FireEye Endpoint Security Tech Preview Module User Guide

JULY 2019

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

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

TABLE OF CONTENTS

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

WELCOME!

Thank you for taking the time and evaluating our latest feature update. FireEye Endpoint Security spent over a year on architecting a new approach to scale your agent and server for rapid feature delivery based upon our investigative findings from our front-line consultants.

TECHNICAL PREVIEW

Technical Previews are an easy way to evaluate Beta-quality features with a meaningful experience, so we can tune the next feature update with your suggestions in mind. Technical Previews is a direct line to our engineering team on what works well, needs to be improved, or enhancements on what would work best for your environment with regards to the feature you are evaluating. Technical Previews gives our engineering team direct to help triage an issue or offer advice on feature enhancements, so our engineering team can immediately work on making the experience better, before it's Generally Available.

Technical Preview features are not a Generally Available solution; therefore, Customer Support can help collect data as needed, but may not be able to dive deeper as these features are still new for them. It is expected that you work with the account team and our FireEye engineering team as you see issues or need to an answer a technical question. Your FireEye account team can provide an introduction to an Endpoint Engineering team lead to better enhance your overall experience.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

INTRODUCING MODULES

Modules are part of our Innovation Architecture, as known as the Rapid Delivery experience. Modules can be loaded into the Endpoint Security Console and those features can be delivered directly to an assigned host set of your choice. New policies will be added and any features with detection capabilities will have their results populate into the existing alert workflow.

Modules gives flexibility to the FireEye Endpoint Security product line, so our Consultants, family of products, and potential partners can add new capabilities to deliver to their audience. It also offers a tailored experience on how you want to define the agent and its security posture within your technical environment. Modules are not tied to each release, rather they are designed to be used on any release of Endpoint Security Consoles v4.9 or higher. There may be cases where a minimum Endpoint Security Console version is required to support a specific module. Minimum version support will be noted in the Modules release note.

IDEAL EXPERIENCE

To better your experience on Technical Previews, our recommendation is to download a virtual console or use a test console, if you have one, and set up Endpoint Security Server v4.8 in your lab. Deploy agents to your test environments. Then load the Modules to understand the workflow and discuss with your team on how a Module should be deployed to your production environment.

You can download a virtual console at no additional cost. Deployed agents do count against your allotment of active nodes. Virtual consoles can run on your local ESX and HyperV infrastructure. Please refer to the FireEye Endpoint datasheet for virtual console requirements.

https://docs.fireeye.com/docs/docs_en/HX/sw/4.8/DG_V/HX_DG_V_4.8_en.pdf

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

ADMIN MODULE

The administration module is the root of how modules will be added over time. It is expected in future builds that this module will be standard on all deployments. However, for this technical preview, **please load the admin module first**, so it enables all subsequent modules to load thereafter. The admin module is used to enable additional modules. It does not offer any additional features.

Note: Please install the Admin Module first, or the additional Modules will not work.

PROCESS TRACKER

Process Tracker collects metadata on unique file executions across your Windows, Mac, and Linux operating systems and streams the data to your Endpoint Security console. The metadata can then be utilized by the Enricher module to detect malicious binaries and the data is accessible on the message bus for your SIEM to retrieve.

Process Tracker has been used by our Consulting teams for well over a year and is fine tuned to look for the following attributes.

1. Is this the first time I have seen this file?
2. Is the file path different from when I last saw this?

If any of the three questions above are true, then Process Tracker will record the file metadata and send the data up as a stream. The data is submitted similar to how acquisitions are submitted, which is archived and sent through our message bus to the Endpoint console.

Process Tracker does not provide any detections or protection capabilities. It is a metadata stream to enhance your investigation efforts. Process Tracker can work independently on its own. It does not require Enricher to be loaded for Process Tracker to stream data.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

After the installation of the Process Tracker feature on the Agent, every process launch will be a new process launch. Therefore, the first 48 hours will see a large stream of metadata entering onto the Endpoint Security Console's message bus. Once that 48 hour period has passed, it is expected that the streams will be much less, since those initial files should not change in path or size. The same logic applies to every agent that has Process Tracker enabled.

It is recommended to enable a few hosts at first, so you can monitor the performance of the endpoint environment and overall bandwidth.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

ENRICHER

Enricher allows MD5 data to be automatically submitted to FireEye's intelligence for verification if a binary launch was malicious or if it's benign. Verification on the file is then added into the message bus. If the binary is malicious, then it is also appends the data into an existing alert. This enrichment of data is how you will use the module.

If FireEye does not have any data about the file, then an additional option to automatically submit the binary to your local AX product for an MVX analysis is available. A binary acquisition is automatically triggered and passed to your MVX. After the MVX analysis is completed, an OS change report is then returned. Data from an OS change report is added to the Endpoint Security message bus. If the file is malicious, a new alert will appear in the Endpoint Security console labeled as PRO. Enricher is also used for additional validation on detections for Malware Protection, MalwareGuard, Exploit Guard, and Real Time Indicators, where those detected binaries can be automatically submitted for further evaluation through the AX product and an OS change report will append to the existing alert.

Enricher will have a local cache of MD5's it has previously collected data on, which means there should not be a resubmission of data. The same local caching logic also applies to your AX, so MVX detonations are not ran for files that share the same MD5.

Enricher can work independently of Process Tracker. Enricher is a server only feature that submits MD5 metadata for additional context on the file and adds it to the message bus and to your alerts. There are no agent features that need to be installed. There is no Enricher policy per host set, like there is for Process Tracker. Enabling Enricher and its sub-configurations will enable it for all hosts.

Similar to Process Tracker in the first 48 hours, Enricher will acquire a lot of binaries. Every binary acquisition Enricher performs will also appear in your acquisition interface. This Technical Preview does not have a filtering function for Enricher only acquisitions. Filtering is expected to come in a future release.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

MODULE INSTALLATION

HOW TO INSTALL THE ADMIN MODULE

Modules require API access at this time. Verify you have API access with the following commands:

Get a Token:

```
$ curl --insecure 'https://localhost:3000/hx/api/v3/token' -X 'GET' -H
'Accept: application/json' -H 'Authorization: Basic
Y2dhcGk6cEBaaaaaaaa=' -I


HTTP/1.1 204 No Content

Date: Fri, 12 Jul 2019 19:45:18 GMT

Server: Apache/2

X-Content-Type-Options: nosniff

Cache-Control: no-cache, no-store, must-revalidate

Pragma: no-cache

Expires: 0

Strict-Transport-Security: max-age=31536000; includeSubDomains

X-FeApi-Token: IM13kYfZg1oznzxGYgGpTsCD7vEAAAAA/53E0evPMmAAAAA=

X-Frame-Options: SameOrigin
```

Use the Token:

```
$ curl --insecure 'https://localhost:3000/hx/api/v3/version' -X 'GET'
-H 'Accept: application/json' -H 'X-FeApi-Token:
IM13kYfZg1oznzxGYgGpTsCD7vEAAAAA/53E0evPMmAAAAA='


{"details":[],"route":"/hx/api/v3/version","data":{"version":"2.15.16"
,"msoVersion":"4.8.0","applianceId":"869AD5A457AA","isUpgraded":true,"
```


© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

intelVersion":"321.101","intelLastUpdateTime":"2019-07-12T19:27:14Z"},"message":"OK"}

Load Your Module:

Load your <module>.cms file into your Endpoint Security Console

NOTE: On the target HX, consider running CLI "show log continuous" to observe module success

NOTE: If you run WINSCP, then it will default to SFTP. Please remember to verify that you are able to SCP to the Endpoint Security Console.

Run an SCP command to the console with the following path:

scp module-admin.cms admin@<ip_address>:/var/home/root

On the Endpoint Security Console, check to see if the module is loaded

```
Jul 12 20:11:58 user1 sshd[79193]: User user1 logged in via ssh2 from 192.168.91.2

Jul 12 20:11:58 user1 scp[79219]: AUDIT: xferlog: user user1: writing file: '/var/home/root/module-admin.cms' --> success

Jul 12 20:11:58 user1 sshd[79193]: ssh secure channel: Received disconnect from 192.168.91.2: 11: disconnected by user

Jul 12 20:11:59 user1 pm[4876]: [pm.NOTICE]: Output from plugin_installer (Plugin Installer) (pid 7329): Verification successful
```


© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

You can also check by querying the API:

https://<ip_address>:3000/hx/api/services/plugin

Example below

```
User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-Sales/Product/HX/Plugins

$ curl --insecure 'https://localhost:3000/hx/api/v3/token' -X 'GET' -H 'Accept: application/json' -H 'Authorization: Basic Y2dhcGk6cEBzc3aaaaa=' -I             HTTP/1.1 204 No Content

Date: Fri, 12 Jul 2019 20:15:25 GMT

Server: Apache/2

X-Content-Type-Options: nosniff

Cache-Control: no-cache, no-store, must-revalidate

Pragma: no-cache

Expires: 0

Strict-Transport-Security: max-age=31536000; includeSubDomains

X-FeApi-Token: IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA=

X-Frame-Options: SameOrigin


User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-Sales/Product/HX/Plugins

$ curl --insecure 'https://localhost:3000/hx/api/services/plugin' -X 'GET' -H 'Accept: application/json' -H 'X-FeApi-Token: IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA='

{"data": [{"config_prefix": "/config/module-admin/1.0.0", "build_date": "2019-06-10T17:24:56", "install_dir": "/data/hx/plugin_manager/data/pluginDoncg", "display_name": "HX Module Administration", "uid": "module-admin_5lNpa", "web_component_uris": {"prod": {"home": {"uri": "/hx/ui/plugins/module-admin_5lNpa/module-
```


© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

admin/1.0.0/prod/pi-management-plugin-bundle.html", "web_component": "pi-management-plugin-home"}, "config": {"uri": "/hx/ui/plugins/module-admin_5lNpa/module-admin/1.0.0/prod/pi-management-plugin-bundle.html", "web_component": "pi-management-plugin-config"}}, "dev": {"home": {"uri": "/hx/ui/plugins/module-admin_5lNpa/module-admin/1.0.0/dev/pi-management-plugin-home.html", "web_component": "pi-management-plugin-home"}, "config": {"uri": "/hx/ui/plugins/module-admin_5lNpa/module-admin/1.0.0/dev/pi-management-plugin-config.html", "web_component": "pi-management-plugin-config"}}}, "contact": "support@fireeye.com", "enabled": false, "components_uri": "/plugin/1/component", "supported_platform": ">=4.1", "name": "module-admin", "disable_uri": "/plugin/1/disable", "source": "git@github1.eng.fireeye.com:HX-Plugins/module-admin.git", "version": "1.0.0", "enable_uri": "/plugin/1/enable", "plugin_uri": "/plugin/1", "versions_uri": "/plugin/version?plugin_name=module-admin", "installed_on": "2019-07-12T20:12:07", "id": 1, "description": "Module Admin is the Admin UI allowing HX Administrators to Install, Unistall, Enable and Disable Modules on an HX instance"}]}

Note the id from the response

To enable the Module, POST on this endpoint

`/hx/api/services/plugin/{id}/enable`

Note: These APIs can only be accessed with a header token that can be obtained from hx/api/v3/token

/hx/api/services/plugin/{id}/enable

Note: These APIs can only be accessed with a header token that can be obtained from hx/api/v3/token

Sample:

```
User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-Sales/Product/HX/Plugins

$ curl --insecure 'https://localhost:3000/hx/api/services/plugin/1/enable' -X 'POST' -H
```


© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

```
'Accept: application/json' -H 'X-FeApi-Token:
IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA='

{}
```

Verify by browsing to:

https://localhost:3000/hx/#/plugin/module-admin

Once the CMS file is copied, the Module will auto-install and your console user interface will have a new menu item listed as **PLUGINS.**

HOW TO INSTALL THE PROCESS TRACKER MODULE

Follow the same steps in the Admin Module but using the Process Tracker file.

scp process-tracker_1.0.0.cms admin@<ip_address>:/var/home/root

Sample Log:

```
Jul 12 20:21:47 user1 pm[4876]: [pm.NOTICE]: Output from
plugin_installer (Plugin Installer) (pid 7329): Verification
successful
```

Once the CMS file is copied, the Module will auto-install and your console user interface will have a new menu item listed as **PLUGINS.** Process Tracker can be activated through the Module drop down. Process Tracker will also appear as a policy to assign your host set. There is only one setting in the policy at this time.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

HOW TO INSTALL THE ENRICHER MODULE

Follow the same steps in the Admin Module but using the Enricher file.

scp enricher_1.0.0.cms admin@<ip_address>:/var/home/root

Sample Log:

```
Jul 12 20:23:47 user1 pm[4876]: [pm.NOTICE]: Output from
plugin_installer (Plugin Installer) (pid 7329): Verification
successful
```

Once the CMS file is copied, the Module will auto-install and your console user interface will have a new menu item listed as **PLUGINS.** Enricher will be configurable through the Module drop down.

To assign your local AX, please create an AX API account.

Please note the following

Username: AX API username

Password: AX API password

URL: https://<AX ip address>:443

Enricher does not work with VX or CloudMVX at this time. VX support is intended to be available in the next Enricher update. CloudMVX support is intended to come later in the year.

As stated before, enabling Enricher activates this for all your hosts data on the Endpoint Security Console. There is no granular policy for Enricher. If you believe there should be one, please let us know.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019

SUPPORT

IMPORTANT: FEEDBACK NEEDED

Technical Previews are your chance to shape this feature moving forward. FireEye Endpoint Security expects the Market Place experience to be better over time, so you do not need to install through SCP. However, all workflows suggestions and feature enhancements are welcomed. Please list out the good and the bad, so we can continue to better the overall approach before it becomes Generally Available.

The direct line to our engineering team can be contacted below:

EndpointTechPreview@fireeye.com

NOTE: Please CC your sales account team as well.

SUPPORTABILITY

Customer Support has been notified to pass any comments or issues to the FireEye Endpoint Security Engineering team. They can assist in collecting data as needed, but they are not expected to provide a deeper level of support. Your support path on Process Tracker and Enricher will be on the Endpoint Technical Preview email and account team above.

UPGRADES

Upgrades are not supported for this first iteration of the Admin Module, Process Tracker, and Enricher. A rip and replacement maybe needed. The existing data should remain in-tact. FireEye Endpoint Engineering will work with you on expectations and how to better the upgrade experience.

Thank you again for evaluating our latest feature developments.

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WRD.EN-US.032019