SSO (Single Sign On)

Single sign-on, or SSO, is one of the best solutions for managing account access and mitigating the problems caused by the growing number of apps and logins.

Gliffy Macro Error

You do not have permission to view this diagram.

When applied at an enterprise level, Single Sign On has a meaningful impact on businesses as following:

Category	Reason	Notes
User	Convenience	Users no longer have to struggle with multiple passwords and remembering which one is for which account
	Productivity	If available apps are easier to access, they will used more effectively.
Security	Reducing Risk	Having only one access point minimizes the likelihood of employees using simple or easy-to-crack passwords
	Compliance	Terns of service agreements are initiated and stored to comply with IT audits
IT	Reduce Help Desk Costs	30% of help desk requests are password resets, a single login reduces the number of authentication problems
	User Management Terms of Service	Tech staff can easily create, delete, or edit accounts across multiple systems

Risk in SSO

If SSO password is cracked, then malicious players also get access to multiple accounts. This is why SSO implementation is paired with

- Identity management and access control
- Multi-factor authentication

Additional features which can make more values

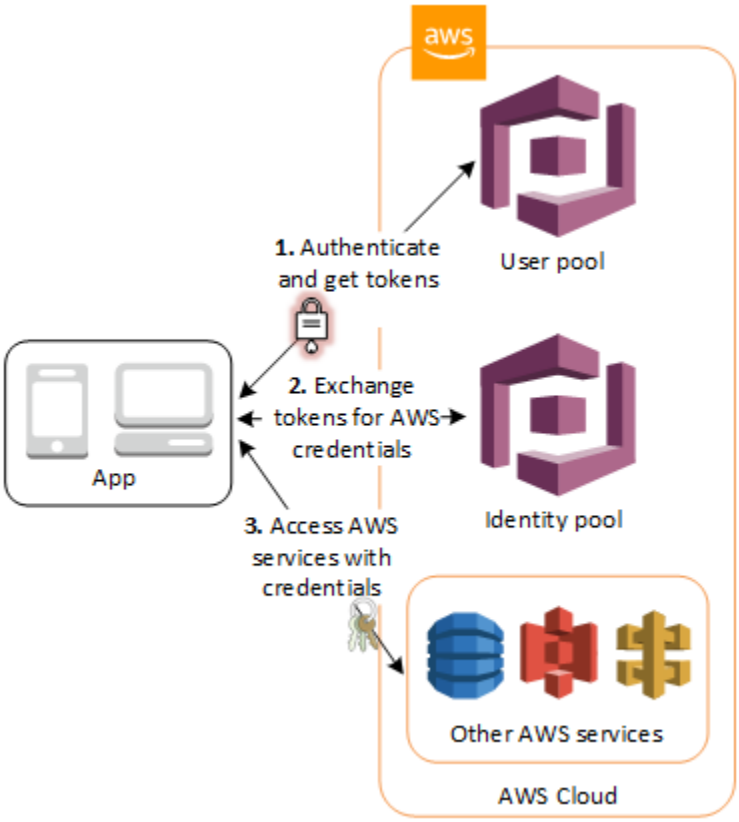
- Mandate SSO Usage - Funneling all logins through a single portal provides a way for access to be effectively monitored and license usage to be audited.
- License Analytics - Accuractely reporting app usage results in smart spending decisions and an average of 30% savings on SaaS costs
- Customizable User Experience - Users can hide, remove, edit, and organize their SSO applications. Setup automatic launch of applications after sign-in
- Integrated Identity and Access Management

Associated technologies

- OAuth — OAuth is simply a secure authorization protocol that deals with the authorization of third party application to access the user data without exposing their password. eg. (Login with fb, gPlus, twitter in many websites..) all work under this protocol.
- SAML (Security Assertion Markup Language) — SAML(Security Assertion Markup Language) allows security credentials to be shared by multiple computers across a network. It describes a framework that allows one computer to perform some security functions on behalf of one or more other computers (Authentication, Authorization)

AWS Cognito

- Amazon Cognito User Pools is a standards-based Identity Provider and supports Identity and Access Management standards, such as Oauth 2.0, SAML 2.0, and OpenID Connect.


aws
User pool
1. Authenticate and get tokens
2. Exchange tokens for AWS credentials
App
Identity pool
3. Access AWS services with credentials
Other AWS services
AWS Cloud