Okta + MuleSoft®

Okta and MuleSoft: Comprehensive API Access Control and Management

API creation and adoption are having a moment. As of January 2018, there are nearly 19,000 public APIs in ProgrammableWeb's API directory. According to recent research, 94% of companies say they either have or are developing an API strategy. APIs are now seen as an enterprise necessity.

Key to an effective API strategy is a thoughtful approach to API security. As the most valuable APIs often contain sensitive business information, the consequences of getting API security wrong can be significant. It's critical, therefore, to implement a scalable, flexible, future-proof solution that enables secure management and access control to your APIs.

Okta, the leading independent provider of identity for the enterprise, and MuleSoft, provider of the leading hybrid integration platform, have partnered to help enterprises get API security right. With the Okta and MuleSoft solution, you can securely connect all your apps, devices, and users via APIs. Out-of-the-box integration between Okta and MuleSoft gives you agility and comprehensive security, so you can innovate at the speed of digital business.

For example, a major software vendor wanted to enable its developers with access to data through a developer portal, but realized those developers had access to sensitive information like compensation data via unsecured APIs. By deploying the Okta and MuleSoft solution, the vendor was able to empower their developers with fine-grained access to only the right data contained within their APIs.

The Solution

The Okta and MuleSoft solution combines Okta API Access Management and MuleSoft's Anypoint Platform. MuleSoft's

Anypoint Platform delivers integrated capabilities across the full API lifecycle. Okta API Access Management provides easy, centralized, identity-driven access management for all of your APIs and all your users.
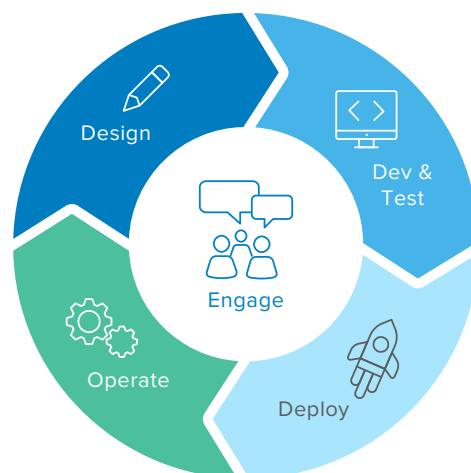
Full API Lifecycle Management with MuleSoft's Anypoint Platform

With MuleSoft's Anypoint Platform, organizations can design, develop, test, deploy, and operate APIs on a single solution, with tools optimized for different personas throughout the lifecycle. Having this broad set of capabilities available on one platform increases the fungibility of developer resources, decreases complexity in securing and deploying applications and APIs, and accelerates time to value.

Anypoint Platform enables app users and API developers to proxy existing APIs with a few clicks, apply security

policies, and engage API consumers with customizable portals. New APIs can be designed and implemented in hours with pre-built templates, application connectors and other reusable building blocks. Once deployed, operators have full visibility into utilization metrics and can create dashboards to measure performance against key business KPIs. Finally, Anypoint Platform is built with a consistent codebase across on-premises, public and private cloud, enabling customers to consider hybrid implementations in multiple configurations.

API Access Management is a Pillar of API Management

Full Lifecycle API Management				
Lifecycle What state is this?	**Interface** What does it expose?	**Access** Who can use it?	**Consumption** How to succeed with it?	**Business** How does it drive business goals?
• How was it designed? • How was it built? • Is it deployed? • To which GWs? • Is it live/available?	• Which resources? • Which methods? • Which objects? • Which fields?	• Which users/ groups? • How do they authenticate? • Using with clients? • In what contexts?	• API Documentation? • Debugging/errors? • Track usage? • Examples/SDKs?	• Partner CRM • Monetization • Marketing • Business Analytics

Okta API Access Management

Okta centralizes all the users and resources that access APIs designed and managed by MuleSoft's Anypoint Platform. This solution offers out-of-the box integration, standard compliant support for OAuth 2.0, a flexible, identity-driven policy engine, and easy, centralized client administration across APIs.

You get fine-grained, centrally-managed access control to all your APIs, so you can easily provision and deprovision them as part of your onboarding and offboarding processes.

When you deploy Okta with MuleSoft, you can:

• **Define access** with flexible policies based on user profile, groups, network, client and consent

• **Update or revoke access** to APIs instantly with user permissions based on user profile and status

• **Provision API access** as easily as you provision application access

• **Create, maintain, and audit** API access policies from one user-friendly console—with no custom coding required

How Does It Work?

The solution works as follows:

- In MuleSoft's Anypoint Platform, organizational administrators can configure Okta as an External Identity Provider from Anypoint Access Management. Once this configuration is complete, user enrollment and provisioning will be delegated to Okta. Then from Anypoint API Manager, users can apply an Okta OAuth 2.0 Token Enforcement policy on an individual API or set of APIs.

- An Okta Universal Directory stores users and provides comprehensive identity management capabilities, including group management, application/API provisioning, adaptive multi-factor authentication, and configurable authorization policies. As a certified OpenID Connect provider, Okta generates tokens with customizable scopes and claims which adhere to the OAuth 2.0 specifications.

- Okta's Authorization Server supports access and authorization policies which grant scopes and provide claims to specific users based on user attributes, group membership, elements of the user context, and even

the application itself. For example, you can grant the "api:write" scope only to members of the "editors" group only when they're using the desktop application.

- When consumers of your API retrieve access tokens, Anypoint Platform can validate those tokens (RFC 7519) and reject or process requests as appropriate.

The Technical Specs

Okta's API Access Management—more colloquially known as "OAuth as a Service"—uses the OAuth Framework (RFC 6749) with numerous extensions to build a robust solution that allows MuleSoft's Anypoint Platform to leverage Okta's authentication and authorization policies in minutes.

First, you set up the scopes within your Okta tenant and then you apply a policy from MuleSoft's API Manager to look for these scopes when a user presents an access token. Tokens containing the required scopes will be relayed to the protected API as designed. Tokens without the required scopes will be rejected according to the configured policies.

Authentication Flow
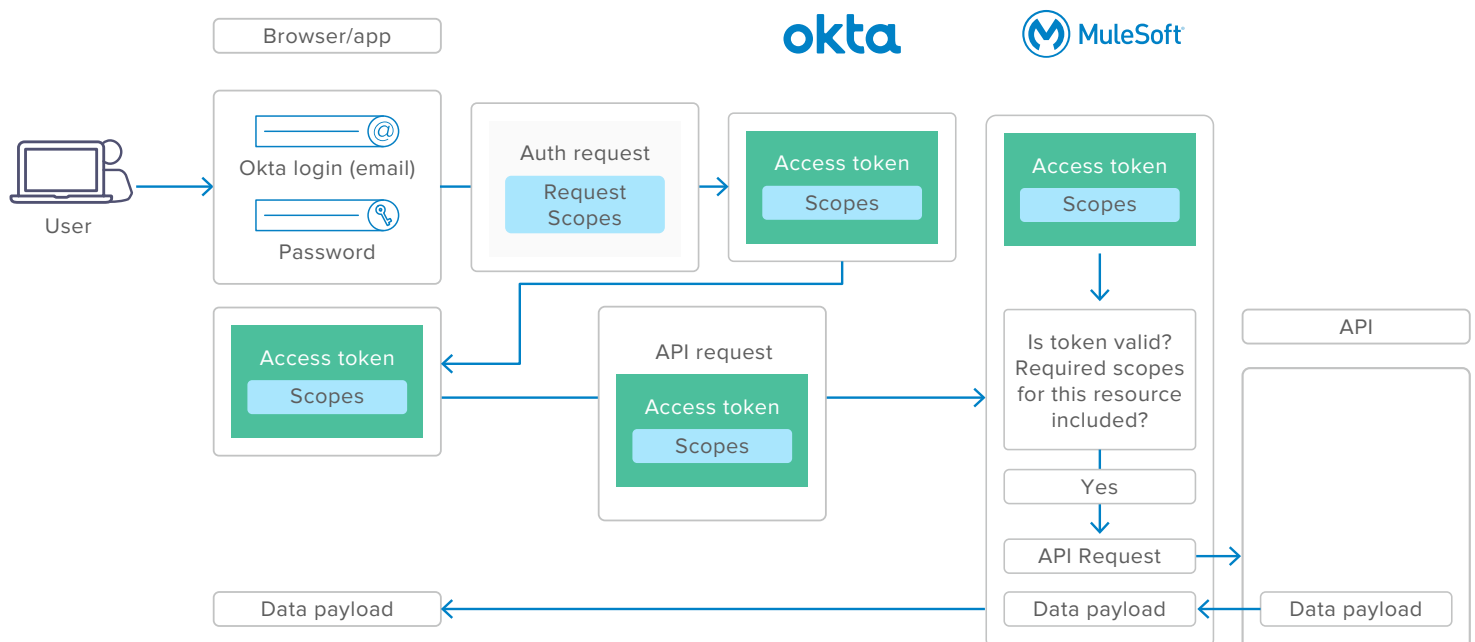
Dynamic Client Registration
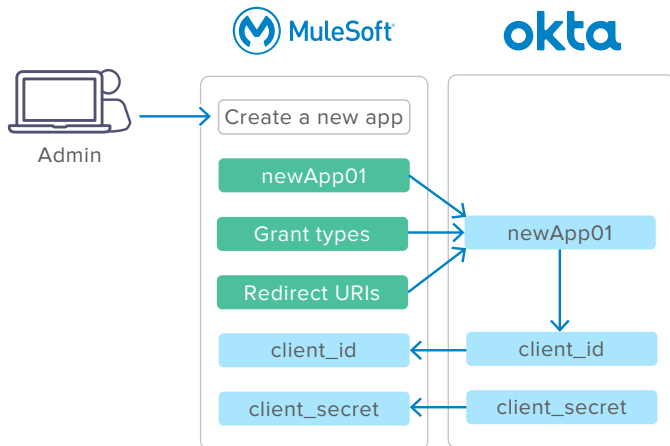
For initial provisioning, you can dynamically create OAuth Clients (RFC 7591) within Okta from the MuleSoft UI.

As in the specification, Okta generates a client_id and—if necessary—a client_secret for MuleSoft to return to the user for configuring their application.

Any user assigned to the OAuth Client can immediately authenticate, retrieve an access token, and make use of your API. Further, as their group membership and profile changes, the authorization policies and resulting scopes take effect on the next Refresh Token exchange without additional configuration.

Additional Information

Okta API Access Management:
https://www.okta.com/products/api-access-management/

MuleSoft API Manager:
https://www.mulesoft.com/platform/api/manager

MuleSoft Documentation:
https://docs.mulesoft.com/access-management/configure-client-management-openid-task