okta

Securing Digital Business with API Access Management

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

API Access Management Overview

Every Organization Goes Digital

Most growing, successful organizations are actively building their digital strategy to take part in the API Economy. Enterprises have built mountains of data over the last decade in their systems of record. The API Economy is enabling an enterprise to build a business around that data, selling the data directly or providing a digital service to customers or partners.

Data is one side of the equation, the other is the clients or devices. Enterprises are thinking about all the different kinds of options for modern clients. When these clients move from being your smartphone to being a connected car or refrigerator, we enter the realm of the Internet of Things (IoT).

There are two IoT access management problems – device to service and user to service to other services. Device to service is straightforward, and mainly about simply authenticating the device, or application running on that device.

User to service to other services is much harder. There will be a growing tsunami of user data with unclear ownership. IAM solutions will need to manage the complex relationships between entities and resources and data access rights. For example, if you stay in an AirBnB, who owns the data that's generated while you watch Netflix there, or your WiFi usage patterns?

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 this revolution and introduced new ways of building web and mobile applications. This technology is now reaching any organization that wants to innovate more quickly. Developers are on the rise both within and outside of IT as higher level technologies enable any knowledge worker to become a developer in 5 years. Developer tools will be easy for anyone to write business logic. Managing and customizing packaged software goes away. You either use SaaS, or you use IaaS and increasingly PaaS and modern dev tools to build custom apps.

The previous generation of web software started roughly 20 years ago with web application servers based on Java or .NET. The software all ran on the server, and your web browser simply displayed the web page based on the HTML sent to it from the web 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 then connect back to backend services, generally exposed via an Application Programming Interface (API). The backend services might simply be a source of data, or, they could go off and run an additional process.

Taking this a step further, all software is evolving to this more decentralized model. 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 – developers can be an order of magnitude more productive.

You can quickly spin up new customer experiences in a fraction of the time it would have taken to build an entire web stack of the past. Platform-as-a-service offerings (such as Twilio for SMS or Okta for Authentication, Authorization and User Management) easily plug into your development projects to get them going even faster.

API Access Management: Securing Modern Applications

API Access Management is the next generation of access management technology that supports modern applications.

The first generation of access management used HTTP headers to maintain your session in a web browser. The second generation added federation with standards like SAML, that allowed one system to authenticate a user, then pass that user off as a “trusted” user to another application on another domain. This powered single sign-on for web applications across different domains and SSO for SaaS applications.

With a new application architecture emerging, there is a need for a new way of authenticating users and granting users and applications access to backend resources. And, going a step further, all the different “micro” components of the microservices landscape need to get authenticated. You need a centralized security authority to manage access across all these systems and ensure data is not exposed or the front door to an application isn’t left unlocked.

Okta Single Sign-on supports OpenID Connect, which provides basic authentication in this new world, enabling users to authenticate to modern mobile apps and single page web apps.

Okta API Access Management goes a step further, providing the authorization layer for apps to access data from backend services, and for any service to access any other services across a microservices architecture.

API Access Management Product Features

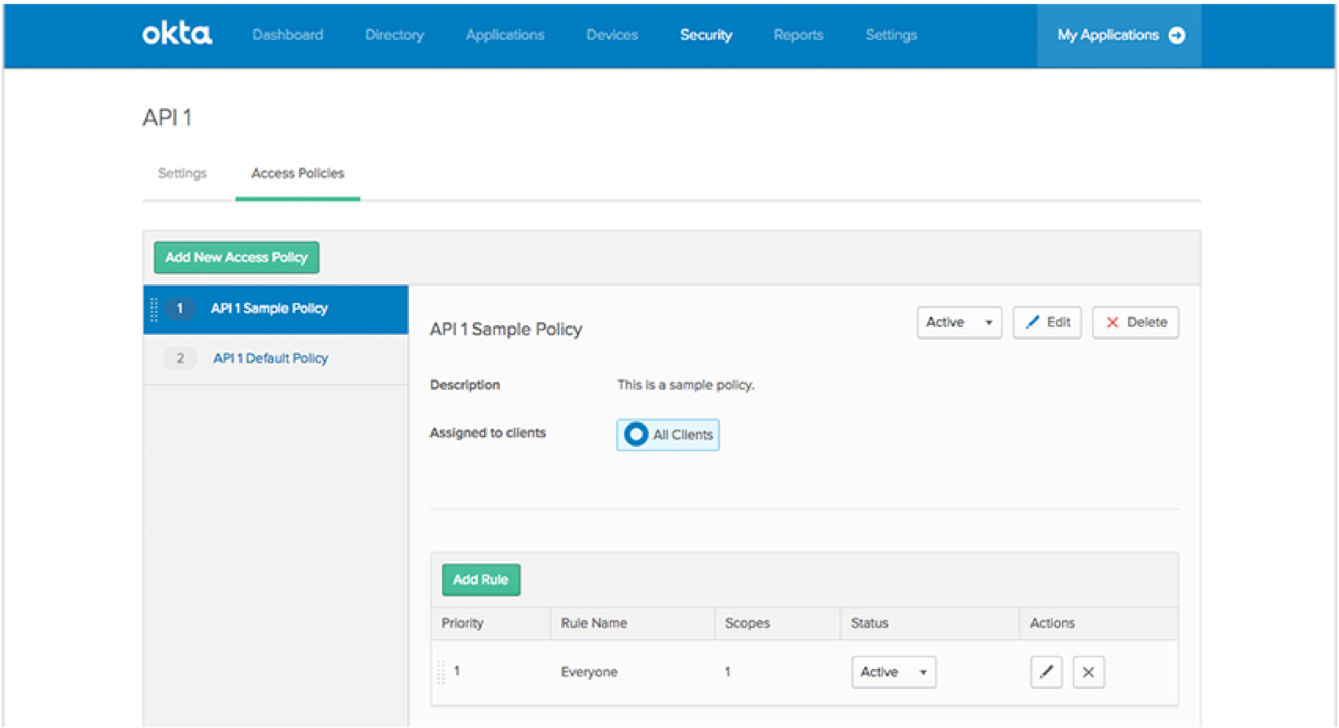
Okta API Access Management provides identity-driven authorization for any app or service, with user-friendly and centralized administration across all your APIs.

OAuth 2.0 API Authorization

- Complete standard-compliant support for OAuth 2.0
- Proven compatibility with 3rd party API management solutions
- Designed for modern web and mobile applications, and service-to-service scenarios

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

- Flexible policies that define access based on user profile, groups, network, client, and consent
- Instant access revocation or updates to user permissions based on user profile and status



API 1

1 API 1 Sample Policy

2 API 1 Default Policy

API 1 Sample Policy

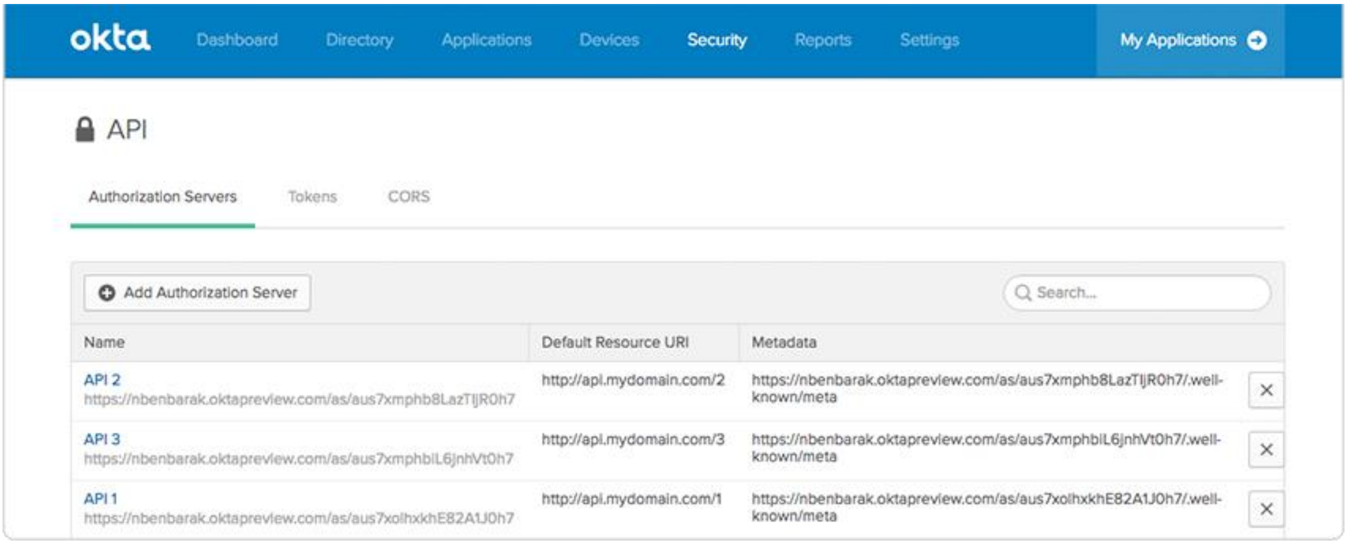
Description: This is a sample policy.

Assigned to clients: All Clients

Priority	Rule Name	Scopes	Status	Actions
1	Everyone	1	Active	

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.



API

Name	Default Resource URI	Metadata
API 2 https://nbenbarak.oktapreview.com/as/aus7xmphb8LazTIjR0h7	http://api.mydomain.com/2	https://nbenbarak.oktapreview.com/as/aus7xmphb8LazTIjR0h7/.well-known/meta
API 3 https://nbenbarak.oktapreview.com/as/aus7xmphbiL6jnhVt0h7	http://api.mydomain.com/3	https://nbenbarak.oktapreview.com/as/aus7xmphbiL6jnhVt0h7/.well-known/meta
API 1 https://nbenbarak.oktapreview.com/as/aus7xolhxkhE82A1J0h7	http://api.mydomain.com/1	https://nbenbarak.oktapreview.com/as/aus7xolhxkhE82A1J0h7/.well-known/meta