Product Release Overview

for Early Access & General Availability in Q3 (July – Sept 2023)

Workforce Identity Cloud

Customer Identity Cloud, powered by Auth0

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 targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. 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 fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key

personnel; global economic conditions could worsen; a network or data security incident that allows unauthorized access to our network or data or our customers' data could damage our reputation and cause us to incur significant costs; we could experience interruptions or performance problems associated with our technology, including a service outage; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; 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 unreleased products, features or functionality referenced in this presentation are not currently available and 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.

okta

Welcome to the Okta Workforce & Customer Identity Cloud Release Overview

Q3 2023

Okta's July – September product releases strengthen your security posture, make your developers more productive, and help you deliver seamless customer experiences.

In addition to introducing Okta AI, our latest batch of product releases help you strengthen security, flexibility, and usability all at once. From FastPass Phishing Resistance to Fine Grained Authorization, Okta powers smarter security that factors in behaviors, devices and shared signals to deliver convenient, intuitive experiences that users expect.

okta

Navigating the Release Overview

The Release Overview has two main sections with the following contents:

Workforce Identity Cloud

- Workforce Identity Cloud overview
- Introducing Okta AI
- Release spotlights
- Release overviews
- Developer resources

Customer Identity Cloud

- Customer Identity Cloud overview
- Introducing Okta AI
- Release spotlights
- Release overviews
- Developer resources

okta

Workforce Identity Cloud

Workforce Identity Cloud connects and protects everyone everywhere, so they can perform at their best — your employees, contractors and business partners on any device, with any app, API, or resource in your organization.

This quarter's new releases help you strengthen security without compromising usability and flexibility.

okta

Okta Workforce Identity Cloud

Employees | Contractors | Business Partners

OKTA INTEGRATION NETWORK | Connect everything

Access Management

Single Sign-On
Adaptive Multi-Factor Authentication
Identity Threat Protection
Device Access
Access Gateway
API Access Management

Identity Governance

Universal Directory
Lifecycle Management
Identity Governance

Privileged Access

Advanced Server Access

PLATFORM | 99.99% Uptime.

| **Workflows** | **Deployment Options** | **Scale Solutions** | **Regulated Offerings** HIPAA, FedRAMP High ATO |

okta

Introducing Okta AI

Okta AI transforms the Identity experience, removing administrative burdens, delivering great user experiences, all while protecting against sophisticated AI–enabled security attacks. With unparalleled access to data across our ecosystem, Okta AI can drive real–time actions and a stronger security posture for your business through Workforce Identity Cloud.

To learn more about how Okta views the role of AI within the future of Identity, read our blog.

Workforce Identity Cloud			
Log Investigator with Okta AI	**Governance Analyzer with Okta AI**	**Policy Recommender with Okta AI**	**Identity Threat Protection with Okta AI**
Get all the answers you need through natural language prompts that enable effective threat investigation in Okta logs, user activity tracking, and anomaly discovery.	Reduce the cognitive burden on decision makers and unlock high-quality Identity decisions and configurations.	Apply strong security policies based on best security practices as well as aggregated insights from across the Okta community.	Continuously assess user risk and automatically remediate Identity threats throughout long-lived sessions.
		Limited EA Q1 2024	*EA Q4 2023*
Limited EA/EA – 2024	*Limited EA/EA – 2024*		

okta

Release Spotlight: Entitlement Management

Cloud-native entitlement management for your apps and resources

What is it

Entitlement Management is a major update to Okta Identity Governance, giving customers the ability to bring in, store, and automate fine-grained access to entitlements in downstream applications.

Customer Challenge:

The number of applications a typical organization has adopted is exploding — which means more apps, and also more entitlements within those apps for IT to manage. This is creating a tangled web of permissions across multiple locations that IT teams need to manage.

Benefits:

Entitlement Management enables organizations to store and manage entitlements from all types of resources in one location, allowing customers to reduce their risk of over-permissioning, minimize their attack surface, and cut down costs of unused licenses.

Why this matters

- Gain increased granular views and management of entitlements in a single plane by using a unified IAM and governance solution. Truly understand a user's access by viewing assigned entitlements in context of one another.

- Experience the freedom to choose the resources that are right for your stack and bring in their respective entitlements into Okta.

- See a faster time to value with a quick and easy deployment of cloud-native entitlement management for your apps and resources that increases productivity and efficiency.

How to get it

This feature will be added to Okta Identity Governance and available to all OIG customers by the end of 2023.

okta
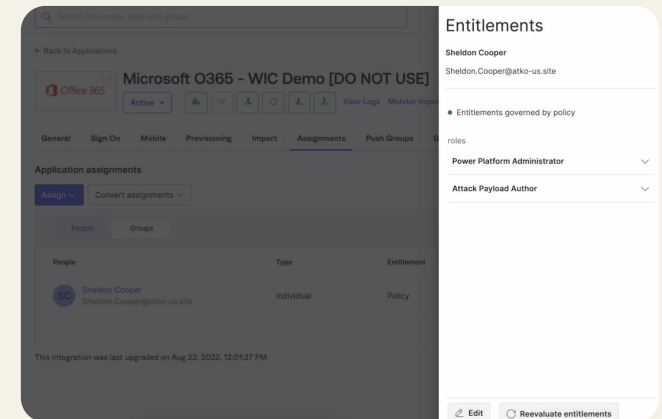
Release Spotlight: Anything-as-a-Source

Import identities from any source of truth

What is it

Anything-as-a-Source is a set of APIs within Lifecycle Management that will allow you to import identities from any Identity source of truth and as a result, use Okta as a single control plane for Identity and Access Management.

Customer Challenge:

Customers are required to either use an out-of-the-box connector or another resource-intensive method to bring identities in to Okta.

Benefits:

With Anything-as-a-Source, customers have the freedom to use the Identity source that is right for them, send Identity updates directly to Okta to drive lifecycle flows, and automate actions in downstream applications.

Why this matters

- Experience increased choice and customization by connecting any Identity source to Okta and have the ability to customize how that integration happens.

- See a faster time to value by Implementing XaaS with fewer resources and less complexity than other import methods.

- Directly leverage existing Okta Lifecycle Management automations.

How to get it

This feature is generally available to all Lifecycle Management customers.
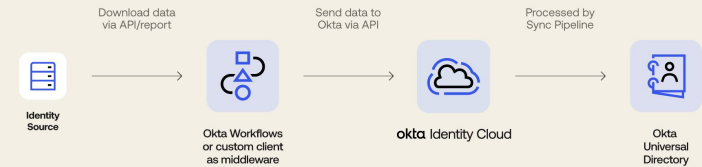
okta

Release Spotlight: FastPass Phishing Resistance

Enhanced security and phishing resistance with Okta FastPass

What is it

Okta FastPass expanded its phishing-resistant protection to encompass unmanaged iOS devices (Early Access). This means that FastPass can now deliver phishing-resistant authentication across all major operating systems, for managed and unmanaged devices, including Android, macOS, Windows, and now iOS.

Additionally, organizations leveraging FastPass will have a phishing-resistant means of enrolling additional devices from a trusted, existing Okta Verify enrollment. With this feature, now in General Availability, Okta takes one step closer to providing end-to-end phishing resistance.

Customer Challenge:

To minimize the risk of increasingly sophisticated phishing attacks across a heterogeneous mix of workforce devices.

Benefits:

Phishing-resistant authentication and enrollment of Okta Verify for managed and unmanaged (BYOD) devices used by employees and extended workforce members.

Why this matters

- Real-time credential phishing prevention via a passwordless, phishing-resistant authenticator at the AAL2 level (as defined by NIST)

- Security for the device in use with risk-aware authentication policies to establish minimum requirements for devices before access is allowed

- Consistent user experience across platforms and devices, enabling organizations to provide employees with the tools they want by supporting and securing a heterogeneous mix of devices

How to get it

- Okta Identity Engine only

- Available with SSO, aSSO, MFA, or aMFA

- Device context for risk-aware authentication policies is available only with aSSO and aMFA
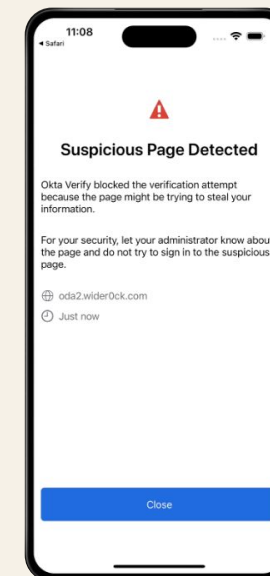
okta

Release Spotlight: Device Access

Extends Okta's leading IAM capabilities — from applications to devices — delivering stronger security and business agility

What is it

Okta Device Access brings the best of Okta's simple, secure authentication experience to the point of desktop login. The product currently consists of two key features:

- Desktop MFA: Integrated step-up authentication for devices. Available for Windows in GA in October and available for macOS in EA in October

- Desktop Password Sync for macOS: Password synchronization with Okta and automatic FastPass enrollment (now in EA)

Customer Challenge:

Devices that are not properly secured remain a point of enterprise vulnerability as the gateway to critical data and apps.

Benefits:

Okta Device Access enables customers to protect local device data and access to cloud apps by extending Okta credentials to the computer login experience.

Why this matters

- **Ease of use, ease of deployment:** Reduced time to value that Okta customers expect with all Okta solutions. Friendly user experience that is well integrated with Windows/macOS and flexibly supports online and offline scenarios.

- **Neutral vendor that supports all devices:** Support for mixed OS deployments and the strongest integrations with best-of-breed technologies. Freedom from vendor lock-in and lower TCO with vendor consolidation (Okta is an IdP and desktop access provider).

- **Integrated Identity from device to apps:** Enforce consistent and comprehensive security access controls at scale, under a single, unified IAM platform. Benefit from the stronger IAM capabilities of the market-leading Identity provider.

How to get it

- Available with the Device Access SKU
- At a minimum, customers need one of the following SKUs: MFA, AMFA, SSO, or ASSO,
- Device Access can be purchased for a subset of users.
- Okta Identity Engine only

okta
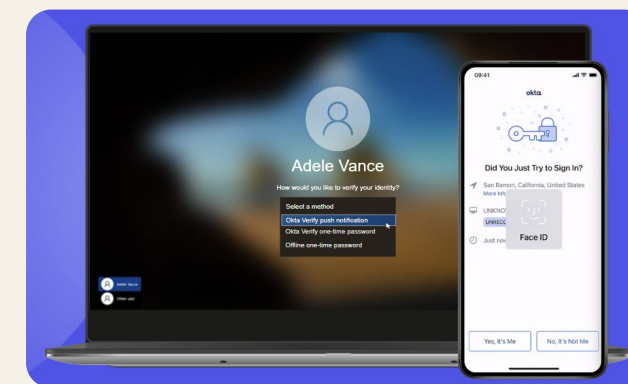
Workforce Identity Cloud Releases

AI is driving a new paradigm shift in security. In this new world, identity needs to evolve beyond MFA. It must become the backbone of a holistic security strategy to help you harness the power of your entire technology stack and keep your business safe. Learn more about how Okta protects people, devices, and apps, all while streamlining identity automation across your tech stack.

Easily identify the platform each release is available in:

| Okta Identity Engine | 16 | | Both | 28 | | Classic | 0 |

okta

Access Management

General Availability

FastPass Phishing Resistance for Unmanaged iOS

`OIE`

Feature of: MFA/ Available in: SSO, ASSO, MFA, AMFA

Extends FastPass phishing-resistant authentication to unmanaged iOS devices, making FastPass phishing resistant across all major platforms, including Android, macOS, and Windows, for managed and unmanaged devices.

Access Scenario Testing Tool (Policy Testing Tool)

`OIE`

Feature of: All Products/ Available in: All SKUs

Test access scenarios and obtain a list of policies that would apply to the user/groups trying to access a specific app, without having to manually log in as a different user or with different device context. Enable support users to run simulations to help troubleshoot access issues and roll out new features into production with confidence.

Smart Card Authenticator

`OIE`

Feature of: MFA/ Available in: MFA, AMFA

A phishing resistant authentication feature that allows admins to enable PIV/CAC cards as step-up MFA for accessing specific, high sensitive apps.

Device Assurance with Google Chrome

`OIE`

Feature of: MFA/ Available in: AMFA, ASSO

Configure Device Assurance policies for ChromeOS devices and for macOS and Windows devices through managed Chrome browsers, with or without Okta Verify, to harden your security posture by layering agentless device posture checks at the time of authentication.

FastPass Phishing Resistance for Unmanaged iOS

okta

Access Management

General Availability

Improved Device Assurance end user remediation

OIE

Feature of: MFA/ Available in: Adaptive MFA, Adaptive SSO

Enhancement to provide users with error remediation steps in the sign-in widget if access to an Okta-protected app is denied from failing a condition in a Device Assurance policy. This may help reduce help desk tickets.

WebAuthn Security Improvements

OIE

Feature of: MFA/ Available in: MFA, Adaptive MFA

Test access scenarios and obtain a list of policies that would apply to the user/groups trying to access a specific app, without having to manually log in as a different user or with different device context. Enable support users to run simulations to help troubleshoot access issues and roll out new features into production with confidence.

Connecting to ⊞

Sign in with your YYZlabs account to access Okta Dashboard

okta

****

Unable to sign in

Your device doesn't meet the security requirements

To sign in, make the following updates. Then, access the app again.

- Update to Android 12
- Enable lock screen

Back to sign in

Forgot password?

Verify with something else

Back to sign in

Improved Device Assurance end user remediation

okta

Access Management

Early Access

Smart Card & Okta FastPass

OIE

Feature of: MFA/ Available in: MFA, Adaptive MFA

Allows customers to use Okta FastPass when their PIV/CAC cards are lost or need renewal. Customers will no longer need a non-phishing-resistant option such as a password in these scenarios. This release is a step toward making end-to-end phishing resistance a reality for our Federal customers.

Okta Device Access – Desktop Password Sync macOS

OIE

Feature of: Device Access/ Available in: Device Access

Enables users to login to macOS using their Okta passwords and automatically enrolls FastPass for passwordless access to any Okta-protected app.
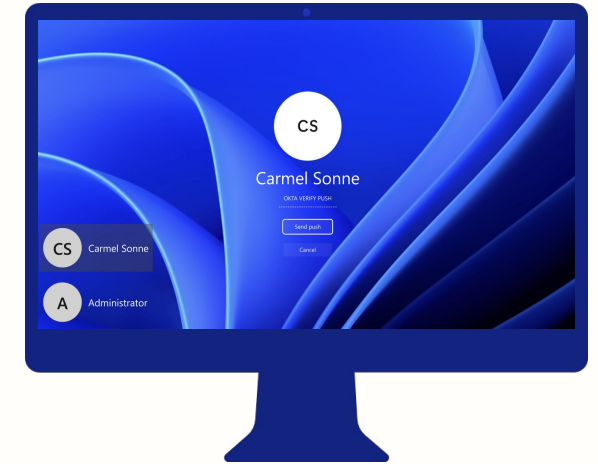
Okta Device Access – Desktop MFA for Windows

OIE

Feature of: Device Access/ Available in: Device Access

Enforce MFA on top of a credential login to unlock a Windows device or server to prevent attackers from logging in with stolen passwords and/or into stolen computers.

Okta Device Access – Desktop MFA for Windows

okta

Identity Governance

General Availability

User Campaigns

`Classic` `OIE`

Feature of: Access Certifications, Okta Identity Governance/ Available in: Okta Identity Governance

Help automate least privilege security. This feature improves security posture and enhances compliance by triggering certifications based on common events that lead to over-provisioning or inadvertent access.

Access Request Workflow integration

`Classic` `OIE`

Feature of: Access Request/ Available in: Okta Identity Governance

Leverage Okta Workflows automations from within Okta Access Requests, allowing for extensibility and customization.

Anything-as-a-Source

`Classic` `OIE`

Feature of: Lifecycle Management/ Available in: Lifecycle Management

Leverage this set of APIs to import identities from any source of truth into Okta and power HR-driven automation. Users will see increased choice and customization, be able to implement faster, and leverage the power of Okta's sync pipeline.

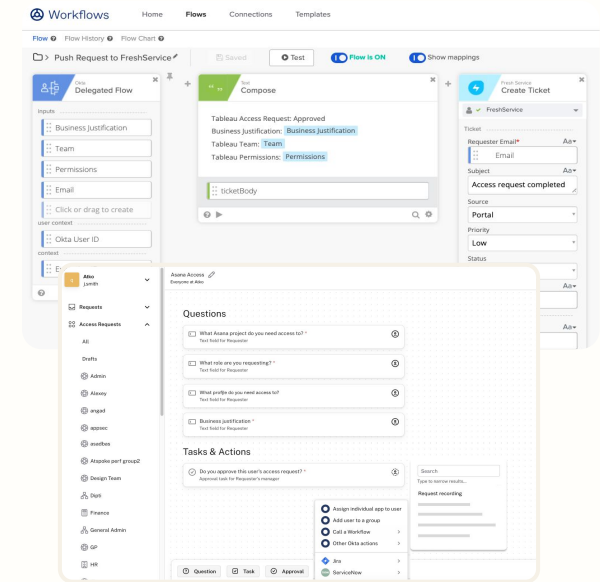### Access Certifications Updated Public APIs

`Classic` `OIE`

Feature of: Access Certification, Okta Identity Governance / Available in: Okta Identity Governance

Create and manage access certifications with features like recurring campaigns, group and group owner reviewers, multi-level reviewers, and user campaigns that were released since the initial API release. All changes are additive, without introducing breaking changes.

Access Request Workflow integration

okta

Identity Governance

Early Access

Entitlement Access Certifications

Classic | **OIE**

Feature of: Okta Identity Governance/ Available in: Okta Identity Governance

Review the entitlements and bundles assigned to users directly to certify the access level they have in the application.

Entitlement Management for OIN Apps

Classic | **OIE**

Feature of: Okta Identity Governance/ Available in: Okta Identity Governance

Discover, store, and manage entitlements within Okta via bundles, policies, and rules with out-of-the-box integrations for 5 Okta Integration Network apps: Office 365, Salesforce, Google, NetSuite, Box.
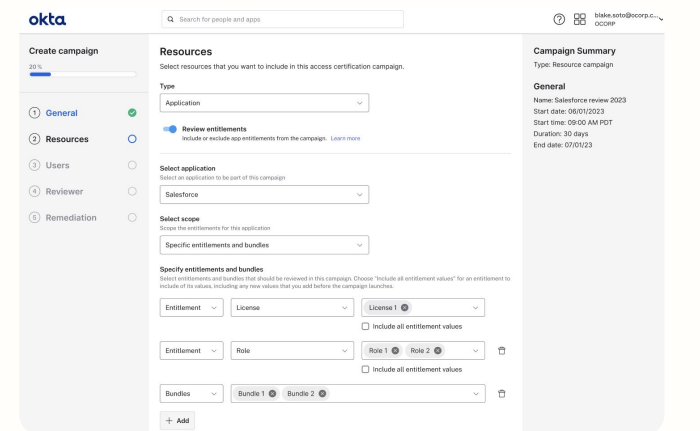
Reports for Entitlements

Classic | **OIE**

Feature of: Reports/ Available in: Okta Identity Governance

View access levels or permissions users have for a given application, see all of the access users have and how they received them, and uncover and correct any elevated or altered access made in the application outside the awareness of the IT Team.

Entitlement Access Certifications

okta

Platform Services

General Availability

```
Unset
curl --location
'https://tenant.oktapreview.com/oauth2/aus8w23r13NvyUwln1d7/v1/tok
--data-urlencode 'scope=okta-aws-cli' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_id=«okta_application_client_id»' \
--data-urlencode 'client_secret=«okta_application_client_secret»'
```

```
Unset
$ aws sts assume-role-with-web-identity \
    --role-session-name "read_files_from_s3_bucket" \
    --role-arn "arn:aws:iam::294719231913:role/Role_S3_Read" \
    --web-identity-token "«okta_bearer_token»"
```

Headless Access to Okta AWS CLI

Headless Access to Okta AWS CLI

OIE

Feature of: Developer Tools / Available in: All SKUs

Enable users to attach the AWS CLI to other headless processes like Continuous Integration and Continuous Delivery. It can work with the existing secrets management process and can be secured to only certain apps and certain operators with access to the app and secrets. It allows interactive and programmatic sessions to coexist with proper authorization.

Improved App Metadata Rollout for Net-new Integrations to Preview & Production

Classic **OIE**

Feature of: Okta Identity Network/ Available in: All SKUs

Migrations of app metadata for deployed net-new apps are even more resilient and uneventful for all Okta customers with newly advanced automation tools. This means faster access to new apps and app improvements in the Okta Identity Network.

okta

Platform Services

Early Access

Conditions for custom admin roles

Classic | OIE

Feature of: SSO, UD, MFA, Lifecycle Management/ Available in: All SKUs

Enables super admins to have fine grained control over delegated admin permissions such as hiding sensitive attributes and granting minimum possible privileges.

Product Offers (Lifecycle Management)

Classic | OIE

Feature of: Lifecycle Management/ Available in: Lifecycle Management

Trial Okta Lifecycle Management in your production or preview org for 30 days. Eligible customers can access the product offer via a notification on their admin dashboard.

New permissions in custom roles

Classic | OIE

Feature of: SSO, UD, MFA, Lifecycle Management/ Available in: All SKUs

Provides granular permissions for: read only view for admin assignments, directories, and applications to enforce least privilege security postures.

Revamped permissions UI

Classic | OIE

Feature of: SSO, UD, MFA, Lifecycle Management/ Available in: All SKUs

Improve the user experience for admin role creation for a scalable UI to accommodate new granular permissions and better layout to help super admins understand what permissions may be needed for a specific job to be done.

Permission name

▼ Users

　　▶ ☐ Manage users

　　▼ Manage admin role assignments

　　　　☐ Read only view for admin assignments

▼ Directories

　　▶ ☐ Manage directories

New permissions in custom roles

okta

Platform Services

Early Access

Platform localization

Classic | OIE

Feature of: All Products/ Available in: All SKUs

Provides localized core admin experiences including administration, the OIN catalog, and help documentation, starting with Japanese, so administrators can choose to manage their Okta tenant using their language of choice.

Platform localization

okta

Platform Services – Workflows

General Availability

New Workflows Connectors

Classic · **OIE**

Feature of: Workflows/ Available in: Workflows

Take more actions on files and their HR data; includes: SFTP, monday.com, SmartHR, Personio.

Workflows No-Code Automation for Customer Identity

Classic · **OIE**

Feature of: Workflows/ Available in: Workflows

Personalize customer identity flows with no-code automation, using Okta Workflows.

Okta Connector Enhancements

Classic · **OIE**

Feature of: Workflows/ Available in: Workflows

Unlock an easier path to use and adopt Okta Workflows Connectors. This launch productizes the Okta APIs into the Okta connector for tools such as: Devices API, OIG connector, and Okta Realms connector.
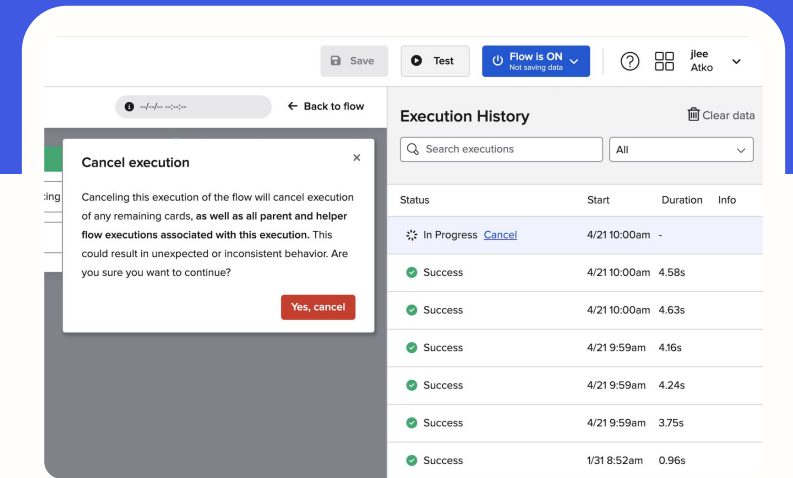
Cancel Flow Execution

Classic · **OIE**

Feature of: Workflows/ Available in: Workflows

Cancel in-progress workflow executions, reducing unnecessary wait time in the test/debug user experience, and create an escape hatch from hanging executions or infinite loops.

Cancel Flow Execution

okta

Platform Services – Workflows

General Availability

Workflows Free Trial

`Classic` `OIE`

Feature of: Workflows/ Available in: Workflows

Allow Workforce Identity Cloud Free Trial users to trial Workflows for 30 days without any existing Okta subscriptions.

Workflows Outbound Client Credential Support

`Classic` `OIE`

Feature of: Workflows/ Available in: Workflows

Connect to third-party services using secure machine-to-machine connections outside of user context. Allow users to securely connect to more services including popular security products like Crowdstrike, Microsoft Defender, and even Auth0 by Okta and improve their security posture.

Workflows Connector Builder Webhooks

`Classic` `OIE`

Feature of: Workflows/ Available in: Workflows

Allow ISVs, partners, and customers to create their own webhook event cards to trigger flows based on actions taken in a third-party system which opens up new use cases, especially in the security realm like ITDR and security orchestration. Expand the value of Connector Builder, attracting new ISVs to integrate with the Workflows platform.
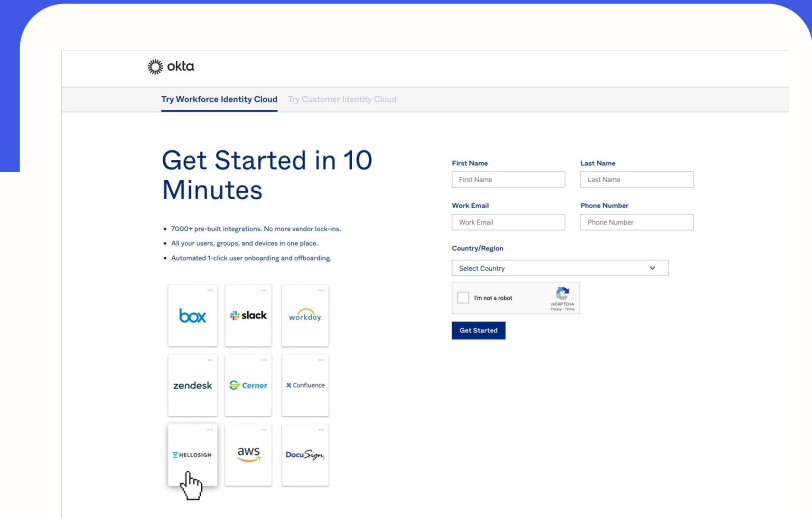
Request Panel Redesign

`Classic` `OIE`

Feature of: Access Requests/ Available in: Okta Identity Governance

Improve the visibility of tasks and make it easy to find out what actions are needed from approvers.

Workflows Free Trial

Developer Resources

Workforce Identity Cloud

Developer blog: https://developer.okta.com/blog/

Languages and SDKs: https://developer.okta.com/code/

Getting Started guides: https://developer.okta.com/docs/guides/

Release Notes: https://developer.okta.com/docs/release-notes/

Okta Developer Community Forum: https://devforum.okta.com/

Okta Community Toolkit and app showcase: https://toolkit.okta.com/apps/

okta

Customer Identity Cloud

Customer Identity Cloud, powered by Auth0, enables the trusted, intuitive digital experiences that your users expect and deserve, all while protecting customer and business data.

This quarter's new releases enable developers to move quickly so that businesses can provide innovative and seamless digital experiences — without compromising on security and privacy.

okta

Okta Customer Identity Cloud

Consumer Apps | SaaS Apps | Developers

Authentication

Single Sign-On
Adaptive Multi-Factor Authentication
Universal Login
Passwordless

Authorization

Fine Grained Authorization

Security

Bot Detection & Prevention
Security Center
Breached Password Detection
Brute Force Protection

PLATFORM | 99.99% Uptime. Billions of Monthly Logins.

| Actions | Deployment Options | SDKs, APIs, Quickstarts | Marketplace |

okta

Introducing Okta AI

Okta AI transforms the Identity experience, removing administrative burdens, delivering great user experiences, all while protecting against sophisticated AI-enabled security attacks. With unparalleled access to data across our ecosystem, Okta AI can drive real-time actions and customer experience improvements for your business through Customer Identity Cloud.

To learn more about how Okta views the role of AI within the future of Identity, read our blog.

Customer Identity Cloud				
Guide with Okta AI	**Actions Navigator with Okta AI**	**Brand Customizer with Okta AI**	**Tenant Security Manager with Okta AI**	**Identity Flow Optimizer with Okta AI**
Comprehensive onboarding assistance that intuitively maps out the best possible steps and seamlessly steers you toward the most valuable workflows	Find the right marketplace integrations based on what you are looking for, even if your search keywords are different from what is included in the integration's title or description.	Design one page template and use AI to adapt the design to all the other required templates. Or, provide a screenshot or logo and have AI build all the templates for you to then customize.	Intelligent security recommendations in Attack Protection just got better with proactive security snapshot alerts and dashboard notifications.	Analyze your tenant's authentication data and receive suggestions on improving the customer experience, sign-up flow, and more.
Available in 2024	*Available in 2024*	*Beta in 2024*	*Available in 2024*	*Available in 2024*

okta

Release Spotlight: Highly Regulated Identity

Elevate security, privacy, and user experience controls for your most sensitive customer scenarios.

What is it

Highly Regulated Identity is a new feature set on the Customer Identity Cloud that elevates security, privacy, and user experience controls for your most sensitive customer transactions and scenarios.

Customer Challenge:

Developing secure and seamless digital app experiences is challenging, especially in highly regulated industries such as financial services and healthcare. You're battling elevated threats, fraud, and regulatory demands while trying to keep pace with increasing consumer expectations around frictionless digital experiences.

Benefits:

- **Increase security and prevent fraud** with Financial Grade Identity™ controls
- **Deliver intuitive user experiences** — integrate with your risk engine to reduce unnecessary approvals and, when required, send enriched approval requests
- **Stay compliant confidently** — manage compliance with UK Open Banking, PSD2, FDX and FAPI 1 Adv

Why this matters

Get all the benefits of Highly Regulated Identity on the world's leading born-in-the-cloud Identity platform.
Get to market faster, lower total cost of ownership, and scale with confidence.

Enable Sensitive Transactions

Make transaction approvals and other sensitive customer operations easy and secure with Strong Customer Authentication (SCA), FAPI 1 Adv protocols, and Customer Managed Keys.

Example: Money transfers, open banking payments, sharing sensitive information in a portal

How to get it

Available in Early Access to select customers November 2023 and Generally Available ~May 2024 — contact your Okta rep if interested in joining EA!

Note: Highly Regulated Identity will be available in dev/test environments to EA participants for a free trial period. When ready to enter production or when the EA Program ends, EA participants must purchase Highly Regulated Identity under the SKU "Advanced Identity Security".

Resources

- [Highly Regulated Identity Product Page](#)
- Docs will be available for Early Access Nov 2023 on [Auth0 by Okta Docs](#)

Review your payment

All Inclusive Resort Package for Two

Amount
$2,460.46

Recipient
Acme Travel, Inc.

Transaction type
One-time payment

Date
November 9, 2022 at 9:41 AM

Use the following account:

Checking ***4567 $3,674.95

Decline   Approve

okta

Release Spotlight: Passkeys

Deliver faster, easier, and more secure login experiences — without a password.

What is it

Based in FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-up and sign-in experiences to consumers across their devices. Unlike passwords, passkeys are phishing resistant.

Customer Challenge:

Though passwords are the most common form of authentication, they've regularly been proven to be insecure and inconvenient, resulting in breaches and lower conversion rates.

Traditional forms of MFA can be used to improve security, but in addition to the friction they create, they are expensive to run and are actively being targeted by
bad actors.

Benefits:

- Passwordless account creation to maximize conversions
- Significantly more phishing-resistant due to FIDO standards
- As easy as unlocking your phone to give consumers convenience

Why this matters

Improve convenience and security for your applications using the latest phishing-resistant, passwordless technology from the FIDO Alliance.

With the flip of a switch, you can reduce login friction and allow customers to sign up for and sign in to applications the same way they unlock their mobile devices, across all their devices.

Many other systems only support narrow aspects of customer identity. Partnering with Okta gives businesses a complete solution, covering multiple forms of authentication, authorization, user management, and security. Paired with the extensibility of our platform and ease of implementation, Okta gives developers and digital teams the tools they need to know, protect, and delight their users.

How to get it

Available in Early Access to all customers on the Customer Identity Cloud, on all plans, for no additional cost.

Resources

- [Passkeys for Database Connections](#)
- [Our Take on Passkeys](#)
- [Passkeys Primer Whitepaper](#)
- [Launch Blog](#)

okta
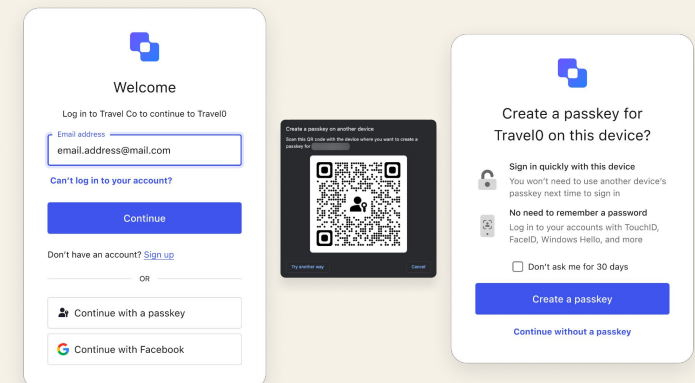
Release Spotlight: Fine Grained Authorization (FGA)

FGA empowers developers with centralized and flexible fine-grained authorization, that provides greater scalability, availability, and auditability than traditional access control methods.

What is it

Fine Grained Authorization streamlines authorization at scale, providing developers with the power to programmatically define fine-grained access control across applications. Seamlessly integrate with existing systems while maintaining absolute control over the level of access granted to users, eliminating complexity and enabling robust security.

Customer Challenge:

Current methods of authorization are implemented at the application level, are static, and have limited precision.

As user roles change and the number of resources increases, access permissions are not updated in real-time, leading to unauthorized or blocked access. This results in wasted development resources, inability to scale, and security and compliance risks.

Benefits:

By taking authorization out of the application, teams can deliver innovation faster and maintain complete control and visibility. Centralized authorization enables businesses to reduce their attack surface and bolster security.

Why this matters

Authorization is a critical component to both security and user experience. Businesses need authorization that is trusted, reliable, and secure. The Okta you know and love can now help you solve your authorization needs in a way that is centralized, scalable, fast, and easy to use.

- Define authorization models
  - Model user groups, roles, and permissions

- Write authorization data
  - Programmatically write authorization-related data to FGA, including user access, group membership, and relationships between objects.

- Add authorization to your API
  - Update your API to check a user's permissions before certain actions.

How to get it

New Product available in Limited EA today; GA in the first half of next year

Resources

- FGA Landing Page
- Supercharge Your Authorization with FGA

okta
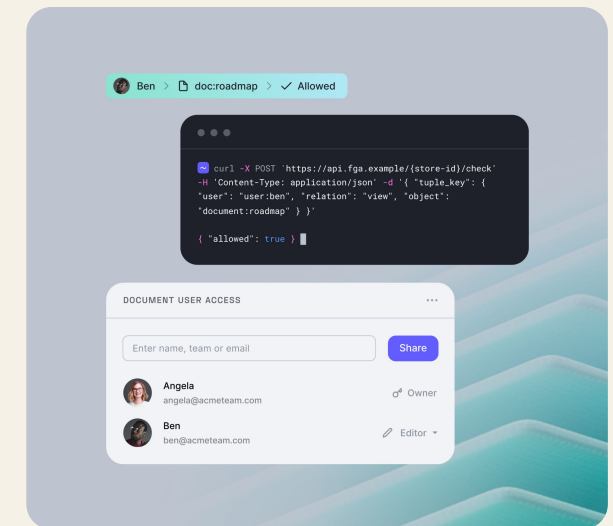
Customer Identity Cloud Releases

As organizations embrace digital transformation to thrive in this new economic environment, differentiation hinges on delivering secure and exceptional digital user experiences. Customer Identity enables and guides organizations to successfully navigate these shifts, leverage new technologies, and accelerate growth, all while seamlessly protecting customer and business data.

okta

Authentication

General Availability

Okta Access Gateway + Customer Identity Cloud Integration

Feature of: Okta Access Gateway/ Available in: Customer Identity Cloud Okta Access Gateway Add-on

Enable secure access to protected applications behind the company firewall for Customer Identity Cloud end users. This is most common in large organizations, including finance, insurance, healthcare, etc. This integration will deliver a seamless login experience for end users and a simplified admin experience.

Guardian App Enhancements

Feature of: MFA/ Available in: Enterprise MFA, Adaptive MFA

Native localization support in 6 languages, with 40+ languages coming soon; added support for enabling Dark Mode.

Additional Email Provider Support

Feature of: Core Platform/ Available in: All Plans

Enable customers to use Outlook on Microsoft 365 or Azure as preferred authentication methods with additional support for Azure Communication Service & Microsoft Modern Auth.

Custom Domains in Guardian SDKs

Feature of: Authentication/ Available in: Enterprise MFA, Adaptive MFA

Builds users' confidence that they are providing their credentials to the proper party. Custom Domains allow authentication to happen within the context of your brand.

Guardian App Enhancements

okta
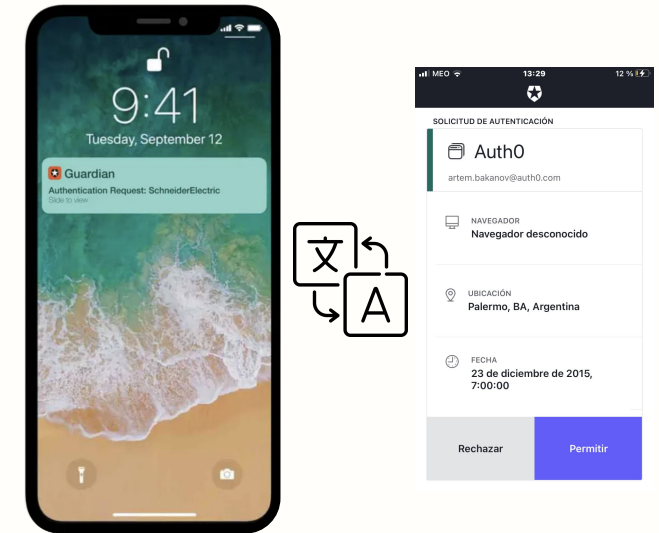
Authentication

Early Access

Customized MFA Challenges in Universal Login

Feature of: MFA/ Available in: Enterprise MFA, Adaptive MFA

Tailor the specific second factor your customers use for MFA to reduce friction and align with your organization's security policies.

Password Reset Using Any Factor in Universal Login

Feature of: MFA/ Available in: Pro MFA, Enterprise MFA, Adaptive MFA

Extend the password reset flow with an MFA challenge, a redirect, or a deny command to provide additional security and/or validation before the password is reset.

Support for FIDO passkey authentication in Universal Login

Feature of: Passkeys/ Available in: All plans

Make customer logins faster, easier, and more secure with passkey. Go passwordless with the latest form of FIDO authentication that gives businesses a phishing-resistant alternative to passwords while maximizing end-user convenience.
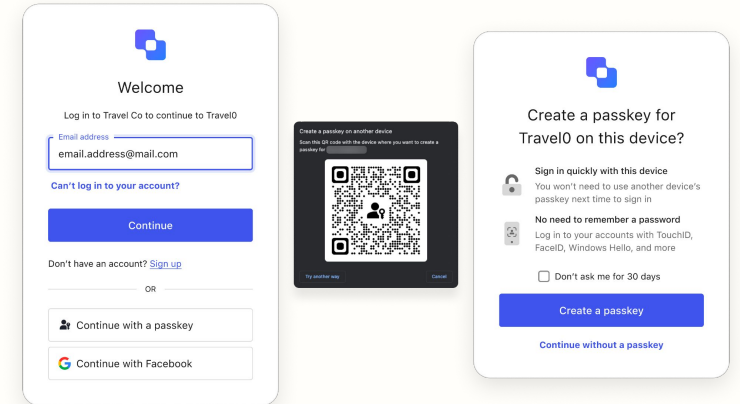
Support for FIDO passkey authentication

okta

Authentication — SaaS Apps

General Availability

OIDC and Okta Workforce Enterprise Connection Enhancements

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

Support PKCE and attribute mapping. PKCE enables you to build more secure connections between Customer Identity Cloud and your connected Identity provider. Attribute mapping allows you to ensure your tenant is leveraging the latest user information from the connected IdP.

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.

Editor – Organizations Role

Feature of: Admin Roles/ Available in: All B2B Professional and Enterprise Plans

Provide your team with least-privilege access to manage business customers with the Organizations Editor Manage Dashboard Role.

Organizations: Improved Login Flows

Feature of: Organizations/ Available in: All B2B and Enterprise Plans

Improve 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 — just their email address. Users who belong to multiple organizations can select one before accessing your SaaS application.

Welcome

Log in to continue to Productzero.

Email Address

Continue

Choose an organization

You're a member of these organizations.

A | Agency Inc.

Big Corp.

Customer Co.

Organizations: Improved Login Flows

okta

Authentication — SaaS Apps

General Availability

## Organization Name support for launching Login flows

Feature of: Organizations/ Available in: All B2B and Enterprise Plans

Simplify your code by using the organization name instead of the ID to initialize authentication flows.

Get Organization Members with Roles

Feature of: Organizations/ Available in: All B2B and Enterprise Plans

Make it easier to build multi-tenant administrative dashboards by optionally including organization members' RBAC roles in the API response. Increases scalability, and reduces total cost of ownership.

Get Organization Members with Roles

okta
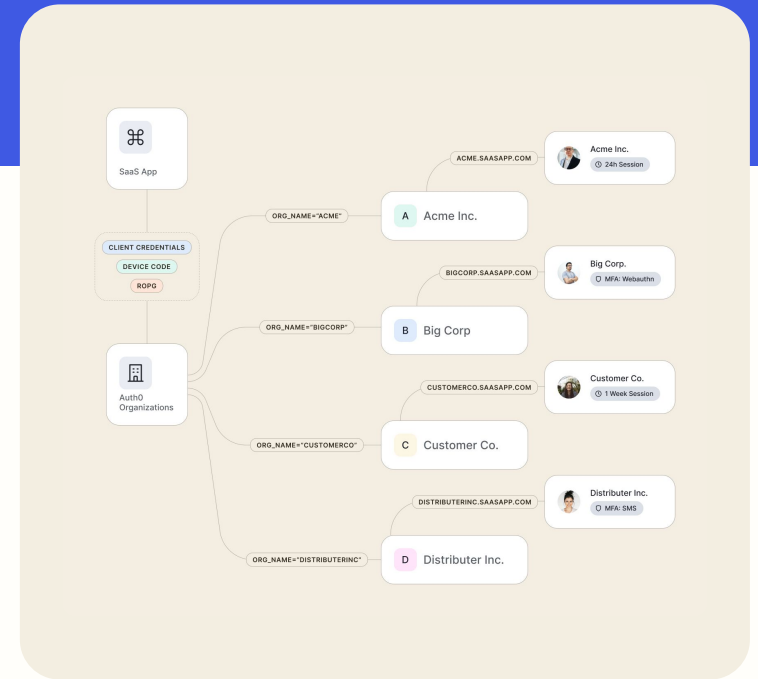
Authorization

Early Access

Fine Grained Authorization Limited Early Access

Feature of: Fine Grained Authorization/ Available in: Fine Grained Authorization Enterprise Basic

Design authorization models, from coarse-grained to fine-grained, in a way that's centralized, flexible, fast, scalable, and easy to use.

Fine Grained Authorization Limited Early Access

okta
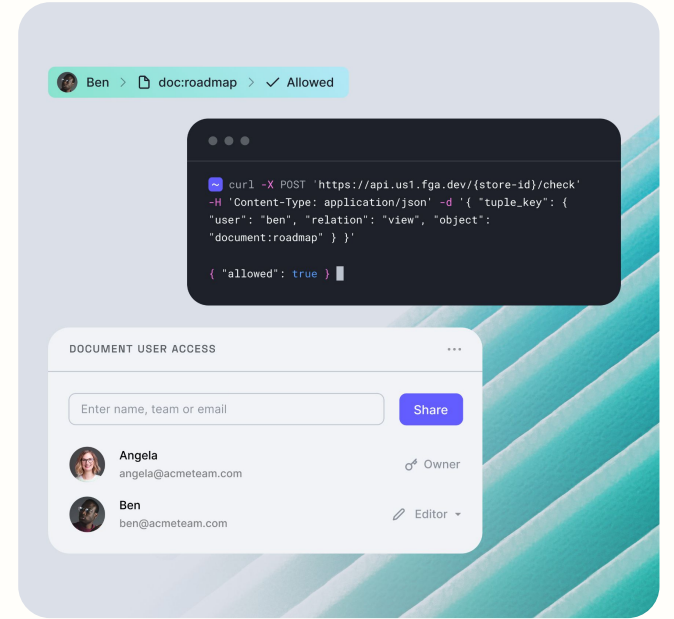
Security

General Availability

Bot Detection Slider for Bot Detection

Feature of: Bot Detection/ Available in: Attack Protection, MFA Bundle, Adaptive MFA Bundle

Customize Bot Detection threshold levels within the Bot Detection dashboard, with the introduction of three preset levels of Low, Medium, and High.

Bot Detection is Now Integrated with Friendly Captcha and hCaptcha

Feature of: Bot Detection/ Available in: Attack Protection, MFA Bundle, Adaptive MFA Bundle

Expanded options to seamlessly integrate with Captcha response providers in Bot Detection, with support for Friendly Captcha and hCaptcha.

Teams: Security Policies – SSO Enforcement

Feature of: Core Platform/ Available in: Enterprise Basic, Enterprise, Enterprise Premium

Provides the option to mandate login to Teams and Manage Dashboard through the organization's enterprise IdP.
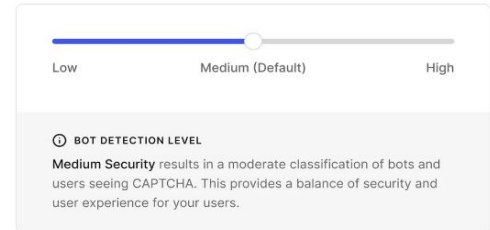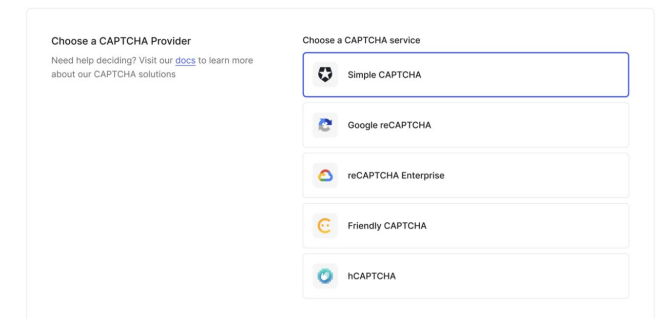

Bot Detection Slider

Addition Integrations Available in Bot Detection

okta

Platform
General Availability

Platform
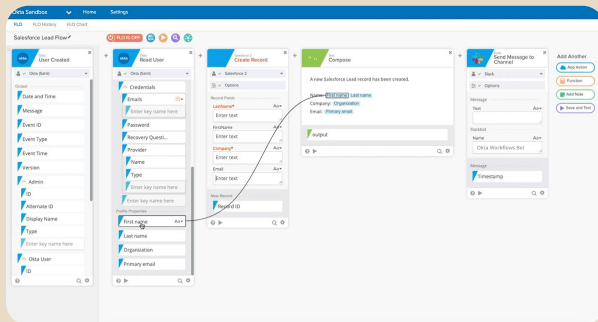## Early Access

Workflows no-code automation

Feature of: Workflows/ Available in: Workflows with a Core Customer Identity AND Workforce Identity Clouds

Kick off a downstream Okta Workflow and provide downstream, asynchronous orchestration, provisioning, security monitoring, log streaming, and more. User Provisioning is a strong feature of Workflows, where based on a user's login or Action trigger, access to additional services can be enabled asynchronously.
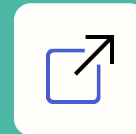
Extensible Password Reset

Feature of: Actions/ Available in: All Plans

Enables customers to extend the existing password reset flow with an action that is triggered after the magic link portion is successful but before the user is prompted to enter a new password.
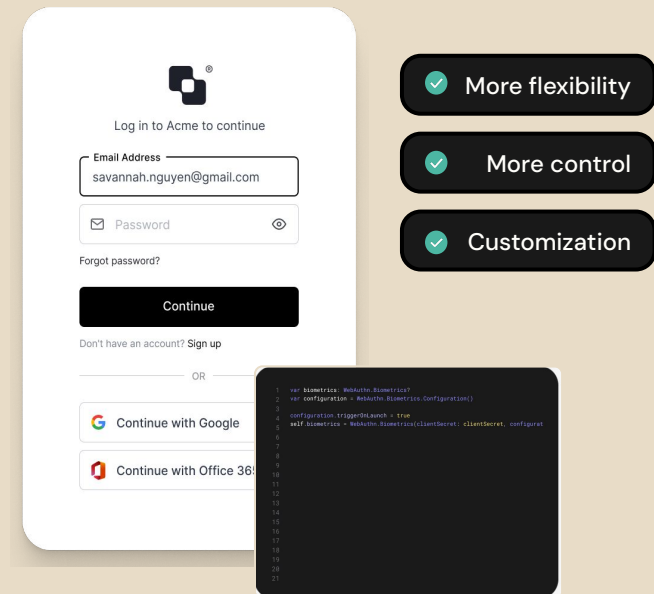
Workflows no-code automation

Post Login + MFA Enhancement Early Access

Feature of: Actions/ Available in: All Plans

Easily define which secondary factors are presented to end-users based on contextual signals such as user attributes, app attributes, or organization information.

✓ More flexibility

✓ More control

✓ Customization

Post Login + MFA Enhancement

okta

Platform – Developer Experience

General Availability

Dark Mode for Docs

Feature of: Core Product/ Available in: All Product Tiers

Add visual theming to docs. Users of the docs can define their preferred theme or let it be controlled by their own OS settings.

Readiness Checks Tool: New Production Readiness Checks Added

Feature of: Core Product/ Available in: All Product Tiers

Help developers go-live with confidence by helping identify best-practice gaps. The feature provides recommended actions and details on how to address checks that are failing.

Auth0 Terraform Provider V1

Feature of: Core Product/ Available in: All Product Tiers

Reverse Terraform support. Automatically export your entire Auth0 resources and configuration for use in Terraform. This feature significantly reduces the time and complexity of getting started with setting up resources in Terraform.

New Capabilities in Actions

Feature of: Actions/ Available in: All Product Tiers

Leverage SAML Mapping, Root-Level User Attributes, and Access Token Scope to unblock unique use cases and complete migrations from legacy Rules and Hooks.

```
> cat terraform.tfstate

{
  "version": 4,
  "terraform_version": "0.12.4",
  "serial": 13,
  "lineage": "6395ed5e-49d9-d469-2bc4-75c44303c8b7",
  "outputs": {},
  "resources": [
    {
      "mode": "managed",
      "type": "aws_route53_health_check",
      "name": "LouisJohnBichardRoute53HealthCheck",
      "provider": "provider.aws",
      "instances": [
        {
          "schema_version": 0,
          "attributes": {
            "child_health_threshold": 0,
            "child_healthchecks": [],
            "cloudwatch_alarm_name": null,
            "cloudwatch_alarm_region": null,
```

Auth0 Terraform Provider V1

okta

Platform – Developer Experience

General Availability

React–native–auth0 V3

Feature of: Actions/ Available in: All Product Tiers

Offers TypeScript support and Hook–based APIs for seamless authentication. Also included in this release is support for real–time user updates, one–line Expo integration, and Android 12.

### Node 18 now available for Actions, Rules and Hooks

Feature of: Actions/ Available in: All Product Tiers

Choose Node 18 while creating new Actions and migrating existing Actions from older Node version. Developers can also select Node 18 in Tenant Global Setting for Rules, Hook, Database scripts, Custom Social Connections, and Universal Login Templates. We strongly recommend that all customers migrate to Node 18 today.

Auth0 Management API

Feature of: Core Platform/ Available in: All Plans

Numerous new features and enhancements for the UI experience.
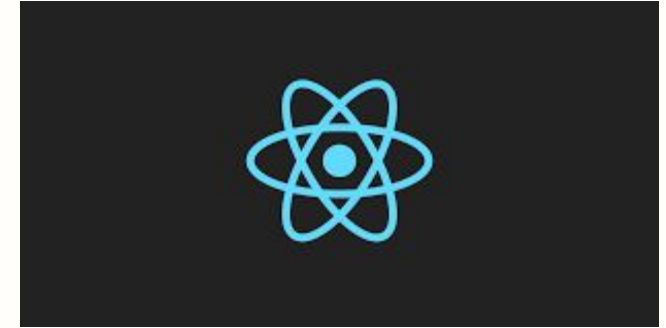
Updates to React Native support

Node.js 18 supported for Actions

okta

Developer Resources

Customer Identity Cloud

Auth0 Developer Center: https://developer.auth0.com/

Auth0 Blog: https://auth0.com/blog/

Auth0 Community: https://community.auth0.com/

Languages and SDKs: https://auth0.com/docs/libraries

Quickstart: https://auth0.com/docs/quickstarts

Auth0 APIs: https://auth0.com/docs/api

Auth0 Developer Blog: https://auth0.com/blog/developers/

Auth0 Marketplace: https://marketplace.auth0.com/

Unveiling New and Improved Product Features — 6 Month Lookback:
https://auth0.com/blog/unveiling-new-and-improved-product-features-6-month-lookback/

okta