Centrify
ZERO TRUST PRIVILEGE

yubico

# Context-based Adaptive Authentication with Yubico and Centrify

The rise of cloud and mobile means that business employees are using more varied devices than ever to access an ever-growing number of cloud and on-premises apps as well as critical enterprise resources — each with their own username and password. With so many credentials to remember, employees resort to re-using simple passwords across apps, devices, and infrastructure which makes it easy for hackers to guess or steal credentials. Centrify and Yubico provide a frictionless security solution that eliminates passwords, bolsters security, and provides secure access to apps, devices, and critical IT resources.

## The New Threatscape

The easiest way for a cyber-attacker to gain access to sensitive data is by compromising an end user's identity. Equipped with the right credentials, cyber adversaries and malicious insiders can wreak havoc on an organization's network, exfiltrate sensitive data, or even siphon off funds — all while concealing their malicious activities from threat detection solutions.

Things get even worse if a stolen identity belongs to a privileged user who has even broader access, and which provides the intruder with "the keys to the kingdom". In fact, 80 percent of security breaches involve privileged credentials, according to Forrester Research. In addition, 65% of enterprises allow for the unrestricted, unmonitored, and shared use of privileged accounts, according to Gartner.

These findings only scratch the surface of how privileged credentials can be exploited and the damage they can cause in the wrong hands. That's where multi-factor authentication (MFA) comes into play, as it reduces the risk of compromised credentials. However, MFA is often too cumbersome for end users, or — in the case of smart cards — requires dedicated readers on all end-user devices.

## Centrify and Yubico Protect You from Hackers Compromising Your Credentials

With password theft rampant, and headline-level breaches a near-daily event, multi-factor authentication has become critical for every business. Yubico and Centrify have partnered to provide simple, context-based, adaptive authentication across privileged users and enterprise resources.

Whether it's for PIV-based authentication, OATH one-time passwords, or as a physical NFC token for mobile devices — Centrify and Yubico provide IT the flexibility to enforce security without user frustration.

Centrify Zero Trust Privilege provides the policy layer that lets IT create adaptive rulesets to integrate MFA into servers, IaaS, and more. And thanks to the simplicity, portability, and flexibility of YubiKeys, users always have a secure second factor that works across devices.

This integration means IT has the flexibility to provide simple multi-factor authentication no matter what their authentication requirements. The Centrify Zero Trust Privilege solution leverages multiple capabilities in the YubiKey — PIV, OATH OTP, or physical NFC token — for secure adaptive authentication without hassles. Centrify can leverage the YubiKey for use cases such as:

- Smart card Active Directory-based login to Linux
- Re-authentication for privilege escalation on Windows
- Smart card login for secure remote access
- YubiKey as OATH H/TOTP for MFA to servers for privileged access session control

## How Does It Work?

A login can be as simple as plugging the YubiKey into your device and typing a PIN (smart card login) to gain access to a critical enterprise resource. In other cases, users may make use of NFC merely touch the YubiKey against their mobile device for quick and easy authentication to servers and more. Enrollment is streamlined, and policy is created simply and enforced across all business users.

## Centrify and Yubico Support FIDO U2F

The partnership between Yubico and Centrify, both members of the Fast IDentity Online Alliance (FIDO), further accelerates the adoption of multi-factor authentication. Using the specially designed YubiKey 4 Security Key by Yubico with Centrify's support for the FIDO Alliance's Universal 2nd Factor (U2F) specification, the Centrify Zero Trust Privilege solution provides the broadest support for various use cases across platforms. This includes:

- FIDO U2F within the Centrify Zero Trust Privilege solution
- OATH-HOTP for secure SSO to servers
- Smart card PIV re-authentication for Windows privilege escalation
- Active Directory-based login to a variety of operating system platforms to meet NIST regulations

By extending its current authentication methods, Centrify gives enterprises the option of using devices that comply with the FIDO U2F requirement as well as meet NIST 800-63b strongest Authentication Assurance Level 3 requirements when combined with the privileged user's password.

Advantages of FIDO U2F include:

- Heightened security - public key cryptography protects against phishing, session hijacking and malware attacks
- Increased ease of use - no codes to re-type and no drivers to install
- Higher privacy - no personal information is associated with a key
- Scalable usage - unlimited number of accounts can be protected by one single device

## More About the YubiKey 4 Series

With a simple touch, the YubiKey protects access to computers, networks, and online services. Touch to trigger FIDO U2F, smart card (PIV), Yubico OTP, Code Signing, OpenPGP, OATH-TOTP, OATH- HOTP, and Challenge-Response.

Each security key has an individualized secure chip which performs cryptographic functions triggered by a simple touch of the key. You never see the details, but behind the scenes a FIDO U2F security key provides a unique public and private key pair for each access request it protects. Only those keys can correctly complete the cryptographic challenge required for login.

**Benefits**

- Use multi-factor authentication everywhere
- Protect sensitive commands and servers with MFA
- Easy to implement using existing Active Directory
- Strong two-factor hardware-based authentication
- Easy and fast authentication with a single touch
- Reduces IT operational costs
- Multiprotocol support on a single key
- Crush-resistant and waterproof
- Choice of USB-A and USB-C form factors

### Benefits

- Simplify Security: One platform secures all your users, and one YubiKey enables MFA across all critical enterprise resources (e.g., servers)
- Speed Adoption: Users get secure access to enterprise resources they need, from the devices they choose — without training or confusion
- Meet Regulations: Comply with NIST regulations requiring smart card authentication

**Features**

- Supported protocols: FIDO U2F, smart card (PIV), Yubico OTP, OpenPGP, OATH-TOTP, OATH-HOTP, and Challenge-Response
- Secure element hardware to protect cryptographic keys
- Crypto Algorithms: RSA 2048, ECC p256, ECC p384
- Interface: USB-A and USB-C
- Works on Microsoft Windows, Mac OS X, Linux, Chrome OS operating systems, and on major browsers
- PIV smart card compatible, mini-driver available on Windows

2,000+ customers, including over half of the Fortune 100, rely on Centrify Zero Trust Privilege.



US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com

Centrify
ZERO TRUST PRIVILEGE