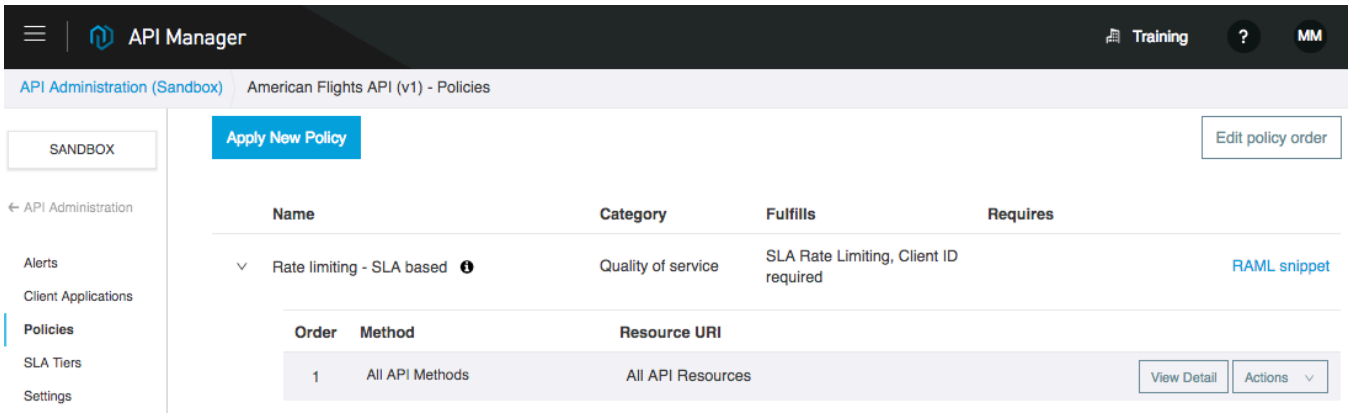
Walkthrough 5-3: Restrict API access with policies and SLAs

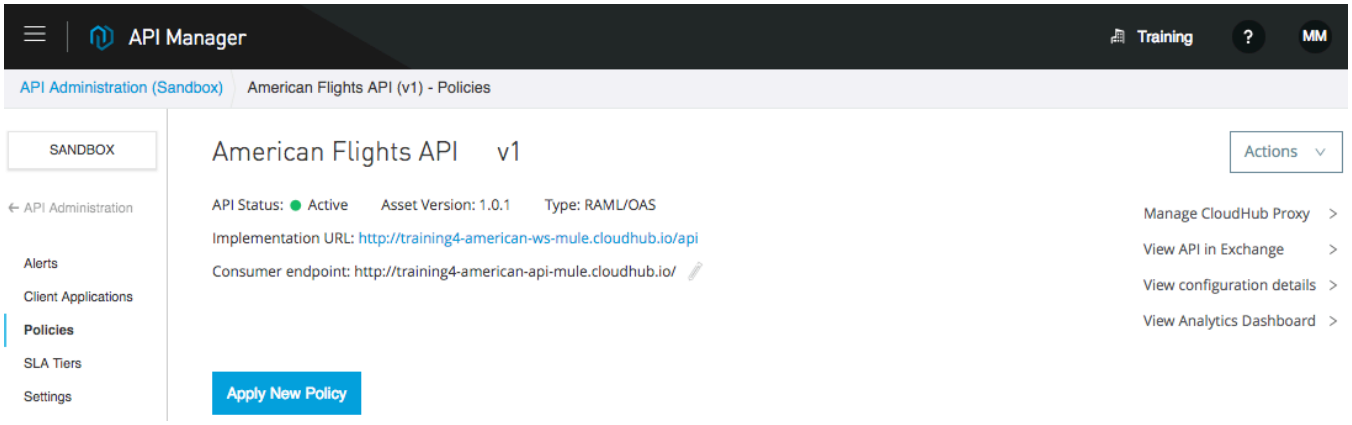
In this walkthrough, you govern access to the API proxy. You will:

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



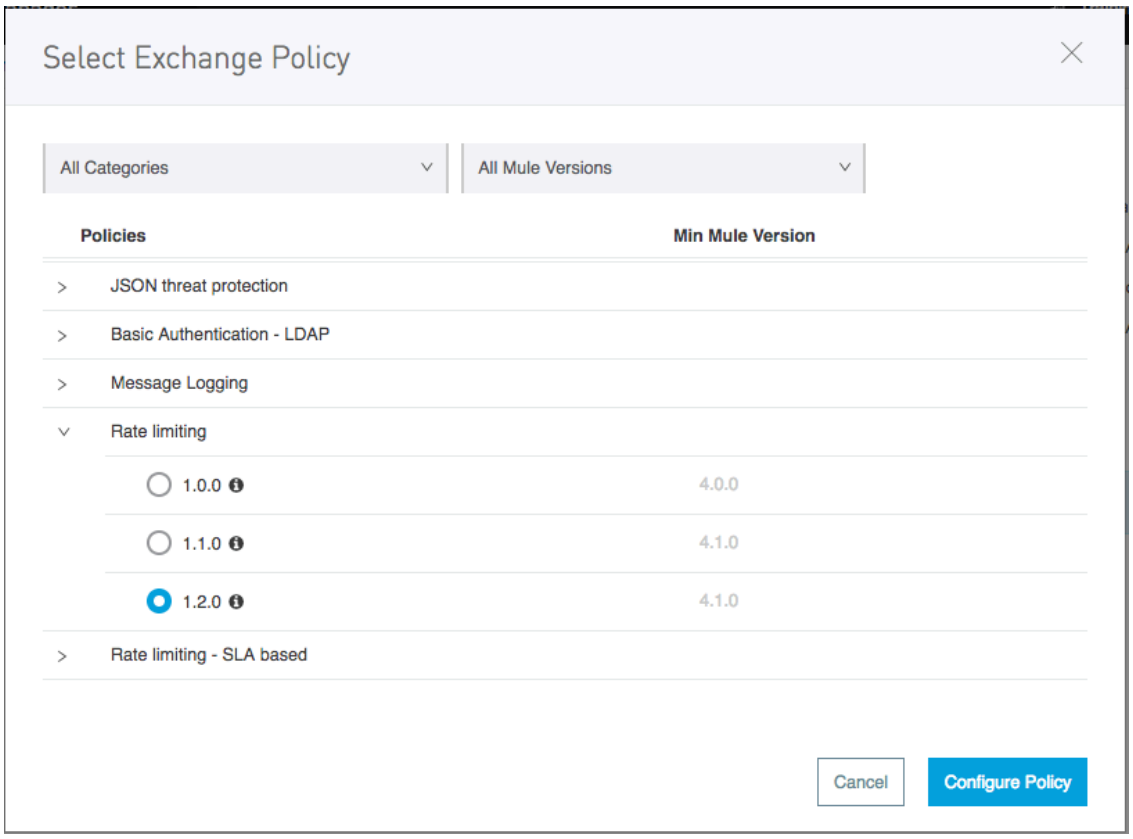
Create a rate limiting policy

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



3. Click the Apply New Policy button.

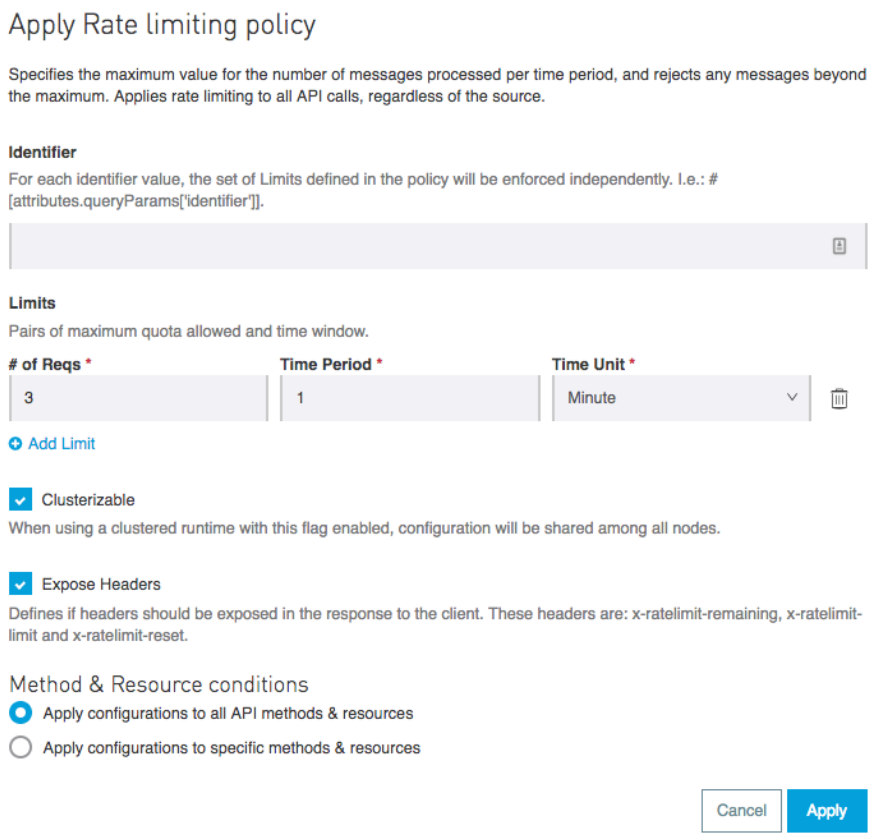
4. In the Select Exchange Policy dialog box, expand Rate limiting and select the latest version for the Mule runtime version you are using.



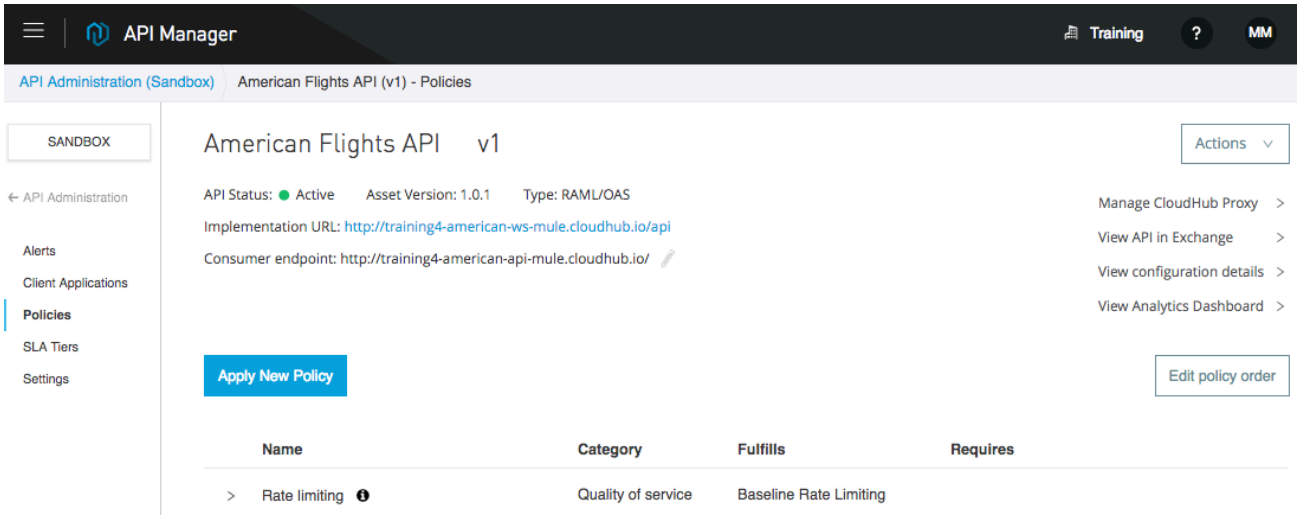
5. Click Configure Policy.

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

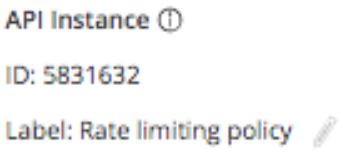
   - # of Reqs: 3
   - Time Period: 1
   - Time Unit: Minute
   - Method & Resource conditions: Apply configurations to all API methods & resources



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



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

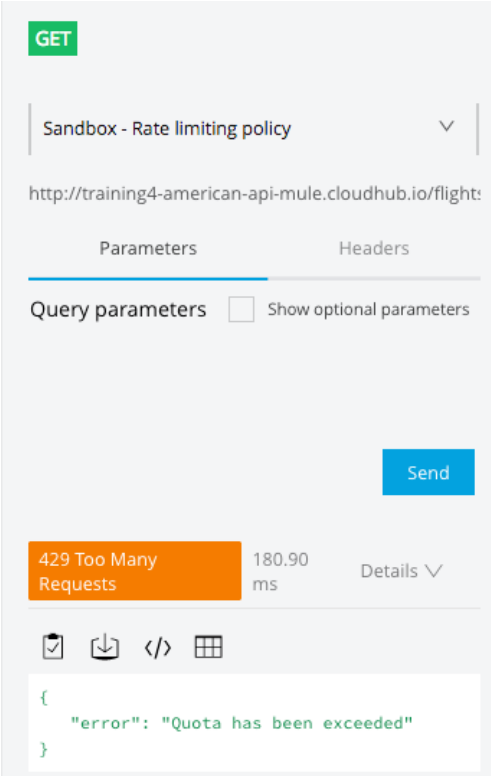


Test the new rate limiting policy

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.

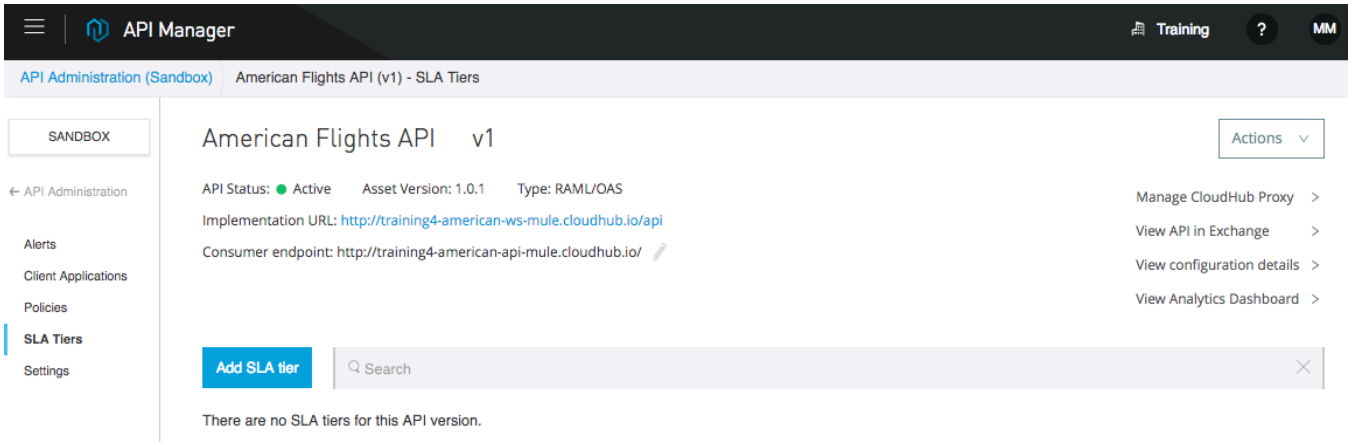
13. Press Send until you get a 429 Too Many Requests response.



Create SLA tiers

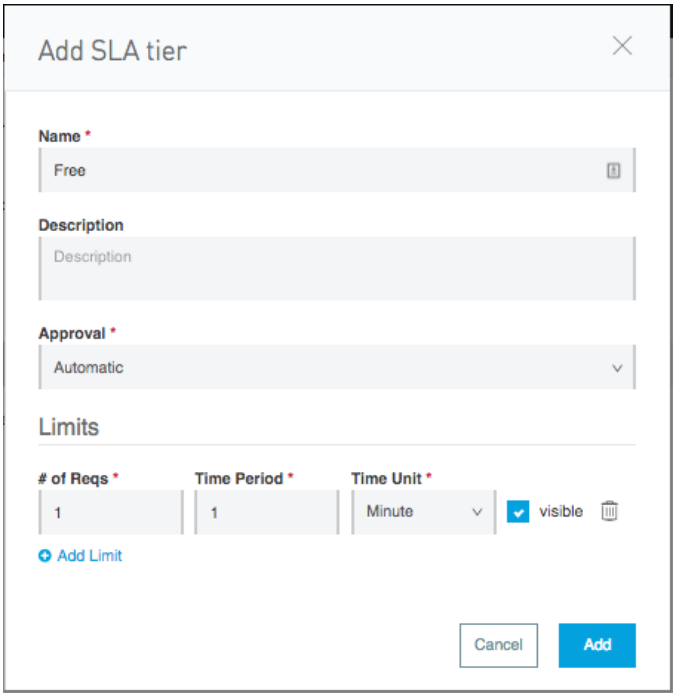
14. Return to the browser tab with your American Flights API in API Manager.
15. In the left-side navigation, select SLA Tiers.

16. Click the Add SLA tier button.



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

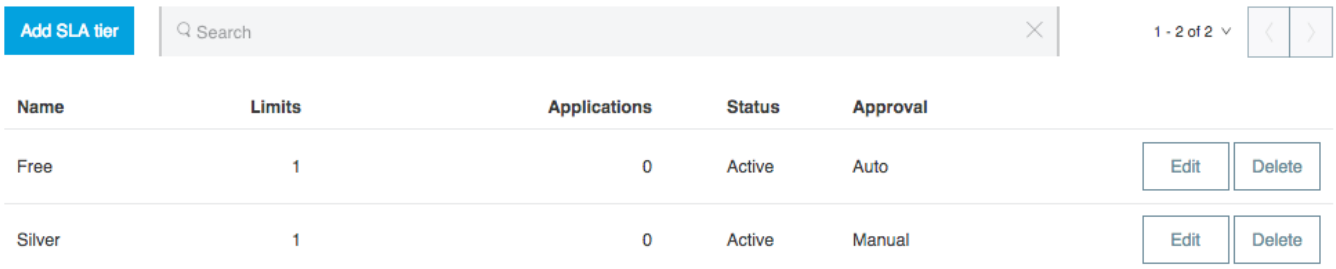
- Name: Free
- Approval: Automatic
- # of Reqs: 1
- Time Period: 1
- Time Unit: Minute



18. Click the Add button.

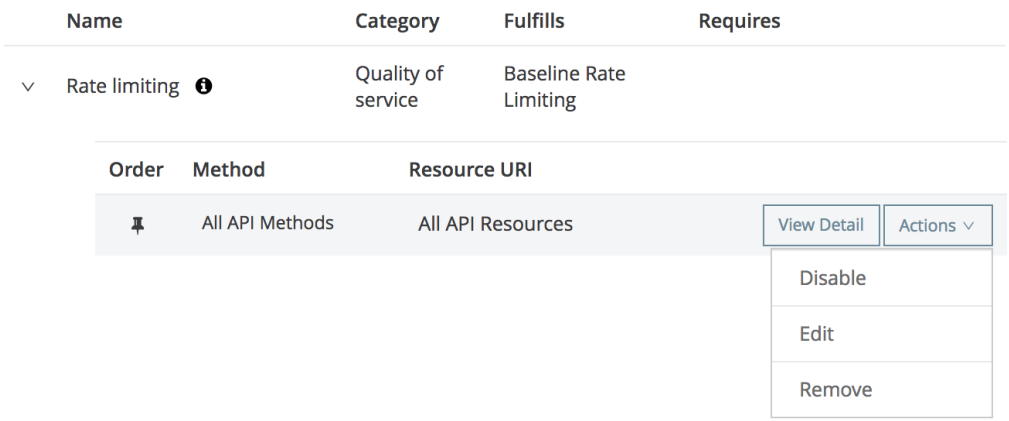
19. Create a second SLA tier with the following values:

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



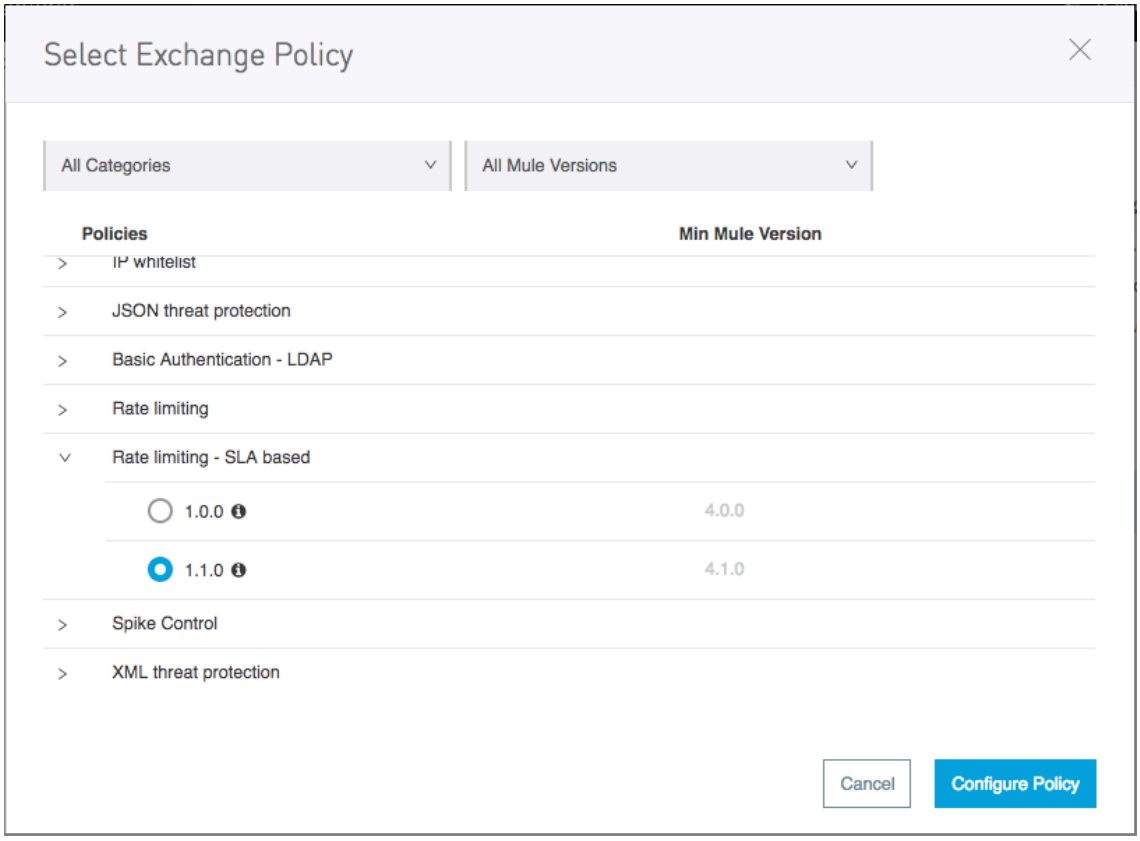
Change the policy to rate limiting – SLA based

20. In the left-side navigation, select Policies.
21. Expand the Rate limiting policy.
22. Click the Actions button and select Remove.

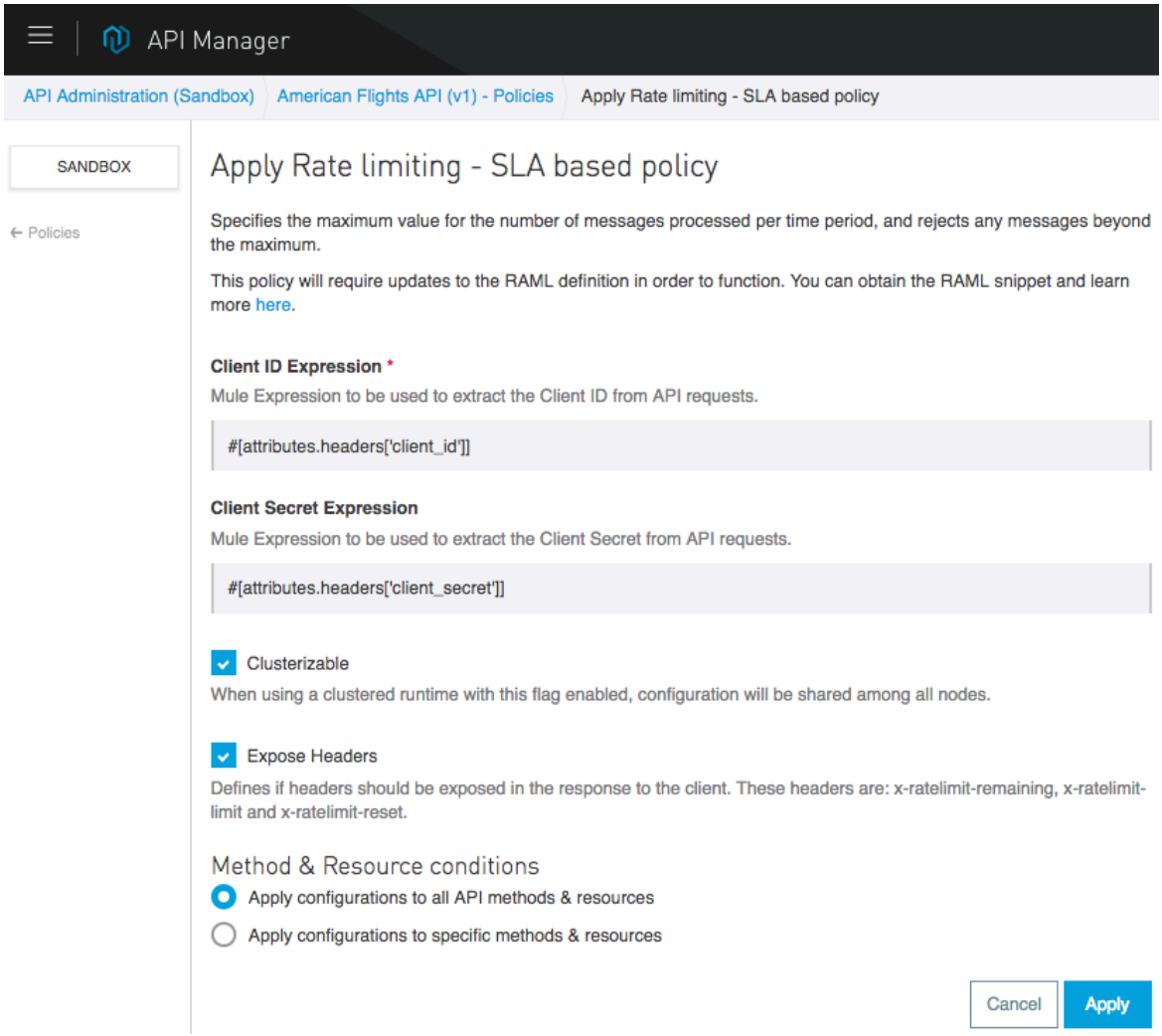


23. In the Remove policy dialog box, click Remove.
24. Click the Apply New Policy button.

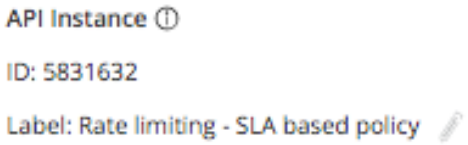
25. In the Select Policy dialog box, expand Rate limiting - SLA based and select the latest version for the Mule runtime version you are using.
26. Click Configure Policy.



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.



28. Click Apply.
29. In the left-side navigation, select Settings.
30. Change the API instance label to 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.