McAfee ePolicy Orchestrator (ePO) for Cyber Defenders

Version 2.0
Date: 1-9-2018
POC: @Wired_Pulse

Date	Version	Changelog	Page(s)	By
3-16-2016	1	Created document	All	@Wired_Pulse
4-5-2016	1.1	Added additional queries and dashboards	22	@Wired_Pulse
9-1-2016	1.2	Relocated HIPs rules, queries, and dashboards from this guide to my Github (www.github.com/wiredpulse)	26	@Wired_Pulse
1-9-2018	2.0	Added lateral movement blocking, reversing quarantined binaries, and detection of executable information.	40, 42,47	@Wired_Pulse

able of Contents

Introduction

McAfee ePolicy Orchestrator (ePO) is a flexible application that has the capability to monitor, detect, and counter against known cyber-threats to an organization. The system is managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System (IPS) and host firewall along with a number of add-on products.

Methodology

The methodology for utilizing ePO in favor of a cyber defender's mission can really be broken down into three parts:

1) Configure the ePO to report, block, quarantine, and/or delete files of interest and alert based on specific rules or emerging threats.

2) Build queries and reports in order to search for and visualize data that the ePO receives.

3) Build dashboards comprising of queries in order to present a holistic view ePO data.

These three concepts are important to understand as one directly affects the other. For example, what good would it be if we configured the HIPS rule with ID 6053 (alert when a user is accessing another users home directory) if we never develop a query to see that data? Furthermore, if we had did the query, that data alone may not make much sense to us. Therefore, building a dashboard to not only present the alert from ID 6053 but that of others could easily depict some lateral movement in our network.

Permissions

If you are an incident responder responding to an incident and the organization has an ePO server, ideal permissions that you may want to request is that of Global Reviewer. You will however, want to also request the following additions:

- Dashboards - Use public dashboards; create and edit private dashboards
- Queries and Reports - Use public groups; create and edit private queries/reports

The recommended course of action in order to set up these permissions is to duplicate the existing Global Reviewer permission set and make the aforementioned changes to it. This will allow the supported organization to easily remove the permissions upon the defender leaving since all they have to do is delete the user account and the duplicate permission set.

Below are the steps for creating said permissions and user accounts.

1) Navigate to User Management -> Permission Sets.

2) Highlight Global Reviewer in the left pane and click Actions at the bottom of the screen.

3) Select Duplicate.

4) Give the new permission set a name and click OK.

5) Click the newly created permission set in the left pane.

6) In the right pane, edit Dashboards and Queries and Reports to reflect the above permissions.

7) Once completed, navigate to User Management -> Users.

8) Click New User at the bottom of the screen.

9) Fill in the required data and for the permission set, be sure to select the newly created permissions.

10) Click Save.

Manual Installation of ePO Agent

When responding to an incident and trying to mitigate infection, there may be systems that will need the agent. Depending on the urgency of the situation, the automated ways of deploying an agent could either take too long or is not a viable option. When either are the case, the agent can manually be installed using the following instructions:

1) On the machine needing the agent, navigate to \\EPOSERVERNAME\C$\Program Files\McAfee\ePOlicyOrchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\

   Note: Depending on the installation of the ePO, this may be on another partition.

2) Double click the FramePkg.exe file and let the agent install. Please note, you will need administrative rights over the workstation to perform this.

3) Open a command prompt window and type the following: cd "C:\Program Files\McAfee\Common Framework"

   Note: In some cases, it may be installed to Program Files (x86).

4) Once in the aforementioned directory, type the following at the command prompt and press return: CmdAgent.exe /s

5) You will now be presented with the McAfee Agent console, click "Collect and Send Props". This prompts the agent to advertise itself to the ePO server and enforce any policies or client tasks that maybe set, which in my case is usually the installation of the ant-virus product and Host Intrusion Protection.

   Note: The newly added machine, if not pre-staged first, will appear under Lost&Found on the ePO.

VirusScan Enterprise (VSE)

While there are several policies that make up VSE, we will only address options within the three policies below and the Access Protection Policy and Unwanted Program Policy.

Key configurations

On-Access Default/Low/High-Risk Processes Policies

- Scan Items
  - Scan files - All options available should be checked
  - Compressed files - Both options should be checked
  - Unwanted Programs Detection - check option to enable

- Exclusions
  - ➢ What not to scan - Put in any tools that the team will be using to ensure that they can run properly

General Options Policy

- Password Options
  - ➢ User interface password - Make sure there is a password here. If not, the user can adjust settings on the local system

On-Access General Policies

- General
  - ➢ Scan - Check all options
  - ➢ Artemis... - Set to either Low or Medium depending on the network. More information regarding Artemis can be found below and in the Global Threat Intelligence section.

Artemis (GTI)

Artemis, part of McAfee Global Threat Intelligence (GTI), is a heuristic network check feature that looks for suspicious programs and DLLs running on VirusScan Enterprise protected client systems. The Artemis feature catches malware before the regular DATs are deployed. According to McAfee, it has been deployed successfully to more than 27 million endpoints and should be enabled at all times.

With Artemis enabled, when VirusScan Enterprise detects a suspicious file it sends a DNS request containing a fingerprint of the suspicious file to a central database server hosted by McAfee Avert Labs. In less than a second, if the fingerprint is identified as known malware, an appropriate response is sent to the user to block or quarantine the file.

Configure the sensitivity level you wish to use when determining if a detected sample is malware. There are five sensitivity levels, between Very low and Very high, plus Disabled. The higher the sensitivity level you choose, the higher the number of malware detections. However, by allowing more detection, you might also get more false positive results.

It is recommended to start at Low and move the sensitivity level to Medium depending on the number of false positive malware detections found.

Access Protection and Unwanted Programs Differences

In Access Protection, the policy can only block the file's execution and/or report on the file being executed. In Unwanted Programs, executing the file will either trigger the system to clean it, deny access to it, or delete it. Also, Access Protection can monitor/ search for ports, files/folders, and registry keys while Unwanted Programs seems to only be able to do to files/exe. Please be aware of the differences as you employ them both and in either cases, test your policies.

Configuring the Access Protection Policy

For potential items of interest in the network, configuring this policy will block the execution and/or allow the execution but report its use. In either case, the activity will be sent to the ePO the next time it checks in.

1) Policy Catalog >VirusScan Enterprise.

2) Duplicate the Access Protection Policies rule-set labeled with McAfee Default.

3) Give the duplicate policy a name and hit Ok.

4) Configure rules as needed in the window.

   Note: For each rule there are two available checkmark spaces. The first column is to block the action and the second is the report the action. If you are going to block something, check both boxes.

   You can also edit the rule and change the rule name and specify processes to include and exclude.

5) Click Save.

6) Wake up systems so they get the updated policy.

While every environment is different, below are the bare minimum recommended baseline rules to configure to at least log on, if not block.

- Block Scripts and all programs from running from the temp directory

** At a minimum, this will require adding cmd.exe, powershell.exe, and iexplore.exe to the included processes list **

-> Anti-spyware Maximum Protection
---> Prevent all programs from running files from the Temp folder
---> Prevent execution of scripts from the Temp folder

- Prevent programs from registering as a service and to autorun.
  -> Common Maximum Protection
  ---> Prevent programs registering to autorun
  ---> Prevent programs registering as a service

For the average environment, it is recommended place a checkmark next to any rule you use in order to report on its execution. Once you are able to tune the network and normalize the data, it is recommended to make exceptions and change the state of specific rules to block.

User-defined Rules can also be set here to block or report files, folders, registry keys, and/or ports. Examples of user-defined rules can be found in Annex B of this document.

Configuring the Unwanted Program Policy

This is another capability used to identify potentially malicious items in the network.

1) Policy Catalog >VirusScan Enterprise.

2) Duplicate the Unwanted Program Policies rule-set labeled with McAfee Default.

3) Give the duplicate policy a name and hit Ok.

4) Click on the name of the newly created policy.

5) Click the User-Defined Items tab and then Add.

6) Specify the name of the file.

7) Click Ok and then Save.

8) Wake up systems so they get the updated policy.

The key with this policy is that when the item of interest is executed, it can be configured to clean, deny access, or delete the file. In order to configure the action, go to VirusScan Enterprise > On-Access Default Processes Policies > Clients > Actions

Global Threat Intelligence (GTI)

Based on activity from millions of sensors world-wide and an extensive research team, McAfee publishes timely, relevant threat activity via McAfee Global Threat Intelligence (GTI). This always-on, cloud-based threat intelligence service enables accurate protection against known and fast-emerging threats by providing threat determination and contextual reputation metrics. McAfee GTI integrates directly with the ePO, instantly protecting against emerging threats to reduce operational efforts and time between detection and containment.

Key benefits

- Compresses the threat protection time period from days to milliseconds.
- Increases malware and zero-day detection rates.
- Reduces downtime and remediation costs associated with malware attacks.

Enabling GTI in HIPS

1) Launch ePO and go to the Policy Catalog.

2) Select Host Intrusion Prevention 8.0 or later: Firewall under Product.

3) Select Firewall Options under Categories.

4) Click Edit corresponding to the policy for which you want to enable GTI.

5) Select a value of either Low Risk or higher from the drop-down list for Incoming/Outgoing Trusted Source Block Threshold.

Enabling GTI in VSE

1) Launch ePO, and then click Menu>Policy>Policy Catalog.

2) Select VirusScan Enterprise 8.7.0 (or later), On Access General Policies.

3) Select to edit the policy for Server or Workstation.

4) Select the General tab, and then select the Sensitivity level under Heuristic network check for suspicious files (or in VSE 8.8, under Artemis (heuristic network check for suspicious files)).

5) Save the policy.

6) Select VirusScan Enterprise 8.7.0 (or later), On Access Default / High-Risk / Low-Risk Process Policies.

7) Select to edit the policy for Server or Workstation.

8) Click the Scan Items tab and enable Find Unknown Programs and Trojans under Heuristics.

9) Save the policy.

Testing GTI

To test that the policy is configured correctly and working as it should, go to https://kc.mcafee.com/corporate/index?page=content&id=KB53733. Listed on the site is sample data that can be used to test that GTI is working as it should.

Host Intrusion Prevention System (HIPS)

McAfee HIPS is incredibly powerful and when used correctly, can provide prevent the execution and spreading of malicious activity throughout a network. Its use particularly helps with the prevention of lateral movement.

Configuring

- HIPS 8.0: General
  - Client UI - Display pop-alerts and other display options
  - Trusted Applications - Place any cyber defender tools here so HIPS doesn't block them

- HIP 8.0: Firewall
  - DNS Blocking - Block domains using wildcard (ex: *yahoo.com) Firewall Options - Enable/disable firewall
  - Firewall Rules - Rule generation/adjusting by protocol, port, or program

- HIP 8.0: IPS
  - IPS Options - Enable/disable HIPs or NIPS
  - IPS Protection - Set the severity level and reaction (Prevent [block], log, ignore)
  - IPS Rules - rule generation/adjusting

Default Queries associated with HIPS

Queries & Reports -> McAfee Groups - > Host Intrusion Prevention

Default Dashboards associated with HIPS

McAfee Dashboards -> Host IPS: Triggered Signatures

McAfee Dashboards -> Host IPS: Dashboard

DNS Blocking

Note: The firewall must be enabled for this to work.

1) Navigate to Policy Catalog -> Host Intrusion Prevention 8.0: Firewall.

2) In the Name column, click the entry for DNS Blocking (or create a new one by duplicating an existing one).

3) List domains that you want to block using the wildcard (*) with the domain name. For example, to block yahoo.com, you would input "*yahoo.com" (without the quotes).

4) Click Save in the bottom right corner.

5) Whatever clients this policy is associated with will be updated on the next check-in. Once the clients have updated their policy, you can open HIPs on one of them and verify the DNS Blocking entry is listed under the Firewall Policy.

Blocking Lateral Movement

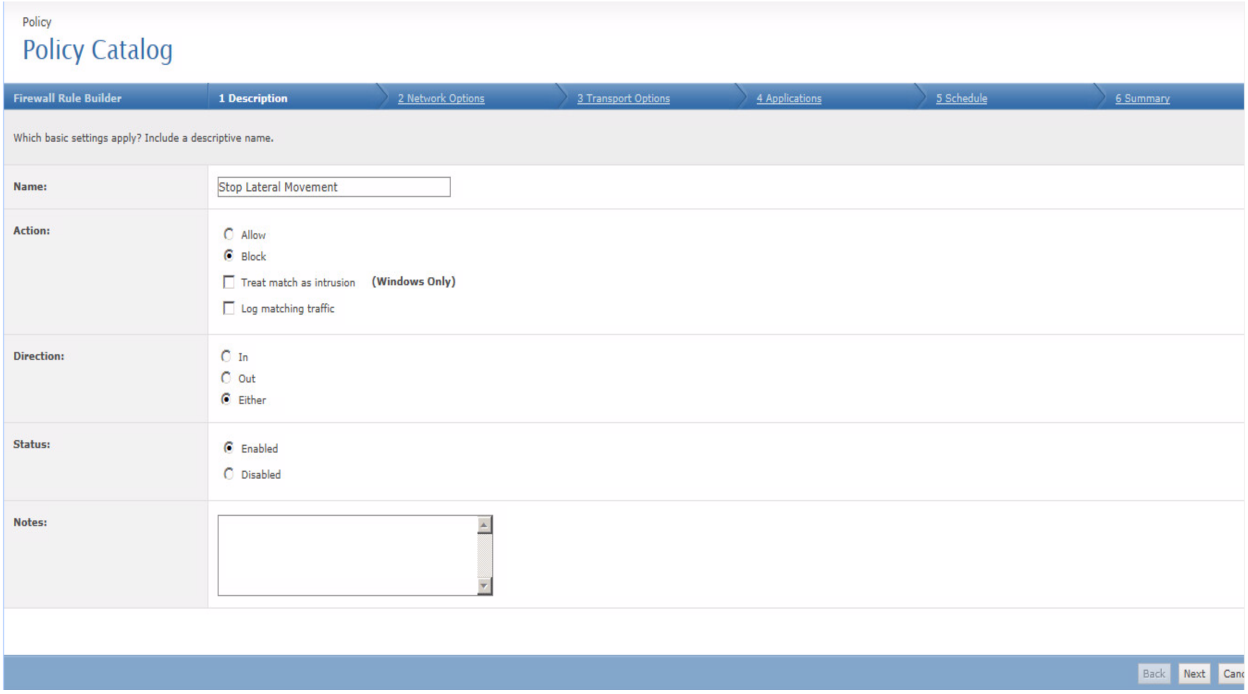
Stopping lateral movement with the ePO Firewall.

1) Open Policy Catalog > Host Intrusion Prevention 8.0 Firewall.

2) Edit the applicable Firewall Rules entry applicable to your mission.

3) Click New Rule at the bottom of the screen.

4) Fill in the requested data in the Description tab as shown below and click Next.


Policy

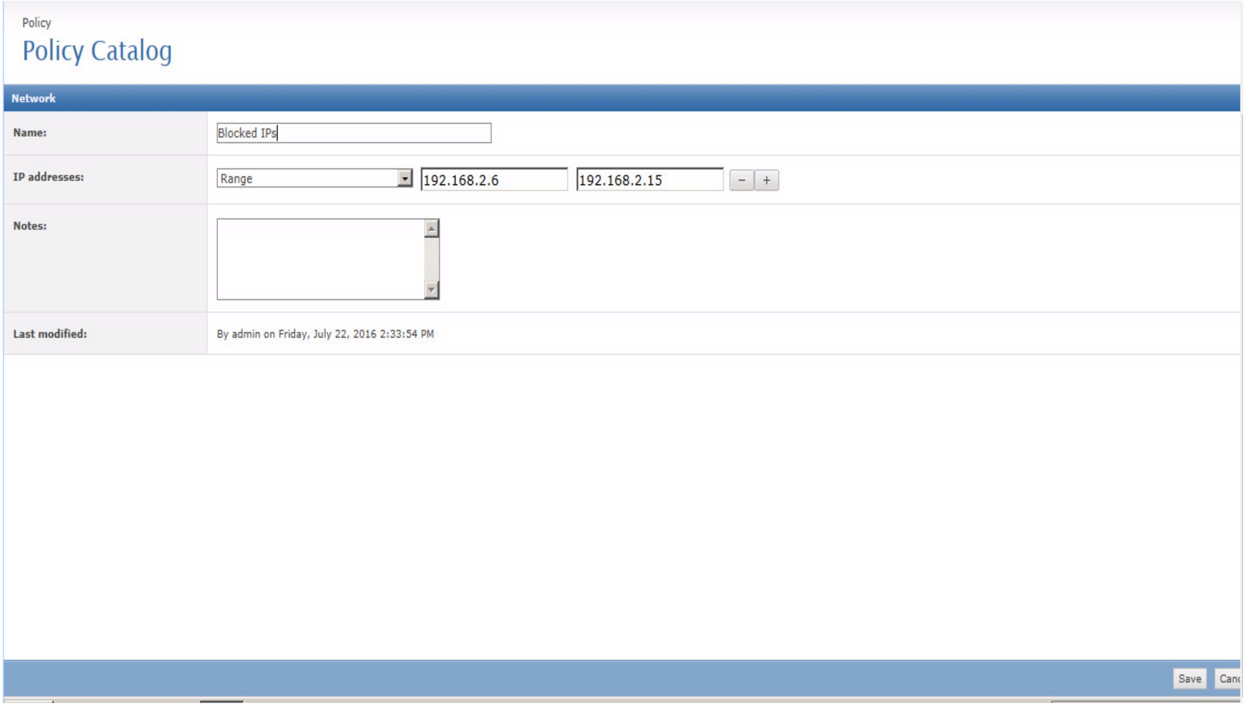
Policy Catalog

Which basic settings apply? Include a descriptive name.

Name:	Stop Lateral Movement
Action:	○ Allow ● Block □ Treat match as intrusion **(Windows Only)** □ Log matching traffic
Direction:	○ In ○ Out ● Either
Status:	● Enabled ○ Disabled
Notes:	

5) In the Network Options tab, hit New (Remote) at the bottom of the screen.

6) Fill the data as show below and click Save.

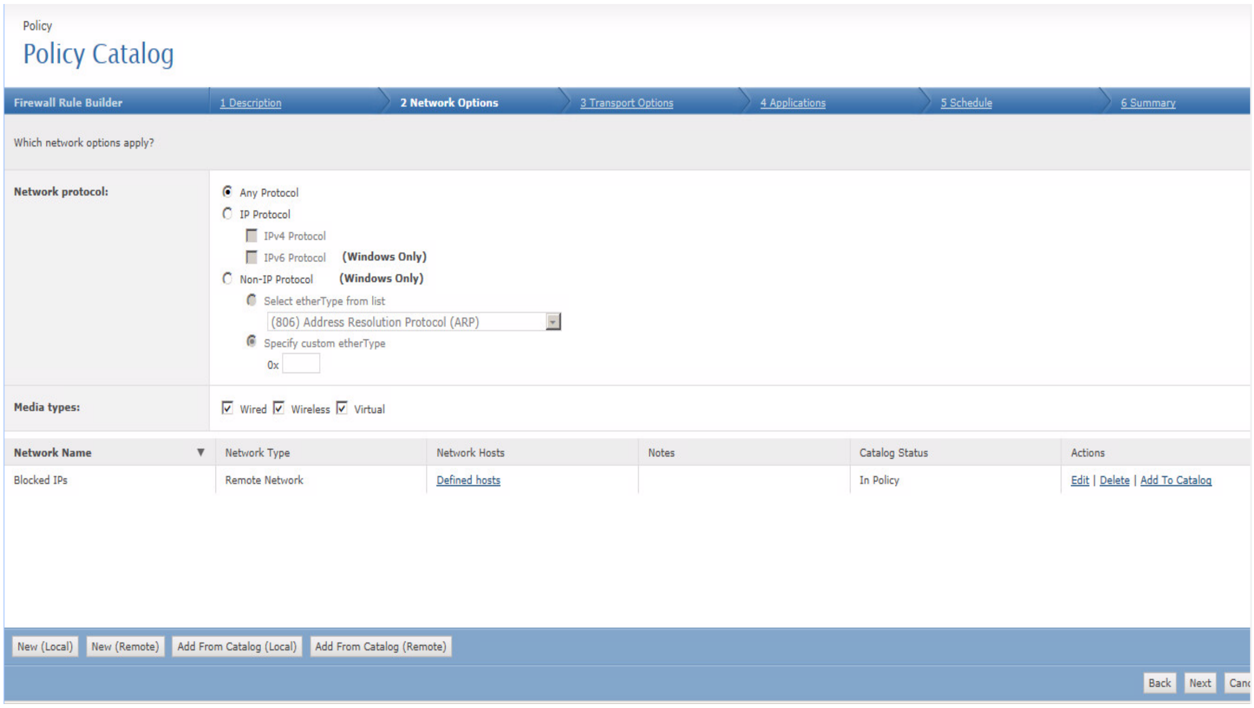

Policy

Policy Catalog

Network

Name:	Blocked IPs
IP addresses:	Range 192.168.2.6 192.168.2.15
Notes:	
Last modified:	By admin on Friday, July 22, 2016 2:33:54 PM

7) Your screen should look similar to the below. Click Next.



Policy

Policy Catalog

Firewall Rule Builder | 1 Description | 2 Network Options | 3 Transport Options | 4 Applications | 5 Schedule | 6 Summary

Which network options apply?

Network protocol:

● Any Protocol
○ IP Protocol
☐ IPv4 Protocol
☐ IPv6 Protocol **(Windows Only)**
○ Non-IP Protocol **(Windows Only)**
○ Select etherType from list
(806) Address Resolution Protocol (ARP)
○ Specify custom etherType
0x

Media types: ☑ Wired ☑ Wireless ☑ Virtual

Network Name	Network Type	Network Hosts	Notes	Catalog Status	Actions
Blocked IPs	Remote Network	Defined hosts		In Policy	Edit | Delete | Add To Catalog

8) Select "All Protocols" for the Transport protocol.

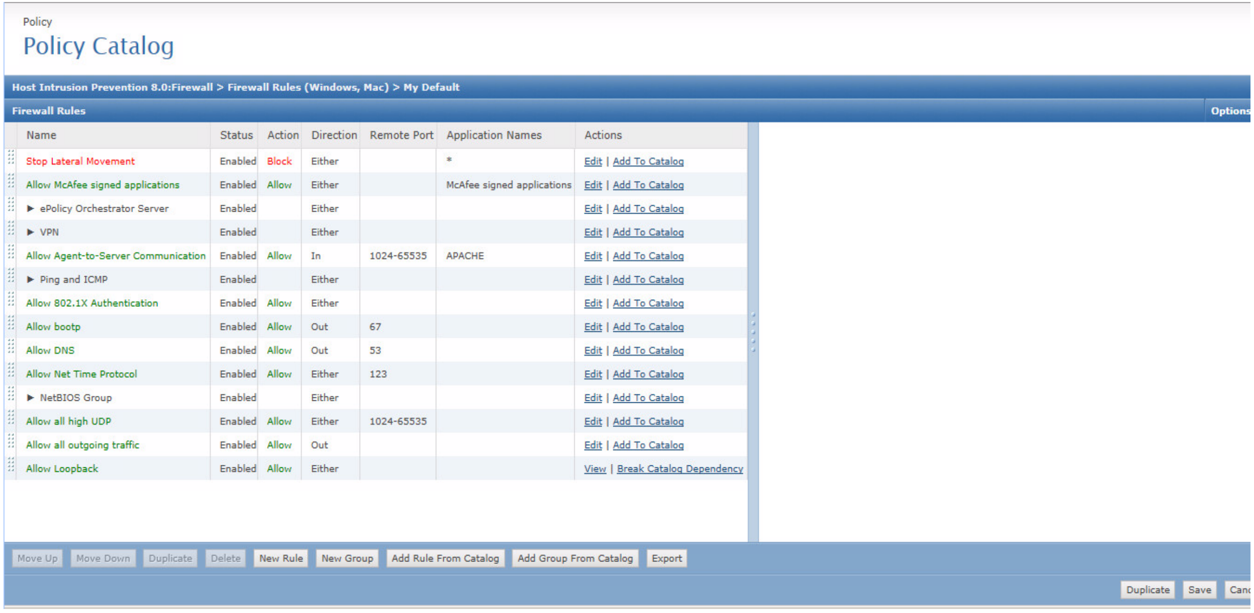
9) In the Applications tab, select New.

10) Input an "*" for the Name and select Save.

11) Click Next twice.

12) Click Save.

In the Firewall Rules window, click and drag the newly created rule to the stop as shown below.



Policy

Policy Catalog

Host Intrusion Prevention 8.0:Firewall > Firewall Rules (Windows, Mac) > My Default

Firewall Rules

Name	Status	Action	Direction	Remote Port	Application Names	Actions
Stop Lateral Movement	Enabled	Block	Either		*	Edit | Add To Catalog
Allow McAfee signed applications	Enabled	Allow	Either		McAfee signed applications	Edit | Add To Catalog
▶ ePolicy Orchestrator Server	Enabled		Either			Edit | Add To Catalog
▶ VPN	Enabled		Either			Edit | Add To Catalog
Allow Agent-to-Server Communication	Enabled	Allow	In	1024-65535	APACHE	Edit | Add To Catalog
▶ Ping and ICMP	Enabled		Either			Edit | Add To Catalog
Allow 802.1X Authentication	Enabled	Allow	Either			Edit | Add To Catalog
Allow bootp	Enabled	Allow	Out	67		Edit | Add To Catalog
Allow DNS	Enabled	Allow	Out	53		Edit | Add To Catalog
Allow Net Time Protocol	Enabled	Allow	Either	123		Edit | Add To Catalog
▶ NetBIOS Group	Enabled		Either			Edit | Add To Catalog
Allow all high UDP	Enabled	Allow	Either	1024-65535		Edit | Add To Catalog
Allow all outgoing traffic	Enabled	Allow	Out			Edit | Add To Catalog
Allow Loopback	Enabled	Allow	Either			View | Break Catalog Dependency

Obtaining executable information

To obtain executable information (including signer, description, and hash) for HIPs using the ClientControl.exe utility, use the below syntax.

Example:

```
C:\Program Files\McAfee\Host Intrusion Prevention> ClientControl.exe /execinfo "C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe"
```

The above command will return the following information:

```
Executable info for "C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe":
        Signer = CN="McAfee, Inc.", OU=IIS, OU=Digital ID Class 3 - Microsoft Software Validation v2,
          O="McAfee, Inc.", L=Santa Clara, S=California, C=US
        Description = McAfee HIP Main Service
        Hash = 0xD967D1F30641EA7A650B01CC7B22278C
```

Default Rules to Enable

By default the below rules are disabled. It is recommended that they be set to at least Low. It may also be a good idea to comb through the other pre-built rules within HIPS and adjust settings as necessary for the environment in which you operate in.

- 101 - Winlogon Registry Key Modification
- 102 - Winlogon Registry Value Modification
- 103 - LSA Registry Key Modification
- 132 - System Executable Creation or Deletion
- 338 - Automatic Logon at Startup Enabled
- 352 - Null User Sessions Enabled
- 354 - Drive AutoPlay Settings Modified
- 371 - Local IP Routing Enabled
- 399 - Remote Shell Service Installation
- 413 - Suspicious Double File Extension Execution
- 415 - Suspicious File Extension Execution
- 752 - Windows Explorer CLSID File Execution
- 797 - Unattended Installation File Illegal Access
- 801 - Anonymous User Name Lookup
- 803 - CD-ROM Autorun Enabled
- 814 - System File Modification
- 836 - SAM Config File Access
- 910 - Uninstall Registry Key Modification
- 949 - Null Session Access Enabled
- 950 - Null Session Access to Named Pipes Modified
- 951 - Null Session Access to Shares Modified
- 990 - New Startup Folder Program Creation
- 1148 - CMD Tool Access by a Network Aware Application

- 1150 - CMD Tool Access by FTP Client
- 1157 - USB Storage Device Inserted
- 2254 - Suspicious Process Invocation - Acrobat Reader
- 2804 - Opening Internet browser as Administrator
- 2806 - Attempt to create a hardlink to a file
- 2834 - Java - Creation of suspicious files in Temp folder
- 3917 - Windows File Share Creation
- 6032 - Suspicious Function Invocation - Target Address Mismatch
- 6047 - Illegal Execution - Writable Memory
- 6048 - Suspicious Function Invocation - Different Stack
- 6049 - Suspicious Function Invocation - No Module
- 6053 - Accessing other users home directory
- 6070 - Hidden PowerShell Detected
- 6073 - Execution Policy Bypass in Powershell

Excluding Tools

Excluding cyber defender tools is extremely important to ensure successful operations. To exclude tools in VSE, go to the following and make the necessary changes:

VirusScan Enterprise > On-Access Default/Low/High-Risk Processes Policies

- Exclusions
  - ➢ What not to scan - Put in any tools that the team will be using to ensure that they can run properly

To make specific tools trusted by HIPS, go to the following and make the necessary changes:

HIPS 8.0: General > Trusted Applications

- ➢ Place any cyber defender tools here so HIPS doesn't block them

Rogue System Detection (RSD)

Rogue System Detection (RSD) searches for system on the network that doesn’t have the McAfee Agent installed. This feature, when deployed, can help determine coverage gaps in the network. It can also illuminate rogue systems who may be used for malicious intent or simply somehow accidently made it on the network. Exceptions can set for systems that can’t have the McAfee Agent installed. For the systems that can have the agent installed, it can be installed right from the RSD window.

Supported Operating Systems

Rogue System Detection (RSD) can run on Windows XP, Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008.

Recommendations

If running DHCP in the network, the DHCP server is a great place to make a Rogue System Detection Sensor but you must enable DHCP Monitoring first (Detection tab of the policy). If DHCP is not being used, you must install at least one sensor per broadcast segment using static IP addresses. For more information, consult the McAfee product guide.

Configuring

1) Policy Catalog -> Rogue System Detection.

2) In the Name column look for McAfee Default and click Duplicate under the Actions column.

3) Give it a name and click Ok.

4) Under the name column, click on the newly created record.

5) The presented columns are depicted below

- General:
  - ➢ Rogue System Sensor - Enable of disable the policy.
  - ➢ Server name or IP address - IP of the ePO.
- Communication:
  - ➢ Sensor's detected system cache lifetime - Time a detected system remains in cache. The lower the number, the more times the same system gets reported.
  - ➢ Reporting time for active sensors - When active sensors report to the ePO.
  - ➢ Active sensor election - Method for choosing active sensors. If using the first option, how often inactive (passive) sensors communicate is set here.
- Interfaces:
  - ➢ Listen only on interface... - Subnets (or IPs) you want to monitor. This can also be added in Menu > System > Detected Systems > Subnet Status.
  - ➢ Do not listen on interfaces... - Subnets (or IPs) you don't want to monitor
- Detection:
  - ➢ DHCP monitoring - Enable if the sensor will be on a DHCP server. This will allow you to use one sensor and monitor on all subnets.

- ➢ Device details detection - Specifies what type of information the sensor should scan for. The sensor uses NetBIOS calls and OS fingerprinting to provide detailed information about devices on your network. You can also excludes subnets (or IPs) here.
- ➢ Report on self-configured networks - Disabled by default. Enabling this feature reports all subnets with a netmask of /32 (or /128 in IPv6). With Layer 2 detections, there may be a large number of erroneous 32-bit subnets appear in the subnet list. McAfee recommends this option only be enabled when using DHCP detection and not Layer 2 detection.

There are a few other settings that are configured at Menu > Server Settings and are as follows:

- Detected System Compliance - The percentage that depicts the red/green/amber statuses can be altered here, if needed.
- Detected System Exception Categories - Adding categories help group like systems together in order to ease the exception handling.
- Detected System Matching - Setting used to determine the detection of rogue systems. It is recommended to use MAC and hostname for this however; your environment ultimately dictates your configuration.
- Detected System OUIs - Authoritative source for depicting the type of NICs identified. IEEE's site is http://standards.ieee.org/regauth/oui/oui.txt however, you can use whatever source you would like.

- Rogue System Sensor - Setting to determine how sensors interact with each other and the ePO. Options available include the amount of time sensors are active, the maximum number of sensors active on each subnet, and how long the server waits to hear from a sensor before categorizing it as missing.

Sensor Installation

Note: All sensors must be managed systems with the McAfee Agent installed.

Rogue System Sensors can be installed on the following different types of systems:

- DHCP servers — this is the best place to install the Rogue System Sensors because DHCP servers are constantly monitoring multicast traffic and are instantly aware when a new system connects to a subnet.
- DNS servers or any system that is always connected to the subnet and monitoring traffic — these are good places to install Rogue System Sensors because these systems are not often turned off and are seldom disconnected from the network.

- All systems on a subnet — this allows you to configure Active sensor election in the Rogue System Detection policy. Once configured, all systems on a subnet periodically, according to configured settings, run an election algorithm to set some sensors as active and the remainder of the systems as passive.

The sensor can be installed using one of a few methods however; we will depict only one way. For the other methods, please consult the McAfee RSD product guide.

1) Navigate to the System Tree.
2) Place a checkmark next to the system(s) that you want to install the sensor on.
3) Click Actions > Rogue Sensor > Add or Remove Rogue Sensor.
4) Select the "Install RSD" option and click OK.
   Note: If needing to remove the sensor, select the "Remove RSD" option.

Utilizing the manual method of installing RSD, you shouldn't have to worry about the Rogue Sensor Blacklist but more details regarding it can be found in the McAfee RSD product guide. In short, the blacklist is a list of managed systems that you don't want the sensor installed on because it could adversely affect the system.

Dashboard

Viewing the detected systems can be done using the Detected Systems window or using a dashboard. McAfee ePO ships with default RSD dashboard however, in Annex A of this document, we have included a customized RSD dashboard that you can import into your ePO.

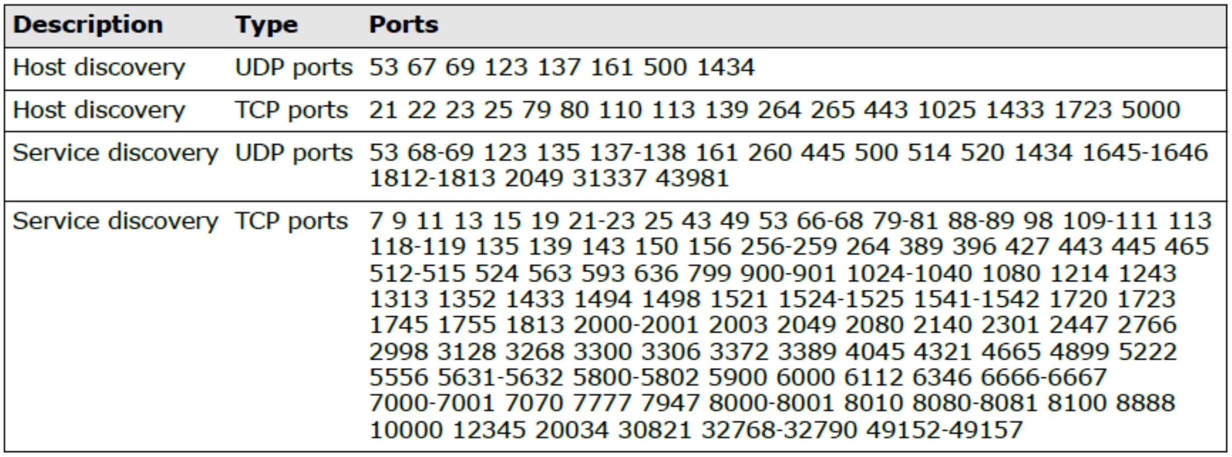
Detected Systems

To view rogue systems using the Detected Systems window, navigate to Menu > Systems > Detected Systems. Below is a breakdown of the presented widgets.

- Subnet Status - Lists the status of the covered subnets and additional subnets to monitor can be added here.
- Overall System Status - gives snapshot of complaint systems. Exceptions can be imported/exported here. They can also be added at Menu > Server Settings > Detected System Compliance.
- Rogue System Sensor Status - shows the health of the sensors. Blacklisted sensors are depicted here as well.
- Detected System Interfaces by Subnet - add systems to the exceptions list, install the McAfee Agent, or delete them if they no longer exist. If you click on the system, details about the system will be displayed.

Ports

RSD gathers information by actively listening to NETBIOS calls and OS fingerprinting. RSD utilizes the ports shown below. With that said, be cognizant of where RSD is installed because it may be somewhat alarming to see this many ports possibly in a listening state on a machine.



Description	Type	Ports
Host discovery	UDP ports	53 67 69 123 137 161 500 1434
Host discovery	TCP ports	21 22 23 25 79 80 110 113 139 264 265 443 1025 1433 1723 5000
Service discovery	UDP ports	53 68-69 123 135 137-138 161 260 445 500 514 520 1434 1645-1646 1812-1813 2049 31337 43981
Service discovery	TCP ports	7 9 11 13 15 19 21-23 25 43 49 53 66-68 79-81 88-89 98 109-111 113 118-119 135 139 143 150 156 256-259 264 389 396 427 443 445 465 512-515 524 563 593 636 799 900-901 1024-1040 1080 1214 1243 1313 1352 1433 1494 1498 1521 1524-1525 1541-1542 1720 1723 1745 1755 1813 2000-2001 2003 2049 2080 2140 2301 2447 2766 2998 3128 3268 3300 3306 3372 3389 4045 4321 4665 4899 5222 5556 5631-5632 5800-5802 5900 6000 6112 6346 6666-6667 7000-7001 7070 7777 7947 8000-8001 8010 8080-8081 8100 8888 10000 12345 20034 30821 32768-32790 49152-49157

Importing Dashboards and Queries

Importing Dashboards and Queries can be accomplished in one of a few ways. It really just depends on what you have been giving. For example, if you have been given a dashboard export, you can just import the dashboard and that will also import the queries associated with it as well. If you were given just an export of a query, you will need to import that first and then build drag the query onto a new or already established dashboard. Below are the instructions on importing dashboards (query included) and a query (dashboard built afterwards).

Import Dashboards (query included)

1) Click Dashboards.

2) Click Dashboard Actions.

3) Select Import.

4) Browse to the location of the saved Dashboard (.xml).

5) Click Ok and Ok.

6) You will then be presented with the imported dashboard on the screen.

7) Click Close near the category drop-down.

8) Lastly, click Save on the Dashboard menu board.

Note: The newly imported dashboard loads under Private Dashboards. You change the visibility after importing the dashboard by selecting Dashboard Actions -> Edit. If the dashboard stays in Private Dashboard only you, the person who imported it, will have access to it. The queries associated with this dashboard will import to root of Private Groups in the query menu. Query Private Groups are only visible by the owner while Query Public Groups are visible by anyone with query permissions. After importation, you can click and drag the query to another container of your choosing. Moving the query to another container will not affect its linkage.

Import Queries (then add to a dashboard)

1) Click Queries & Reports.

2) In the center pane at the bottom, click Actions -> Import Definitions.

3) Browse to the location of the .xml query.

4) Create a New Group to store the query in or select from existing groups. Note: Anything under Private Groups will only be accessible by the person who uploaded it.

5) Click Save

6) Queries are now imported.
1) Note: If you want to rename a query, checkmark the box to the left of the query name. Select Actions -> Duplicate.

7) Go to the dashboard that you want to import a query into or create a new dashboard.

8) Near the top center of the screen, select Add Monitor

9) Select Queries from the Category drop-down menu

10) Click and drag the Queries chart onto the Dashboard. When dragging, if the box is orange, that means the query will not fit in the current spot. Whenever the box is white, that means it will fit. If the screen is full, you can try to right side of the screen or the bottom of the screen.

11) From the screen that appears, you can select the query you want to import and the refresh interval.

12) Click Ok

13) The query will now appear on the dashboard.

2) Note: To rename the monitor on the dashboard, click the triangle to the left of the monitor name and select Edit.

Exporting Dashboards and Queries

Export Dashboard (query included)

1) Go to the Dashboard screen.

2) Select Dashboard Actions -> Export.

3) If you are doing this from IE, you can use the Save As option to set the file name. If you are doing this from Firefox, you will have to save the file and then rename it, if needed.

4) Verify the file has downloaded and its location.

5) Done!

Note: Any query that was associated with the exported dashboard was also exported as well and is in the downloaded .xml.

Export a Query

1) Go to the Query window.

2) Checkmark the queries you want to export.

3) Select Actions -> Export Definitions.

4) If you are doing this from IE, you can use the Save As option to set the file name. If you are doing this from Firefox, you will have to save the file and then rename it, if needed.

5) Done

Annex A: Custom Dashboards and Queries

Example Dashboards and Queries

On my Github (github.com/wiredpulse) are custom dashboards and queries that CW2(P) Chanel Bernal and myself made. They are a good baseline for pulling out the data within the ePO that you desire to see and could be customized to fit your needs.

Note: When importing any of the attached dashboards, the necessary queries will be imported as well.

Annex B: Custom VSE User-defined Rules

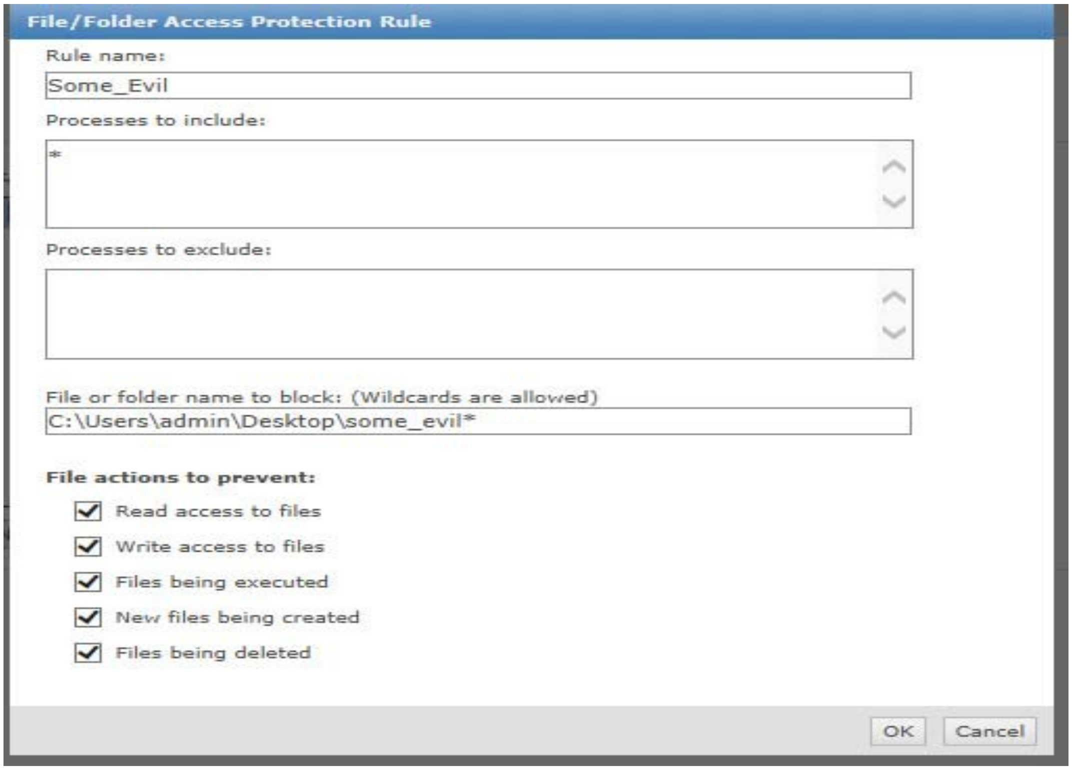
On top of McAfee's pre-defined list of rules in VSE, user-defined rules can also be implemented to further strengthen the defensive stance of the system. User-defined rules to have three main purposes which are:

- Prevent malicious code from running in the first place
- If malicious code is running, prevent it from spreading to other computers
- If malicious code is running, prevent a payload from damaging the local computer

The three purposes can be achieved using one of three options in the user-defined rules menu which are listed below with examples.

File/Folder Access

- ➢ Example rule: prevents read, write, execution, creation, or deletion of a file named some_evil*. The '*' is a wildcard for anything.



File/Folder Access Protection Rule

Rule name:
Some_Evil

Processes to include:
*

Processes to exclude:

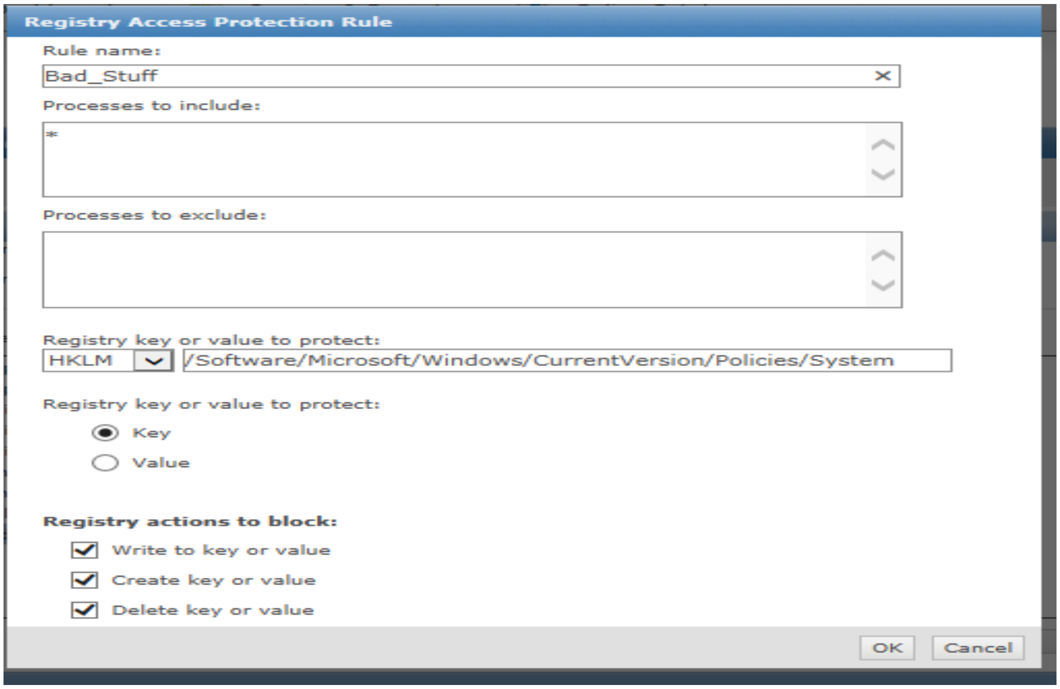
File or folder name to block: (Wildcards are allowed)
C:\Users\admin\Desktop\some_evil*

File actions to prevent:

☑ Read access to files
☑ Write access to files
☑ Files being executed
☑ New files being created
☑ Files being deleted

Registry Access

- Example rule: blocks the writing, creation, or deletion of any key within the System key. If we wanted to do monitor any entries within a key, we would use the value option.



Registry Access Protection Rule

Rule name:
Bad_Stuff

Processes to include:
*

Processes to exclude:

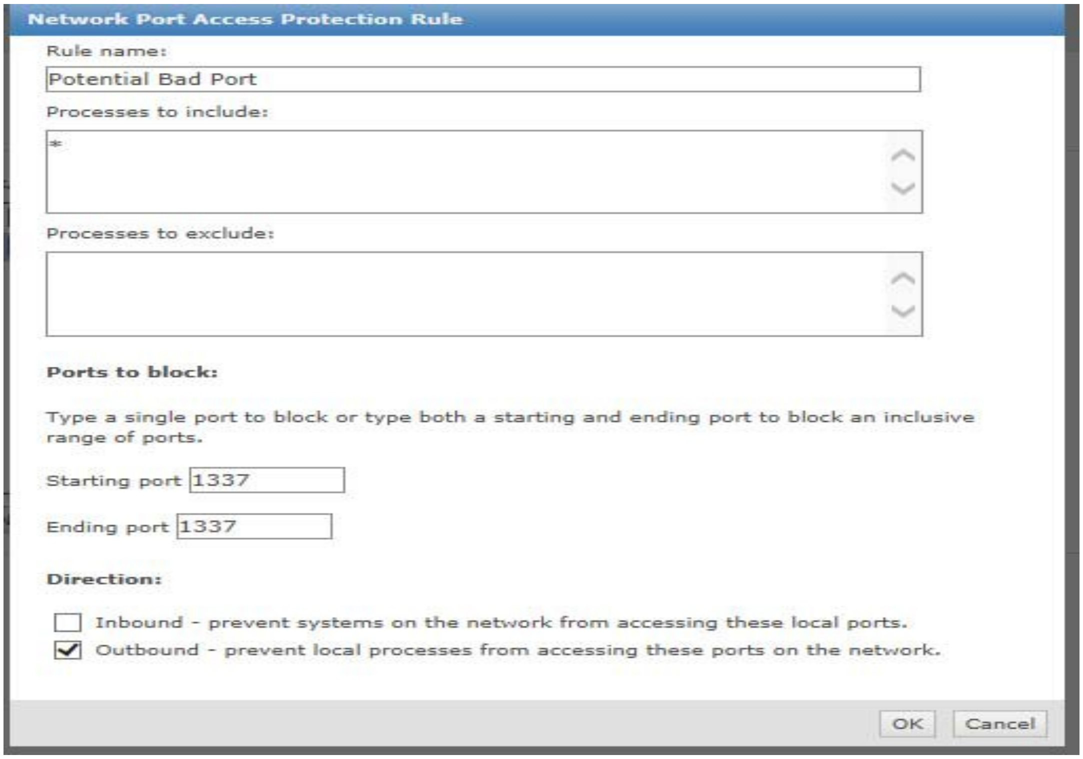
Registry key or value to protect:
HKLM /Software/Microsoft/Windows/CurrentVersion/Policies/System

Registry key or value to protect:
● Key
○ Value

Registry actions to block:
☑ Write to key or value
☑ Create key or value
☑ Delete key or value

Network Port Access

Example rule: blocking port 1337 from going outbound. We could also block range and/or inbound as well.



Network Port Access Protection Rule

Rule name: Potential Bad Port

Processes to include: *

Processes to exclude:

Ports to block:

Type a single port to block or type both a starting and ending port to block an inclusive range of ports.

Starting port 1337

Ending port 1337

Direction:

□ Inbound - prevent systems on the network from accessing these local ports.

☑ Outbound - prevent local processes from accessing these ports on the network.

More information regarding user-defined rules can be found at https://kc.mcafee.com/corporate/index?page=content&id=KB81095.

Annex C: Custom HIPS Rules

Building Expert Subrules

Located on my Github at (www.github.com/wiredpulse) are some HIPS Expert Subrules that can be tweake for your use. The McAfee EPO product guide located here also addresses making custom Expert Rules beginning at page 101.

Dump McAfee Rules

You can also see how McAfee made their default rules by dumping the FireSvc process in task manager on an endpoint that has HIPS running. Once dumped, open it with something that can handle big files like vim or notepad ++ and take a gander. This will allow you to better write custom rules by getting a view at the ones they have already written. To dump the process, do the following.

1) Open Task Manager
2) Select the Process tab
3) Place a checkmark next to "Show processes from all users"
4) Right-click FireSvc.exe and select "Create Dump File"

Rule Severity Levels

For each rule there is a severity level, below are there meaning. Please be aware that when configuring a new rule, there are severity levels listed. Those severity levels have no play when we are using Expert Subrules and are for Standard Subrules. Therefore, you must set the severity in the rule itself.

- level 4 = High (Critical)
- Level 3 = Medium (Warning)
- Level 2 = Low (Notice)
- Level 1 = Informational (Information)

Annex D: Event IDs

Below are a list of HIPS and ePO Event IDs. The list will help you in building queries to search for the data you desire. It is also worth mentioning that not all Event IDs that are generated on a client system will be sent back to the ePO. To get a list of those that will and to add/remove others, you can do so by going to Menu > Server Settings > Event Filtering.

HIPS Events

Event ID	**Description**
18000	Host intrusion detected and handled
18001	Network intrusion detected and handled
18002	Application blocked
18003	Failed Quarantine check (Trusted Source Block)
18006	Timed Group Enabled / Expired (see the second bullet in the following Notes)
18007	Policy Load Status

18999	The IPS Event table is full. Further events will be ignored until events are archived.

NOTE: Firewall blocking events are not sent back to the ePO because of excessive bandwidth use.

ePO Events

Event ID	Name	Severity
1000	NetShield service started successfully	Informational
1001	NetShield service ended successfully	Informational
1002	Task started successfully	Informational
1003	Error starting Task	Informational
1004	Task has completed successfully	Informational

1005	Error while stopping task	Informational
1024	Infected file found	Critical
1025	Infected file successfully Cleaned	Major
1026	Unable to clean infected file	Critical
1027	Infected file deleted	Major
1028	Unable to delete infected file	Critical
1029	File to be excluded from scans	Informational
1030	Unable to exclude item from scans	Critical
1031	Infected file access denied	Major
1032	Infected file was moved to quarantine area	Major
1033	Unable to move infected file to quarantine	Critical
1034	Scan completed. No viruses found	Informational
1035	Scan was cancelled	Informational
1036	Memory infected	Critical
1037	Infected boot record found	Critical
1038	Scan found infected files	Critical
1039	Scan found and cleaned infected files	Major
1040	Activity Log error	Informational
1041	Scan reports memory allocation error	Informational
1042	Path too long	Warning
1043	Media is write protected	Informational
1044	Specified media not found	Informational
1045	Specified scan item is invalid	Informational
1046	File I/O errors	Informational
1047	Disk I/O errors	Informational
1048	Scan reports general system error	Informational

1049	Scan reported an internal application error	Informational
1050	Unable to repair password protected	Major
1051	Unable to scan password protected	Major
1052	Infected Binder Object	Critical
1053	Infected file found	Critical
1054	Infected file deleted	Major
1055	Unable to delete infected file	Critical
1056	File moved to quarantine	Major
1057	Unable to move infected file to quarantine	Critical
1059	Scan Timed Out	Major
1060	Boot sector virus was cleaned	Major
1061	Error while cleaning boot sector virus	Critical
1062	Error sending alert	Informational
1063	Invalid options specified	Informational
1064	Service was started	Informational
1065	Service ended	Informational
1066	Task started ok	Informational
1067	Unable to start scheduled task	Warning
1068	Scheduled task was stopped	Informational
1069	Error stopping scheduled task	Warning
1070	Task was successful	Informational
1071	Task was cancelled	Warning
1076	Error logging information	Informational
1077	Memory allocation error	Informational
1086	Scan Process Error	Critical
1087	On-access Scan started	Informational

1088	On-access scan stopped	Informational
1089	Scan Settings	Informational
1090	OAS stopped	Warning
1091	JavaScript security violation detected and blocked	Major
1092	Access Protection rule violation detected and blocked	Minor
1093	Buffer Overflow detected; Blocked successfully	Critical
1094	Port blocking rule violation detected	Minor
1095	Access Protection rule violation detected and NOT blocked	Minor
1099	Buffer Overflow detected and NOT blocked	Critical
1100	Macro Detected in file	Minor
1101	Macro Deleted from file	Minor
1118	The update was successful	Informational
1119	The update failed; see event log	Warning
1120	The update is running	Informational
1121	The update was cancelled	Warning
1122	The upgrade is running	Informational
1123	The upgrade failed; see event log	Major
1124	The upgrade was cancelled	Informational
1125	The DAT version was not new enough	Informational
1126	Scan was cancelled by AutoUpdate of DAT files	Warning
1127	OAS Scanning Engine Disabled	Warning
1128	Scan time exceeded	Warning
1129	Scan shut down by Windows	Warning
1200	Process started	Informational
1201	Process Ended	Informational
1202	On-demand scan started	Informational

1203	On Demand scan complete	Informational
1204	Report OS & Serial	Informational
1270	file infected. No cleaner available, quarantined successfully	Major
1271	file infected. No cleaner available, heuristic detection, quarantined successfully	Major
1272	file infected. Undetermined clean error, quarantined successfully	Major
1273	file infected. Clean error, Encrypted file, quarantined successfully	Major
1274	file infected. No cleaner available, quarantine failed	Critical
1275	file infected. No cleaner available, heuristic detection, quarantine failed	Critical
1276	file infected. Undetermined clean error, quarantine failed	Critical
1277	file infected. Clean error, Encrypted file, quarantine failed	Critical
1278	file infected. No cleaner available, file deleted successfully	Major
1279	file infected. No cleaner available, heuristic detection, deleted successfully	Major
1280	file infected. Undetermined clean error, deleted successfully	Major
1281	file infected. Clean error, Encrypted file, deleted successfully	Major
1282	file infected. No cleaner available, delete failed	Critical
1283	file infected. Clean error, heuristic detection, delete failed	Critical
1284	file infected. Undetermined clean error, delete failed	Critical
1285	file infected. Clean error, Encrypted file, delete failed	Critical
1286	file infected. No cleaner available, continued scanning (ODS)	Critical
1287	file infected. Clean error, heuristic detection, continued scanning (ODS)	Critical
1288	file infected. Undetermined clean error, continued scanning (ODS)	Critical
1289	file infected. Clean error, Encrypted file, continued scanning (ODS)	Critical
1290	file infected. No cleaner available, OAS denied access and continued	Critical

1291	file infected. Clean error, heuristic detection, OAS denied access and continued	Critical
1292	file infected. Undetermined clean error, OAS denied access and continued	Critical
1293	file infected. Quarantine failed, deleted successfully	Major
1294	file infected. Quarantine failed, delete failed	Critical
1295	file infected. Move failed, continued scanning (ODS)	Critical
1296	file infected. Move failed, denied access and continued (OAS)	Critical
1297	file infected. Delete failed, quarantined	Major
1298	file infected. Delete failed, quarantine failed	Critical
1299	file infected. Delete failed, continued scanning (ODS)	Critical
1300	file infected. Delete failed, denied access and continued (OAS)	Critical
1500	Infected email cleaned	Major
1501	Infected email quarantined	Minor
1502	Unable to clean infected mail	Critical
1503	Infected email detected	Major
1504	Infected mail item deleted	Critical
1505	Email content filtered	Warning
1506	Email content blocked	Warning
1507	Inbound email suspend for low disk	Minor
1508	Inbound Mail Resumed	Warning
1509	Startup request successfully processed	Informational
1510	Shutdown request successfully processed	Informational
1511	Warning - abnormal termination!	Minor
1512	A maximum load condition is occurring!	Major
1513	Mail virus quarantined and cleaned	Minor
1514	Mail virus quarantined (not cleaned)	Critical

1515	Infected email has had virus replaced	Major
1700	GroupShield Exchange - service started successfully	Informational
1701	GroupShield Exchange - service ended successfully	Informational
1702	GroupShield Exchange - File copy has been blocked	Minor
1703	GroupShield Exchange - Message is infected	Major
1704	GroupShield Exchange - Message blocked	Minor
1705	GroupShield Exchange - Infected file found	Major
1706	GroupShield Exchange - Infected file successfully cleaned	Minor
1707	GroupShield Exchange - Infected file was moved to quarantine area	Minor
1708	GroupShield Exchange - Scheduled Once Scan Started	Informational
1709	GroupShield Exchange - Scheduled Repeat Event Scan Started	Informational
1710	GroupShield Exchange - Scheduled Scan Finished	Informational
1711	GroupShield Exchange - Scheduled Scan Failed To Start	Major
1712	GroupShield Exchange - Internal Error occurred	Major
1713	GroupShield Exchange - On-Demand Scan Started	Informational
1714	GroupShield Exchange - On-Demand Scan Finished	Informational
1715	GroupShield Exchange - AV Engine has been stopped	Informational
1716	GroupShield Exchange - AV Engine has been started	Informational
1717	GroupShield Exchange - An update Failed	Major
1718	GroupShield Exchange - An update has started	Informational
1719	GroupShield Exchange - No update is available	Warning
1720	GroupShield Exchange - An update was successful	Informational
1721	GroupShield Exchange - Disk space is low	Major
1722	GroupShield Exchange - Infected file	Major
1725	GroupShield Exchange - Nearly end of designed life	Informational
1726	GroupShield Exchange - End of designed life reached	Informational

1750	GroupShield Exchange - Packer	Informational
1751	GroupShield Exchange - Phish detection	Informational
1752	GroupShield Exchange - Scanner control filtering	Informational
1753	GroupShield Exchange - Signed mail (digital signature)	Informational
1754	GroupShield Exchange - Encrypted content is found in the mail	Informational
1755	GroupShield Exchange - Content is found to be corrupted	Informational
1756	GroupShield Exchange - DOS attack - Multiple Nesting Level, Max Expanded File Size & Max Scan Time	Informational
1757	GroupShield Exchange - A password set on an attachment	Informational
1758	GroupShield Exchange - The attachment is an archive or zip file that is password protected	Informational
1759	GroupShield Exchange - There is partial mime content or some external content	Informational
1760	GroupShield Exchange - Statistical event	Informational
1800	GroupShield Domino: Task started successfully	Informational
1801	GroupShield Domino: Error starting task	Warning
1802	GroupShield Domino: Task has completed	Warning
1803	GroupShield Domino: Error while stopping task	Warning
1804	GroupShield Domino: File virus found and cleaned	Warning
1805	GroupShield Domino: Infected file successfully quarantined	Warning
1806	GroupShield Domino: Infected file deleted	Warning
1807	GroupShield Domino Infected file ignored	Warning
1808	GroupShield Domino Quarantined a Lotus Script Exception	Warning
1809	GroupShield Domino Lotus Script Exception found and ignored	Warning
1810	GroupShield Domino Quarantined a Formula Exception	Warning
1811	GroupShield Domino Formula Exception found and ignored	Warning
1812	GroupShield Domino Quarantined a Content Exception	Warning

1813	GroupShield Domino Content Exception found and ignored	Warning
1814	GroupShield Domino Unable to read configuration database	Warning
1815	GroupShield Domino Unable to write to configuration database	Warning
1816	GroupShield Domino AutoGO update unable to restart task	Warning
1817	GroupShield Domino AutoGO update failed	Warning
1818	GroupShield for Lotus Domino: Attachments Blocked	Warning
1850	GroupShield Domino - Packer detected	Informational
1851	GroupShield Domino - Phish detection	Informational
1852	GroupShield Domino - Scanner control filtering	Informational
1853	GroupShield Domino - Signed mail (digital signature)	Informational
1854	GroupShield Domino - Encrypted content is found in the mail	Informational
1855	GroupShield Domino - Content is found to be corrupted	Informational
1856	GroupShield Domino - DOS attack - Multiple Nesting Level, Max Expanded File Size & Max Scan Time	Informational
1857	GroupShield Domino - A password set on an attachment	Informational
1858	GroupShield Domino - The attachment is an archive or zip file that is password protected	Informational
1859	GroupShield Domino - There is partial mime content or some external content	Informational
1860	GroupShield Domino - Statistical event	Informational
1900	New MIB File Available	Informational
2000	Infected file found	Critical
2001	Infected file successfully cleaned	Critical
2002	Unable to clean infected file	Critical
2003	Infected file deleted	Critical
2004	Unable to delete infected file	Critical
2005	File to be excluded from scans	Informational

2006	Unable to exclude item from scans	Informational
2007	Infected file access denied	Critical
2008	Infected file was moved to quarantine area	Critical
2009	Unable to move infected file to quarantine	Critical
2010	Centralized Alerting - Infected file found	Critical
2011	Centralized Alerting - Infected file successfully cleaned	Critical
2012	Centralized Alerting - Unable to clean infected file	Critical
2013	Centralized Alerting - Infected file deleted	Critical
2014	Centralized Alerting - Unable to delete infected file	Critical
2015	Centralized Alerting - File to be excluded from scans	Informational
2016	Centralized Alerting - Unable to exclude item from scans	Informational
2017	Centralized Alerting -	Critical
2018	Centralized Alerting - Infected file was moved to quarantine area	Critical
2019	Centralized Alerting - Unable to move infected file to quarantine	Critical
2020	Boot record infection found	Critical
2021	Boot record infection cleaned	Critical
2022	Boot record infection clean error	Critical
2023	New File Virus Found	Critical
2024	New File Virus Found And Deleted	Critical
2025	New File Virus Found But Move Failed	Critical
2026	New File Virus Found And Moved	Critical
2027	New File Virus Found But Move Failed	Critical
2028	MBR Virus Found	Critical
2100	Outbreak Rule Name	Critical
2201	ePOlicy Orchestrator Agent: Failed to install software package	Warning
2202	ePOlicy Orchestrator Agent: Install retry limit reached for software package	Warning

2204	ePOlicy Orchestrator Agent: Insufficient disk space to install software	Warning
2208	ePOlicy Orchestrator Agent: Insufficient disk space to download software	Warning
2216	ePOlicy Orchestrator Agent: Cannot install software due to OS version mismatch	Warning
2232	ePOlicy Orchestrator Agent: Enforce Policy Failed	Warning
2264	ePOlicy Orchestrator Agent: Property Collection Failed	Warning
2328	ePOlicy Orchestrator Agent: Enforce Task Failed	Warning
2401	Update Successful	Critical
2402	Update Failed	Critical
2411	Deployment Successful	Critical
2412	Deployment Failed	Critical
2413	Attempt to uninstall ePOlicy Orchestrator Agent	Major
3000	Scan task completed. No viruses found	Informational
3001	Task was cancelled	Informational
3002	Virus found in Memory	Critical
3003	Infected boot record found	Informational
3004	Task found infected files	Critical
3005	Task found and cleaned infected files	Critical
3006	Task error while accessing activity log file	Warning
3007	Task reports memory allocation error	Warning
3008	Directory length access error	Warning
3009	Media is write protected	Warning
3010	Specified media not found	Warning
3011	Specified scan item is invalid	Warning
3012	File I/O errors	Warning

3013	Disk I/O errors	Warning
3014	Task reports general system error	Critical
3015	Task reported an internal application error	Critical
3016	Error opening Service Manager	Warning
3017	Error starting drivers	Critical
3018	Error occurred starting log subsystem	Warning
3019	Error obtaining device driver versions	Warning
3020	Invalid virus signature files	Critical
3021	Scan engine error	Critical
3022	Initialization error with scan buffer	Warning
3023	Memory allocation error	Warning
3024	Unknown error reported	Warning
3025	Error sending new options to device driver	Warning
3026	Error sending exclude information to the driver	Warning
3027	Error sending move to folder to the driver	Warning
3028	Error obtaining log data from device driver	Warning
3029	Error occurred while enabling driver	Warning
3030	Error occurred while disabling driver	Warning
3031	Error while obtaining statistical data from driver	Warning
3032	Error while trying to open/create activity log file	Warning
3033	Activity log file maximum size reached	Warning
3034	Unable to write the activity log file	Warning
3035	Error launching a program upon virus infection	Warning
3036	Error during initialization of the activity log file	Warning
3037	Memory grant unavailable	Warning
3038	Error writing to log	Warning

3039	Centralized Alerting - Scan completed. No viruses found	Informational
3040	Centralized Alerting - Scan was cancelled	Informational
3041	Centralized Alerting - Virus found in Memory	Critical
3042	Centralized Alerting - Infected boot record found	Critical
3043	Centralized Alerting - Scan found infected files	Critical
3044	Centralized Alerting - Scan found and cleaned infected files	Critical
3045	Centralized Alerting - Error while accessing activity log file	Warning
3046	Centralized Alerting - Scan reports memory allocation error	Warning
3047	Centralized Alerting - Directory length access error	Warning
3048	Centralized Alerting - Media is write protected	Warning
3049	Centralized Alerting - Specified media not found	Warning
3050	Centralized Alerting - Specified scan item is invalid	Warning
3051	Centralized Alerting - File I/O errors	Warning
3052	Centralized Alerting - Disk I/O errors	Warning
3053	Centralized Alerting - Scan reports general system error	Critical
3054	Centralized Alerting - Scan reported an internal application error	Critical
3055	Error stopping drivers	Critical
4600	WebShield - URL Blocked	Critical
4650	Detected Spam Email	Critical
4651	Spam Email Scanning Statistics	Informational
4700	Failed to connect to CMA updater	Informational
4701	Failed to connect to CMA scheduler	Informational
4702	Failed to save schedule data into CMA	Informational
8000	Infected item found	Critical
8500	Banned item found	Critical
8501	Encrypted/Corrupted item found	Critical

8502	Item matched filtering criteria	Critical
8503	Item matched spam criteria	Critical
8601	Security for Exchange - McAfee Global Threat Intelligence file reputation failed	Critical
8602	Security for Exchange - Failed to download DATs/Anti-Virus Engine	Critical
8603	Security for Exchange - Insufficient disk space at the database location	Critical
8604	Security for Exchange - Failed to load Anti-Virus Engine	Critical
8605	Security for Exchange - On-demand Scan task failed	Critical
8606	Security for Exchange - Failed to quarantine or log detections	Critical
8607	Security for Exchange - Process RPCServ.exe failed to recreate	Critical
8608	Security for Exchange - Failed to download Anti-Spam Rules	Critical
8621	Security for Exchange - Failed to load VSAPIScanSource module	Critical
8622	Security for Exchange - Failed to load TransportScan module	Critical
8623	Security for Exchange - Postgres process stopped responding	Critical
8624	Security for Exchange - RPCServ process stopped responding	Critical
8625	Security for Exchange - Failed to load DLLhost	Critical
8626	Security for Exchange - Product Service failed to start	Critical
10016	scan started	Informational
10017	scan finished	Informational
10018	Informational Event	Informational
10029	scan host started	Informational
10030	scan host finished	Informational
10031	module results	Informational
10032	probe start	Informational
10033	probe stop	Informational

10034	Informational Event	Informational
10046	probe results header	Informational
10047	probe hop	Informational
10048	update start	Informational
10049	update stop	Informational
10050	Informational Event	Informational
10061	update results header	Informational
10062	update download file	Informational
10063	update installfile	Informational
10064	crack started	Informational
10065	crack finished	Informational
10066	Informational Event	Informational
10080	grind start	Informational
10081	grind stop	Informational
10082	Informational Event	Informational
10094	smb grind status	Informational
10095	smb grind result	Informational
10096	sentry started	Informational
10097	sentry finished	Informational
10098	Informational Event	Informational
10110	sentry results verbose	Informational
10111	sentry results non-verbose	Informational
10112	IDS start	Informational
10113	IDS stop	Informational
10114	Informational Event	Informational
10127	IDS testing text	Informational

10128	Upgrade start	Informational
10129	Upgrade stop	Informational
10130	Informational Event	Informational
10143	upgrade results	Informational
10144	AutoDiscovery start	Informational
10145	AutoDiscovery stop	Informational
10157	AutoDiscovery host started	Informational
10158	AutoDiscovery host finished	Informational
10159	AutoDiscovery results	Warning
10160	ThreatScan start	Informational
10161	ThreatScan stop	Informational
10173	ThreatScan host started	Informational
10174	ThreatScan host finished	Informational
10175	ThreatScan results	Warning
10176	Audit start	Informational
10177	Audit stop	Informational
10189	Audit host started	Informational
10190	Audit host finished	Informational
10191	Audit results	Warning
11001	Intrusion detected (DTFW 7.5.x) or application blocked (DTFW 8.x)	Major
11002	Failed Quarantine check	Minor
12000	Rogue System Sensor started successfully	Informational
12001	Rogue System Sensor failed to start	Major
12002	Rogue System Sensor stopped	Informational
13001	The machine is compliant or non-compliant with rules	Informational
13002	System Compliance Profiler rule violation	Major

14000	Entercept IPS Security Event	Critical
14500	Entercept Firewall Event	Critical
16000	Computers are non-compliant	Informational
16001	Reserved for future use	Informational
16002	Master Repository Update succeeded	Informational
16003	Master Repository Update failed	Informational
16004	Distributed Repository Replication succeeded	Informational
16005	Distributed Repository Replication failed	Informational
16006	New Rogue System detected	Informational
16007	Subnet has become unmonitored by Rogue System Sensor	Informational
16008	Active Directory Discovery task ran successfully	Informational
16009	Active Directory Discovery task failed	Informational
16012	Active Directory Discovery task added computers	Informational
16013	Active Directory Discovery task removed computers	Informational
21024	Unwanted program found	Major
21025	Unwanted program successfully cleaned	Major
21026	Unable to clean unwanted program	Critical
21027	Unwanted program deleted	Major
21028	Unable to delete unwanted program	Critical
21031	Unwanted program access denied	Major
21032	Unwanted program was moved to quarantine area	Major
21033	Unable to move unwanted program to quarantine	Critical
21036	Unwanted program found in memory	Critical
21054	Unwanted program deleted	Major
21055	Unable to delete unwanted program	Critical
21056	Unwanted program moved to quarantine	Major

21057	Unable to move unwanted program to quarantine	Critical
21270	Unwanted program quarantined-no cleaner	Major
21271	Unwanted program quarantined, Heuristics	Major
21272	Unwanted program quarantined, can't clean	Major
21273	Unwanted program quarantined, encrypted	Major
21274	Unwanted program not cleaned or quarantined	Critical
21275	Unwanted program, heuristics, quarantine failed	Critical
21276	Unwanted program, clean error, quarantine failed	Critical
21277	Unwanted program, encrypted, quarantine failed	Critical
21278	Unwanted program, no cleaner, deleted	Major
21279	Unwanted program, heuristics, no cleaner, deleted	Major
21280	Unwanted program, clean error, deleted	Major
21281	Unwanted program, encrypted, deleted	Major
21282	Unwanted program, no cleaner, delete failed	Critical
21283	Unwanted program, heuristics, delete failed	Critical
21284	Unwanted program, clean error, delete failed	Critical
21285	Unwanted program, encrypted, delete failed	Critical
21286	Unwanted program, no cleaner, continued	Critical
21287	Unwanted program, heuristics, continued	Critical
21288	Unwanted program, clean error, continued	Critical
21289	Unwanted program, encrypted, continued	Critical
21290	Unwanted program, no cleaner, denied access	Critical
21291	Unwanted program, heuristics, denied access	Critical
21292	Unwanted program, clean error, denied access	Critical
21293	Unwanted program, quarantine failed, deleted	Major
21294	Unwanted program, quarantine failed, delete failed	Critical

21295	Unwanted program, quarantine failed, continued	Critical
21296	Unwanted program, quarantine failed, denied access	Critical
21297	Unwanted program, delete failed, quarantined	Major
21298	Unwanted program, delete failed, quarantine failed	Critical
21299	Unwanted program, delete failed, continued	Critical
21300	Unwanted program, delete failed, denied access	Critical
21400	User-specified unwanted program found	Major
21401	User-specified unwanted program, clean error, continued	Critical
21402	User-specified unwanted program, clean error, quarantine failed	Critical
21403	User-specified unwanted program, clean error, quarantined	Major
21404	User-specified unwanted program, clean error, delete failed	Critical
21405	User-specified unwanted program, clean error, deleted	Major
21406	User-specified unwanted program was moved to quarantine area	Major
21407	User-specified unwanted program, quarantine failed, delete failed	Critical
21408	User-specified unwanted program, quarantine failed, deleted	Major
21409	User-specified unwanted program, quarantine failed, continued	Critical
21410	User-specified unwanted program deleted	Major
21411	User-specified unwanted program, delete failed, quarantine failed	Critical
21412	User-specified unwanted program, delete failed, quarantined	Major
21413	User-specified unwanted program, delete failed, continued	Critical
30000	Intrusion detected (firewall rule)	Critical
34150	Security for Microsoft Exchange - Packer detected	Informational
34151	Security for Microsoft Exchange - Phish detected	Informational
34152	Security for Microsoft Exchange - Mail size filter rule triggered	Informational
34153	Security for Microsoft Exchange - Signed content detected	Informational
34154	Security for Microsoft Exchange - Encrypted content detected	Informational

34155	Security for Microsoft Exchange - Corrupted content detected	Informational
34156	Security for Microsoft Exchange - Denial of service triggered	Informational
34157	Security for Microsoft Exchange - Protected content triggered	Informational
34158	Security for Microsoft Exchange - Password protected content detected	Informational
34159	Security for Microsoft Exchange - Blocked mime type detected	Informational
34160	Security for Microsoft Exchange - statistics and average scan time	Informational