PingID® is a cloud-based, adaptive multi-factor authentication (MFA) solution that balances secure access to applications with ease of use for employees and partners while allowing businesses to define and enforce authentication policies that are tailored to their needs.

PingID provides organizations with a fast and easy way to deploy MFA for a wide range of use cases without draining IT resources. From protecting workforce apps accessed via PingFederate or PingOne for Enterprise single sign-on solutions, to integrating seamlessly with VPNs, Microsoft Azure AD, Active Directory Federation Services (AD FS), Windows Login or Mac login—PingID has you covered.

PingID comes with multiple implementation options, including the PingID mobile application for Apple and Android devices, which is fully managed by Ping Identity, the PingID desktop app and PingID APIs. PingID supports a wide range of authentication methods, can integrate in minutes, and is versatile enough to secure all your applications and services regardless of where they’re hosted.
Put MFA Where Your Enterprise Needs It

When an administrator enables PingID, the user is prompted to walk through a self-registration process to register their first authentication device. First, they install the PingID mobile app on their Apple or Android phone or tablet. Next, they scan a QR code to pair their device. Once registered, PingID is ready for use. If the user does not have an Apple or Android device, they can elect to authenticate using one-time passcodes (OTPs) that are sent via SMS, voice 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, Mac Login or any RADIUS-compliant VPN server or remote access system, as well as on shared devices like kiosks and shared tablets.

Plus, PingID’s integrations with Microsoft Azure AD and Active Directory Federation Services (AD FS) enable it to provide convenience and security for hybrid IT environments that utilize a mix of on-premises, private cloud and SaaS applications, including non-Microsoft resources. PingID makes leveraging Office 365 and Azure AD easier, more secure and more productive for your enterprise. Whether your user’s journey starts with authenticating via on-premises Active Directory or cloud-based Azure Active Directory, the user experience is the same: seamless, secure access to all applications, regardless of where they reside. When a user changes roles, PingID will apply authentication policies according to the new role and the accessed applications. When users leave the organization, PingID provides automated de-provisioning capabilities to disable and delete users from the service.

Features & Benefits

- Cloud-based MFA service
- MFA for web apps, VPN, SSH, Windows login, Mac login, RDP, AD FS and Azure AD
- Adaptive and risk-based authentication policies to balance security and productivity
- Employee self-service for enrollment and device management
- PingID customized with your brand
- Available in North America, Europe and Australia data centers

Supported Authentication Methods

- PingID Mobile App
  - Fingerprint
  - Facial Recognition
  - Swipe
  - Mobile Soft Token
  - Apple Watch
- FIDO2 Biometrics
- Security Key
- Desktop Soft Token
- Authentication App
- OATH Token
- YubiKey - Yubico OTP
- Email
- SMS OTP
- Voice OTP
Balance Security & Productivity

When policy dictates the need for strong authentication, the PingID service will send a notification to the user’s smartphone through the PingID mobile 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 mobile app to be authenticated. PingID also includes native Apple Watch and iPad support. In the event a user is unable to get a signal to their mobile phone, an offline mode is available where PingID generates an OTP. Alternatively, the OTP can be delivered via SMS, voice, email or desktop application. Finally, FIDO-compliant security keys, such as YubiKeys, can also be used in sensitive environments or for users without device or phone access. The registration and authentication process is localized and branded.

Use Facial Recognition or Fingerprint as an Authentication Factor

To make it easy for employees and partners to authenticate, PingID can be configured to use facial recognition or the fingerprint reader on the registered device. It works on Microsoft Windows Hello devices, Apple’s iPhone, iPad and Mac devices, Android devices and supporting security key tokens.
Define Adaptive & Risk-based Authentication Policies to Meet Your Enterprise’s Needs

To meet your enterprise’s specific security needs, administrators can define advanced authentication, pairing and device posture policies, such as:

- Limiting MFA and available authentication methods to specific groups, IP addresses or applications.
- Employing geo-fencing to skip MFA requirement if a trusted device is accessing from a “secure” location or network.
- Restricting users from sharing authentication devices and from using 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.).
- Prompting users and bypassing sessions if an authentication is considered risky according to the organization user’s pattern.

To learn more about PingID, visit pingidentity.com/pingID.