Release Overview

for Early Access & General Availability in Q3 (July - September 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.

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

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.

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

Welcome to the Okta Workforce & Customer Identity Cloud Release Overview

Q3 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 Q3.

Learn how the Workforce Identity Cloud is investing to protect our customers with stronger security controls to access privileged resources, devices, protect sensitive actions, and enhanced dynamic network zones. And a customer favorite - Okta Workflows - is post-audit for FedRAMP High with Authorization expected in Q4.

For Customer Identity Cloud, discover Forms and updates around our Free, Professional, and Essential plans.

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

Navigating the overview

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

okta
Workforce
Identity Cloud

Slide 5

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

okta
Customer
Identity Cloud
powered by Auth0

Slide 27

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

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

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 customers strengthen their security posture and governance controls across devices, users, and privileged resources.

Spotlights

Workforce Identity Cloud

- Workflows Post-Audit for FedRAMP High, Authorization expected in Q4

Workforce and Customer Identity Clouds

- Secure Identity Assessment
- Interoperability Profile for Secure Identity in the Enterprise

All releases

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

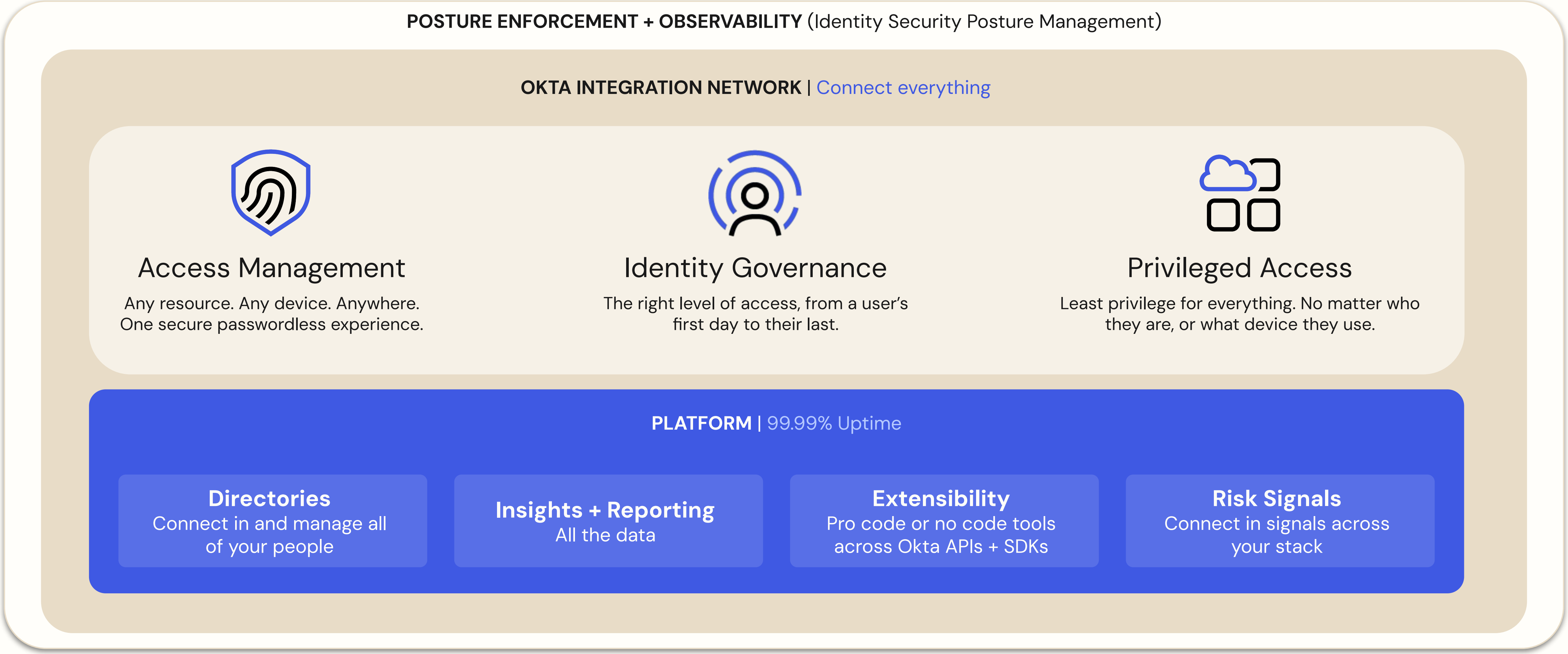
Developer resources

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

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 and/or its affiliates. All rights reserved.

Post-Audit

Spotlight: Workflows is Post-Audit for FedRAMP High

Authorization expected in Q4. Available to FedRAMP High and eligible FedRAMP Moderate 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.

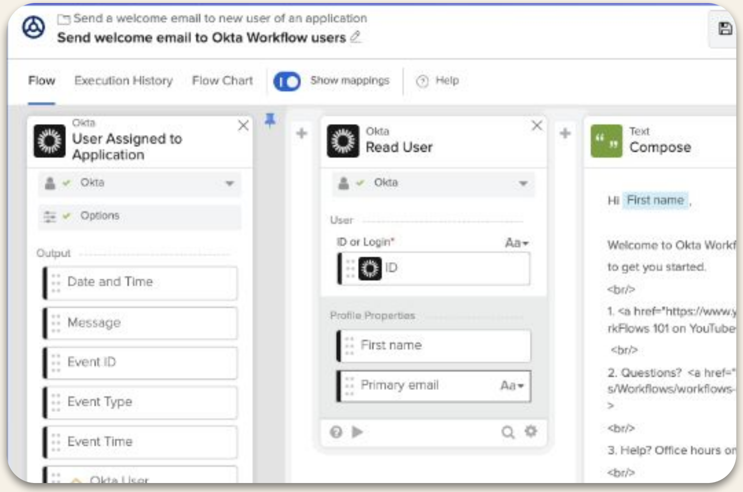
Why this matters

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.



Send a welcome email to new user of an application

Send welcome email to Okta Workflow users

Hi First name ,

Welcome to Okta Workf
to get you started.
<br/>
1. <a href="https://www.y
rkFlows 101 on YouTube
<br/>
2. Questions? <a href="
s/Workflows/workflows-
>
<br/>
3. Help? Office hours on
<br/>

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

Spotlight: Secure Identity Assessment

Professional services offering to help customers mitigate their technical debt.

Available:
Workforce and Customer Identity Clouds

What is it?

Secure Identity Assessment (SIA) is Okta's end-to-end approach to reduce our customers' technical debt. In helping track security maturity progress, providing expert guidance for security best practices, and identifying vulnerabilities like admin sprawl, SIA helps close security gaps and build a stronger security foundation.

Customer Challenge:

Organizations often face tough decisions when prioritizing security resources. Companies will often stretch the value of existing systems instead of modernizing them. This creates technical debt in security, particularly identity debt: orphaned accounts, shadow IT, ghost accounts, and misconfigured identities. These issues cause vulnerabilities, making identity management more difficult over time.

Why this matters

Okta's new professional services offering will help customers remain secure-by-default, with end-to-end expert support during the following phases:

- **Diagnose**: Okta helps customers track progress on their security maturity with tools like the IMM or security checklist, to establish a roadmap to stay secure.
- **Tailor**: Customers receive expert advice with Okta Expert Assist, helping get set up, achieve certifications to implement Okta, and work towards best practices on an ongoing basis.
- **Fix**: Okta can pinpoint security gaps (e.g. orphaned accounts, shadow IT, admin sprawl) and customers can use tools like OIG or FGA to address immediate risks and work towards ongoing adherence.

How to get it

Secure Identity Assessment is an end-to-end offering from Okta's professional services team.

The assessment ties into Okta's Secure Identity Commitment (OSIC), and specifically the pillar around championing best practices.

There are three tiers for the assessment:

- **Premier**: Kick off with an Expert Assist-driven roadmap and in-depth discovery sessions.
- **Advanced**: Engage with Okta's team for partner-assisted discovery and targeted identity debt reduction suggestions.
- **Essential**: Start with the identity checklist and work through partner-led sessions or self-guided remediation with support.

Each offers prescriptive instructor-led training (ILT) alongside certificate pathing.

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

Spotlight: Interoperability Profile for Secure Identity in the Enterprise

Announcement: Workforce and Customer Identity Clouds

What is it?

The Interoperability Profile for Secure Identity in the Enterprise [IPSIE] is an in-progress open industry standard that provides a framework for enterprises to enhance the end-to-end security of their products. It encompasses key aspects of identity security, including centralized authentication (SSO), automated user lifecycle management, privileged access control, security information sharing, and rapid session termination in response to threats, leveraging protocols like OIDC, SCIM, and CAEP/SSF to enable these capabilities across enterprise applications.

Customer Challenge:

Enterprises face fragmented identity security implementations, making it difficult to ensure consistent security and efficient integration across various SaaS applications. This fragmentation leads to increased vulnerability, complex management, and potential gaps in security coverage.

Why this matters

By standardizing identity security, organizations can maintain a uniform level of protection across all their SaaS tools, reducing weak points and simplifying security management.

With clear guidelines, SaaS developers can more easily implement robust security features, while users benefit from a more secure and user-friendly experience across different applications.

Organizations can select the best-fit SaaS solutions without compromising on security, as the standard helps ensure compatibility and consistent security practices across different identity providers.

A standardized approach makes it easier for organizations to meet regulatory requirements and streamlines the process of integrating new SaaS tools into existing security frameworks.

How to get it

Stay informed about Okta's ongoing efforts in developing these open standards:

Follow Okta's communications and participate in webinars or conferences where these standards are discussed and developed.

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

Workforce Identity Cloud Releases

The Workforce Identity Cloud (WIC) is a unified identity security solution that brings together and enables discovery and remediation of identity posture risks, implementation and enforcement of strong authentication and governance policies, and identity threat detection and response across all users, all resources, and all devices.

Learn more about our new WIC capabilities released in Q3 2024.

Easily identify the platform each release is available in:

Classic	Okta Identity Engine (OIE)

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

Workforce Identity Cloud

Access Management

General Availability

Control SAML App Session Duration

Available in: MFA/SSO

Enhance application security by restricting the lifespan of authentication tokens.

Learn more

Classic OIE

Desktop Passwordless Login for Windows

Available in: Okta Device Access

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

Learn more

OIE

Device Assurance Dynamic OS Version Policy Option

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.

Learn more

OIE

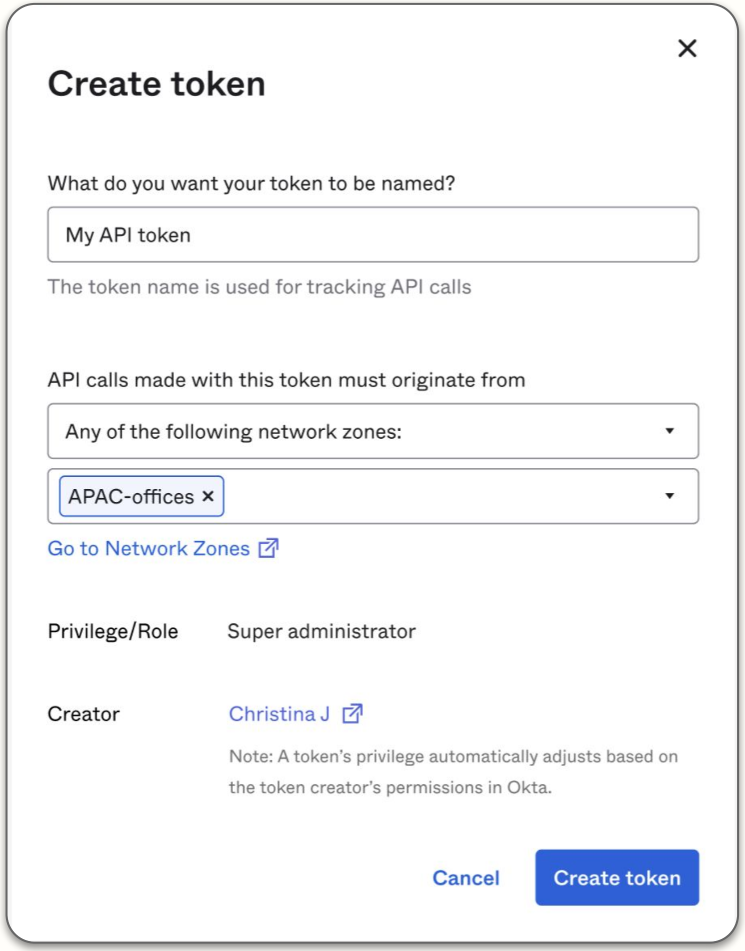
Enforce an Allowlisted Network Zone for Use of Static (SWSS) API Tokens

Available in: All SKUs

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



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

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

Access Management

General Availability

Enhanced Dynamic Network Zones – AMFA SKU functionality

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

Enhance security with granular control within dynamic zones, enabling organizations to block access based on service categories, locations, and ASNs. Achieve greater control over network resources, and stay resilient against unauthorized access and evolving threats. Learn more

Classic

OIE

Enhanced Dynamic Network Zones – Base SKU functionality

Available in: AMFA

Protect first-party assets like the Admin Console, App Dashboard, and User Registration page with a default, non-editable dynamic zone that blocks all anonymizers when you enable this feature.

Learn more

OIE

Identity Threat Protection with Okta AI

Available in: Identity Threat Protection

Continuously detect and configure automated responses to Identity threats, including credential theft and session hijacking, both during and post-authentication by using machine learning, first-party signals from Okta, and third party signals from security event providers in your security stack. Learn more

OIE

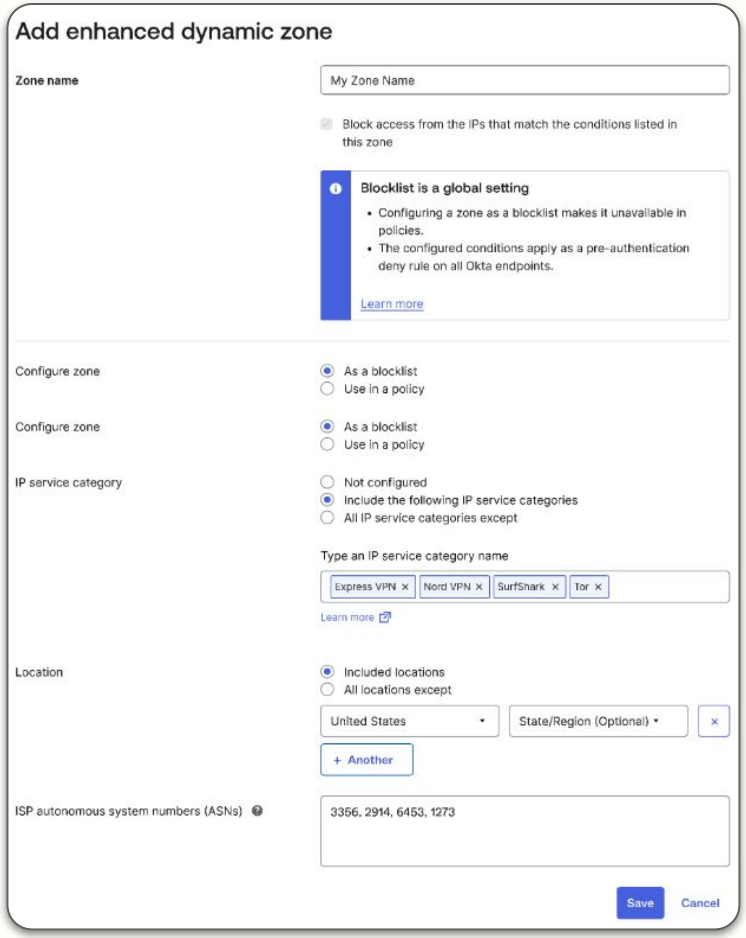
MFA for Protected Actions in the Okta Admin Console

Available in: All SKUs

Limit the risk of malicious access and unauthorized high-impact actions from stolen sessions or compromised devices of users with administrative permissions by enabling a new feature that requires MFA for any Okta admin type looking to execute on a list of protected actions within the Okta Admin Console.

Classic

OIE



Add enhanced dynamic zone

Zone name: My Zone Name

☑ Block access from the IPs that match the conditions listed in this zone

Blocklist is a global setting
- Configuring a zone as a blocklist makes it unavailable in policies.
- The configured conditions apply as a pre-authentication deny rule on all Okta endpoints.

Learn more

Configure zone: ● As a blocklist ○ Use in a policy

Configure zone: ● As a blocklist ○ Use in a policy

IP service category: ○ Not configured ● Include the following IP service categories ○ All IP service categories except

Type an IP service category name: Express VPN × Nord VPN × SurfShark × Tor ×

Learn more

Location: ● Included locations ○ All locations except

United States · State/Region (Optional) · ×

+ Another

ISP autonomous system numbers (ASNs): 3356, 2914, 6453, 1273

Save Cancel

Enhanced Dynamic Network Zone

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

okta

Access Management

General Availability

MFA to the Okta Admin Console

Available in: All SKUs

Protect access to Okta by privileged administrator accounts and reduce the risk of unauthorized access by enforcing MFA to the Okta Admin Console.

Learn more

Classic

OIE

Okta Verify Troubleshooter

Available in: All SKUs

Empower users to troubleshoot push notification and FastPass issues within the mobile Okta Verify app.

Learn more

Classic

OIE

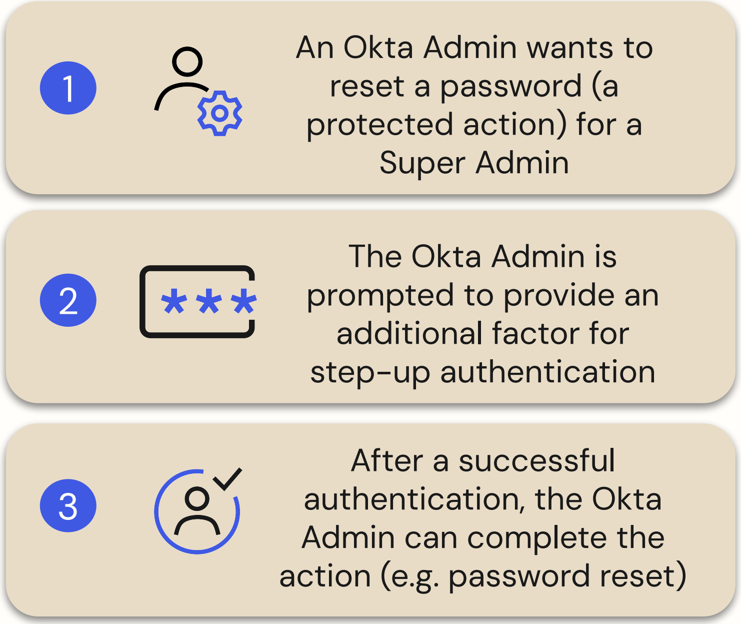
Trusted App Filters for FastPass

Available in: AMFA/ASSO

Enhance security against malicious or unauthorized software by configuring app sign-in policies to require that only trusted apps may invoke FastPass.

Learn more

OIE



1 An Okta Admin wants to reset a password (a protected action) for a Super Admin

2 The Okta Admin is prompted to provide an additional factor for step-up authentication

3 After a successful authentication, the Okta Admin can complete the action (e.g. password reset)

MFA for Protected Actions in the Okta Admin Console

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

Workforce Identity Cloud

Access Management

Early Access

Authenticator Sequencing

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

Bolster application security and mitigate the risk of account compromise by specifying the sequence of authenticator methods a user must complete before accessing an app. Learn more

OIE

Authenticator Enrollment + Recovery with ASoP

Available in: All SKUs

Enhance protection against social engineering attacks with granular control over enrollment and recovery auth flows. Learn more

OIE

Desktop MFA Recovery for macOS

Available in: Okta Device Access

Decrease productivity disruption by securely enabling admins to provide end users with time-limited recovery codes to login to their devices in the event of a lost phone, security key, etc.

Learn more

OIE

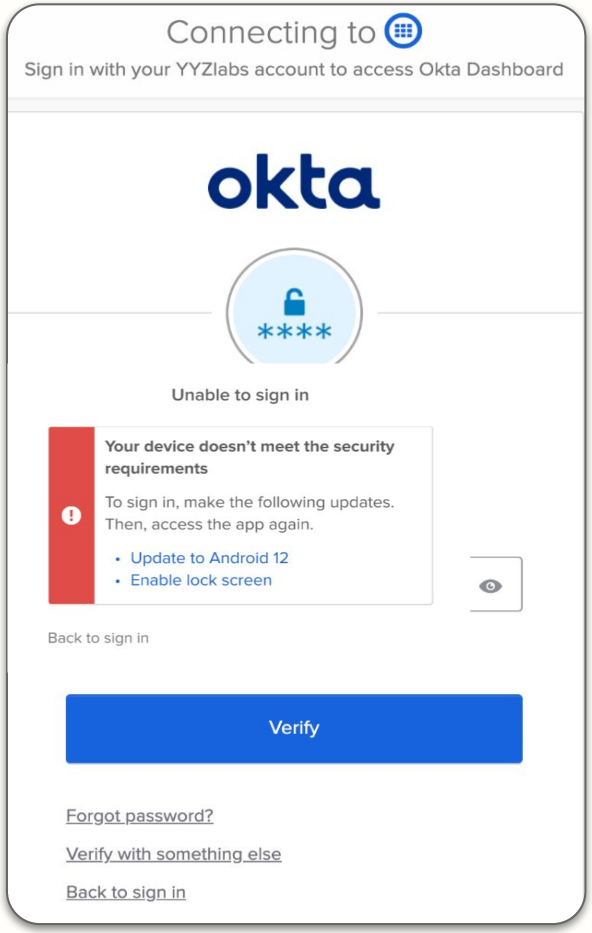
Device Assurance Grace Period for Policy Compliance

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

Provide end users with access to essential resources during configurable timeframes to empower them to self-remediate any device compliance issues before being locked out.

Learn more

OIE



Connecting to

Sign in with your YYZlabs account to access Okta Dashboard

okta

Unable to sign in

Your device doesn't meet the security requirements

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

- Update to Android 12
- Enable lock screen

Back to sign in

Device Assurance Grace Period for Policy Compliance

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

Access Management

Early Access

Granular Admin Permissions to Access Identity Providers

Available in: Okta Identity Engine

Assign specific IdPs to other admins through granular admin permissions when creating custom admin roles,. ensuring only authorized users are provided access to the configuration of IdPs.

Learn more

OIE

Just-in-Time Local Account Creation for macOS

Available in: Okta Device Access

Enable users to create local macOS accounts with standard or administrator privileges to facilitate low-touch account management, especially for shared devices.

OIE

Yubico FIDO Pre-reg

Available in: AMFA/ MFA

Help protect your organization and offer users a quick, user-friendly way to secure their accounts with Yubico FIDO Pre-reg.

OIE

Smart Card Just in Time Provisioning

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

Enable federal employees to seamlessly access systems and resources with their PIV/CAC card across agencies, without requiring custom code.

Learn more

OIE

Yubico FIDO Pre-reg

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

Access Management

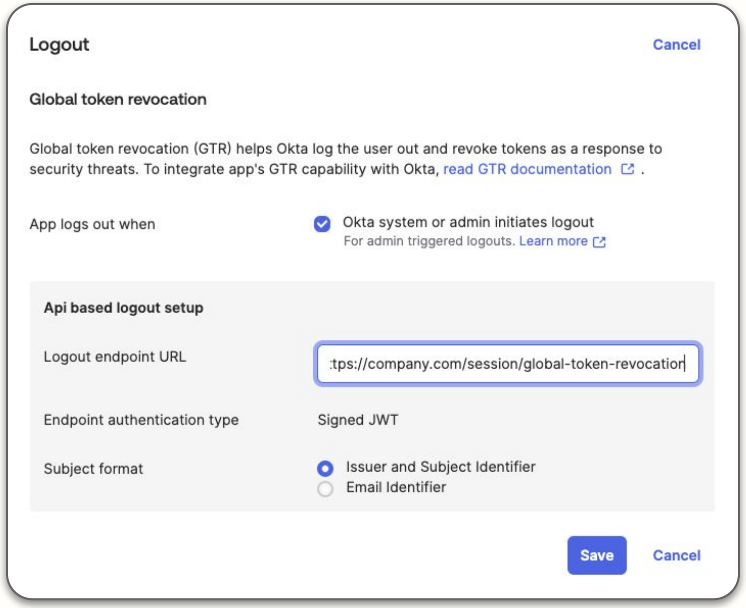
Early Access

Universal Logout Support for Custom SAML and OIDC apps

Available in Identity Threat Protection

Organizations with internal applications that are assigned to their users can now leverage Universal Logout. This is currently available with ITP SKU.

OIE



Logout Cancel

Global token revocation

Global token revocation (GTR) helps Okta log the user out and revoke tokens as a response to security threats. To integrate app's GTR capability with Okta, read GTR documentation .

App logs out when ☑ Okta system or admin initiates logout
For admin triggered logouts. Learn more

Api based logout setup

Logout endpoint URL: tps://company.com/session/global-token-revocation

Endpoint authentication type: Signed JWT

Subject format: ● Issuer and Subject Identifier
○ Email Identifier

Universal Logout Support for Custom SAML and OIDC apps

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

Identity Management

General Availability

Auto-Update for LDAP Agents

Available in: Universal Directory

Schedule and automate AD agent updates to ensure you're leveraging the most secure and latest LDAP Agent capabilities.

Learn more

Classic

OIE

MS Graph based domain federation for O365

Available in: SSO + LCM

Streamline the set up of automatic domain federation with the OAuth-based consent flow.

Learn more

Classic

OIE

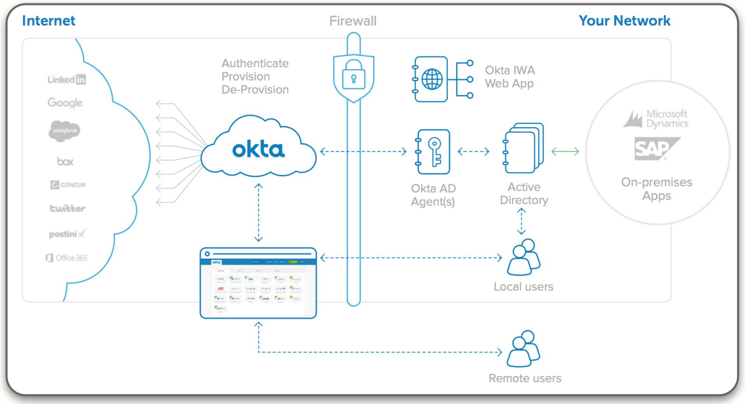
Secure Communication and Deployment for AD Agent

Available in: Universal Directory

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

Classic

OIE



Secure Communication and Deployment for AD Agent

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

Workforce Identity Cloud

Identity Management

Early Access

Certificate Based Authentication with Office 365

Available in: Universal Directory

Enable Windows device logon using smart card certificates with certificate based authentication support for Azure AD/Office 365.

OIE

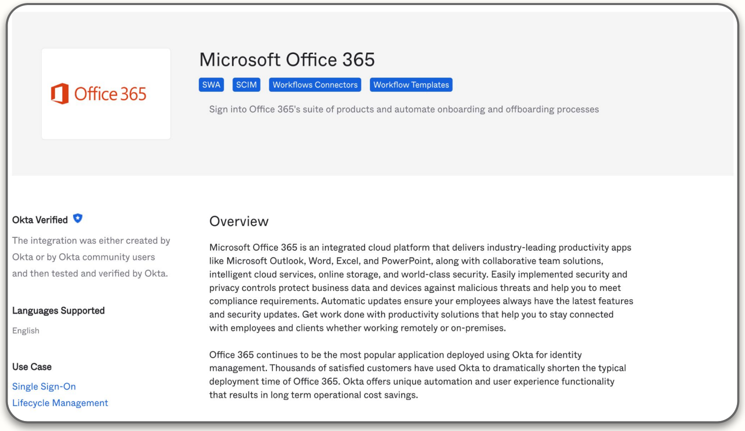
Step-up Authentication for Microsoft O365 Apps

Available in: SSO

Strengthen sign on policies within Okta when Entra ID policies require step up authentication.

Learn more

OIE



Microsoft Office 365

SWA SCIM Workflows Connectors Workflow Templates

Sign into Office 365's suite of products and automate onboarding and offboarding processes

Okta Verified

The integration was either created by Okta or by Okta community users and then tested and verified by Okta.

Languages Supported

English

Use Case

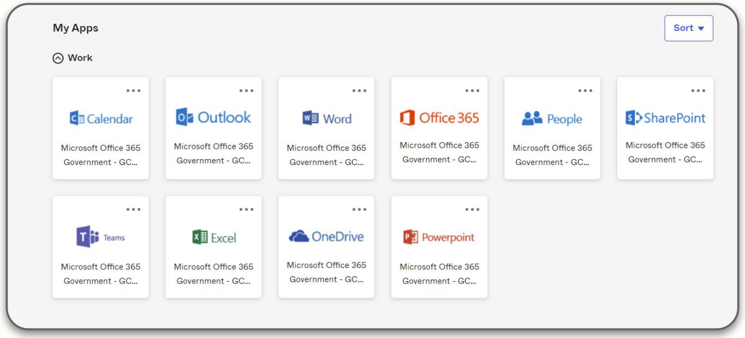
Single Sign-On

Lifecycle Management

Overview

Microsoft Office 365 is an integrated cloud platform that delivers industry-leading productivity apps like Microsoft Outlook, Word, Excel, and PowerPoint, along with collaborative team solutions, intelligent cloud services, online storage, and world-class security. Easily implemented security and privacy controls protect business data and devices against malicious threats and help you to meet compliance requirements. Automatic updates ensure your employees always have the latest features and security updates. Get work done with productivity solutions that help you to stay connected with employees and clients whether working remotely or on-premises.

Office 365 continues to be the most popular application deployed using Okta for identity management. Thousands of satisfied customers have used Okta to dramatically shorten the typical deployment time of Office 365. Okta offers unique automation and user experience functionality that results in long term operational cost savings.


My Apps
Sort
Work
Calendar
Microsoft Office 365 Government - GC...
Outlook
Microsoft Office 365 Government - GC...
Word
Microsoft Office 365 Government - GC...
Office 365
Microsoft Office 365 Government - GC...
People
Microsoft Office 365 Government - GC...
SharePoint
Microsoft Office 365 Government - GC...
Teams
Microsoft Office 365 Government - GC...
Excel
Microsoft Office 365 Government - GC...
OneDrive
Microsoft Office 365 Government - GC...
Powerpoint
Microsoft Office 365 Government - GC...

Step-up Authentication for Microsoft O365 Apps

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

Workforce Identity Cloud

Identity Governance

General Availability

Bidirectional Group Management with Active Directory

Available in: Okta Identity Governance

Streamline administration of memberships to AD-sourced group through Okta Identity Governance with bidirectional syncing.

Learn more

Classic OIE

Configurable reviewer context

Available in: Okta Identity Governance

Choose and provide the right context to provide access certification reviewers, including application usage, group membership, and application assignment date to give reviewers the right context to inform access decisions quickly and effectively.

Learn more

Classic OIE

Just-In-Time User Provisioning for Okta Access Requests

Available in: Okta Identity Governance

JIT user provisioning allows customers to automatically assign the Okta Access Requests app to users who are associated with a request or task, avoiding the need to provision to all users while limiting friction to approve or review requests.

Classic OIE

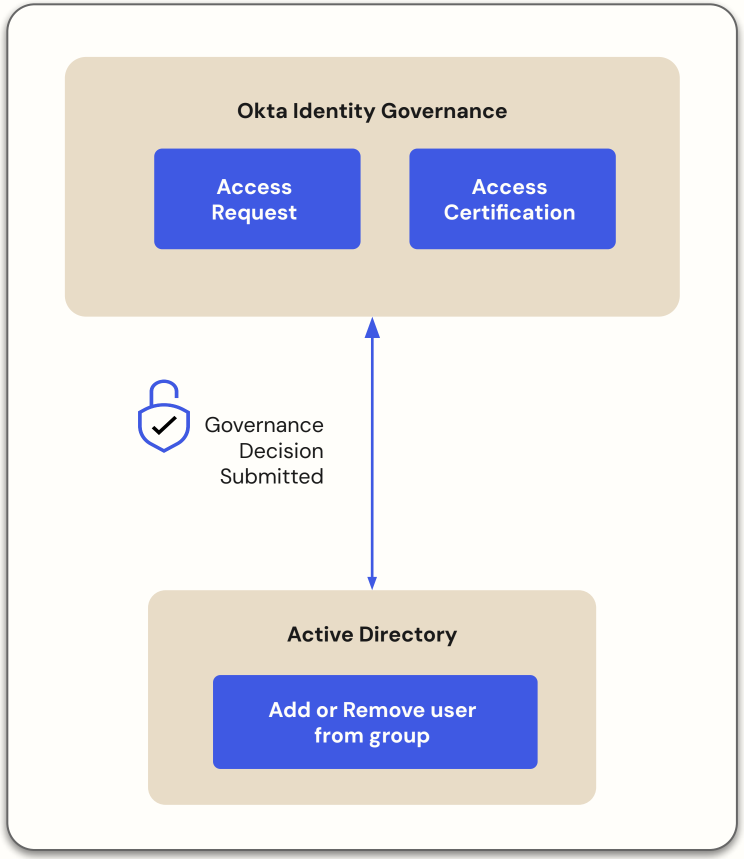
OIN Apps for Entitlement Management - Cisco Webex, Coupa, Dropbox, ServiceNow, etc.

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 6 new OIN apps: Cisco Webex, ServiceNow, Dropbox, DocuSign, Coupa, and SmartRecruiters.

Learn more

Classic OIE



Bidirectional Group Management with Active Directory

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

okta

Identity Governance

Early Access

Custom Entitlements Integrations for On-Prem Apps

Available in: Okta Identity Governance

Enable OIG/entitlements integrations for custom on-prem applications using Okta’s SCIM APIs and Okta’s latest on-prem provisioning agent

Classic

OIE

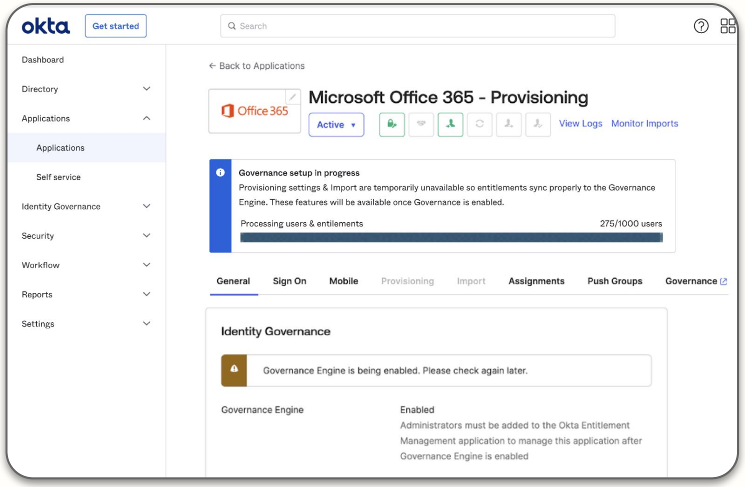
One-click Governance Enablement for Provisioning Enabled Applications

Available in: Oka Identity Governance

Automate Entitlements Management setup for existing app instances when opting into Governance Engine, migrating existing user entitlements into Governance Engine with safeguards to protect provisioning flows.

Classic

OIE



Microsoft Office 365 - Provisioning

Governance setup in progress

Provisioning settings & Import are temporarily unavailable so entitlements sync properly to the Governance Engine. These features will be available once Governance is enabled.

Processing users & entitlements 275/1000 users

Identity Governance

Governance Engine is being enabled. Please check again later.

Governance Engine: Enabled

Administrators must be added to the Okta Entitlement Management application to manage this application after Governance Engine is enabled

One-click Governance Enablement for Provisioning Enabled Applications

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

Privileged Access

General Availability

Sudo Support

Available in: Okta Privileged Access

Centrally manage Sudo on Linux servers in order to increase security, enforce least privilege principles, and avoid over-permissioned scenarios..

[Learn more]

Classic

OIE

Workflows Connector for Okta Privileged Access

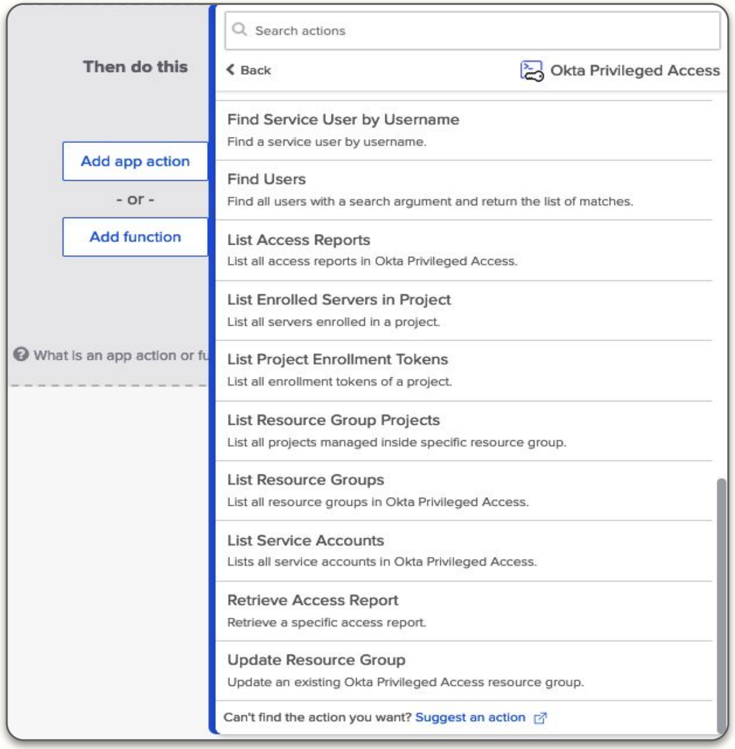
Available in: Okta Privileged Access

Simplify and automate common management tasks in Okta Privileged Access with a set of pre-built action cards.

[Learn more]

Classic

OIE



Search actions

Then do this

< Back

Okta Privileged Access

Add app action

- or -

Add function

What is an app action or fu

Find Service User by Username
Find a service user by username.

Find Users
Find all users with a search argument and return the list of matches.

List Access Reports
List all access reports in Okta Privileged Access.

List Enrolled Servers in Project
List all servers enrolled in a project.

List Project Enrollment Tokens
List all enrollment tokens of a project.

List Resource Group Projects
List all projects managed inside specific resource group.

List Resource Groups
List all resource groups in Okta Privileged Access.

List Service Accounts
Lists all service accounts in Okta Privileged Access.

Retrieve Access Report
Retrieve a specific access report.

Update Resource Group
Update an existing Okta Privileged Access resource group.

Can't find the action you want? Suggest an action

Workflows Connector for Okta Privileged Access

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

Platform Services

General Availability

Connector Enhancements

Available in: Workflows

Enhancements for our most popular connectors to manage roles, create tasks, and trigger workflows with Okta events, ServiceNow tasks, Google Workspace roles and more.

Learn more

Classic

OIE

Platform Localization

Available in: All SKUs

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

Classic

OIE

Rollback of Okta Integration Network (OIN) Apps

Available in: All SKUs

Minimize downtime for OIN Apps in the event an error is identified. Rollback can be initiated and carried out to help apps bounce back.

Learn more

Classic

OIE

Seamless System for Cross-domain Identity Management (SCIM) ISV Experience with Manual Testing

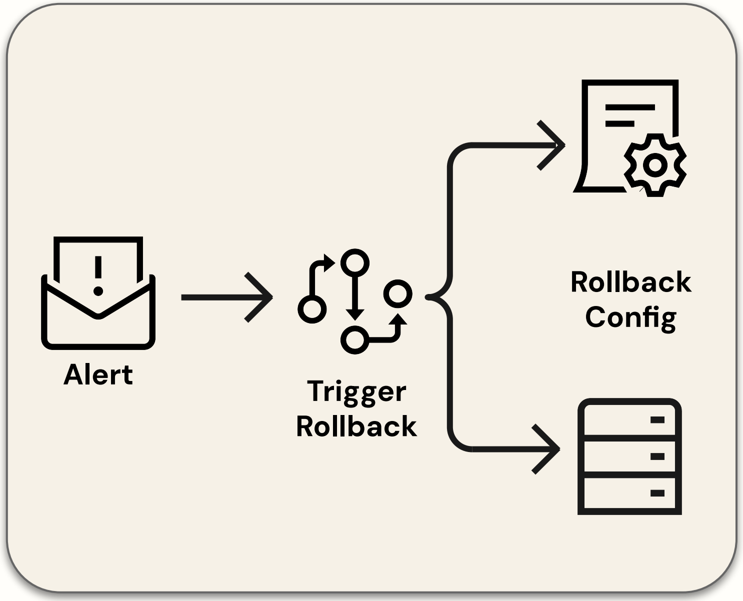
Available in: All SKUs

Reduce time to: 1) Submit SCIM OIN integration due to manual 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



Rollback of Okta Integration Network (OIN) Apps

Platform Services

Early Access

Execution History Inspector

Available in: Workflows

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. Track metadata for every flow, or just for specific high-risk or high-impact flows.

Learn more

Classic

OIE

Execution Log Streaming

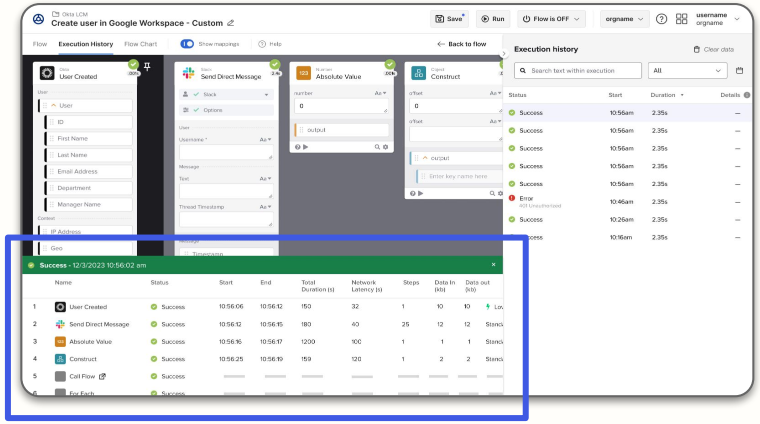
Available in: Workflows

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

Learn more

Classic

OIE



Status	Start	Duration	Details
Success	10:56am	2.35s	—
Success	10:56am	2.35s	—
Success	10:56am	2.35s	—
Success	10:56am	2.35s	—
Success	10:56am	2.35s	—
Error 401 Unauthorized	10:46am	2.35s	—
Success	10:26am	2.35s	—
ccess	10:16am	2.35s	—

Success - 12/3/2023 10:56:02 am

	Name	Status	Start	End	Total Duration (s)	Network Latency (s)	Steps	Data In (kb)	Data out (kb)	
1	User Created	Success	10:56:06	10:56:12	150	32	1	10	10	Lo
2	Send Direct Message	Success	10:56:12	10:56:15	180	40	25	12	12	Stand
3	Absolute Value	Success	10:56:16	10:56:17	1200	100	1	1	1	Stand
4	Construct	Success	10:56:25	10:56:19	159	120	1	2	2	Stand
5	Call Flow	Success								
6	For Each	Success								

Execution History Inspector

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

Workforce Identity Cloud

Okta Personal

General Availability

Okta Personal for Workforce

Available in: All SKUs

Classic

OIE

A set of features that integrate Okta Personal (consumer password manager) to Okta's workforce offering – GA in Production in early October.

- End-user interface updates to separate personal data from enterprise environment
- App migration of personal apps from work to personal account
- Account switcher in dashboard and plugin
- Domain blocking settings (for admins)

Learn more

Okta Personal for Workforce: GA Update

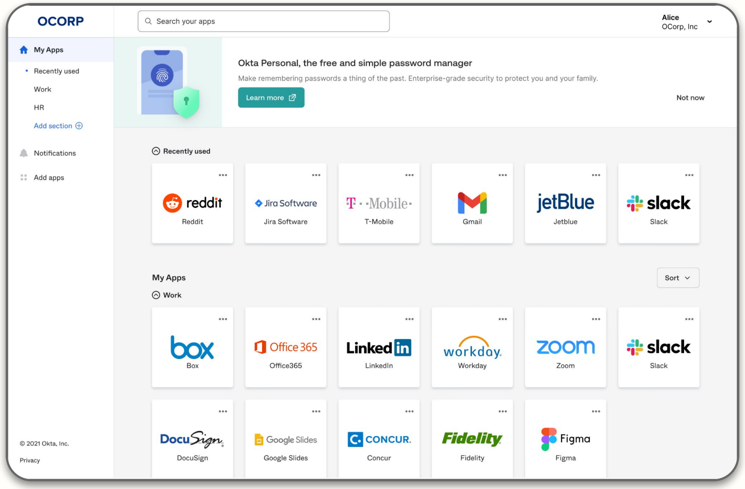
Available in: All SKUs

Classic

OIE

Starting In October 2024, eligible Okta Workforce organizations will start to see Okta Personal entry points in their end users' Workforce dashboard and plugin experiences. See if your organization is eligible and how to change your preferences.

Learn more



Okta Personal, the free and simple password manager

Make remembering passwords a thing of the past. Enterprise-grade security to protect you and your family.

Okta Personal for Workforce: GA Update

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

okta

Developer Resources

Workforce Identity Cloud

Build, integrate, and ship Identity and Access Management experiences that your users will enjoy. 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

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

Resources

Connect with the Okta team and learn more

Release Website

View here

Contact sales here

Best of Oktane Webinar

Sign up here

WIC Release Highlights

View here

Release Notes

Read here

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

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
- Brand new options for free and self-service plans to help you get started and scale with a single identity platform
- Security enhancements that give teams the power to protect customers before, at, and after the login box

Spotlights

- Forms
- Auth0 plans just got an upgrade
- Auth for GenAI

All features

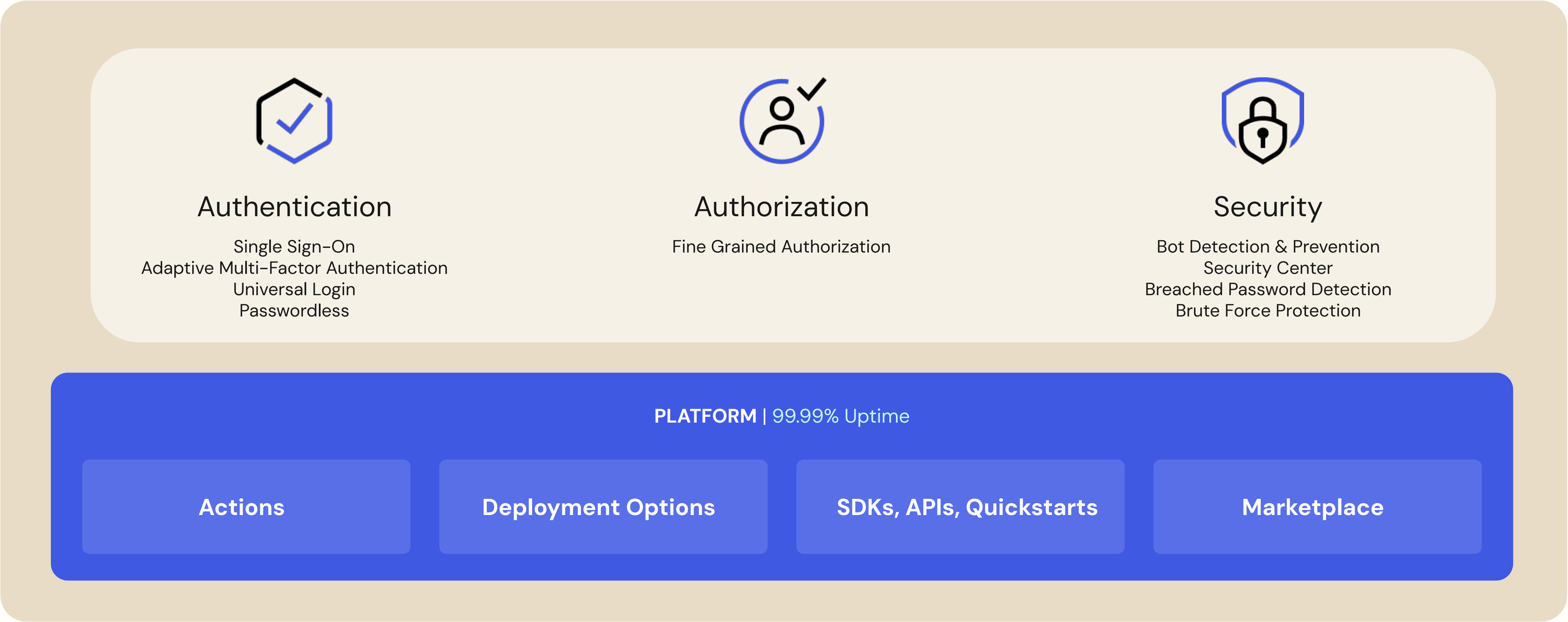
- Authentication
- Authentication — SaaS Apps
- Authorization
- Security
- Platform

Developer resources

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

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

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

General Availability

Spotlight: Forms

Unlock new JTO (journey-time orchestration) capabilities

Available in: Advanced Extensibility SKU

What is it?

Forms is a feature of Okta Customer Identity Cloud's extensibility offerings 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 enable operations to be efficient and secure, but also help drive customer retention and growth, adapt to unique security needs, and 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.

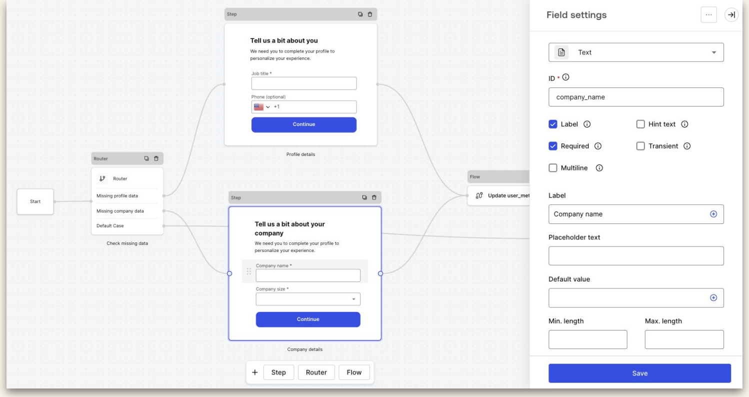
- **Accelerate time to market:** Easily build and edit forms with a no-code visual editor.
- **Build frictionless customer experiences:** Simplify adding custom policies and terms to signup and login flows.
- **Improve form conversion rates:** Collect and activate relevant customer data and enrich customer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

How to get it

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

While Forms is included in every CIC plan, the new Advanced Extensibility SKU unlocks an unlimited* number Actions + Forms.

Read the blog



Tell us a bit about you

We need you to complete your profile to personalize your experience.

Job title *

Phone (optional) +1

Continue

Tell us a bit about your company

We need you to complete your profile to personalize your experience.

Company name *

Company size *

Continue

Field settings

Text

ID *: company_name

☑ Label ☐ Hint text

☑ Required ☐ Transient

☐ Multiline

Label: Company name

Placeholder text:

Default value:

Min. length: Max. length:

Save

*Subject to system limitations

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

okta

General Availability

Spotlight: Auth0 plans just got an upgrade

Auth0 Free, Professional and Essential Plans are new and improved

Available in: Free and Self-Serve Plans

What is it?

We're excited to announce that we're expanding our Auth0 free and self-serve pricing plans.

We heard your feedback, and we've made it easier to build, deploy, and scale your app no matter what your authentication needs are.

Customer Challenge:

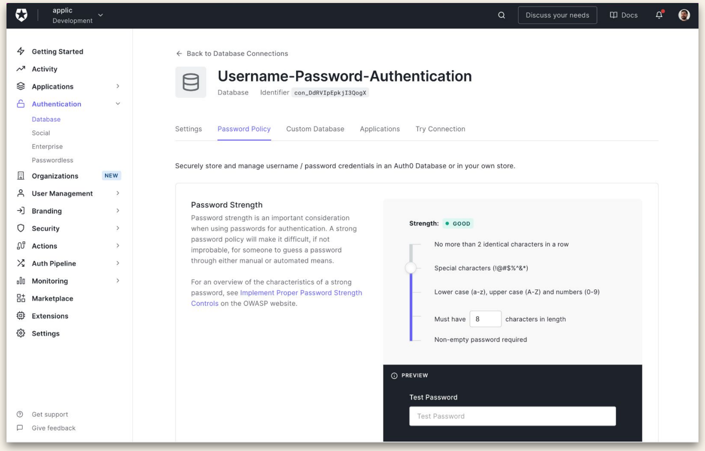
Our new free and self-serve plans tackle key customer challenges by simplifying complex identity management and enhancing security without significant costs. These plans offer scalable solutions that grow with your business, allowing you to focus on core development while ensuring robust, cost-effective authentication and authorization.

Why this matters

- **New Free Plans include:**
  - 25,000 MAUs so you can scale.
  - Unlimited* Okta Connections & Unlimited* Social Connections so users can easily access your app.
  - A custom domain so you can fully brand your authentication.
- **New Paid Plans include:**
  - 10 Organizations on B2C Plans and Unlimited* on B2B Plans so you can better manage your customers and partners.
  - Increased MFA offerings so you can mitigate the growing threat of AI-based attacks.
  - The ability to get up to 15 Enterprise Connections in B2B Pro via add-ons so you get more seamless integration across apps.

How to get it

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



Username-Password-Authentication

Database Identifier `con_DdRVIpEpkjI3QogX`

Securely store and manage username / password credentials in an Auth0 Database or in your own store.

Password Strength

Password strength is an important consideration when using passwords for authentication. A strong password policy will make it difficult, if not improbable, for someone to guess a password through either manual or automated means.

For an overview of the characteristics of a strong password, see Implement Proper Password Strength Controls on the OWASP website.

Strength: GOOD

No more than 2 identical characters in a row

Special characters (!@#$%^&*)

Lower case (a-z), upper case (A-Z) and numbers (0-9)

Must have 8 characters in length

Non-empty password required

Test Password: Test Password

* subject to system limitations

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

okta

Announcement

Spotlight: Auth for GenAI

Build AI into your apps securely

What is it?

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

It is a series of features that allows you to confirm that your AI agents have the right and least privileged access to sensitive information, can call APIs securely on behalf of users to integrate with other apps, and can securely implement on-demand user authentication when background/async AI agents need user confirmation for actions.

Customer Challenge:

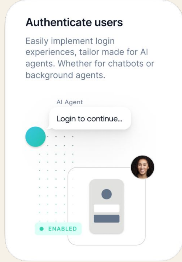
GenAI apps can introduce vulnerabilities because their behavior is non-deterministic. They also rely on UX patterns that are different than those of web/mobile apps. Auth for GenAI allows implementing those patterns easy, while helping protect from vulnerabilities.

Why this matters

- **Call APIs on user's behalf** – As GenAI apps (e.g. chatbots) integrate user products to provide delightful experiences, calling APIs on behalf of users will become a commonplace need. You need to do this securely to prevent vulnerabilities that can be caused by hallucinating LLMs and admin like agent credentials.
- **Async User Confirmation** – As AI agents go mainstream, async agents (or agent running in the background) to perform processing or wait for conditions will become commonplace. Those agents will need to authenticate users on-demand, to avoid keeping user credentials around indefinitely.
- **Authorization for RAG** – GenAI apps use RAG to minimize hallucinations. Feeding documents/content the user has no access to can lead to security violations
- **Chat sharing** – As GenAI apps make chatbots prevalent, sharing chat sessions with co-workers/friends will be common and help with organic product growth.

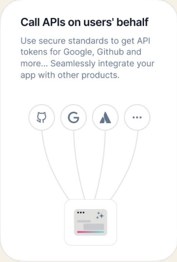
How to get it

Interested? Join our waitlist here to be the first to find out when features become available.



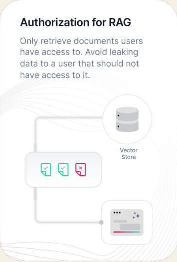
Authenticate users

Easily implement login experiences, tailor made for AI agents. Whether for chatbots or background agents.



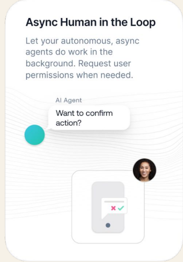
Call APIs on users' behalf

Use secure standards to get API tokens for Google, Github and more... Seamlessly integrate your app with other products.



Authorization for RAG

Only retrieve documents users have access to. Avoid leaking data to a user that should not have access to it.



Async Human in the Loop

Let your autonomous, async agents do work in the background. Request user permissions when needed.

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

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 Q3 2024.

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

Authentication

General Availability

New Localization Languages for Universal Login

Feature of: Universal Login / Available in: All plans

We've added 27 new languages to Universal Login's extensive list of localization options. This means customers can now localize authentication journeys with out of the box translations for 78 different languages!

Learn more

Native Login for Passkeys

Feature of: Core Platform / Available in: All plans

Customers will be able to add passkey enrollment and authentication capabilities to native applications without requiring the use of a Webview.

Learn more

Customized Sign-Up and Login

Feature of: Core Platform / Available in: All plans

Universal Login now enables customers to add fields and text to the signup and login prompts to collect additional information and store that information in the user profile. Customers can now require that custom fields to be completed (checked, filled-out, etc.) before continuing with the authn process.

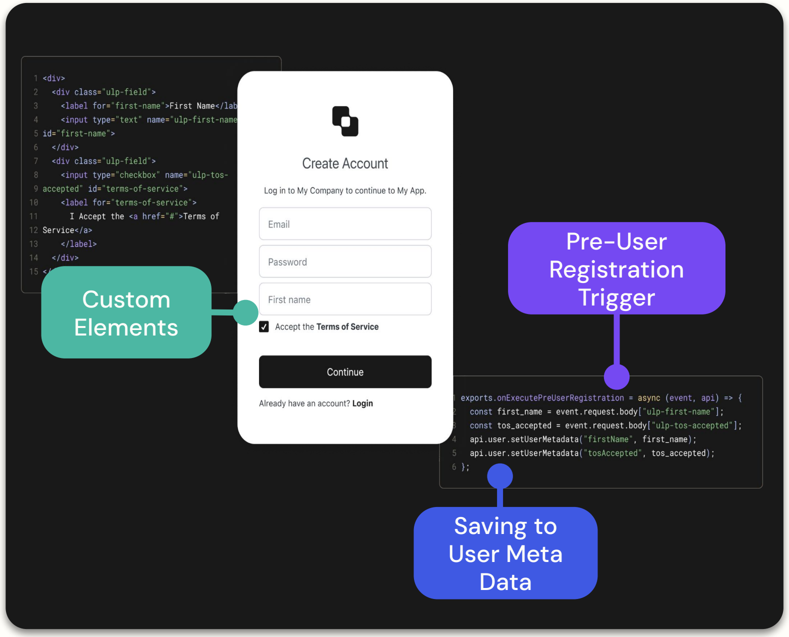
Learn more

JWT Access Tokens Profiles

Feature of: Core Platform / Available in: All plans

Opt-in to use RFC 9068 or Auth0 JWT profile for access tokens depending on the API. Increase compatibility across API gateways and simplify onboarding on to Auth0 from other Identity solutions.

Learn more



```
<div>
  <div class="ulp-field">
    <label for="first-name">First Name</lab
    <input type="text" name="ulp-first-name
id="first-name">
  </div>
  <div class="ulp-field">
    <input type="checkbox" name="ulp-tos-
accepted" id="terms-of-service">
    <label for="terms-of-service">
      I Accept the <a href="#">Terms of
Service</a>
    </label>
  </div>
</
```

Create Account

Log in to My Company to continue to My App.

Email

Password

First name

☑ Accept the Terms of Service

Continue

Already have an account? Login

```
exports.onExecutePreUserRegistration = async (event, api) => {
  const first_name = event.request.body["ulp-first-name"];
  const tos_accepted = event.request.body["ulp-tos-accepted"];
  api.user.setUserMetadata("firstName", first_name);
  api.user.setUserMetadata("tosAccepted", tos_accepted);
};
```

Customized Sign-up and Login

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

Authentication

General Availability

Flexible Identifiers

Feature of: Core Platform / Available in: All plans

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

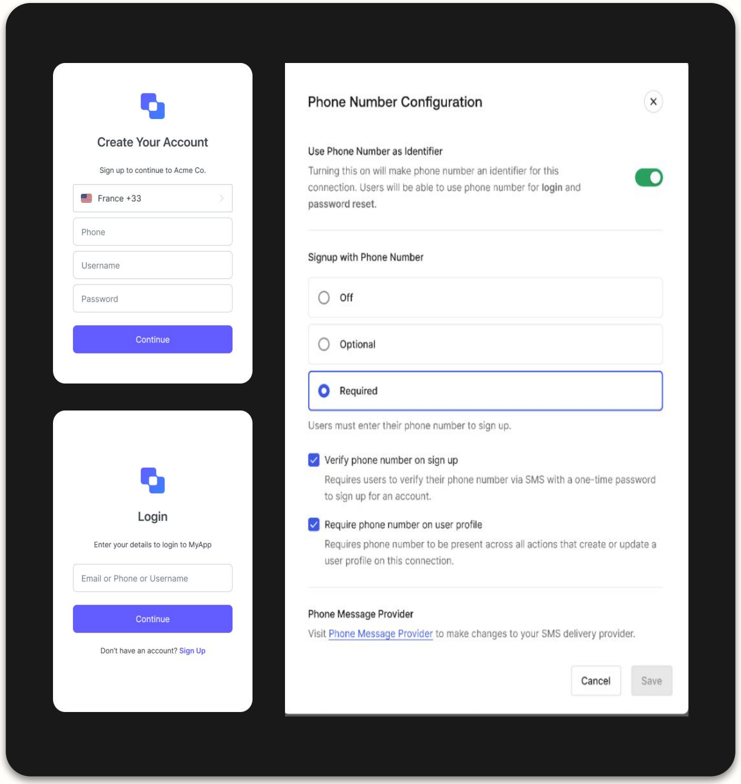
Learn more

WCAG 2.2 AA

Feature of: Core Platform / Available in: All plans

Web Content Accessibility Guidelines (WCAG) version 2.2 AA for Universal Login. Includes several accessibility improvements to Universal Login as part of our efforts to reach WCAG 2.2 AA guideline conformance.

Learn more



Create Your Account

Sign up to continue to Acme Co.

France +33

Login

Enter your details to login to MyApp

Don't have an account? Sign Up

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

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

Authentication

Early Access

Passwordless Support for Custom Prompts

Feature of: Core Platform / Available in: All plans

Enable passwordless features like SMS, Magic Link, and more when using Custom Prompts for the sign-up or sign-in flow.

Learn more

Phone Extensibility

Feature of: Core Platform / Available in: All plans

Customize outbound flexible identifier phone messages and providers.

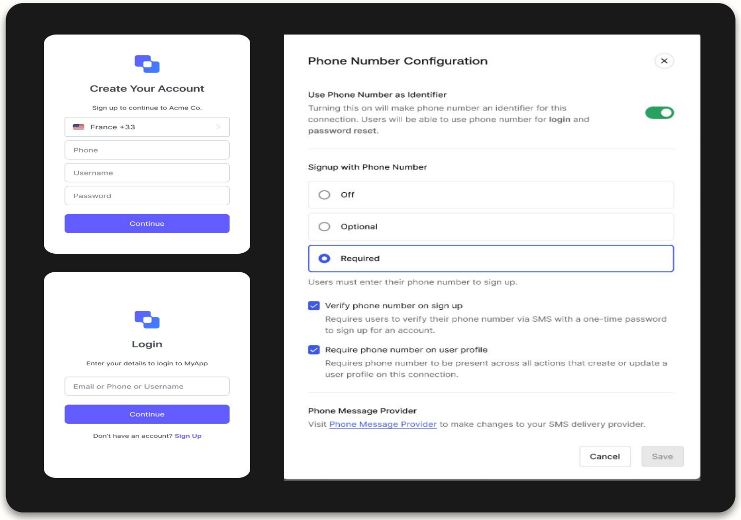
Learn more

Email OTP Verification for Sign-up and Password Reset

Feature of: Core Platform / Available in: All plans

Configure a connection using Email OTP or Link. Email OTP for verification helps prevent fake account creation and prevent the likelihood of account creation errors.

Learn more



Create Your Account

Sign up to continue to Acme Co.

France +33

Phone

Username

Password

Continue

Login

Enter your details to login to MyApp

Email or Phone or Username

Continue

Don't have an account? Sign Up

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.

Cancel Save

Phone Extensibility

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

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 enabling compliance & authentication.

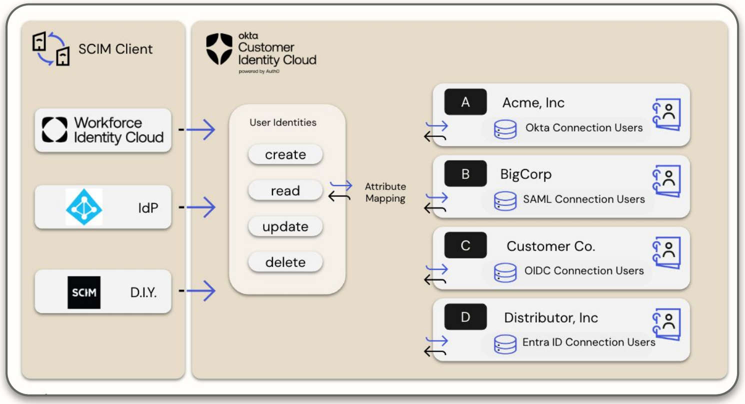
Learn more

Inbound SCIM for Enterprise Connections Log Stream Filter

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

A new log stream filter category streams out only SCIM tenant logs when SCIM is enabled on the tenant. Through this capability, customers can monitor the full details of all the SCIM requests that Auth0 receives and get notified when a user is created, updated, or deleted using SCIM.

Learn more



Inbound SCIM

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

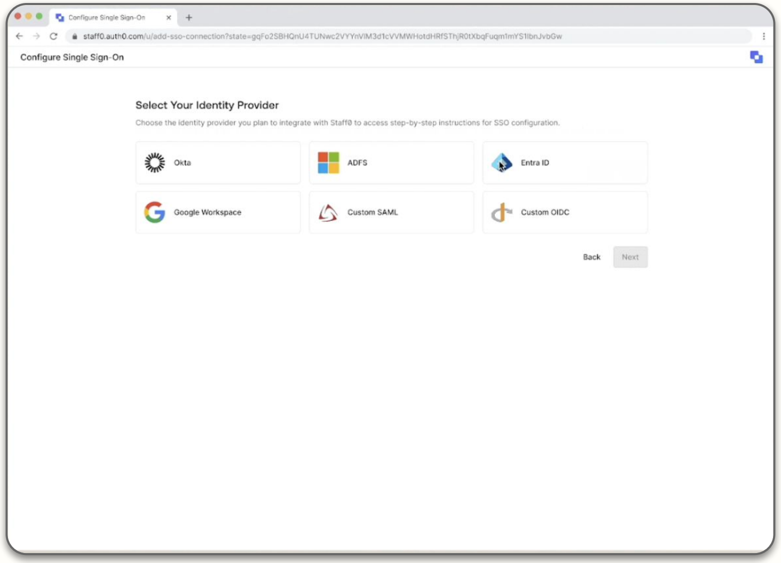
Authentication — SaaS Apps

Early Access

Self-Service SSO

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

Provide your business customers with a hosted workflow to configure Single Sign-on (SSO) access to your SaaS application that works with the major identity providers.



Configure Single Sign-On
staff0.auth0.com/u/add-sso-connection?state=gqFo2SBHQnU4TUNwc2VYYnVIM3d1cVVMWHotdHRfSThjR0tXbqFuqm1mYS1lbnJvbGw
Configure Single Sign-On
Okta
ADFS
Entra ID
Google Workspace
Custom SAML
Custom OIDC
Back
Next

Select Your Identity Provider

Choose the identity provider you plan to integrate with Staff0 to access step-by-step instructions for SSO configuration.

Self-Service SSO

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

Authorization

General Availability

Private Cloud Support for AWS

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

Enables FGA to be deployed in Private Cloud environments for AWS.

Learn more

Query Consistency Options

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

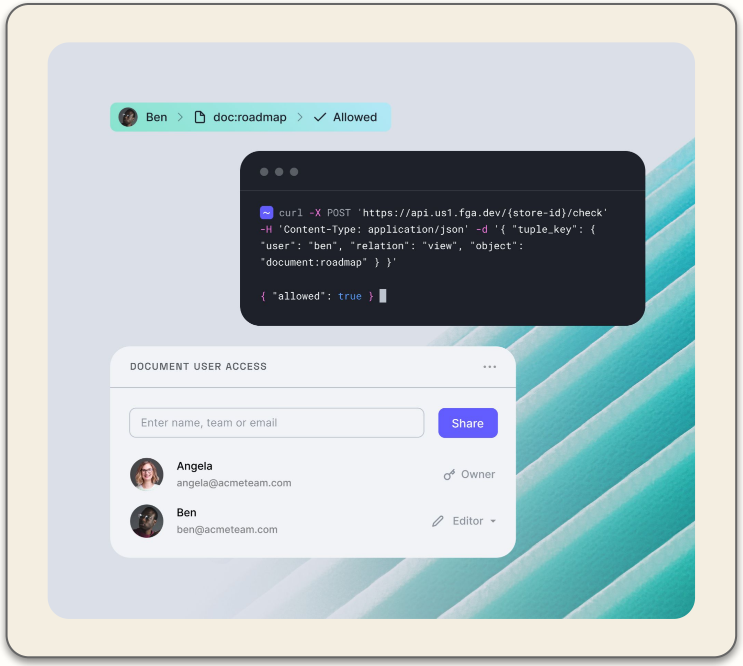
Provides a way for FGA clients to perform authorization queries that have higher consistency requirements

Learn more

Telemetry in SDKs

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

OpenFGA SDKs now emit metrics using the OpenTelemetry standard, allowing customers to monitor RPS, error rates, and latency using their observability infrastructure.



```
~ curl -X POST 'https://api.us1.fga.dev/{store-id}/check'
-H 'Content-Type: application/json' -d '{ "tuple_key": {
"user": "ben", "relation": "view", "object":
"document:roadmap" } }'

{ "allowed": true }
```

DOCUMENT USER ACCESS

Enter name, team or email

Share

Angela
angela@acmeteam.com
Owner

Ben
ben@acmeteam.com
Editor

Fine Grained Authorization (FGA)

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

Security

General Availability

Bot Detection Now Upgraded with ASN Reputation Signals

Feature of: Attack Protection / Available in: Attack Protection

Latest upgrade to our fourth-generation Bot Detection, featuring enhanced ASN reputation signals and untrusted IP data. By integrating these data sources into our proprietary Bot Detection ML model, we can more effectively target scripted attacks that frequently change. Learn more

Prioritized Log Streams

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

Stream a predefined set of security risk-related log events through a dedicated architecture with higher confidence. Customers can stream events to SIEM tools, monitor, and take action on Security events without interruption when there is an attack on the customer's tenant or abnormally high user activity. Learn more

Thresholds in Security Center Dashboard

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

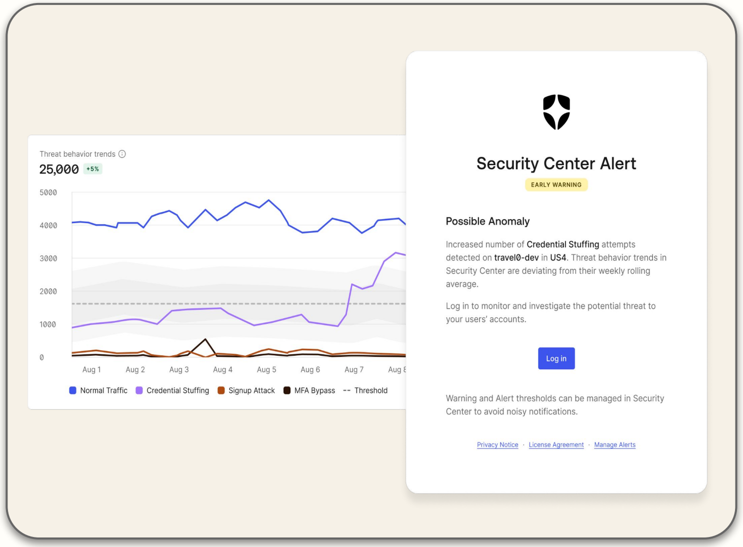
New Security Center features offer configurable, intelligent baselines and anomaly detection, turning data into actionable insights.

Learn more

Bot Detection: Enhanced sign-up attack detection

Feature of: Attack Protection / Available in: Attack Protection

New ML model is designed to detect attacks commonly occur at sign-up.



Security Center Alert

Possible Anomaly

Increased number of **Credential Stuffing** attempts detected on **travel0-dev** in **US4**. Threat behavior trends in Security Center are deviating from their weekly rolling average.

Log in to monitor and investigate the potential threat to your users' accounts.

Warning and Alert thresholds can be managed in Security Center to avoid noisy notifications.

Security Center

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

okta

Security

Early Access

Managing Session and Refresh Tokens in Actions

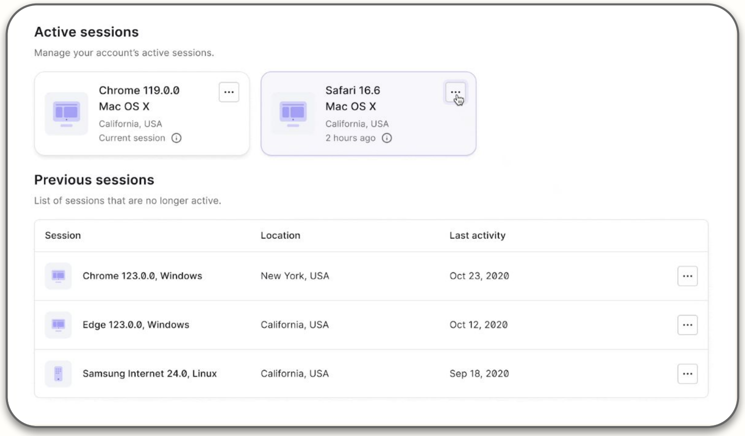
Available in: All Enterprise Plans

Improved capabilities to manage sessions and refresh_tokens in Actions. These are powerful building blocks that can help you dynamically manage access for a wide variety of use cases, for example, you can improve your security posture by revoking sessions based on risk assessments. Learn more

Customer Managed Keys

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

Introducing Early Access for Bring Your Own Key (BYOK) and Control Your Own Key (CYOK) as part of our Highly Regulated Identity offerings. BYOK enables you to securely replace your Auth0 root key with a custom one, while CYOK allows you to manage its lifecycle directly via the management API. Learn more



Active sessions

Manage your account's active sessions.

Chrome 119.0.0
Mac OS X
California, USA
Current session ⓘ

Safari 16.6
Mac OS X
California, USA
2 hours ago ⓘ

Previous sessions

List of sessions that are no longer active.

Session	Location	Last activity	
Chrome 123.0.0, Windows	New York, USA	Oct 23, 2020	···
Edge 123.0.0, Windows	California, USA	Oct 12, 2020	···
Samsung Internet 24.0, Linux	California, USA	Sep 18, 2020	···

Session Extensibility

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

Platform

General Availability

New Private Cloud Region in UAE

Feature of: Private Cloud / Available in: Private Cloud

Adding to our deployment flexibility, we have added a new Private Cloud deployment region for AWS in UAE.

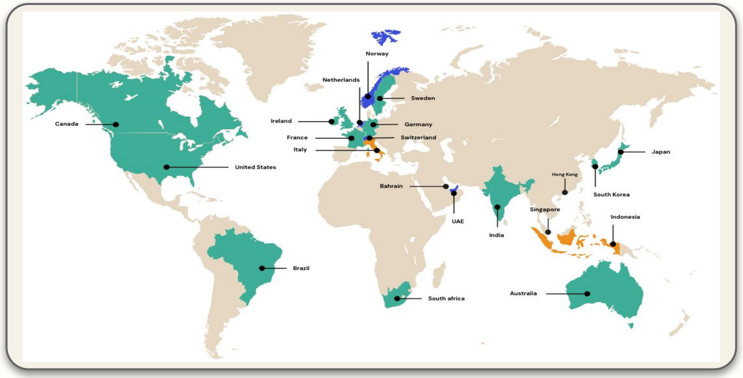
Learn more

Forms

Feature of: Actions / Available in: All CIC plans, as well as the Advanced Extensibility SKU for more than 30 Actions+Forms.

A no-code visual editor that enables developers and UX teams to customize signup and login experiences, available as a feature of Okta's Customer Identity Cloud Actions extensibility platform.

Learn more



Deployment Flexibility

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

Customer Identity Cloud

Platform

Early Access

Guide with Okta AI

Feature of: Core Platform / Available in: All plans

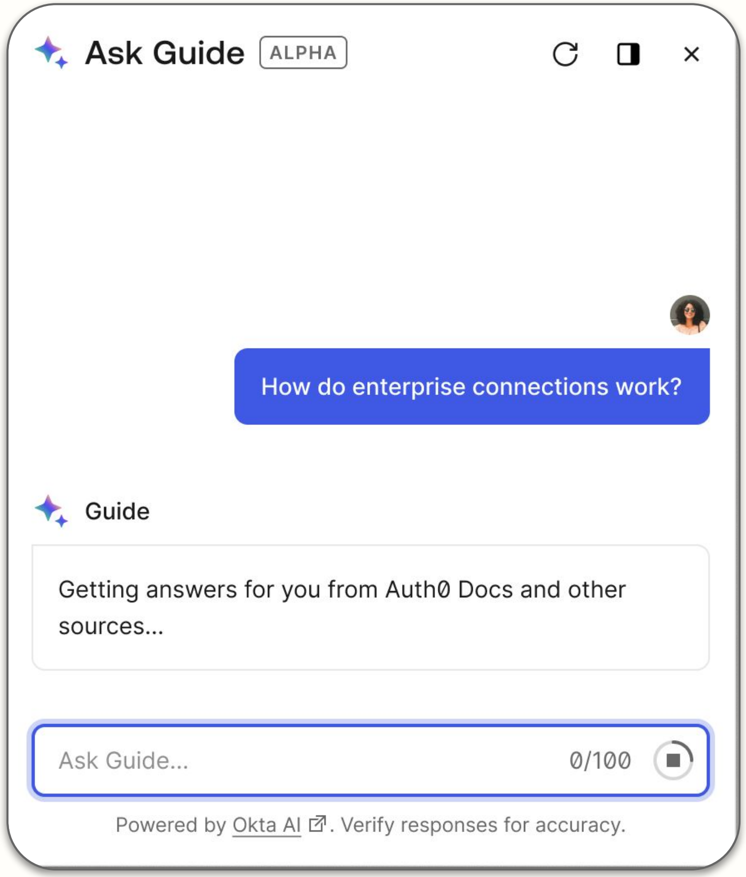
Guide is trained on all Okta Customer Identity Cloud documentation and specifications. It can respond to natural language queries in a way that guides builders towards the most efficient solution or workflow.

Learn more

Compliance: ENS and TISAX

Feature of: Core Platform / Available in: All Plans

Customer Identity Cloud is now ENS (Esquema Nacional de Seguridad) High and TISAX (Trusted Information Security Assessment Exchange) certified. ENS establishes robust information security for public sector data in Spain, while TISAX establishes stringent security practices for the automotive industry. These certifications reflect our dedication to maintaining the highest levels of data protection and security.



How do enterprise connections work?

Guide

Getting answers for you from Auth0 Docs and other sources...

Guide with Okta AI

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

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

Auth0 Developer Release Guide: Click here

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

Resources

Connect with the Okta Team and learn more

Release Website

View here

Contact sales here

Best of Oktane and DevDay

Sign up here

Developer Release PDF

View here

Changelog

Read here

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

okta