Release Overview

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

US Public Sector

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

Safe harbor

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

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

Okta offers these opportunities to learn more about our latest innovations and what’s to come

Okta US Public Sector Resource Page

Dive further into the latest innovation and find resources to learn more **here**.

Connect with the Sales team **here.**

Okta Workforce Identity Product Roadmap Webinar

Get a sneak peek of upcoming product releases.

Register for the Okta Workforce Identity product roadmap webinars **here**.

Release Highlight videos + Release Notes

Get a concise and informative overview of the latest updates, features, and enhancements. **Watch the highlights.**

See the Release Notes **here.**

Welcome to the US Public Sector Release Overview

Q4 2024

Welcome to the first edition of Okta's Quarterly Release Overview for US Public Sector. We cannot wait to share with you all the innovation we've released in Q4 2024.

Explore how the Okta platform enhances security through a unified policy that protects against social engineering attacks and uses an AAL3 authenticator, to name a few.

Navigating the overview

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

Okta Workforce Identity

- Okta Workforce Identity overview
- Release overviews

Okta Customer Identity

- Okta Customer Identity overview
- Spotlights
- Release overviews

Okta Workforce Identity Releases

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

Learn more about our new capabilities released in Q4 2024.

Easily identify the platform each release is available in:

Classic

Okta Identity Engine (OIE)

Compliance Available or Authorized status:

Available – This product functions as expected and is fully supported in Okta's Public Sector portfolio.

Authorized – This product or feature is Available and FedRAMP and/or DISA authorized.

okta

Access Management

General Availability

Okta Device Access

Available in: Okta Device Access

FedRAMP High/DOD IL4 Authorized

FedRAMP Moderate Available

Using the same authenticators used to secure your Okta-protected apps and workforce devices, your users can verify their identity and sign in to their devices with a secure, seamless experience.

OIE

Just-in-time Local Account Creation for macOS

Available in: Okta Device Access

FedRAMP Moderate/High/DOD IL4 Available

Enable users to create local macOS accounts with standard or administrator privileges to facilitate low-touch account management, especially for shared devices.

Learn more

OIE

Multiple Identifiers

Available in: SSO

FedRAMP Moderate/High/DOD IL4 Authorized

Admins can streamline the sign in experience by giving users more options to identify themselves with Admins can specify which identifiers can be used across various applications.

Classic

OIE

Breached Password Protection

Available in: Universal Directory

FedRAMP High/DOD IL4 Authorized

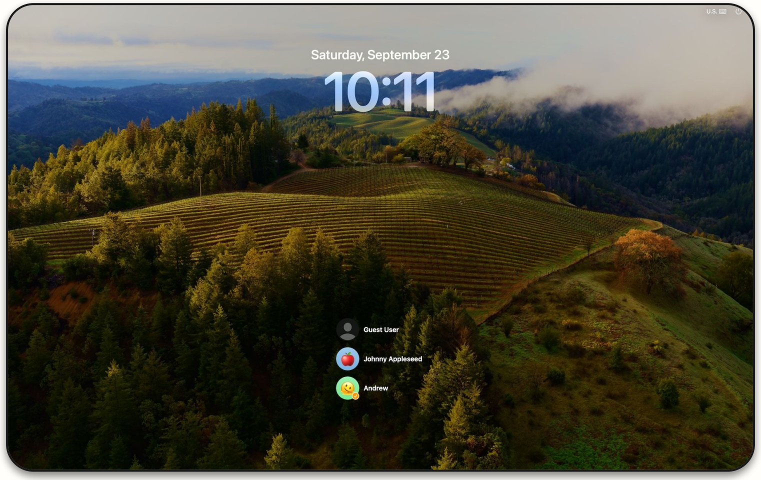
FedRAMP Moderate Available

In-house detection and remediation for the mining of breached credentials. Leverage webhook-eligible system log events to take additional actions outside of the default password reset remediation.

Learn more

Classic

OIE



Just-in-time Local Account Creation for macOS

Access Management

Early Access

Authentication Method Reference (AMR) Claims Mapping

FedRAMP Moderate/High/DOD IL4 Authorized

OIE

Available in: MFA

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

Authenticator Enrollment + Recovery with ASOP

FedRAMP Moderate/High/DOD IL4 Authorized

OIE

Available in: Core

Enhance protection against social engineering attacks with granular control over enrollment and recovery auth flows.

Learn more

Claims Sharing Between Okta Orgs

FedRAMP Moderate/High/DOD IL4 Authorized

Classic

OIE

Available in: Core

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

Enhance Account Linking Restriction

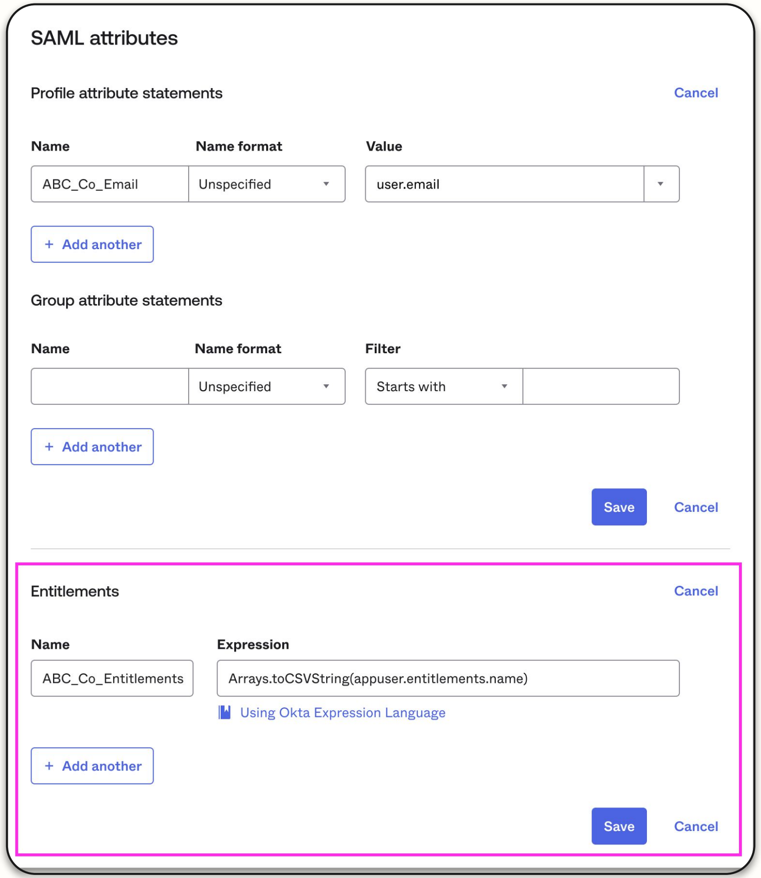
FedRAMP Moderate/High/DOD IL4 Authorized

OIE

Available in: Core

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

Learn more



SAML attributes

Profile attribute statements

Cancel

Name	Name format	Value
ABC_Co_Email	Unspecified	user.email

+ Add another

Group attribute statements

Name	Name format	Filter
	Unspecified	Starts with

+ Add another

Save Cancel

Entitlements

Cancel

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

Using Okta Expression Language

+ Add another

Save Cancel

Entitlements in Assertion and token claims

okta

Access Management

Early Access

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

FedRAMP Moderate/High Authorized

DOD IL4 Available

OIE

Available in: MFA, AMFA

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

Granular Admin Permissions for Configuring Identity Providers

FedRAMP Moderate/High/DOD IL4 Available

OIE

Available in: Core

Assign specific IdPs to other admins through granular admin permissions when creating custom admin roles, ensuring only authorized users are provided access to the configuration of IdPs.

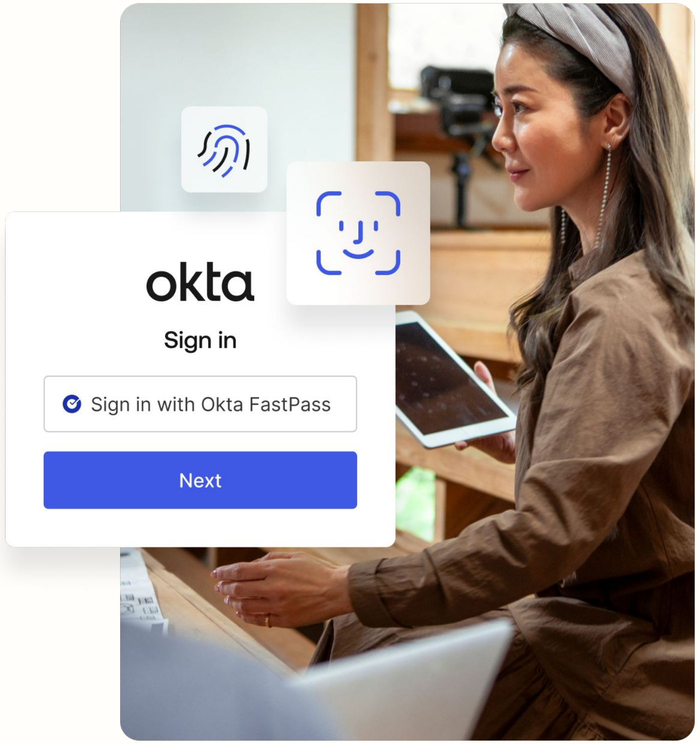
Learn more

Support Universal Logout for Cerby Application

FedRAMP Moderate Available

Available in: Identity Threat Protection

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



Federal Employees can use FastPass as a NIST SP 800-63 AAL3 Authenticator

Identity Management

Early Access

Secure Partner Access

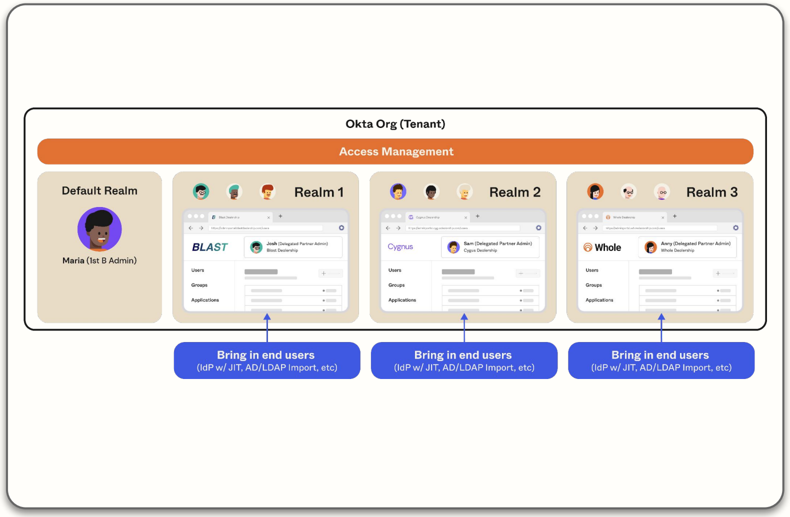
Available in: Secure Partner Access

FedRAMP High/DOD IL4 Authorized

FedRAMP Moderate Available

OIE

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



Secure Partner Access

Platform Services

General Availability

Revamped Permissions UI

FedRAMP Moderate/High/DOD IL4 Authorized

Classic

OIE

Available in: Workforce Identity Cloud Platform

Improve the user experience for admin role creation for a scalable UI to accommodate new granular permissions and better layout to help super admins understand what permissions may be needed for a specific job to be done.

Workflows Authorized for FedRAMP High

FedRAMP Moderate/High Authorized

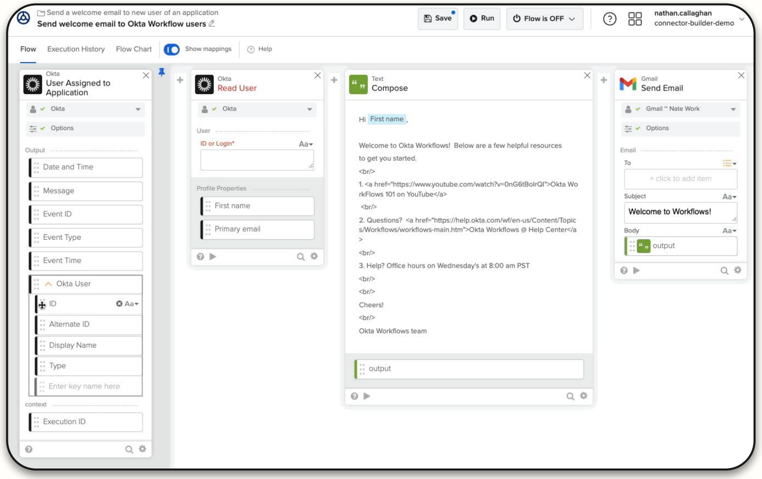
Classic

OIE

Available in: All Workflows

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

Learn more



```
Hi First name,

Welcome to Okta Workflows!  Below are a few helpful resources
to get you started.
<br/>
1. <a href="https://www.youtube.com/watch?v=0nG6tBolrQI">Okta WorkFlows 101 on YouTube</a>
 <br/>
2. Questions?  <a href="https://help.okta.com/wf/en-us/Content/Topics/Workflows/workflows-main.htm">Okta Workflows @ Help Center</a>
<br/>
3. Help? Office hours on Wednesday's at 8:00 am PST
<br/>
<br/>
Cheers!
<br/>
Okta Workflows team
```

Workflows Authorized for FedRAMP High

Platform Services

Early Access

Dynamic Resource Sets

FedRAMP Moderate/High/DOD IL4 Available

Classic

OIE

Available in: Workforce Identity Cloud Platform

Dynamically assign resources to admins in custom admin roles.

Learn more

Okta Admin App Assignment

FedRAMP Moderate/High/DOD IL4 Available

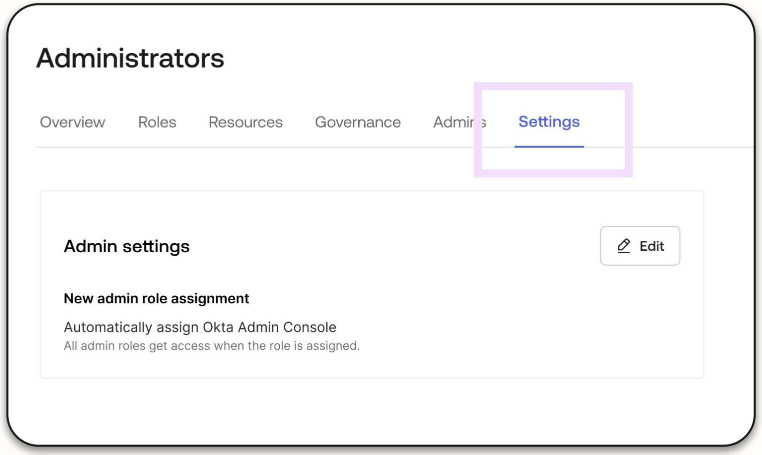
Classic

OIE

Available in: Workforce Identity Cloud Platform

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

Learn more



Administrators

Admin settings

New admin role assignment

Automatically assign Okta Admin Console

All admin roles get access when the role is assigned.

Okta Admin App Assignment

Okta Customer Identity Releases

Okta Customer Identity—formerly known as Customer Identity Solution (CIS)—is dedicated to ensuring that security comes first when it comes to providing seamless digital experiences. It enables organizations to accelerate growth, navigate evolving security challenges, and protect customer and business data effectively.

Learn more about our new capabilities released in Q4 2024.

General Availability

Spotlight: Okta Customer Identity for US Public Sector

Secure public sector digital experiences with Okta Customer Identity

What is it?

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

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

Why this matters

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

How to get it

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

Contact us

Okta Customer Identity

General Availability

Okta Account Management Policies

FedRAMP Moderate/High/DOD IL4 Authorized

OIE

Feature of: Okta Customer Identity

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

Demonstration of Proof of Possession (DPoP)

FedRAMP Moderate/High/DOD IL4 Available

OIE

Feature of: Okta Customer Identity

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

New End User Profile & MFA Settings Page

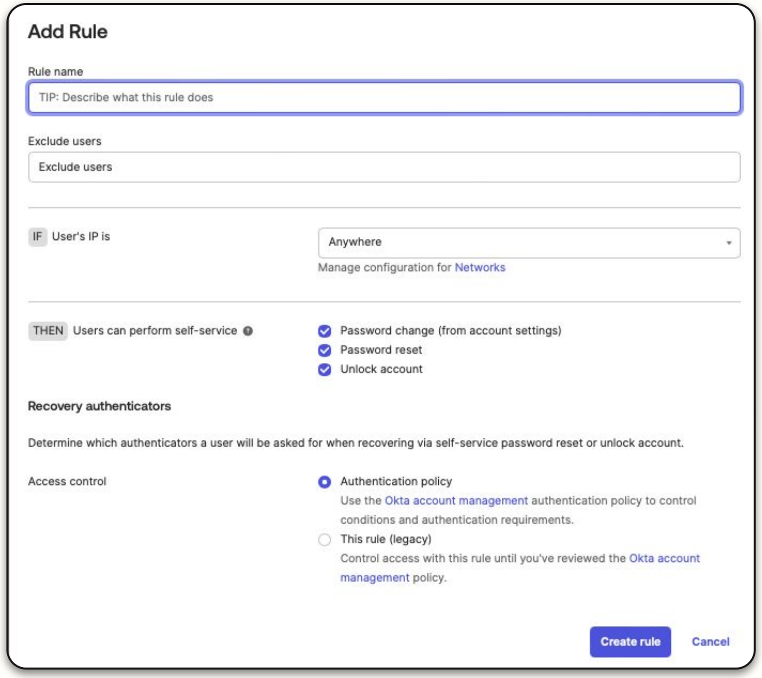
FedRAMP Moderate/High/DOD IL4 Available

Classic

OIE

Feature of: Okta Customer Identity

Expanded ThreatInsight detection and response to all API endpoints. Allows customers to detect and block client access from ThreatInsight IPs across the public API surface.



Add Rule

Rule name

TIP: Describe what this rule does

Exclude users

Exclude users

IF User's IP is: Anywhere

Manage configuration for Networks

THEN Users can perform self-service

☑ Password change (from account settings)

☑ Password reset

☑ Unlock account

Recovery authenticators

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

Access control

● Authentication policy

Use the Okta account management authentication policy to control conditions and authentication requirements.

○ This rule (legacy)

Control access with this rule until you've reviewed the Okta account management policy.

Okta Account Management Policies

Okta Customer Identity

Early Access

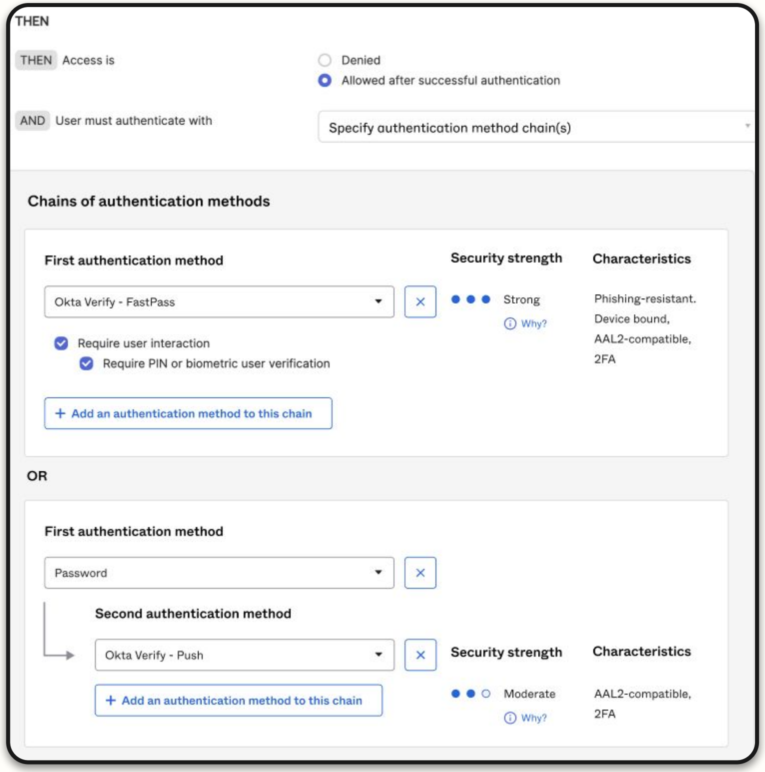
Authenticator Sequencing

FedRAMP Moderate/High/DOD IL4 Authorized

Feature of: Okta Customer Identity

OIE

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



THEN

THEN Access is ○ Denied
● Allowed after successful authentication

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

Chains of authentication methods

First authentication method: Okta Verify - FastPass ×
☑ Require user interaction
☑ Require PIN or biometric user verification
+ Add an authentication method to this chain

Security strength: ●●● Strong (ⓘ Why?)
Characteristics: Phishing-resistant, Device bound, AAL2-compatible, 2FA

OR

First authentication method: Password ×

Second authentication method: Okta Verify - Push ×
+ Add an authentication method to this chain

Security strength: ●●○ Moderate (ⓘ Why?)
Characteristics: AAL2-compatible, 2FA

Authenticator Sequencing

okta