Authentication Capabilities

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

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.

Account security

Full complexity passwords

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

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.

2-Factor Authentication

Customers can choose to require 2FA when users log in to the dashboard.

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.

AppsFlyer provides the most thorough authentication security measures in the mobile attribution industry.

Activity capabilities

Audit logs and notifications

Use the Audit log and notifications page to view team member activities (such as, login activity, API calls, or change to integrated partner configurations).

Failed logins

While the recommended setting is to block users after 10 failed login attempts, AppsFlyer blocks users after 5.

Trusted by the World's Best Companies:

Avast McAfee Microsoft Walmart Save money. Live better. ebay VISA

"We're always on high alert. Always. We check and recheck our activity and seek to improve ourselves in every aspect in order to protect our systems. We don't just check boxes, we are constantly thinking about how we can expand and go beyond."

Dikla Saad Ramot
Chief Information Security officer,
AppsFlyer

For more information about AppsFlyer's extensive Security & Privacy Program, please visit our Trust Hub.