5 Principles for Building Highly Scalable and Successful Apps

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Chances are, your app's features and designs look and function a lot different today than when first released. This is par for the course in today's digital environment: the success of any application relies on its ability to adapt and grow along with customer needs—which are constantly evolving. As such, the app you first release is simply a starting point; one that needs the proper foundations to support developers and users as it evolves.

While you can't predict future needs or opportunities, you can build your application with scalability and identity at the core. This approach allows you to move quickly and easily respond to customer requirements—whether it's a brand new use case or added features—while keeping the experience seamless and secure for everyone.

With all of this in mind, here are five principles that can help your developers build highly scalable apps while also creating identity experiences that customers trust and enjoy.

1 Build on open standards

Before your developers can begin building an app, you need to determine which identity standards make the most sense. This will help you create a truly cross-channel strategy—one with consistent support for your developers and use cases.

Companies often start with just a few standards and protocols—OAuth 2.0, OpenID Connect (OIDC), SAML 2.0, and SCIM are among the most common—and then adopt others (e.g. social and passwordless authentication, FIDO2, WebAuthn, and Webhooks) as they scale their applications for new users and markets.

These identity standards can be pivotal in reducing your time to market and minimizing your dependence on original developers. For example, let's say your company has a simple web application, but plans to add additional mobile apps next year. As part of your security and identity strategy for the app, your team adopts OAuth 2.0/OIDC and uses JSON Web Tokens (JWTs), signed objects/payloads holding claims such as user data, to authenticate and authorize users in a secure manner.

Since JWTs are an open standard, developers can choose among various libraries to create, verify, and inspect these tokens. The mobile experience team can then use the same resources and code bases that operate with OAuth/OIDC/JWT, without having to deal with the web development team. This helps keep your company agile, and allows you to bypass some of the obstacles that typically hinder app development.

Benefits of using open standards

- Lowers overhead costs due to minimal refactoring
- Enables more agility and reduces time to market
- Streamlines authentication experiences across your applications
- Contributes to seamless and secure user experiences
- Attracts new customers and increases customer retention
- Increases customer trust in your app and your company

How Okta can help

Okta SDKs and APIs enable companies to authenticate their users with numerous standards, such as OIDC and OAuth 2.0, which eliminates the need to build and maintain the support within your platform. This also allows developers to focus on core business objectives and increase productivity instead of sinking resources into complex identity solutions.

Of course, as with other technology solutions, identity standards are always changing. Okta keeps up with these updates by deploying 48 releases per year, which makes it easy for our customers to adopt the latest protocols as they release new products and update the functionality of their apps.

2 Centralize user stores

Applications are often rolled out with their own unique, separate customer data stores, which can be the root of several problems. For one, managing multiple repositories can be both error-prone and costly for developers—but it may also impact the overall user experience. When customer data is siloed across different applications or components of a platform, for example, it can hinder their ability to access accounts and services.

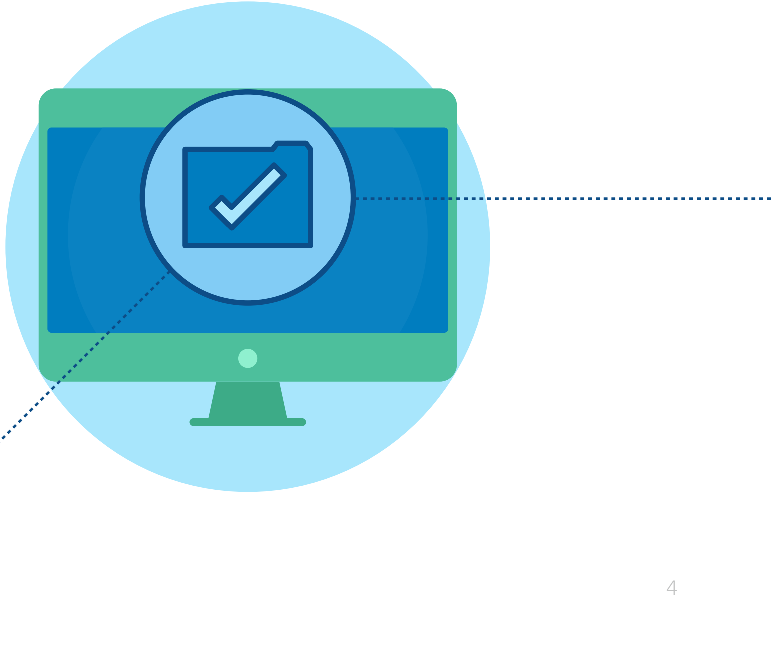
Because customer data is key to delivering relevant content and enticing offers, multiple user stores also make it challenging—if not impossible—for a company to get a full picture of its customers' unique needs. In a time where personalization is a key customer offering, this could result in retention issues, ultimately inhibiting a platform from scaling.

The core purpose of a basic user store is to act as a repository for your user identities and credentials. But doing this in a safe and reliable way can be quite complex: to protect users' accounts, your developers need the tools to encrypt data at rest and in motion, hash passwords, manage password complexity, reset passwords, and unlock accounts, among other things. For repositories that contain additional information, such as roles and permissions, businesses also need a way to organize that data and transmit it to applications.

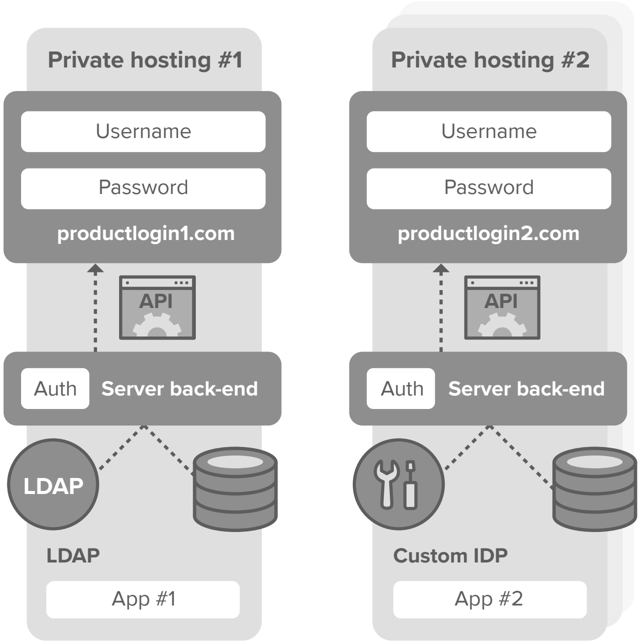
By centralizing user stores, you can present a 360-degree view of your customers both internally to employees and externally to partners. This streamlined approach to user management can make it easier to scale, as you can always access the same set of identities and credentials.

Best practices for centralizing user stores

- Keep original credentials
- Reuse other data, regardless of a new schema
- Centralize as much as possible to reduce application dependencies

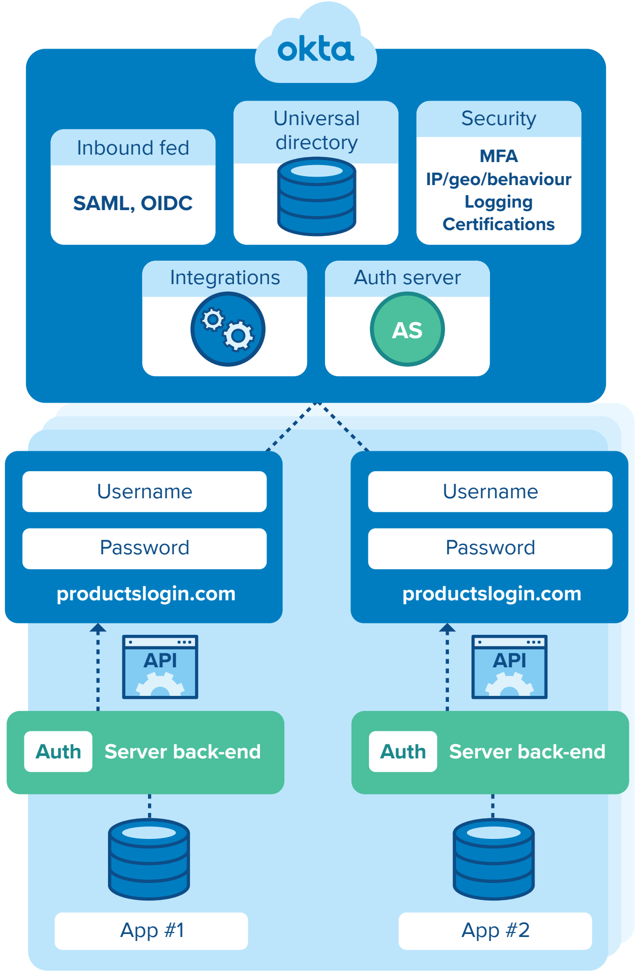


Identity Tech Stack Before Okta



Every app has its own identity stack

Identity Tech Stack with Okta



How Okta can help

With Okta, your company can focus on business growth and excellent customer service, instead of the time-consuming task of managing user stores. Our centralized console allows security and administrative teams to oversee user permissions and security policies, freeing up much of your developers' time.

In addition, Okta handles the high availability, disaster recovery, and security of user information and helps to ensure your applications and data practices comply with the GDPR, CCPA, HIPAA, and other regulations. Our user management capabilities are also exposed by well documented REST APIs and management SDKs, which further help your team speed up deployment and innovation by transferring the burden of documentation and management to our service.

3 Meet customers where they are

Customers have shorter attention spans and higher expectations than ever before. They want simple, personalized experiences tailored to their unique needs —and are quick to judge when a product or service doesn't quite hit the mark.

While it may seem daunting to create experiences that are as seamless as those offered by Netflix, Amazon, and Facebook, technology and identity standards are constantly changing. And that means there will always be new ways to engage with customers and earn their trust from the very first time they interact with your brand and throughout their entire customer journey.

Onboarding, for example, should be as streamlined as possible. When a customer starts using your application, it's essential to demonstrate how much you understand their needs—security and otherwise. Gathering as much information from them as possible is one of the best ways to gain more insight into their preferences. However, each new input adds an additional point of friction. By carefully considering each step in the sign-up process, your company can deliver the safe and enjoyable experiences that customers want.

To meet customers where they are, many companies apply a "digital front door" approach and make their applications accessible through social sign-on solutions. This not only creates a more seamless experience, but also allows customers to manage their own profiles and passwords—instead of relying on organizations and developers to troubleshoot. Identity providers such as Okta can also relieve you of burdensome activities, like performing password resets and account linking.

In conjunction with centralized user stores, adopting these solutions can enable you to surface attributes or information about a user at any time, reducing friction, simplifying the administration experience, and keeping your developer teams agile.

How Okta can help

Generic OIDC, one feature of Okta's out-of-the-box federation support, allows customers to sign in and/or register with third parties such as Microsoft, Facebook, or Google, as well as use existing credentials from any OIDC or SAML identity provider. By combining these integrations with Okta's extensible user store and profiles, you can customize attribute mappings and other rules based on the federation provider. The result? Customer onboarding and administration turn into a frictionless self-serve process.

4 Open up your ecosystem

To achieve real scale, your company must be able to quickly move in the direction the market requires. This can mean adding more features, accommodating more users, or adding more use cases. Often the stumbling block for this is a closed system, which means internal teams, partners, and even customers cannot access your APIs or code. By creating a clean, open platform for your internal, or even external development teams, future teams can more quickly and effectively adopt your identity service, making it easy for devs to scale your product.

In an open ecosystem, developers must be able to:

1. Quickly register to a selection of APIs with scoped access
2. Authenticate to the API or application and start interacting with your API

To do this, companies must securely manage developer credentials, such as API keys and user accounts and authorize with different permissions, in both single-tenant and multi-tenant architectures.

For example, you can give internal teams access to create applications with the scope of modifying internal users and configurations. At the same time, you can restrict developers from modifying customer-based resources.

For platforms offering an external API, the next step is to properly gate and monetize access to premium resources—all while reducing barriers to entry for external developers. Companies such as Salesforce, Expedia, and eBay successfully use this model. Companies not monetizing APIs will likely struggle to keep up with competitors taking advantage of this lucrative opportunity.

While opening your ecosystem might seem counterintuitive to growing and scaling, this approach can lead to new products, increased usage, and opportunities for new revenue streams. What's more, by providing easy and scoped access to your APIs for internal teams, partners, and external developers, you can expand your ecosystem more securely.

How Okta can help

Our API Access Management solution is designed to protect any number of backend APIs and tightly scope different levels of access to each. On top of that, you can develop a more comprehensive API strategy by adding features—such as API monitoring, throttling, and logging—by integrating with several API gateways.

Furthermore, our delegated administration structure improves internal development by allowing different internal teams to have tightly scoped permissions. By using this for specific individuals, you can open up areas of the platform for development. Finally, Okta lets you act as an identity provider, allowing external developers to authenticate their apps against your platform and therefore add users to your ecosystem.

5 Prioritize Security

The internet is a fantastic place, but it can also be a scary one; the media is constantly reporting on data breaches, hacks, and other cyber security attacks. This growing number of potential threats and vulnerabilities has put security and privacy at the forefront of everyone's mind.

- Companies worry about the cost of recovering from a cyber security attack, as well as the often unrecoverable damage an incident can cause to their reputation.

- Customers understand the risks of unprotected data, and are starting to carefully consider security when choosing products and services.

Each time you create a connected app, your company is exposed to software-layer attacks on the web. But the hardware layer is also open to vulnerabilities on desktop and mobile devices. While it's impossible to build a service that's immune to all attacks and vulnerabilities, you can build apps that are prepared to handle and withstand these threats—something customers both expect and appreciate.

The key to improving security and reducing risk is building security into your apps from the beginning.

In addition to making apps highly scalable, the strategies mentioned above—building on open standards, centralizing user stores, and meeting customers with federation—all add an additional level of security:

- With open standards, the evolving protocols quickly patch any new vulnerabilities. Once the protocols are updated, any security issues in your app due to the standards are automatically resolved. Your developers are no longer responsible for identifying, tracking down, and fixing every security issue.

- When user data is stored in one centralized place, cyber criminals have fewer entry points to attack.

- Identity federation reduces the burden of storing sensitive credentials and potential user data. Additionally, by using third-party authentication providers, critical parts of your app are maintained by leading security experts and regularly monitored.

Beyond these approaches, there are a few things you can do to actively secure your application:

- **Gather and use as much context as possible to enrich access decisions.** If your app makes an access decision with a single piece of information, such as a password, the likelihood of unauthorized access increases. By using multi-factor authentication (MFA), you can supplement logins with additional context, such as geo-location, device fingerprint, or IP address.

- **Develop a robust logging and monitoring service with integration in mind.** This should contain all the context listed previously; it should also be flexible, exportable, and capable of keying off certain events to send Webhooks to downstream services such as SIEM or CASB. Building in this way will future-proof your platform as security concerns arise.

How Okta can help

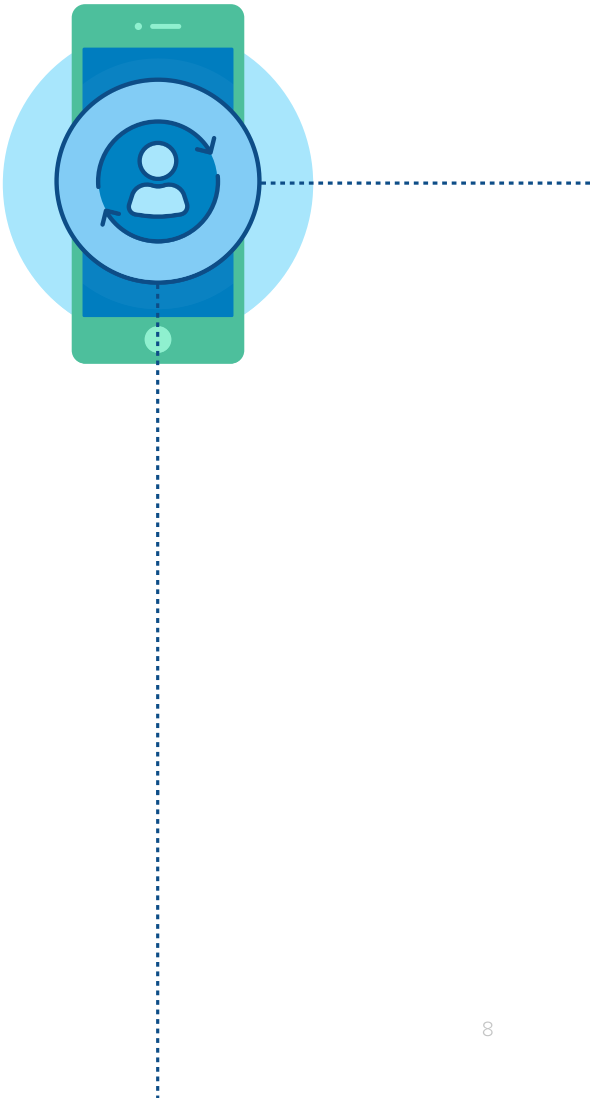
Okta's suite of security tools can log and capture verbose information about every access request, configuration change, and user action. Those logs are then exposed using APIs and Webhooks. Once the risk of a given login request is assessed, the user may be prompted to input additional information through our Adaptive MFA solution in order to validate their identity.

To reduce manual coding, we also include out-of-the-box security integrations with numerous security tools, from identity proofing to threat identification and response. In addition to logging and monitoring, Okta's ThreatInsight tool preemptively blocks numerous malicious requests, allowing you to easily enrich your user access decisions through adaptive policies.

Building scalable apps for today and tomorrow

Each of the five principles mentioned above can help organizations build highly scalable and successful applications—especially when used together. More than simply applying these principles, however, it's important to ensure that each is tailored specifically to your application to help prevent commoditization, and make your app truly stand out in the market. Only by putting scalability and identity at the core of your strategy, can you build an app that will exceed user expectations today and in the future.

To learn more about how Okta can help you build highly scalable and secure applications, get in touch.



okta