



ENDPOINT SECURITY

AMSI v1.1.0

MODULE USER GUIDE

TECHNICAL PREVIEW 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.

Copyright © 2021 FireEye, Inc. All rights reserved.

Endpoint Security Agent - AMSI Module User Guide

Software Release v1.1.0

Revision 1.2

FireEye Contact Information:

Website: www.fireeye.com

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

Phone (US):

1.408.321.6300

1.877.FIREEYE

CONTENTS

MODULE OVERVIEW	4
PART I: INSTALLING AMSI MODULE	5
INSTALLING THE AMSI AGENT MODULE	5
PART II: UNINSTALLING AMSI MODULE	6
UNINSTALLING THE AMSI AGENT MODULE.....	6
PART III: CONFIGURING AMSI MODULE	7
CONFIGURING AMSI AGENT POLICY	7
CONFIGURING AMSI SERVER SETTINGS	9
CONFIGURATION API.....	10
PART IV: ALERTS	12
Hosts (ALERT DETAILS).....	12
APPENDIX A: FREQUENTLY ASKED QUESTIONS.....	14
HOW TO VERIFY IF THE AMSI INSTALLATION SUCCEEDED?	14
ARE THERE ANY LOG FILES CREATED DURING INSTALLATION ON THE ENDPOINT AGENTS?	14
IS THERE A LOG ON THE HX APPLIANCE FOR THE AMSI SERVER MODULE?	15
WHAT ARE THE PROCESSES CREATED WHEN AMSI MODULE IS INSTALLED AND ENABLED?	15
WHAT IS YARA?	15
WHY AMSI IS NOT BLOCKING THE SCRIPT EXECUTION?	15
CAN AMSI MODULE FUNCTION WHEN MULTIPLE AMSI PROVIDERS FROM DIFFERENT AV VENDORS ARE REGISTERED?	15
WHY IS FIREEYE AMSI PROVIDER NOT LOADING IN POWERSHELL OR ANY OF THE SUPPORTED SCRIPTING ENGINES?	16
WHERE DOES AMSI CONTENT COME FROM? CAN I MODIFY EXISTING OR ADD MY OWN RULE?	16
WHAT IS THE SIZE OF THE INITIAL AMSI CONTENT?	16
WHY AMSI MODULE DOES NOT GENERATE MULTIPLE ALERTS IF I RUN POWERSHELL SCRIPT (FILE ON DISK) IN A LOOP?.....	16
DEPENDENCIES / LIMITATIONS / KNOWN ISSUES.....	17

Module Overview

The AMSI module for FireEye Endpoint Security monitors and detects suspicious scripts utilizing the AMSI interface on Windows OS.

AMSI module detects the execution of malicious scripts using AMSI interface to send script objects for additional FireEye Endpoint Security scan. An event with detection metadata is sent to Endpoint Security (HX) controller which will be viewable in *Alerts* page.

Prerequisites

This release of AMSI module is supported on **Endpoint Security 5.0.4** with **agent 32** running on **Windows 10, Server 2016 and above**. The Module is supported only on the Windows platform. Please review Appendix A for more details on dependencies, limitations and known issues in the current release.

Note: It is not recommended to install AMSI Module v1.1.0 on Endpoint Security 5.0.3 (and lower) with agent 31 or lower. This is not a supported scenario.

PART I: Installing AMSI Module

AMSI is an (non-core) optional module available for **Endpoint Security 5.0.4** with **agent 32**. It is installed using Endpoint Security Web UI by downloading the module installer package (.cms file) from the FireEye Market and then uploading the module .cms file to your Endpoint Security Web UI. The module is disabled by default. Refer to *Part IV: Configuring the AMSI Module* for steps to enable the server module. After the module is installed successfully, it appears on the Modules menu tab.

For detailed steps on server module installation or upgrade refer to **Chapter 31: Using Modules** in [FireEye Endpoint Security Server User Guide](#).

Installing the AMSI Agent Module

The **AMSI** module consists of a **server module** and an **agent module**. The above section provides steps to upload the AMSI module to the HX server. To install the **agent module** on a given host set:

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 assigned to the host set you want to deploy AMSI to, and select **Edit Policy**.
4. Click on the **Categories** button in the **Edit Policy** page and select **AMSI – <version number>** (e.g., AMSI – 1.1.0) and click **Apply**.
5. On the **Edit Policy** page, click **Save**.

The above steps will inform the endpoints (local systems) to download the agent module and install it during configuration update. Please review *Part IV: Configuring the AMSI Module* section below to understand various policy options.

PART II: Uninstalling AMSI Module

To uninstall the AMSI module from Endpoint Security Web UI:

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 **AMSI** module and click the Actions icon (the gear icon) and select *Uninstall* to uninstall the module. A confirmation window appears before uninstallation can proceed. Click *Uninstall* to start the uninstallation of the module.

A message at the top of the page tells you that module uninstallation succeeded.

The **AMSI** module consists of a **server module** and an **agent module**. Uninstalling the **AMSI** module removes AMSI policy settings from all policies and ensures that **server module** is removed from Management Server and the **agent modules** are removed from endpoints (Hosts/Client systems).

Uninstalling the AMSI Agent Module

The **AMSI** module consists of a **server module** and an **agent module**. The above section provides steps to uninstall the AMSI module completely from the HX server and managed FireEye endpoints. To remove only the **agent module** for a given host set:

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 assigned to the agent on which you want to remove the **AMSI**, and select **Edit Policy**.
4. Click on the **Categories** button in the **Edit Policy** page and unselect **AMSI- <version number>** (e.g., AMSI – 1.1.0) and click **Apply**.
5. On the **Edit Policy** page, click **Save**.

PART III: Configuring AMSI Module

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

- The **agent module** is installed and enabled on agents using the AMSI policy.
- Once the **server module** is enabled, disabling the **server module** will **disable** the **agent module** in **all the policies**.
- Uninstalling the **AMSI** module removes AMSI policy settings from all policies and ensures that both **server module** and the **agent module** are removed from endpoints (Hosts/Client systems).

For detailed steps on server module configuration refer to **Chapter 31: Using Modules** in [FireEye Endpoint Security Server User Guide](#).

Configuring AMSI Agent Policy

This section describes the various configuration settings provided in the AMSI policy.

Enabling the AMSI Agent Module

To enable AMSI on a given host set, toggle the **Enable AMSI on the host** to **ON** and save the policy changes. Upon configuration update on the agent, AMSI module will be enabled on the endpoint.

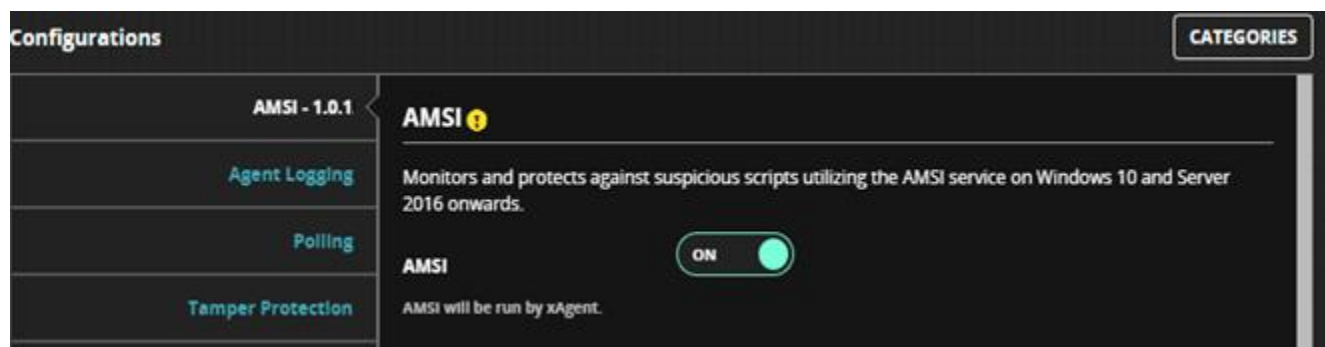


Figure 1 - AMSI module Policy Settings

Rule Updates

AMSI module uses YARA rules to detect suspicious script execution. These rules are made available as a part of FireEye DTI content and downloaded to HX controller at regular intervals. This policy option enables endpoints to poll for latest content and download at configured intervals.

Rule Updates

Update rules every:

Hours

1

:

Minutes

0

:

Seconds

0

Figure 2 – AMSI Rule Updates Interval Policy Settings

Agent Database

AMSI module stores scan data in an encrypted SQLite database on the endpoint. This value can be tuned based on the needs. Lower database size leads to compact size but will have less historical data and vice versa.

Agent Database

Maximum Database Size

100

MB

Figure 3 – AMSI Agent Database Policy Settings

Alerting

AMSI module generates alerts when any of the scripts match rule(s). To provide better control over the kind of alerts, a confidence threshold is introduced as a policy. Confidence threshold provides the ability to suppress alerts based on triggered rule’s confidence level. For example, setting this to “**High**” will only alert on rules with a high confidence and setting this to “**Low**” will alert on everything.

The alert includes a part of the suspicious script for quick analysis. The size of the context data can be controlled via the policy option shown below.

Alerting

Confidence Threshold for Alerting

High

Context data size

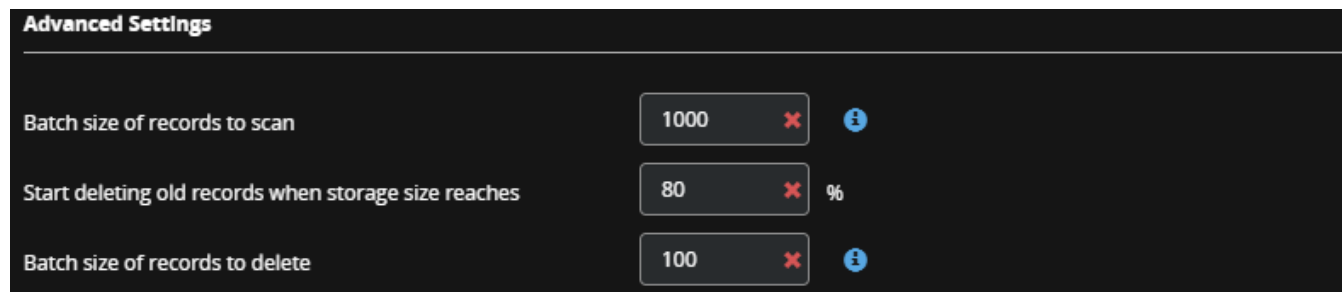
1

KB

Figure 4 – AMSI Confidence Threshold Policy Settings

Advanced Settings

AMSI module provides several advanced settings that can be used to tune the performance and disk IO operations. Default values should address most of the scenarios. However, make sure to validate that you get the desired outcome if you plan to modify.








Advanced Settings		
Batch size of records to scan	1000	 
Start deleting old records when storage size reaches	80	 %
Batch size of records to delete	100	 

Figure 5 – AMSI Agent Additional Policy Settings

Configuring AMSI Server settings

This section describes the various configuration settings provided in the AMSI module Server.

To access the AMSI 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 **AMSI** 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 an **AMSI Settings** page.

Logging Settings

The below server config setting provides to ability to set the log level for AMSI server module.

Logging Levels Settings

Set configurations for the log levels (i.e. amount of logging data) to determine the type of messages that are logged. Log levels are listed below in order by logging level (with Emergency included in each selection)

- ☐ **Emergency:** System failure messages identifying total system failures that usually cause the agent to stop functioning.
- ☐ **Alert:** Messages identifying crucial conditions that should be corrected immediately, such as a corrupted system database.
- ☐ **Critical:** Critical messages identifying serious conditions, such as hard device errors.
- ☐ **Error:** Error messages identifying program errors, such as when a file cannot be found.
- ☐ **Warning:** Warning messages identifying non-critical, correctable errors, such as a specified value that is too large.
- ☒ **Notice:** Notification messages identifying minor problems that do not inhibit regular agent functioning and for which defaults are used until the problem is resolved.
- ☐ **Info:** Informational messages about regular system processing.
- ☐ **Debug:** Debugging messages, normally used only when debugging a program - this includes all the types of logging messages.

Figure 6 – AMSI Module Server Logging 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 the Endpoint Security Server API, please refer to FireEye document Endpoint Security REST API Guide Release 5.0.

Get Configuration

Calling this API route will return the current configuration tree for the AMSI module.

Request

HTTP Verb	Route	Parameters
GET	hx/api/services/config/tree	?node_name=/config/amsi

Response

Key	Value
-----	-------

Data	List of configuration properties. Each property has the following attributes: <ul style="list-style-type: none"> 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
-------------	--

Configuration Options

Property	Route	Data Type
Logging Level	/config/amsi/logging/level	Type: string Default: notice

Update Configuration

As well as using the UI, you can also use the API to update the AMSI module's **server** configuration settings by leveraging similar routes.

Request route

HTTP Verb	Route	Parameters
PUT	hx/api/services/config/tree	?node_name=/config/amsi

Request Headers

Header Property	Value
Content-Type	application/json
X-FeApi-Token	{{ random token string }}

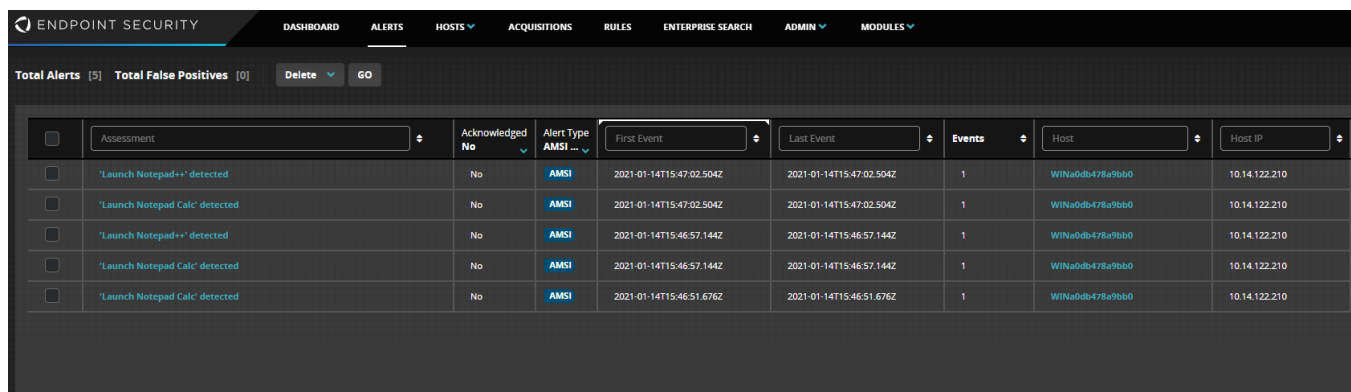
Request Body

The request body will contain a JSON object with a "data" property containing an array of JSON objects for each configuration setting to update. Below is an example for updating the **logging level** setting to "info":

```
{
  "data": [
    {
      "default_value": "notice",
      "name": "/config/amsi/logging/level",
      "type": "string",
      "value": "info"
    }
  ]
}
```

PART IV: Alerts

Alerts from AMSI Module shows up on the Alerts page of the Endpoint Security Web UI with the Alert Type as **AMSI**.



The screenshot shows the 'Alerts' page in the Endpoint Security Web UI. The top navigation bar includes 'DASHBOARD', 'ALERTS', 'HOSTS', 'ACQUISITIONS', 'RULES', 'ENTERPRISE SEARCH', 'ADMIN', and 'MODULES'. Below the navigation bar, there are filters for 'Total Alerts [5]' and 'Total False Positives [0]', along with 'Delete' and 'GO' buttons. The main table displays a list of alerts with columns for checkboxes, Assessment, Acknowledged No, Alert Type (AMSI), First Event, Last Event, Events, Host, and Host IP. The alerts are for 'Launch Notepad++ detected' and 'Launch Notepad Calc detected'.

	Assessment	Acknowledged No	Alert Type AMSI	First Event	Last Event	Events	Host	Host IP
<input type="checkbox"/>	'Launch Notepad++' detected	No	AMSI	2021-01-14T15:47:02.504Z	2021-01-14T15:47:02.504Z	1	WINa0db478a9bb0	10.14.122.210
<input type="checkbox"/>	'Launch Notepad Calc' detected	No	AMSI	2021-01-14T15:47:02.504Z	2021-01-14T15:47:02.504Z	1	WINa0db478a9bb0	10.14.122.210
<input type="checkbox"/>	'Launch Notepad++' detected	No	AMSI	2021-01-14T15:46:57.144Z	2021-01-14T15:46:57.144Z	1	WINa0db478a9bb0	10.14.122.210
<input type="checkbox"/>	'Launch Notepad Calc' detected	No	AMSI	2021-01-14T15:46:57.144Z	2021-01-14T15:46:57.144Z	1	WINa0db478a9bb0	10.14.122.210
<input type="checkbox"/>	'Launch Notepad Calc' detected	No	AMSI	2021-01-14T15:46:51.676Z	2021-01-14T15:46:51.676Z	1	WINa0db478a9bb0	10.14.122.210

Figure 7 – Sample of AMSI alert on the Alerts page

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

Hosts (Alert Details)

Upon selecting an AMSI alert from Alerts page, details of the alerts are shown on the Hosts page of the Endpoint Security Web UI.

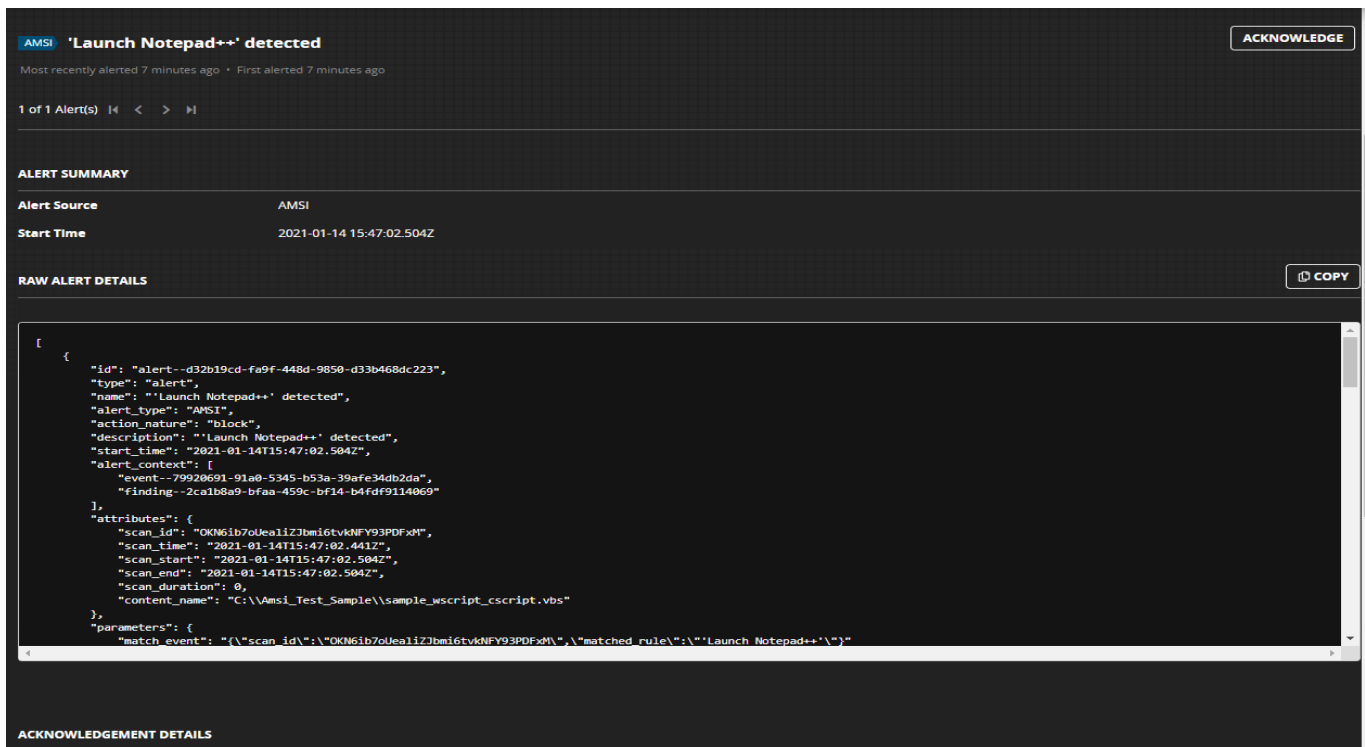


Figure 8 – Sample of AMSI alert on the Hosts page

Current version of HX server provides a raw view of the alert details in JSON format and here are some of the notable alert fields that AMSI module generates.

Alert Fields	Description
Event_at	Script execution time as reported by AMSI interface.
Content_name	Represents the script name if the file is on the disk. This field can also be used to recognize when a DotNet assembly gets dynamically loaded.
matched rule	Matched rule Json object containing rule name and additional meta data such as <i>MetaData</i> and <i>MatchedStrings</i> that would help analyze the detection.
Intel_version	Version of the overall intel package which includes AMSI rules.
Rules_version	AMSI rules package version
Amsi_data	Part of the scanned data resulted in detection.
Arguments	Command line arguments passed to the source process.
Attributes	Scan meta data
Account_name	User account under which the scripting engine ran.

Note: Raw JSON data will be formatted and displayed using proper UI widgets in upcoming HX releases.

APPENDIX A: Frequently Asked Questions

How to verify if the AMSI installation succeeded?

Once the AMSI Module is installed and enabled, check for the existence of module files under *C:\ProgramData\FireEye\xagt\exts\amsi\sandbox*, *C:\Windows\FireEye* and *C:\ProgramData\FireEye\xagt\exts\plugin\amsi*

The working status of the plug-in can be verified on the HX server via API to review the system information (Sysinfo) received from the endpoint agent. You should see the following fields in Sysinfo JSON data.

```
"AmsiStatus": "running",
  "Amsi": {
    "version": "1.1.0",
    "plugin-supported": "true",
    "provider-registered": "true",
    "intel-version": "464-lb.101",
    "rules-version": "2021.01.20",
    "intel-timestamp": "2021-02-17T19:04:16Z",
    "intel-received-timestamp": "2021-03-02T16:00:48Z",
    ...
  }
```

Field Name	Description
plugin-supported	AMSI is only supported on Windows 10 or Windows 2016 and above. When this is set to 'false' the OS does not support AMSI feature.
provider-registered	Indicates whether FireEye AMSI module is registered with Windows OS.
Intel-version	Overall Intel version as seen in HX controller.
Rules-version	AMSI rules version (sub package under overall Intel package)
Intel-timestamp	Intel timestamp as seen in HX controller.
Intel-received-timestamp	Intel timestamp when the endpoint receives AMSI rules.

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

AMSI **agent module** creates log files under *c:\Windows\Temp*. Depending on the scenario, the following files get created:

- *amsi_install.log*
- *amsi_uninstall.log*
- *amsi_preupgrade.log*
- *amsi_upgrade.log*

We can also refer to agent logs to find out if there are any installer messages related to plug-in installation.

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

You can find the log file under `/var/log/supervisord/amsi-server_<version>_<unique_id>.log`

What are the processes created when AMSI Module is installed and enabled?

After installation, AMSI Module spawns an instance of `xagt.exe` with AMSI in its command line. This is a container application to interact with agent services. This process runs under the System account like any other agent instance. AMSI module registers `FeAmsiProvider.dll` as a FireEye AMSI provider with Windows® OS. Along with `FeAmsiProvider.dll`, additional FireEye libraries such as `AmsiProxy.dll` and other necessary runtime libraries will be loaded into PowerShell® and other scripting processes (engines) that support AMSI.

What is YARA?

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description or rule consists of a set of strings and a Boolean expression which determines its logic. Refer <https://virustotal.github.io/yara/> for further details. The AMSI module uses the YARA engine for scanning the scripts.

Why AMSI is not blocking the script execution?

The AMSI module supports **detection mode only** in technical preview release. You may be able to get alert if the AMSI module detects malicious activities and the policy is configured to report them. Note that AMSI relies on content to detect malicious activities. Make sure that AMSI is initialized and has content successfully downloaded. This information is available in `agentInfo` (aka `sysInfo`) audit.

Can AMSI module function when multiple AMSI providers from different AV vendors are registered?

The AMSI module can detect malicious scripts if it gets invoked by the scripting engine. Internal testing on various latest Windows® 10 releases lead us to believe that it works fine. However, this behavior is controlled by Microsoft® AMSI framework. With multiple AMSI providers, the order in which the providers are invoked by the AMSI framework decides which provider gets to scan the script first. If any of the earlier AMSI provider convicts a script as malicious, other scripts may not get a chance to scan it.

Why is FireEye AMSI provider not loading in PowerShell or any of the supported scripting engines?

When FireEye Endpoint Security is installed side-by-side with other competing security solutions, you may see this behavior. You may have to work with the other security products to trust or exclude FireEye binaries so that they can co-exist.

Where does AMSI content come from? Can I modify existing or add my own rule?

FireEye Endpoint Security team releases AMSI content via DTI on regular cadence. AMSI content is released as a part of overall intel content package. All the Endpoint Security appliances/cloud instances download content from DTI. Endpoint agents receive this content at a regular polling interval as configured in the AMSI policy. The current release does not provide any ways to modify the content or create new custom rules. These may be included in future releases.

What is the size of the initial AMSI content?

AMSI content is based on YARA rules, and these are simple JSON formatted text files. As of this release, each rule is around 1KB on average. The overall content size depends upon the number of rules we release to DTI which may be a few hundred rules in initial release and may fluctuate over time.

Why AMSI module does not generate multiple alerts if I run PowerShell script (file on disk) in a loop?

Based on research and testing, it is found that scripting engines implement some form of performance optimization techniques and avoid scanning script contents repeatedly. In the case of PowerShell, it is observed that unless the script file on the disk gets modified or a new instance of PowerShell is invoked, AMSI module gets to scan the content of the file only once.

Please refer to the Dependencies/Limitations/Known Issues section for additional reasons, if any.

Dependencies / Limitations / Known Issues

- This technical preview release of AMSI is supported on Endpoint Security 5.0.4 with agent 32 **(GA)** running on Windows 10/Server 2016 and above only.
- Windows 8.x and Windows Server 2012 and below, Mac OS and Linux platforms are **not** supported.
- It is not possible to mark an alert as false positive.
- The AMSI module cannot detect script execution if they run before the AMSI module is initialized and running.

Please refer to release notes for a list of known issues in the current release