E-book

Beyond MFA: The FastPass advantage

Securing identity in a Zero Trust environment

okta

Contents

Introduction

In today's threat landscape, attackers aren't just breaking in — they are logging in, and not just with stolen usernames and passwords. Increasingly, attackers are bypassing traditional multi-factor authentication (MFA) using more advanced techniques.

Okta FastPass is a phishing-resistant, passwordless authentication method that supports secure access across the user journey. Delivered via the Okta Verify app, it is designed for a Zero-Trust architecture and supports contextual, phishing-resistant authentication beyond the initial login, helping protect each access attempt.

Phishing-resistant multi-factor authentication (MFA) is increasingly viewed as a standard security expectation, particularly in high-assurance environments. For example, U.S. federal agencies are required to implement phishing-resistant MFA under OMB M-22-09[1], and many private sector organizations are adopting similar controls to align with Zero Trust practices.

Unlike other advanced authenticators, FastPass can evaluate an extensive range of device signals in real time, each time the user attempts to access a new protected resource. It provides a user-friendly, secure, and consistent experience across all major platforms and devices, managed or unmanaged. In many enterprise deployments, IT teams report a significant drop in help desk tickets post-FastPass rollout, particularly related to password resets and login issues. This reinforces FastPass as not just a security tool, but a driver of productivity.[2]

Use this eBook to help your team move beyond initial setup and unlock the full value of your FastPass implementation. Inside, you'll find advanced best practices to support:

- Maximizing adoption and delivering a seamless user experience
- Strengthening security posture, reducing risk, and supporting compliance
- Driving operational agility

These best practices align with the Okta Identity Maturity Model (IMM)[3], helping you progress from foundational MFA to advanced, phishing-resistant, passwordless authentication that supports Zero Trust initiatives.

You'll also discover how FastPass compares to traditional MFA methods — and why its modern, phishing-resistant approach is essential for enterprises adopting Zero Trust principles.

---

[1] U.S. Office of Management and Budget, M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"

[2] Password resets represent a significant expense for IT support, frequently accounting for 50% of help desk inquiries. By implementing Okta FastPass, organizations can achieve operational efficiencies and boost productivity by removing the need for passwords. This transition to seamless and secure passwordless authentication reduces user friction. Sources: FastPass Technical Whitepaper, p. 3; Secure Sign-In Trends Report 2024, p. 31

[3] Okta, A Guide for Your Identity Maturity Journey.

Understanding Okta FastPass and Okta Verify

Okta FastPass and **Okta Verify** work together to deliver secure, seamless authentication.

Okta FastPass is a phishing-resistant, passwordless authentication method **supported by the Okta Verify app**. It enables users to securely access resources without passwords.

Okta Verify is the mobile or desktop app that powers FastPass. It supports additional authentication methods, including push notifications and one-time passcodes (OTPs).

To use **Okta FastPass**, users must install the latest version of the **Okta Verify** app and enroll their device(s).

Together, these tools support a range of use cases from traditional MFA to passwordless authentication aligned with Zero Trust principles.

Adopting **FastPass** with **Okta Verify** helps organizations mature to the advanced stages of the Okta Identity Maturity Model by phasing out passwords and foundational MFA and implementing biometric-based MFA and context-aware access across platforms.

[4] Okta FastPass documentation

Section 1

Maximizing adoption and providing a great end-user experience

Securing enterprise users and data requires more than single sign-on (SSO) and traditional MFA. As attackers become more sophisticated, the need for strong, phishing-resistant authentication will continue to grow. Secure MFA methods like Okta FastPass are critical for protecting your workforce and sensitive resources.

Mature identity organizations recognize that user experience is critical to security transformation. According to the Okta IMM, delivering seamless, passwordless access through phishing-resistant methods like FastPass is a hallmark of the Advanced and Strategic stages.

At the same time, your workforce — employees, contractors, and partners — needs a consistent and seamless authentication experience that doesn't slow them down. End users can enjoy passwordless authentication to all FastPass-protected resources. This significantly improves the employee experience by reducing the friction introduced by passwords (and password resets).[5]

Planning your FastPass implementation requires understanding the technical requirements for the initial pilot program and wider rollout, as well as a thoughtful communications plan for successful adoption across the organization.

[5] Okta FastPass Technical Whitepaper, p. 5

Customer Spotlight: Hubspot

Ownership and reviewers

80%	reduction in help desk access provisioning tickets
100%	of logins use phishing-resistant MFA from registered devices[6]
80%	of access-request tickets resolved via automation

"[Okta Identity Engine] was a real game-changer for HubSpot because it gave us access to FastPass, phishing resistance, and a holistic, end-to-end solution. We can get granular on a per-application basis and integrate device trust and user information to make the right front-end authentication choices."

Eric Richard
HubSpot SVP of Engineering and
Chief Information Security Officer

HubSpot's success with FastPass demonstrates how organizations can evolve from non-phishing-resistant MFA to a more advanced identity experience, consistent with IMM's advanced stage of operational agility and user satisfaction.

[6] In this context, "registered devices" refers to devices enrolled with Okta Verify, regardless of whether they are mobile device management (MDM)-managed or unmanaged.

Checklist: Onboarding

Pre-deployment

- ✓ Verify your Okta environment is upgraded to the Okta Identity Engine to support FastPass deployment.
- ✓ Set up a Global Session Policy in Okta to control users' access to your environment. A global session policy supplies the context necessary for the user to advance to the next authentication step after Okta identifies them.
- ✓ Evaluate which phishing-resistant factors will be supported in your organization (e.g., FastPass with biometrics, FIDO2 key, or both). Note that biometric setup and fallback options may affect support readiness and user experience.

Pilot phase

- ✓ Select a small group of early adopters to test the user experience and refine your rollout strategy.
- ✓ Use the Step-by-Step Guide to automate Okta Verify via mobile device management (MDM), if available.[7]

Rollout phase

- ✓ Distribute clear, platform-specific instructions (via the Launch Kit for Okta Admins quick start guides) for installing Okta Verify on users' devices.
- ✓ Use email templates from the Launch Kit for Okta Admins to plan user communication and training.
- ✓ Confirm users have installed the latest version of the Okta Verify app and created an account on their desktops, laptops, or mobile devices.[9]
- ✓ Continuously gather and act on end-user feedback at each rollout stage to improve adoption and satisfaction.

---

[7] Step-by-step guide to becoming phishing-resistant with Okta FastPass, p. 17

[8] Launch Kit for Okta Admins, see the Setup Okta Verify QRG and Sign in using Okta FastPass QRG.

[9] Okta FastPass documentation

Communication

- ✓ Communicate the Okta FastPass rollout to your organization in phases. Utilize the Launch Kit for Okta Admins for customizable email templates, quick start guides, and a FastPass FAQ to assist end users and the IT help desk.
- ✓ Prepare your support team for common help desk inquiries such as failed Okta Verify enrollment, FastPass activation errors, missing biometric permissions, registration timeouts, fallback factor confusion, or devices not meeting device posture policy. Document troubleshooting steps for escalation and proactively inform your support team.

Section 2

Strengthening security, risk mitigation, and compliance

Okta FastPass is a passwordless, phishing-resistant authentication solution that supports modern enterprise security requirements and compliance mandates. It helps protect users when they log in, and throughout the lifespan of their active sessions, helping your organization comply with access control, user assurance, and device posture requirements.

This section describes how organizations can align with the Okta IMM **Security and Compliance** outcomes, emphasizing phishing-resistant authentication, device posture enforcement, and risk-based access as indicators of identity maturity.

Customer spotlight: ManTech

A leading federal government contractor, ManTech uses Okta to help them meet strict compliance requirements, including ~25 percent of the 110 NIST 800-171 (CMMC) controls.

> "FastPass gives us the rare chance to offer something that's both more secure and makes it easier for end users simultaneously..."Improving both at once is almost unheard of."
>
> **Mike Uster**
> CIO and CTO, ManTech

ManTech's deployment of FastPass to help meet strict federal compliance requirements illustrates the regulatory alignment and zero-trust enforcement seen at the advanced and strategic stages of the Okta IMM.

FastPass and threat prevention

FastPass is a phishing-resistant authenticator that combines device context, user verification, policy enforcement, and phishing resistance to thwart several attacks. As your identity program progresses, the ability to block sophisticated attack techniques is a key indicator of advancement into the Advanced IMM stage.

Attack type	How FastPass protects
Credential Theft, Replay, and Adversary-in-the-Middle (AiTM) Phishing	FastPass uses cryptographically signed challenges (nonces) tied to device possession and biometric verification. It verifies the origin URL and prevents replay by never exposing shared secrets. AiTM attacks are blocked by rejecting spoofed domains and enforcing phishing-resistant policies.[10]
Session Hijacking	Performs silent device posture checks on each new app launch or reauthentication, blocking stolen session reuse.[11]
Brute-Force Login Attacks	Significantly reduces guessable credentials; relies on possession + biometric factors.[12]
SIM Swap / SMS Interception	Avoids SMS entirely; no reliance on phone number–based OTP.[13]
Unauthorized Authenticator Enrollment	Require FastPass enrollment before allowing users to enroll new authenticators, to reduce shadow MFA authenticator sprawl.[14]
Device Spoofing / Access from Non-Compliant Devices	Enforces real-time device assurance checks (e.g., management attestation, OS patch level, encryption, jailbreak status) and blocks access from devices not meeting policy requirements.[15]

[10] FastPass Technical Whitepaper, p. 4, 7–8; 19–21; Secure Sign-In Trends Report 2024, p. 39–40, How to go passwordless with Okta, p. 4–5

[11] FastPass Technical Whitepaper, p. 16; Secure Sign-In Trends Report 2024, p. 31

[12] Secure Sign-In Trends Report 2024, p. 41

[13] Secure Sign-In Trends Report 2024, p. 25

[14] Step-by-step Guide to Becoming Phishing-Resistant, p. 6-7

[15] FastPass Technical Whitepaper, p. 15–17; Step-by-step Guide to Becoming Phishing-Resistant, p. 17–18

Compliance Alignment: Mapping FastPass to security frameworks

FastPass supports more secure, phishing-resistant authentication that better aligns with regulatory mandates and Zero Trust principles.

Framework	How FastPass helps
Secure Authentication (NIST SP 800-63 (Revisions 3 and 4)	• Enables passwordless, phishing-resistant MFA. • Supports Authentication Assurance Level 3 (AAL3) — the highest authentication assurance level defined by NIST — when used with a FIPS 140-3 Level 2 compliant device.[16]
Zero Trust Architecture (U.S. Executive Order 14028, CISA)	• Supports device trust and user assurance. • Supports device posture checks throughout active SSO sessions. • Integrates with endpoint detection and response (EDR) tools like CrowdStrike and Windows Security Center (WSC) to enforce policy and detect threats.[17]

Checklist: FastPass best practices for security and compliance

Use this checklist to guide your initial confirmation, rollout, and enforcement of FastPass in your environment.

Pre-deployment

✓ **Enable FastPass as a primary login factor.**
Enable Okta FastPass to deliver phishing-resistant, passwordless authentication. When used with FIPS 140-3 Level 2 devices, FastPass can help you meet NIST AAL2/AAL3 compliance requirements.[18]

✓ **Restrict FastPass to trusted applications.**
To enhance security, limit FastPass invocation to trusted applications only. Trusted applications possess established security protocols, administrator-managed settings, and validated integrations. This practice reduces the risk of session hijacking and origin spoofing.

✓ **Support phishing-resistant access across all device types.**
Deploy FastPass on managed and unmanaged Windows, macOS, iOS, and Android devices - including virtual desktop infrastructure (VDI) environments like Windows 365, Citrix, and AWS WorkSpace.[19]

[16] FastPass Technical Whitepaper, p. 2

[17] FastPass Technical Whitepaper, p. 4–5, 15, 25

[18] FastPass Technical Whitepaper, p. 2–3

[19] FastPass Technical Whitepaper, p. 5; Sign in with Okta FastPass QRG

- ✓ **Integrate with platform biometrics.**
  Use device-native platform authenticators like Face ID, Touch ID, and Windows Hello to help you meet NIST AAL3 requirements for inherence factors and to strengthen user verification.[20]
- ✓ **Enforce device assurance policies.**
  To maintain compliance and reduce risks, require devices and browsers to meet minimum security standards (e.g., device OS version, security patch levels, disk encryption, and jailbreak status) before allowing access.[21]
- ✓ **Disable or limit weaker MFA methods.**
  (see Table: MFA Method Comparison).
  Deprioritize legacy MFA methods like SMS, push notifications, or Time-based One-Time Password (TOTP). Instead, favor phishing-resistant options such as FastPass with biometrics, or FastPass with a hardware key (e.g., a FIDO2 key).[22]
- ✓ **Continuously evaluate and enforce device compliance in real time — even for unmanaged or BYOD devices.**
  FastPass can enforce device compliance checks at each login for unmanaged or BYOD devices, extending Zero Trust protection across your device ecosystem.

  Note: Devices not managed by MDM can still be registered via Okta Verify, enabling Okta FastPass to enforce context-aware access.[23] [24]
- ✓ **Protect active sessions through silent context evaluation.**
  FastPass supports silent re-evaluation of device posture throughout active SSO sessions, at every new app launch or re-authentication point, helping detect risk changes and enforce session security.[25]
- ✓ **Integrate third-party security signals to enhance policy decisions.**
  Enhance policy decisions by integrating endpoint risk scores and device health signals from tools like CrowdStrike and Windows Security Center. These signals can help trigger risk-based access controls or automated remediation actions via Okta Workflows.

---

[20] FastPass Technical Whitepaper, p. 7–8; Sign in with Okta FastPass QRG, p. 3

[21] FastPass Technical Whitepaper, p. 15–16

[22] Secure Sign-in Trends Report 2024, p. 25–29

[23] FastPass Technical Whitepaper, p. 15–17

[24] Step-by-step Guide, p. 17; FastPass Technical Whitepaper, p. 8, 25

[25] FastPass Technical Whitepaper, p. 16; Secure Sign-in Trends Report 2024, p. 31p. 8, 25

Table: MFA method comparison

Many organizations rely on older MFA methods that are still vulnerable to phishing or lack device binding or device assurance. This table shows how Okta FastPass compares to these methods.

MFA method	Factors used	Common usage	User Experience	Phishing resistant	Device binding	FastPass advantage
Password + SMS	Knowledge + Possession	Legacy	Inconsistent	No	No	FastPass is passwordless. It greatly reduces the risk of Adversary-in-the-Middle (AiTM) attacks common with SMS.
Password + Email OTP	Knowledge + Possession	Legacy or fallback MFA	Inconsistent | possible email delays.	No	No	FastPass offers a passwordless, phishing-resistant alternative with device context.
Password + TOTP (Authentication apps)	Knowledge + Possession	Common in MFA deployments	Manual entry adds user friction.	No	No	FastPass enables seamless, passwordless login with no codes to enter manually.
Password + Push	Knowledge + Possession	Common enterprise MFA method	Low friction may lead to MFA prompt fatigue.	No	No	FastPass can be leveraged alongside biometrics for seamless and secure user verification.

[26] Device binding ensures the credential is only usable from a specific device for phishing resistance and preventing session theft. Device assurance checks device security posture before allowing access – a requirement for Zero Trust.

Table: Phishing-resistant MFA comparison

If you're already considering deploying one or more types of phishing-resistant authentication, here is a comparison of FastPass with FIDO2 hardware authenticators and passkeys.

MFA method	Factors used	Common usage	User Experience	Phishing resistant	Device binding	FastPass advantage
FIDO2 hardware tokens (e.g., YubiKey, Feitian)	Possession + Inherence (when biometrics are used on the key), OR Possession only	High-security and regulated environments	Simple, but requires the user to carry and manage a physical device.	Yes	Yes (origin binding to hardware authenticator)	FastPass meets the NIST 800-63B Authentication Assurance Level 2 (AAL2) and AAL3 when configured appropriately.
FIDO2 as Passkeys (Apple, Google, Microsoft)	Possession + Inherence (Biometric PIN, etc.)	Consumer and business	Seamless and passwordless, it is native to platforms (Apple iCloud Keychain, Google Password Manager, Windows Hello). Some cross-platform limitations exist, though they are improving with ecosystem efforts (e.g., passkey syncing).	Yes	Yes (credential bound to user device)	FastPass supports centralized enterprise-grade policy control, real-time device posture checks, and works across heterogeneous OS environments (i.e., it is not dependent on a specific platform ecosystem). It also supports cross-platform policy enforcement through Okta.
Okta FastPass	Possession + Inherence (Biometric)	Enterprise Zero Trust MFA	Consistent experience across desktops and mobile devices.	Yes	Yes	Prepare your support team for common help desk inquiries such as failed Okta Verify enrollment, FastPass activation errors, missing biometric permissions, registration timeouts, fallback factor confusion, or devices not meeting device posture policy. Document troubleshooting steps for escalation and proactively inform your support team.

Section 3

Realizing operational agility and value

Password resets are among the most costly IT support requests, often comprising 50 percent of help desk volume.[27] Industry analysts have estimated that a password reset costs about $70 per incident, depending on the organization's helpdesk and average time to resolution.[28] Organizations adopting Okta FastPass can realize operational and productivity gains by eliminating passwords and reducing friction through seamless and secure passwordless authentication. As defined by the Okta IMM, organizations in the Advanced and Strategic stages can reduce identity-related support costs by automating passwordless authentication and aligning their access policies to include contextual and risk signals.

Okta FastPass delivers a familiar and secure passwordless sign-in experience consistent across supported operating systems, browsers, and applications.

By streamlining authentication with low challenge times and minimal user error rates, FastPass boosts workforce productivity at every access point.

IT teams become more efficient by eliminating password resets, lowering help desk volume, and eliminating the need to manage multiple legacy MFA methods. This helps organizations reduce costs and administrative challenges related to password management.

[27] FastPass Technical Whitepaper, p. 3; Secure Sign-In Trends Report 2024, p. 31

[28] This estimate is widely referenced in industry research, including reports from Forrester Research (via secondary sources)

Customer Spotlight: Jamf

75% reduction in time to migrate employees from acquired companies using Okta

90% reduction in time to provision new hires

60% increase in Day One employee productivity with automated provisioning

"We have a layered security approach to our conditional access policies to enable this to be the case. We are using network location, Okta's ThreatInsight's risk scoring, Okta Device Trust, and Okta FastPass. All of them are working together to make sure that users have a great seamless login experience while still providing strong security."

Mitch Francese
Senior IT Systems Administrator, Identity and Access Management, Jamf

This customer demonstrates identity maturity by achieving operational agility and improved user experiences via context-aware access enforcement and automation.

Checklist: Operational agility and business value with FastPass

Use this checklist to guide best practices that reflect the Okta Identity Maturity Model's Operational Agility category, by reducing support overhead and user friction.

Before rollout

- ✓ **Promote C-suite and Board alignment by making MFA adoption an executive metric.**
  Track and report adoption to executive leadership monthly.[29]
- ✓ **Benchmark the current help desk volume for password reset tickets.**
  Establish pre-rollout metrics to track ROI.[30]
- ✓ **Remove phishable factors from existing authentication policies.**
  Replace SMS, TOTP, and push notifications with phishing-resistant options where possible.[31]
- ✓ **Edit authentication policies in increments and test thoroughly.**
  Use phased policy changes to reduce user impact and isolate issues during rollout.[32]
- ✓ **Verify BYOD and unmanaged device compatibility with FastPass.**
  Confirm FastPass works across user devices, including mobile and VDI.[33]
- ✓ **Apply phishing-resistant policies to low-traffic and non-sensitive applications first.**
  Start with apps with the least amount of use to verify your policies work, before enforcing org-wide.[34]
- ✓ **Roll out in segments by application risk and user role.**
  Prioritize high-risk users (IT, execs) and sensitive apps.[35]
- ✓ **Configure silent or opt-in enrollment for initial rollout.**
  Use non-mandatory sign-in prompts to ease adoption and reduce friction.[36]
- ✓ **Roll out in segments by application risk and user role.**
  Configure device checks such as OS version, encryption, and jailbreak status.[37]
- ✓ **Integrate third-party EDR/UEM tools (e.g., CrowdStrike, Windows Security Center)**
  Add external risk context for richer access decisions.[38]

[29] Secure Sign-In Trends Report 2024, p. 49

[30] Internal ROI baseline best practice; supported by metrics in FastPass Datasheet and Secure Sign-In Trends Report 2024, p. 31

[31] How to go passwordless with Okta, Okta, p. 2–4

[32] FastPass Technical Whitepaper, Okta, p. 13

[33] FastPass Technical Whitepaper p. 3-5

[34] FastPass Technical Whitepaper, p. 13; Secure Sign-In Trends Report 2024, p. 21

[35] Secure Sign-In Trends Report 2024, p. 21; How to go passwordless with Okta, p. 5

[36] FastPass Technical Whitepaper, p. 9; Secure Sign-In Trends Report 2024, p. 33

[37] FastPass Technical Whitepaper, p. 15; Secure Sign-In Trends Report 2024, p. 31

[38] FastPass Technical Whitepaper, p. 25; Secure Sign-In Trends Report 2024, p. 39

After rollout

- ✓ **Track post-rollout help desk volume and compare to baseline.** Quantify savings from reduced password-related tickets.[39]
- ✓ **Benchmark productivity impact across departments.** Measure time saved per login and user sentiment on the authentication experience.[40]
- ✓ **Track authenticator usage: FastPass vs fallback methods.** Use the MFA Usage report to see how often FastPass (authentication method: *Okta Verify-signed_nonce*) is used across applications and time. This helps identify adoption trends and supports efforts to deprecate weaker factors.[41]
- ✓ **Report challenge time improvements from FastPass adoption.** Highlight login time reductions vs. passwords or OTPs.[42]
- ✓ **Build phishing alert and remediation workflows via Okta Workflows.** Act on FastPass origin header failures for real-time protection.[43]
- ✓ **Treat FastPass as both a security control and a UX improvement.** Reinforce that phishing resistance can enhance the user experience.[44]

[39] FastPass Datasheet; Secure Sign-In Trends Report 2024, p. 31

[40] Secure Sign-In Trends Report 2024, p. 29

[41] Step-by-step guide to becoming phishing-resistant with Okta FastPass, p. 11.

[42] Secure Sign-In Trends Report 2024, p. 29

[43] Okta FastPass Technical Whitepaper, p. 20; Secure Sign-In Trends Report 2024, p. 39

[44] Secure Sign-In Trends Report 2024, p. 47, 49

Section 4

Authentication in context: where FastPass fits in the Identity Maturity Model

This table shows how FastPass contributes to the Identity Maturity Model stages and categories related to MFA. To learn more about different MFA factors, see the tables on typical MFA methods and phishing-resistant MFA methods.

IMM Stage	Governance Focus	Security Posture	User Experience	Operational Agility
Fundamental	Password-based login, SMS/OTP MFA enabled for some users	Credentials are phishable; no device context or policy enforcement	Inconsistent logins, frequent friction, reliance on passwords	High help desk burden (e.g., password resets); no centralized MFA reporting
Scaling	MFA with SSO; adoption of possession/ inherence factors like push or biometrics	Stronger assurance for managed users; posture checks collected but not enforced	Push-based or biometric login enabled; fallback methods used for some	Centralized MFA policies deployed; admins monitor authenticator usage across apps
Advanced	Passwordless, phishing-resistant MFA with FastPass and device-native biometrics	Device posture evaluated in real-time; enforcement for OS, encryption, jailbreak status	Seamless, no-prompt logins on compliant devices; users remediate posture when needed	FastPass usage tracked via reporting; legacy factors deprecated; fewer login-related tickets
Strategic	Continuous, risk-aware access using FastPass and contextual policies	Session posture re-evaluated; FastPass policy decisions integrate EDR/ UEM signals	Adaptive experience based on user and device risk; zero trust enforced silently	FastPass adoption KPIs tracked; security, UX, and compliance teams aligned on posture policy impact.

Section 5

Continuing your FastPass Journey

Okta Learning

To help deepen your expertise and maximize the value of your FastPass deployment, we recommend the following Okta Learning courses.

General IAM skills

- Identity Access Management: Exploration: A foundational IAM overview for those new to IAM or Okta concepts.
- Badge: Explore Identity Foundations: Build a strong foundation with this quick course that explores key concepts of IAM, industry standards, and Okta solutions. You can earn a skills badge by passing the exam at the end of this course.

Administration and certification path

- Administration: Onboarding: This course provides IT administrators with skills to build key secure identity management skills such as user and group management, user lifecycle management, application integration with SSO methods like SAML, and authentication policy enforcement, including passwordless authentication. You'll have opportunities to collect some skill badges along the way and get a head start in preparing for the Okta Certified Professional Exam.

FastPass-specific deployment

- Get Started with FastPass: Learn how to deploy and optimize FastPass for passwordless, phishing-resistant authentication.
- Enable FastPass with Okta Verify: Follow this step-by-step guide to enable FastPass on users' devices and choose the optimal user verification method (preferred or required) for enrollment.

Join the conversation

Join the Okta customer support community for FastPass to find expert-led learning sessions, latest news and announcements.

YouTube resources

Okta's YouTube channel contains many videos on setting up, deploying, and optimizing FastPass.

Customer success

For further assistance in deploying FastPass, contact your Okta Customer Success team.

Appendix: Resources

Section 1: Adoption and end-user experience

Use Case / Phase	Recommended Resources
Planning a passwordless or phishing-resistant strategy	Launch Kit for Okta Admins Step by Step Guide to Becoming Phishing-Resistant with FastPass FastPass Technical Whitepaper
Configuring and testing FastPass in a pilot environment	Configure Okta FastPass Video: Okta FastPass Configuration Step by Step Guide to Becoming Phishing-Resistant with FastPass
Rolling out to early adopters or admin teams	Webinar: Okta's Journey to Passwordless
Communicating benefits to stakeholders	Okta FastPass Product Page

Section 2: Security and compliance

After initial FastPass deployment, you can use these resources to learn about policy enforcement, validation, and Zero Trust alignment.

Use Case / Phase	Recommended Resource
Strategic Planning and Executive Justification	How to Go Passwordless with Okta
Architecture and Technical Understanding	FastPass Technical Whitepaper
Zero Trust Framework Alignment	Video: Okta FastPass: Zero Trust Authentication For Phishing-Resistant, Passwordless Access
Factor Selection and Compliance Mapping	Datasheet: Factor Types and Assurance Levels
Initial Deployment and Phishing-Resistant Rollout	Step-by-step guide to becoming phishing resistant with Okta FastPass
Establishing Device and Posture Policies	Support article: Setting Up Policies for a Passwordless Authentication Experience with FastPass
Securing Unmanaged and BYOD Devices	Support article: Is Okta FastPass Considered a Phishing-Resistant Authenticator for Unmanaged BYOD Devices
Validating Authentication Security Posture	Support article: Okta Security Knowledge – Phishing Resistant Factors
Audit, Logging, and Compliance Validation	Support article: How to Verify User Login via FastPass from System Logs
Zero Trust Maturity Measurement and Reporting	Support article: ZTA Score and Okta Verify FastPass
Reference Validation for Compliance and Security Audits	Datasheet: Factor Types and Assurance Levels

Section 3: Operational agility and value

Use Case / Phase	Recommended Resource
Staying current with FastPass feature updates	Okta FastPass Product Page
Executive justification and value alignment	How to Go Passwordless with Okta
Technical validation for scaling FastPass	FastPass Technical Whitepaper
Learning from internal deployment success	Webinar: Okta's Journey to Passwordless & Phishing-Resistance
Benchmarking industry trends in authentication	Secure Sign-in Trends Report 2024 | Okta
Showcasing business value and user impact	Customer Story: HubSpot strengthens Identity security through phishing-resistant MFA
Comparing FastPass to hardware authenticators	Advantages of Okta FastPass over YubiKey
Understanding posture evaluation with fallback MFA	Device Status when Authenticating with Another Factor Aside from FastPass