# Strong authentication for compliance

## Duo and Yubico together satisfy government guidance on DFARS/NIST SP 800-171, NIST SP 800-63-3 AAL3, and CMMC.

**Government employees and contractors are highly likely to be targeted by nation-states and cyber criminals. This necessitates impenetrable processes and technologies for establishing and using digital identities for secure access to government networks from a variety of user devices. Because identity proofing, authentication, authorization, and federation are key steps in securing user access, and involve the processing of user information, this can create huge privacy risks[1] if not appropriately executed.**

### Secure and compliant authentication, even across modern devices

Duo and Yubico are working closely together to simplify authentication, authorization and federation, and to ensure that government agencies stay protected against hackers and meet necessary compliance regulations such as NIST SP800-63B, DFARS/NIST SP 800-171 and CMMC. With Duo and the YubiKey, government agencies receive phishing resistant and federal compliant, strong hardware-backed authentication that is simple to deploy across multiple applications as well as modern devices, with single sign on (SSO) capabilities.

Duo's trusted access platform leverages the FIPS 140-2 validated, Department of Defense (DOD) approved YubiKey (Overall Level 2, Physical Security Level 3) to provide strong two-factor (2FA) and multi-factor authentication (MFA) so government employees and contractors can securely access data and applications on the network or in the cloud. Our combined, leading edge authentication technologies enable government agencies to meet the federal guidelines outlined in NIST SP 800-63-3 Authenticator Assurance Level 3—the highest level. Duo Access works with the YubiKey 5 FIPS Series as well as other YubiKey form factors.

**Bryan Rosensteel, Cybersecurity Architect, Public Sector, Duo Security:**

"The past few years have seen a focus from NIST, OMB, and the Federal Identity, Credential, and Access Management (FICAM) community on the importance of aligning strong authenticators with Dynamic Authentication solutions. OMB M-19-17, M-20-19, NIST SP 800-63-3, and NIST SP 800-207, all highlight and emphasize the importance of flexibility within the FICAM community to meet the challenges of today's diverse cloud and mobile environments. Together, Duo and Yubico build upon these Zero Trust core tenants to provide stronger, smarter authentication in an easy to use and extremely effective way; achieving the highest levels of assurance for trusted access."

[1] Digital Identity Guidelines, NIST SP 800-63-3

## Trusted security leaders

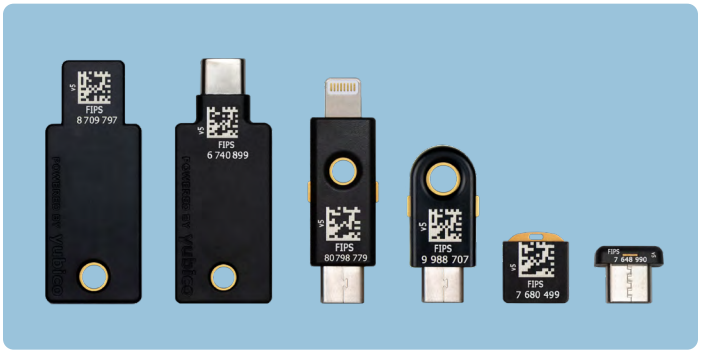
Duo and Yubico are proven leaders in security with the same tenacity and dedication to solving the authentication challenge. The world's largest enterprises and government agencies trust Duo and the YubiKey to protect their accounts, networks, and devices against unauthorized access. Both Duo and Yubico are FIDO Alliance members and are empowering government agencies to modernize to leading edge multi-factor authentication technologies like FIDO2/WebAuthn and FIDO U2F.

## Lowest Total Cost of Ownership

Deploying NIST-compliant, AAL3 2FA and MFA with Duo and the YubiKey 5 FIPS Series is a fast, simple, and inexpensive process, thanks to the joint solution's seamless compatibility with existing security infrastructures. Agency-wide deployment to thousands of users is attainable in a matter of days. The joint solution reduces IT operational costs by nearly eliminating help desk calls and end-user support tickets related to authentication.

**Jeff Phillips, VP of Public Sector, Yubico:**

"This federal partnership with Duo underscores our joint commitment to the highest-levels of data protection, as well as our responsibility as industry leaders to help government agencies protect the individuals they serve. We've made it our shared mission to advocate for easy to use security, and encourage the adoption of new open standards like FIDO2/WebAuthn to meet AAL3."



The YubiKey 5 FIPS Series is the first FIPS certified FIDO2/WebAuthn, multi-protocol, and NFC tap-and-go authenticator. From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS.

# Joint features and benefits

### High security

Duo and the YubiKey jointly offer a robust, highly-secure and federal-compliant authentication solution that has been tested and proven in the most security conscious government and enterprise environments.

### Multi-protocol flexibility

Duo works with the multi-protocol YubiKey 5 FIPS Series, ensuring a single solution across legacy and modern applications and devices, including mobile. Authentication protocols include FIDO2/WebAuthn, FIDO U2F, Yubico OTP, and HOTP.

### Broad compatibility

Duo and the YubiKey work across modern devices, and major browsers and operating systems, including but not limited to Windows, MacOS, Linux, Android and iOS, making deployment fast and simple.

**About Yubico** Yubico sets new global standards for simple and secure access to computers, servers, and internet accounts. Founded in 2007, Yubico is privately held, with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Discover why nine of the top 10 internet brands trust the YubiKey: yubico.com.

**About Duo** Duo helps defend organizations against breaches through its easy and effective cloud-based trusted access product suite. Duo verifies the identity of users, and the health of their devices, before granting them access to applications. Duo is trusted partner to thousands of companies worldwide. For more information, visit duo.com.