FIREEYE ENDPOINT SECURITY POLICY API TOOL

Authored by Erin Hughes (erin.hughes@fireeye.com)

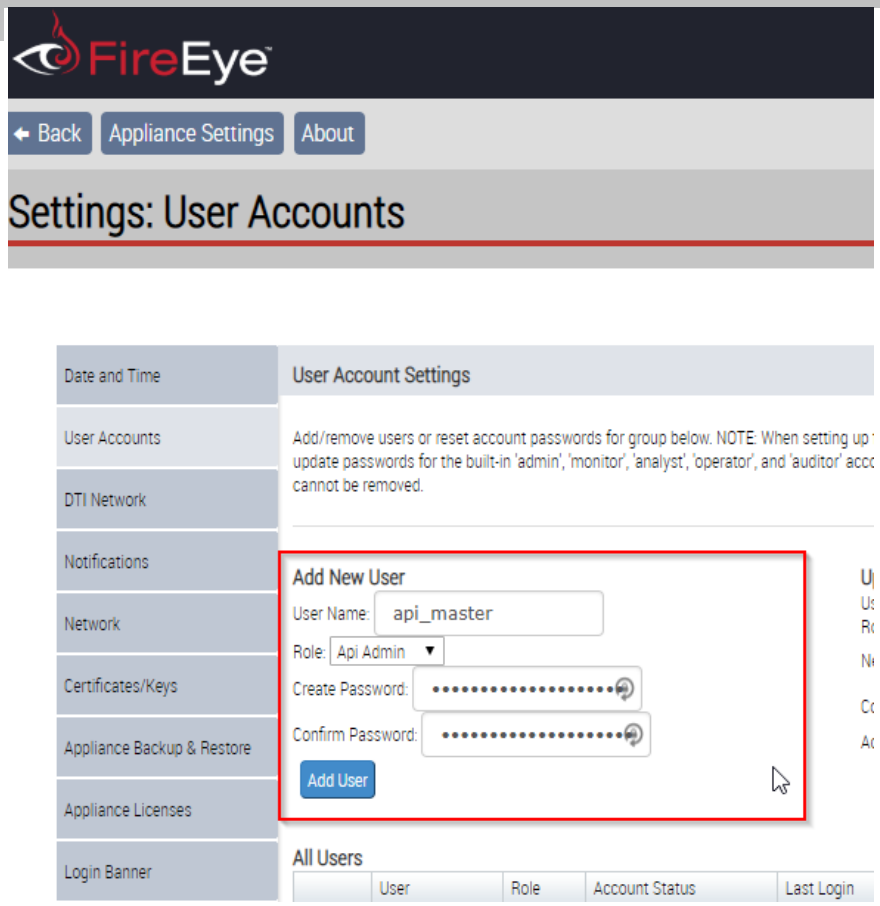
FireEye's Endpoint Security Policy API provides a rich API to allow users to explore functions within the API. The Policy API Tool allows users to add remove and list policy exceptions quickly as well as list create policies for the tool.

Overview

To get started with the API you will need to create an API user or API Admin to access the API. The API can not be accessed by normal system users.
API calls can be made with curl and at the beginning of every command section there is an example of what the commands accomplish.

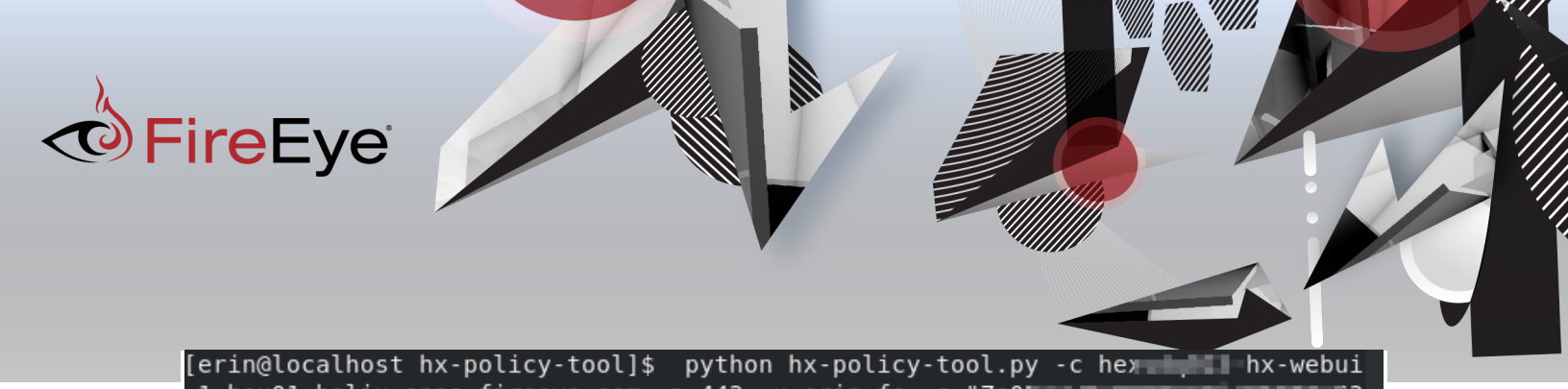
SETUP YOUR API ACCOUNT

An API_Analyst or API_Admin is needed to utilize the API accounts. To provision an API account on the host controller on the dashboard go to > Admin > Appliance Settings > Add New User > Set the Username > Select the Role "API_Admin" or "API_Analyst" > set the password (should be at least 25 characters with letters upper and lower case, numbers, and special characters).



POLICY TOOL COMMANDS

Running the hx-policy-tool.py with the -h commands lists all of the options.



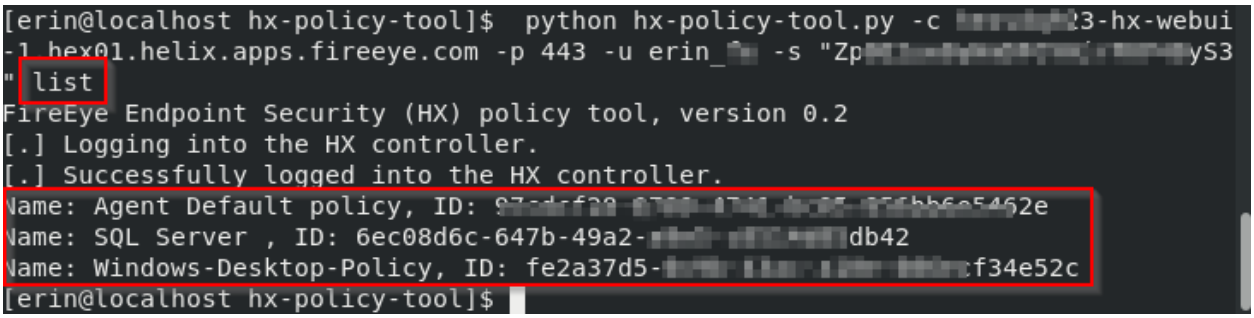
```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c hex[redacted] hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u erin_fe -s "Zp0[redacted]S3
" -h
usage: hx-policy-tool.py -h for more information.

FireEye Endpoint Security (HX) policy tool, version 0.2

positional arguments:
  {list,clone,export,import,external-import,rt-exclusions,mp-exclusions}
                        Options
    list                List policies
    clone               Clone policies
    export              Export policy
    import              Import policy
    external-import     Import exclusions from a line delimited text file
    rt-exclusions       Copy realtime exclusions from one policy to another
    mp-exclusions       Copy Malware Protection(A/V) exclusions from one
                        policy to another

optional arguments:
  -h, --help            show this help message and exit

main arguments:
  -c HX_HOST, --hx-host HX_HOST
                        The IP address or fully qualified domain name of the
                        HX controller to connect to. Required: True
  -p HX_PORT, --hx-port HX_PORT
                        The port on which to communicate with the HX
                        controller, defaults to: 3000. Required: False
  -u HX_USERNAME, --hx-user HX_USERNAME
                        The username with which to login to the HX controller.
                        Required: True
  -s HX_PASSWORD, --hx-password HX_PASSWORD
                        The password with which to login to the HX controller.
                        Note: if you do not supply one, you will be prompted
                        for one. Required: False
[erin@localhost hx-policy-tool]$
```

LIST POLICIES

List policies allows you to show what policies are available.

To use list;

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> list

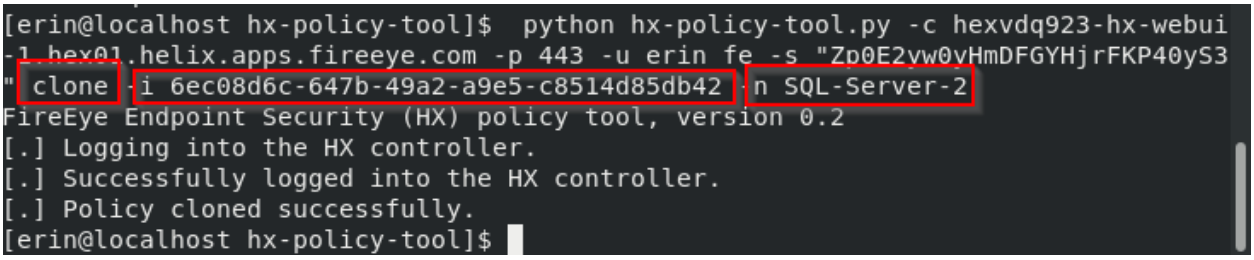


CLONE A POLICY

Clone allows you to make a copy of an existing policy.

To use clone;

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> clone -i <policy_id> -n <New Policy Name>



EXPORT POLICIES

Export takes the integer value of the Policy ID as an argument and then exports it in JSON format to an output file

To use export;

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> export -i <policy ID> -o <file name>

```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c h[redacted]-hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u [redacted] -s "[redacted]
" export -i fe2a37d5-0c9b-43ac-a10e-086ecf34e52c -o windows-policy.txt
FireEye Endpoint Security (HX) policy tool, version 0.2
[.] Logging into the HX controller.
[.] Successfully logged into the HX controller.
[.] Successfully wrote policy JSON for fe2a37d5-0c9b-43ac-a10e-086ecf34e52c to w
indows-policy.txt.
```

IMPORT A POLICIY

Import takes a file and allows you to import a JSON file with a complete policy in it.

To use import;

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> import -i <File Name>

```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c h[redacted]-hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u [redacted]e -s "Zp0E2[redacted]
" import -i windows-policy2.txt
FireEye Endpoint Security (HX) policy tool, version 0.2
[.] Logging into the HX controller.
[.] Successfully logged into the HX controller.
[.] Policy imported successfully.
```

EXTERNAL IMPORT

External Import is very useful if you want to update the exclusions for Real Time Indicators or Malware Guard. To overwrite existing rules with the new policy, -o flag, otherwise the new policies will append to the current one.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> external-import -i <file name> -t <type: md5, process, filepath> -d <Destination ID> -s <source: malware-protection, realtime>

```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c h[redacted]-hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u erin fe -s "Zp0[redacted]
" external-import -i import-path -t filepath -d 6ec08d6c-647b-49a2-a9e5-c8514d85
db42 -s malware-protection
FireEye Endpoint Security (HX) policy tool, version 0.2
[.] Logging into the HX controller.
[.] Successfully logged into the HX controller.
[.] Successfully imported Malware Protection exclusions from import-path to 6ec0
8d6c-647b-49a2-a9e5-c8514d85db42
```

The import file format is below

"C:\\\\Program Files\\\\Trend Micro*",

"C:\\\\Program Files\\\\avs\\\\bin*",

"\"C:\\Program Files\\receptor*\""

"C:\\\\Program Files\\\\ESET*",

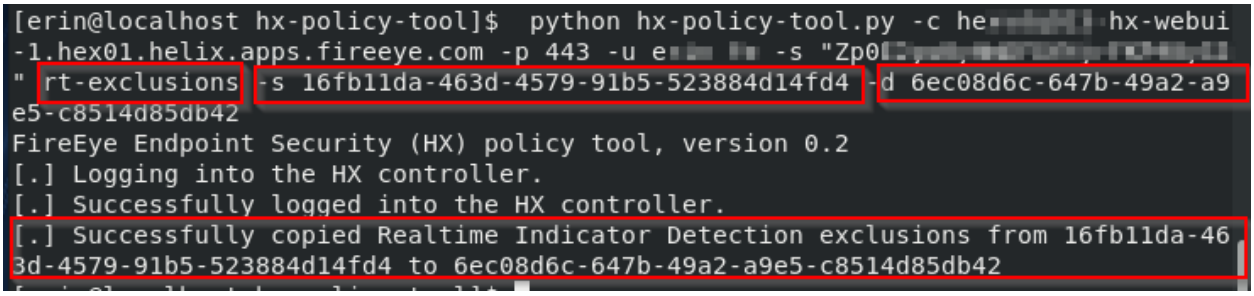
"C:\\\\Program Files\\\\aws\\\\bin*",

"C:\\Program Files\\bitdefender*\"";

REAL TIME EXCLUSIONS

RT-Exclusions are for copying Real Time Indicators of Compromise exclusions from one policy to another policy. To overwrite existing rules with the new policy, -o flag, otherwise the new policies will append to the current one.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> rt-exclusions -s <Source Policy> -d <Destination Policy>



MALWARE EXCLUSIONS

Malware-Exclusions are for copying Malware Exclusions from one policy to another policy. When copying Malware-Exclusions to overwrite existing rules with the new policy, -o flag, otherwise the new policies will append to the current one.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> ml-exclusions -s <Source Policy> -d <Destination Policy>