Product Release Overview

for Early Access & General Availability in Q1 (January - March 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, long-term financial plans, product development, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as “expect,” “anticipate,” “should,” “believe,” “hope,” “target,” “project,” “goals,” “estimate,” “potential,” “predict,” “may,” “will,” “might,” “could,” “intend,” “shall” and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may be unable to retain key personnel; global economic conditions could worsen; a prior or future network, data or cybersecurity incident that has allowed or does allow unauthorized access to our network or data or our customers’ data could damage our reputation, cause us to incur significant costs or impact the timing or our ability to land new customers or retain existing customers; we could experience interruptions or performance problems associated with our technology, including a service outage; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

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

Welcome to the Okta Workforce & Customer Identity Cloud Release Overview

Q1 2024

Welcome back to Okta's Quarterly Release Overview. We're off to a fast and exciting start to 2024, and we cannot wait to share with you all the innovation we've released in the first quarter.

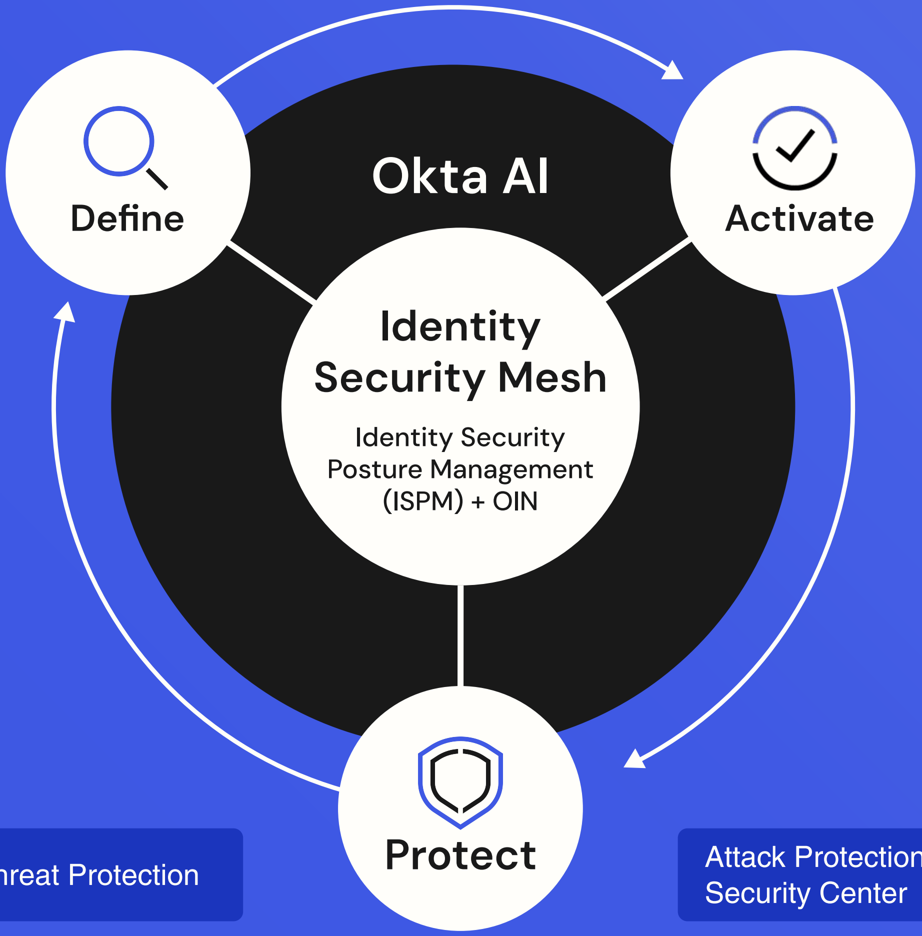
Learn how we're raising the bar on security with features such as Fine Grained Authorization (FGA), as well as Directory Sync with Inbound SCIM for the Customer Identity Cloud. For Workforce Identity you can now allow-list network zones for API tokens, use FastPass phishing resistance for Windows Virtual Desktop Infrastructure (VDI) environments, and ensure least privileged access with new features in Okta Privileged Access.

Okta’s Identity Security Framework

Comprehensive approach to enforce the security posture before, during and after authentication

Identity Governance
Identity Security Posture Management

Strong Password Policies
Breached Password Detection



Okta AI

Define

Activate

Protect

Identity Security Mesh

Identity Security Posture Management (ISPM) + OIN

Single Sign On
MFA
Privileged Access Management

Bot Detection
Adaptive MFA
Passkeys
Actions

Identity Threat Protection

Attack Protection
Security Center

Navigating the overview

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

okta Workforce Identity Cloud

Slide 6

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

okta Customer Identity Cloud

powered by Auth0

Slide 25

- Okta Customer Identity Cloud overview
- Customer Identity Cloud spotlights
- Feature 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 new capabilities double-down on our investments to protect our customers' most sensitive users and resources, helping them discover risky accounts, adhere to principles of least privilege access, and manage security from a single control plane.

Spotlights

- Custom Labels for Servers
- Entitlement Management

All features

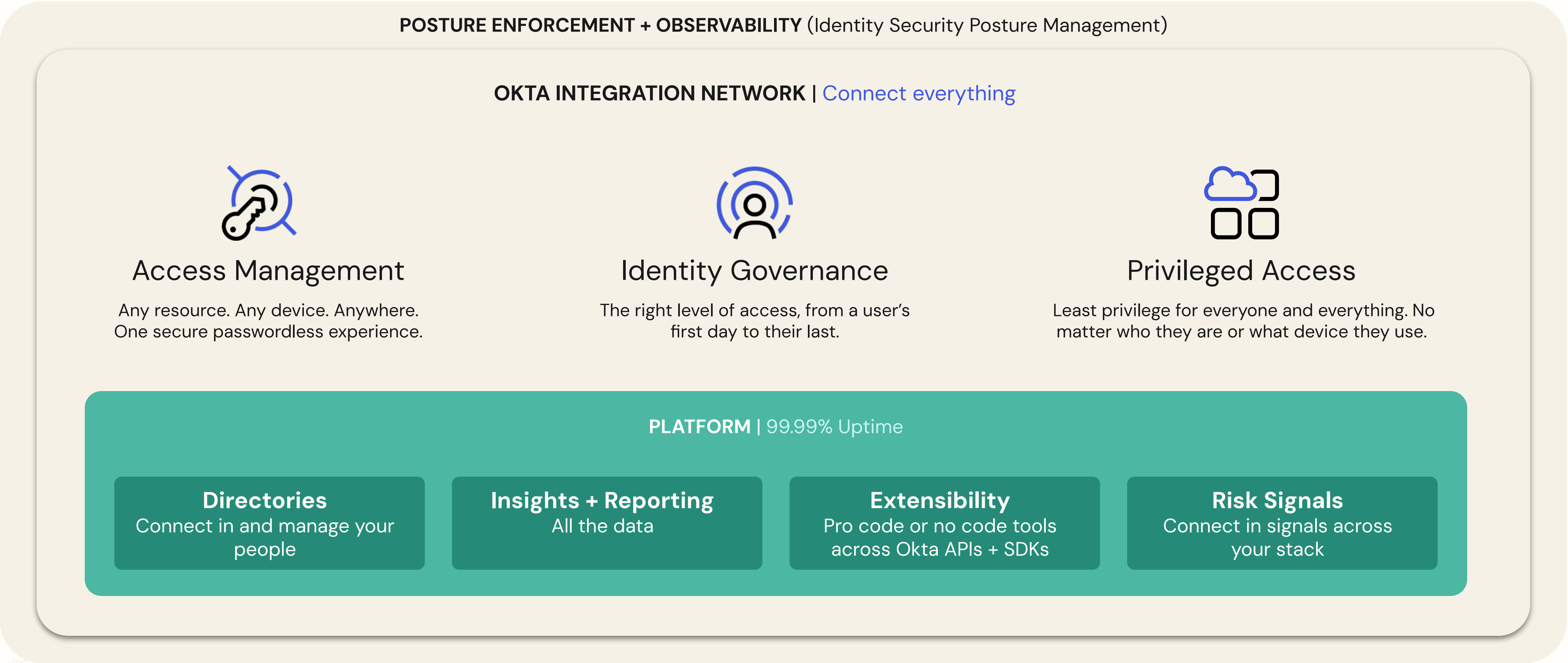
- Access Management
- Identity Governance
- Platform Services
- Privileged Access
- Okta Personal

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 everyone and everything. No matter who they are or what device they use.

PLATFORM | 99.99% Uptime

Directories
Connect in and manage 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

Workforce Identity Cloud

Q1 Release Spotlights

Okta Privileged Access

Custom Labels for Servers

Customers can categorize individual and group servers and create policies for each label.

Okta Identity Governance

Entitlement Management

Automate fine-grained lifecycle management for your organization and limit standing privileges.

Privileged Access
General Availability

Spotlight: Custom Labels for Servers

Discover the newest capability for Okta Privileged Access

Available in: Okta Privileged Access

What is it?

Labels can be set on individual servers which can be used in a Security Policy.

Customer challenge:
Customers are managing hundreds if not thousands of servers, and need a way to categorize and organize groups of servers.

Benefits:
Customize server access on a granular level based on label values.

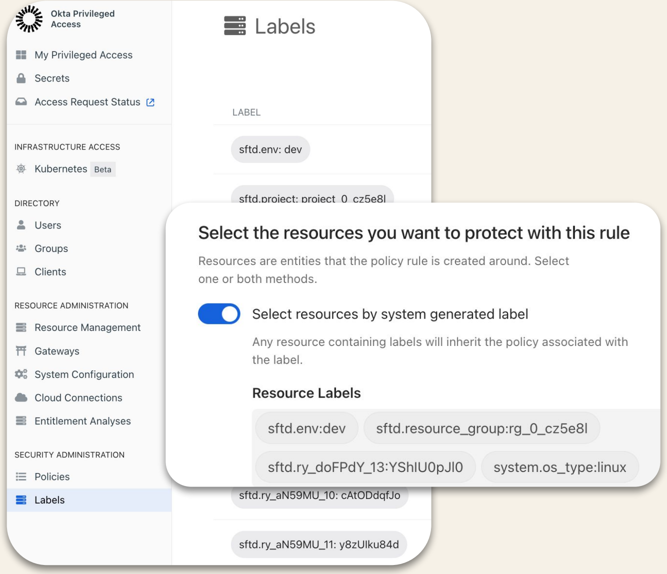
Why this matters

Stronger security: Enforce least privilege access right down to individual servers where necessary.

Flexibility: The Security Policy can leverage system-generated and custom labels to allow for dynamic and granular access control configurations.

How to get it

Okta Privileged Access is Generally Available and connects people, machines, and applications to privileged resources such as servers, containers, and enterprise apps, Just-in-Time (JIT), while supporting compliance.



Labels

LABEL

sftd.env: dev

sftd.project: project_0_cz5e8l

sftd.ry_aN59MU_10: cAtODdqfJo

sftd.ry_aN59MU_11: y8zUlku84d

Select the resources you want to protect with this rule

Resources are entities that the policy rule is created around. Select one or both methods.

● Select resources by system generated label

Any resource containing labels will inherit the policy associated with the label.

Resource Labels

sftd.env:dev sftd.resource_group:rg_0_cz5e8l sftd.ry_doFPdY_13:YShIU0pJI0 system.os_type:linux

Spotlight: Entitlement Management

Discover and manage fine grained entitlements with Workforce Identity Cloud

Available in: Okta Identity Governance

What is it?

Discover, create, and manage entitlements for apps in Okta.

Customer challenge:

Organizations struggle to maintain least privilege across users and a broad set of resources, often resulting in siloed Identity management, manual processes, and non-compliant access controls.

Benefits:

Drive better security outcomes by limiting standing privileges across your workforce. Automate fine grained lifecycle management across your organization, and simplify compliant-by-design processes.

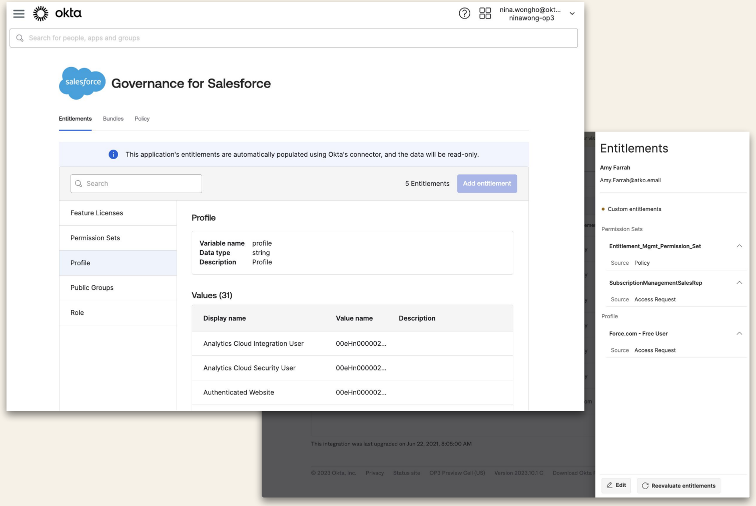
Why this matters

- According to Okta's Businesses at Work Report 2024, the average Okta customer uses 93 different applications.
- Driving a least privileged access approach for each of these applications becomes even more complex when teams have to take into account each application's unique set of entitlements, roles, and licenses.
- Without a proper governance solution in place, over-permissioning and a reduced security posture become real consequences.
- Centralizing on a single source of truth removes Identity silos and reduces the manual workload required to reduce risk and better secure your workforce, and helps close potential security and compliance gaps.

How to get it

Entitlement Management is a new feature within the Okta Identity Governance (OIG) product. It is Generally Available today.

Read our Entitlement Management announcement and learn more about OIG.



Governance for Salesforce

This application's entitlements are automatically populated using Okta's connector, and the data will be read-only.

5 Entitlements

Profile

Variable name profile
Data type string
Description Profile

Values (31)

Display name	Value name	Description
Analytics Cloud Integration User	00eHn000002...	
Analytics Cloud Security User	00eHn000002...	
Authenticated Website	00eHn000002...	

This integration was last upgraded on Jun 22, 2021, 8:05:00 AM

Entitlements

Amy Farrah
Amy.Farrah@atko.email

● Custom entitlements

Permission Sets

Entitlement_Mgmt_Permission_Set
Source Policy

SubscriptionManagementSalesRep
Source Access Request

Profile

Force.com - Free User
Source Access Request

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 Q1 2024.

Easily identify the platform each release is available in:

Okta Identity Engine	25
Both	14
Classic	15

Access Management

General Availability

App Sign On Policy Security Improvements: Granular Authentication Methods

OIE

Available in: Any SKU in OIE

Customers can now choose more granular, specific factor combinations, such as FastPass and Yubikey, to satisfy security requirements

Content Security Policy for Custom Domains

Classic OIE

Available in: All SKUs

Customers can now protect their customized sign-in and error pages on Okta tenants with a custom domain.

Custom Languages for Email Template Customizations

OIE

Available in: Any SKU in OIE

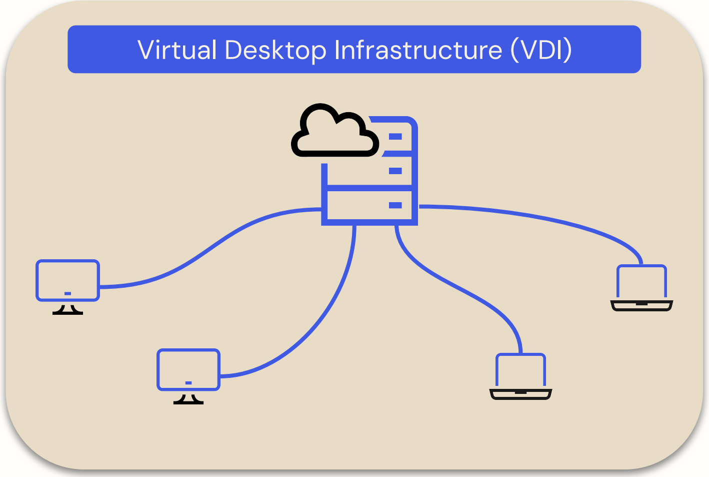
Customize Okta-generated emails in any languages to reduce sign-on friction for multilingual user populations.

FastPass for Windows Virtual Desktop Infrastructure (VDI)

OIE

Available in: SSO, ASSO, MFA, or AMFA

Extend the secure authentication flows and adaptive policy checks of Okta Verify and FastPass to your Windows Virtual Desktop Infrastructure (VDI) environments.



FastPass for Windows VDI

Access Management

General Availability

Keep Me Signed In

OIE

Available in: Any SKU in OIE

Improves user experience and security and reduces the number of security prompts when logging into Okta from a trusted device.

Password Prompt Order

OIE

Available in: Any SKU in OIE

Enforce possession factors as a prerequisite before a knowledge factor (e.g. password) is prompted for authentication, to mitigate the risk of password spraying or brute force attacks.

Phishing Resistant Enrollment Enhancements

OIE

Available in: SSO, ASSO, MFA, or AMFA

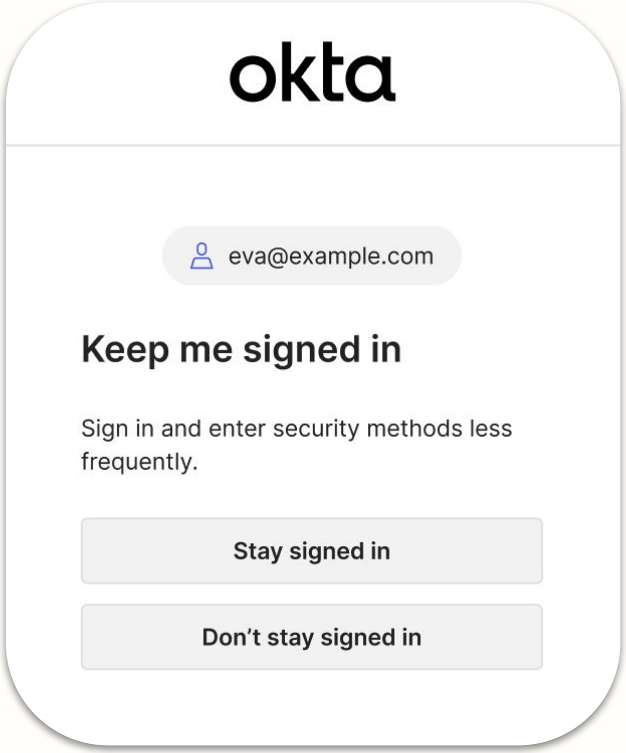
Enforce the use of higher security methods by end users for Okta Verify enrollment by removing enrollment channels like SMS, email, and QR code.

Smart Card AltSecID

OIE

Available in: MFA, AMFA

Allows federal employees across departments to use a single smart card to access shared resources.



okta

eva@example.com

Keep me signed in

Sign in and enter security methods less frequently.

Keep Me Signed In

Access Management

Early Access

Customer Rotation of Signing Keys

Classic OIE

Available in: All SKUs

Notify customers about SAML applications that are using expired and soon to be expiring certificates so they can proactively rotate the certificates. This increases the security posture of applications by constantly rotating signing certificates and the proactive notifications minimizes application downtime.

Device Assurance Dynamic OS Version Policy Option

OIE

Available in: ASSO, AMFA

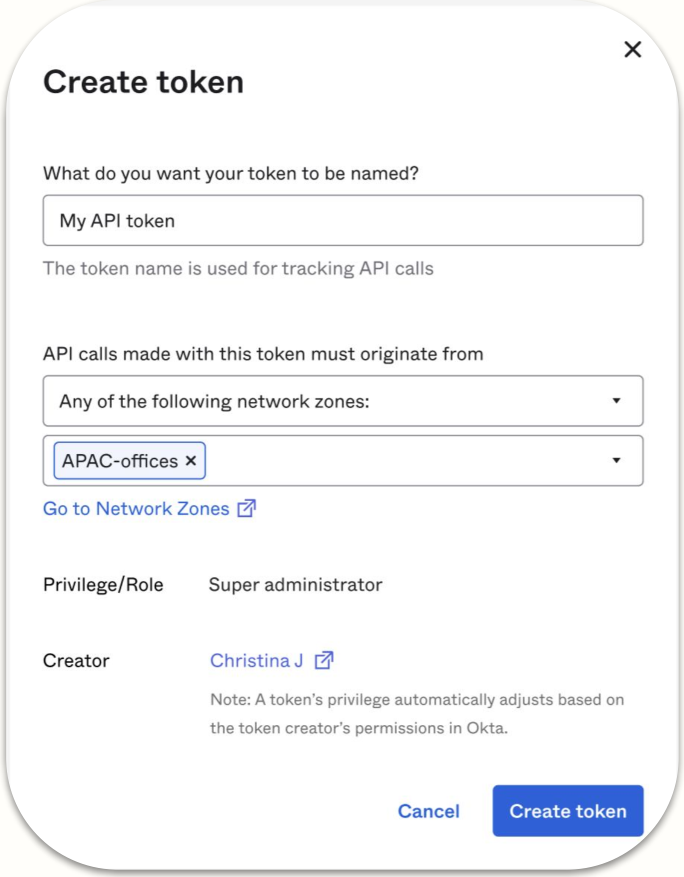
Require devices to have the latest OS updates through a more flexible, low-touch policy configuration that dynamically gates access based on minimum OS versions.

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

Classic OIE

Available in: All SKUs

Okta will enhance the security of Okta API tokens by allowing administrators to specify an allowlisted network zone for each token, thereby controlling which IP addresses or ranges the static (SSWS) API tokens can be used from to call Okta APIs. This will restrict attackers and malware from stealing SSWS tokens and from replaying them outside of the specified IP range in order to gain unauthorized access.



Create token

What do you want your token to be named?

My API token

The token name is used for tracking API calls

API calls made with this token must originate from

Any of the following network zones:

APAC-offices ×

Go to Network Zones

Privilege/Role: Super administrator

Creator: Christina J

Note: A token's privilege automatically adjusts based on the token creator's permissions in Okta.

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

Access Management

Early Access

FastPass User Verification with Passcode

OIE

Available in: MFA or AMFA

Provide end users with the flexibility to complete FastPass user verification with either a PIN, biometrics, or both.

Preventing Account Lockups for all users

Classic OIE

Available in: All SKUs

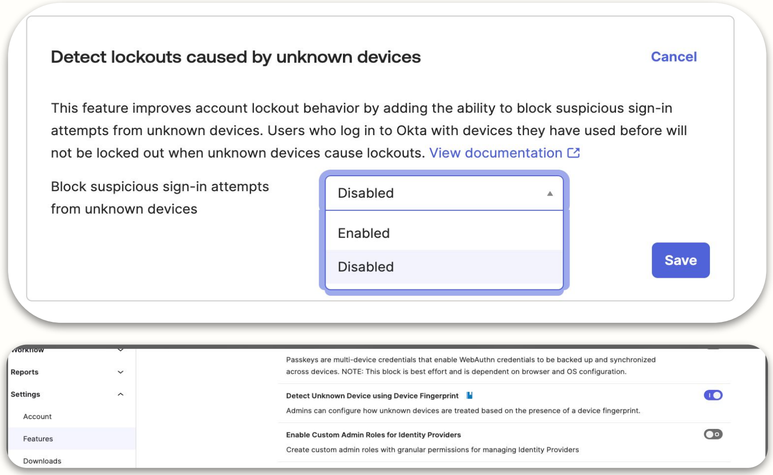
Prevents legitimate users from being locked out if another device that is unknown to Okta causes a lockout. Enables customers to block suspicious sign-in attempts from unknown devices, while users who sign in to Okta with devices that they've used before are not locked out.

Trusted App Filters for FastPass

OIE

Available in: ASSO or AMFA

Minimize the risk of malware and unauthorized local access with FastPass – the safest way to authenticate – by taking policies to the next level, requiring that only trusted apps may invoke FastPass.



Detect lockouts caused by unknown devices

This feature improves account lockout behavior by adding the ability to block suspicious sign-in attempts from unknown devices. Users who log in to Okta with devices they have used before will not be locked out when unknown devices cause lockouts. View documentation

Block suspicious sign-in attempts from unknown devices: Disabled

Passkeys are multi-device credentials that enable WebAuthn credentials to be backed up and synchronized across devices. NOTE: This block is best effort and is dependent on browser and OS configuration.

Detect Unknown Device using Device Fingerprint

Admins can configure how unknown devices are treated based on the presence of a device fingerprint.

Enable Custom Admin Roles for Identity Providers

Create custom admin roles with granular permissions for managing Identity Providers

Preventing User Account Lockouts

Identity Governance

General Availability

Custom Permissions for Directory Integrations

Classic OIE

Feature of: Universal Directory / Available in: SSO

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.

Import Enhancements for OIN Applications

Classic OIE

Feature of: Universal Directory / Available in: Lifecycle Management and Okta Identity Governance

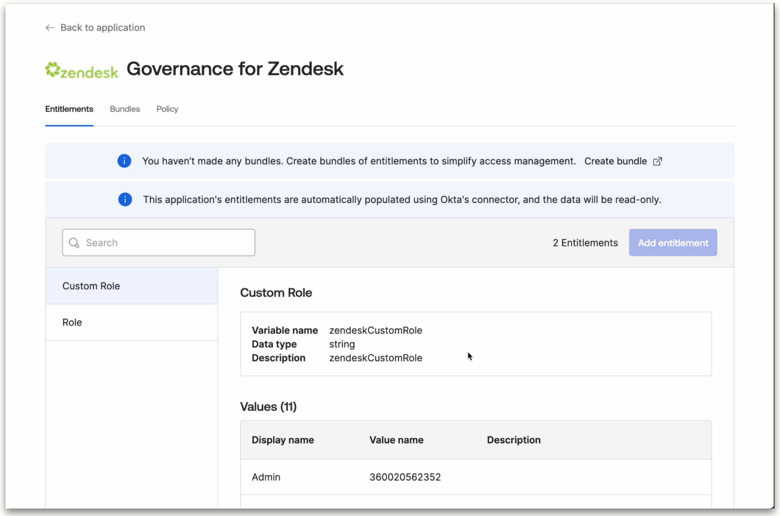
We have invested in Sync Delta service, a new import performance feature that makes imports faster by filtering out unchanged users during imports and only processing changed (new, updated, or deleted) user data resulting in 90% more efficient import processing and faster import times for customers.

OIN Apps for Entitlement Management – PagerDuty, Zendesk

Classic OIE

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 2 Okta Integration Network (OIN) apps: PagerDuty and Zendesk.



Governance for Zendesk

You haven't made any bundles. Create bundles of entitlements to simplify access management. Create bundle

This application's entitlements are automatically populated using Okta's connector, and the data will be read-only.

Custom Role

Variable name zendeskCustomRole
Data type string
Description zendeskCustomRole

Values (11)

Display name	Value name	Description
Admin	360020562352	

Zendesk Connector for Entitlement Management

Identity Governance

General Availability

Support for System Roles in Google as Entitlements

Classic OIE

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

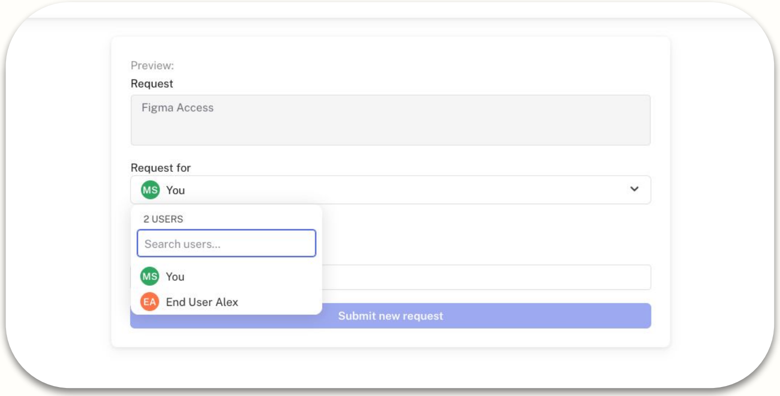
Discover, import, store, and manage System Roles in Google within Okta.

Request on Behalf of

Classic OIE

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

Submit requests on behalf of other individuals in Access Requests (e.g. manager requesting access for their direct reports)



Preview:

Request: Figma Access

Request for: MS You

Request on Behalf of Another User

Identity Governance

Early Access

Realms

Classic OIE

Feature of: Universal Directory / Available in: Okta Identity Governance, Universal Directory (need both SKUs)

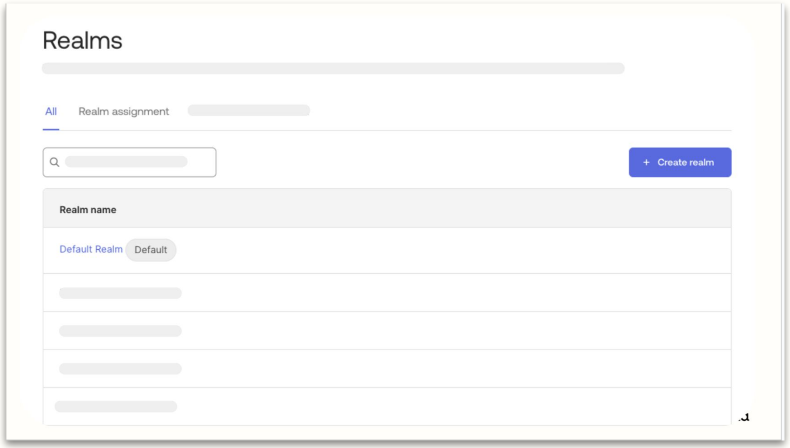
Enable management of complex organizations in a scalable, secure and user-friendly manner, while continuing to maintain a principle of least privilege within a single org.

Sequences & Sequence Editor

Classic OIE

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

Scale the orchestration of access request sequences for admins, re-using sequence frameworks for similar resources.



Realm name
Default Realm Default

Realms

Platform Services

General Availability

Application API Coverage for Top 25 OIN Apps

Classic OIE

Available in: All SKUs

New application metadata contracts have been added to the Okta Core API. Operators, and developers can easily create instances in our popular OIN apps programmatically in their ecosystem.

Enhanced Disaster Recovery

Classic OIE

Available in: Enhanced Disaster Recovery

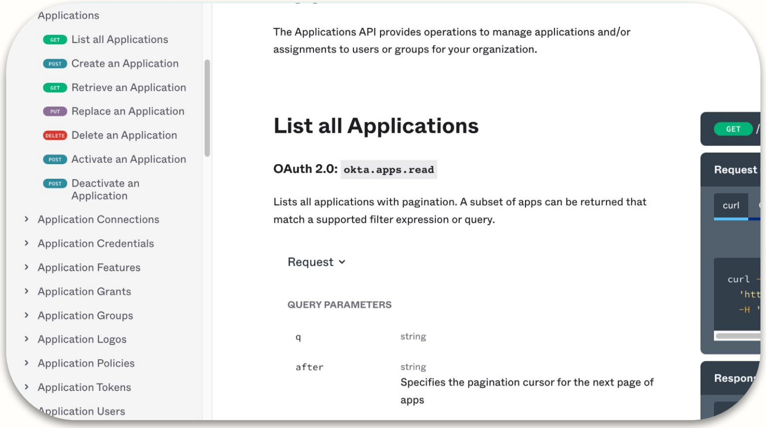
Enhanced Disaster Recovery allows for customer based failover (at the individual org level) as well as reduced Recovery Time (read-only), from up to 1 hour (with standard DR) to a guaranteed 5 minutes in the event of a regional outage with our cloud providers.

OAuth Scope Customization

Classic OIE

Feature of: Workflows / Available in: All Workflows SKUs

When OAuth Scope Customization is enabled for a connector, users gain the flexibility to create connections tailored to their specific needs. They can limit flows to only essential actions required in a third-party application, minimizing the risk associated with overly permissive connections.



The Applications API provides operations to manage applications and/or assignments to users or groups for your organization.

List all Applications

OAuth 2.0: `okta.apps.read`

Lists all applications with pagination. A subset of apps can be returned that match a supported filter expression or query.

Request

QUERY PARAMETERS

q	string
after	string Specifies the pagination cursor for the next page of apps

```
curl -
  'htt
  -H '
```

Application API Coverage for Top 25 OIN Apps

Platform Services

Early Access

Govern Okta Admin Roles

Classic OIE

Available in: All SKUs in Okta Identity Governance

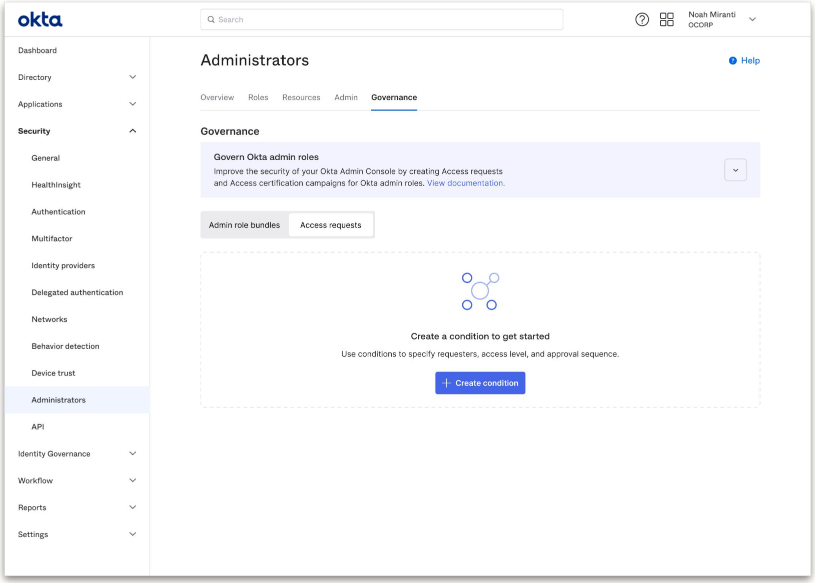
Deliver zero standing privileges for your most critical identity infrastructure — your Okta administrator privileges. Create time-bound, ad-hoc access requests for individual access and review ongoing access for existing administrators.

Granular Directories Permission for Custom Admins

Classic OIE

Feature of: Universal Directory / Available in: Universal Directory

Assign permissions to view and manage directories as part of a custom admin role, allowing admins to handle directory-specific tasks, without requiring universal application administrator permissions.



Administrators

Governance

Govern Okta admin roles

Improve the security of your Okta Admin Console by creating Access requests and Access certification campaigns for Okta admin roles. View documentation.

Create a condition to get started

Use conditions to specify requesters, access level, and approval sequence.

Govern Okta Admin Roles

Privileged Access

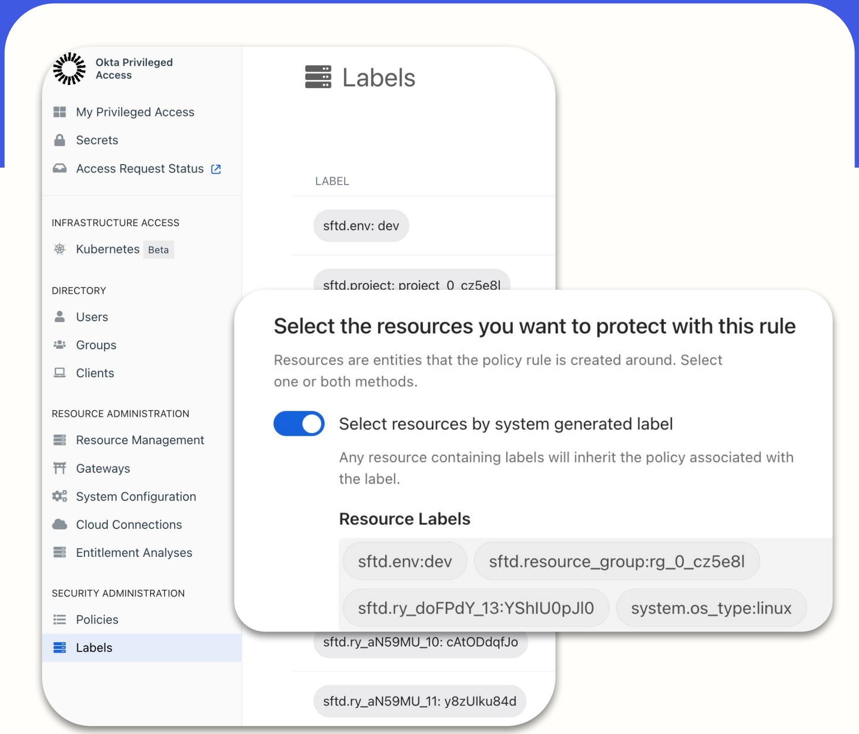
General Availability

Custom Labels for Servers

Classic OIE

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

Assign custom labels for servers and then use the Privileged Access Management (PAM) security policy to assign granular server access based on label values.



Labels

LABEL
sftd.env: dev
sftd.project: project_0_cz5e8l
sftd.ry_aN59MU_10: cAtODdqfJo
sftd.ry_aN59MU_11: y8zUlku84d

Select the resources you want to protect with this rule

Resources are entities that the policy rule is created around. Select one or both methods.

● Select resources by system generated label

Any resource containing labels will inherit the policy associated with the label.

Resource Labels

sftd.env:dev sftd.resource_group:rg_0_cz5e8l sftd.ry_doFPdY_13:YShIU0pJl0 system.os_type:linux

Custom Labels for Servers

Okta Personal

Early Access

Okta Personal Android app

Feature of: Okta Personal (consumer product) / Available for everyone

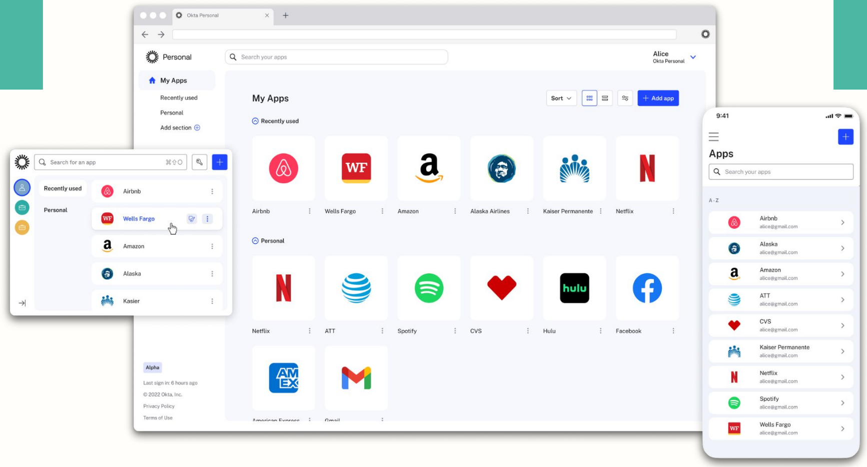
The Android app for Okta Personal is now available in the Google Play Store. Consumers are prompted to download the mobile app (iOS or Android) to set up and sign in to their secure password vault.

Okta Personal for Workforce

Classic OIE

Feature of: Okta Personal (consumer product) / Available in: Workforce Core SKU

Okta Personal for Workforce is a set of features that integrates Okta Personal (consumer password manager) to the Workforce Identity Cloud. Features for end users include account switcher and personal app migration (if the Okta org allows for these features). Features for admins include the ability to block additional domains during the personal app migration process.



Okta Personal for Workforce

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

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 new capabilities center on bolstering security measures, enhancing user experience, and streamlining developer workflows so you can continue to deliver seamless and trustworthy digital interactions for business customers and consumers.

Spotlights

- Fine Grained Authorization (FGA)
- Directory Sync with Inbound SCIM

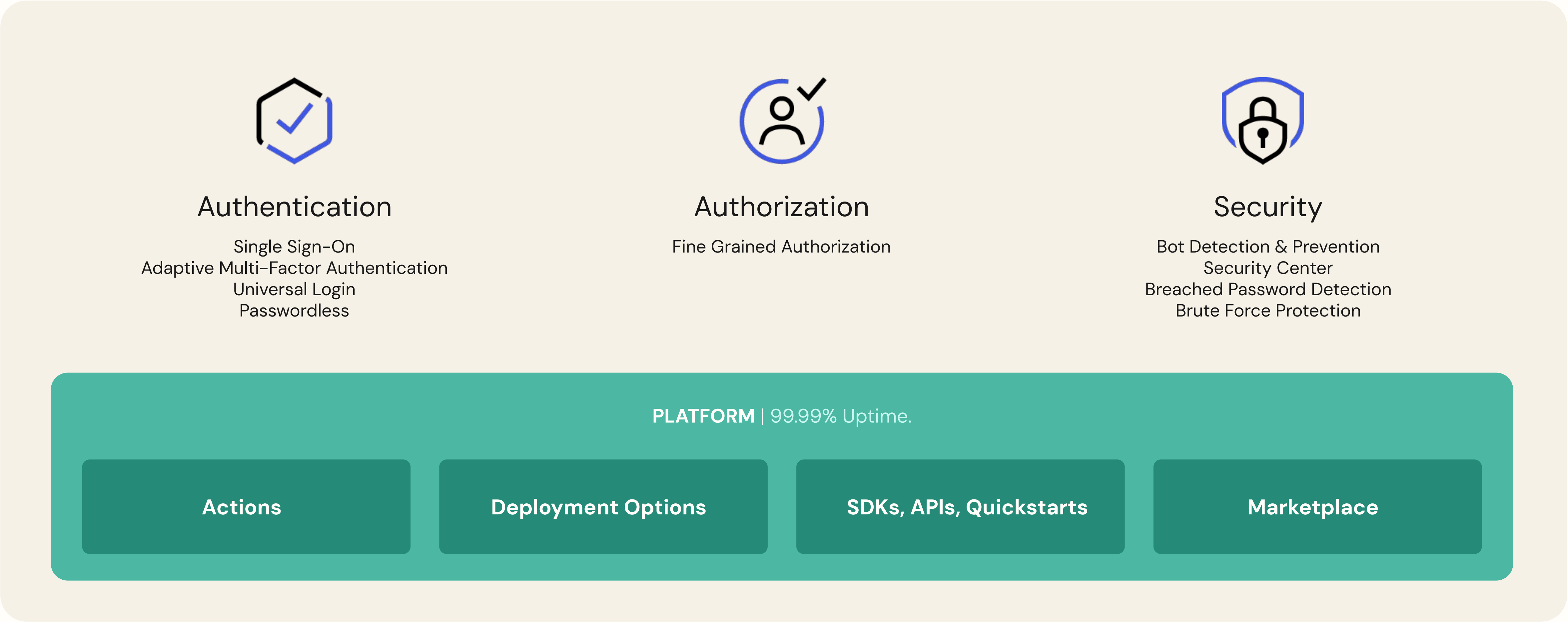
All features

- 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

Authorization
General Availability

Spotlight: Fine Grained Authorization (FGA)

A new, generally available authorization-as-a-service offering from Okta.

Available in: Fine Grained Authorization

What is it?

Authorization-as-a-service that empowers developers with centralized and flexible authorization that provides greater scalability, availability, and auditability than traditional access control methods like RBAC, ABAC, or PBAC.

Customer challenge:

- Ensuring the right users have the right level of access.
- Visibility into who has access to what is crucial for meeting security and compliance goals.
- Increased expectations for user collaboration features like sharing and editing, but building these features into apps is time-consuming.

Benefits:

- Centralized authorization logic for increased visibility to simplify audit and compliance.
- Enable collaboration features for users in your applications in less time.
- Customize your authorization models as business evolves with support for multi-tenancy, roles, groups, and granular access control.

How it works

- **Coarse-grained, fine-grained, or anything in between.** Make access control more granular as your product grows.
- **Seamlessly manage authorization for all your systems.** Easily manage permissions to specific resources for groups, teams, organizations, or any set of users.
- **Authorization at scale, without the complexity.** Manage 100 billion relationships and over 1 million requests per second, with low latency.
- **Centralized authorization logic to simplify auditing and compliance.** Make it easier to achieve security and compliance goals with elevated visibility of authorization logic and authorization audit logs.

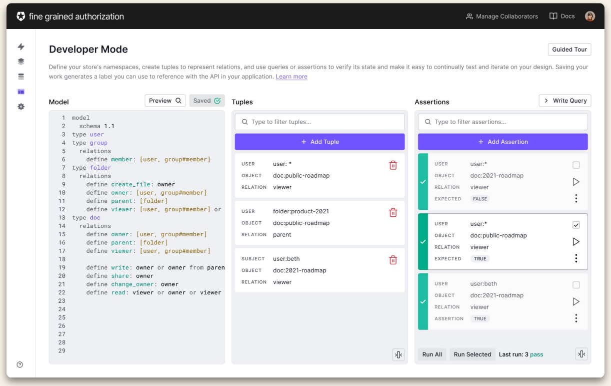
How to get it

FGA is a standalone SKU that is independent of the Workforce Identity Cloud (WIC), Customer Identity Cloud (CIC), and Customer Identity Solution (CIS).

Available for new customers and existing CIS/CIC/WIC customers.

Available in the US, EU, and Australia. Public Cloud only. Private Cloud coming soon.

Get started for free at fga.dev or contact sales to purchase.



Developer Mode

Define your store's namespaces, create tuples to represent relations, and use queries or assertions to verify its state and make it easy to continually test and iterate on your design. Saving your work generates a label you can use to reference with the API in your application. Learn more

Model

```
model
  schema 1.1
type user
type group
  relations
    define member: [user, group#member]
type folder
  relations
    define create_file: owner
    define owner: [user, group#member]
    define parent: [folder]
    define viewer: [user, group#member] or
type doc
  relations
    define owner: [user, group#member]
    define parent: [folder]
    define viewer: [user, group#member]

    define write: owner or owner from paren
    define share: owner
    define change_owner: owner
    define read: viewer or owner or viewer
```

Tuples

USER user: *
OBJECT doc:public-roadmap
RELATION viewer

USER folder:product-2021
OBJECT doc:public-roadmap
RELATION parent

SUBJECT user:beth
OBJECT doc:2021-roadmap
RELATION viewer

Assertions

□ USER user:*
OBJECT doc:2021-roadmap
RELATION viewer
EXPECTED FALSE

☑ USER user:*
OBJECT doc:public-roadmap
RELATION viewer
EXPECTED TRUE

□ USER user:beth
OBJECT doc:2021-roadmap
RELATION viewer
ASSERTION TRUE

Last run: 3 pass

Authentication – SaaS Apps
Early Access

Spotlight: Directory Sync with Inbound SCIM

Simplify and automate user management, ensuring secure and seamless access to applications at scale.

Available in: SaaS Enterprise, B2B Professional, and B2B Essential SKUs

What is it?

SCIM enables businesses to automate provisioning and de-provisioning, ensuring consistent and up-to-date user identities across applications.

Customer challenge:

- Manual provisioning and de-provisioning of business users for your B2B applications reduces efficiency.
- Customer onboarding delays due to existing provisioning processes.
- Unauthorized user access to applications create security vulnerabilities.

Benefits:

- Become enterprise-ready by enabling automation and security that is often required by large enterprise customers.
- Quickly and easily enable inbound SCIM user provisioning and de-provisioning from your customer’s directories into Customer Identity Cloud.

How it works

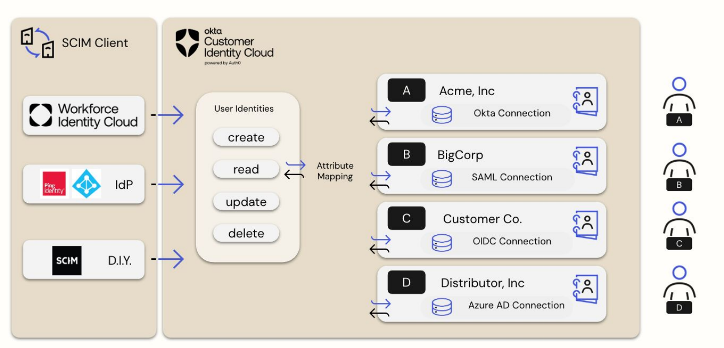
- **Automate user account provisioning and de-provisioning** across multiple systems and applications, ensuring consistent and up-to-date data to improve security posture.
- **Simplify user identity management** enabling seamless scaling of identities across your stack, so your business can grow with confidence.
- **Enable faster and more efficient onboarding** of users to your applications, providing a seamless and secure user experience from the start.

How to get it

Inbound SCIM is part of SaaS Enterprise, B2B Professional, and B2B Essential SKUs.

Available for new and existing CIC customers globally.

Contact Sales to get started.



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 Q1 2024.

Authentication

General Availability

Passkeys

Feature of: Core Platform / Available in: All plans

With passkeys, Auth0 customers can transform their sign-in process, enjoying faster, easier, and more secure access to websites and applications. Passkeys are FIDO credentials that are discoverable by browsers or by security keys for passwordless authentication.

CISCO DUO Authenticator v4 Upgrade

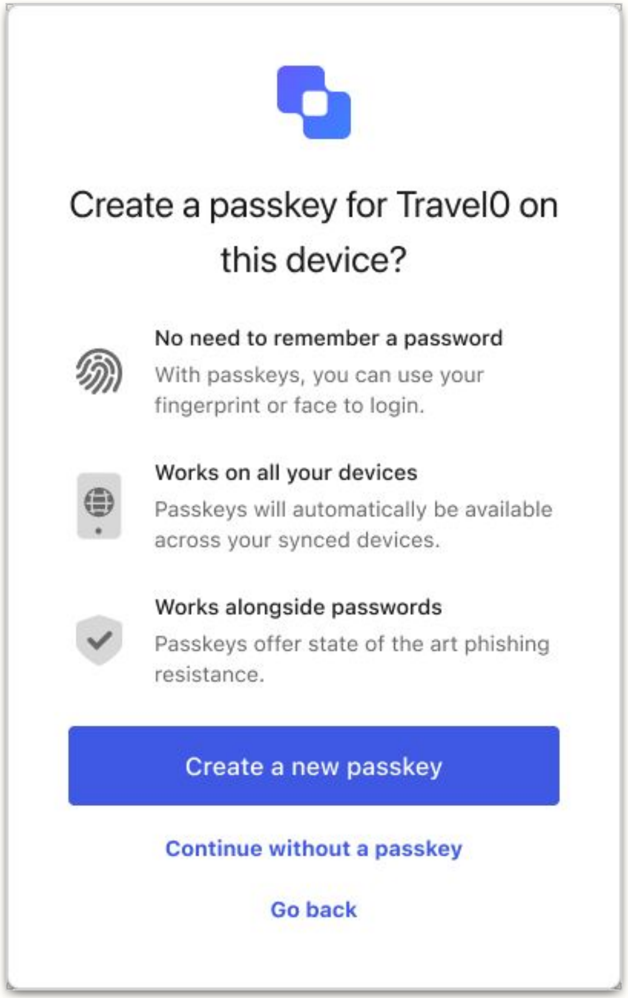
Feature of: Multifactor Authentication (MFA) / Available in: Professional and Enterprise plans

Cisco Duo is a multi-faceted authentication provider and can only be used on your Auth0 tenant if all other factors are disabled. Your Duo account can support push notifications, SMS, OTP, phone callback, and more based on your configuration.

Customizations for Universal Login Signup and Login

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

Pro-code solution to add new fields to the Universal Login signup and login pages for additional data capture.



Create a passkey for Travel0 on this device?

No need to remember a password
With passkeys, you can use your fingerprint or face to login.

Works on all your devices
Passkeys will automatically be available across your synced devices.

Works alongside passwords
Passkeys offer state of the art phishing resistance.

Passkeys

Authentication

General Availability

Guardian App Mobile- Only Enrollment

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

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

Progressive Factor Enrollment

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

Using a post-login Action, businesses can use predetermined logic, contextual signals, and organization policies to define the secondary factors their end-users must enroll with as secondary factors.

Monday, June 6

9:41

Guardian 9:41 AM
Authentication request

Guardian App Mobile-Only Enrollment

Authentication

Early Access

Contextual Strong Customer Authentication

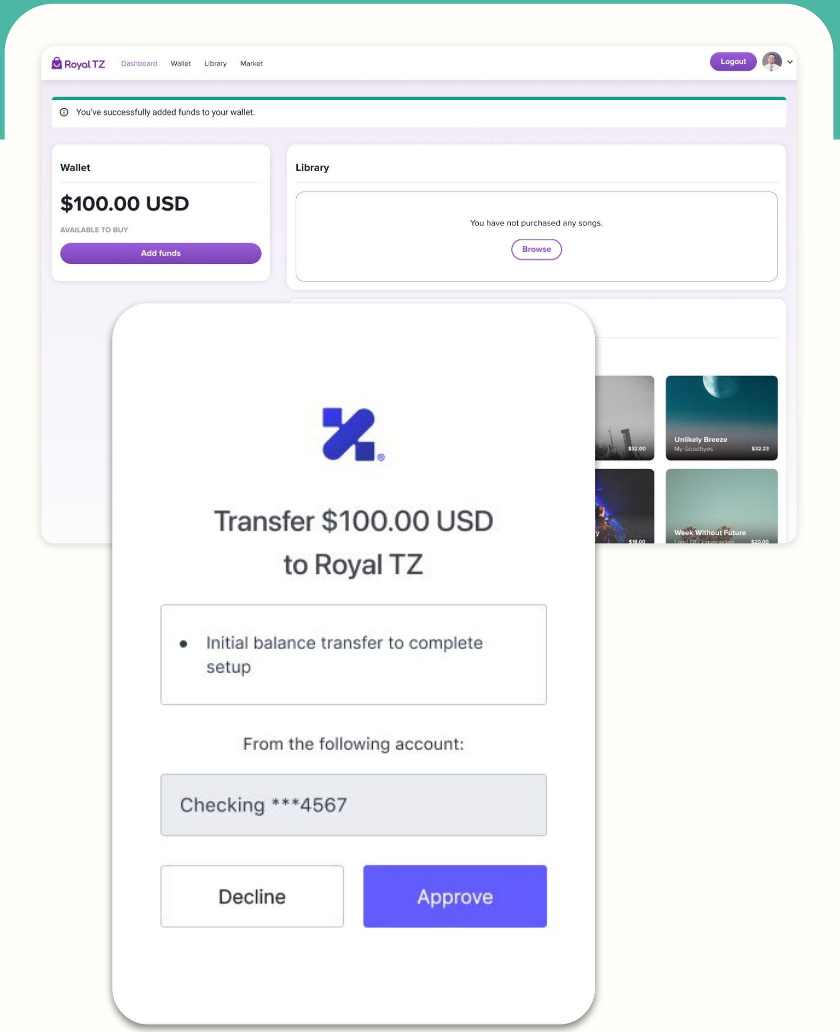
Feature of: Highly Regulated Identity / Available in: Advanced Identity Security or Enterprise Premium Security Solution Bundle

Flexibly step-up authentication for sensitive operations beyond login (e.g. a transaction over x amount), and provide details of the sensitive operation for the user to review at time of approval with dynamic linking.

Highly Regulated Identity

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

Highly Regulated Identity (HRI) is Auth0's Financial-Grade Identity™ solution to secure sensitive data operations and services important for your business.



You've successfully added funds to your wallet.

Wallet

$100.00 USD

AVAILABLE TO BUY

Library

You have not purchased any songs.

Transfer $100.00 USD to Royal TZ

- Initial balance transfer to complete setup

From the following account:

Checking ***4567

Contextual Strong Customer Authentication

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 that helps your tenant leverage the latest user information from the connected IdP.

Support for Organization Name in Authorization Flows

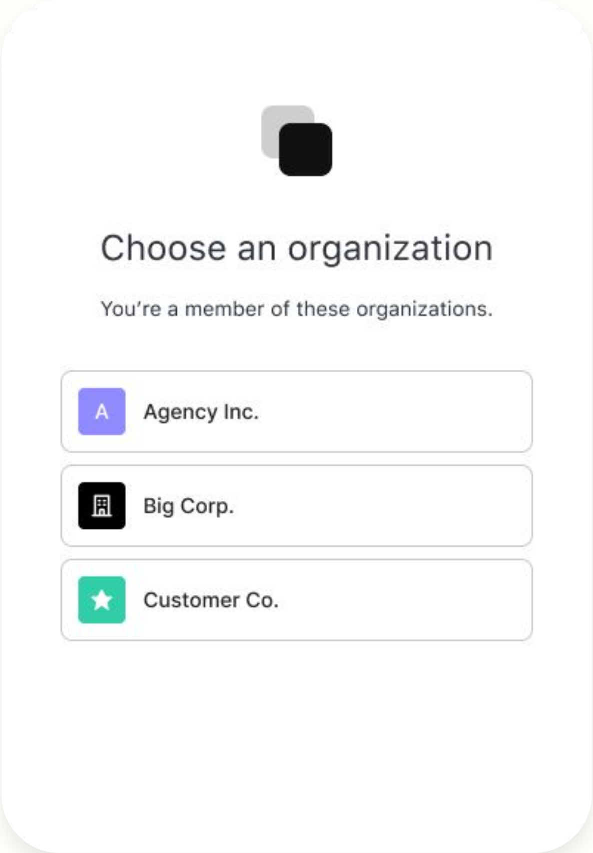
Feature of: Organizations / Available in: All B2B and Enterprise plans

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.



Choose an organization

You're a member of these organizations.

Improved Login Flows for Organizations

Authentication — SaaS Apps

General Availability

“Show as Button” for Organizations associated Enterprise Connections

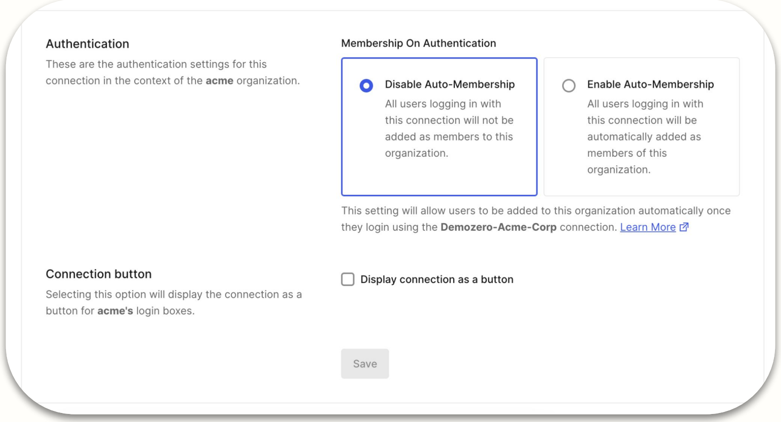
Feature of: Organizations / Available in: All B2B and Enterprise plans

Utilize hidden Enterprise Connections to support multiple customers using a single Organization login.

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.



Authentication

These are the authentication settings for this connection in the context of the **acme** organization.

Membership On Authentication

● Disable Auto-Membership
All users logging in with this connection will not be added as members to this organization.

○ Enable Auto-Membership
All users logging in with this connection will be automatically added as members of this organization.

This setting will allow users to be added to this organization automatically once they login using the **Demozero-Acme-Corp** connection. Learn More

Connection button

Selecting this option will display the connection as a button for **acme's** login boxes.

□ Display connection as a button

“Show As Button” for Organizations

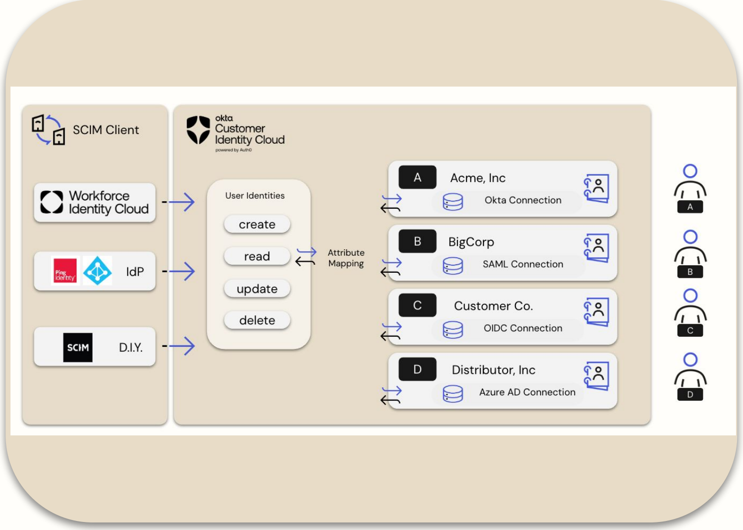
Authentication — SaaS Apps

Early Access

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.



Directory Sync with Inbound SCIM

Authorization

General Availability

Fine Grained Authorization (FGA)

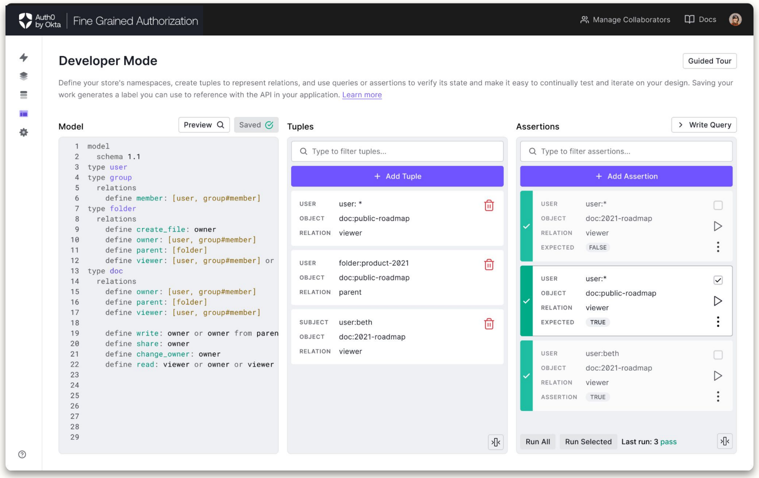
Feature of: Fine Grained Authorization / Available in: Fine Grained Authorization

FGA is Authorization as a Service product that enables developers to implement authorization for their applications in a flexible and performant manner at scale.

Modular Authorization Models

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

To solve authorization for developers, we need to enable organizations with multiple teams to work together defining the authorization model for a product.



Developer Mode

Define your store's namespaces, create tuples to represent relations, and use queries or assertions to verify its state and make it easy to continually test and iterate on your design. Saving your work generates a label you can use to reference with the API in your application. Learn more

Model

```
model
  schema 1.1
type user
type group
  relations
    define member: [user, group#member]
type folder
  relations
    define create_file: owner
    define owner: [user, group#member]
    define parent: [folder]
    define viewer: [user, group#member] or
type doc
  relations
    define owner: [user, group#member]
    define parent: [folder]
    define viewer: [user, group#member]

    define write: owner or owner from paren
    define share: owner
    define change_owner: owner
    define read: viewer or owner or viewer
```

Tuples

Type to filter tuples...

USER user: *
OBJECT doc:public-roadmap
RELATION viewer

USER folder:product-2021
OBJECT doc:public-roadmap
RELATION parent

SUBJECT user:beth
OBJECT doc:2021-roadmap
RELATION viewer

Assertions

Type to filter assertions...

□ USER user:*
OBJECT doc:2021-roadmap
RELATION viewer
EXPECTED FALSE

☑ USER user:*
OBJECT doc:public-roadmap
RELATION viewer
EXPECTED TRUE

□ USER user:beth
OBJECT doc:2021-roadmap
RELATION viewer
ASSERTION TRUE

Last run: 3 pass

Fine Grained Authorization

okta

Security

General Availability

Autonomous System Network Binding to Auth0 Dashboard Administrators Sessions

Feature of: Core Platform / Available in: All plans

The session cookies of both Teams and Auth0 Dashboard dashboard users will now be bound to the originating Autonomous System Network (ASN) as part of the session creation.

Back-Channel Logout & Initiators

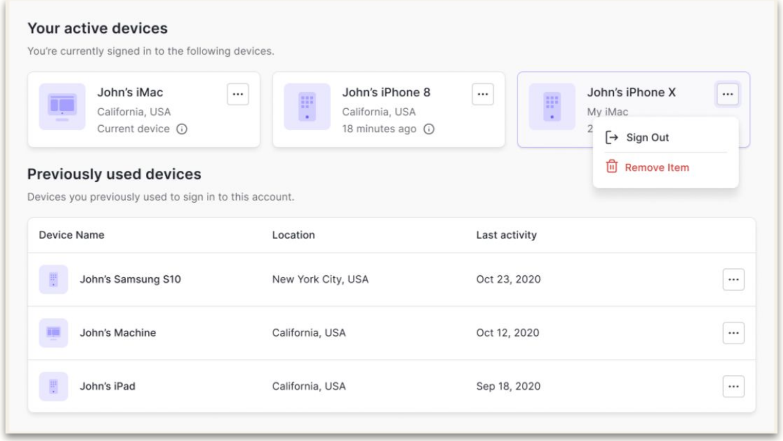
Feature of: Core Platform/ Available in: All Enterprise plans

Provides a standard implementation for single logout across Applications. When configured, Back-Channel Logout is automatically notifying applications of IdP/RP initiated logout events.

Refresh Tokens Management API

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

Session Management API brings fundamental elements of IdP session internals into the Management API so developers can retrieve users' sessions and refresh token information for customer support roles and end-users to self-service session capabilities.



Your active devices

You're currently signed in to the following devices.

John's iMac
California, USA
Current device

John's iPhone 8
California, USA
18 minutes ago

John's iPhone X
My iMac
2

Sign Out

Remove Item

Previously used devices

Devices you previously used to sign in to this account.

Device Name	Location	Last activity
John's Samsung S10	New York City, USA	Oct 23, 2020
John's Machine	California, USA	Oct 12, 2020
John's iPad	California, USA	Sep 18, 2020

Refresh Tokens Management API

Platform

General Availability

Open Source Templates for Actions

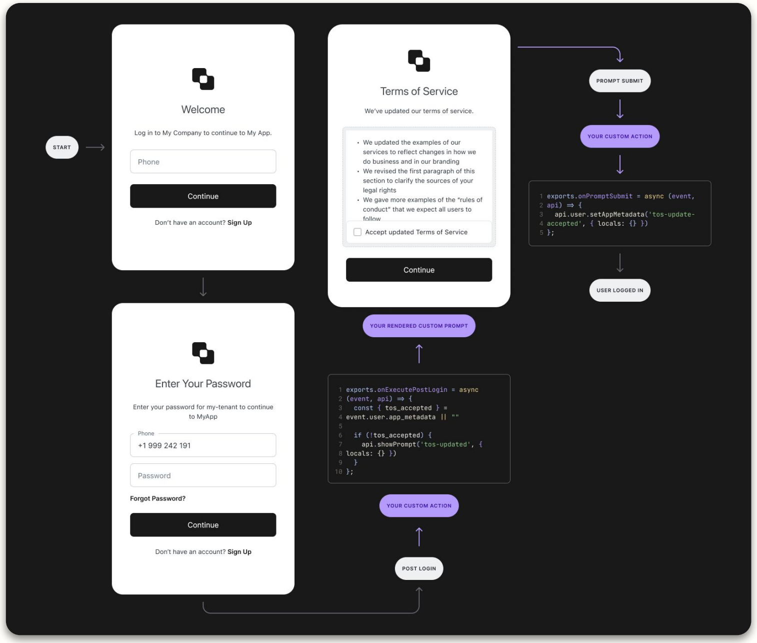
Feature of: Core Platform / Available in: All plans

Allows developers to contribute to the template library.

Sessions Extensibility in Actions

Feature of: Core Platform / Available in: All plans

Access to the event’s session state (expiry, authenticated_at, ip, …) from actions, check users’ sessions and react to session termination events (new session ended trigger).



Log in to My Company to continue to My App.

We’ve updated our terms of service.

- We updated the examples of our services to reflect changes in how we do business and in our branding
- We revised the first paragraph of this section to clarify the sources of your legal rights
- We gave more examples of the “rules of conduct” that we expect all users to follow

□ Accept updated Terms of Service

```
exports.onPromptSubmit = async (event,
api) => {
  api.user.setAppMetadata('tos-update-
accepted', { locals: {} })
};
```

Enter your password for my-tenant to continue to MyApp

Phone: +1 999 242 191

```
exports.onExecutePostLogin = async
(event, api) => {
  const { tos_accepted } =
event.user.app_metadata || ""

  if (!tos_accepted) {
    api.showPrompt('tos-updated', {
locals: {} })
  }
};
```

Progressive Factor Enrollment with Actions

Platform - Developer Experience

General Availability

Auth0 Teams

Feature of: Core platform/ Available in: All plans

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

Audit Logs for Teams

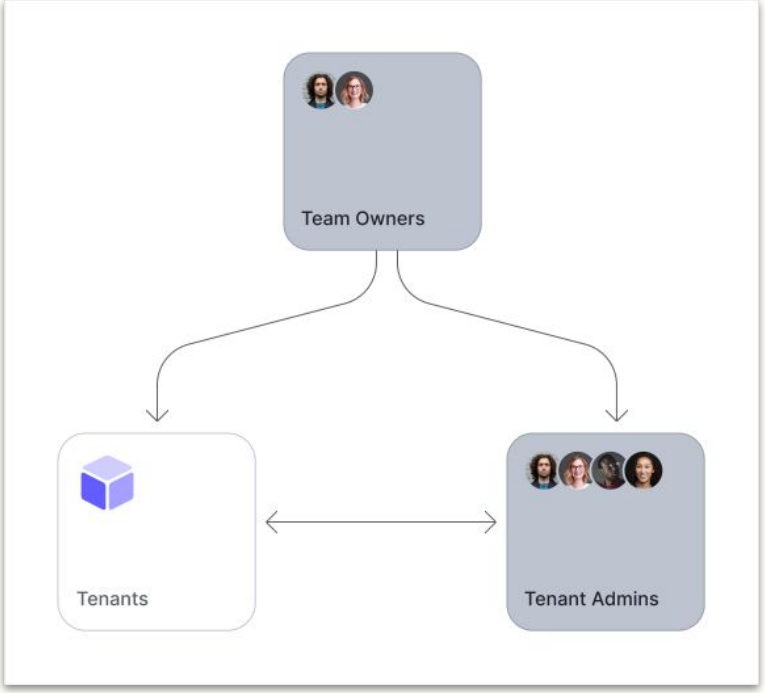
Feature of: Core platform/ Available in: All plans

Allows Team Owners to view and audit logs based on member invite, setting changes, and login and logout events.

MFA for Dashboard Administrators

Feature of: Core platform/ Available in: All plans

MFA now required as mandatory (was optional previously) for dashboard users logging in with username/password or 3rd party social connections when logging into Auth0.



Auth0 Teams

Platform - Developer Experience

General Availability

Tenant Member invite on Auth0 Dashboard

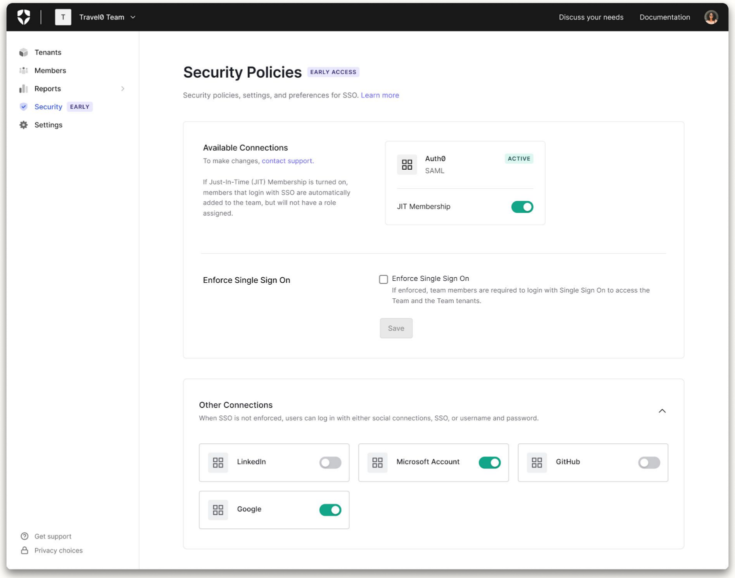
Feature of: Core platform / Available in: All plans

Designed to help you centrally manage your onboarding and off-boarding workflow of tenant dashboard members.

Expanded tiers and add-ons for self service users

Feature of: MFA, Enterprise Connections / Available in: Professional plans

The following will be available via Self Service: Enterprise MFA Lite add-on for Professional Plans, up to 5 Enterprise Connections with B2B Professional, and B2B Professional will return to being available for purchase within Self Service.



Security Policies EARLY ACCESS

Security policies, settings, and preferences for SSO. Learn more

Available Connections

To make changes, contact support.

If Just-In-Time (JIT) Membership is turned on, members that login with SSO are automatically added to the team, but will not have a role assigned.

Auth0 SAML ACTIVE

JIT Membership: on

Enforce Single Sign On

□ Enforce Single Sign On

If enforced, team members are required to login with Single Sign On to access the Team and the Team tenants.

Save

Other Connections

When SSO is not enforced, users can log in with either social connections, SSO, or username and password.

LinkedIn: off
Microsoft Account: on
GitHub: off
Google: on

Tenant Member invite on Auth0 Dashboard

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

Unveiling New and Improved Product Features — 6 Month Lookback blog: Click here

Resources

Connect with the Okta Team and learn more

Release Website

View here

Contact sales here

Code::Identity Webinar

Sign up here

New: Developer Release PDF

View here

Changelog

Read here

okta