DATASHEET

PingOne® MFA

PingOne MFA is a cloud-based multi-factor authentication (MFA) service that enables your business to provide extraordinary customer experiences that balance user convenience with security.

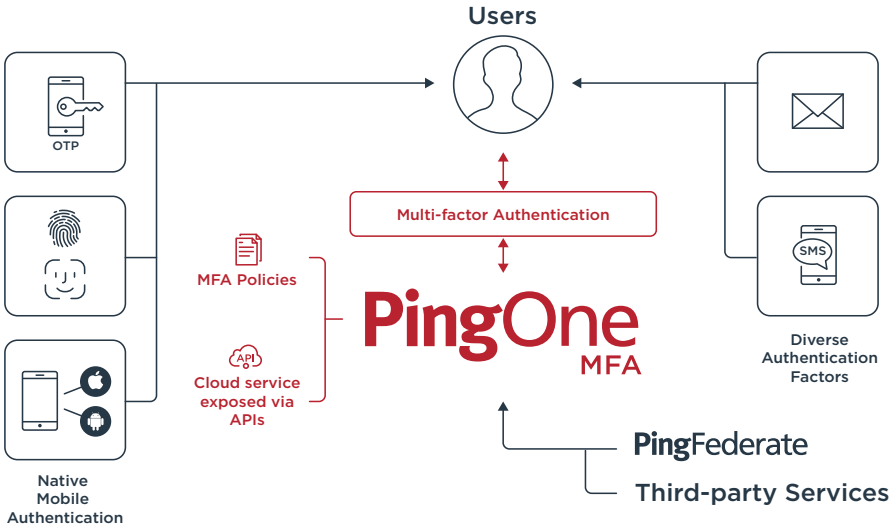
With PingOne MFA, your organization can embed MFA directly into your mobile application, enabling your customers to easily and securely log in from their trusted devices. PingOne MFA offers simple and convenient authentication methods like push notification from custom apps, SMS and email, and can enhance the end-user experience through advanced authentication policies. By prompting a customer to re-authenticate only in high-risk or high-value situations, such as approving a transaction, you remove unnecessary friction without sacrificing security.

EMBED MFA INTO YOUR MOBILE APP

You can embed multi-factor authentication capabilities with PingOne MFA natively into your own iOS or Android mobile application. This allows you to deliver convenient and secure MFA to your customers, without requiring them to download a separate application. And, device authorization behind the scenes can provide an additional layer of security without introducing friction when a user logs into your mobile application, resulting in a seamless authentication experience.

ENHANCE EXISTING AUTHENTICATION WORKFLOWS

PingOne MFA can send push notifications—the most secure and convenient multi-factor authentication method—during web, mobile web, call center, face-to-face, high-value transaction or other customer interaction. By adding MFA to your native mobile app, you drive application adoption. Additionally, PingOne MFA augments your existing authentication workflow. Customers who have your app benefit from additional MFA security, while customers who don't have your app aren't required to download it and instead can utilize SMS and email authentication methods.



ELIMINATE FRICTION WITH ADVANCED AUTHENTICATION POLICIES

Apply advanced authentication policies that use context to prompt customers for MFA only in certain situations, such as when they haven't authenticated recently. Additionally, when using PingOne MFA with PingOne Risk Management or PingOne for Customers, leverage risk-based policies that evaluate several signals, including IP reputation, anonymous network detection and impossible travel, to determine if the customer is in a scenario requiring MFA.

MANAGE TRANSACTION APPROVALS

You can require strong authentication for high-value transactions like 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.

SIMPLIFY ADMINISTRATION

Make it easy for administrators to set up and manage authentication flows. PingOne MFA gives you the flexibility to choose between configuring policies in the administration console or using developer-friendly APIs. Either way, administrators can create separate sign-on policies per application and leverage risk management capabilities to verify customer identity via adaptive authentication. Plus, give developers a head start with sample code and authenticator applications to rapidly integrate MFA into the customer experience.

Features & Benefits

- Cloud-based MFA service that balances convenience and security
- MFA embedded into your mobile app
- Variety of authentication methods, including push notifications
- Seamless MFA that instantly signs on users on trusted mobile devices
- Adaptive authentication policies
- Transaction approvals across channels
- Customized and consistent branding
- Dashboards for admin insight into MFA usage and SMS costs
- Sample application to rapidly develop and deploy your own authenticator app
- Ability to use your organization's Twilio account
- Integration with PingFederate, PingOne Risk Management
- Included with PingOne for Customers Global Plan
- Available in North America, Europe and Australia data centers

Supported Authentication Methods

- Mobile Push
  - Fingerprint
  - Facial Recognition
  - Apple Watch
- Email OTP
- SMS OTP
- TOTP Authenticator Apps
- FIDO2 Bound Biometrics and Security Keys

#3527 | 12.14.20 | v01