**API Manager Policies**

A policy extends the functionality of an API and enforces certain capabilities such as security, compliance and quality of service. Policies can apply on these:

1. An API running on CloudHub
2. Design an API on Anypoint Platform, configure a proxy for Cloudhub, and apply a policy.

Once deployed to CloudHub, URL proxies and policies need to be put in place.  Roughly, an API is either created or exported to the API Manager.  Once there, a proxy application is created that covers the backend CloudHub deployment, adding things like access policies.  The proxy application can then be monitored for status and logs checked for potential problems.  An API Portal allows endpoints to be manually accessed and an analytics graph charts access.

All microservices are applying below policies provided by the CloudHub.

1. **IP Whitelist:**

Here is the list of Sungard AS global IP’s to add for DEV & INT, further staging and production IP’s needs get from actual consumers. Before configure this policy product owner needs to be communicate with customer.

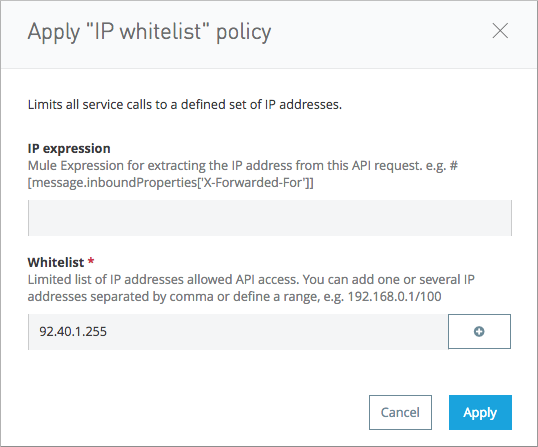
Wayne: 216.203.6.10 or 216.203.6.11

Bangalore: 103.88.30.36

Pune: 103.88.28.36

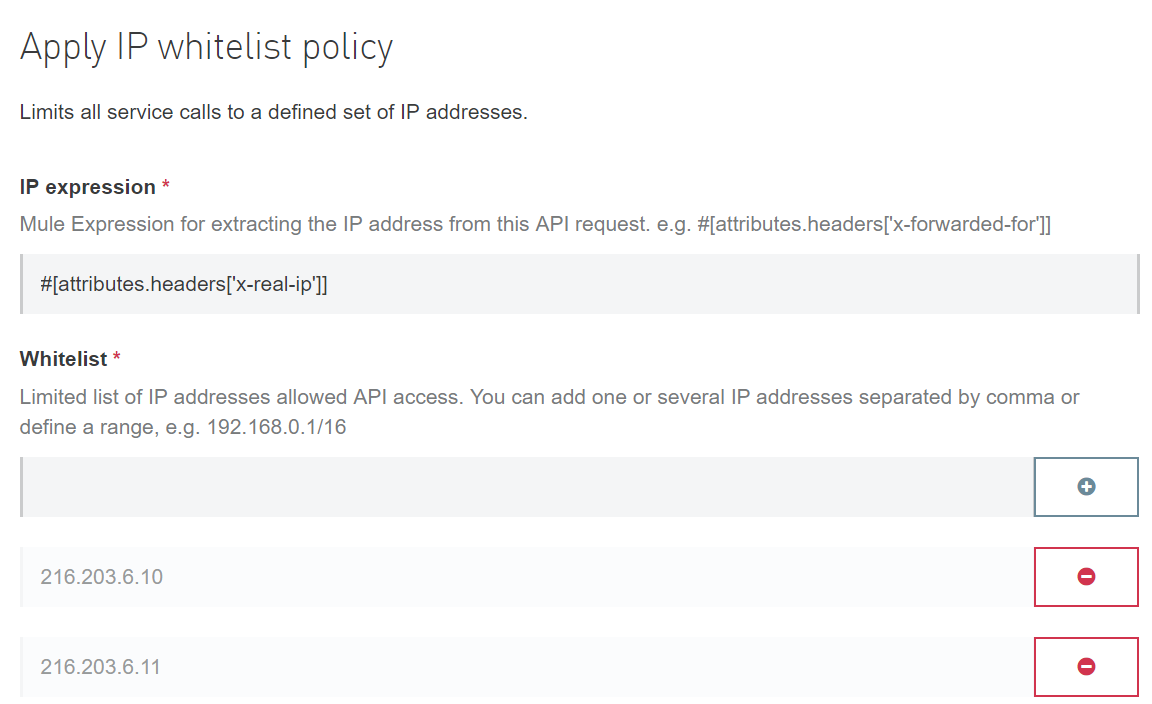
Configurations steps:

1. In API Manager > API Administration, click a version number for an API.
2. Click Policies > Apply New Policy.
3. In Select Policy, choose IP Whitelist, and click Configure Policy.
4. Specify an address or a range or addresses as follows:
5. Define a specific IP address. For example, 192.168.1.1.
6. Define a subset of addresses by identifying a subnet mask, such as 192.168.3.1/30. This includes the consolidated range: 192.168.3.0 - 192.168.3.3.
7. Define a whole range of IP addresses by stating the relevant octets of the IP address you want to permit. For example, setting 192.168 will include IP addresses from 192.168.0.0 to 192.168.255.255.
8. Enter IP addresses in **Whitelist** popup



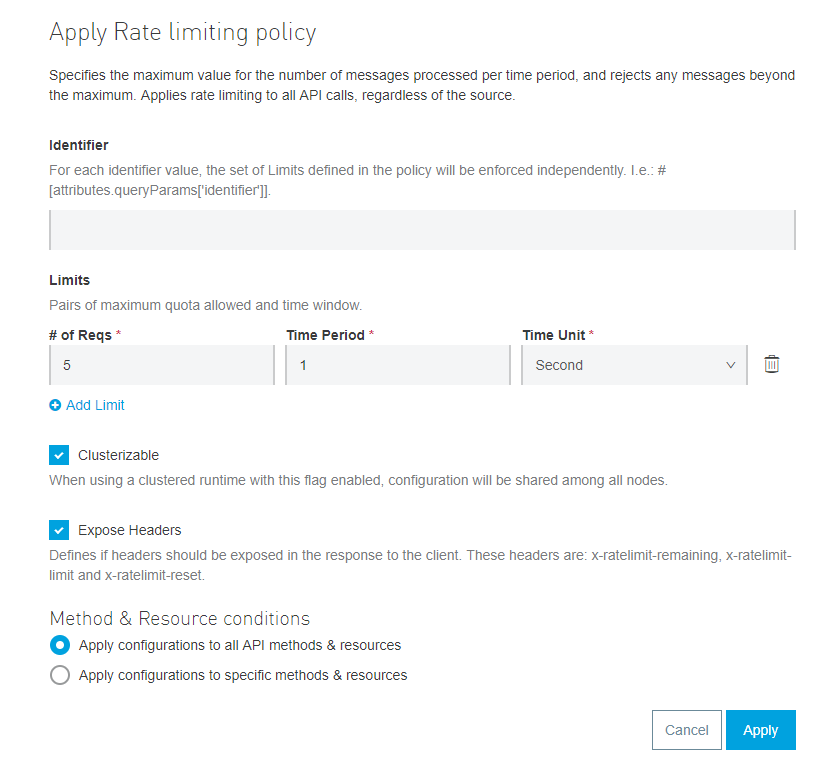
1. **Click on +** symbol to add more IP’s.

The greyed-out IP address and a deletion control appears below the Whitelist text entry field.



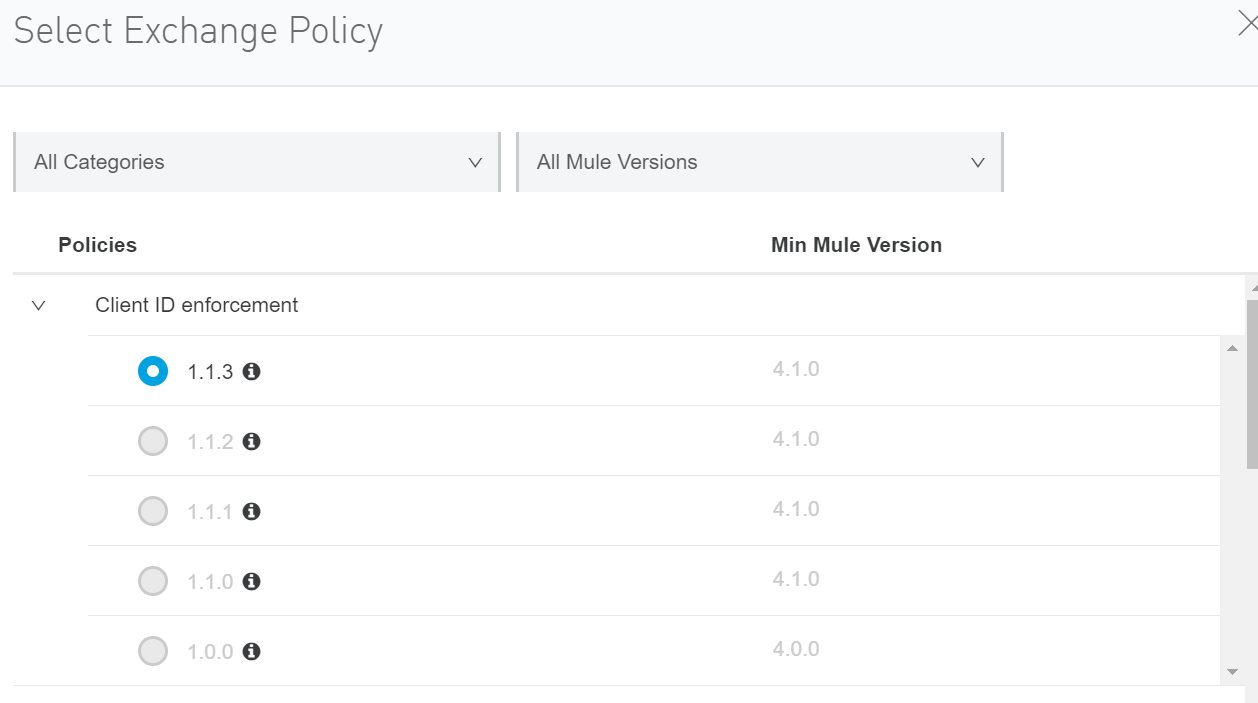
3. Click on **Apply**.

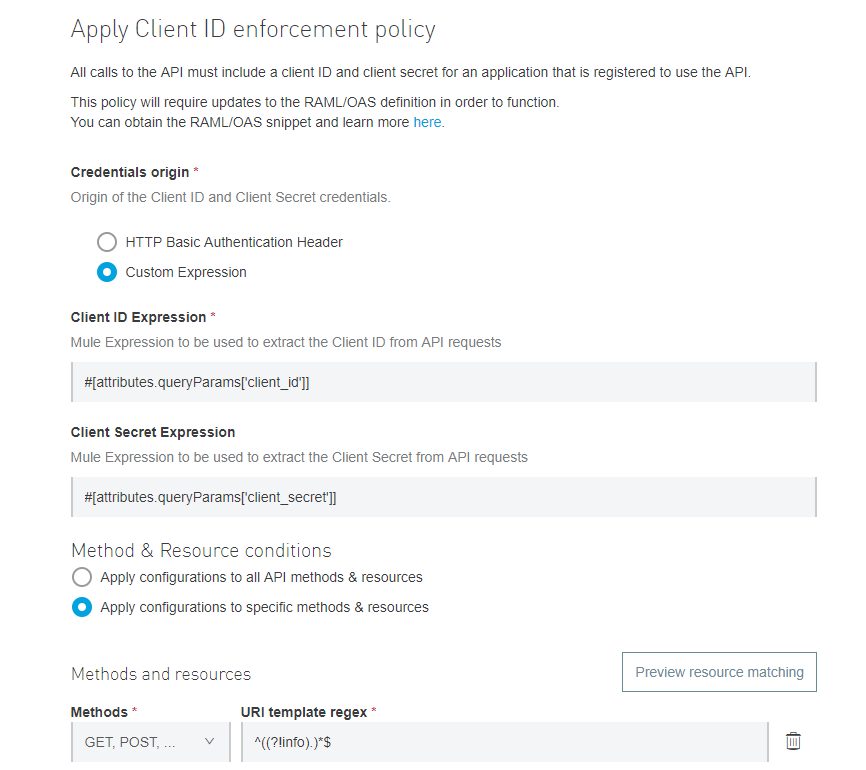
1. **Rate Limiting Policy**
2. In API Manager > API Administration, click a version number for an API.
3. Click Policies > Apply New Policy.
4. In Select Policy, click Rate Limiting and Configure Policy.
5. In Apply Rate Limiting Policy, you can set the number of requests, period of time for receiving the requests, and a time unit.
6. Click on Apply



Click on **Configure**

1. **Client ID enforcement Policy**
2. In API Manager > API Administration, click a version number for an API.
3. Click Policies > Apply New Policy.
4. Click on Client ID enforcement policy





Click on **Apply**