Stealth Watch Information

Local Stealth Watch Connection Information: <https://192.168.128.109>

Cisco Stealth Watch API Official Documentation:

<https://developer.cisco.com/docs/stealthwatch/#!reporting-api-version-1> (Reporting API version1)

<https://developer.cisco.com/docs/stealthwatch/#!reporting-api-version-2> (Reporting API version2)

<https://developer.cisco.com/docs/stealthwatch/#!configuration-management-api> (Configuration API version1)

(It’s better to refer the documentation from the local Stealth Watch web interface.

It can slightly differ with the official documentation, but reflects the correct version of document)

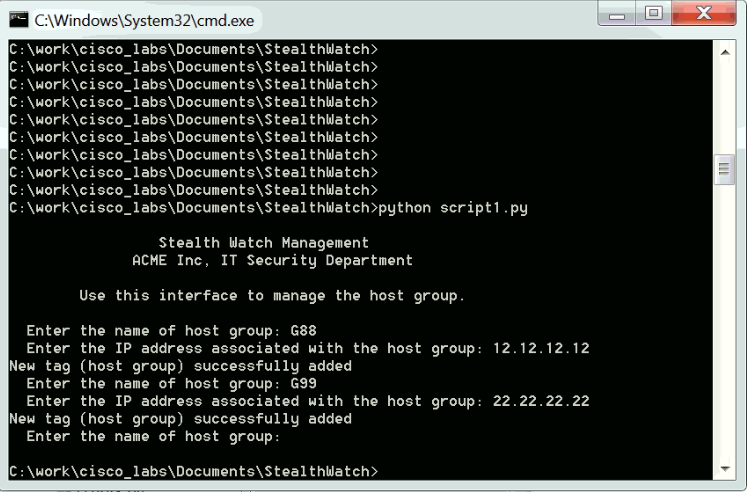
<https://192.168.128.109/sw-reporting/v1/docs> (Reporting API version1)

<https://192.168.128.109/sw-reporting/v2/docs> (Reporting API version2)

<https://192.168.128.109/smc-configuration/rest/v1/docs> (Configuration API version1)

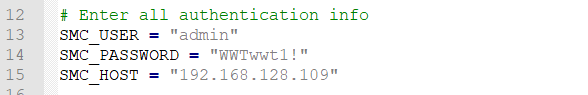
Script1.py

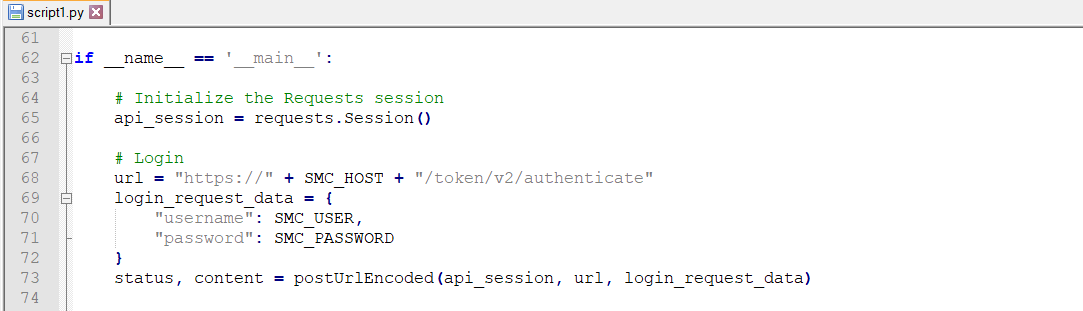
Add a host group

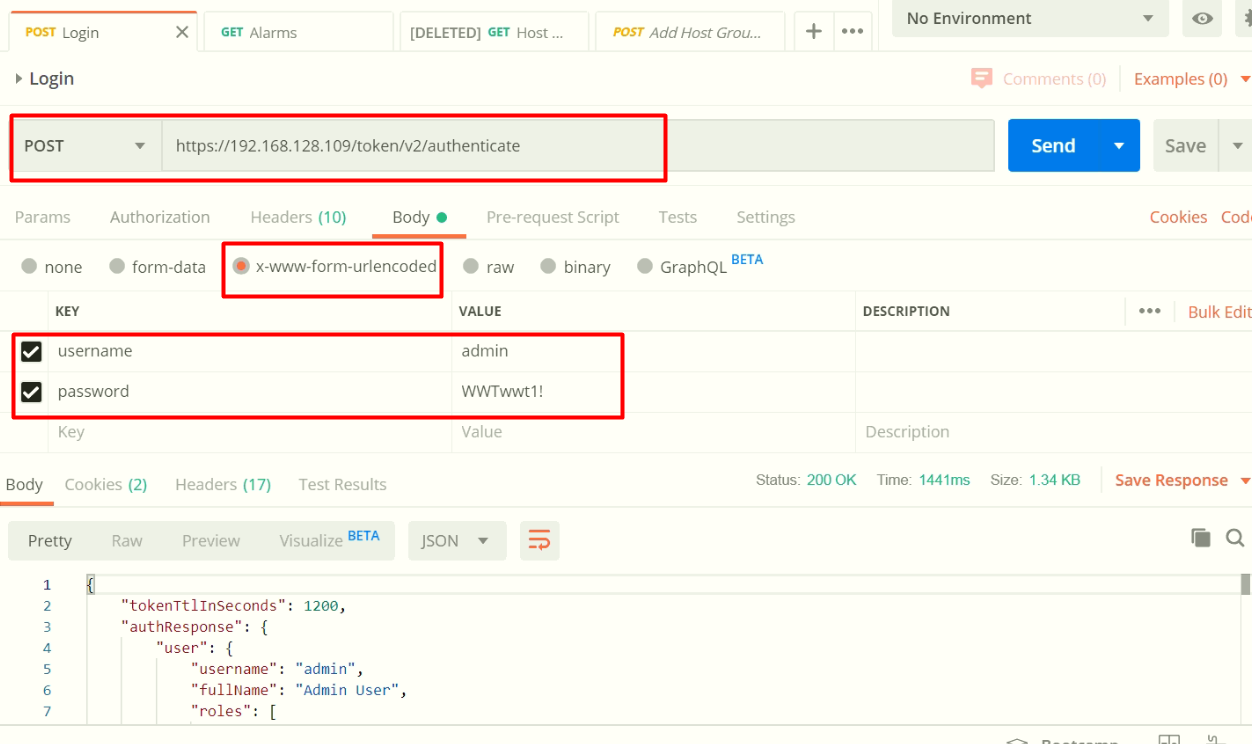


Login

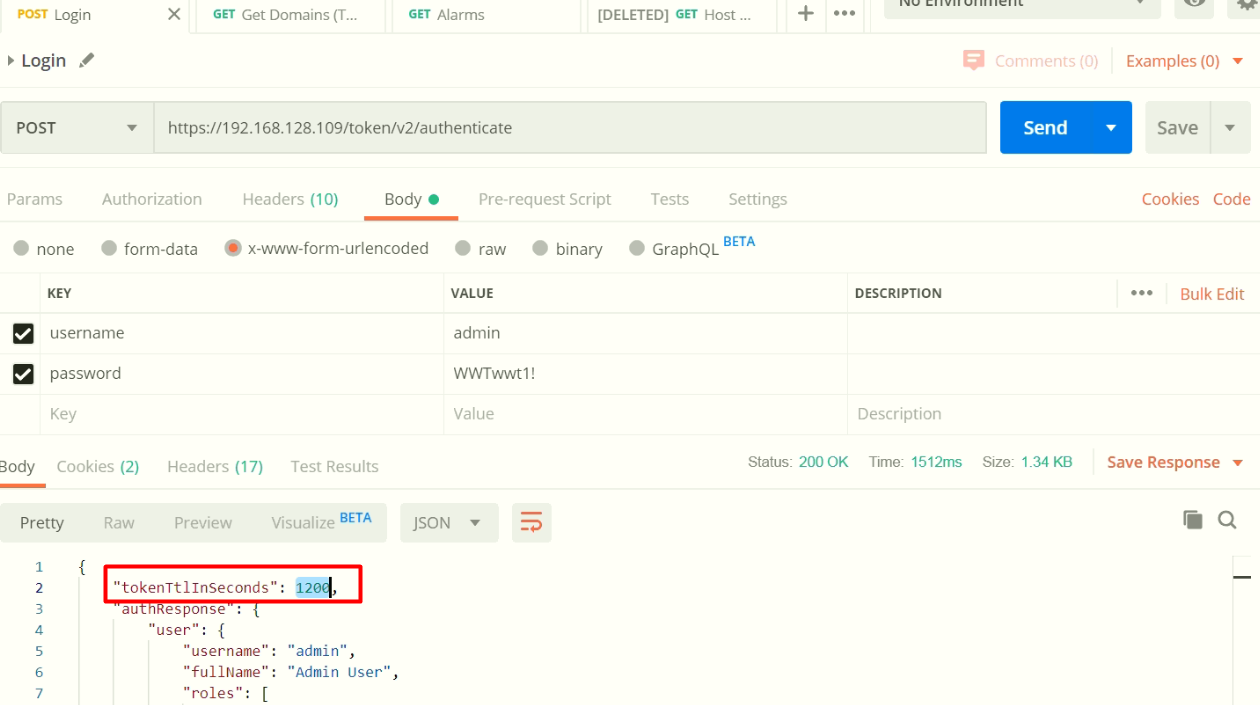
Login information





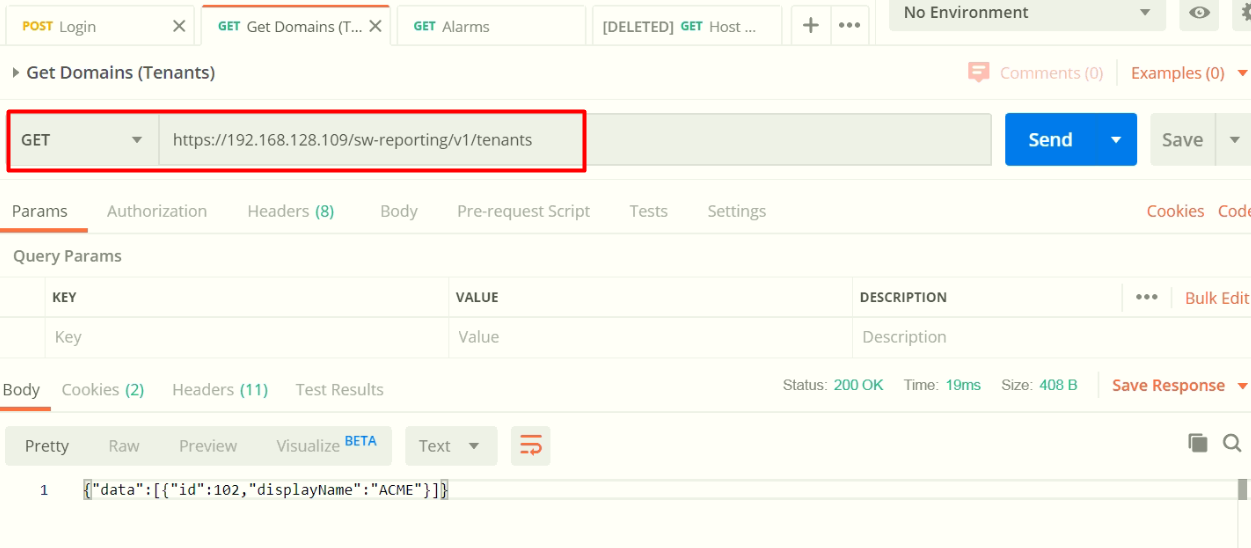


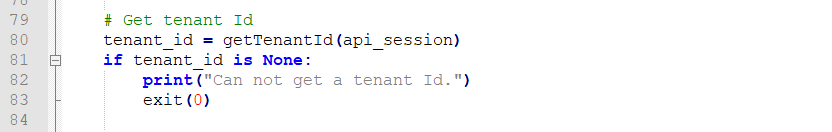
All subsequent calls use the session which is made by Login API call. After 1200 seconds from login, re login is needed for calling further APIs.

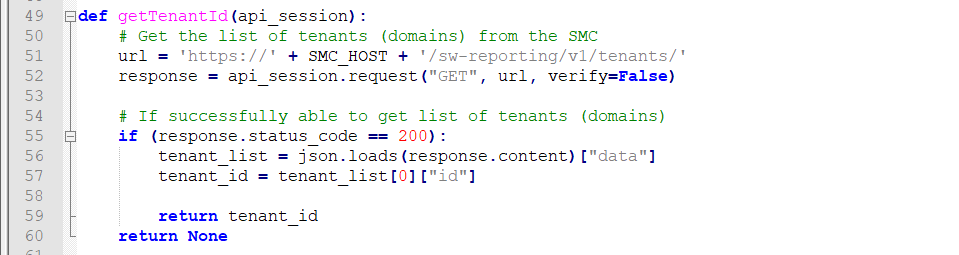


Get tenant ID

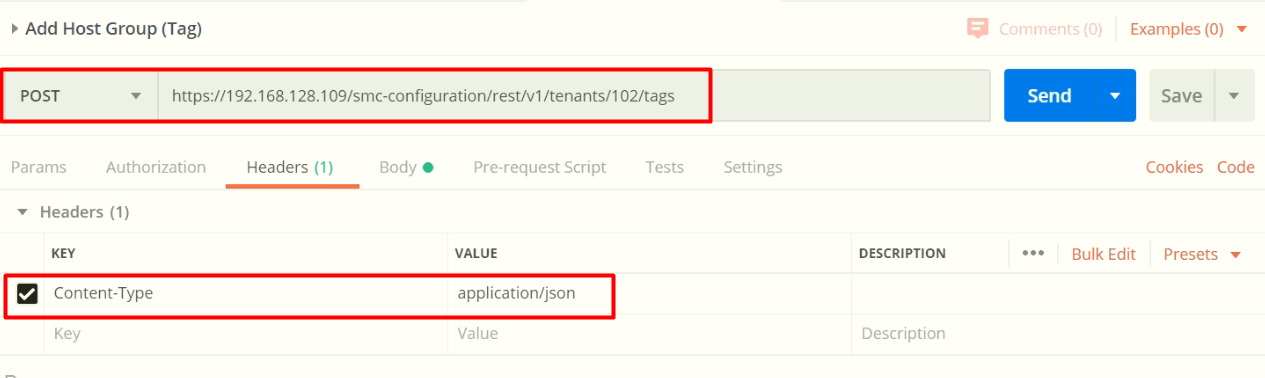
No parameter is need.

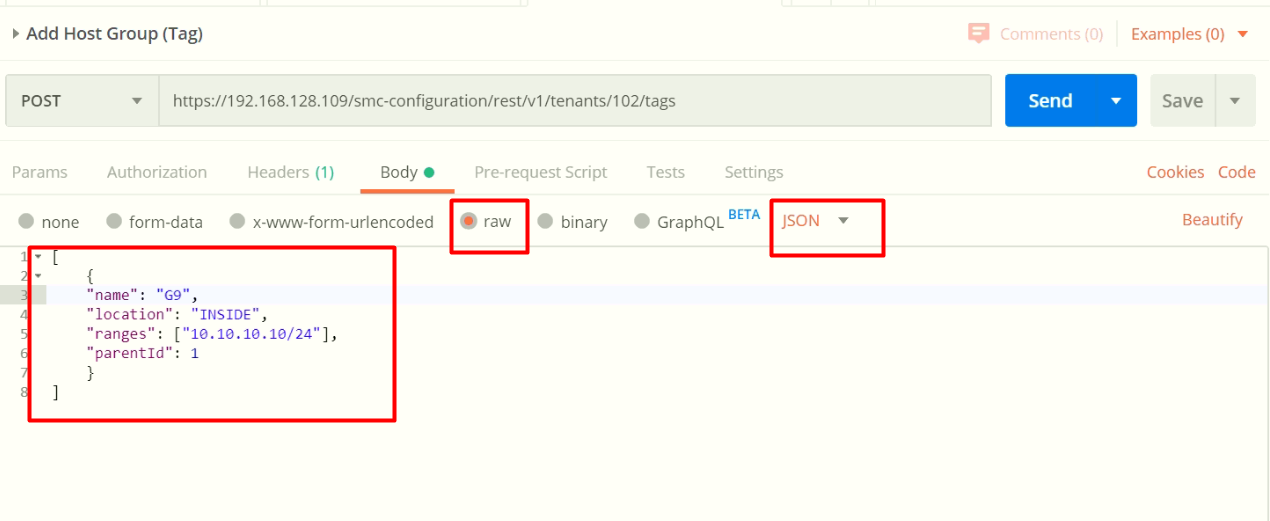


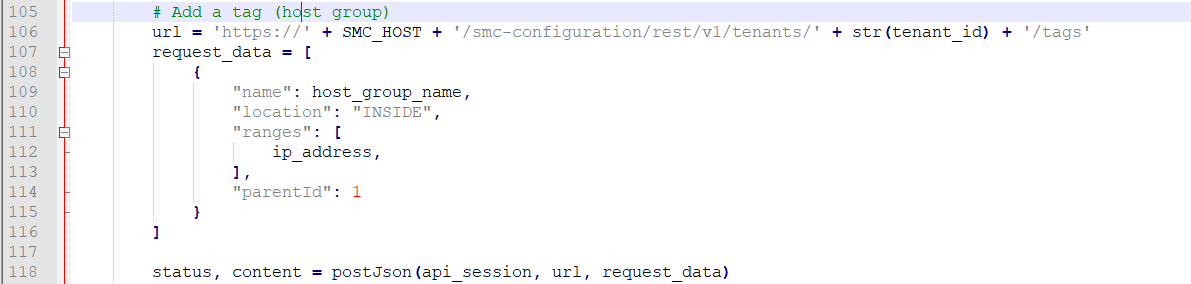




Add a host group

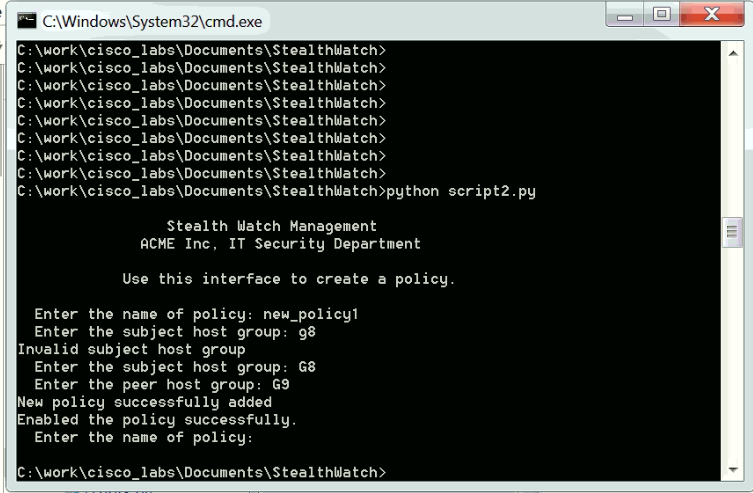




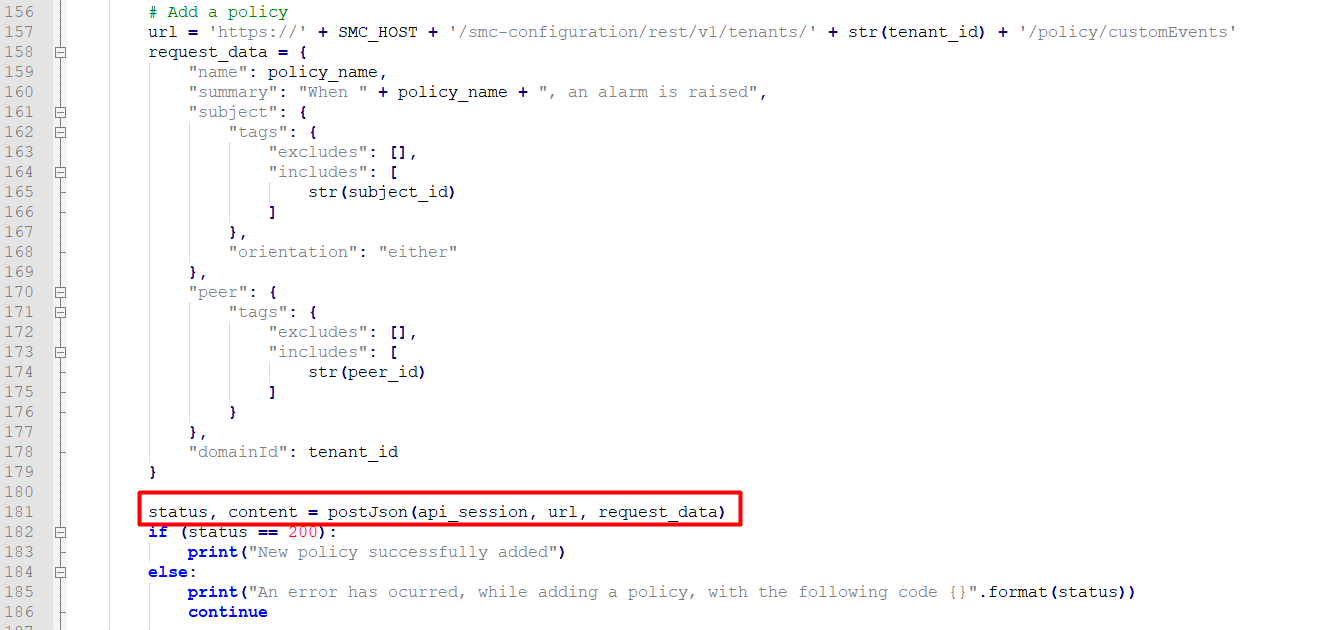


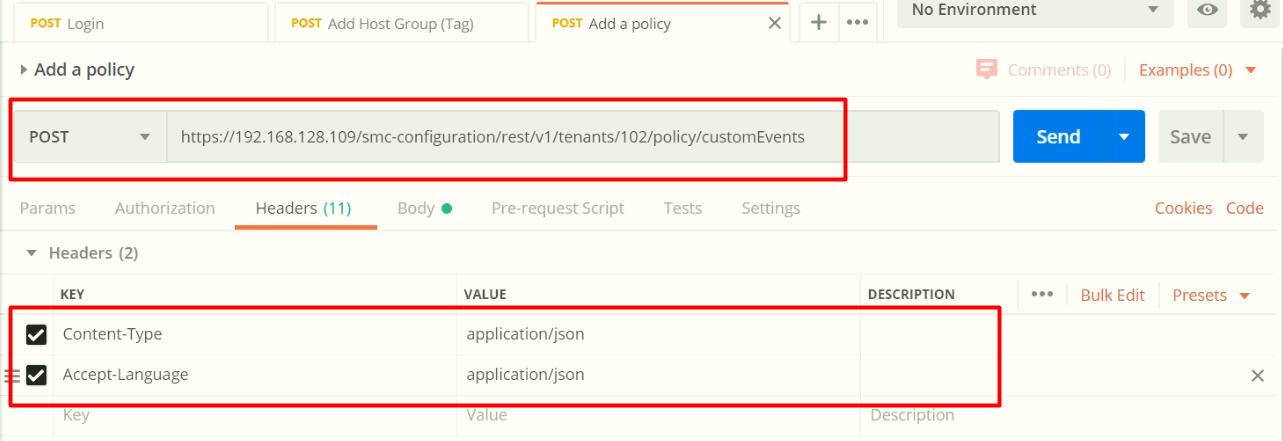
Script2.py

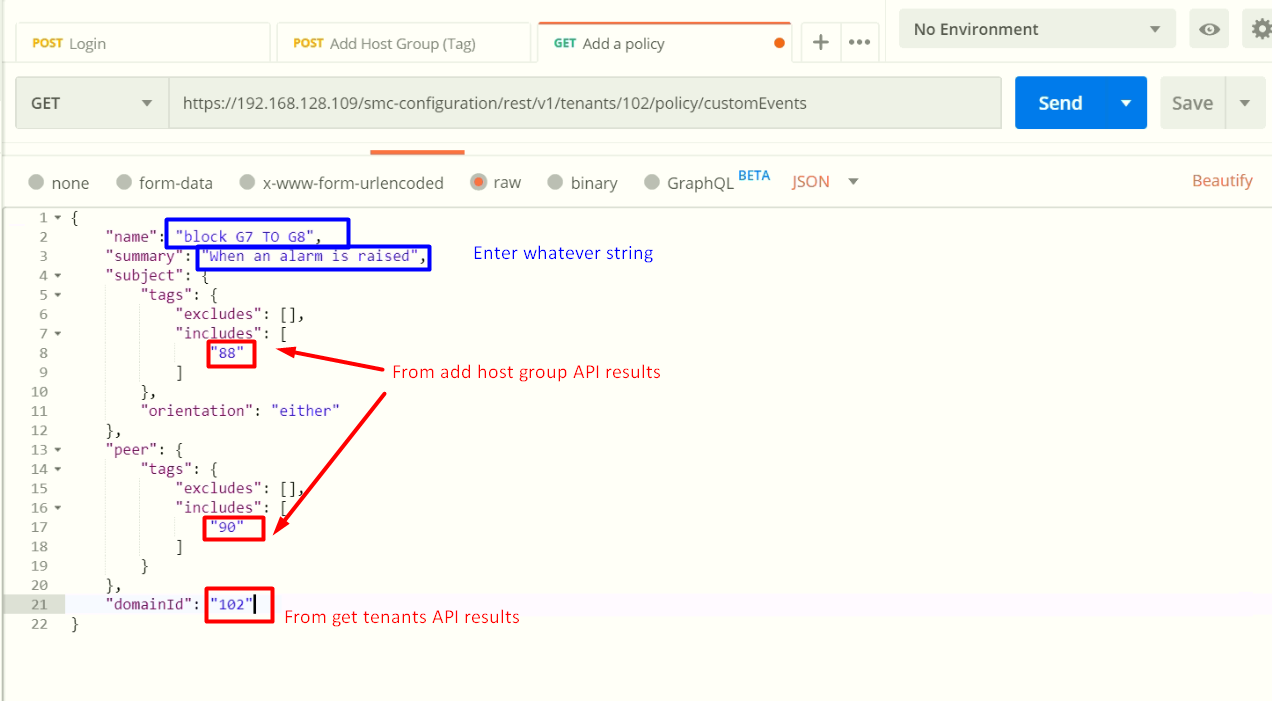
Add a policy between 2 host groups.



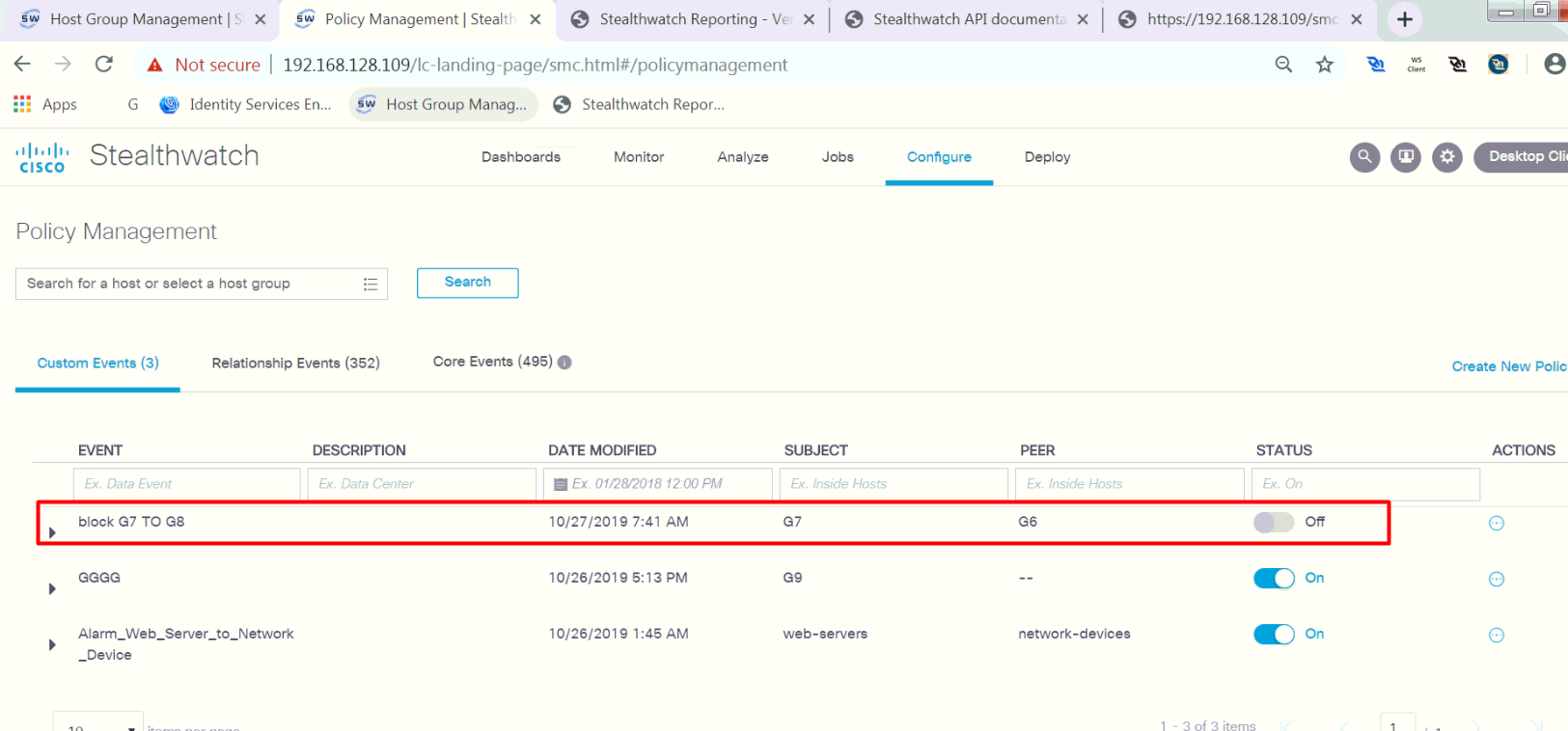
Add a policy





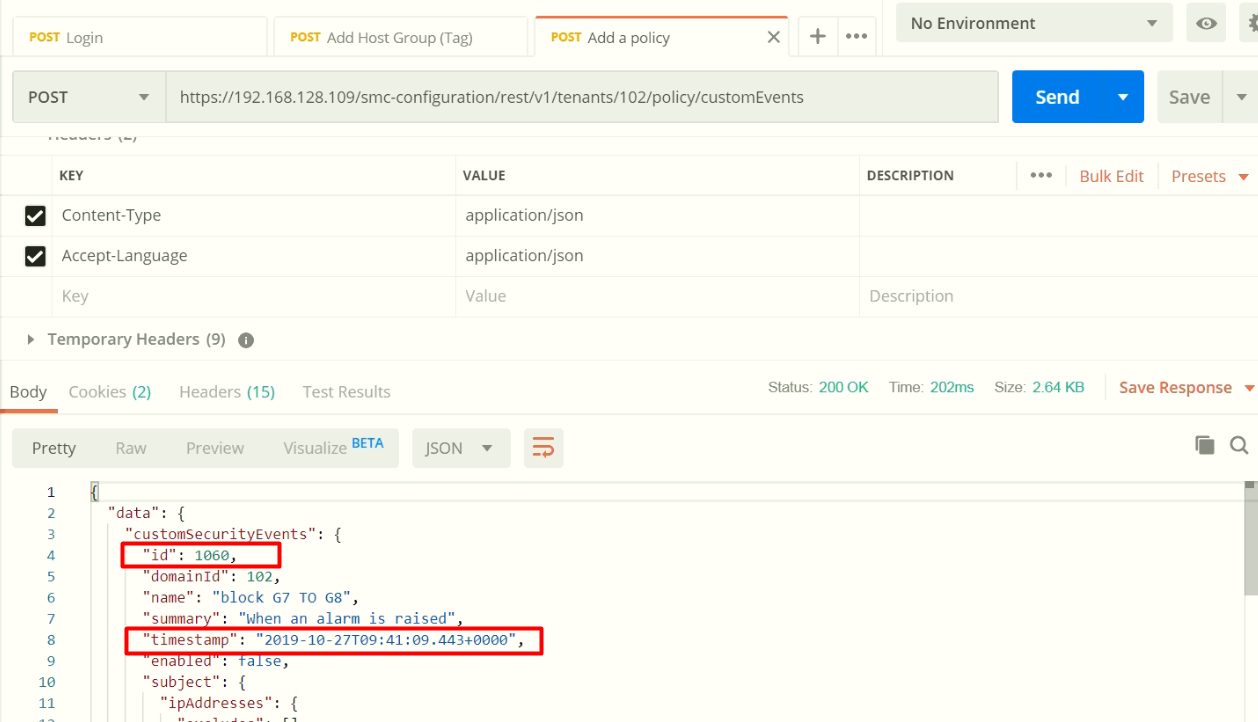


Now, created a policy as disabled state.

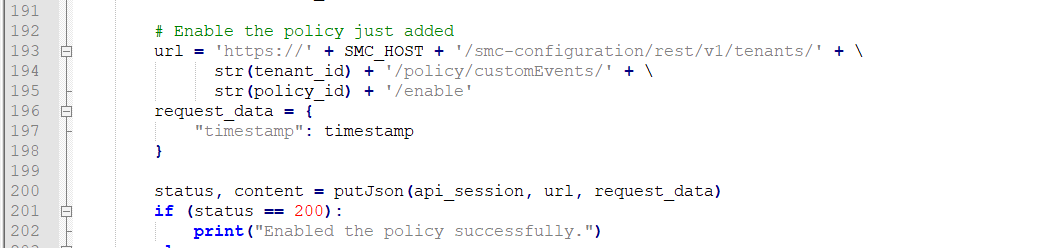


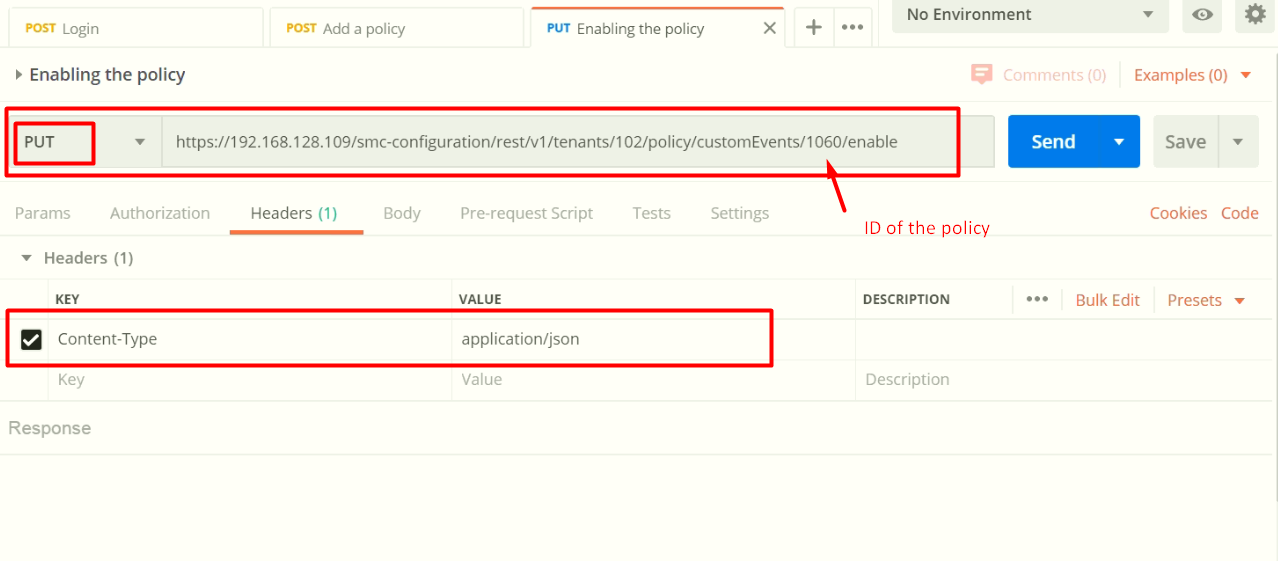
Remember the ID and timestamp of newly created policy.

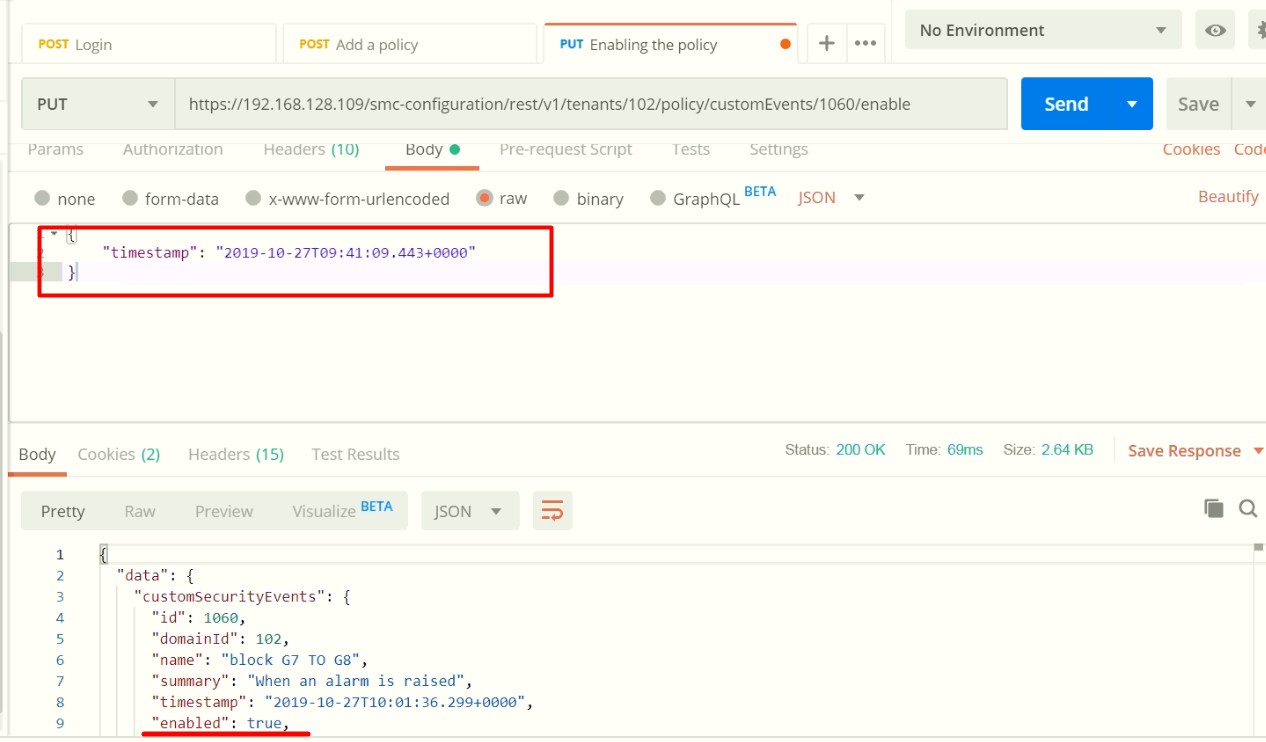
We will use it when enabling the policy.

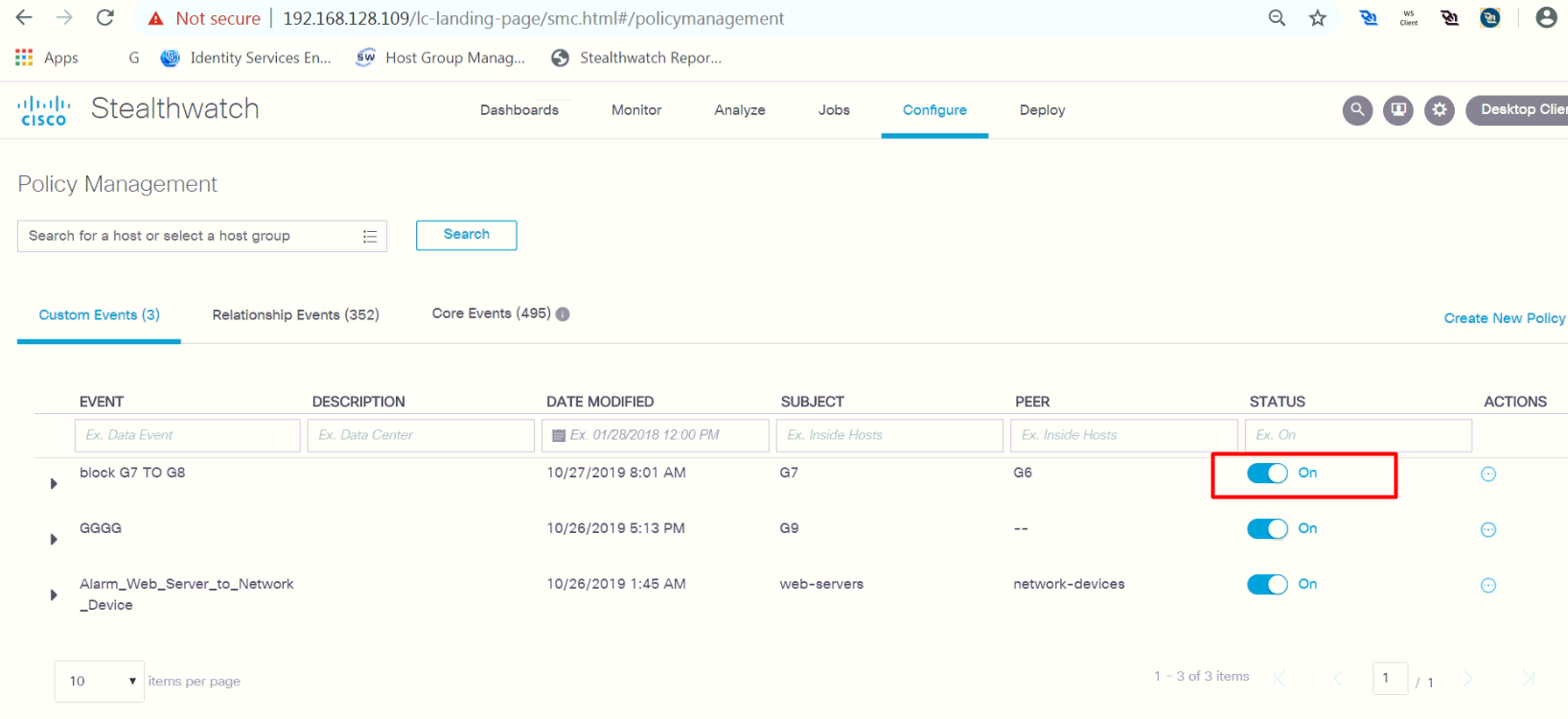


Enable the policy



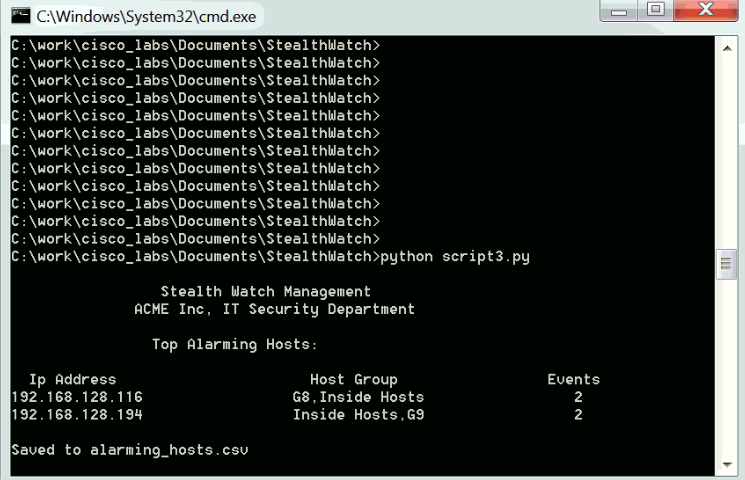




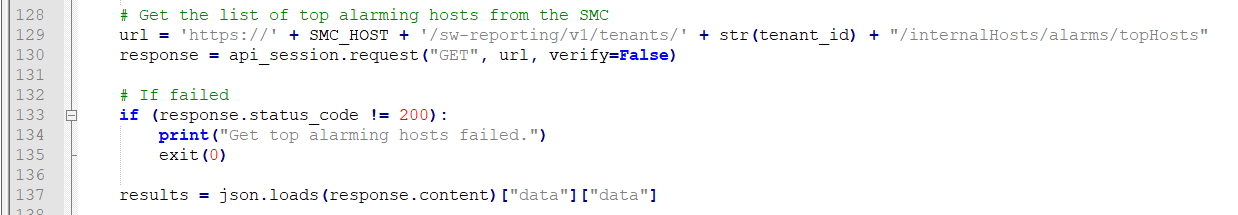


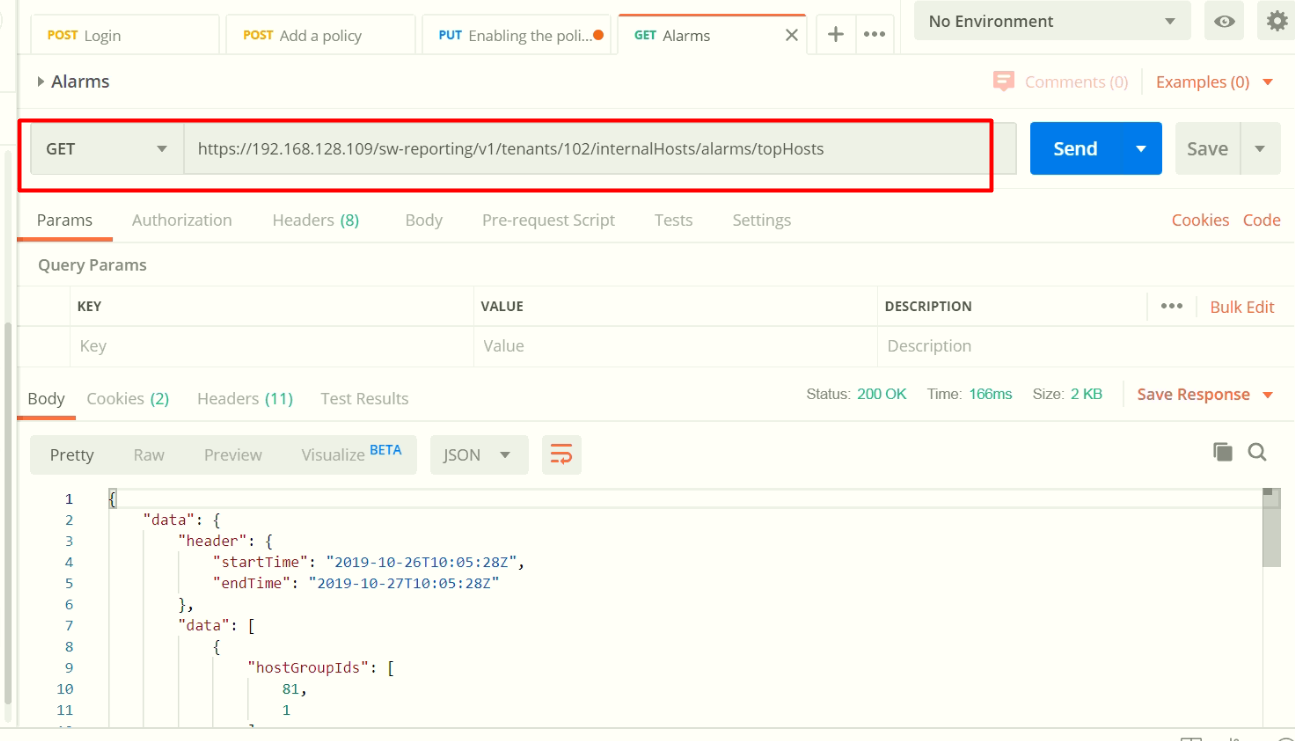
Script3.py

Print top alarming hosts and save as csv file.

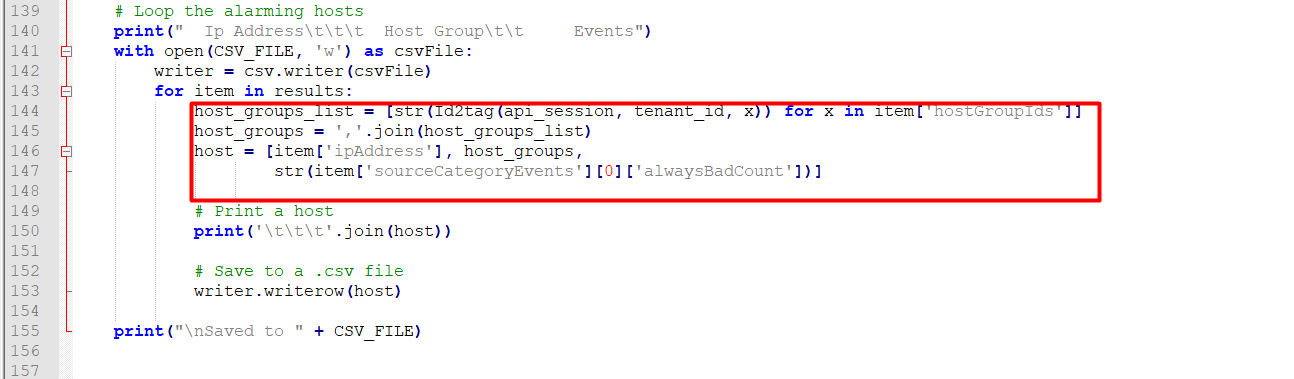


Get the top alarm hosts

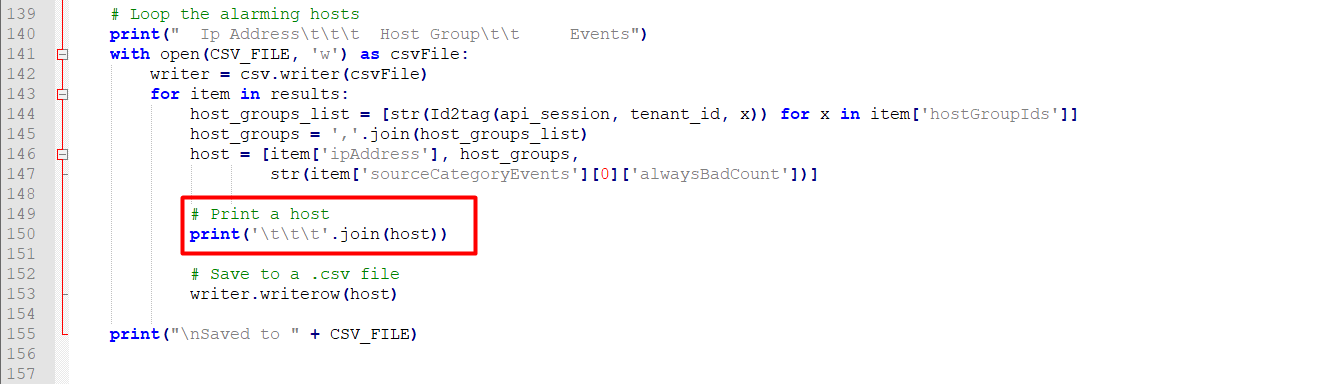




Data manipulation for output to screen and csv file.



Print to console



Save as csv file.

