ENDPOINT SECURITY

ENDPOINT ENRICHER

MODULE USER GUIDE

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 Enricher Module

Software Release 1.4.3

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

Contents

PART I: Module Overview

The Enricher module adds FireEye Intelligence information to the information about the file or event that is displayed in the Endpoint Security Web UI to help determine when a file is malicious and aid in incident response investigations.

You can use the Enricher module to gain additional context about alerts in your environment. Enrichment provides an automated workflow that collects and analyzes artifacts, which reduces the time it takes to prioritize malicious activity in your enterprise.

The two basic functions of the Enricher module are:

- Submitting data to FireEye intelligence for verification
- Submitting data to additional data sources for verification:
    - FireEye Malware Analysis (AX)
    - Local MVX
    - Detection on Demand

NOTE: You must have an on-premises AX or VX Series appliance for the Enricher module to be able to submit data to FireEye Malware Analysis / Local MVX. You must have an active Detection on Demand subscription to submit data to Detection on Demand.

The Enricher module submits MD5 data to FireEye's intelligence for verification and the verification information is then added into the message bus. If the file is malicious, then the data is appended to an existing alert.

If FireEye does not have any data about the file, you can choose to automatically submit the file to your on-premises FireEye Malware Analysis or FireEye Local MVX product for MVX analysis or to your Detection on Demand subscription. A file acquisition is automatically triggered and submitted for analysis. After analysis is complete, an OS change report is generated and the data from this report is added to the Endpoint Security message bus.

The Enricher module also provides additional detection validation for Malware Protection, MalwareGuard, Exploit Guard, and Real-Time Indicators, where files detected by those features can be automatically submitted to the FireEye Malware Analysis product and any other configured submission service.

To reduce data resubmission, the Enricher module includes a local cache of MD5s about which it has previously collected data. If the MD5 is currently in the local cache, files with that MD5 will not be run through your additionally configured submission options (Malware Analysis or Detection on Demand). The local cache ages MD5s out after 30 days.

The Enricher module is a server-only feature and does not require any Agent functionality to be installed. Unlike some modules, the Enricher module does not have a host set policy component. When you enable the Enricher module, it is enabled for all hosts.

NOTE: If you are using the Enricher module in conjunction with the Process Tracker module, the Enricher module acquires many files during the first 48 hours after you enable Process

Tracker. Each acquisition Enricher performs also appears in your list of acquisitions on the Acquisitions page.

Prerequisites

This general availability release of Endpoint Enricher is supported on **Endpoint Security 5.0.2**.

Note: Endpoint Enricher 1.4.3 **will NOT work** on Endpoint Security 5.0 or lower. This is not a supported scenario.

PART II: Configuring Endpoint Enricher Module

You can enable, disable, and configure settings for the Enricher module, including the data source and feed setting, the logging level, and the aging settings directly in the Endpoint Security Web UI.

This section covers the following topics:

- Enabling the Enricher Module
- Disabling the Enricher Module
- Configuring the Data Source and Feed
- Configuring the Enricher Module Logging Level
- Configuring the Enricher Module Aging Setting

Enabling the Endpoint Enricher Module

You can enable the Enricher module from the Modules page in the Endpoint Security Web UI.

To enable the Enricher 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.
    - On the **Modules** page, locate the **Enricher** module and click the **Actions** icon () and select **Enable** to enable the module

Disabling the Endpoint Enricher Module

You can disable the Enricher module from the Modules page in the Endpoint Security Web UI.

To disable the Enricher 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.

- On the **Modules** page, locate the **Enricher** module and click the **Actions** icon () and select **Disable** to enable the module

Enricher over Proxy

Context API and Detection on Demand data sources will use any web proxy settings that are configured via Endpoint Security Policy Settings. No additional settings are required for Context API and Detection on Demand enrichment to utilize the web proxy settings.

Note: Malware Analysis and Local MVX data sources do not utilize the web proxy for enrichment requests. Please ensure that your network is configured to allow your Endpoint Security server to make requests to your AX or VX appliance.

Configuring additional Data Sources

To configure additional Enricher module data sources:

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 **Enricher** module, click the **Actions** icon ( ), and select **Configure** to access the **Enricher Module Settings** page.
4. From the **Data Sources & Feed** tab, click **Multi-Vector Virtual Execution (MVX).** By default, additional data sources are disabled

    Malware Analysis setup:

    1. Enter a username, password and URL for the data source (such as: https://{IP_or_domain_name}:{port}) in the provided fields.
    2. If you want to limit the number of concurrent file submissions to MVX, select the checkbox and enter the maximum number of files.

    Note: For customers concerned about their AX performance, the concurrent submission limit will prevent enricher from adding high volumes of traffic to AX. However, if enricher is unable to complete within 6 hours, the submission will timeout. To help prevent enricher timeouts, customers can remove the concurrent submission limit and/or increase the enricher timeout option in the configuration API, which defaults to 6 hours (21600 seconds).

    Local MVX setup:

    1. Enter a username, password and URL for the data source (such as: https://{IP_or_domain_name}:{port}) in the provided fields.

a. The IP or Domain name should be the IP or Domain Name of your VX appliance.

b. Port will be 443

2. If you want to limit the number of concurrent file submissions to MVX, select the checkbox and enter the maximum number of files.

Detection on Demand setup:

1. Enter an API Key and in the provided field. The default URL should not need to be changed.

5. Click **Save Settings**.
6. **Test Connection**. You MUST save your settings before attempting to use the Test Connection button. The test connection button will verify that your login and URL information is correct and data can be submitted to your additional data source.

NOTE: The connection will automatically test on save.

Configuring the Enricher Module Logging Level

To configure the Enricher module logging level:

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 **Enricher** module, click the **Actions** icon ( ), and select **Configure** to access the **Enricher Module Settings** page.

4. On the **Enricher Module Settings** page, click the **Logging** tab and select the logging level for the Enricher module. The table below describes each logging level. *Notice* is the default logging level.

Logging Level	Description
Emergency	Logs system failure messages that identify total system failures on the host endpoint. These system failures usually cause the agent to stop functioning.

Logging Level	Description
Alert	Logs messages that identify crucial conditions on the host endpoint that require immediate remediation, such as a corrupted system database.
Critical	Logs critical messages that identify serious conditions on the host endpoint, such as hard drive errors.
Error	Logs error messages that identify program errors on the host endpoint, such as when a file cannot be found.
Warning	Logs warning messages that identify non-critical and correctable errors on the host endpoint, such as a specified value that is too large.
Notice	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.
Info	Logs Informational messages about regular system processing.
Debug	Logs debugging messages. This logging level is normally used when debugging a program only. It includes all the types of logging messages.

Configuring the Enricher Module Aging Settings

You can use the Endpoint Security Web UI to define how long enrichment data should be kept on the system before the data is deleted.

To configure the aging settings for the Enricher 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 **Enricher** module, click the **Actions** icon (), and select Configure to access the **Enricher Module Settings** tab.

4. On the **Enricher Module Settings** page, select **Aging Settings** tab.

5. In the **Delete files after** field, enter the number of days the enrichment files should remain on the system before it is deleted. The default period is 30 days.

6. In the **Delete database entries after** field, enter the number of days the enrichment data should remain on the system before it is deleted. The default period is 30 days.

7. Click **Save Settings.**

PART III: Viewing Enrichment Results

You can use the Enrichment Results page in the Enricher module to view the results of the enrichment process.

To view the enrichment results:

1. Log in to the Endpoint Security Web UI.

2. From the **Modules** menu, select **Enricher** to access the **Enrichment Results** page.

3. If Detection on Demand is your source of Enrichment, you can view FireEye's Detection on Demand report by clicking the View Report link in the "Alert URLs" column off the enricher grid.

The table below explains the information you can view on the Enrichment Results page, and indicates which columns are displayed by default.

Column Name	Description	Displayed By Default
MD5	The MD5 hash of the file.	Yes
Status	The status of the enrichment request. Possible values are: • Requested--Queued for Enricher • Pending--Picked up and processing • Complete--Context API is complete without a detection conclusion • Benign--Benign conclusion • Malicious--Malicious conclusion • Whitelisted--Whitelisted file	Yes

Column Name	Description	Displayed By Default
Created	The date and time that the enrichment request was submitted.	Yes
SHA256	The SHA256 hash of the file.	Yes
SHA1	The SHA1 hash of the file.	Yes
Size	The file size of the file.	Yes
MVX Verdict	The verdict received from MVX. Possible values are: • Benign • Malicious • Indeterminate--MVX does not have an opinion on the file sample	Yes
FireEye Verdict	The detection conclusion returned from the context API. Possible values are: • Benign • Malicious • Indeterminate--the context API does not have an opinion on the file sample	Yes
FireEye Analysis Conclusion	The analysis conclusion from the context API.	Yes
Threat Names	The CSV list of malware names received from MVX.	Yes
Risk Level	The level of risk returned from the context API.	Yes
Type	The type returned from the context API.	Yes
Mime Type	The label for the type of Multipurpose Internet Mail Extension returned from the context API.	Yes
Alert URLs	The CSV list of the URLs to the alerts generated by MVX.	Yes
First Seen by FireEye	The date and time when the file was first encountered as reported by the context API.	Yes
Last Seen by FireEye	The date and time when the file was most recently encountered as reported by the context API.	Yes
Count	The number of times the file has been encountered as reported by the context API.	Yes
Labels	The CSV list of labels returned from the context API that are associated with the file.	Yes
Risk Summary	The risk summary returned from the context API for the file.	Yes

Column Name	Description	Displayed By Default
MVX Severity	The level of severity for the file as determined by MVX. Possible values are Critical, Major, and Low or Minor.	No
MVX Malicious Class Type	The class or type of malicious file to which the file belongs.	No
MVX Malicious Message	The malicious alert message returned from MVX.	No
MVX Type	Show who provided Enrichment, AX, VX or DoD	No
FireEye Description	The description returned from the context API.	No
FireEye Kill Chain Phases	The CSV list of kill chain phases returned from the context API.	No
Network Traffic Source Address	The source address of the network traffic returned from the context API.	No
Network Traffic Destination Address	The destination address of the network traffic returned from the context API.	No
Network Traffic Source Domains	The CSV list of network traffic source domains returned from the context API.	No
Network Traffic Destination Domains	The CSV list of network traffic destination domains returned from the context API.	No
Threat Actors	The CSV list of threat actors returned from the context API.	No
Threat Labels	The CSV list of threat labels returned from the context API.	No
Vendors	The CSV list of AV vendors returned from the context API.	No
Total Vendor Scanned	The total number of AV vendors scanned returned from the context API.	No
Total Vendor Malicious	The total number of AV vendors reporting the file sample as malicious returned from the context API.	No
Vendor Confidence	The maximum AV vendor confidence returned from the context API.	No

Technical Support

For technical support, contact FireEye through the Support portal:

https://csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required):

https://docs.fireeye.com/