Fast And Easy Multi-Factor Authentication

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 web single sign-on (SSO), to integrating seamlessly with Microsoft Azure AD, Active Directory Federation Services (AD FS) and Windows Login, to embedding advanced MFA functionality directly into your own mobile app—PingID has you covered.

PingID is designed to support a wide range of customer, partner and workforce use cases. PingID comes with multiple implementation options including the PingID mobile application for Apple and Android devices that is fully managed by Ping Identity, the PingID desktop app, PingID APIs, and PingID SDKs that allow you to embed multi-factor authentication capabilities directly into your Apple and Android mobile applications. 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.

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

-Forrester
PingID for Employee & Partner Use Cases

How It Works
When an administrator enables PingID, the user is prompted to walk through a self-registration process to register their 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 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, 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, many of which are non-Microsoft. Our PingID solution makes leveraging Office 365 and Azure AD easier, more secure and 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 users change roles or leave the organization, PingID provides automated de-provisioning capabilities to update, disable and delete users from the service.

Balance Security 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 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 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. Alternately, 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. Users can also self-manage their trusted authentication devices.

Use Facial Recognition or Fingerprint as an Authentication Factor
For the ultimate in convenience, PingID can be configured to use facial recognition or the fingerprint reader on the registered device. After the notification is sent to the phone, the user will simply touch the fingerprint reader or conduct a face scan for authentication. This is an optional feature that works with Apple’s Face ID, Touch ID and select Android devices.

Define Adaptive 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 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.).
PingID for Customer Use Cases

How It Works
For consumers, 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
PingID can send push notifications, the most secure and convenient method of second-factor authentication, during web, mobile web, call center, face-to-face, high-value transactions or any other customer interaction. Also, PingID supports OTPs sent via SMS, voice or email, which can be used as a backup authentication method when push notifications aren’t an option for the user. Additional device-based context can also enhance security during mobile app authentications. The security PingID’s mobile SDK adds through your native mobile app is a benefit you can promote to customers to drive mobile app adoption. PingID 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.

Usernameless and Passwordless Authentication
Your customers can now log in to web applications without entering a username or password. Simply display an on-screen QR code that users can scan using your mobile application — with the PingID SDK inside — to instantly log in. No username. No password.

Support Out-of-band Web Authentication
PingID 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 MFA capabilities to replace their password.

Manage 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.

Strengthen Security With Trusted Device Authorization
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. PingID can also integrate with leading enterprise mobility management (EMM) and mobile device management (MDM) solutions such as Microsoft Intune, VMware AirWatch and MobileIron to make policy decisions based on the user’s device posture, which mitigates security risks.

Enable Customer-managed Network of Trusted Devices
PingID lets your customers 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.

Simplify Administration
From a single, user-friendly administrative 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 tenant can be utilized for multiple mobile applications and managed from an easy-to-use administrative portal.
# Compare Our Customer & Workforce MFA Solutions

## Workforce MFA

<table>
<thead>
<tr>
<th>Primary Use Case</th>
<th>Employees &amp; Partners</th>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation</td>
<td>Standalone Ping Identity MFA Mobile App and SaaS Configuration (Mobile App Not Required for All Use Cases)</td>
<td>Custom iPhone / Android SDK Embedded in Your Own Mobile Application (APIs can be Used Instead of Mobile SDK for Some Use Cases)</td>
</tr>
<tr>
<td>User-managed Network of Trusted Devices</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transaction Approvals</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Branding/Customization</td>
<td>Customization Options</td>
<td>Complete Customization</td>
</tr>
<tr>
<td>Trusted Device Authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reduced Permission Devices</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Service APIs</td>
<td>Public Web APIs</td>
<td>Server: Public REST APIs Mobile: Mobile SDK APIs</td>
</tr>
<tr>
<td>Authentication Methods Supported</td>
<td>Mobile App Push Notifications, FIDO2 and U2F compliant security keys, Fingerprint/face scan, SMS, Voice, Email, Watch, Desktop, YubiKey and Soft Tokens</td>
<td>Mobile App Push Notifications, Fingerprint/face scan, Watch, QR Code, Voice, Email, SMS and Soft Tokens</td>
</tr>
<tr>
<td>Contextual Access Supported</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise Application Integrations</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Out-of-the-box Registration and Authentication Flows</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Customer MFA

To learn more about PingID, visit pingidentity.com.