

Ping Identity Without Coding Fast Integration to Mobile Apps

Add Ping Intelligent Identity Services
to any Android and iOS App Without Coding

WHAT IS PING INTELLIGENT IDENTITY?

The Ping Intelligent Identity platform enables organizations to leverage a unified digital identity for a secure and seamless user experience across all enterprise resources. Ping's standard-based identity platform was designed for cloud and hybrid IT environments. It enables users and devices to securely access all cloud, SaaS, on-premises, and mobile applications from one single platform, proven to scale with over 2 billion identities under management.

THE CHALLENGE OF USING PING IN MOBILE APPS

Generally speaking, mobile apps don't come out-of-the-box ready to leverage Ping Intelligent Identity Services, such as PingFederate® or PingID®. Mobile apps are typically built to use basic authentication (e.g., username and passwords) rather than modern authentication or multi-factor authentication (MFA) methods. This makes using Ping's Intelligent Identity Services inside mobile apps a challenge.

To use Ping inside a mobile app, developers need to manually code new workflows and modern authentication standards such as OpenID Connect, OAuth 2.0, or SAML inside the app. Developers also need to add Ping specific APIs and/or SDKs into the app. Building a mobile app to trust a third party identity service is a challenging undertaking. The challenge often leads to delays or cancellations of mobile identity projects.

DELIVERING PING IN MOBILE APPS FAST

Appdome and Ping teamed up to deliver a faster, simpler mobile identity solution, enabling everyone to use Ping Intelligent Identity Services with all mobile apps.

Using Appdome, organizations and mobile developers can add modern authentication using PingFederate or mobile MFA using PingID to any Android or iOS app in seconds. Appdome uses technology to complete the integration work, including adding the required authentication workflows, standards, APIs or SDKs to the app. All the work

is done instantly, without coding, changing network infrastructure, or changing the app. This enables enterprises to migrate all mobile apps to PingFederate or PingID quickly, easily, and risk-free.

APPDOME MAKES PING IDENTITY EASY

Using Appdome for Ping Identity is straightforward and simple. Upload an app (.ipa for iOS and .apk for Android) to Appdome, select the specific Ping service needed in the app, and click "Fuse My App." In less than a minute, Appdome's technology builds the implementation and generates a new app that includes the desired Ping Intelligent Identity Service. Once the new app is generated, it can also be set-up and controlled via PingOne.

Appdome for Ping Identity has no development prerequisites or limitations. Appdome is 100% compatible with all Android and iOS apps, developed in any environment, no matter how the app is built. Appdome supports all native, hybrid and non-native apps. Appdome doesn't require access to source code or require any standards, SDKs or APIs to be added to the app manually. Appdome-Fused apps can be deployed through any public or private app store.

PingFederate® **PingID™**

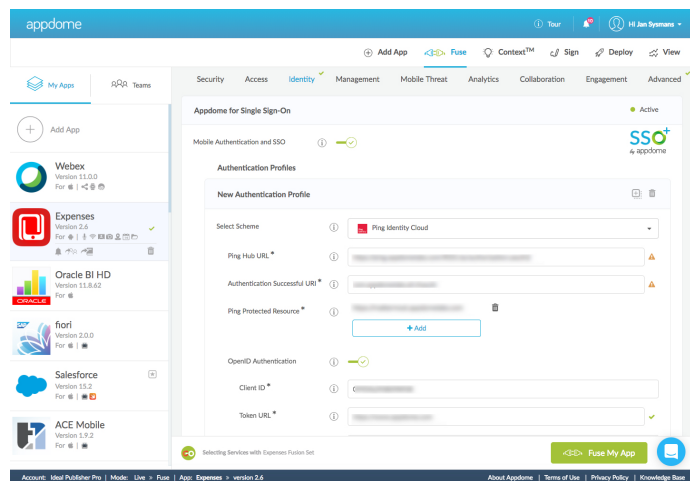
MULTIPLE NO-CODE OPTIONS FOR PING INTELLIGENT IDENTITY SERVICES

PingFederate – SSO, Identity Federation & Authentication

Appdome provides a no-code implementation of PingFederate to any mobile app. PingFederate is Ping's global authentication authority. PingFederate can be deployed on-premises or in the cloud. It integrates with diverse user directories and third-party authentication sources while supporting current and past versions of identity standards like SAML, WS-Federation, WS-Trust, OAuth and OpenID Connect. Adding PingFederate to mobile apps on Appdome allows mobile apps to be set up and controlled via PingOne and leverage any authentication method available with PingFederate.

PingID - Passwordless Multi-factor Authentication (MFA)

Appdome provides a no-code implementation of PingID to any mobile app. PingID allows mobile apps to use multiple authentication methods such as mobile push authentication, OTP, and facial recognition. On Appdome, PingID is available in one of two implementation options: 'In-app' – embedding PingID MFA inside any iOS or Android app, 'PingID app' – allowing PingID enabled apps to use PingID MFA app for authentication.



Learn more about Appdome for Ping Intelligent Identity at www.appdome.com and open a free Appdome account at fusion.appdome.com and start fusing!

TOP BENEFITS APPDOME FOR PING IDENTITY

The following benefits of Appdome for Ping Identity come with every implementation:

- **No-Code Implementation**
Users of Appdome for Ping Identity can implement the full range of Ping Identity services to Android and iOS apps built in any development framework or environment, without writing code, needing developer time or requiring access to the mobile app source code.
- **No In-App Standards Required**
Using Appdome, there is no need to manually implement or support SAML, OAuth, OIDC or MFA in apps. Appdome's technology adds all the workflows, standards and methods automatically.
- **Cross-App Identity**
Allows mobile apps to share authentication state no matter what Ping Identity service is used. Signing into one app automatically unlocks other apps in the group.
- **Conditional Access**
Grants access to restricted resources using separate resource-level authentication and authorization, no matter what Ping Identity service is used.
- **Direct ID brokering**
Mobile apps authenticate directly to the Ping Identity service of choice, without using public identity brokers.
- **In-App Secure ID**
Encrypts all mobile app credentials, cookies, and tokens. Stores them securely in a non-shared area within the app's Fusion Layer.
- **Multi-Vendor Implementations**
Combine Ping Identity services with other mobile services from multiple vendors to speed application delivery and gain efficiencies (eg: Ping/EMM or Ping/Security), all within a single Fusion Set.
- **Comprehensive App Security**
ONEShield™ by Appdome secures identities, the identity of the provider service, and the code of the app itself. ONEShield includes code obfuscation, code encryption as well as anti-tampering, anti-debugging, anti-reversing and more. These features prevent hackers from gaining access to sensitive resources, user credentials, or discovering the structure of the app itself.

ABOUT APPDOME

Appdome is the industry's first no-code mobile integration platform. Appdome's patented*, Fusion technology and its AI-Digital Developer™, known as AMI, powers a self-service platform that allows anyone to complete the integration of thousands of mobile services, standards, vendors, SDKs and APIs in security, authentication, access, mobility, mobile threat, analytics and more, adding these services to any mobile app instantly. Leading financial, healthcare, government and e-commerce providers use Appdome to deliver rich mobile experiences, eliminating development complexity and accelerating mobile app lifecycles. For more information, visit www.appdome.com.

*Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.