Data Sheet

Auth Connect

Secure Single Sign-On Made Easy

Ionic Auth Connect provides a simple, secure method for integrating with authentication providers to enable single sign-on (SSO) within your Ionic apps.

Auth Connect is easy to install and provides all the infrastructure you need for login, logout, and token refresh in an Ionic app, using the latest native security best practices.

Auth Connect helps enterprise teams:

- Integrate with any OAuth-based provider — all from a single connector API.
- Easily connect with Azure Active Directory, Auth0, AWS Cognito, and more.
- Deliver the best possible security to safeguard users and protect sensitive data.
- Prevent unauthorized access to usernames, passwords, and sensitive company data.
- Enjoy peace of mind knowing your auth workflows will automatically remain up-to-date with the latest security best practices and platform requirements.

Why Auth Connect

PROTECT YOUR USERS & DATA

Prevent unauthorized access to usernames, passwords, and sensitive company data, by using best-in-class native authentication methods.

ONE API, ANY AUTH PROVIDER

Avoid vendor lock-in and easily enable secure SSO with any authentication provider, including Auth0, AWS Cognito, or Azure AD — all from a single connector API.

FOCUS ON YOUR BUSINESS

Your auth workflows automatically remain up-to-date with the latest security best practices and platform requirements — no extra effort required.

How it Works

Using the OAuth and OpenID Connect authentication standards, Auth Connect provides a simple interface for login, logout, registration, and retrieving security tokens back after a successful login.

Developers simply fill in a configuration with their authentication service details, such as provider and URL, and Auth Connect takes care of the rest, including redirects, WebView presentation, and selecting the appropriate view controller based on the device's operating system.

Addressing Common Auth Challenges

By implementing the latest in native security best practices, Auth Connect helps solve several common challenges that app dev teams face when implementing their own authentication workflows.

COMMON PITFALLS & CHALLENGES	HOW AUTH CONNECT SOLVES IT
Embedded Browsers Standard authentication workflows involve a complex handshake between the app and the backend server, typically implemented using an embedded web browser. After the user logs in, the server hands back an access token as well as a refresh token that can be use to authenticate against the rest of the app backend.	Native System Controls Rather than using an embedded browser, Auth Connect displays the UI from the auth provider using native System Components, so neither your app nor the Auth Connect plugin is able to access user information required to log in. This makes sure your users stay protected and are not at risk of a JavaScript injection or other MITM-style attacks.
Out-of-Date Security Practices Rapidly evolving security standards make it hard to keep pace with the latest platform	Active Maintenance & Updates Auth Connect allows your team to deliver the best possible protection, without having to

requirements and best practices.
For example, as of iOS 10, the recommended way to accomplish the OAuth flow was to use the SafariViewController component. In iOS 11, that changed to SFAuthenticationSession, which was then deprecated in iOS 12 in favor of ASWebAuthenticationSession. These constantly shifting standards can make it challenging for app development teams to keep up.

On top of that, the native plugins offered by auth providers and members of the open source community are often out of date and not kept current with the latest security standards.

become experts in native mobile authentication or keep pace with ongoing security best practices.

Plus, as an Auth Connect subscriber, you receive ongoing security patches, integrations with new auth providers, and ongoing feature updates, plus access to Ionic Support for help troubleshooting issues with the Auth Connect plugin or API.

Rework & Vendor Lock-In

Many development teams need to support multiple authentication providers, which requires parallel development efforts and custom integrations with each provider.

At the same time, standardizing on a single authentication provider can result in large portions of each client-side application having to be rewritten if and when you do decide to change vendors. In fact, the time and costs associated with a change will often compel businesses to stick with a provider they're no longer happy with, simply to avoid the costs of switching.

Single API, Any Auth Provider

Auth Connect makes it easy to integrate with multiple auth providers using a single, easy-to-use API. It includes pre-built integrations with popular providers like Auth0, AWS Cognito, and Azure Active Directory. It can also work with any other OAuth-based provider, including custom authentication solutions.

You have the freedom to choose the best auth provider for your needs — now and in the future, with a simple, vendor-agnostic API based on the underlying protocols and standards shared by all OAuth solutions. Thus, if you ever need to switch vendors, you simply update your authentication configuration to the new vendor, with no changes to your app's business logic.

Learn More

Ionic Auth Connect is available as part of Ionic Enterprise. To learn more about how Auth Connect can help protect your users, get in touch with one of our team members at sales@ionic.io.

Ready to explore how **Ionic Enterprise** can help your organization build critical apps, faster?

Contact us!

sales@ionic.io
ionicframework.com/enterprise