



Launch Week Release Overview

for Early Access & General Availability (October 2025 – March 2026)

US Public Sector

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

Launch Week Webpage

Dive further into the latest innovations, watch the replay from Showcase, and find resources to learn more [here](#).

Connect with the Sales team [here](#).

Launch Week Webinar

Get a sneak peek of upcoming product releases.

Register for the Okta product webinars [here](#).



Welcome to the US Public Sector Release Overview

Q4 2025–Q1 2026

Welcome back to Okta's first Release Overview of 2026 for US Public Sector. Our innovations are designed to help Okta Administrators that work for or service the US Public Sector, or have certain compliance requirements, build a comprehensive identity security fabric—a modern architecture to protect every identity, use case, and resource.

Explore how our latest updates for the Okta platform enhances missions by bringing AI agents, customers, and partners into your identity security fabric.



Navigating the overview

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

Okta Workforce Identity

- [Okta Workforce Identity overview](#)
- [Spotlights](#)
- [Release overviews](#)

Okta Customer Identity

- [Okta Customer Identity overview](#)
- [Spotlights](#)
- [Release overviews](#)



Spotlight: Okta for AI Agents

Your AI strategy starts with identity

What is it?

AI agents are your newest digital workforce, but right now, most are operating in the shadows.

Okta for AI Agents provides an identity layer for the agentic era. We bring every AI agent into your identity security fabric—allowing you to see, manage, and govern AI at scale. Don't let your AI strategy become your greatest security liability.

Customer Challenge:

- AI agents are being deployed quickly and in silos within organizations – lacking a single source of truth for visibility and permissions.
- These agents operate quickly, on behalf of users or autonomously, and often are over privileged.
- Many governance and security tools can't keep pace with the real-time, cross-app nature of AI agents.

Why this matters

AI agents don't behave like human users, and they don't fit neatly into traditional identity models. That creates big security gaps causing:

- **Increased risk:** Unintentional data exposure triggers critical privacy and security breaches. Lack of audit trails can comprise compliance & audit goals.
- **Widespread credential sprawl:** AI agents often become "super admins" by default. They rely on risky, long-lived tokens that create a massive and indefensible credential attack surface.
- **Widening governance gap:** While 91% of organizations use AI, 44% have no governance in place. Human oversight can't keep up with "agent speed," which stalls innovation and locks away value.*

* Okta, AI at Work 2025: Securing the AI-powered workforce (Aug. 12, 2025).

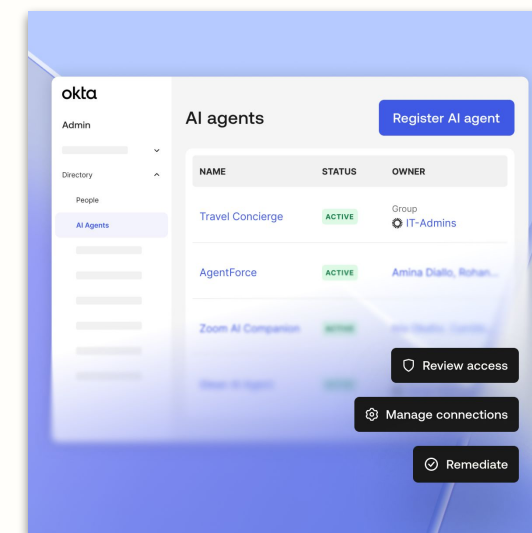
How to get it

Okta for AI Agents is an Early Access (EA) bundle which includes components that are **currently not available in our FedRAMP Moderate, FedRAMP High, and DoD IL4 environments.**

Okta for AI Agents SKU: Includes the power of the Okta Platform for AI Agents.

Available on the Okta Identity Engine (OIE) platform only

To learn more, read [the blog](#).



Spotlight: Okta for US Military (IL5+NSS Readiness)

Mission-critical identity at the speed of relevance

What is it?

Okta for US Military, Okta's U.S. Department of War (DoW) Provisional Authorization (PA), is expected to be renewed by the U.S. Defense Information Systems Agency (DISA) at Impact Level 5 (IL5).

This anticipated PA will allow Okta to service workloads and applications up to IL5 in our Okta for US Military environment.

Customer Challenge:

Legacy and on-prem solutions that can no longer effectively support critical mission functions or equip the nation's warfighters with the best technology.

Why this matters

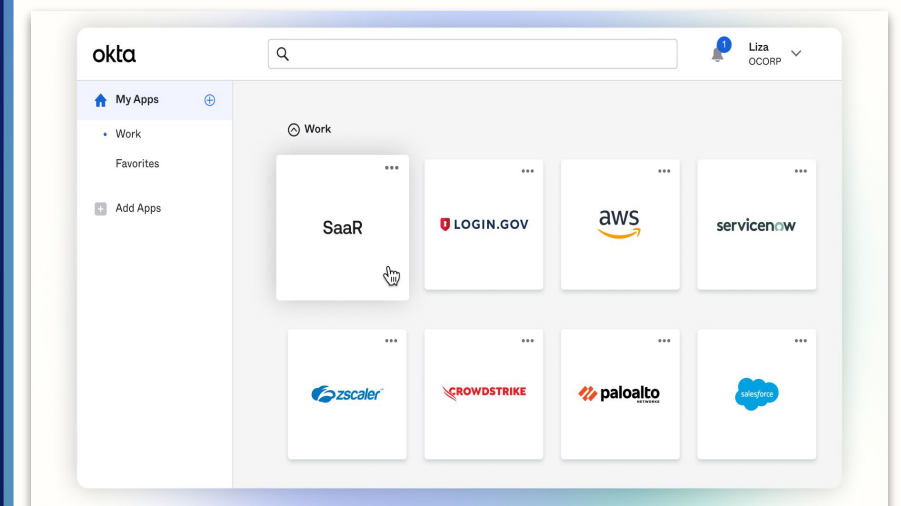
- Okta will service nonpublic, unclassified National Security Systems (NSS) data or nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, assets, or individuals.
- With a single cloud for both IL4 and IL5 applications and workloads, Okta will eliminate the overhead of managing fragmented identity stacks, shifting the focus from infrastructure to innovation.
- Okta will combine IL5 data handling with attribute-level workflows, eliminating privilege creep and fulfilling core Zero Trust mandates.

How to get it

Okta's PA renewal is expected to be available CY26 Q2.

Cell Add-on: Okta for US Military (existing SKU) and the existing [product availability and assessment](#) will not change.

[See how an IL4 identity provider successfully services IL5 environments.](#)



Spotlight: Identity Security Fabric Use Cases

Threads weave into the fabric 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 today's most critical security challenges. Together, Okta delivers end-to-end identity security across all identity types, use cases, and resources, including:

- Secure hybrid & on-premises environments (GA*)
- Enable security-driven governance (GA)
- Secure workforce onboarding (GA)

Customer Challenge:

- **Complex hybrid environments** expand the attack surface of organizations, fragmented security tools limit visibility and control.
- **Legacy governance** creates silos, causing reactive fixes, blind approvals, and poor visibility.
- **Identity security gaps during onboarding** can quickly escalate into breaches and operational risk, turning onboarding into a threat vector.

* Certain features are in EA

Why this matters

Secure hybrid & on-premises environments

- Enhance your hybrid environment's security posture
- Centralize management for on-prem resources
- Accelerate your journey to the cloud

Enable security-driven governance

- Triage security incidents by reviewing access immediately after a high-risk event
- Prevent toxic combinations of access in real-time
- Help ensure users have no permanent permissions to sensitive resources

Secure workforce onboarding

- Establish trust from the first interaction
- Provision devices & authenticators securely
- Govern the provisioning of birthright apps

How to get it

Available as part of Okta Workforce Identity Cloud. An identity security fabric is Okta's perspective on a modern approach to identity architecture. It's not a single product you can buy.

Resources: [Landing page](#), [Click-through demo](#), Secure hybrid & on-premises environments [blog](#), Secure workforce onboarding [blog](#) and [demo](#).



Spotlight: Device-Bound Single Sign-On

An easier, more secure way for your workforce to get where they need to go, starting from device login

What is it?

Device-Bound Single Sign-On (SSO) initiates a hardware-protected SSO session for seamless access to your downstream apps after device login on macOS and Windows devices with Okta Device Access. This feature stops Okta session replay and delivers a streamlined login experience.

Customer Challenge:

Employees require secure access to the apps and tools they depend on, at any time and from any location. However, one thing is clear: traditional SSO and MFA are not enough. Not only are users frustrated with repeated authentication prompts, but these standard defenses may also fail to protect against more sophisticated identity-based attacks, such as session hijacking.

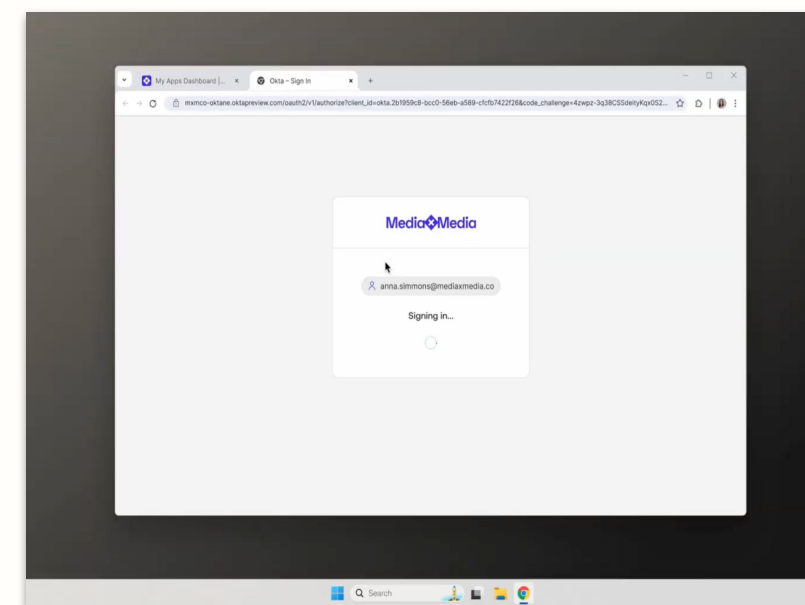
Why this matters

- **Enhanced security posture:** Enable a hardware-protected and cryptographically secure session, which helps make identity-based attacks much less possible. This is because access is tied not only to the user but also to their device, so if a threat actor is able to steal an active Okta SSO session, they won't be able to leverage it from a different device.
- **Seamless access to downstream apps:** Leverage a successfully completed device login with Okta Device Access to gain access to downstream resources requiring the same level of security assurance. This feature decreases how often you are asked to authenticate, reducing the entry points for threat actors.

How to get it

Device-Bound SSO is a new feature of Okta Device Access. To leverage this feature, both the Device Access and Adaptive MFA products are required.

To learn more, [read the blog](#).



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 Q4 2025 and Q1 2026.

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.

okta

Access Management

General Availability

Device Assurance Dynamic OS Version Policy Option

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

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

Grace Period for Device Assurance Compliance

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

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

[Learn more](#)

OIE

Device Posture Provider

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

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

[Learn more](#)

OIE

Platform SSO support in macOS Setup Assistant

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

Deliver an enhanced device onboarding experience that automatically creates a local macOS account enrolled in Desktop Password Sync, leveraging Okta user profile attributes and credentials.

[Learn more](#)

OIE



Single Sign-On for Mac

With single sign-on, you only have to sign in with MediaXMedia once to securely access your Mac and apps.



Automatically Registered

Your Mac is registered to use single sign-on with MediaXMedia.



Passwords Sync

Your Mac password automatically syncs with your MediaXMedia password.



Access to Apps and Data

Use your MediaXMedia password to access your organization's apps, personal data, and this Mac.

Continue

Platform SSO support in macOS Setup Assistant



Access Management

General Availability

Custom Admin permissions for Access Policies

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

Custom admin permissions that enable consistent, granular control over access policies (authentication, session, and account management policies).

[Learn more](#)

OIE

Password Complexity OEL (formerly Enhanced Credential Security)

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

Use Okta Expression Language (OEL) to define custom password complexity requirements for end users creating passwords.

[Learn more](#)

OIE

OAG automation APIs

Feature of: Okta Access Gateway || Supported in: FedRAMP Moderate/High/DOD IL4

Customers can now automate apps and IDP configurations on Okta Access Gateway (OAG) via ReST API calls.

[Learn more](#)

Classic

OIE

Unified Claims Generation for Okta Federated Apps

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

Enable best-in class, personalized experiences for federated apps with a streamlined interface for configuring SAML attributes and OIDC claims types.

[Learn more](#)

OIE

Block restricted content

☒ Use an OEL statement to block restricted content

Block passwords that match the Okta Expression Language statement below. Reference the password as 'password.value'.

```
password.value.contains("blockedword") OR password.value.contains("blockedword2")
```

958 characters remaining

Password

.....

👁

Passwords can't include restricted content. Please create another password or contact your admin.

Password Complexity Okta Expression Language (OEL)



Access Management

General Availability

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

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

[Learn more](#)

OIE

Admin-selected Factor for 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 to reduce disclosure of user information and streamline passwordless flows.

[Learn more](#)

OIE

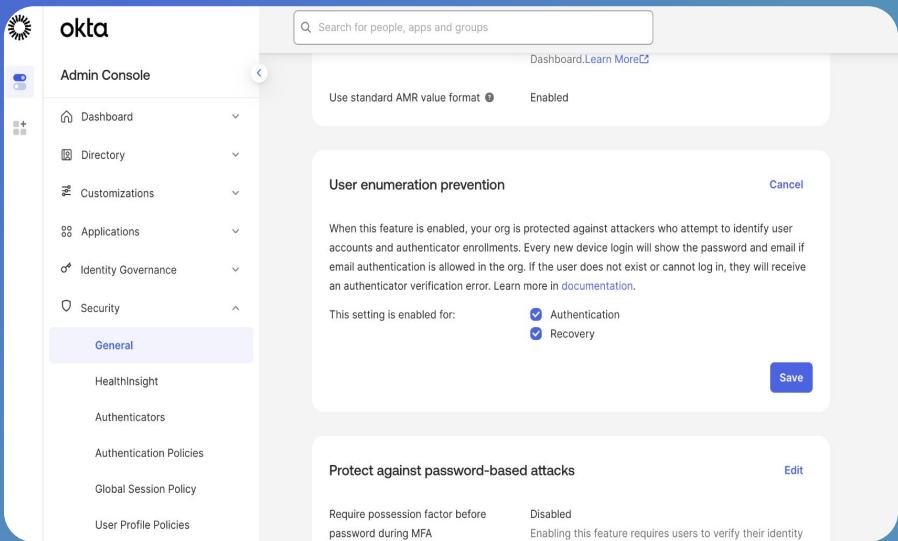
ID Verification Additional Biographical Attributes

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

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



User Enumeration Prevention (UEP) Challenge



Access Management

General Availability

Support for Higher Assurance Certificates from Certificate Authorities

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

Use Okta Custom Domains with higher security certificate encryption options (SHA-384 and SHA-512) to enable greater assurance of authenticity and integrity.

[Learn more](#)

OIE

Network Restrictions on Token Endpoint

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

Enhance security by allowlisting network zones to restrict token requests to trusted IPs and defend against replay attacks, token theft, DoS, and rate limit abuse.

[Learn more](#)

OIE

New EDNZ IP categories for Residential Proxies and Blockchain VPNs

Feature of: 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, etc.

[Learn more](#)

Classic

OIE

Custom Admin Roles for Identity Threat Protection

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Enforce least-privilege access with precise, scoped admin permissions for managing ITP configurations, such as who can manage user sessions, configure risk policies, or set up Shared Signals Framework (SSF) integrations.

[Learn more](#)

OIE

Edit Enhanced Dynamic Zone

Zone name

Residential Proxy Block

☒

Block access from IPs matching 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](#)

IP service category

☐ Not configured

☒ Include the following IP service categories

☐ All IP service categories except

Type an IP service category name

ALL_ANONYMIZERS

ALL_ANONYMIZERS_EXCEPT_TOR

ANONYMIZER_TOR

BLOCKCHAIN_VPNs

RESIDENTIAL_PROXIES

ABUSIVE_PROXY

Locations

ISP ASNs

Save

Cancel

New EDNZ IP categories for Residential Proxies and Blockchain VPNs



Access Management

General Availability

Identity Threat Protection (ITP) Landing Page

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

A converged experience to easily navigate to all features in ITP. Easily discover new features, understand configurations, and tune controls to streamline your deployment and strengthen security posture.

[Learn more](#)

OIE

Suspicious Login From An IP Flagged By FastPass

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

This detection indicates that a sign-in event occurred from an IP address that Okta FastPass flagged in a phishing event.

[Learn more](#)

OIE

Suspicious Login From an IP Flagged In Credential Based Attack

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

This detection indicates that a successful sign-in event occurred from an IP address where multiple sign-in failures also occurred.

[Learn more](#)

OIE

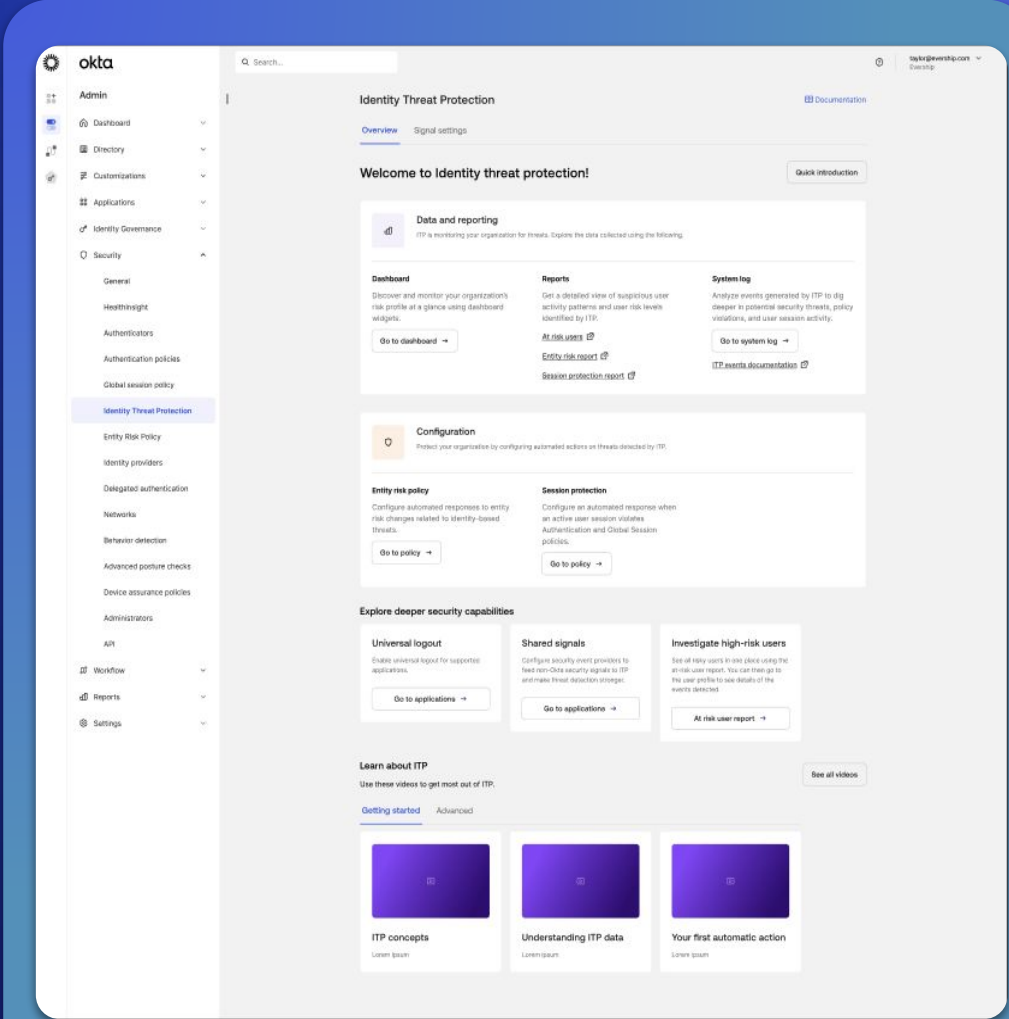
Breached Credential Detected

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

This detection indicates that a username–password combination in your org appears in a third-party list of public data breaches.

[Learn more](#)

OIE



ITP Landing Page



Access Management

General Availability

Bring Your Own (BYO) Custom IDV

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

Ability to bring your own Identity Verification (IDV) vendor or custom in-house solution to Okta's IDV offering across onboarding, authentication, account recovery, and help desk support.

[Learn more](#)

OIE

Native Passkey Support

Feature of: MFA / AMFA || Authorized in: FedRAMP Moderate

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

[Learn more](#)

OIE

Passkey for Multiple Subdomains

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

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

[Learn more](#)

OIE

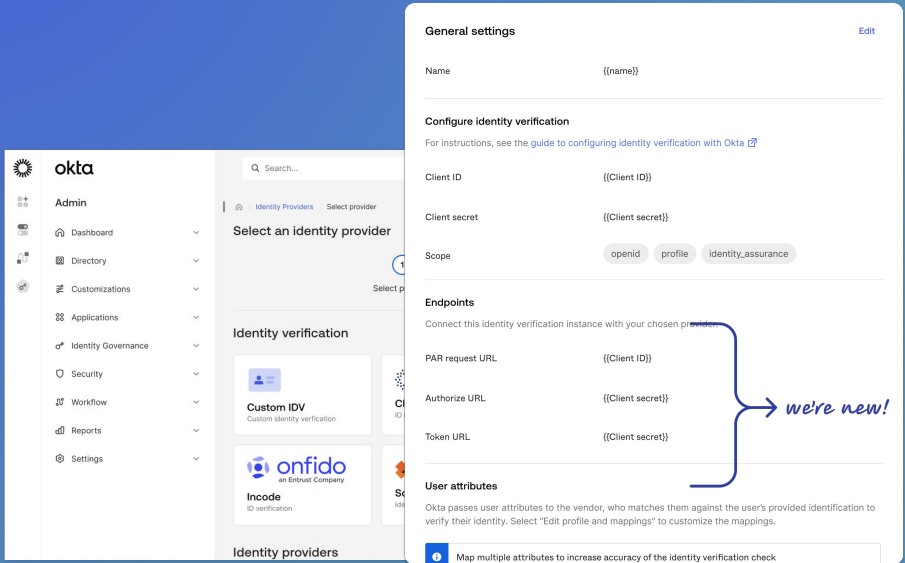
Custom AAGUID

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

Limit end-user authenticator enrollment to only approved authenticators and password managers.

[Learn more](#)

OIE



BYO Custom IDV



Access Management

Early Access

Device-Bound Single Sign-On (Windows and macOS)

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

Enable hardware-protected sessions that stop Okta session replay and streamline access to downstream apps after device login.

[Learn more](#)

OIE

Advanced Posture Checks (Windows and macOS)

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

Collect and assess device context—on any Windows or macOS device attribute or security setting—so you can further strengthen Zero Trust security during authentication.

[Learn more](#)

OIE

Okta as the fallback IdP in Routing Rules

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

This feature introduces a configurable fallback mechanism to route users to the Okta IdP if an external, third-party Identity Provider (IdP) fails during sign-in.

[Learn more](#)

OIE

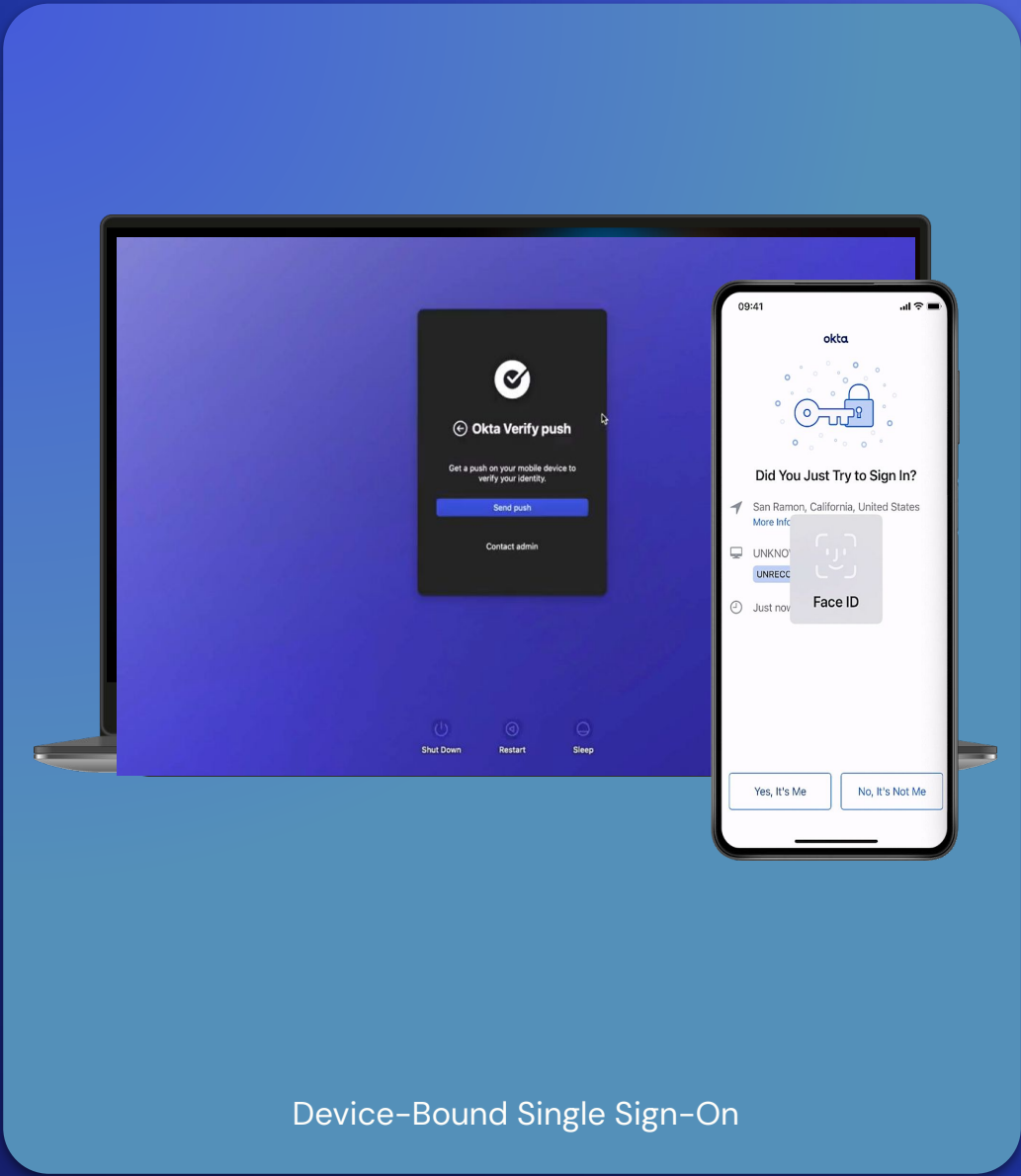
Support SHA256 digest in SAML AuthN Request

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

This feature upgrades Okta's SAML implementation to use the SHA-256 digest algorithm instead of the deprecated SHA-1 standard.

[Learn more](#)

OIE



Access Management

Early Access

Authenticator Rollout Insights

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

This enhancement to the Authentication Activity report helps admins see exactly how Okta FastPass and other factors are being used—by device type, login method, management state, and registration status.

[Learn more](#)

OIE

Threat Intelligence detection improvements

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Enrich the Okta Threat Intelligence detection with IOC information like IP address and ASN.

OIE

Bot Protection with Okta AI

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Enhanced security posture against automated bot attacks commonly seen in credential stuffing, brute force attacks, and account takeover attempts.

OIE

Improved Session Protection Controls

Feature of: Identity Threat Protection || Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4

Admins can configure which session context changes initiate policy re-evaluation, providing granular control based on organizational risk tolerance.

[Learn more](#)

OIE

Session violation detection

Define the session conditions that will trigger a session violation detection when Global session policy or Authentication policy violations occur. This detection helps identify potential unauthorized access.

IF

User's IP address OR Device details change during an active session

AND

Risk level is

High

Flags only High risk sessions. This provides the lowest security and the most frictionless user experience.

Medium and above

Flags Medium or High risk sessions. This provides balanced security and a good compromise between detection effectiveness and user experience.

Low and above

Flags all sessions with a risk level. This provides the highest security, which may result in a higher volume of detections and potential friction for users.

AND

User's new IP is

Detection is based on your configured network zones. View and configure [network zones](#).

Not in any of the following Network zones

Network zones

My super-secure-network-zone

US-offices

Default-exempt-zone

AND

User's session violates Global session policy or Authentication policy conditions

A violation is recorded when the new session conditions result in a rule evaluating to a Deny or an insufficient MFA.

Enforcement settings

THEN

Action

MFA if possible

Prompts the user for MFA. This action is taken only if required by the Global Session Policy and is only possible if the user is on an Okta page.

Okta logout

Logs the user out of Okta if MFA is not possible, is answered incorrectly, or if the Global Session Policy results in a Deny.

Run an additional action

This action runs when Global session policy or an Authentication policy associated with an app in the session is violated.

AND

Additional action

App logout

Logs the user out of active applications configured for logout.

Run a workflow

Select from your delegated Workflows to run.

AND

Groups impacted

All groups

The following groups:

Improved Session Protection Controls

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

okta

Access Management

Early Access

Device Conditions in OAMP

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

Enables admins to restrict account management activities, such as self-service password resets and new authenticator enrollments, to registered/managed devices.

[Learn more](#)

OIE

OAG Offline Access

Feature of: Okta Access Gateway || Supported in: FedRAMP Moderate/High/DOD IL4

When Okta Access Gateway (OAG) loses connection to Okta, users can continue accessing on-prem applications.

Classic

OIE

IF

IF User's user type is

Any user type

AND User's group membership includes

Any group

AND User is

Any user

AND Device state is

☐ Any

☒ Registered

Setup Okta Verify as Authenticator

AND Device management is

☐ Not managed

☒ Managed

Go to Device Management

AND Device assurance policy is

Any of the following device assurance policies:

macOs

Go to Device Assurance Policies

AND Device platform is

Any platform

Device platform is securely verified for registered devices. For unregistered devices, it's determined by the user-agent and can be modified. Learn more about Device platform security

AND User's IP is

Any IP

Device Conditions in OAMP



Identity Management

General Availability

Security Access Review

Available in: OIG || Authorized in¹: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Conducts a user-centric access review for End-users, especially post-security incident, to evaluate user access levels.

[Learn More](#)

Classic

OIE

Upgrading LDAPi to OIDC

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

Shifts the LDAPi approach for Super Admins and Managers from directory integration to an App Instance model.

OIE

Profile Edits for Deactivated Users

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

Allows administrators to edit Okta profile attributes for deactivated users, enabling profile updates without needing to reactivate a user.

Classic

OIE

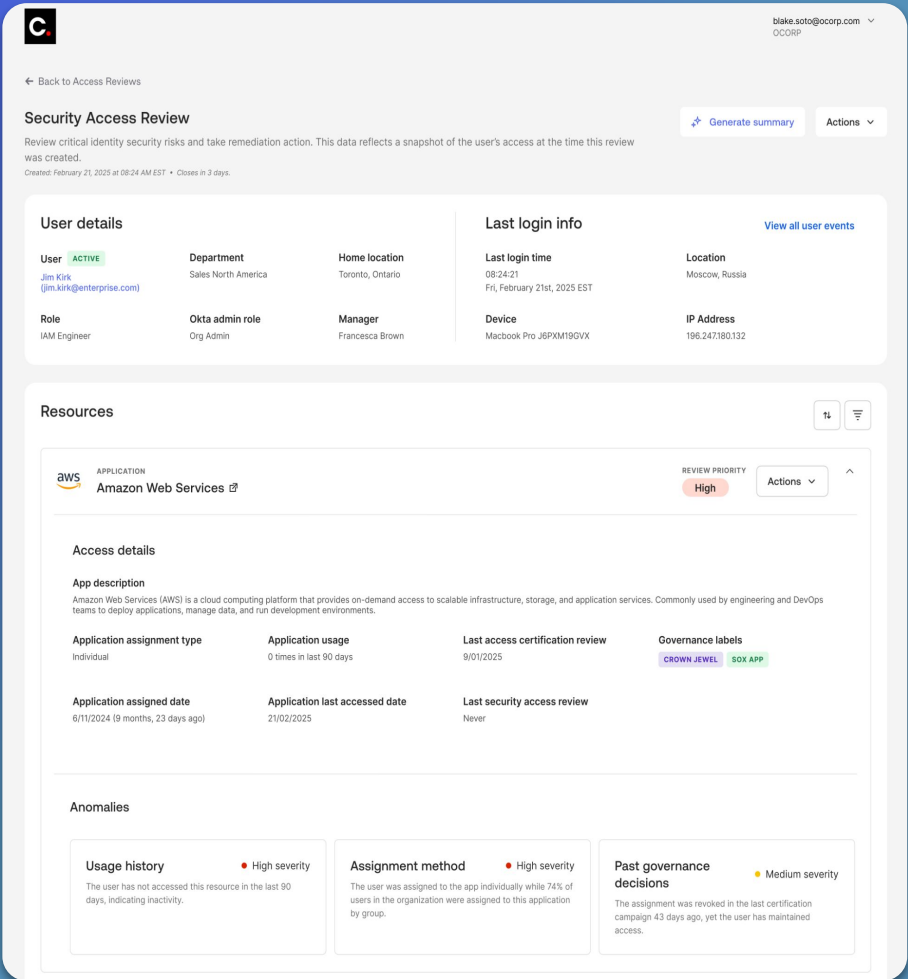
Access request automation enhancements

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

Returns request user-facing ID via Get Request APIs. Passes request ID as "Caller Context" in Delegated Workflows V1 integration.

Classic

OIE



Security Access Review ¹

¹. AI LLM generated summaries is currently not available in our FedRAMP and DoD authorized cloud offerings, but it is under evaluation for inclusion.



Identity Management

General Availability

Access Granted and Revoked Notifications

Available in: [OIG II](#) Authorized in ¹: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Notifies requesters when access is granted or revoked, clarifying the access request process.

Classic

OIE

Export OIG Reports as PDF

Available in: [OIG II](#) Authorized: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Exports reports as PDFs for Auditors and controls analysts to review evidence of compliance, delighting Auditors and GRC staff with their preferred format.

Classic

OIE

Governance Labels

Available in: [OIG II](#) Authorized: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Allows Admins to add labels to resources within Okta, supporting OIG use cases.

Classic

OIE

[Learn More](#)



Your access to this resource has been revoked.
Access was revoked on October 15, 2025 at 10:30 a.m. PST.

Resource details		
Resource	Access level	Access level description
Figma	Read only	Description of the access level that can go up to 3 lines...

To stop receiving notifications [unfollow this request](#) or [change your notification preference](#).

Revoked Notifications via email



Okta_accessrequests APP 9:16 AM

Your access to Figma has been revoked

Revoked on October 15, 2025 at 10:30 a.m. PST

[Submit new request](#)

Resource	Access level
Figma	all_employees_access

Revoked Notifications via Slack¹

¹. Slack generated notifications is currently not available in our FedRAMP and DoD authorized cloud offerings, but it is under evaluation for inclusion.



Identity Management

General Availability

Entitlement History

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

Visualize how entitlement assignments change over time for an app. Understand access changes and simplify user access auditing for Super Admins and Auditors.

[Learn More](#)

Classic

OIE

Office 365 application for GCC environment

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

Supports Office 365 integration within Microsoft's GCC environment. This feature is managed by Administrators.

Classic

OIE

LDAP Bidirectional APIs

Available in: Directory Integrations || Authorized in: FedRAMP High/Moderate

Easily add or remove users from on-prem groups based on triggers set in Okta using APIs for LDAP.

Classic

OIE

Resource Owners

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

Drives policies based on resource traits and simplifies governance by assigning tasks to accountable resource owners.

[Learn More](#)

Classic

OIE

Access details

Tom Haverford (Tom.Haverford@pawneeparks.com)
Last assigned to [app_name] on February 21, 2023 at 10:24 AM EST

Entitlements Assignment history



- Tom Haverford's access was removed from:
February 21, 2025 at 10:24 AM EST [View access snapshot](#)
[entitlement_name]
Value A Value B Value C
- Tom Haverford was assigned:
February 21, 2025 at 10:24 AM EST [View access snapshot](#)
[entitlement_1_name]
Value A Value B Value C Value [long_name] Value [long_name]
Value A Value A Value B Value B Value B Value C
Value [long_longer_name]
- Tom Haverford was assigned:
February 21, 2025 at 10:24 AM EST [View access snapshot](#)
[entitlement_1_name]
Value A Value B Value C Value [long_name] Value [long_name]
Value A Value A Value B Value B Value B Value C
Value [long_longer_name]

Entitlement History



Identity Management

General Availability

Unified Audit Reports in Access Certifications

Available in: [OIG](#) [II](#) Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Generates compliance audit data easily from one location in Access Certifications for all reporting needs.

[Learn More](#)

Classic
OIE

Access Requests for Active Directory Groups

Available in: [OIG](#) [II](#) Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Requests access to Active Directory groups for users, leveraging AD Bi-directional sync for adding users and time-based revocation.

[Learn More](#)

Classic
OIE

Assign Approvals to Resource Owners

Available in: [OIG](#) [II](#) Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Simplify and downsize the number of access request sequences by using generic owners tied to resources.

Classic
OIE

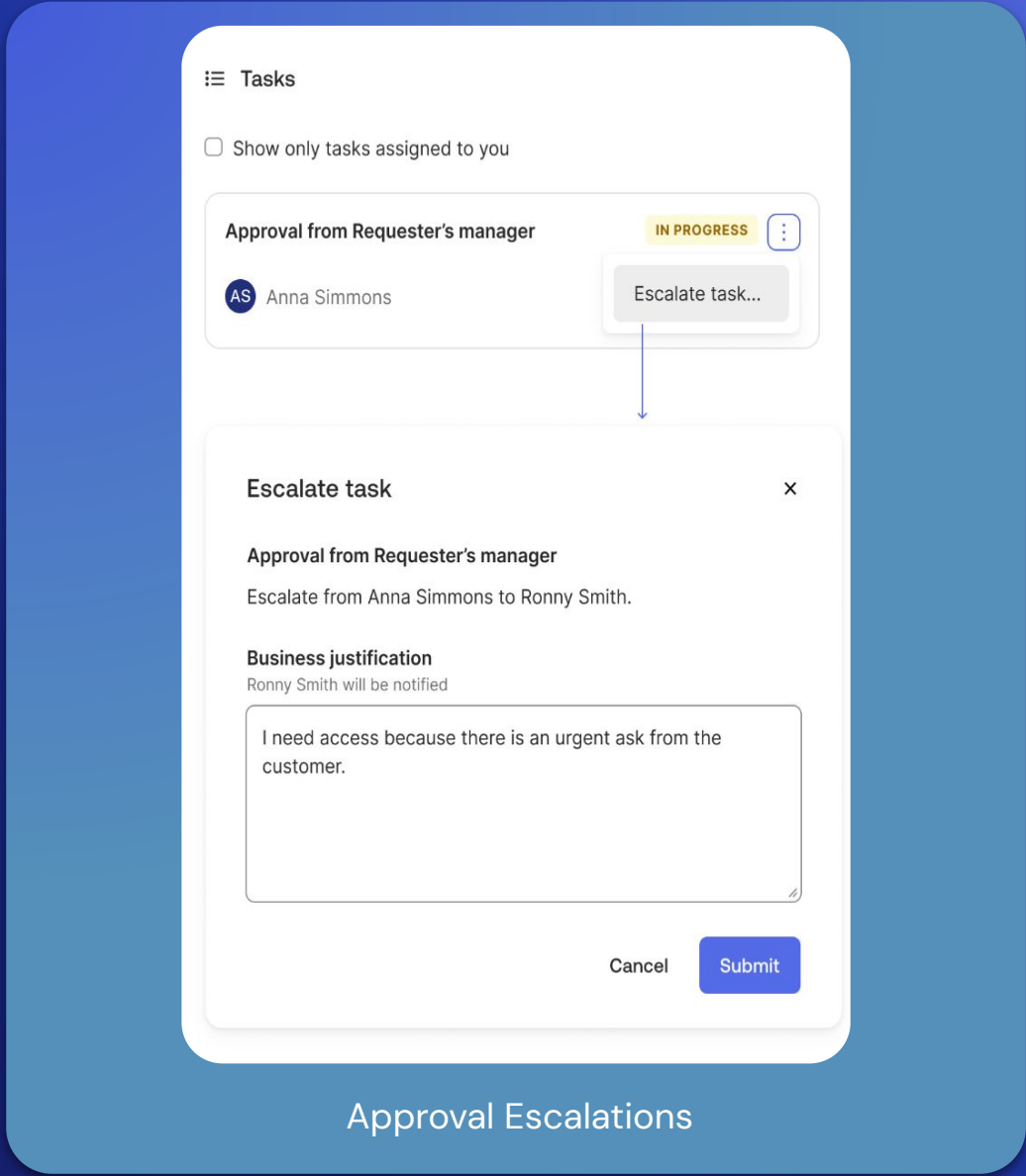
Approval Escalations

Available in: [OIG](#) [II](#) Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Streamline approvals by allowing requesters to escalate when their approvers are out of office or unavailable.

[Learn More](#)

Classic
OIE



Approval Escalations



Identity Management

General Availability

Anything-as-a-Source (XaaS) Groups Available in: LCM Authorized in: FedRAMP Moderate/High/DOD IL4 Manage groups and group membership with Anything-as-a-Source APIs.	Classic OIE
New Provisioning/ Entitlement Integrations Feature of: OIG, LCM OIG Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate. LCM Authorized in: FedRAMP Moderate/High/DOD IL4 New Provisioning/ Entitlement Integrations for Crowdstrike, LucidChart, Netskope, Oracle IAM, SAP Analytics, SAP Concur, Trend Micro, and Mimecast.	Classic OIE
Imports Visibility Enhancements Available in: LCM Authorized in: FedRAMP Moderate/High/DOD IL4 Provide admins with deeper visibility into import steps and progress to increase their trust in Okta's process with transparency and reliability.	Classic OIE



Identity Management

Early Access

Workday Incremental Imports

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

Enables faster importation of changed user identities and access from Workday into Okta, ensuring Admins have the latest user and group data available quickly.

Classic

OIE

Access Certifications for Service Accounts

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

Manage certification campaigns for Service accounts within Okta Privileged Access.

[Learn More](#)

Classic

OIE

Access Certifications for Collections

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

Execute access certification campaigns on collections for Super Admins.

Classic + OIE

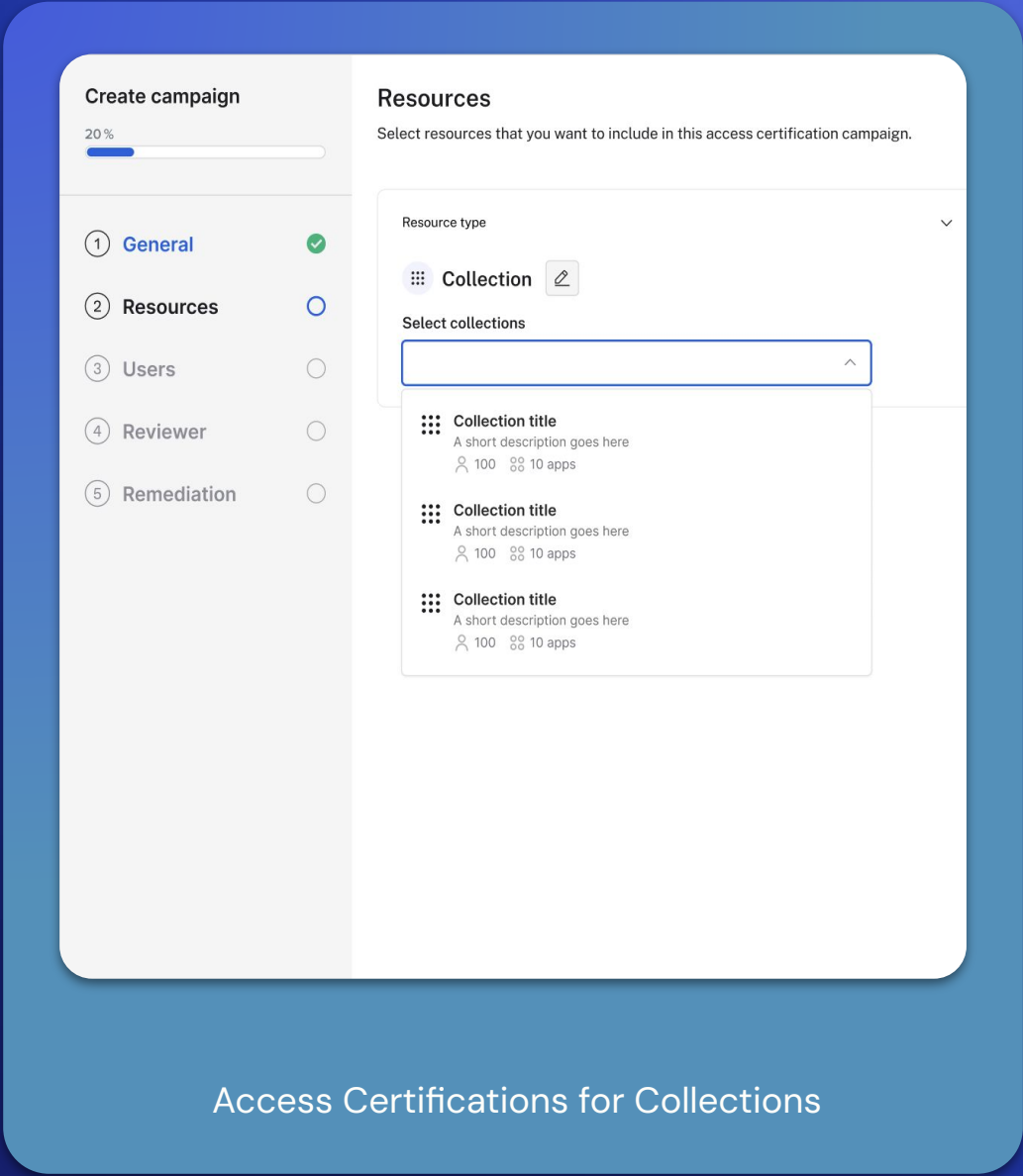
Flexible entitlement assignments

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

Assign entitlements to users without editing existing assignments, giving Admins more flexibility in managing assignments.

Classic

OIE



Platform Services

General Availability

Identity Threat Protection, Okta Identity Governance, and Workflows for US Public Sector

Feature of: Okta Platform || Identity Threat Protection, Authorized in: FedRAMP Moderate/High, Supported in: DOD IL4. Okta Identity Governance and Workflows, Authorized in: FedRAMP High/DOD IL4, Supported in: FedRAMP Moderate

Provides a unified foundation for implementing core security tenets emphasized by frameworks like DoW Instruction 8520.04 (“Identity Assurance”), DoW CIO Memorandum, “Modernizing SAAR and AAP through ICAM Workflows,” and others.

[Learn more](#)

Classic

OIE

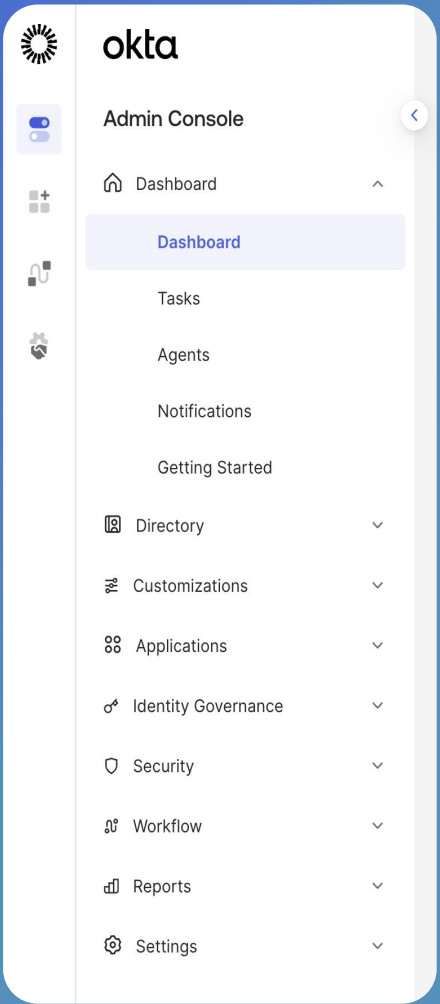
App switcher enhancements

Feature of: Okta Platform || Available in: All plans || Authorized in: FedRAMP Moderate/High/DOD IL4

Non-Okta admin users can utilize app switcher for quick and seamless navigation experience amongst multiple Okta first-party apps. More Okta products are added to the App Switcher, creating a single, convenient place to access your Okta ecosystem.

Classic

OIE



App switcher enhancements



Platform Services

Early Access

RBAC Folder Roles

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

Grants users access to individual folders where they can use and manage only specific flows, tables, and connections. Allows customers to expand their use of Workflows beyond the IT team.

[Learn more](#)

Classic

OIE

Governance for Workflows

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

Empowers organizations to securely govern access to the Workflows platform leveraging the power of OIG Access Requests and Certifications. Streamlines role assignments & grant time-bound access with with customized access requests.

[Learn more](#)

OIE

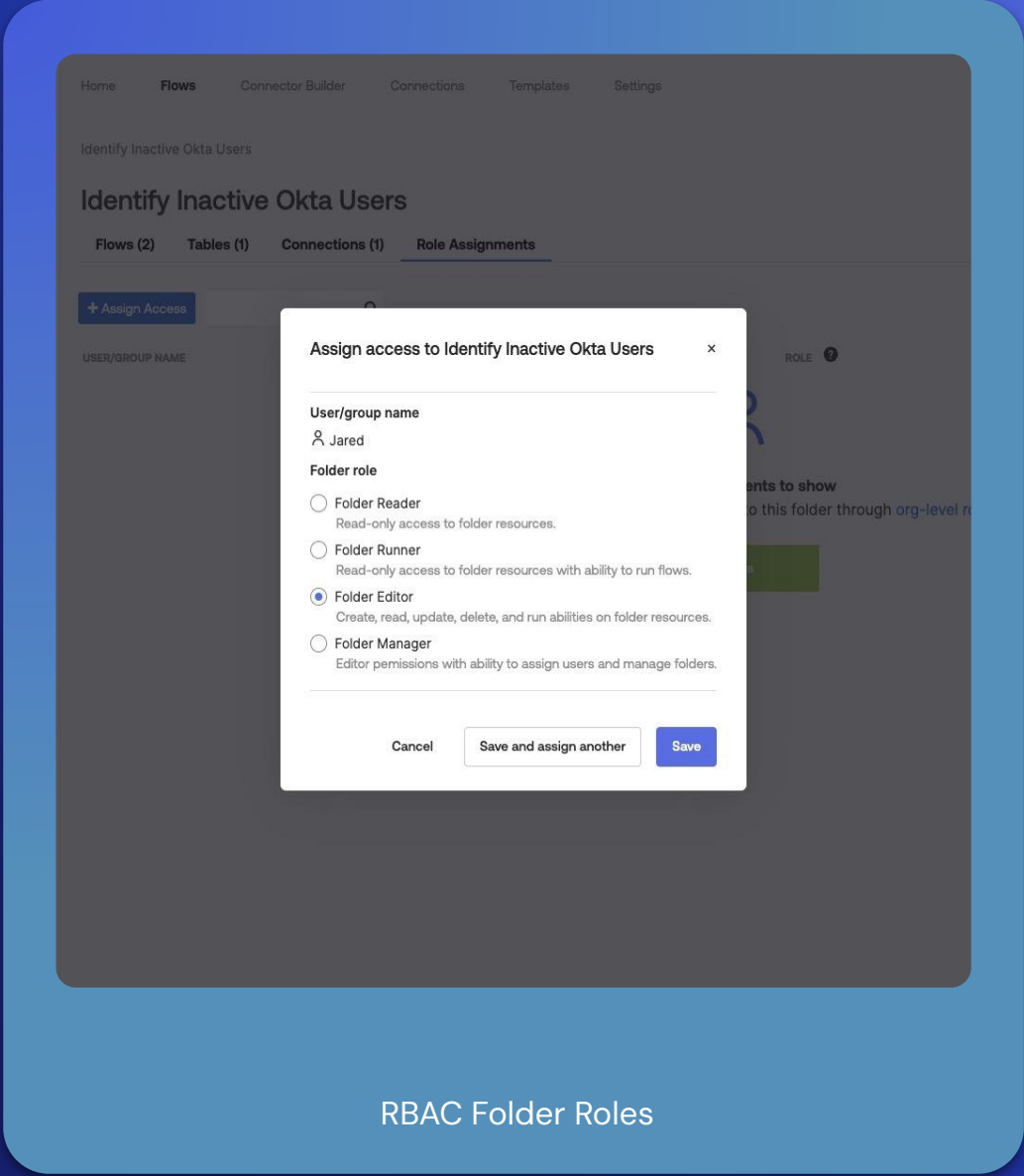
Admin role enhancements and auditor role

Feature of: Okta Platform || Available in: All plans || Authorized in: FedRAMP Moderate/High/DOD IL4

Ability to give Okta admin users a read-only version of any standard or custom admin role. It enforces the principle of least privilege access for users and API services integrations while still being able to delegate audit tasks.

Classic

OIE



RBAC Folder Roles



Okta Learning

General Availability

Protect Non-Human Identities Feature of: product / Available in: SKU This learning path introduces Non-human identities, how to identify them, and Okta’s offerings of ISPM and OPA for management. Learn more	Classic OIE
Brand Your Okta Customer Identity Experience Feature of: product / Available in: SKU This learning path provides a comprehensive solution by teaching you how to transform the default Okta login experience into a fully custom, branded user interface. Learn more	Classic OIE
Expert Learning Pass Feature of: product / Available in: SKU Okta Identity Governance learning paths & skill badges: • Access Requests • Entitlement Management • Access Certifications Live Learning Labs – recently added new FastPass labs to the calendar through March.	Classic OIE
Certification Feature of: product / Available in: SKU New hands-on exams for Okta Certified Professional and Administrator certifications.	Classic OIE

LEARNING PATH

Protect Non-Human Identities

Non-human identities (NHIs) are automated digital accounts (service accounts, API keys, AI agents) with unique security risks like increased attack surface, lack of visibility, and over-privilege. Solutions include Zero-Trust, least privilege, secret rotation, monitoring, and ownership. Okta offers ISPM and OPA for management.

OKTA WORKFORCE IDENTITY

What Are Non-Human Identities?

Non-human identities (NHIs) are automated digital accounts with unique security risks surface, present lack of visibility, and over-privilege.

OKTA LEARNING RESOURCE

Identify Non-Human Identities with ISPM

Use ISPM to quickly identify identities that perform non-human tasks.

Learning Path: Protect Non-Human Identities



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 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.



Spotlight: Secure Customer Identities advancements

Continuous identity security across the entire journey: before, during, and after login.

What is it?

Okta Identity Threat Protection (ITP) for OCI is a continuous, identity-centric control plane designed for organizations managing external identities at scale. It expands security from a single point-in-time check at login to a continuous monitoring model that evaluates risk throughout the entire active session lifecycle

Customer Challenge:

For CIAM leaders, every millisecond of friction can lead to abandoned sign-ups and lost revenue, yet security teams are facing a surge in sophisticated fraud. Traditional "front-door" security fails to stop attackers who use automated bots to inflate user growth analytics with fake accounts or those who hijack legitimate sessions to drain loyalty points and sensitive data after a user has authenticated. Balancing a seamless, high-conversion user experience with the need to protect brand reputation and prevent large-scale fraud has never been more difficult.

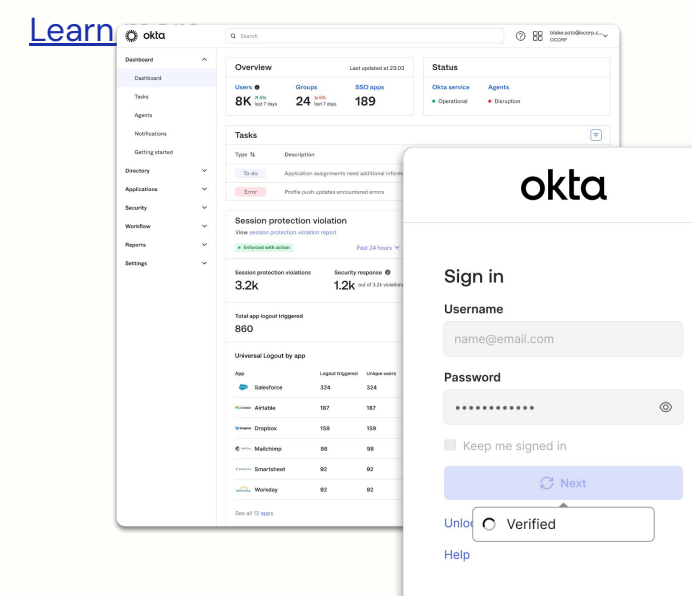
Why this matters

- **Before Login (Proactive Bot & Fraud Defense):** Blocks automated scripts and "fake account" registrations before they reach your database, ensuring your growth analytics reflect real human customers.
- **During Login (Precision Access Verification):** Instantly identifies and blocks compromised credentials in real-time to neutralize account takeover (ATO) attempts without adding friction for legitimate users.
- **After Login (Continuous Post-Auth Protection):** Monitors active sessions for "Impossible Travel" or token theft, triggering right steps to instantly kill hijacked sessions across all supported apps.

How to get it

ITP for OCI is Early Access (EA) and is **currently authorized in our FedRAMP Moderate and FedRAMP High environments, and supported in our DoD IL4 environment.**

OCI ITP SKU: This requires Enterprise and AMFA SKUs, with quantities matching the Enterprise aMAU count. This feature is available on the Okta Identity Engine (OIE) platform only.



Okta Customer Identity

General Availability

Advanced Directory Management (fka. Secure Partner Access) Feature of: OCI / Available in: OIG for OCI SKU Authorized in: FedRAMP High/DOD IL4, Supported: FedRAMP Moderate Provide partners secure, seamless access to internal resources with minimal IT overhead. Learn more	Classic
Universal Logout support for OCI (fka.CIS) apps Feature of: OCI Available in: ALL SKUs Authorized in: FedRAMP Moderate/High/DOD IL4 Zero development effort for app developers to build Universal Logout into their Okta Customer Identity (formerly CIS) applications. Learn more	OIE
Unified Claims Generation for Okta Federated Apps Feature of: OWI & OCI Available in: ALL SKUs Authorized in: FedRAMP Moderate/High/DOD IL4 Streamline SAML and OIDC integration via a single interface. Use Okta Expressions to filter Group, Profile, and Device claims into refined, relevant payloads. Learn more	OIE
Profile Edits for Deactivated Users Feature of: OWI & OCI Available in: Universal Directory SKU Authorized in: FedRAMP High/Moderate/DOD IL4 Update inactive profiles to keep records current for long-term analytics and seamless customer returns..	Classic
	OIE



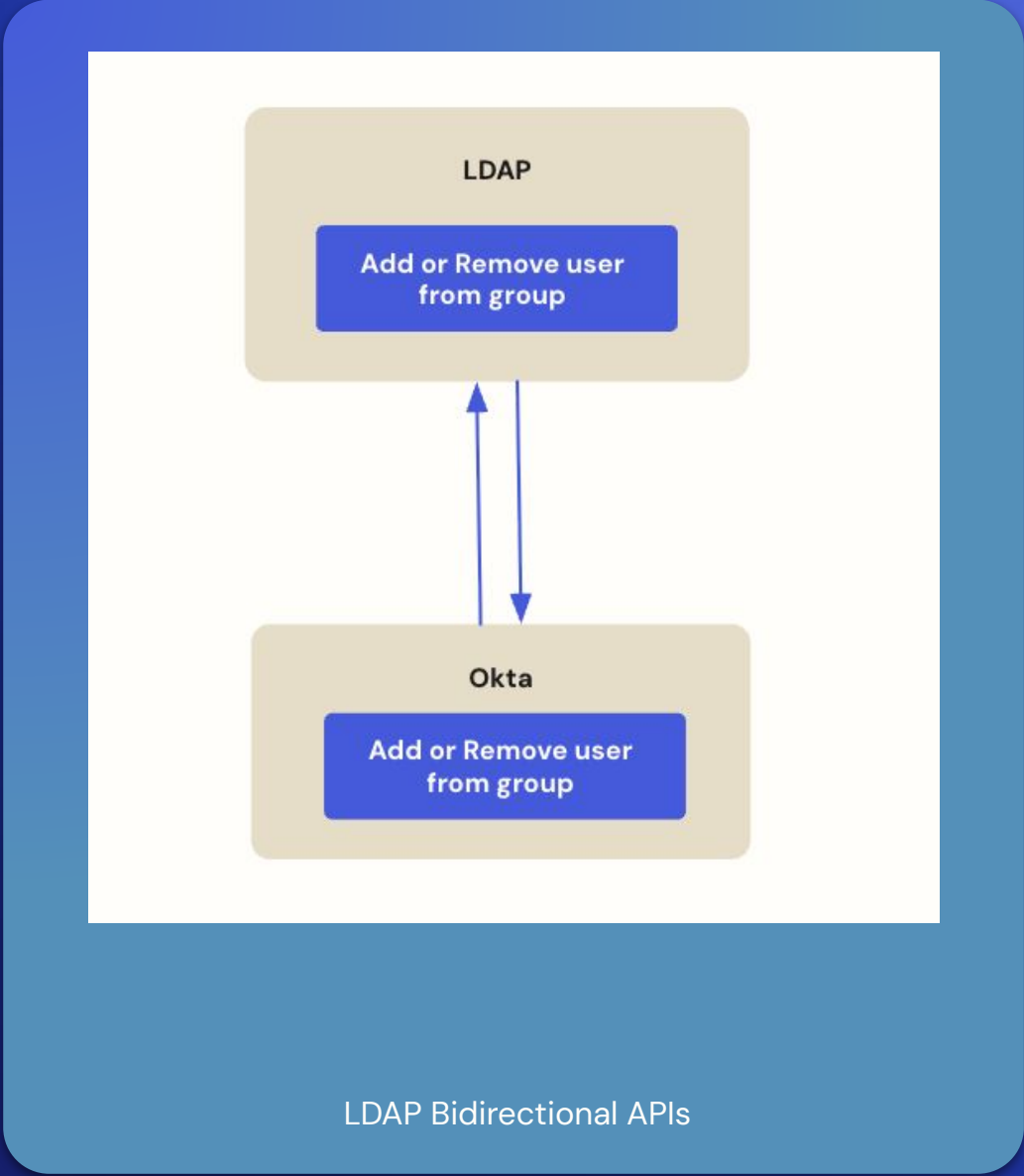
[Learn more](#)



Okta Customer Identity

General Availability

Export OIG Reports as PDF Feature of: OWI & OCI Available in: OIG Authorized in: FedRAMP High/DOD IL4, Supported: FedRAMP Moderate Simplify how you share identity insights. Move beyond raw data by exporting access certification results into a polished PDF format.	Classic OIE
ITP, OIG, and Workflows in IL4 Feature of: OWI & OCI Available in: OIG OIG and Workflows are Authorized in IL4, FRH, and Supported in FRM, ITP is Authorized in FRM, FRH, and Supported in IL4 DoD customers will be able to use ITP, OIG, and Workflows in IL4 regulated cells (OM1 and associated product-specific cells).	Classic OIE
LDAP Bidirectional APIs Available in: Directory Integrations Authorized in: FedRAMP Moderate/High Easily add or remove users from on-prem groups based on triggers set in Okta using APIs for LDAP. Learn more	Classic OIE
Upgrading LDAPi to OIDC Available in: UD Authorized in: FedRAMP High/Moderate/DOD IL4 Shifts the LDAPi approach for Super Admins and Managers from directory integration to an App Instance model.	OIE



Okta Customer Identity

General Availability

OIDC Token Encryption

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Protects the transmission of highly confidential personal information to a trusted federated resource while also preventing interception by unauthorized 3rd parties and malicious attackers.

[Learn more](#)

Classic

OIE

Okta Account Management Policy support for Password Expiry

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Enable greater control over assurance requirements when the end-user's password expires or is compromised.

[Learn more](#)

OIE

Custom Admin permissions for Access Policies

Feature of: OWI & OCI || Available in: SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Enables consistency and granular control over authentication, session, and account management policies.

[Learn more](#)

OIE

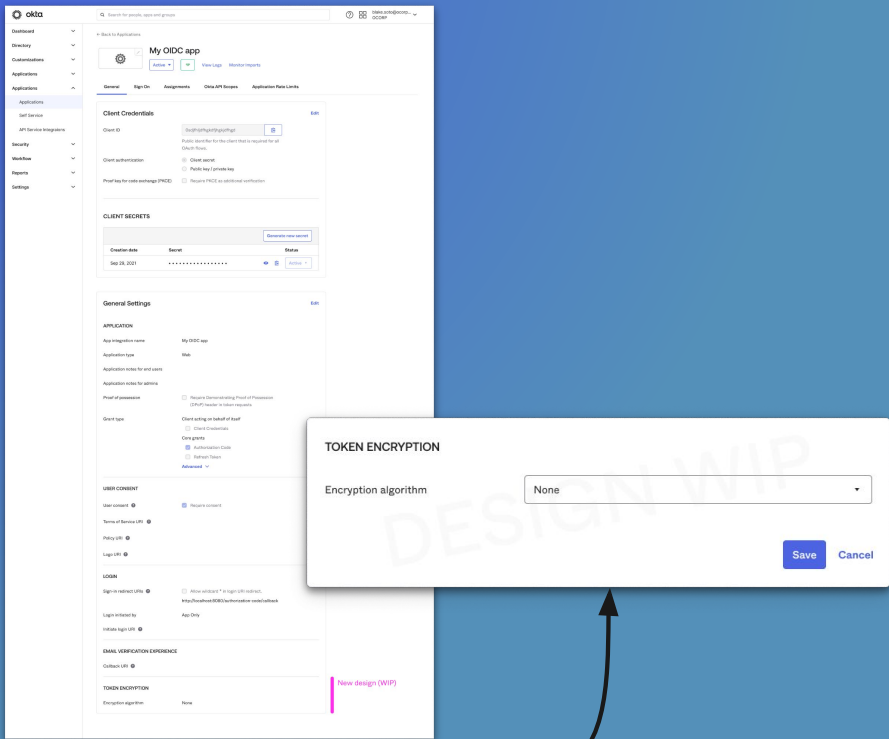
Support for Higher Assurance Certificates from Certificate Authorities

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

This will expand support for certificates that are used in Custom Domains flows to higher assurance (SHA-384 + SHA-512).

[Learn more](#)

OIE



OIDC Token Encryption



Okta Customer Identity

General Availability

Password Complexity OEL (formerly Enhanced Credential Security)

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Bolster password and allied protections by adding a defense-in-depth layer of security, thus supporting customers on their journey to passwordless.

[Learn more](#)

OIE

Device Conditions in OAMP

Feature of: OWI & OCI || Available in: ALL SKU || Supported in: FedRAMP Moderate/High/DOD IL4

Use device-based conditions to ensure that self-service recovery and security updates are only accessible from a user's trusted devices. Adds a powerful layer of security that protects from sophisticated phishing and social engineering.

[Learn more](#)

OIE

Enhanced Dynamic Network Zones – Residential Proxies

Feature of: OWI & OCI || Available in: AMFA SKU || Supported in: FedRAMP Moderate/High/DOD IL4

Shield your customer portal from sophisticated threats by blocking traffic from residential proxies, VPNs, and anonymizers. Provides granular control to stop botnets and attackers who mimic legitimate customer locations to bypass security.

Classic

OIE

Network Restrictions on Token Endpoint

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Define an allowlisted network zone for each client to restrict token requests to specific IP addresses or ranges, enhancing token endpoint security.

[Learn more](#)

OIE

IF

IF

User's user type is

Any user type

AND

User's group membership includes

Any group

AND

User is

Any user

AND

Device state is

☐ Any

☒ Registered

Setup Okta Verify as Authenticator

AND

Device management is

☐ Not managed

☒ Managed

Go to Device Management

AND

Device assurance policy is

Any of the following device assurance policies:

macOs

Go to Device Assurance Policies

AND

Device platform is

Any platform

Device platform is securely verified for registered devices. For unregistered devices, it's determined by the user-agent and can be modified. Learn more about Device platform security

AND

User's IP is

Any IP

Device Conditions in OAMP



Okta Customer Identity

General Availability

ID Verification Additional Biographical Attributes

Feature of: OWI & OCI || Available in: MFA / AMFA || Authorized in: FedRAMP Moderate/High/DOD IL4

Ability to add additional biographical attributes while performing verifiable claims mapping during ID verification. Examples: DOB, email, phone number.

[Learn more](#)

OIE

Support SHA256 digest in SAML AuthN Request

Feature of: OWI & OCI || Available in: ALL SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

This feature upgrades Okta's SAML implementation to use the secure SHA-256 digest algorithm instead of the deprecated SHA-1.

[Learn more](#)

OIE

Custom AAGUID

Feature of: OWI & OCI || Available in: MFA / AMFA SKU || Supported in: FedRAMP Moderate/High/DOD IL4

Limit end-user authenticator enrollment to only approved authenticators and password managers.

[Learn more](#)

OIE

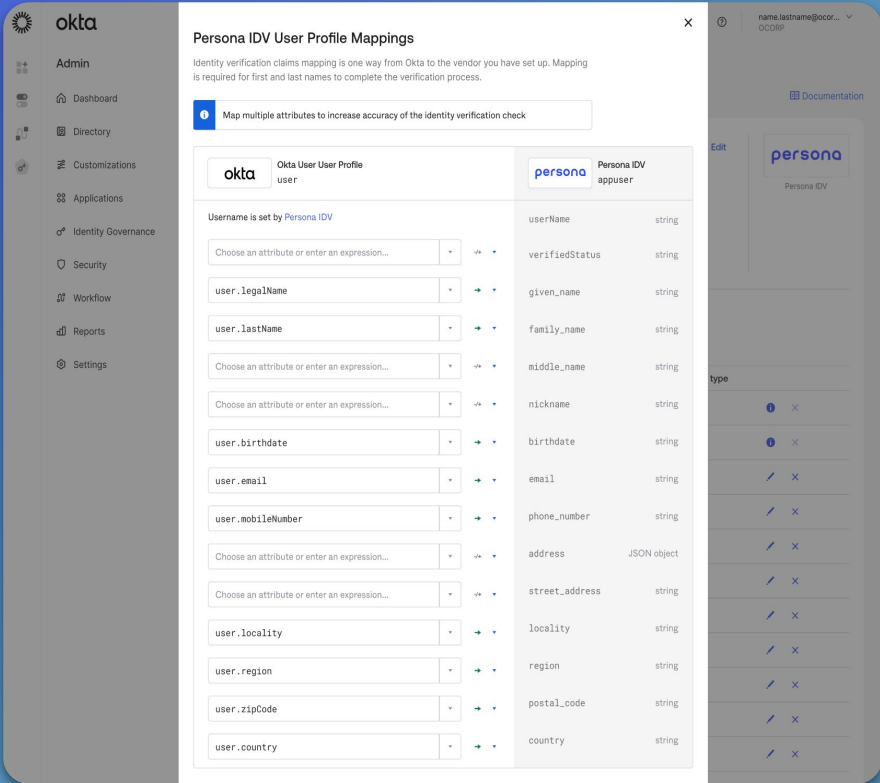
New Provisioning/ Entitlement Integrations

Feature of: Workflows || Available in: Okta Platform || Authorized in: FedRAMP Moderate/High/DOD IL4

Integrates with more HR systems and popular applications to manage users, groups, and entitlements, including Crowdstrike, LucidChart, Netskope, Oracle IAM, SAP Analytics, SAP Concur, Trend Micro, and Mimecast.

Classic

OIE



ID Verification Additional Biographical Attributes



Okta Customer Identity

General Availability

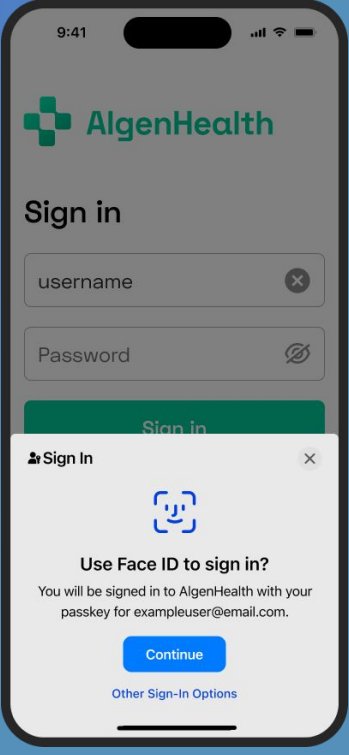
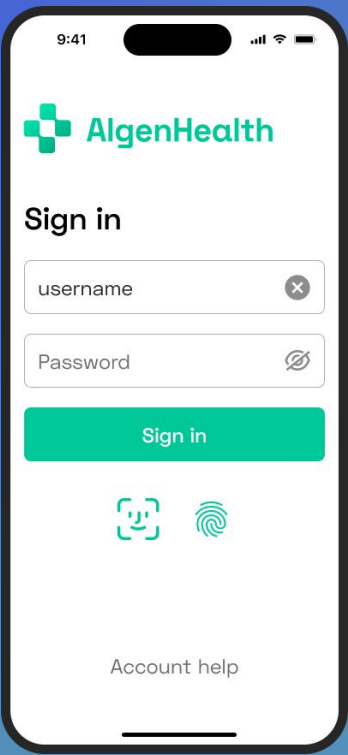
Native Passkey Support

Feature of: OWI & OCI || Available in: MFA/AMFA SKU || Supported in: FedRAMP Moderate

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

[Learn more](#)

OIE



Native Passkey Support



Okta Customer Identity

Early Access

ITP for OCI SKU launch

Feature of: OCI || Available in: ITP OCI SKU || Authorized in: FedRAMP Moderate/High. Supported: DOD IL4

Continuously protect against identity threats by assessing user, device, and context risk before, during and after authentication.

[Learn more](#)

OIE

Native to Web SSO

Feature of: OCI || Available in: ALL SKU s|| Supported in: FedRAMP Moderate/High/DOD IL4

Eliminates repeated logins, enhancing user satisfaction, retention, and engagement. Simplifies development and reduces authentication complexity for both B2C and B2B use cases.

[Learn more](#)

OIE

Authenticator Rollout Insights

Feature of: OWI & OCI || Available in: MFA / AMFA SKU || Supported in: FedRAMP Moderate/High/DOD IL4

This enhancement to the Authentication Activity report helps admins see exactly how factors are being used by login method, management state, and registration status.

[Learn more](#)

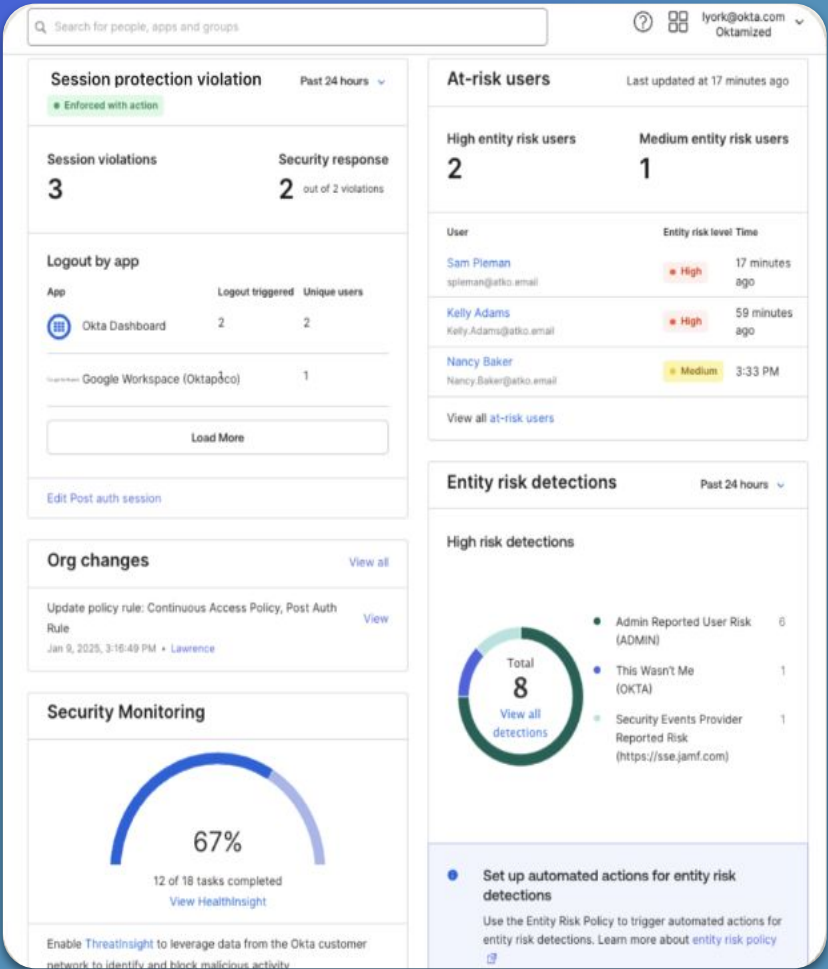
OIE

WebAuthn Rebrand + Sign In with Passkey

Feature of: OWI & OCI || Available in: All SKUs || Supported in: FedRAMP Moderate/High/DOD IL4

A simplified, standardized authentication experience that provides customers with more control over the passkey journey.

OIE



ITP for OCI



Okta Customer Identity

Early Access

OAG Offline Access

Feature of: OWI & OCI || Available in: Okta Access Gateway || Supported in: FedRAMP Moderate/High/DOD IL4

When Okta Access Gateway (OAG) loses connection to Okta, users can continue accessing on-prem applications.

Classic

OIE

Policy insights

Feature of: OWI & OCI || Available in: MFA / AMFA SKU || Authorized in: FedRAMP Moderate/High/DOD IL4

Enables admins to confidently make policy changes with improved insights, staged updates, and easy rollbacks.

[Learn more](#)

OIE

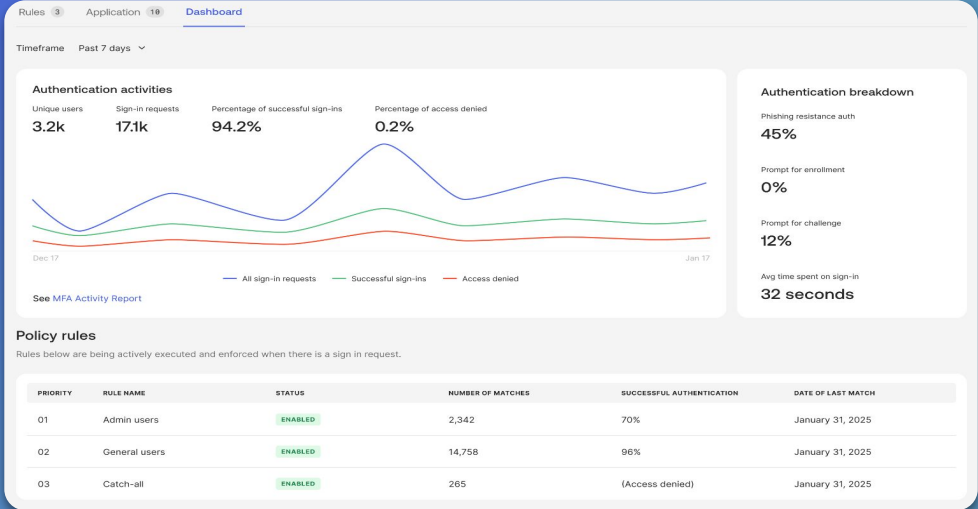
RBAC Folder Roles

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

Grants users access to individual folders where they can use and manage only specific flows, tables, and connections. Allows customers to expand their use of Workflows beyond the IT team.

Classic

OIE



Policy Insights

[Learn more](#)



okta