okta

Release Overview

for Early Access & General Availability in Q1 (January - March 2025)

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

Safe harbor

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

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

Okta 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 Product Roadmap Webinar

Get a sneak peek of upcoming product releases.

Register for the Okta 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.

Welcome to the Okta Platform Release Overview

Q1 2025

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

Explore how Okta Workforce Identity enhances security for devices and non-human identities.

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

Okta Workforce Identity enables customers to raise the bar on Identity security, unlock business growth with automation, and modernize IT to 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

Okta Workforce Identity

- Secure Identity Integrations
- Protect Non-Human Identities
- Advanced Posture Checks
- On-prem Connector

All features

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

Developer resources

Okta Platform brings the Identity Security Fabric to life

Secure Identity Products

Governance

- Okta Identity Governance

Posture Management

- Identity Security Posture Management

Okta Privileged Management

- Okta Privileged Access

Access Management

- Universal Directory
- Single Sign-On
- Adaptive MFA
- API Access Management
- Secure Partner Access
- Okta Access Gateway
- Customer Identity

Device Access

- Okta Device Access

Identity Threat Protection

- Okta Identity Threat Protection

Secure Identity Orchestration

Secure Identity Integrations

Infrastructure

IaaS

On Prem Servers

Applications

Cloud Apps

On Prem Apps

APIs

Public

Private

Identities

Directories

Non Human / AI Agents

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

okta

General Availability

Spotlight: Secure Identity Integrations (SII)

Deploy powerful protection in minutes across your most business-critical apps

What is it?

Secure Identity Integrations deliver powerful protection for your most critical SaaS apps. Go beyond SSO and MFA with out-of-the-box capabilities that streamline access, support compliance, and enable instant threat response and remediation. With solutions like fine-grained Entitlements Management, Identity Security Posture Management, and Universal Logout, you can safeguard users before, during, and after login. And because each integration deploys in under a minute, you get deep, hassle-free security without adding to your IT team's workload.

Customer Challenge:

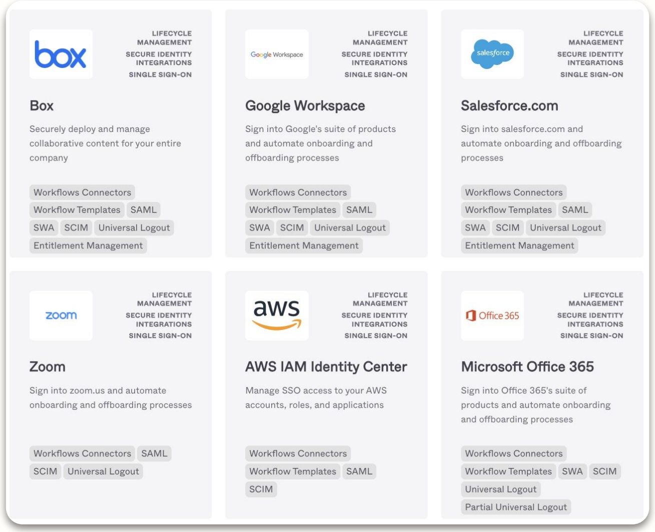
Managing identity across enterprise SaaS apps comes with serious challenges. Security gaps leave organizations vulnerable to breaches, yet many identity solutions only offer surface-level protection. At the same time, complex deployments and manual processes can drain IT resources and add unnecessary burden. Limited integration options can further restrict flexibility, forcing organizations to choose tools based on ease of connection rather than what's best.

Why this matters

- SIIs deliver the deep identity security capabilities needed to protect critical enterprise SaaS applications and strengthen overall security posture.
- Eliminate operational burdens with integrations that deploy in seconds and scale automatically—providing powerful security without added complexity.
- Give customers the freedom to choose the best SaaS apps for their business – without being locked into a single provider's ecosystem just to make integrating easier.

How to get it

Secure Identity Integrations are available without charge to customers who purchase Okta-aligned products. Integrations can be found on the Okta Integration Network (OIN) in the Secure Identity Integrations link in the left-hand navigation.



LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

Box

Securely deploy and manage collaborative content for your entire company

Workflows Connectors | Workflow Templates | SAML | SWA | SCIM | Universal Logout | Entitlement Management

LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

Google Workspace

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

Workflows Connectors | Workflow Templates | SAML | SWA | SCIM | Universal Logout | Entitlement Management

LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

Salesforce.com

Sign into salesforce.com and automate onboarding and offboarding processes

Workflows Connectors | Workflow Templates | SAML | SWA | SCIM | Universal Logout | Entitlement Management

LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

Zoom

Sign into zoom.us and automate onboarding and offboarding processes

Workflows Connectors | SAML | SCIM | Universal Logout

LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

AWS IAM Identity Center

Manage SSO access to your AWS accounts, roles, and applications

Workflows Connectors | Workflow Templates | SAML | SCIM

LIFECYCLE MANAGEMENT
SECURE IDENTITY INTEGRATIONS
SINGLE SIGN-ON

Microsoft Office 365

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

Workflows Connectors | Workflow Templates | SWA | SCIM | Universal Logout | Partial Universal Logout

okta

Early Access

Spotlight: Protect Non-Human Identities

Discover and secure undermanaged Privileged Service Accounts with the Okta platform

What is it?

Non-human identities (NHIs) often operate outside traditional Identity governance frameworks, leaving organizations vulnerable to security risks. Okta Identity Security Posture Management and Privileged Access help organizations discover, secure, and manage NHIs.

Customer Challenge:

Many organizations struggle with visibility and control over NHIs, leading to security risks such as credentials that are rarely rotated, accounts with excessive privileges, and no centralized enforcement. With the rise of AI-driven automation and machine-to-machine interactions, the number of NHIs is growing exponentially—expanding the attack surface and increasing the need for strong identity governance.

Okta addresses these risks by bringing visibility to undermanaged NHIs and providing centralized controls for access and security policies – without disrupting user productivity.

Why this matters

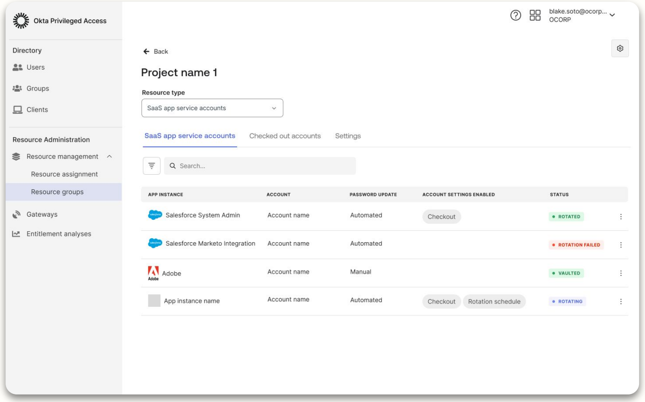
- **Security Gaps:** Unmanaged NHIs—including service accounts, automation scripts, and AI-powered agents—are a major attack vector due to static credentials, lack of MFA, and excessive privileges.
- **AI & Machine-to-Machine Scale:** NHIs outnumber human identities 20:1. The rapid growth of AI-driven workflows, chatbots, and autonomous agents has dramatically increased the number of NHIs interacting with business-critical applications. These identities now have greater access privileges, making them a prime target for attackers.
- **Compliance Risks:** Without clear ownership and governance, organizations struggle with audits and regulatory compliance, as NHIs often bypass traditional identity security frameworks.
- **Operational Efficiency:** Automating NHI discovery and governance with Okta reduces manual effort while improving security and access controls in AI-driven environm

How to get it

Okta Identity Security Posture Management and Privileged Access help organizations gain visibility, enforce least privilege, and remediate risks in real-time.

- Identity Security Posture Management is GA
- Okta Privileged Access is GA globally

Learn more



Project name 1

Resource type: SaaS app service accounts

SaaS app service accounts | Checked out accounts | Settings

APP INSTANCE	ACCOUNT	PASSWORD UPDATE	ACCOUNT SETTINGS ENABLED	STATUS
Salesforce System Admin	Account name	Automated	Checkout	● ROTATED
Salesforce Marketo Integration	Account name	Automated		● ROTATION FAILED
Adobe	Account name	Manual		● VAULTED
App instance name	Account name	Automated	Checkout Rotation schedule	● ROTATING

Early Access

Spotlight: Advanced Posture Checks

Go beyond patch management and enforce device compliance with extensible, real-time posture checks

What is it?

Advanced Posture Checks empower you to 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. This feature seamlessly connects with your technology ecosystem to gather signals that inform access policies and continuous risk assessment.

Customer Challenge:

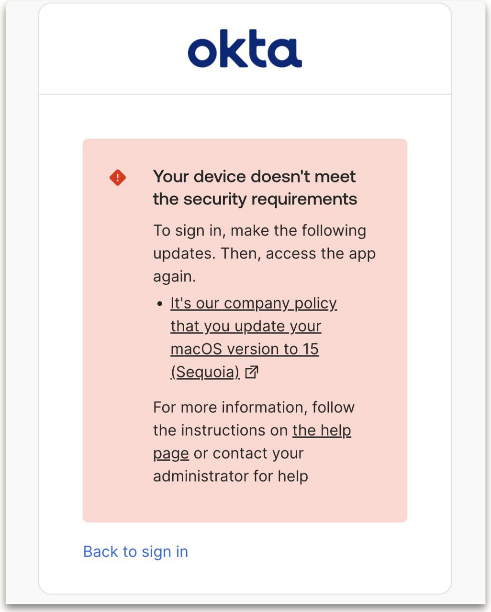
Non-compliant devices with access to resources are targets for bad actors, elevating security risk for the entire organization. However, managed devices are prone to MDM configuration drift due to policy enforcement delays and stale views of device compliance states.

Why this matters

- **Support Zero Trust Security**: Assess devices against predefined policies—collecting any device attribute from the device fleet in real time when starting a new session, opening a new app, or for continuous risk assessment with Identity Threat Protection—so that only secure and compliant devices can access corporate resources
- **Reduce IT Workload**: Enable end users to self-remediate with custom, detailed guidance on why access was denied and how to swiftly bring their devices into compliance to unblock access without burdening IT admins

How to get it

Advanced Posture Checks is available with Adaptive MFA and will be a self-service Early Access feature starting April 17.



okta

Your device doesn't meet the security requirements

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

- It's our company policy that you update your macOS version to 15 (Sequoia)

For more information, follow the instructions on the help page or contact your administrator for help

Early Access

Spotlight: On-prem Connector

Simplifying Governance for On-prem Applications

What is it?

Okta On-prem Connector is a new out-of-the-box connector that allows customers to integrate their on-premises apps with Okta Identity Governance, enabling the discovery, visibility, and management of fine-grained application entitlements within Okta.

Customer Challenge:

- Legacy on-prem systems remain critical but rely on outdated architectures.
- Managing on-prem and cloud systems creates operational silos and governance challenges.
- Disconnected governance exposes vulnerabilities, compliance gaps, and insider threats.

Why this matters

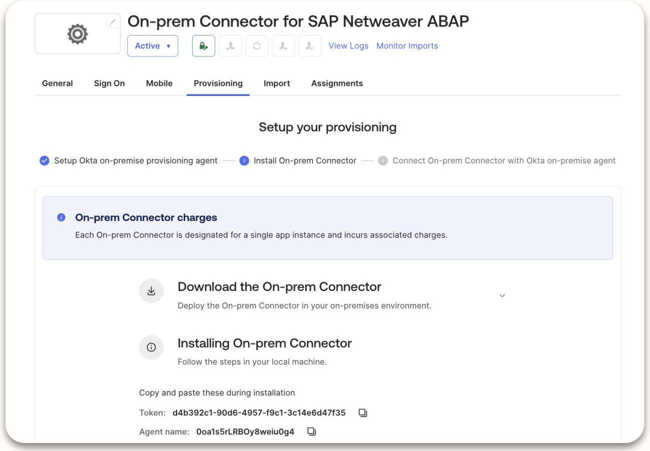
- **Extends Okta Identity Governance to On-Prem Applications**: Enables governance and lifecycle management for critical legacy applications like SAP, which remain essential to business operations.
- **Strengthens Security & Centralizes Identity Management:** Unified provisioning, deprovisioning, and entitlement management across cloud and on-prem environments while enforcing consistent access controls, visibility, and compliance
- **Accelerates Time-to-Value**: Simplifies deployment, reduces manual processes, and improves operational efficiency compared to legacy identity solutions.
- **Supports Migration from Legacy IGA Systems**: Helps organizations transition off SAP IDM and similar on-prem identity solutions as they reach end-of-life.

How to get it

The On-prem Connector is now available for Early Access (EA) starting with SAP NetWeaver ABAP and will be Generally Available (GA) by the end of H2.

Available as an add-on SKU with Okta Identity Governance

See the blog



On-prem Connector for SAP Netweaver ABAP

Setup your provisioning

✓ Setup Okta on-premise provisioning agent — 2 Install On-prem Connector — 3 Connect On-prem Connector with Okta on-premise agent

On-prem Connector charges

Each On-prem Connector is designated for a single app instance and incurs associated charges.

Download the On-prem Connector

Deploy the On-prem Connector in your on-premises environment.

Installing On-prem Connector

Follow the steps in your local machine.

Copy and paste these during installation

Token: d4b392c1-90d6-4957-f9c1-3c14e6d47f35

Agent name: 0oa1s5rLRBOy8weiu0g4

okta

Okta Workforce Identity Releases

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

Learn more about our new capabilities released in Q1 2025.

Easily identify the technology each release is available in*:

Classic | Okta Identity Engine (OIE)

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

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

Identity Security Posture Management (ISPM)

General Availability

Okta ISPM - Non Human Identities (NHI) v2

Feature of: Identity Security Posture Management (ISPM)

Gain enhanced visibility for Non-Human Identities with a dedicated dashboard section that tracks inventory and identifies 15+ specific NHI risks, including unrotated API keys and over-privileged service accounts. This comprehensive approach helps security teams quickly detect and remediate NHI-related vulnerabilities that could lead to breaches.

Classic

OIE

Connectors gallery

Feature of: Identity Security Posture Management (ISPM)

The enhanced Connectors Gallery offers a simplified self-service installation for Azure, GCP, Jira, Google Workspace, and GitHub integrations. The simplified settings page displays all available connectors, streamlining deployment and automating data collection across your technology ecosystem.

Classic

OIE

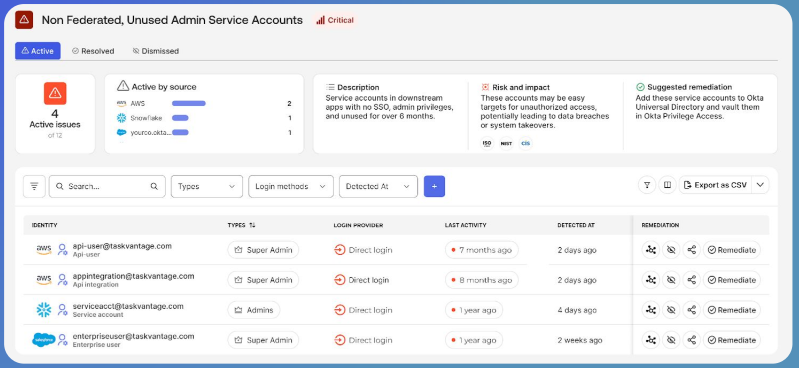
MFA and SSO deep analysis dashboard and org graph

Feature of: Identity Security Posture Management (ISPM)

The newly released MFA and SSO deep analysis dashboard delivers comprehensive visibility through consolidated reporting with per-app granularity. The dashboard displays MFA status at both user and app levels, highlights phishing-resistant authentication factors, and validates SSO implementation. An intuitive organizational graph provides a visual representation of your MFA and SSO deployment across the enterprise.

Classic

OIE



Non Federated, Unused Admin Service Accounts

4
Active issues
of 12

Active by source

AWS	2
Snowflake	1
yourco.okta...	1

Description
Service accounts in downstream apps with no SSO, admin privileges, and unused for over 6 months.

Risk and impact
These accounts may be easy targets for unauthorized access, potentially leading to data breaches or system takeovers.

Suggested remediation
Add these service accounts to Okta Universal Directory and vault them in Okta Privilege Access.

IDENTITY	TYPES	LOGIN PROVIDER	LAST ACTIVITY	DETECTED AT	REMEDIATION
aws api-user@taskvantage.com Api-user	Super Admin	Direct login	7 months ago	2 days ago	Remediate
aws appintegration@taskvantage.com Api integration	Super Admin	Direct login	8 months ago	2 days ago	Remediate
serviceacct@taskvantage.com Service account	Admins	Direct login	1 year ago	4 days ago	Remediate
salesforce enterpriseuser@taskvantage.com Enterprise user	Super Admin	Direct login	1 year ago	2 weeks ago	Remediate

Non Human Identities v2

Identity Security Posture Management (ISPM)

Early Access

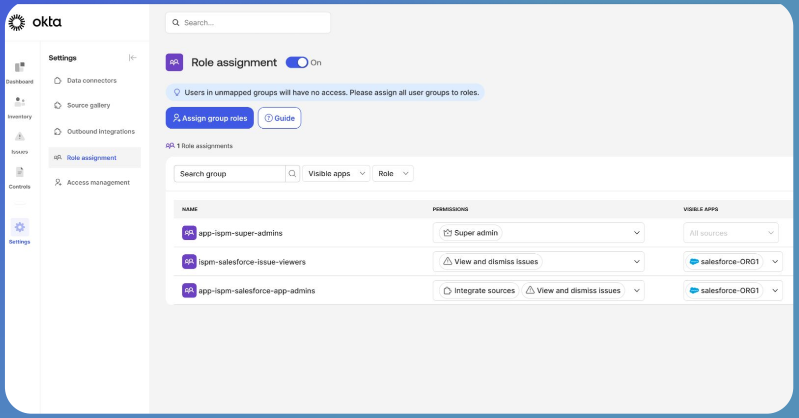
Role Based Access Control v1

Feature of: Identity Security Posture Management (ISPM)

App owners (e.g. Salesforce.com Admin) get limited access to ISPM – view only selected data sources, so that security teams can delegate issue resolution to app owners.

Classic

OIE



Role assignment On

Users in unmapped groups will have no access. Please assign all user groups to roles.

Assign group roles | Guide

1 Role assignments

NAME	PERMISSIONS	VISIBLE APPS
app-ispm-super-admins	Super admin	All sources
ispm-salesforce-issue-viewers	View and dismiss issues	salesforce-ORG1
app-ispm-salesforce-app-admins	Integrate sources View and dismiss issues	salesforce-ORG1

Role Based Access Control v1

Access Management

General Availability

Admin Initiated Universal Logout for Okta Access Gateway-protected Apps

Available in: Okta Access Gateway (OAG)

Admins can trigger Universal Logout to revoke app sessions protected by Okta Access Gateway.

Learn more

OIE

Authentication Method Chain (formerly known as Authenticator Sequencing)

Available in: Adaptive Multi-Factor Authentication. Authorized for FedRAMP Moderate/High/DOD IL4

Strengthen security by requiring users to complete a specific sequence of authenticators before accessing an app.

Learn more

OIE

Desktop Password Sync for macOS Sequoia

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

Set auth policies requiring Identity Provider (IdP) password authentication at FileVault, Unlock, and Login screens. Users can sync passwords directly from FileVault.

Learn more

OIE

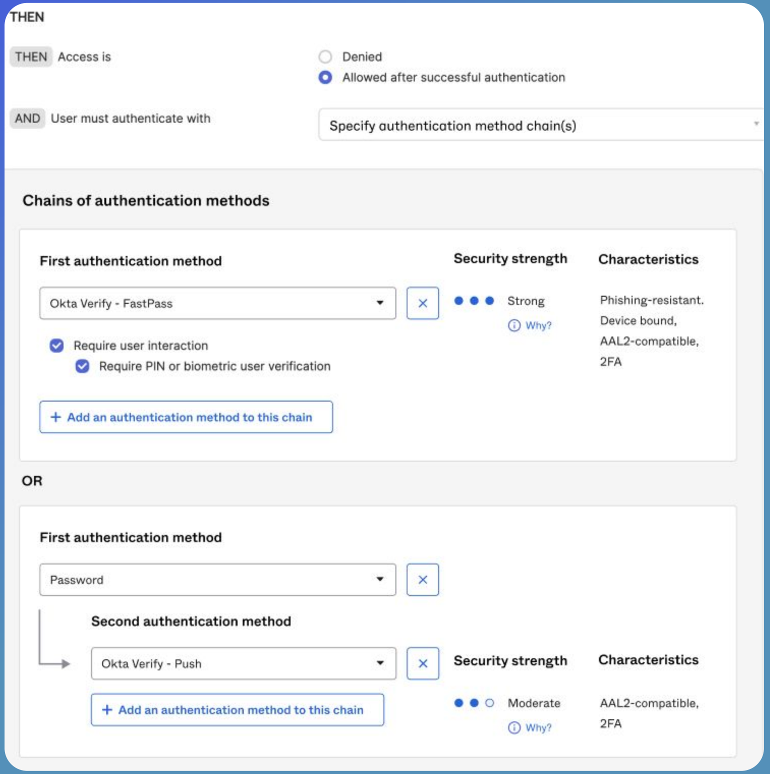
Enhance Account Linking Restriction

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

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

Learn more

OIE



THEN

THEN Access is
○ Denied
● Allowed after successful authentication

AND User must authenticate with: Specify authentication method chain(s)

Chains of authentication methods

First authentication method: Okta Verify - FastPass
☑ Require user interaction
☑ Require PIN or biometric user verification

Security strength: ● ● ● Strong

Characteristics: Phishing-resistant. Device bound, AAL2-compatible, 2FA

OR

First authentication method: Password

Second authentication method: Okta Verify - Push

Security strength: ● ● ○ Moderate

Characteristics: AAL2-compatible, 2FA

Authentication Method Chain

Access Management

General Availability

FIDO2 Security Keys for Desktop MFA for Windows

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

Allow your users to login to their Windows machines with supported FIDO2 security keys.

Learn more

OIE

Okta Account Management Policy

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.

Learn more

OIE

Push notifications with number challenge for Desktop MFA

Available in: Device Access. *Authorized for FedRAMP Moderate/High/DOD IL4
*This feature does not meet NIST 800-63 requirements.

Enforce number challenges for push notifications in Desktop MFA for Windows and macOS.

Learn more

OIE

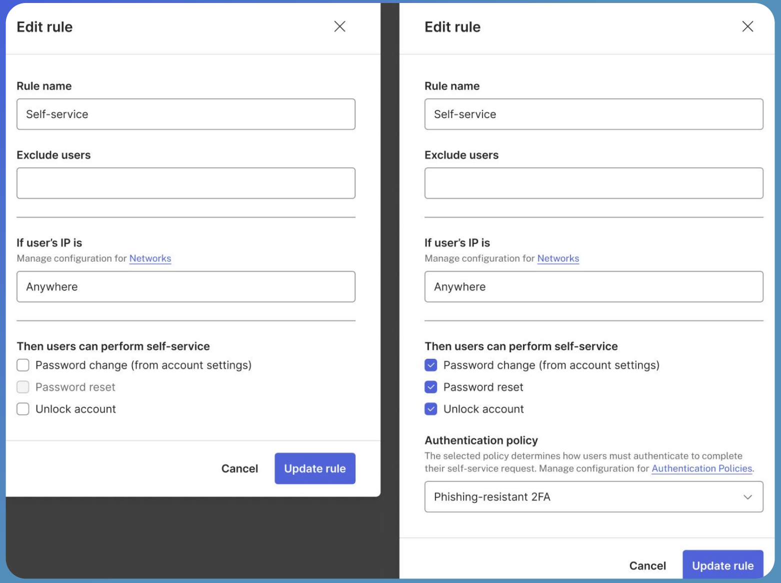
Support Group Sync for OIDC Identity Provider

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

Admins can now do Group Assignments for Just-In-Time (JIT) settings to specific groups or missing groups, simplifying migration to OIDC.

Learn more

OIE



Edit rule

Rule name: Self-service

Exclude users:

If user's IP is
Manage configuration for Networks
Anywhere

Then users can perform self-service
☐ Password change (from account settings)
☐ Password reset
☐ Unlock account

Cancel | Update rule

Edit rule

Rule name: Self-service

Exclude users:

If user's IP is
Manage configuration for Networks
Anywhere

Then users can perform self-service
☑ Password change (from account settings)
☑ Password reset
☑ Unlock account

Authentication policy
The selected policy determines how users must authenticate to complete their self-service request. Manage configuration for Authentication Policies.
Phishing-resistant 2FA

Cancel | Update rule

Okta Account Management Policy

Access Management

General Availability

Universal Logout Support for Cerby Applications

Available in: Identity Threat Protection with Okta AI. Authorized for FedRAMP Moderate/High/DOD IL4

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

Learn more

OIE

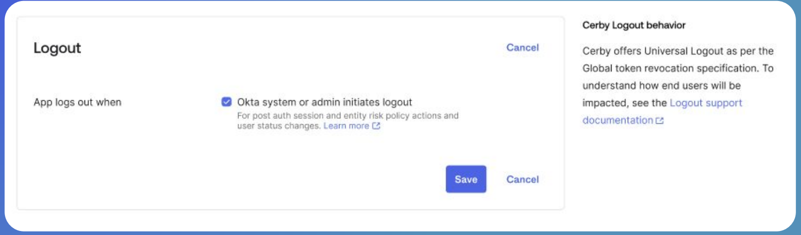
Identity Verification Integration with Persona

Available in: Multi-Factor Authentication, Adaptive Multi-Factor Authentication. Authorized for FedRAMP Moderate/High/DOD IL4

Use Okta and Persona to enforce ID verification across critical touch points of the user journey, including onboarding, authentication, and recovery.

Learn more

OIE



Logout

App logs out when ☑ Okta system or admin initiates logout

For post auth session and entity risk policy actions and user status changes. Learn more

Cerby Logout behavior

Cerby offers Universal Logout as per the Global token revocation specification. To understand how end users will be impacted, see the Logout support documentation

Universal Logout Support for Cerby Application

Access Management

Early Access

Authentication Method Reference (AMR) Claims Mapping

Available in: Multi-Factor Authentication. 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.

Learn more

OIE

Claims Sharing Between Okta Orgs

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

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

Learn more

Classic

OIE

Entitlements in Assertion and Token Claims

Available in: Okta Identity Governance (OIG). Authorized for FedRAMP Moderate, Supported in FedRAMP High/DOD IL4

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

Granular Admin Permissions to Access Identity Providers

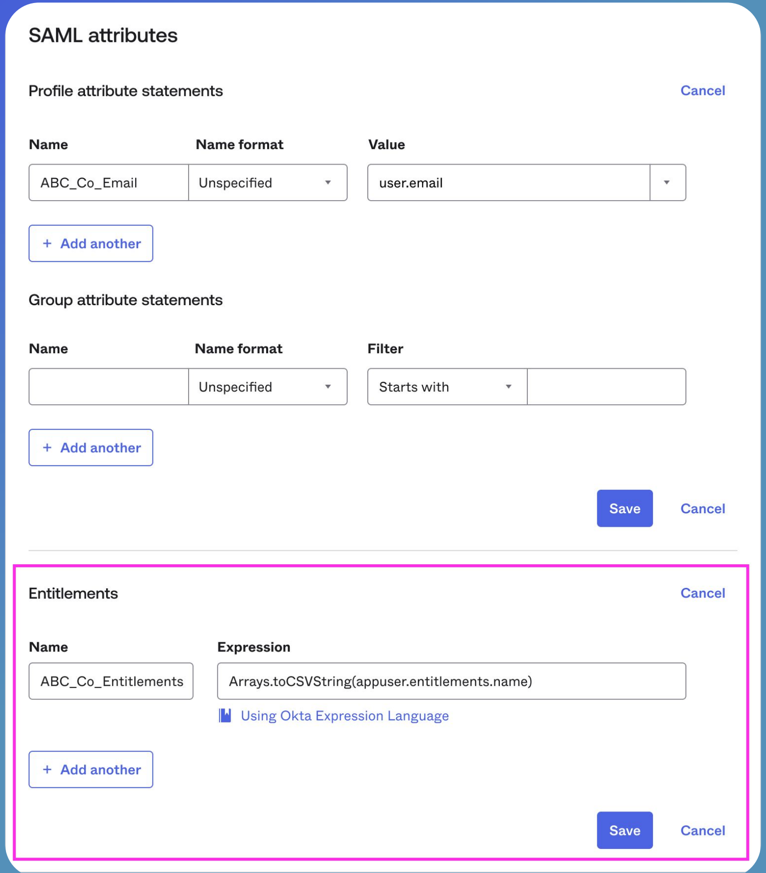
Available in: All SKUs. Supported in FedRAMP Moderate/High/DOD IL4

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

Classic

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

okta

Access Management

Early Access

Identity Verification Integration with Incode

Available in: Multi-Factor Authentication, Adaptive Multi-Factor Authentication. Authorized for FedRAMP Moderate/High/DOD IL4

Use Okta and Incode to enforce ID verification across critical touch points of the user journey, including onboarding, authentication, and recovery. Learn more

OIE

Okta Access Gateway Secure-By-Design Changes

Available in: Okta Access Gateway (OAG)

By default, the OAG admin console will be accessible only on the local network and require a password change for both the admin console and CLI. Learn more

OIE

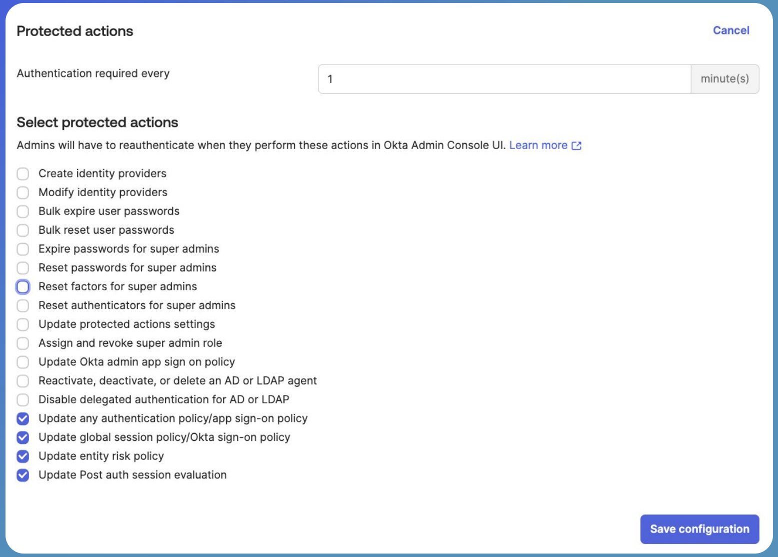
Policy Updates as Protected Actions

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

Admins must complete step-up authentication when updating app sign-on, global sign-on, ITP, and account management policies in the Okta Admin Console. This prevents a bad actor from making updates when they have access to an admin session.

Learn more

OIE



Protected actions

Authentication required every: 1 minute(s)

Select protected actions

Admins will have to reauthenticate when they perform these actions in Okta Admin Console UI. Learn more

- ☐ Create identity providers
- ☐ Modify identity providers
- ☐ Bulk expire user passwords
- ☐ Bulk reset user passwords
- ☐ Expire passwords for super admins
- ☐ Reset passwords for super admins
- ☐ Reset factors for super admins
- ☐ Reset authenticators for super admins
- ☐ Update protected actions settings
- ☐ Assign and revoke super admin role
- ☐ Update Okta admin app sign on policy
- ☐ Reactivate, deactivate, or delete an AD or LDAP agent
- ☐ Disable delegated authentication for AD or LDAP
- ☑ Update any authentication policy/app sign-on policy
- ☑ Update global session policy/Okta sign-on policy
- ☑ Update entity risk policy
- ☑ Update Post auth session evaluation

Policy Updates as Protected Actions

Identity Management

General Availability

Contains Search

Available in: Universal Directory (UD). Authorized for FedRAMP Moderate

Introduces the contains search operator for users and groups in both the UI and via API, and for devices and realms via API. Facilitates searches without needing to recall exact names.

Learn more

Classic

OIE

End-to-end encryption for AD Agent

Available in: Universal Directory (UD). Authorized for FedRAMP Moderate/High/DOD IL4

Add an extra layer of security with monitoring for AD agent configuration file and message-level encryption for each payload between Okta and AD agent.

Learn more

Classic

OIE

Group Description for Active Directory Groups

Available in: Universal Directory (UD). Authorized for FedRAMP Moderate/High/DOD IL4

Surface Active Directory descriptions for any AD sourced groups in Okta during Access Request and Access Certification tasks.

Classic

OIE

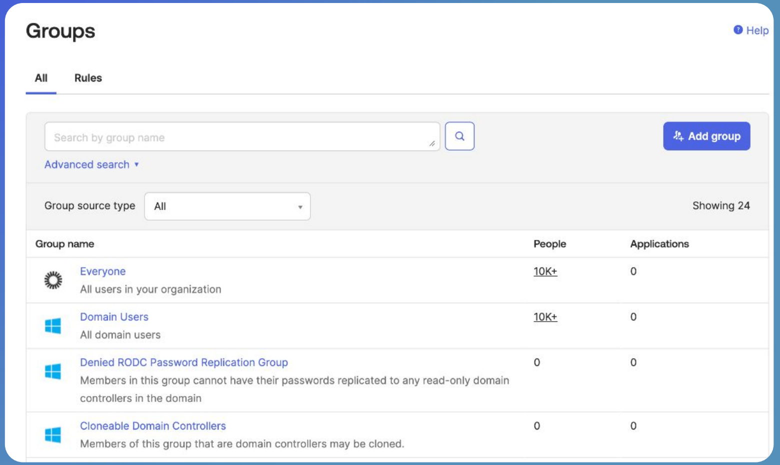
Secure AD Agent Config File

Available in: Universal Directory (UD). Authorized for FedRAMP Moderate/High/DOD IL4

Secure configuration of AD Agents by monitoring sensitive attributes to protect against threats or unexpected changes on-prem.

Classic

OIE



Groups

Group source type: All

Showing 24

Group name	People	Applications
Everyone All users in your organization	10K+	0
Domain Users All domain users	10K+	0
Denied RODC Password Replication Group Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain	0	0
Cloneable Domain Controllers Members of this group that are domain controllers may be cloned.	0	0

Group Description for Active Directory Groups

Identity Management

General Availability

Simplifying Identity Complexity with Realms

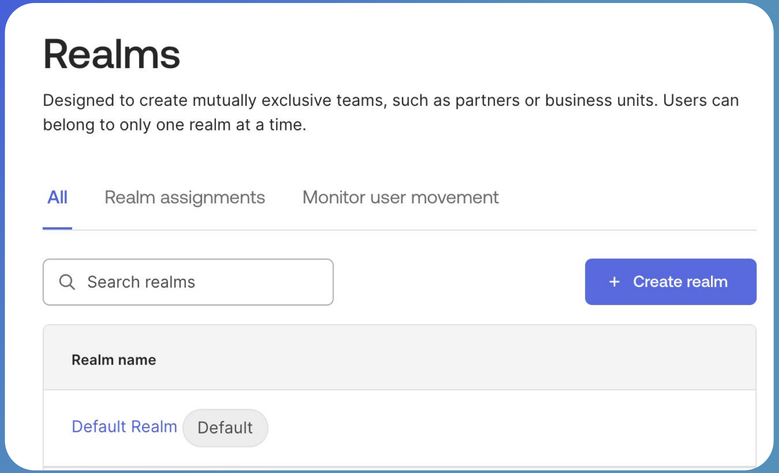
Available in: Okta Identity Governance (OIG) or Secure Partner Access (SPA)

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

Learn more

Classic

OIE



Realms

Designed to create mutually exclusive teams, such as partners or business units. Users can belong to only one realm at a time.

Realm name
Default Realm Default

Simplifying Identity Complexity with Realms

Identity Management

Early Access

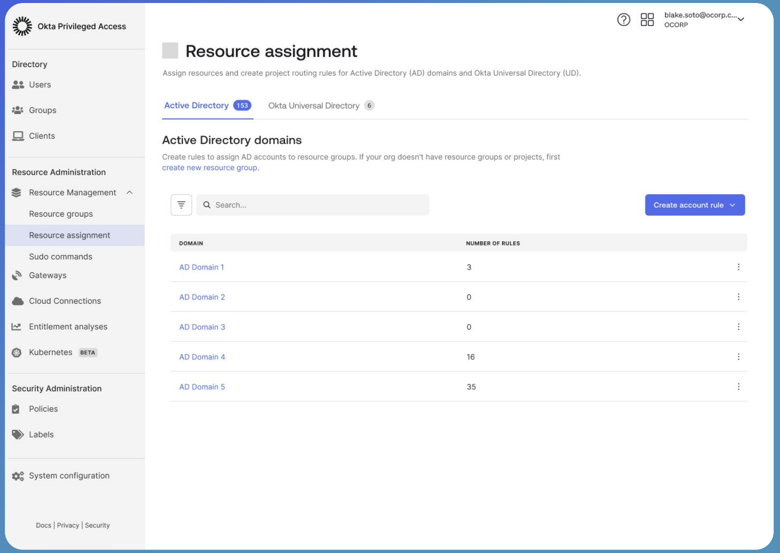
Active Directory Integration with Okta Privileged Access

Available in: Okta Privileged Access (OPA)

Okta Privileged Access Active Directory integration helps reduce risks associated with undermanaged privileged Active Directory accounts. Okta Privileged Access will discover accounts and manage the passwords, enforce access controls such as RBAC, MFA, Access Requests and Check-Out with time-based-limits, while also providing an audit trail for monitoring and compliance.

Classic

OIE



Resource assignment

Assign resources and create project routing rules for Active Directory (AD) domains and Okta Universal Directory (UD).

Active Directory domains

Create rules to assign AD accounts to resource groups. If your org doesn't have resource groups or projects, first create new resource group.

DOMAIN	NUMBER OF RULES
AD Domain 1	3
AD Domain 2	0
AD Domain 3	0
AD Domain 4	16
AD Domain 5	35

Active Directory Integration

Identity Governance

General Availability

Governance for Disconnected Apps

Available in: Okta Identity Governance (OIG)

Support governance for on-premise, disconnected apps for which out-of-the-box connectors/integrations are not used.

Classic

OIE

Governance APIs

Available in: Okta Identity Governance (OIG)

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

Classic

OIE

Enhanced Group Remediation for Access Certifications

Available in: Okta Identity Governance (OIG)

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

Classic

OIE

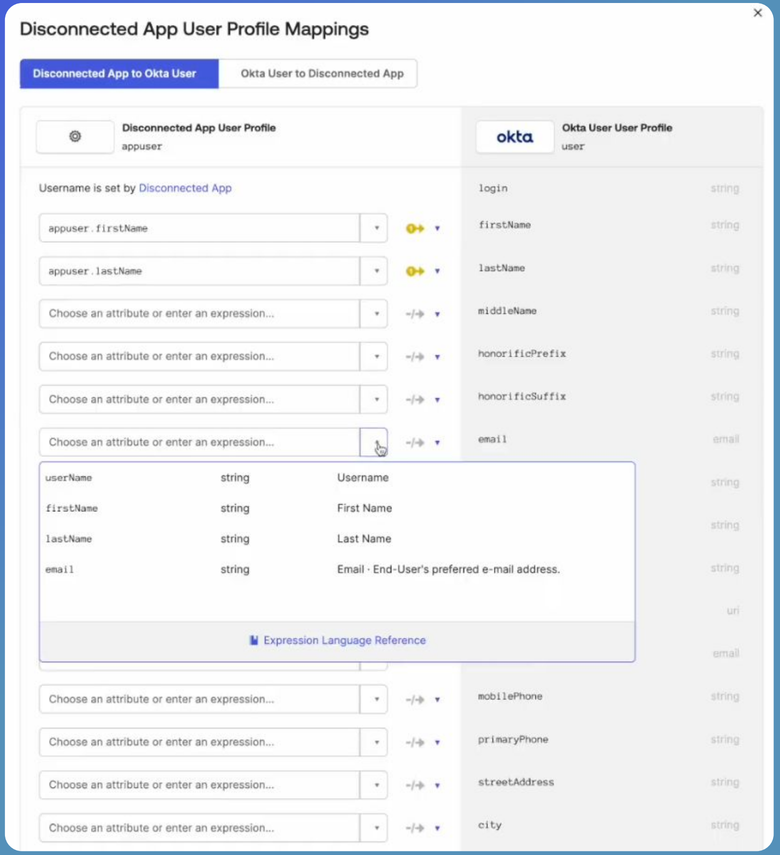
OIN Apps for Entitlement Management

Available in: Okta Identity Governance (OIG)

Discover, import, store, and manage entitlements within Okta via bundles, policies, and rules with out-of-the-box integrations for 2 OIN apps: Splunk, Zoho Mail

Classic

OIE



Disconnected App User Profile Mappings

Disconnected App to Okta User | Okta User to Disconnected App

Disconnected App User Profile
appuser

okta Okta User User Profile
user

Username is set by Disconnected App

	login	string
appuser.firstName	firstName	string
appuser.lastName	lastName	string
Choose an attribute or enter an expression...	middleName	string
Choose an attribute or enter an expression...	honorificPrefix	string
Choose an attribute or enter an expression...	honorificSuffix	string
Choose an attribute or enter an expression...	email	email
		string
		string
		string
		uri
		email
Choose an attribute or enter an expression...	mobilePhone	string
Choose an attribute or enter an expression...	primaryPhone	string
Choose an attribute or enter an expression...	streetAddress	string
Choose an attribute or enter an expression...	city	string

userName	string	Username
firstName	string	First Name
lastName	string	Last Name
email	string	Email · End-User's preferred e-mail address.

Expression Language Reference

Attribute mapping for Disconnected Apps

Identity Governance

Early Access

Governance Analyzer Risk Scoring

Available in: Okta Identity Governance (OIG)

Harness risk signals from across Okta to drive better governance decision making with Governance Analyzer.

Classic

OIE

Resource Collections

Available in: Okta Identity Governance (OIG)

Streamline entitlement management by packaging multiple apps and groups together, ensuring users receive the right access quickly and efficiently while reducing the complexity for requests and approvers.

Classic

OIE

On-prem Connector

Available as an add-on SKU with Okta Identity Governance (OIG)

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

Classic

OIE

Entitlements in SAML Assertion and Token Claims

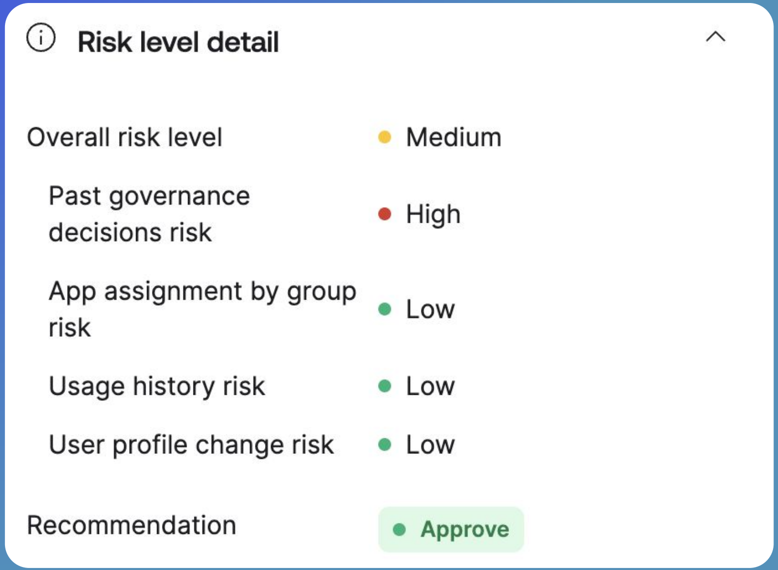
Available in: Okta Identity Governance (OIG)

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



Risk level detail

Overall risk level	● Medium
Past governance decisions risk	● High
App assignment by group risk	● Low
Usage history risk	● Low
User profile change risk	● Low
Recommendation	● Approve

Governance Analyzer Risk Scoring

Platform Services

General Availability

Role-Based Access Control (RBAC)

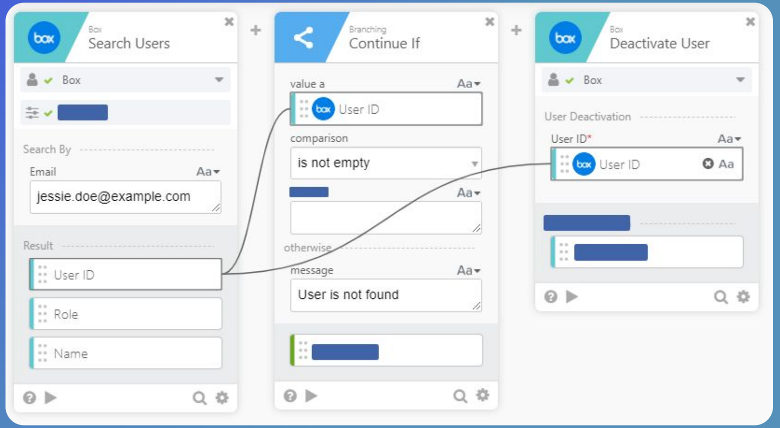
Available in: Workflows. Supported in FedRAMP Moderate, Authorized for FedRAMP High

Allows customers to expand their use of Workflows beyond Super-Admins, enabling more team members to have access and permission to create workflows for critical use cases.

Learn more

Classic

OIE



Email: jessie.doe@example.com

comparison: is not empty

message: User is not found

Role-Based Access Control (RBAC)

Platform Services

Early Access

Okta first-party app switcher

Feature of: Workforce Identity + Customer Identity / Available in: All SKUs. Supported in FedRAMP Moderate

An admin utility for quick navigation between Okta first-party apps.

Classic

OIE

Unified Platform look and feel for Okta apps

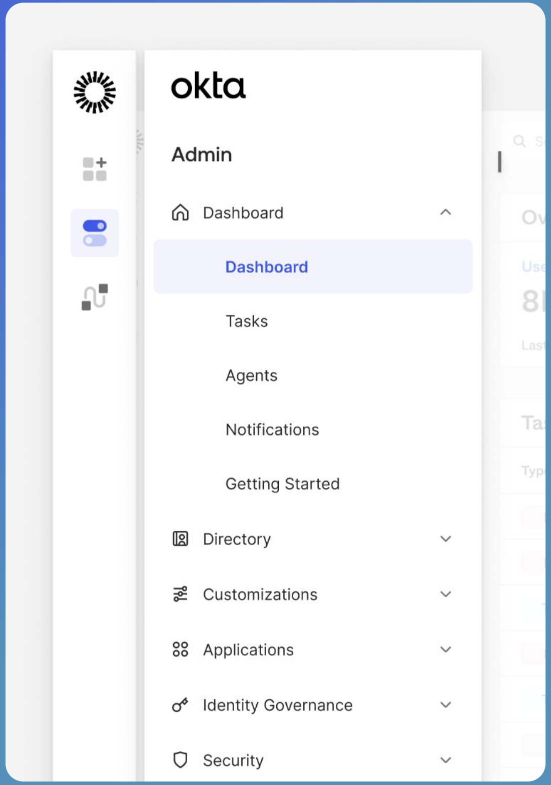
Feature of: Workforce Identity / Available in: Platform. Supported in FedRAMP Moderate

Provides ease of use with consistent side and top navigation across Okta first party apps.

Learn more

Classic

OIE



Unified Platform look and feel – Navigation Rail

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

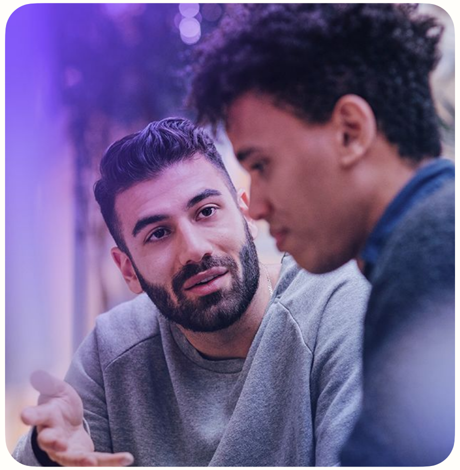
Okta Customer Identity Releases

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.

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

General Availability

Spotlight: Okta Account Management Policy

Customize your identity experience with granular control over sign-in and recovery

What is it?

Okta Account Management Policy centralizes sign-in, recovery, and enrollment, enabling granular control to tailor security based on user context. This strengthens defenses against social engineering while ensuring a seamless user experience.

Customer Challenge:

Organizations face increasing social engineering threats, where attackers exploit weak authentication and recovery processes.

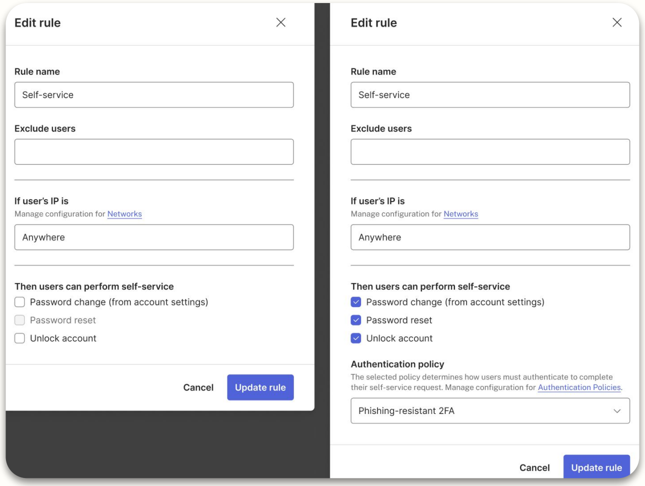
Businesses struggle to balance security and user experience, lacking granular controls to enforce tailored policies for diverse user populations, leading to friction, security gaps, and compliance challenges.

Why this matters

- Prevent social engineering and fraud by enforcing secure authentication and recovery policies
- Balance security with ease of access, reducing friction for different user groups
- Customize authentication and recovery flows to fit business needs, ensuring security without one-size-fits-all restrictions
- Centralize policy control for sign-in, recovery, and enrollment, reducing complexity and administrative overhead

How to get it

Okta Account Management Policy is available with All SKUs on the Okta Platform (OIE Only)



Edit rule

Rule name: Self-service

Exclude users:

If user's IP is
Manage configuration for Networks
Anywhere

Then users can perform self-service
□ Password change (from account settings)
□ Password reset
□ Unlock account

Cancel | Update rule

Edit rule

Rule name: Self-service

Exclude users:

If user's IP is
Manage configuration for Networks
Anywhere

Then users can perform self-service
☑ Password change (from account settings)
☑ Password reset
☑ Unlock account

Authentication policy
The selected policy determines how users must authenticate to complete their self-service request. Manage configuration for Authentication Policies.
Phishing-resistant 2FA

Cancel | Update rule

Okta Customer Identity

General Availability

Authentication Method Chain (formerly known as Authenticator Sequencing)

Available in: Adaptive Multi-Factor Authentication. Authorized for FedRAMP Moderate/High/DOD IL4

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

OIE

Okta Account Management Policy

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

Support Group Sync for OIDC Identity Provider

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

Admins can now do Group Assignments for Just-In-Time (JIT) settings to specific groups or missing groups, simplifying customer identity migration to OIDC.

OIE

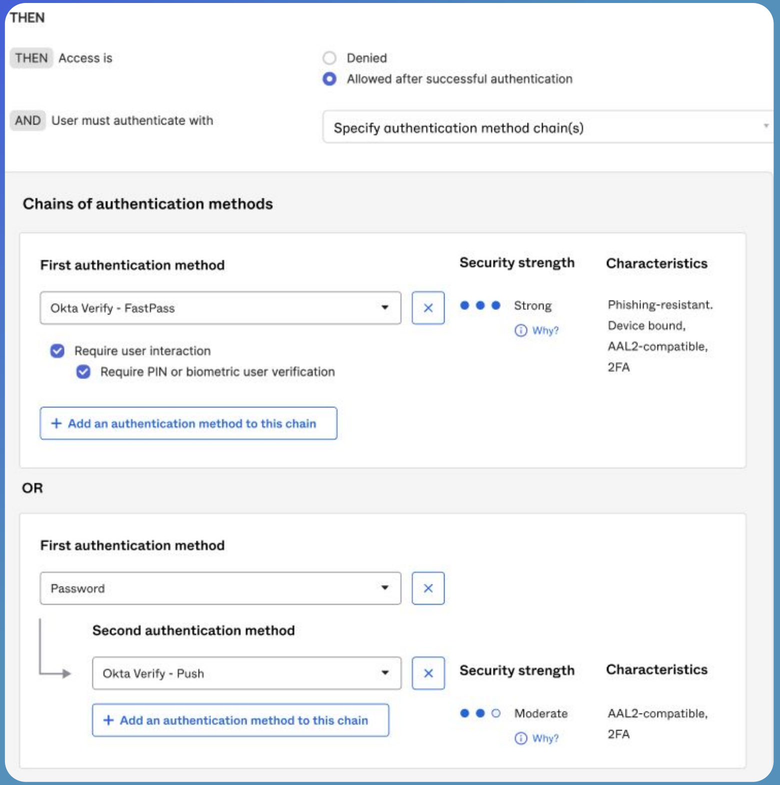
Unified Platform look and feel for Okta Dashboard

Available in: Platform. Supported in FedRAMP Moderate

Provides ease of use with consistent side and top navigation across Okta first party apps.

Classic

OIE



THEN

THEN Access is
○ Denied
● Allowed after successful authentication

AND User must authenticate with: Specify authentication method chain(s)

Chains of authentication methods

First authentication method: Okta Verify - FastPass
☑ Require user interaction
☑ Require PIN or biometric user verification
Security strength: ●●● Strong (Why?)
Characteristics: Phishing-resistant, Device bound, AAL2-compatible, 2FA

+ Add an authentication method to this chain

OR

First authentication method: Password

Second authentication method: Okta Verify - Push
Security strength: ●●○ Moderate (Why?)
Characteristics: AAL2-compatible, 2FA

+ Add an authentication method to this chain

Authentication Method Chain

Okta Customer Identity

General Availability

Role-Based Access Control (RBAC) for Workflow Admins

Classic | OIE

Available in: Workflows. Supported in FedRAMP Moderate, Authorized for FedRAMP High

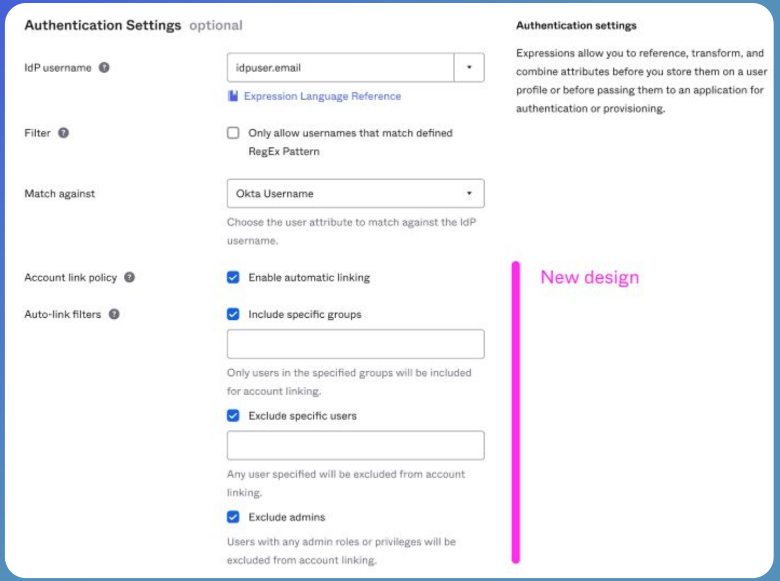
Allows customers to expand their use of Workflows beyond Super-Admins, enabling designated users to create and manage workflows securely for critical use cases.

Enhance Account Linking Restriction

Classic | OIE

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

Strengthen security by enforcing policy-based controls that restrict account linking to designated accounts, helping to ensure compliance and reducing unauthorized access risks.



Authentication Settings optional

IdP username: idpuser.email

Expression Language Reference

Filter: □ Only allow usernames that match defined RegEx Pattern

Match against: Okta Username

Choose the user attribute to match against the IdP username.

Account link policy: ☑ Enable automatic linking

Auto-link filters: ☑ Include specific groups

Only users in the specified groups will be included for account linking.

☑ Exclude specific users

Any user specified will be excluded from account linking.

☑ Exclude admins

Users with any admin roles or privileges will be excluded from account linking.

Authentication settings

Expressions allow you to reference, transform, and combine attributes before you store them on a user profile or before passing them to an application for authentication or provisioning.

New design

Enhance Account Linking Restriction

Okta Customer Identity

Early Access

Policy Updates as Protected Actions

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

When App sign on policies, global sign on policies, ITP policies, account management policies are updated in the admin console, the admin is required to complete step up authentication. This prevents a bad actor from making updates when they have access to an admin session.

OIE

Okta Access Gateway Secure-By-Design Changes

Feature of: Okta Access Gateway

By default, the OAG admin console will be accessible only on the local network and require a password change for both the admin console and CLI.

OIE

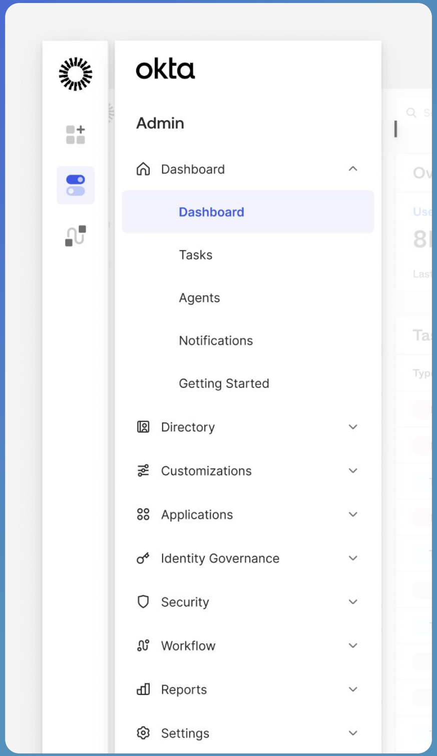
Okta first-party app switcher

Feature of: product / Available in: SKU. Supported in FedRAMP Moderate

Provide admins with a seamless inter-app switching experience and a single place to house all relevant Okta apps.

Classic

OIE



Unified Platform look and feel – Navigation Rail

okta