Identity and Access Management

Stephanie Twomey

salesforce
zendesk
Google Workspace
workday
monday.com
zapier
Office 365
JET BRAINS
zoom
ATLASSIAN
greenhouse
ClickUp
Figma

Onboarding/Offboarding without identity providers and SSO

Onboarding: check your email for 20+ emails asking you to set up an account on your first day, hope you don’t forget any of them or you’re gonna have to submit a lot of tickets to IT :)

Offboarding: IT manually checks 20+ apps for accounts and deactivate them one by one.

Name	Email	MS Office	Miro	Monday	Slack	Zoom	Adobe
Jane	x	x	x				
Bob		x		x		x	x

Definitions

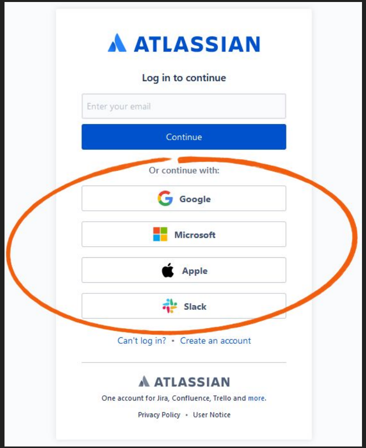
okta

IdP (Identity Provider) - Stores and manages users' digital identity. Some examples are Azure, Okta, and Google

OAuth 2.0 (Open Authorization) - An authorization framework that allows a website or app to access resources hosted by other web apps on behalf of a user. Some examples are the "Log in with Facebook" or "Log in with Google" buttons.

OIDC (OpenID Connect) - Framework that extends OAuth 2.0 with user authentication and Single Sign-On (SSO) functionality

SAML (Security Assertion Markup Language) - An authentication framework for exchanging authentication and authorization data between parties.



ATLASSIAN

Log in to continue

Enter your email

Continue

Or continue with:

Google

Microsoft

Apple

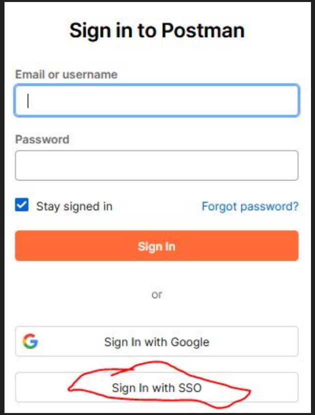
Slack

Can't log in? • Create an account

ATLASSIAN

One account for Jira, Confluence, Trello and more.

Privacy Policy • User Notice



Sign in to Postman

Email or username

Password

☑ Stay signed in Forgot password?

Sign In

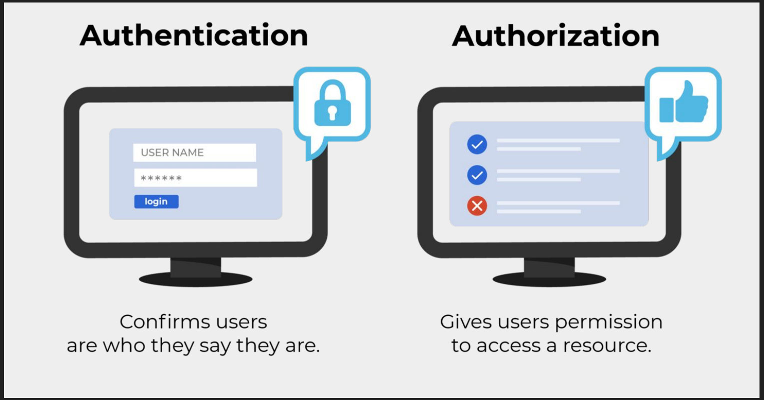
or

Sign In with Google

Sign In with SSO

Important distinction

- Authentication: The act of validating that users are whom they claim to be. This is the first step in any security process. Most common authentication factor is a username and password.
- Authorization: The process of giving the user permission to access a specific resource or function.



Authentication

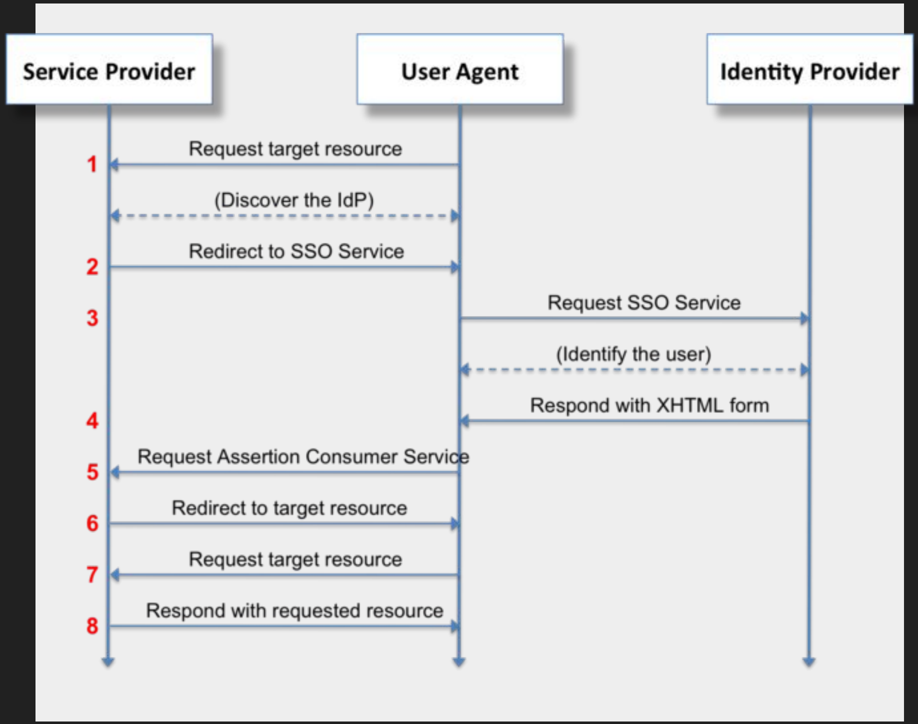
Confirms users are who they say they are.

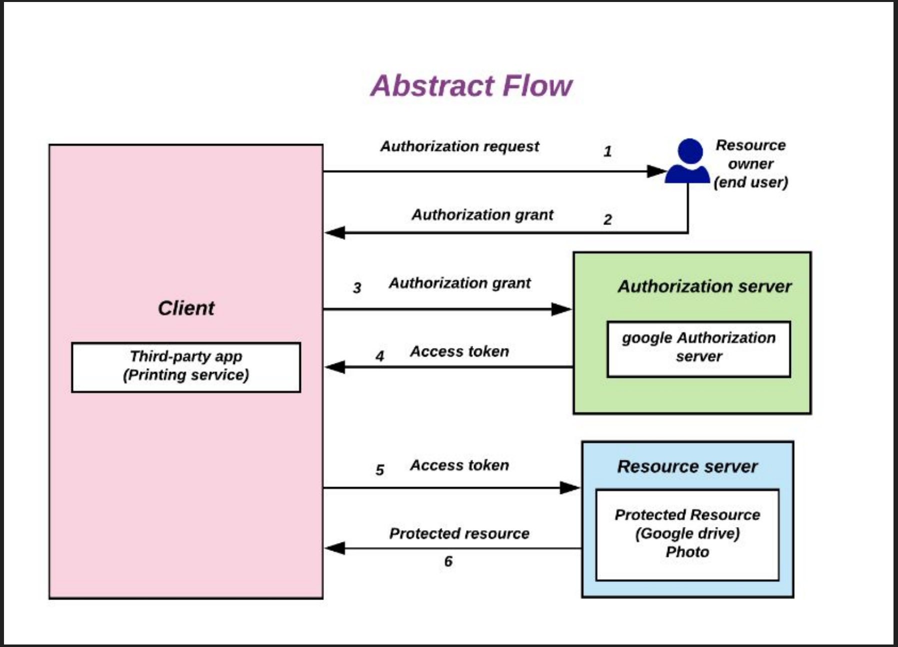
Authorization

Gives users permission to access a resource.

okta

SAML vs OAuth





Why having only one account for everything is actually more secure

- You probably use the same password for everything anyway
- Since you only have one account, you can focus on making that one account very secure
- Better login tracking and metrics
- Less administrative overhead
- Decreases potential attack surface
- Creates a single source of truth

Automating account creation

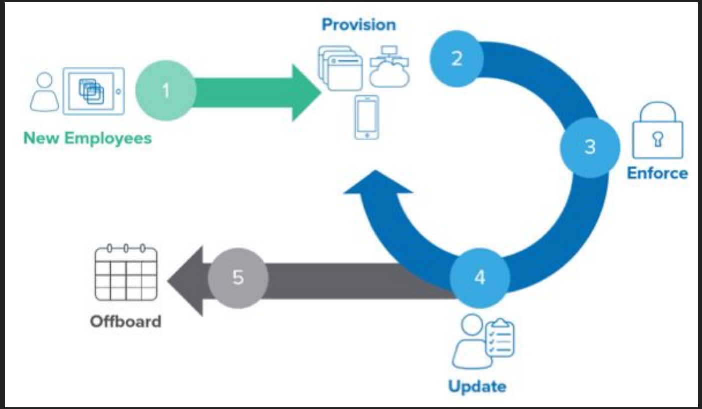
Now, OAuth and SAML are only good for authentication/authorization an existing account. However, it doesn’t create accounts

After granting access to an application in our IdP, how can we automatically create accounts?

With SCIM provisioning!

SCIM

- System for Cross-domain Identity Management, is an open standard that allows for the automation of user provisioning.
- Uses an API to communicate with the SP (Service Provider, or SaaS app) to run CRUD (create, read, update, delete) operations
- SCIM can also sync other information, such as job title or department, for more granular access control



Also, reminder to use MFA

Sources

- https://www.okta.com/identity-101/why-your-company-needs-an-identity-provider/
- https://auth0.com/intro-to-iam
- https://www.okta.com/blog/2017/01/what-is-scim/
- https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management
- https://www.okta.com/identity-101/authentication-vs-authorization/
- https://developer.okta.com/docs/concepts/scim/
- https://developer.okta.com/docs/concepts/oauth-openid/