Technical Requirements Specification

for

App2RuleAPI

Version 1.0

Prepared by Amit Tarneja

18 September 2019

Table of Contents

Table of Contents ii

Revision History ii

1. Introduction 3

1.1 Purpose 3

1.2 Intended Audience and Reading Suggestions 3

1.3 Project Scope 3

1.4 References 3

2. Overall Description 3

2.1 Product Perspective 3

2.2 Product Features 3

2.3 User Classes and Characteristics 4

2.4 Operating Environment 4

2.5 Setup Instructions 4

3. Sample 4

4. Security Consideration 5

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
| Amit Tarneja | 18th September, 2019 | Initial Version | 1.0 |
|  |  |  |  |

# Introduction

## Purpose

The purpose of this document is to show the working of a GET API that can map the Auth0 Application and rules that are specific to that Application.

## Intended Audience and Reading Suggestions

The document is indented for all the staff members who will use these new REST endpoints.

## Project Scope

Currently, the Auth0 management interface can only show the Client specific Application and rules that exist in your account, but there is no interface to show the mapping between the Application and the specific rules that got created for it. Generally, the rules apply to all applications, until or unless you modify the script to run for a specific app.

## References

<https://auth0.com/docs/api/management/v2>

<https://auth0.com/docs/api/management/v2/tokens>

<https://auth0.com/blog/manage-a-collection-of-secure-api-endpoints-with-postman/>

# Overall Description

## Product Perspective

This API got built on top of the Management v2 API. To access the endpoint, we need the JWT token and the Auth0 domain to retrieve the information we are looking for.

## Product Features

Currently, we only developed a GET endpoint to map the Application and the specific rules, but it can further be enhanced to perform more functionalities (Creating/Updating and Deleting Clients/Rules).

## User Classes and Characteristics

The typical user of the system will be a Solution Architect who wants to understand the existing clients and the mapping of rules that existing in their environment.

## Operating Environment

For this to work, we need to have eclipse and Java installed on the system. Anyone can deploy this on any environment (on-prem or cloud) or can consume the service with a Node frontend.

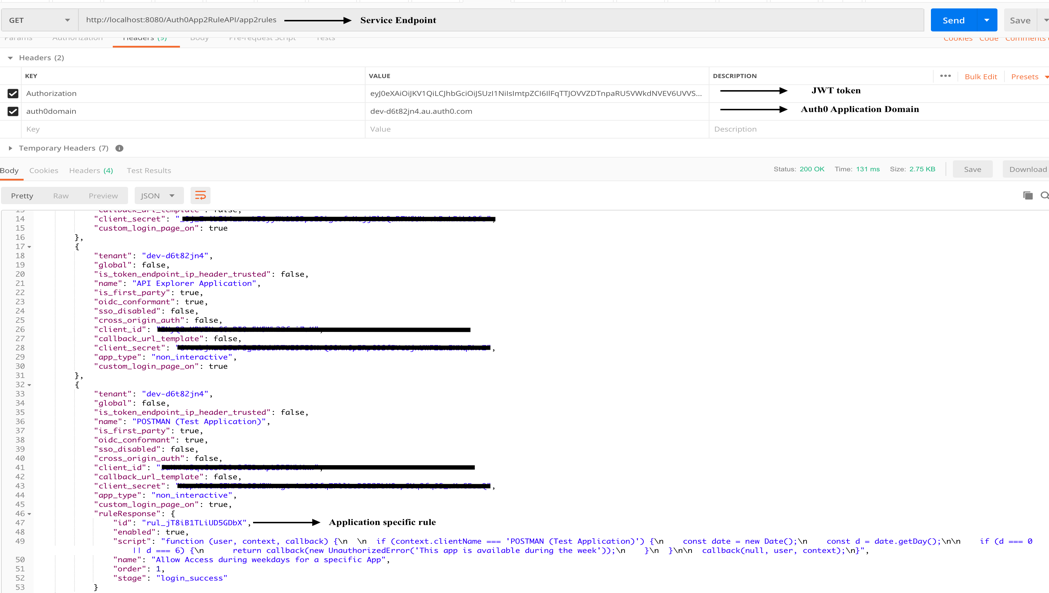
## Setup Instructions

1. Clone or download the code from the GitHub repository [https://github.com/amittarneja/Auth0App2RuleAPI](https://github.com/amittarneja/weather-rest-adapter).
2. Open the code in Eclipse and perform Maven clean/Install.
3. Right-click on the project -> properties -> Deployment assembly -> Add -> Java Build Path Entries -> Maven dependencies -> Apply and close. This step is to avoid the NOCLASSDEFFOUNDERROR exception.
4. Right-click on the project and select Run As -> Run on Server (I ran it on Apache Tomcat). Follow the instruction in the link to set up Tomcat in eclipse (https://help.eclipse.org/neon/index.jsp?topic=%2Forg.eclipse.stardust.docs.wst%2Fhtml%2Fwst-integration%2Fconfiguration.html).
5. Use your Auth0 API token and Domain URL to get the response from the Auth0 Management V2 API.
6. In the POSTMAN app, create a New GET request and fill the request information. Enter the URL as http://localhost:8080/Auth0App2RuleAPI/app2rules and Add the header information as shown in the Technical Specification Documents attached.

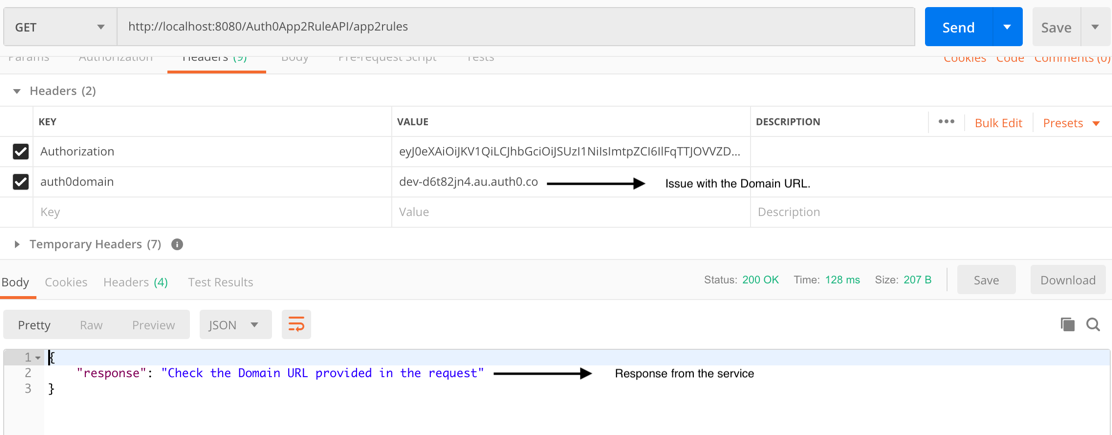
# Sample

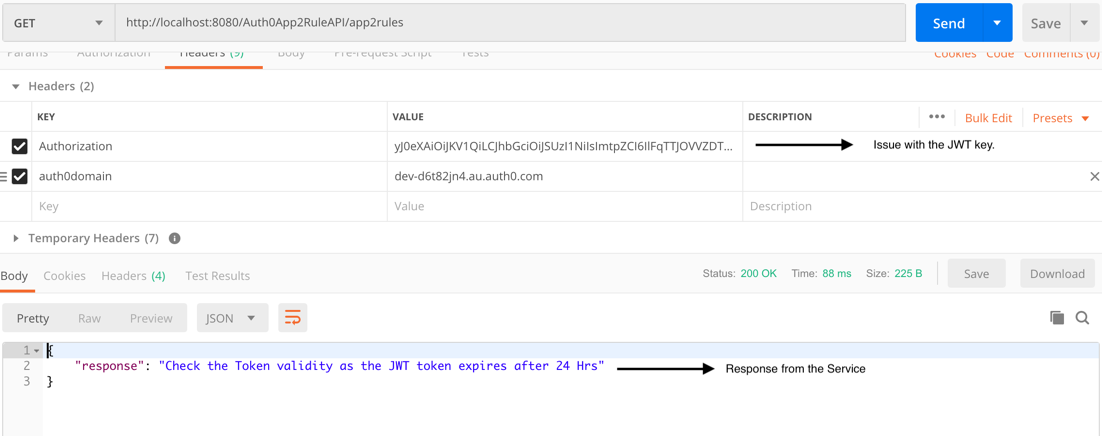
One of the benefits of using REST is that it is easy to test. There are several ways of testing a REST application, and I have used POSTMAN and the app deployed by Eclipse to validate the new API’s.

1. Open POSTMAN and create a new GET request to hit <http://localhost:8080/Auth0App2RuleAPI/app2rules>. Get the JWT token and Domain URL from your Auth0 account.



1. Below are a few exception scenarios where we have to take a look at our JWT token or Domain URL.



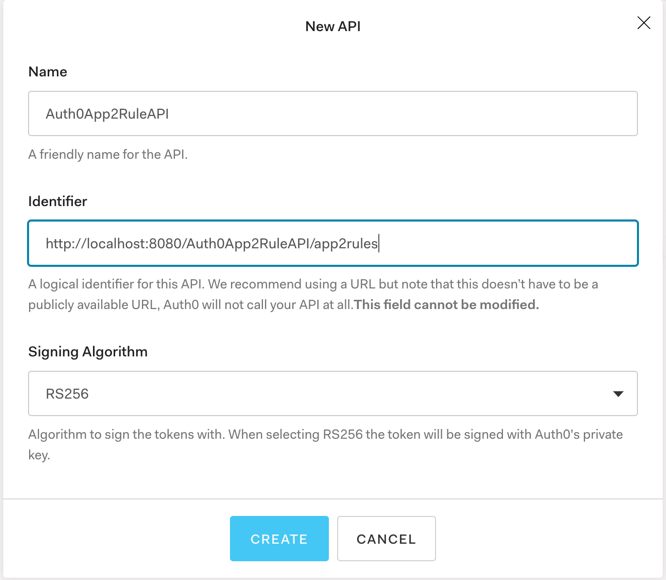


# Security Consideration

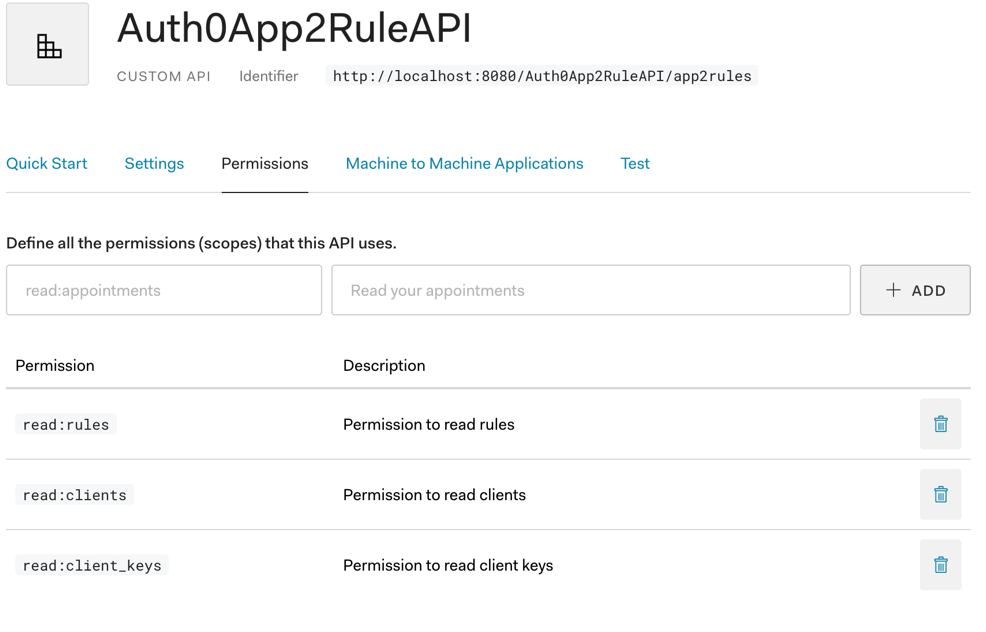
The below instructions can be used to create a whitelisted user that can use the application to retrieve the clients and rules. Auth0 interface provides a great way of authorizing users who can use the API and retrieve the information. This way, the Administrator can have control over the intended use of the information.

From the Auth0 dashboard, click on API on the left-hand panel. Click the Create API button.

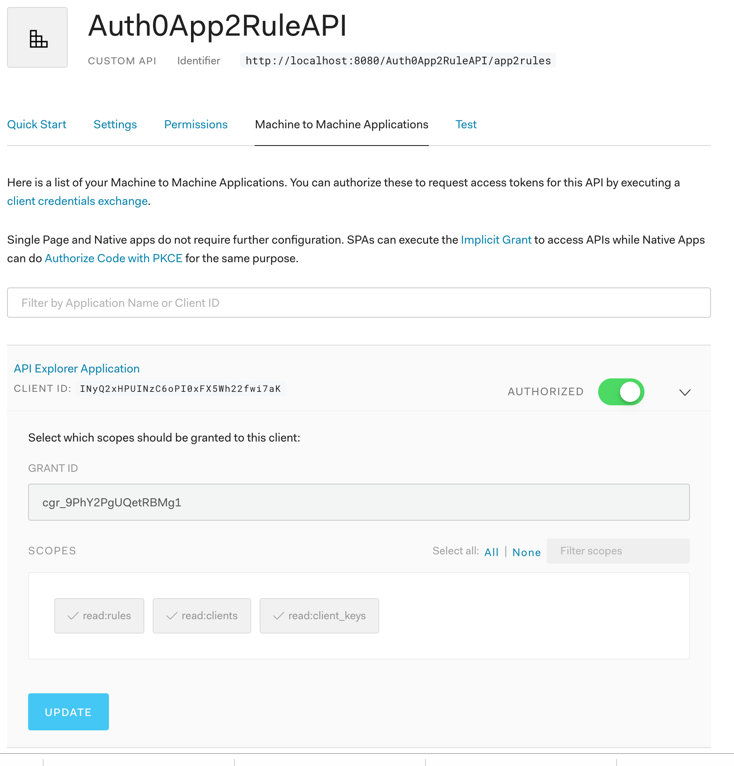
1. Fill the information to create a new API.



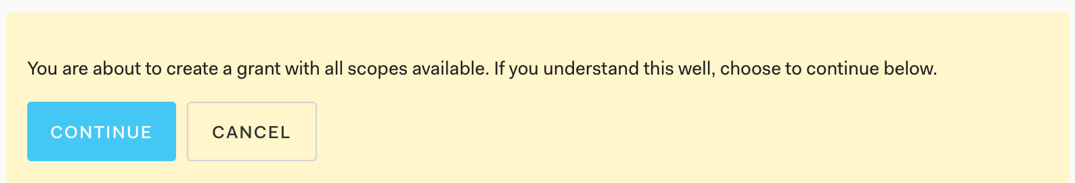
1. Click on the newly created API and add the desired permissions to the client.



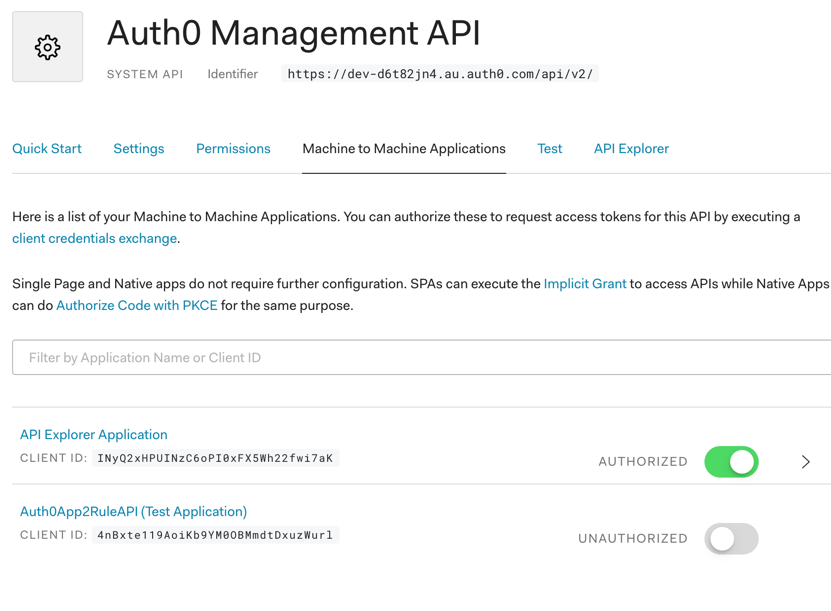
1. Authorize the API to view the Management API, and the request add the requested permissions. Click on the Update button.



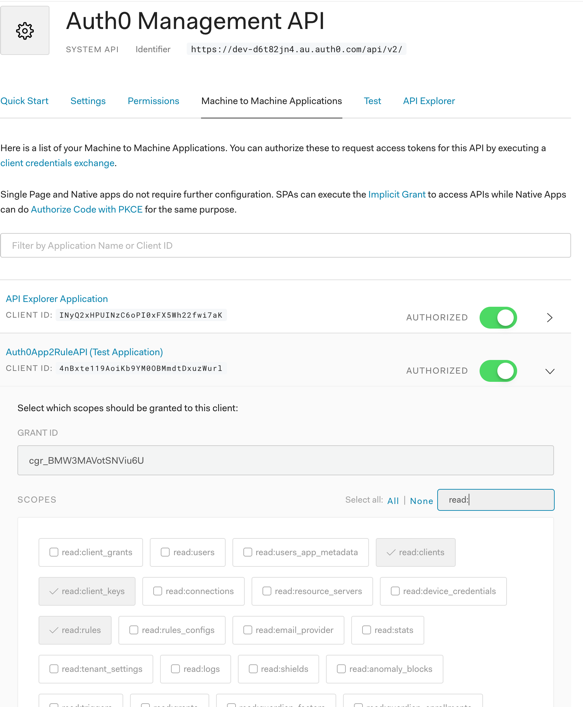
1. Click on the Continue button.



1. Go back to the API page and access the Management API and open the Machine to Machine Applications tab.



1. Click on the button to Authorize the API and add the below permissions to the API. Click on the update button.



7.Click on the Test tab and select your application from the drop-down. Copy the token from below to use as a JWT key.

