okta

# Release Overview

for Early Access & General Availability in Q2 (April-June 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 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 Okta Platform Release Overview

**Q2 2025**

As the identity attack surface grows—with more devices, AI agents, and distributed environments—protecting every identity is more important than ever.

This quarter, we're introducing new capabilities that help you tackle that complexity. With the latest enhancements in Okta Workforce Identity, you can:

- Strengthen device security across your ecosystem
- Discover and manage the full lifecycle of non-human identities

These updates support a proactive, identity-first security approach, because identity is security.

# 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 strengthens your security posture by automating access decisions and enforcing consistent policies. This approach reduces manual effort for your team and simplifies IT operations.

This quarter, our releases build on that foundation, delivering stronger governance and security controls across your most critical assets: devices, users (including AI Agents), and privileged resources.

## Spotlights

### Okta Workforce Identity

- Security Before, During, and After Authentication
- Active Directory Accounts
- Identity Threat Protection with Okta AI Updates
- Cross App Access (for AI Agents)
- Okta US Public Sector compliance roadmap updates

## All features

- Identity Security Posture Management (ISPM)
- Access Management
- Identity Management
- Identity Governance
- Privileged Access
- Platform Services
- Premier Success Plans
- Okta Learning

## 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
- Okta Access Gateway
- Customer Identity

### Device Access

- Okta Device Access

### Identity Threat Protection

- Identity Threat Protection with Okta AI

## 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.

# Spotlight: Security Before, During, and After Authentication

## Active Directory Accounts

- Leverage your existing Okta AD agent to discover privileged accounts
- Protect AD accounts with access policies and automatic credential rotations,

## Identity Security Posture Management Enhancements

- Visualize multi-tenant access relationships and MFA gaps across Okta instances
- Identify MFA bypasses and policy weaknesses across your identity ecosystem

## Identity Threat Protection with Okta AI Enhancements

- Enhance the security of admin accounts
- Unify threat detection and response across your environment and in real-time

Early Access

# Spotlight: Active Directory Accounts

Manage Active Directory Accounts

## What is it?

This feature allows you to connect to Active Directory environments leveraging your existing Okta AD Agent, discover privileged AD accounts and manage their passwords, create robust access policies, and audit all admin and user activities.

**Customer Challenge:**

Privileged accounts in Active Directory are typically unmanaged and highly exploitable.

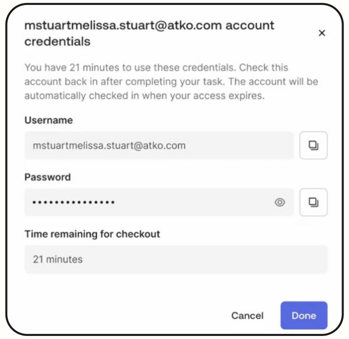
## Why this matters

Whether driven by compliance or better security posture, Active Directory accounts must be protected from unauthorized users. Best practices state that privileged accounts should be vaulted, have regular password rotations, and security leaders should know who has access to specific resources.

## How to get it

Globally available in Okta Privileged Access. Talk to your CSM or AE to get it turned on for your environment.

See the blog



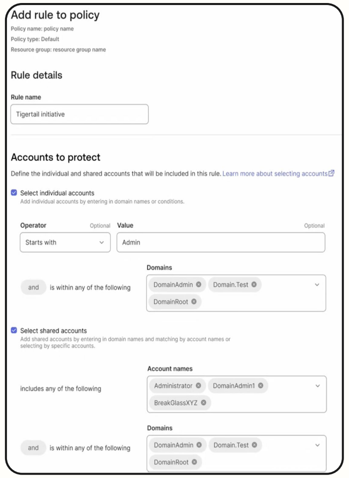
mstuartmelissa.stuart@atko.com account credentials

You have 21 minutes to use these credentials. Check this account back in after completing your task. The account will be automatically checked in when your access expires.

Username: mstuartmelissa.stuart@atko.com

Password: •••••••••••••••

Time remaining for checkout: 21 minutes



Add rule to policy

Policy name: policy name
Policy type: Default
Resource group: resource group name

Rule details

Rule name: Tigertail initiative

Accounts to protect

Define the individual and shared accounts that will be included in this rule. Learn more about selecting accounts

☑ Select individual accounts
Add individual accounts by entering in domain names or conditions.

Operator (Optional): Starts with
Value (Optional): Admin

and is within any of the following
Domains: DomainAdmin, Domain.Test, DomainRoot

☑ Select shared accounts
Add shared accounts by entering in domain names and matching by account names or selecting by specific accounts.

includes any of the following
Account names: Administrator, DomainAdmin1, BreakGlassXYZ

and is within any of the following
Domains: DomainAdmin, Domain.Test, DomainRoot

# Spotlight: Identity Threat Protection with Okta AI Updates

Expand threat visibility and automate actions across your tech stack in real-time

## What is it?

**Custom Admin Roles for ITP** – Enforce least-privilege access by assigning admin permissions for managing ITP configurations.

**ITP Detections for Super Admin Roles*** – Monitor and detect anomalous behavior targeting Super Admins to identify account takeover attempts.

**SSF Integration with Palo Alto Networks** – Correlate identity signals with insights from xDR platforms, like Palo Alto Network,  to improve detection, reduce siloes, and drive coordinated actions across your ecosystem.

**SSF Transmitter** – Use Okta's identity signals to trigger automated actions (e.g., session revocation, MFA challenges) in third-party tools, like Apple Business Manager, accelerating incident response workflows.

*Now available for Adaptive MFA customers

## Why this matters

These updates deliver stronger control over admin permissions, deeper visibility into risk over these highly privileged accounts, and the ability to respond to threats faster and more proactively across your environment.

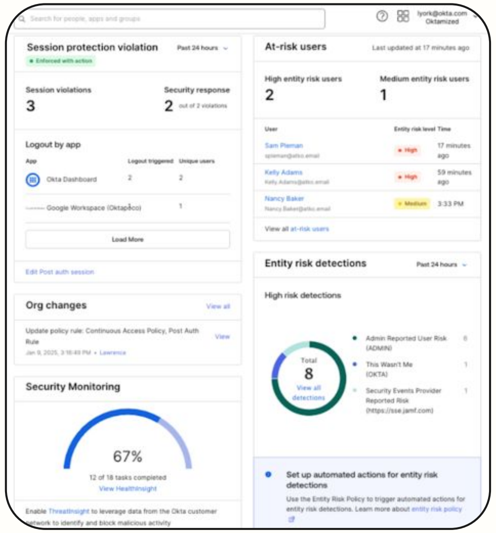
**Customer Challenge:**

Organizations often struggle to enforce least privilege for admins, leaving critical configurations exposed through overly permissive roles. At the same time, limited visibility into Super Admin activity increases the risk of undetected account takeovers. Without integrated identity signals and automated response capabilities, threat detection and response remain fragmented and slow, weakening overall security posture.

## How to get it

- Custom Admin Roles for ITP, SSF Integration for Palo Alto Networks, and SSF Transmitter are available with the **ITP SKU**.
- ITP Detections for Super Admin Roles is now available with the  **Adaptive MFA SKU.**

[Learn more]



Session protection violation — Past 24 hours
Enforced with action

Session violations 3
Security response 2 out of 2 violations

Logout by app

| App | Logout triggered | Unique users |
|---|---|---|
| Okta Dashboard | 2 | 2 |
| Google Workspace (Oktapāco) | | 1 |

Org changes — View all

Update policy rule: Continuous Access Policy, Post Auth Rule — View
Jan 9, 2025, 3:16:49 PM • Lawrence

Security Monitoring

67%
12 of 18 tasks completed
View HealthInsight

Enable ThreatInsight to leverage data from the Okta customer network to identify and block malicious activity

At-risk users — Last updated at 17 minutes ago

High entity risk users 2
Medium entity risk users 1

| User | Entity risk level | Time |
|---|---|---|
| Sam Pleman<br>spleman@atko.email | High | 17 minutes ago |
| Kelly Adams<br>Kelly.Adams@atko.email | High | 59 minutes ago |
| Nancy Baker<br>Nancy.Baker@atko.email | Medium | 3:33 PM |

View all at-risk users

Entity risk detections — Past 24 hours

High risk detections

Total 8
View all detections

| | |
|---|---|
| Admin Reported User Risk (ADMIN) | 6 |
| This Wasn't Me (OKTA) | 1 |
| Security Events Provider Reported Risk (https://sse.jamf.com) | 1 |

Set up automated actions for entity risk detections

Use the Entity Risk Policy to trigger automated actions for entity risk detections. Learn more about entity risk policy

# Spotlight: Cross App Access (for AI Agents)

Secure the invisible layer of app and AI agent integration – ISVs can start building today, available as an Okta feature for select customers in Q3 FY26

## What is it?

Cross App Access for AI Agents is a protocol that enables trusted connections between apps and AI agents. It shifts control and consent to the IT admin so they can decide what apps are connecting—and see exactly what's being accessed.

**Customer Challenge:**

AI agents act independently to complete tasks, make decisions, and connect with other systems – without asking for permission. AI agents are creating a hidden layer of privileged access across systems. This poses a new, urgent security risk that traditional identity tools weren't built to handle.

## Why ISVs should adopt

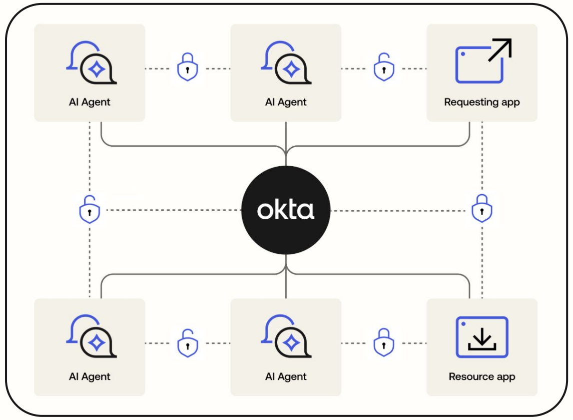
Securing agentic AI takes an ecosystem of builders, identity platforms, and enterprises working together. ISVs play a critical role.

As AI agents grow in number and sophistication – and act on a user's behalf across systems – so do the security gaps they create. Okta's Cross App Access brings modern oversight to this new reality, giving ISVs a scalable, secure way to control how autonomous agents and applications communicate. It helps B2B SaaS builders meet enterprise demands while enabling innovation with confidence.

## Where to learn more

ISVs can start building today. Customer Early Access Available Q3 FY26

- Learn more
- **Attend our digital event: Identity Summit: Securing Agentic AI** (Learn More)



# 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)

***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

### Non Human Identities - visibility and risk analysis

Feature of: Identity Security Posture Management (ISPM)

Security teams gain visibility required to protect against NHI driven breaches: Discover and report on top risky service accounts, human users with NHI credentials, and unrotated keys and tokens.

Classic

OIE

### SFDC AI Agents misconfigurations

Feature of: Identity Security Posture Management (ISPM)

Detect risky misconfigurations for SFDC AI Agents, including overprivileged access and weak authentication methods that could enable unauthorized data access or AI agent exploitation.

Classic

OIE

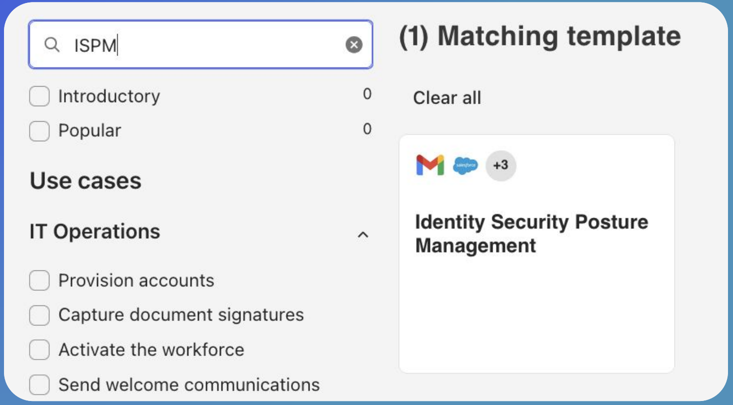
### Auto-Remediation Okta Workflows templates

Feature of: Identity Security Posture Management (ISPM)

Empowers customers to trigger auto-remediation actions with just a few clicks - ISPM now features an official workflow that initiates remediation steps such as account suspension, password resets, and MFA enforcement or enrollment.

Classic

OIE



ISPM

□ Introductory 0

□ Popular 0

**Use cases**

**IT Operations**

□ Provision accounts

□ Capture document signatures

□ Activate the workforce

□ Send welcome communications

**(1) Matching template**

Clear all

**Identity Security Posture Management**

Auto-Remediation Okta Workflows templates

# Identity Security Posture Management (ISPM)

## Early Access

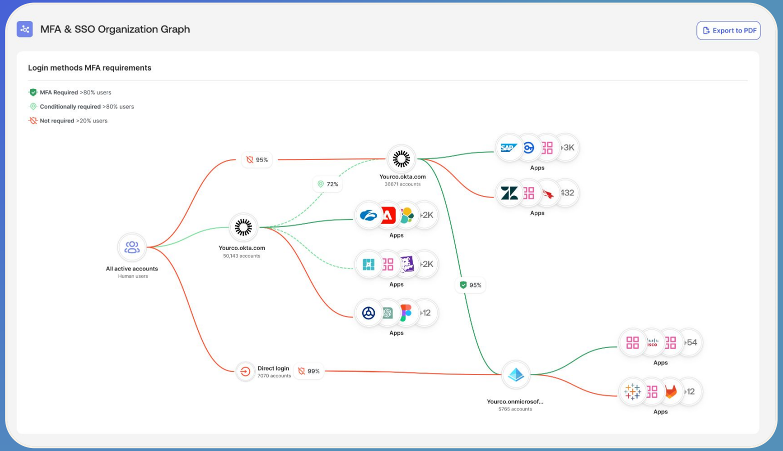
### MFA and SSO Analysis – Dashboard and Graph

Feature of: Identity Security Posture Management (ISPM)

Gain granular MFA, Factors and SSO analysis in an exportable dashboard to help identify top trends and risks.

Classic

OIE



MFA and SSO Analysis – Dashboard and Graph

# 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

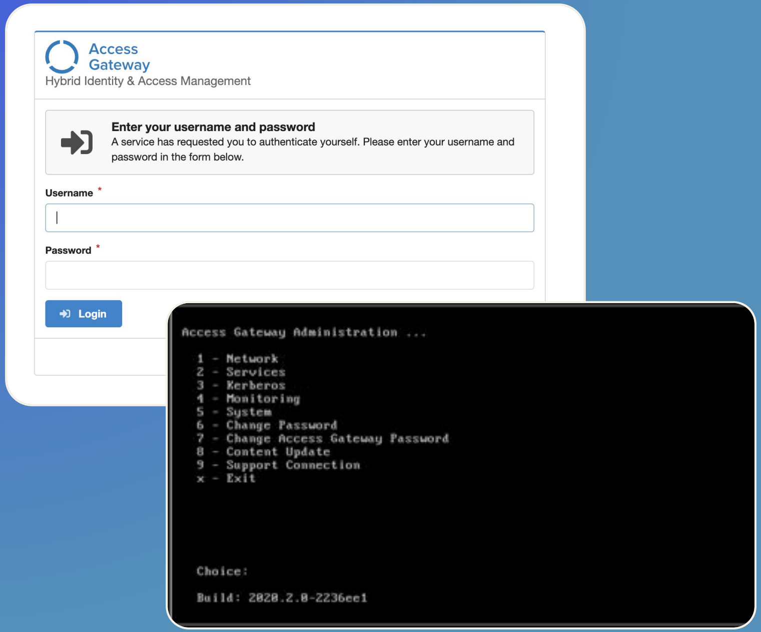
Classic | OIE

### 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



Access Gateway
Hybrid Identity & Access Management

**Enter your username and password**
A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username *

Password *

```
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: 2020.2.0-2236ee1
```

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

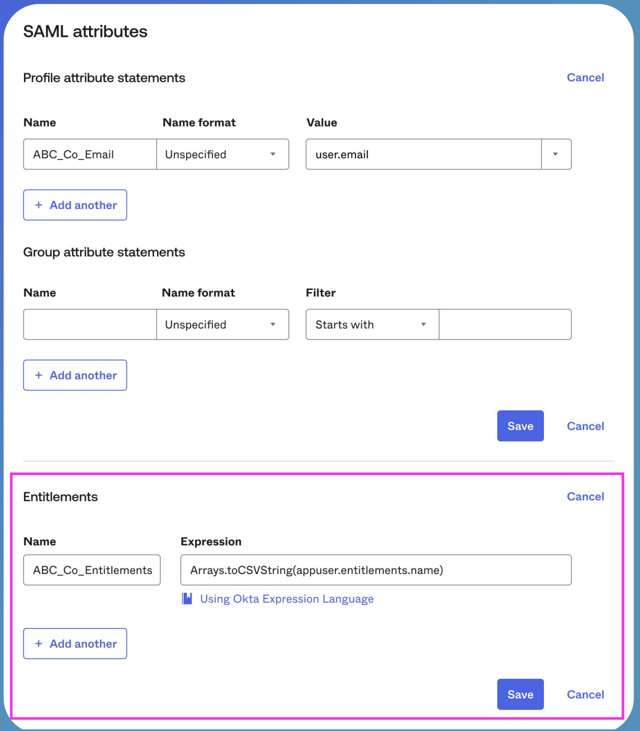
### Granular Admin Permissions to Access Identity Providers

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

| 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

# 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

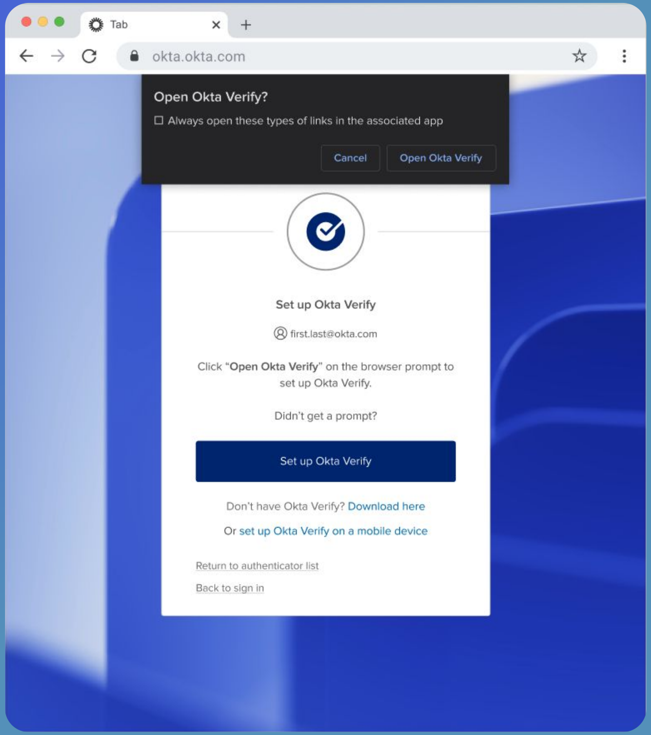
Available in: All SKUs. ‖ Authorized in: FedRAMP Moderate/High/DOD IL4

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

Learn more

Classic

OIE



Open Okta Verify?

☐ Always open these types of links in the associated app

Set up Okta Verify

first.last@okta.com

Click "**Open Okta Verify**" on the browser prompt to set up Okta Verify.

Didn't get a prompt?

Don't have Okta Verify? Download here

Or set up Okta Verify on a mobile device

Return to authenticator list

Back to sign in

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

### Breached Credentials Protection (Phase 2)

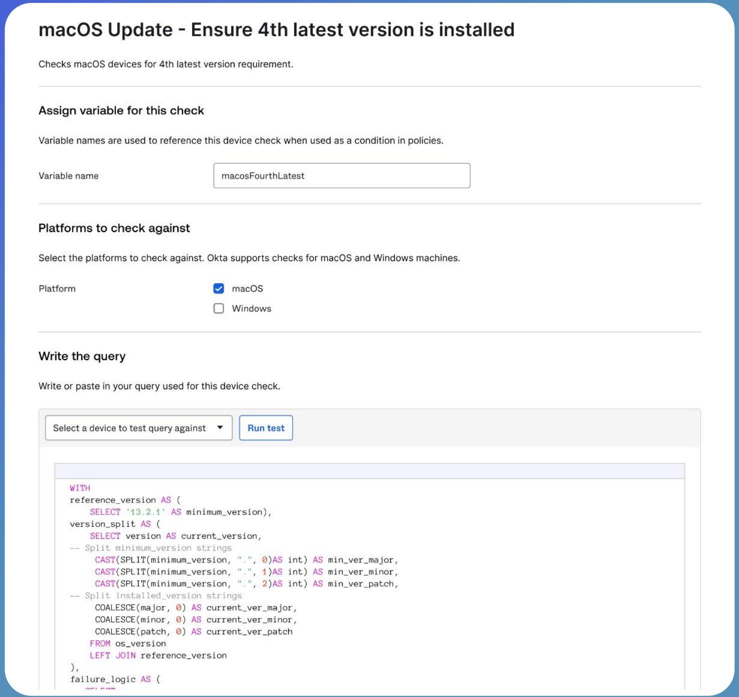
Available in: All SKUs

Customizable responses to breached credential events with the ability for admins to validate the breached credential flow using a test account.

Learn more

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: macosFourthLatest

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.

```
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, ".", 0)AS int) AS min_ver_major,
     CAST(SPLIT(minimum_version, ".", 1)AS int) AS min_ver_minor,
     CAST(SPLIT(minimum_version, ".", 2)AS int) AS min_ver_patch,
-- Split installed_version strings
     COALESCE(major, 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 (
```

Advanced Posture Checks

# Access Management

## Early Access

### 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.

Classic

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.

Learn more

Classic

OIE

### 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

OIE

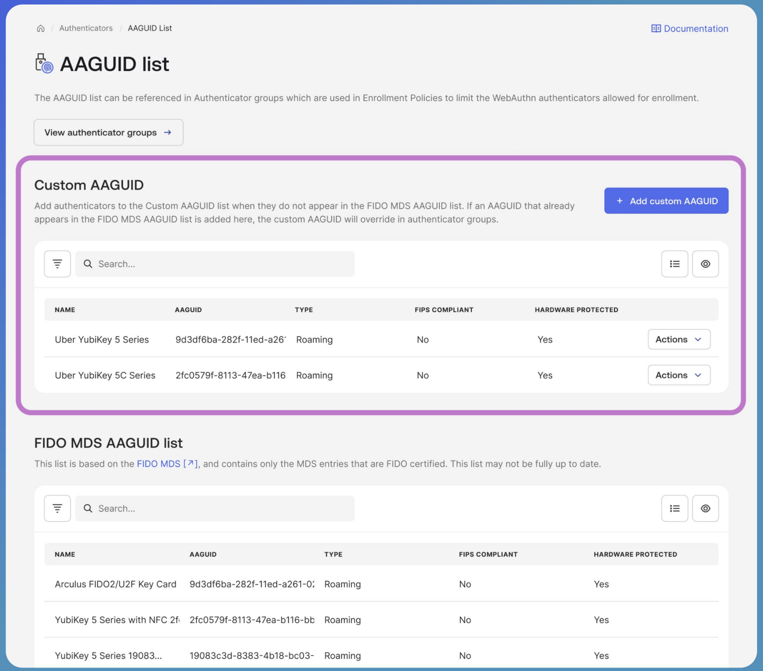
### Microsoft EAM support (External Authentication Method)

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

OIE



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.

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.

| NAME | AAGUID | TYPE | FIPS COMPLIANT | HARDWARE PROTECTED | |
|---|---|---|---|---|---|
| Uber YubiKey 5 Series | 9d3df6ba-282f-11ed-a26 | 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.

| NAME | AAGUID | TYPE | FIPS COMPLIANT | HARDWARE PROTECTED |
|---|---|---|---|---|
| Arculus FIDO2/U2F Key Card | 9d3df6ba-282f-11ed-a261-0 | Roaming | No | Yes |
| YubiKey 5 Series with NFC 2f | 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

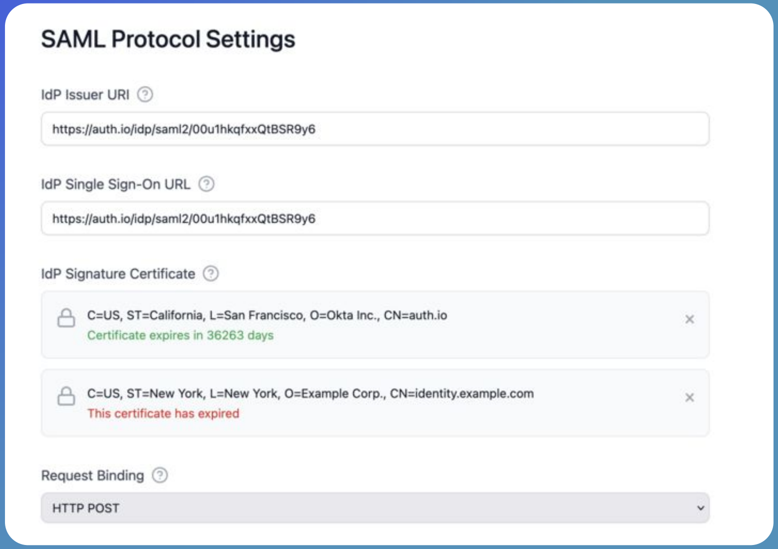
### Universal Logout support for Okta Customer Identity Apps

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

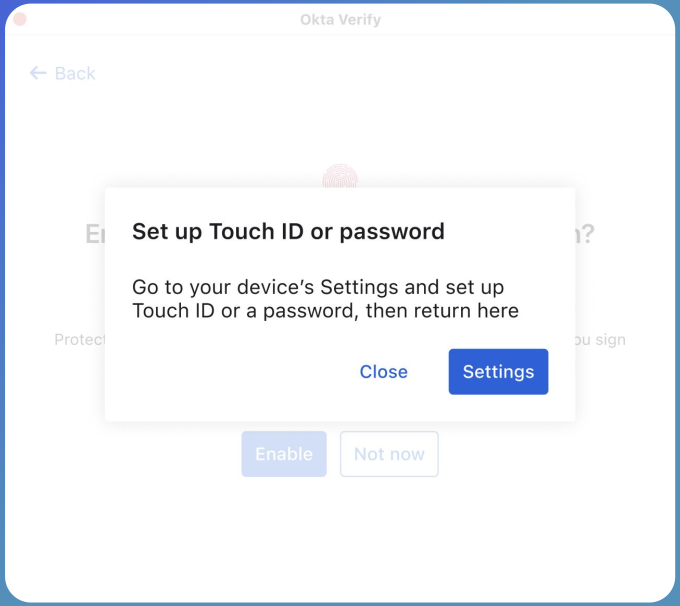
### User Verification Remediation

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



Set up Touch ID or password

Go to your device's Settings and set up Touch ID or a password, then return here

User Verification Remediation

# 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

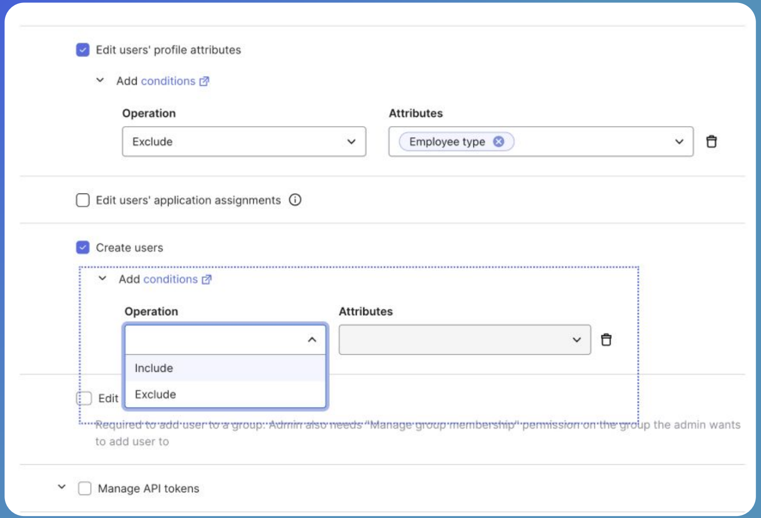
### Permission Conditions for Create User

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



☑ Edit users' profile attributes

Add conditions

Operation: Exclude

Attributes: Employee type

□ Edit users' application assignments

☑ Create users

Add conditions

Operation:

Include

Exclude

Attributes:

□ Edit

Required to add user to a group: Admin also needs "Manage group membership" permission on the group the admin wants to add user to

□ Manage API tokens

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

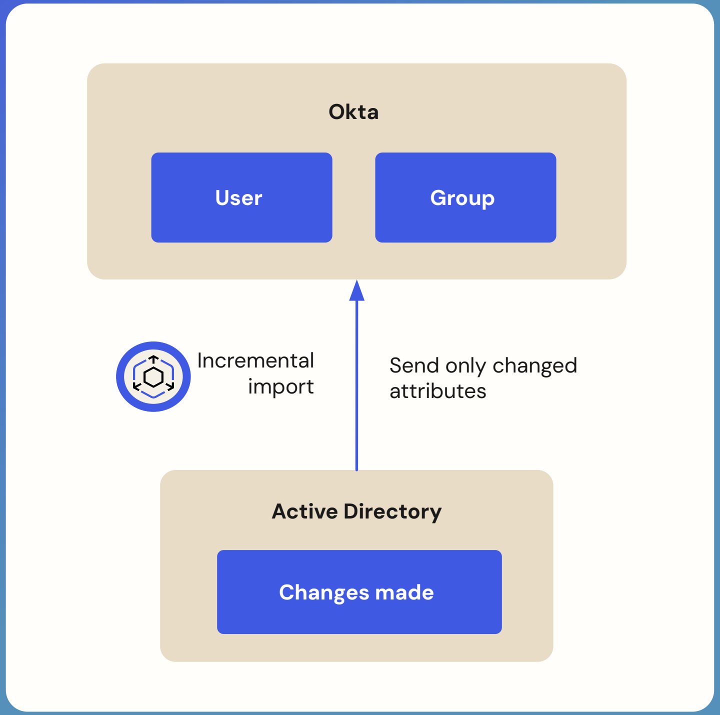
Available with Okta Identity Governance (OIG) ‖ Supported in: DOD IL4

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



Incremental Imports with DirSync

# Identity Governance

## General Availability

### 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

Classic

OIE

### 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

Classic

OIE

### 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

Classic

OIE

### Separation of Duties

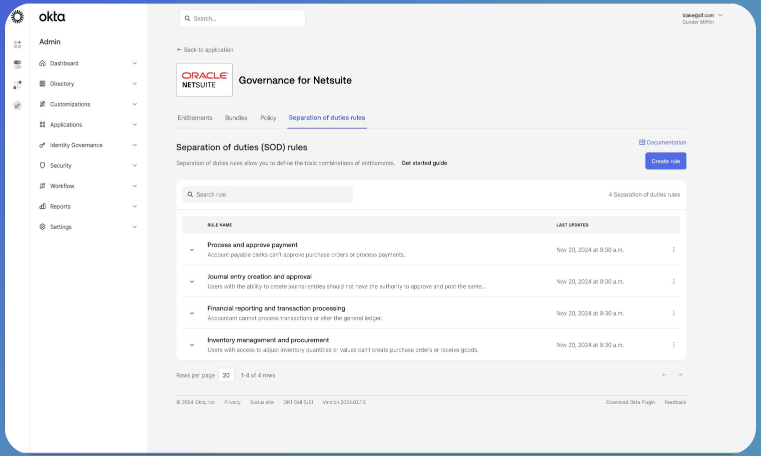
Available in: Okta Identity Governance (OIG) - Access Governance. ‖ Supported in: DOD IL4

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

Learn more

Classic

OIE



Governance for Netsuite

Separation of duties (SOD) rules

Separation of duties rules allow you to define the toxic combinations of entitlements. Get started guide

4 Separation of duties rules

| RULE NAME | LAST UPDATED |
|---|---|
| Process and approve payment<br>Account payable clerks can't approve purchase orders or process payments. | Nov 20, 2024 at 9:30 a.m. |
| Journal entry creation and approval<br>Users with the ability to create journal entries should not have the authority to approve and post the same... | Nov 20, 2024 at 9:30 a.m. |
| Financial reporting and transaction processing<br>Accountant cannot process transactions or alter the general ledger. | Nov 20, 2024 at 9:30 a.m. |
| Inventory management and procurement<br>Users with access to adjust inventory quantities or values can't create purchase orders or receive goods. | Nov 20, 2024 at 9:30 a.m. |

Rows per page 20 1-4 of 4 rows

© 2024 Okta, Inc Privacy Status site OK1 Cell (US) Version 2024.02.1 E Download Okta Plugin Feedback

Separation of Duties

# Privileged Access

## Early Access

### Active Directory Accounts

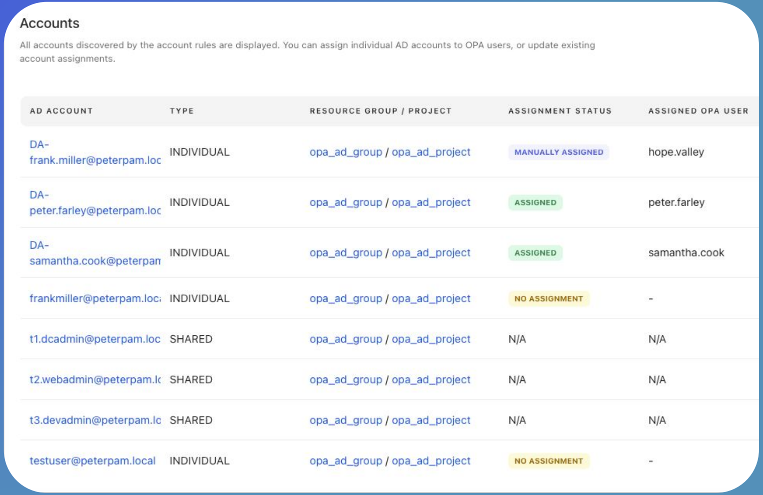
Available in: Okta Privileged Access

Manage privileged Active Directory account passwords without adding operational complexity. Use your existing Okta Active Directory Agent to discover AD accounts, create access policies, automate credential rotations, and audit all admin and user activities.

Learn more

Classic

OIE



Accounts

All accounts discovered by the account rules are displayed. You can assign individual AD accounts to OPA users, or update existing account assignments.

| AD ACCOUNT | TYPE | RESOURCE GROUP / PROJECT | ASSIGNMENT STATUS | ASSIGNED OPA USER |
|---|---|---|---|---|
| DA-frank.miller@peterpam.loc | INDIVIDUAL | opa_ad_group / opa_ad_project | MANUALLY ASSIGNED | hope.valley |
| DA-peter.farley@peterpam.loc | INDIVIDUAL | opa_ad_group / opa_ad_project | ASSIGNED | peter.farley |
| DA-samantha.cook@peterpan | INDIVIDUAL | opa_ad_group / opa_ad_project | ASSIGNED | samantha.cook |
| frankmiller@peterpam.loc | INDIVIDUAL | opa_ad_group / opa_ad_project | NO ASSIGNMENT | - |
| t1.dcadmin@peterpam.loc | SHARED | opa_ad_group / opa_ad_project | N/A | N/A |
| t2.webadmin@peterpam.lc | SHARED | opa_ad_group / opa_ad_project | N/A | N/A |
| t3.devadmin@peterpam.lc | SHARED | opa_ad_group / opa_ad_project | N/A | N/A |
| testuser@peterpam.local | INDIVIDUAL | opa_ad_group / opa_ad_project | NO ASSIGNMENT | - |

Active Directory Accounts

# 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

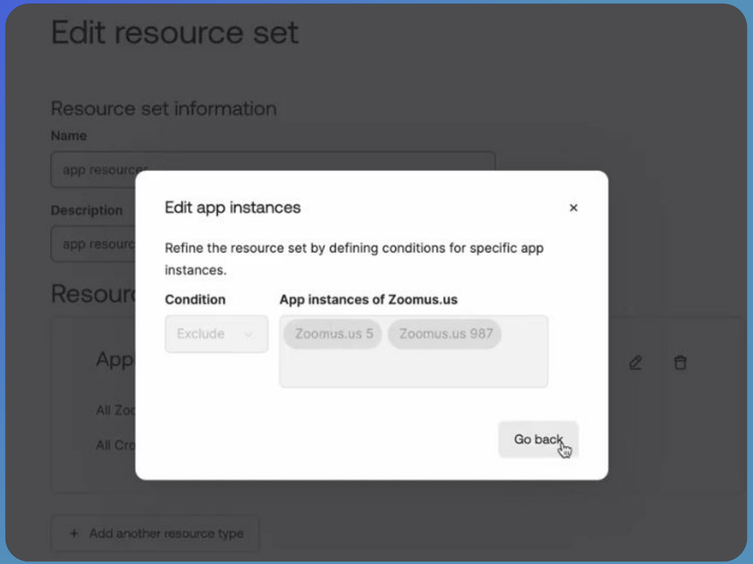
Available in: Workflows. || Authorized in: FedRAMP High, Supported in: FedRAMP Moderate/DOD IL4

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

Learn more

Classic

OIE



Edit resource set

Resource set information

Name

app resource

Description

app resourc

Resourc

App

All Zoo

All Cro

Edit app instances

Refine the resource set by defining conditions for specific app instances.

Condition: Exclude

App instances of Zoomus.us: Zoomus.us 5, Zoomus.us 987

Dynamic Resource Sets

# Platform Services

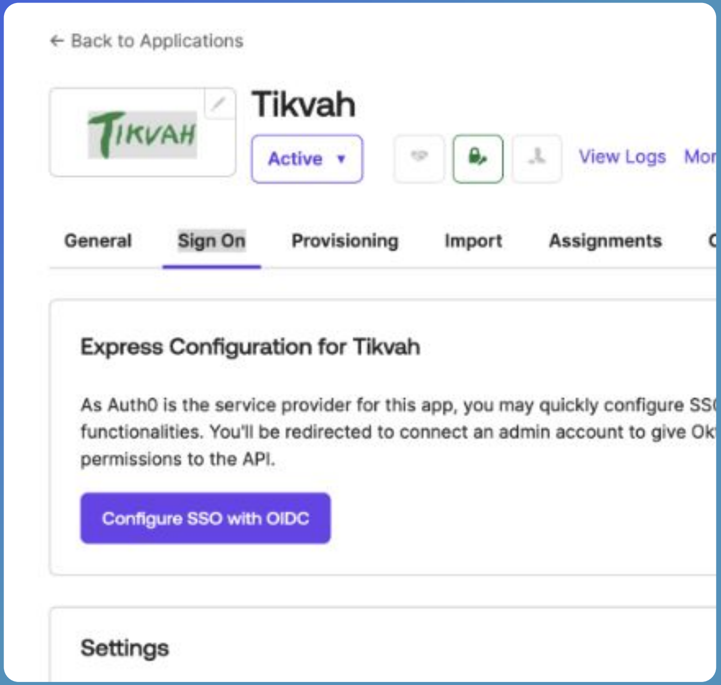
## General Availability

### Feature Oktane ISV Bundle: Express Configuration

Available in: All SKUs

Express Configuration lets enterprise customers quickly add an instance of Auth0-enabled OIDC apps published in the OIN catalog to their Okta org. This process uses automated data sharing between Okta and Auth0.

OIE



Express Configuration for Tikvah

As Auth0 is the service provider for this app, you may quickly configure SS functionalities. You'll be redirected to connect an admin account to give Ok permissions to the API.

Express Configuration

# 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

### ISV Bundle: Activate Program

Available in: Okta Platform (Okta Integration Network)

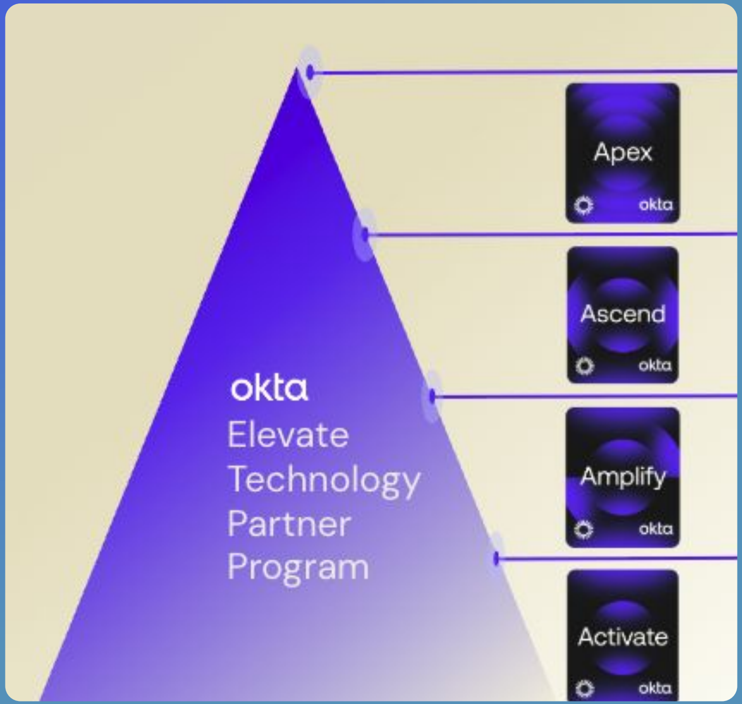
A program that enables ISVs to unlock visibility, enablement support, and self-serve marketing benefits with Okta by simply building, publishing, and maintaining SSO and LCM integrations.

Learn more

### ISV Bundle: secureintegrations.dev

Available in: All SKUs

Standards-focused microsite that will guide developers on exactly how to build, including updated information to include IPSIE levels that have already been ratified.



Activate Program

# Premier Success Plans

## General Availability

### Identity Maturity Checklist

Available in: Silver Premier Success Plan

A self-serve, step-by-step checklist on how to improve identity maturity based on selected business goals and recent adoption data, plus additional event and education resources. Learn more

OIE

### Identity Maturity Plan

Available in: Gold Premier Success Plan

Personalized recommendations to drive identity maturity based on selected business goals and recent adoption data, plus on-demand activation metrics, collaboration with your CSM, suggested Okta Learning paths, and other education resources. Learn more

OIE

### Expert Learning Pass

Available in: Silver and Gold Premier Success Plans

Unlock access to an exclusive on-demand catalog, live expert-led learning sessions, and certification vouchers. Silver customers receive one Expert Learning Pass and Gold customers receive six Expert Learning Passes. Learn more

Classic

OIE

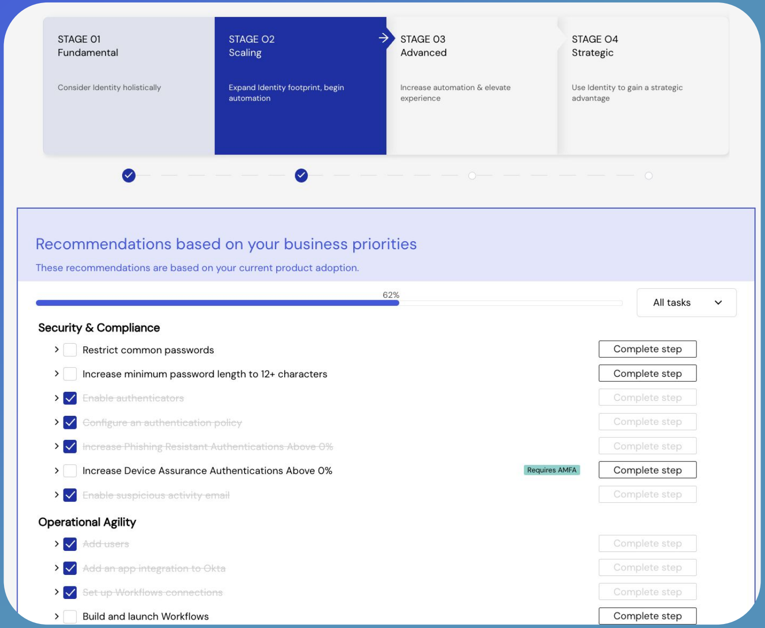
### Dedicated Technical Account Manager

Available as an add-on to Gold Premier Success Plan

A technical advisor with extensive knowledge of your products and architecture in order to provide tailored and long-term adoption and optimization strategies.

Classic

OIE



STAGE 01
Fundamental
Consider Identity holistically

STAGE 02
Scaling
Expand Identity footprint, begin automation

STAGE 03
Advanced
Increase automation & elevate experience

STAGE 04
Strategic
Use Identity to gain a strategic advantage

Recommendations based on your business priorities

These recommendations are based on your current product adoption.

Security & Compliance

- ☐ Restrict common passwords
- ☐ Increase minimum password length to 12+ characters
- ☑ ~~Enable authenticators~~
- ☑ ~~Configure an authentication policy~~
- ☑ ~~Increase Phishing Resistant Authentications Above 0%~~
- ☐ Increase Device Assurance Authentications Above 0% — Requires AMFA
- ☑ ~~Enable suspicious activity email~~

Operational Agility

- ☑ ~~Add users~~
- ☑ ~~Add an app integration to Okta~~
- ☑ ~~Set up Workflows connections~~
- ☐ Build and launch Workflows

Identity Maturity Checklist

# Okta Learning

## General Availability

### Security Series I- NEW OSIC Courses

Available in: Public Catalog

Misconfigured Identity is an entry point for a bad actor or negligent insider. It's important to ensure you have the right Identity configuration from the start. This plan shows you the key areas of focus and best practices to follow as part of Okta's Secure Identity Commitment (OSIC).

Learn more

Classic

OIE

### New Okta Skill Badge- Optimize Device Security and Management

Available in: Public Catalog

Discover how Okta integrates with various device management solutions to secure and manage desktops and mobile devices. Explore tailored security configurations and in-depth attestation processes that strengthen device security and streamline management tasks for a safer, more productive workplace.

Learn more

OIE

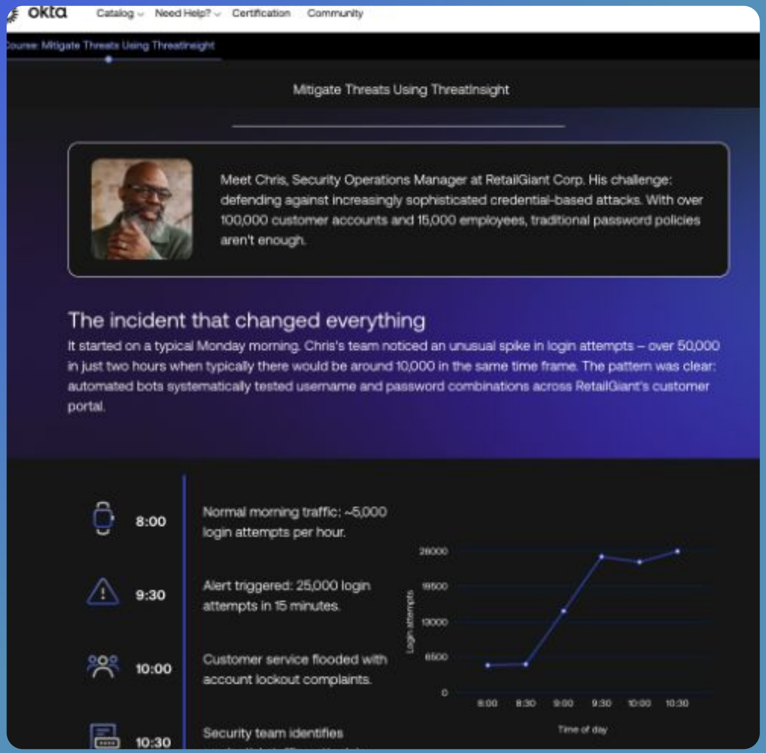
### New Okta Skill Badge! Manage BYOD via Identity-Aware Integration

Available in: Public Catalog

Transform your organization's mobile security landscape by implementing platform-specific BYOD strategies that leverage Okta's identity-first approach to protect both corporate data and user privacy. Plus, earn an Okta Skill Badge after completing the path!

Learn more

OIE



Mitigate Threats Using ThreatInsight

Meet Chris, Security Operations Manager at RetailGiant Corp. His challenge: defending against increasingly sophisticated credential-based attacks. With over 100,000 customer accounts and 15,000 employees, traditional password policies aren't enough.

The incident that changed everything

It started on a typical Monday morning. Chris's team noticed an unusual spike in login attempts – over 50,000 in just two hours when typically there would be around 10,000 in the same time frame. The pattern was clear: automated bots systematically tested username and password combinations across RetailGiant's customer portal.

8:00 Normal morning traffic: ~5,000 login attempts per hour.

9:30 Alert triggered: 25,000 login attempts in 15 minutes.

10:00 Customer service flooded with account lockout complaints.

10:30 Security team identifies

NEW Mitigate Threats Using ThreatInsight – Security Series I

# 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

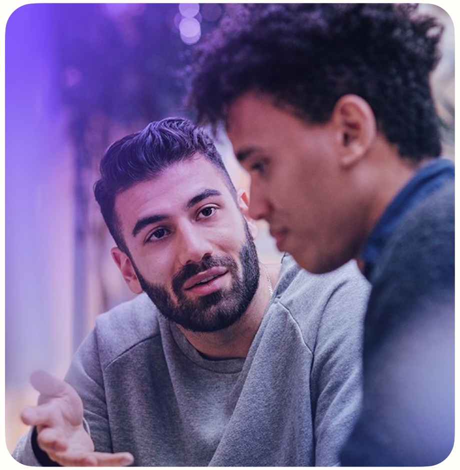
# Okta Customer Identity Releases

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 Customer Identity

Extend your identity security fabric across customers and partners

## What is it?

Okta Customer Identity (OCI) extends the trusted identity security and management capabilities you rely on for your workforce to your external users, including customers, partners, and citizens. It's a comprehensive platform designed to manage and secure external identities at scale, providing seamless and secure access to your digital apps while enhancing user experience.

**Customer Challenge:**

Many organizations deal with fragmented identity solutions for their workforce and external users, leading to operational complexity, security gaps, and inconsistent user experiences. Managing separate identity systems for employees, customers, and partners creates silos, increases the attack surface, and hinders digital transformation initiatives.

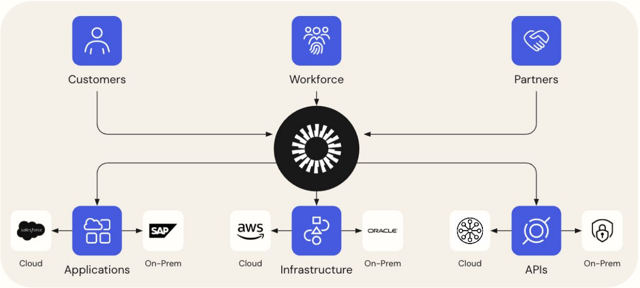
## Why this matters

- **Unified Identity Platform:** OCI allows you to consolidate workforce and customer identity management on a single, unified Okta platform. This reduces complexity, streamlines operations, and provides a holistic view of all your identities, enhancing security posture and compliance.
- **Reduced Risk and Enhanced Security:** Extend your trusted Okta identity security fabric to customers and partners, leveraging robust authentication and threat detection to minimize risks across your digital ecosystem.
- **Improved User Experience and Trust:** Provide a consistent, secure, and friction-free experience for all your users, whether they are employees, customers, or partners. This builds trust, fosters loyalty, and drives engagement with your digital services.

## How to get it

Reach out to your Okta representative or our sales team to discuss your specific needs and learn how Okta Customer Identity can benefit your organization.

Learn more



okta

Early Access

# Spotlight: Breached Credentials Protection

Proactively defend against credential stuffing and account takeover.

## What is it?

Automatically checks user passwords against continuously updated, third-party dataset of known compromised credentials. This proactive measure identifies if any user's password has been exposed in a data breach, even if that breach occurred elsewhere.

**Customer Challenge:**

In an era of frequent data breaches, credential stuffing and account takeover (ATO) attacks are pervasive threats. Organizations struggle to detect when their users' credentials have been compromised elsewhere on the internet, leaving them vulnerable to attackers who reuse stolen credentials to gain unauthorized access to their systems.

## Why this matters

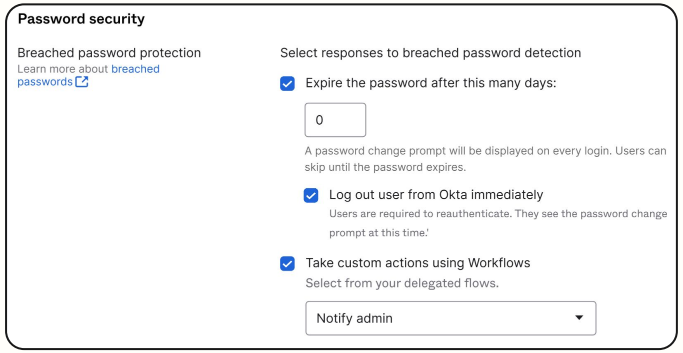
- **Proactive Threat Defense:** Automatically detects and mitigates the risk of credential stuffing and account takeover attacks by identifying compromised passwords before they can be exploited, safeguarding your users and your data.
- **Customizable Security Policies:** Provides administrators with granular control to configure specific responses when a breached credential is detected. This allows for tailored security actions, such as prompting a password reset or requiring additional authentication.
- **Enhanced Security Posture:** Improves your overall security posture by adding a critical layer of defense against one of the most common attack vectors. This helps prevent unauthorized access and reduces the potential for data breaches.

## How to get it

This feature is in Early Access.

Reach out to your Okta representative or our sales team to discuss your specific needs and learn how Okta Customer Identity can benefit your organization.

[Learn more]



**Password security**

Breached password protection
Learn more about breached passwords

Select responses to breached password detection

☑ Expire the password after this many days:

0

A password change prompt will be displayed on every login. Users can skip until the password expires.

☑ Log out user from Okta immediately
Users are required to reauthenticate. They see the password change prompt at this time.'

☑ Take custom actions using Workflows
Select from your delegated flows.

Notify admin ▾

# 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

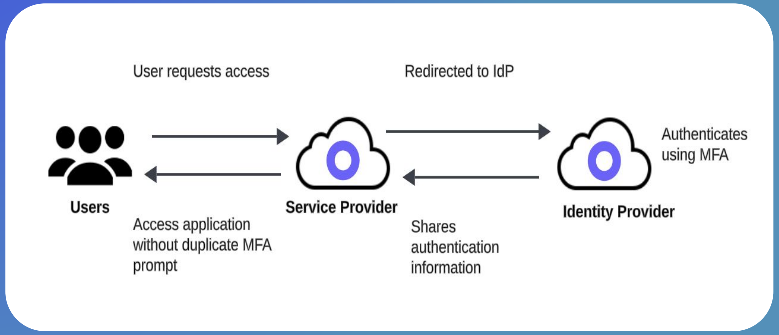
### Permission Conditions for Create User

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

### Non Human Identities (NHI) - visibility and risk analysis

Feature of: Identity Security Posture Management (ISPM)

Security teams gain visibility required to protect against NHI driven breaches. Discover and report on top risky service accounts, human users with NHI credentials, and unrotated keys and tokens.

Classic

OIE

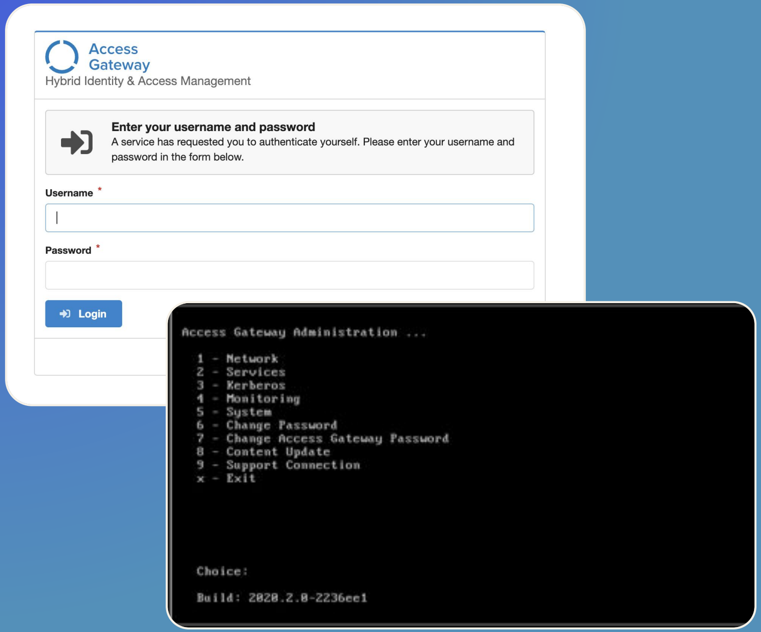
### OAG Secure-By-Design Changes

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.

Classic

OIE



**Enter your username and password**
A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username *

Password *

```
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: 2020.2.0-2236ee1
```

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.

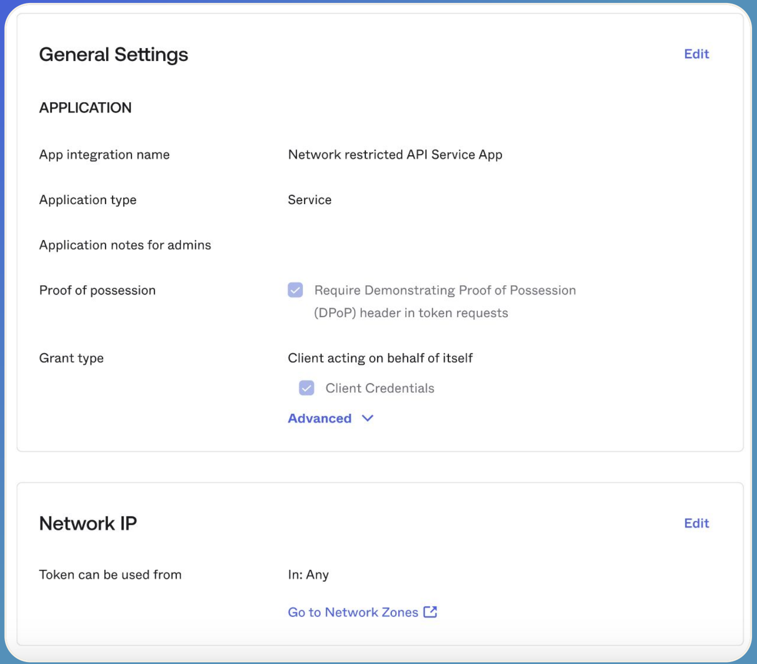
Classic OIE

### 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<br>☑ Client Credentials<br>Advanced |

Network IP Edit

| | |
|---|---|
| Token can be used from | In: Any<br>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

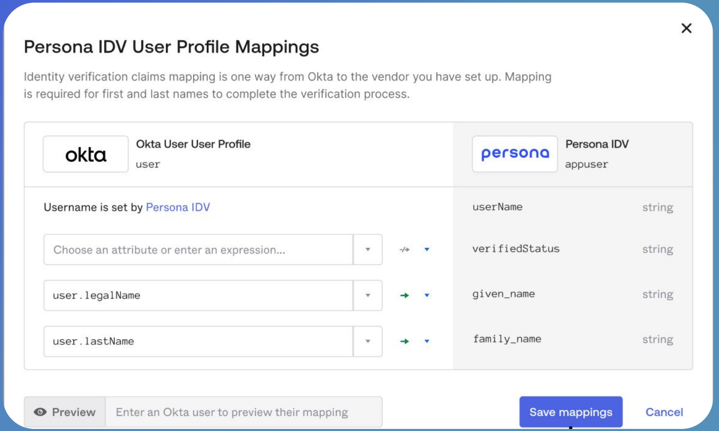
### Breached Credentials Protection (Phase 2)

Available in: All SKUs

Lets admin tailor user experiences and verify workflows using test accounts, improving both security and operational confidence.

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<br>user | | persona Persona IDV<br>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.

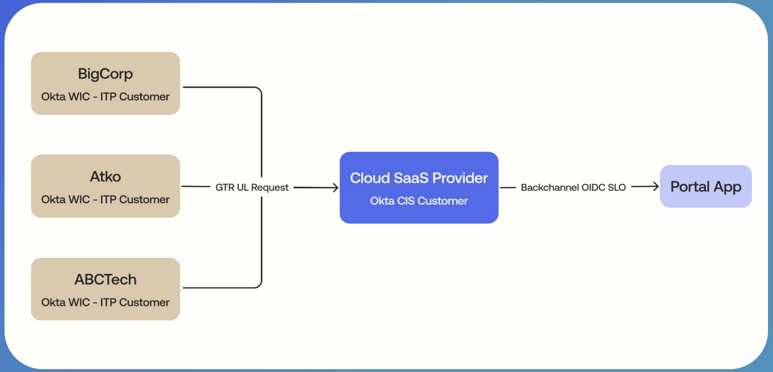
OIE

### 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

okta