Ping Identity

DATASHEET

SAMSUNG
Ping ID
10:03 AM
Verifying
Pair Your Device
To activate PingID, first scan your QR code to pair your device.
Enter Pairing Key Manually

PingID

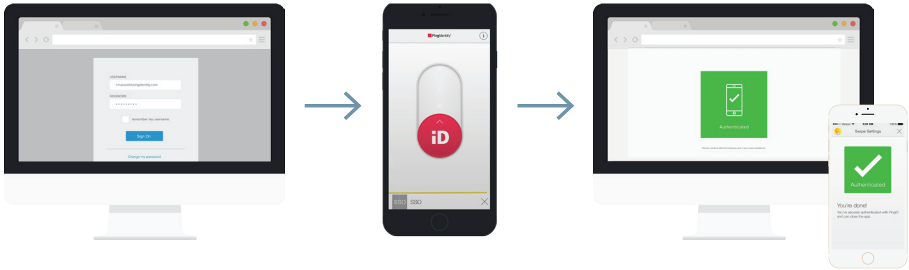
PingID® is an IDaaS, adaptive multi-factor authentication (MFA) solution. It balances secure access to applications with ease of use for the end user, while allowing enterprises to define and enforce authentication policies that are tailored to their needs.

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

IMPLEMENTATION OPTIONS FOR MFA

Ping offers two implementation options for MFA: the PingID App and PingID SDK. The PingID App is a standalone mobile application for Apple and Android devices. It’s most often used for employee and partner use cases, and is fully managed by Ping Identity. The PingID SDK allows you to embed multi-factor authentication capabilities right into your own mobile application. Primarily intended for customer use cases, it supports Apple and Android mobile apps.

PINGID APP FOR EMPLOYEES & PARTNERS



FINGERPRINT AS A SECOND 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.

HOW IT WORKS

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. 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 utilize a Yubikey hard token or the Windows or Mac desktop applications. 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.

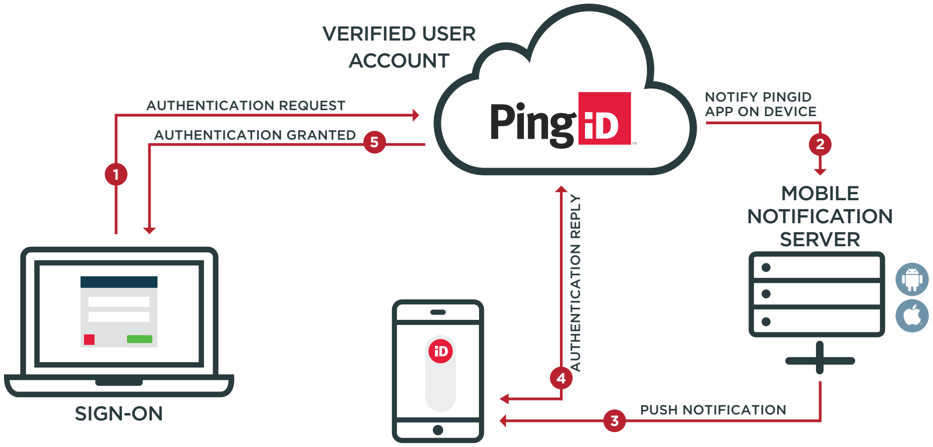
SECURITY BALANCED WITH CONVENIENCE

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. Finally, a YubiKey hard token can also be used in sensitive environments or for users without device or phone access. The registration and authentication process is localized and branded. Users can also self-manage their trusted authentication devices.

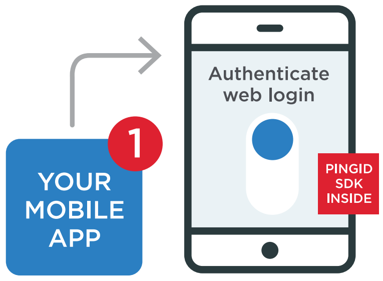
ADAPTIVE AUTHENTICATION SUPPORT

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

- 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.).



PINGID SDK FOR CUSTOMERS



HOW IT WORKS

PingID has a mobile SDK for Apple and Android that enables you to embed multi-factor authentication capabilities natively into your own mobile application. This allows you to deliver convenient and secure MFA to your customers, without requiring them to download a separate application.

ENHANCE EXISTING AUTHENTICATION WORKFLOWS

The PingID SDK can send push notifications to request a second authentication factor during web, mobile web, call center, face-to-face, high-value transactions or any other customer interaction. Additional device-based authorization can also enhance security during mobile app authentications. The security PingID SDK adds through your native mobile app is a benefit you can promote to customers to drive mobile app adoption. The PingID SDK augments your existing authentication workflow. Customers who have your app benefit from additional MFA security. Customers who don't aren't required to download it and can instead utilize your existing authentication process.

OUT-OF-BAND WEB AUTHENTICATION

PingID SDK allows you to require approval from a customer-defined, trusted device when a customer attempts to log in to a web application. You also have the option to achieve passwordless authentication by requiring customers to enter only their username and allowing PingID SDK's MFA capabilities to replace their password.

TRANSACTION APPROVALS

You can require strong, out-of-band authentication for high-value transactions. These transactions may include transferring funds, making purchases, updating account information and more. Transaction details can also be sent to the customer's trusted device so they know exactly what they're approving. Selectively requiring MFA to approve high-value transactions allows you to mitigate a significant amount of security risk with little effect on customer experience.

TRUSTED DEVICE AUTHENTICATION

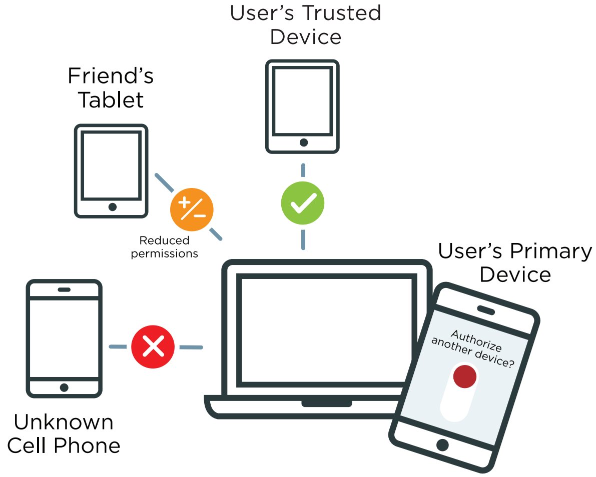
Mobile app authentication can be strengthened by ensuring that customers are authenticating from a trusted device. This ensures a user-friendly, secure mobile app login experience for customers, while preventing hackers from using stolen credentials to authenticate from apps on untrusted devices.

CUSTOMER-MANAGED NETWORK OF TRUSTED DEVICES

PingID SDK enables your customers to self-manage their own network of trusted devices. Initially, customers can add a primary trusted device by simply authenticating from your mobile application and utilizing behind the scenes pairing. They can also add a trusted device manually through an authorization code delivered by a secure process that you define. From their primary device, customers can add other trusted devices, change their primary device and add devices with reduced permissions. PingID SDK's APIs allow you to build interfaces into web or mobile applications for customers to self-manage their trusted device networks.

EASY-TO-USE ADMINISTRATIVE PORTAL

From a single, user-friendly interface, you can set up and manage new applications that utilize PingID's mobile SDK, manage users, and run transaction and user reports. A single PingID SDK tenant can be utilized for multiple mobile applications and managed from an easy-to-use administrative portal.



COMPARE THE PINGID APP & THE PINGID SDK

	PingID App	PingID SDK
Primary Use Case	Employees & Partners	Customers
Implementation	Standalone Ping Identity MFA Mobile App	Custom iPhone / Android SDK Embedded in Your Own Mobile Application
User-managed Network of Trusted Devices	Yes	Yes
Transaction Approvals	No	Yes
Branding/Customization	Customization Options	Complete Customization
Trusted Device Authentication	Yes	Yes
Reduced Permission Devices	No	Yes
Service APIs	Public Web APIs	Server: Public REST APIs Mobile: Mobile SDK APIs
SMS, Voice, Email, Desktop and YubiKey Alternatives to Mobile App Authentication	Yes	No
Enterprise Application Integrations	Yes	No
Out-of-the-box Registration and Authentication Flows	Yes	Sample App

To learn more about PingID, visit pingidentity.com.

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, Disney, 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, directory and data governance capabilities.