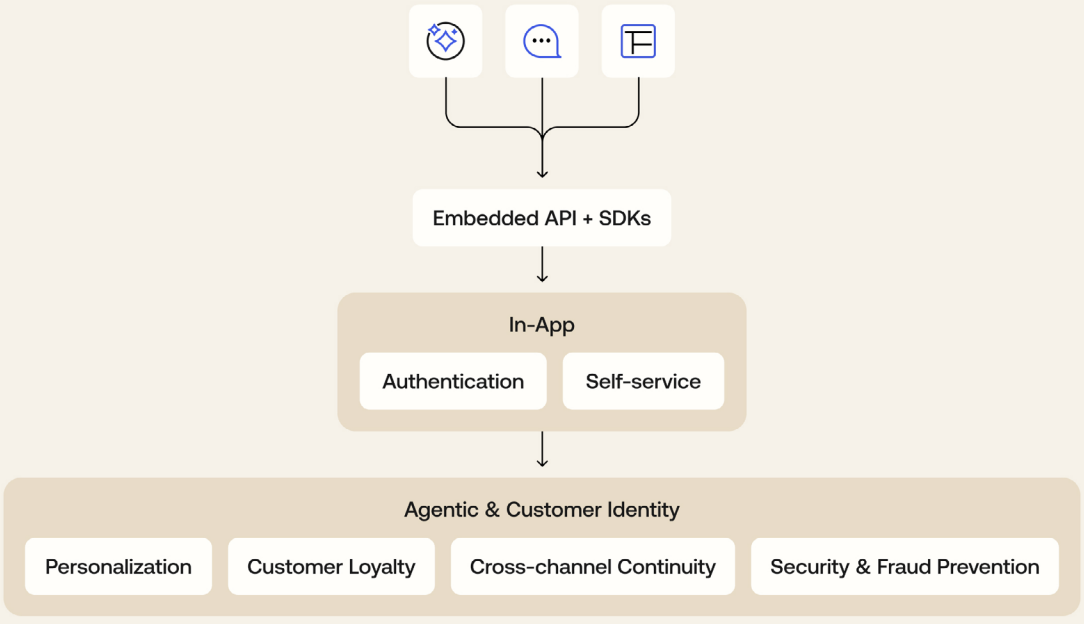
Embedded Login

Convert more users. Put your applications in control of identity.

Embedded Login is Auth0's API-based approach to identity that enables teams to optimize in-app identity flows and deliver seamless experiences that drive conversion.

Using Auth0 APIs, SDKs, and components, teams can embed identity flows directly into their application code, giving them full control over when, how, and what users authenticate across mobile, web, and agentic experiences. This enables teams to fine-tune every part of the customer journey and place identity exactly where users convert. With no redirects or webviews, users remain engaged within the application throughout the entire journey. This reduced friction translates to higher conversion rates, increased registration completion, and a seamless brand experience that builds customer trust from the very first interaction.

A View Of How Embedded Login Works

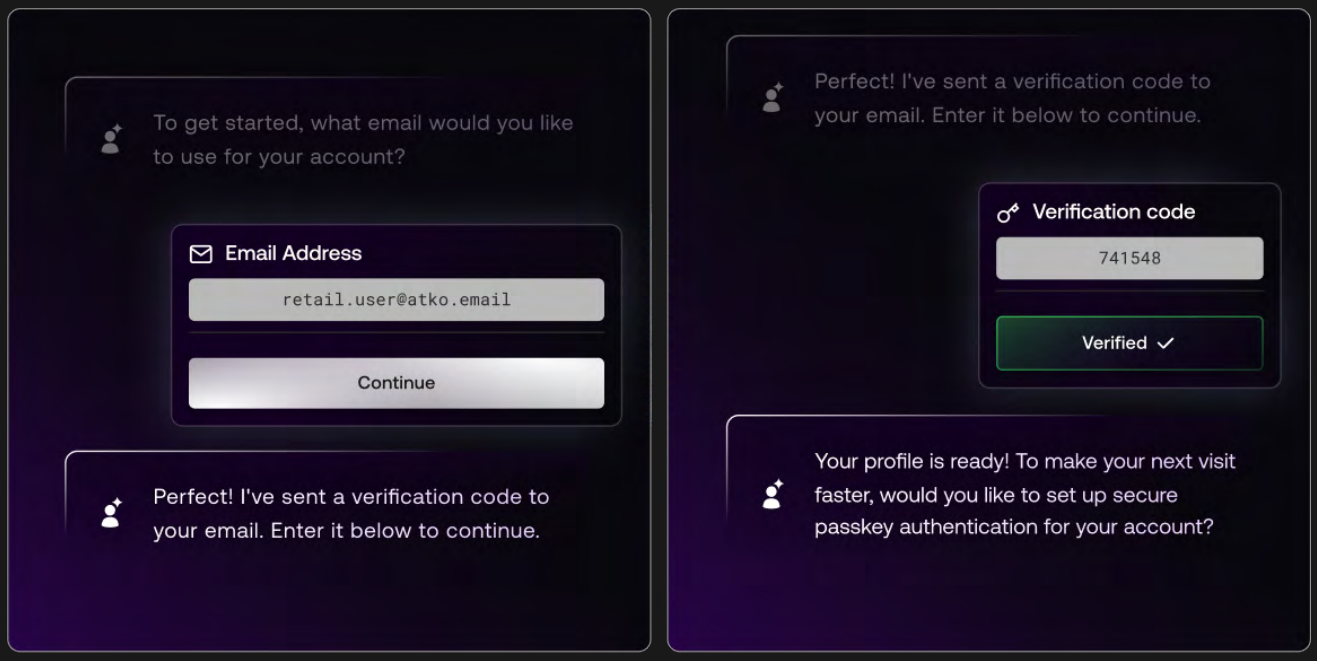


Applications connect to Embedded APIs, SDKs and components to execute identity flows and unlock Auth0 offerings.

Example user journeys powered by Embedded Login

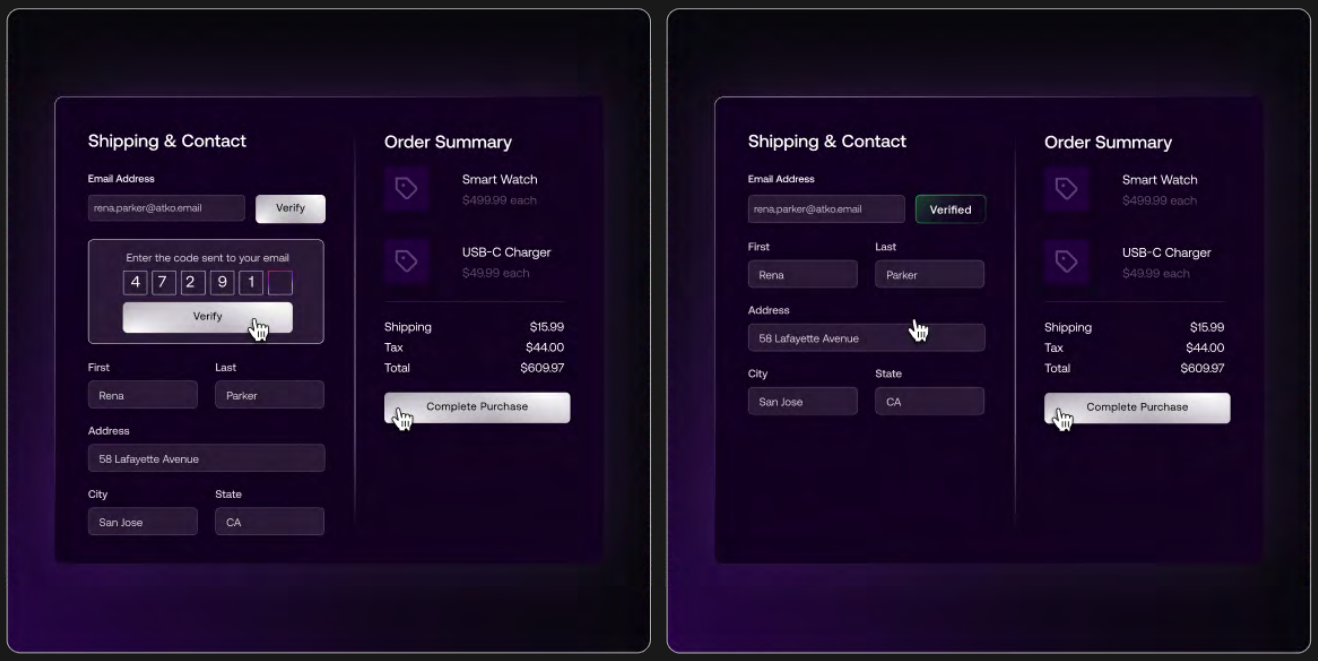
Agentic applications

Enable agentic first party applications to authenticate users and authorize services directly within the chat interface, preserving the user's context by eliminating redirects.



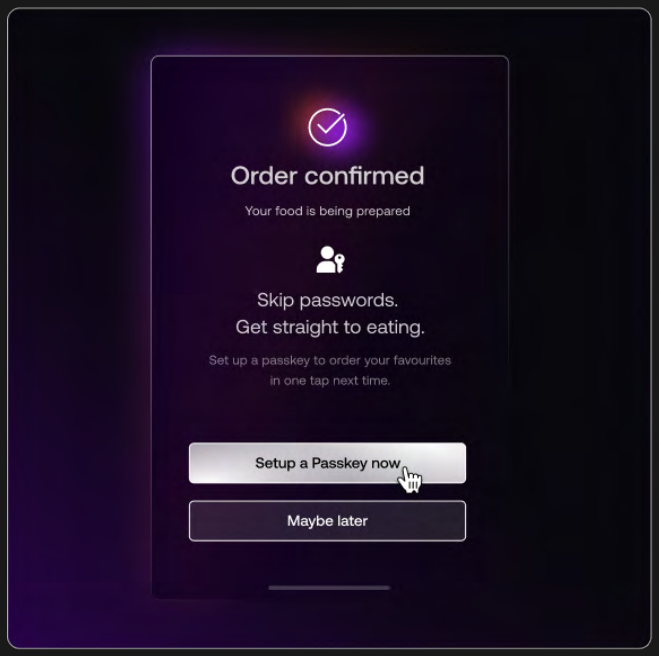
Cart-integrated identity

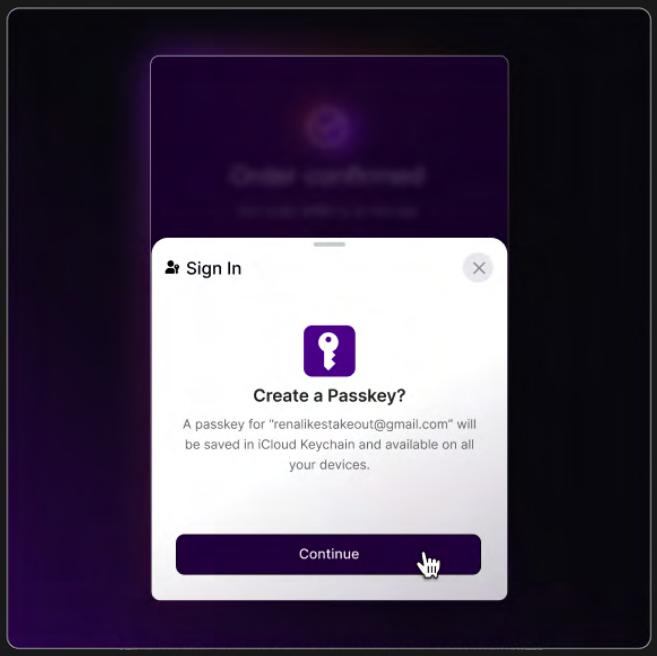
Embed sign-up and authentication into checkout flows to reduce friction and improve conversion rates.



Progressive enrollment

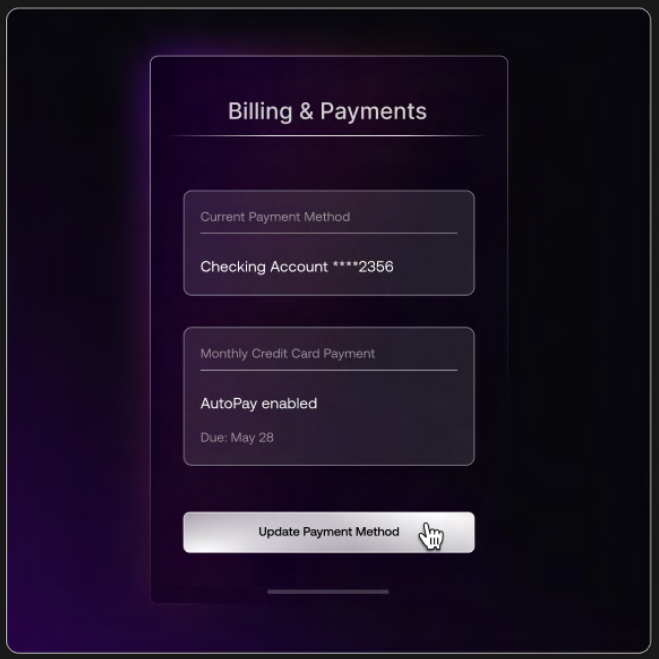
Enroll users in additional authentication methods after a high-value action without disrupting it.

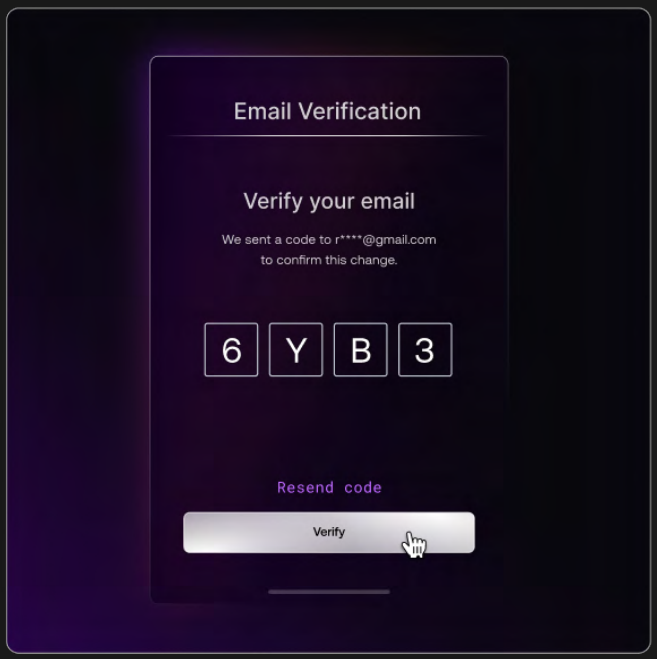




Inline step-up for sensitive operations

Re-authenticate users for high-risk actions (i.e. payment updates, account changes) with an inline authentication challenge without leaving the app.





Get identity right, and unlock greater business value

Convert more users

Fine-tune every part of the user journey to deliver seamless in-app experiences that convert.

Accelerate development with less identity overhead

Free developer cycles by reducing custom code with expanded feature support and built-in, security tooling.

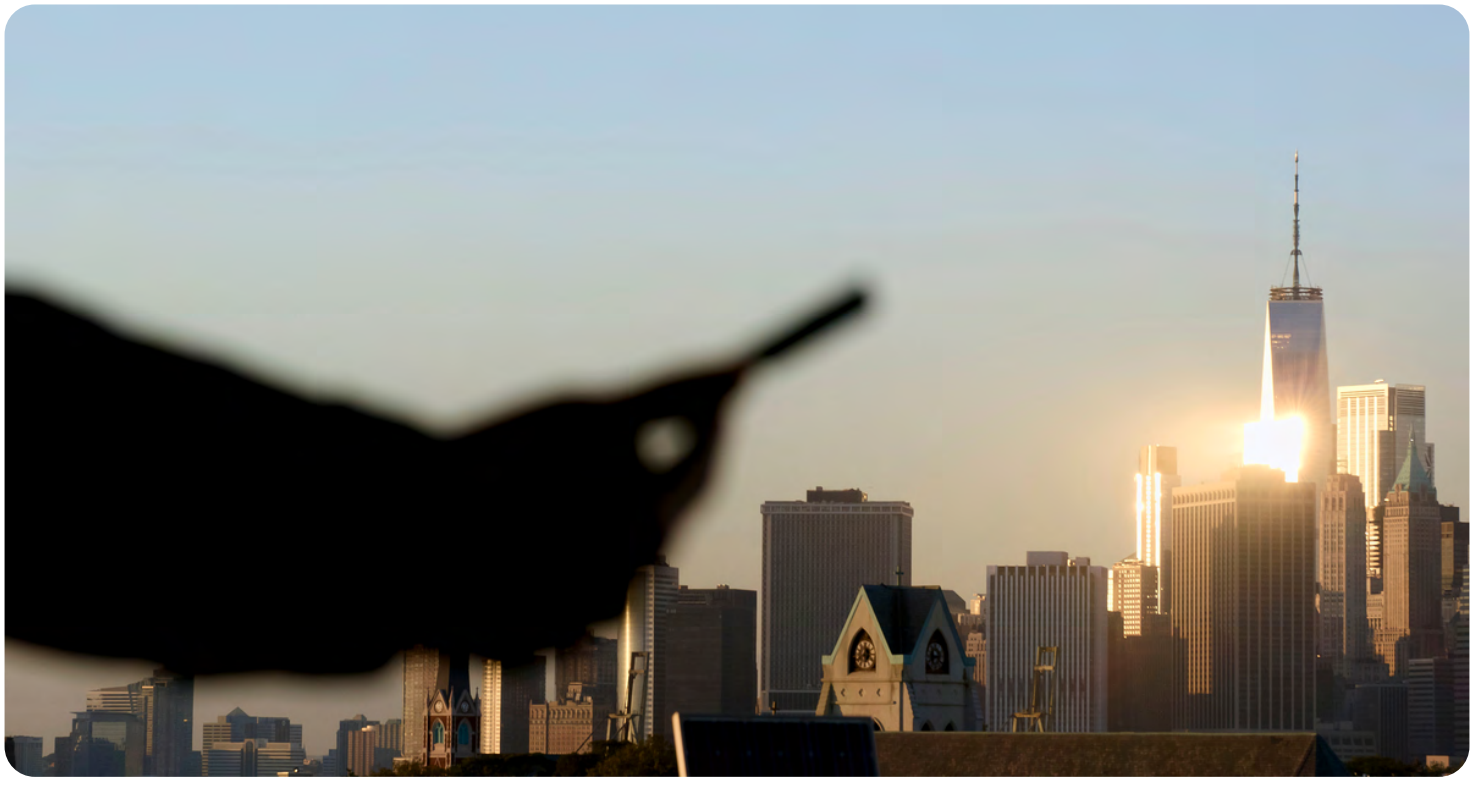
Security that doesn't slow you down

Sail through security reviews and ship faster with built-in security features and tools that won't stall your roadmap.

Key advancements behind Embedded Login

Previously, Embedded Login required significant custom code and security work to implement safely at scale. Now, two critical shifts in the landscape have created an uptake in embedded identity use:

- **The security landscape has matured:** Emerging standards such as OAuth 2.0 for First-Party Applications now enable embedded login flows at scale, while modern security controls like application attestation and DPoP help reduce risks such as impersonation and token theft.
- **Teams have new ways to reduce identity overhead:** Improved SDKs, built-in tooling, and AI-assisted development are accelerating implementation and reducing the custom code required to build, maintain, and scale embedded flows.



The following table outlines key capabilities that make building embedded identity easier.

In-app Flows	• Step-up authentication for sensitive actions • Progressive factor enrollment • Self-service account management: profile, credentials, devices • Passkeys enrollment and authentication challenges
Developer Tooling	• UI Components & SDKs for authentication flows • Passkeys APIs (Web & Native) • Passwordless authentication APIs (email/SMS OTP) • Extensible flows for custom app logic (e.g., approvals, branching auth)
Built-in Security	• Configurable Level of Assurance (LOA) per API or action • Step-up policy enforcement based on risk or scope • DPoP (proof-of-possession tokens) support • Expanded MFA grant types (passkeys, OTP, refresh token flows) • Fine-grained access controls & permissions • Multi-resource refresh token support

Review our Embedded Login documentation to explore the latest Embedded Login capabilities and updates.

Get Started

Ready to build in-app authentication experiences that convert?

1. **Explore our product page**
   Visit our Embedded Login site for full details on capabilities and updates.
2. **Schedule a consultation**
   Chat with one of our experts about your specific requirements and how you can best optimize your identity flows to convert.

Embedded Login, Universal Login or Both.

Your authentication options just got more flexible. Choose the identity approach that fits your application, user journey, and business goals—whether that's Universal Login, Embedded Login, or a hybrid of both.

Criteria	Universal Login	Embedded Login
Implementation model	Hosted authentication managed by Auth0	API-driven authentication integrated into your application
Authentication experience	Redirect-based authentication hosted by Auth0	Authentication stays within the application (no redirects or webviews)
Control over identity flows in the user journeys	Configure and extend login experience; post-login flows via Actions and Forms	Full control over when, where, and how authentication happens within the user journey
Developer model	No-code and pro-code customization options	Pro-code implementation using APIs, SDKs, and embeddable components
UI customization	Advanced Customization for Universal Login (ACUL) enables you to use your own design system, tooling UI investments on top of Auth0	Complete control over UI using your own design system and application components
Typical use case	More secure, consistent login experience with minimal engineering effort	Deeply integrated, in-app authentication experiences tailored to product flows
Identity Security Features Support	Complete, out-of-the-box support for all Attack Protection features. Hosted browser environment allows UL to natively support advanced security controls that require a UI or browser state (i.e. displaying CAPTCHAs for Bot Detection and Brute Force Protection).	Supports many core security features. Bring-your-own (BYO) Approach: Since authentication occurs within the application interface, the user is responsible for implementing security controls that rely on client-side rendering or cookies (i.e. CAPTCHA-based bot detection).
Most suited for	Apps prioritizing speed, simplicity, and managed authentication (e.g. SaaS apps, third-party apps, teams with low-code preference)	First-party applications (web, mobile, agentic) where authentication is tightly coupled to conversion-critical user journeys

You don't have to choose one.

Applications can mix Universal and Embedded Login within the same tenant, or even within the same app. For example, use a refresh token issued by Universal Login and perform step-up over an embedded API, or transition between native and web sessions using Native to Web SSO.

Visit our guide to evaluate which Embedded Login vs Universal Login features align with your roadmap goals.