yubico

What's new in YubiKey 5.7
Product specifications

The new YubiKey 5.7 firmware fast-tracks enterprises to passwordless authentication with a secure, simple, and scalable solution that ensures the highest assurance authentication for modern enterprises.

Enterprise Attestation

Enterprise Attestation (EA) empowers identity providers to facilitate the retrieval of serial numbers from the YubiKey during FIDO2 registration with custom programmed keys, streamlining asset tracking requirements and account recovery processes by allowing end users to prove they have a specific FIDO2 device.

FIDO2 enhancements

YubiKey 5.7 implements Client-to-Authenticator Protocol (CTAP) 2.1, embracing the latest FIDO2 protocol features.

Force PIN Change supports FIDO Pre-reg and other enroll-on-behalf-of scenarios by ensuring temporary PINs set during FIDO2 enrollment are changed before the security key can be used.

Minimum PIN Length addresses PIN requirements for self-service enrollments by allowing organizations to enforce the minimum PIN Length set on YubiKeys.

These enhancements empower organizations to enforce compliance requirements and elevate security measures surrounding PIN usage.
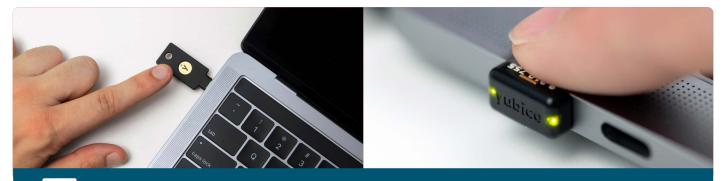
Expanded storage

YubiKey 5.7 expands storage capabilities for FIDO2 discoverable credentials and OATH one-time passwords, accommodating up to 100 passkeys, 24 PIV certificates, 64 OATH seeds, and 2 OTP seeds at once for a total of 190 credentials. This amplifies user authentication needs, providing ample space while maintaining robust security standards.

Smart Card/PIV enhancements

The PIV application undergoes significant improvements, now supporting larger RSA keys (RSA-3072 and RSA-4096), as well as Ed25519 and X25519 key types. This aligns with the August 2023 Department of Defense (DoD) memo requirements and offers advanced key management functions such as move and delete PIV keys, enhancing flexibility for organizations.

PIN complexity

Enterprises benefit from enhanced PIN complexity settings across all YubiKey applications, including FIDO2, PIV, and OpenPGP. By blocking simple patterns and common PINs at the hardware level, compliance with upcoming NIST requirements and corporate mandates is ensured.

YubiKeys deployed in:

9 of the top 10 global technology companies

4 of the top 10 U.S. banks

5 of the top 10 global retailers

YubiKey 5.7 firmware

YubiKey 5.7 firmware focuses on **fast-tracking enterprises to passwordless** authentication.

New capabilities	YubiKey 5 Series	Security Key Series	Security Key Series Enterprise Edition (Subscription-only)
PIN management flexibility			
Temporary FIDO2 PIN can be set (forces user to change upon next use)	✓	✓	✓
Configure FIDO2 minimum PIN Length	✓	✓	✓
Enhanced asset tracking			
Enterprise Attestation capable (requires custom configuration)	✓		✓
Serial number retrievable by client software in Windows without admin rights	✓ *Also applies to earlier firmware versions*		✓ *New in 5.7*
Enhanced Smart Card capabilities (PIV)			
RSA-3072 and RSA-4096 support	✓		
Ed25519 and X25519 support	✓		
Future proofed for compliance			
Enhanced PIN complexity	✓ *Requires custom config*		✓ *Enabled by default*
Configure FIDO2 minimum PIN Length	✓	✓	✓
Enhanced credential storage			
Support for 100 passkeys	✓	✓	✓
Support for 24 PIV certificates	✓		
Support for 64 OATH credentials	✓		
Support for 2 OTP seeds	✓		

Contact us
yubi.co/contact

Learn more
yubi.co/yk5