FIREEYE ENDPOINT SECURITY POLICY API TOOL

Authored by Erin Hughes (erin.hughes@fireeye.com) and Elazar Broad (elazar.broad@fireeye.com)

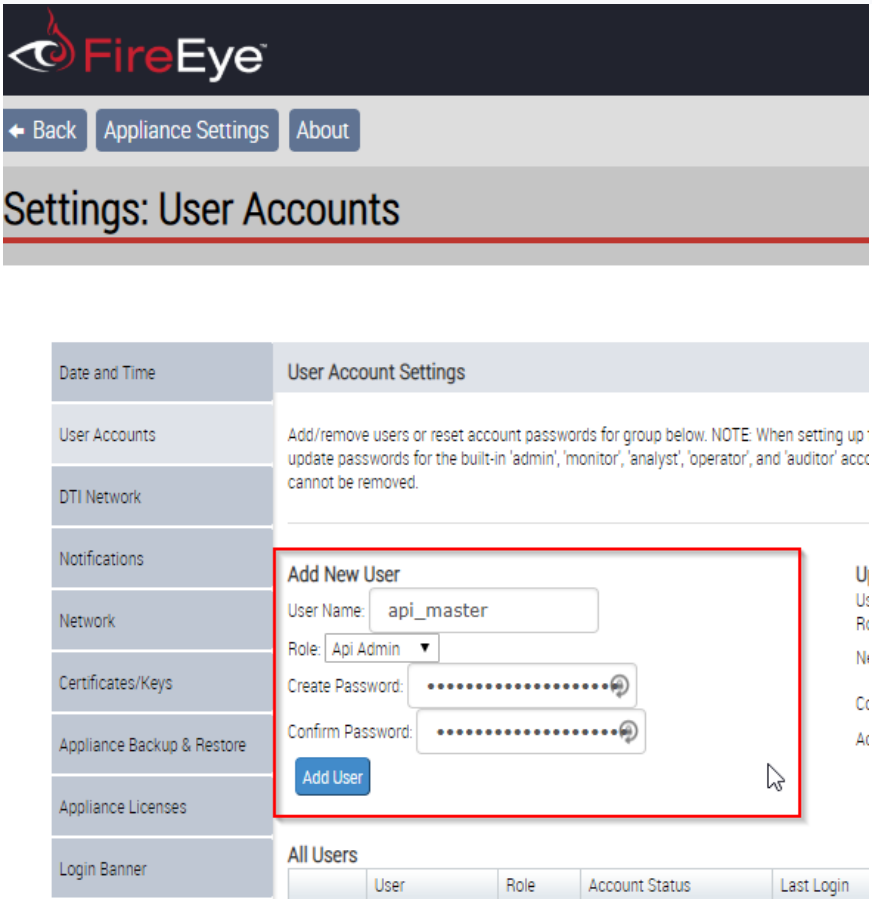
FireEye's Endpoint Security Policy API provides a rich API to allow users to explore functions within the API. The Policy API Tool allows users to add remove and list policy exceptions quickly as well as list create policies for the tool.

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.

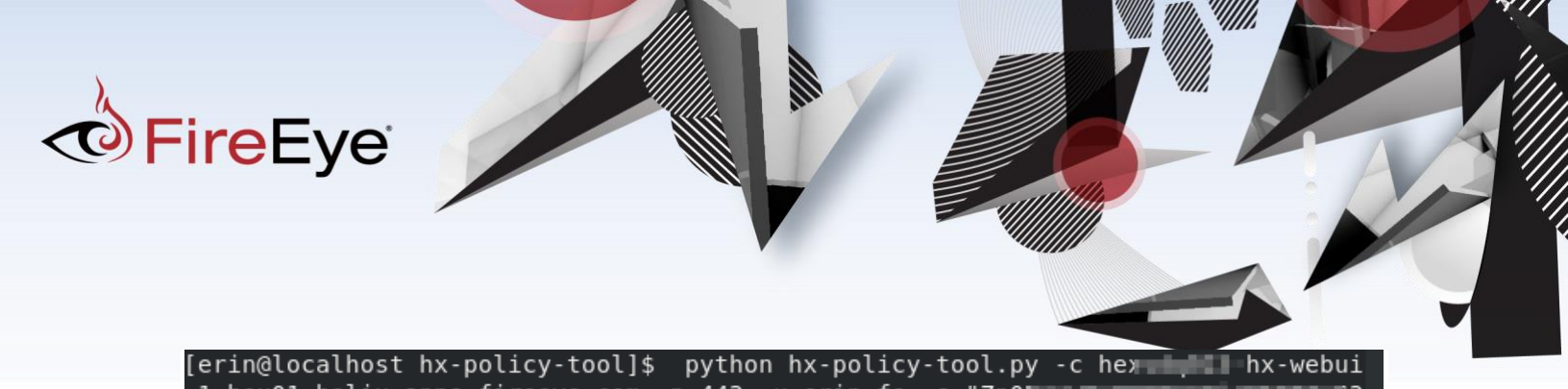
SETUP YOUR API ACCOUNT

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. Use the -P/--hx-proxy flag to utilize a proxy when communicating with the HX controller.



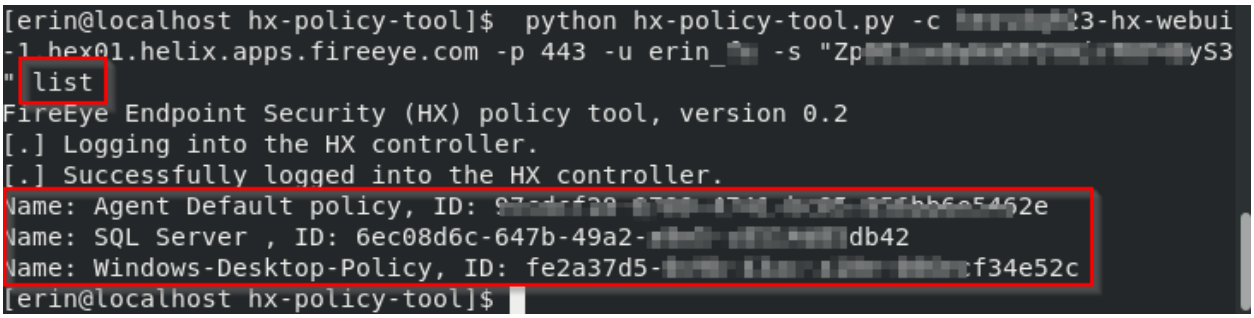
```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c hex[redacted] hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u erin_fe -s "Zp0[redacted]S3
" -h
usage: hx-policy-tool.py -h for more information.

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

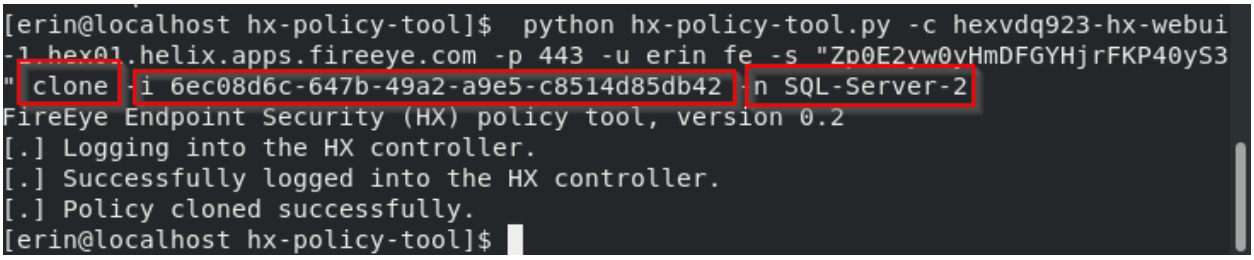


CLONE A POLICY

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>

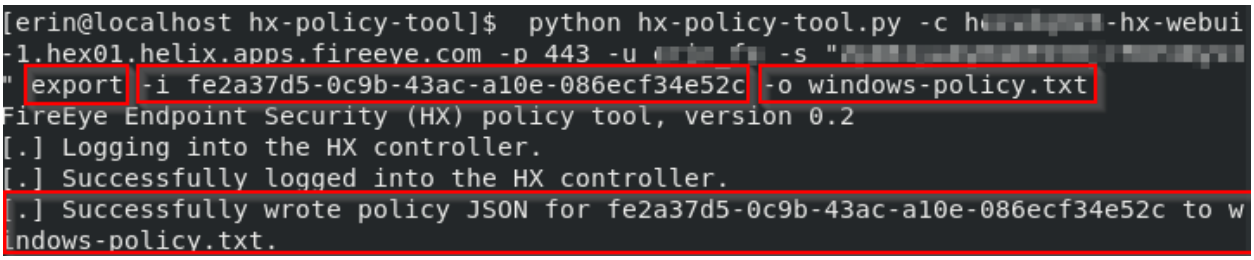


EXPORT POLICIES

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>

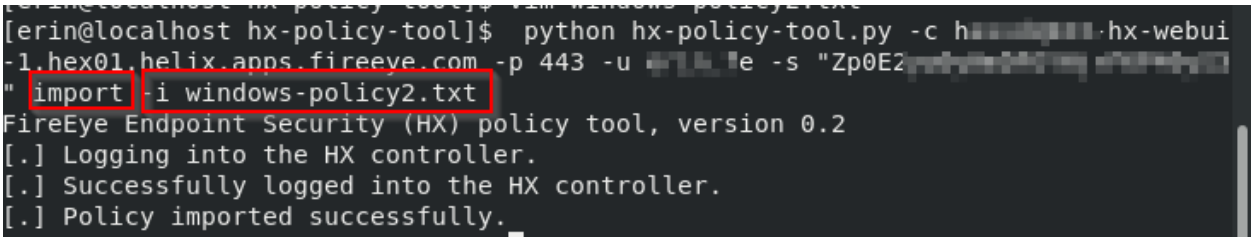


IMPORT A POLICY

Import takes a file and allows you to import a JSON file with a complete policy in it. NOTE: If a policy with the same name already exists on the controller the import will fail – use the -n flag to rename it.

To use import;

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> import -I <File Name> [-n policy name]



EXPORT ALL POLICIES

This feature allows one to export all policies on the controller to the path specified by -p/--output-path. The files will be named <Policy Name>.json.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> export -a -p <path to output policy files to>

IMPORT ALL POLICIES IN A DIRECTORY

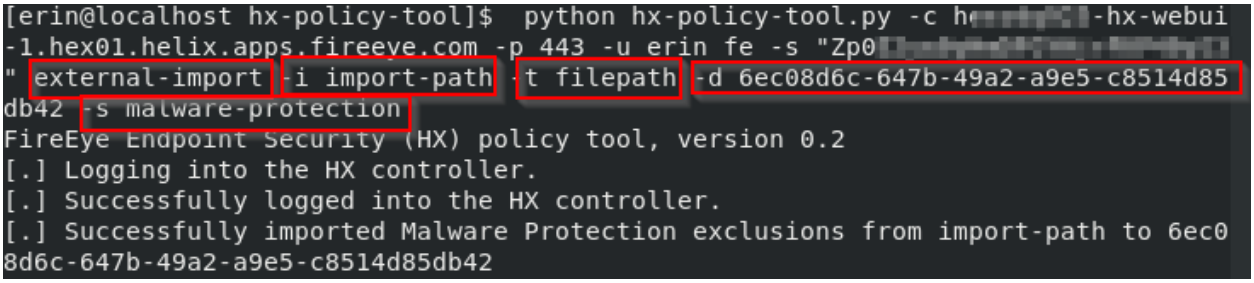
This feature allows one to import the resultant policy files of the export all policies command. This can be done by passing a wildcard to the -I/--input-file argument. Note that import will fail if a policy with the same name already exists on the controller.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> import -I *.json

EXCLUSION IMPORT

Exclusion import is very useful if you want to update the exclusions for a policy. To overwrite existing rules with the new policy, -o flag, otherwise the new policies will append to the current one. The import function can consume either a flat file or CSV format. For an example of all CSV items, export an existing policy.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> import-exclusions -I <file name> -f csv|flat -t <type: md5, process, filepath> -d <Destination ID> -s <source: malware-protection, realtime> -O <platform>



Flat file format:

"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*\"";

CSV Format:

item	item_type	module	platform
e930b05efe23891d19bc354a4209be3e	excludedMD5s	malware_protection	platform#win
C:\No_Scan*	excludedFiles	malware_protection	platform#win

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.

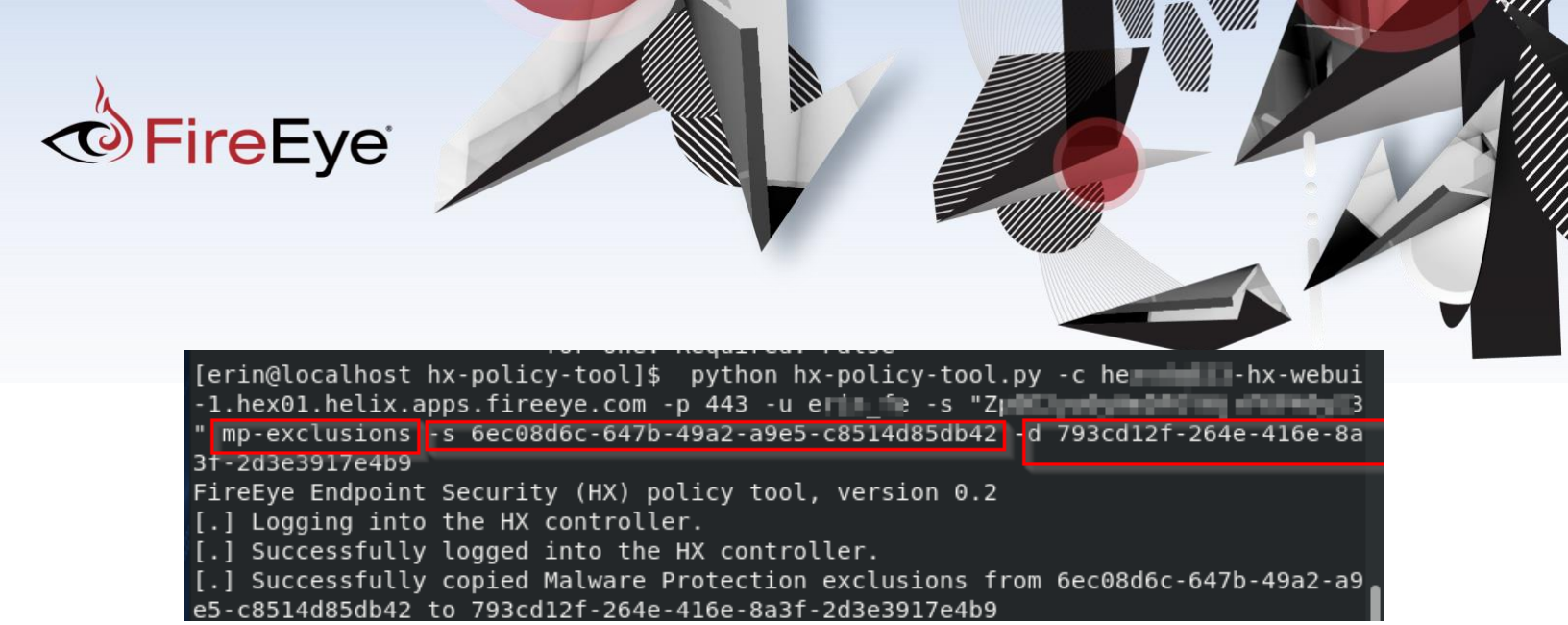
python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> rt-exclusions -s <Source Policy> -d <Destination Policy>

```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c he[redacted]hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u e[redacted] -s "Zp0[redacted]
" rt-exclusions -s 16fb11da-463d-4579-91b5-523884d14fd4 -d 6ec08d6c-647b-49a2-a9
e5-c8514d85db42
FireEye Endpoint Security (HX) policy tool, version 0.2
[.] Logging into the HX controller.
[.] Successfully logged into the HX controller.
[.] Successfully copied Realtime Indicator Detection exclusions from 16fb11da-46
3d-4579-91b5-523884d14fd4 to 6ec08d6c-647b-49a2-a9e5-c8514d85db42
```

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> mp-exclusions -s <Source Policy> -d <Destination Policy> -O <platform>



```
[erin@localhost hx-policy-tool]$  python hx-policy-tool.py -c he       -hx-webui
-1.hex01.helix.apps.fireeye.com -p 443 -u er     e -s "Z                    3
" mp-exclusions -s 6ec08d6c-647b-49a2-a9e5-c8514d85db42 -d 793cd12f-264e-416e-8a
3f-2d3e3917e4b9
FireEye Endpoint Security (HX) policy tool, version 0.2
[.] Logging into the HX controller.
[.] Successfully logged into the HX controller.
[.] Successfully copied Malware Protection exclusions from 6ec08d6c-647b-49a2-a9
e5-c8514d85db42 to 793cd12f-264e-416e-8a3f-2d3e3917e4b9
```

AGENT POLICY INFORMATION

The Agent Policy Information command allows one to display the host set membership of a single agent and the policies applied to those host sets.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> agent-policy -q <agent ID/hostname/IP address>

EXPORT EXCLUSIONS FROM A SINGLE POLICY

The Exclusion Export command allows one to export exclusions for all engines/modules to a CSV file.

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

EXPORT EXCLUSIONS FROM ALL POLICIES

The Exclusion Export command allows one to export exclusions for all engines/modules to a CSV file.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> export-exclusions -a -P <CSV output path>

EXPORT FALSE POSITIVES

The False Positive Export command allows one to export user defined false positives (items marked False Positive in the Endpoint Security Web UI)

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

IMPORT FALSE POSITIVES

The False Positive Import command allows one to import user defined false positives (items marked False Positive in the Endpoint Security Web UI). The format must be that of which is exported, see the export-fp command.

python hx-policy-tool.py -c <host> -p <port> -u <api_user> -s <PASSWORD> import-fp -I input file