



# Release Overview

for Early Access & General Availability in Q2 (April – May 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](https://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 key innovations spotlighted in Launch Week 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 webinar [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

**Q2 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 US Public Sector, or have certain compliance requirements.

We hope you enjoy exploring how the Okta platform enhances mission security with enhanced identity federation, support for External Authentication Methods like Microsoft Entra, Okta's latest Accessibility Compliance Reports, and more.



# Navigating the overview

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

## Okta Workforce Identity

- Spotlight
- Okta Workforce Identity overview
- Release overviews

## Okta Customer Identity

- Okta Customer Identity overview
- Release overviews





# Spotlight: Okta US Public Sector compliance roadmap updates

## What is it?

Okta's comprehensive platform now delivers new authorized and audit-ready identity solutions for the US public sector. Our integrated Identity Governance, Workflows, and Threat Protection with Okta empower agencies to modernize operations while ensuring enhanced support in identity management.

### Customer Challenge:

- Achieve measurable modernization and efficiency goals while demonstrating strict compliance
- Keep risks at or below specific acceptable levels
- Address resource constraints and skills shortages

## Why this matters

- Okta's solution provides a unified platform that delivers real-time cybersecurity readiness and mission-aligned workforce productivity.
- Through customized identity flows, continuous intelligence on access patterns, and unparalleled visibility, public sector organizations can proactively identify and mitigate threats, streamline operations, and achieve measurable cost savings.

## How to get it

- [Announcement blog](#)
- [Product Assessment support page](#)
- Same product SKUs with the cell add-ons
  - Okta for Government Moderate
  - Okta for Government High
  - Okta for US Military



# Okta Workforce Identity Releases

Okta Workforce Identity brings all of your identities—from users and devices to AI agents—into a single security fabric.

Our latest capabilities extend this fabric, helping you harden privileged AD accounts, automate threat response across your security stack, and enforce least privilege for admins.

Easily identify the technology each release is available in\*:

Classic

Okta Identity Engine (OIE)



# Access Management

## General Availability

### Authentication Method Reference (AMR) Claims Mapping

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

Enhance Identity federation by enabling secure, seamless access to resources across Okta Orgs.

[Learn more](#)

Classic

OIE

### Claims Sharing between Okta and External IdPs

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

Enhance identity federation by enabling secure, seamless access to resources across Okta and third-party IDPs without compromising security.

Learn more: [SAML](#) | [OIDC](#)

Classic

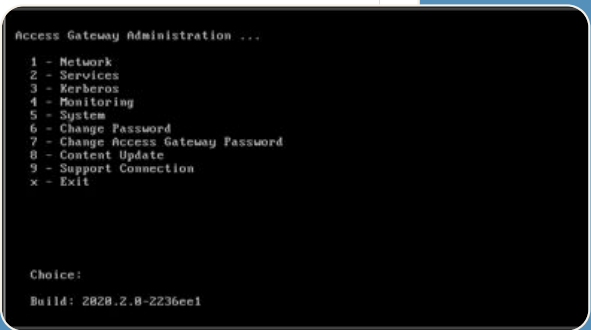
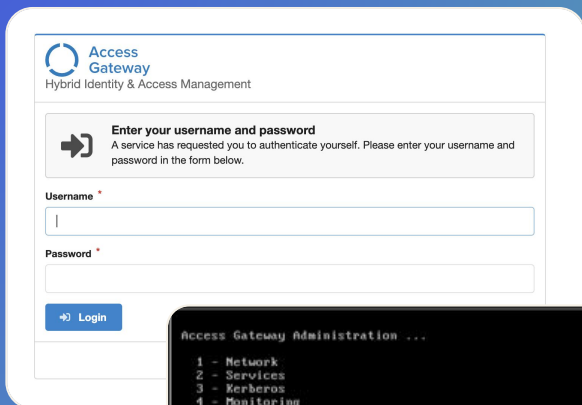
OIE

### OAG Secure-By-Design Changes

Available in: Okta Access Gateway. || Supported in: FedRAMP Moderate/High/DOD IL4

OAG admin console will only be accessible on the local network by default and forces change of admin password for both admin console and admin management CLI. These changes are made to honor Okta's secure by design commitment.

OIE



OAG Secure-By-Design Changes





# Access Management

## General Availability

### Desktop MFA Recovery for macOS

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

Prevent productivity disruption by securely enabling admins to provide end users with time-limited recovery codes to login to their devices in the event of a lost phone, security key, etc.

[Learn more](#)

OIE

### Entitlements in Assertion and Token Claims

Available in: Okta Identity Governance (OIG). || Supported in: DOD IL4

Admins can now configure custom claims in SAML Assertion attributes and OpenID Connect tokens, enforcing least privileges and reducing reliance on groups.

[Learn more](#)

Classic

OIE

### Granular Admin Permissions to Access Identity Providers

Available in: Okta Identity Engine (OIE). || Authorized in: FedRAMP Moderate/High/DOD IL4

Admins can now assign specific IdPs to other admins through granular admin permissions. Improve security posture by granting only authorized users access the configuration of IdPs.

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



# Access Management

## General Availability

### Policy Updates as Protected Actions

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

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

Classic

OIE

### Same-Device Enrollment for Okta Verify

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

Enable improved Okta Verify and FastPass end user enrollment flows for desktops and mobile devices.

Classic

OIE

### Okta Verify Troubleshooter for iOS

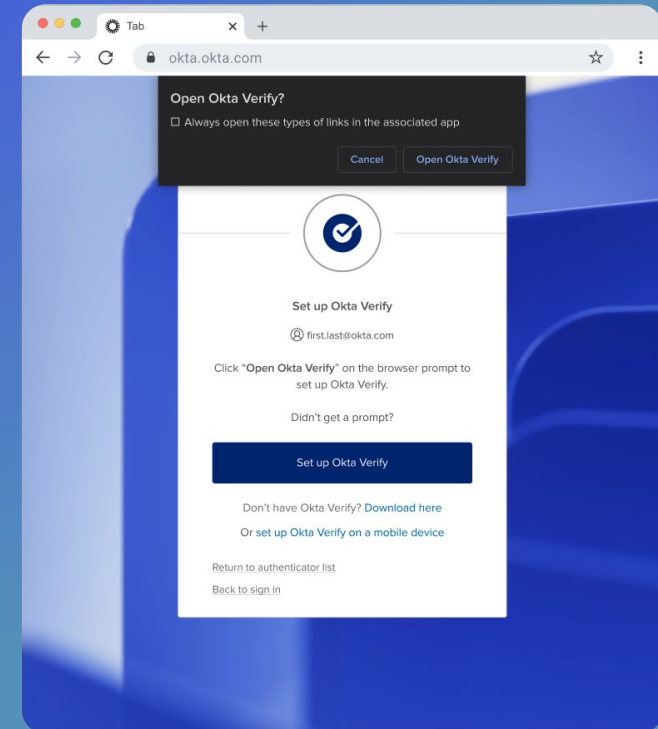
Available in: All SKUs. || Authorized in: FedRAMP Moderate/High/DOD IL4

Empower users to troubleshoot push notification and FastPass issues within the Okta Verify app.

[Learn more](#)

Classic

OIE



Same-Device Enrollment for Okta Verify



# Access Management

## Early Access

### Advanced Posture Checks

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

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

[Learn more](#)

OIE

### Android Device Trust for Device Assurance

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

Enforce an extensive array of additional device checks on Android as part of a Device Assurance policy.

[Learn more](#)

OIE

### Augmenting appID Context for OIDC and SAML applications

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

Passes application details (ID, Name) to external IdPs during Okta-initiated federation (SAML/OIDC) to enable richer security and policy decisions at the IdP.

Classic

OIE

#### macOS Update - Ensure 4th latest version is installed

Checks macOS devices for 4th latest version requirement.

##### Assign variable for this check

Variable names are used to reference this device check when used as a condition in policies.

Variable name

##### Platforms to check against

Select the platforms to check against. Okta supports checks for macOS and Windows machines.

Platform ☒ macOS ☐ Windows

##### Write the query

Write or paste in your query used for this device check.

Select a device to test query against

```
WITH
  reference_version AS (
    SELECT '13.2.1' AS minimum_version,
    version_split AS (
      SELECT version AS current_version,
      -- Split minimum_version strings
      CAST(SPLIT(minimum_version, ".") AS int) AS min_ver_major,
      CAST(SPLIT(minimum_version, ".") AS int) AS min_ver_minor,
      CAST(SPLIT(minimum_version, ".") AS int) AS min_ver_patch,
      -- Split installed version strings
      COALESCE(minor, 0) AS current_ver_major,
      COALESCE(minor, 0) AS current_ver_minor,
      COALESCE(patch, 0) AS current_ver_patch
    FROM os_version
    LEFT JOIN reference_version
  ),
  failure_logic AS (
    -- Logic to determine if the device is out of date
  )
```

Advanced Posture Checks



# Access Management

## Early Access

Classic

OIE

Classic

OIE

OIE

OIE

### Custom FIDO2 AAGUID

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

Enable the addition of approved AAGUID-based authenticators – such as browser password managers – for use in FIDO2 (WebAuthn) groups.

### Residential Proxy as an IP Service Category

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

Enhanced Dynamic Zones now support Residential Proxies and Blockchain VPNs as IP Service Categories, enabling organizations to block access before policy evaluation.

[Learn more](#)

### ID Verification Name Matching

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

Differentiate between legal and preferred name while performing verifiable claims mapping during ID verification.

[Learn more](#)

### Microsoft EAM support (External Authentication Method)

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

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

[Learn more](#)

AuthenticatorsAAGUID ListDocumentation

AAGUID list

The AAGUID list can be referenced in Authenticator groups which are used in Enrollment Policies to limit the WebAuthn authenticators allowed for enrollment.

View authenticator groups →

Custom AAGUID

Add authenticators to the Custom AAGUID list when they do not appear in the FIDO MDS AAGUID list. If an AAGUID that already appears in the FIDO MDS AAGUID list is added here, the custom AAGUID will override in authenticator groups.

+ Add custom AAGUID

Search...

NAME	AAGUID	TYPE	FIPS COMPLIANT	HARDWARE PROTECTED	
Uber YubiKey 5 Series	9d3df6ba-282f-11ed-a261-	Roaming	No	Yes	Actions
Uber YubiKey 5C Series	2fc0579f-8113-47ea-b116-	Roaming	No	Yes	Actions

FIDO MDS AAGUID list

This list is based on the FIDO MDS [?], and contains only the MDS entries that are FIDO certified. This list may not be fully up to date.

Search...

NAME	AAGUID	TYPE	FIPS COMPLIANT	HARDWARE PROTECTED
Arculus FIDO2/U2F Key Card	9d3df6ba-282f-11ed-a261-01	Roaming	No	Yes
YubiKey 5 Series with NFC 25	2fc0579f-8113-47ea-b116-bb	Roaming	No	Yes
YubiKey 5 Series 19083...	19083c3d-8383-4b18-bc03-	Roaming	No	Yes

Custom FIDO2 AAGUID



# Access Management

## Early Access

### Network Restrictions for Token Endpoint

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

Enhance security by allowlisting network zones per client, restricting token requests to trusted IPs and protecting against replay attacks, token theft, DoS, and rate limit abuse.

[Learn more](#)

OIE

### OAG auto-update

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

Customers can now enable auto-updates to ensure their OAG deployments run the latest version.

[Learn more](#)

OIE

### Overlapping IdP Signing Certificates

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

Support multiple active signing certificates per IdP to enable seamless certificate rotation, reducing downtime and reducing operational overhead while improving security.

[Learn more](#)

Classic

OIE

### Universal Logout support for Okta Customer Identity Apps

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

Easily integrate Universal Logout into your Okta Customer Identity (formerly CIS) apps – zero development effort required.

[Learn more](#)

OIE

### SAML Protocol Settings

IdP Issuer URI ⓘ

https://auth.io/idp/saml2/00u1hkqfxxQtBSR9y6

IdP Single Sign-On URL ⓘ

https://auth.io/idp/saml2/00u1hkqfxxQtBSR9y6

IdP Signature Certificate ⓘ

C=US, ST=California, L=San Francisco, O=Okta Inc., CN=auth.io  
Certificate expires in 36263 days

C=US, ST=New York, L=New York, O=Example Corp., CN=identity.example.com  
This certificate has expired

Request Binding ⓘ

HTTP POST

Overlapping IdP Signing Certificates



# Access Management

## Early Access

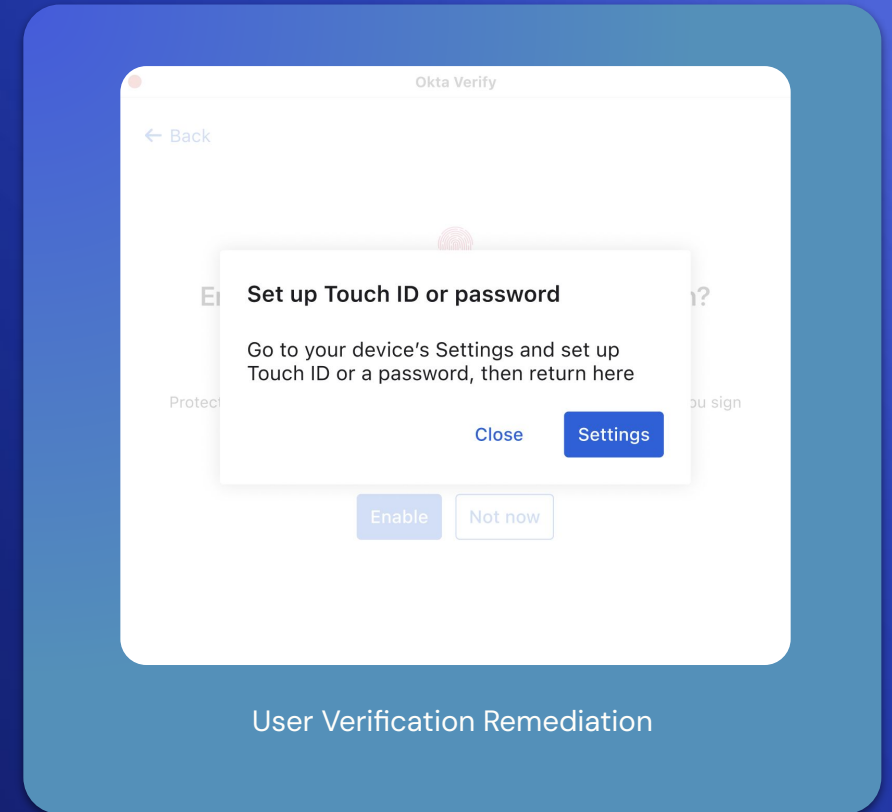
### User Verification Remediation

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

Guide end users through enabling or stepping up user verification to meet authentication policy requirements.

Classic

OIE





# Identity Management

## General Availability

### End-to-end encryption for LDAP Agent

Available in: Directory Integrations. || Supported in: FedRAMP Moderate/High/DOD IL4

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

Classic

OIE

### OIN Apps for Entitlement Management – Splunk, Zoho Mail

Available in: Okta Identity Governance (OIG) || Supported in: DOD IL4

Discover, import, store, and manage entitlements within Okta via bundles, policies, and rules with out-of-the-box integrations for 4 OIN apps: Splunk, Zoho Mail, Crowdstrike, Oracle IAM.

Classic

OIE

### Permission Conditions for Create User

Feature of: Custom Admin Roles, Secure Partner Access / Available in: Secure Partner Access. || Authorized in: FedRAMP Moderate/High/DOD IL4

Prevents delegated or partner admins from assigning sensitive attribute values (like roles or departments) that could unintentionally grant access to critical systems. Helps enforce attribute-based access control policies by ensuring only the right admins can set identity attributes tied to authorization. Reduces risk of misconfiguration during user onboarding, especially in environments with delegated administration.

Classic

OIE

The screenshot displays the 'Create users' configuration page in the Okta Admin Console. It features a section for 'Add conditions' with a dropdown menu for 'Operation' set to 'Exclude' and a dropdown for 'Attributes' set to 'Employee type'. Below this, there is a section for 'Edit users' application assignments, which is currently unchecked. At the bottom, there is a section for 'Manage API tokens', also unchecked. A tooltip is visible over the 'Operation' dropdown, showing 'Include' and 'Exclude' options. A small text note at the bottom of the tooltip reads: 'Required to add user to a group: Admin also needs "Manage group membership" permission on the group the admin wants to add user to'.

Permission Conditions for Create User



# Identity Management

## Early Access

### Incremental Imports with DirSync

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

Improve incremental imports from Active Directory resulting in faster and more efficient imports, and fewer fallbacks to full imports.

[Learn more](#)

Classic  
OIE

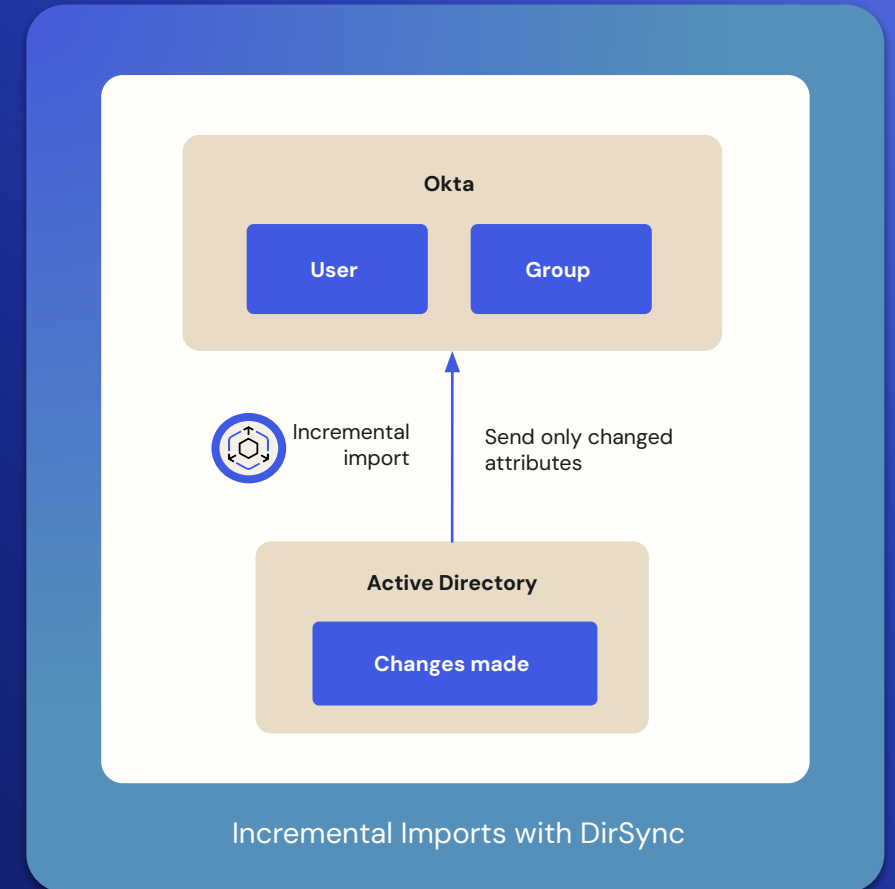
### On-prem Connector for Oracle EBS

Available with Okta Identity Governance (OIG) || Supported in: DOD IL4

Simplifies identity governance for on-prem applications bridging legacy systems with modern app stacks to deliver enhanced security, seamless automation, and compliance.

[Learn more](#)

Classic  
OIE



# Identity Governance

## General Availability

Classic

OIE

Classic

OIE

Classic

OIE

Classic

OIE

### Accessibility improvements and redesign for Access Request

Available in: Access Governance. || Supported in: DOD IL4

Enables easier navigation with a UI consistent across Okta’s first-party apps. Supports accessibility compliance with redesigned, inclusive layouts. Reduces user friction by aligning with familiar Okta design patterns.

[Learn more](#)

### New LCM/Okta Identity Governance (OIG) Integrations

Available in: All SKUs. || LCM is Authorized in: FedRAMP Moderate/High/DOD IL4, OIG is Supported in: DOD IL4

Integrate with more HR systems and popular applications (Splunk) to manage users, groups, and entitlements.

[Learn more](#)

### Resource Collections

Available in: Okta Identity Governance (OIG) – Access Governance. || Supported in: DOD IL4

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

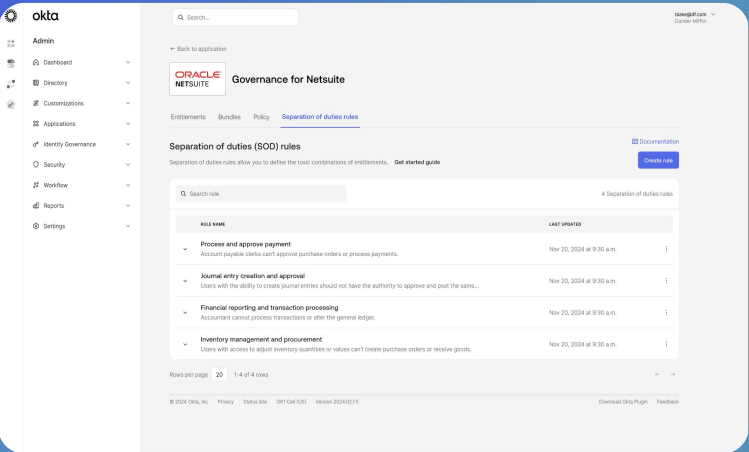
[Learn more](#)

### Separation of Duties

Available in: Okta Identity Governance (OIG) – Access Governance. || Supported in: DOD IL4

Create rules to define toxic combination of entitlements and run certification campaigns to remediate toxic combinations that exist for users.

[Learn more](#)



Separation of Duties



# Platform Services

## General Availability

### Accessibility ACRs

Assessment: VPATS cover all Okta environments, including FedRAMP Moderate/High/DOD IL4

Provide visibility into current state of accessibility of product for customers; also useful for meeting legal and compliance requirements especially for Fed and Sled customers.

[Learn more](#)

Classic  
OIE

### Dynamic Resource Sets

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

Allow customers to reserve access to sensitive resources to a small subset of admins.

[Learn more](#)

Classic  
OIE

### New Workflows Connectors

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

Integrate with more Okta APIs and popular applications (Coupa, Splunk) to manage users and groups.

[Learn more](#)

Classic  
OIE

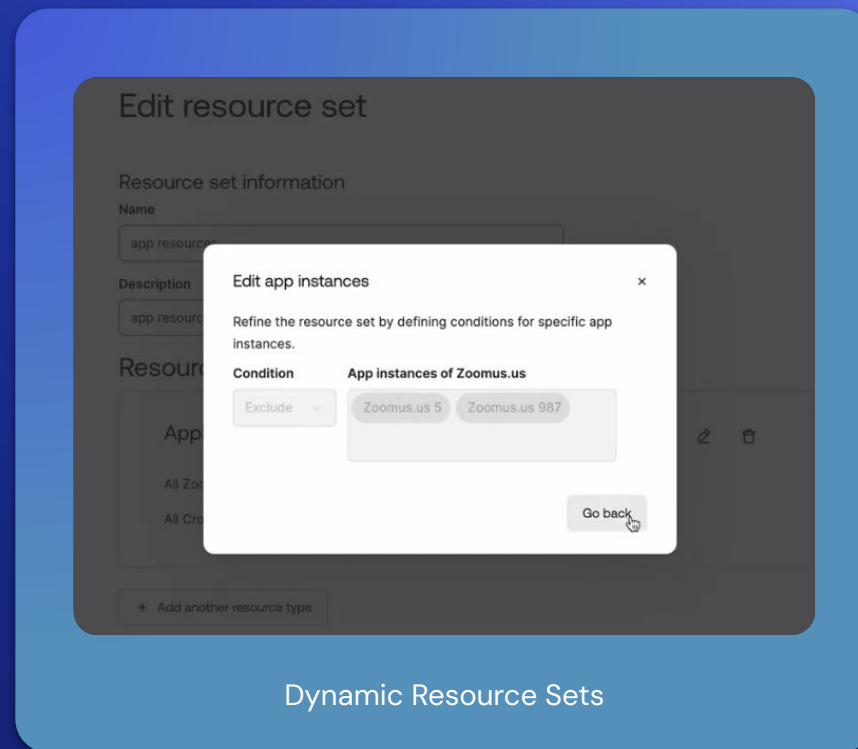
### Okta ITP Connector for Workflows

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

Use the Okta ITP connector for debugging or auditing ITP events and creating or updating user risk levels.

[Learn more](#)

Classic  
OIE



# Platform Services

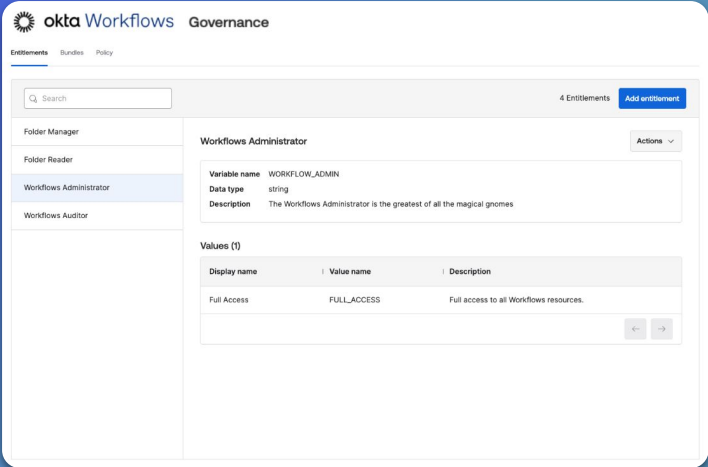
Early Access

## Governance for Workflows

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

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

OIE



Governance for Workflows



# Okta 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

### Claims Sharing between Okta and External IdPs

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

Enhance user experience while maintaining strong security by accepting and validating trusted claims from external IdPs at the Okta service provider.

Classic  
OIE

### Claims Sharing Between Okta Orgs

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

Enhance Identity federation by enabling secure, seamless access to resources across Okta Orgs.

Classic  
OIE

### New Workflows Connectors

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

Integrate with more Okta APIs and popular applications (Coupa, Splunk) to manager users and groups.

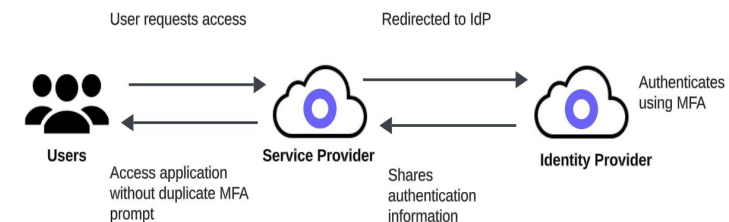
Classic  
OIE

### Permission Conditions for Create User

Feature of: Custom Admin Roles, Secure Partner Access / Available in: all SKUs. || Authorized in: FedRAMP Moderate/High/DOD IL4

Prevent delegated or partner admins from assigning sensitive attributes, enforcing attribute-based access control and reducing misconfiguration risks during user onboarding.

Classic  
OIE



Claims Sharing between Okta Orgs



# Okta Customer Identity

## General Availability

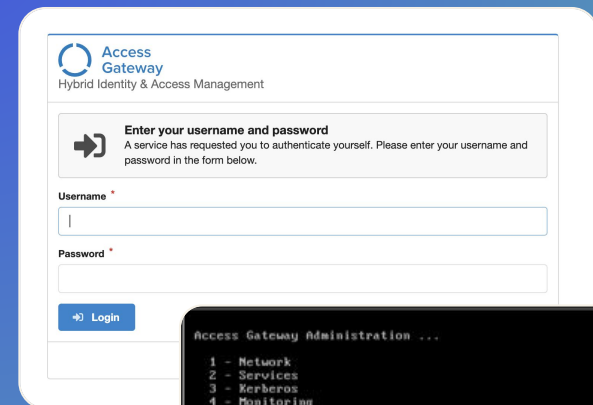
### OAG Secure-By-Design Changes

Available in: Okta Access Gateway. || Supported in FedRAMP Moderate/High/DOD IL4

OAG admin console will only be accessible on the local network by default and forces change of admin password for both admin console and admin management CLI. These changes are made to honor Okta's secure by design commitment.

Classic

OIE



```
Access Gateway Administration ...  
1 - Network  
2 - Services  
3 - Kerberos  
4 - Monitoring  
5 - System  
6 - Change Password  
7 - Change Access Gateway Password  
8 - Content Update  
9 - Support Connection  
x - Exit  
  
Choice:  
Build: 2828.2.0-2236ee1
```

OAG Secure by Design Changes



# Okta Customer Identity

## Early Access

### Cascading of the SLO request to external IdP

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

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

OIE

### Network Restrictions for Token Endpoint

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

Enable client-specific allowlisted zones to minimize the risk of token abuse, safeguard customer sessions, and protect backend systems from DoS attacks and rate limit exhaustion.

OIE

### Residential Proxy as an IP Service Category

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

Enhanced Dynamic Zones now support Residential Proxies and Blockchain VPNs as IP Service Categories, enabling organizations to block access before policy evaluation.

Classic

OIE

### Incremental Imports with DirSync

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

Improve incremental imports from Active Directory resulting in faster and more efficient imports, and fewer fallbacks to full imports – crucial for delivering seamless customer experiences.

Classic

OIE

#### General Settings [Edit](#)

##### APPLICATION

App integration name Network restricted API Service App

Application type Service

Application notes for admins

Proof of possession ☒ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type Client acting on behalf of itself

☒ Client Credentials

[Advanced](#) ▾

##### Network IP [Edit](#)

Token can be used from In: Any

[Go to Network Zones](#) ↗

#### Network Restrictions for Token Endpoint



# Okta Customer Identity

Early Access

## ID Verification Name Matching

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

Improves accuracy and user experience by clearly distinguishing legal and preferred names, enhancing trust and security across onboarding, authentication, account recovery, and support workflows.

OIE

## Augmenting appID Context for OIDC and SAML applications

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

Passes application details (ID, Name) to external IdPs during Okta-initiated federation (SAML/OIDC) to enable richer security and policy decisions at the IdP.

OIE

## Overlapping IdP Signing Certificates

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

Support multiple active certificates per IdP to enable seamless certificate rotation, eliminating downtime and reducing operational overhead while improving security.

Classic  
OIE

### Persona IDV User Profile Mappings

Identity verification claims mapping is one way from Okta to the vendor you have set up. Mapping is required for first and last names to complete the verification process.

Okta	Okta User User Profile	persona	Persona IDV
	user		appuser
Username is set by Persona IDV		userName	string
Choose an attribute or enter an expression...		verifiedStatus	string
user.legalName		given_name	string
user.lastName		family_name	string

Preview Enter an Okta user to preview their mapping Save mappings Cancel

ID Verification Name Matching



# Okta Customer Identity

## Early Access

### Universal Logout support for Okta Customer Identity Apps

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

Easily integrate Universal Logout into your Okta Customer Identity (formerly CIS) apps – zero development effort required.

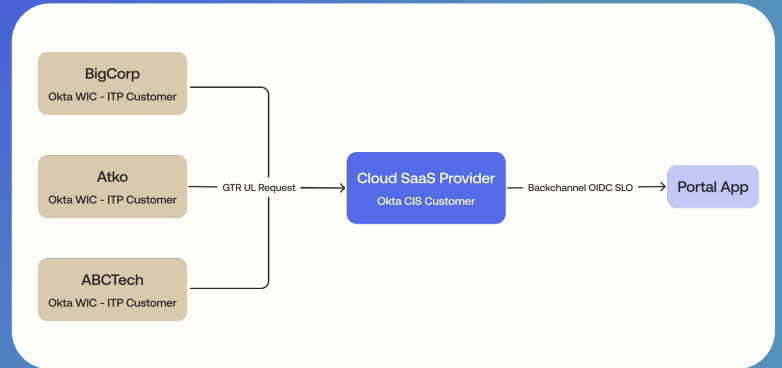
OIE

### Governance for Workflows

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

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

OIE



Universal Logout support for OCI Apps



The image features the word "okta" in a white, lowercase, sans-serif font, centered on a solid blue background. The background has a subtle gradient and decorative geometric shapes in the corners: a series of overlapping rounded rectangles in the top-left and bottom-right corners, creating a layered effect.

okta