



ENDPOINT SECURITY

PROCESS GUARD v1.3.1

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 © 2020 FireEye, Inc. All rights reserved.

Endpoint Security Agent - Process Guard Module User Guide

Software Release v1.3.1

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.....	3
PART I: MODULE OVERVIEW	4
PREREQUISITES	4
PART II: INSTALLING PROCESS GUARD MODULE	5
DOWNLOADING THE INSTALLER PACKAGE	5
UPLOADING THE INSTALLER PACKAGE	6
INSTALLING THE PROCESS GUARD AGENT MODULE.....	6
PART III: UNINSTALLING PROCESS GUARD MODULE	7
UNINSTALLING THE PROCESS GUARD AGENT MODULE	7
PART IV: CONFIGURING PROCESS GUARD MODULE.....	8
ENABLING THE PROCESS GUARD MODULE	8
DISABLING THE PROCESS GUARD MODULE	9
CONFIGURING PROCESS GUARD AGENT POLICY.....	10
PART V: PROCESS GUARD MODULE HOME PAGE	12
APPENDIX A: FREQUENTLY ASKED QUESTIONS.....	13
HOW TO VERIFY IF THE PROCESS GUARD INSTALLATION SUCCEEDED?	13
ARE THERE ANY LOG FILES CREATED DURING INSTALLATION ON THE ENDPOINT AGENTS?	13
IS THERE A LOG ON THE HX APPLIANCE FOR THE PROCESS GUARD SERVER MODULE?	13
WHAT ARE THE PROCESSES CREATED WHEN PROCESS GUARD MODULE IS INSTALLED AND ENABLED?	13
WHY DOESN'T THE EXCLUSIONS IN PROCESS GUARD POLICY WORK?	14
DEPENDENCIES / LIMITATIONS / KNOWN ISSUES.....	14

PART I: Module Overview

The Process Guard Module for FireEye Endpoint Security prevents attackers from obtaining access to credential data or key material stored within the lsass.exe process, thus protecting endpoints against common credential theft attacks.

Process Guard will take action to prevent the request if a process requests access to critical processes with credential data. An event is generated when a process requests access to this data and it is viewable in the Process Guard module home page on Endpoint Security (HX) controller. This page will help admins to analyze and troubleshoot any potential compatibility issues. By default, Process Guard will block all processes from accessing credential data and all the events are available in the events table under the Process Guard home page.

Process Guard provides a whitelisting feature that allows admins to bypass the preventative actions of Process Guard by specifying a full process path as excluded process. This alleviates any issues with incompatible legitimate applications that require full system access to perform normal operations.

Prerequisites

This technical preview release of Process Guard v1.3.0 is supported on **Endpoint Security 5.0.0** with **xAgent 32.0.0** running on **Windows 7/Server 2012 and above**. The Module is supported only on the Windows platform and for more details on dependencies, limitations and known issues for the current release please review Appendix A.

Note: It is not recommended to install Process Guard v1.3.0 on Endpoint Security 4.9.x with xAgent 31 or lower. This is not a supported scenario.

PART II: Installing Process Guard Module

Process Guard is an (non-core) optional module available for **Endpoint Security 5.0.0** with **xAgent 32.0.0**. 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: Enabling the Process Guard Module* for steps to enable the server module. After the module is installed successfully, it appears on the Modules menu tab.

Downloading the Installer Package

To download the module installer package:

1. Log in to the Endpoint Security Web UI with your administrator credentials.
2. From the **Modules** menu, select **HX Module Administration** to access the **Modules** page.
3. On the **Modules** page, click **Find Modules** to access the FireEye Market. The FireEye Market opens in a new browser tab.
4. In the **Types** filter list on the FireEye Market, select **Endpoint Security Modules**.
5. In the Search Results, click the **Process Guard** module
6. On the **Process Guard Module** FireEye Market page, click on **Download** button to download the module .cms file to your local drive.

Be sure to note the navigation path to the directory where you downloaded the .cms file.

Uploading the Installer Package

To upload the Process Guard module installer package to your 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, click **Upload Modules** to upload the module .cms file from your local drive to the Endpoint Security Console. The .cms file includes **server module** and an **agent module** of Process Guard Module.
4. In the **Upload Module** dialog box, click **Select File**.
5. Navigate to the downloaded module .cms file, select the .cms file, and click **Open**.

The selected .cms file appears in the **Upload Module** dialog box.

6. In the **Upload Module** dialog box, click **Upload**.

A message at the top of the page tells you that module installation has been initiated.

After you have uploaded the Process Guard module successfully, the module appears in the list of modules on the Modules page.

NOTE: You may need to refresh the Endpoint Security Web UI before the new module appears on the Modules page.

Installing the Process Guard Agent Module

The **Process Guard** module consists of a **server module** and an **agent module**. The above section provided steps to upload the Process Guard 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 for the agent on which you want to activate Process Guard, and select **Edit Policy**.
4. Click on the **Categories** button in the **Edit Policy** page and select **Process Guard – <version number>** (e.g., Process Guard – 1.3.0) 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 the *Configuring Process Guard Agent Policy* section below to understand various policy options.

PART III: Uninstalling Process Guard Module

To uninstall the Process Guard 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 **Process Guard** 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 **Process Guard** module consists of a **server module** and an **agent module**. Uninstalling the **Process Guard** module removes Process Guard 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 Process Guard Agent Module

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

6. Log in to the Endpoint Security Web UI as an administrator.
7. From the **Admin** menu, select **Policies** to access the **Policies** page.
8. 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 **Process Guard**, and select **Edit Policy**.
9. Click on the **Categories** button in the **Edit Policy** page and unselect **Process Guard – <version number>** (e.g., Process Guard – 1.3.0) and click **Apply**.
10. On the **Edit Policy** page, click **Save**.

PART IV: Configuring Process Guard Module

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

Enabling the Process Guard Module

The above operation can be performed from both the Modules and Policies pages in the Endpoint Security Web UI.

Before proceeding, please review the [Configuring Process Guard Agent Policy](#) section below. It is important to understand the implications of these settings before enabling Process Guard on endpoint agents.

To enable the Process Guard 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 Guard** module and click the **Actions** icon (the gear symbol) and select **Enable** to enable the module.

To enable the Process Guard 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 assigned to the agent on which you want to activate Process Guard, and select **Edit Policy**.
4. In the **Configurations** area of the **Edit Policy** page, click **Process Guard – 1.3.0**.
5. Toggle the **Enable Process Guard on the host** selector to **ON**.
6. If you are editing Agent Default Policy, leave all other settings at the default value. If you wish to make any adjustments, please review the [Configuring Process Guard Agent Policy](#) section below first.
7. On the **Edit Policy** page, click **Save**.

Disabling the Process Guard 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 Guard** module and click the **Actions** icon (the gear icon) and select **Disable** to disable the module.

Disabling the Process Guard **server module** (once enabled) will disable the **agent module** in all the policies, causing it to be disabled on associated endpoints (Host/Client 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 Guard, and select **Edit Policy**.
4. In the **Configurations** area of the **Edit Policy** page, click **Process Guard -1.3.0**
5. Toggle the **Enable Process Guard on the host** selector to **OFF**.
6. On the **Edit Policy** page, click **Save** button.

Configuring Process Guard Agent Policy

This section describes the various configuration settings provided in the Process Guard policy.

Enable the Process Guard Agent Module

To enable Process Guard on a given host set, toggle the **Enable Process Guard on the host** to **ON** and save the policy changes. Upon configuration update on the agent, Process Guard module will be enabled on the endpoint and it will block attackers from obtaining credential data or key material stored within in critical processes.

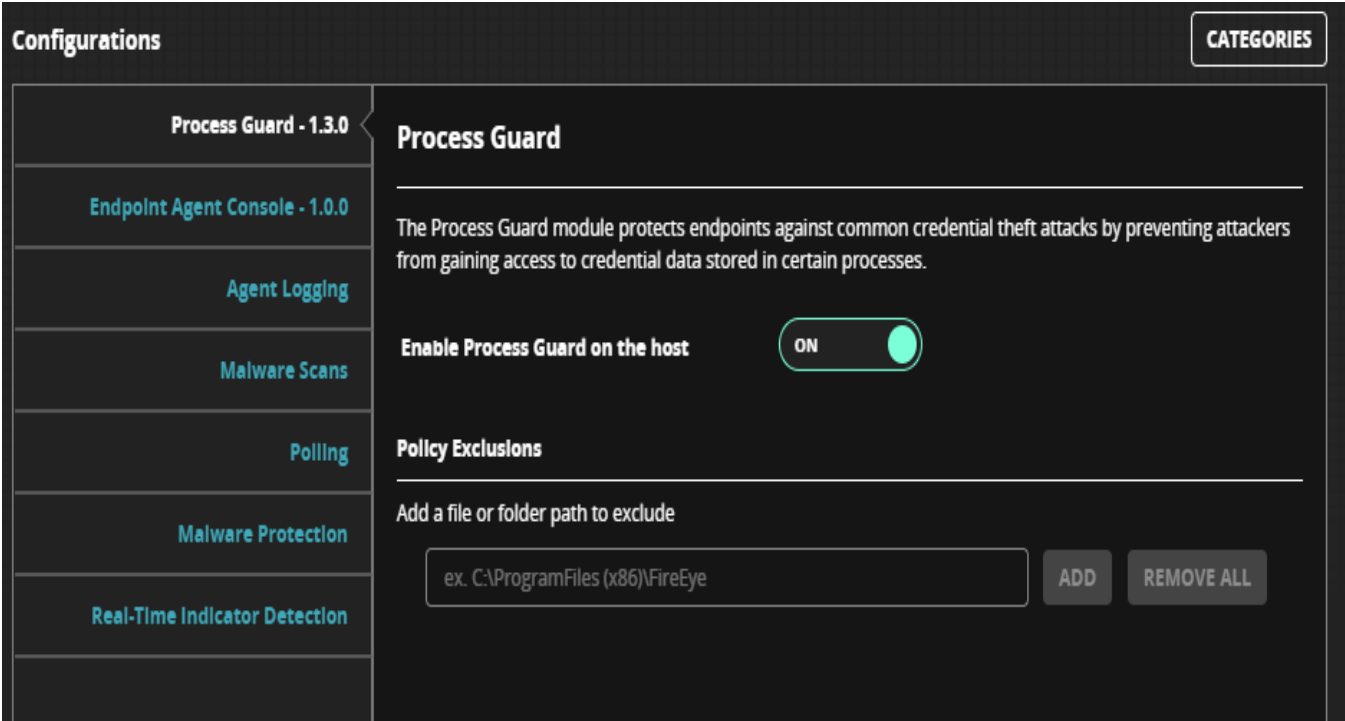


Figure 1- Process Guard Policy on Endpoint Security Server

Add Policy Exclusions (Whitelisting the Processes)

Process Guard takes preventative actions on all processes by default and this could cause some legitimate applications to not function properly. These risks can be mitigated by adding such processes to the exclusion list as shown below.

To add process exclusions to Process Guard, enter the absolute (full) path of the process that needs to be whitelisted and click on **Add** button. Each process paths need to be added separately in order to exclude multiple processes on the host.

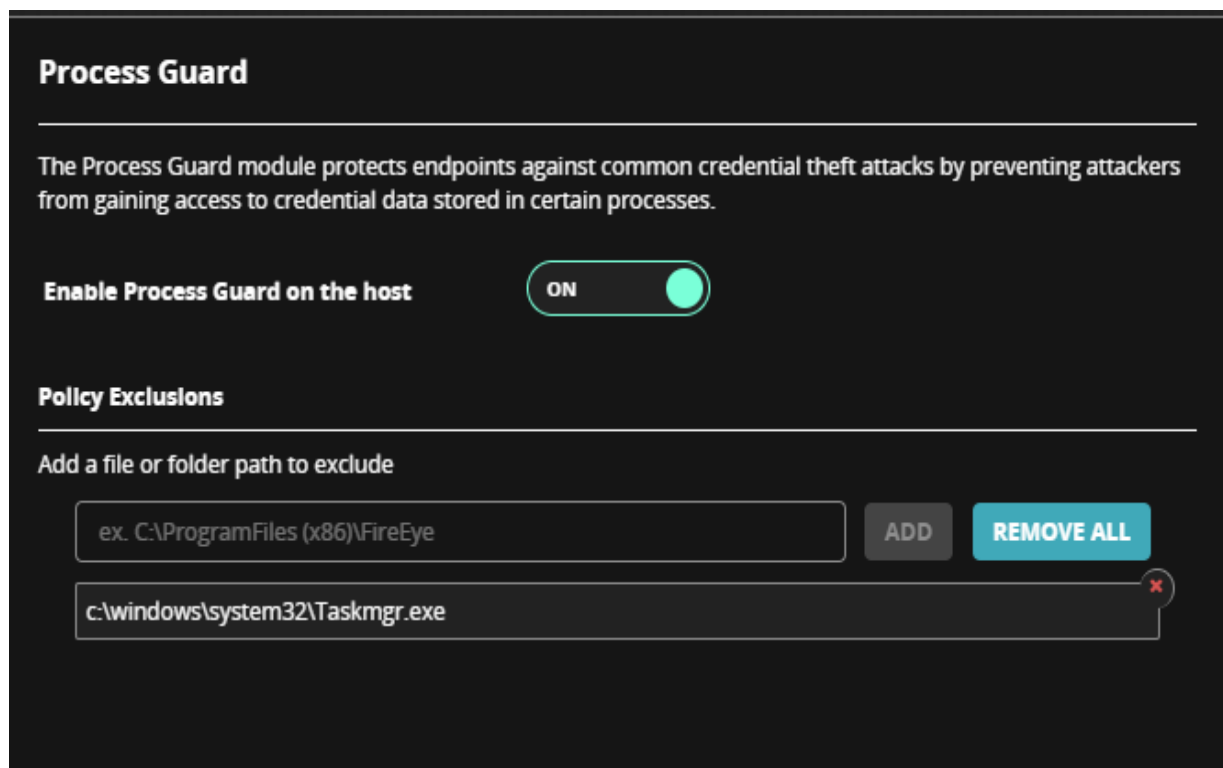
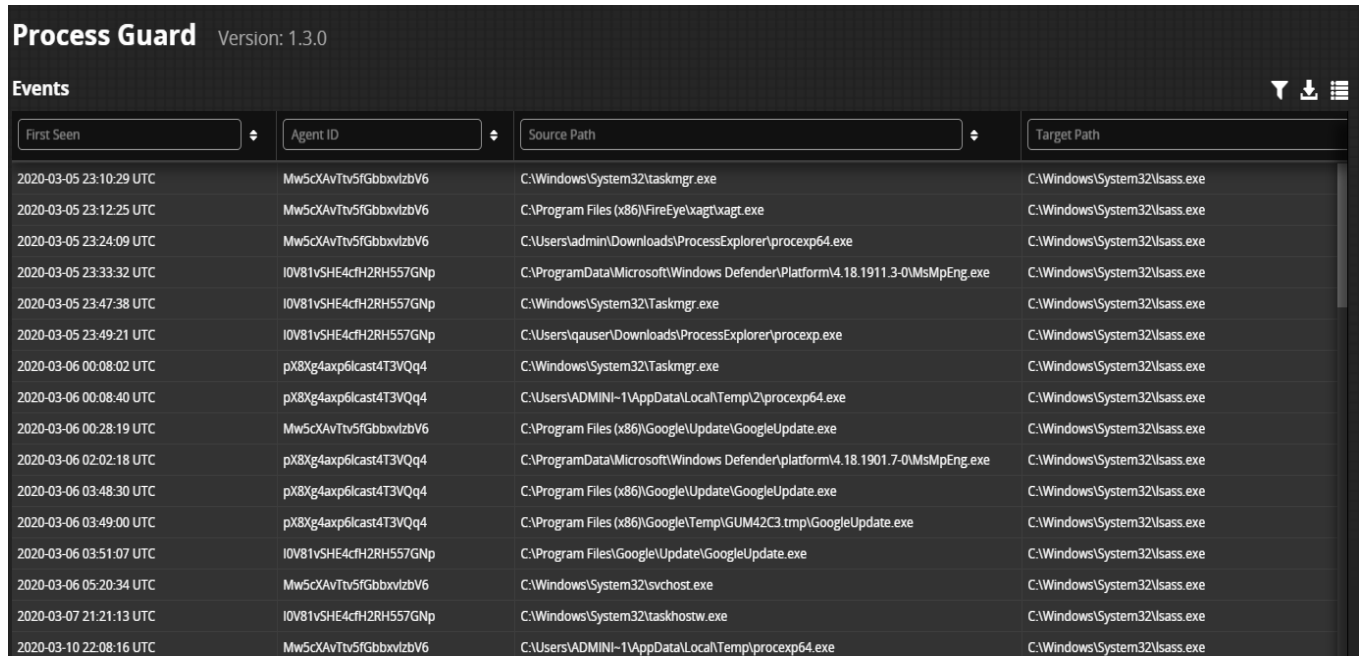


Figure 2- Process Guard Exclusion Policy Settings

PART V: Process Guard Module Home Page

Process Guard Module Home Page allows admin to track and analyze events generated by Process Guard Agent module on the hosts when a process requests access to credential data as shown in the picture below



The screenshot shows the 'Process Guard' interface with version 1.3.0. It features a table of events with columns for 'First Seen', 'Agent ID', 'Source Path', and 'Target Path'. The table lists various system and user processes attempting to access protected data, such as taskmgr.exe, explorer.exe, and googleupdate.exe.

First Seen	Agent ID	Source Path	Target Path
2020-03-05 23:10:29 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Windows\System32\taskmgr.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:12:25 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Program Files (x86)\FireEye\vxagt\vxagt.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:24:09 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Users\admin\Downloads\ProcessExplorer\procexp64.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:33:32 UTC	I0V81vSHE4cfH2RH557GNp	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1911.3-0\MsMpEng.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:47:38 UTC	I0V81vSHE4cfH2RH557GNp	C:\Windows\System32\Taskmgr.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:49:21 UTC	I0V81vSHE4cfH2RH557GNp	C:\Users\qaiser\Downloads\ProcessExplorer\procexp.exe	C:\Windows\System32\lsass.exe
2020-03-06 00:08:02 UTC	pX8Xg4axp6lcast4T3VQq4	C:\Windows\System32\Taskmgr.exe	C:\Windows\System32\lsass.exe
2020-03-06 00:08:40 UTC	pX8Xg4axp6lcast4T3VQq4	C:\Users\ADMINI~1\AppData\Local\Temp\I2\procexp64.exe	C:\Windows\System32\lsass.exe
2020-03-06 00:28:19 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	C:\Windows\System32\lsass.exe
2020-03-06 02:02:18 UTC	pX8Xg4axp6lcast4T3VQq4	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1901.7-0\MsMpEng.exe	C:\Windows\System32\lsass.exe
2020-03-06 03:48:30 UTC	pX8Xg4axp6lcast4T3VQq4	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	C:\Windows\System32\lsass.exe
2020-03-06 03:49:00 UTC	pX8Xg4axp6lcast4T3VQq4	C:\Program Files (x86)\Google\Temp\GUM42C3.tmp\GoogleUpdate.exe	C:\Windows\System32\lsass.exe
2020-03-06 03:51:07 UTC	I0V81vSHE4cfH2RH557GNp	C:\Program Files\Google\Update\GoogleUpdate.exe	C:\Windows\System32\lsass.exe
2020-03-06 05:20:34 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Windows\System32\svchost.exe	C:\Windows\System32\lsass.exe
2020-03-07 21:21:13 UTC	I0V81vSHE4cfH2RH557GNp	C:\Windows\System32\taskhostw.exe	C:\Windows\System32\lsass.exe
2020-03-10 22:08:16 UTC	Mw5cXAvTtv5fGbbxvlzbV6	C:\Users\ADMINI~1\AppData\Local\Temp\procexp64.exe	C:\Windows\System32\lsass.exe

Figure 3 – Process Guard Home Page on Endpoint Security Server

Events provides a list of events generated on the endpoint (host/client system). These can be accessed by selecting **Event** and a side card with event details will appear on the right side of the pane

The current release of the Process Guard provides following events details

Event Data	Description
First Seen	Incident time when the event occurred first
Agent ID	Unique ID of xAgent installed on host
Source Path	Absolute file path of process that attempted to access the protected process
Target Path	Absolute file path of protected process

APPENDIX A: Frequently Asked Questions

How to verify if the Process Guard installation succeeded?

Once the Process Guard is installed and enabled, check for the existence of module files under *C:\ProgramData\FireEye\xagt\exts\ProcGuard\sandbox* and *C:\ProgramData\FireEye\xagt\exts\plugin\ProcGuard*

The working status of the plug-in can be verified on the HX server via API to review the system info received from the endpoint agent.

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

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

- pg_install.log
- pg_uninstall.log
- pg_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 Process Guard server module?

You can find the log file under */var/log/supervisor/proguard-watcher-server_<version>_<unique_id>.log*

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

After successful installation following processes will be created.

- An instance of xagt.exe with “--mode ProcGuard” in its command line. This is a container application to interact with agent services. This process runs under system account like any other agent instances.
- ICeAf, Kernel driver service, runs under system account.

Why doesn't the exclusions in Process Guard policy work?

We must make sure that excluded process paths are absolute (full) file paths including the drive letter (for ex: C:\Windows\System32\TaskMgr.exe). Other file path types like folder paths, wildcard paths will be considered as invalid and not supported.

Dependencies / Limitations / Known Issues

- This technical preview release of Process Guard is supported on Endpoint Security 5.0.0 with xAgent 32.0.0 running on Windows 7/server 2012 and above only. Mac OS and Linux platforms are not supported.