okta

Release Overview

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

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

US Public Sector Resource Page

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 US Public Sector Release Overview

Q1 2025

Welcome back to Okta's Quarterly Release Overview for US Public Sector. We've made great strides to sharing our exciting updates and innovations for Okta Administrators that work for or service the U.S. Public Sector, or have certain compliance requirements.

We hope you enjoy exploring how the Okta platform enhances mission security before accessing an app, for Windows and macOS desktops, and for recovery policies.

Navigating the overview

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

Okta Workforce Identity

- Okta Workforce Identity overview
- Release overviews

Okta Customer Identity

- Okta Customer Identity overview
- Release overviews

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.

Access Management

General Availability

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

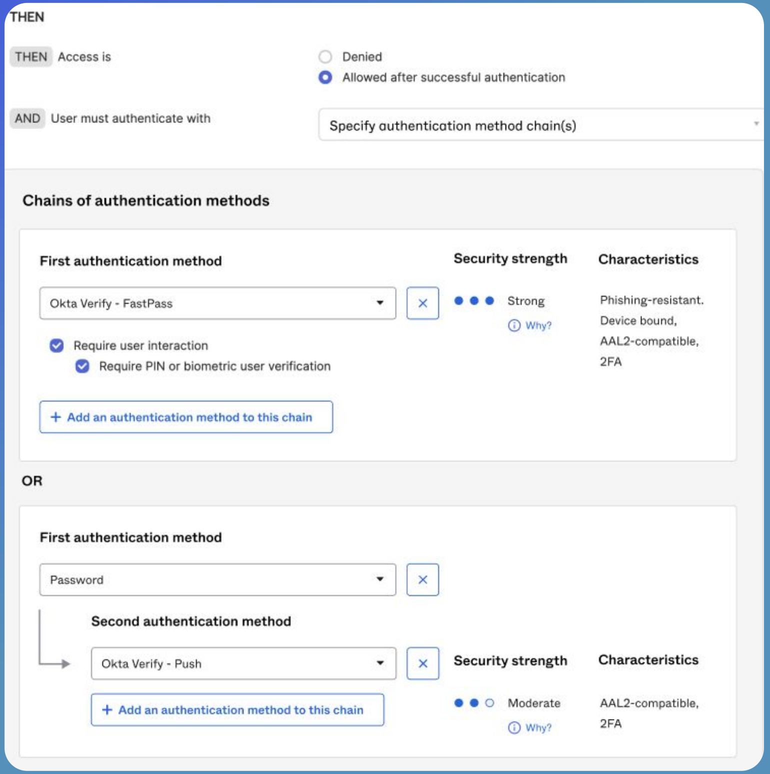
Enhance Account Linking Restriction

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 ✕

Security strength: ●●● Strong (Why?)

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

☑ Require user interaction
☑ Require PIN or biometric user verification

+ 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

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

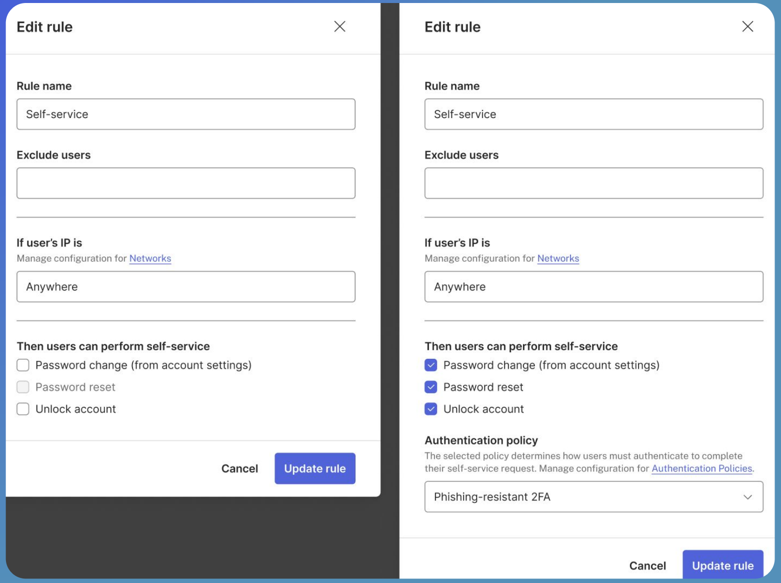
Support Group Sync for OIDC Identity Provider

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

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

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

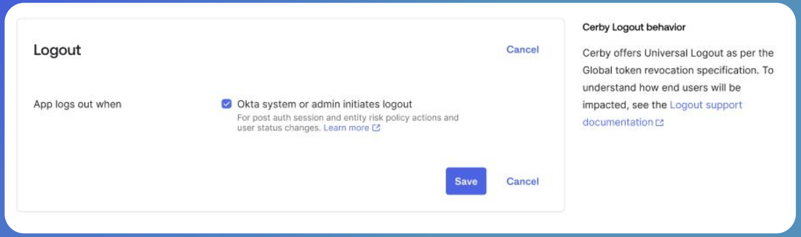
Identity Verification Integration with Persona

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

Cancel

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

Okta Workforce Identity

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

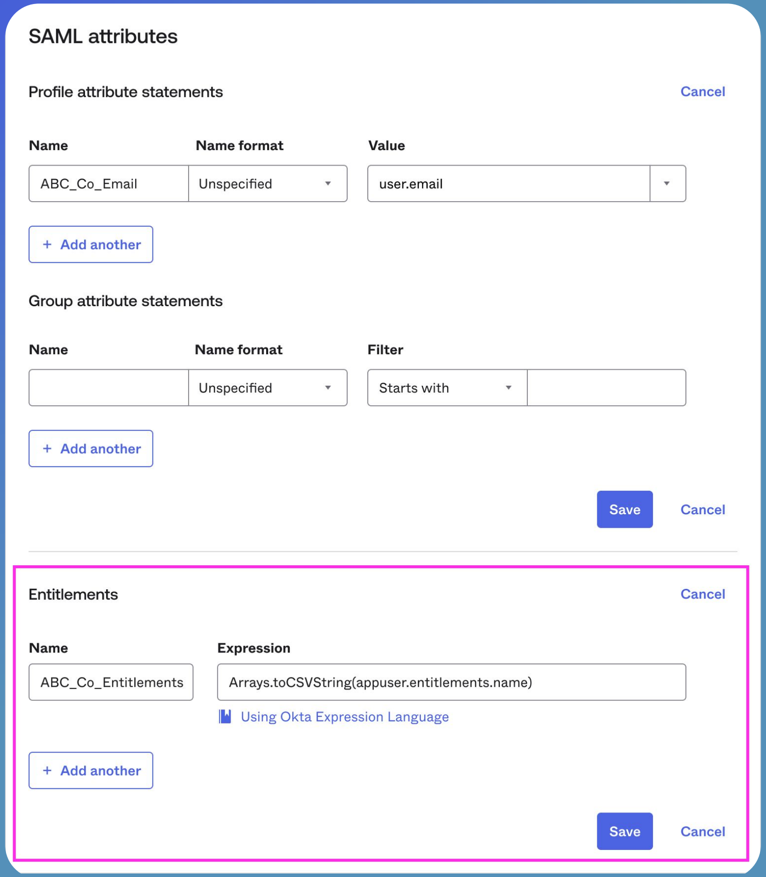
Available in: All SKUs. Supported in FedRAMP Moderate/High/DOD IL4

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

Name	Name format	Value
ABC_Co_Email	Unspecified	user.email

Group attribute statements

Name	Name format	Filter	
	Unspecified	Starts with	

Entitlements

Name	Expression
ABC_Co_Entitlements	Arrays.toCSVString(appuser.entitlements.name)

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

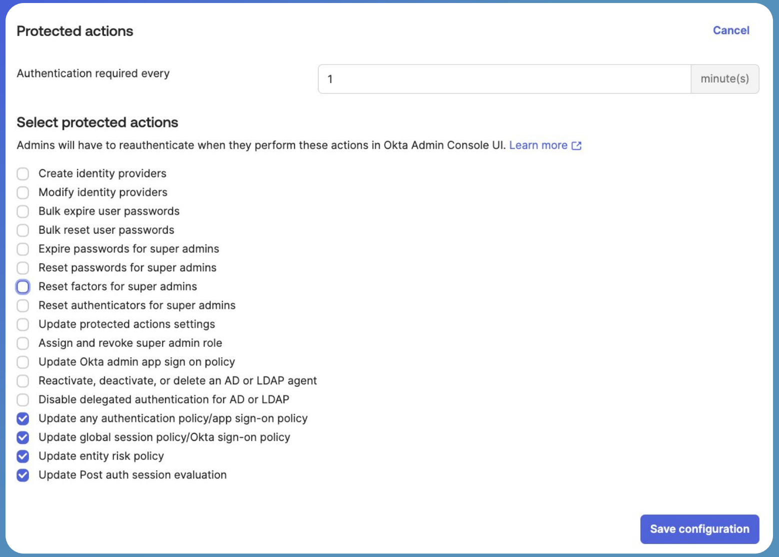
Policy Updates as Protected Actions

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

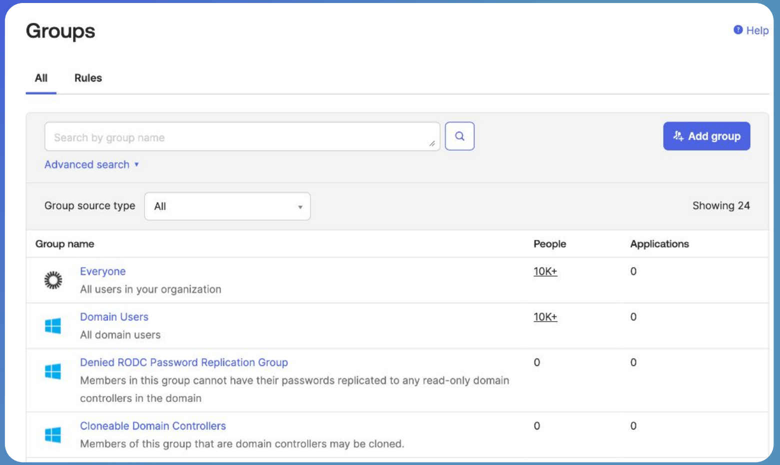
Secure AD Agent Config File

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



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

Platform Services

General Availability

Role-Based Access Control (RBAC)

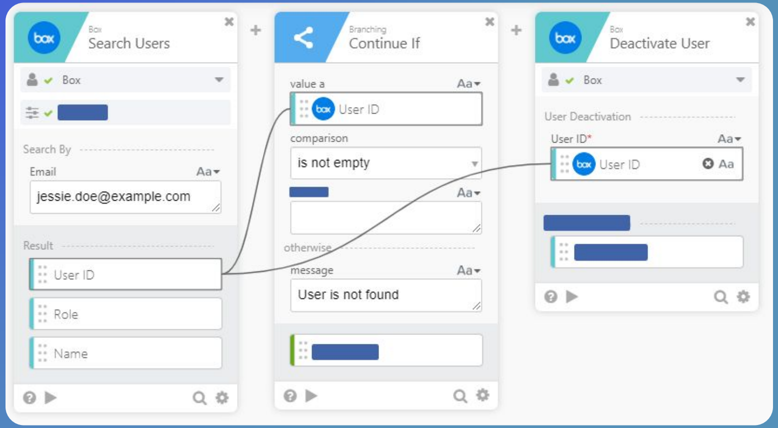
Available in: Workflows. Supported in FedRAMP Moderate, Authorized for FedRAMP High

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



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

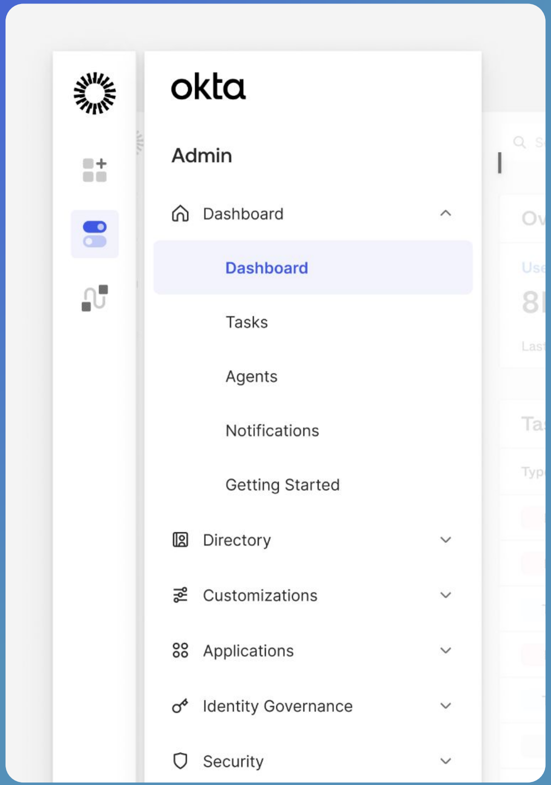
Feature of: Workforce Identity / Available in: Platform. Supported in FedRAMP Moderate

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

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

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

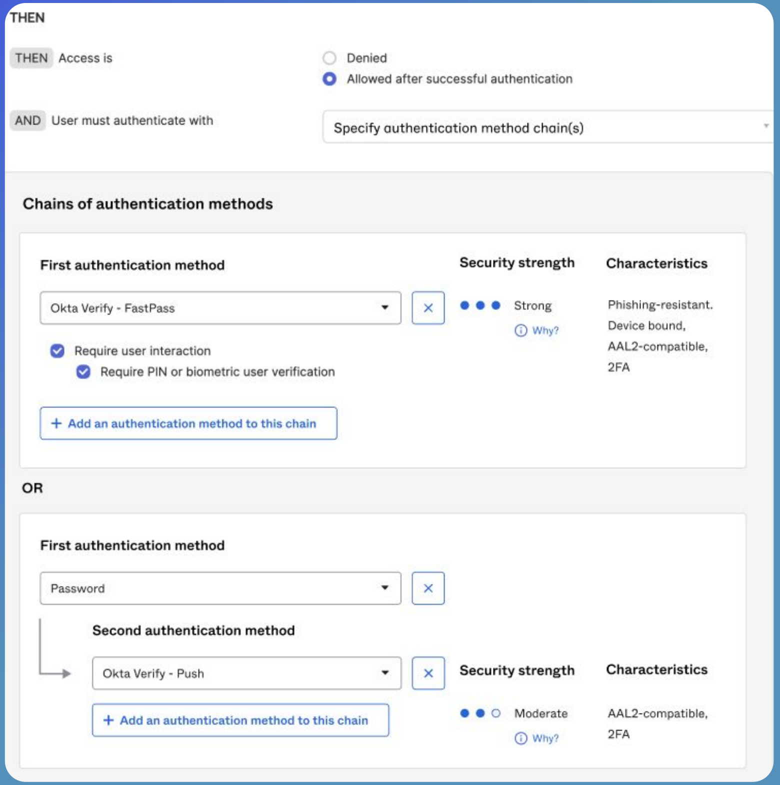
Unified Platform look and feel for Okta Dashboard

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
Security strength: ●●● Strong
Characteristics: Phishing-resistant. Device bound, AAL2-compatible, 2FA
☑ Require user interaction
☑ Require PIN or biometric user verification

OR

First authentication method: Password
Second authentication method: Okta Verify - Push
Security strength: ●●○ Moderate
Characteristics: AAL2-compatible, 2FA

×
ⓘ Why?
+ Add an authentication method to this chain
×
×
+ Add an authentication method to this chain
ⓘ Why?

Authentication Method Chain

Okta Customer Identity

General Availability

Role-Based Access Control (RBAC) for Workflow Admins

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.

Classic

OIE

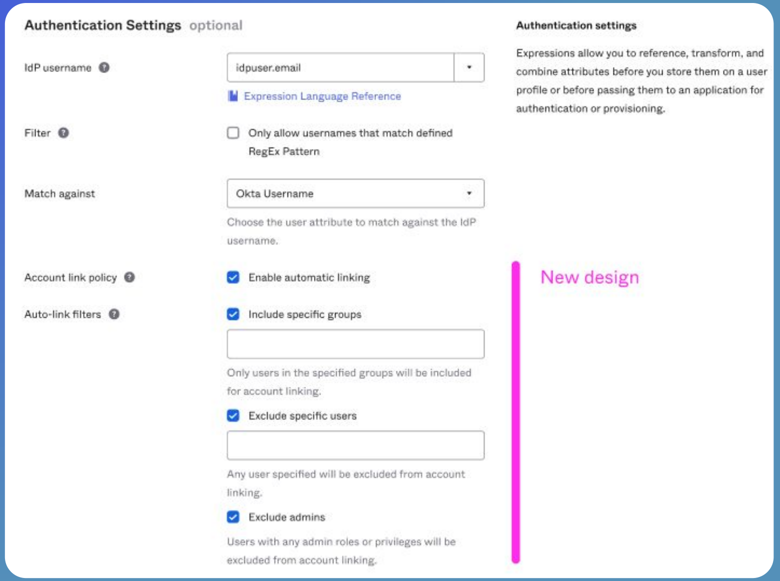
Enhance Account Linking Restriction

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.

Classic

OIE



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

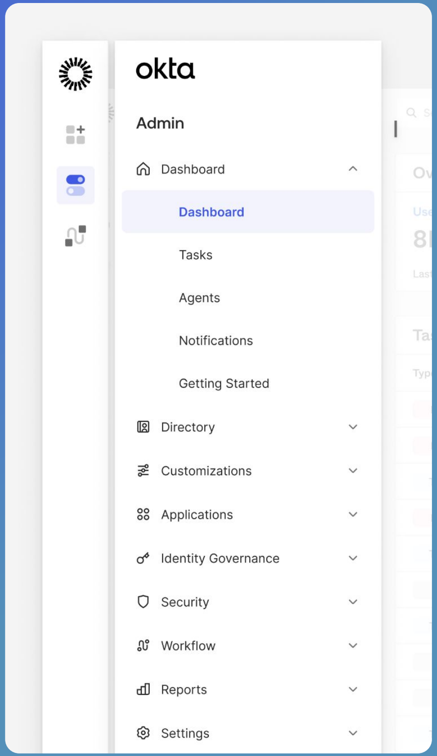
Okta first-party app switcher

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