

Walkthrough 5-3: Restrict API access with policies and SLAs

In this walkthrough, you govern access to the API proxy. You will:

- Add and test a rate limiting policy.
- Add SLA tiers, one with manual approval required.
- Add and test a rate limiting SLA based policy.

The screenshot shows the API Manager interface. The top bar has the API Manager logo and user information. The left sidebar shows navigation options: Alerts, Client Applications, Policies, SLA Tiers, and Settings. The main content area shows the Policies page for the American Flights API (v1). It includes a table of policies with columns: Name, Category, Fulfills, and Requires. A policy named 'Rate limiting - SLA based' is listed under the 'Quality of service' category. Below this, a detailed view of the policy is shown with columns: Order, Method, and Resource URI. The policy is ordered 1, uses 'All API Methods', and applies to 'All API Resources'. There are buttons for 'View Detail' and 'Actions'.

Create a rate limiting policy

1. Return to the Settings page for your American Flights API in Anypoint Manager.
2. In the left-side navigation, select Policies.

The screenshot shows the API Manager interface. The top bar has the API Manager logo and user information. The left sidebar shows navigation options: Alerts, Client Applications, Policies, SLA Tiers, and Settings. The main content area shows the Settings page for the American Flights API (v1). It includes the API status (Active), Asset Version (1.0.1), and Type (RAML/OAS). There are links for the Implementation URL and Consumer endpoint. On the right, there are links for 'Manage CloudHub Proxy', 'View API in Exchange', 'View configuration details', and 'View Analytics Dashboard'. There is an 'Apply New Policy' button at the bottom.

3. Click the Apply New Policy button.

4. In the Select Exchange Policy dialog box, expand Rate limiting and select the latest version for the Mule runtime version you are using.

Select Exchange Policy

All Categories ▾ All Mule Versions ▾

Policies	Min Mule Version
> JSON threat protection	
> Basic Authentication - LDAP	
> Message Logging	
▾ Rate limiting	
<input type="radio"/> 1.0.0 ⓘ	4.0.0
<input type="radio"/> 1.1.0 ⓘ	4.1.0
<input checked="" type="radio"/> 1.2.0 ⓘ	4.1.0
> Rate limiting - SLA based	

Cancel Configure Policy

5. Click Configure Policy.

6. On the Apply Rate limiting policy page, set the following values and click Apply:

- # of Reqs: 3
- Time Period: 1
- Time Unit: Minute
- Method & Resource conditions: Apply configurations to all API methods & resources

Apply Rate limiting policy

Specifies the maximum value for the number of messages processed per time period, and rejects any messages beyond the maximum. Applies rate limiting to all API calls, regardless of the source.

Identifier

For each identifier value, the set of Limits defined in the policy will be enforced independently. I.e.: # [attributes.queryParams["identifier"]].

Limits

Pairs of maximum quota allowed and time window.

# of Reqs *	Time Period *	Time Unit *
3	1	Minute

[+ Add Limit](#)

☒ Clusterizable

When using a clustered runtime with this flag enabled, configuration will be shared among all nodes.

☒ Expose Headers

Defines if headers should be exposed in the response to the client. These headers are: x-ratelimit-remaining, x-ratelimit-limit and x-ratelimit-reset.

Method & Resource conditions

- ☒ Apply configurations to all API methods & resources
- ☐ Apply configurations to specific methods & resources

[Cancel](#) [Apply](#)

7. Click Apply; you should see the policy listed for your API.

API Manager

Training ? MM

API Administration (Sandbox)

American Flights API (v1) - Policies

SANDBOX

← API Administration

Alerts

Client Applications

Policies

SLA Tiers

Settings

American Flights API v1

Actions

API Status: Active Asset Version: 1.0.1 Type: RAML/OAS

Implementation URL: <http://training4-american-ws-mule.cloudhub.io/api>

Consumer endpoint: <http://training4-american-api-mule.cloudhub.io/>

Apply New Policy

Edit policy order

Manage CloudHub Proxy >

View API in Exchange >

View configuration details >

View Analytics Dashboard >

Name	Category	Fulfills	Requires
> Rate limiting ⓘ	Quality of service	Baseline Rate Limiting	

8. In the left-side navigation, select Settings.
9. Change the API instance label to Rate limiting policy.

API Instance ⓘ

ID: 5831632

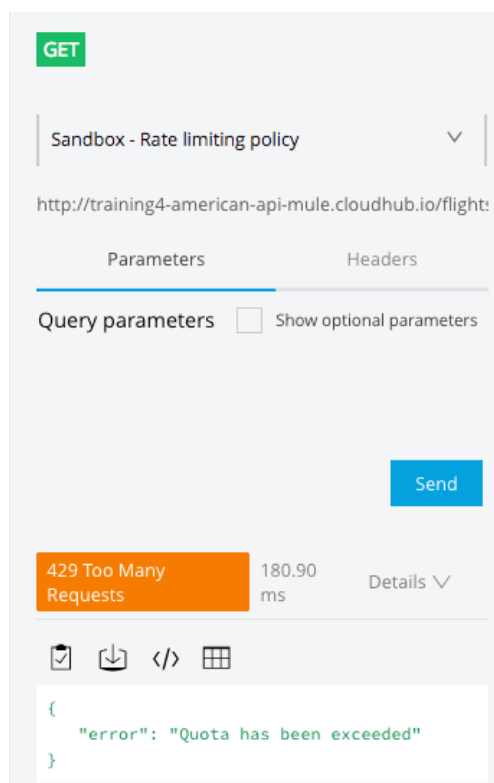
Label: Rate limiting policy ✎

Test the new rate limiting policy

10. Return to the browser tab with your American Flights API in Exchange.
11. Return to the page with the API console for the flights:/GET resource.
12. Select the Sandbox – Rate limiting policy API instance.

Note: You may need to refresh the page to see the new label for the API instance.

13. Press Send until you get a 429 Too Many Requests response.



Create SLA tiers

14. Return to the browser tab with your American Flights API in API Manager.
15. In the left-side navigation, select SLA Tiers.

16. Click the Add SLA tier button.

17. In the Add SLA tier dialog box, set the following values:

- Name: Free
- Approval: Automatic
- # of Reqs: 1
- Time Period: 1
- Time Unit: Minute

18. Click the Add button.

19. Create a second SLA tier with the following values:

- Name: Silver
- Approval: Manual
- # of Reqs: 1
- Time Period: 1
- Time Unit: Second

Add SLA tier

Search

1 - 2 of 2

Name	Limits	Applications	Status	Approval		
Free	1	0	Active	Auto	Edit	Delete
Silver	1	0	Active	Manual	Edit	Delete

Change the policy to rate limiting – SLA based

20. In the left-side navigation, select Policies.

21. Expand the Rate limiting policy.

22. Click the Actions button and select Remove.

Name	Category	Fulfills	Requires
▼ Rate limiting ⓘ	Quality of service	Baseline Rate Limiting	
Order	Method	Resource URI	
⌵	All API Methods	All API Resources	<div>View Detail</div> <div>Actions ▼</div> <div>Disable</div> <div>Edit</div> <div>Remove</div>

23. In the Remove policy dialog box, click Remove.

24. Click the Apply New Policy button.

25. In the Select Policy dialog box, expand Rate limiting - SLA based and select the latest version for the Mule runtime version you are using.
26. Click Configure Policy.

Select Exchange Policy

All Categories

All Mule Versions

Policies	Min Mule Version
> IP whitelist	
> JSON threat protection	
> Basic Authentication - LDAP	
> Rate limiting	
▼ Rate limiting - SLA based	
<input type="radio"/> 1.0.0 ⓘ	4.0.0
<input checked="" type="radio"/> 1.1.0 ⓘ	4.1.0
> Spike Control	
> XML threat protection	

Cancel

Configure Policy

27. On the Apply Rate limiting – SLA based policy page, look at the expressions and see that a client ID and secret need to be sent with API requests as headers.

The screenshot shows the 'API Manager' interface. The top navigation bar includes a hamburger menu, the 'API Manager' logo, and three tabs: 'API Administration (Sandbox)', 'American Flights API (v1) - Policies', and 'Apply Rate limiting - SLA based policy'. On the left, there is a 'SANDBOX' button and a 'Policies' link. The main content area is titled 'Apply Rate limiting - SLA based policy'. It contains a description: 'Specifies the maximum value for the number of messages processed per time period, and rejects any messages beyond the maximum. This policy will require updates to the RAML definition in order to function. You can obtain the RAML snippet and learn more [here](#).' Below this are two sections: 'Client ID Expression *' with a description 'Mule Expression to be used to extract the Client ID from API requests.' and a text input field containing '#{attributes.headers['client_id']}'; and 'Client Secret Expression' with a description 'Mule Expression to be used to extract the Client Secret from API requests.' and a text input field containing '#{attributes.headers['client_secret']}'. There are two checked checkboxes: 'Clusterizable' (with a description 'When using a clustered runtime with this flag enabled, configuration will be shared among all nodes.') and 'Expose Headers' (with a description 'Defines if headers should be exposed in the response to the client. These headers are: x-ratelimit-remaining, x-ratelimit-limit and x-ratelimit-reset.'). Below these is the 'Method & Resource conditions' section with two radio buttons: 'Apply configurations to all API methods & resources' (which is selected) and 'Apply configurations to specific methods & resources'. At the bottom right are 'Cancel' and 'Apply' buttons.

28. Click Apply.
29. In the left-side navigation, select Settings.
30. Change the API instance label to Rate limiting – SLA based policy.

API Instance ⓘ
ID: 5831632
Label: Rate limiting - SLA based policy ✎

Test the rate limiting – SLA based policy in Exchange

31. Return to the browser tab with your API in Exchange.
32. Refresh the page and select to make a call to the Sandbox – Rate limiting – SLA based policy.

33. Click Send; you should get a 401 Unauthorized response with a message that there is an invalid client id or secret.

The screenshot shows an API client interface. At the top, a green button labeled "GET" is visible. Below it, a dropdown menu is set to "Sandbox - Rate limiting - SLA based policy". The URL field contains "http://training4-american-api-mule.cloudhub.io/flight:". There are two tabs, "Parameters" and "Headers", with "Parameters" being the active tab. Under the "Parameters" tab, there is a section for "Query parameters" with a checkbox labeled "Show optional parameters" which is currently unchecked. A blue "Send" button is located at the bottom right of the parameter section. Below the "Send" button, the response status is displayed as "401 Unauthorized" in an orange box, followed by the response time "819.80 ms" and a "Details" link with a downward arrow. At the bottom, there are icons for a clipboard, download, code editor, and table view. The response body is displayed in a code editor, showing a JSON object:

```
{  "error": "Invalid client id or secret"}
```