okta | yubico

Okta and Yubico—delivering phishing-resistant MFA and a bridge to passwordless

YubiKeys and Okta FastPass work together to provide the strongest levels of identity assurance against phishing while delivering a fast and easy user experience.

By combining Okta's suite of MFA solutions with Yubico's hardware-based authentication services, organizations can streamline access controls while adding a stronger layer of protection against modern cyber attacks. With phishing and other forms of account takeovers on the rise, the need for phishing-resistant MFA is more critical than ever before. And while any form of MFA is better than a password, not all MFA is created equal. Organizations have a choice of MFA options to raise the bar for security and there are security and usability tradeoffs with each option. Both Okta FastPass and YubiKeys offer phishing-resistance and address different organizational needs.

Okta FastPass

- Okta FastPass is a phishing-resistant solution meeting a high security assurance level
- FastPass is an agent that is installed on the device (phone, computer) and is device-specific thus requiring setup across platforms

Okta FastPass—what you need to know

- FastPass is proprietary, device-reliant, software-based MFA, requiring the Okta Verify app running on Okta Identity Engine (OIE)

Okta FastPass—what it works well for

- FastPass is easy and convenient as it eliminates the need for repeated password entry
- FastPass can only be used on SAML, OIDC, or WS-Fed applications within Okta

Solution highlights

YubiKeys

- YubiKeys offer the highest security assurance
- YubiKeys secure the user across platforms and moves with the user, and is not device-specific, allowing for strongest security with the greatest flexibility

YubiKeys extend phishing-resistant authentication use cases with:

- Bootstrapping of FastPass using a YubiKey
- Interoperability and authentication on all platforms: macOS, Linux, iOS and Android or devices without TPM or Biometric support
- Support for FIDO and smart card open standards
- Ability to meet stricter security and compliance requirements

yubico

Enable secure onboarding and recovery

The MFA that customers decide to implement is only as secure as the registration and recovery. Registration or onboarding processes using phishable methods like sending OTP codes lead to vulnerable MFA deployment. If anyone can register or reset the FIDO credential then it defeats the purpose of using phishing-resistant MFA. Organizations need to have a robust onboarding and recovery solution to bootstrap the enrollment of the MFA method. Using a pre-enrolled YubiKey provisioned and delivered to the end-user creates the strong binding needed to bootstrap the setup of FastPass. This significantly raises the bar for security and usability creating a robust credential lifecycle strategy that an organization can build upon.

YubiKeys satisfy Federal mandates for highest security assurance

- YubiKeys are allowed in secured areas where mobile devices are prohibited
- YubiKeys can help when government agencies have legacy or custom built systems that are not compatible with Okta FastPass
- FIPS certification is only for Okta Verify, not specifically Okta FastPass

Zero Trust and phishing-resistant MFA are mandated for government agencies and vendors

- 800-53 is mandatory for all US federal systems to comply with and it is referenced in 800-171
- CMMC requires the use of MFA by DoD Contractors.
- CCM v4 requirement for MFA tracks back to NIST 800-53

	Okta FastPass	YubiKey FIDO2	YubiKey PIV/CAC
Passwordless and phishing-resistant	✓	✓	✓
Supports Windows sign-in		✓	✓
Supports Web sign-in	✓	✓	✓
Supports shared workstations	✓[1] requires 1 shared user profile on OS	✓	✓
Supports on-prem resources	✓[2]	✓	✓
Portable to other devices	✓	✓	✓
Works on mobile	✓	✓[3]	✓
Works on macOS	✓	✓	✓
Works on Linux		✓	✓
Supports other RPs	✓[4]	As multi-protocol key	As multi-protocol key

[1] For each Okta user account, it is expected that there would be different Okta Verify enrollments for each individual user; which would be stored securely on the same OS user profile. Source: Okta Verify FastPass Shared Workstations
[2] Requires the resource to be Okta-protected; must support OIDC, SAML, WS-Fed
[3] Android FIDO2 beta support released
[4] If RP is federated to Okta

Contact us yubi.co/contact

Learn more yubi.co/okta

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, please visit: www.yubico.com.