Securing Digital Business with API Access Management

Okta Inc.
100 First Street
San Francisco, CA 94105

Every Organization Goes Digital

While the API Economy and Digital Transformation are buzzwords that have been thrown around for a decade, successful organizations have mapped them into a few core concepts: APIs, devices, and data.

The first involves the massive mountains of data enterprises have collected in their systems of record. The API Economy is enabling organizations to turn that data into improved operations, better services, and completely new products. Using APIs, an enterprise can customize and move the data analysis and therefore the decision making from the highest levels of the organization directly to the department, division, or even the project that needs it in the form they need it. When the same data applies outside the enterprise, APIs allow the organization to put the power in the hands of customers and partners.

The next aspects are client applications and devices. While most organizations planned their systems and operations around a web browser on a computer in the office, modern clients are more complex, more flexible, and less static than ever before. When a customer moves from their desktop at the office to their phone during their commute home to the smart TV in their living room, a unified and consistent user experience becomes vital. The hidden aspect is that the same service is used in fundamentally different ways at every step on every device.

The third and most complex aspect is the sheer volume of data created and where it resides. Your browsing activity is the simplest scenario. As we consider the Internet of Things (IoT) and authenticate into a device that isn't ours or is shared among numerous users, the lines become blurry to the point of being invisible. This unclear ownership requires Identity and Access Management (IAM) solutions to track, control, and even destroy that data as relationships and context changes between ourselves and our devices.

With this data and the explosion of clients, there's also a loss of control. Some of surrender of control is purposeful where we want to give flexibility and power to our teams, partners, and customers to accomplish their goals. Unfortunately, the rest is by accident where our APIs often lack the same security practices and policies that govern the rest of the organization. Gartner predicts that by 2022, APIs will be the leading vector for data breaches but with the successful attacks on credit reporting agencies, travel companies, dating websites, and even government agencies, 2022 may be optimistic.

The Technology Revolution Supporting Mainstream Digital Business

At the foundation of this shift in approach to business, is truly a revolution in application development. The leaders in consumer technology, including Apple, Google and Facebook, started a revolution and introduced new ways to build web and mobile applications. This technology is now driving any organization that needs to innovate more quickly. While there are more developers than ever, the tooling and services they can call upon and build into an application with a few lines of code is staggering.

As these trends continue, concepts that are hard today become APIs and packaged components tomorrow. Further, some of those packaged components become easily configurable where it doesn't take a developer to wire, build, and deploy business logic. Managing and customizing packaged software becomes easier and more focused on your core competencies as you use SaaS or a PaaS to build custom applications.

The previous generation of web software started roughly 20 years ago with web application servers based on Java or .NET. One hundred percent of the code ran on the server and your browser simply displayed the HTML sent from the server. In the new world, you have mobile apps on your smartphone or "single page apps" running in your browser that run code on the device or client-side. These apps connect to backend services, generally exposed via an API. The backend services might simply be a source of data or execute additional complex processes but this is transparent to the client application.

While this is the external view of the application, once we look inside, the same decentralized or service-based model applies. A loose coupling of different services and applications running that handle small tasks, and call each other's APIs to interact. This is often referred to as "microservices." The end result – your developers can be an order of magnitude more productive and solve problems that were considered complex last year.

In concrete terms, a developer can plug Platform-as-a-Service offerings such as Twilio for SMS, Stripe for credit card transactions, and Okta for Authentication, Authorization and User Management into their projects in minutes and accomplish huge tasks with a few lines of code.

API Access Management: Securing Modern Applications

As we open our systems to internal teams, partners, and customers, we still have to take security into account. The web application model of using cookies and sessions is insufficient here as backend services and applications don't necessarily have a browser. The next model of SAML to accomplish user federation and Single Sign On (SSO) is the beginning of the right concept but – as noted above – we don't always have a user. IoT devices and backend services could act on their own behalf. The new application architecture required a new way to authenticate both users and systems and providing an approach for granular access management for specific use cases, context, and scenarios.

Enter OAuth 2.0 and OpenID Connect

OAuth 2.0 provides an authorization framework that is both flexible and extensible while still allowing for centralized control and management. The single most important part are the extensions which provide consistent models for authenticating and authorizing users, applications, services, and even devices. This ensures interoperability between infrastructure components such as API gateways, application frameworks such as Spring or Laravel, and application libraries such as AppAuth with no explicit collaboration.

One of the most important extensions is OpenID Connect. While OAuth 2.0 itself is a flexible framework, OpenID Connect is a strict contract that specifies a user's profile and the data which should be within it. This provides a nearly 1:1 replacement for SAML for SSO use cases. Further, since this specification received early and widespread support from companies such as Google, Facebook, LinkedIn, and Okta, it has emerged as the modern de facto standard for single sign on across the internet as a whole. Okta Single Sign On supports both SAML and OpenID Connect to bridge these two worlds seamlessly with minimal configuration required.

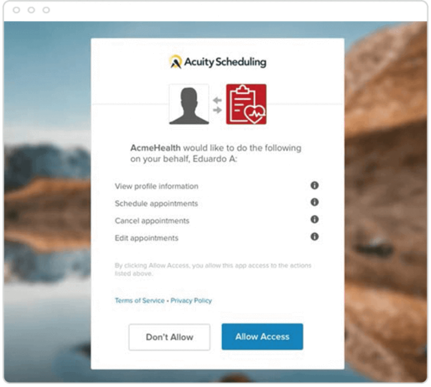
Okta API Access Management goes a step further implementing numerous OAuth 2.0 extensions to provide a consistent and predictable authorization layer for any user and any service to access the services and systems necessary regardless of the language, framework, or architecture.

API Access Management Product Features

Okta API Access Management provides identity-driven authorization for any app or service, with user-friendly and centralized administration across all your APIs.

OAuth 2.0 API Authorization

- Designed for modern web and mobile applications, and service-to-service scenarios
- Provides standards-compliant support for OAuth 2.0 and numerous extensions
- Implements OAuth-compliant token introspection and revocation
- Demonstrated out of the box integration with numerous 3rd party API management solutions and API gateways
- Supports explicit User Consent to better comply with data protection and privacy regulations such as GDPR and CCPA



Acuity Scheduling

AcmeHealth would like to do the following on your behalf, Eduardo A:

View profile information

Schedule appointments

Cancel appointments

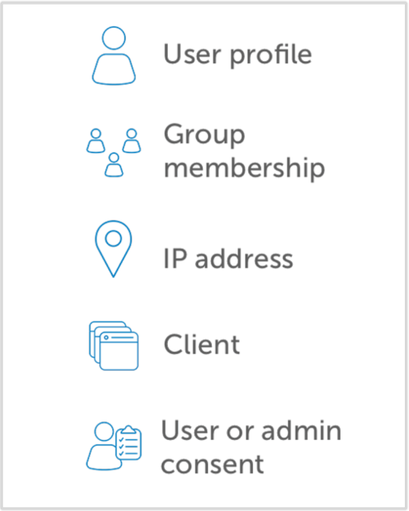
Edit appointments

By clicking Allow Access, you allow this app access to the actions listed above.

Flexible Identity-Driven Policy Engine for Any Type of User or Service

- Provides flexible policies built on Okta Universal Directory to allow authorization policies based on user profile, group membership, on/off network status, client application, and user consent
- Integrated with the core Okta API to support user management, group membership, provisioning, and all API-supported actions
- Allows configurable access token and refresh token lifetime to customize per use case
- Integrates with internal systems via a simple Hooks model to retrieve sensitive or dynamic data or additional entitlements for downstream applications

Define access policies by



Easy and Centralized Administration Across All Your APIs

- Purpose-built, user-friendly console for consistent creation, maintenance, and audit of API access policies based on native identity objects without any custom code
- Integrated with the overall Okta System Log to provide a single interface and integration point for downstream Security Information and Event Management (SIEM) systems

Summary

Organizations large and small, public and private are building and depending on APIs more and more every day. While they support the immediate goal of mobile applications and reusable components, they also create and solve use cases that we do not imagine at the onset. Fundamentally, while we want our teams, partners, and customers to innovate and explore new problems and markets, we still need to protect our organization, the data we're entrusted, and the systems which support everything. A strong, standards based approach using OAuth 2.0 and OpenID Connect backed by a single source of truth and integrated with our existing security operations is the only way to secure ourselves, enable our partners, and protect our customers. Okta API Access Management built on Universal Directory is a scalable and proven combination currently in use by JetBlue, Allergan, Dignity Health, and Pitney Bowes.

For Further Reading

- Okta's guide on Building Secure APIs [book] [website]
- OAuth 2.0 Simplified by Aaron Parecki
- Authorization Product Overview
- JetBlue Case Study
- Allergan Case Study
- Dignity Health Customer Story
- Pitney Bowes Case Study
- Okta Integration Network: API Gateways
- Recommended Practices for API Access Management