PingID and YubiKey

ADDITIONAL SECURITY FOR OUT-OF-BAND AUTHENTICATION

PARTNER SOLUTION BRIEF

Introduction

Relying solely on username and password for security puts enterprise data at risk. Catastrophic security breaches top world headlines every day, and for good reason. A single corporate security breach costs an average of $3.86 million,[1] and 81% of breaches are caused by stolen or weak passwords.[2]

As a result, IT organizations can't rely exclusively on passwords to protect access to corporate data. They have to adopt stronger employee and vendor authentication—or risk becoming the next target.

> "Strong multi-factor authentication is one of the core components of an enterprise IAM strategy."
>
> \- Forrester

A modern multi-factor authentication (MFA) solution ensures your users are who they say they are. Requiring users to authenticate via multiple factors, such as a username/password along with a one-time password (OTP) delivered via a hard token, allows your organization to apply the correct levels of security based on associated risk, strengthening your security posture.

PingID and YubiKey together comprise a modern MFA solution, enabling your users to access the resources they need, seamlessly and securely.

[1] *"2018 Cost of Data Breach Study," Ponemon Institute Research Report,* https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[2] *"2017 Data Breach Investigations Report 10th Edition," Verizon,* http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

MFA Everywhere

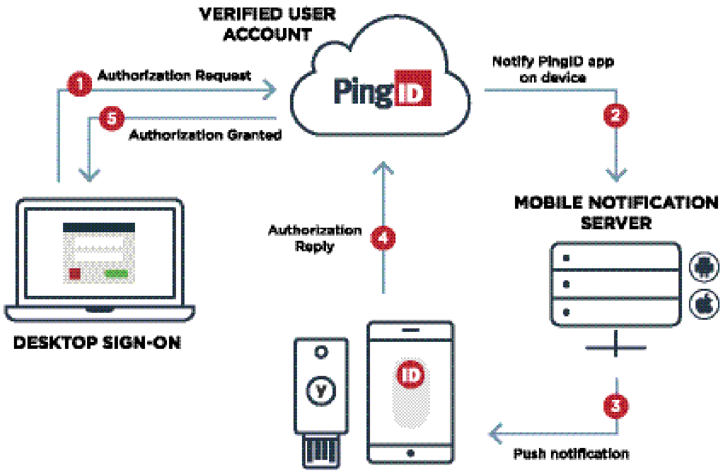
PingID is an identity-as-a-service (IDaaS), adaptive multi-factor authentication solution. It balances secure access to applications with ease of use for the end user, while allowing enterprises to define and enforce authentication policies that are tailored to their needs. With PingID, users can add and select from multiple authentication methods and devices on the fly—ultimately reducing support calls.

PingID provides support for all of your enterprise use cases, giving you the freedom to put MFA everywhere it is needed for your employees, partners and customers.

Adaptive Authentication Support

Administrators can define advanced authentication, pairing and device posture policies, like:

- Limiting MFA to specific groups, IP addresses or applications.
- Employing geo-fencing to skip MFA requirement if trusted device is within a "secure" area.
- Restricting devices that are rooted or jailbroken through root detection.
- Defining sessions that allow users to avoid prompt for MFA if authenticated within a predefined amount of time (hours, minutes, days, etc.).



Implementation Options for MFA

In sensitive environments or for users without mobile device or phone access, a YubiKey hard token used as a second factor can help you deliver the security your organization needs.

By combining PingID and YubiKey, an enterprise gives their users an additional, secure form factor for out-of-band authentication. The YubiKey hardware gives your enterprise a variety of form factors to allow the user to authenticate combined with the contextual awareness of PingID.

A YubiKey hardware authenticator can be used in sensitive environments or for users without device or phone access. Examples of environments where phone or device access is limited:

- Call centers
- Hospitals
- Financial (e.g., stock exchanges)
- Federal buildings
- Industrial control centers

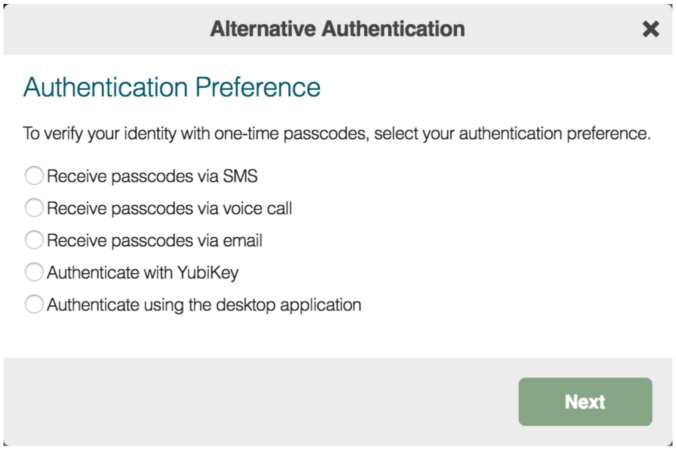
PingID App for Employees and Partners

Setting Up the PingID Mobile App

When an administrator enables the PingID App, the user is prompted to walk through a self-registration process to register their device. First, they install the PingID App on their Apple or Android phone or tablet. Next, they scan a QR code to pair their device. Once registered, the PingID App is ready for use.

PingID
Finish pairing PingID
PingID

If the user does not have an Apple or Android device, they can elect to authenticate using one-time passwords (OTPs) that are sent via SMS, voice call or email. Alternatively, they can use a YubiKey with the Windows or Mac desktop applications.



Alternative Authentication

Authentication Preference

To verify your identity with one-time passcodes, select your authentication preference.

○ Receive passcodes via SMS
○ Receive passcodes via voice call
○ Receive passcodes via email
○ Authenticate with YubiKey
○ Authenticate using the desktop application

The PingID service adds adaptive multi-factor authentication to PingOne®, PingFederate®, PingAccess®, third-party applications, Secure Shell (SSH) applications, Windows Login/RDP or any RADIUS compliant VPN server or remote access system.

Authenticating with PingID

When policy dictates the need for strong authentication, the PingID service will send a notification to the user's smartphone through the PingID App. On iOS and Android devices, this is sent via the Apple or Android notification service, eliminating the expense of sending an SMS or voice call. The notification prompts the user to swipe in the device's PingID App to be authenticated. The PingID App also includes native Apple Watch support. In the event a user is unable to get a signal to their mobile phone, an offline mode is available where the PingID App generates an OTP. Alternately, the OTP can be delivered via SMS, voice, email or desktop application. The registration and authentication process is localized and branded. Users can also self-manage their trusted authentication devices.

LOGIN
username
password
SIGN IN
ID
y
Authenticated
Settings
Authenticated
YOU'RE DONE!

Fingerprint as an Authentication Factor

For the ultimate in convenience, the PingID App can be configured to use the fingerprint reader on the registered device. After the notification is sent to the phone through the PingID App, the user will simply touch the fingerprint reader for authentication. This is an optional feature that works with Apple's Touch ID and select Android devices.

YubiKey: The Key to strong Enterprise Authentication

Get proven, strong multi-factor authentication that's easy to use and reduces IT costs—all from the trusted leader in modern enterprise authentication.

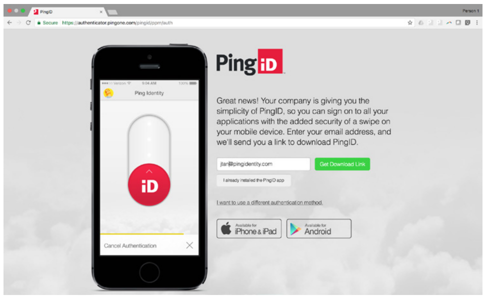
Account takeover prevention and phishing defense for secure enterprise authentication
The YubiKey stores the authentication secret on a secure element hardware chip. This secret is never transmitted and therefore cannot be copied or stolen.

Reduces IT costs
The YubiKey dramatically reduces the number one IT support cost—password resets—which costs Microsoft over $12 million per month.[3] By switching from mobile OTPs to YubiKeys, Google reduced password-support incidents by 92% because YubiKeys are more reliable, faster and easier to use.

Easy to use, fast and reliable
The YubiKey 5 Series is the industry-leading multi-protocol security key, supporting FIDO2/WebAuthn, FIDO U2F, one-time password (OTP), OpenPGP and smart card. The YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5C, and YubiKey 5Ci conveniently fit on a keyring, while the YubiKey 5 Nano and YubiKey 5C Nano are designed to remain in the USB port. This ensures that every YubiKey is easy to access and provides the same level of digital security.

Setting Up the YubiKey

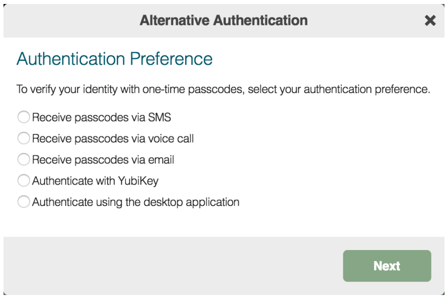
Users don't need to install anything—customers or employees simply register their own YubiKey, and then pair it with their PingID account. Pairing creates a trust between the YubiKey and your account, so you can use the YubiKey to authenticate during the login process.


PingID
Person 1
Secure https://authenticator.pingone.com/pingid/ppm/auth
Ping Identity
Cancel Authentication
PingiD

Great news! Your company is giving you the simplicity of PingID, so you can sign on to all your applications with the added security of a swipe on your mobile device. Enter your email address, and we'll send you a link to download PingID.

jtan@pingidentity.com

Get Download Link
I already installed the PingID app
I want to use a different authentication method.
Available for iPhone & iPad
Available for Android

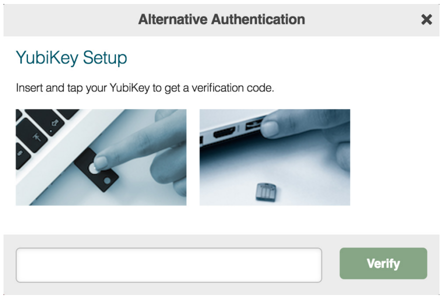


Alternative Authentication

Authentication Preference

To verify your identity with one-time passcodes, select your authentication preference.

○ Receive passcodes via SMS
○ Receive passcodes via voice call
○ Receive passcodes via email
○ Authenticate with YubiKey
○ Authenticate using the desktop application

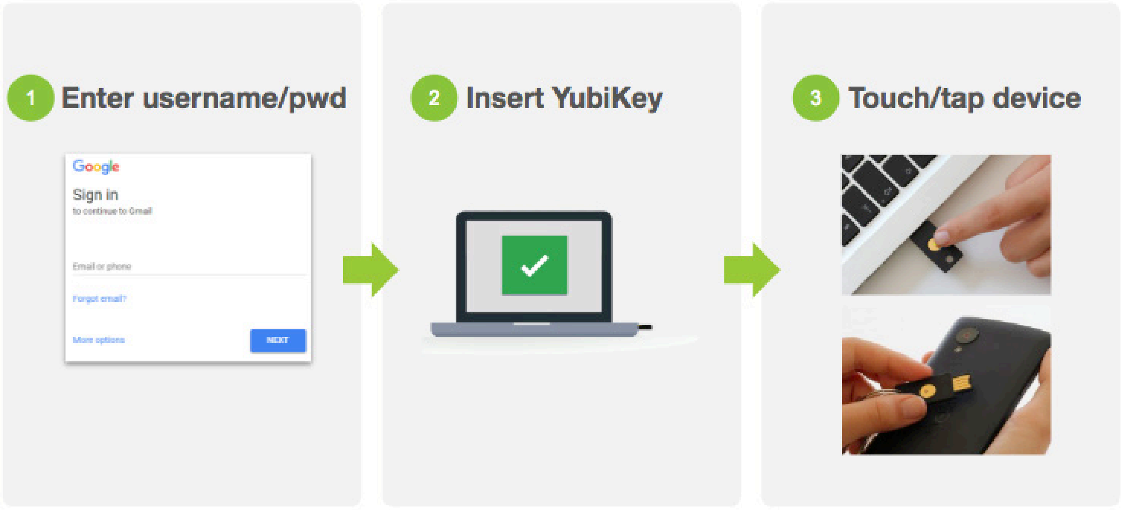


Alternative Authentication

YubiKey Setup

Insert and tap your YubiKey to get a verification code.

Authenticating with YubiKey



Conclusion

The enterprise environment is changing rapidly, increasingly requiring organizations to support the access needs of mobile employees, partners and customers. These users need flexibility in how to authenticate. In these times of digital transformation, you can't afford to overlook any available tool in your security toolkit. PingID and YubiKey together give you an additional option for enforcing access policies for users that need strong out-of-band authentication, helping ensure your organization achieves the security it needs.

For more information about how Ping Identity and Yubico joint solutions can help your business, please contact us.

About Yubico

Yubico sets new global standards for easy 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. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

About Ping Identity

Ping Identity envisions a digital world powered by identity. As the identity security company, we simplify how the world's largest organizations prevent security breaches, increase employee and partner productivity and provide personalized customer experiences. Enterprises choose Ping for our identity expertise, open standards leadership, partnership with companies like Microsoft, Amazon and Google, and collaboration with customers like Boeing, Cisco, GE, Kraft Foods, Walgreens and over half of the Fortune 100. The Ping Identity Platform allows enterprises and their users to securely access cloud, mobile and on-premises applications while managing identity and profile data at scale. Architects and developers have flexible options to enhance and extend their existing applications and environments with multi-factor authentication, single sign-on, access management, API security, directory and data governance capabilities. Visit www.pingidentity.com.

Ping Identity is the identity security company. We simplify how the world's largest organizations, including over half of the Fortune 100, prevent security breaches, increase employee and partner productivity and provide personalized customer experiences. With Ping, enterprises can securely connect users to cloud, mobile and on-premises applications while managing identity and profile data at scale.