okta

Release Overview

for Early Access & General Availability in Q3 (July - September 2025)

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

Safe harbor

This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, global economic conditions have in the past and could in the future reduce demand for our products; we and our third-party service providers have in the past and could in the future experience cybersecurity incidents; we may be unable to manage or sustain the level of growth that our business has experienced in prior periods; our financial resources may not be sufficient to maintain or improve our competitive position; we may be unable to attract new customers, or retain or sell additional products to existing customers; customer growth has slowed in recent periods and could continue to decelerate in the future; we could experience interruptions or performance problems associated with our technology, including a service outage; we and our third-party service providers have failed, or were perceived as having failed, to fully comply with various privacy and security provisions to which we are subject, and similar incidents could occur in the future; we may not achieve expected synergies and efficiencies of operations from recent acquisitions or business combinations, and we may not be able to successfully integrate the companies we acquire; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any products, features, functionalities, certifications 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.

okta

Okta offers opportunities to learn more about our latest innovations and what's to come

Release Overview Webpage

Dive further into the latest innovation and find resources to learn more here.

Connect with the Sales team here.

Best of Oktane: Okta Platform edition

Stay ahead on securing AI. In under an hour, get the key Okta Platform highlights and live demos from Oktane. Choose your session and secure your spot today.

Register now.

Release Highlight videos + Release Notes

Get a concise and informative overview of the latest updates, features, and enhancements. Watch the highlights.

See the Release Notes here.

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

okta

Welcome to the Okta Platform Release Overview

Q3 2025

Welcome back to Okta's Quarterly Release Overview. Everything we release on the Okta Platform is designed to help you build a comprehensive identity security fabric—a modern architecture to protect every identity.

Explore how our latest updates for Okta Workforce Identity bring AI agents, customers, and partners into your identity security fabric.



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

okta

Navigating the overview

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

Okta Workforce Identity

- Okta Workforce Identity overview
- Announcements and Spotlights
- Release overviews
- Developer resources

Okta Customer Identity

- Okta Customer Identity overview
- Spotlights
- Release overviews

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

Okta Workforce Identity

Okta Workforce Identity gives you the tools you need to build an identity security fabric that strengthens your security posture and automates complex IT and security tasks. It secures every employee, app, and AI agent

This quarter, our releases build on that foundation, delivering stronger governance and security controls across your most critical assets: devices, users (including AI Agents), and privileged resources.

[1] Okta Identity Governance is audit-ready for Okta for Government High, supported for eligible Okta for Government Moderate, and available with a signed BAA for HIPAA customers.

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

Spotlights and Announcements

Okta Workforce Identity

- Okta for AI agents
- Threads in the identity security fabric
- Enhancements to Okta for Government High and Okta for Government Moderate[1]
- Trusted digital experiences for Okta Customer Identity
- Okta Privileged Access with Axiom
- Okta's Global Expansion
- Okta Private Cloud

All features

- Identity Security Posture Management (ISPM)
- Access Management
- Identity Management
- Identity Governance
- Privileged Access
- Platform Services
- Premier Success Plans
- Okta Learning

Developer resources

Okta Platform brings the identity security fabric to life

Secure Identity Products

- **Posture Management** — Identity Misconfigurations
- **Governance** — Policy Violations
- **PAM** — Resource Access
- **Access Management** — Risk Signal Sharing
- **Device Access** — Device Posture Signals
- **Identity Threat Protection** — Ecosystem Signals + Universal Logout

Secure Identity Orchestration

Secure Identity Integrations

Infrastructure	Applications	APIs	Identities
IaaS, On Prem Servers	Cloud Apps, On Prem Apps	Public, Private	Directories, Machine / AI Agents

99.99% Uptime. Tens of Billions of Monthly Logins. Zero Planned Downtime.

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

okta

Announcement: Okta for AI Agents

AI Agents are your next insider threat; Okta gives you the power to see, manage, and govern them

What is it?

Okta will bring AI agents into your identity security fabric providing visibility to discover and identify risky agents with ISPM, control and management of their access with Universal Directory, and automated governance with access certifications to enforce security policies and manage the end-to-end lifecycle.

Customer Challenge:

AI agents are rapidly transforming how businesses operate — and how attackers exploit gaps. Over half of companies are already deploying AI agents, yet considering security as an afterthought.

Unlike humans, AI agents:

- Don't have a fixed owner
- Can't complete traditional MFA
- Spin up and down quickly
- Often reuse or share credentials

You can't secure what they can't see, manage, or govern. As AI agents become more autonomous and influential, they need identity-first security — just like human users.

Why this matters

AI agents are the new attack surface. As agents scale, Okta helps prevent them from becoming attack vectors by embedding them into your identity security fabric:

Detect & Discover

- Agent discovery
- Risk assessment
- Remediation plans

Provision & Register

- Agent object creation
- Human owner assignment
- Credential protection

Authorize & Protect

- Agent-specific policies
- Least privileged access

Govern & Monitor

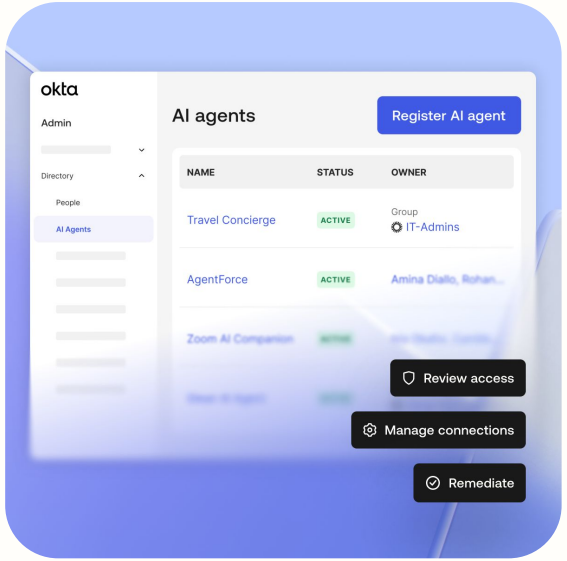
- Access certifications
- Activity monitoring
- Continuous threat detection

How to get it

Okta for AI Agents is coming soon in FY27.

Learn more

See the blog (Available 9/30)



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

okta

Announcement: Identity security fabric use cases

Use cases interwoven as threads to secure every identity end to end

What is it?

Modern security demands a unified identity security fabric. Okta brings this fabric to life through interconnected use cases—our threads—that address the most critical challenges facing security teams.

By weaving the threads into a cohesive fabric, Okta delivers end-to-end, orchestrated identity security before, during, and after authentication for every identity—human, non-human, and AI agents—across all environments.

Customer Challenge:

- **Cyberattacks** are getting more frequent and sophisticated, especially from non-human identities like AI agents.
- **Fragmented point solutions** create security gaps and complexity.
- **Integrating disparate systems** drains resources and distracts security and IT teams from strategic initiatives.

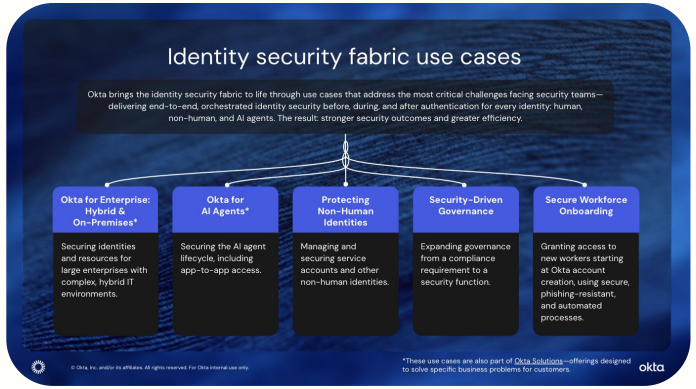
Why this matters

- **Drive broader, deeper security outcomes:** Okta delivers end-to-end identity security before, during, and after authentication.
- **Enhance efficiency and reduce operational cost:** A unified identity platform helps eliminate fragmented tools, simplifying operations for security and IT teams.
- **Confidently secure every identity at scale:** Okta secures every identity—human, non-human, and AI—across all environments with consistent, scalable controls.

How to get it

Available as part of Okta Workforce Identity Cloud. Contact your Okta rep.

See the blog here (available on 9/22).



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

okta

Spotlight: Enhancements to Okta for Government High and Government Moderate

Building the future of secure federal operations

What is it?

Okta Identity Governance: Audit-Ready for Okta for Government High (FedRAMP High), supported for eligible Okta for Government Moderate (FedRAMP Moderate), and available with a signed BAA for HIPAA customers. OIDC ID Token Encryption is audit-ready for the full Okta US Public Sector portfolio.

Customer Challenge:

Mission app owners manually identify and remediate inappropriate user access to enforce least privilege and prepare for audits. This process consumes valuable resources and diverts focus from mission-critical objectives.

Agencies that need to embed highly sensitive PII in OIDC tokens or have compliance mandates (like NIST SP 800-63C FAL3) cannot do so securely.

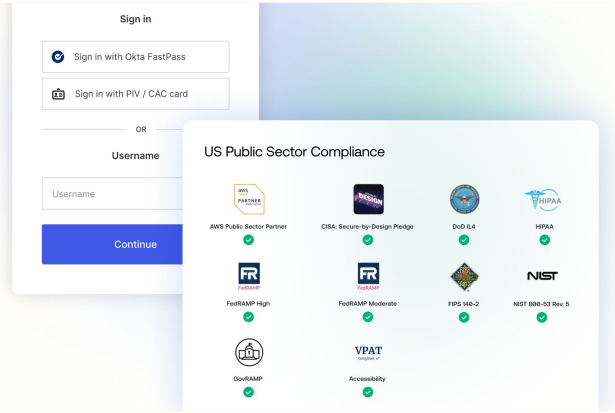
Why this matters

- **Enforce least privileged access and simplify audits with Okta Identity Governance**, giving mission app owners smart, context-rich insights, automatically highlighting unusual access or policy outliers.
- **Implement JSON Web Encryption (JWE) with OIDC ID Token Encryption**, helping agencies to secure highly sensitive PII so that only a trusted Relying Party can decrypt and consume the token.

How to get it

- Product assessment support page
- Same product SKUs with the cell add-ons
  - Okta for Government Moderate
  - Okta for Government High
  - Okta for US Military

See the announcement blog



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

okta

Announcement: Okta Privileged Access with Axiom

Expanding access controls to more sensitive resources

What is it?

Okta acquired Axiom Security, a Privileged Access Management (PAM) product that helps organizations eliminate standing privileges and secure access to critical infrastructure.

Axiom's technology will be integrated in Okta Privileged Access, expanding access controls to more sensitive resources that Okta customers can use to further strengthen their identity security fabric.

Customer Challenge:

- Disparate solutions for controlling access to servers, infrastructure, Kubernetes, and databases
- Lack of traceability to tie access back to an individual

Why this matters

- This acquisition will help Okta customers extend their identity security fabric to more privileged access and resources
- This acquisition allows Okta to accelerate our roadmap for expanded functionality around JIT access for databases and Kubernetes
- Okta Privileged Access is and will continue to be the single control plane for customers privileged resources

How to get it

New capabilities from Axiom will be added to Okta Privileged Access in H1 2026.

Read more



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

Announcement: Okta's Global Expansion

New regions in Canada and India, plus French language support

What is it?

The Okta Platform is expanding its regional availability to include Canada and India to help customers support data residency and compliance requirements.

We're also extending admin console and help documentation to support French language translations.

Why this matters

- **Regional Data Storage:** Customers will have additional regional options to store production data for both their primary and disaster recovery deployments of the Okta Platform.
- **Improved Performance:** Customers may experience lower latency and improved performance by connecting to local data centers, leading to a better user experience for their employees and customers.
- **Support French language admins:** Enable customers to use Okta in their preferred language.

How to get it

Canada and India cells will launch in Q1 2026.

French language support will launch in Q1 2026. Once available,



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

Announcement: Okta Private Cloud

Enterprise-grade identity infrastructure with dedicated, single-tenant deployment

What is it?

Single-tenant, dedicated Okta instance purpose built for security-conscious, performance-sensitive, and high-growth enterprise environments.

Why this matters

Okta Private Cloud eliminates multi-tenant risks for our most security-conscious and performance-driven customers, delivering the ultimate in data isolation and guaranteed performance.

- **Data Isolation:** Safeguard your identity data with physical and logical isolation, minimizing multi-tenant risks while meeting the most stringent security and compliance requirements.
- **Dedicated Infrastructure:** Performance on demand with sustained, reserved capacity to handle your most intense write-heavy operations.
- **Scale:** Future-proof identity platform designed to scale with your long-term growth.

How to get it

Okta Private Cloud Early Access is available today for Workforce and Customer Identity. This offering is not yet available for existing customers.



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

General Availability

Spotlight: Live Learning Labs

Hands-on learning, real-world skills

What is it?

Live Learning Labs are expert-led, hands-on sessions that let you safely explore product features, practice new skills, and test real-world use cases. They offer a low-risk way to experiment and validate your knowledge before making changes in production.

Customer challenge

Identity and access management is complex, and applying theory to real-world situations isn't always straightforward. Learning by doing is effective, but practicing in a live environment carries risks, and setting up a dedicated sandbox can be costly and time-consuming.

Why this matters

- **Build confidence:** Practice in a safe, guided environment without risking your live system.
- **Get practical insight:** Develop a deeper, hands-on understanding of Okta and Auth0 features.
- **Experiment freely:** Try advanced configurations and complex integrations to see what's possible.
- **Strengthen skills:** Learn to build and troubleshoot a wide range of use cases, from simple to complex.

How to get it

Live Learning Labs are an exclusive feature of the **Expert Learning Pass**. The pass includes access to all Live Learning Labs, expert-led sessions, and other exclusive resources.

Expert Learning Pass | Live Learning Labs



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

okta

Spotlight: New Capabilities

Okta Privileged Access EMEA Preview Environment

- Expanded regional coverage with a Preview environment in EMEA
- Enables EMEA customers to test upcoming features and validate configurations in a non-production environment

Available in:
Okta Privileged Access

Generally Available

Identity Security Posture Management EMEA and APJ Availability

- Global Expansion of Identity Security Posture Management comes to APJ and EMEA regions

Available in:
Identity Security Posture Management

Generally Available in Q4

Enhanced Disaster Recovery Available in Japan

- Expanding coverage of Enhanced Disaster Recovery to Japan deployments.
- Add-on to reduces failover times for a customer from 1 hour to less than 5 minutes (once outage is confirmed by Okta) in the event of a regional infrastructure outage.

Available in:
Okta Workforce Identity Cloud

Generally Available in Q4

Okta Aerial

- Unified console to centrally manage all Okta organizations
- Controlled access to managed orgs with granular admin roles
- Zero-standing privileges to reduce risk and strengthen security

Available in:
Okta Workforce Identity Cloud

Early Access

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

okta

Okta Workforce Identity Releases

Okta Workforce Identity unifies Identity security by identifying and fixing posture risks, enforcing strong authentication and governance, and detecting threats across all users, resources, and devices.

Learn more about our new capabilities released in Q3 2025.

Easily identify the technology each release is available in*:

Classic | Okta Identity Engine (OIE)

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

***Supported in FedRAMP Moderate/High/DOD IL4:** This product functions as expected and is fully supported in Okta's Public Sector portfolio.

***Authorized for FedRAMP Moderate/High/DOD IL4:** This product or feature is available, fully supported, and FedRAMP and/or DISA authorized.

Identity Security Posture Management (ISPM)

General Availability

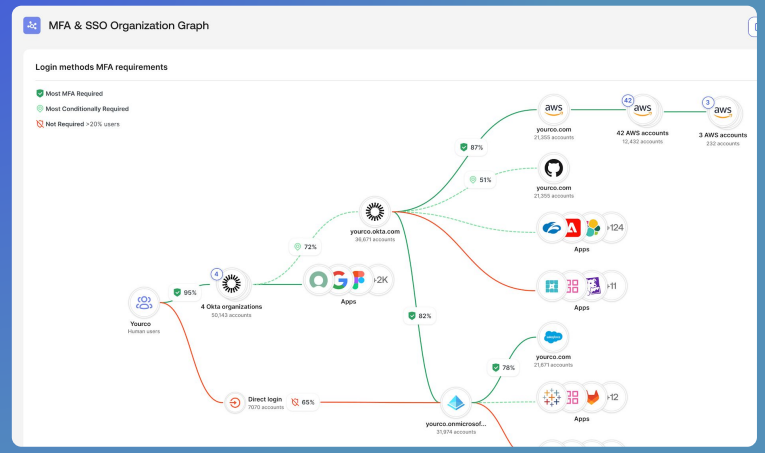
MFA and SSO analysis - Dashboard and graph

Feature of: ISPM

Security leaders gain granular MFA, Factors and SSO analysis in an exportable dashboard to identify top trends and risks.

Classic

OIE



MFA and SSO analysis - Dashboard and graph

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

Identity Security Posture Management (ISPM)

Early Access

ISPM Visibility of Active Directory

Feature of: ISPM

Security teams gain visibility into Active Directory identities and groups, to reduce attack surface.

Classic OIE

Non-Human Identities - Workload App Identities

Feature of: ISPM

Visibility and risk analysis of highly-privileged identities that empower AI Agents, apps and 3rd party products to seamlessly connect.

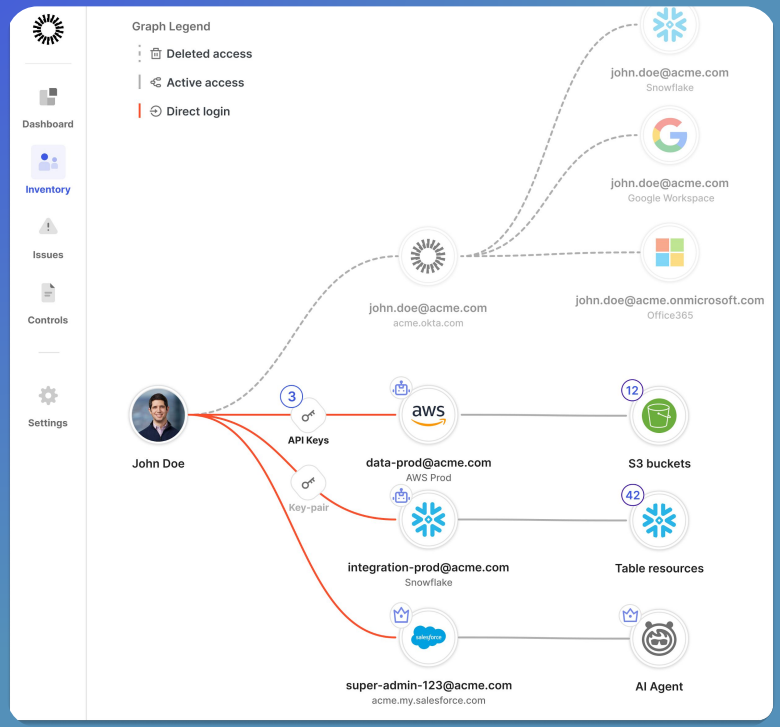
Classic OIE

ISPM Integration With Workday

Feature of: ISPM

Security teams visibility and risk detection into Workday, Detecting and prioritizing Non Human Identities, privileged and local accounts and provisioning. Deep MFA analysis.

Classic OIE



ISPM Visibility of Active Directory

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

Access Management

General Availability

Augment Application Context for OIDC and SAML applications

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

Pass application details (ID, Name) to an external identity provider when a user accesses an app. This enables richer security and policy decisions at the IdP.

Learn more

Classic OIE

Breached Credentials Protection

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

Enable customizable responses to breached credential events and allow administrators to validate the breached credential flow using a test account.

Learn more

Classic OIE

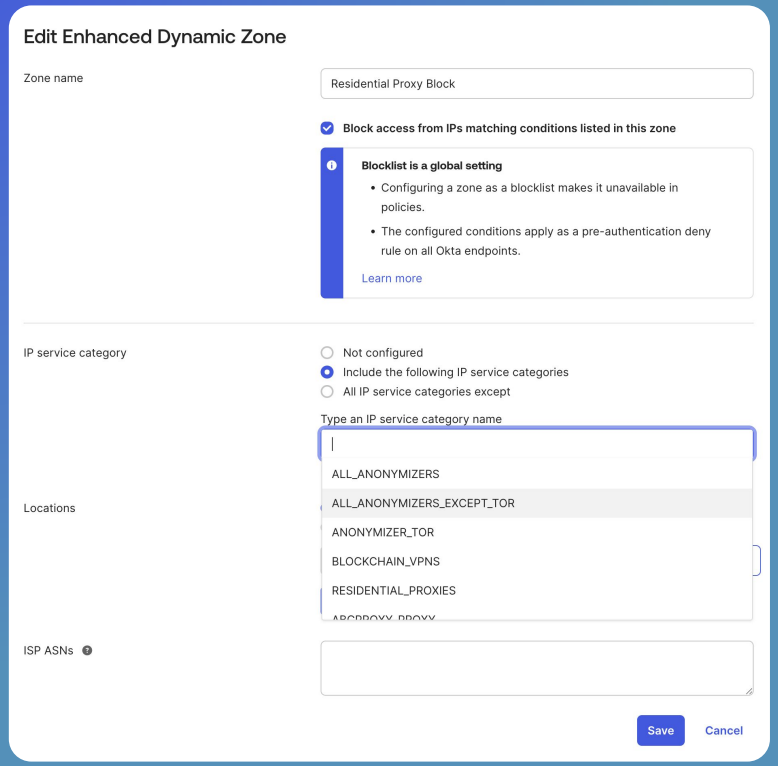
Enhanced Dynamic Network Zones – Residential Proxies

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

Enhance the ability to allow or deny access based on whether an IP is associated with a commercial VPN, anonymous proxies, ToR network.

Learn more

Classic OIE



Enhanced Dynamic Network Zones – Residential Proxies

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

Access Management

General Availability

Microsoft EAM support (External Authentication Method)

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

Allows users to satisfy MFA and other assurance requirements using Okta when accessing applications secured by Entra ID.

Learn more

OIE

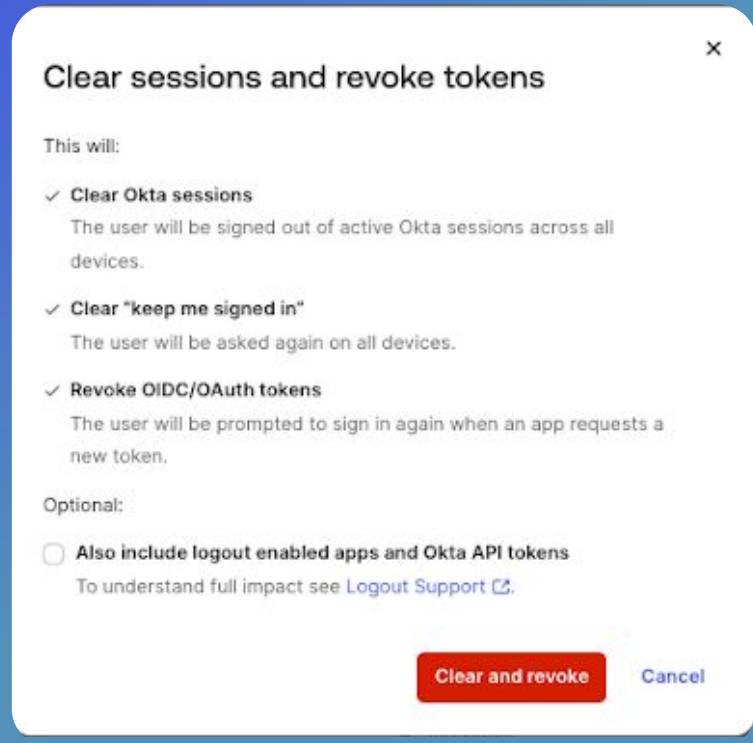
Universal Logout support for AMFA customers

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

Improve session security by enabling administrators to trigger a Universal Logout across supported applications directly from the Okta Admin Console when risky activity is detected.

Learn more

OIE



Universal Logout support for AMFA customers

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

Access Management

Early Access

Associated Domain Customizations

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

Define 'well-known endpoints' for native passkey support on iOS, Android, and WebAuthn. This enables easier adoption through autofill and in-app passkey prompts.

Learn more

OIE

Authenticator Enrollment Grace Periods

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

Configure a grace period for end users to enroll in new authenticators to reduce support tickets and prevent account lockouts.

Learn more

OIE

Cascading of the SLO request to external IdP

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

Sign users out of an external IdP when they trigger Single Logout (SLO) in Okta for configured applications.

Learn more

OIE

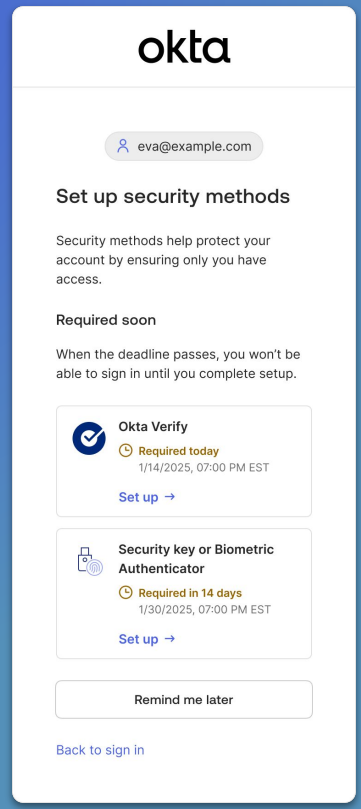
Custom AAGUID

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

Add authenticators by AAGUID to limit end-user authenticator enrollment to only approved authenticators and password managers.

Learn more

OIE



Authenticator Enrollment Grace Periods

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

okta

Access Management

Early Access

Desktop MFA Recovery for Windows

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

Admins will be able to generate temporary PINs for end users to get back into their Desktop MFA secured Windows devices.

Learn more

OIE

Device Logout for macOS

Feature of: Okta Device Access / Available in: Device Access || Authorized in: FedRAMP Moderate/High/DOD IL4

Administrators can log a user out from a Desktop MFA-secured macOS device through a manual trigger or an Identity Threat Protection policy

Learn more

OIE

Device Posture Provider

Available in: AMFA/ASSO

Administrators can enrich Device Assurance policies with posture signals from customer-owned compliance services using SAML assertions.

Learn more

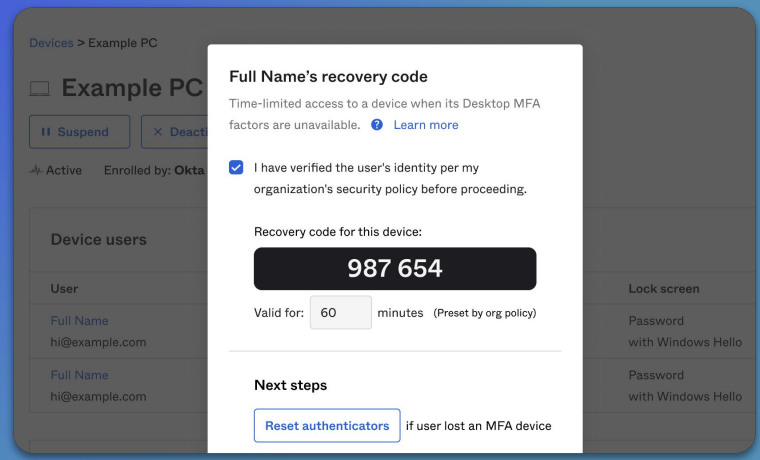
OIE

Device Signal Collection Policy

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

Specify how Okta collects device data (e.g., exclude usernames) – instead of relying on application policy rules – for more precise policy evaluation.

OIE



Desktop MFA Recovery for Windows

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

Access Management

Early Access

ID Verification Additional Biographical Attributes

Available in: MFA/AMFA

Allows mapping of additional biographical data (e.g., date of birth, email, phone) during identity verification to strengthen user matching and increase assurance.

Learn more

OIE

OAuth for Email Provider

Available in: All SKUs

Customers using an Email Provider for BYO SMTP can connect with OAuth authentication.

Learn more

Classic

OIE

OIDC Token Encryption

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

A standards-based approach for encrypting OIDC ID tokens using JSON web encryption between an Okta IdP and a relying party (RP).

Learn more

Classic

OIE

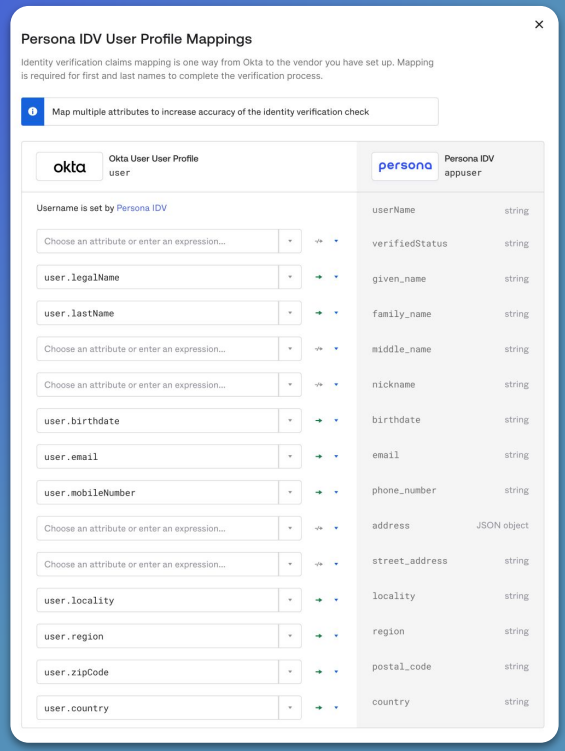
Okta Account Management Policy support for Password Expiry

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

Expand protection for password expiry flows in the OAMP policy, providing greater control over assurance requirements.

Learn more

OIE



ID Verification Additional Biographical Attributes

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

Access Management

Early Access

Overlapping IdP Signing Certificate

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

Support for multiple active signing certificates per IdP to enable seamless certificate rotation with minimal downtime and operational overhead.

Learn more

Classic OIE

Passkey for Multiple Subdomains

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

Allows the configuration of the Relying Party ID (rpID) to enable passkey registration and authentication across multiple subdomains.

Learn more

OIE

Support for Higher Assurance Certificates in Custom Domains

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

Customers can now use Custom Domains with higher security certificate encryption options, which enables greater assurance of authenticity and integrity.

Learn more

OIE

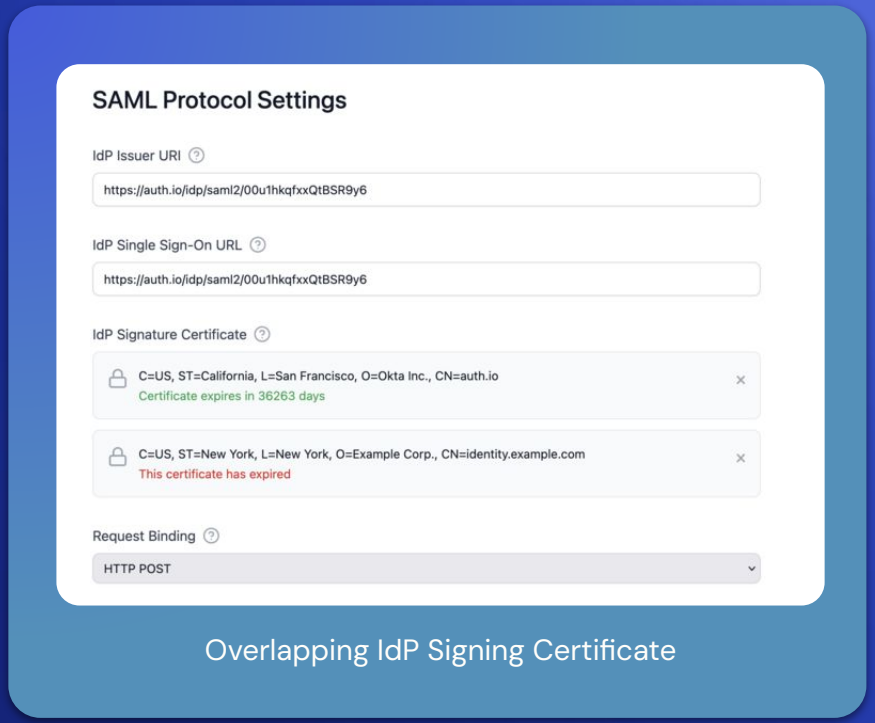
Unified Claims Generation for Okta Federated Apps

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

Simplified interface for configuring existing and new SAML attributes and OIDC claims types.

Learn more

OIE



Overlapping IdP Signing Certificate

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

okta

Access Management

Early Access

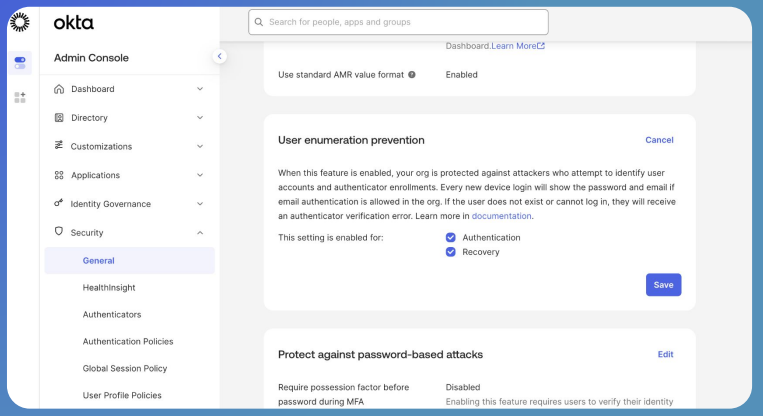
User Enumeration Prevention (UEP) Challenge

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

Enforce stronger factors (e.g., Okta Verify push, FastPass) for UEP challenges. This reduces disclosure of user information and streamline passwordless flows.

Learn more

OIE



User Enumeration Prevention (UEP) Challenge

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

Identity Management

General Availability

Approver UX Enhancements

Available in: Access Governance || Supported in: FedRAMP Moderate/High/DOD IL4

Upgrades to the approver user experience across Okta Access Requests app, Slack, and Email.

Classic OIE

Entitlements onboarding tools and experience

Available in: OIG Access Governance || Supported in: FedRAMP Moderate/High/DOD IL4

End to end onboarding experience for Governance Engine, allowing admins to leverage existing group configurations to setup entitlement policies and bundles

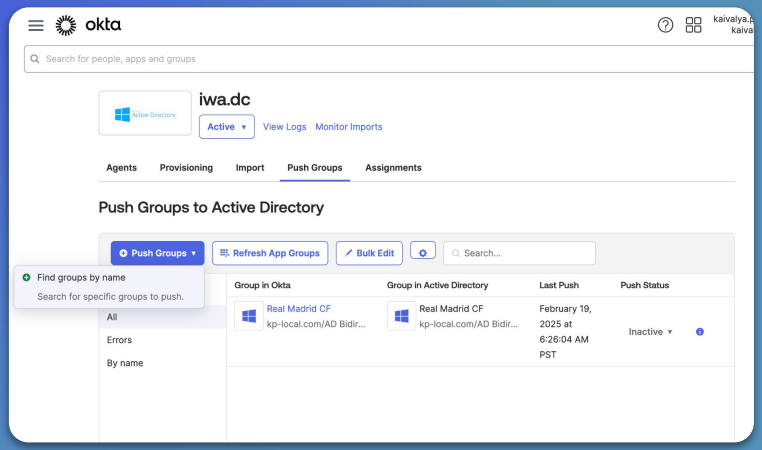
Classic OIE

Group Push APIs

Available in: Lifecycle Management || Authorized in: FedRAMP Moderate/High/DOD IL4

Provision groups to supported applications at scale using public APIs for configuring group push.

Classic OIE



Group Push APIs

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

okta

Identity Management

General Availability

OIN Apps for Entitlement Management (Oracle Cloud SCM, Oracle IAM, SAP Analytics)

Available in: LCM and OIG

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

Learn more

Classic OIE

Resource Collections

Available in: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

A package of all the resources and access that a user needs to perform a role or project

Learn more

Classic OIE

Secure Partner Access for Workforce

Available in: SPA || Authorized in: FedRAMP Moderate/High/DOD IL4

Secure Partner Access enables secure and efficient collaboration with supply chain and distribution partners. GA focus: scalability and security

Learn more

OIE

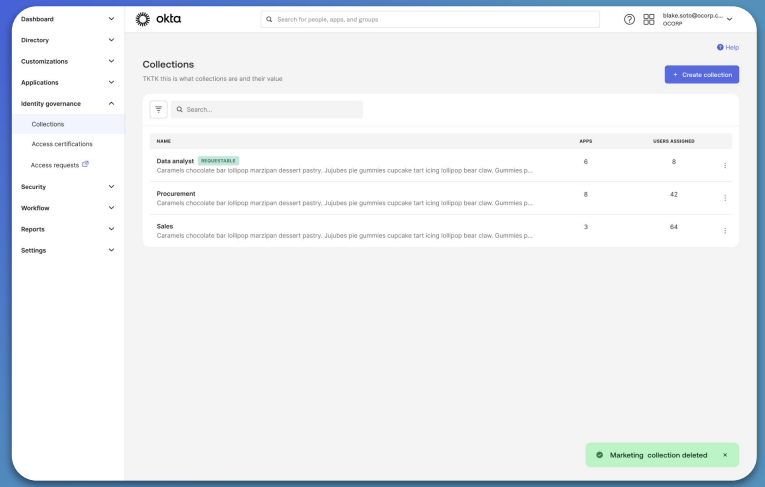
Support for additional attributes in Office 365

Available in: UD || Authorized in: FedRAMP Moderate/High/DOD IL4

Okta is enhancing it's Microsoft Office 365 Profile Sync provisioning by adding support for more additional attributes accessible through Microsoft Graph API.

Learn more

Classic OIE



Resource Collections

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

Identity Management

General Availability

Terraform Provider for OIG

Available in: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

Integrate OIG APIs into the Okta Terraform provider, allowing customers to maintain governance and resource configurations using Terraform.

Classic
OIE

Upgrading LDAPi to OIDC

Available in: UD || Authorized in: FedRAMP Moderate/High/DOD IL4

LDAPi is shifting from a directory integration to an App Instance model.

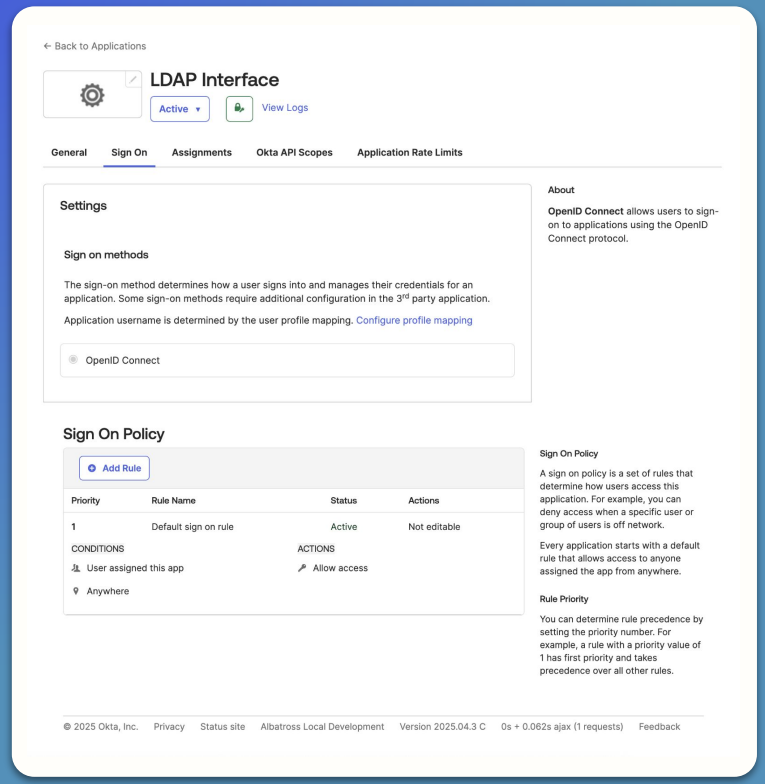
OIE

Workday Entitlement Management

Available in: LCM and OIG

Govern access to Workday User-based Security Groups with Workday OIN application. Import Groups as Entitlements for assignment, SOD evaluation, and access reviews.

Classic
OIE



Upgrading LDAPi to OIDC

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

Identity Management

Early Access

Anything-as-a-Source (XaaS) - Support for Groups

Available in: LCM || Authorized in: FedRAMP Moderate/High/DOD IL4

Now manage groups and group memberships with Anything-as-a-Source that enables teams to create and manage identities in Okta from any source.

Learn more

Classic OIE

Coupa - Schema Discovery

Available in: LCM

Enable discovering a broader set of user profile attributes from Coupa including Coupa default attributes and customer defined attributes.

Learn more

Classic OIE

Export OIG Reports as PDF

Available in: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

Export OIG reports as PDFs, allowing auditors to review compliance evidence like access certification campaign results in their preferred format.

Learn more

Classic OIE

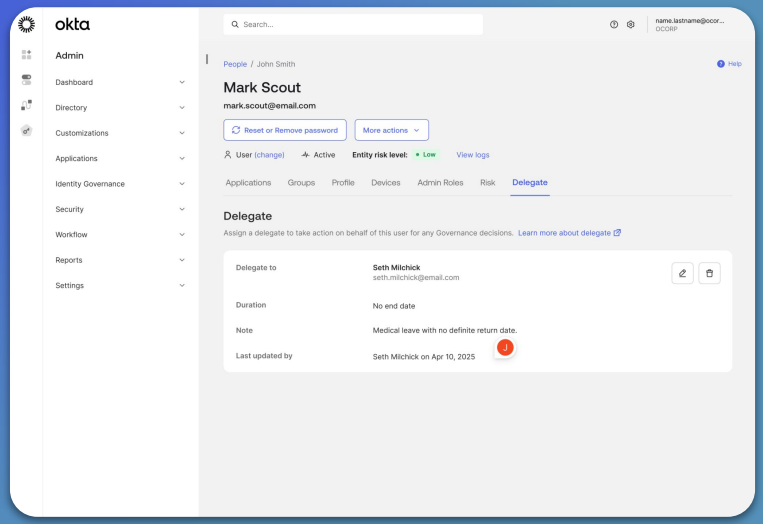
Governance Delegates

Feature of: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

Assign governance delegates to approve access requests and complete certifications reviews on behalf of other user, supporting temporary and long-term delegation needs.

Learn more

Classic OIE



Governance Delegates

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

okta

Identity Management

Early Access

Governance Labels

Available in: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

Admins can now add labels to resources in Okta for OIG use cases.

Classic OIE

Imports Visibility Enhancements

Available in: LCM || Authorized in: FedRAMP Moderate/High/DOD IL4

Provide customers with visibility into directory import progress to reduce delays and support tickets, increasing transparent and reliable identity syncing process.

Classic OIE

On-prem apps: JDBC connector

Available in: OPC (requires OIG)

Out-of-the-box connector for LCM provisioning and Entitlement Management for generic DBs via a "JDBC connector"

Learn more

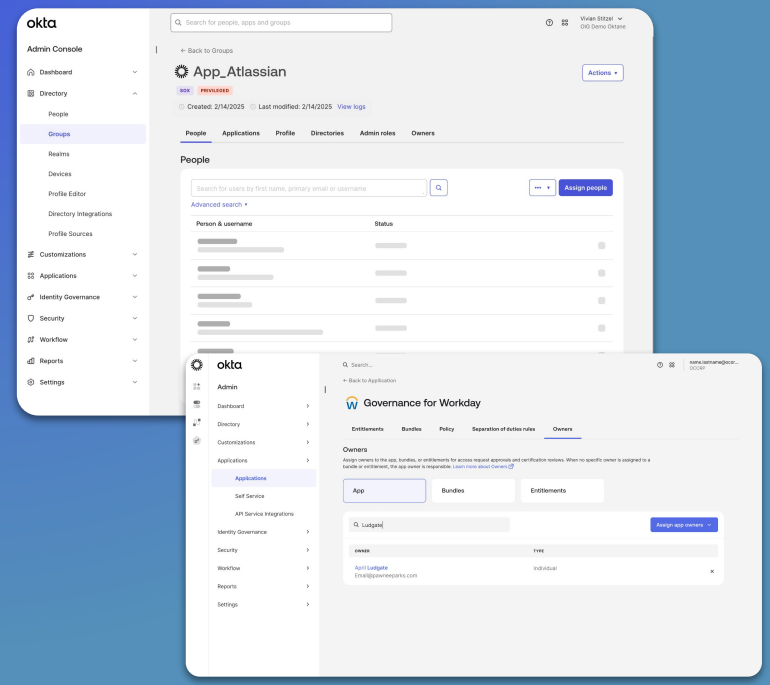
Classic OIE

Resource Owners for Governance

Available in: OIG || Supported in: FedRAMP Moderate/High/DOD IL4

Drive policies and business processes based on characteristics of the resource and simplify governance by assigning relevant tasks to owners accountable for the resource

Classic OIE



Resource Owners for Governance

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

okta

Privileged Access

General Availability

OP2 Cell (EMEA Preview Environment)

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

A new preview environment powered by the OP2 cell, offering the EMEA region the ability to test implementations and gain confidence before going live.

Classic OIE

Password Character Exclusions

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

Gives administrators control to prevent password rotation failures by configuring the system password generator to exclude specific symbols that are not supported by target systems.

Classic OIE

Secrets Search

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

Empowers end-users with a new search capability in the secrets web interface to quickly find secrets by name, folder, or description.

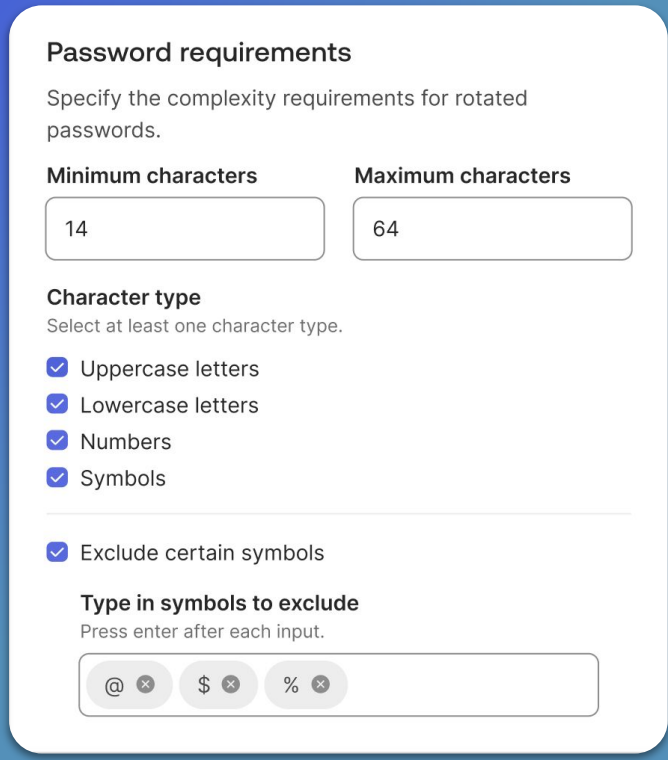
Classic OIE

Self-Service Password Generation

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

A new self-service feature that enables end-users to instantly generate and securely vault a new, strong, random password for an unmanaged account.

Classic OIE



Password Character Exclusions

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

okta

Privileged Access

Early Access

Active Directory Account Don't Rotate on Import

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

Account Rule setting to control whether accounts will have their password rotated when first discovered and imported into Okta Privileged Access.

Classic OIE

Active Directory Account Import Filtering

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

Ability to filter accounts within the Organizational Unit that match starts-with/ends-with/contains criteria or by Group.

Classic OIE

Active Directory Account RDP Click-to-Connect

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

Click-to-connect RDP with AD accounts to support password-less style SSO for RDP

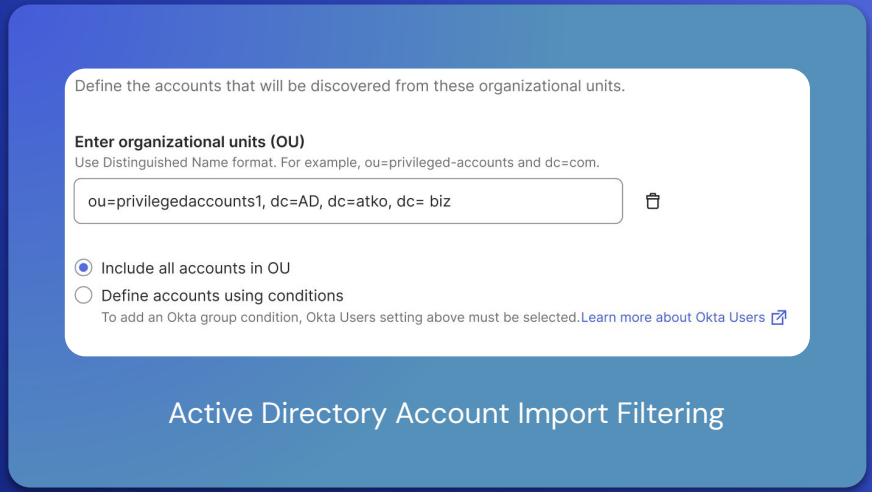
Classic OIE

Active Directory Account RDP Domain Controllers

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

Officially support the OPA Agent on Domain Controller hosts so RDP access to Domain Controllers can be protected with OPA

Classic OIE



Active Directory Account Import Filtering

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

Privileged Access

Early Access

Active Directory Account RDP Gateway Support

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

Ability to route AD RDP sessions through OPA Gateway

Classic OIE

Active Directory Account RDP Local Server Permission

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

Ability to give local server permissions to AD Accounts, or optionally do not give local server permissions for environments where that is controlled by something else such as Group Policy

Classic OIE

Active Directory Account Rotate Now for End Users

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

The ability for an end user who is granted permission the ability to trigger a rotation of an AD Account password.

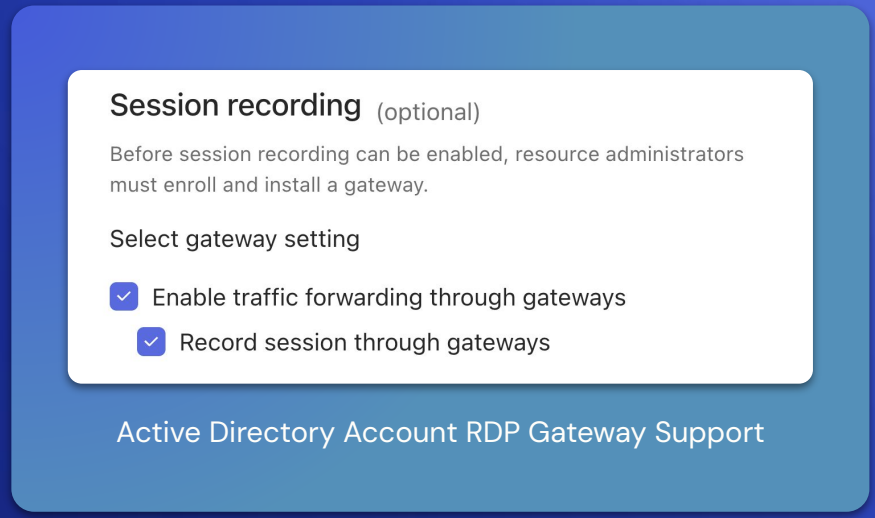
Classic OIE

Active Directory Privileged Account Password Vaulting

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

AD Account Rule setting which enables OPA-managed AD accounts to be Okta Users.

Classic OIE



Active Directory Account RDP Gateway Support

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

Platform Services

General Availability

Execution History Inspector

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Provides granular access to the full execution context of workflows, directly within the Workflows UI. This helps customers debug, troubleshoot errors, and better understand flow execution metrics.

Learn more

Classic OIE

Execution Log Streaming

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Improves Workflows observability by enabling customers to seamlessly transmit real-time execution logs from Okta Workflows directly to a downstream security information and event management (SIEM) or log parsing tool of choice. This helps customers to proactively monitor flow health, rapidly identify issues, and maintain long-term audit trails within their existing observability tools.

Learn more

Classic OIE

New Provisioning/ Entitlement Integrations

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

New LCM and OIG integrations: Splunk, Oracle HCM Cloud

Learn more

Classic OIE

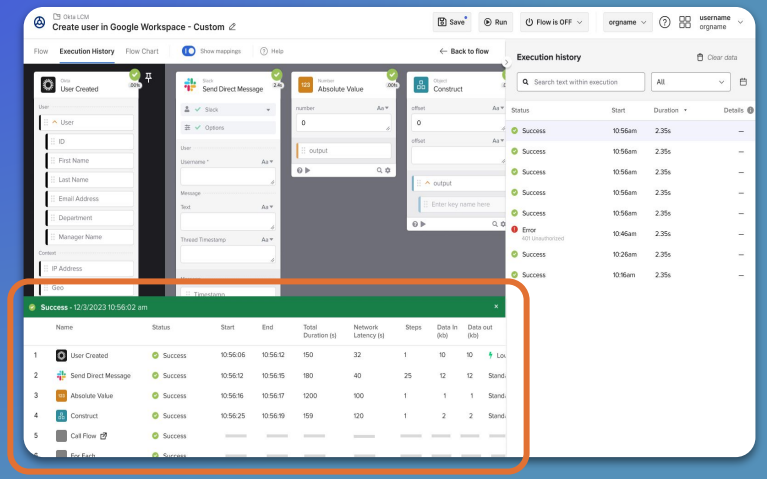
New Workflows Connectors

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

New Connectors: Okta ITP, Oracle IAM, Citrix Sharefile, Netskope

Learn more

Classic OIE



Workflows Execution History Inspector

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

okta

Platform Services

General Availability

Workflows Onboarding Flow

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Customized Workflows onboarding experience based on users' proficiency with automation, use cases and the apps they use.

Classic OIE

Okta admin app assignment

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

Customers will be able to assign an admin role without actually assigning the Okta admin app to delegated admins.

Learn more

Classic OIE

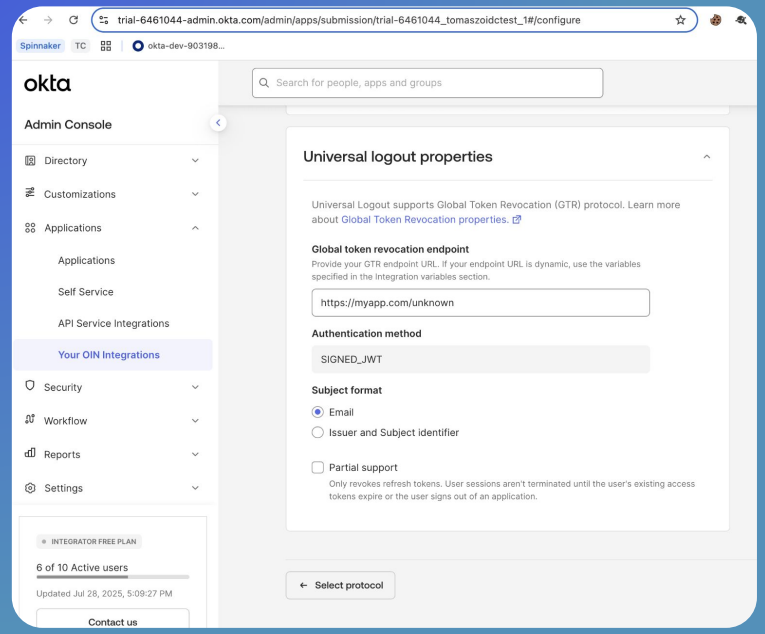
Simplifying Universal Logout (ULO) Integrations for ISVs

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

Enable Technology Integrators to configure, automatically test, submit, and manage Universal Logout integrations in the Admin Console using a template. Once submitted, the metadata will be automatically reflected in the Monolith.

Learn more

Classic OIE



Seamless ISV Experience for Universal Logout (ULO) Integrations

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

okta

Platform Services

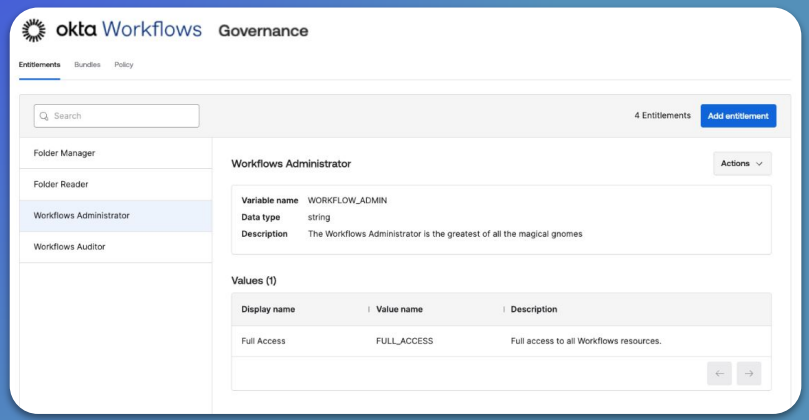
Early Access

Governance for Workflows

All Workflows + OIG-eligible customers || Workflows Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4, Okta Identity Governance Supported in: FedRAMP Moderate/High/DOD IL4

Leverage the power of OIG Access Requests and Certifications for Workflows roles and resources to streamline role assignments and grant time-bound access with customized access requests.

OIE



Governance for Workflows

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

Okta Learning

New Okta Badges

Sign in Your Users and Secure Sessions with Okta

Feature of: Okta Workforce Identity / Available in: Classic + OIE

Learn how the Okta Application Integration Wizard and Client SDKs make it easy to connect your custom applications, no matter the app type, authentication protocol, or deployment method.

Learn more

Classic OIE

Implement Passwordless Authentication

Feature of: Okta Workforce Identity / Available in: Classic + OIE

Gain the skills to configure and implement passwordless authentication, a modern approach that enhances security and improves the user experience.

Learn more

Classic OIE

Navigate ITP Architecture and Risk Models

Feature of: Okta Workforce Identity / Available in: Classic + OIE

Evaluate the Okta Identity Threat Protection (ITP) architecture and its various components, and assess an organization's security posture to mitigate risk.

Learn more

Classic OIE

Get Started with Continuous Session Evaluation

Feature of: Okta Workforce Identity / Available in: Classic + OIE

Build dynamic and adaptive access policies with this powerful feature that uses real-time signals to continuously evaluate session risk.

Learn more

Classic OIE



Grow with Okta Learning

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

okta

Developer Resources

Okta Workforce Identity

With Okta, you can build, integrate, and ship 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



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

okta

Okta Customer Identity Releases

Okta Customer Identity is dedicated to ensuring that security comes first when it comes to providing seamless digital experiences. It enables organizations to accelerate growth, navigate evolving security challenges, and protect customer and business data.

Learn more about our newest releases.

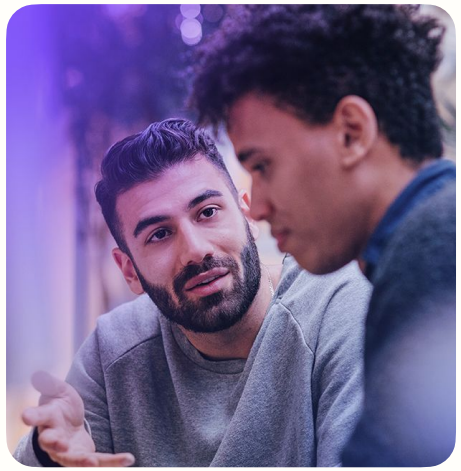


© Okta and/or its affiliates. All rights reserved.

okta

Okta Customer Identity is built for your identity needs today, and tomorrow

Okta Customer Identity powers thousands of customers



Built for IT and Security teams across industries



Designed to fuel seamless user experiences



Advanced security features to give you visibility to detect and respond to attacks



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

okta

Unify and Secure All Identities with Okta

Okta Platform

Okta Workforce Identity

Build secure access for your internal users with all the identity tools you need for end-to-end visibility, management, and governance.

- Posture Management
- Secure Partner Access
- PAM

Okta Customer Identity

Build seamless, secure experiences for all of your external identities whether its customers, partners, or suppliers.

- Advanced Directory Management
- Social Login
- Lifecycle Management

Shared Identity Platform

Single Sign-On, Passwordless, Adaptive MFA, Identity Threat Protection, Governance

Orchestration and Integration

- Automated Workflows
- API-driven Connectivity
- Seamless Application Access

Platform Scale and Reliability

- Zero planned downtime
- Self-healing nodes
- Granular rate limiting
- Redundant SaaS, PaaS, and IaaS
- Data Residency
- > 99.99% Uptime
- Built to Scale
- Multi-layer encryption architecture

Meet your compliance requirements

FR · CSA STAR CERTIFICATION · HIPAA COMPLIANT · PCI DSS COMPLIANT · Sarbanes-Oxley Compliant · GDPR · AICPA SOC · VPAT Compliant

Unify every identity into your identity security fabric

- Citizens
- Employees
- Contractors
- Consumers
- B2B Customers
- Partners
- ISVs
- AI agents

Early Access

Spotlight: Passkeys

Simple. Secure. Passwordless.

What is it?

Passkeys are a modern replacement for passwords that use public key cryptography for a phishing-resistant, user-friendly, and always-available authentication experience. Instead of remembering complex passwords, customers authenticate with a familiar biometric unlock like Face ID or Touch ID, or a device PIN.

Customer Challenge:

Passwords are a broken security model. They are the weakest link, vulnerable to phishing and other attacks, which drives up support costs and frustrates customers. Traditional MFA methods like SMS and email OTPs add friction without providing a truly phishing-resistant experience. Customers need a login that is both secure and seamless.

Why this matters

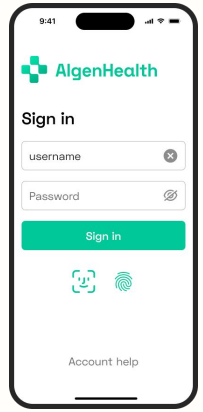
- **Simple & Fast:** Customers can log in with a simple biometric scan or PIN, leading to a higher login success rate and faster login times compared to passwords.
- **Phishing-Resistant:** Passkeys are cryptographically bound to a specific website, meaning they cannot be used on fake sites, making them inherently resistant to phishing attacks.
- **No Password to Steal:** With passkeys, there is no password to be stolen in a data breach or to be guessed by attackers, providing a more secure and resilient identity for the customer.

How to get it

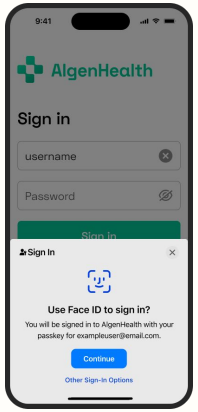
To get started today, all you need is Okta's MFA or AMFA SKU.

Learn More About Passkeys with Okta

- Passkey Management
- Help Documentation



Native app



Biometric sign in with passkey

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

General Availability In October

Announcement: Okta Identity Governance

Trust and control: A unified approach to customer identity

What is it?

Okta Identity Governance (OIG) for Okta Customer Identity (OCI) automates access policies and reviews to reduce privilege sprawl for external users. This helps with compliance and streamlines operations. A key part of this offering is Advanced Directory Management, which enables secure, delegated administration so external partners can manage their own users and access rights within a single governance framework.

Customer Challenge:

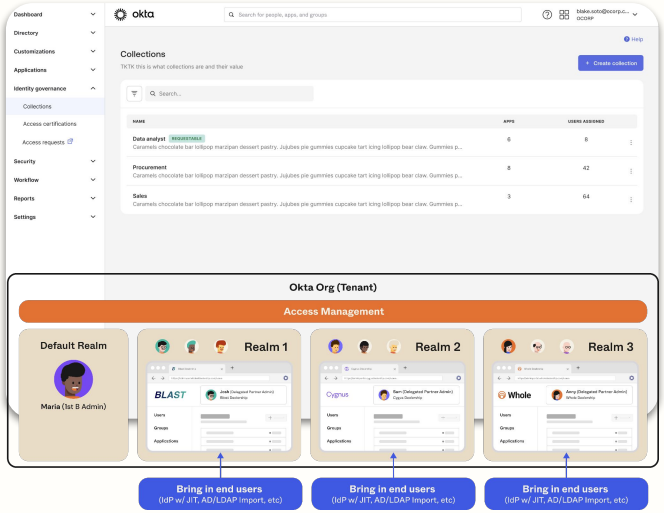
Customers today face significant challenges in managing the identity and access of their external users, such as partners and customers. They struggle with maintaining security and compliance, as manually managing access at scale leads to security gaps like privilege sprawl, which can be exploited by bad actors. Furthermore, the lack of a centralized, automated system makes it difficult to prove compliance during audits and creates an administrative burden for IT teams.

Why this matters

- **Reduces Security Risks:** It helps prevent privilege sprawl and unauthorized access by automating access policies and reviews, ensuring external users only have the permissions they need.
- **Improves Compliance:** It streamlines operations and provides an auditable trail of who has access to what, making it easier for organizations to demonstrate compliance with industry regulations.
- **Enables Business at Scale:** The inclusion of Advanced Directory Management allows for secure, delegated administration, which empowers partners and customers to manage their own users. This scales business operations without overwhelming central IT teams.

How to get it

Okta Identity Governance and Advanced Directory Management will be available as part of OIG for OCI SKU.



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

Okta Customer Identity

General Availability

Associated Domain Customizations

Available in: MFA SKUs || Authorized in: FedRAMP Moderate/High/DOD IL4

Customers can define 'well-known endpoints' for native passkey support on iOS, Android, and WebAuthN. Easier adoption of Passkeys through platform native integrations - enabling autofill and passkey prompt in app.

OIE

Augmenting appID context for OIDC and SAML applications

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

Enhances security by passing application details (ID, Name) to external Identity Providers (IdPs). This enables more granular security and policy decisions during Okta-initiated federation.

Classic

OIE

Breached Credentials Protection

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

Lets admin tailor user experiences and verify workflows using test accounts, improving both security and operational confidence.

Classic

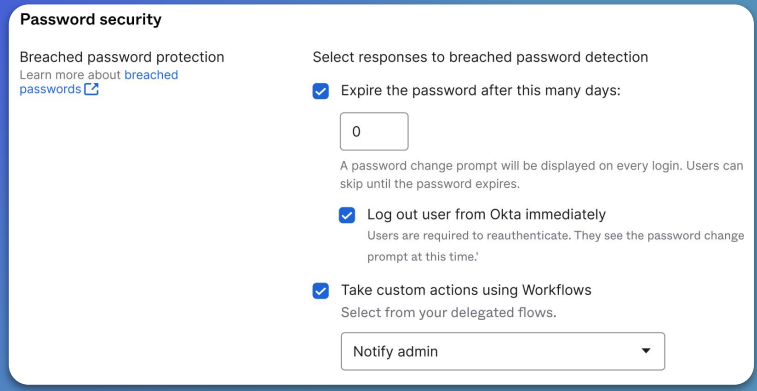
OIE

Cascading of the SLO Request to External IdP

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

Deliver increased security for Okta Customer Identity (formerly CIS) customers who have shared device use cases.

OIE



Breached Credentials Protection

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

Okta Customer Identity

General Availability

Enhanced Dynamic Network Zones - Residential Proxies

Available in: AMFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Enhance security with granular control within enhanced dynamic network zones, enabling organizations to block access from proxies, anonymizers, VPNs, and ToRs. Achieve greater control over network resources, better adhere to compliance standards, and stay resilient against unauthorized access and evolving threats.

Classic

OIE

Enrollment Policy Periods Grace Periods

Available in: MFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Encourages your customers to adopt new authenticators by giving them control over their enrollment timeline. This reduces support burden and prevents scenarios where users are blocked from accessing services.

OIE

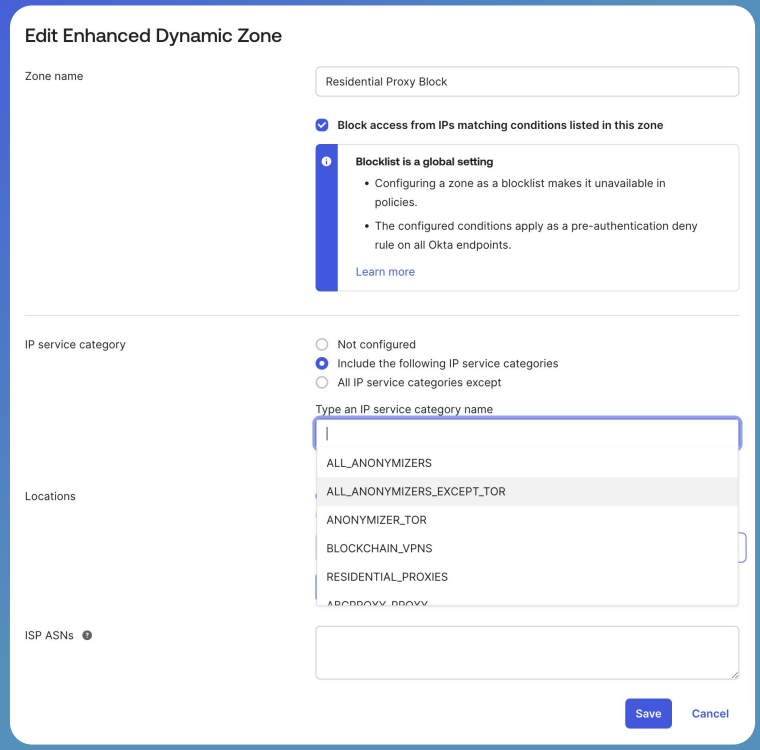
Execution History Inspector

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Quickly and easily troubleshoot issues with your customer-facing workflows. This feature gives you a single view of recent execution history for each workflow within the UI. You can triage errors, view successes, and understand why a flow might be performing slower than expected. The inspector provides detailed metrics on each step, empowering you to address performance concerns without needing to file a support ticket.

Classic

OIE



Enhanced Dynamic Network Zones - Residential Proxies

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

Okta Customer Identity

General Availability

Execution Log Streaming

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Get real-time visibility into the performance of your customer identity processes. This feature allows you to stream execution logs to your preferred monitoring and analytics tools (like Splunk, Sumo Logic, or Datadog). This enables you to troubleshoot errors, analyze user behavior, and gain a holistic view of your customer identity system's activity to inform future design decisions.

Classic OIE

Group Push APIs

Available in: Lifecycle Management || Authorized in: FedRAMP Moderate/High/DOD IL4

Effortlessly synchronize customer groups and access entitlements to your supported applications at scale using public APIs.

Classic OIE

New Provisioning / Entitlement Integrations

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Integrates with more HR systems and popular applications (Oracle HCM Cloud) to manage users, groups, and entitlements.

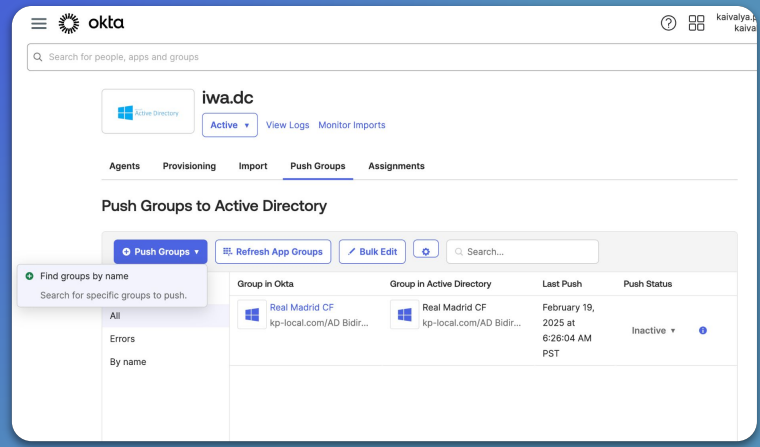
Classic OIE

New Workflow Connectors

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Integrates with more Okta APIs and popular applications (Okta ITP, Oracle IAM, Citrix Sharefile, Netskope) to manager users and groups.

Classic OIE



Group Push APIs

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

okta

Okta Customer Identity

General Availability

Okta Admin App Assignment

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

Least privileged access. Skip assigning the admin app if your organization has users who don't need access, such as business partners, vendors who won't be managing other users.

Classic OIE

Seamless ISV Experience for Universal Logout (UL) Integrations

Available in: AMFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Simplifies the process for technology integrators to submit Universal Logout integrations to the Okta Integration Network (OIN). The improved workflow allows for seamless testing and validation, significantly reducing the time required to publish new integrations.

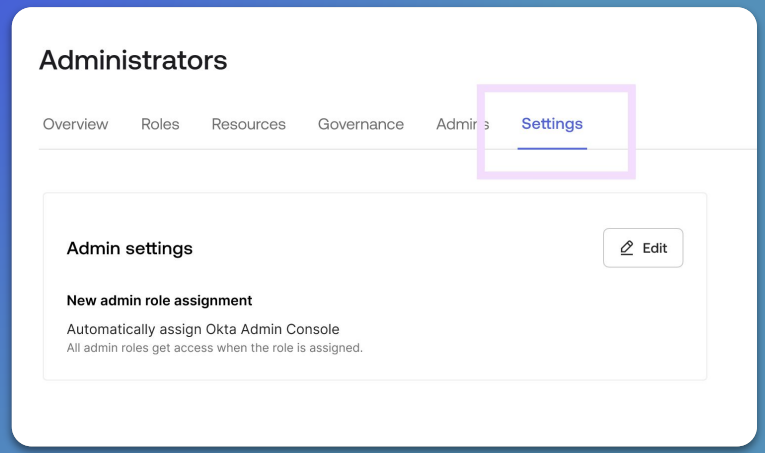
Classic OIE

Unified Platform look and feel - UI Shell & App Switcher

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

Provide ease of use with consistent side and top navigation across Okta first party apps. Provide admins with seamless inter-app switching experience and single placehouse all relevant Okta apps.

Classic OIE



Okta Admin App Assignment

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

okta

Okta Customer Identity

General Availability

Upgrading LDAPi to OIDC

Available in: Universal Directory || Authorized in: FedRAMP Moderate/High/DOD IL4

Allows you to set up multiple LDAPi instances in a single organization. This provides the flexibility to create specific sign-on policies for each instance, moving beyond generic, organization-wide rules.

OIE

Workflows Adoption through improved usability

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Provide the ability to minimize flow cards, giving you a better overview of your entire flow and reducing visual clutter.

Classic

OIE

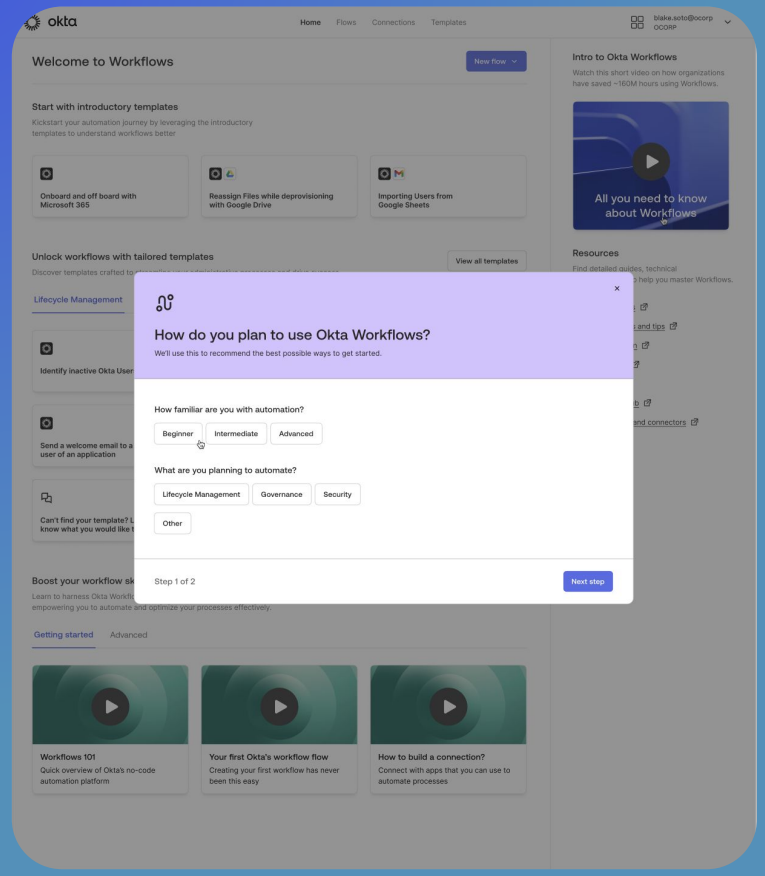
Workflows Onboarding Flow

Available in: Workflows || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Provides a tailored onboarding experience for new Workflows users. The flow helps determine user proficiency, use cases, and app preferences to customize the user's initial experience with the platform.

Classic

OIE



Workflows Onboarding Flow

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

Okta Customer Identity

Early Access

Authenticator Rollout Insights

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

Provides enhanced visibility into your customers' authentication behavior through the MFA Activity Report. The report now offers deeper insights into FastPass usage, including details on device type, login method, and management and registration status.

OIE

Custom AAGUID

Available in: MFA/AMFA SKU || Supported in: FedRAMP Moderate/High/DOD IL4

Enhances security by allowing you to control which authenticators and password managers your customers can use. You can limit end-user authenticator enrollment to only approved authenticators, ensuring a higher level of trust.

OIE

Device Signal Collection Policy

Available in: AMFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Gives administrators more control over device signal collection. For example, admins can now configure Okta Verify to not collect certain data, such as the username, providing greater flexibility beyond the default settings.

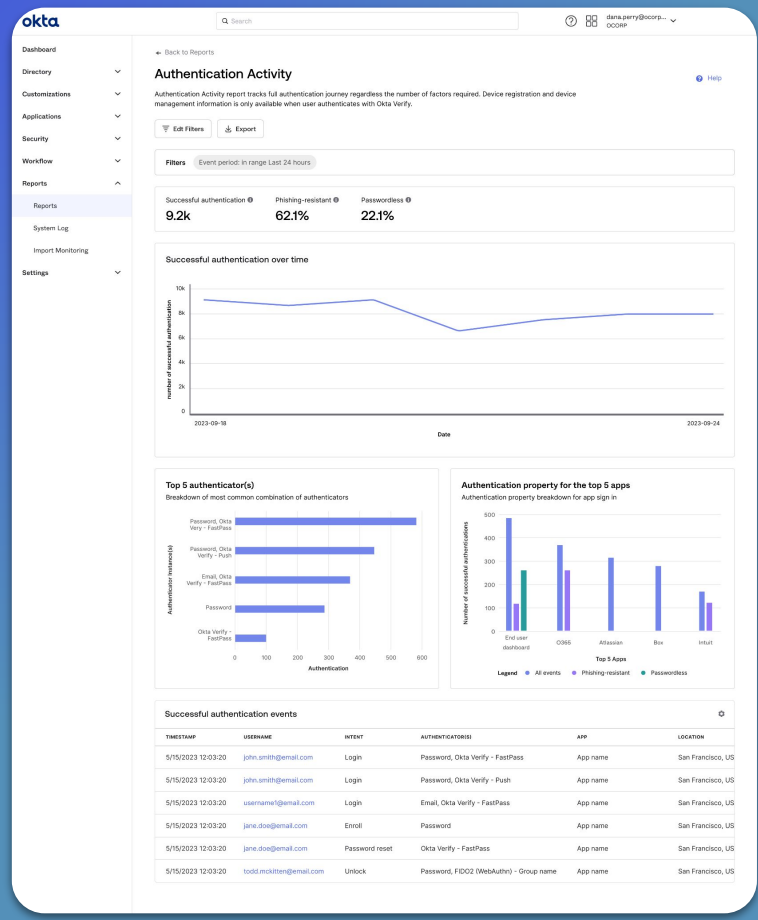
OIE

Enhanced Credential Security

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

Strengthens password and related security measures with an added layer of protection, helping customers transition to a passwordless environment.

OIE



Authenticator Rollout Insights

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

Okta Customer Identity

Early Access

Enhanced Login Page Customizations (Design Tokens)

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

Expands the options for customizing the look and feel of your login pages. This feature provides a user-friendly interface to configure the Sign-In Widget using a wider range of design tokens, allowing you to create a more on-brand experience for your customers.

OIE

ID Verification Additional Biographical Attributes

Available in: MFA/AMFA SKU

Enhances ID verification by allowing you to collect and map additional biographical information during the process, such as date of birth, email, and phone number. This provides richer data for identity validation.

OIE

Imports Visibility Enhancements

Available in: All SKUs || Supported in: FedRAMP Moderate/High/DOD IL4

Gain increased visibility into the progress and stages of imports from on-prem directories and applications.

Classic

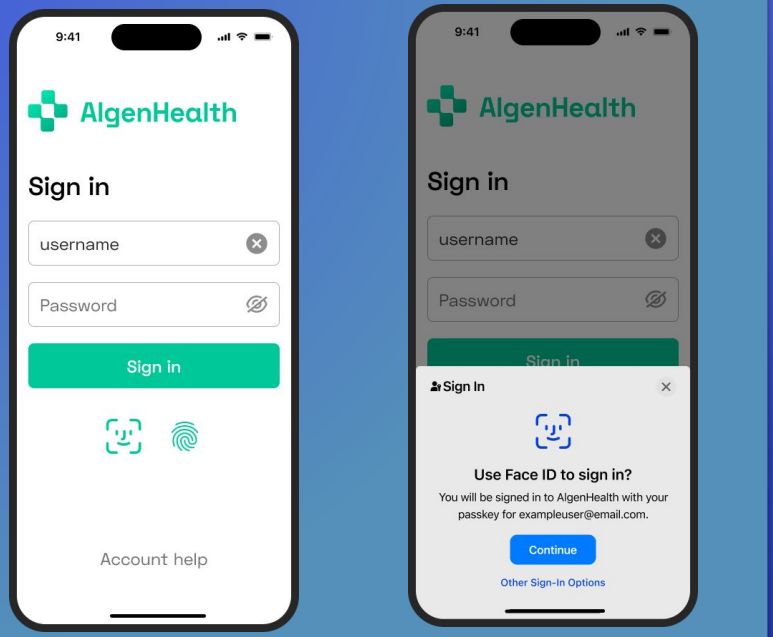
OIE

Native Passkey Support

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

Enables a secure and user-friendly experience by allowing seamless passkey authentication directly within native mobile apps, bypassing the need for a web browser.

OIE



Native app

Biometric sign in with passkey

Native Passkey Support

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

okta

Okta Customer Identity

Early Access

OAuth for Email Provider

Available in: All SKUs

Strengthens the security of your customer communications. Customers using an Email Provider for their own SMTP can now connect with OAuth authentication, replacing basic authentication for a more secure connection.

Classic OIE

OIDC Token Encryption

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

Secures the transmission of sensitive user data to trusted resources. This feature prevents interception by unauthorized parties and malicious attackers, ensuring your customers' information remains confidential.

Classic OIE

Okta Account Management Policy support for Password Expiry

Available in: MFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Provides greater control over your customers' password security. This feature expands the Okta Account Management Policy (OAMP) to include password expiration, allowing you to enforce stronger security requirements when a password expires or is compromised.

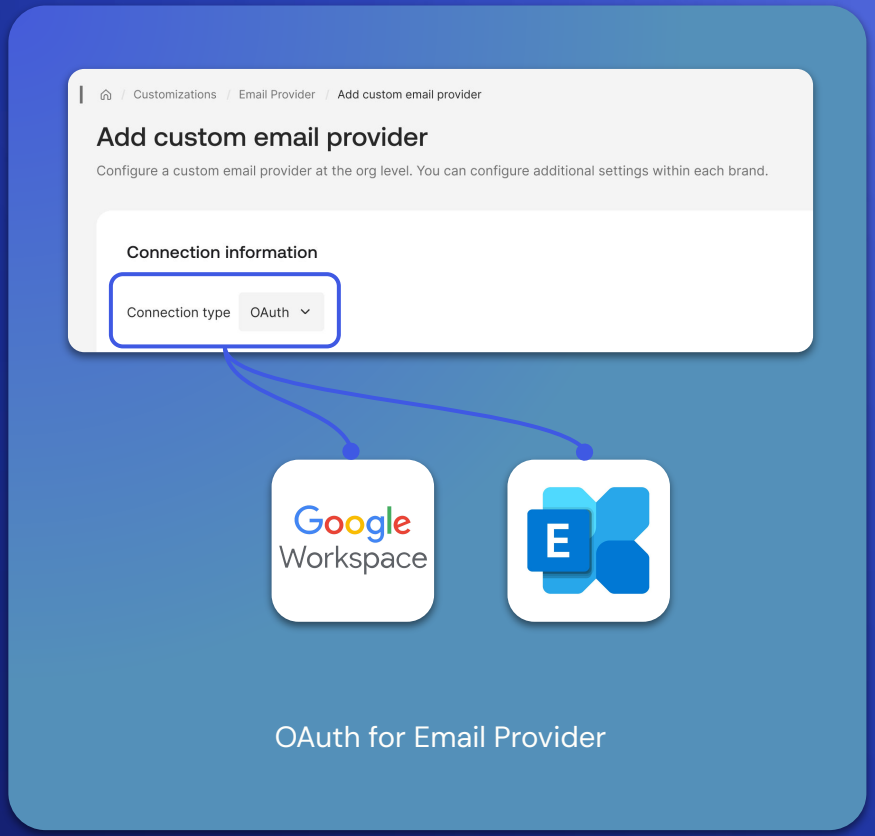
OIE

OV Inline Enrollment Per Device

Available in: All SKUs || Supported in: FedRAMP Moderate/High/DOD IL4

Improves the user experience by allowing customers to enroll Okta Verify (OV) on new devices without being blocked from signing in. This supports multi-device use cases and helps drive OV adoption.

OIE



OAuth for Email Provider

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

Okta Customer Identity

Early Access

Overlapping IdP Signing Certificate

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

Eliminates downtime and streamlines the process of updating Identity Provider (IdP) certificates. This improves the reliability and security of your federated authentication flows with minimal operational effort.

Classic

OIE

Preferred Factor - Remember last used factor

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

Enhances the customer login experience by remembering and automatically prompting their most recently used authentication method. Administrators have the flexibility to customize which factors are remembered and when, allowing for a more secure and tailored experience.

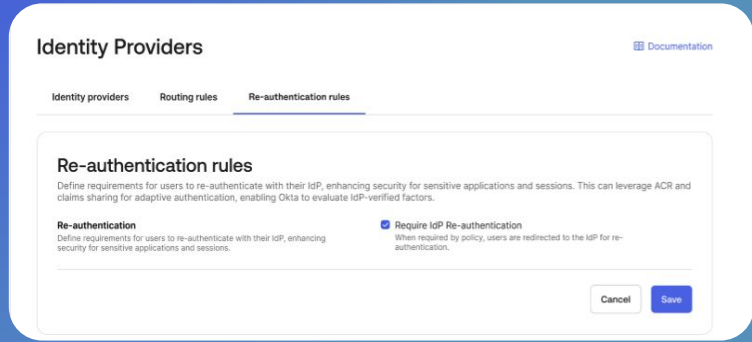
OIE

Re-authentication to IdPs

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

Enhances both security and user experience by keeping authentication centralized at the Identity Provider. This feature forces a fresh login at the IdP, preventing reliance on long-lived sessions and eliminating the need for users to re-enroll factors in Okta.

OIE



Re-authentication to IdPs

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

Okta Customer Identity

Early Access

Support for Higher Assurance Certificates from Certificate Authorities

Available in: MFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Expands support for Custom Domain flows by including higher assurance certificates (SHA-384 and SHA-512). This provides a more secure connection and builds greater trust with your customers.

OIE

User Enumeration Prevention choose challenge authenticator

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

Improves security for passwordless authentication by preventing user disclosure when a password is not being used. This feature allows administrators to maintain strong security while providing a seamless, passwordless experience.

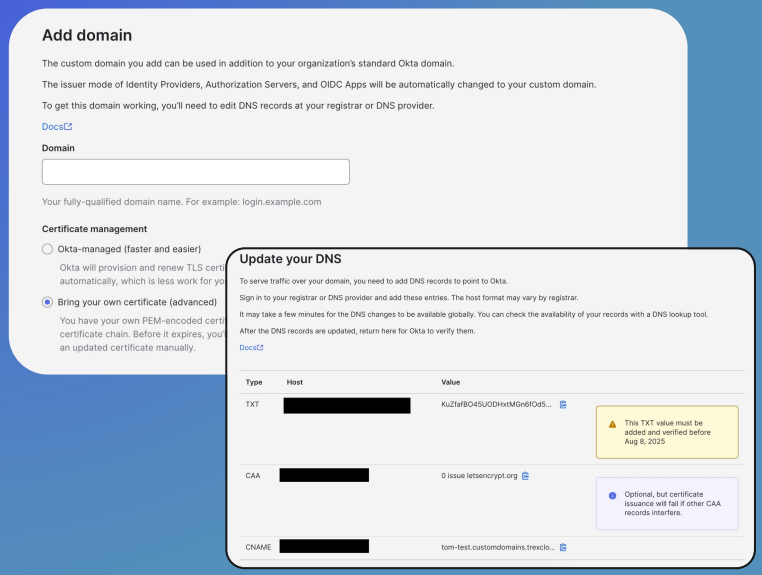
OIE

Universal Logout Support for OCI apps

Available in: All SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Allows app developers to easily implement Universal Logout for their Okta Customer Identity (OCI) applications with zero development effort.

OIE



Support for Higher Assurance Certificates from Certificate Authorities

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


okta