HXTool 4.5

Technical documentation

FireEye, Inc. I 601 McCarthy Blvd. Milpitas, CA 95035 I 408.321.6300 I 877.FIREEYE (347.3393) I info@fireeye.com I www.fireeye.com

Chapter 1: Introduction **4**
What is HXTool 4
HXTool Features 4
Chapter 2: Before you start **6**
Things to consider 6
Requirements 6
Chapter 3: Installation **7**
Installing Python 7
Linux 7
Microsoft Windows 7
Apple MacOS 7
Acquiring HXTool software 8
Installing HXTool 8
Upgrading HXTool 8
Configuring HXTool 8
Running HXTool 9
Chapter 4: Account management **10**
Adding Endpoint Security consoles to HXTool 10
Setting up accounts in Endpoint Security 10
Logging in 11
Setting background processing credentials 11
Chapter 5: Using HXTool **13**
Dashboards 13
Alerts 15
Alert investigation panel 16
Find a host 16
Enterprise Search 17
Manage OpenIOC 18
Bulk acquisition 18

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

Script builder 20
Manage scripts 20
Task profiles 21
File writer 21
IP Sender 22
Upload to Helix 22
Multi-file acquisition 23
Data stacking 24
Indicators 26
Build 26
Manage 26
Categories 27
Custom configuration channel 27
Logging out 28
Chapter 6: License 29

CHAPTER 1: INTRODUCTION

WHAT IS HXTOOL

HXTool is an extended user interface for the FireEye HX Endpoint product. HXTool can be installed on a dedicated server or on your physical workstation. HXTool provides additional features and capabilities over the standard FireEye Endpoint Security web user interface. HXTool uses the fully documented REST API that comes with Endpoint Security for communication with the endpoint security environment.

HXTOOL FEATURES

HXTool current set of features

- Dashboard
  - Main operational dashboard
  - Agent dashboard
  - Anti-virus dashboard
- Alerts
  - Chronological alerts listing with selectable time range
  - Alert investigation panel
    view alerts per endpoint and access acquisitions
  - Event annotation and state
- Hosts
  - Find a host search bar
  - Contain, approve containment, stop containment
  - Triage and File acquisitions
  - Custom Data acquisition (based on script xml/json)
  - Remove hosts
- Enterprise Search
  - Run a search based on OpenIOC 1.1
  - Store OpenIOC 1.1 indicators in HXTool
  - Run searches based on schedule
    - Run now
    - Run at specific time/date
    - Run on an interval
- Script builder
  - Build acquisition scripts using all available xAgent audit modules
  - Improve set of parameters
  - Parameter descriptions
- Bulk acquisition
  - Run acquisitions against all hosts in a host-set
  - Background downloading of acquisitions to directory
  - Run bulk acquisitions on a schedule
    - Run now
    - Run at specific time/date
    - Run on an interval
  - Post processing modules for forwarding of collected data
    - File writer module to store data in local files
    - IP sender to stream collected data using TCP/UDP
    - Helix Upload
  - Use script stored in HXTool or from file
- Post-download handlers
  - Data stacking
    - Services
    - Processes
    - Scheduled tasks
    - Driver modules

        - Driver signature
        - Ports
        - Master boot record
        - Linux Ports
    - Multi-file acquisition
        - List files on all endpoints in a host-set using path and regular expression
        - Download selected files from listing results in one click
- Real-time indicators
    - Build new real-time indicators of compromise using full set of events and fields
    - View indicators
    - Clone indicators
    - Edit indicators
    - Export and import indicators
    - Manage indicator groups
- Custom configuration channel
    - Manage custom configuration channels (view, add, remove)
- Scheduler
    - View scheduler queue and status
    - Remove tasks from scheduler

CHAPTER 2: BEFORE YOU START

THINGS TO CONSIDER

HXTool is a Python application that requires an installation of Python on the machine where you want to run the application. You also need to install several libraries in Python so choose an install location where you are in control of the Python configuration. Also keep in mind that Python shipped with several operating systems may be used by the operating system itself, so the safest choice is to manage a separate environment for your download Python application such as HXTool. HXTool also supports Docker for easy installation

REQUIREMENTS

HXTool software requirements

- Python 2.7 or 3.x
- Python library: Flask
- Python library: Requests
- Python library: Pycryptodome
- Python library: TinyDB
- Python library: Pandas

HXTool hardware requirements

- 1 core
- 2Gb of RAM
- 1Gb of disk

Please note that hardware requirements differ greatly depending on how HXTool is used. The following capabilities will greatly increase the hardware requirements

- Bulk acquisition downloader
- Data stacking
- Multi-file acquisition
- Task processor
- A very high number of alerts that has to be processed (Dashboard, Alerts and alert investigation panel)

When heavily using these features in a shared environment a dedicated physical or virtual server is recommended.

CHAPTER 3: INSTALLATION

INSTALLING PYTHON

Python can be installed and used with many operating systems. This guide does not give you all the information that might be required in order to install Python on your workstation or server but please refer to the documentation available on the python website for further assistance.

LINUX

Many distributions come with a built-in Python installation. If the version of Python shipped with your operating system is sufficient and you are sure that installing additional Python libraries won't affect other software on the operating system you can go ahead and install the HXTool dependencies using the operating system utility to install software packages. These operating systems usually refers to this as "package-managers". Examples of these are "apt", "aptitude" and "yum".

As an alternative, you can install a separate Python installation on your operating system. Instructions how to do this is available on www.python.org. Please also note that PYENV might be useful in these situations. More information on PYENV here: https://github.com/pyenv/pyenv

MICROSOFT WINDOWS

Python is not shipped with Microsoft windows so you have to install it by downloading the software package from www.python.org. After download simply run the installer and install Python into a directory on your harddrive.

After installation of Python you sometimes need to acquire the additional tool called "pip" in order to install libraries in Python. The "pip" application is usually found in the "scripts" subfolder of your Python installation but can also be acquired by downloading this Python script:

https://pip.pypa.io/en/stable/installing/

After 'pip' has been installed you can install the additional libraries by running the following command:

"pip install <libraryname>"

APPLE MACOS

Apple MacOS comes shipped with Python 2.7. Our recommendation on MacOS is to install a separate Python environment and use that for HXTool.

Head on over to: https://brew.sh/ and read up on "Homebrew" which allows you to install both Python2 and Python3 and manage them as separate environments on your Mac.

ACQUIRING HXTOOL SOFTWARE

HXTool can be downloaded from the FireEye Market. Go to the following URL:

https://fireeye.market/apps/211931

Download the latest HXTool zip-file.

INSTALLING HXTOOL

Once you have the HXTool zip-file we can go ahead and install HXTool into its destination directory.

1. Create a new directory on your hard drive
2. Unzip the contents of the HXTool zip-file into this directory

UPGRADING HXTOOL

Download the new HXTool version from the FireEye Market and un-zip it to a new directory.

1. Stop the old version of HXTool
2. Copy the file hxtool.db from your old installation directory to the new installation directory
3. Start the new version of HXTool

CONFIGURING HXTOOL

Before you run HXTool for the first time you need to review the configuration and also make sure your machine can communicate with the FireEye Endpoint Security console properly.

You should be able to access the FireEye Endpoint Security Web user interface from the machine you are installing HXTool on. The address to the Endpoint Security WebUI is usually https://<hostname>:3000. Please note that if you are using a proxy server there might be additional configuration required in the HXTool configuration file.

Now we need to review the settings in the HXTool configuration file. Open the file conf.json in a text-editor.

HXTool configuration file reference

Module	Item	Description
log_handlers	rotating_file_handler	Default log mechanism, stores logs to files
	file	Name of the master log file
	max_bytes	Max size of the log file until its archived
	backup_count	The number of archived files to store
	level	The HXTool log level
	format	The log format used by the logging mechanism
network	ssl	Enabled for HTTPS and disabled for HTTP
	port	The TCP port HXTool will listen on
	listen_address	The interface HXTool will listen on (0.0.0.0 = all interfaces)
ssl	cert	The name of the certificate file used when you have ssl enabled

Module	Item	Description
	key	The name of the key file used when you have ssl enabled
background_processor	poll_interval	The number of seconds between each poll done by the background processor threads
	poll_threads	The number of simultaneous background processor threads. Set this to the number of CPU cores you have on the system
headers	<header>	If you need to pass specific headers in the API requests add them here
cookies	<cookie>	If you need to pass specific cookies in the API requests add them here

RUNNING HXTOOL

After configuration and installation is completed you can go ahead and start HXTool.

"python hxtool.py"

Please note that the name of the Python application can be different depending on operating system and how you installed Python. Common names are "python2" and "python3"

Make sure HXTool works by pointing your web-browser to the URL of HXTool:

https://<hostname>:<configured port>/

You should see the HXTool login screen.

Recommended web browsers

- Google Chrome
- Firefox
- Safari

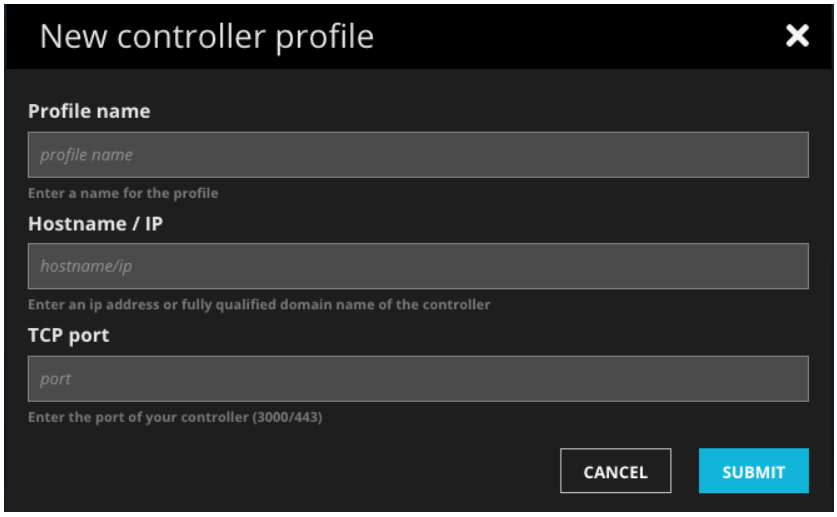
CHAPTER 4: ACCOUNT MANAGEMENT

ADDING ENDPOINT SECURITY CONSOLES TO HXTOOL

In order to use HXTool you must configure a profile on the HXTool login page to tell HXTool where to connect to. HXTool supports several profiles but you can only login to one profile at a time.

How to add a new profile

1. Go to the HXTool login page.
2. Click “New”
3. Enter name, hostname/ip and port in the dialogue
4. The default port for endpoint security API is always 3000, this might be different if endpoint security is located behind a proxy server/reverse proxy or if you are using the cloud version of endpoint security or Helix. Cloud endpoint security and Helix uses port 443.
5. Click “Submit”



SETTING UP ACCOUNTS IN ENDPOINT SECURITY

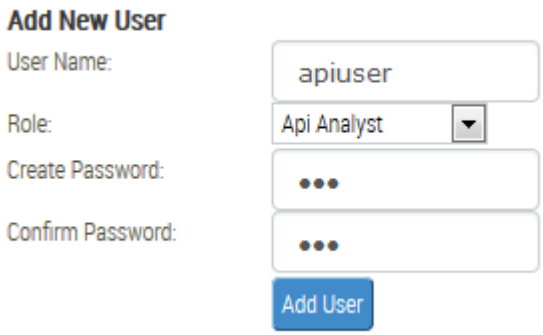
In order to login you need credentials for the Endpoint Security Controller you have selected on the login page. Only two account roles are valid for HXTool and those are

- API Analyst
  - API Analysts has access to all HXTool features except full containment and custom configuration channels
- API Admin
  - API Admins can access all HXTool capabilities. When an API admin contains a host both the request and approval happen at the same time

To setup a new account login as an administrator to the endpoint security web user interface and follow these steps:

- Click “Admin->Appliance settings”

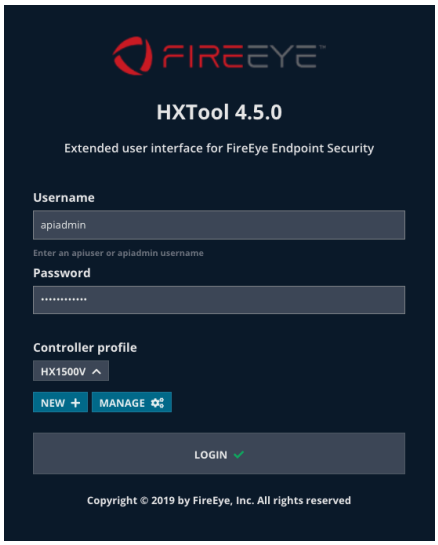
- Click “User accounts”
- Add a new user and choose the role “api analyst” or “api admin”
- Set a password and click “add user”



FireEye Endpoint Security “Add new user”

LOGGING IN

To login simply provide the username and password and select the proper controller profile in the drop-down list and click “Login”



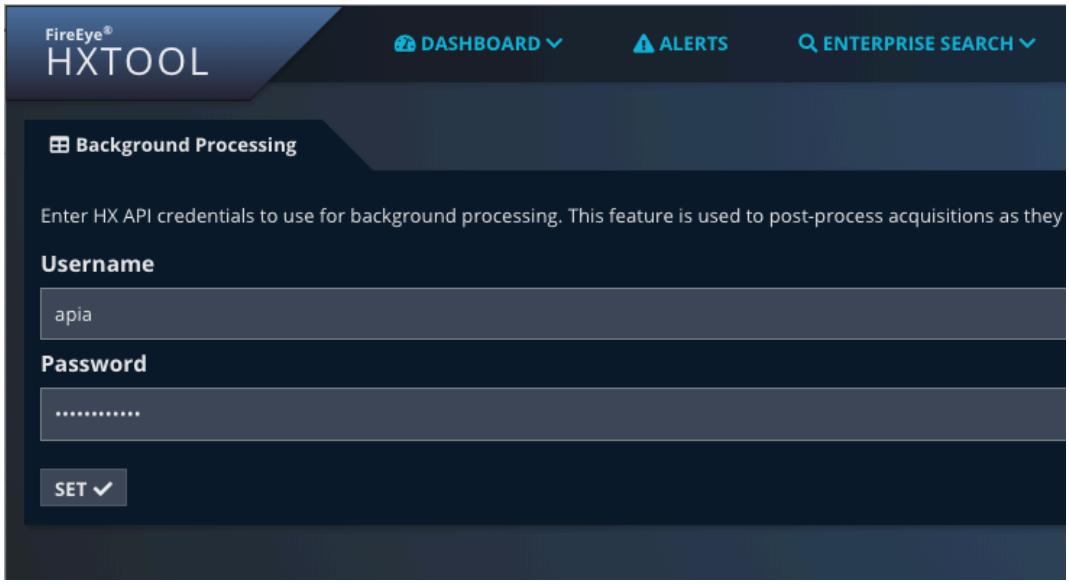
SETTING BACKGROUND PROCESSING CREDENTIALS

In order to utilize the following features, you have to set credentials to allow HXTool to communicate with the endpoint security profile/controller when you are not logged into HXTool. We recommend creating a service account for this task.

To set the background processing credentials

- Login to the controller in HXTool
- Click Admin->HXTool settings
- Provide a username and password valid for the controller (api_analyst role)

Save the credentials



CHAPTER 5: USING HXTOOL

DASHBOARDS

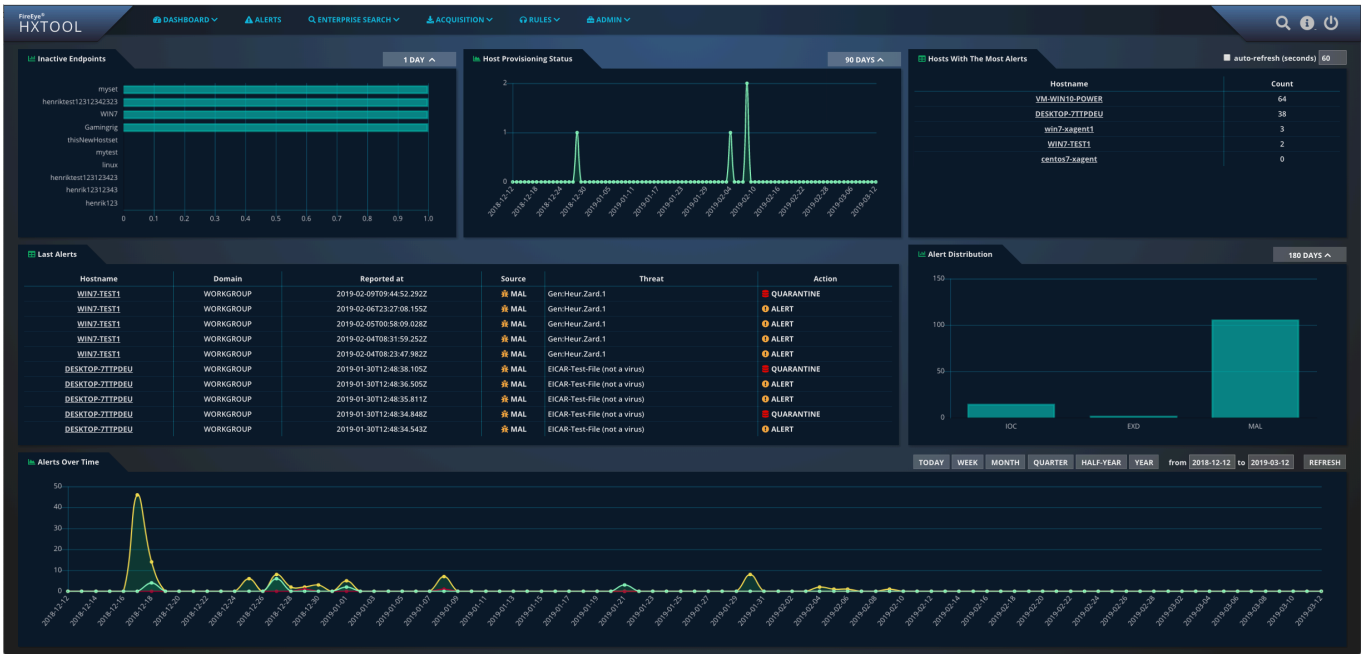
The dashboards can be accessed by clicking the dashboard navigation bar on the menu.

The dashboards show you information and statistics in your FireEye Endpoint Security environment.

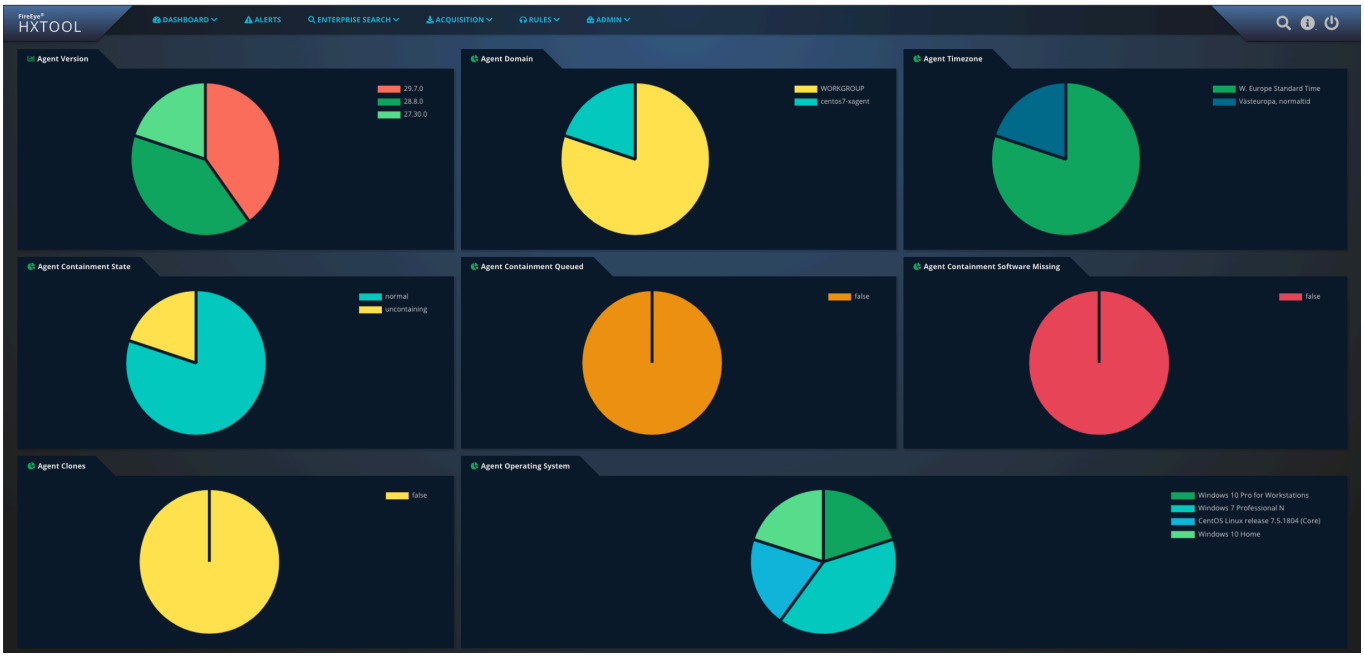
Some panels allow interaction where you can choose time periods and other settings. When changing this the panels update automatically.

By selecting the checkbox “auto” that panel will auto-refresh

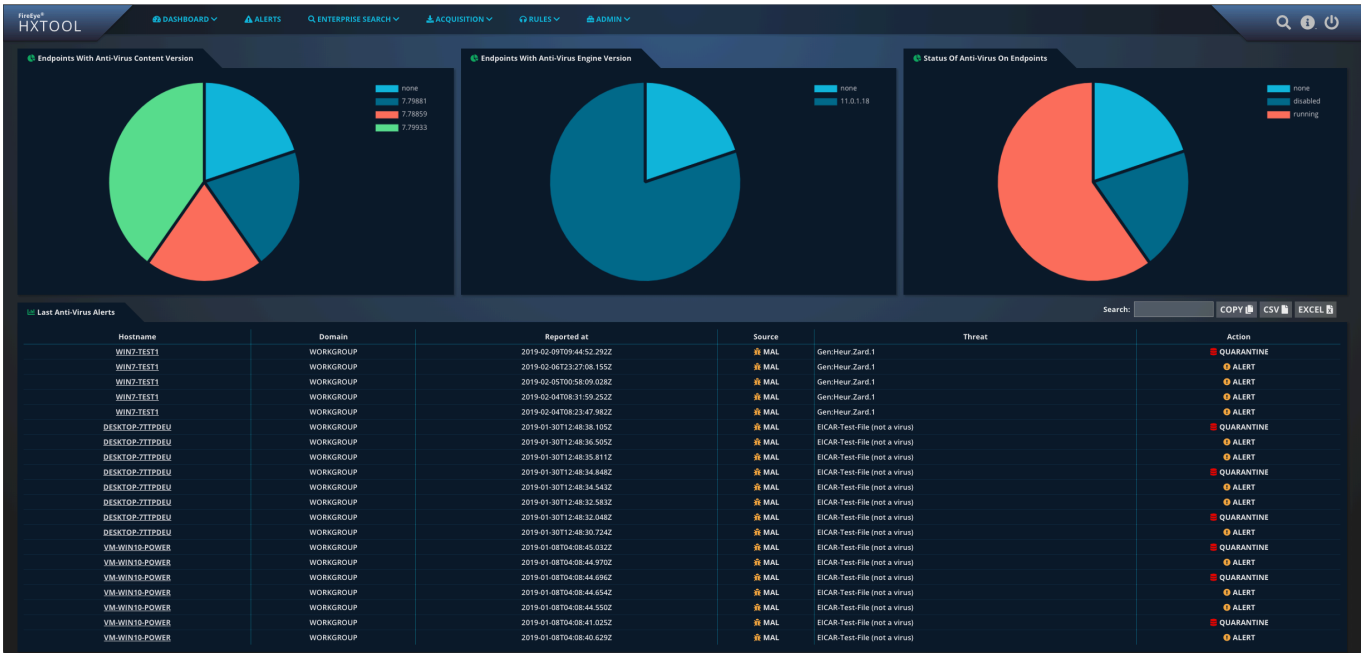
By clicking on the host-name you will navigate to the alert investigation panel for that host



Main dashboard



Agent dashboard



Antivirus Dashboard

ALERTS

The alerts feature can be accessed by clicking the alerts link on the menu.

The alerts feature shows you an alert feed from the FireEye Endpoint Security sorted in chronological order with descending timestamp.

Alerts can be annotated with a specific status. To annotate an alert, click the “annotate” button, type in your text and select either “investigating” or “completed” as status.

Annotated alerts will have another background color to them.

Yellow: Alert is under investigation

Green: Investigation completed.

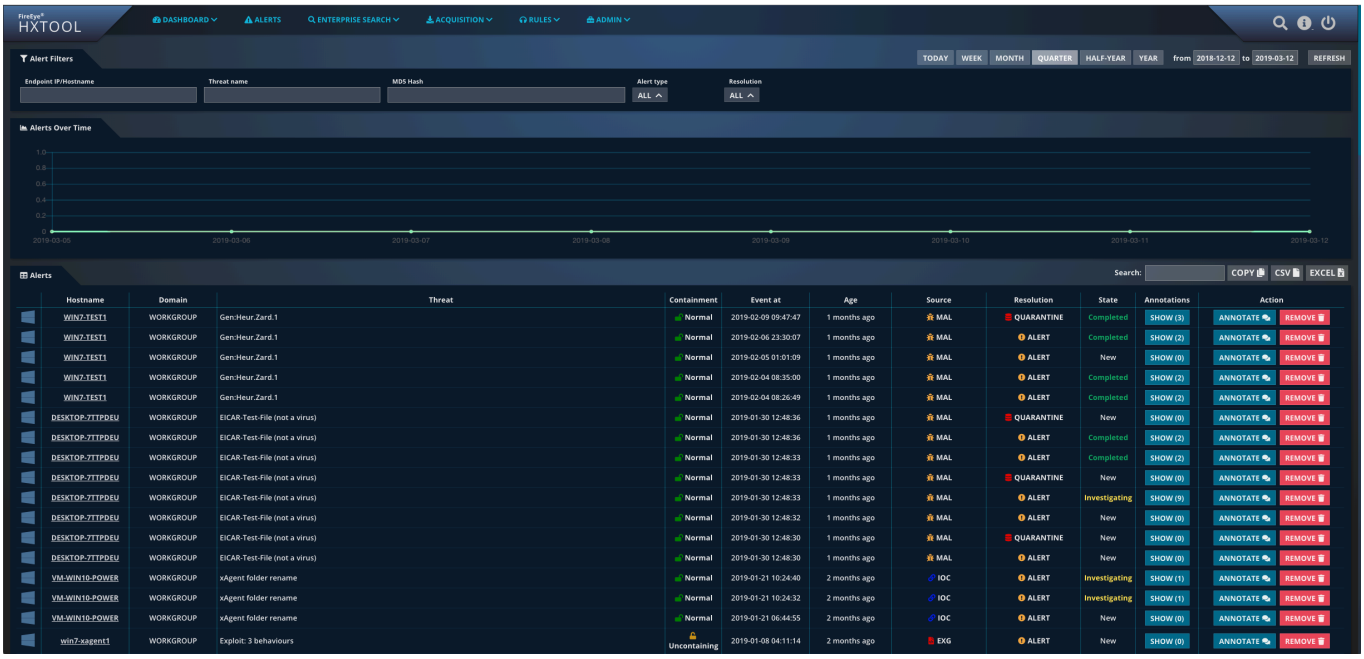
The button “HX” will open a new tab in your browser and navigate to the host investigation view of the agent that reported the alert.

By clicking on the host-name you will navigate to the alert investigation panel for that host.

The buttons at the top of the page controls which time-period that is to be shown. A user defined time period can also be chosen by inputting values in the from and to boxes and then selecting “refresh”

Filtering is available for hostname/ip, threat name, MD5 hash, alert type and resolution.

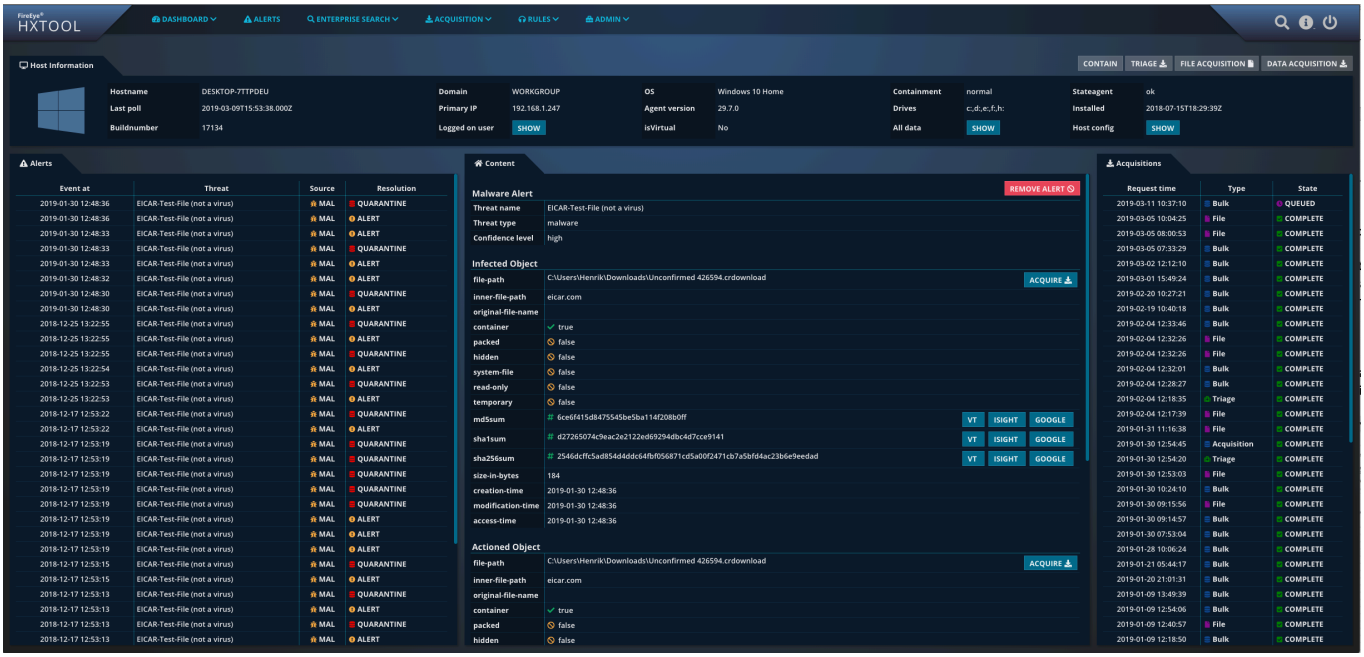
The copy button allows you to copy all alerts shown to the clipboard and CSV/Excel downloads the information in CSV or Excel file formats.



ALERT INVESTIGATION PANEL

The alert investigation panel is a drill-down view where you can see the following information

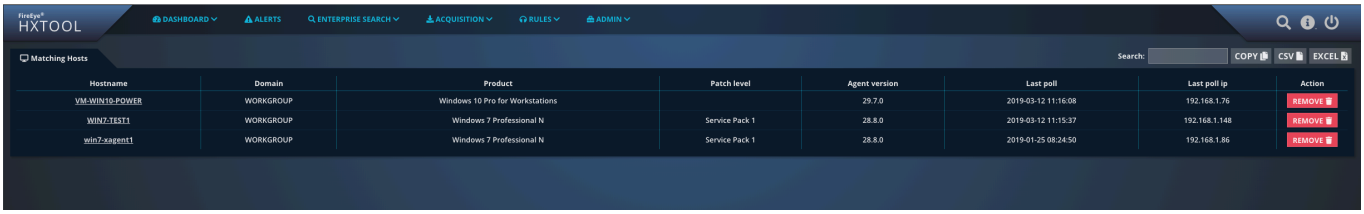
- Host information
- List of recent alerts
- Alert action (alert / block)
- Granular alert information
- Containment, triage, file and data acquisition capability
- Triage acquisition, File acquisition and Data acquisition results



FIND A HOST

On the top of the screen you can always see the “magnification icon”. To use this functionality simply enter a search string into the field and hit the “enter” button.

A list of hits for your search will be shown on the screen. From this view you can pivot to the alert investigation panel or remove the host from the endpoint security environment



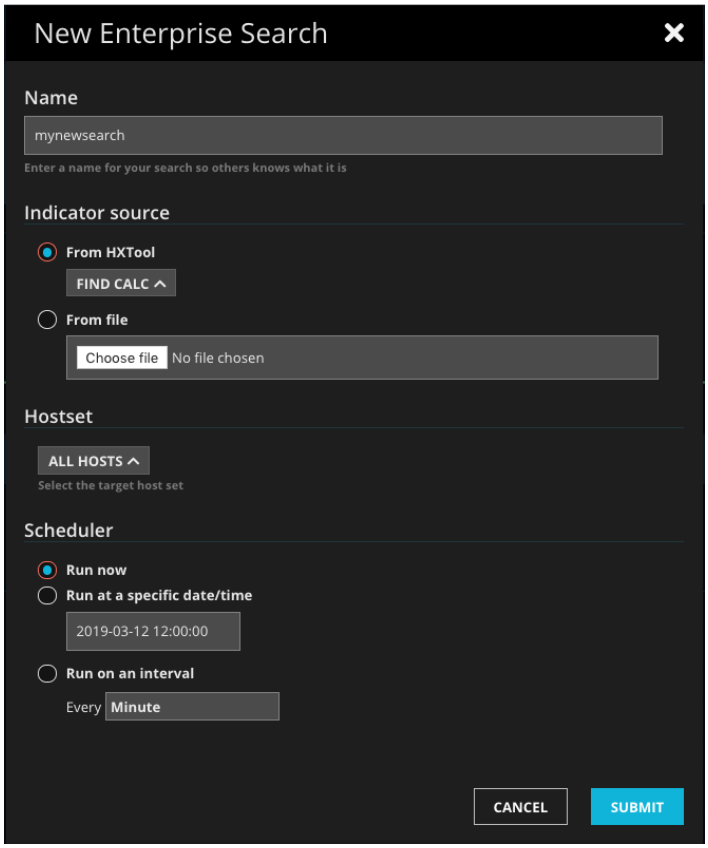
ENTERPRISE SEARCH

The enterprise search feature can be accessed by clicking the Enterprise Search link on the menu.

Please note that you need to set background processing credentials to use this feature.

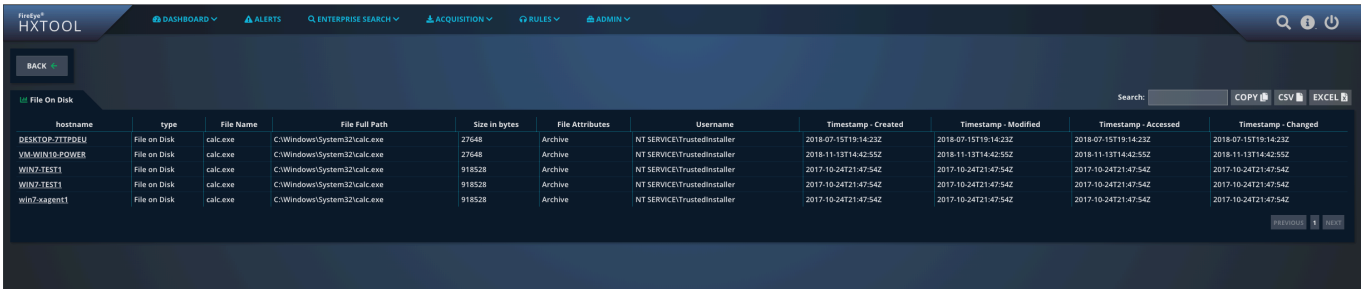
This feature allows you to start an Enterprise Search in Endpoint Security based on an OpenIOC file instead of ad-hoc query. To use this feature, you need an OpenIOC 1.1 file.

- Click “From file” and select your OpenIOC file or select an indicator from the drop-down menu “From HXTool”
- The option “skip unsupported terms” will be available if you are using FireEye Endpoint Security 4.5 or later. This feature allows the system to filter out non-supported terms from your indicator automatically.
- Select the target host-set
- Choose if you want the search to start immediately, in the future or run on an interval.
- Click the “Start Enterprise search” button
- A new Enterprise Search will now start and it will be listed in the table below
- To view the results of the enterprise search, click the line in the table or access the endpoint security WebUI and view it there.



To show the results of an acquisition hover over a row in the table and click the row

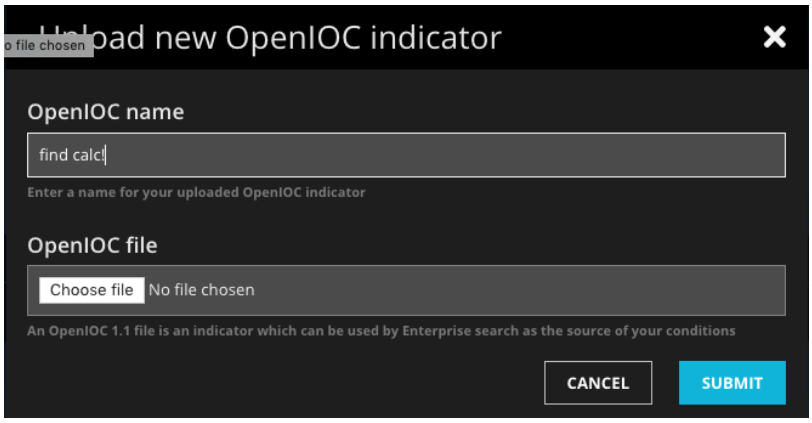
The results will then be showed in a drill-down view



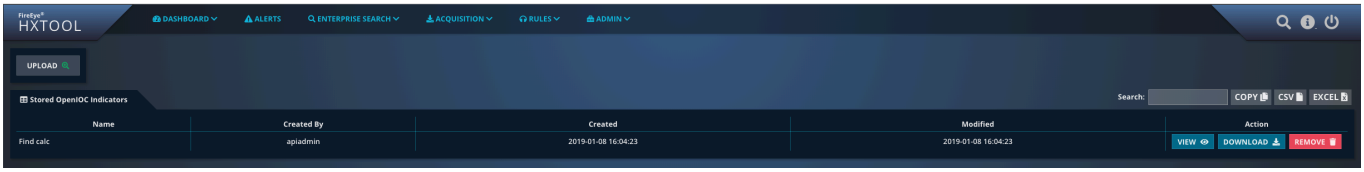
MANAGE OPENIOC

This feature allows the user to upload OpenIOC 1.1 indicators to HXTool for future use.

1. Choose a name for the indicator
2. Click on “choose file” and select the indicator you want to upload and store within HXTool
3. Click “Upload IOC”



From this page you can also view, download and delete indicators by clicking on their respective buttons



BULK ACQUISITION

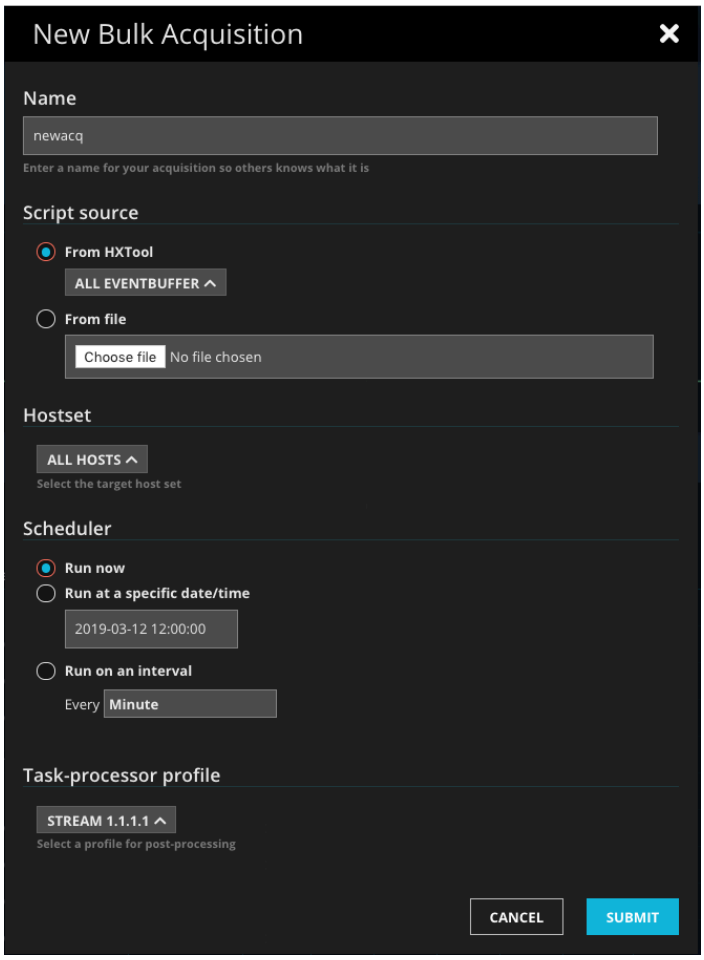
The bulk acquisition feature can be accessed by clicking the “Bulk Acquisition” link on the menu.

Please note that you need to set background processing credentials to use this feature.

This feature allows you to start a data acquisition for an entire host-set in HX.

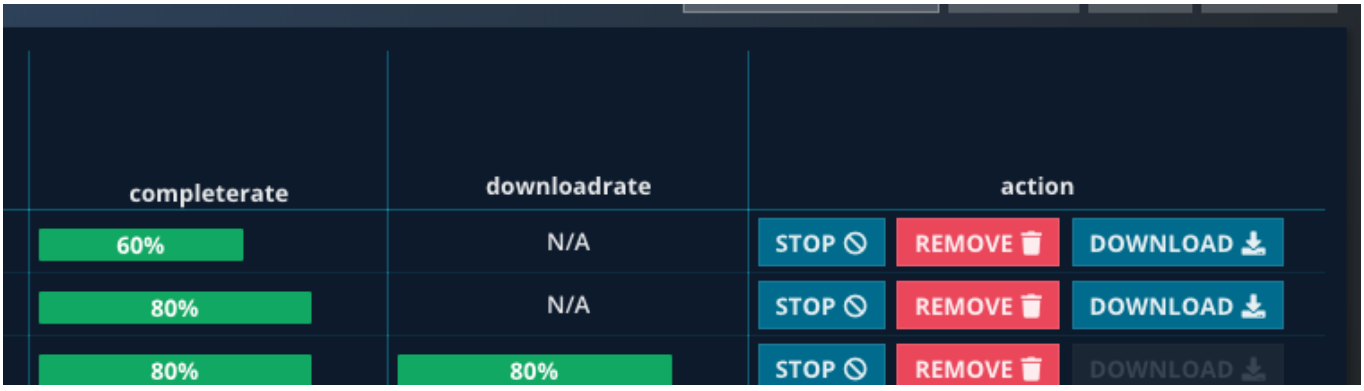
1. Click “From file” and select a valid acquisition script for FireEye HX. You can download these in the FireEye Endpoint Security WebUI by accessing “Data acquisition scripts” under the admin tab, create them manually or build them in HXTool by accessing the script builder.
2. Provide a comment so others can easily identify your bulk acquisition
3. Select a target host-set

4. Choose to run the bulk acquisition now, in the future or on an interval
5. If desired check the “use task-processor profile” checkbox and choose a task-processor profile. These profiles allow post-processing of acquired results such as store all acquired data in a file or stream the data to another destination. See task-processor profiles.
6. Click Start bulk acquisition



You can monitor the acquisition progress in the table below and also drill-down into the results by clicking the corresponding line in the table to your acquisition.

To download acquisition results, click the “Download acquisition” link.



Bulk Acquisition actions

- If you want to download all acquisitions results in the background click on the “download” button next to the bulk acquisition
- If you want to stop the bulk acquisition and cancel all acquisition jobs not completed click the “stop” button
- If you want to stop the bulk acquisition and remove all results from the controller click the “remove button”

When you click download the background processor will place all your files in the bulkdownload/ directory. Each bulk acquisition has its own directory indicated by the name of the profile and the ID of the acquisition

SCRIPT BUILDER

This feature allows you to construct and build acquisitions scripts that can be used with the feature Bulk acquisition.

To build a new acquisition script:

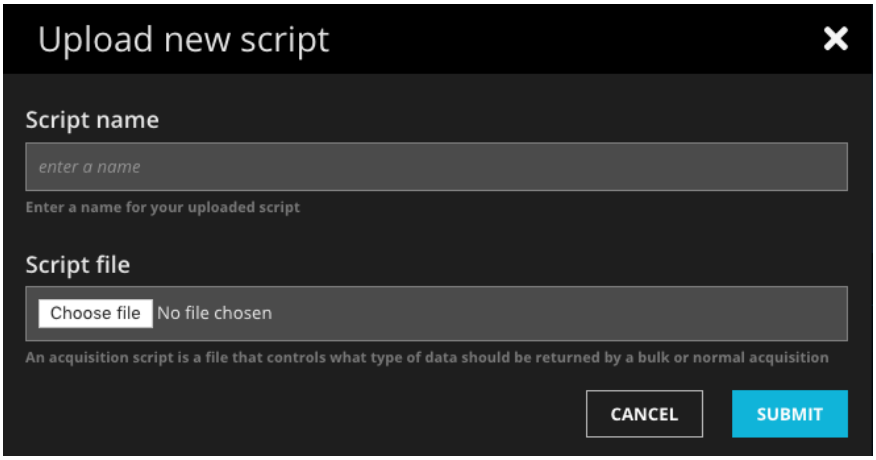
1. Enter a name for your script in the “script name” field
2. Choose the platform you want to create a script for
3. Click the drop-down menu “audit modules” and select the audit module you want to add to your script. This action can be repeated to add more than one audit module to your script
4. Enter values into each parameter of your script
5. Optional values can be removed if desired. This is done by clicking the trashcan icon next to the parameter name
6. Some parameters can be repeated. When this is available you will see the “repeat” button appear.
7. Click “create script”. Your script will now be stored in the HXTool script store.

MANAGE SCRIPTS

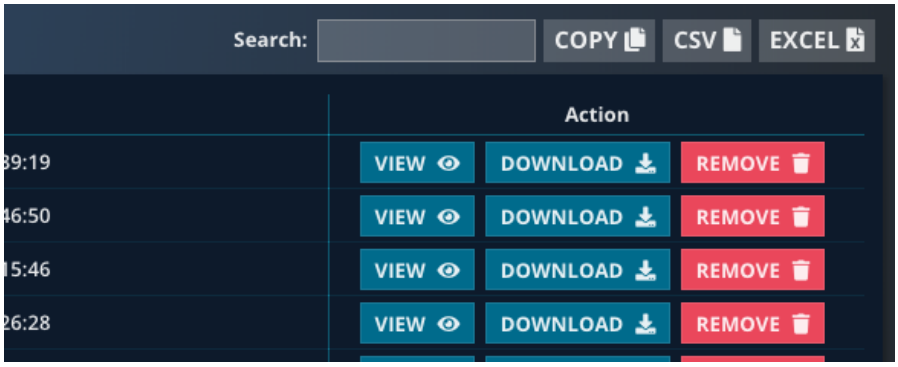
This feature allows you to manage and upload new acquisition scripts to HXTool.

To upload a new acquisition script

1. Provide a script name
2. Click the “choose file” button and select a valid Endpoint Security acquisition script file
3. Click “upload script”



You can also delete, download and view scripts from here by using each respective button



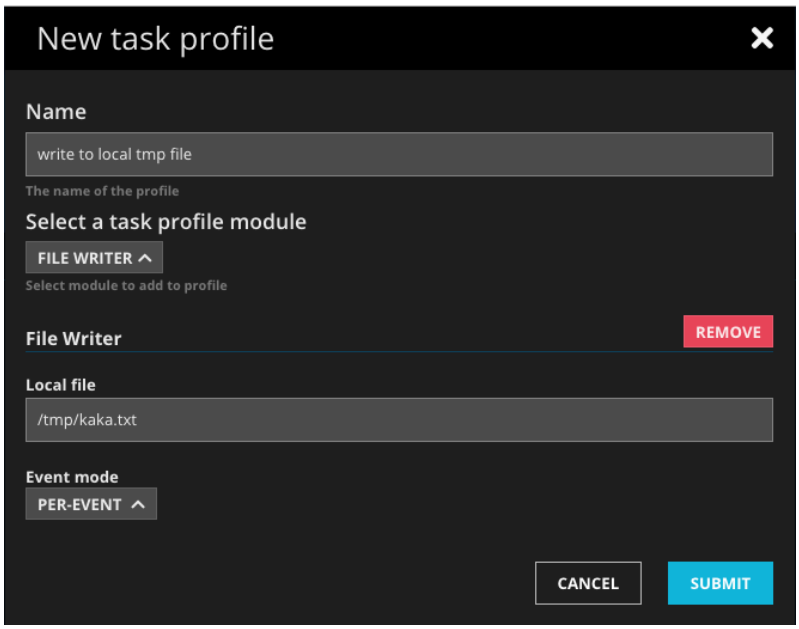
TASK PROFILES

This feature allows you to create the profile definitions that can be used with bulk acquisitions. These definitions will determine what scheduler / background processing does with the acquired results within a bulk acquisition.

To build a new task profile:

1. Enter a profile name

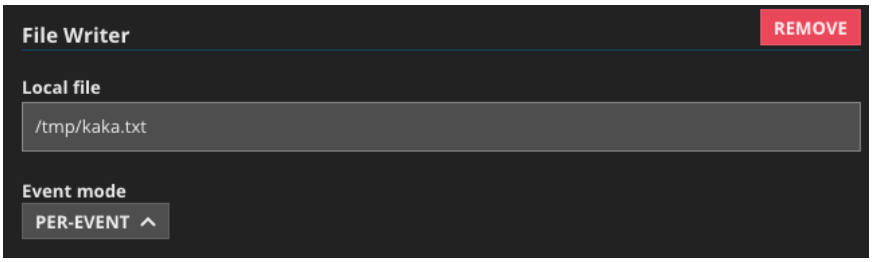
In the drop-down menu for “core task profile module” select one of the available ones. This operation can be repeated several times



FILE WRITER

File writer stores all acquired data in a single file on the filesystem. The “local file” option allows you to enter a file location on the filesystem that will be used. If the file does not exist it will be created.

Event mode allows the user to choose if collected events will be stored in a single JSON object (batch mode) or in several JSON objects (per-event mode)

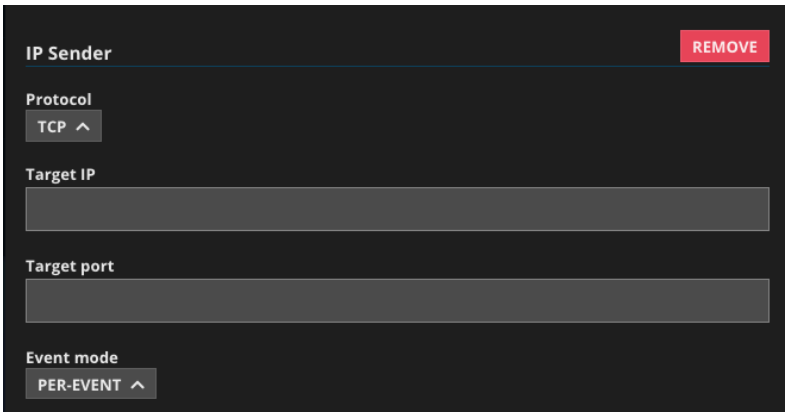


IP SENDER

IP Sender allows the collected results to be streamed to another destination over the network.

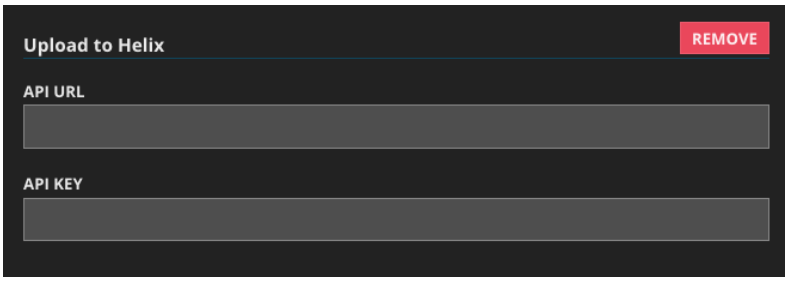
1. Protocol allows you to choose TCP or UDP. Keep in mind that when using UDP information loss might occur if the packets never reach their destination
2. Target IP is the ip address you wish to send the results to
3. Target Port is the port of the Target IP you want to use

Event mode allows the user to choose if collected events will be stored in a single JSON object (batch mode) or in several JSON objects (per-event mode)



UPLOAD TO HELIX

Upload to helix requires an active FireEye Helix subscription. Add your Helix URL and API Key.

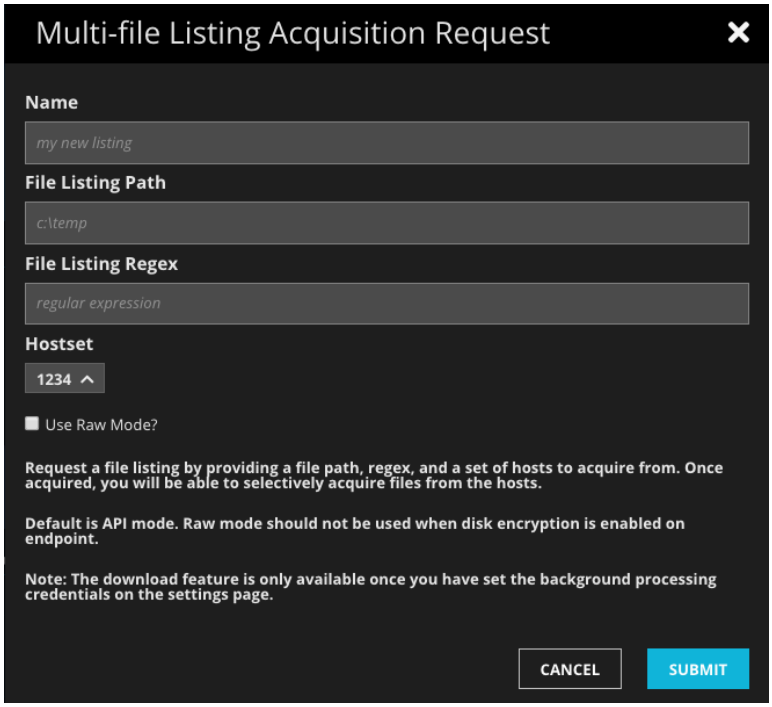


MULTI-FILE ACQUISITION

Please note that you need to set background processing credentials to use this feature

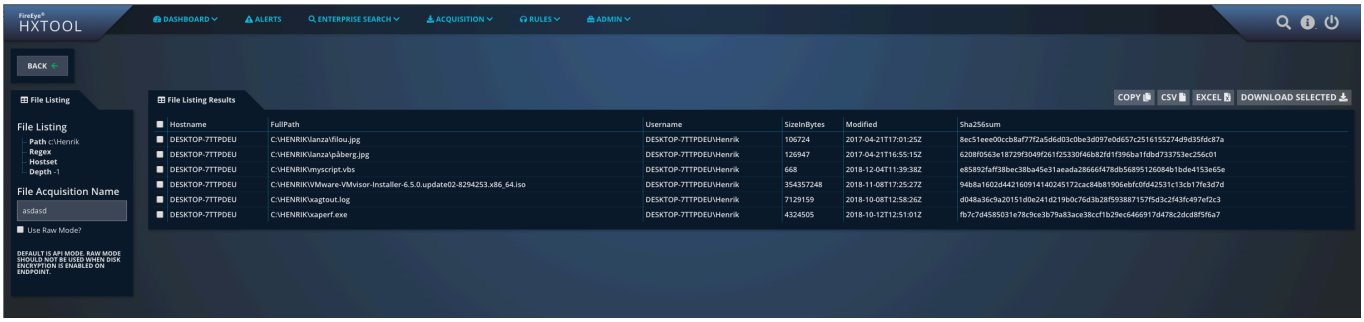
The multi-file acquisition allows you to list and acquire files on endpoints directly. To use the feature, do the following:

Construct a new file listing request using a name, target path, regular expression (RE2) and select a target host-set.



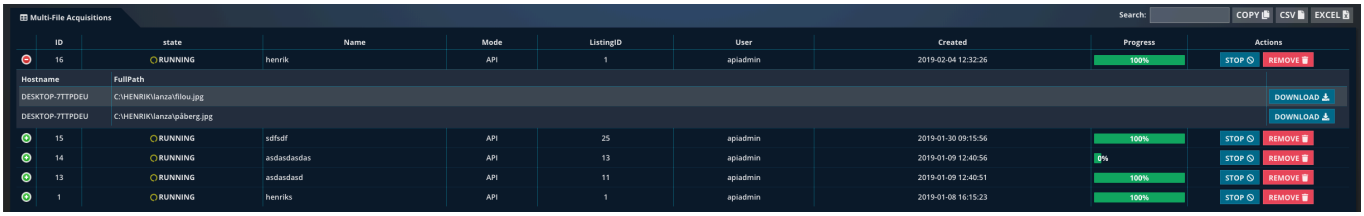
New multi-file acquisition

As results start to come in you notice that the progress bar on the view to the top-right increases. When there are results to display the “view” button appears (you have to reload the page). Click the “view” button to review the findings



Review multi-file acquisition results

Select the files that you wish to acquire and give the acquisition a name to the left hand side. Then click the “download selected” button on the top.



Select file to download to your workstation

A new job will now be shown on the multi-file acquisition landing page where you can download and access all the files you selected in the previous step.

Please note that for this acquisition API mode acquisition is standard but RAW can be chosen if required.

DATA STACKING

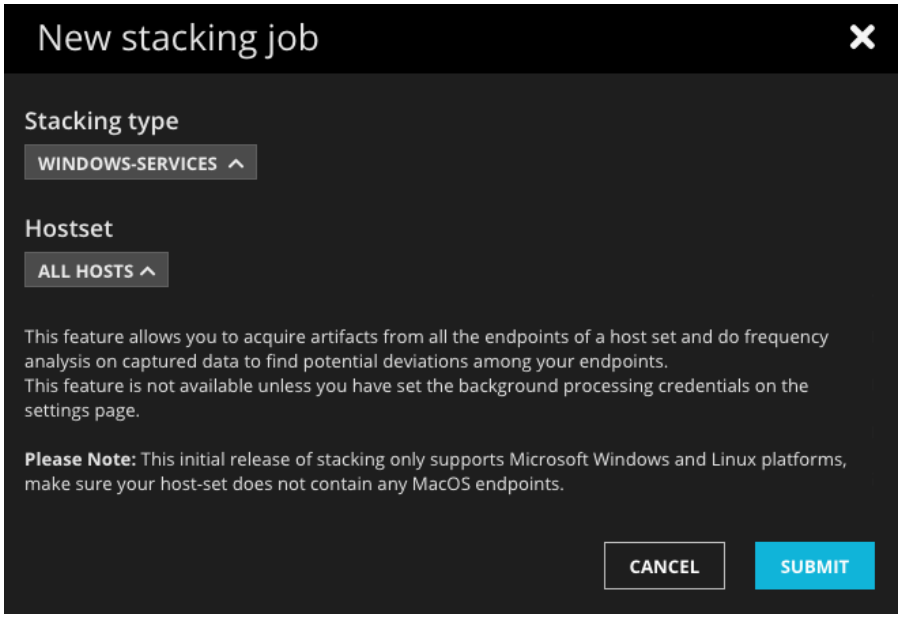
Please note that you need to set background processing credentials to use this feature

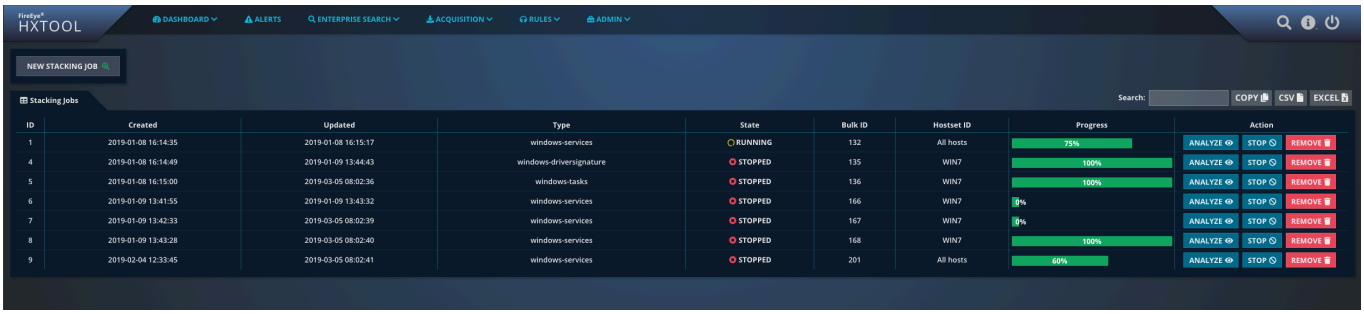
Data stacking is a proactive hunting mechanism in HXTool. It will automatically create bulk acquisitions, run them against a specific host-set, download and post-process the results making them available for you to review on the analysis page.

There are several stacking jobs that you can choose from for Microsoft windows endpoints:

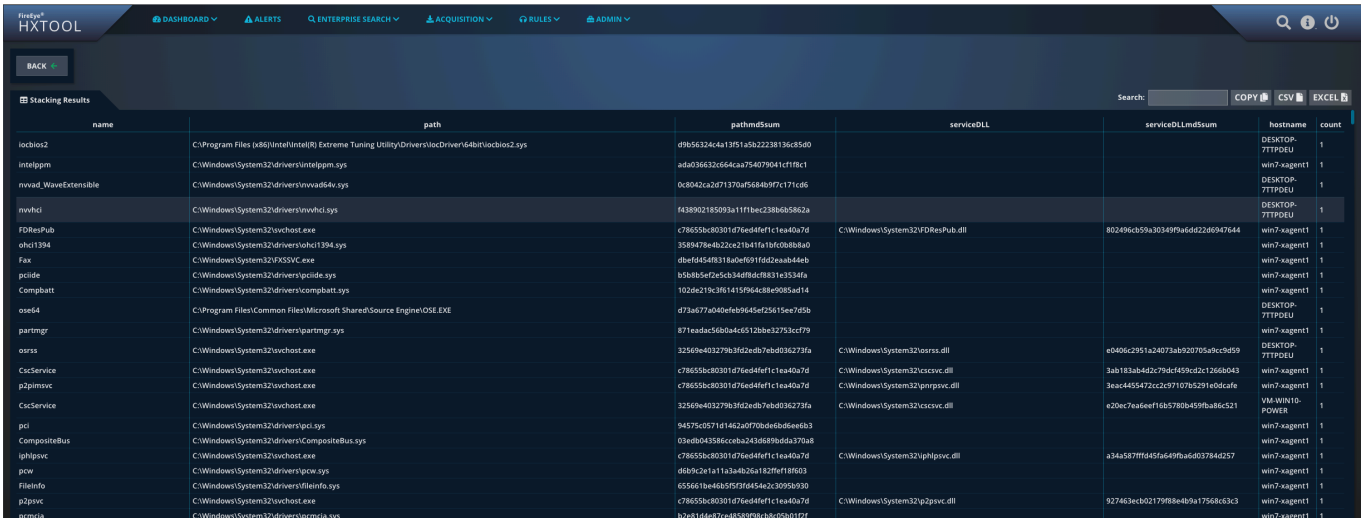
- Services md5
- Driver modules
- Driver signature
- Ports
- Process
- Scheduled task
- Master boot record
- Linux: Ports

To start a stacking job, select the job type you want to run and select the target host-set. Be careful to make sure there are no unsupported platforms within the host-set.





When results start coming in you can review them by clicking on the “analyze” button.



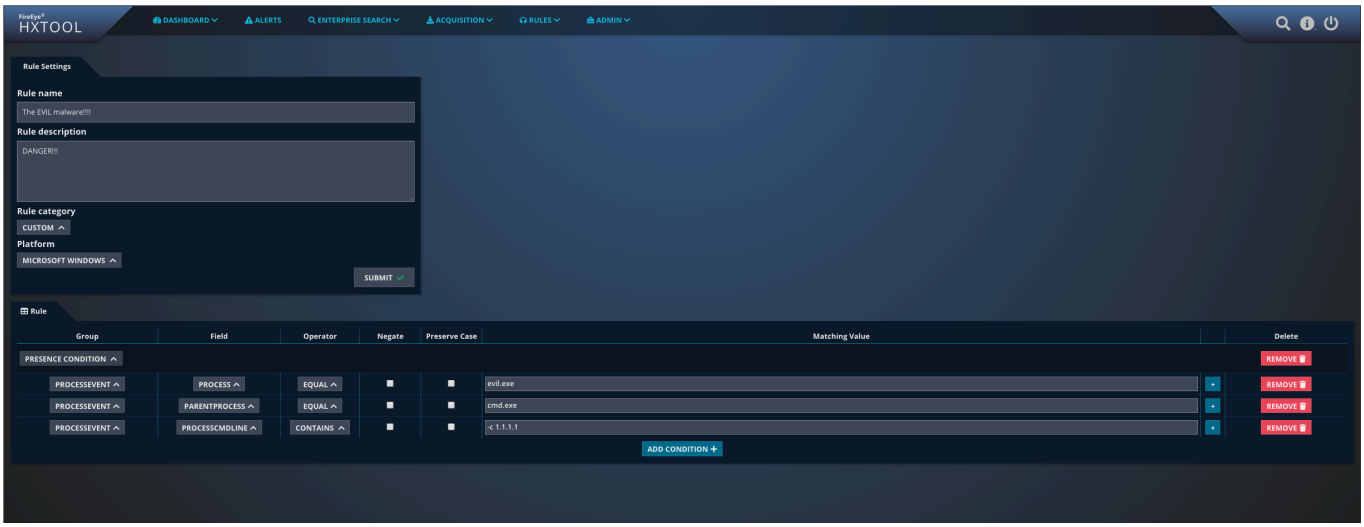
Items will be shown grouped and sorted in ascending mode based on count

INDICATORS

BUILD

This feature allows you to build real-time indicators of compromise for FireEye Endpoint Security. To build a new indicator:

1. Choose a name for the new indicator and type it into the Indicator name box
2. Provide a description for your indicator
3. Select the desired indicator category
4. Select the desired platform
5. Add a new endpoint security condition by clicking the “Add condition”.
6. Select the condition type in the dropdown menu (presence / execution)
7. Add elements to the condition by clicking on the “+” buttons
8. Select group, field, operator, negate status, preserve case status and enter a matching condition into each element
9. Click “submit” when you are done



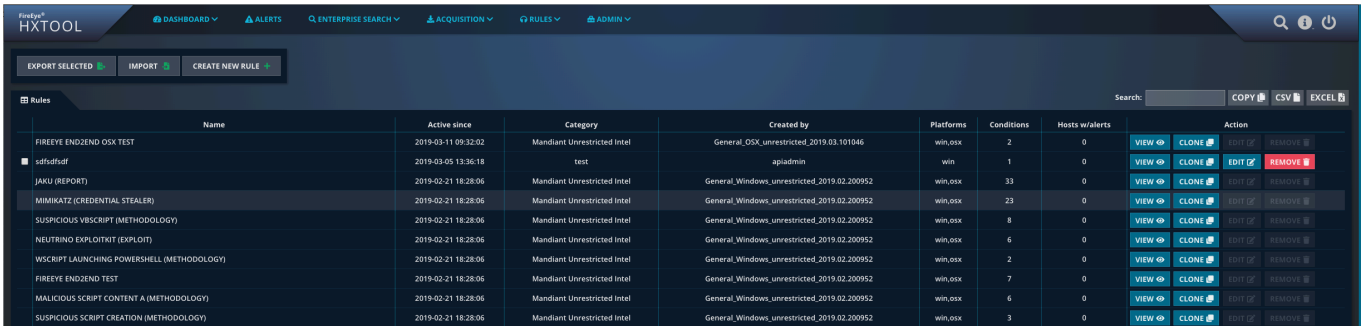
MANAGE

This feature allows you to view, clone, edit, import and export indicators.

The table will show you all the visible indicators in FireEye HX. Clicking them will show you the conditions that make up the indicator.

To export indicators, click one or several indicators and then click the “Export selected” button. Indicators will be stored in the HXTOOL indicator format (JSON)

To import indicators, click the “Import indicators…” button, select a valid HXTOOL export file and then click “Import indicators”.

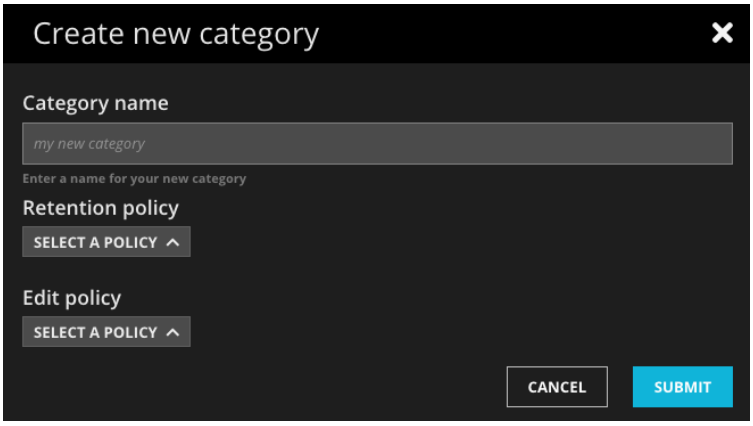


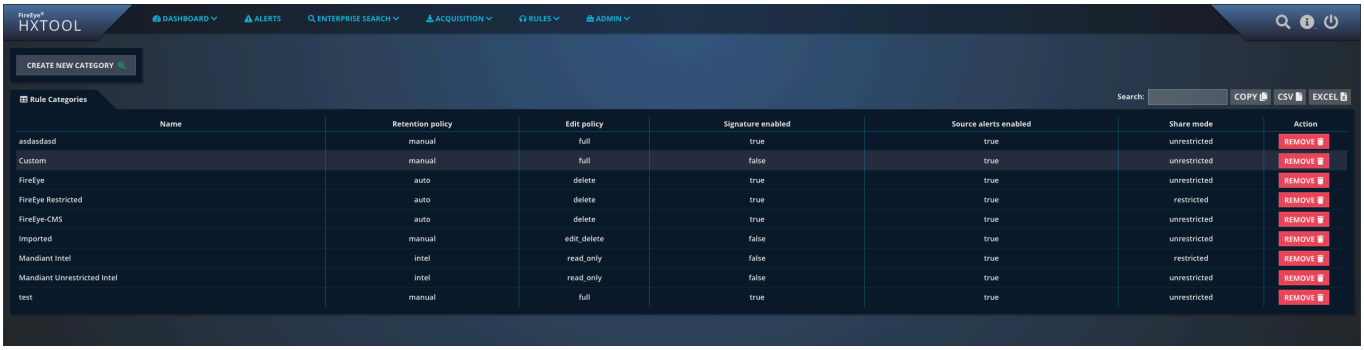
CATEGORIES

This feature allows you to view and create new categories in FireEye Endpoint Security.

The table will show you a full list of all the available categories.

To add a new category, click the “Create category” button, supply a name for the new category and click “Create”. The new category will now be available for real-time indicators.

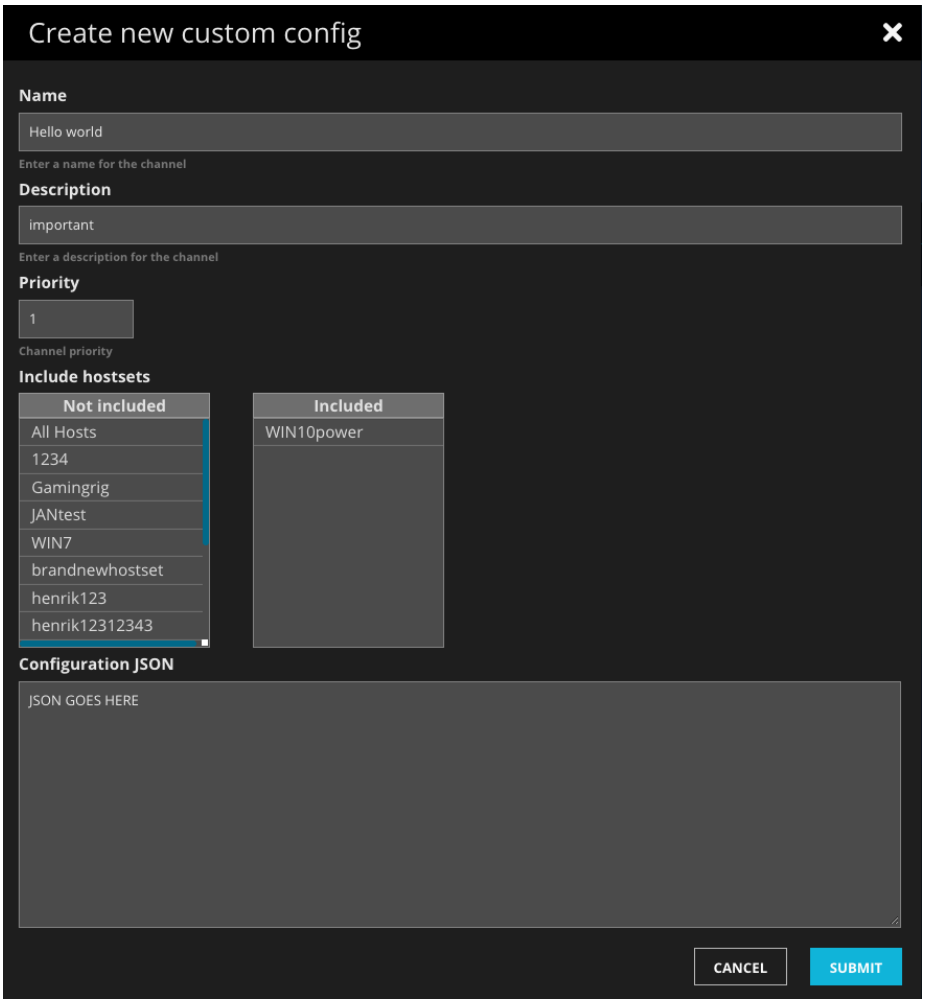




CUSTOM CONFIGURATION CHANNEL

Custom configuration channel is a capability in FireEye Endpoint Security that allows administrators to customize the agent configuration file for agents that belong to a specific host-set. To use this feature, you need to build a host-set that contains the hosts you want to affect and also build/acquire a json configuration file with the configuration you wish to use.

The feature allows you to view, list and add configuration channels. For more information read up on the topic in the FireEye Endpoint Security administration guide.



LOGGING OUT

To logout of HXTool simply click the grey power button on the top-right corner of your screen

CHAPTER 6: LICENSE

HXTool™ Software License 2.0

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files made available with this software (the "Software") to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- The above copyright notice, this permission notice, and the following provisions shall be included in all copies or substantial portions of the Software.
- You agree to be bound to any and all license provisions applicable to third-party software, if any, contained in the Software.
- You give the authors, copyright holder, and others the right to freely use any of your ideas, comments, suggestions, or modifications pertaining to the Software or its use that you choose to disclose.
- You shall not use the trade names, trademarks, service marks, or product names of the Licensor (including, without limitation, HXTool), except HXTool may be used (i) as required for reasonable and customary use in describing the origin of the Software, and (ii) in connection with or referring to the original Software that is not modified by you.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY SUPPORT OR MAINTENANCE OF THE SOFTWARE, ITS INTEGRATION OR COMPATIBILITY WITH OTHER PRODUCTS, ANY ERROR, DEFECT OR VULNERABILITY IN THE SOFTWARE, OR ANY CLAIM, DAMAGES (INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, EXEMPLARY, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER), OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OF, INABILITY TO USE OR OTHER DEALINGS IN THE SOFTWARE, EVEN IF ADVISED OF THE POSSBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE FOR DETERMINING THE APPROPRIATENESS OF USING OR DEALING IN THE SOFTWARE, AND ASSUME ANY RISKS ASSOCIATED WITH YOUR EXERCISE OF PERMISSIONS UNDER THIS LICENSE.