



Release Overview

for Early Access & General Availability in Q4 (October – December 2024)

Okta Workforce Identity
Okta Customer Identity

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

Safe harbor

This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, business strategy and plans, market trends and market size, opportunities and positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, global economic conditions have in the past and could in the future reduce demand for our products; we and our third-party service providers have in the past and could in the future experience cybersecurity incidents; we may be unable to manage or sustain the level of growth that our business has experienced in prior periods; our financial resources may not be sufficient to maintain or improve our competitive position; we may be unable to attract new customers, or retain or sell additional products to existing customers;

customer growth has slowed in recent periods and could continue to decelerate in the future; we could experience interruptions or performance problems associated with our technology, including a service outage; we and our third-party service providers have failed, or were perceived as having failed, to fully comply with various privacy and security provisions to which we are subject, and similar incidents could occur in the future; we may not achieve expected synergies and efficiencies of operations from recent acquisitions or business combinations, and we may not be able to successfully integrate the companies we acquire; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

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



Welcome to the Okta Platform Release Overview

Q4 2024

Welcome back to Okta's Quarterly Release Overview. This year has already brought lots of exciting updates, and we cannot wait to share with you all the innovation we released to the Okta Platform in Q4.

Explore how Okta Workforce Identity enhances security with advanced controls for privileged access, device protection, sensitive actions, and improved dynamic network zones.



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](#).

Okta Workforce Identity Product Roadmap Webinar

Get a sneak peek of upcoming product releases.

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

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](#).



Navigating the overview

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

Okta Workforce Identity

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

Okta Customer Identity

- Okta Customer Identity overview
- Spotlights
- Release overviews




Okta Workforce Identity

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




This quarter's releases double-down on our commitment to help customers strengthen their security posture and governance controls across devices, users, and privileged resources.

Spotlights

Customer First

 Okta Learning

Okta Workforce Identity

-  Okta Workforce Identity Suites
-  A More Unified and Seamless Okta Experience
-  Secure Partner Access

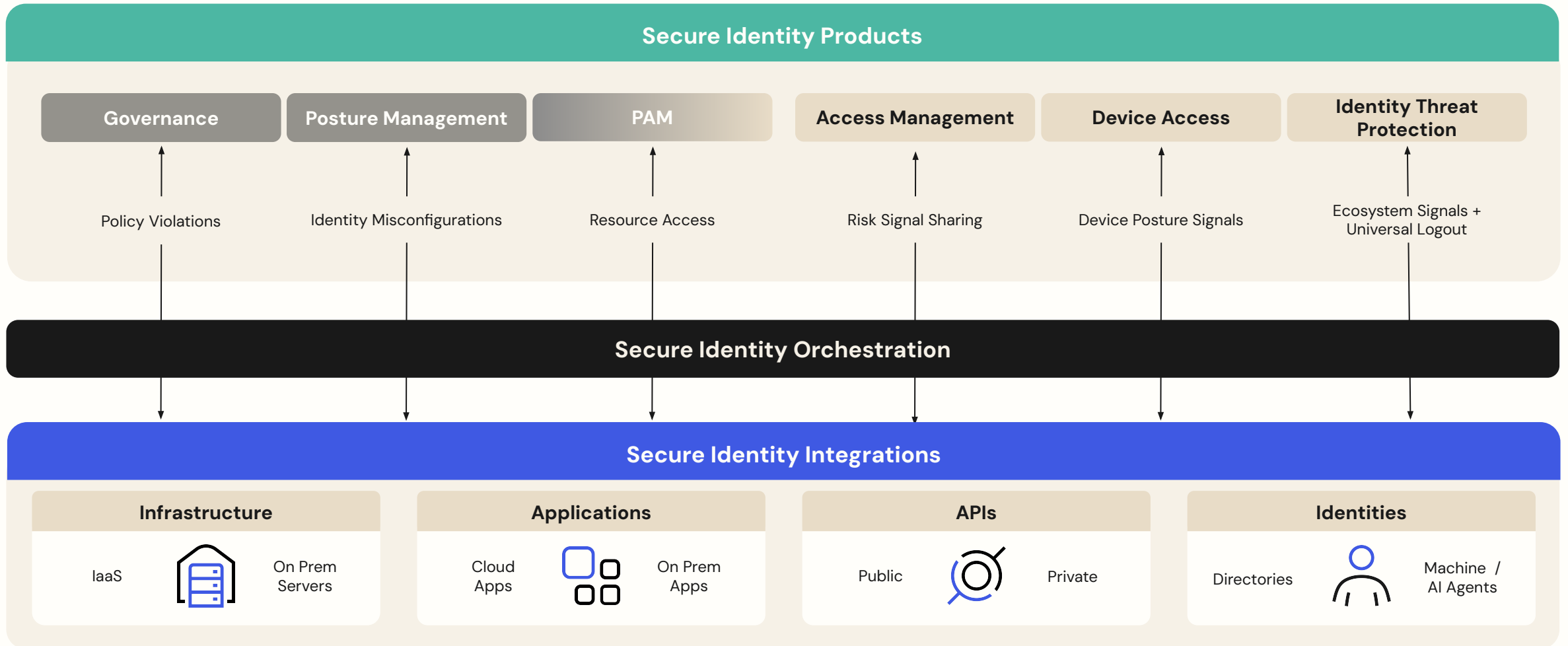
All releases

-  Identity Security Posture Management (ISPM)
-  Access Management
-  Identity Management
-  Identity Governance
-  Privileged Access
-  Platform Services

Developer resources



Okta Platform brings Modern Identity Security to life



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



Spotlight: Okta Learning

Grow critical skills, enhance security, and drive business outcomes with Okta Learning

What is it?

Okta Learning is our Training and Certification program reinvented – a comprehensive, role-based, and security-focused learning experience featuring 200+ public courses, curated learning paths, badging recognition program, and much more.

Okta Learning now offers the Expert Learning Pass which empowers teams to unlock Okta's full potential with our deepest level of education – access to exclusive content, live expert-led learning sessions, and certifications that validate critical skills with industry-recognized credentials.

Customer Challenge:

Teams are often unaware of how to fully utilize Okta Platform capabilities to drive security and Identity maturity, instead they are weighed down by Identity asks – troubleshooting instead of innovating.

Why this matters

- Drive team impact and productivity**
 Help grow key knowledge to configure and manage Okta efficiently and effectively with curated, modernized learning experiences built with the busy practitioner in mind.
- Stay ahead of evolving threats**
 Help validate that your team has the critical knowledge needed to modernize your organization with the latest product capabilities and Identity security best practices.
- Deliver more business value**
 As your business needs change, so should your team's skills. Explore courses on new features, use cases, and ways to drive Identity maturity.

How to get it

Access our comprehensive, role-based, and security-focused learning experience today.

[Explore training for your team!](#)

The screenshot shows the Okta Learning dashboard. At the top, it says "Welcome to Okta Learning" and includes a statistic: "10,395 Identity experts built their skills and careers in 2024". Below this is a section for "Explore recommended Learning Plans" with buttons for "Administration", "Development: OIE", "Development: Auth", "Security", and "More". There are also two promotional cards: "Build new skills and become more efficient" with a "Start Now" button, and "Tour our new learning experience" with a "Watch the video" button. A sidebar on the left says "Invest in security and expand your expertise in Identity." and "Explore the content catalog".





Spotlight: Okta Workforce Identity Suites

New pricing designed to give you a unified solution tailored to your security and workforce Identity needs

What is it?

Okta Workforce Identity Suites are solution-based packages designed to provide a unified identity solution tailored to your needs – enabling you to adopt capabilities in phases and without the complexity of selecting individual tools.

Customer Challenge:

Businesses of all sizes and stages of identity maturity come to Okta to address critical workforce identity use cases – from securing and automating onboarding and access to devices and apps, to reducing M&A risk through integration efficiency. To help you more easily plan and progress along your unique identity security journey, Okta is introducing Okta Workforce Identity Suites so you can realize the value of Identity sooner.

Why this matters

- **Flexible purchasing:** Bundled solutions that align with familiar buying models, providing more value and clarity than piecemeal solutions.
- **Faster time to value:** Customers can quickly adopt a unified identity solution tailored to their needs, enabling faster realization of identity benefits.
- **Path to identity maturity:** Comprehensive solutions that align with how customers evolve their identity practices to meet new challenges and business priorities.

How to get it

Okta Workforce Identity Suites will be generally available to customers starting March 10, 2025.

The screenshot displays four pricing tiers for Okta Workforce Identity Suites:

- Starter:** "Starting your identity journey? Put a strong foundation in place." Includes a "Start free trial" button and features: Universal Directory, Workflows (5 flows), Single Sign-On, and Multi-Factor Authentication.
- Essentials:** "Want to keep identity at pace with business growth? Get more must-haves." Includes a "Contact us" button and features: Everything in Starter plus; Workflows (50 flows), Adaptive MFA, Lifecycle Management, Access Governance, and Privileged Access.
- Professional:** "Looking to scale? Add device access and AI-powered intelligence." Includes a "Contact us" button and features: Everything in Essentials plus; Workflows (Unlimited flows), Device Access, Identity Threat Protection with Okta AI, Identity Security Posture Management, and Sandbox.
- Enterprise:** "Orchestrate end-to-end security for real-time detection and response." Includes a "Contact us" button and features: Everything in Professional plus; API Access Management, Access Gateway, and Machine-to-Machine Tokens.

*\$1500 annual contract minimum required. All suites are billed annually.





Spotlight: A More Unified and Seamless Okta Experience

Bringing a consistent, modern interface across Okta's products and workflows.

What is it?

Okta is rolling out a more unified experience across key products to simplify navigation while maintaining familiar workflows.

The first phase, launching in March 2025, will introduce a refreshed Admin Console and End-User Dashboard, along with a new App Switcher for admins to facilitate seamless access between Okta applications.

Future updates will extend this modern, consistent experience across more products.

Why this matters

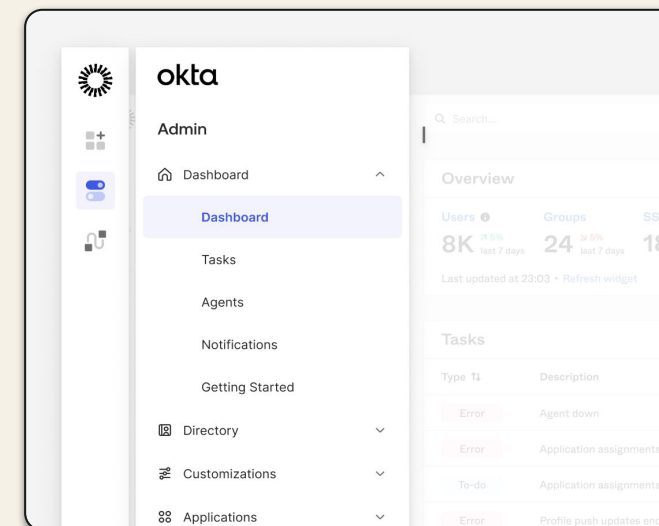
- **More intuitive experience** – A modernized, streamlined interface makes it easier for admins to navigate and manage identity tasks.
- **Enhanced usability and accessibility** – The updated design improves readability, reduced visual strain and optimizes workflows for efficiency.
- **Simplified learning curve** – A consistent look and feel across Okta products makes it easier to adopt new products and get up to speed faster.
- **Smooth transition** – Familiar settings and workflows remains intact, so admins can adopt the new experience without disruption.

How to get it

Early Access – Admins can opt-in starting February 2025 via self-service settings.

General Availability – Expanding in phases across key Okta products throughout 2025.

In-product guidance & resources – Updates will be communicated via release notes, admin notifications, and support documentation.





Spotlight: Secure Partner Access

Drive collaboration and growth through secure, streamlined partner access to resources and apps.

Available in: *Secure Partner Access*

What is it?

Secure Partner Access is a new solution that helps customers securely manage business partner access to shared applications at greater scale.

Customer Challenge:

In today's digital economy, secure collaboration with partners is critical. As cyber threats rise, IT & Security teams face increasing pressure to minimize risk while driving operational agility.

Yet, manual processes and a lack of purpose-built identity solutions for B2B collaboration create security gaps, drive up costs, and burden IT teams.

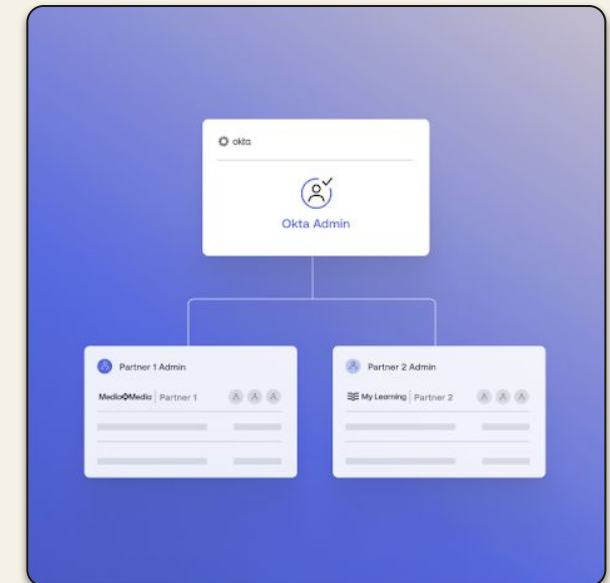
Why this matters

- Secure Partner Access (SPA) simplifies partner management across organizations by securely separating users into distinct populations within a single tenant to enhance visibility and control.
- Reduce operational costs associated with maintaining duplicate environments and access policies across multiple partner organizations.
- Enhance security and free up valuable IT resources by delegating least-privilege admin rights to partners (e.g., manage users, group membership, and app assignments).
- A dedicated partner admin portal helps ensure that partner admins have access only to the users they are authorized to manage, reducing risk and limiting exposure.
- For Okta Identity Governance customers, SPA provides increased observability into partner access.

How to get it

Secure Partner Access is available as its own SKU on the Okta Workforce Identity platform (OIE only).

[Learn more](#)



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 2024.

Easily identify the platform each release is available in:

Classic

Okta Identity Engine (OIE)





Identity Security Posture Management (ISPM)

General Availability

MFA insights and graph

Feature of: ISPM

Easily identify which apps lack MFA enforcement, compare MFA status for direct logins vs. SSO, and visualize login methods with a clear graphical overview. Gain insights into conditional MFA requirements based on location, device, and more.

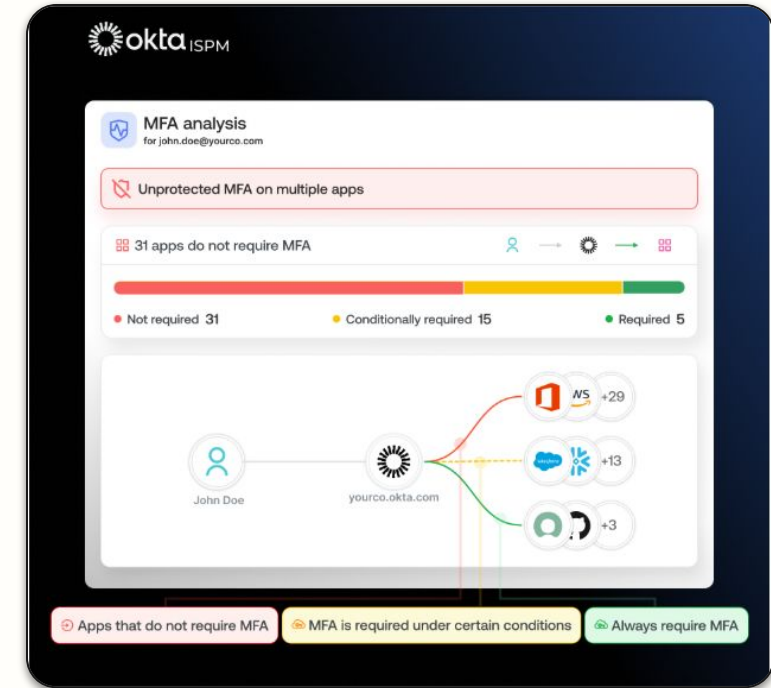
Classic

Entra ID enhancements (fetch stability, data quality)

Feature of: ISPM

ISPM now offers Entra ID enhancements, improving fetch stability and data quality to ensure more reliable and accurate identity security insights.

Classic



MFA insights and graph





Identity Security Posture Management (ISPM)

Early Access

Non Human Identities V2

Feature of: ISPM

ISPM enhances NHI visibility, helping security teams prevent breaches by identifying service accounts, API keys, tokens, and user identities with NHI credentials. Gain executive insights with dashboard trends and risk reports for proactive security.

Classic

RBAC V1 (limited access to Okta)

Feature of: ISPM

Enable security teams to delegate issue resolution to app owners (e.g. Salesforce.com Admin) by giving them limited access to view only selected data sources.

Classic

Self served "add connector" for post poc

Feature of: ISPM

Allow customers to self-serve integrate additional data sources after PoC ends, including: 1- Gallery experience and installation wizards, 2- Integrations health table, 3- Improved visibility to installation status.

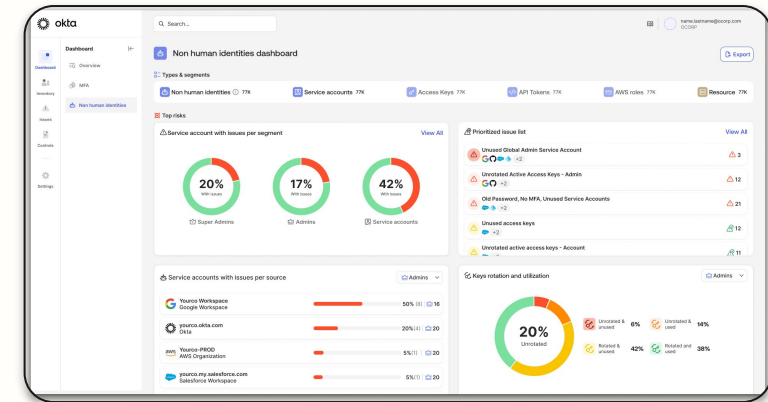
Classic

GW and Azure Cloud enhancements

Feature of: ISPM

Now includes GW and Azure Cloud enhancements, providing deeper visibility and control over security risks. Gain improved insights into gateway protections, cloud configurations, and identity security for a more resilient defense.

Classic



ISPM NHI dashboard





Apple Business Manager Federation

Available in: UD, SSO, LCM

Simplify Managed Apple ID provisioning while using Okta as a Federation layer for Apple devices and services. This integration enables secure logins into Apple devices and services with Okta credentials and sends security detections via the Shared Signals Framework (SSF) to Apple, enabling immediate action to protect Managed Apple IDs from compromise.

[Learn more](#)

OIE

Just-in-time Local Account Creation for macOS

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

Enable users to create local macOS accounts with standard or admin privileges, streamlining account management for shared devices.

[Learn more](#)

OIE

Multiple Identifiers

Available in: SSO. Authorized for FedRAMP Moderate/High/DOD IL4

Streamline the sign-in experience by allowing users to choose from multiple identifiers, with admins specifying which identifiers are valid across various applications

OIE

Yubico FIDO Pre-reg

Available in: AMFA

Help protect your organization and provide users with a quick, user-friendly way to secure their accounts with Pre-enrolled YubiKey.

[Learn more](#)

OIE



Apple Business Manager Federation





Authentication Method Reference (AMR) Claims Mapping

Available in: MFA. Authorized for FedRAMP Moderate/High/DOD IL4

With MFA required for all admin accounts, org-to-org admins can use AMR claims to enhance user experience, while maintaining strong security.

OIE

Authenticator Enrollment + Recovery with App Sign-on Policies

Available in: Core. Authorized for FedRAMP Moderate/High/DOD IL4

Strengthen protection against social engineering attacks with granular control over authenticator enrollment and recovery flows.

[Learn more](#)

OIE

Claims Sharing Between Okta Orgs

Available in: Core. Authorized for FedRAMP Moderate/High/DOD IL4

Enhance Identity federation by enabling secure, seamless access to resources across Okta Orgs without compromising security.

Classic

OIE

Enhance Account Linking Restriction

Available in: Core. Authorized for FedRAMP Moderate/High/DOD IL4

Boost security with the ability to restrict account linking to specific accounts within policies.

[Learn more](#)

OIE

SAML attributes

Profile attribute statements Cancel

Name	Name format	Value
ABC_Co_Email	Unspecified	user.email
+ Add another		

Group attribute statements

Name	Name format	Filter
	Unspecified	Starts with
+ Add another		

[Save](#) [Cancel](#)

Entitlements Cancel

Name	Expression
ABC_Co_Entitlements	Arrays.toCSVString(appuser.entitlements.name)
Using Okta Expression Language	
+ Add another	

[Save](#) [Cancel](#)

Entitlements in Assertion and token claims





US Public Sector Employees can use FastPass as a NIST SP 800-63 AAL3 Authenticator

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

Enable federal customers to use Okta FastPass as an AAL3 authenticator (when properly configured and on appropriate devices) as an alternative to PIV/CAC cards and FIDO tokens.

OIE

Granular Admin Permissions for Configuring Identity Providers

Available in: Core. Authorized for FedRAMP Moderate/High/DOD IL4

Assign specific Identity Providers (IdPs) to admins through granular admin permissions, ensuring only authorized users can configure IdPs when creating custom admin roles.

[Learn more](#)

OIE

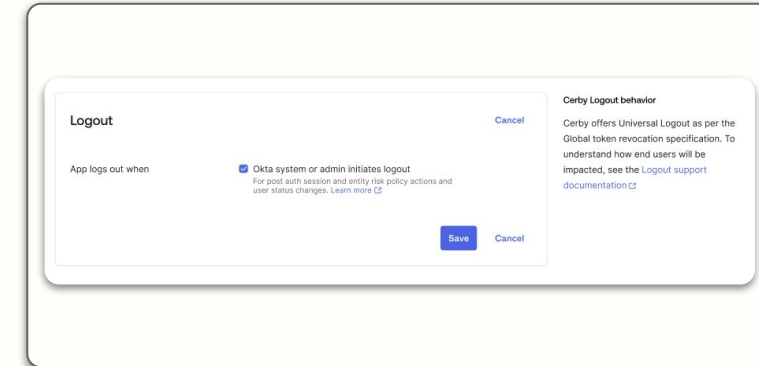
Support Universal Logout for Cerby Application

Available in: Identity Threat Protection, FedRAMP Moderate

Configure Universal Logout for Cerby Application with one single checkbox, enabling immediate password resets and logout for downstream applications when a Universal Logout request is triggered.

[Learn more](#)

OIE



Support Universal Logout for Cerby Application





Identity Management

General Availability

Microsoft Office 365 Provisioning and Federation

Available in: SSO

Provision and federate Microsoft Office 365 with Graph API OAuth scope, eliminating dependency on Azure admin credentials.

Classic
OIE

Microsoft Office 365 Government Support

Available in: SSO

Easily integrate Microsoft Office 365 Government - GCC High, now available in the Okta Integration Network catalog.

Classic
OIE

Microsoft Office 365
SWA | SCIM | Workflows Connector | Workflow Templates

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

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

Languages Supported
English

Use Case
[Single Sign-On](#)
[Lifecycle Management](#)

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

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

My Apps Sort ▾

Work

- Calendar
- Outlook
- Word
- Office 365
- People
- SharePoint
- Teams
- Excel
- OneDrive
- Powerpoint

Microsoft Office 365 Government Support





Identity Management

Early Access

Secure Partner Access

Available in: *Secure Partner Access, FedRAMP Moderate. Authorized for FedRAMP High/DOD IL4*

Enable business partners to securely and seamlessly access shared resources, without requiring significant development, customization, and management tasks from IT.

[Learn more](#)

OIE

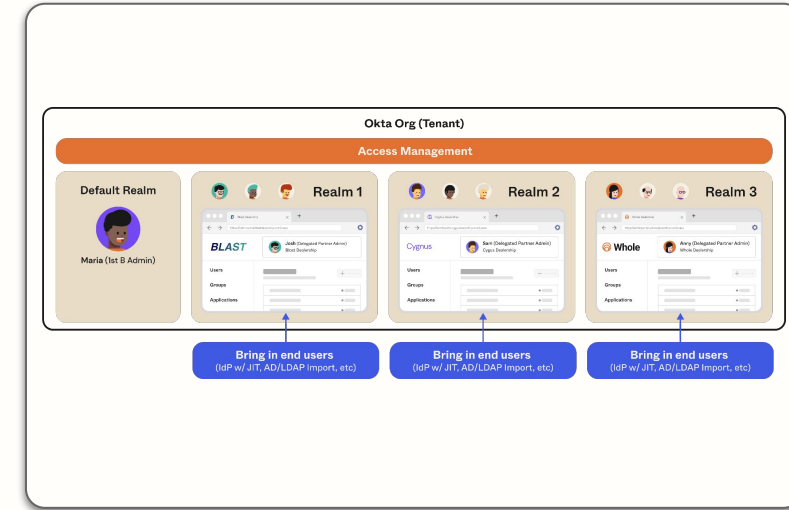
Step-up Authentication for Microsoft Office 365 Apps

Available in: *SSO*

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

Classic

OIE



Secure Partner Access





Access Request Conditions

Available in: *Okta Identity Governance*

Flexibly configure time-based access requests to require different approvals based on a requester's profile and group memberships.

[Learn more](#)

Classic
OIE

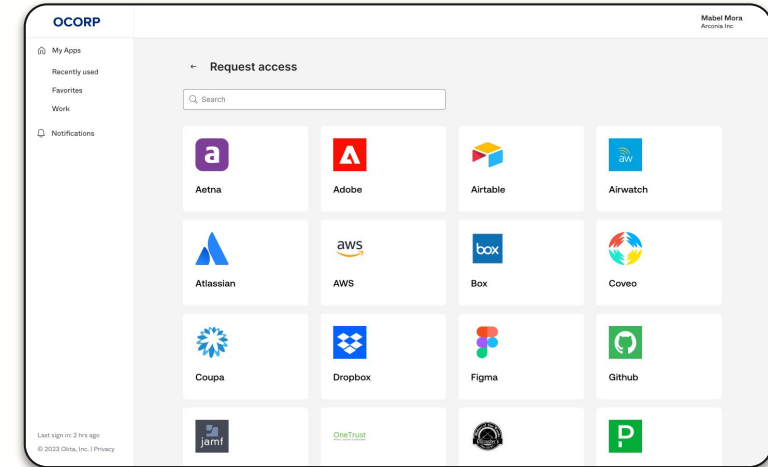
Resource Centric Access Request Catalog

Available in: *Okta Identity Governance*

Request access and SSO from the same end user dashboard. This unifies the end user experience to the single most frequently used interface.

[Learn more](#)

Classic
OIE



Resource Centric Access Request Catalog





Governance APIs

Available in: *Okta Identity Governance*

Leverage public Governance APIs to set up Access Certifications and Access Requests at scale without having to click through the UI.

Classic

OIE

Preconfigured Access Certification Campaigns

Available in: *Okta Identity Governance*

Effortlessly launch user-specific access review campaigns with a single click, leveraging two pre-configured options: 1) Discover Inactive Users, and 2) Okta Administrators Review.

Classic

OIE

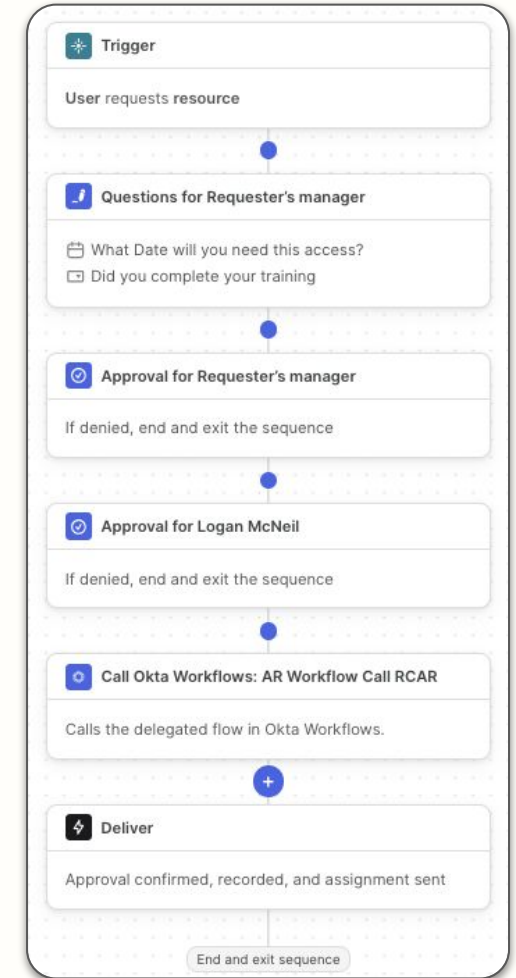
Enhanced Group Remediation for Access Certifications

Available in: *Okta Identity Governance*

Automatically remediate user access to group-assigned apps, instead of assigning these review items for manual remediation.

Classic

OIE



Sequences for Resource Centric Access Requests





Identity Governance

Early Access

On-prem Connector

Available as an add-on SKU with Okta Identity Governance

Seamlessly bridge legacy systems and modern fine-grained identity governance with an out-of-the-box connector for on-prem SAP

Classic

OIE

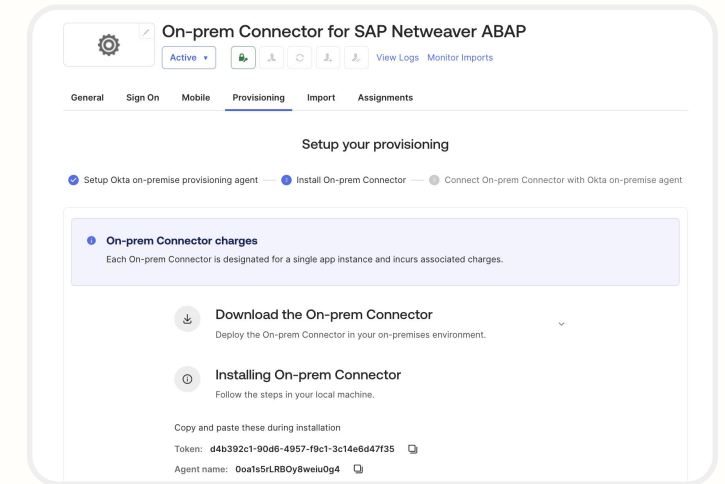
One-click Governance Enablement for Provisioning Enabled Applications

Available in: Okta Identity Governance

Streamline entitlement management/governance engine enablement for existing app instances that are provisioning enabled.

Classic

OIE



On-prem Connector setup in the admin console





Collections with Entitlement Management

Available in: *Okta Identity Governance*

Streamline and simplify entitlement management policies by packaging multiple apps and groups together, ensuring users receive the right access quickly and efficiently via birthright and ad hoc access requests.

Classic
OIE

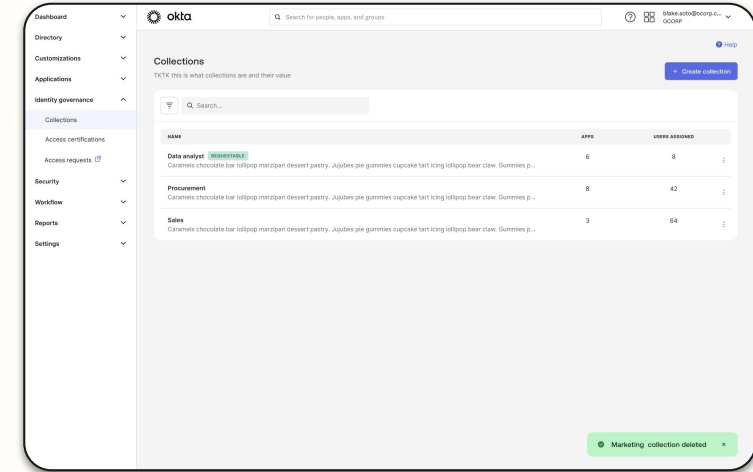
Entitlements in SAML Assertion and Token Claims

Available in: *Okta Identity Governance*

Enforce least privilege access with granular entitlements included in SAML assertions and token claims, reducing reliance on Okta groups to model authorization.

[Learn more](#)

Classic
OIE



Collections with Entitlement Management



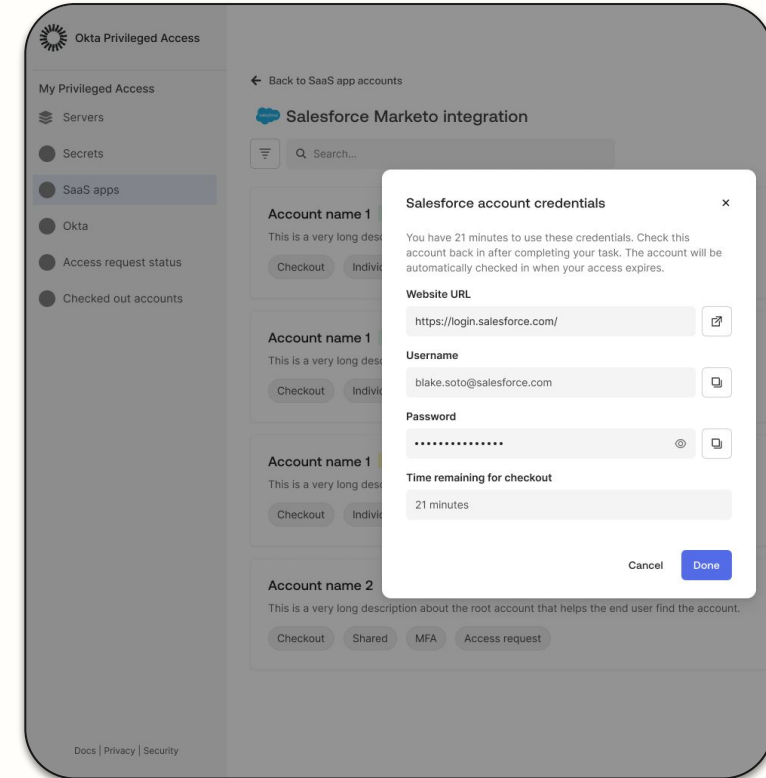


Secure SaaS Service Accounts

Available in: *Okta Privileged Access*

Protect service accounts for critical SaaS applications across an organization with account takeover, vaulting, and password rotations.

Classic
OIE



Secure SaaS Service Accounts





Platform Services

General Availability

Revamped Permissions UI

Available in: *Workforce Identity Cloud Platform. Authorized for FedRAMP Moderate/High/DOD IL4*

Improved user experience for admin role creation with a more scalable UI to accommodate new granular permissions. This helps super admins understand what permissions may be needed for a specific job to be done.

Classic OIE

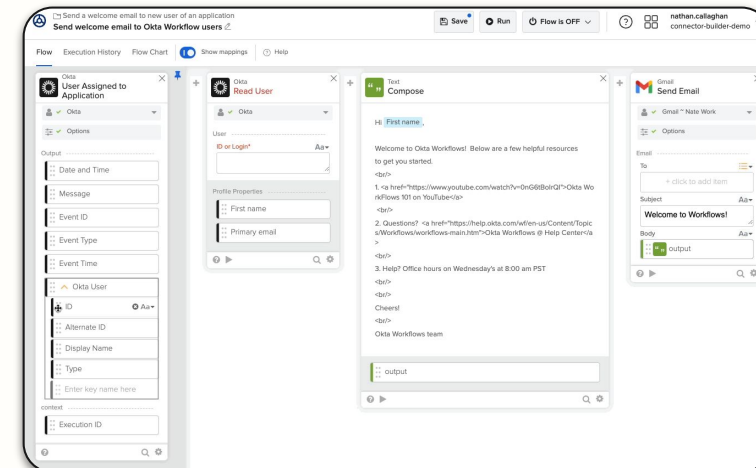
Workflows Authorized for FedRAMP High

Available in: *All Workflows, Authorized for FedRAMP High and eligible FedRAMP Moderate customers*

Unlock Workflows low- to no-code automation for FedRAMP High and eligible FedRAMP Moderate customers. Takes care of U.S. government (or organizations with FedRAMP compliance requirements) labor-intensive Identity processes — at scale — by replacing custom code and scripts.

[Learn more](#)

Classic OIE



Workflows Authorized for FedRAMP High





Dynamic Resource Sets

Available in: Workforce Identity Cloud Platform. Authorized for FedRAMP Moderate/High/DOD IL4

Dynamically assign resources to admins in custom admin roles.

[Learn more](#)

Classic

OIE

Okta Admin App Assignment

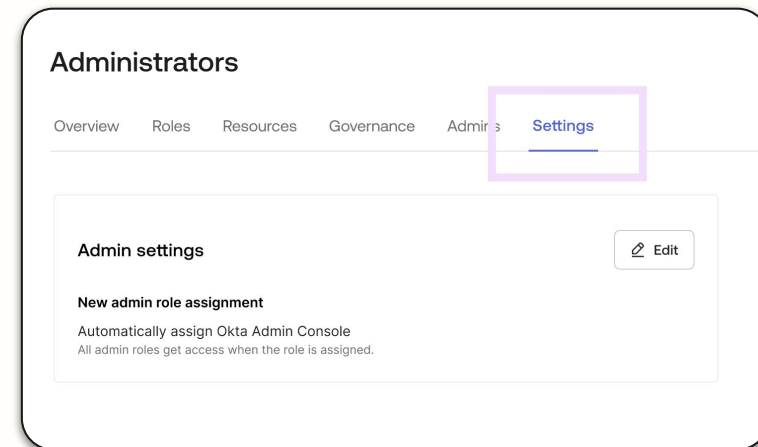
Available in: Workforce Identity Cloud Platform. Authorized for FedRAMP Moderate/High/DOD IL4

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

[Learn more](#)

Classic

OIE



Okta Admin App Assignment



Developer Resources

Okta Workforce Identity

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

Resources

Okta Architecture Center: Click [here](#)

Enterprise Readiness workshops: Click [here](#)

Developer blog: Click [here](#)

Languages and SDKs: Click [here](#)

Getting Started guides: Click [here](#)

Release Notes: Click [here](#)

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

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

OktaDev YouTube channel: Click [here](#)



Okta Customer Identity Releases

Okta Customer Identity—formerly known as Customer Identity Solution (CIS)—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 effectively.

Learn more about our new capabilities released in Q4 2024.



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





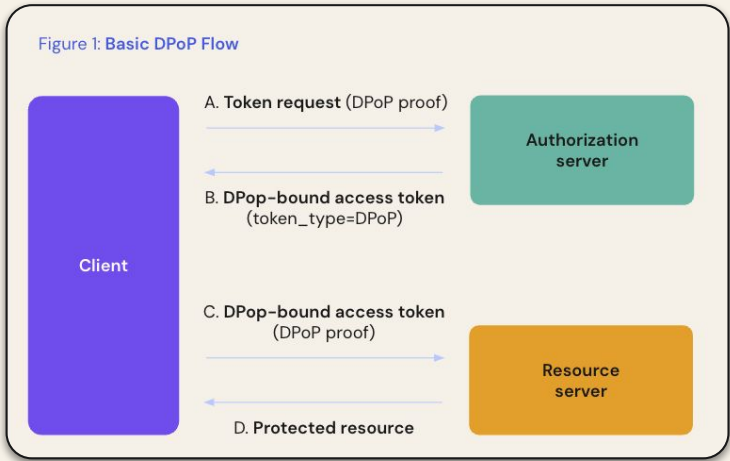
You asked, we listened.

Recent releases from this year

Demonstration of Proof of Possession (DPoP)

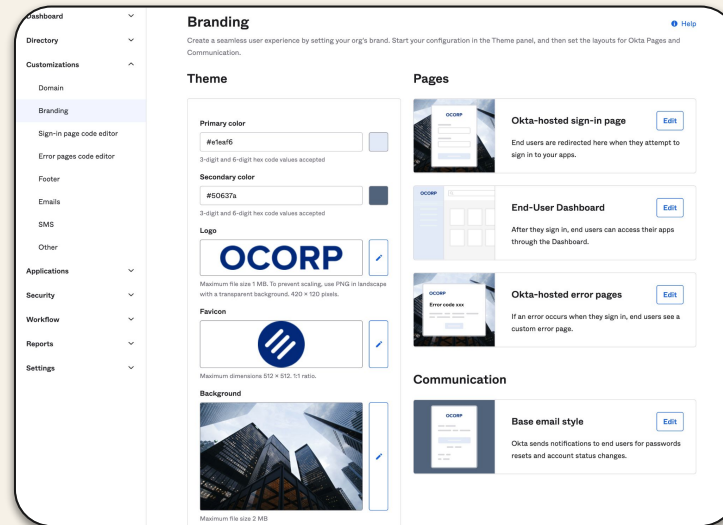
Cryptographically bind access tokens to a client for enhanced security. This secure alternative to bearer tokens prevents token theft and replay attacks, strengthening application and API security

Figure 1: Basic DPoP Flow



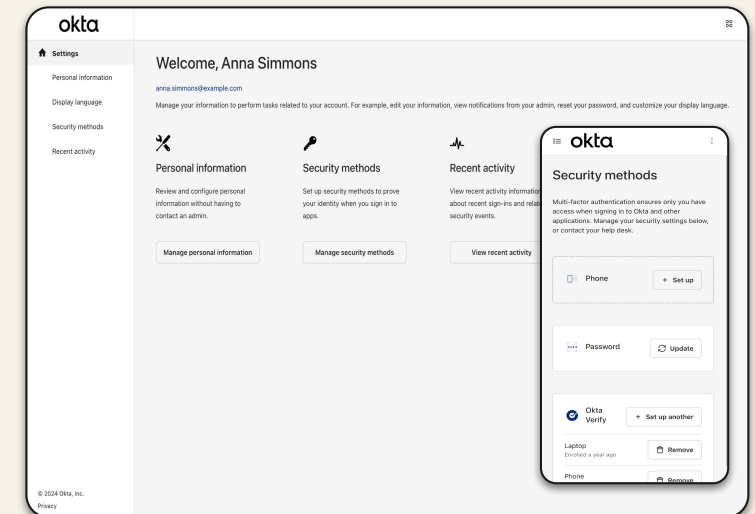
Multi-Brand

Set up multiple brands in a single Okta tenant including brand themes, custom domains, and end-user touch points like emails, sign in, and error pages.



New End User Profile & MFA Settings Page

Easily update your profile, manage MFA settings, and review recent activity—all from any device.



*Within platform performance limitations





Spotlight: Okta Customer Identity for US Public Sector

Secure public sector digital experiences with Okta Customer Identity

What is it?

A US FedRAMP and DOD authorized Okta Customer Identity ensures agencies can securely serve constituents in the digital age. Okta's advanced security features offer robust protection for safe and seamless service delivery. Integration with public and private sector digital identity infrastructure provides choice and convenience for government interactions.

Customer Challenge:

US public sector customers face growing pressure to meet strict compliance while delivering secure, seamless digital services. They must tackle rising fraud threats, scale for increased demand, and integrate with trusted Identity providers to build public trust.

Why this matters

- **Secure and Compliant Identity for US Public Sector Organizations:** Okta's cloud-native, FedRAMP and DoD authorizations provides assurances of compliance with strict security frameworks, making it ideal for organizations serving the US public sector.
- **Empowering Constituents and Mitigating Risks:** By enabling individuals to take control of their identities and accounts. Okta helps builds trust, protects against fraud, and provides secure access to public-facing applications.
- **Streamlining and Enhancing User Experiences:** It simplifies the verification process, accommodates large user volumes, and provides options like social login, reducing churn and efficient delivery of public benefits.

How to get it

Okta Customer Identity for US Public Sector is available to all Okta for Government Moderate (FedRAMP Moderate), Okta for Government High (FedRAMP High), and Okta for US Military (DoD Impact Level (IL) 4 customers. To use this solution, customers must be on the Okta Identity Engine.

[Contact us](#)





Okta Account Management Policies

Feature of: Okta Customer Identity / Available in: All SKUs, Authorized for FedRAMP Moderate/High/DOD IL4

A unified policy to manage authentication, recovery, and enrollment, providing granular control to strengthen defenses against social engineering attacks.

OIE

Add Rule

Rule name

Exclude users

IF User's IP is
Manage configuration for Networks

THEN Users can perform self-service Password change (from account settings)
 Password reset
 Unlock account

Recovery authenticators
Determine which authenticators a user will be asked for when recovering via self-service password reset or unlock account.

Access control
 Authentication policy
Use the Okta account management authentication policy to control conditions and authentication requirements.
 This rule (legacy)
Control access with this rule until you've reviewed the Okta account management policy.

Okta Account Management Policies





Okta Customer Identity

Early Access

Password Complexity Policy

Feature of: Okta Customer Identity / Available in: All Customer Identity SKUs

Allows customers to customize password requirements using Okta Expression Language to define restricted content. This will enhance password security with additional complexity requirements.

OIE

ID Proofing / Verification

Feature of: Okta Customer Identity / Available in: SSO/MFA

Use Okta's authentication policies with your identity verification provider to enforce ID verification. Strengthen defenses against social engineering with document and liveness checks, enhancing security and trust across onboarding, authentication, recovery, and support.

OIE

Authenticator Sequencing

*Feature of: Okta Customer Identity / Available in: Adaptive MFA
Authorized for FedRAMP Moderate/High/DOD IL4*

Design a specific sequence of authenticator methods that users must complete before accessing an app. This layered approach enhances application security and reduces the risk of account compromise.

OIE

Enhanced Dynamic Network Zone

Feature of: Okta Customer Identity / Available in: Adaptive MFA

Gain granular control over traffic with IP-based allow/deny lists. Block unauthorized access pre-authentication, reduce false positives, and enhance admin oversight with network filtering.

Classic

OIE

Verify your identity with Persona to continue

Verify your identity with Persona and share the results with Okta to finish activating your account.

Continue

[Back to sign in](#)

Persona's [Terms of Use](#) and [Privacy Policy](#) will apply to Persona's verification of your identity.

By clicking "Continue", I agree that Persona will share my verification results with Okta.

ID Proofing/Verification



okta