



# Product Release Overview

for Early Access & General Availability in Q1 (January – March 2024)

## Developer Releases, Auth0 by Okta

*These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at [okta.com/agreements](https://okta.com/agreements).*

# 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, long-term financial plans, product development, 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, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may be unable to retain key personnel;

global economic conditions could worsen; a prior or future network, data or cybersecurity incident that has allowed or does allow unauthorized access to our network or data or our customers’ data could damage our reputation, cause us to incur significant costs or impact the timing or our ability to land new customers or retain existing customers; we could experience interruptions or performance problems associated with our technology, including a service outage; 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 or functionality referenced in this presentation that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.



# Welcome to the Developer Release Overview

Q1 2024



© Okta and/or its affiliates. All rights reserved.

DATA CLASSIFICATION: OKTA INTERNAL





okta

# Auth0 Developer Product Releases

Auth0 is focused on delivering secure, seamless, and developer-friendly Identity solutions. Our latest releases aim to strengthen security, improve user experience, and streamline developer workflows, helping you build secure digital experiences.

---

## Developer Features and Products.

-  Now Generally Available
-  Now Early Access
-  Updated
-  Added





# Now Generally Available

## Passkeys

*Feature of: Core Platform / Available in: All plans*

Passkeys are now Generally Available! Passkeys are a new and innovative way, based on FIDO authentication, to sign in to apps and websites, offering several compelling advantages over traditional passwords and other authentication methods. Use Auth0 to set up passkeys to add that extra layer of security to your application.

Check out how you can implement and leverage passkeys to improve the security within your app:

- [Passkeys](#)
- [Reduce friction with passkeys](#)
- [Passkey Playground](#)

## Fine Grained Authorization (FGA)

*Feature of: Fine Grained Authorization / Available in: Fine Grained Authorization*

Fine Grained Authorization is now live and Generally Available! FGA enables user collaboration and granular access control in your applications using developer friendly APIs.

Play around on our FGA Playground [here](#)!

Learn how easy FGA is for app builders and how to add FGA to your apps:

- [Fine Grained Authorization documentation](#)
- [fga.dev](#)





# Now Generally Available

## Auth0 Teams

*Feature of: Core platform / Available in: All plans*

Auth0 Teams consolidates managing tenants, tenant members, and a view into your customer's subscription in one central place.

Learn how Teams can improve visibility, compliance, and security on your Auth0 dashboard:

- [Auth0 Teams](#)
- [Tenant Member Management](#)





# Now Early Access

## Directory Sync with Inbound SCIM

*Feature of: SaaS Identity/Available in: B2B Essential, B2B Professional, Enterprise, Enterprise Premium SKUs*

We're excited to announce that Inbound SCIM (System for Cross-domain Identity Management) is now in Early Access. Customers can now leverage SCIM and integrate this to manage CRUD (create, replace, update, delete) operations, apply queries and filters and create user groups within your organizations. In addition, SCIM allows you to automate user lifecycles and maintain user accounts across platforms.

**See how SCIM can securely manage and communicate user data across multiple domains:**

- [System for Cross-domain Identity Management \(SCIM\)](#)
- [Datatracker System for Cross-domain Identity Management\\*](#)

## JWT Access Tokens Profiles

*Feature of: Core Platform Available in: All Plans*

This feature will help remove friction for customers to migrate to Auth0 from external systems, such as Ping, ForgeRock, etc.

**Learn how to securely implement authentication with JWTs using Auth0 on any stack & any device in less than 10 minutes:**

- [Access Tokens](#)
- [jwt.io](#)





# Now Early Access

## Highly Regulated Identity

*Feature of: Highly Regulated Identity / Available in: Advanced Identity Security*

Highly Regulated Identity is now in Limited Early Access. This is for Auth0 customers operating in highly regulated industries. Now, this enables you (if you're a customer) to elevate the security of your Identity solutions, protect your user data and privacy, and comply with regulations for strong customer authentication.

If you think your company is a good fit for this, please fill out [this questionnaire](#).

Understand how Highly Regulated Identity works and elevates your security and data privacy:

- [Highly Regulated Identity](#)
- [Advanced security with OpenID Connect \(FAPI\)](#)
- [Authorization Code Flow with Rich Authorization Requests \(RAR\)](#)







# Updated

## CISCO DUO Authenticator v4 Upgrade

Feature of: MFA / Available in: Professional and Enterprise plans

Auth0 now supports Duo Web SDK V4 for MFA.

If you are currently using Duo Web SDK V2, additional information about this change was or will be sent to your tenant administrators, including detailed instructions and links to related documentation.

## Learn more about Cisco Duo Authenticator Upgrade:

- [Configure Cisco Duo Security for MFA](#)
- [Create custom enrollment tickets](#)
- [Cisco Duo Getting Started\\*](#)

## Customizations for Universal Login Signup and Login

Feature of: Core Platform / Available in: Professional and Enterprise plans

Businesses using Auth0's Universal Login can leverage a new pro-code option to customize signup and login flows to address their unique needs. This new capability is available to customers on Professional plans or higher and allows them to address unique data capture, security, and compliance requirements.

## You don't have to do any integration work to handle different methods of authentication- learn how with Universal Login:

- [Auth0 Universal Login](#)
- [Customize Signup and Login Prompts](#)





# Updated

## MFA for Dashboard Administrators

*Feature of: Core Platform / Available in: All Plans*

As we continue to keep your dashboard user accounts secure, we now require all users to enroll in MFA.

Note: This change applies to your Auth0 account login and does not impact applications or websites you have configured with Auth0.

**\*Check out some guidance on implementing industry standards to help keep your dashboard user accounts secure:**

- [Configure Security Policies](#)
- [Community Post](#)

## Audit Logs for Teams

*Feature of: Core platform / Available in: All plans*

You can now access, view and audit logs based on your Teams member invite, settings, login and logout events. With audit logs for Teams, you have a better pulse on your Teams in general while ensuring security is in the forefront of all of your tenants.

**Understand how you can have better insight into your Teams:**

- [Team Member Management](#)

\*These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at [okta.com/agreements](https://okta.com/agreements)





# Updated

## Support for Organization Name in Authorization Flows

*Feature of: Organizations / Available in: All B2B and Enterprise plans*

Use the organization name instead of the organization ID in login flows for a simpler developer experience.

Learn how you can configure your tenant to use names as an identifier:

- [Use Organization Names in Authentication API](#)
- [Ability to provide organization name during Authorization Code Flow](#)





# Added

## Guardian App Mobile- Only Enrollment

*Feature of: Highly Regulated Identity / Available in: Advanced Identity Security*

Guardian Application now supports localization in all the languages supported by Universal Login. Our plan is to keep the Guardian App up to date with all supported languages in Universal Login.

See how we're keeping Auth0 Guardian up to date to support all languages:

- [Auth0 Guardian](#)
- [Install Guardian SDK](#)





## Added

### Organizations: Improved Login Flows

*Feature of: Organizations/ Available in: All B2B and Enterprise plans*

We've improved login success rates and time-to-login for users logging in with Organizations. End-users no longer need to provide an Organization name prior to logging in, simply they only need to provide their email address. Users who belong to multiple organizations can select one before accessing your SaaS application, making the login flow much easier.

Check out how end-users only need their email addresses to login with Organizations:

- [Enable Organization Connections](#)
- [Login Flows for Organizations](#)
- [Configure Identifier First Authentication](#)

### "Show as Button" for Organizations associated Enterprise Connections

*Feature of: Organizations/ Available in: All B2B and Enterprise plans*

Now you can choose whether you show an Enterprise Connection during Organizations based logins. Similar to how Enterprise Connections work at the Application level, you can now navigate to Organizations -> "Your Organization" -> Connections -> "Your Connection" and then select whether you want to display that connection as a button on the login screen.

Paired with Home Realm Discovery, this gives you powerful options to utilize hidden enterprise connections to support multiple customers using a single organization login, or hiding a support staff login from a customer's organization.

Take a look at our new "Show as Button" to help you navigate your dash better:

- [Enable Organization Connections](#)





# Added

## Auth Challenge for Bot Detection & Bot Detection on Password Recovery Flow

*Feature of: Bot Detection / Available in: Attack Protection*

This invisible, frictionless CAPTCHA alternative uses a series of browser and device challenges to make it tougher on bots but frictionless for users.

Auth Challenge raises costs to attackers while keeping the user interaction as simple as clicking a checkbox.

Learn how Auth Challenge & Bot Detection works in your favor:

- [Bot Detection](#)
- [Configure Bot Detection](#)

## Refresh Tokens Management API

*Feature of: Core Platform Available in: All Enterprise Plans*

As part of our commitment to protect users, we are giving developers remote control of their users' authentication status through additional management API endpoints. These endpoints enable developers to list, explore, and terminate all or individual sessions and refresh tokens.

See how Refresh Tokens interacts with your application in order to get a new access token without interaction:

- [Manage Refresh Tokens with Auth0 Management API](#)
- [Revoke Refresh Tokens](#)





## Added

### Open Source Templates for Actions

*Feature of: Core Platform / Available in: All plans*

Allows developers to contribute to the template library.

### Explore Auth0 open source projects that you can leverage:

- [Open Source projects build at Auth0](#)

### Guardian App and SDK now support OTP enrollment without requiring a QR code

*Feature of: Highly Regulated Identity / Available in: Advanced Identity Security*

End users can now enroll in One-time Password (OTP) Multi-factor Authentication (MFA) using the Guardian App or a custom app using the Guardian SDK on the same mobile device as the application. This allows users to complete OTP MFA enrollment flows using Guardian without having to scan a QR code.

### Take a look at how you can complete OTP MFA enrollment without scanning a QR code

- [Auth0 Guardian](#)
- [Changelog Description](#)



# 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 facilitate more transactions.

## Resources

### Auth0

**Auth0 Developer Center:** [Click here](#)

**Auth0 Blog:** [Click here](#)

**Auth0 Community:** [Click here](#)

**Languages and SDKs:** [Click here](#)

**Quickstart:** [Click here](#)

**Auth0 APIs:** [Click here](#)

**Auth0 Developer Blog:** [Click here](#)

**Auth0 Marketplace:** [Click here](#)





okta