# ENDPOINT SECURITY

## PROCESS GUARD v1.4.1

MODULE USER GUIDE

GENERAL AVAILIBILITY RELEASE

Endpoint Security Agent - Process Guard Module User Guide

Software Release v1.4.1

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



 

# 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 detects or blocks access requests to the critical process (lsass.exe) with credential data. An event is sent to the Endpoint Security (HX) controller and viewable in Process Guard module home page. This page helps administrators to analyze and troubleshoot any potential compatibility issues. By default, Process Guard detects all processes accessing credential data without blocking.

Process Guard provides a whitelisting feature that allows administrators to bypass detection (or block action). This alleviates any issues with legitimate applications that require full system access to perform normal operations.

## Prerequisites

This release of Process Guard is supported on **Endpoint Security 5.0.0** with **agent 32.30.10 (MR)** running on **Windows 7/Server 2012 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 Process Guard v1.4.1 on Endpoint Security 4.9.x and it is also not recommended to enable the feature on agent 32.30.0 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 **agent 32.30.10(MR)**. 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 Process Guard 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 Process Guard Agent Module

The **Process Guard** module consists of a **server module** and an **agent module**. The above section provides 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 assigned to the host set you want to deploy Process Guard to, 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 – 1.4.1) 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 *Part IV: Configuring the Process Guard Module* 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 i**s 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 provides steps to uninstall the Process Guard module completely from the HX server and managed FireEye endpoints. To remove only the **agent module** for 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 – 1.4.1) 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).

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

## Configuring Process Guard Agent Policy

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

**Enabling 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.


*Figure 1 - Process Guard module Policy Settings*

### Enabling the Block on Detection

To enable blocking the access to critical process on a given host set, toggle **Block on Detection** to **ON**. Upon configuration update on the agent, Process Guard module will block attackers from obtaining credential data or key material stored within in “lsass.exe” process.

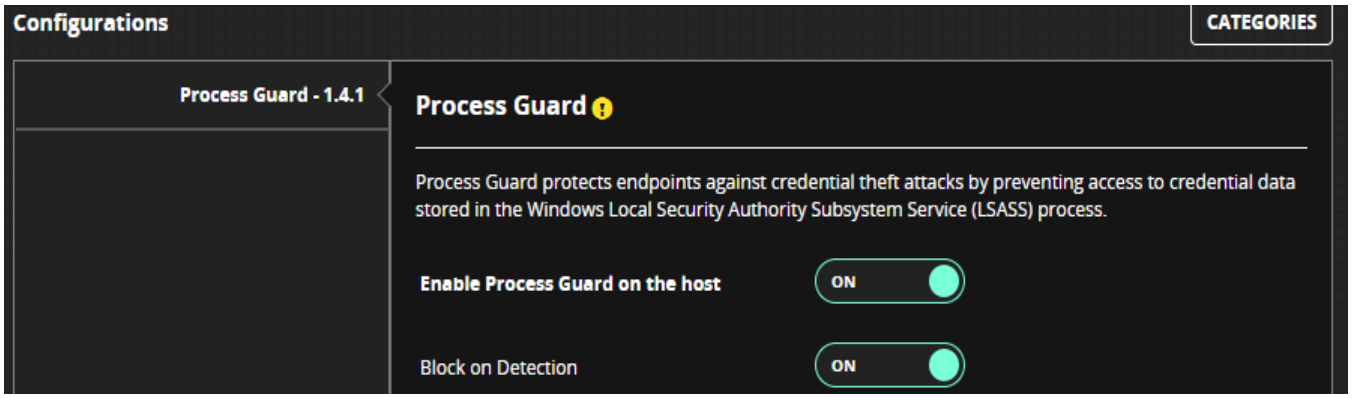


*Figure 2 - Process Guard Action Policy Settings*

*Note:* This behavior has changed from Technical Preview release which blocked the processes by default and there was no detection only capability.

### Add Policy Exclusions (Whitelisting the Processes)

Process exclusions are provided to bypass detection (or block action) of legitimate applications. Configuring exclusions for Process Guard will prevent it from flooding an Endpoint Security server with events.

To add process exclusions, enter the full path of the process that needs to be whitelisted and click on **Add** button. Each executable path needs to be added separately in order to exclude multiple processes on the host.

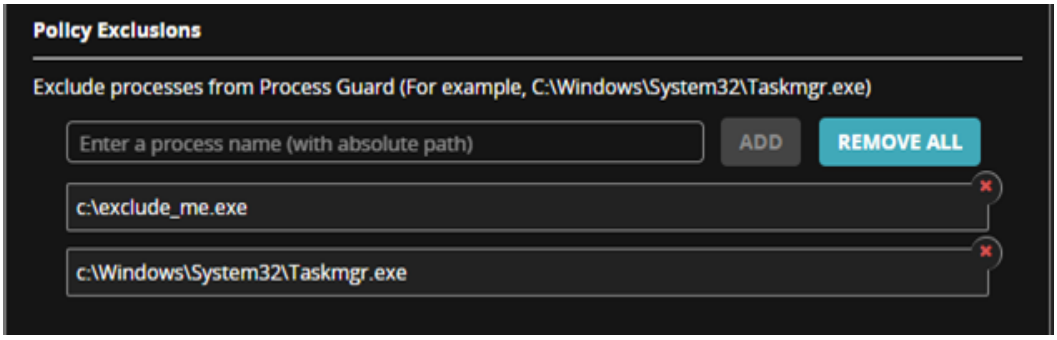


*Figure 3 - Process Guard Exclusion Policy Settings*

**Event Throttling (Event suppression)**

Process Guard generates detection or block events for every access request. These events, if not throttled, can increase network traffic and increase load on the Endpoint Security server. The **Throttling interval** can be set to defined interval to aggregate the duplicate (attempts to access lsass.exe from the same process and same method) events generated within the throttle period.

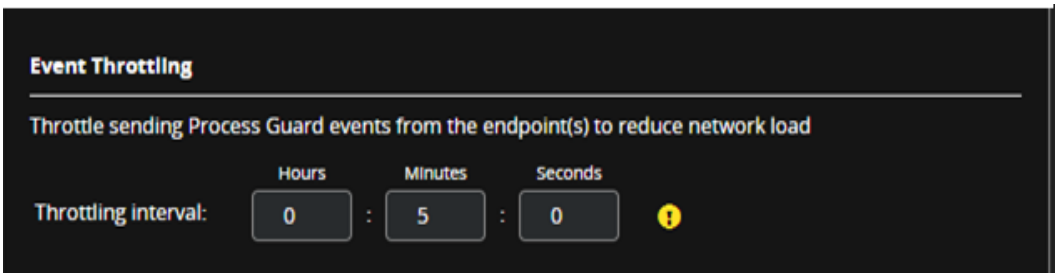


*Figure 4 - Process Guard Throttle Interval Policy Settings*

## Configuring Process Guard Server settings

This section describes the various configuration settings provided in the Endpoint Security Server.

To access the Process Guard 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 Guard** 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 **Process Guard Settings** page.

## Enrichment Settings

Enricher module enriches process information and provides valuable insights. Upon selecting **Enable Enrichment of Process Guard Events** Process Guard submits requests to enricher for further analysis. Enricher may request acquisition of executable running the process for investigation. Enrichment of data may take some time depending upon its cached information and its integration with FireEye products. Further documentation on Enricher module can be downloaded from FireEye Market.

Note: Enricher module must be installed on the same HX Server and enabled for this option to function.

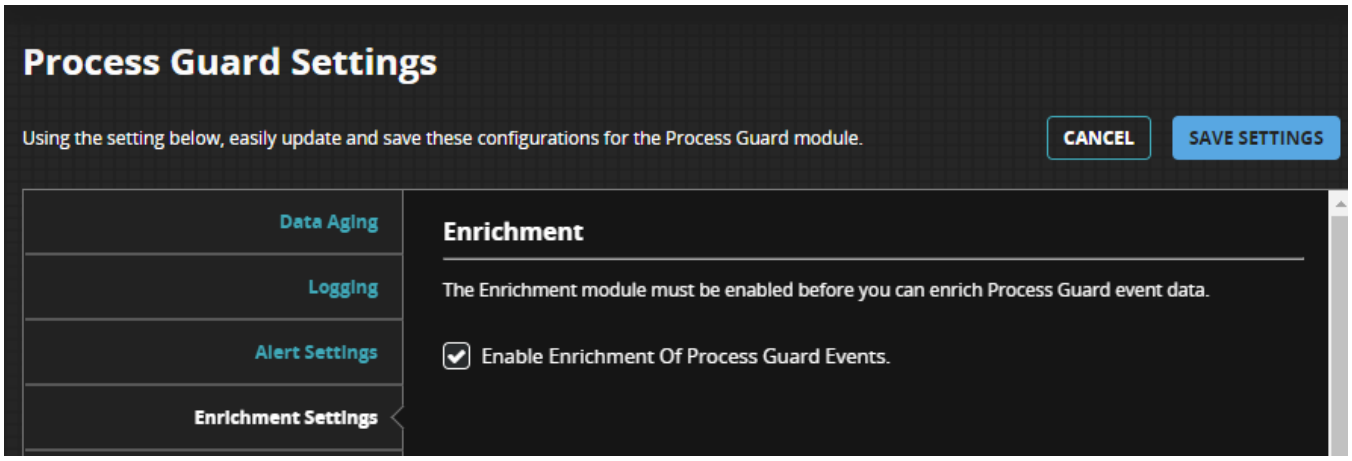


*Figure 5 - Process Guard Server Enrichment Settings*

## Alert Settings

The Process Guard module can generate alerts for events on processes accessing LSASS. Select **Enable Alerts for Process Guard Events** to generate alerts. Note that generation of alerts is not controlled by enricher verdict. Please go through the *Appendix A: Frequently Asked Questions* on the recommended way to setup Process Guard before enabling alerts.

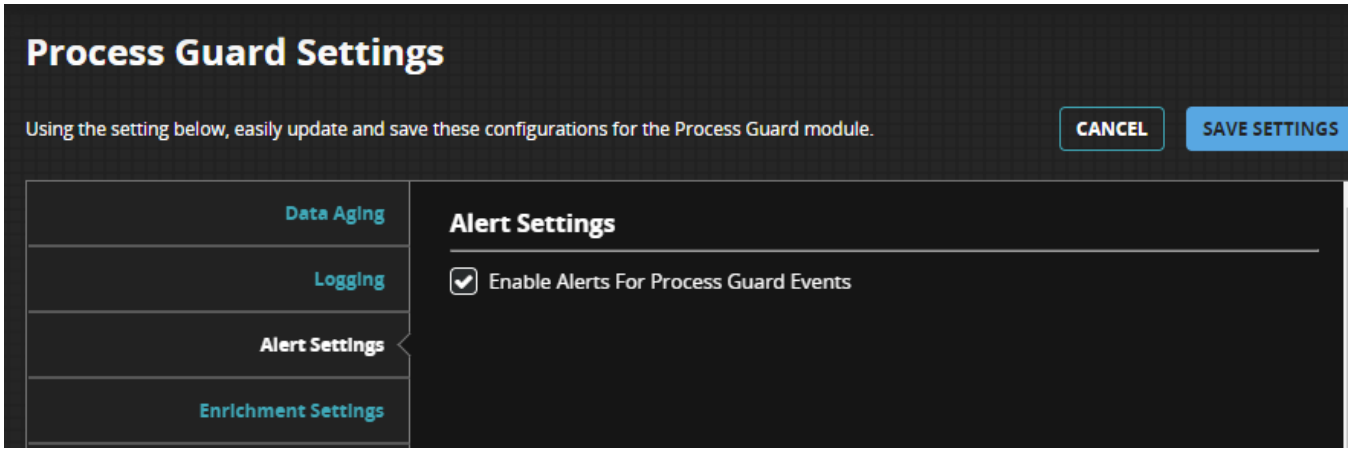


*Figure 6 - Process Guard Server Alert Settings*

### Data Aging

Process Guard receives events from the endpoints for each unique process attempt to access LSASS. These events are stored in HX database for a finite period, after which they are discarded. Use the Data Aging Settings to specify how long to retain events. The default value is 30 days.

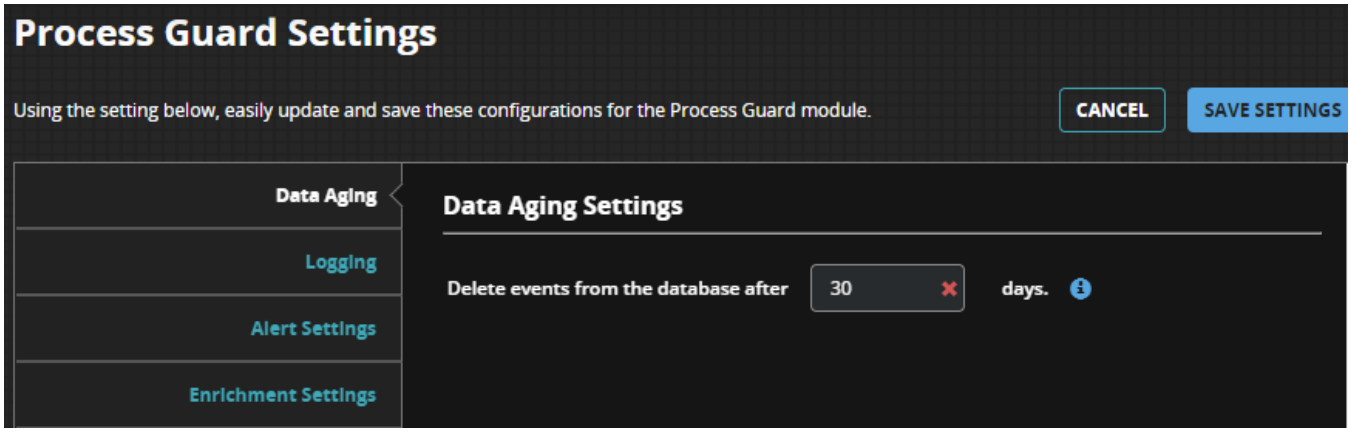


*Figure 7 - Process Guard Server Event Aging Settings*

## 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 Process Guard's Current Configuration

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

**Request**

| HTTP Verb | Route | Parameters |
|---|---|---|
| **GET** | hx/api/services/config/tree | ?node_name=/config/procguard-watcher |

**Response**

| Key | Value |
|---|---|
| **data** | List of configuration properties. Each property has the following attributes:<br>• name – the name of the configuration property<br>• type – the shape of the value for this configuration property<br>• value – the current value of this configuration property<br>• default_value – the default value of this configuration property |

**Configuration Options**

| Property | Route | Data Type |
|---|---|---|
| **Aging Limit** | config/procguard-watcher/aging/database/age_limit | Type: **Int32**<br>Default: **30 (days)** |
| **Alerting Enabled** | config/procguard-watcher/alerting/enabled | Type: **bool**<br>Default: **false** |
| **Enrichment Enabled** | config/procguard-watcher/enrichment/enabled | Type: **bool**<br>Default: **false** |
| **Logging Level** | config/procguard-watcher/logging/level | Type: **string**<br>Default: **info** |

## Updating Process Guard's Configuration via API

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

**Request route**

| HTTP Verb | Route | Parameters |
|---|---|---|
| **PUT** | hx/api/services/config/tree | ?node_name=/config/procguard-watcher |

**Request Headers**

| Header Property | Value |
|---|---|
| **Content-Type** | Application/json |
| **X-FeApi-Token** | {{generated api token value}} |

**Request Body**

The request body will contain a JSON object with a single property “data”, containing an array of JSON objects for each configuration setting to update. Here’s an example for updating the **age limit** setting:

```
{
    "data": [
        {
            "default_value": "30",
            "name": "/config/procguard-watcher/aging/database/age_limit",
            "type": "int32",
            "value": "60"
        }
    ]
}
```

## Module REST API

The following API endpoints are provided by the Process Guard module. Note that these API endpoints focus around retrieval of LSASS process access 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.

| API | Route | Description |
|---|---|---|
| **Status** | /health/state | GET – Returns the module’s status, e.g. whether the server component is running or not. If running, will return “healthy”. |
| **Meta-data** | /grid/metadata | GET – Returns the column definitions and metadata for the grid table |
| **Events** | /grid/data | GET – Returns events in JSON format |
| | /grid/export | GET – Exports events details in CSV format |
| **Settings** | /grid/settings | GET – Returns user settings for events grid UI<br>POST – Saves user settings<br>DELETE – Deletes user settings |
| | /grid/settings/import | POST – Imports grid UI settings |

# PART V: Process Guard Module Home Page

Process Guard Module Home Page allows administrators to view events generated by Process Guard module.

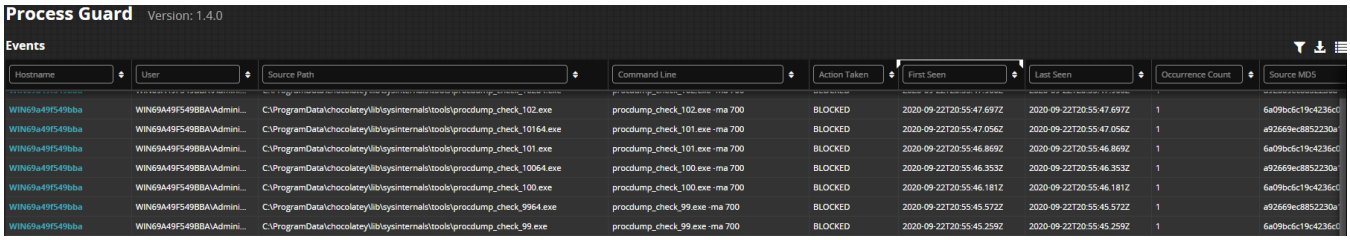


*Figure 8 – Process Guard Home Page on Endpoint Security Server*

Home page lists the default columns and can be modified to suite your needs. Standard features such as exporting the grid data to CSV format and creating private/public filters are supported. Selecting an event opens a side card with all the event details.

| Event Data | Description |
|---|---|
| Hostname | Host name of the machine. Clicking on this hyperlink opens Host page |
| User | Username of logged in user account |
| First Seen | Timestamp of an event seen for the first time after Process Guard module installation |
| Last Seen | Most recent timestamp of the same event |
| Agent ID | The unique ID of agent installed on host |
| Source Path | The fully qualified path of the executable associated to the process |
| Source MD5 | The MD5 hash of the source process file |
| Source PID | The process ID of source process |
| Command Line | The command arguments supplied to the process when it executed |
| Action Taken | Action (blocked or detected) taken by the endpoint |
| Occurrence Count | Total count of repeated attempts |
| Process Cert | Source process digital signature details |
| Signature Verified | Source process digital certificate verification status |
| Is Signed | Indicator if a signature exists for the file associated to the process |
| Source Parent Path | The fully qualified path of the file associated to the parent process of the process being executed |
| Parent PID | Process ID of the parent process |
| Target Path | Absolute file path of protected process |
| Target PID | Target Process ID |
| Enrichment Status | FireEye Intelligence verification on the source process |

# PART VI: Alerts

Alerts from Process Guard show up on the Alerts page of the Endpoint Security Web UI with the Alert Type as **PG**.

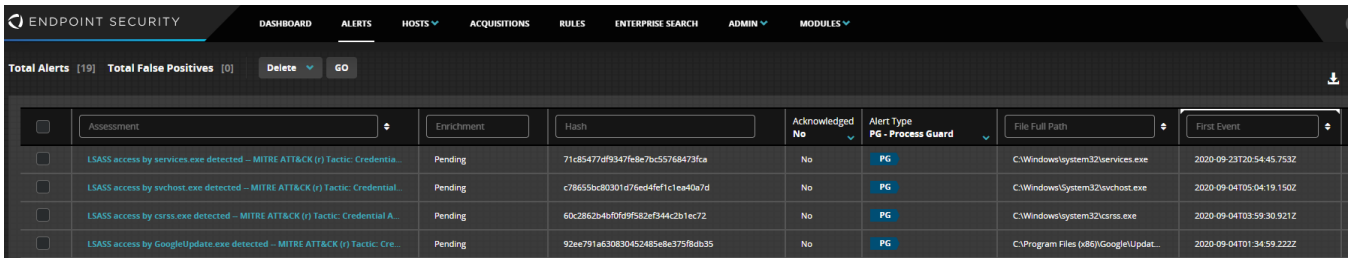


*Figure 9 – Sample of Process Guard alert on the Alerts page*

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

## Hosts (Alert Details)

Upon selecting a Process Guard alert from Alerts page details of the alerts are shown on the Hosts page of the Endpoint Security Web UI.

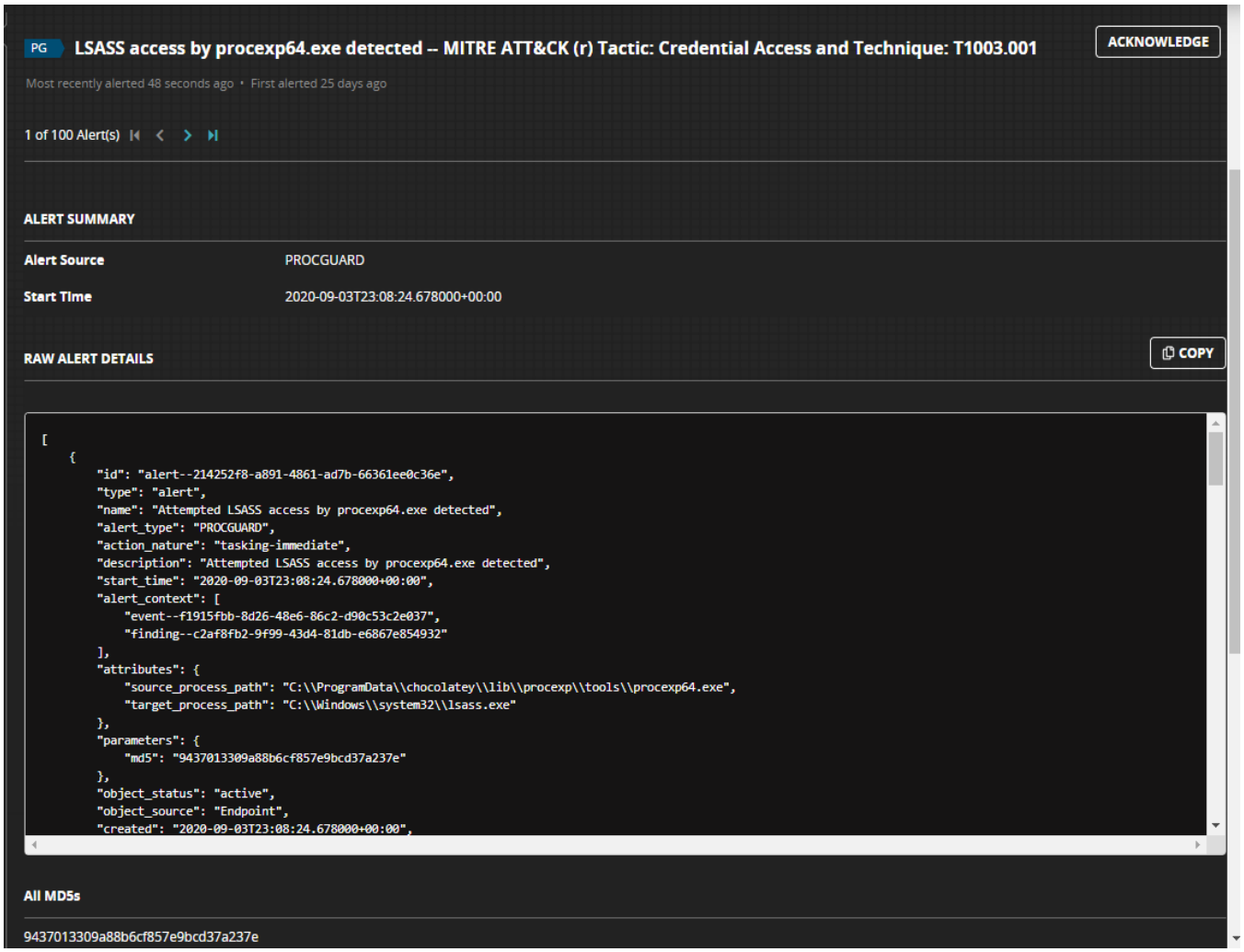


*Figure 10 – Sample of Process Guard alert on the Hosts page*

Current version of HX server provides a raw view of the alert details in JSON format. Most of the information available in the Process Guard home page are reformatted to generalize the alerts data coming from various modules.

| Alert Fields | Description |
|---|---|
| attributes.source_process_path | Process file path accessing lsass.exe |
| attributes. target_process_path | File path of lass.exe |
| parameters.md5 | Hash of the source process file |
| signature_verified | True if signature of the source process is verified |
| signature_exists | True if signature exists for the source process |
| arguments | Command line arguments passed to source process |

*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 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 "/hx/api/v3/hosts/<agent_id>/sysinfo" to review the system information (Sysinfo) received from the endpoint agent. You should see following fields in Sysinfo JSON data.

```
"ProcGuard": {
   "version": "1.4.1",
   "plugin_state": "2",
   ...
}
```

| Module Status (plugin_state) | Description |
|---|---|
| 0, 1 | Not initialized, initializing. |
| 2 | Initialized. Process Guard is fully functional in this state. |
| 3, 4, 5, 6 | Failed to obtain driver interfaces, failed to guard LSASS process, generic failure cases |
| 7, 8 | Uninitializing, uninitialized |

## 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_preupgrade.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 installation, Process Guard spawns an instance of xagt.exe with ProcGuard 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 instances.

## Why doesn’t the exclusions in Process Guard policy work?

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.

## Why do I see multiple entries of a process from the same host in Process Guard home page?

Process Guard uses multiple attributes to uniquely identify a process. This includes process file path, file hash, parent process file path, command line, user account, and action taken (detect/block). If any of these attributes change, it will be treated as a new unique event.

## Why do I see “Permission denied!” for some of the events?

This text appears due to limitations/issues when obtaining certain information. This happens mostly due to permission issues (e.g. Windows Protected Processes, Anti-Malware Protected Process Light- AMPPL, other) security products preventing access, short-lived processes, etc.

## What are the recommended steps for using Process Guard?

By default, Process Guard runs in detection mode. In this mode access to LSASS is not blocked, but an event is sent to HX server upon detection. After installation, it is recommended to run in detection mode to find out all applications that need access to LSASS. This can be achieved by reviewing entries in the Process Guard home page. Use this analysis to add such processes to Process Guard exclusion policy and monitor for any new events. Once a reasonable baseline is established you can enable blocking mode and alerting capability. Enabling alerting functionality too early might cause many alerts to be reviewed/acknowledged.

## Why should I not enable blocking mode immediately after installation?

We recommend establishing a baseline of legitimate processes that need access to LSASS and exclude them using Process Guard exclusion. Without this step, there are chances of causing disruption to your critical/important business applications.

## Why Process Guard is not blocking the processes?

This could be due to following reasons

- Process Guard policy is not setup to **Block on Detection** mode. Please note that the default behavior of Process Guard has changed to detection only mode in default installation mode. In order to block it, one must enable to **Block on Detection** option.
- Process is excluded via Process Guard exclusions.
- There is no compatible agent version installed. Please note that Process Guard requires agent v32 MR update (v32.30.10) installed to be fully operational.

## Why Process Guard is not publishing Alerts?

This could be due to following reasons

- By default, Process Guard Alert Settings will be disabled. This setting needs to be enabled to publish alerts
- Publishing of Alerts might get delayed if Enrichment settings is enabled as the Enricher module may request acquisition of process file for investigation. Enrichment of data make take some time depending upon its cached information and its integration with FireEye products.
- Enrichment settings is enabled; however, Enricher module is not properly configured.

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

## Are there any compatibility issues with other security solution?

Yes, The Process Guard may not work as designed when other security solutions have been enabled and protect the process lsass.exe This may result in failure to obtain a process handle to access memory for lsass.exe as other security products attempt to perform the similar action. Below are the features/products where this behavior might occur

- Windows LSA protection feature - run lsass as Protected Process Light (PPL)
- Credential Guard
- Any other security product protecting lsass.exe

In order to confirm that Process Guard is working as expected, one could look into "plugin_state" field in the Process Guard SysInfo JSON data (table provided in Process Guard installation FAQ above)

## Dependencies / Limitations / Known Issues

- This general availability release of Process Guard is supported on Endpoint Security 5.0.0 with agent 32.30.10 **(MR)** running on Windows 7/server 2012 and above only. Mac OS and Linux platforms are **not** supported.
- It is not possible to mark an alert as false positive. However, the process can be added to Process Guard exclusion if deemed necessary and avoid receiving alerts.
- Process Guard can't detect / block processes from accessing LSASS if they run before Process Guard module is initialized and running.
- Process Guard may detect Endpoint Agent process "xagt.exe" in some rare scenarios and generate an event.
- Please refer to release notes for list of known issues in the current release