Auth0 by Okta

Preparing for the New Identity Security Standard

Proposed IPSIE use cases	Auth0 capabilities that meet IPSIE's proposed standards
Single Sign On (SSO)	☑ Single Sign On (SSO)
Lifecycle Management (SCIM)	☑ System for Cross-domain Identity Management (SCIM)
Entitlements	☑ Fine Grained Authorization (FGA)
Session Termination	☑ Universal Logout

How Developers can Get Apps IPSIE-ready using Auth0 tools

Today, SaaS developers are inundated with customer requests for all types of Identity-related integrations that meet the needs of different enterprise Identity providers. To avoid duplicating efforts while staying up to date with the latest security protocols and Identity standards, there needs to be standardized guidance.

Okta spearheaded the creation of a working group within the OpenID Foundation to create the first unified Identity security standard for enterprise apps, resources, and workloads – Interoperability Profile for Secure Identity in the Enterprise (IPSIE).
This is an open industry standard that will enhance the end-to-end security of enterprise SaaS products and provide a framework for builders to more easily meet evolving enterprise security needs. Once finalized, the IPSIE standard will bring together an opinionated set of existing and new standards, covering a wide range of proposed use cases, including Single Sign On (SSO), System for Cross-domain Identity Management (SCIM), Entitlements and Session Termination / Token Revocation.
Okta intends to keep Auth0 in compliance with IPSIE as it evolves, so developers building their apps on Auth0 will be well on the way to achieving the developing IPSIE standards.

Read how developers can get their apps IPSIE-ready using Auth0 tools.

Single Sign On (SSO)

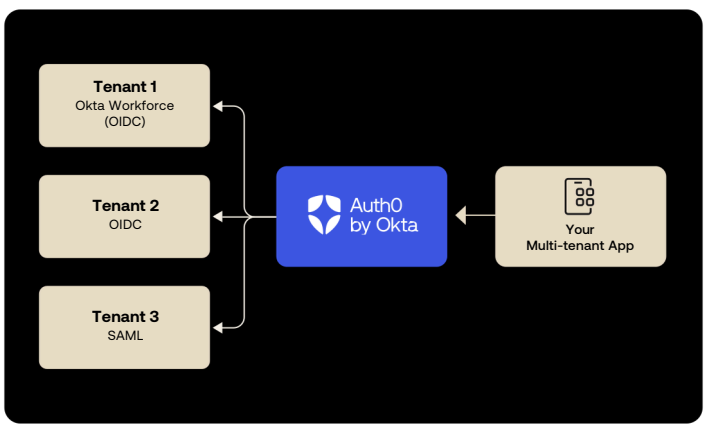
Centralize login, policies, and enforcement.

Single Sign On (SSO) establishes the Identity of the user and then shares that information with each application that requires the data. It provides a seamless experience when using applications and services, as users can simply log in once and access a SaaS provider's full suite of applications.

Different SSO protocols, such as OpenID Connect (OIDC), Lightweight Directory Access Protocol (LDAP), and Security Assertion Markup Language (SAML), share session information in different ways. But the essential concept is the same: there is a central domain through which authentication is performed, and the session is shared with other domains.

Auth0 by Okta uses the OIDC protocol for all Okta Workforce connections. For B2B SaaS businesses, Auth0 supports common Enterprise Federation scenarios such as Microsoft Entra ID, LDAP, SAML, and Ping. For B2C or Customer Identity Access Management (CIAM), it allows authentication through popular social Identity providers, like Google, Facebook, LinkedIn and X to provide frictionless access.

Get started with SSO and try Auth0 for free, or read more in our SSO whitepaper.



Auth0 by Okta

System for Cross-domain Identity Management (SCIM)

Automate user management and prevent security risks like orphaned accounts and shadow directories, avoiding unauthorized access.

System for Cross-domain Identity Management (SCIM) is a set of application-level protocols to securely manage and communicate user and group data across multiple domains, saving IT administration time, reducing the risk of errors and ensuring security policy compliance across all accounts.

Provisioning consists of a set of actions between an identity provider like Okta and the SaaS builder. Using REST-style architecture and JSON objects, the SCIM protocol communicates data about users or groups. With inbound SCIM for Workforce Connection in Auth0, SCIM integration is automated, tracking and implementing to IPSIE's proposed SCIM profile.
Auth0's Inbound SCIM feature supports integrations with enterprise Identity providers including SAML, OIDC, Workforce Identity Cloud, and Microsoft Entra ID. And with Auth0, customers can automate provisioning and deprovisioning for commercial applications and use SCIM to extend to their own internal applications.

Learn how to get started with SCIM and manage provisioning actions between SCIM-enabled cloud applications. Read more about SCIM or try Auth0.

Manage Entitlements using Okta's Fine Grained Authorization (FGA)

Enforce least privilege access and move toward zero standing privileges.

As Authorization becomes more complex, developers will need to incorporate a solution to manage an app's authorization models so that enterprise identity providers can manage entitlements in their app using SCIM. Fine Grained Authorization (FGA) enables developers to design authorization models, from coarse-grained to fine-grained, in a way that is centralized, flexible, fast, scalable, and easy to use. It allows developers to limit user permissions to only what's needed and gain visibility over authorization policies and access control logs, helping to enhance security and manage compliance while spending less developer time building and maintaining authorization.

FGA systems allow developers to manage permissions for billions of objects and users — even permissions that can change rapidly as a system continually adds objects and updates access permissions for its users. FGA delivers authorization at scale and gives businesses the power to simplify access control across multiple applications, parameters, and users. FGA's Domain-Specific Language (DSL) builds a representation of a system's authorization model, which informs FGA's API on the object types in the system and how they relate to each other.

Watch a video overview on Okta's FGA, dive into the technical details of Okta's FGA, add FGA in your Next.js app, or learn how to define an FGA authorization model.

Manage Termination and Token Revocation with Okta's Universal Logout

Immediately terminate all user sessions in response to detected threats.

Universal Logout is an Auth0 feature based on the Global Token Revocation specification. Apps that build an API supporting this specification can allow security management incident tools like Okta Identity Threat Protection in Okta Workforce Identity Cloud (WIC) to send a request to revoke users' sessions and tokens when it identifies a change in risk. This, in the end, supports the mitigation of risks across the ecosystem and can improve security.

Okta customers who use Auth0's Okta Workforce Connections no longer need to build their own global token revocation endpoint. This is done by simply enabling it in Auth0 and providing the endpoint URL to the Okta Workforce admin. When Auth0 receives a request to log out a user from a specific Okta Workforce Connection, it validates the request using the same key set used to validate ID tokens issued from Okta Workforce. It then terminates all Auth0 sessions and revokes all Auth0 refresh tokens for the user. Application sessions need to be revoked which can be done by enabling the OpenID Connect backchannel feature in Auth0.

Okta Universal Logout for Okta Customer Identity Cloud, powered by Auth0, is now in Early Access.