AppsFlyer

Authentication Capabilities

At AppsFlyer, data security, scalability and privacy are our lifeblood.

AppsFlyer provides the most thorough authentication security measures in the mobile attribution industry. We feel strongly that customers should have full control over access to their own data.

Among the available authentication capabilities, many settings are fully configurable to suit individual organizational standards and needs.

Full Complexity Passwords

All users must create full complexity passwords, which include a minimum of 8 characters, uppercase and lowercase letters, numbers and symbols.

2-Factor Authentication

Customers can choose to require 2FA when users log in to the dashboard from a new device or after a long period of dormancy.

Single Sign-On

Customers using an IDP solution within their organization can connect it to the AppsFlyer dashboard. AppsFlyer works with the SAML 2.0 standard for SSO.

Failed Logins

While the recommended setting is to block users after 10 failed login attempts, AppsFlyer blocks users after 5. Customers can determine the duration of the lockout.

SHA-2 + Salt Password Hashing

Customer passwords are not stored in clear text in AppsFlyer's servers. AppsFlyer uses SHA-2 hash standard for storing all passwords.

Temporary Passwords

AppsFlyer requires new users to create a new password immediately after signing in with a temporary password.

Trusted by the World's Best Companies:

avast! McAfee Microsoft CHASE Walmart Save money. Live better. ebay VISA

AppsFlyer