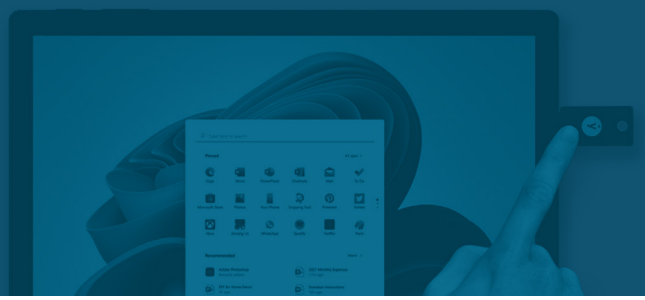
yubico | Microsoft



YubiKeys together with WHfB are your bridge to passwordless phishing-resistant MFA

Yubico and Microsoft are recognized as global leaders in cybersecurity and deliver solutions to provide passwordless phishing-resistant multi-factor authentication (MFA). Learn how Windows Hello for Business and YubiKeys work in concert to provide solutions for your organization and your customers.

What you need to know about Windows Hello for Business (WHfB)

Windows Hello for Business works well for:

- Strong phishing-resistant authentication for Windows
- An easy and user-friendly sign-on experience
- Hybrid and cloud-only environments when Entra ID (formerly known as Azure AD) is the primary identity provider
- Those using dedicated Windows workstations

YubiKeys extend phishing-resistant authentication use cases with:

- Authentication on all platforms like legacy and current Windows, macOS, Linux, iOS and Android or devices without TPM or Biometric support
- Shared or rotating workstations where re-registering WHfB on each workstation is not desirable or possible
- Account recovery workflows when WHfB is broken and also providing the ability to authenticate and remain productive when Windows device is lost or stolen
- Bootstrapping of WHfB on other devices with strong phishing-resistant authentication
- Customers with Bring your own device (BYOD) policies
- Where other alternate authentication methods are required for legacy and non-Entra ID federated apps or services. YubiKeys support many protocols like FIDO2, PIV, OATH, YubiOTP, OpenPGP which are supported by hundreds of enterprise services in our Works With YubiKey catalog
- Organizations with stricter security and compliance requirements

yubico | Microsoft

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

- 800-53 is mandatory for all US federal system to comply with and it is referenced in 800-171 (Government contractors guideline to control unclassified data), Cloud Controls Matrix (cyber framework for cloud computing)
- FIPS is also a requirement for all government agencies due to FISMA, and to be FEDRAMP high and FEDRAMP medium compliant. FIPS is also required as a part of 800-171, also in 800-63 (Digital identity guidelines)
- 800-53 rev 5 IA-2(6) Access to Accounts effectively states that a multi-factor authentication device must be separate from the system you are using

YubiKeys satisfy federal mandates

- 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 WHfB
- WHfB is only certified for use when the secret is stored on the Trusted Platform Module (TPM)
- WHfB is considered AAL3 only if the auditors agree that secrets on the TPM are the same as "separate cryptographic device"
- FIPS certification is achieved when you run both Entra ID and the endpoint in FIPS mode which means WHfB is not individually certified

	WHfB	YubiKey FIDO2	YubiKey PIV/CBA
Passwordless and Phishing-Resistant	✓	✓	✓
Supports Windows & Web Sign-in	✓	✓	✓
Supports Shared Workstations	*10 maximum users*	✓	✓
Supported with RDP	*Certificate trust only*	✓	✓
Portable to other devices	✗	✓	✓
Works on mobile	✗	*iOS/iPadOS Browser Only*	✓
Works on macOS and Linux	✗	✓	✓
Support other RPs	*only as FIDO2 platform*	*As multi-protocol key*	*As multi-protocol key*

CONTACT US
yubi.co/contact-us

FIND INTEGRATIONS
yubi.co/wwyk

LEARN MORE
yubi.co/msft-365-mfa

YUBICO IN THE AZURE MARKETPLACE
yubi.co/msftam

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy with phishing-resistant MFA. Yubico is setting global standards for secure access to computers, mobile devices, and more, and is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.