developers to integrate and extend the platform with custom functionality. The platform also provides a web-based management console that simplifies the administration of user accounts and permissions.

Pricing
Cloud hosting plans start at $37/month, and self-hosting plans start at $125/month.

Pros of FusionAuth:

- FusionAuth offers a wide range of authentication and authorization services, including user registration, login, passwordless authentication, single sign-on, and multi-factor authentication.
- The platform is designed to be easy to use and easy to integrate with other applications, and it supports cloud-based on-premises or hybrid deployments.
- FusionAuth has an event-based architecture that allows for the creation of custom workflows, as well as a web-based management console for user accounts and permission administration.
- Its API-first architecture enables developers to easily integrate and extend the platform with custom functionality.
- FusionAuth has a free community edition that includes many of its core features, making it accessible to small businesses and startups.

Cons of FusionAuth:

- Some users have reported that the documentation and support resources can be lacking at times, which may require more effort from developers when integrating with the platform.
- The pricing can be complex and may not be transparent, depending on the deployment type and usage levels.
- The user interface may not be as intuitive as other IAM platforms, which could require additional training for non-technical staff.

• SSOJet

SSOJet is specifically designed for modern, fast-moving SaaS companies, making it an ideal fit for B2B tech startups catering to mid to large-scale enterprises. SSOJet is an advanced API platform that enables developers to rapidly create and deploy enterprise-level capabilities such as Single Sign-On (SSO), Directory Sync, Team Management, Multi-Factor Authentication (MFA), and Audit Log. By leveraging SSOJet, SaaS businesses can expedite their transition to Enterprise Ready status, ensuring that their application possesses all the essential features required for seamless adoption across large organizations.

This all-in-one solution streamlines user management for your B2B SaaS, reducing onboarding time and making it easy for new team members to get started. With its simple integration, less code, and hassle-free approach, SSOJet offers modern user management for B2B SaaS. It serves as a customer identity solution, ensuring smooth customer onboarding and authentication.

Pricing
Pricing Start from $99 for 2 SSO connection with all features and no limit of MAUs. Pay As you Go for each SSO connection.

Pros of SSOJet:

- SSOJet is designed for fast-moving SaaS companies and B2B tech startups, which may be a good fit for companies in these industries.
- It is an all-in-one solution for user management that can reduce onboarding time and simplify the process of getting new team members up and running.
- SSOJet offers simple integration with less code, which can be a benefit for developers.
- Its customer identity solution is designed to make customer onboarding and authentication as seamless as possible.

Cons of SSOJet:

- A relatively new solution in the market as compared to its competitors
- Has limited support for programming languages.
- It may not have a feature set or support network as some of its more established competitors.

Conclusion

In conclusion, there are many alternatives to Auth0 for single sign-on (SSO) solutions. Auth0 is a popular and powerful identity and access management platform, but it may not be the right fit for every organization. The alternatives we've discussed - Keycloak, FusionAuth, Frontegg, and WorkOS - each has their unique strengths and weaknesses.

When choosing an alternative to Auth0, it's important to consider your organization's specific needs, budget, and technical expertise. By evaluating these factors and weighing the pros and cons of each option, you can select the B2B identity management solution that's best for your business. Whether you opt for cloud-based or on-premise deployment, the right IAM platform will help you streamline user management, secure your applications and APIs, and provide a seamless authentication and authorization experience for your customers and employees alike.