|  |  |  |  |
| --- | --- | --- | --- |
| Scope | Inbound / Outbound | Policy | Comments |
| Product | Inbound | Content Security Policy |  |
| Product | Inbound | Throttling | To limit the request for a particular time span |
| Product | Outbound | Mask URL |  |
| Product | Inbound | Change header | To hide .NET framework & other sensitive information |
| Product | Inbound | CORS | To set permission to outside of Application |
| Product | Inbound | Retry |  |
| Product | Outbound | Validate content | To validate content type, to change content type String → JSON |
| API | Outbound | Set context variable |  |
| API | Inbound | Authentication |  |

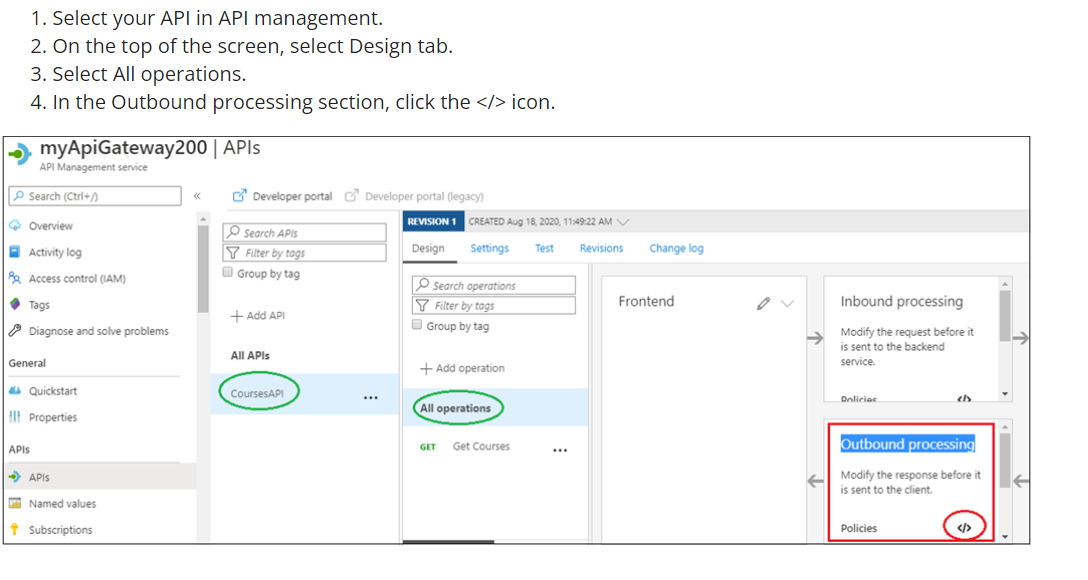
1)

https://www.youtube.com/watch?v=6OybCb53ASY

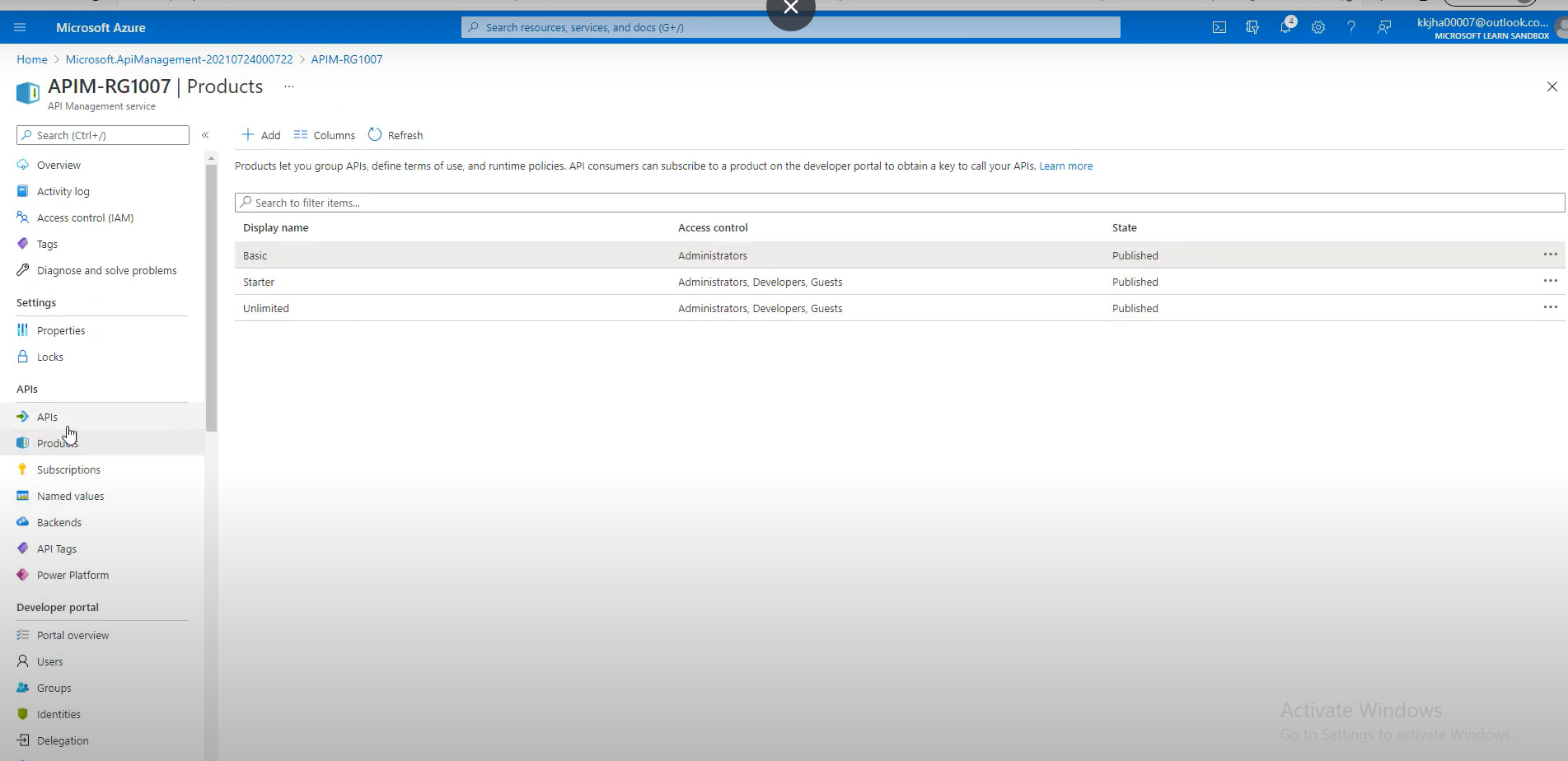
Product

<https://www.c-sharpcorner.com/article/protect-apis-with-security-headers-using-azure-api-management-policies/>

Inbound Processing

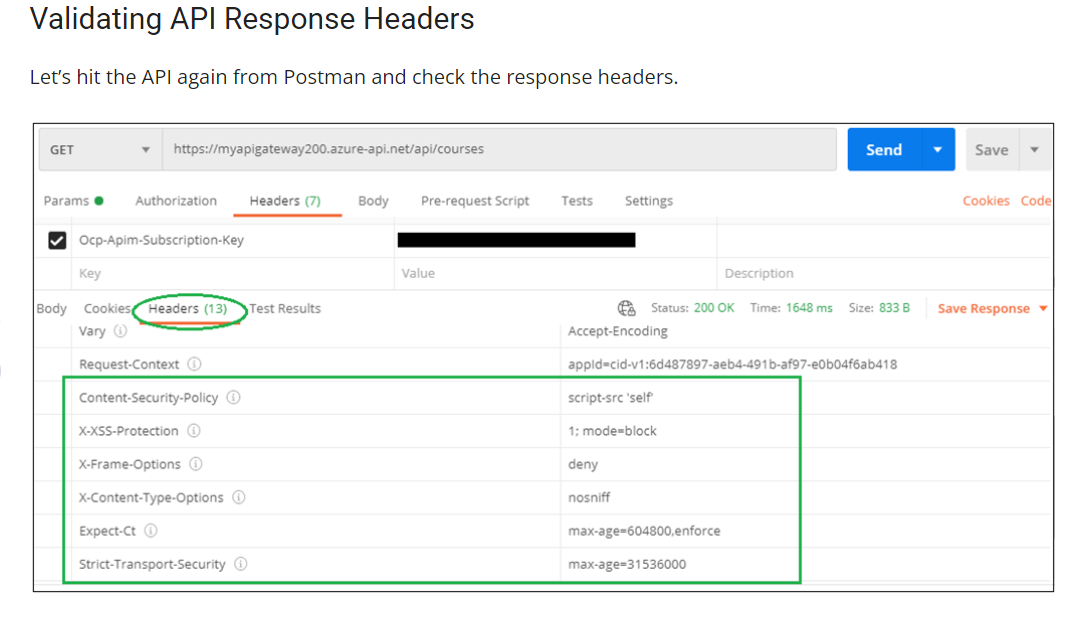


1. In Product we add the product

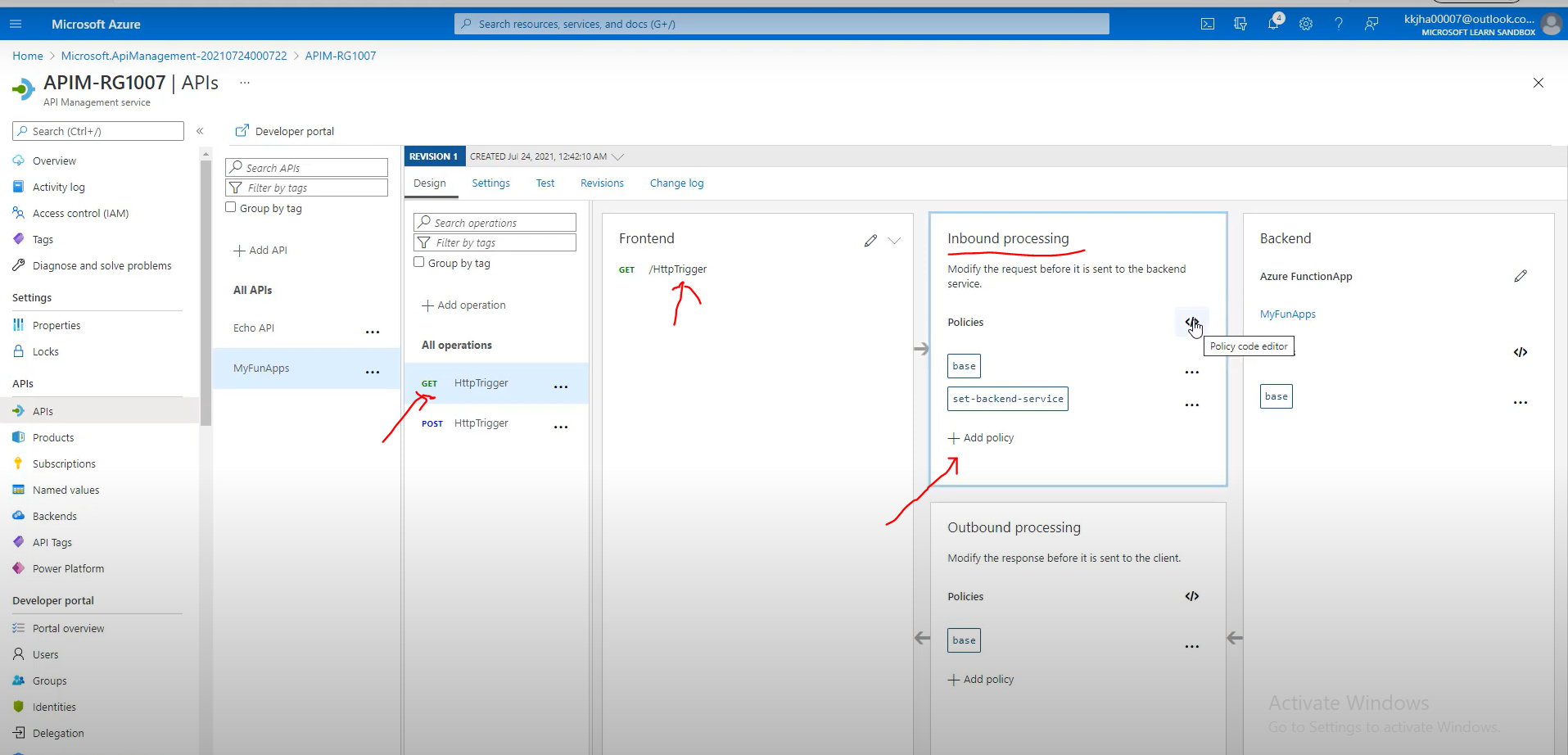


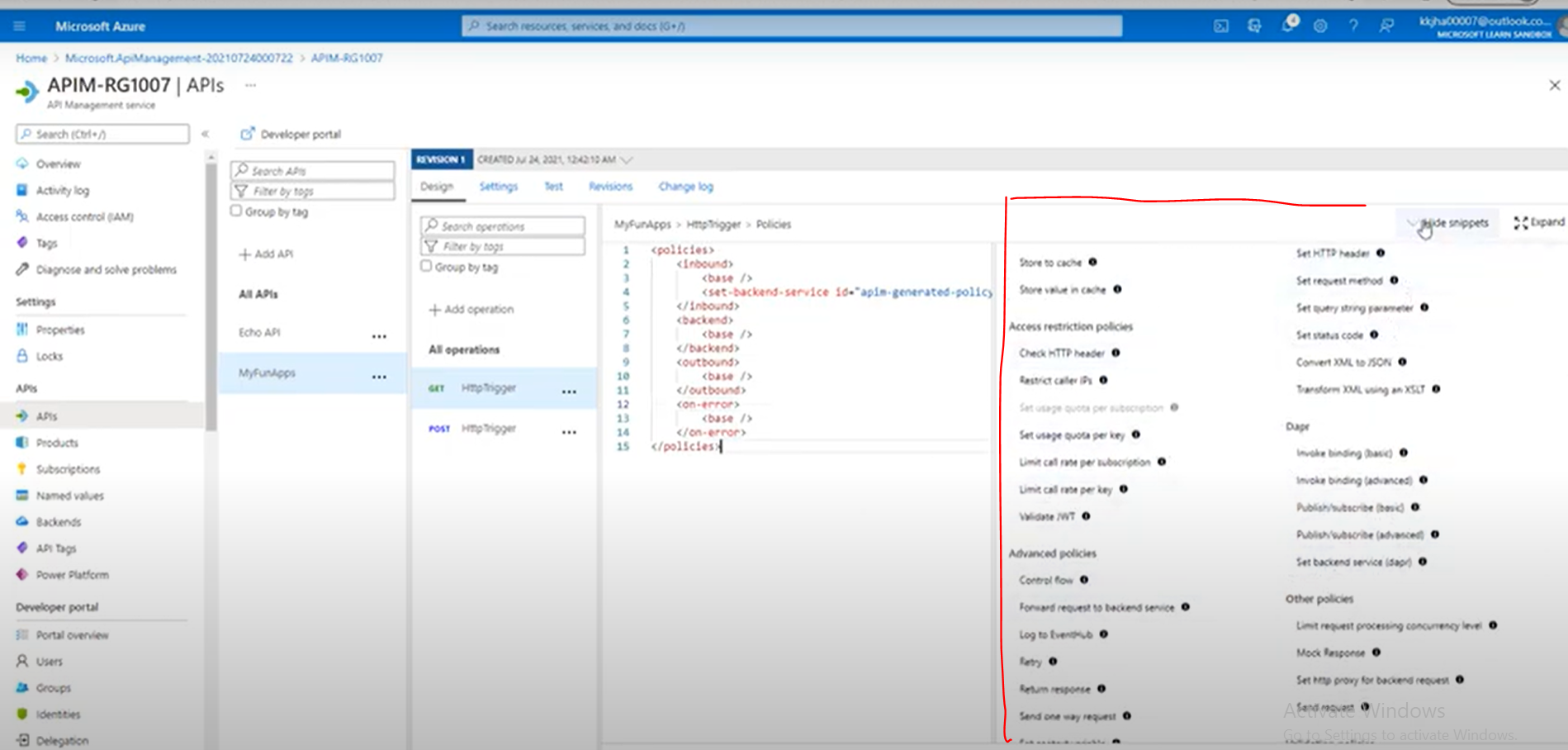
1. <inbound>
2. <set-header name="Strict-Transport-Security" exists-action="override">
3. <value>max-age=31536000</value>
4. </set-header>
5. <set-header name="X-XSS-Protection" exists-action="override">
6. <value>1; mode=block</value>
7. </set-header>
8. <set-header name="Content-Security-Policy" exists-action="override">
9. <value>script-src 'self'</value>
10. </set-header>
11. <set-header name="X-Frame-Options" exists-action="override">
12. <value>deny</value>
13. </set-header>
14. <set-header name="X-Content-Type-Options" exists-action="override">
15. <value>nosniff</value>
16. </set-header>
17. <set-header name="Expect-Ct" exists-action="override">
18. <value>max-age=604800,enforce</value>
19. </set-header>
20. <set-header name="Cache-Control" exists-action="override">
21. <value>none</value>
22. </set-header>
23. <set-header name="X-Powered-By" exists-action="delete" />
24. <set-header name="X-AspNet-Version" exists-action="delete" />
25. </inbound>

URL : **https://content-security-policy.com/**

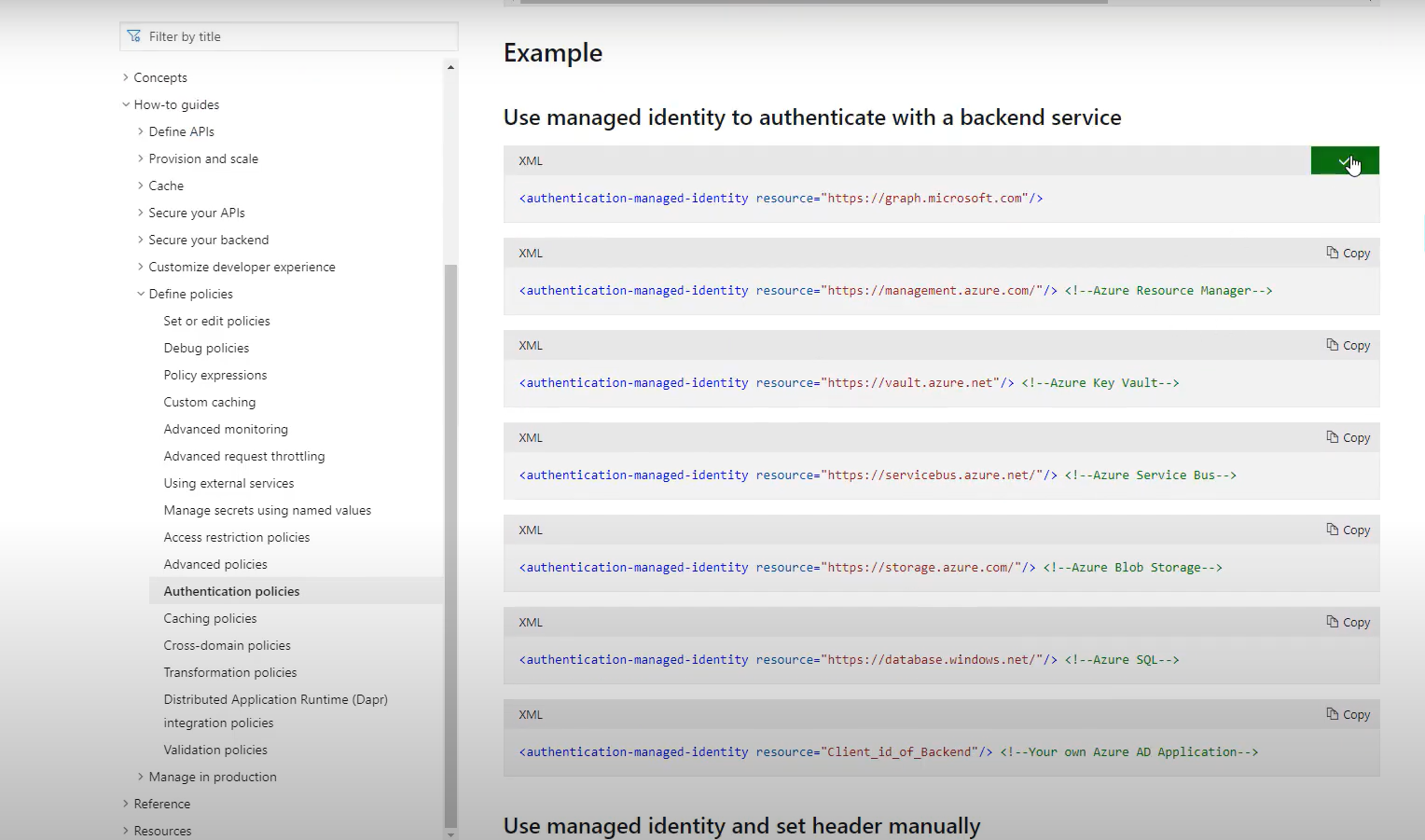


1. In APi Get operation on design if we add inbound processing in which we have added policy





https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-policies



2)

|  |  |  |  |
| --- | --- | --- | --- |
| Product | Inbound | Throttling | To limit the request for a particular time span |

<https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>

**IP address throttling**

<rate-limit-by-key calls="10"

renewal-period="60"

counter-key="@(context.Request.IpAddress)" />

<quota-by-key calls="1000000"

bandwidth="10000"

renewal-period="2629800"

counter-key="@(context.Request.IpAddress)" />

## User identity throttling

<rate-limit-by-key calls="10"

renewal-period="60"

counter-key="@(context.Request.Headers.GetValueOrDefault("Authorization","").AsJwt()?.Subject)" />

## Client driven throttling

<rate-limit-by-key calls="100"

renewal-period="60"

counter-key="@(request.Headers.GetValueOrDefault("Rate-Key",""))"/>

<policies>

<inbound>

<base />

<rate-limit-by-key calls="100"

renewal-period="60"

counter-key="@(request.Headers.GetValueOrDefault("Rate-Key",""))"/>

</inbound>

</policies>