ENDPOINT SECURITY

Process Tracker

MODULE USER GUIDE v1.2.4

GENERAL AVAILABLITY RELEASE

FireEye and the FireEye logo are registered trademarks of FireEye, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

FireEye assumes no responsibility for any inaccuracies in this document. FireEye reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Endpoint Security Process Tracker Module

Software Release 1.2

Revision 1

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: https://csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

PART I: Module Overview

Process Tracker recognizes unique process execution events on a Windows, macOS, or Linux host, and streams the associated execution metadata to your Endpoint Security Server. These events are published on a public message bus topic that is accessible by Helix™ or your SIEM. The events are also stored locally within a database and are accessible via API. You can also view the events within the Endpoint Security Web UI using a new page provided by Process Tracker.

If the Enricher module is installed and enabled, then you can use the standard Enricher workflow to process all Process Tracker events and obtain a verdict. For a malicious verdict, you can configure Process Tracker to fire an alert. The Process Tracker alert can be configured to trigger an automatic triage.

If the Enricher module is not installed and enabled, then Process Tracker can still post messages on the bus and store them in its database. Process Tracker does not require the Enricher module to be installed and enabled to stream the event data.

Unique Process Execution

These execution events are unique, meaning that they are reported the first time that they are observed on the endpoint. If a process executes more than once, only the first execution is reported unless any of the following exceptions occur:

- The process is executed from a new file path that has not been seen before on the endpoint

- The hash of the process executable is one that has not been seen before on the endpoint. For instance, the process has been updated to a new binary.

If the same process executes on more than one endpoint, each endpoint will individually report the execution event.

General Description of Flow

With the module installed and enabled on the agent, it will monitor process execution events to determine if a unique process execution is occurring in order to report it. For a unique process execution, the module collects metadata associated to the event and forwards the information the server module. Aside from reporting these events, the agent will report its runtime health via the Agent Info Audit.

The server module receives the event information reported by the agent. For the module to function on an agent, *Real-Time Indicator Detection* must also be turned on for that same agent.

For each event

- It will publish the process execution event on a message bus topic, including the metadata collected by the agent.

- It will store the event within its local database so that it is accessible via the Endpoint Security Web UI, and the REST API.

- If Enrichment is enabled, enrichment will be requested for event. The Enricher module will execute its standard workflow to decorate the event with additional information that is available from the data sources that is configured with that module. Process Tracker will monitor for the completion of the enrichment request, and when received it will publish an update of the event on the message bus topic, now further decorated with an enrichment verdict. Process Tracker will also update the event within its local database.

- If a malicious enrichment verdict is received, and alerting is enabled, the server module will publish a generic alert of type **PRO** to the Alerting Service of the Endpoint Security server. This alert will be associated to the host where the process executed. The alert information will be available within the Endpoint Security Web UI, accessible via REST API, published on a message bus topic, and provided within a CEF notification.

Prerequisites

This technical preview release of the Process Tracker module is supported on **Endpoint Security 5.0.0** with **xAgent 32** running on Windows, macOS or Linux.

Note: You should not install the 1.2.x version of Process Tracker module on Endpoint Security 4.9.x with xAgent 31 or lower. This is not a supported scenario. If you are running a release prior to version 1.2.x of the Process Tracker module you **must** uninstall it, then install this version. An upgrade from a prior version is not a supported scenario.

PART II: Configuring the Process Tracker Module

The Process Tracker module consists of a **server module** and an **agent module**. It is important to understand the following relationships between the server and agent modules:

- You install and enable the Process Tracker module via HX Module Administration. This enables the server module and makes the agent module available to be installed on the agents that you identify via policy.

- You install and enable the Process Tracker module on agents using the Process Tracker category within a policy. Agents who have this policy assigned with Process Tracker enabled will automatically download the agent module, install and run it.

- If you disable the **server module**, this will disable the **agent module** in all policies that contain the Process Tracker category. Agents who prior had this enabled will stop the Process Tracker **agent module** and uninstall it.

- Uninstalling the Process Tracker **server module** removes the Process Tracker category from all policies. Agents who prior had this category with Process Tracker enabled will stop the Process Tracker **agent** module and uninstall it.

Enabling the Process Tracker Module

You can perform these tasks from the Modules and Policies pages in the Endpoint Security Web UI. It is important that you understand the concepts of host sets and assigning policy described within the ***Endpoint Security User's Guide Release 5.0*** before you enable this module.

Before proceeding, please review the *Configuring Process Tracker section below.* You should understand the implications of these settings before enabling Process Tracker on endpoint agents.

To enable the Process Tracker server module:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.

3. On the **Modules** page, locate the **Process Tracker** module on the **User Modules** tab and click the **Actions** icon (the gear symbol) and select **Enable** to enable the module.

Note: Having the server module enabled does not automatically enable it for agents. You must use the next steps to enable the feature on the agent.

To enable the Process Tracker agent module:

1. Log in to the Endpoint Security Web UI as an administrator.

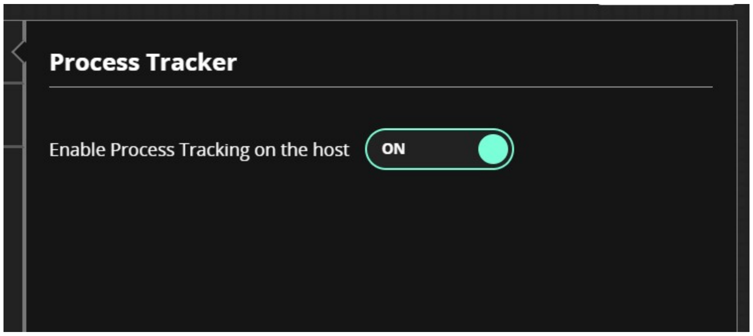
2. From the **Admin** menu, select **Policies** to access the **Policies** page.

3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent(s) on which you want to activate Process Tracker, and select **Edit Policy**.

4. In the **Configurations** area of the **Edit Policy** page, click **Process Tracker Agent – 1.2.x**.

   a. If the **Process Tracker Agent** configuration is not listed, add it via the **Categories** button.

5. Toggle the **Enable Process Tracking on the host** selector to **ON**.



Process Tracker

Enable Process Tracking on the host ON

Figure 1 Enable Process Tracking

6. On the **Edit Policy** page, click **Save**.

Disabling the Process Tracker Module

To disable the server module:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.

3. On the **Modules** page, locate the **Process Tracker** module on the **User Modules** tab and click the **Actions** icon (the gear icon) and select **Disable** to disable the module.

Disabling the Process Tracker **server module** (once enabled) will disable the **agent module** in all the policies, causing it to be disabled on associated endpoints (local systems).

To disable the agent module:

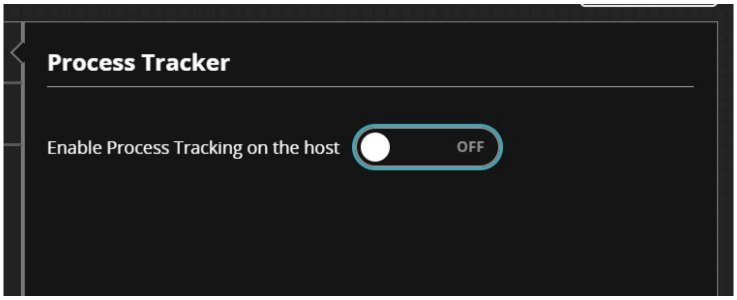
1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Admin** menu, select **Policies** to access the **Policies** page.

3. On the **Policies** page, click the **Actions** icon (the gear icon) for the policy for the agent on which you want to disable Process Tracker, and select **Edit Policy**.

4. In the **Configurations** area of the **Edit Policy** page, click **Process Tracker Agent – 1.2.x**.

5. Toggle the **Enable Process Tracking on the host** selector to **OFF**.



Process Tracker

Enable Process Tracking on the host

Figure 2 Disable Process Tracking

6. On the **Edit Policy** page, click **Save** button.

Configuring Process Tracker Server Module

This section describes the various configuration settings provided in the Process Tracker module configuration. Configuration can be accomplished through the Endpoint Security Web UI, or by accessing the API. The API is discussed at the end of this section.

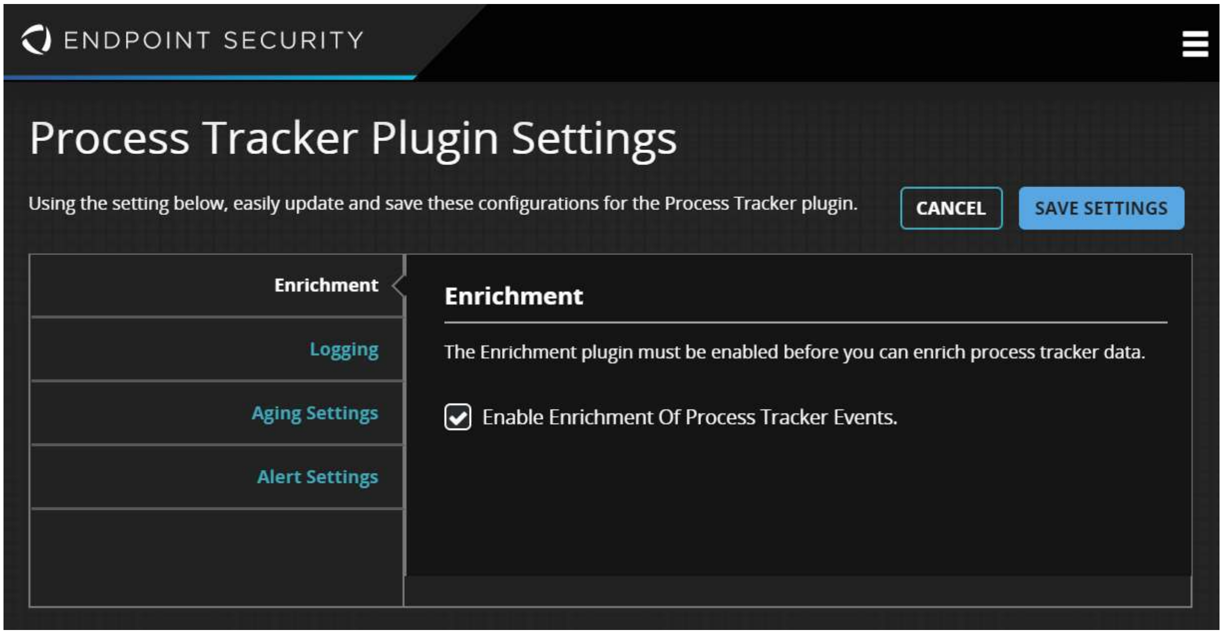
To access the Process Tracker module configuration:

1. Log in to the Endpoint Security Web UI as an administrator.

2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.

3. On the **Modules** page, locate the **Process Tracker** module on the **User Modules** tab and click the **Actions** icon (the gear symbol) and select **Configure** to configure the module.

4. You will be presented with a page for **Process Tracker Plugin Settings** from which you can configure the behavior of the module.



Process Tracker Plugin Settings

Using the setting below, easily update and save these configurations for the Process Tracker plugin.

Enrichment

The Enrichment plugin must be enabled before you can enrich process tracker data.

☑ Enable Enrichment Of Process Tracker Events.

Figure 3 Process Tracker Plugin Settings on HX Server

Enrichment

The Process Tracker module can collaborate with the Enricher module to perform analysis of process execution events. If you want to receive enriched information for process execution events, then check the checkbox for **Enable Enrichment of Process Tracker Events.** When this option is selected, Enricher will engage its workflow for Process Tracker events, and it will provide a value for *Enrichment Status* to associate to each event. Refer to *The Process Tracker Page* section for a description of this field.

Note that the Enricher module must be installed on the same HX Server and enabled for this option to function. Also note that for events from endpoints that are running a distribution of Linux that has prelinking enabled, enrichment will not occur for a process that has been launched from a prelinked binary.

Logging

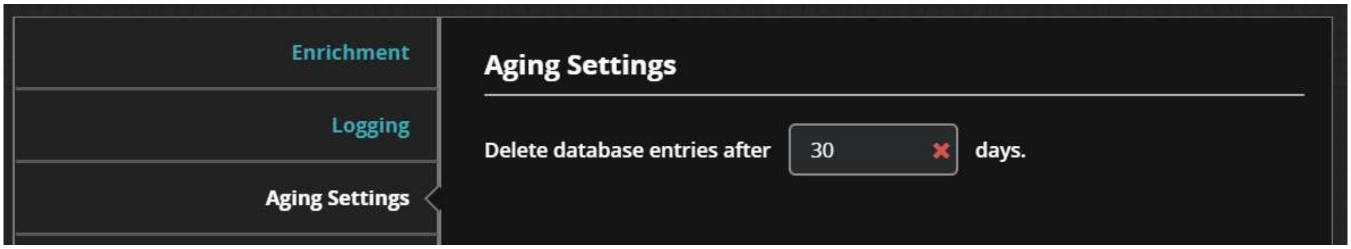
You can adjust the level of detail provided in the log messages by the Process Tracker server module. The agent side logging detail is picked up from the Agent Logging configuration in policy and is not independently adjustable for the Process Tracker plugin. The following table describes the logging options that are available. Note that each log level option includes the messages also generated by the level below it. For example, Alert includes Emergency messages, Critical includes Alert and Emergency messages. Therefore, the lowest severity logging level will produce the highest volume of messages. Refer to the FireEye document ***CLI Command Reference*** for information regarding access to the log file and notifications related to its content.

Logging Level	Description
Debug	Logs Debugging messages. This logging level is normally used when debugging a program only. It includes all the types of logging messages.
Info	Logs Informational messages about regular system processing.

Logging Level	Description
Notice (default)	Logs notification messages that identify minor problems on the host endpoint that do not inhibit regular agent function and for which defaults are used until the problem is resolved
Warning	Logs warning messages that identify non-critical and correctable errors on the host endpoint, such as a specified value that is too large.
Error	Logs error messages that identify program errors on the host endpoint, such as when a file cannot be found.
Critical	Logs critical messages that identify serious conditions on the host endpoint, such as hard drive errors.
Alert	Logs messages that identify crucial conditions on the host endpoint that require immediate remediation, such as a corrupted system database.
Emergency	Logs system failure messages that identify total system failures on the host endpoint. These system failures usually cause the agent to stop functioning.

Aging Settings

Process Tracker receives events from the endpoints for each unique process execution. These events are held within the Process Tracker database for a finite period, after which they are discarded. While the events are in the database, they can be retrieved via the API, and viewed within the Process Tracker grid in the Endpoint Security Web UI. To manage the size of the database, old events need to be discarded. Use the **Aging Settings** to specify how long to retain events before they are discarded. The default value is 30 days.



Aging Settings

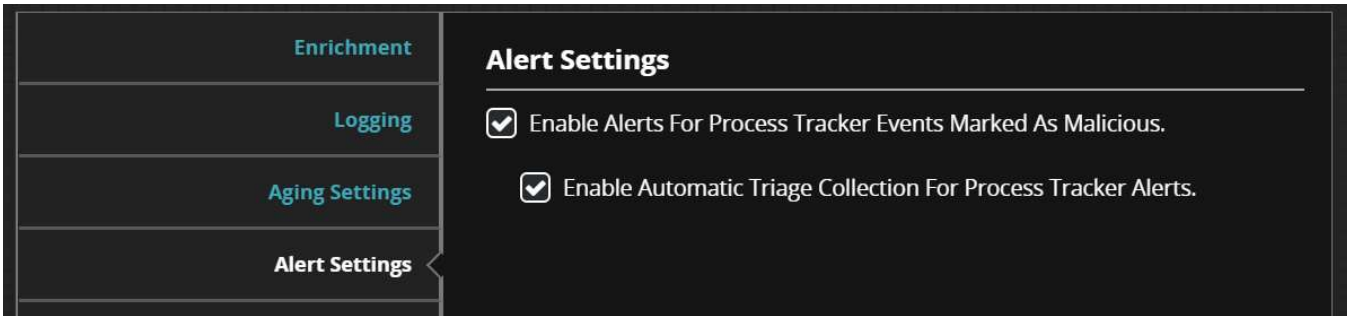
Delete database entries after 30 days.

Figure 4 Aging Settings

Alert Settings

The Process Tracker module can generate alerts for events that relate to a malicious process execution. It does so via collaboration with the **Enrichment** setting described above, which must be selected. If you want to receive alerts for malicious process execution events, then check the checkbox for **Enable Alerts for Process Tracker Events Marked As Malicious.** When this option is enabled, Process Tracker will generate an alert when enrichment returns as status of **Malicious**.

Further, if you desire to have automatic triage collection on an endpoint involved with a Process Tracker alert, select the **Enable Automatic Triage Collection for Process Tracker Alerts**. When an alert is generated, the HX Security Server will automatically request a standard triage package from the endpoint who originated the process execution event.



Alert Settings

☑ Enable Alerts For Process Tracker Events Marked As Malicious.

☑ Enable Automatic Triage Collection For Process Tracker Alerts.

Figure 5 Alert Settings

Configuration API

The configuration API is made available via the configuration endpoint of the Endpoint Security Server REST API. For complete details on how to interact with Endpoint Security Server API, please refer to FireEye document ***Endpoint Security REST API Guide Release 5.0*****.**

Get Process Tracker Configuration

Returns the current configuration for the Process Tracker module as a JSON result.

HTTP Verb	Server
GET	hx/api/services/config/tree

Query Parameters

Parameter	Notes
node_name=/config/process-tracker	Pulls the Process Tracker configuration

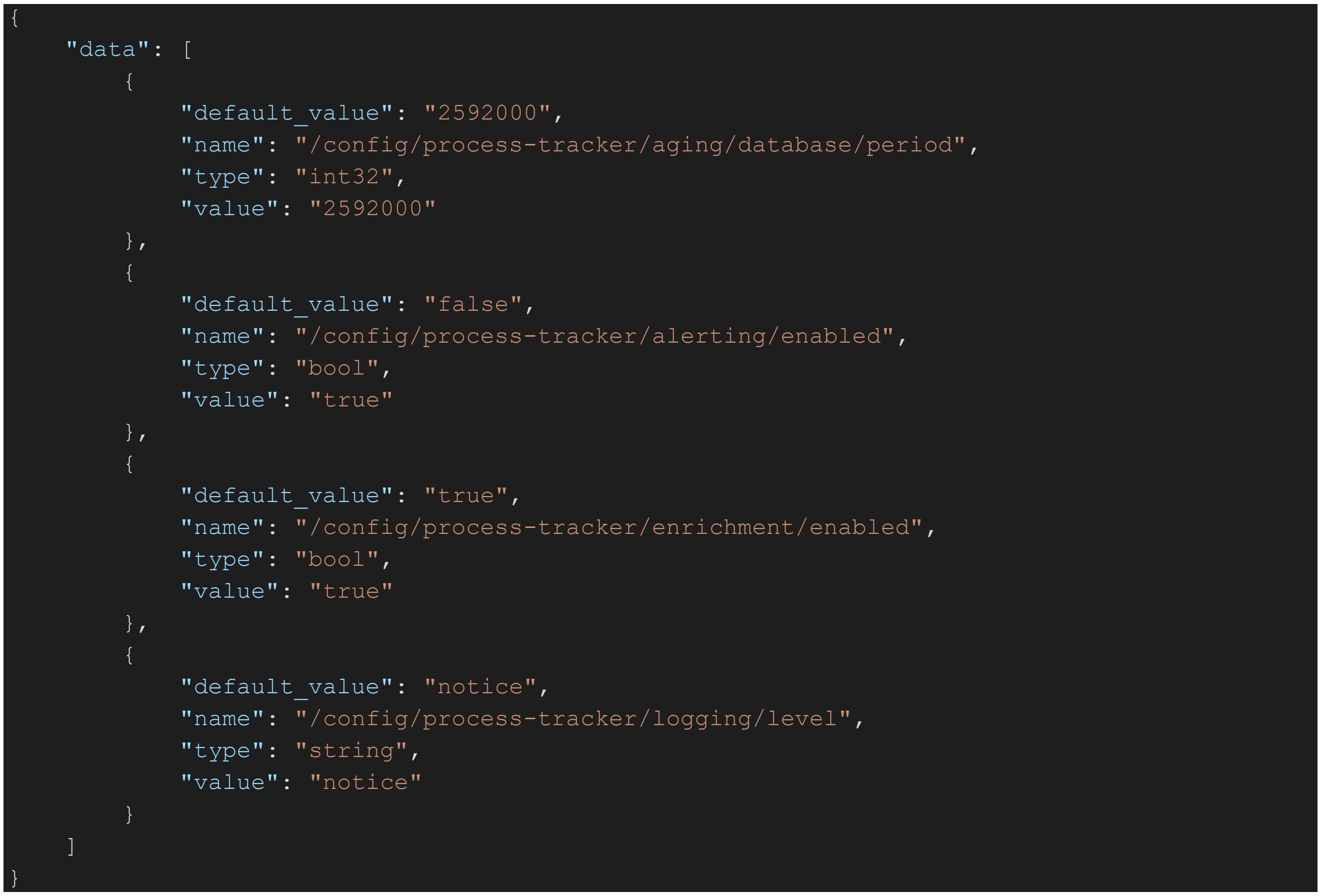
Response

The information that is returned is a JSON dictionary with the following keys

Key	Notes
data	List of configuration properties. Each property has the following attributes: • name – the name of the configuration property • type – the shape of the value for this configuration property • value – the current value of this configuration property • default_value – the default value of this configuration property

The following is a list of configuration properties for the Process Tracker Module.

Purpose	Name	Type {Values}
Enrichment	/config/process-tracker/enrichment/enabled	Boolean {**true** | false}
Logging level	/config/process-tracker/logging/level	String {‘debug’ | ‘info’ | ‘warning’ | ‘**notice’** | ‘error’ | ‘critical’ | ‘alert’ | ‘emergency’}
Aging setting	/config/process-tracker/aging/database/period	Int32 (number of seconds) Default = **30 days as seconds**
Alert setting	/config/process-tracker/alerting/enabled	Boolean {true | **false**}



```
{
    "data": [
        {
            "default_value": "2592000",
            "name": "/config/process-tracker/aging/database/period",
            "type": "int32",
            "value": "2592000"
        },
        {
            "default_value": "false",
            "name": "/config/process-tracker/alerting/enabled",
            "type": "bool",
            "value": "true"
        },
        {
            "default_value": "true",
            "name": "/config/process-tracker/enrichment/enabled",
            "type": "bool",
            "value": "true"
        },
        {
            "default_value": "notice",
            "name": "/config/process-tracker/logging/level",
            "type": "string",
            "value": "notice"
        }
    ]
}
```

Figure 6 Sample Response

Set Process Tracker Configuration

Update a configuration property for the Process Tracker module. See the list of configuration properties, above.

HTTP Verb	Server
PUT	hx/api/services/config/tree

Query Parameters

Parameter	Notes
node_name=/config/process-tracker	Pulls the Process Tracker configuration

Query Headers

The following header is highlighted to indicate that there will be JSON formatted request data within the body

Content-Type	Application/json

Query Body

List of configuration properties to be set, formatted as JSON. For example, the following request body will specify that the Logging level be updated to a value of *Error.*

```
{"data": [{"default_value": "notice", "name": "/config/process-tracker/logging/level", "type":
"string", "value": "error" }]}
```

Note that this request will not provide feedback in the response if an invalid *value* is specified. The value is accepted. However, the Process Tracker module when finding an invalid configuration property *value*, will replace that value with the default value for that property. Also note, that you cannot modify the default value of a configuration property using this request.

Configuring Process Tracker Agent Policy

The sole configuration that is adjustable within policy is to enable/disable the agent plugin. This is described in the prior sections on *Enabling the Process Tracker Module* and *Disabling the Process Tracker Module.*

For the module to function on the agent, *Real-Time Indicator Detection* must also be turned on. If you install the module on an agent without this turned on, no process execution events will be detected.

Onboarding Endpoints

When the module is enabled on the agent, the endpoint will begin streaming unique process execution events. The first time that module observes a process execution, one that it has not reported before, the event will be streamed. Therefore, when Process Tracker is first enabled, many of the process execution events will be for ones that are reported for the first time. Over time uniqueness of the process execution events will taper off. This aspect of initial burst and taper for events being streamed should be considered when the plan is to onboard a large population of endpoints. It is recommended that the onboarding is to be performed with a group of endpoints at a time so as not to overwhelm the Endpoint Security Server. Monitoring the process when a group is enabled will inform the size of the next group, according to the available capacity of your system.

Exclusions

You may need to fine tune the exclusions that Process Tracker ignores for process execution events. Process Tracker makes use of the same list of excluded files/folders and processes that are configured in policy under the *Real Time Indicator Detection* category.

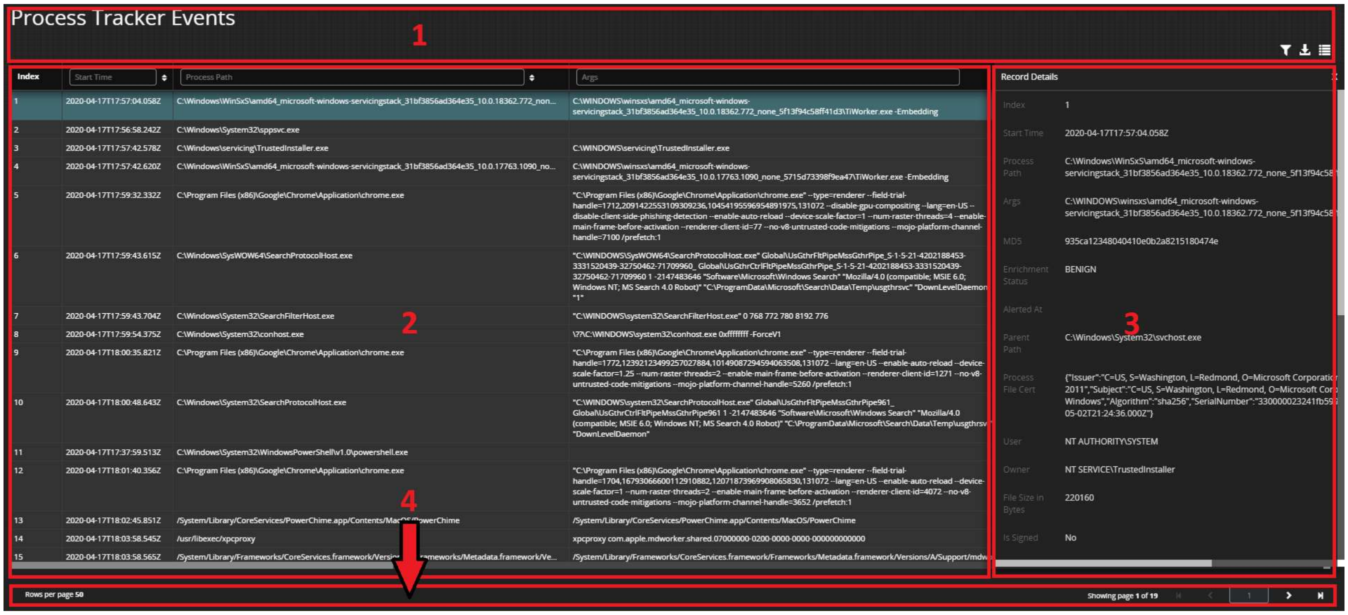
PART III: Using the Process Tracker Web Interface

This section describes how to use the Process Tracker user interface on the Endpoint Security Web UI.

To access the Process Tracker web interface:

1. Log in to the Endpoint Security Web UI using your credentials.
2. From the **Modules** menu, select **Process Tracker** to access the web interface of the module.

The Process Tracker Page



Process Tracker Events

Index	Start Time	Process Path	Args
1	2020-04-17T17:57:04.058Z	C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.772_non...	C:\WINDOWS\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\TiWorker.exe -Embedding
2	2020-04-17T17:56:58.242Z	C:\Windows\System32\sppsvc.exe	
3	2020-04-17T17:57:42.578Z	C:\Windows\servicing\TrustedInstaller.exe	C:\WINDOWS\servicing\TrustedInstaller.exe
4	2020-04-17T17:57:42.620Z	C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.1090_no...	C:\WINDOWS\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.1090_none_5715d73398f9ea47\TiWorker.exe -Embedding
5	2020-04-17T17:59:32.332Z	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1712,2091422553109309236,10454195596954891975,131072 --disable-gpu-compositing --lang=en-US --disable-client-side-phishing-detection --enable-auto-reload --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=77 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=7100 /prefetch:1
6	2020-04-17T17:59:43.615Z	C:\Windows\SysWOW64\SearchProtocolHost.exe	"C:\WINDOWS\SysWOW64\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-4202188453-3331520439-32750462-71709960_ Global\UsGthrCtrlFltPipeMssGthrPipe_S-1-5-21-4202188453-3331520439-32750462-71709960 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon "1"
7	2020-04-17T17:59:43.704Z	C:\Windows\System32\SearchFilterHost.exe	"C:\WINDOWS\system32\SearchFilterHost.exe" 0 768 772 780 8192 776
8	2020-04-17T17:59:54.375Z	C:\Windows\System32\conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
9	2020-04-17T18:00:35.821Z	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1772,12392123499257027884,10149087294594063508,131072 --lang=en-US --enable-auto-reload --device-scale-factor=1.25 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=1271 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=5260 /prefetch:1
10	2020-04-17T18:00:48.643Z	C:\Windows\System32\SearchProtocolHost.exe	"C:\WINDOWS\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe961_ Global\UsGthrCtrlFltPipeMssGthrPipe961 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsv "DownLevelDaemon"
11	2020-04-17T17:37:59.513Z	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	
12	2020-04-17T18:01:40.356Z	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1704,16793066600112910882,12071873969908065830,131072 --lang=en-US --enable-auto-reload --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=4072 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3652 /prefetch:1
13	2020-04-17T18:02:45.851Z	/System/Library/CoreServices/PowerChime.app/Contents/MacOS/PowerChime	/System/Library/CoreServices/PowerChime.app/Contents/MacOS/PowerChime
14	2020-04-17T18:03:58.545Z	/usr/libexec/xpcproxy	xpcproxy com.apple.mdworker.shared.07000000-0200-0000-0000-000000000000
15	2020-04-17T18:03:58.565Z	/System/Library/Frameworks/CoreServices.framework/Versio[illegible]rameworks/Metadata.framework/Ve...	/System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdw

Record Details

Index	1
Start Time	2020-04-17T17:57:04.058Z
Process Path	C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58
Args	C:\WINDOWS\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58
MD5	935ca12348040410e0b2a8215180474e
Enrichment Status	BENIGN
Alerted At	
Parent Path	C:\Windows\System32\svchost.exe
Process File Cert	{"Issuer":"C=US, S=Washington, L=Redmond, O=Microsoft Corporatio 2011","Subject":"C=US, S=Washington, L=Redmond, O=Microsoft Cor Windows","Algorithm":"sha256","SerialNumber":"330000023241fb59 05-02T21:24:36.000Z"}
User	NT AUTHORITY\SYSTEM
Owner	NT SERVICE\TrustedInstaller
File Size in Bytes	220160
Is Signed	No

Rows per page **50**

Showing page **1** of **19**

Figure 7 The functional areas of the Process Tracker page

The Process Tracker page is comprised of four functional areas. They are:

1. The Banner & Tools area
2. The Grid
3. The Record Details flyout
4. The Navigation area

Banner & Tools Area

This area provides the banner that identifies the page as the one assigned to the Process Tracker Module. On the right side there is a set of tools that provides for interaction with the Grid.

Filter Sets – this tool provides for the management of filter sets. Filter sets are a way to define and save specific filters that are applied to the grid area. This allows for quick access to views that organize your insights into the events data. With this tool you can

- Save the current filter applied within the **Grid Area** as a new filter set
- Control who has access to this filter set (private/public)
- Export and Import filter sets
- Remove filter sets that are no longer useful

Export to CSV – this tool provides for the export of the current grid data to a CSV file. The data that is exported is sorted and filtered according to the active settings applied in the grid. It is worthy to note that the export to CSV is convenient but is not intended for routine export of large numbers of rows. The limit is capped at 10,000 rows for export so as not to overburden the Endpoint Security Server. If you need to routinely export large numbers of rows, with or without filters applied, the **Module REST API** provides very efficient access to that data.

Manage Columns – this tool provides for the configuration of the columns that are displayed in the grid and you can adjust their order of presentation. The top-down order of the columns in this tool represents the left-right position of the columns within the grid. To move a column, click and drag a column name up or down the list, then release when it is in the position that you desire.

Grid Area

The grid area provides for a tabular display of the events collected by the Process Tracker Module. There will be one row in this table per process execution event. See **Unique Process Execution** for the definition of a process execution event.

The columns of the grid convey the following information

Column	Description	Notes
Agent ID	The unique system-generated ID for the host endpoint that reported the event.	
Alerted At	Timestamp of the associated alert, if one was generated	
Args	The command arguments supplied to the process when it executed	
Attributes	Attributes associated with the process file. Possible values are: • Archive • Compressed • Encrypted • Hidden • ReadOnly	Only available on Windows
Creation Time	The creation time of the process file	Not available on Linux

Column	Description	Notes
Enrichment Status	The status from the Enrichment workflow (if enabled). Possible values are: • Requested – queued for Enrichment • Pending – Enrichment analysis in progress • Complete – Context API analysis is complete, but inconclusive • Benign – benign conclusion from analysis • Malicious – malicious conclusion from analysis • Whitelisted – analysis skipped due to white listing	
Event At	The timestamp for when the process execution was detected on the endpoint	
File Size (bytes)	The size of the file associated to the process	
Group	The name of the user group associated with the process file	Not available on Windows
Index	The ordinal of the event as it was received by the Process Tracker module	
Is Prelinked	The file associated to the process was prelinked, therefore making enrichment of the file not possible (if enabled)	Only available on Linux
Is Signed	The file associated to the process is signed (Yes/No)	Only available on Windows
Last Accessed Time	The last access time of the process file	May not be available on some Windows
Last Status Change Time	The last metadata update time of the process file	Not available on Windows
MD5	The MD5 hash of the process file	
Modified Time	The time for last content modification of the process file	
Owner	The owner associated to the process file	
Parent Path	The fully qualified path of the file associated to the parent process of the process being executed	
Parent PID	The process ID of the parent process	
PID	The process ID of the process that was executed	
Process File Cert	Certificate details, if the process file was signed. Possible values are: • Algorithm • Expiration Time • Issuer • Serial Number • Subject	Only available on Windows
Process File Exists	Indicator if the associated process file existed on disk at the time that the event was detected (Yes/No)	

Column	Description	Notes
Process Path	The fully qualified path of the file associated to the process	
Signature Verified	Indicator if a verified signature exists for the file associated to the process (Yes/No)	Only available on Windows
Start Time	The time that the process started execution on the endpoint	
Type	This event is a Start or Stop event. Note that Stop events are only issued for processes for which an associated Start event was not detected.	
User	The ID of the user who launched the process.	

The order and visibility of the columns is adjusted by the **Manage Columns** tool in the **Banner & Tools** area. You can adjust the width of each column. You can restore the default width, with the **Manage Columns** tool.

For each column in the grid, you can apply a filter that will show only the rows that match your criteria. You can filter on more than one column at a time, according to the information that you are seeking to reveal. Your filter settings can be saved and recalled by using the **Filter Sets** tool in the **Banner & Tools** area.

The rows in the grid can be sorted ascending/descending on most columns. Columns that can be sorted will have an ⇕ indicator to the right of the column name in the header. This is what you click to activate a sort on the column. A sort cannot be applied to more than one column at a time.

Record Details Flyout Area

When you click on a row within the grid, a flyout is presented from the right that lists the details of the selected row (record). The list of details shows a value for every column that is available in the grid, not only the ones that were configured visible within the grid. Clicking another row will update the details to those of the new row. Horizontal and vertical scroll bars are presented when the flyout cannot fit all the information. The size of the flyout area is not adjustable. To dismiss the flyout area, click on the **X** in the upper right corner of the area.

Navigation Area

The navigation area provides you the ability to page through the rows of the grid, providing information about how many pages exist and your current position within the list of pages. Details about this area are:

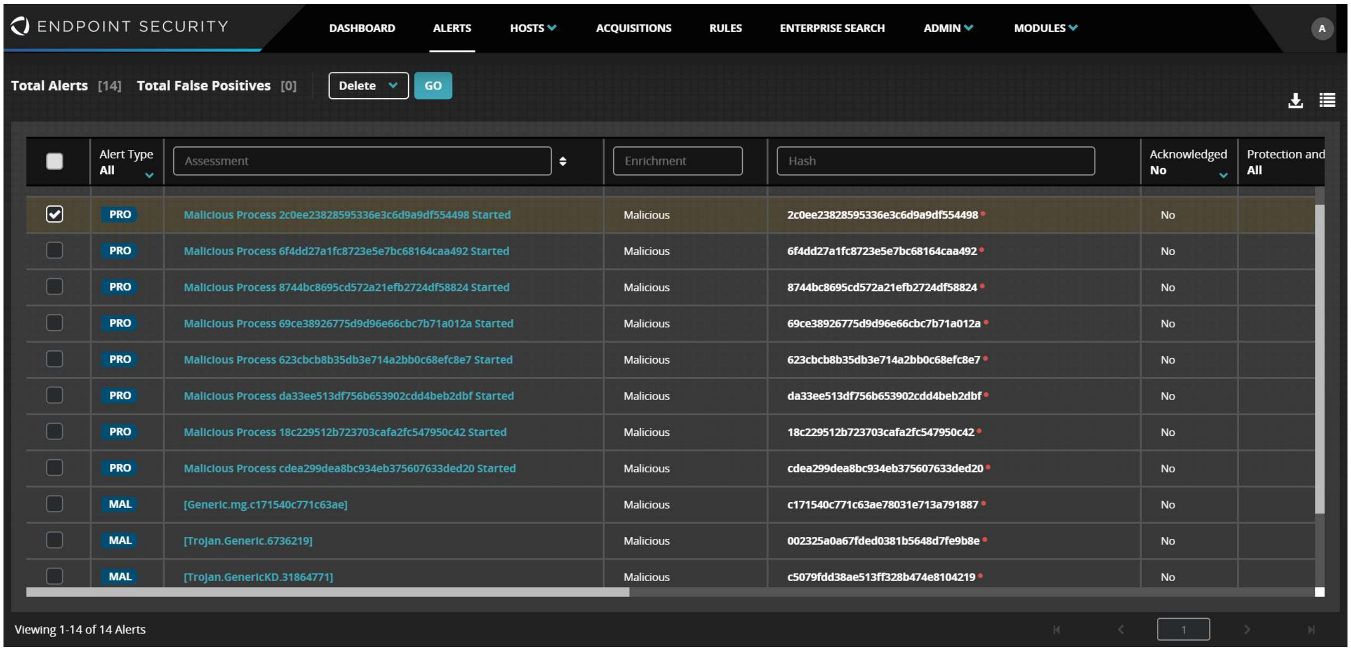
- The rows displayed per page is shown on the left. This value is not adjustable and currently set to 50.
- The current page is indicated by the text *Showing page X of Y*, where *X* is the current page position and *Y* is the total number of pages.
- You can move to the next page by clicking the **>** button
- You can move to the previous page by clicking the **<** button
- You can move to the last page by clicking the **>|** button
- You can move to the first page by clicking the **|<** button

- You can move to any page number by entering the desired page number into the entry field and pressing enter

Alerts

Alerts from Process Tracker will show on the **Alerts** page of the Endpoint Security Web UI. They will appear with the following distinguishing characteristics:

- Alert Type – PRO
- Assessment – Malicious Process <*md5 hash*> Started



Total Alerts [14] Total False Positives [0]

□	Alert Type All	Assessment	Enrichment	Hash	Acknowledged No	Protection and All
☑	PRO	Malicious Process 2c0ee23828595336e3c6d9a9df554498 Started	Malicious	2c0ee23828595336e3c6d9a9df554498	No	
□	PRO	Malicious Process 6f4dd27a1fc8723e5e7bc68164caa492 Started	Malicious	6f4dd27a1fc8723e5e7bc68164caa492	No	
□	PRO	Malicious Process 8744bc8695cd572a21efb2724df58824 Started	Malicious	8744bc8695cd572a21efb2724df58824	No	
□	PRO	Malicious Process 69ce38926775d9d96e66cbc7b71a012a Started	Malicious	69ce38926775d9d96e66cbc7b71a012a	No	
□	PRO	Malicious Process 623cbcb8b35db3e714a2bb0c68efc8e7 Started	Malicious	623cbcb8b35db3e714a2bb0c68efc8e7	No	
□	PRO	Malicious Process da33ee513df756b653902cdd4beb2dbf Started	Malicious	da33ee513df756b653902cdd4beb2dbf	No	
□	PRO	Malicious Process 18c229512b723703cafa2fc547950c42 Started	Malicious	18c229512b723703cafa2fc547950c42	No	
□	PRO	Malicious Process cdea299dea8bc934eb375607633ded20 Started	Malicious	cdea299dea8bc934eb375607633ded20	No	
□	MAL	[Generic.mg.c171540c771c63ae]	Malicious	c171540c771c63ae78031e713a791887	No	
□	MAL	[Trojan.Generic.6736219]	Malicious	002325a0a67fded0381b5648d7fe9b8e	No	
□	MAL	[Trojan.GenericKD.31864771]	Malicious	c5079fdd38ae513ff328b474e8104219	No	

Viewing 1-14 of 14 Alerts

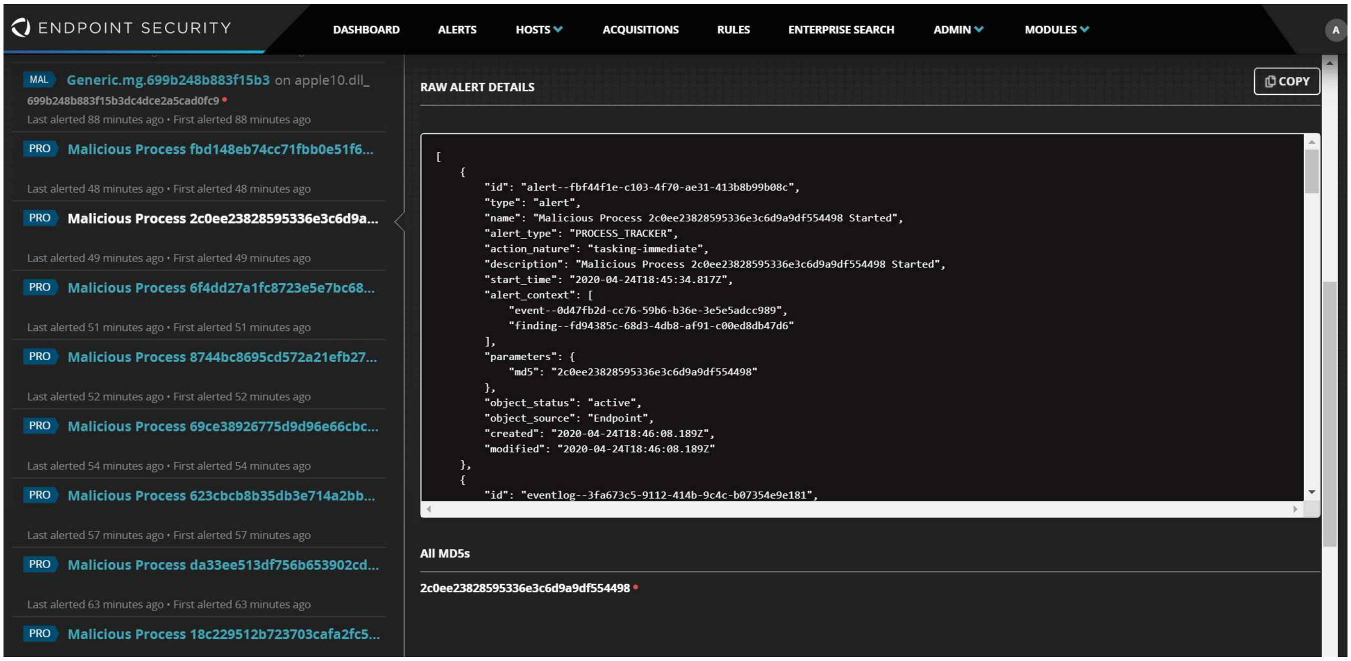
Figure 8 Sample of a Process Tracker Alert on the Alerts page of the Endpoint Security Web UI.

Clicking on the alert will bring you to the **Hosts** page to reveal the details of the alert.

Hosts (Alert Details)

Alerts from Process Tracker will show on the **Hosts** page of the Endpoint Security Web UI. They will appear with the following distinguishing characteristics:

- Alert Type – PRO
- Assessment – Malicious Process <*md5 hash*> Started



MAL Generic.mg.699b248b883f15b3 on apple10.dll_
699b248b883f15b3dc4dce2a5cad0fc9
Last alerted 88 minutes ago • First alerted 88 minutes ago

PRO Malicious Process fbd148eb74cc71fbb0e51f6...
Last alerted 48 minutes ago • First alerted 48 minutes ago

PRO Malicious Process 2c0ee23828595336e3c6d9a...
Last alerted 49 minutes ago • First alerted 49 minutes ago

PRO Malicious Process 6f4dd27a1fc8723e5e7bc68...
Last alerted 51 minutes ago • First alerted 51 minutes ago

PRO Malicious Process 8744bc8695cd572a21efb27...
Last alerted 52 minutes ago • First alerted 52 minutes ago

PRO Malicious Process 69ce38926775d9d96e66cbc...
Last alerted 54 minutes ago • First alerted 54 minutes ago

PRO Malicious Process 623cbcb8b35db3e714a2bb...
Last alerted 57 minutes ago • First alerted 57 minutes ago

PRO Malicious Process da33ee513df756b653902cd...
Last alerted 63 minutes ago • First alerted 63 minutes ago

PRO Malicious Process 18c229512b723703cafa2fc5...

RAW ALERT DETAILS

```
[
    {
        "id": "alert--fbf44f1e-c103-4f70-ae31-413b8b99b08c",
        "type": "alert",
        "name": "Malicious Process 2c0ee23828595336e3c6d9a9df554498 Started",
        "alert_type": "PROCESS_TRACKER",
        "action_nature": "tasking-immediate",
        "description": "Malicious Process 2c0ee23828595336e3c6d9a9df554498 Started",
        "start_time": "2020-04-24T18:45:34.817Z",
        "alert_context": [
            "event--0d47fb2d-cc76-59b6-b36e-3e5e5adcc989",
            "finding--fd94385c-68d3-4db8-af91-c00ed8db47d6"
        ],
        "parameters": {
            "md5": "2c0ee23828595336e3c6d9a9df554498"
        },
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "eventlog--3fa673c5-9112-414b-9c4c-b07354e9e181",
```

All MD5s

2c0ee23828595336e3c6d9a9df554498

Figure 9 Sample of a Process Tracker alert on the Hosts page in the Endpoint Security Web UI.

Additionally, the **Raw Alerts Details** provides the alert information in JSON format. The data model for this format is a set of interrelated objects, each that carry attributes related to a specific aspect of the alert. Within this data model the following object types are called out

Alert	High level attributes of the alert
DigitalSignature	Signature attributes of the file related to the process execution
Event	Attributes related to the execution detection
File	File information related to the process execution
Process	Information related to the process and the parent process

The Process Tracker fields map into this model as follows:

Field	Data Model Destination
Agent ID	Not represented. It is implicated by the Host being viewed.
Alerted At	**Alert**.start_time
Args	**Process**.arguments
Attributes	**File**.is_archive, **File**.is_compressed, **File**.is_encrypted, **File**.is_hidden, **File**.write
Creation Time	**File**.file_created
Enrichment Status	Not represented. Malicious is implied as the verdict
Event At	**Event**.start_time
File Size (bytes)	**File**.size_in_bytes

Field	Data Model Destination
Group	**File**.owner_group
Index	Not represented.
Is Prelinked	Not represented.
Is Signed	**DigitalSignature**.signature_exists
Last Accessed Time	**File**.file_last_accessed
Last Status Change Time	Not represented
MD5	**Alert**.parameters.md5, **File**.hashes.value
Modified Time	**File**.file_last_modified
Owner	**File**.owner_user
Parent Path	**Process**.parent.(**File**.path, **File**.name, **File**.file_extension)
Parent PID	**Process**.parent.pid
PID	**Process**.pid
Process File Cert	**DigitalSignature**.certificate_issuer, **DigitalSignature**.certificate_subject
Process File Exists	Not represented
Process Path	**File**.path, **File**.name, **File**.file_extension
Signature Verified	**DigitalSignature**.signature_verified
Start Time	**Event**.start_time
Type	**Event**.event_type
User	**Event**.account_name

Figure 10 Field mapping into Raw Alert Details

The following is a sample alert copied from Raw Alert Details. The fields that have been populated by the specific Process Tracker alert are indicated in **bold**.

```
[
    {
        "id": "alert--fbf44f1e-c103-4f70-ae31-413b8b99b08c",
        "type": "alert",
        "name": "Malicious Process 2c0ee23828595336e3c6d9a9df554498 Started",
        "alert_type": "PROCESS_TRACKER",
        "action_nature": "tasking-immediate",
        "description": "Malicious Process 2c0ee23828595336e3c6d9a9df554498 Started",
        "start_time": "2020-04-24T18:45:34.817Z",
        "alert_context": [
            "event--0d47fb2d-cc76-59b6-b36e-3e5e5adcc989",
            "finding--fd94385c-68d3-4db8-af91-c00ed8db47d6"
        ],
        "parameters": {
            "md5": "2c0ee23828595336e3c6d9a9df554498"
        },
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "eventlog--3fa673c5-9112-414b-9c4c-b07354e9e181",
        "type": "eventlog",
        "extensions": {
            "cef-log-ext": {
                "meta_information": {
                    "categoryTechnique": "Malware",
                    "categoryDeviceType": "Process Tracker",
                    "categoryTupleDescription": "Process Tracker found a compromise indication",
                    "categoryOutcome": "Success",
                    "categoryBehavior": "Found",
                    "categorySignificance": "Compromise"
                }
            }
        }
    },
    {
        "id": "file--79920691-91a0-5345-b53a-39afe34db2da",
        "type": "file",
        "name": "hipAutomationWhiteListTest10164.exe",
        "file_extension": ".exe",
        "file_path": "C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup\\hipAutomationWhiteListTest10164.exe",
        "size_in_bytes": 186861,
        "file_created": "2020-04-24T18:45:21.234Z",
        "file_last_modified": "2020-04-24T18:45:21.250Z",
        "file_last_accessed": "2020-04-24T18:45:21.250Z",
        "is_archive": true,
        "is_compressed": false,
        "is_encrypted": false,
        "is_hidden": false,
        "write": true,
        "hashes": [
            {
                "hash_algorithm": "md5",
                "value": "2c0ee23828595336e3c6d9a9df554498"
            }
        ],
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z",
        "owner_user": "BUILTIN\\Administrators",
        "owner_group": null,
        "digital_signatures": [
            "digital-signature-info-type--bca29082-6209-4543-87d0-35517feaf8fe"
        ]
    },
    {
        "id": "file--2cca9aa5-a3a9-5969-b2c8-1b5a7e6f5a1e",
        "type": "file",
        "name": "cmd.exe",
        "file_extension": ".exe",
        "file_path": "C:\\Windows\\System32\\cmd.exe",
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "process--0431d562-b9cd-4f24-9623-39a6139dfb98",
        "type": "process",
        "pid": 3620,
        "binary": "file--79920691-91a0-5345-b53a-39afe34db2da",
        "parent": "process--c45cdb05-bb5a-49d7-b0a7-2f8caf5cfe97",
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z",
        "arguments": "\"C:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Startup\\hipAutomationWhiteListTest10164.exe\"  /auto C:\\"
    },
    {
        "id": "process--c45cdb05-bb5a-49d7-b0a7-2f8caf5cfe97",
        "type": "process",
        "pid": 4384,
        "binary": "file--2cca9aa5-a3a9-5969-b2c8-1b5a7e6f5a1e",
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "finding--fd94385c-68d3-4db8-af91-c00ed8db47d6",
        "type": "finding",
        "risk_nature": "malicious",
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "software--79920691-91a0-5345-b53a-39afe34db2da",
        "type": "software",
        "name": "Enricher",
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "action--114e445e-6f84-59c2-a50a-0b7c5e7d8e0d",
        "type": "action",
        "name": "process-start",
        "action_nature": "observed",
        "start_time": "2020-04-24T18:45:33.446Z",
        "objects": [
            "process--0431d562-b9cd-4f24-9623-39a6139dfb98"
        ],
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:46:08.189Z",
        "modified": "2020-04-24T18:46:08.189Z"
    },
    {
        "id": "event--0d47fb2d-cc76-59b6-b36e-3e5e5adcc989",
        "type": "event",
        "event_type": "start",
        "name": "process-event observed and analyzed",
        "start_time": "2020-04-24T18:45:33.446Z",
        "objects": [
            "file--79920691-91a0-5345-b53a-39afe34db2da",
            "process--0431d562-b9cd-4f24-9623-39a6139dfb98",
            "finding--fd94385c-68d3-4db8-af91-c00ed8db47d6",
            "software--79920691-91a0-5345-b53a-39afe34db2da"
        ],
        "object_status": "active",
        "object_source": "Endpoint",
        "created": "2020-04-24T18:45:33.446Z",
        "modified": "2020-04-24T18:45:33.446Z",
        "account_name": "WINE51B13E84DB6\\Administrator"
    },
    {
        "id": "analysis--79920691-91a0-5345-b53a-39afe34db2da",
        "type": "analysis",
        "name": "enrich-context",
        "action_nature": "tasking-immediate",
        "is_automated": true,
        "performer": "software--79920691-91a0-5345-b53a-39afe34db2da",
        "parameters": {
            "hash": "2c0ee23828595336e3c6d9a9df554498"
        },
        "results": [
            "finding--fd94385c-68d3-4db8-af91-c00ed8db47d6"
        ]
    },
    {
        "id": "relationship--b1165b5d-55e0-4615-afc0-153deb7a3f58",
        "type": "relationship",
        "source": "event--0d47fb2d-cc76-59b6-b36e-3e5e5adcc989",
        "target": "analysis--79920691-91a0-5345-b53a-39afe34db2da",
        "relationship_type": "triggered"
    },
    {
        "id": "digital-signature-info-type--bca29082-6209-4543-87d0-35517feaf8fe",
        "type": "digital-signature-info-type",
        "signature_verified": false,
        "signature_exists": false
    }
]
```

Figure 11 Sample of Raw Alert Details

Part IV: The Process Tracker Data Interface

Data Availability

As mentioned in the notes on the columns for the **Grid Area** in the Web Interface, there are a few attributes that are not available on all platforms. For example, if an attribute *X* is only available on Windows, the value for that attribute when the event is reported by a platform other than Windows will be *null*. This is important to understand when parsing the attributes that are made available in the interfaces that we are about to describe.

Message Bus

The Endpoint Security Server provides two message bus topics that the Process Tracker module will post activity upon. One will stream the process execution events that are posted by the endpoints, the other will stream the alerts generated by the module.

Access to the message bus is made available via the Endpoint Security Server REST API. For complete details on how to interact with that API, please refer to FireEye document ***Endpoint Security REST API Guide Release 5.0.*** We will cover the details that are relevant to the Process Tracker module here.

Note that these are message bus topics, not permanent storage. Therefore, if you interface with a topic, do so with a process that can pull messages in a timely manner. Eventually old messages will roll off as new ones are created.

Process Execution Events

The process execution events are available on the **PROCESS_TRACKER** topic. Messages are recorded here when an agent posts a unique process event. If **Enrichment** of events is enabled, a secondary update message is posted when the enrichment status for the event is received from Enricher.

HTTP Verb	Server	URI
GET	/hx/api/services	/topic/PROCESS_TRACKER

Request Headers

X-OFFSET	The offset ID of the first message to retrieve. This can be omitted for the first request. A response header will provide an updated value for your next request. If you provide a value that is below the earliest message available, then the earliest available message is provided in the response.
X-MAX-MESSAGES	Optional, to limit/require the number of messages returned. Default is 500.
X-POLL-TIMEOUT	Maximum number of seconds to wait for X-MAX_MESSAGES to become available.

Response Codes (subset)

200	Success
204	No content

Response Headers (subset)

X-OFFSET	The new position in the topic. This should be saved and provided as the X-OFFSET in the next GET request.
Warning	Provides details regarding issues with X-OFFSET

Response

The response is newline terminated text base that is a combination of boundary tags, message header information and JSON message payload.

```
--Boundary_409686_968730724_1587661791987
TS: 1587146250151
BTS: 1587146250151
MID: 186ca9acbbd6842c
SID: PROCESS-TRACKER
CID: tVC951q7Ri4dQglrR5NrtQ
AID: PROCESS-TRACKER
TPC: PROCESS_TRACKER
Content-Disposition: form-data; name="PROCESS_TRACKER"; filename="PROCESS-TRACKER"
Content-Type: application/binary

{"type":"event","data":{"uuid":"7e4a1da6-7e49-4829-9f5d-
566e1c7d16c6","id":2,"md5":"acbdfdbdfb5f1995d26e34ca351a6657","agent_id":"BH3E2ZjPcd3bUeKIrjYe5n","eve
nt_at":"2020-04-
17T17:56:58.242Z","process_file_exists":true,"process_path":"C:\\Windows\\System32\\sppsvc.exe","pid":
17612,"parent_path":"C:\\Windows\\System32\\services.exe","parent_pid":700,"file_size":4589056,"file_c
reated_at":"2020-03-17T17:25:36.446Z","file_last_accessed_at":"2020-03-
17T17:25:36.717Z","file_last_modified_at":"2020-03-
17T17:25:36.717Z","args":null,"type":"end","started_at":"2020-04-17T17:56:58.242Z","user":"NT
AUTHORITY\\NETWORK SERVICE","owner":"NT
SERVICE\\TrustedInstaller","is_signed":true,"file_attributes":"Archive","process_file_cert":{"Issuer":
"C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Windows Production PCA
2011","Subject":"C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft
Windows","Algorithm":"sha256","SerialNumber":"330000023241fb59996dcc4dff000000000232","ExpirationTime"
:"2020-05-
02T21:24:36.000Z"},"signature_verified":true,"group":null,"last_status_change_time":null,"is_prelinked
":null,"updated_at":"2020-04-17T17:57:30.135Z","created_at":"2020-04-
17T17:57:30.118Z","alerted_at":null,"enrichment_status":"REQUESTED","enrichment_requested_at":"2020-
04-17T17:57:30.134Z"}}
--Boundary_409686_968730724_1587661791987--
```

Figure 12 Sample Response of a request to get one message.

Process Execution Event Payload

The payload is a key-value dictionary with the following keys:

Key	Notes
type	"event" – denotes that this message within the topic is for a process execution event "event_update" – denotes that this message in an update for a prior message posted within the topic
data	Dictionary of attributes associated to the event

The following table maps the keys in the data dictionary to the fields that are described in the **Grid Area** of the Web Interface or describes the value directly, if it is not available within the grid.

data.key	Notes
agent_id	Grid Area.Agent ID
alerted_at	Grid Area.Alerted At
args	Grid Area.Args
attributes	Grid Area.Attributes
created_at	Timestamp that the event was consumed by the server module
enrichment_requested_at	Timestamp of when the event was posted to the Enricher module
enrichment_status	Grid Area.Enrichment Status
event_at	Grid Area.Event At
file_created_at	Grid Area.Creation Time
file_last_accessed_at	Grid Area.Last Accessed Time
file_last_modified_at	Grid Area.Modified Time
file_size	Grid Area.File Size (bytes)
group	Grid Area.Group
id	Grid Area.Index
is_prelinked	Grid Area.Is Prelinked
is_signed	Grid Area.Is Signed
last_status_change_time	Grid Area.Last Status Change Time
md5	Grid Area.MD5
owner	Grid Area.Owner
parent_path	Grid Area.Parent Path
parent_pid	Grid Area.Parent PID
pid	Grid Area.PID
process_file_cert	Grid Area.Process File Cert
process_file_exists	Grid Area.Process File Exists
process_path	Grid Area.Process Path
signature_verified	Grid Area.Signature Verified
started_at	Grid Area.Start Time
type	Grid Area.Type
updated_at	Timestamp of last update to this event
user	Grid Area.User

data.key	Notes
uuid	Unique ID for the event. This can be used to tie events and update_events together.

Figure 13 Mapping of Data Keys to Grid Data

Process Tracker Alerts

If the Process Tracker module is configured to generate alerts for malicious process executions, it will post the alert to the **HX_ALERTS** topic. This topic will hold messages for all alert types generated on your instance of the Endpoint Security Server, not only the ones produced by the Process Tracker module.

HTTP Verb	Server	URI
GET	/hx/api/services	/topic/HX_ALERTS

The request headers, response codes and response headers are the same as those called out for **Process Execution Events**, above.

Response

The response is newline terminated text base that is a combination of boundary tags, message header information and JSON message payload.

```
--Boundary_300_380661968_1587754355337
TS: 1587751687198
BTS: 1587751687198
MID: f9b04b28bf4c87f3
SID: app-processor
CID: baAHA18PHEgdx80GtPZyiI
AID: HX
TPC: HX_ALERTS
Content-Disposition: form-data; name="HX_ALERTS"; filename="HX"
Content-Type: application/binary

{"type":"alert","producer":"app-
processor","subtype":"PROCESS_TRACKER","data":{"_id":5,"agent":{"_id":"6Kk3YlsJus6dTm1E9zS3yc","url":"
/hx/api/v3/hosts/6Kk3YlsJus6dTm1E9zS3yc","containment_state":"normal"},"event_at":"2020-04-
24T18:07:20.115Z","matched_at":"2020-04-24T18:07:20.115Z","reported_at":"2020-04-
24T18:07:48.571Z","source":"PROCESS_TRACKER","subtype":null,"matched_source_alerts":[],"resolution":"A
LERT","is_false_positive":false,"decorators":[],"md5values":["cdea299dea8bc934eb375607633ded20"],"deco
rator_statuses":[],"url":"/hx/api/v3/alerts/5","condition":null,"indicator":null,"event_id":null,"even
t_type":null,"event_values":[{"id":"alert--ff8367cb-1451-4a1d-88b0-
e715dcf162ef","type":"alert","name":"Malicious Process cdea299dea8bc934eb375607633ded20
Started","alert_type":"PROCESS_TRACKER","action_nature":"tasking-immediate","description":"Malicious
Process cdea299dea8bc934eb375607633ded20 Started","start_time":"2020-04-
24T18:07:20.115Z","alert_context":["event--79920691-91a0-5345-b53a-39afe34db2da","finding--644ad639-
b5fa-49e0-968f-
1c7b556ca305"],"parameters":{"md5":"cdea299dea8bc934eb375607633ded20"},"object_status":"active","objec
t_source":"Endpoint","created":"2020-04-24T18:07:48.528Z","modified":"2020-04-
24T18:07:48.528Z"},{"id":"eventlog--9ac4b4a6-3af0-4641-93ce-
644a7771f9b8","type":"eventlog","extensions":{"cef-log-
ext":{"meta_information":{"categoryTechnique":"Malware","categoryDeviceType":"Process
Tracker","categoryTupleDescription":"Process Tracker found a compromise
indication","categoryOutcome":"Success","categoryBehavior":"Found","categorySignificance":"Compromise"
}}}},{"id":"file--79920691-91a0-5345-b53a-
39afe34db2da","type":"file","name":"RandomEvent.exe","file_extension":".exe","file_path":"C:\\Program
Files\\RandomEvent\\RandomEvent.exe","size_in_bytes":2272432,"file_created":"2016-10-
16T01:19:22.000Z","file_last_modified":"2016-10-16T01:20:22.000Z","file_last_accessed":"2016-10-
28T18:26:12.144Z","is_archive":true,"is_compressed":false,"is_encrypted":true,"is_hidden":false,"write
":true,"hashes":[{"hash_algorithm":"md5","value":"cdea299dea8bc934eb375607633ded20"}],"object_status":
"active","object_source":"Endpoint","created":"2020-04-24T18:07:48.528Z","modified":"2020-04-
24T18:07:48.528Z","owner_user":"BUILTIN\\Administrators","owner_group":"wheel","digital_signatures":["
digital-signature-info-type--0d9619a3-048e-4da4-8684-7c70b4208bf0"]},{"id":"file--2cca9aa5-a3a9-5969-
b2c8-
1b5a7e6f5a1e","type":"file","name":"explorer.exe","file_extension":".exe","file_path":"C:\\Windows\\ex
plorer.exe","object_status":"active","object_source":"Endpoint","created":"2020-04-
24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z"},{"id":"process--2b652c42-970a-4720-bc40-
bc44de64a2f5","type":"process","pid":11864,"binary":"file--79920691-91a0-5345-b53a-
39afe34db2da","parent":"process--cc72747d-cd9d-4d29-b8f1-
ad93afc6bb86","object_status":"active","object_source":"Endpoint","created":"2020-04-
24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z","arguments":"\"C:\\Program
Files\\RandomEvent\\RandomEvent.exe\""},{"id":"process--cc72747d-cd9d-4d29-b8f1-
ad93afc6bb86","type":"process","pid":2032,"binary":"file--2cca9aa5-a3a9-5969-b2c8-
1b5a7e6f5a1e","object_status":"active","object_source":"Endpoint","created":"2020-04-
24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z"},{"id":"finding--644ad639-b5fa-49e0-968f-
1c7b556ca305","type":"finding","risk_nature":"malicious","object_status":"active","object_source":"End
point","created":"2020-04-24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z"},{"id":"software--
79920691-91a0-5345-b53a-
39afe34db2da","type":"software","name":"Enricher","object_status":"active","object_source":"Endpoint",
"created":"2020-04-24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z"},{"id":"action--735adbdc-
6553-5b19-b6f4-2ceca35afafd","type":"action","name":"process-
start","action_nature":"observed","start_time":"2020-04-24T00:00:00.000Z","objects":["process--
2b652c42-970a-4720-bc40-
bc44de64a2f5"],"object_status":"active","object_source":"Endpoint","created":"2020-04-
24T18:07:48.528Z","modified":"2020-04-24T18:07:48.528Z"},{"id":"event--79920691-91a0-5345-b53a-
39afe34db2da","type":"event","event_type":"start","name":"process-event observed and
analyzed","start_time":"2020-04-24T00:00:00.000Z","objects":["file--79920691-91a0-5345-b53a-
39afe34db2da","process--2b652c42-970a-4720-bc40-bc44de64a2f5","finding--644ad639-b5fa-49e0-968f-
1c7b556ca305","software--79920691-91a0-5345-b53a-
39afe34db2da"],"object_status":"active","object_source":"Endpoint","created":"2020-04-
24T00:00:00.000Z","modified":"2020-04-
24T00:00:00.000Z","account_name":"FIREEYE\\matthew.tardiff"},{"id":"analysis--79920691-91a0-5345-b53a-
39afe34db2da","type":"analysis","name":"enrich-context","action_nature":"tasking-
immediate","is_automated":true,"performer":"software--79920691-91a0-5345-b53a-
39afe34db2da","parameters":{"hash":"cdea299dea8bc934eb375607633ded20"},"results":["finding--644ad639-
b5fa-49e0-968f-1c7b556ca305"]},{"id":"relationship--4baee7d9-d716-4ee3-beec-
e2d0508d0ab9","type":"relationship","source":"event--79920691-91a0-5345-b53a-
39afe34db2da","target":"analysis--79920691-91a0-5345-b53a-
39afe34db2da","relationship_type":"triggered"},{"id":"digital-signature-info-type--0d9619a3-048e-4da4-
8684-7c70b4208bf0","type":"digital-signature-info-
type","signature_verified":true,"signature_exists":true,"certificate_issuer":"C=US, S=Washington,
L=Redmond, O=Microsoft Corporation, CN=Microsoft Windows Production PCA
2011","certificate_subject":"sha256"}]}}
--Boundary_300_380661968_1587754355337
```

Figure 14 Sample Response

Process Tracker Alert Payload

The payload is a key-value dictionary with the following keys:

Key	Notes
type	"alert" – denotes that this message within the topic is for a new alert "alert_update" – denotes that this message in an update for a prior alert posted within the topic
data	Dictionary of attributes associated to the alert

The information that is returned within the *data* dictionary of the response is structured exactly the same as what is described in **Hosts (Alert Details)**, above.

CEF Notifications

The Process Tracker module will submit a CEF notification for every alert that it creates. See FireEye document ***Alert Notifications CEF | LEEF | CSV | XML | JSON, Release 2020.1*** for background information on CEF notifications and field definitions. Also refer to appendix B, *CEF Logs and Output* within the ***Endpoint Security Server User Guide***

Process Tracker Hit Found (Endpoint Security) - Sample Message:

```
CEF:0|fireeye|hx|9.9.0|Process Tracker Hit Found|Process Tracker Hit Found|10|rt=May 01 2018 05:42:14
UTC dvchost=abc-hx.helix.apps.fireeye.com categoryDeviceGroup=/IDS categoryDeviceType=Process Tracker
categoryObject=/Host cs1Label=Host Agent Cert Hash cs1=Doug5I839radPSmAwf3512 dst=10.1.49.81 dmac=00-50-
56-88-e5-99 dhost=Home-PC-11 dntdom=WORKGROUP deviceCustomDate1Label=Agent Last Audit
deviceCustomDate1=May 01 2018 04:54:30 UTC cs2Label=FireEye Agent Version cs2=26.21.8 cs5Label=Target
GMT Offset cs5=+PT2H cs6Label=Target OS cs6=Windows 10 Pro 16299 externalId=3407 start=May 01 2018
05:42:13 UTC categoryOutcome=/Success categorySignificance=/Compromise categoryBehavior=/Found
cs7Label=Resolution cs7=ALERT cs8Label=Alert Types cs8=PRT cs13Label=Malware Engine cs13=AV
cs12Label=Malware Category cs12=file-event act=Detection PRT Hit msg=Host Home-PC-11 Malware alert
categoryTupleDescription=Process Tracker found a compromise indication. cs4Label=Process Name
cs4=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe cs9Label=MD5
cs9=94bcdff4b00947b34795c6f2209c9707 cs10Label=SHA1 cs10=918652d77d2ffce0ea282fe1f61fffd207b5d6ab
cs11Label=Malware Signature cs11=Trojan.GenericKD.30688709 categoryTechnique=Malware
```

Module REST API

The following API endpoints are provided by the Process Tracker module. Note that these API endpoints focus around retrieval of process execution events. To access other aspects that tie into Endpoint Security Server artifacts such as alerts, policies, etc., refer to the FireEye document ***Endpoint Security REST API Guide Release 5.0*** for details.

Endpoint	Purpose
/events	GET the process execution events currently available as JSON
/events/export	GET the process execution events currently available as CSV
/events/:id	GET a specific process execution event

Accessing these API endpoints is controlled in the same manner as the base API for the Endpoint Security Server. Please refer to the FireEye document ***Endpoint Security REST API Guide Release 5.0*** for details.

API: Get Process Execution Events

Returns process execution events from the Process Tracker database as a JSON result.

HTTP Verb	Server	URI
GET	/hx/api/plugins	/process-tracker/v1/events

Query Parameters

Parameter	Notes
limit=<unsigned 32>	Limits the number of records returned. The default is 50.
offset=<unsigned 32>	Used for pagination. Returns the records starting with this offset. Default is 0.
sort=<text>	Sorts the result by the specified field and direction. Default is `id:ascending`. **Valid fields**: `agent_id, alerted_at, args, enrichment_requested_at, enrichment_status, event_at, file_attributes, file_created_at, file_last_accessed_at, file_last_modified_at, file_size, group, id, is_prelinked, is_signed, last_status_change_time, md5, owner, parent_path, parent_pid, pid, process_file_cert, process_file_exists, process_path, signature_verified, started_at, type, user, uuid` **Valid directions**: `ascending, descending`

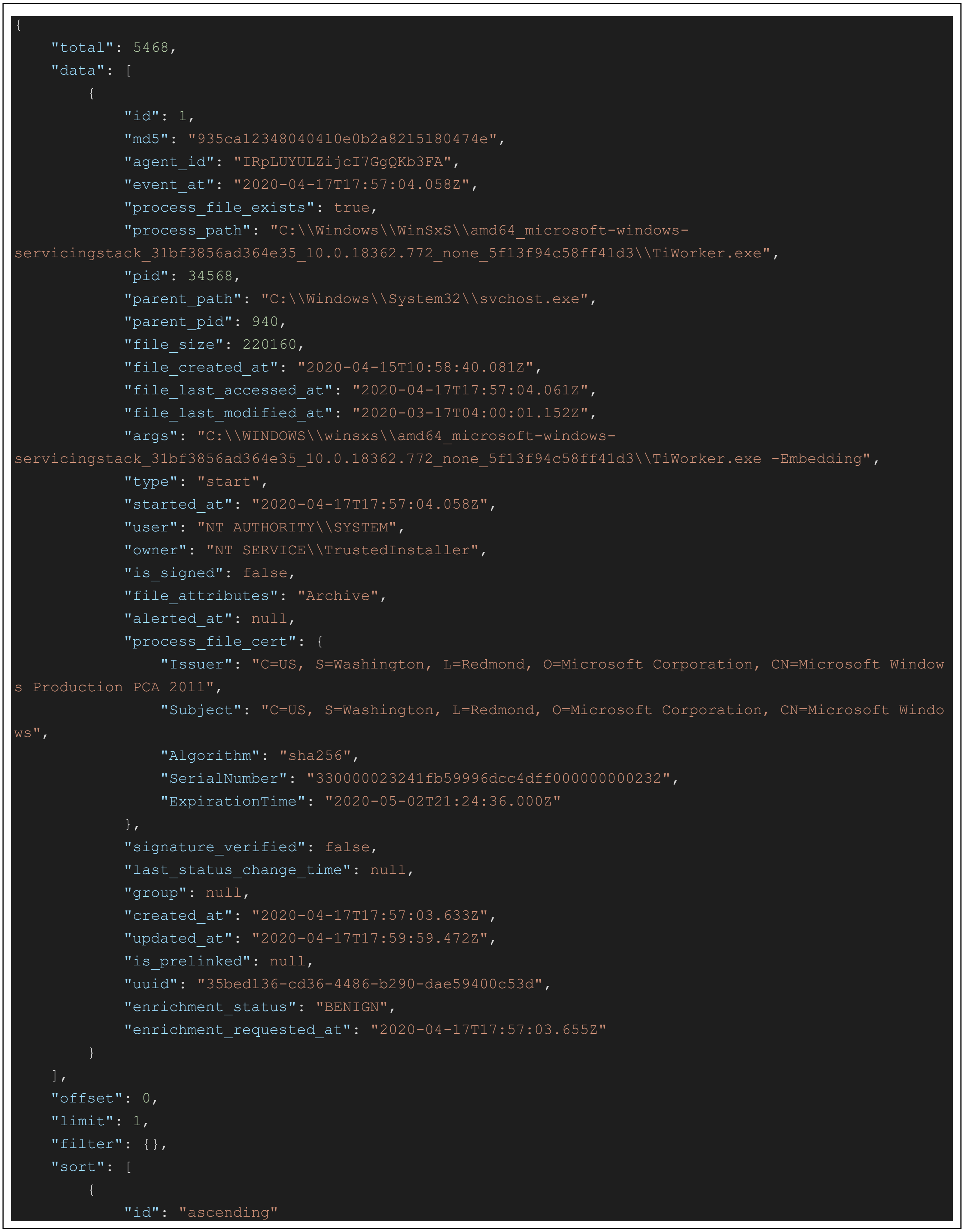
Parameter	Notes

filter=<filter spec list>	Specifies how to filter the events. The Default is no filter.
	A filter spec is declared with the following keys and values:
	`{`
	`   “operator”:”eq”,`
	`   “field”:”file_size”,`
	`   “arg”:[30000]`
	`}`
	Where `field` is any of the listed **Valid Fields** above, `arg` is the value(s) to match against.
	
	Valid values for operator are:
	`eq, contains, between`
	
	A complex filter can contain more than one filter spec as follows:
	`filter=[{filter spec 1},{filter spec 2},…]`
	where the implied operation between filter specs is AND

Response

The information that is returned is a JSON dictionary with the following keys

Key	Notes
total	Number of data rows (events) available
data	List of rows, each as a key-value dictionary with a key for each `field` listed in the **Valid Fields**, above.
offset	The offset requested
limit	The limit requested
filter	The filter requested
sort	The sort requested



```
{
    "total": 5468,
    "data": [
        {
            "id": 1,
            "md5": "935ca12348040410e0b2a8215180474e",
            "agent_id": "IRpLUYULZijcI7GgQKb3FA",
            "event_at": "2020-04-17T17:57:04.058Z",
            "process_file_exists": true,
            "process_path": "C:\\Windows\\WinSxS\\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\\TiWorker.exe",
            "pid": 34568,
            "parent_path": "C:\\Windows\\System32\\svchost.exe",
            "parent_pid": 940,
            "file_size": 220160,
            "file_created_at": "2020-04-15T10:58:40.081Z",
            "file_last_accessed_at": "2020-04-17T17:57:04.061Z",
            "file_last_modified_at": "2020-03-17T04:00:01.152Z",
            "args": "C:\\WINDOWS\\winsxs\\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\\TiWorker.exe -Embedding",
            "type": "start",
            "started_at": "2020-04-17T17:57:04.058Z",
            "user": "NT AUTHORITY\\SYSTEM",
            "owner": "NT SERVICE\\TrustedInstaller",
            "is_signed": false,
            "file_attributes": "Archive",
            "alerted_at": null,
            "process_file_cert": {
                "Issuer": "C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Window
s Production PCA 2011",
                "Subject": "C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Windo
ws",
                "Algorithm": "sha256",
                "SerialNumber": "330000023241fb59996dcc4dff000000000232",
                "ExpirationTime": "2020-05-02T21:24:36.000Z"
            },
            "signature_verified": false,
            "last_status_change_time": null,
            "group": null,
            "created_at": "2020-04-17T17:57:03.633Z",
            "updated_at": "2020-04-17T17:59:59.472Z",
            "is_prelinked": null,
            "uuid": "35bed136-cd36-4486-b290-dae59400c53d",
            "enrichment_status": "BENIGN",
            "enrichment_requested_at": "2020-04-17T17:57:03.655Z"
        }
    ],
    "offset": 0,
    "limit": 1,
    "filter": {},
    "sort": [
        {
            "id": "ascending"
```

```
        }
    ]
}
```

Figure 15 Sample Response

API: Get Process Execution Events, CSV Formatted

Returns process execution events from the Process Tracker database as CSV(Comma Separated Values) formatted data

HTTP Verb	Server	URI
GET	/hx/api/plugins	/process-tracker/v1/events/export

Query Parameters

Parameter	Notes
limit=<unsigned 32>	Limits the number of records returned. The default is 50. The maximum allowed is 10,000.
offset=<unsigned 32>	Used for pagination. Returns the records starting with this offset. Default is 0.
sort=<text>	Sorts the result by the specified field and direction. See //events for the remaining details of this parameter.
filter=<filter spec list>	Specifies how to filter the events. The Default is no filter. See //events for the remaining details of this parameter.
columns=<text>	A comma separated list of **Valid Fields** to include in the export. Default is all fields.

Response

The information that is returned is CSV formatted data. Each row of the CSV data is terminated by a newline. The first row is the column header row. Note that the column headers are representative of the text that is shown in the data grid. For example, field *id* is returned as *Index* because that is how it is represented in the **Grid Area** of the Web Interface. The following fields are also available that are not in the Grid Area. Their description can be found within Figure 13 under **Message Bus Process Execution Events**.

- Created At
- Enrichment Requested At
- Updated At
- UUID

```
Index,UUID,MD5,Agent ID,Event At,Process File Exists,Process Path,PID,Parent Path,Parent PID,File Size
in Bytes,Creation Time,Last Accessed Time,Modified Time,Args,Type,Start Time,User,Owner,Is
Signed,Attributes,Alerted At,Process File Cert,Signature Verified,Last Status Change Time,Group,Is
Prelinked,Enrichment Status,Enrichment Requested At,Created At,Updated At

1,35bed136-cd36-4486-b290-dae59400c53d,935ca12348040410e0b2a8215180474e,IRpLUYULZijcI7GgQKb3FA,2020-
04-17T17:57:04.058Z,true,C:\Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\TiWorker.exe,34568,C:\Windows\Sys
tem32\svchost.exe,940,220160,2020-04-15T10:58:40.081Z,2020-04-17T17:57:04.061Z,2020-03-
17T04:00:01.152Z,C:\WINDOWS\winsxs\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\TiWorker.exe -
Embedding,start,2020-04-17T17:57:04.058Z,NT AUTHORITY\SYSTEM,NT
SERVICE\TrustedInstaller,false,Archive,,"{""Issuer"":""C=US, S=Washington, L=Redmond, O=Microsoft
Corporation, CN=Microsoft Windows Production PCA 2011"",""Subject"":""C=US, S=Washington, L=Redmond,
O=Microsoft Corporation, CN=Microsoft
Windows"",""Algorithm"":""sha256"",""SerialNumber"":""330000023241fb59996dcc4dff000000000232"",""Expir
ationTime"":""2020-05-02T21:24:36.000Z""}",false,,,,BENIGN,2020-04-17T17:57:03.655Z,2020-04-
17T17:57:03.633Z,2020-04-17T17:59:59.472Z

2,7e4a1da6-7e49-4829-9f5d-566e1c7d16c6,acbdfdbdfb5f1995d26e34ca351a6657,BH3E2ZjPcd3bUeKIrjYe5n,2020-
04-
17T17:56:58.242Z,true,C:\Windows\System32\sppsvc.exe,17612,C:\Windows\System32\services.exe,700,458905
6,2020-03-17T17:25:36.446Z,2020-03-17T17:25:36.717Z,2020-03-17T17:25:36.717Z,,end,2020-04-
17T17:56:58.242Z,NT AUTHORITY\NETWORK SERVICE,NT
SERVICE\TrustedInstaller,true,Archive,,"{""Issuer"":""C=US, S=Washington, L=Redmond, O=Microsoft
Corporation, CN=Microsoft Windows Production PCA 2011"",""Subject"":""C=US, S=Washington, L=Redmond,
O=Microsoft Corporation, CN=Microsoft
Windows"",""Algorithm"":""sha256"",""SerialNumber"":""330000023241fb59996dcc4dff000000000232"",""Expir
ationTime"":""2020-05-02T21:24:36.000Z""}",true,,,,REQUESTED,2020-04-17T17:57:30.134Z,2020-04-
17T17:57:30.118Z,2020-04-17T17:57:30.135Z
```

Figure 16 Sample Response. The first events were requested. Note that a blank line was inserted in this response to denote the presence of a newline character.

API: Get Specific Process Execution Event

Returns information about a specific event, identified by the id. The id is the value represented by *Index* in the **Grid Area** of the Web Interface, which is the same as the value returned in the *id* attribute of these API.

HTTP Verb	Server	URI
GET	/hx/api/plugins	/process-tracker/v1/events/:id

Query Parameters

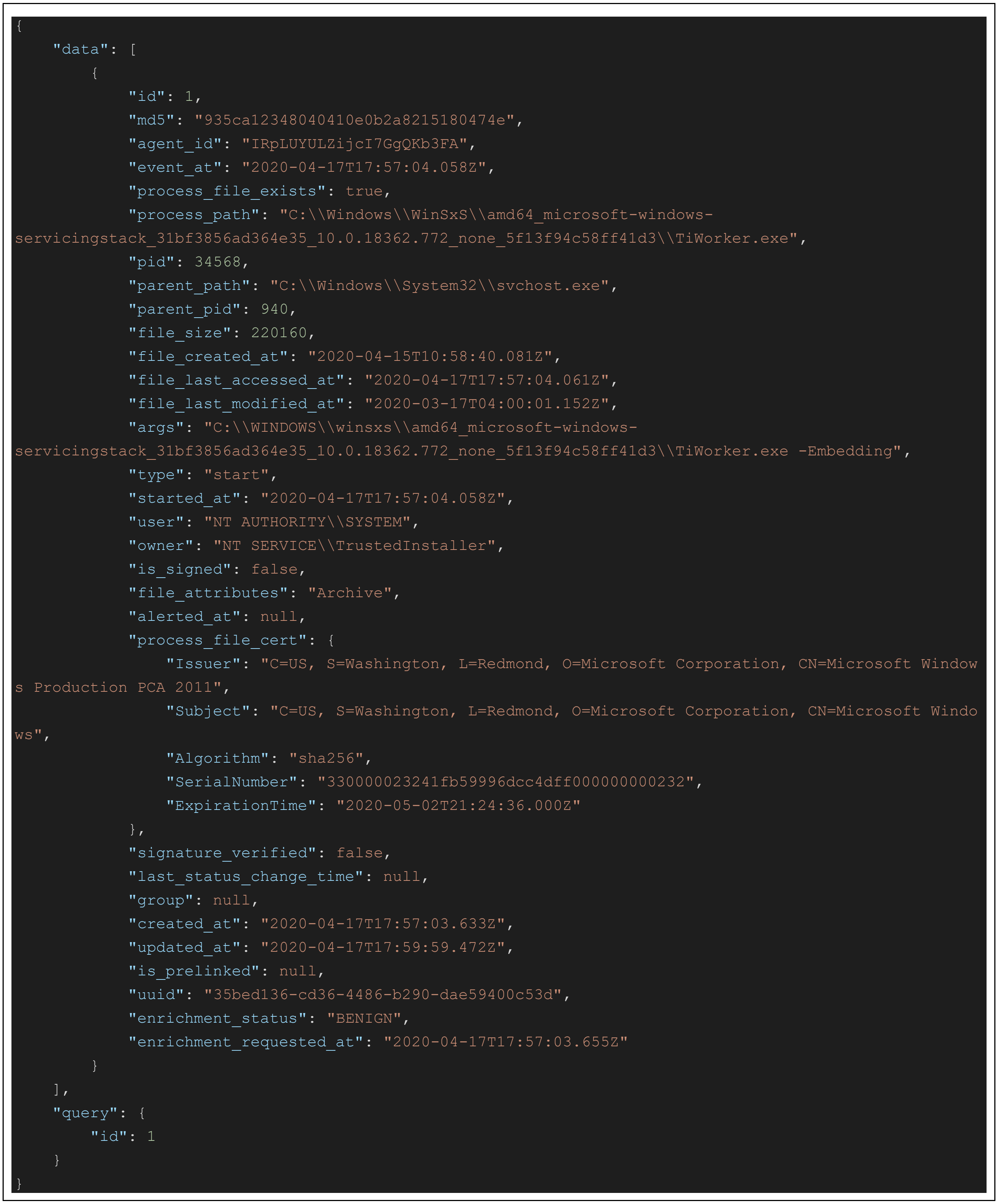
None. The URI specifies the query.

Response

The information that is returned is a JSON dictionary with the following keys

Key	Notes
data	A one element list for the inquired row, where the element is a key-value dictionary with a key for each `field` listed in the V**alid Fields**, above.

Key	Notes
query	The id of the event requested



```
{
    "data": [
        {
            "id": 1,
            "md5": "935ca12348040410e0b2a8215180474e",
            "agent_id": "IRpLUYULZijcI7GgQKb3FA",
            "event_at": "2020-04-17T17:57:04.058Z",
            "process_file_exists": true,
            "process_path": "C:\\Windows\\WinSxS\\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\\TiWorker.exe",
            "pid": 34568,
            "parent_path": "C:\\Windows\\System32\\svchost.exe",
            "parent_pid": 940,
            "file_size": 220160,
            "file_created_at": "2020-04-15T10:58:40.081Z",
            "file_last_accessed_at": "2020-04-17T17:57:04.061Z",
            "file_last_modified_at": "2020-03-17T04:00:01.152Z",
            "args": "C:\\WINDOWS\\winsxs\\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.772_none_5f13f94c58ff41d3\\TiWorker.exe -Embedding",
            "type": "start",
            "started_at": "2020-04-17T17:57:04.058Z",
            "user": "NT AUTHORITY\\SYSTEM",
            "owner": "NT SERVICE\\TrustedInstaller",
            "is_signed": false,
            "file_attributes": "Archive",
            "alerted_at": null,
            "process_file_cert": {
                "Issuer": "C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Window
s Production PCA 2011",
                "Subject": "C=US, S=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Windo
ws",
                "Algorithm": "sha256",
                "SerialNumber": "330000023241fb59996dcc4dff000000000232",
                "ExpirationTime": "2020-05-02T21:24:36.000Z"
            },
            "signature_verified": false,
            "last_status_change_time": null,
            "group": null,
            "created_at": "2020-04-17T17:57:03.633Z",
            "updated_at": "2020-04-17T17:59:59.472Z",
            "is_prelinked": null,
            "uuid": "35bed136-cd36-4486-b290-dae59400c53d",
            "enrichment_status": "BENIGN",
            "enrichment_requested_at": "2020-04-17T17:57:03.655Z"
        }
    ],
    "query": {
        "id": 1
    }
}
```

Figure 17 Sample Response

Part V: Agent Reporting via Agent Info Audit

An agent with Process Tracker enabled will report the following additional information within the Agent Info audit. The prefix for the keys on the following fields is *AgentInfo/ProcessTracker*.

Field<type>	Description
version<text>	Version of the Process Tracker agent plugin installed on the endpoint
operational<bool>	The plugin is operational and monitoring for process execution events
processEventCount<unsigned 64>	Number of process execution events encountered since install
uniqueProcessCount<unsigned 64>	Number of unique process execution events encountered since install
augmentationErrors<unsigned 64>	Number of process execution events for which the plugin failed to collect the event metadata
lastEventTimestamp<text>	Time of last process execution event that was encountered, ISO 8601
lastMessageTimestamp<text>	Time of last process execution event streamed to the Endpoint Security server, ISO 8601
lastDBResetTimestamp<text>	Time of last database reset, ISO 8601
store<enum-text>	Database storage mode: **database** – disk, persistent **memory-only** – in memory, degraded, lost upon restart
queueDepth<unsigned 64>	Number of process execution events awaiting augmentation, ahead of being streamed to the Endpoint Security server
maxQueueDepth<unsigned 64>	High water mark of the queueDepth, since restart.
minQueueTimeMs<float>	Minimum time queued for processing, since restart
maxQueueTimeMs<float>	Maximum time queued for processing, since restart
avgQueueTimeMs<float>	Average time queued for processing, since restart
queueTimeStdDevMs<float>	Standard deviation for time queued for processing, since restart
maxRunTimeMs<float>	Maximum time elapsed while processing an event, since restart
minRunTimeMs<float>	Minimum time elapsed while processing an event, since restart
avgRunTimeMs<float>	Average time elapsed while processing an event, since restart
runTimeStdDevMs<float>	Standard deviation for elapsed time while processing an event, since restart
excludedProcessPaths<unsigned 64>	Number of times that a process event was excluded via process exclusion, since install. (See **Configuring Process Tracker Agent Policy**)

Field<type>	Description
excludedFilePatterns<unsigned 64>	Number of times that a process event was excluded via file/path exclusion, since install. (See **Configuring Process Tracker Agent Policy**)
excludedAgentProcs<unsigned 64>	Number of times that Endpoint Security agent excluded itself, since install.

APPENDIX A: Frequently Asked Questions

How to verify if the Agent installation succeeded?

The Host Management module plugin provides a view into what is installed on each host in your endpoint population connected to the Endpoint Security Server. When the Process Tracker module is installed, it will make two additional columns available to be displayed within this view. If the columns are not shown, you may need to make them visible using the **column manager** tool above the grid in the Host Management view

- Process Tracker Status
- Process Tracker Version

To verify that the Process Tracker module is installed and running on a host, use this view to locate the target host and observe the values within these two columns. You should find that the value of status is *running* and version is *1.2.4*.

Are there any log files created during installation on the endpoint agents?

There are no log files specific to the Process Tracker module. The log entries from the module can be found within the log file of the main agent.

Is there a log on the HX appliance for the Process Tracker server module?

There are no log files specific to the Process Tracker module. The log entries from the module can be found within the log file of the base Endpoint Security Server.

What are the processes created when Process Tracker is installed and enabled?

On the agent, a new process is created as a sub-process of the main agent. The process is named the same, *xagt*.

Dependencies / Limitations

For Process Tracker to function on the agent, the agent must have Real-Time Indicator Detection turned on.

Known Issues

The following issues are known in Process Tracker release 1.2.4. The relevant issue tracking number for each item is included in parenthesis.

- Process Tracker crash on Windows after changing Real-Time Indicator Detection storage mode (**ENDPT-56226**)

- Filter sets, import overwrites existing filters without warning (**ENDPT-31929**)

- Private filters do not export (**ENDPT-53913**)

- Process Tracker crash on Linux after updating policy to turn off active event collection (**ENDPT-53453**)

- During backup of Process Tracker, a stack trace is printed in the logs (**ENDPT-58213**)

- Export of Process Tracker grid filtered by *IsPrelinked* does not contain the same data as seen in the grid of the Web UI (**ENDPT-54455**)

- Configuring Process Tracker Server Module, user not prompted to save updates before navigation off page. Updates are not saved. (**ENDPT-47766**)

- Process Tracker grid loses filter and sort settings when page is refreshed (**ENDPT-46541**)

- Enrichment *status* filter is case sensitive / inconsistent with *status* filter within the Enricher grid. (**ENDPT-53392**)

- Polymer exceptions appear in the log when accessing the Process Tracker Web UI. (**ENDPT-52944**)

- Filter of *Path* and *Parent Path* does not work as expected when using a single '\' as a path separator. (**ENDPT-58331**)

- Custom date picker does not appear when creating a filter on a timestamp column in the grid. (**ENDPT-57903**)