



Release Overview

for Early Access & General Availability in Q2 (April – June 2024)

Workforce Identity Cloud Customer Identity Cloud, powered by Auth0

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.

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.



Welcome to the Okta Workforce & Customer Identity Cloud Release Overview

Q2 2024

Welcome back to Okta's Quarterly Release Overview. This year has already brought lots of exciting updates, and we cannot wait to share with you all the innovation we've released in Q2.

Learn how we're raising the bar on security through Workforce Identity Cloud products such as Identity Security Posture Management, Identity Threat Protection with Okta AI, and Workflows which is Audit Ready for FedRAMP High. For Customer Identity Cloud, discover Highly Regulated Identity and Forms for Actions.



Navigating the overview

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



Slide 5

- Okta Workforce Identity Cloud overview
- Workforce Identity Cloud spotlights
- Release overviews
- Developer resources
- Connect with the Okta team and learn more



Slide 28

powered by Auth0

- Okta Customer Identity Cloud overview
- Customer Identity Cloud spotlights
- Release overviews
- Developer resources
- Connect with the Okta team and learn more






Workforce Identity Cloud






The Okta Workforce Identity Cloud enables customers to raise the bar on Identity security, unlock business growth with automation, and modernize IT to reduce operational expenses and drive business efficiency.

This quarter's releases double-down on our commitment to help keep customers secure by empowering customers to harden their Identity security posture, protect from vulnerabilities throughout the user journey through continuous authentication, and more.

Spotlights

-  Identity Security Posture Management (ISPM)
-  Identity Threat Protection with Okta AI (ITP)
-  Workflows Audit Ready for FedRAMP High

All releases

-  Access Management
-  Identity Management
-  Identity Governance
-  Platform Services
-  Privileged Access

Developer resources



Okta Workforce Identity Cloud

A unified solution for everyone and every Identity need

Employees | Contractors | Business Partners

POSTURE ENFORCEMENT + OBSERVABILITY (Identity Security Posture Management)

OKTA INTEGRATION NETWORK | [Connect everything](#)



Access Management

Any resource. Any device. Anywhere.
One secure passwordless experience.



Identity Governance

The right level of access, from a user's
first day to their last.



Privileged Access

Least privilege for everything. No matter who
they are, or what device they use.

PLATFORM | 99.99% Uptime

Directories

Connect in and manage all
of your people

Insights + Reporting

All the data

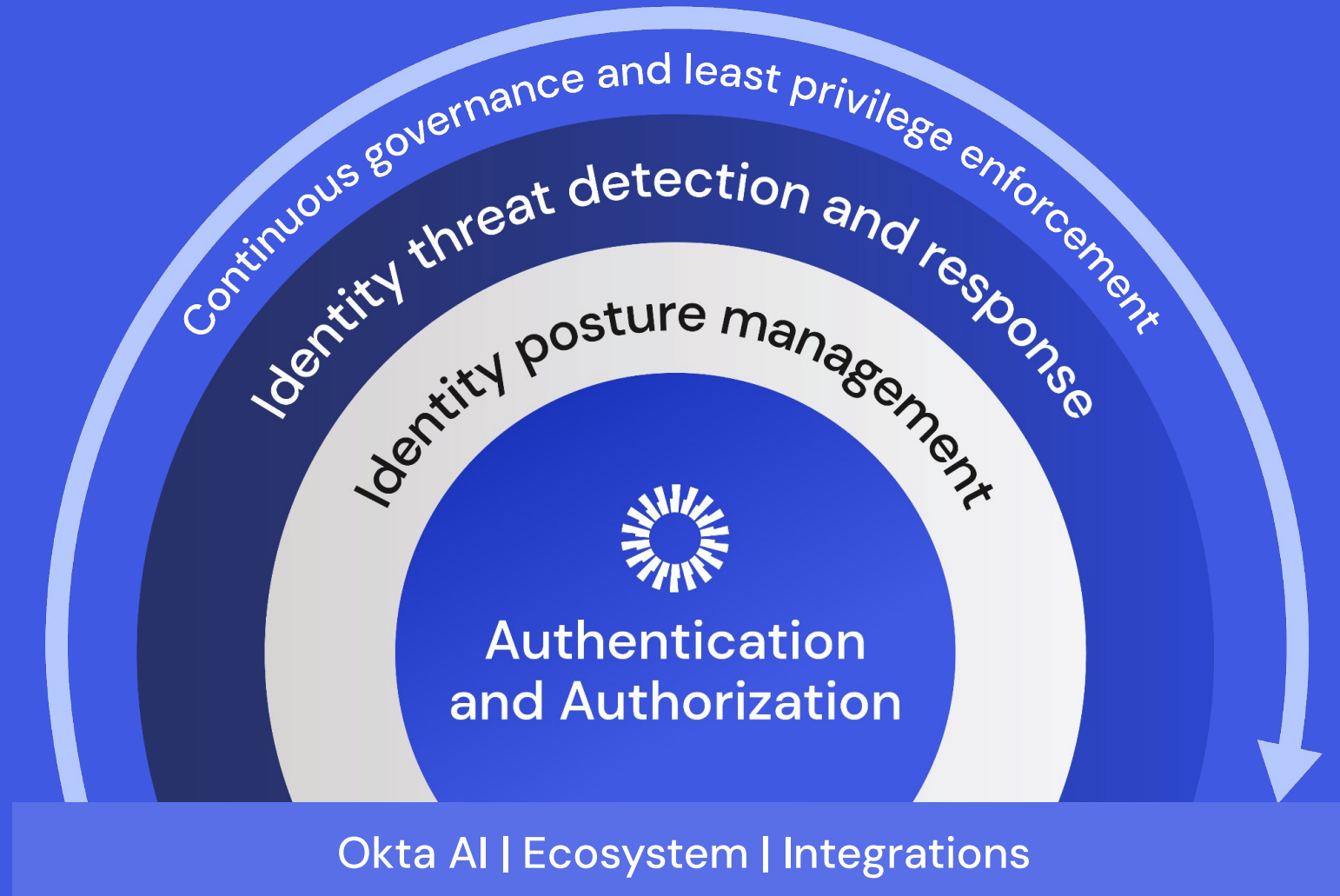
Extensibility

Pro code or no code tools
across Okta APIs + SDKs

Risk Signals

Connect in signals across
your stack

Okta's Secure by Design, Multi Layered Defense Strategy



Workforce Identity Cloud

Q2 spotlights



Identity Security Posture Management

Proactively identify vulnerabilities and security gaps before they can even be exploited.



Identity Threat Protection with Okta AI

Stay ahead of sophisticated identity attacks. Continuously detect and respond to threats during and post-authentication leveraging Okta's native intelligence, amplify security signal sharing across your ecosystem, and automatically orchestrate remediation actions.



Workflows Audit Ready for FedRAMP High

Available for all eligible customers

Support high impact systems and data through Okta Workflows, which is now Audit Ready for Okta for Government High, Okta's FedRAMP High authorized Identity platform.





Spotlight: Identity Security Posture Management (ISPM)

Stop chasing fires, proactively defend against Identity breaches

Available in: IT Products – Identity Security Posture Management

What is it?

Okta Identity Security Posture Management (ISPM) empowers enterprises to proactively take control of their identity sprawl and harden their identity security posture, reducing their attack surface and risk of being breached.

Customer Challenge:

As organizations embrace hybrid /multi-cloud and SaaS infrastructures, security and IT teams struggle to maintain visibility and control over their identity security posture and face new challenges:

- Fragmented and siloed identity data
- Proliferation of dormant and over privileged accounts
- Incomplete MFA coverage
- Gaps in adherence to common security frameworks

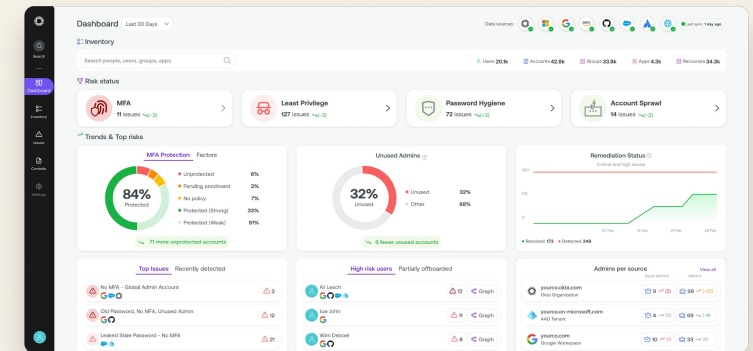
Why this matters

Identity is security, and identity security starts with proactive ISPM. ISPM empowers organizations to take a proactive stance in reducing their identity attack surface and addresses critical identity security challenges by providing:

- A bridge between Security and IT teams to regain control over their identity security posture
- A centralized view of identity security posture across their entire ecosystem
- A proactive approach to detect vulnerabilities, misconfigurations, and policy violations
- A fast path to prioritization and resolution of the most critical identity security issues, such as inconsistent MFA enforcement or excessive privileged access

How to get it

ISPM is available as part of its direct SKU. The product is available as a stand-alone (without WIC or CIC).





Spotlight: Identity Threat Protection with Okta AI (ITP)

Continuous, adaptive security for comprehensive Identity protection

Available in: Identity Threat Protection

What is it?

Identity Threat Protection with Okta AI (ITP) is a real-time security solution that continuously monitors and detects identity-based threats, ensuring robust protection beyond initial login through continuous policy evaluation and reassessment of risks.

Customer Challenge:

Customers face fragmented security landscapes, with multiple apps and devices creating disjointed views of identity risk. This complexity makes it difficult to connect the dots and manage threats effectively, often leaving gaps in security post-authentication.

Why this matters

- ITP provides a unified view of threats by integrating alerts from various security tools, enabling continuous real-time threat detection and response. This holistic approach enhances the overall security posture by ensuring that potential threats are identified and mitigated promptly.
- Continuous monitoring and reassessment of risks help prevent security gaps, particularly post-authentication, where many attacks occur.
- ITP streamlines security operations and improves incident response times by automating threat detection, analysis, and remediation. This allows security teams to efficiently manage identity risks, minimizing manual efforts and ensuring rapid response to potential threats.

How to get it

ITP is available as part of its direct SKU. More information is available on our [pricing page](#). Customers will need to have the following prerequisites before purchasing ITP.

- Universal Directory
- Single Sign On
- Advanced MFA
- Okta Identity Engine

The screenshot displays the 'Post auth session violations' dashboard for the last 24 hours. It shows 14 session violations and 22 security responses. A table below details logouts by app, with 'Okta Dashboard' having 13 logouts and 'salesforce (UL)' having 1. A 'Load More' button and an 'Edit Post auth session' link are also visible.

Post auth session violations		Past 24 hours
Enforced with action		
Session violations	14	Security response 22 out of 22 violations
Logout by app		
App	Logout triggered	Unique users
Okta Dashboard	13	13
salesforce (UL)	1	1





Spotlight: Workflows is Audit Ready for FedRAMP High

Available for all eligible customers

Available in: Workflows Platform SKU

What is it?

Workflows is Okta's no-code automation and orchestration platform that helps customers cut costs and speed up development time by replacing custom code and scripts with Identity automation. With simple "if this then that" logic, templates, pre-built connectors, and the connector builder, almost any identity process can be automated.

Customer Challenge:

The rapid digitization of public services over the past decade has produced complicated tech stacks whose benefits are outweighed by the inconvenience they build into essential functions, and government services are looking for ways to modernize and catch up to core efficiency and productivity standards — including the adoption of tools that allow secure and easy access to essential resources — sets an agency apart.

Why this matters

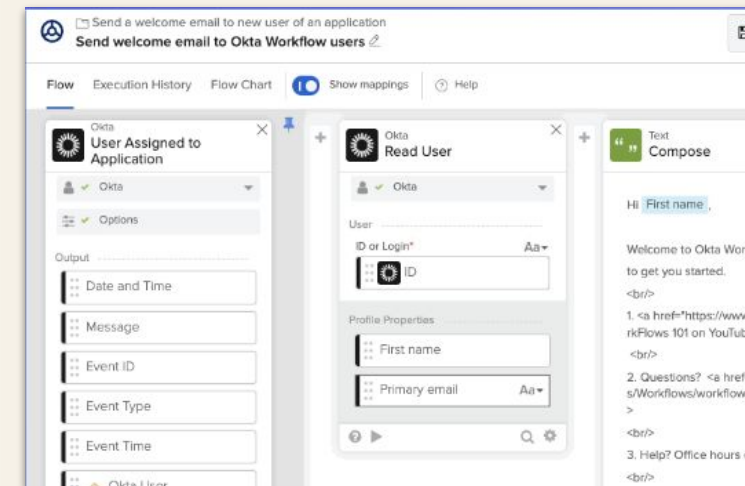
Okta's modern, Identity-centric automation tools offer Federal teams low- and no-code options for building and managing complex functions, maintaining compliance standards, and improving experience management.

- **Centralized Identity-Led Experiences:** Okta centralizes workstreams around the user, helping agencies to develop personalized and protected experiences for everyone, be they a public servant, contractor, member of the public, or partner of an extended ecosystem — all within one centralized platform.
- **Deep, Flexible Partnerships:** Okta has ready-to-integrate integrations as pre-built connectors in Workflows, as well as the ability to connect to any API — making Okta the leading partner in consolidating and protecting those and that which is connected to your agency.
- **Automation at Scale:** Agencies must develop their tech stack with and for their users to ensure it solves actual problems and at scale. Okta's Identity automation boosts agencies' ability to act strategically.

How to get it

Workflows can be purchased through the [Platform SKU](#), in a range of plans from Light (50 flows) to Unlimited.

[Read the blog](#)



Workforce Identity Cloud Releases

The Workforce Identity Cloud (WIC) is a unified solution that ensures the right people have access to the right resources — with least standing privileges — at the right time and in the right context, reassessed continuously. All while delivering a delightful experience for admins and users.

Learn more about our new WIC capabilities released in Q2 2024.

Easily identify the platform each release is available in:

Classic

Okta Identity Engine (OIE)





Identity Security Posture Management

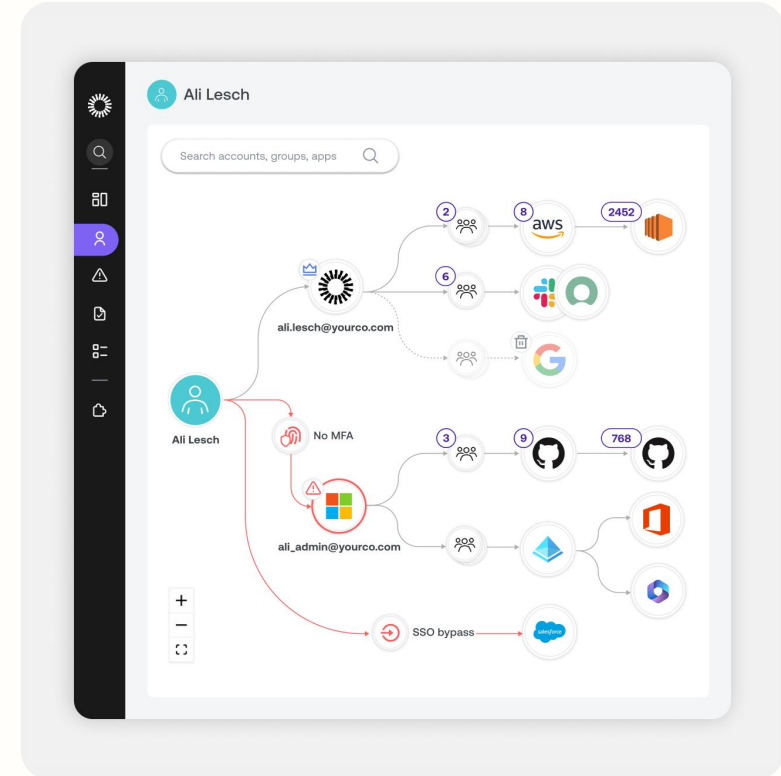
General Availability in North America

Okta Identity Security Posture Management

Feature of: Identity Security Posture Management (ISPM) / Available in: Identity Security Posture Management (ISPM)

Okta ISPM helps organizations identify vulnerabilities, prioritize risks, and streamline remediation, reducing the identity attack surface and the risk of being breached.

[Learn more](#)



Identity Security Posture Management





Access Management

General Availability

Desktop MFA for macOS

Available in: Okta Device Access, FedRAMP Moderate/High/DOD IL4 Audit Ready

Enforce an additional layer of security with MFA on top of a credential login at the desktop unlock screen for macOS.

[Learn more](#)

OIE

Desktop Passwordless Login for Windows

Available in: Okta Device Access, FedRAMP Moderate/High/DOD IL4 Audit Ready

Enable a passwordless experience at Windows login by allowing end users to securely sign in to their Windows workstations using only Okta Verify Push with biometrics.

[Learn more](#)

OIE

Desktop Password Sync Enhancement

Available in: Okta Device Access, FedRAMP Moderate/High/DOD IL4 Audit Ready

Ensure that macOS account passwords remain in sync with Okta with support for Desktop Password Sync at the login screen and lock screen.

[Learn more](#)

OIE

Enforce an Allowlisted Network Zone for use of Static (SWSS) API Tokens

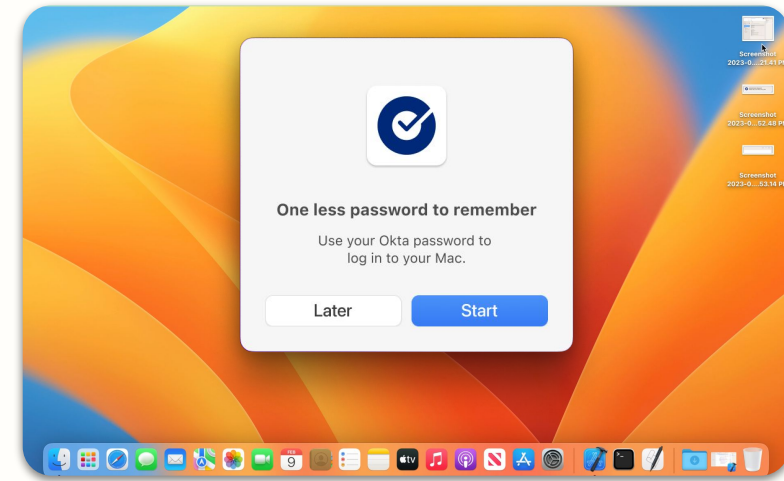
Available in: All SKUs, FedRAMP Moderate/High/DOD IL4 Authorized

Enhances the security of Okta API tokens by preventing attackers from stealing and using SSWS tokens outside the specified IP range to gain unauthorized access.

[Learn more](#)

Classic

OIE



Desktop Password Sync Enhancement





Access Management

General Availability

FastPass User Verification with Passcode

Available in: MFA, AMFA, FedRAMP Moderate/High/DOD IL4 Authorized

Provide end users with the flexibility to complete FastPass user verification with either a device-bound passcode or biometrics.

[Learn more](#)

OIE

FIDO2 Security Keys for Desktop MFA for macOS

Available in: Okta Device Access, FedRAMP Moderate/High/DOD IL4 Authorized

Secure the macOS login experience by allowing end users to use a FIDO2 security key, a high security assurance authenticator, to meet their Desktop MFA challenge.

[Learn more](#)

OIE

Multiple Identifiers

Available in: All SKUs, FedRAMP Moderate/High/DOD IL4 Authorized

Admins can streamline the sign in experience by giving users more options to identify themselves with. Admins can specify which identifiers can be used across various applications.

[Learn more](#)

OIE

Preventing Account Lockups for All Users

Available in: SSO, FedRAMP Moderate/High/DOD IL4 Authorized

Prevents legitimate users from being locked out if another device that is unknown to Okta causes a lockout. Enables customers to block suspicious sign-in attempts from unknown devices, while users who sign in to Okta with devices that they've used before are not locked out.

Classic

OIE

← Back to all user profile policies

Default Policy Help

Enrollment Identification Apps (20+)

Profile identification + Add Identifier

Determine the default profile attributes that users can provide for identification. You can add up to 2 additional attributes. [Learn more](#)

PRIORITY	DISPLAY NAME	VARIABLE NAME	
1	Username	login	
2	Employee ID	employeeId	
3	Custom attribute 2	customAttr2	

To change the labels shown to users, go to [Brands](#) and edit the sign-in page.

Multiple Identifiers





Access Management

General Availability

Session and Token Correlation in the System Log

Available in: All SKUs, FedRAMP Moderate/High/DOD IL4 Authorized

Consistent traceability across system log events generated within a session or with an API token.

Classic

OIE

Sign On Policy: Granular Authentication Methods

Available in: SSO and MFA, FedRAMP Moderate/High/DOD IL4 Authorized

Specify which authenticators are permissible to ensure precise control over user access and compliance, while optimizing the authentication experience across devices and user profiles.

[Learn more](#)

OIE

Actor	Event Info
Feb 01 10:19:43	Frances Burke (User) Reset all factors for user SUCCESS
<ul style="list-style-type: none"> ▶ Actor ▶ Client ▼ Event <ul style="list-style-type: none"> ▼ AuthenticationContext <ul style="list-style-type: none"> AuthenticationProvider AuthenticationStep CredentialProvider CredentialType ExternalSessionId Interface Issuer RootSessionId DisplayMessage EventType Outcome Published SecurityContext Severity System <ul style="list-style-type: none"> ▼ DebugContext <ul style="list-style-type: none"> ▶ DebugData LegacyEventType Transaction <ul style="list-style-type: none"> ▼ Detail <ul style="list-style-type: none"> RootApiTokenId ID Type UUID 	Frances Burke(id: 00u3hk8uoXQ8qV1KO1s6) 0 trsm2J15S57T_-7wyKRZMxbLQ trsgfZJJ9fTkeHWFajh3Ej_Q Reset all factors for user user.mfa.factor.reset_all 2024-02-01T15:19:43.867Z INFO core.user.factor.reset_all 00Tih8osgxp4F5bg1s5 Zbu2j6UGew1UY4gbN83aOAAABS4 WEB 53c09cb3-c115-11ee-9eee-8792a1fd0b0f

Session and Token Correlation in the System Log





Access Management

Early Access

Apple Business Manager Federation

Available in: Universal Directory, SSO, LCM, FedRAMP Moderate/High/DOD IL4 Authorized

Simplify Managed Apple ID provisioning while using Okta as a Federation layer into Apple devices and services. This integration allows an end-user to securely log into Apple devices and services using their Okta credentials while also allowing Okta to send security detections through our Shared Signals Framework (SSF) to Apple so that immediate action can be taken to prevent any Managed Apple IDs to be compromised. [Learn more](#)

OIE

Breached Password Protection

Available in: Universal Directory, FedRAMP Moderate/High/DOD IL4 Audit Ready

In-house detection and remediation for the mining of breached credentials. Leverage webhook-eligible system log events to take additional actions outside of the default password reset remediation. [Learn more](#)

Classic

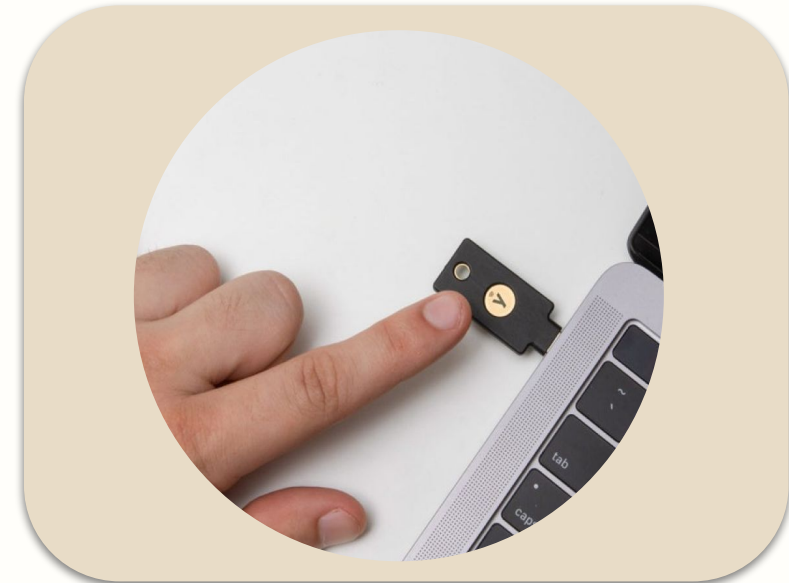
OIE

FIDO Pre-Reg

Available in: AMFA, FedRAMP Moderate/High/DOD IL4 Authorized

Okta Admin can set up the new employee onboarding workflow to get a pre-enrolled FIDO2 YubiKey for that employee. That key is shipped to the employee directly via the Yubico Enterprise Delivery subscription. Okta admins can also seamlessly enforce phishing resistant authentication for their existing employee base with a pre-enrolled FIDO2 authenticator

OIE



FIDO Pre-Reg





Access Management

Early Access

Identity Threat Protection with Okta AI

Available in: Identity Threat Protection

Stay ahead of sophisticated identity attacks. Continuously detect and respond to identity threats during and post-authentication, amplify security signal sharing across your ecosystem, and automatically orchestrate remediation actions.

[Learn more](#)

Classic
OIE

MFA to the Okta Admin Console

Available in: SSO, ASSO, MFA, AMFA, FedRAMP Moderate/High/DOD IL4 Authorized

Raise the bar for secure access to Okta by an administrator and reduce the likelihood of a breach by enforcing MFA to the Okta Admin Console.

Classic
OIE

Same-Device Enrollment for Okta FastPass

Available in: All SKUs, FedRAMP Moderate/High/DOD IL4 Authorized

Enable improved Okta Verify and FastPass end user enrollment flows for desktops and mobile devices.

[Learn more](#)

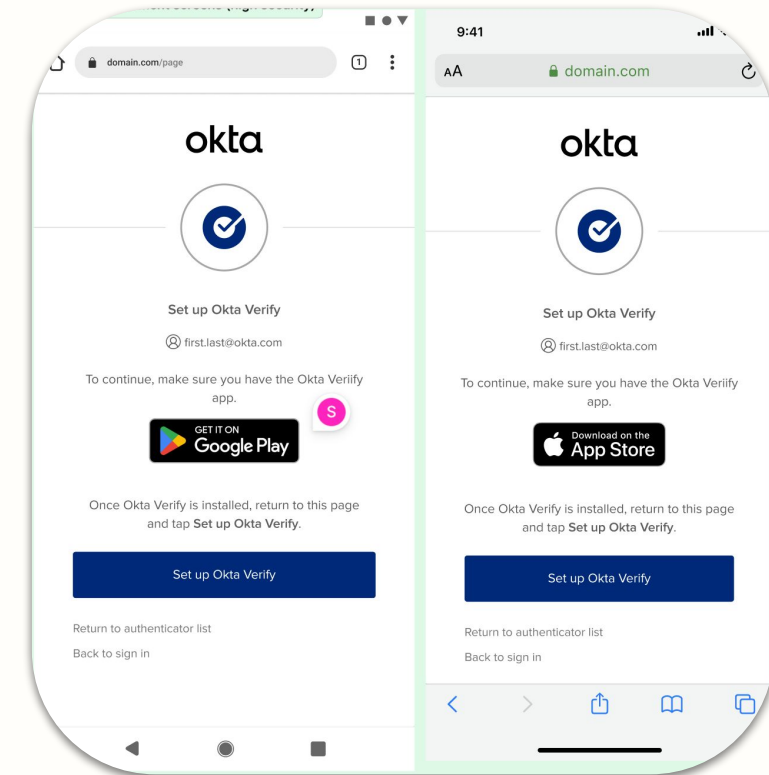
OIE

Supporting NotOnOrAfter property in Single Logout

Available in: SSO and Core, FedRAMP Moderate/High/DOD IL4 Authorized

Provides an additional layer of security by limiting the time period of a message passed in the SAML assertion.

OIE



Same-Device Enrollment of Okta FastPass





Identity Management

General Availability

Agent Permission for Custom Admins

Feature of: Universal Directory / Available in: Universal Directory

This enables customers to grant directory management capabilities via custom admin roles framework and avoids the need for Super admin for managing Directory integrations. Permissions available include ability to configure AD/LDAP directories, update configuration settings, etc.

Classic

OIE

Secure Communication and Deployment for AD Agent

Feature of: Universal Directory / Available in: Universal Directory

Secure AD agent deployment with a device registration flow that isolates the agent from admin accounts.

Classic

OIE

Fine Grained Scopes for Office 365 Provisioning and Federation

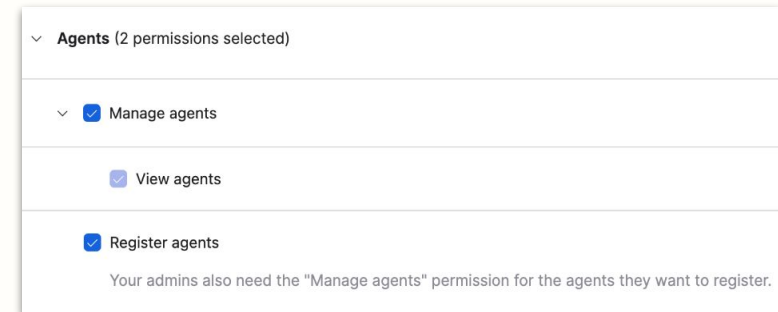
Feature of: Universal Directory / Available in: Universal Directory

Provision and federate O365 with Graph API OAuth scope, eliminating dependency on Azure admin credentials.

Classic

OIE

[Learn more](#)



Agent Permission for Custom Admins





Identity Governance

General Availability

OIN Apps for Entitlement Management – GitHub Teams

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

Discover, import, store, and manage entitlements within Okta via bundles, policies, and rules with out-of-the-box integrations for GitHub Teams.

[Learn more](#)

Classic
OIE

Request on Behalf Of

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

Optimize onboarding use cases by enabling managers and IT teams to proactively initiate ad hoc access requests on behalf of users, speeding access for end users.

[Learn more](#)

Classic
OIE

Preview:
Request

App Y

Request for

GA You

5 USERS

Search users...

GA You

AH Alex New Hire

AV Ali VP

NK naini khajanchi

SM Sam Manager

ed access to X resource? *

source? *

Submit new request

Request on Behalf Of





Identity Governance

Early Access

Configurable Reviewer Context

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

Choose the right contextual insights to provide access certification reviewers, including application usage, group membership, and application assignment date so reviewers can make the right access decision quickly and effectively.

Classic
OIE

Flexible Access Request Conditions

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

A flexible experience for admins configuring access requests that gives them the ability to require different approvals based on a requester's profile and group memberships, so that common access request configurations can be reused.

[Learn more](#)

Classic
OIE

Resource-Centric Access Request Catalog

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

Give users the ability to request and view existing access from the same dashboard experience they already use on a daily basis.

[Learn more](#)

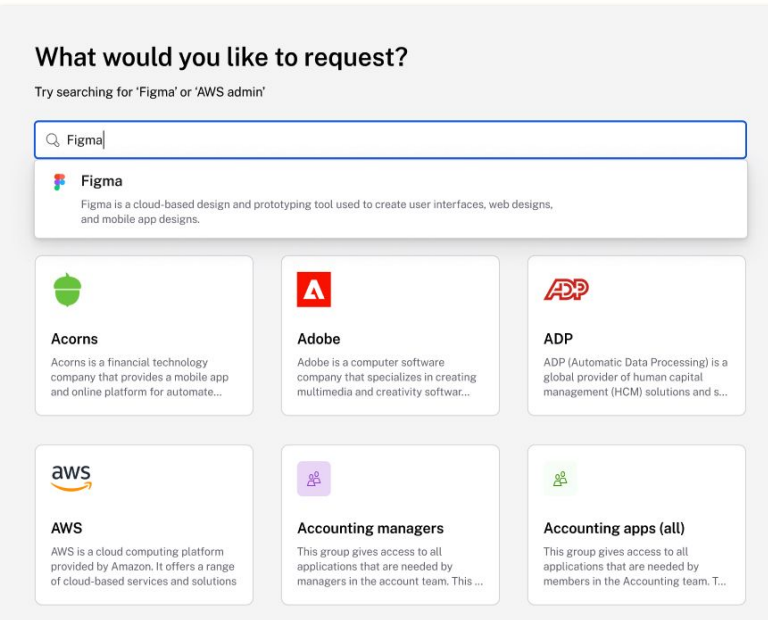
Classic
OIE

Third Party Access Request Context

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

Ingest third party access request decisions and context from tools like JIRA and SNOW to fulfill and document access request decisions alongside Okta Access Requests to deliver a centralized, audit-friendly experience.

Classic
OIE



Resource-Centric Access Request Catalog





Identity Governance

Early Access

Time-Based Access

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

Give admins the ability to time-bound access for only the duration a user needs it, increasing security and minimizing the risk of unauthorized standing access.

Classic
OIE

Search for people and apps

Review assignment to O365 for Sheldon Cooper

User will lose access to this app (Access duration)

TKTKT something if needed including this applies to everything - app and entitlements

- Never
- On date
- After duration

Entitlements

TKTKT Set access level

Time-Based Access





Platform Services

General Availability

Apply IP Session Binding to all Okta Admin sessions

Feature of: all SKUs, FedRAMP Moderate/High/DOD IL4 Authorized

Prevent session takeover by invalidating Okta admin sessions when the source IP changes. This is done by automatically revoking an admin session if the IP address during an API or web request differs from the originating IP. [Learn more](#)

Classic

OIE

Okta Workflows Connector Enhancements

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 and Okta Realms connector. [Learn more](#)

Classic

OIE

Oracle HCM Cloud Connector

Feature of: Workflows / Available in: Workflows

A new HR connector for all customers that want to use Oracle HCM and Anything-as-a-Source. [Learn more](#)

Classic

OIE

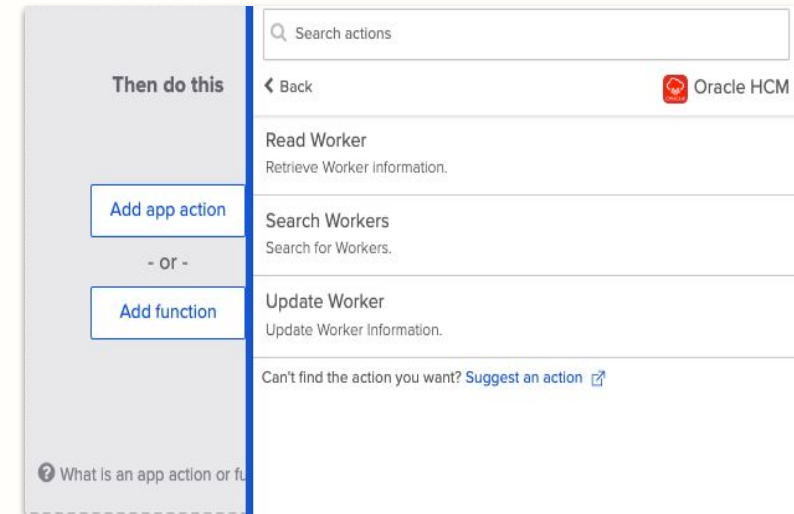
Seamless SAML & OIDC ISV Experience with the OIN Wizard Automated Testing

Feature of: OIN Wizard / Available in Admin Console

Reduce time to: 1) Submit SAML OIN integration due to automated testing and validation of integration metadata during submission process 2) Publish integrations due to reduction in OIN Operations responsibilities to manually add metadata. [Learn more](#)

Classic

OIE



Okta Workflows Connector Enhancements





Platform Services

Early Access

Workflows Execution History Inspector

Feature of: Workflows / Available in: Workflows, FedRAMP Moderate/High Audit Ready

Provides visibility into Workflow execution performance, helping customers troubleshoot errors and better understand flow execution metrics.

Classic
OIE

Workflows Execution Log Streaming

Feature of: Workflows / Available in: Workflows, FedRAMP Moderate/High Audit Ready

Equips Admins with a single view of recent execution history per workflow within the Workflows UI so they can best triage errors and view success.

Classic
OIE

Workflows Audit Ready for FedRAMP High (Available for all eligible customers)

Feature of: Workflows, FedRAMP Moderate/High Audit Ready

Okta Workflows is our no-code automation and orchestration platform for building and managing complex functions, maintaining compliance standards, and improving experience management. Workflows has reached audit-ready status for Okta for Government High, our modern Identity platform built exclusively for U.S. government agencies and their mission partners, at the FedRAMP High authorization level.

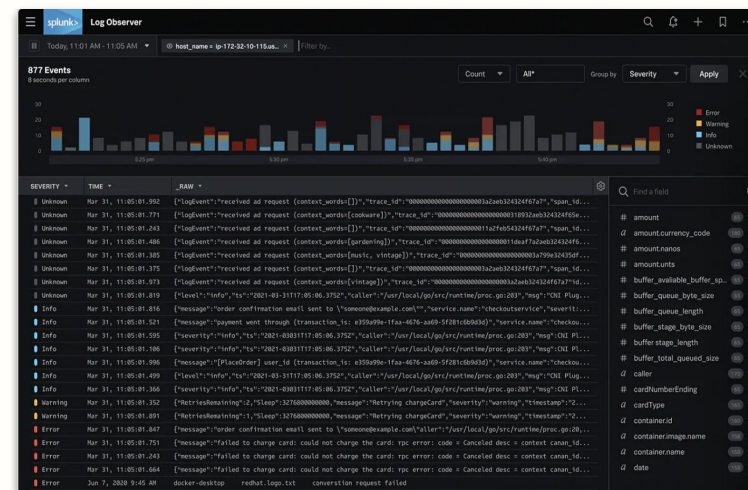
Classic
OIE

Role-Based Access Control (RBAC)

Feature of: Workflows / Available in: Workflows, FedRAMP Moderate/High Audit Ready

Allows customers to expand their use of Workflows beyond Super-Admins, enabling more team members to have access and permission to create workflows for critical use cases.

Classic
OIE



Workflows Execution Log Streaming





Privileged Access

General Availability

Checkout

Feature of: Okta Privileged Access / Available in: Okta Privileged Access

Limit access to shared privileged accounts to one person at a time with time-bound control.

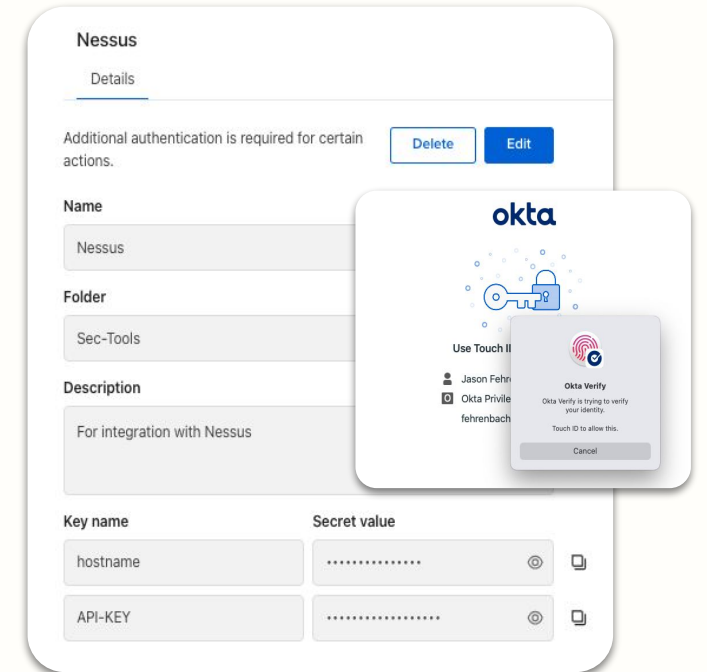
Classic
OIE

Transactional MFA for Secrets

Feature of: Okta Privileged Access / Available in: Okta Privileged Access

Enforce stronger security by requiring user to use MFA before revealing secrets.

Classic
OIE



Transactional MFA for Secrets



Developer Resources

Workforce Identity Cloud

Build, integrate, and ship Identity and Access Management experiences that your users will love. Get the latest release updates, curated guides, and community feedback on your builds.

Resources

Okta Architecture Center: Click [here](#)

Enterprise Readiness workshops: Click [here](#)

Developer blog: Click [here](#)

Languages and SDKs: Click [here](#)

Getting Started guides: Click [here](#)

Release Notes: Click [here](#)

Okta Developer Community forum: Click [here](#)

Okta Community Toolkit – App Showcase: Click [here](#)

OktaDev YouTube channel: Click [here](#)



Resources

Connect with the Okta team and learn more



Release Website

View [here](#)
Contact sales [here](#)



WIC Product Roadmap Webinar

Sign up [here](#)



WIC Release Highlights

View [here](#)



Release Notes

Read [here](#)





Customer Identity Cloud

Okta Customer Identity Cloud, powered by Auth0, enables secure and seamless digital experiences that businesses and customers expect.

This quarter's releases empower app builders with:

- Powerful extensibility capabilities for more customization
- Okta AI-driven security enhancements to boost security without disrupting users
- Streamlined authorization options for added flexibility

Spotlights

-  Highly Regulated Identity
-  Forms for Actions

All features

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

Developer resources



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

Actions

Deployment Options

SDKs, APIs, Quickstarts

Marketplace



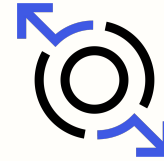
Customer Identity Cloud

Q2 spotlights



Highly Regulated Identity (HRI)

This Solution Suite on the Customer Identity Cloud delivers Financial Grade Identity™ with elevated security, privacy, and UX controls for sensitive customer operations beyond login.



Forms for Actions

This new feature of Actions allows customers to easily orchestrate, personalize and secure Identity flows with a no code, visual editor. Forms for Actions gives customers a quick way to build frictionless customer experiences, accelerate time to market, improve form conversion rates, and stay competitive with UX.





Spotlight: Highly Regulated Identity

Elevate security, privacy, and user experience beyond login.

Available in: *Highly Regulated Identity SKU*
or *Enterprise Premium Security Solution Bundle*

What is it?

Highly Regulated Identity is a Solution Suite on the Okta Customer Identity Cloud that delivers Financial Grade Identity™ controls. Elevate security and privacy while maintaining compliance and intuitive user experiences for your most sensitive customer interactions beyond login.

Customer Challenge:

Sensitive customer interactions beyond login are difficult to execute:

- Step up security and consent controls can be frustrating or non-existent.
- Higher risk operations face elevated fraud targeting users and the end-to-end flow.
- Ever-evolving compliance is hard to keep up with.

Why this matters

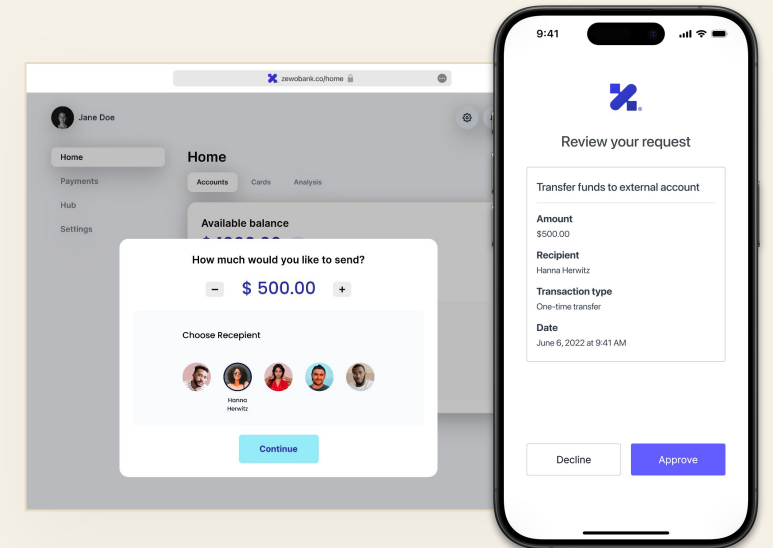
Safeguard sensitive customer operations such as updating account information, admin or security settings, accessing sensitive data or apps, sending money, making an open banking payment, and more.

- **Step-up security and avoid fraud** – Strong Customer Authentication (SCA) is a financial grade contextual authorization framework for sensitive customer operation approvals.
- **Empower informed approvals in real-time** – Dynamic linking ties transaction details to the SCA approval confirmation, Rich Authorization Requests (RAR) relay this context to the user to review to avoid transaction tampering.
- **Invisible to users, elevate data privacy and app security** – with a certified FAPI 1 Advanced security profile implementation.
- **Implement faster** – use Actions and UX templates for low or no code custom flows.

How to get it

The new [Highly Regulated Identity](#) SKU unlocks a growing Solution Suite of Financial Grade Identity™ controls for sensitive customer interactions beyond login.

[Explore Highly Regulated Identity](#)





Spotlight: Forms for Actions

New feature of Actions Extensibility Platform

Available in: *Advanced Extensibility SKU*

What is it?

Forms for Actions is a feature of Okta's Customer Identity Cloud Actions extensibility platform that provides developers and UX teams with a no-code visual editor to easily and quickly build forms to customize the login and sign up experience.

Customer Challenge:

Frictionless sign-up and login experiences are crucial for winning over customers and staying competitive. Businesses today need tools that not only ensure operations are efficient and secure, but that also help drive customer retention and growth, can be flexible to their unique security needs, and that unify and activate data across multiple apps and systems.

Why this matters

Extensibility is key for every customer today, helping Deliver frictionless end-user experiences and boost revenue. There are various use cases and customizations that require extending an Identity solution to deliver business outcomes.

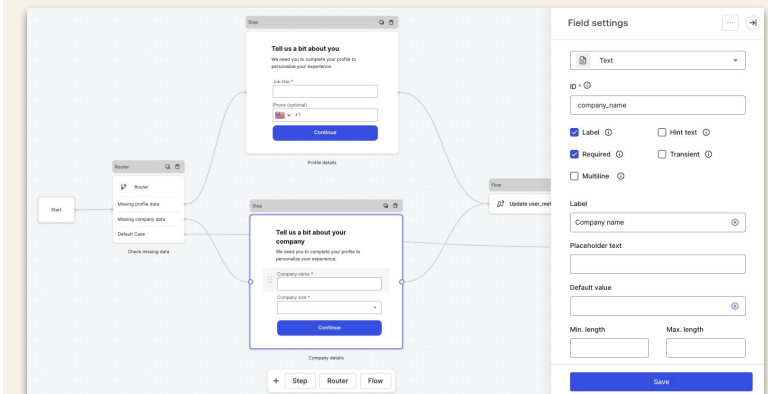
- **Accelerate time to market:** Easily build and edit forms with a no-code visual editor.
- **Build frictionless customer experiences:** Simplify adding custom policies and terms to signup and login flows.
- **Improve form conversion rates:** Collect and activate relevant customer data and enrich customer profiles over time with progressive profiling.

How to get it

Okta offers Actions, Auth0 Marketplace, and now Forms for Actions, enabling you to customize according to your needs and leverage the full spectrum of solutions with pro- or no-code.

The new [Advanced Extensibility](#) SKU unlocks new Actions + Forms capabilities.

[Read the blog](#)



Customer Identity Cloud Releases

Okta Customer Identity Cloud (CIC) is dedicated to ensuring that security comes first when it comes to providing seamless digital experiences. CIC enables organizations to take advantage of technologies that accelerate growth and provides tools to help teams successfully navigate the ever-evolving security landscape, while seamlessly protecting customer and business data.

Learn more about our new CIC capabilities released in Q2 2024.





Authentication

General Availability

WCAG 2.2 AA

Feature of: Core Platform / Available in: All plans

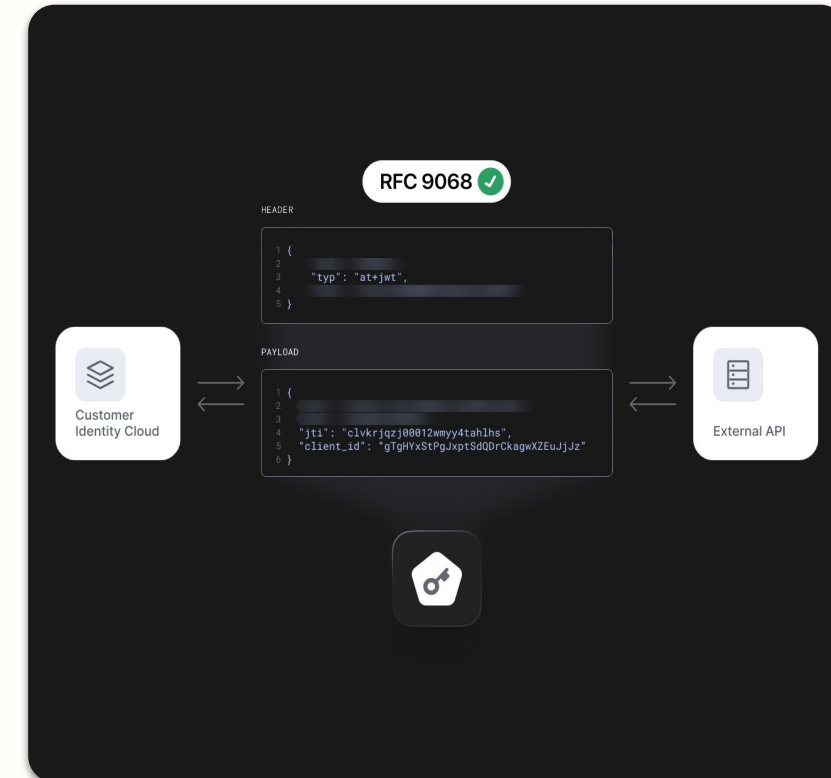
This is a self-service opt-in, Early Access release of several accessibility improvements to Universal Login as part of our efforts to reach WCAG 2.2 AA guideline conformance. The release allows customer to opt-in to these and future improvements.

JSON Web Token (JWT) Access Token Profiles

Feature of: Core Platform / Available in: All plans

Support for JWT Profile for OAuth 2.0 Access Tokens – RFC9068. This identity industry standard will maximize compatibility and interoperability with other solutions as well as reusability of community tools.

[Learn more](#)



JWT Access Token Profiles





Authentication

Early Access

Flexible Identifiers

Feature of: Core Platform / Available in: All plans

Flexible identifiers enable the use of any combination of phone number, email, or username at sign-up and sign-in.

[Learn more](#)

Phone Number Configuration ✕

Use Phone Number as Identifier
Turning this on will make phone number an identifier for this connection. Users will be able to use phone number for login and password reset.

Signup with Phone Number

Off

Optional

Required

Users must enter their phone number to sign up.

Verify phone number on sign up
Requires users to verify their phone number via SMS with a one-time password to sign up for an account.

Require phone number on user profile
Requires phone number to be present across all actions that create or update a user profile on this connection.

Phone Message Provider
Visit [Phone Message Provider](#) to make changes to your SMS delivery provider.

Flexible Identifiers





Authentication — SaaS Apps

General Availability

Directory Sync with Inbound SCIM

Feature of: Enterprise Connections / Available in: B2B Essential, B2B Professional, Enterprise, Enterprise Premium SKUs

Streamline user management by automating the provisioning and de-provisioning of user access across applications. Reduce manual effort, increase security, and enable your organization to scale with ease while ensuring compliance.

[Learn more](#)

Sign-up with Organization Memberships

Feature of: Organizations / Available in: B2B Essentials, Professional, Enterprise plans

Allow users to seamlessly sign up for an Organization directly through our login page, removing the need to create custom UIs that leads to lengthy development cycles.

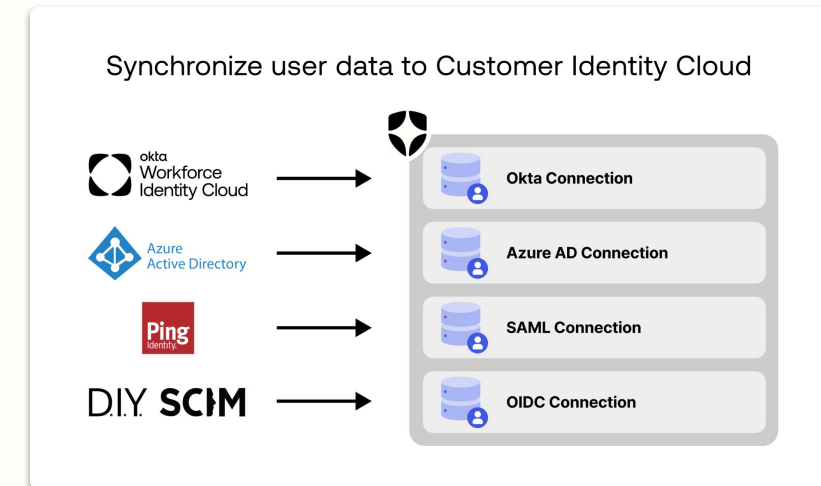
[Learn more](#)

B2B SaaS reference app – SaaSStart

Feature of: Auth0 / Available in All

An up and running reference application that allows developers to easily explore and gain experience with key B2B Customer Identity function such as multi-tenancy access control, user provisioning, security policies, and more.

[Learn more](#)



Directory Sync with Inbound SCIM





Authorization

General Availability

Authorization for Fine Grained Authorization (FGA) Store Credentials

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

Provide different credentials for each FGA store. These credentials can have permission sets.

[Learn more](#)

Spring Security

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

Use the @PreAuthorize Spring Security annotation with an FGA bean that will require an authorization check to pass before executing a method.

[Learn more](#)

Modular Models

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

FGA now enables you to compose an authorization model from multiple modules. Each module lives in a different file, owned by each application team.

[Learn more](#)

FGA Support JetBrains–Based IDEs

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

Improve how users of JetBrains IDEs can create and test FGA models.

[Learn more](#)

The screenshot displays the 'Authorized Clients' interface in the Okta Admin Console. It features a table with three entries: 'Company Knowledgebase' (ID: KHVFBVTCULG232NX3BIUWF9FEF1C2XRQN), 'Web Application' (ID: RQPP9ANBQZE790F51PLNBCHXSZ5KB10A), and 'Native Application' (ID: 47QEXFPDZKEMUUSSTVMPLIUJFICRSHXF). Each entry has a 'Manage' link. A '+ Create Client' button is located in the top right corner. A modal window titled 'Internal HR Application' is open, showing 'Client Permission Sets' with three options: 'Read/Write model, changes, and assertions', 'Write and delete tuples', and 'Read and query'. The 'Read and query' option is selected. A 'Create' button is at the bottom right of the modal.

Fine Grained Authorization Store Credentials





Security

General Availability

Fourth Generation Bot Detection

Feature of: Attack Protection / Available in: Attack Protection

This upgrade combines the capabilities of our CIC machine learning model with third-party bot scoring, significantly enhancing our ability to identify and thwart bots more effectively and safeguarding against malicious traffic.

[Learn more](#)

Auth Challenge

Feature of: Attack Protection / Available in: Attack Protection

Auth Challenge is the new default Bot Detection response that offers an invisible, frictionless alternative to CAPTCHA. Auth Challenge uses a series of non-intrusive challenges to make it tougher on bots but frictionless for users.

Bot Detection on Recovery Flow

Feature of: Attack Protection / Available in: Attack Protection

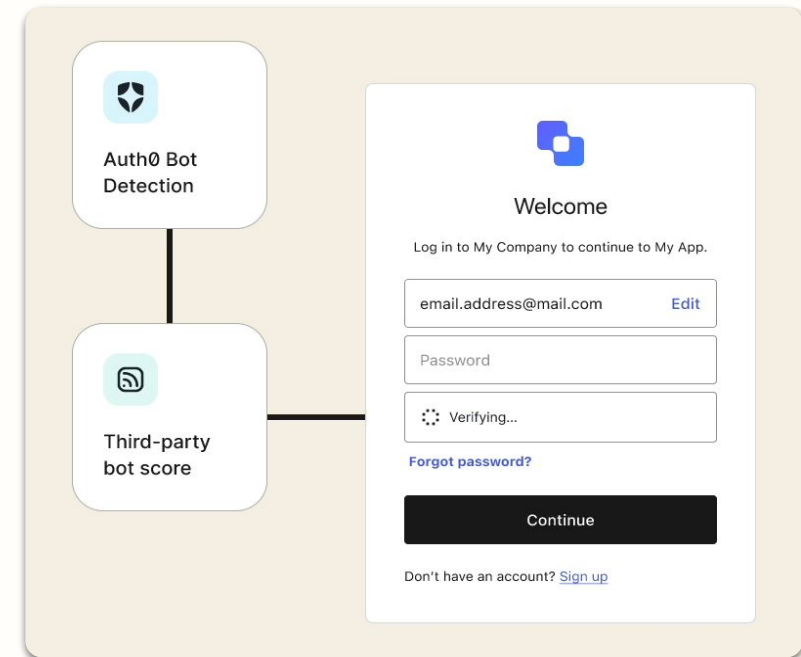
We're extending the capabilities of our bot detection to protect against scripted attacks and bots in the password reset flow. If we suspect a request is coming from a bot, we'll challenge the request with a CAPTCHA.

[Learn more](#)

Session and Refresh Token Management API

Feature of: Session Management / Available in: Enterprise

Gives developers remote control of their user's authentication status through additional management API endpoints to list, explore and terminate session and refresh tokens.



Bot Detection Enhancements





Security

Early Access

Bring Your Own Key

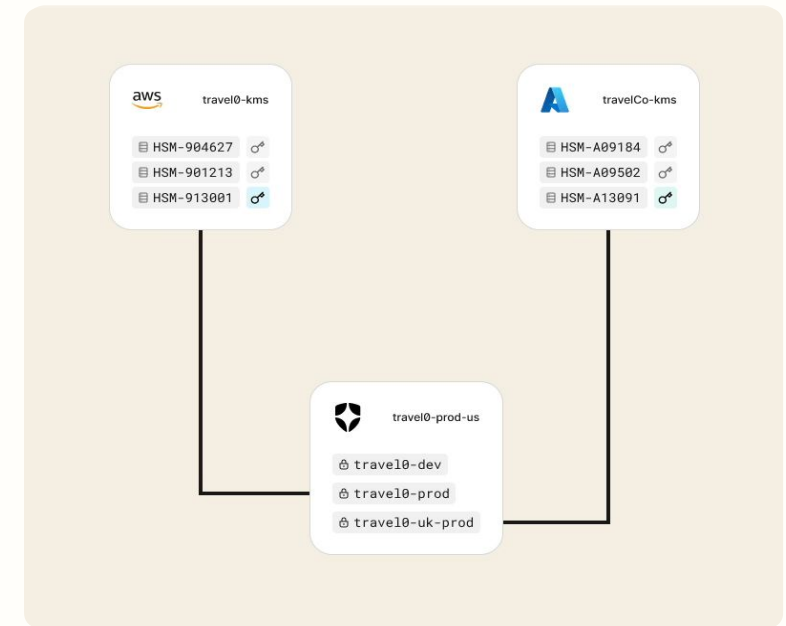
Feature of: Highly Regulated Identity / Available in: Highly Regulated Identity

Allows to upload customer self-generated keys for the encryption of tenant master keys.

Control Your Own Key

Feature of: Highly Regulated Identity / Available in: Highly Regulated Identity

Provide a CLI-based interface to tenant master key rotation (that is, Key Rotation CLI) that allows specific incident management role(s) to rotate the KMS Keys and the direct namespace key (NSK) rotation.



Bring Your Own Key





Platform

General Availability

Actions Migration Tooling

Feature of: Actions

Simplify the migration process of Rules to Actions by using the Rule Migration tooling in the AuthO Dashboard. In addition to facilitating the switch from a Rule to an Action, the new tooling also offers built-in guidance and fixes for common Rule patterns.

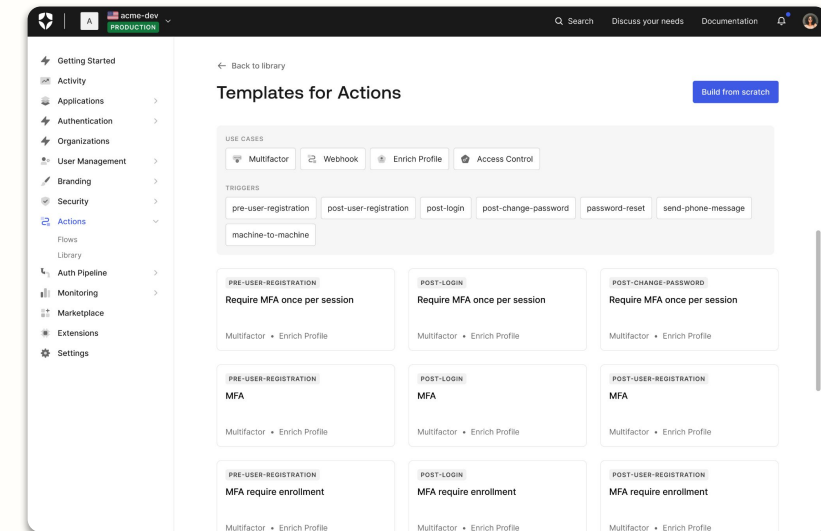
[Learn more](#)

Templates for Actions

Feature of: Actions

Templates help you kickstart Actions with one click pre-built templates for common use cases. Now, we've released a series of hands on guides to help Developers build even faster.

[Learn more](#)



Actions Templates





Platform Developer Experience

General Availability

Account Activity Audit Logs available on Teams

Feature of: Teams / Available in: All Plans

We've updated the Teams Dashboard to include a new report called Team Activity under the Reports section of the Teams Dashboard. Team Activity allows Team Owners to view and audit event logs generated by team members.

[Learn more](#)

Mandatory Apple Privacy Manifest Changes for Auth0.swift

Feature of: Auth0 SDKs / Available in: All Plans

Apple's privacy initiative is designed to enhance user transparency and control over personal data. By aligning with these changes, we ensure our SDK maintains its reputation for privacy and security, adheres to industry standards, and remains accessible on the App Store.

[Learn more](#)

Extensibility as a Custom Provider for Phone Notifications

Customize outbound flexible identifier phone messages and providers with a new Phone Extensibility Action.

Personalized App Integration

Feature of: Auth0 Dashboard / Available in: All Plans

Offers a personalized guided walkthrough for developers for the following options: Integrating an existing developer app, learning how to integrate using a sample auth0 app.

Member	Event Type	Event	Date	
John Doe	Team invitation	John Doe invited Jane Doe to Travel0	Mar 23 2022, 11:23 AM	View Details
Jaya Odo	Tenant invitation	Jaya Odo invited Jane Doe to tenant1	Mar 23 2022, 11:23 AM	View Details
Yishai Kyung	Team role	Yishai Kyung updated Jane Doe's role to Team Owner	Mar 23 2022, 11:23 AM	View Details
Billy Aiden	Security policies	Billy Aiden enforced SSO	Mar 23 2022, 11:23 AM	View Details

Account Activity Audit Logs for Teams





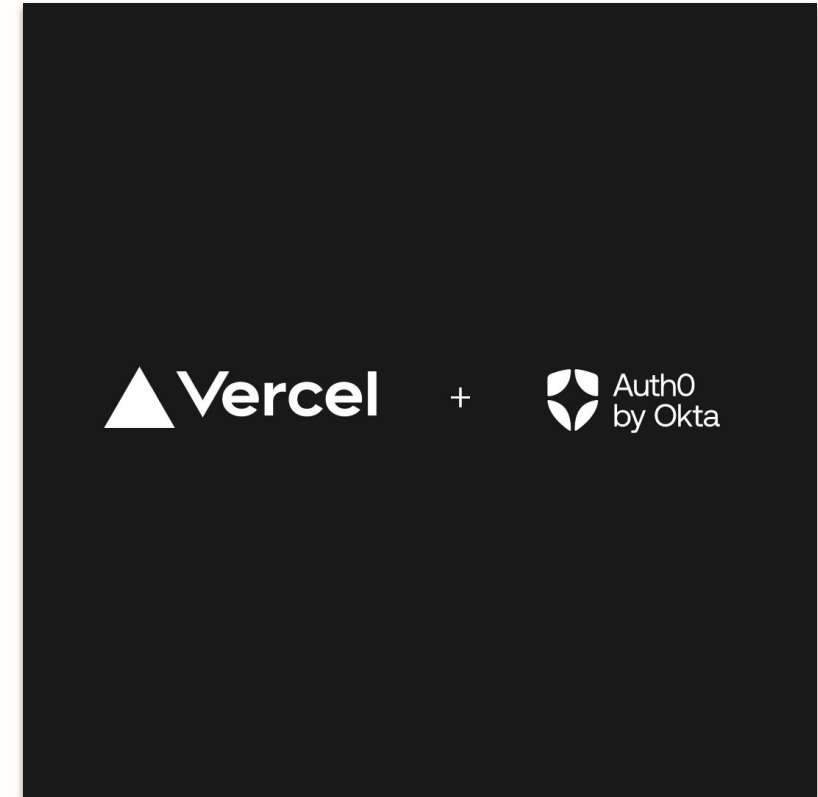
Platform Developer Experience

General Availability

Vercel Integration

Feature of: Okta CIC, powered by Auth0 / Available in: Okta CIC, powered by Auth0

Securely integrate Auth0 into Vercel-powered application with just a few clicks, empower developers to deploy their app in seconds while maintaining a secure and convenient login experience



Vercel + Auth0 Integration



Developer Resources

Customer Identity Cloud

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

Customer Identity Cloud

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](#)



Resources

Connect with the Okta Team and learn more



Release Website

View [here](#)
Contact sales [here](#)



CIC Product Roadmap Webinar

Sign up [here](#)



Developer Release PDF

View [here](#)



Changelog

Read [here](#)



okta