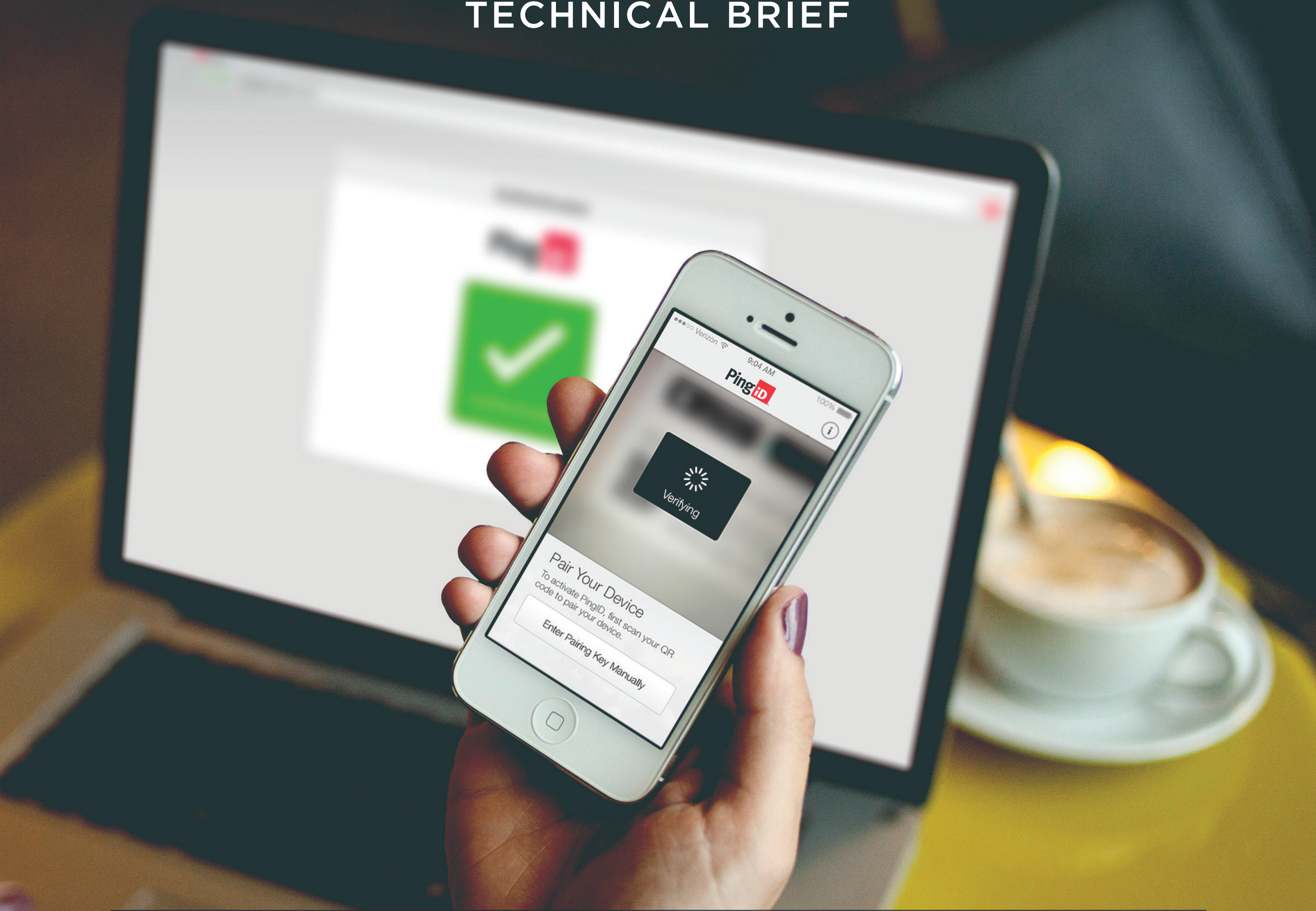
Ping Identity

PingID

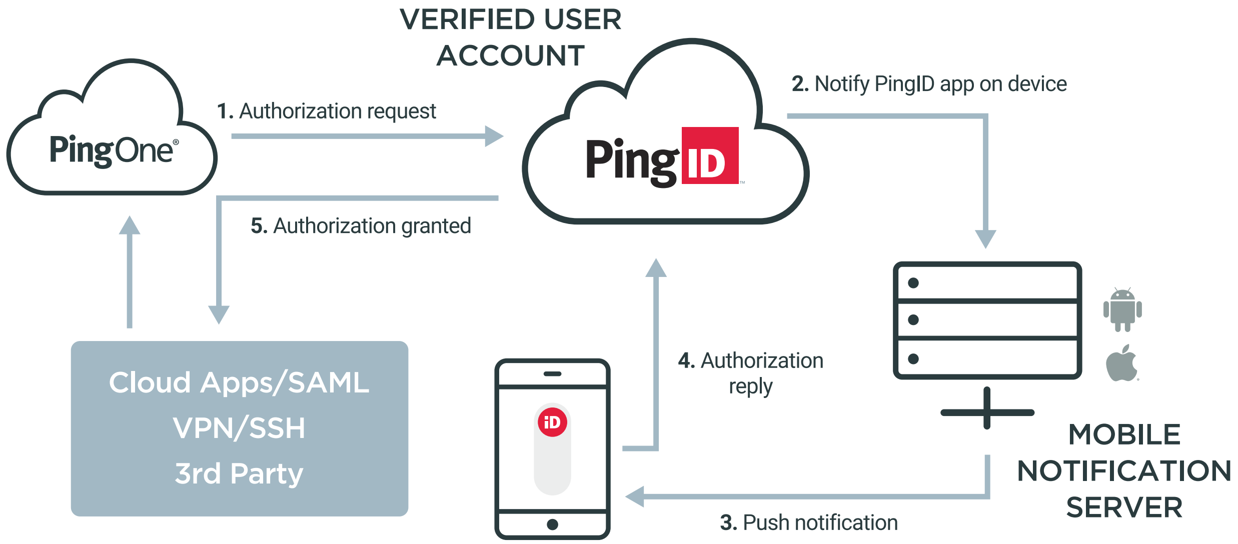
TECHNICAL BRIEF



Verizon
9:04 AM
100%
PingiD
Verifying
Pair Your Device
To activate PingID, first scan your QR code to pair your device.
Enter Pairing Key Manually

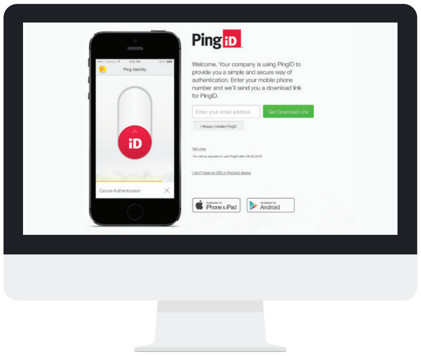
PingID is a multi-factor authentication (MFA) solution delivered through the PingOne platform. PingID provides multi-factor authentication for cloud-based applications, on-premises applications, VPNs Windows Servers and RDP, and Secure Shell (SSH). The PingID service is administered via an admin console hosted in PingOne.

For the most common use case, end users install an app on their Apple or Android smartphone or tablet that provides the "something your have" required for strong authentication. When users are required to authenticate, a notification is sent to the device, and users simply swipe the app to sign on. The PingID app also provides secure one-time passwords (OTPs) for fallback or offline use. PingID provides a simple and unobtrusive mechanism for users that delivers the security that IT requires.



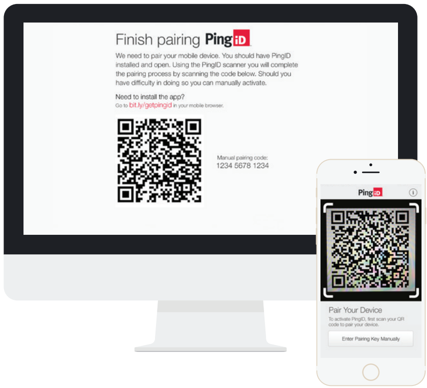
Registration

Once enabled, users are prompted to install the PingID app on their phone or tablet during the next authentication event. A self-service workflow guides the user through registering with PingID, although it's possible to pre-register users if required. Registering with the mobile app is a simple process where users scan a QR code with the camera on their device. Users that are unable to use an iOS or Android device can choose to authenticate with OTP sent via voice call, SMS, email or to the PingID Windows or Mac desktop application. In addition, users can authenticate via a Yubikey hard token device.


PingID

Welcome. Your company is using PingID to provide you a simple and secure way of authentication. Enter your mobile phone number and we'll send you a download link for PingID.

You will be required to use PingID after 08.29.2016


Finish pairing PingID

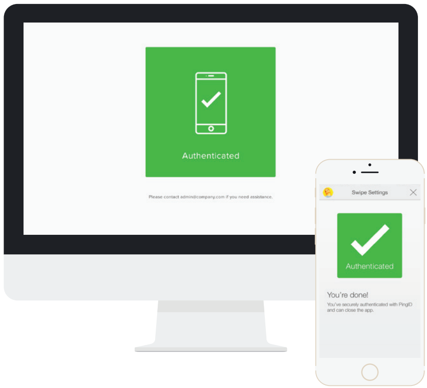
We need to pair your mobile device. You should have PingID installed and open. Using the PingID scanner you will complete the pairing process by scanning the code below. Should you have difficulty in doing so you can manually activate.

Need to install the app?
Go to bit.ly/getpingid in your mobile browser.

Manual pairing code:
1234 5678 1234

Pair Your Device

To activate PingID, first scan your QR code to pair your device.


Authenticated

Please contact admin@company.com if you need assistance.

Swipe Settings

Authenticated

You're done!

You've securely authenticated with PingID and can close the app.

Hard Token Support

PingID supports the YubiKey hard token from Yubico. A YubiKey is a small device that is registered with PingID and provides OTPs for MFA. Instead of swiping the app or typing an OTP, the user plugs the YubiKey into the USB port of their computer and presses the button on the YubiKey, which automatically enters an OTP. No drivers are required for YubiKeys since they appear as a custom keyboard device to the computer. YubiKeys can be ordered from Yubico or from Amazon stores worldwide.

Authentication Methods

- Swipe by PingID app
- Fingerprint scan by PingID app (Apple and Samsung devices)
- Apple Watch tap
- OTP delivered by PingID app
- OTP delivered by SMS, voice or email
- OTP delivered by a Windows or Mac desktop application
- OTP from a YubiKey hard token

Supported Platforms

The PingID app works on Apple and Android tablets and phones. Supported platforms are Android 2.2 or later and Apple iOS 5.1.1 or later. Delivery of an OTP via SMS, voice or email is available for users without smartphones or tablets. YubiKey integration is available for any computer that supports USB keyboards.

PLATFORM	MOBILE APP	OTP SOFT TOKEN	SMS/VOICE OTP	EMAIL OTP	YUBIKEY
Apple iOS	✓	✓	✓	✓	✗
Android	✓	✓	✓	✓	✗
Windows Phone	✗	✗	✓	✓	✗
Blackberry	✗	✗	✓	✓	✗
Mac OS X	✗	✗	✗	✓	✓
Windows	✗	✗	✗	✓	✓

Supported Services

- SSO by PingFederate
- SSO by PingOne
- SSO by PingOne native app
- VPN and remote access systems using the RADIUS protocol
- SSH and local login for Unix systems
- Windows server and RDP login

Password Replacement

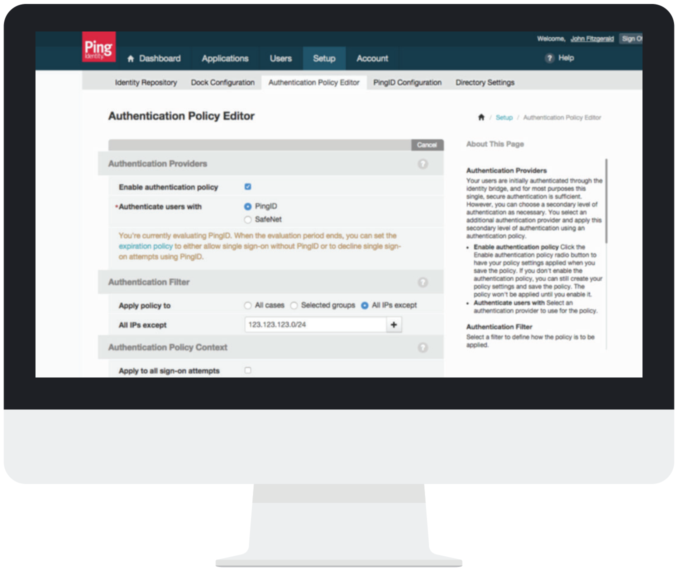
PingID can be used as the primary factor of authentication when the PingID service is integrated with PingFederate. The PingFederate adapter selectors can be used to create simple or complex authentication scenarios, including using PingID as the only form of authentication.

How is PingID administered and configured?

PingID is administered via a web-based administration console hosted in PingOne.

How does a user set up PingID?

- Users are prompted to install the PingID app on their phone or tablet during the first authentication event that requires MFA.
- The user chooses from the available authentication methods (PingID app, SMS, voice, email or YubiKey).
- The app enrollment screen includes links to both Apple and Google mobile markets.
- The enrollment web page also provides the ability to send an email to the user which includes the links to the apps.



Authentication Policy Editor

Authentication Providers

Enable authentication policy ☑

*Authenticate users with ● PingID ○ SafeNet

You're currently evaluating PingID. When the evaluation period ends, you can set the expiration policy to either allow single sign-on without PingID or to decline single sign-on attempts using PingID.

Authentication Filter

Apply policy to ○ All cases ○ Selected groups ● All IPs except

All IPs except 123.123.123.0/24 +

Authentication Policy Context

Apply to all sign-on attempts □

About This Page

Authentication Providers

Your users are initially authenticated through the identity bridge, and for most purposes this single, secure authentication is sufficient. However, you can choose a secondary level of authentication as necessary. You select an additional authentication provider and apply this secondary level of authentication using an authentication policy.

- **Enable authentication policy** Click the Enable authentication policy radio button to have your policy settings applied when you save the policy. If you don't enable the authentication policy, you can still create your policy settings and save the policy. The policy won't be applied until you enable it.
- **Authenticate users with** Select an authentication provider to use for the policy.

Authentication Filter

Select a filter to define how the policy is to be applied.

What types of authentication policies does PingID support?

PingID supports standard policies that limit MFA to selected groups, ip addresses or specific applications. In addition, Administrators can define more advanced authentication, pairing and device posture policies, including:

- Geo-fencing allows users to avoid prompt for MFA is inside a “secure” area
- Root detection allows users to avoid prompt for MFA if their device is rooted/jailbroken
- MFA session allows users to avoid prompt for MFA if user was authenticated within last X minutes

Can the user change devices?

Yes, users have a self-service option to change to a new device. This is available in the PingID app.

What if the user does not have network access?

If the user does not have access to a data network to receive the push notification, an OTP can be used instead. This functionality is included with the PingID app. Additionally, the OTP feature supports voice calls, email or the PingID desktop application for Windows or Mac.

What about users who may not have mobile phones at all?

YubiKey support is available to provide a strong authentication option for users that do not have a mobile phone or do not have access to a data network. Additionally, the OTP feature supports voice which can route to a hard line as well as email.

Where does the PingID service run?

PingID is delivered as a cloud service by Ping Identity. Details about the security of the service can be found here.

What VPN and remote access systems does PingID support?

PingID works with VPN and remote access systems from Cisco, Juniper, Checkpoint, Fortinet, Citrix, CyberArk, Dell SonicWall, F5, Palo Alto and Microsoft UAG, among others. Contact us to see if your specific model or version is supported.

How does PingID VPN support work?

The PingID RADIUS validator is installed on the PingFederate server and is configured to communicate with the VPN server via RADIUS. The validator has a local administration page for various configurations (e.g., LDAP groups which work with PingID). Users are managed via the administration console at PingOne.

How is the PingID server protocol secured?

The PingID app communicates with the PingID service via REST over HTTPS. The communication is further secured through HMAC-SHA1 signed messages that include the session ID, the device fingerprint and the device ID.

Is PingID using the OATH standard for OTP generation?

Yes, the OTP generated by the PingID app is an HOTP (HMAC-based OTP).