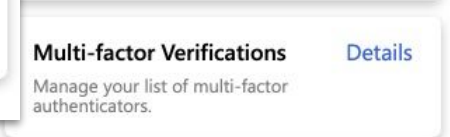
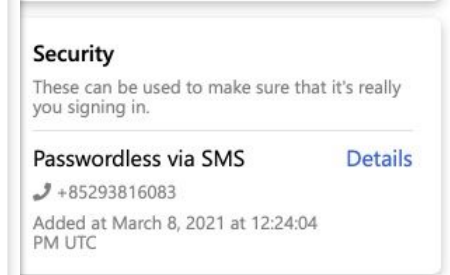
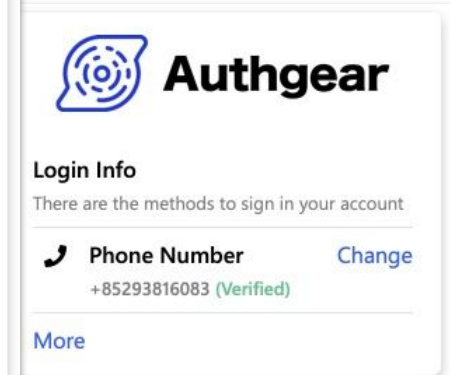
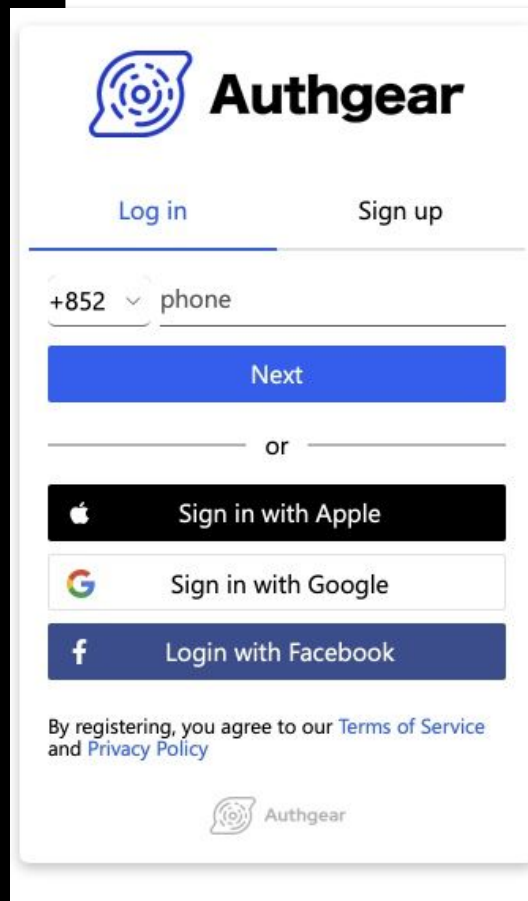


OURSKY

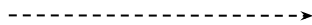
# Authenticate your app users securely

Authgear, a secure  
authentication service for your  
applications

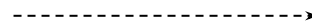


# Authgear is a OIDC 2.0 compliance authentication service that can be integrated to your app via SDKs

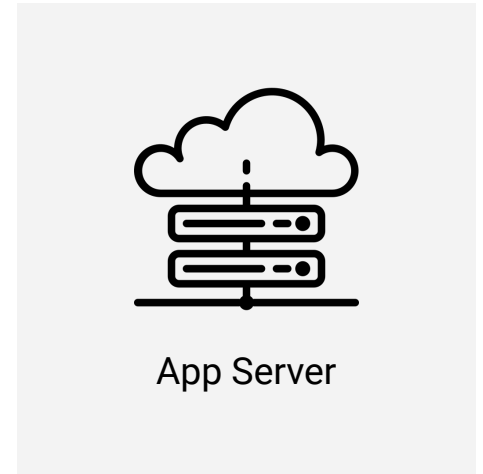
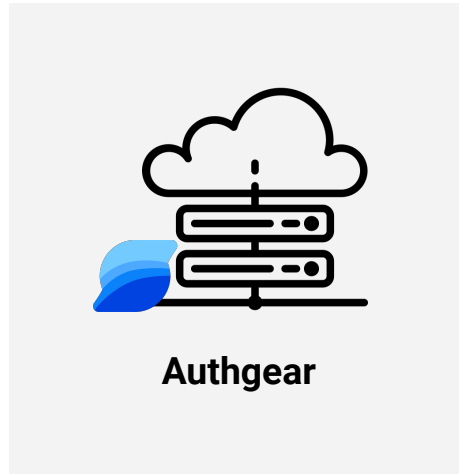
A user signs up  
in your app



Authgear  
authenticate the user



Manage sessions for  
your app servers



# Why Authgear?



## Speed up the time to market

With the cross-platform SDKs, Authgear can be integrated to iOS, Android and Web apps within days. The use of the UI kit can further reduce the development time.



## Bake security into your applications

Authgear provides essential security mechanisms to enable security and privacy to be baked into the development process regardless of whether developers have the resources to implement or augment them.



## Unify login experience

Authgear can be extended to all your app portfolio, which means you can store all your user data in ONE single place and provide a streamlined login experience.

# Core features



Single Sign On



User management  
for admins



Simple integration  
with OpenID connect



Social login - Google,  
Facebook and more



Password policy  
and MFA



Session  
management



Customisable look  
and feel



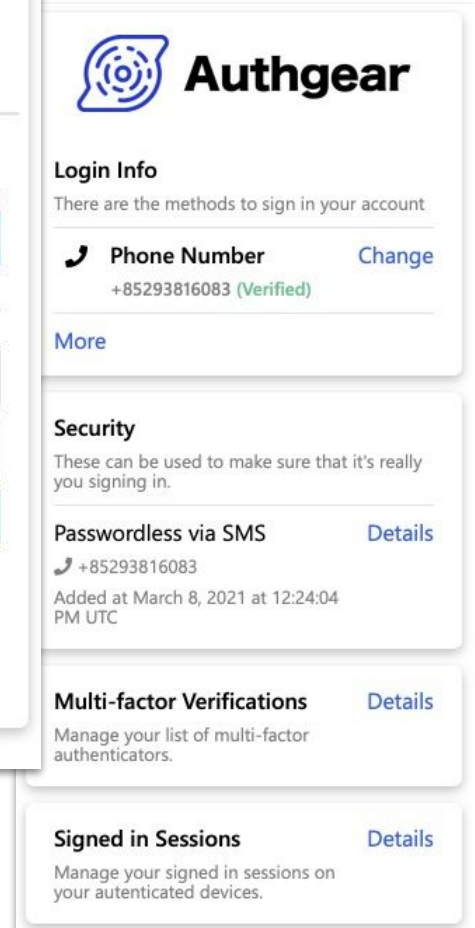
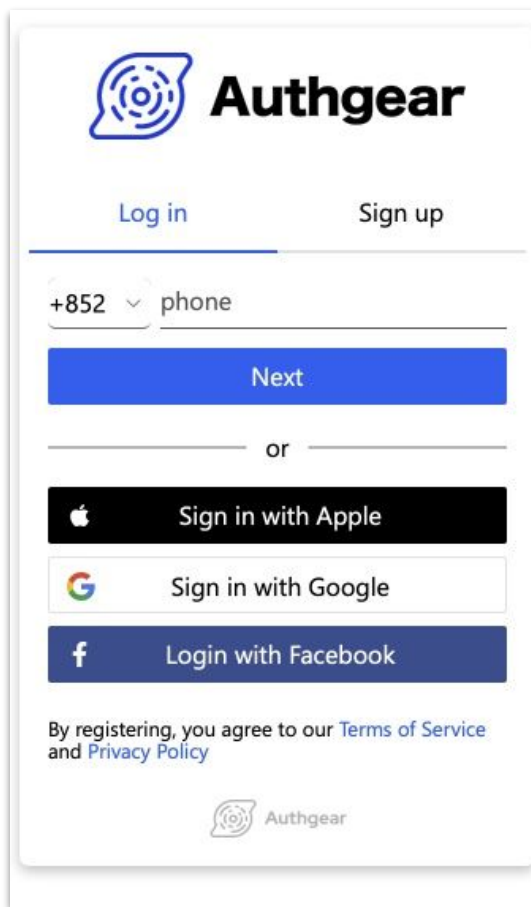
LDAP and Active  
directory support

# Batteries Included UI

Simply plug the iOS/Android/Web SDK to your app to use our carefully designed UI.

From login/signup to user settings for 2FA configuration, changing passwords or checking out other logged in devices, all UI are readily available, implemented securely, and nice looking!

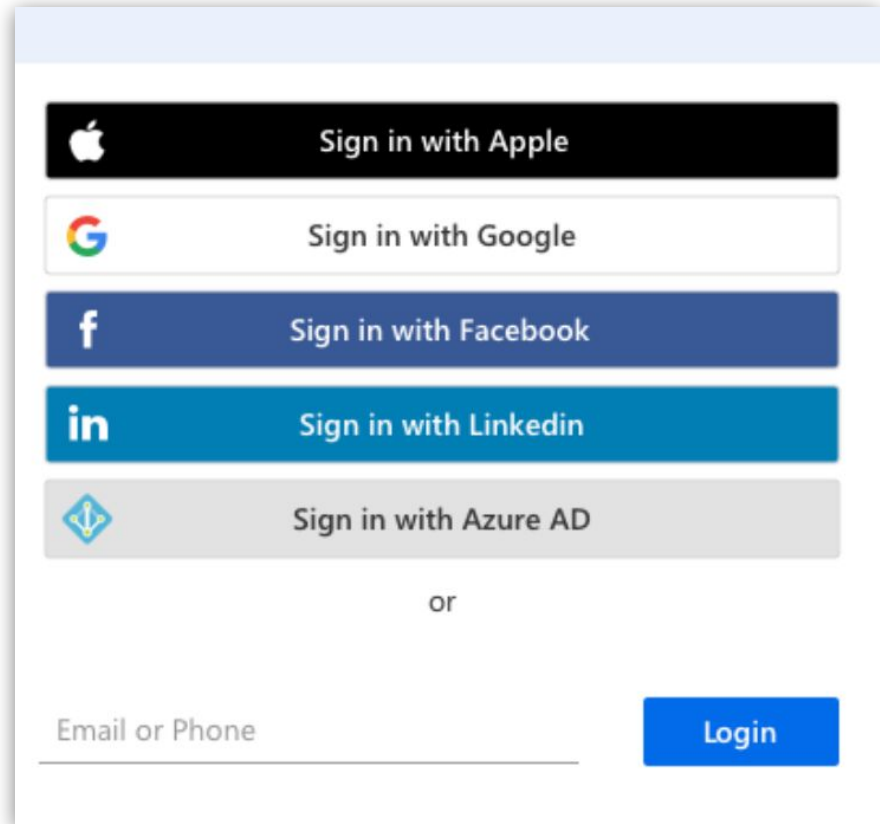
Everything from Theme, Localization and various messages are configurable.



# SSO / Social Media Login

Including, but not limited to:

- Sign in with Apple
- Sign in with Google
- Sign in with Facebook
- Sign in with LinkedIn
- Sign in with Azure AD/ADFS
- Sign in with Wechat



The image shows a login interface with a light blue header. Below the header, there are five horizontal buttons for social media and SSO login, each with a logo on the left and text on the right:

- Sign in with Apple**: Black button with the Apple logo.
- Sign in with Google**: White button with a thin border and the Google logo.
- Sign in with Facebook**: Dark blue button with the Facebook 'f' logo.
- Sign in with LinkedIn**: Teal button with the LinkedIn 'in' logo.
- Sign in with Azure AD**: Light gray button with the Azure AD logo.

Below these buttons is the word "or" centered. At the bottom, there is a text input field labeled "Email or Phone" and a blue "Login" button to its right.

# User Management

Built-in User Management Portal for your customer supports:

- Delete or Disable users
- Reset Password
- Remove MFA devices
- Add / remove identities (email, phone no. etc)
- List of all logged in sessions and termination
- Audit logs (Signed up, last login, etc)

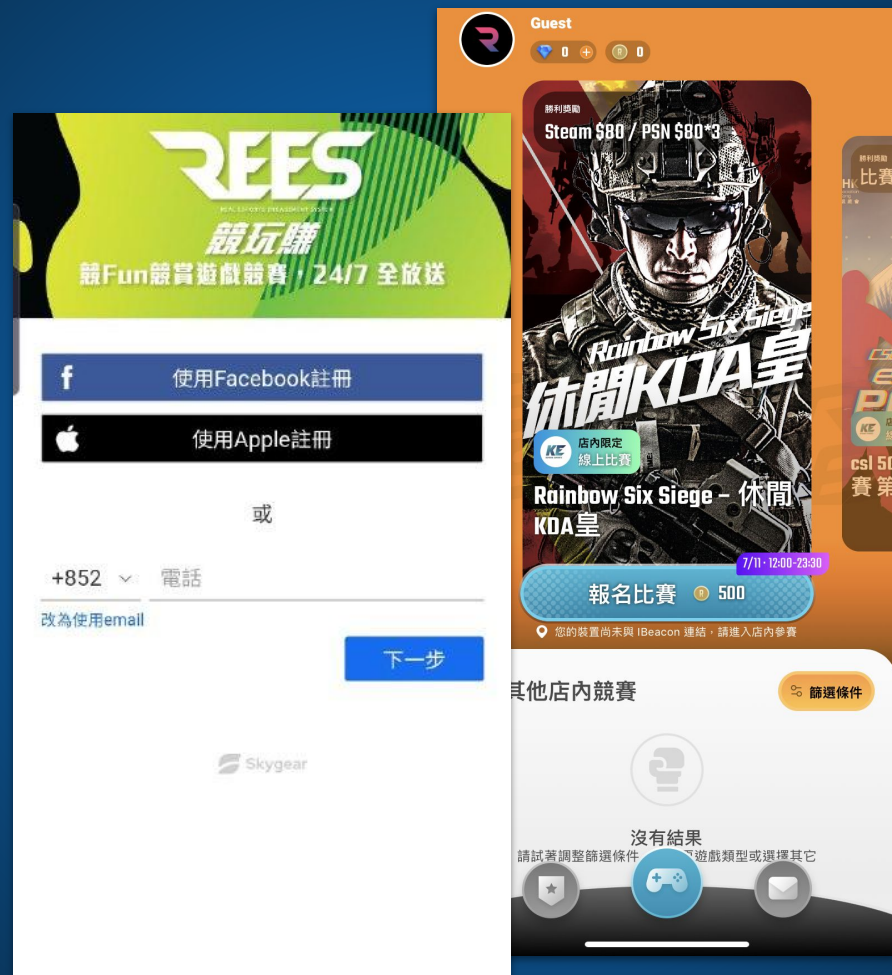
The screenshot displays the Authgear user management interface. At the top, a blue header bar contains the Authgear logo and the URL 'bencheng-test - https://bencheng-test.authgear-staging.com'. Below the header, a sidebar menu is visible with the following items: 'Users' (selected), 'Authentication', 'Anonymous Users', 'Single-Sign On', 'Passwords', 'Applications' (expanded to show 'Allowed Origins', 'Applications', and 'Custom Domains'), 'UI Settings', 'Localization', and 'Settings'. The main content area shows the 'User Details' page for the user 'bencheng@oursky.com'. The user's profile includes a blue circular icon with a person silhouette, the email address, and login information: 'Signed Up: 12/29/2020, 4:39 PM' and 'Last Login: 2/1/2021, 2:36 PM'. Below this, there are three tabs: 'Account Security' (active), 'Identities', and 'Sessions'. Under 'Account Security', there are sections for 'Primary Authenticators' and 'Multi-factor Authentications'. The 'Primary Authenticators' section shows a 'Password' entry with the text 'Last updated at 1/25/2021, 3:19 PM' and a blue 'Reset Password' button. The 'Multi-factor Authentications' section lists 'Authenticator Apps / Devices', including a 'TOTP @ 2021-01-25T06:56:38Z' entry with 'Added: 1/25/2021, 2:56 PM' and a red 'Remove' button. Below that, a 'Verification code via SMS' entry shows the phone number '+85293816083' with 'Added: 1/25/2021, 3:57 PM' and another red 'Remove' button.

# Case study: Speed up time-to-market with the Authgear UI

Rees is an mobile app that connects esports players. Players initiate a competition with other users in the app.

To support a seamless mobile experience, the team wishes to implement SMS-based passwordless login. They also do not want to spend too much time on the authentication server since it is not the highlight of their app.

Authgear provides passwordless login function out-of-the-box and reduce the development time of the Authentication module to a few days.







Authgear for developers

# Why Authgear?



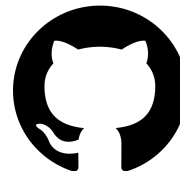
## Comprehensive documentations

From getting started to detailed API reference, all useful tutorials are at your fingertip on <https://docs.authgear.com/>.



## User Friendly Configuration GUI

Most functions are configurable, be it password policy, or session management. It comes with a GUI that allows you to configure your application effortlessly.



## Open source, avoid vendor lock-in

Authgear is open source, therefore, you need not worry about vendor lock-in. If don't want to use our managed service, it can be deployed on a server of your choice.

# A snapshot of the developer portal

The screenshot shows the Authgear developer portal interface. At the top, there is a blue header with the Authgear logo and the text "Authgear > bencheng-test - https://bencheng-test.authgear-staging.com". Below the header is a navigation menu on the left with the following items: Users, Authentication, Anonymous Users, Single-Sign On, Passwords, Applications, Custom Domains, **UI Settings** (highlighted), Localization, and Settings. The main content area is titled "Light Mode" and contains a "Theme Color" section with a 3x3 grid of color options: Default (blue), Tropical (green), Sunrise (red), Contrast (black), Summer (light blue), Unicorn (purple), Orange, Luxurious (gold), and Custom (plus sign). Below the grid are three color pickers for "Primary Color" (blue, #176df3), "Text Color" (black, #000000), and "Background Color" (white, #ffffff). At the bottom of the main content area is the "App Logo" section. On the right side, there is a "Preview Mode" section showing a preview of the login page. The preview includes the Authgear logo, "Log in" and "Sign up" links, an email input field, a "Next" button, and social login options for Apple, Google, Facebook, LinkedIn, Microsoft, and WeChat. At the bottom of the preview, there is a link to the Terms of Service and Privacy Policy, and the Authgear logo.

Authgear > bencheng-test - https://bencheng-test.authgear-staging.com

Save Reset

Users

Authentication

Anonymous Users

Single-Sign On

Passwords

Applications

Custom Domains

**UI Settings**

Localization

Settings

### Light Mode

#### Theme Color

Hello Default	Hello Tropical	Hello Sunrise
Hello Contrast	Hello Summer	Hello Unicorn
Hello Orange	Hello Luxurious	+ Custom

Primary Color

Text Color

Background Color

#### App Logo

### Preview Mode

Authgear

Log in Sign up

Email

Use phone instead

Next

or

Sign in with Apple

Sign in with Google

Login with Facebook

Sign in with LinkedIn

Sign in with Microsoft

Login with WeChat

By registering, you agree to our Terms of Service and Privacy Policy

Authgear

# How Authgear Enhance your Auth System Security

- Encryption-at-Transit and Encryption-at-Rest for SaaS Deployment (Private Cloud Deployment: if Applicable)
- Built on top of battle tested OpenID Connect Standard
- Carefully picked hash algorithm for password (Default: bcrypt with cost 10), auto-migration to latest hash algorithm if integrated with legacy system
- Conducted Architecture Design Security Review, Automated DAST scanning, manual Penetration Test based on OWASP Top 10 by eWalker Consulting (HK) Limited as Authgear was whitelabelled for Hong Kong Productivity Council;
- Default configuration to prevent CSRF and XSS attacks via CSP HTTP
- Built-in Active Sessions Management
- Rate Limit for SMS Verification Code / Password etc to prevent Brute Force attack
- Abnormal activities detection (depends on Licenses)

About us

# Who is OURSKY?



Founded in 2008 by engineers,  
comprising teams with **10 times  
more developers** than sales reps

12+ years of experience in  
**mobile app development**

**DevSecOps**-enabled with  
expertise in **containerization** and  
**Kubernetes**

A huge fan of **open source**

**2 locations**, Hong Kong and  
Taiwan

Let's Innovate Together!