Passkeys Done Right

Phishing-Resistant, Passwordless Enterprise Deployments with YubiKeys

What are Passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable multifactor authentication (MFA) with more secure passwordless experiences.

To learn more about passkey basics click here.

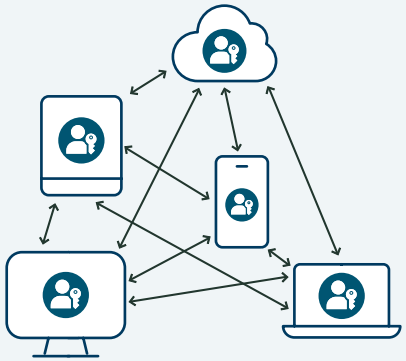

Figure 1: Synced passkeys – consumer grade

Types of passkeys—one is NOT for the Enterprise

There are two types of passkeys, synced and device-bound, the latter being hardware backed. Synced passkeys are shareable credentials that can travel across various devices such as smartphones, laptops, and tablets connected to a user account. These passkeys are universally accepted to be unsuitable for enterprises creating chilling failure points due to the higher potential for compromise.

By contrast, device-bound passkeys have a few variations themselves and are all enterprise-grade.

yubico

Considering passkeys for your enterprise

Follow proven best practices to stay consistently protected

Device-bound passkeys **on modern FIDO hardware security keys** offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach, organizations can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements and regulations. Setting up, or bootstrapping, any other type of device-bound passkey with a hardware security key ensures that the solution is stronger and more secure.

Device-bound passkeys can also be built-in **on modern everyday devices such as smartphones and laptops** and offer enterprises and their users an easy and convenient way to use passkey technology where passkeys stay local to their device. Some smartphone device-bound passkey solutions like Microsoft Authenticator (MA) may offer limited portability of its passkeys. This portability enables bootstrapping passkeys on other devices in some scenarios. However the whole lifecycle of how users create passkeys in the first place is critical. Creating device-bound passkeys initially backed by passwords or one-time passcodes, which is often the case for Microsoft Authenticator, creates downstream onboarding and recovery risks if MA is then used to bootstrap/set up passkeys on Windows Hello for Business. **And, what happens when a user loses their device?** Enterprise helpdesks typically have to temporarily downgrade user protection by using lesser, phishing-prone methods, as the user waits for a replacement smartphone or laptop.

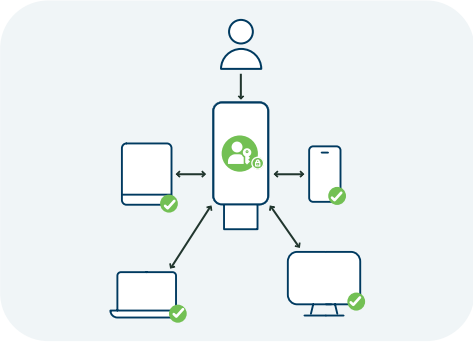

Figure 2: Passkeys stored in security keys like YubiKeys offer the strongest protection when used to bootstrap, or set up, local passkeys.

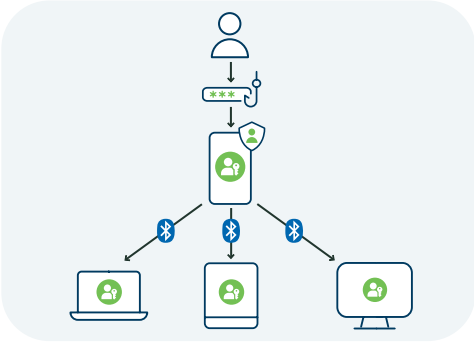

Figure 3: Setting MA up with a temporary access passcode (TAP), and then using it to set up Windows Hello for Business creates security exposure.

Think you have to pick one or the other? Think again.

Pairing built-in/local passkeys with portable hardware passkeys, such as those found on YubiKeys, protects users and the enterprise from modern cyber attacks and social engineering schemes to attack the helpdesk processes. Having a portable root of trust like a YubiKey offers the most robust portable passkey solution that works for the enterprise that not only supports stronger bootstrapping but also enables full enterprise coverage, so your users can remain productive and secure across all environments when devices are upgraded or even lost.

We recommend a proven best practice as you begin your journey

1. Put your credential on a portable device such as a YubiKey
2. Use the portable YubiKey to set up your local credential on Microsoft Authenticator or Windows Hello for Business.

Best Practice: Embrace a pragmatic rollout strategy

Yubico—pioneer of modern authentication and a leader in passkey innovation—advocates for organization-wide adoption of phishing-resistant, passwordless authentication. Information workers often present the most straightforward starting point. There's no need to delay securing this group while resolving edge-case complexities affecting IT administrators. Embrace a pragmatic rollout strategy—progress over perfection—and begin deploying secure credentials where feasible. Each user who authenticates with phishing-resistant credentials further minimizes your organization's attack surface. To do this effectively, Yubico advises mapping out your key user personas and determining the most suitable passkey method for each.

Identify your user personas

Context and user choice matter

When implementing phishing-resistant, passwordless authentication in your organization, it's helpful to take a user persona-based approach. Determine the user personas relevant for your organization. This step is critical to your project because different personas have different needs. Yubico recommends considering and evaluating the following key personas in your organization. In most cases, we recommend using passkeys on hardware security keys with other passkey types.

User Persona	Description
Information workers	**Examples include:** • Office productivity staff, such as in marketing, finance, or human resources. • Information workers such as executives and other high-sensitivity workers who need special controls • Users that have a 1:1 relationship with their mobile and computing devices; possibly bring their own devices (BYOD), especially for mobile
Frontline workers	**Examples include:** • Retail store workers, factory workers, manufacturing workers • Users typically work only on shared devices or kiosks; and may not be allowed to carry mobile phones
IT Pros/DevOps workers	**Examples include:** • IT admins for Active Directory, Microsoft Entra ID, Okta Workforce Identity Cloud or other privileged accounts. • DevOps workers or DevSecOps workers who manage and deploy software. • Users that have multiple user accounts, one unprivileged and one privileged for administrative access. • Commonly use remote access protocols, such as Virtual Private Network (VPN), Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH), to administer remote systems • May work on locked down devices with Bluetooth disabled
Workers in highly regulated environments	**Examples include:** • US federal government workers subject to Executive Order 14028 requirements • State and local government workers, or workers subject to specific security regulations • Users typically have a 1:1 relationship with their devices, but have specific regulatory controls that must be met on those devices and for authentication • Mobile phones may not be allowed in secure areas • May access air-gapped environments without internet connectivity • Users may work on locked down devices with Bluetooth disabled

Strengthen local passkeys with the portable YubiKey

Securing Microsoft Authenticator and Windows Hello for Business

YubiKeys can be used with Microsoft Authenticator or Windows Hello for Business to provide a secure, passwordless login experience. When the user starts with their credential on a YubiKey, and then bootstraps or sets up their Microsoft Authenticator or Windows Hello for Business credential, it allows for authentication never being downgraded. Or if a user's device is lost or compromised, the YubiKey enables fast and secure account recovery. It also offers greater security and efficiency in shared workstation environments.

How It Works:

Pre-Registration:
Enterprises can opt for pre-enrolled YubiKeys that are pre-programmed for a particular user to make user onboarding fast and easy–as easy as activating a credit card! We recommend getting a pre-enrolled YubiKey with Entra ID for fast tracking to phishing-resistance and passwordless.

Registration:
With their credentials on a YubiKey the user should use their portable YubiKey to authenticate and set up their workstations and smartphones with a new local passkey credential stored in either Windows Hello for Business or Microsoft Authenticator.

Authentication:
Once Windows Hello for Business is bootstrapped, the user can just log in with a PIN or biometrics on the Windows machine. The YubiKey then becomes the backup root of trust authentication device, or can be used to bootstrap and set up another device. For shared workstations, the YubiKey will need to be used for each login.

Enhanced Security:
By using a YubiKey, the IT helpdesk or the user never has to rely on temporary access codes or other phishable user authentication methods to enable access to their accounts while the user is waiting to replace their smartphone or laptop. During this time, downgrading of authentication leaves the user and the organization greatly exposed to bad actors. The physical possession of the YubiKey makes it nearly impossible for attackers to impersonate the user and start a damaging sequence of attacks in the organization.

Top Benefits:

- Stronger Security
- Consistent phishing-resistance
- Easier user onboarding
- Faster account recovery

Key Considerations:

Simplified user onboarding and fast track to passwordless:
Consider sending pre-registered YubiKeys to your users for a fast track to phishing-resistance and a move to passwordless. Yubico Enrollment Suite delivers a ground-breaking way.

Windows Hello for Business and Microsoft Authenticator setup:
Use a YubiKey to securely authenticate to Entra ID to bootstrap Windows Hello for Business and/or Microsoft Authenticator app.

Rapid account recovery with no downgrade to security:
Continue to use YubiKey for recovery scenarios, during device upgrades, and other user personas or business scenarios where a portable passkey is required.

YubiKey best practices:
We recommend having a primary and a spare YubiKey, just as you would a house or car key. This is in case your primary YubiKey is lost or damaged.

yubico

Passkeys done right: Top 5 Takeaways

YubiKeys strengthen every passkey and deliver user choice

Passkeys beat passwords —and setup is everything

Passkeys are more secure and easier to use than passwords, but how you create them matters. Passkeys backed by passwords or synced across devices are vulnerable to theft.

Hardware-backed passkeys close the gaps

YubiKeys store passkeys securely on hardware, delivering phishing-resistant, device-bound protection that is proven to stop attackers in their tracks.

Consistent protection—even when devices are lost

User onboarding and recovery create downstream risks.. Using YubiKeys eliminates the need for weak backup codes or helpdesk resets, ensuring security never gets downgraded—even during device loss or replacement.

Better together with built-in passkeys

YubiKeys complement passkeys on Windows Hello for Business, delivering convenience backed up with the durability and trust of the YubiKey to achieve cyber resilience and peace of mind.

The world's most trusted brands are already there

Global organizations like T-Mobile, Hyatt, Okta, Cloudflare and others rely on YubiKeys to deliver phishing-resistant protection at scale.

Yubico (Nasdaq 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 passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com

Contact us
yubi.co/contact