Netsurion | EventTracker®

Integrate Comodo Endpoint Protection

EventTracker v9.2 and later

Publication Date: December 28, 2020

Abstract

This guide provides instructions to retrieve the **Comodo Endpoint Protection** events. Once **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor **Comodo Endpoint Protection**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Comodo Endpoint Protection.**

Audience

Administrators who are assigned the task to monitor **Comodo Endpoint Protection** events using EventTracker.

Table of Contents

1. Introduction

Comodo Endpoint Protection (EP) is a powerful event analysis tool that provides real-time monitoring and detection of malicious events on Windows endpoints. Endpoint Protection allows you to view the threats in a detailed timeline while instantly alerts about an attack.

Comodo Endpoint protection agent writes events automatically on Windows event viewer. EventTracker agent picks logs and sends to EventTracker. Comodo sends events like antivirus scan, HIPS, HIDS, containment, file rating, autorun, and configuration changes. Generates reports on potentially unwanted applications, antivirus scan detail, file rating, intrusion activities, configuration changes on Endpoint, alerts, threats detected, and unwanted files removed, etc. It contains username, client IP address, status, action, file path, file name, and hash. Graphically displays threat detected by file name, device name, device IP, file management Intrusion detected by filename, etc.

2. Prerequisites

- Comodo Endpoint Manager should be installed.
- Administrative access on Comodo EP Console.
- EventTracker agent should be installed on the system where comodo agent is installed.

Note: Comodo Endpoint Protection cloud platform send logs using syslog if EventTracker have the public IP address.

3. Configuring Comodo Endpoint Protection logging

Configuring Syslog Message Forwarding for windows:

1. Log in to Comodo Endpoint Agent console.
2. Click **Settings > General Settings > Logging**.

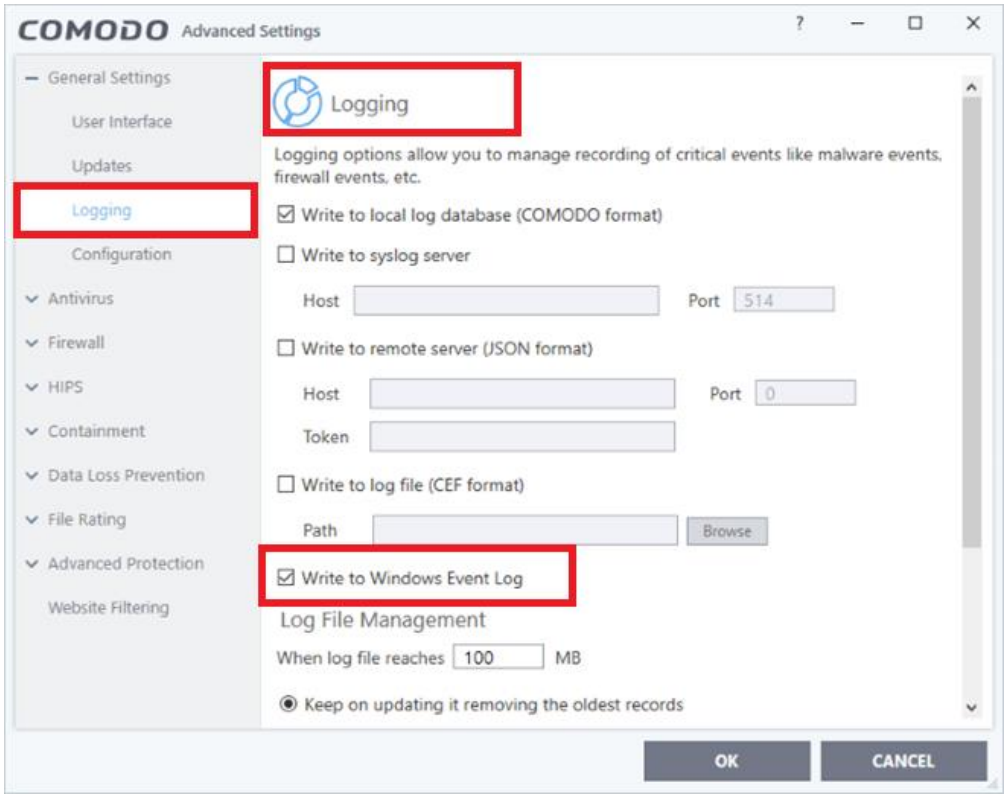

Figure 1

3. Enable **Write to Windows Event Log**. (Default = Enabled)
4. Click **OK.**

Configuring Syslog Message Forwarding for Linux and Mac:

Method 1

1. Log in to Comodo Endpoint Agent console.
2. Click **Settings** > **General Settings** > **Logging**. (as shown in Figure1).
   - Enable **Write to Syslog server**.
   - Enter **EventTracker manager IP** in Host.

Method 2

1. Log in to Comodo Cloud Platform from the admin account.
2. Click **Application** > **Endpoint Protection.**

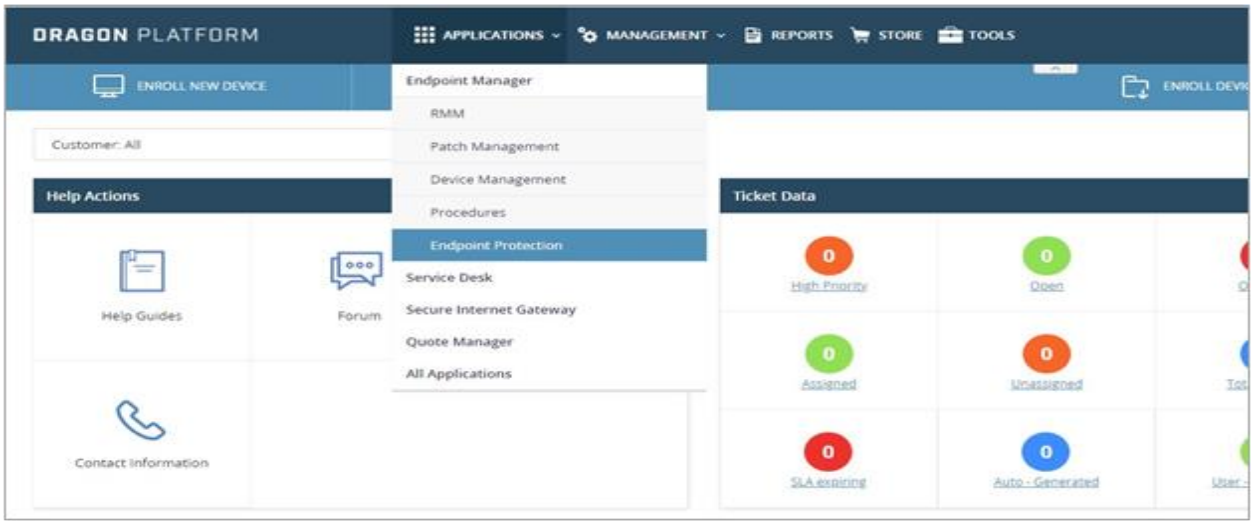

Figure 2

3. From the sidebar, click **Configuration Template** > **Profiles.**

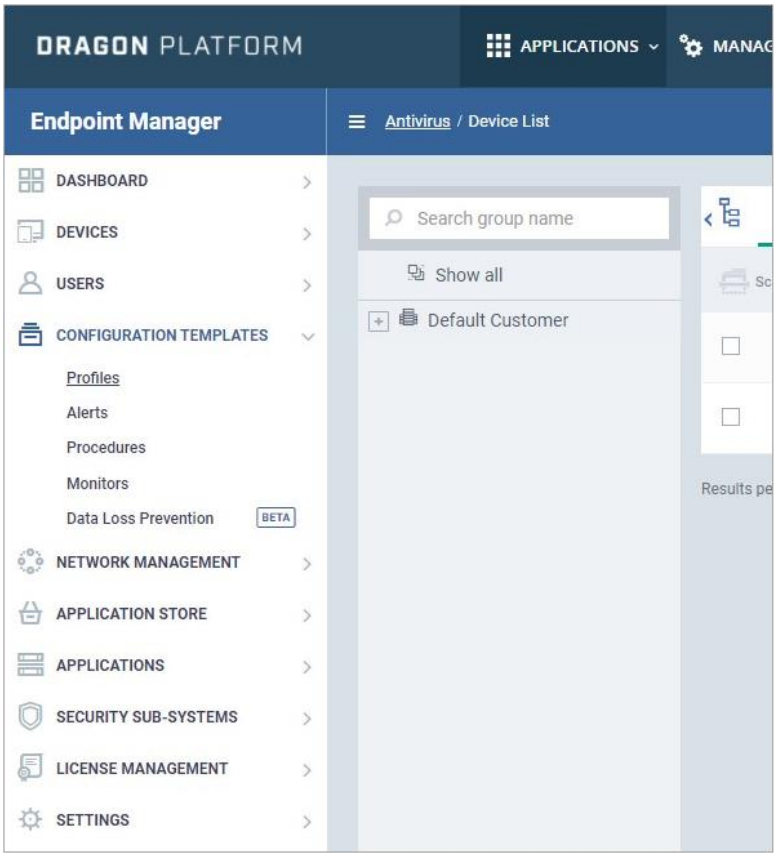

Figure 3

4. Select the Linux or Mac Profile used in the organization.

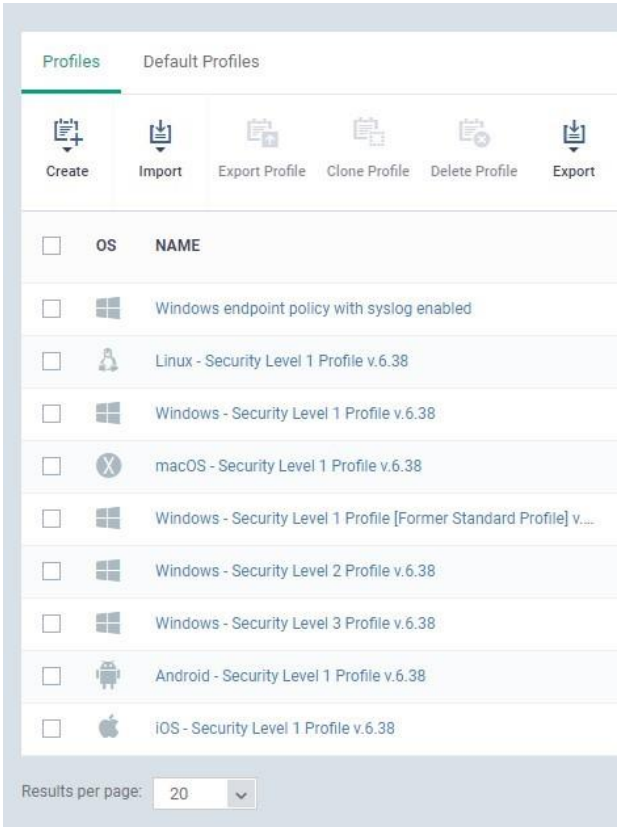

Figure 4

5. Go to **Logging Settings.** Click **Edit.**

Figure 5

6. Enable **Write to Syslog.**
7. Enter the **EventTracker Manager Public IP** in host.
8. Click **Save.**

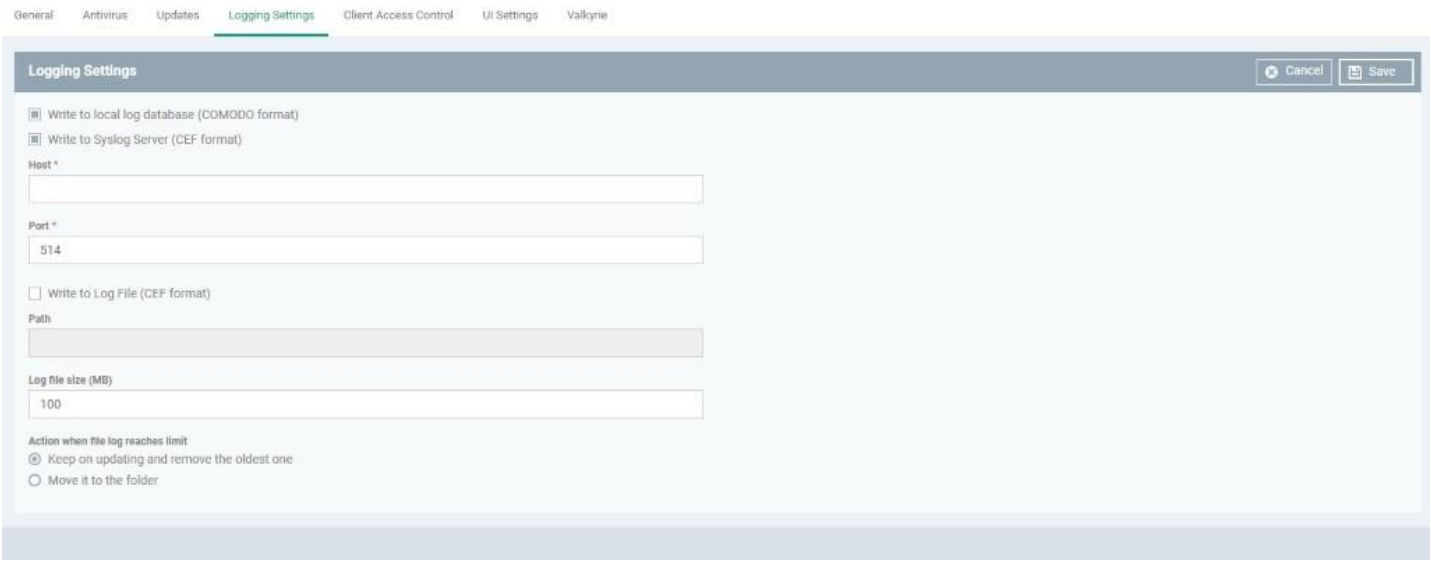

Figure 6

4. EventTracker Knowledge Pack

Once Comodo EP events are enabled and Comodo EP events are received in EventTracker, alerts, and reports can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support Comodo EP monitoring.

4.1 Categories

- **Comodo EP: Antivirus scan activities -** This category provides events information related to antivirus scan detail.
- **Comodo EP: Autorunning process -** This category provides events information related to the process running automatically.
- **Comodo EP: Configuration changes -** This category provides events information related to Comodo Endpoint configuration changes.
- **Comodo EP: File rating -** This category provides events information related to the application by file rating as unrecognized, malicious, and trusted.

- **Comodo EP: Intrusion prevention system activities -** This category provides event information related to hosting intrusion prevention system activities.
- **Comodo EP: Unknown or potentially unsafe application -** This category provides events information related to unknown or potentially unsafe application detail.

4.2 Alerts

- **Comodo EP: Configuration changes -** This alert will trigger whenever the Comodo Endpoint configuration changes.
- **Comodo EP: Threat detected -** This alert will trigger whenever a threat is detected on the host.
- **Comodo EP: Unrecognized files removed -** This alert will trigger whenever the Comodo Endpoint removes the unrecognized file on the host.

4.3 Reports

Comodo EP - Autorunning process – This report provides information related to the running process automatically in the host. It shows details like file path, file hash, reason, and IP address.

Log_sample

```
Nov 30 2020 13:02:21 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|D3287774-7AA1-4731-B6D2-017AB3A83F08|Autorun Event|5|act=Scheduled<space>Task reason=Ignore cat=autorun cs1Label=modifier cs1=SYSTEM cs2Label=location cs2=C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\ScheduledActionScripts\UnknownProcessExport.bat cs3Label=context cs3=Antivirus<space>Scan cs4Label=status cs4=Success fileHash=F62769AAD1C5A14EB0930F901BDEC9EF33B1FEC9 dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

Sample_Report

LogTime	Computer	IP Address	File Path	Context	Modified by	File Hash	Reason
12/15/2020 07:08:04 PM	WKSTS3W21\COMODO_EDR	172.29.9.183	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\ScheduledActionScripts\ETSFeedsImport.bat	Antivirus<space>Scan	SYSTEM	A8D0625FF8FB6FAF1469C938526B9429E7E3541E	Ignore
12/15/2020 07:08:04 PM	WKSTS3W21\COMODO_EDR	172.29.9.181	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\ScheduledActionScripts\TargetsReportExport.bat	Antivirus<space>Scan	SYSTEM	564EC1CD1A633FF062E9A3E8AC01894B4F4891AB	Ignore

Figure 7

- **Comodo EP - Configuration changes -** This report provides information related to configuration changes on Comodo Endpoint protection. It provides information like IP address, old value, new value, reason, action, and context.

Log_Sample

```
Nov 30 2020 09:04:15 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|17C8EA70-EBF0-4E26-8235-DFD7410AA9E4|Configuration changes|5|act=Option<space>Changed reason=Administrator cat=configuration cs1Label=obj_type cs1=Containment:<space>Virtual<space>Desktop<space>password cs2Label=old_value cs2=*** cs3Label=new_value cs3=*** dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

Sample_Report

LogTime	Computer	Action	IP Address	Context	Old Value	New Value	Reason
12/15/2020 07:08:25 PM	WKSTS32W\COMODO_EDR	Removed	172.29.9.183	HIPS<space>Protected<space>COM<space>Interface	<object<space>UID\="{6B41FB88-48F2-4C8C-9B74-F77FCF51B2D9}"<space>Flags\="1"<space>DeviceName\="Internet<space>Explorer/Windows<space>Shell"<space>/>		Administrator
12/15/2020 07:08:25 PM	WKSTS32W\COMODO_EDR	Changed	172.29.9.181	Detect<space>shellcode<space>injection:<space>Exclusion	<object<space>UID\="{2BC1F438-A318-4CCC-A065-86425D4B75E5}"<space>Name\="Unrecognized<space>Files<space>Scan"<space>Enabled\="true"<space>Flags\="0"<space>ScheduleType\="4"<space>ScheduleDoW\="0"<space>ScheduleDoM\="0"<space>ScheduleFlags\="1"<space>ScheduleOrdinaryDoW\="0"<space>UseMaintenanceMode\="true"<space>ScheduleTime\="1606651200"><Targets<space>/><Regions><Region<space>UID\="{0DA18181-F7D2-4E43-8871-CB0A805D5667}"<space>/></Regions><ScanSettings<space>Flags\="672"<space>MaxScanFileSize\="40"<space>HeurLevel\="1"<space>ScanPriority\="65536"<space>DefaultAction\="65537"<space>AVProfileDetectUnwantApp\="true"<space>ScanAutoruns\="true"<space>AutorunsCleanAction\="0"<space>ScanTimeout\="9"<space>/></object>	<object<space>UID\="{2BC1F438-A318-4CCC-A065-86425D4B75E5}"<space>Name\="Unrecognized<space>Files<space>Scan"<space>Enabled\="true"<space>Flags\="0"<space>ScheduleType\="4"<space>ScheduleDoW\="0"<space>ScheduleDoM\="0"<space>ScheduleFlags\="1"<space>ScheduleOrdinaryDoW\="0"<space>UseMaintenanceMode\="true"<space>ScheduleTime\="1606737600"><Targets<space>/><Regions><Region<space>UID\="{0DA18181-F7D2-4E43-8871-CB0A805D5667}"<space>/></Regions><ScanSettings<space>Flags\="672"<space>MaxScanFileSize\="40"<space>HeurLevel\="1"<space>ScanPriority\="65536"<space>DefaultAction\="65537"<space>AVProfileDetectUnwantApp\="true"<space>ScanAutoruns\="true"<space>AutorunsCleanAction\="0"<space>ScanTimeout\="9"<space>/></object>	Administrator

Figure 8

- **Comodo EP - Unknown and potentially unsafe applications -** This report provides information related to unknown or potentially unsafe applications. It provides information like IP address, file path, parent path, file rating, reason, device name, and device external id.

  Log_Sample

```
Nov 30 2020 11:46:30 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|BE6DE3B3-4677-4B87-A837-F887F517EB70|Containment Event|5|filePath=C:\Windows\System32\dllhost.exe fname=dllhost.exe act=Run<space>Virtually cat=containment reason=Contained<space>Process cs1Label=rating cs1=Trusted cs2Label=parent_path cs2= cs3Label=parent_hash cs3= dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

  Sample_Report

LogTime	Computer	IP Address	File Path	Parent Path	Rating
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\Agent\Integrator\Microsoft<space>365\Microsoft<space>365<space>Integrator.exe	C:\Windows\explorer.exe	Unrecognized
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\System32\conhost.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	Trusted
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe		Trusted
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe		Trusted
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	Trusted

Figure 9

- **Comodo EP - File rating -** This report provides information related to file rating for applications as trusted, unrecognized, and malicious. It provides information like file path, action, reason, old rating, new rating, source rating, file hash, device name, and device IP.

  Log_sample

```
Nov 30 2020 13:02:21 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|9FB5B608-55DE-4704-A02C-71BD45426149|Rating Info|5|filePath=C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\WCWindows\SrvShell.exe fname=SrvShell.exe act=Added cat=rating reason=COMODO cs1Label=old_rating cs1=Unrecognized cs2Label=new_rating cs2=Unrecognized cs3Label=src_rating cs3=FLS<space>(by<space>Vendor) fileHash=7223DAF24C8E8D03320B2EF6685B2779CCB0DB4C dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

  Sample_Report

LogTime	Computer	IP Address	File Path	File Name	File Hash	Old Rating	New Rating
12/15/2020 07:08:04 PM	WKSTS43\COMODO_EDR	172.29.9.183	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\ScheduledActionScripts\IblocklistBlueTackProxyIPListImport.bat	IblocklistBlueTackProxyIPListImport.bat	A12BE637B3C5609B6D89C913E039313BE7B7C84E	Trusted	Trusted
12/15/2020 07:08:04 PM	WKSTS43\COMODO_EDR	172.29.9.181	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\AdvancedReports\EventTracker.Reporter.exe	EventTracker.Reporter.exe	C371FF495ABF22BB7D129287BFAC42F644FCEAE6	Unrecognized	Unrecognized
12/15/2020 07:08:04 PM	WKSTS43\COMODO_EDR	172.29.9.183	C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\ScheduledActionScripts\IblocklistBlueTackBogonIPListImport.bat	IblocklistBlueTackBogonIPListImport.bat	6EBE409A44437E86B7E31B506B1D9930449B2C00	Trusted	Trusted

Figure 10

- **Comodo EP - Host Intrusion Prevention System activities -** This report provides information related to intrusion prevention system activities captured by Comodo HIPS. It provides detail like user name, target path, file path, file name, reason, action, user privilege, device IP, etc.

  Log_Sample

```
Nov 30 2020 11:46:25 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|C55C7A22-19CA-4B3A-B9E7-AB9EF20F2CA1|HIPS Event|5|act=terminateProcess reason=detect cat=hips cs1Label=target cs1=C:\Program<space>Files<space>(x86)\Microsoft\Edge\Application\msedge.exe filePath=C:\Program<space>Files<space>(x86)\Microsoft\Edge\Application\msedge.exe fname=msedge.exe suser=Administrator spriv=Administrator deviceNtDomain=WIN-MCKKRLN6KOI ssid=S-1-5-21-470948759-222244469-1961120547-500 fileHash=8F296BECC34DDA167A535C3C3274BF8A965955AD dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

Sample_Report

LogTime	Computer	User Name	Target	File Path	File Name
12/15/2020 07:08:51 PM	WKSTS324\COMODO_EDR	Administrator		C:\Program<space>Files<space>(x86)\Prism<space>Microsystems\EventTracker\Agent\Integrator\nssm.exe	nssm.exe
12/15/2020 07:11:01 PM	WKSTS324\COMODO_EDR	kenneth		C:\Users\Administrator\Downloads\eicar_com.zip	eicar_com.zip
12/15/2020 07:12:08 PM	WKSTS324\COMODO_EDR	maya	C:\Program<space>Files\COMODO\COMODO<space>Internet<space>Security\cis.exe	C:\Windows\explorer.exe	explorer.exe
12/15/2020 07:12:08 PM	WKSTS324\COMODO_EDR	maxx	C:\Program<space>Files\COMODO\COMODO<space>Internet<space>Security\cis.exe	C:\Windows\explorer.exe	explorer.exe
12/15/2020 07:12:54 PM	WKSTS324\COMODO_EDR	Administrator		C:\Users\Administrator\Downloads\eicar_com.zip	eicar_com.zip

Figure 11

- **Comodo EP - Scan detail -** This report provides information related to Antivirus scan details like action, reason, device name, device IP, scan file count, unrecognized file count, username, etc.

Log_Sample

```
Nov 30 2020 13:02:21 0000 WIN-MCKKRLN6KOI CEF:0|comodo|cis.cas.endpoint|12.5.0.8351|ACBA8518-B7EB-4E04-A44B-27B6D34F6D5E|Antivirus scan|6|act=scan reason=av_unrecognized_files_scan cat=av cs1Label=second_cat cs1=av cs2Label=total cs2=380 cs3Label=found cs3=4 cs4Label=complete_code cs4=0 suser=SYSTEM start=1606741341000 end=1606741341000 dvchost=WIN-MCKKRLN6KOI dvc=172.29.9.183 deviceExternalId=B6593A8AE71A5F0F99A6A81DDF32F8B4BC4FCA25
```

Sample_Report

LogTime	Computer	User Name	Reason	Total Files Scanned	Unrecognized Files count	IP Address	Complete Code
12/15/2020 07:08:52 PM	WKSTSR45\COMODO_EDR	SYSTEM	av_quick_scan	29016	4	172.29.9.183	0
12/15/2020 07:10:15 PM	WKSTSR45\COMODO_EDR	SYSTEM	av_unrecognized_files_scan	343	6	172.29.9.183	0
12/15/2020 07:10:15 PM	WKSTSR45\COMODO_EDR	SYSTEM	av_quick_scan	0	0	172.29.9.183	
12/15/2020 07:10:15 PM	WKSTSR45\COMODO_EDR	SYSTEM	av_reevaluate_scan	0	0	172.29.9.183	
12/15/2020 07:10:15 PM	WKSTSR45\COMODO_EDR	SYSTEM	av_reevaluate_scan	3	0	172.29.9.183	0

Figure 12

4.4 Dashboards

- **Comodo EP - Configuration changes**

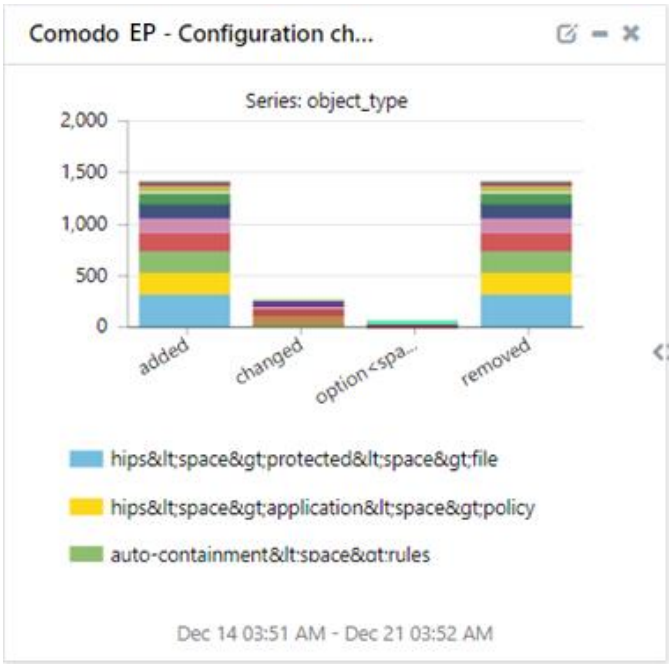

Figure 13

- **Comodo EP - Autorunning process**

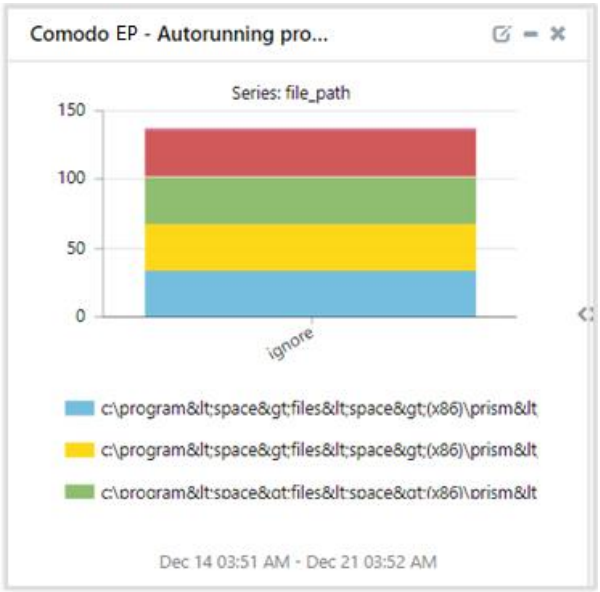

Figure 14

- **Comodo EP - Threat detected by filename**

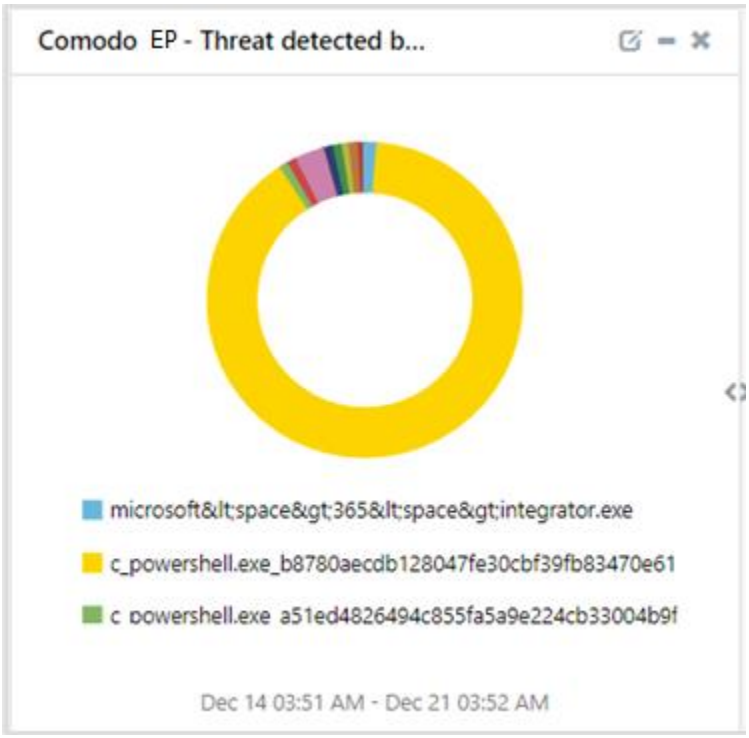

Figure 15

- **Comodo EP - Threat detected by hostname**

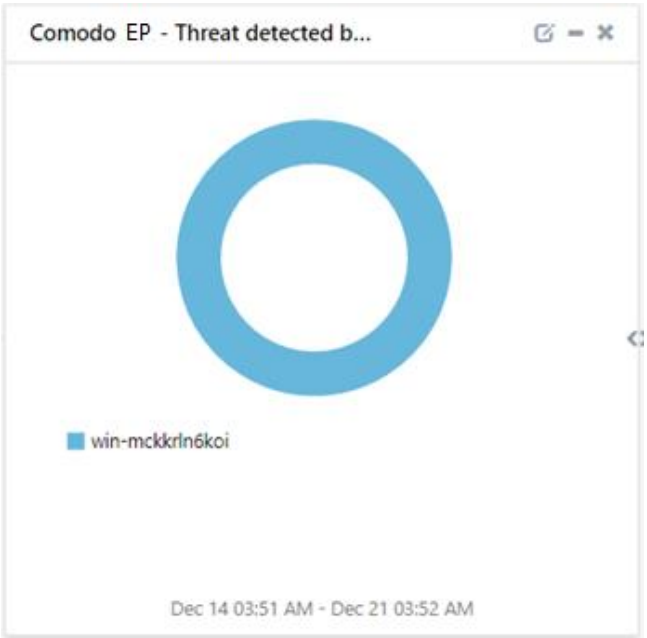

Figure 16

- **Comodo EP - Threat detected by IP address**

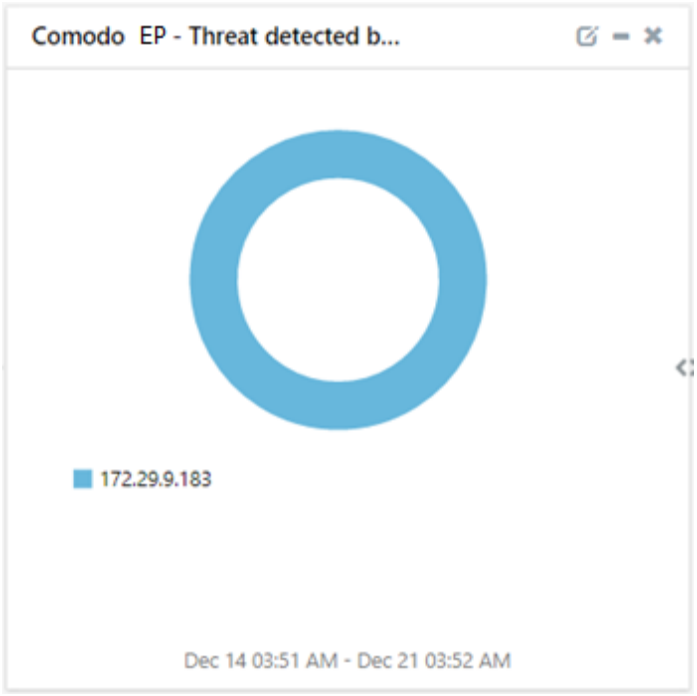

Figure 17

- **Comodo EP - Intrusion detected by filename**

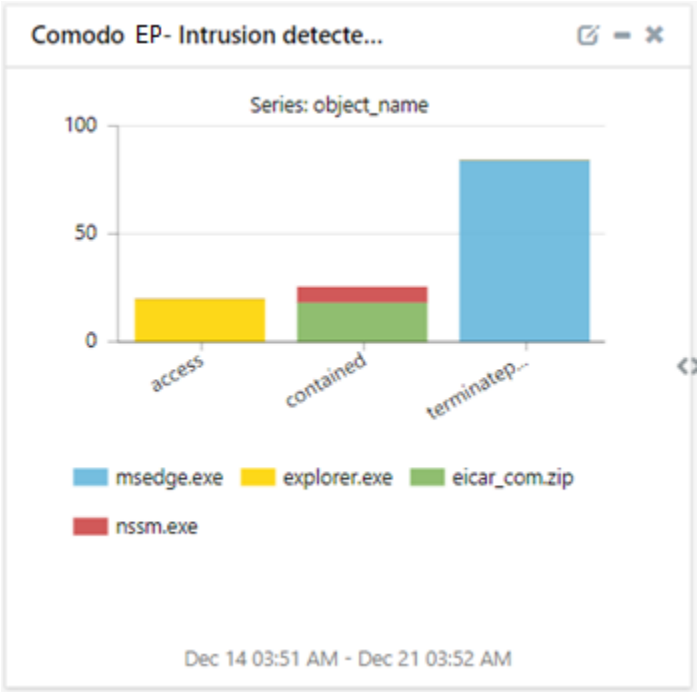

Figure 18

- **Comodo EP - IPS detected malicious files hash**

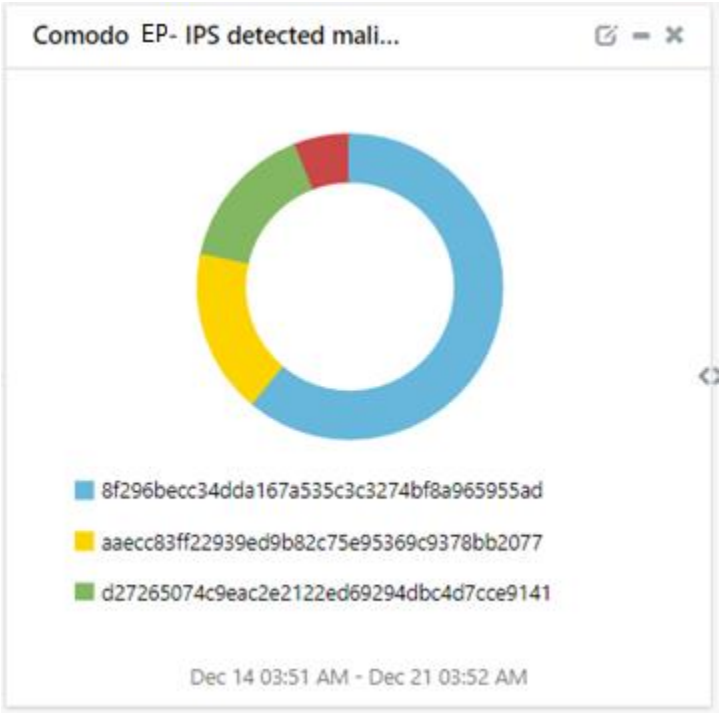

Figure 19

- **Comodo EP - File management**

Figure 20

5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

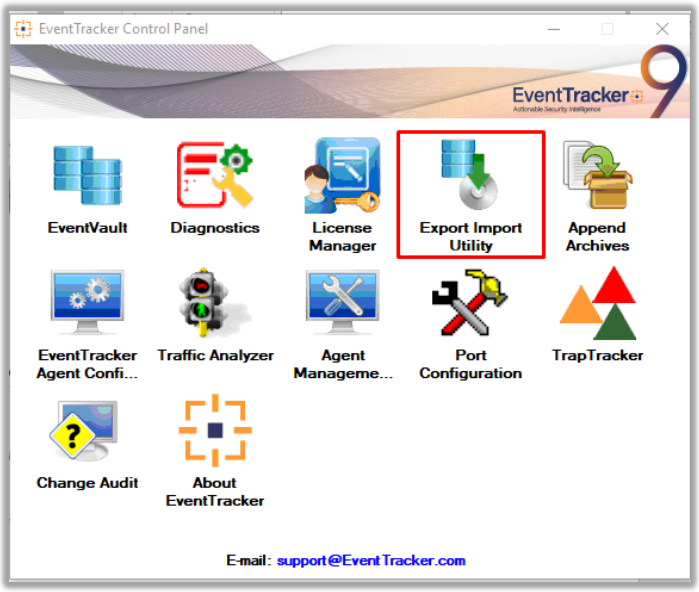

Figure 21

Export-Import Utility window opens.

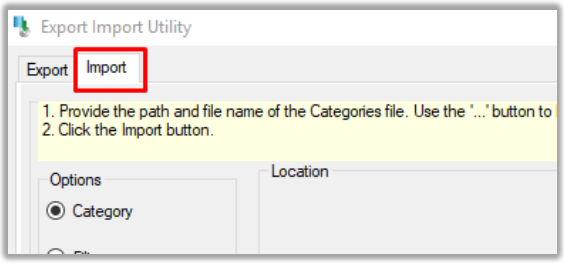

Figure 22

3. Click the **Import** tab.

5.1 Categories

1. In **Export-Import Utility** window, select the **Category** option, and click **Browse** . ...
2. Navigate to the knowledge pack folder and select the file with the extension **".iscat",** like **"Categories_Comodo EP. iscat"** and click "**Import**".

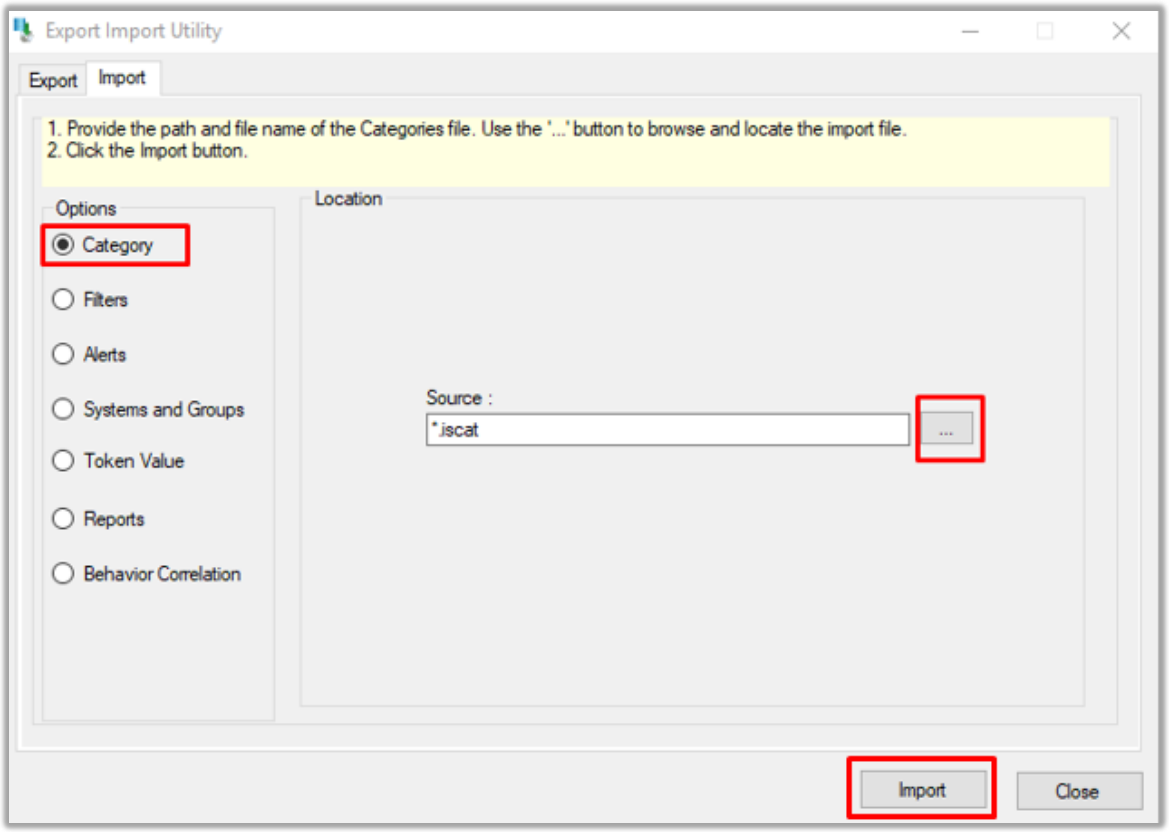

Figure 23

EventTracker displays a success message.

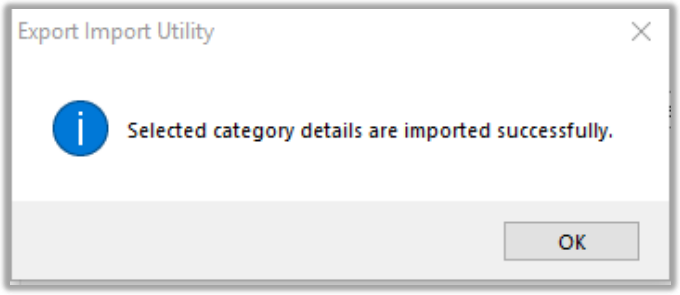

Figure 24

5.2 Alerts

1. In **Export-Import Utility** window , select the **Alert** option and click **Browse**.
2. Navigate to the knowledge pack folder and select the file with the extension **".isalt"**, **e.g**. "**Alerts_ Comodo EP.isalt**" and click "**Import**".

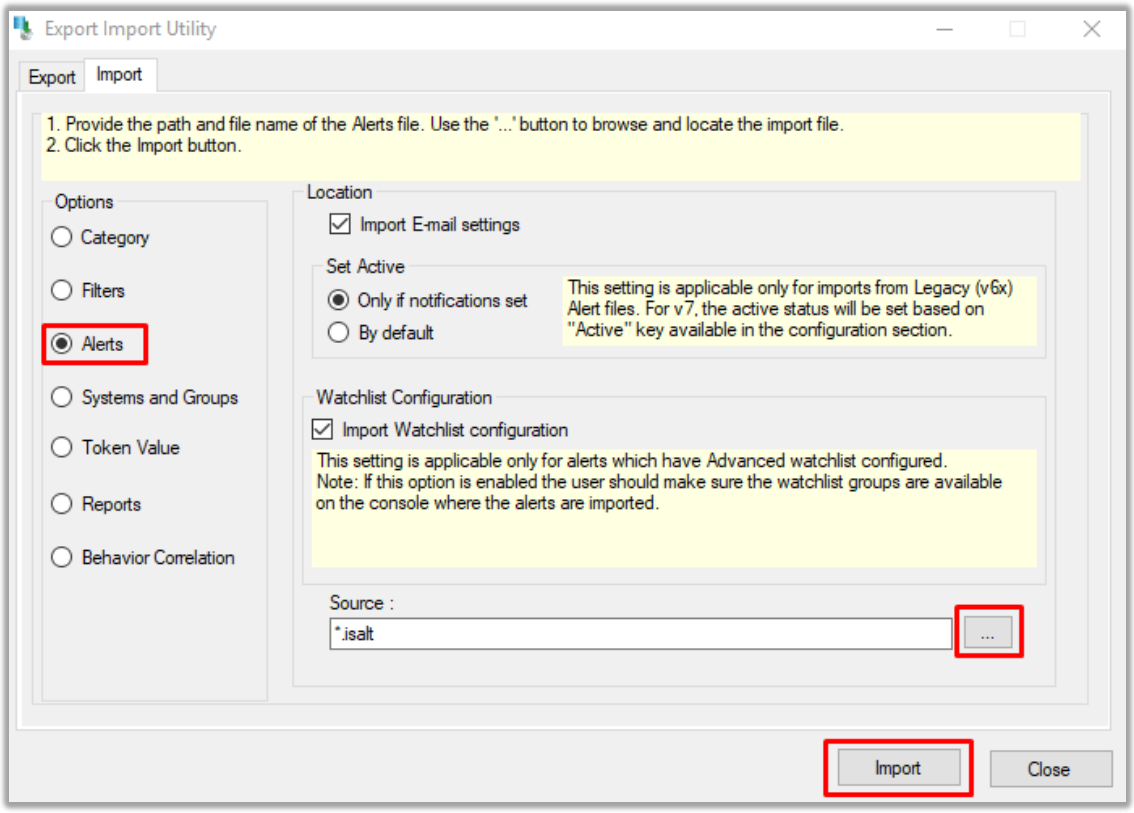

Figure 25

EventTracker displays a success message.

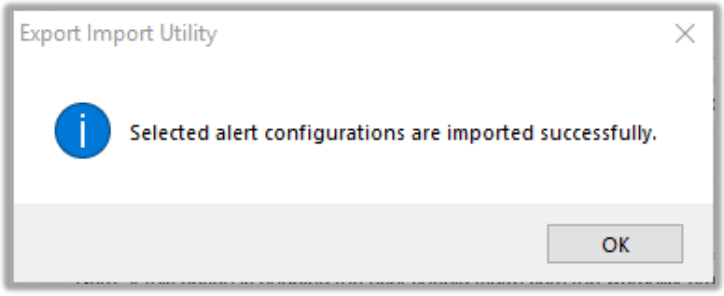

Figure 26

5.3 Flex Reports

1. In **Export-Import Utility** window, select the **Import tab**. Click the **Reports** option, and choose "**New (*.etcrx)**".

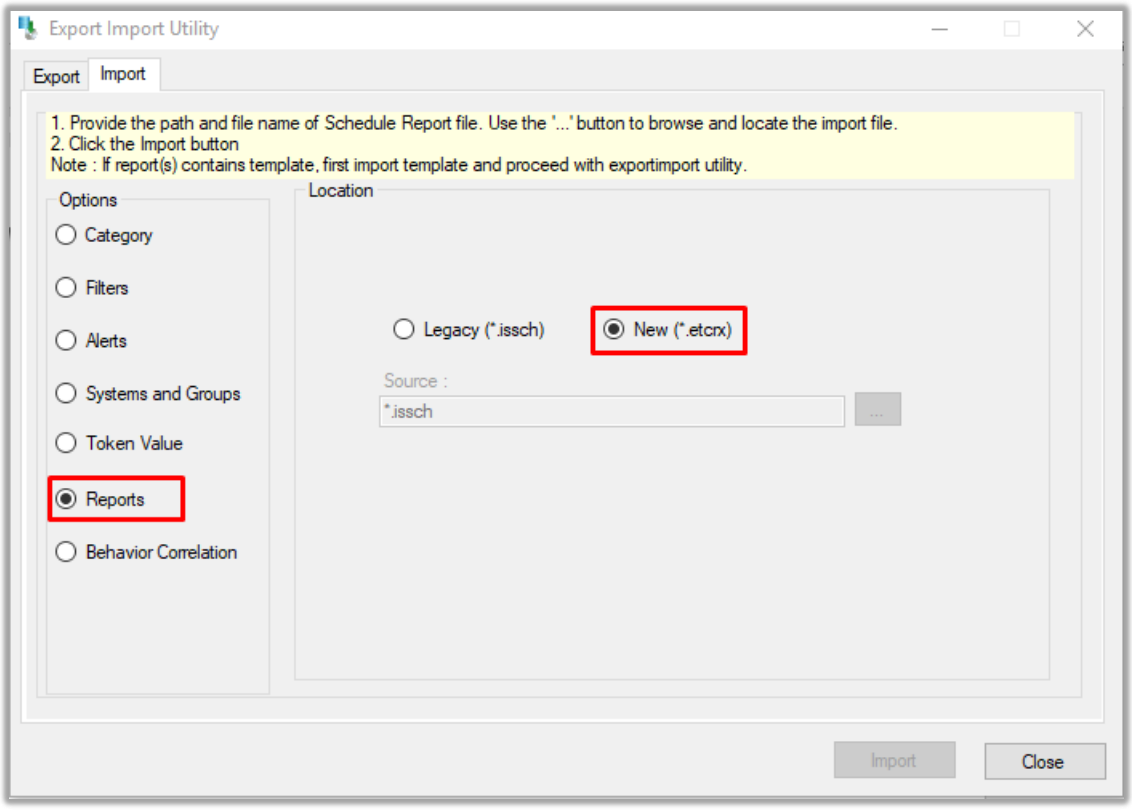

Figure 27

2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g. "Reports_Comodo EP.etcrx".**

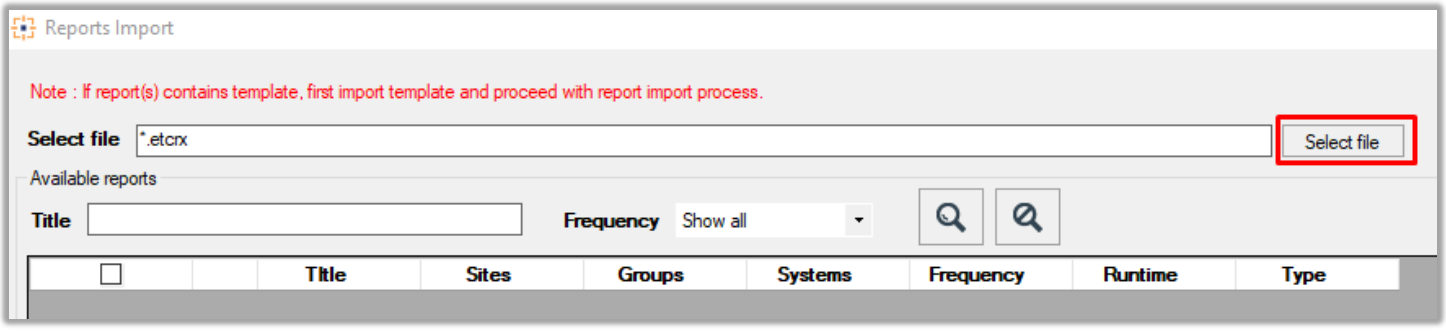

Figure 28

3. Wait while reports populate. Select all the relevant reports and click **Import** .

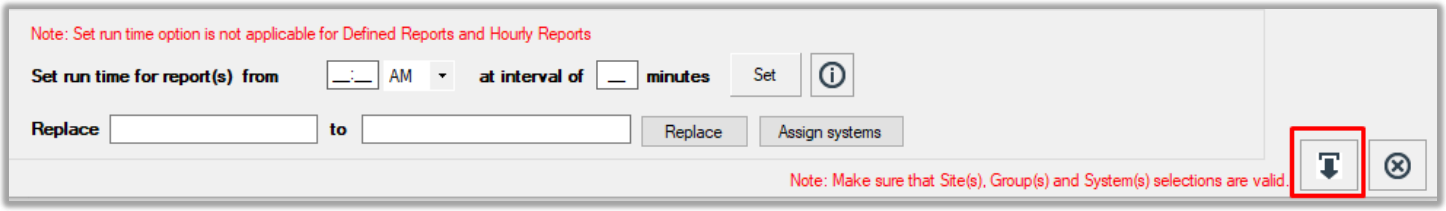

Figure 29

EventTracker displays a success message.

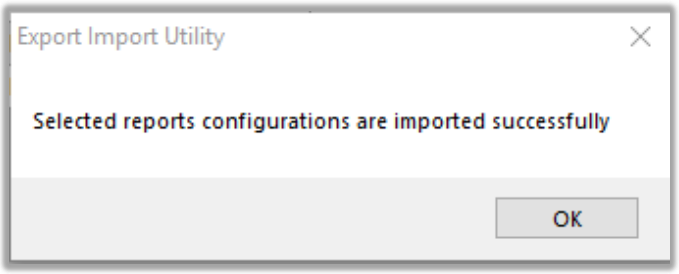

Figure 30

5.4 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

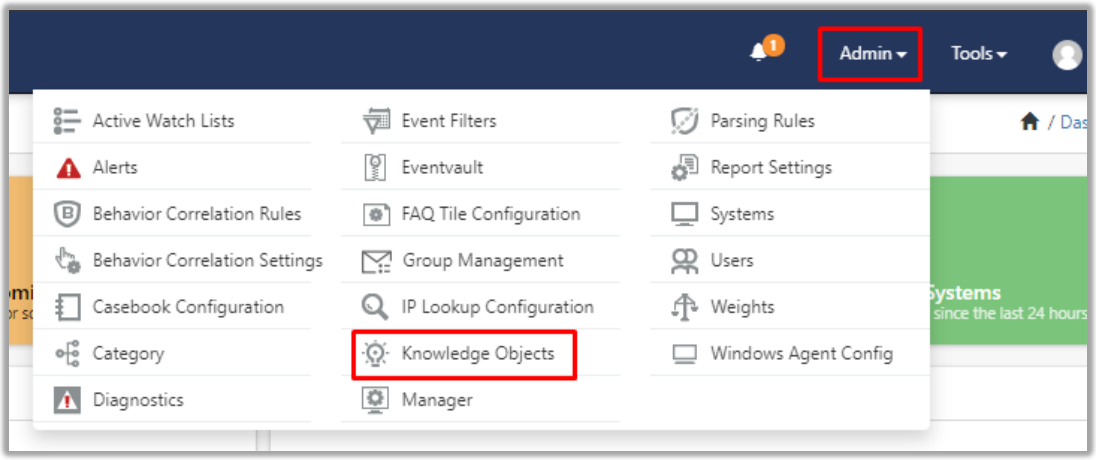

Figure 31

2. Click the **import object** icon.

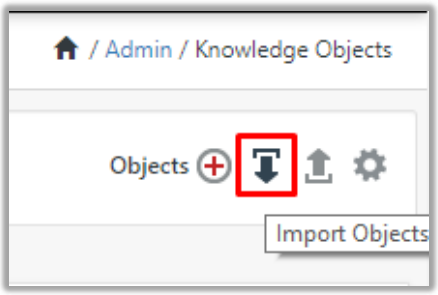

Figure 32

3. A pop-up box appears, click "**Browse**" and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g. "KO_Comodo EP.etko"** and click "**Upload**".

Figure 33

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones, and click "**Import**".

Figure 34

5.5 Dashboards

1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In **My Dashboard**, Click the **Import** button**.**

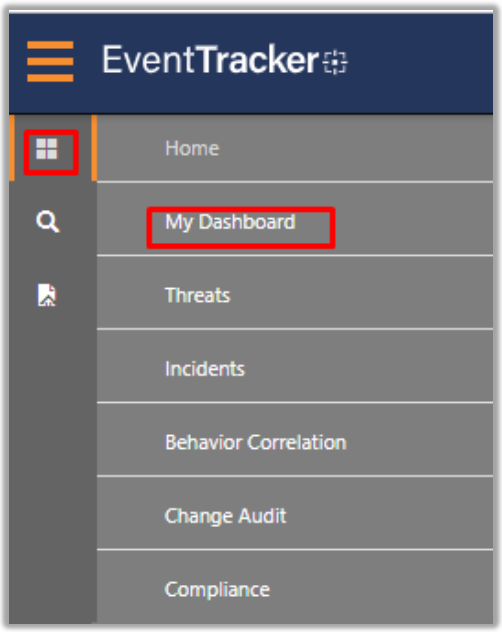

Figure 35

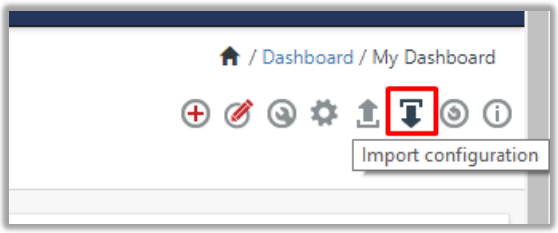

Figure 36

4. Click **Browse** and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.** "**Dashboard_Comodo EP.etwd**" is saved and click "**Upload**".

5. Wait while EventTracker populates all the available dashboards. Enable **Select All** and click **"Import"**.

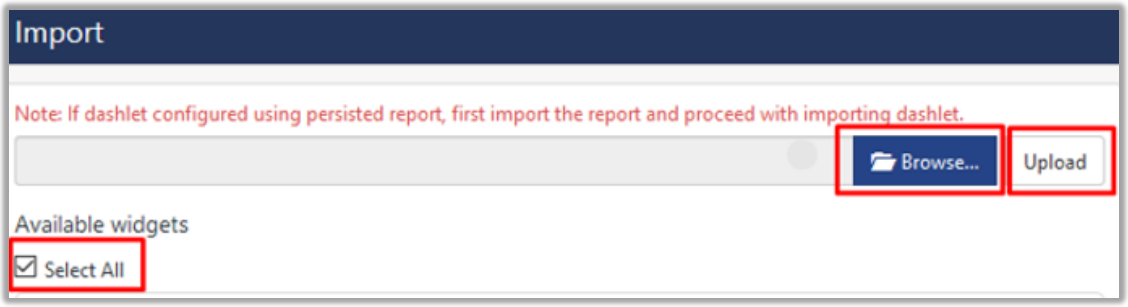

Figure 37

Figure 38

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and click **Categories**.
3. In **Category Tree** to view imported categories, click the **Search** tab and enter **Comodo EP** in the search**.**

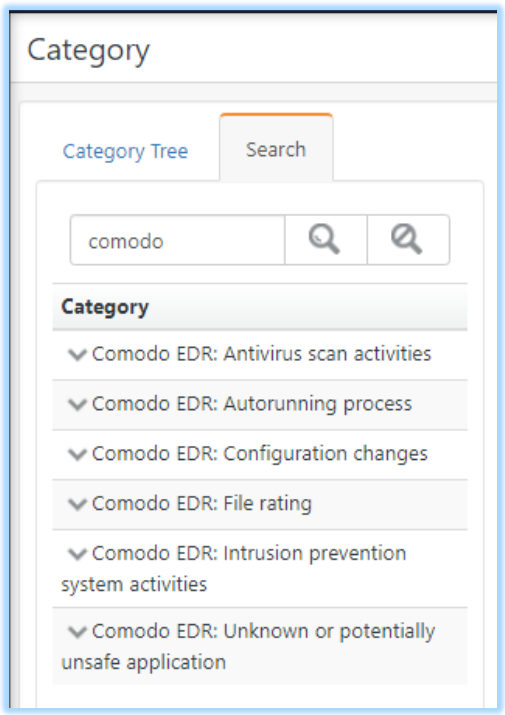

Figure 39

6.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **Comodo EP** and click **Search**.

   EventTracker displays an alert related to Comodo EP**.**

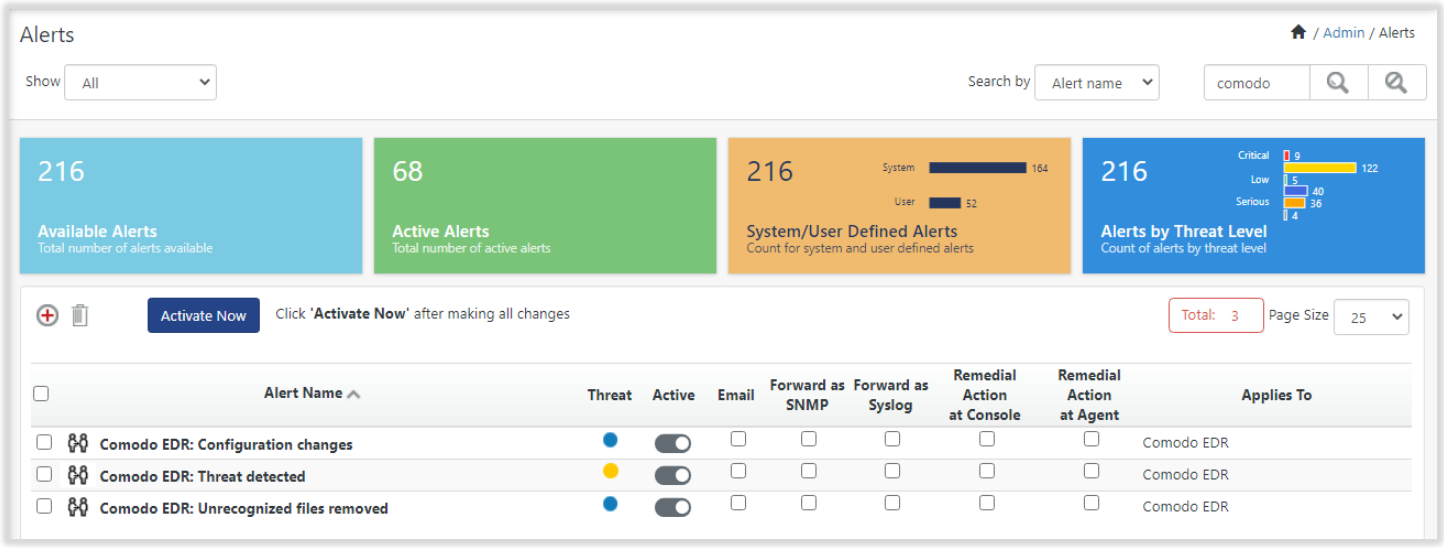

Figure 40

6.3 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

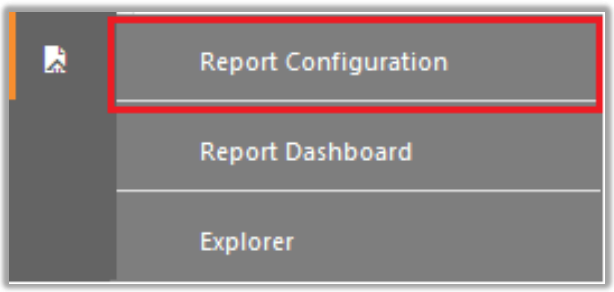

Figure 41

2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click on the **"Comodo EP"** group folder to view the imported reports.

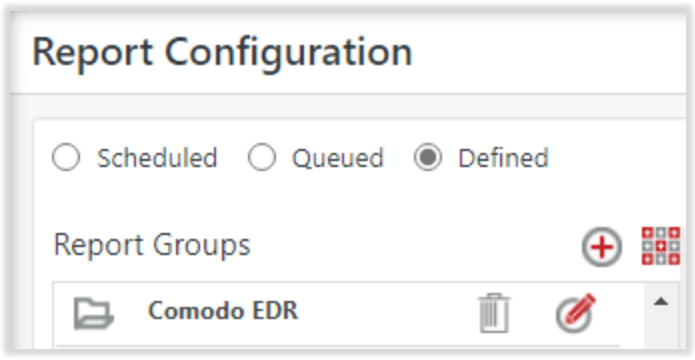

Figure 42

6.4 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **"Comodo EP"** group folder to view the imported Knowledge objects.

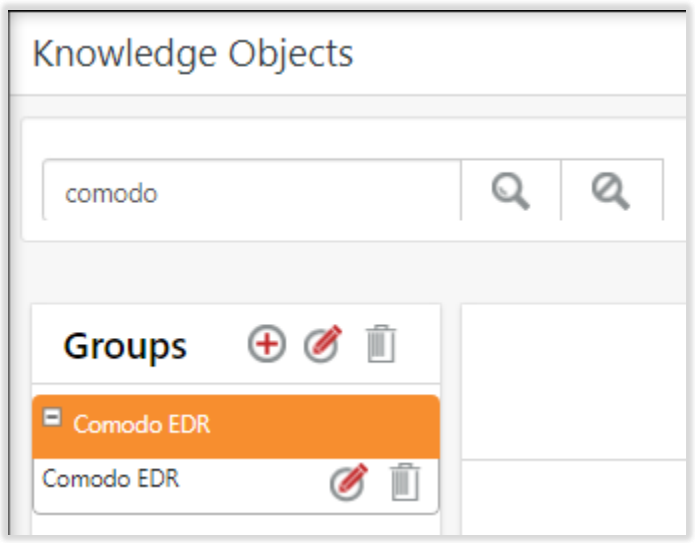

Figure 43

6.5 Dashboards

1. In the EventTracker web interface, Click **Home** and select "**My Dashboard**".

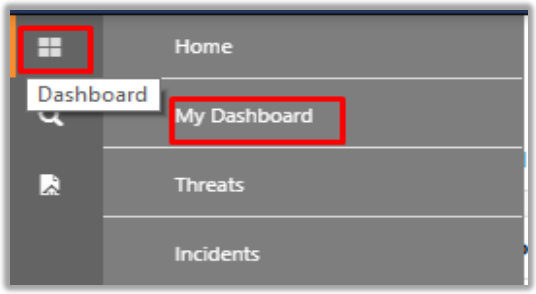

Figure 44

2. In the "**Comodo EP"** dashboard you see the following screen.

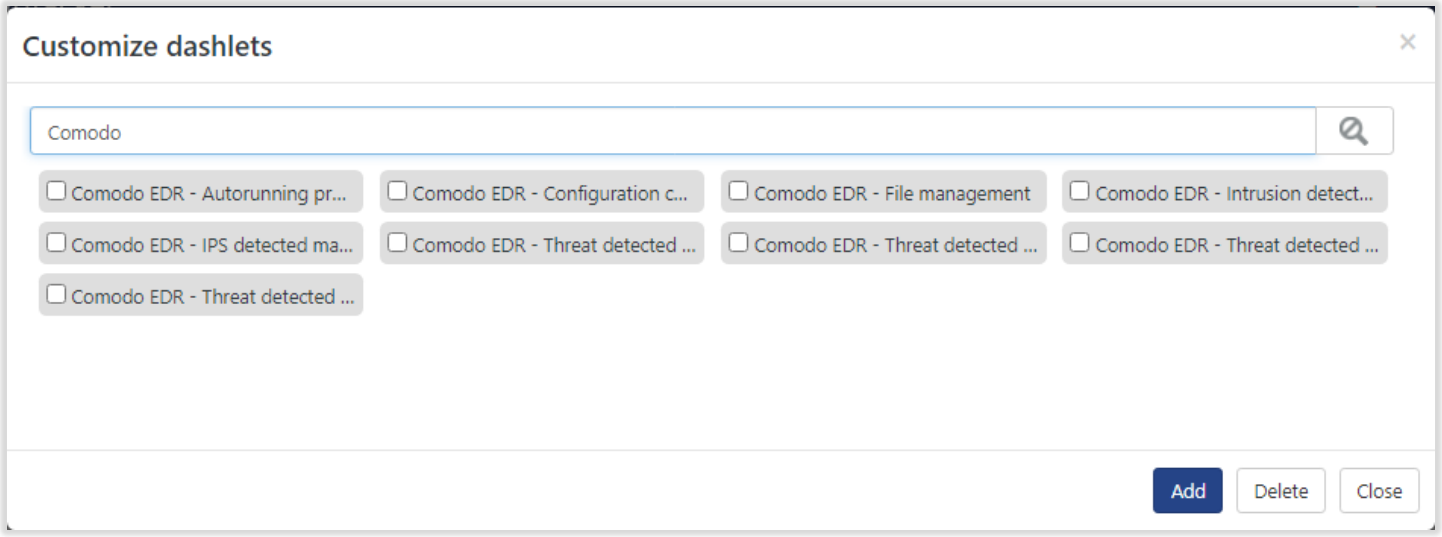

Figure 45