auth0

Release Overview

for Early Access & General Availability in Q1 (January - March 2025)

Safe harbor

This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, global economic conditions have in the past and could in the future reduce demand for our products; we and our third-party service providers have in the past and could in the future experience cybersecurity incidents; we may be unable to manage or sustain the level of growth that our business has experienced in prior periods; our financial resources may not be sufficient to maintain or improve our competitive position; we may be unable to attract new customers, or retain or sell additional products to existing customers; customer growth has slowed in recent periods and could continue to decelerate in the future; we could experience interruptions or performance problems associated with our technology, including a service outage; we and our third-party service providers have failed, or were perceived as having failed, to fully comply with various privacy and security provisions to which we are subject, and similar incidents could occur in the future; we may not achieve expected synergies and efficiencies of operations from recent acquisitions or business combinations, and we may not be able to successfully integrate the companies we acquire; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any products, features, functionalities, certifications, authorizations, or attestations referenced in this presentation that are not currently generally available or have not yet been obtained or are not currently maintained may not be delivered or obtained on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature, functionality, certification or attestation and you should not rely on them to make your purchase decisions.

Opportunities to learn more about our latest innovations and what's to come

Release Overview Webpage

Dive further into the latest innovation and find resources to learn more here.

Connect with the Sales team here.

Auth0 Product Roadmap Webinar

Get a sneak peek of upcoming product releases.

Register for the Auth0 product roadmap webinars here.

Release Highlight videos + Changelog

Get a concise and informative overview of the latest updates, features, and enhancements. Watch the highlights.

See the Changelog here.

Auth0

Customer expectations are changing fast. Auth0 makes it easy for you to deliver seamless experiences that are secure by design.

This quarter's releases empower app builders with:

- Even more functionality included in Enterprise plans
- Powerful extensibility capabilities for more customization
- Security enhancements that give teams the power to protect customers before, at, and after the login box

Spotlights

- Auth0 Platform: Innovations for Secure Experiences
- Auth0 for GenAI
- Enterprise Ready Customer Identity

All features

- Authentication
- Authentication — SaaS Apps
- Authorization
- Security
- Platform

Developer resources

Auth0 Platform: Create great experiences, with Security built in.

Secure Experience

Before Login - Unknown Customer

- Progressive Profiling
- Bot Detection
- Breached Password Detection
- SCIM

At Login - Known Customer

- Passwordless
- Adaptive MFA
- Universal Login
- Social Login
- Organizations

After Login - Repeat, Trusted Customer

- Fine Grained Authorization
- Highly Regulated Identity
- Continuous Session Protection
- Secure APIs
- Universal Logout

Orchestration

Developer Tooling

APIs, SDKs, Quickstarts

Custom Authentication Flows

Forms and Actions

Security Operations

Security Center, Log Streaming

Extensibility

Data Platforms

CDPs and CRMs  Analytics Tools

Applications and APIs

Cloud Apps  Public and Private APIs

Devices

Web and Mobile  IoT

Identities

Human  AI Agents

10B+ Monthly Authentications. *99.99% Uptime.

auth0

*12-month availability, as indicated at trust.okta.com

Early Access

Spotlight: Auth0 Platform: Innovations for Secure Experiences

Better user experiences, stronger security

What is it?

Our latest Auth0 enhancements add increased benefits to current plans that help organizations get Customer Identity right in order to deliver on these experiences. They enable cross-channel continuity, power personalization, and strengthen security and fraud prevention.

Customer Challenge:

Expectations are raising the bar for every experience and every business. Modern digital experiences are driving new customer expectations and reshaping what businesses must deliver to remain competitive. Today's customers expect engaging, convenient, and trusted experiences—that as a business, you understand their unique needs and personalize their offers, provide ease of use across all channels, and can be trusted with their data. To get the experience right, you have to get Customer Identity right.

Why this matters

Protect the user before login:

- Tenant Access Control - Create and manage rules to control access to your application; when a request matches a rule, allow, block, or redirect the request.

Protect the user at login:

- Advanced Customization for Universal Login - The next evolution in customization for Universal Login, empower customers to control every pixel that's rendered on the Universal Login screens.

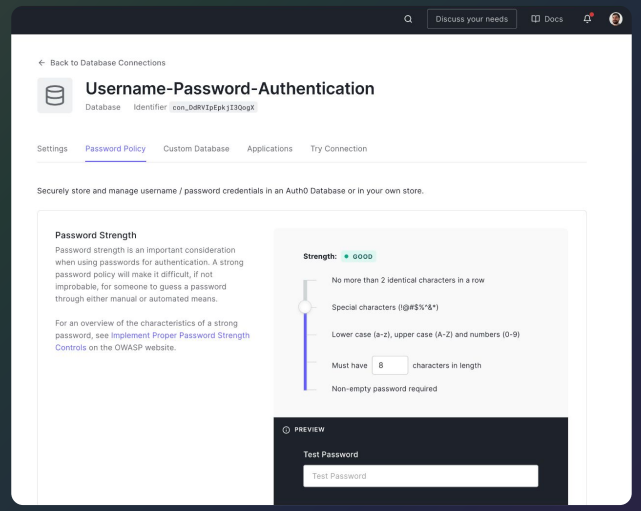
Protect the user after login:

- FAPI 2 Certification - Deliver advanced API protections to protect privacy and prevent transaction tampering.
- CIBA - Also known as a decoupled authentication flow — is a protocol that enables a client application (e.g., call center systems, POS terminals, in-person service tools, or autonomous AI agents) to initiate the authentication process on behalf of the customer. AND, it's included in Enterprise Plans!
- Native to Web SSO – Streamline the customer experience by eliminating the need to re-login when moving from a mobile app to a web app.

How to get it

We hope that these changes make it easier to build, deploy, and scale your app at your pace with the tools you need. Get started with Auth0 free today. If you're an early-stage company, check if you're eligible for our Auth0 for Startups program. We are also proud to offer preferential pricing for nonprofits—making the leading Identity service even more accessible.

Get started



Developer Preview

Spotlight: Auth for GenAI

Build AI into your apps securely

What is it?

Auth for GenAI makes it easier for you to build your GenAI applications securely.

It is a suite of features that allows you to enable your AI agents to securely call APIs on behalf of your users, both interactively and asynchronously, by requesting for the right and least privileged access to users' sensitive information.

Customer Challenge:

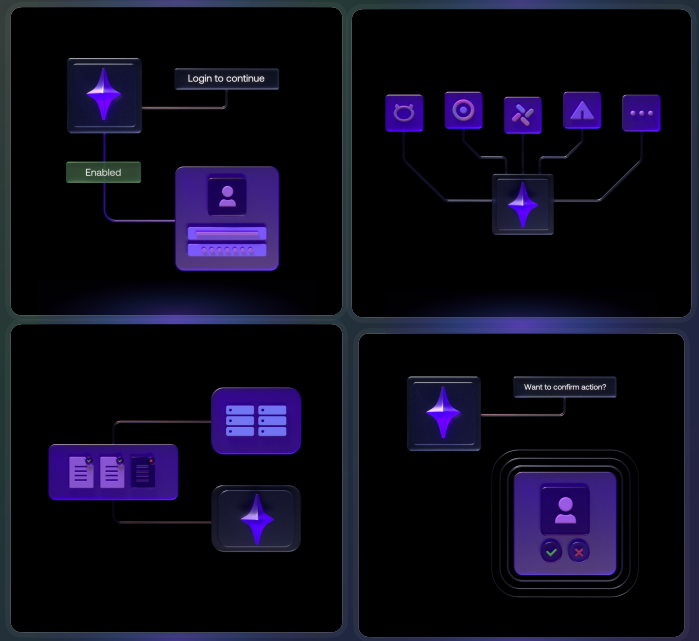
GenAI apps can introduce vulnerabilities because their behavior is non-deterministic. They also rely on UX patterns that are different than those of web/mobile apps. Auth for GenAI provides a streamlined implementation of these patterns, making it easy to protect your app from security vulnerabilities.

Why this matters

- **Authenticate users** - AI agents need to know who the user is in order to have user specific interactions.
- **Call APIs on user's behalf** - As GenAI apps (e.g. chatbots) integrate user products to provide delightful experiences, calling APIs on behalf of users will become a commonplace need. Auth for GenAI helps you to balance a seamless user experience with enhanced security and compliance.
- **Asynchronous workflows** - Async agents (or agent running in the background) may take time to complete tasks or wait for complex conditions to be met. They might require human approval for certain actions and need on-demand authentication to reduce security risks from storing credentials long-term.
- **Authorization for RAG** - GenAI apps enhance responses by using RAG to merge LLM content with real-time data. Authorization for RAG only allows users to access documents they're authorized to view, preventing data leaks.

How to get it

Sign up here to start using the product and be among the first to find out when features become available.



Early Access

Spotlight: Enterprise Ready Customer Identity

Unlock Growth with Enterprise-Ready Customer Identity

What is it?

Auth0, with a suite of enterprise-differentiating identity and access management capabilities, delivers a faster, more efficient, and more cost-effective way to meet stringent enterprise requirements on authentication, authorization and security, enabling you to unlock large enterprise deals.

Customer Challenge:

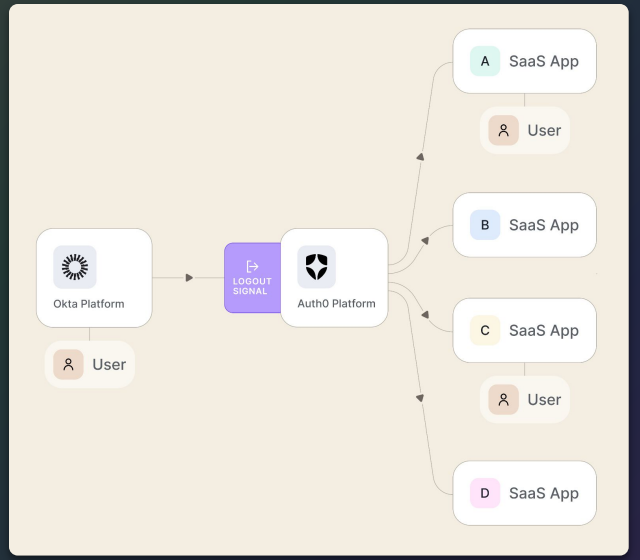
Moving upmarket is essential for B2B SaaS vendors to grow their business, but it isn't easy. In addition to ensuring your core app features meet the needs of enterprise buyers, you also have to satisfy a long list of critical identity requirements. Coding these capabilities in-house requires specialized expertise and substantial engineering resources, diverting focus from your core product feature development.

Why this matters

- Highly flexible, scalable and easy to use authentication and authorization models to build out multi-tenant and fine-grained access control to meet even the most stringent enterprise requirements
- Comprehensive self-service capabilities to delegate core administrative tasks to your business customers, from SSO configuration, to directory provision, to domain verification, reducing burden on your dev team and streamlining management across your customer base
- Enhance security and mitigate risks across your ecosystem by allowing security management incident tools liks Okta Identity Threat Protection to revoke user sessions and tokens when risk level is elevated

How to get it

- Learn more about Auth0 here.
- Get started with Auth0 for free today. Sign up here.
- Check if you're eligible for Auth0 for Startups or for Non-profit programs.



auth0

Auth0 Releases

Auth0 puts security first without sacrificing user experience. It helps organizations adopt technologies that drive growth and offers tools to navigate evolving security threats, protecting both customer and business data.

Learn more about our new Auth0 capabilities released in Q1 2025.

auth0

Security

Early Access

Tenant Access Control List

Feature of: Secure Identity / Available in: Enterprise Plans (1 rule), Attack Protection (10 rules)

The Tenant ACL (Access Control List) feature allows you to create and manage rules that control access to your app. When a request matches a rule, it can allow, block, or redirect the request.

Protect your password reset flow with Breached Password Detection

Feature of: Secure Identity / Available in: Attack Protection

Detect and block compromised passwords during reset to prevent account takeovers.

Learn more

Customer-Provided Signature Public Keys

Feature of: Secure Identity / Available in: Highly Regulated Identity [Limited Early Access]

Facilitate migrating from legacy Identity Providers to Auth0 by allowing Customers to import their legacy public signature keys to their Auth0 tenant.

Breached Password Detection for password reset

Authentication

General Availability

Client Initiated Back-channel Authentication (CIBA)

Feature of: Secure Identity / Available in: Enterprise Plans

A protocol that enables a client application (e.g., call center systems, POS terminals, in-person service tools, or autonomous AI agents) to initiate the authentication process on behalf of the customer.

Optimized TOTP Enrollment for Mobile Devices

Feature of: MFA / Available in: All Paid Plans

For end users enrolling into a Time-Based One-time Password (TOTP) factor on a mobile device, Auth0 skips the QR code and prompts for manual code entry with the QR code as a fall back option.

Learn more

Email OTP Verification

Feature of: Core Platform / Available in: All Plans

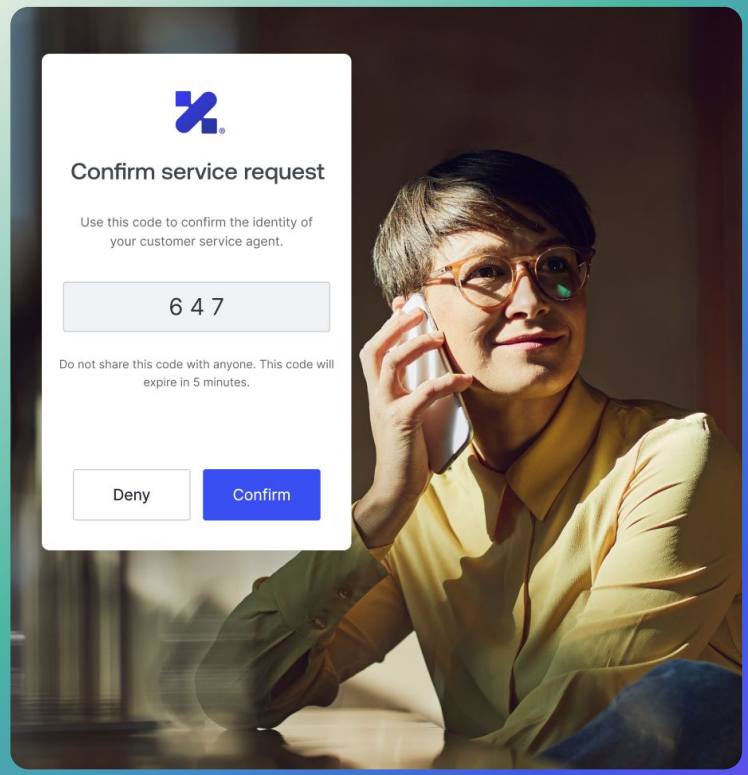
Users are required to enter a One-Time Password (OTP) sent to their email during the signup or password reset process, ensuring email verification happens before account creation or password reset is completed. This offers enhanced security and reducing the chances of mistyped or fake email accounts.

Custom Email Providers

Feature of: Core Platform / Available in: All Plans

Customers can configure custom email providers and customize emails so they can have full control of the email delivery process.

Learn more



CIBA

Authentication

Early Access

Advanced Customizations for Universal Login (ACUL)

Feature of: Consumer Identity / Available in: All paid plans

The next evolution in customization for Universal Login, empower customers to control every pixel that's rendered on the Universal Login screens.

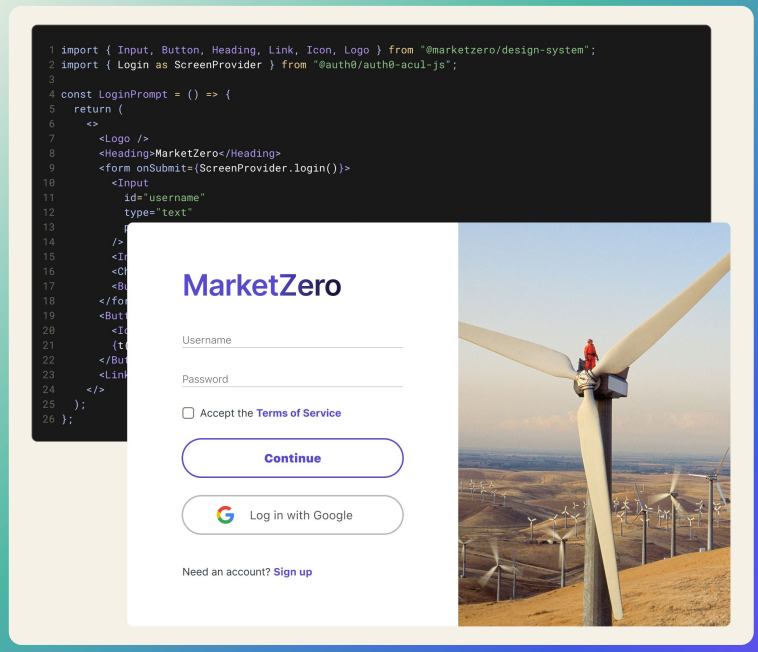
Learn more

Custom Token Exchange

Feature of: Consumer Identity / Available in: Enterprise Plans

Provides a flexible solution using Actions that allows customers to provide their custom logic to control the exchange – i.e. effectively providing the means to implement custom authentication semantics using Actions.

Learn more



Advanced Customizations for Universal Login (ACUL)

Authentication — SaaS Apps

General Availability

Universal Logout Integration Support in Auth0

Feature of: Core Platform / Available in: All plans

Terminate user sessions and revoke refresh tokens for Auth0-powered apps when Identity Threat Protection identifies a change in risk. Configure Universal Logout in Okta, generic SAML and OIDC apps without needing to build a global token revocation endpoint.

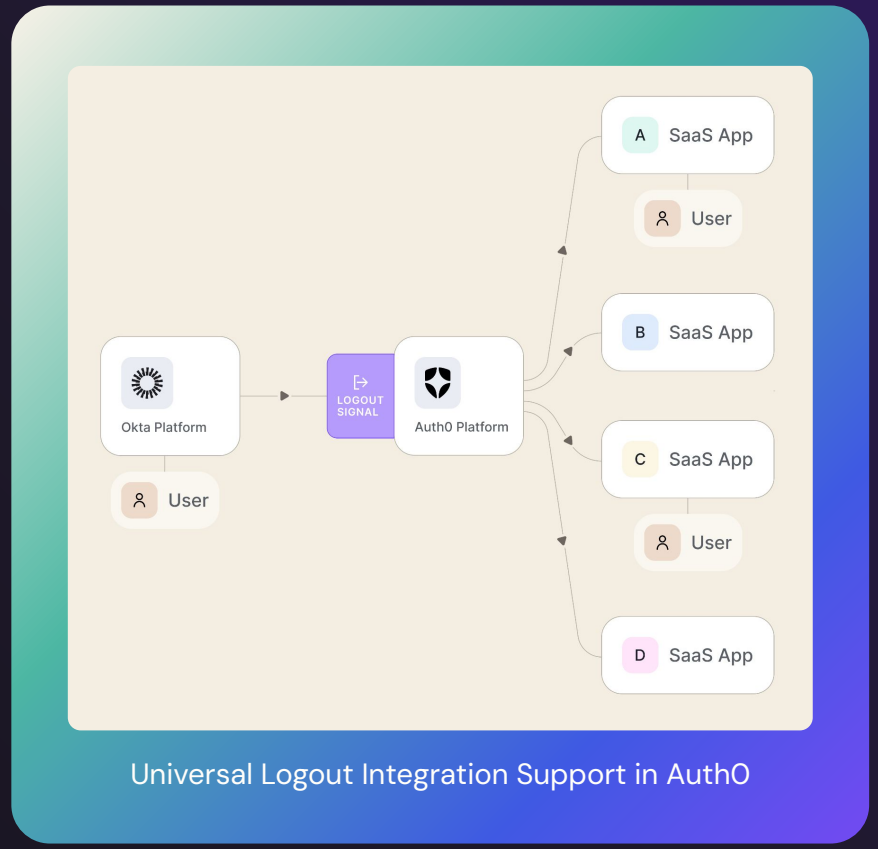
Learn more

Self-Service SSO - Advanced SAML Config & UI Ticketing

Feature of: Enterprise Connections / Available in: B2B Professional and Enterprise Plans

Create SSO tickets from the Dashboard and allow business customers to configure more SAML settings, including Identity Provider (IdP) Initiated SAML requests and SAML algorithm assignment, providing more flexibility and customization.

Learn more



Universal Logout Integration Support in Auth0

Authentication — SaaS Apps

Early Access

Enterprise OIDC Federation Improvements

Feature of: Enterprise Connection / Available in: B2B Essentials/PRO/Enterprise+

A range of new features for the OIDC and Okta enterprise connectors, including federated logout, private key client assertion JWT, additional signing algorithms for ID token verification, and JSON web encryption. Together, these offer more secure authentication methods between Auth0 and external Identity Providers.

Learn more

Self-Service Domain Verification

Feature of: Enterprise Connections / Available in: B2B Professional and Enterprise Plans

A hosted workflow for your enterprise customers to manage home realm discovery and domain verification process on their own.

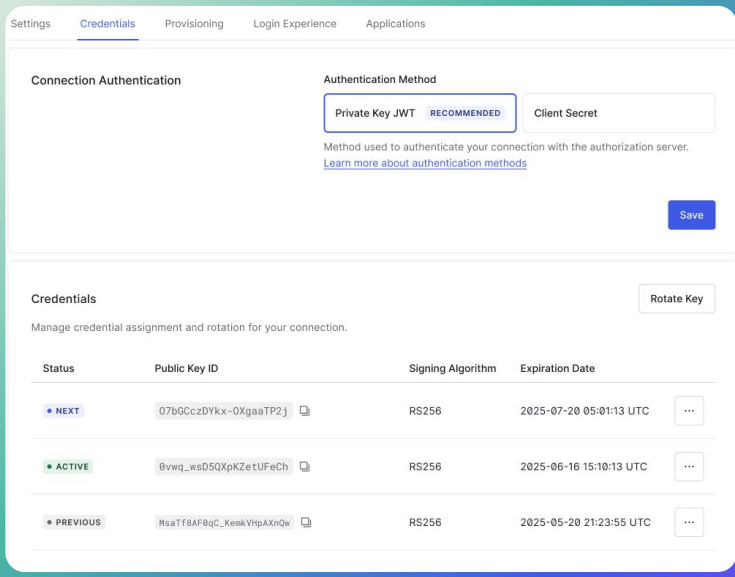
Learn more

My Account Self-Service API

Feature of: Core Platform / Available in all plans

Auth0's new self-service API, enabling customers to build identity management solutions in the context of the user - beginning with authentication method management then followed by, profile management, session management and more

Learn more



Enterprise OIDC Federation Improvements

Authorization

General Availability

Usage Metrics Dashboard

Feature of: Auth0 Fine-Grained Authorization (Auth0 FGA) / Available in: Auth0 FGA

Provides customers with deeper visibility into their authorization usage by helping teams monitor, analyze, and manage their Auth0 FGA consumption efficiently.

Learn more

New Access Controls Using Per-Module Authorization

Feature of: Auth0 Fine-Grained Authorization (Auth0 FGA) / Available in: Auth0 FGA

Enables large organizations to securely share authorization models by specifying which application credentials can update data for specific modules.

Learn more

Usage Metrics Dashboard

Security

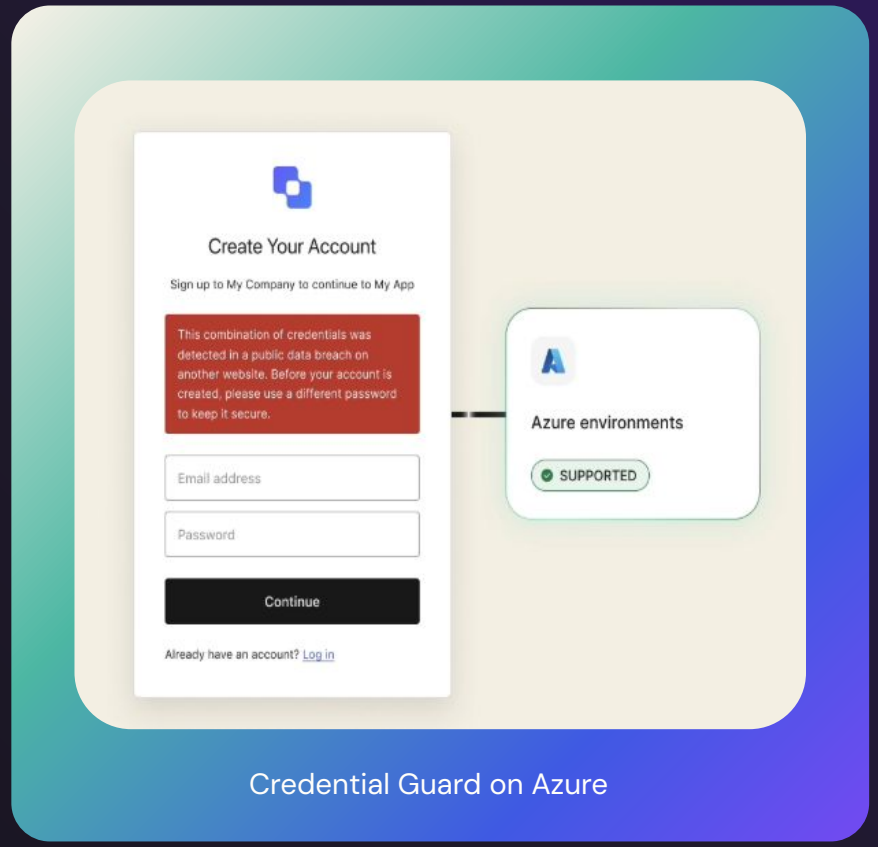
General Availability

Credential Guard on Azure

Feature of: Secure Identity / Available in: Attack Protection

Detect stolen credentials fast to prevent takeovers now available on Azure Private Cloud.

Learn more



Credential Guard on Azure

Platform

General Availability

New Public Cloud Performance Tiers

Feature of: Auth0 / Available in: Public Cloud Performance

Provides additional scaling options for Public Cloud Enterprise Customers, to choose 300 RPS and 400 RPS tiers. Ability to choose higher shared capacity of 200 RPS (1200 RPM) for up to 48 hours a month is already supported.

Private Cloud Performance - 10,000 RPS

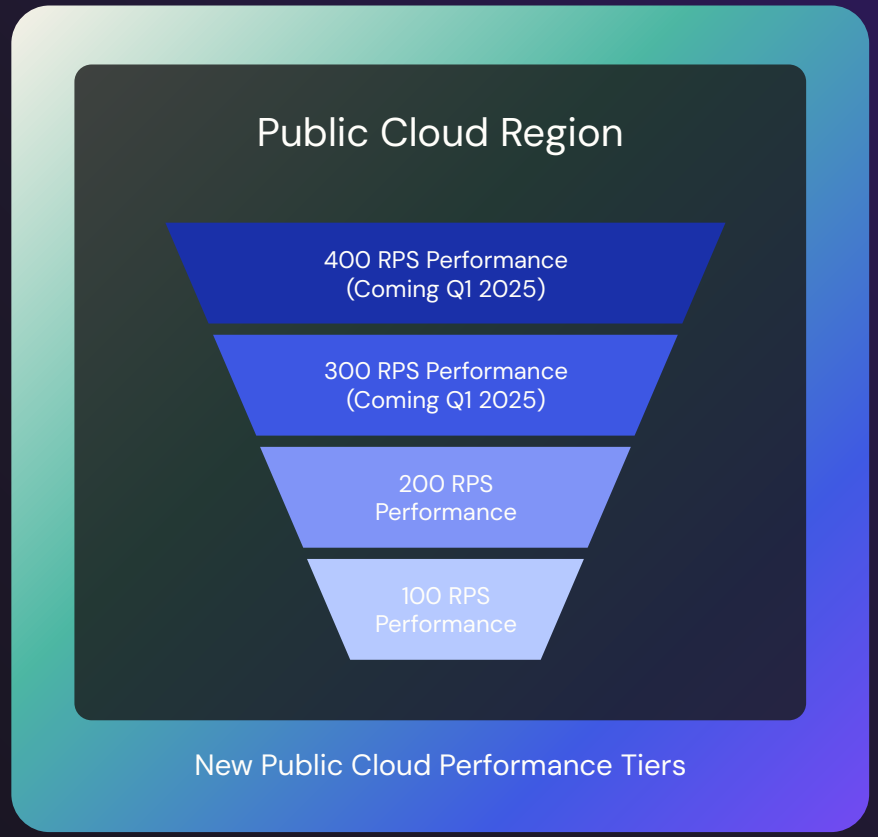
Feature of: Auth0 / Available in: Private Cloud

Supports scaling Private Cloud deployments for the largest applications in the world.

Enhanced Rate Limit Reporting

Feature of: Auth0

New rate limit warning log communicates when customers have consumed 80% of their request limit. The frequency of rate limit logs has increased from 1x per hour to 1x per minute.



Certifications

Financial-Grade API (FAPI) v2 Compliance

Achieved for: Secure Identity / Available in: Highly Regulated Identity

Provide support for Financial Grade Identity beyond standard OAuth2 and OpenID Connect protocols. Support compliance with the FAPI v2 Security Profile for securing your APIs for Financial Services' transactions, and other sensitive, high-risk scenarios.

Learn more

IRAP Protected - Australian

Achieved for: Auth0

IRAP (Information Security Registered Assessors Program) provides a framework for assessing the implementation and effectiveness of an organization's security controls against the Australian government's security requirements, as outlined in the Information Manual (ISM) and Protective Security Policy Framework (PSPF).

FAPI v2 Compliance

Developer Resources

Auth0

From improving customer experience through seamless sign-on to making MFA as easy as a click of a button — your login box must find the right balance between user convenience, privacy and security.

Identity is so much more than just the login box. Optimize for user experience and privacy. Use social login integrations, lower user friction, incorporate rich user profiling, and drive repeat customers.

Resources

Auth0.com
Auth0 Developer Center: Click here
Auth0 blog: Click here
Auth0 Community: Click here
Languages and SDKs: Click here
Quickstarts: Click here
Auth0 APIs: Click here
Auth0 Developers blog: Click here
Auth0 Marketplace: Click here
Auth0 Developer Release Guide: Click here