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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright Comodo EP is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Intr	oduction	3
Prei	requisites	3
Con	figuring Comodo Endpoint Protection logging	3
Eve 4.1	ntTracker Knowledge Pack Categories	7 7
4.2	Alerts	8
4.3	Reports	8
4.4	Dashboards	12
Imp 5.1	orting knowledge pack into EventTracker Categories	16 17
5.2	Alerts	18
5.3	Flex Reports	19
5.4	Knowledge Objects	20
5.5	Dashboards	21
Veri 6.1	ifying knowledge pack in EventTracker Categories	23 23
6.2	Alerts	24
6.3	Flex Reports	24
6.4	Knowledge Objects	25
6.5	Dashboards	25
	Intr Prei Con Eve 4.1 4.2 4.3 4.4 Imp 5.1 5.2 5.3 5.4 5.5 Ver 6.1 6.2 6.3 6.4 6.5	Introduction Prerequisites Configuring Comodo Endpoint Protection logging EventTracker Knowledge Pack 4.1 Categories 4.2 Alerts 4.3 Reports 4.4 Dashboards Importing knowledge pack into EventTracker 5.1 Categories 5.2 Alerts 5.3 Flex Reports 5.4 Knowledge Objects 5.5 Dashboards Verifying knowledge pack in EventTracker 6.1 Categories 6.2 Alerts 6.3 Flex Reports 6.4 Knowledge Objects 6.5 Dashboards

Netsurion. EventTracker

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.

Netsurion. EventTracker[®]

allow you to manage re	and a start start start file			^
allow you to manage re	a second to be and second at the back of the	1021		
UC.	ecording of critical events like	e malware	events,	
l log database (COMOD	O format)			
og server				
	Port 514			
ote server (JSON format	1)			
	Port 0			
file (CEF format)				
	Browse			
dows Event Log				1
agement				
aches 100 MB				
ating it removing the o	ldest records			
t H H H	og server lote server (JSON formal file (CEF format) idows Event Log hagement eaches 100 MB dating it removing the o	og server Port 514 Note server (JSON format) Port Port file (CEF format) Browse Ndows Event Log Nagement eaches 100 MB dating it removing the oldest records OK	og server Port 514 Note server (JSON format) Port 0 file (CEF format) Ndows Event Log Nagement eaches 100 MB dating it removing the oldest records OK	og server Port 514 iote server (JSON format) Port file (CEF format) Browse idows Event Log hagement eaches 100 MB dating it removing the oldest records OK CANCEL

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 Figure 1).
 - 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.



4



Figure 2

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







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



Figure 4

5. Go to Logging Settings. Click Edit.

Add Profile Export Profile Close Profile Delete Profile Make Default	
General Antivirus Updates Logging Settings Client Access Control UI Settings Valkyrie	
Logging Settings	🍞 Edit 🔋 Delete
Write to local log database (COMODO format) Enabled	
Write to Systog Server (CEF format) Disabled	
Host Not set	
Port 514	
Write to Log File (CEF format) Disabled	
Path Not set	
Log file size (MB) 100	
Action when file log reaches limit Keep on updating and remove the oldest one	

Figure 5



6. Enable Write to Syslog.

Logging Settings Client Access Control UI Settings

7. Enter the EventTracker Manager Public IP in host.

Vallevrie

8. Click Save.

Logging Settings	🕲 Cancel 🖺 Sa
Write to local log database (COMODO format)	
Write to Syslog Server (CEF format)	
Host*	
191	
314	
Write to Log File (CEF format)	
Path	
an file ulas (MD)	
300	
100	
Action when file log reaches limit	
Keep on updating and remove the oldest one	
Move it to the folder	

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\U nknownProcessExport.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\ScheduledActionScri pts\ETSFeedsImport.bat</space></space></space>	Antivirus <space>Scan</space>	SYSTEM	A8D0625FF8FB6FAF1469C93852 6B9429E7E3541E	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\ScheduledActionScri pts\TargetsReportExport.bat</space></space></space>	Antivirus <space>Scan</space>	SYSTEM	564EC1CD1A633FF062E9A3E8AC 01894B4F4891AB	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>CO</space></space>	<object<space>UID\="{6B41FB88-48F2-4C8C-</object<space>		Administrator
				M <space>Interface</space>	9B74-		
					F77FCF51B2D9}" <space>Flags\="1"<space>De</space></space>		
					viceName\="Internet <space>Explorer/Windows</space>		
					<space>Shell"<space>/></space></space>		
12/15/2020 07:08:25 PM	WKSTS32W/COMODO_EDR	Changed	172.29.9.181	Detect <space>shellcode<space>in</space></space>	<object<space>UID\="{2BC1F438-A318-4CCC-</object<space>	<object<space>UID\="{2BC1F438-A318-</object<space>	Administrator
				jection: <space>Exclusion</space>	A065-	4CCC-A065-	
					86425D4B75E5}" <space>Name\="Unrecognize</space>	86425D4B75E5}" <space>Name\="Unreco</space>	
					d <space>Files<space>Scan"<space>Enabled\=</space></space></space>	gnized <space>Files<space>Scan"<spac< td=""><td></td></spac<></space></space>	
					"true" <space>Flags\="0"<space>ScheduleType</space></space>	e>Enabled\="true" <space>Flags\="0"<sp< td=""><td></td></sp<></space>	
					\="4" <space>ScheduleDoW\="0"<space>Sched</space></space>	ace>ScheduleType\="4" <space>Schedul</space>	
					uleDoM\="0" <space>ScheduleFlags\="1"<space< td=""><td>eDoW\="0"<space>ScheduleDoM\="0"<s< td=""><td></td></s<></space></td></space<></space>	eDoW\="0" <space>ScheduleDoM\="0"<s< td=""><td></td></s<></space>	
					>ScheduleOrdinaryDoW\="0" <space>UseMaint</space>	pace>ScheduleFlags\="1" <space>Sched</space>	
					enanceMode\="true" <space>ScheduleTime\="1</space>	uleOrdinaryDoW\="0" <space>UseMainte</space>	
					606651200"> <targets<space>/><regions><re< td=""><td>nanceMode\="true"<space>ScheduleTim</space></td><td></td></re<></regions></targets<space>	nanceMode\="true" <space>ScheduleTim</space>	
					gion <space>UID\="{0DA18181-F7D2-4E43-</space>	e\="1606737600"> <targets<space>/><r< td=""><td></td></r<></targets<space>	
					8871-	egions> <region<space>UID\="{0DA1818</region<space>	
					CB0A805D5667}" <space>/><scans< td=""><td>1-F7D2-4E43-8871-</td><td></td></scans<></space>	1-F7D2-4E43-8871-	
					ettings <space>Flags\="672"<space>MaxScanFi</space></space>	CB0A805D5667}" <space>/><</space>	
					leSize\="40" <space>HeurLevel\="1"<space>Sc</space></space>	ScanSettings <space>Flags\="672"<spac< td=""><td></td></spac<></space>	
					anPriority\="65536" <space>DefaultAction\="655</space>	e>MaxScanFileSize\="40" <space>HeurL</space>	
					37" <space>AVProfileDetectUnwantApp\="true"</space>	evell="1" <space>ScanPriority\="65536"<</space>	
					<space>ScanAutoruns\="true"<space>Autorun</space></space>	space>DefaultAction\="65537" <space>A</space>	
					sCleanAction\="0" <space>ScanTimeout\="9"<s< td=""><td>VProfileDetectUnwantApp\="true"<space< td=""><td></td></space<></td></s<></space>	VProfileDetectUnwantApp\="true" <space< td=""><td></td></space<>	
					pace>/>	>ScanAutoruns\="true" <space>Autoruns</space>	
						CleanAction\="0" <space>ScanTimeout\="</space>	
						9" <space>/></space>	

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>(x</space></space>	C:\Windows\explorer.exe	Unrecognized
			86)\Prism <space>Microsystems\Ev</space>		
			entTracker\Agent\Integrator\Micros		
			oft <space>365\Microsoft<space>3</space></space>		
			65 <space>Integrator.exe</space>		
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\System32\conhost.ex	C:\Windows\Microsoft.NET\Frame	Trusted
			e	work64\v4.0.30319\csc.exe	
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Frame		Trusted
			work64\v4.0.30319\cvtres.exe		
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Frame		Trusted
			work64\v4.0.30319\csc.exe		
12/15/2020 07:08:25 PM	WKSTS345\COMODO_EDR	10.12.30.43	C:\Windows\Microsoft.NET\Frame	C:\Windows\Microsoft.NET\Frame	Trusted
			work64\v4.0.30319\cvtres.exe	work64\v4.0.30319\csc.exe	

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>(x</space></space>	IblocklistBlueTackProxyIPListImport.	A12BE637B3C5609B6D89C913E03	Trusted	Trusted
			86)\Prism <space>Microsystems\Ev</space>	bat	9313BE7B7C84E		
			entTracker\ScheduledActionScript				
			s\lblocklistBlueTackProxylPListImpo				
			rt.bat				
12/15/2020 07:08:04 PM	WKSTS43\COMODO_EDR	172.29.9.181	C:\Program <space>Files<space>(x</space></space>	EventTracker.Reporter.exe	C371FF495ABF22BB7D129287BF	Unrecognized	Unrecognized
			86)\Prism <space>Microsystems\Ev</space>		AC42F644FCEAE6		
			entTracker\AdvancedReports\Even				
			tTracker.Reporter.exe				
12/15/2020 07:08:04 PM	WKSTS43\COMODO_EDR	172.29.9.183	C:\Program <space>Files<space>(x</space></space>	IblocklistBlueTackBogonIPListImport	6EBE409A44437E86B7E31B506B1	Trusted	Trusted
			86)\Prism <space>Microsystems\Ev</space>	.bat	D9930449B2C00		
			entTracker\ScheduledActionScript				
			s\lblocklistBlueTackBogonIPListImp				
			ort.bat				

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 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>(x</space></space>	nssm.exe
				86)\Prism <space>Microsystems\Ev</space>	
				entTracker\Agent\Integrator\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\</space>	C:\Windows\explorer.exe	explorer.exe
			COMODO <space>Internet<space></space></space>		
			Security\cis.exe		
12/15/2020 07:12:08 PM	WKSTS324\COMODO_EDR	maxx	C:\Program <space>Files\COMODO\</space>	C:\Windows\explorer.exe	explorer.exe
			COMODO <space>Internet<space></space></space>		
			Security\cis.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

			Total Files Scann	Unrecognized		
Computer	User Name	Reason	ed	Files count	IP Address	Complete Code
WKSTSR45\COMODO_EDR	SYSTEM	av_quick_scan	29016	4	172.29.9.183	0
WKSTSR45\COMODO_EDR	SYSTEM	av_unrecognized_files_scan	343	6	172.29.9.183	0
WKSTSR45\COMODO_EDR	SYSTEM	av_quick_scan	0	0	172.29.9.183	
WKSTSR45\COMODO_EDR	SYSTEM	av_reevaluate_scan	0	0	172.29.9.183	
WKSTSR45\COMODO_EDR	SYSTEM	av_reevaluate_scan	3	0	172.29.9.183	0
	Computer WKSTSR45\COMODO_EDR WKSTSR45\COMODO_EDR WKSTSR45\COMODO_EDR WKSTSR45\COMODO_EDR WKSTSR45\COMODO_EDR	Computer User Name WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM WKSTSR45\COMODO_EDR SYSTEM	ComputerUser NameReasonWKSTSR45\COMODO_EDRSYSTEMav_quick_scanWKSTSR45\COMODO_EDRSYSTEMav_unrecognized_files_scanWKSTSR45\COMODO_EDRSYSTEMav_quick_scanWKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scanWKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scanWKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan	ComputerUser NameReasonTotal Files Scann edWKSTSR45\COMODO_EDRSYSTEMav_quick_scan29016WKSTSR45\COMODO_EDRSYSTEMav_unrecognized_files_scan343WKSTSR45\COMODO_EDRSYSTEMav_quick_scan0WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan0WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan3	ComputerUser NameReasonTotal Files Scann edUnrecognized Files countWKSTSR45\COMODO_EDRSYSTEMav_quick_scan290164WKSTSR45\COMODO_EDRSYSTEMav_unrecognized_files_scan3436WKSTSR45\COMODO_EDRSYSTEMav_quick_scan00WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan00WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan30	ComputerUser NameReasonTotal Files Scann edUnrecognized Files countIP AddressWKSTSR45\COMODO_EDRSYSTEMav_quick_scan290164172.29.9.183WKSTSR45\COMODO_EDRSYSTEMav_unrecognized_files_scan3436172.29.9.183WKSTSR45\COMODO_EDRSYSTEMav_quick_scan00172.29.9.183WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan00172.29.9.183WKSTSR45\COMODO_EDRSYSTEMav_reevaluate_scan30172.29.9.183

Figure 12

Netsurion. EventTracker[®]

4.4 Dashboards



• Comodo EP - Configuration changes



• 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



• Comodo EP - Intrusion detected by filename



Figure 18





• Comodo EP - IPS detected malicious files hash



• 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.





Export-Import Utility window opens.

🥾 Ехро	rt Import	Utility				
Export	Import					
1. Provide the path and file name of the Categories file. Use the '' button to 2. Click the Import button.						
Opt	ions		Location			
۲	Category					

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".

🐁 Export Import Utility	-		\times
Export Import			
1. Provide the path and file nan 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.		
Options Category Filters Alerts	Location		
 Systems and Groups Token Value Reports Behavior Correlation 	Source : *iscat		
	Import	Clo	se

Figure 23

EventTracker displays a success message.

Export Im	port Utility	\times
1	Selected category details are imported successfully.	
	ОК	





5.2 Alerts

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

Export Import 1. Provide the path and file name 2. Click the Import button.	e of the Alerts file. Use the '' butt	on to browse and locate the import file.
 Provide the path and file name Click the Import button. 	e of the Alerts file. Use the '' butt	on to browse and locate the import file.
	1	
Options	Location	
Category	Import E-mail settings	
	Set Active	
○ Filters	Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7 the active status will be set based on
Alerts	O By default	"Active" key available in the configuration section.
O Systems and Groups	Watchlist Configuration	
O Token Value	Import Watchlist configurati	on
	This setting is applicable only f	or alerts which have Advanced watchlist configured.
◯ Reports	on the console where the alert	s are imported.
O Behavior Correlation		
	Source :	
	*.isalt	
		Import Close

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)".

🥾 Export Import Utility	_		\times
Export Import			
1. Provide the path and file name 2. Click the Import button Note : If report(s) contains templ	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility.		
Options	Location		
○ Category			
⊖ Filters			
○ Alerts	Legacy (*.issch) New (*.etcnx)		
O Systems and Groups	Source : *issch		
O Token Value			
Reports			
O Behavior Correlation			
	Import	Clos	se



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".

ቶ Reports Import					
Note : If report(s) contains template, first import temp	late and proceed with report imp	ort process.			
Select file *.etcrx					Select file
Available reports					
Title	Frequency	Show all 👻	Q Q		
	Sites Group	s Systems	Frequency	Runtime	Туре

Figure 28



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

Note: Set run time option is not applicab	le for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of minutes	Set
Replace	to Replace	Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.



EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations are imported successfully	
ОК	

Figure 30

5.4 Knowledge Objects

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

		🔎 Admin -	Tools 👻 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	🏫 / Da
Alerts	🖉 Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🍓 Behavior Correlation Settings	Group Management	🗙 Users	
mi Sr sc Casebook Configuration	Q IP Lookup Configuration	r Weights	Systems since the last 24 hour
● Category	·☆· Knowledge Objects	Windows Agent Config	_
▲ Diagnostics	Manager		



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



Netsurion EventTracker[®]



Figure 32

 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".

Import	
KO_ <product name="">.etko</product>	Frowse 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**".





5.5 Dashboards

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



≡	Event Tracker ⊕
	Home
٩	My Dashboard
	Threats
	Incidents
	Behavior Correlation
	Change Audit
	Compliance



🔒 / Dashboard / My Dashboard
+ 🖉 Q 🌣 İ 🏹 O ()
Import configuration



- 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".

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
🗁 Browse	Upload
Available widgets	
Select All	





	J
Import	•

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.

Category				
Category Tree Search				
comodo Q Q				
Category				
✓ Comodo EDR: Antivirus scan activities				
✓ Comodo EDR: Autorunning process				
✓ Comodo EDR: Configuration changes				
🗸 Comodo EDR: File rating				
 Comodo EDR: Intrusion prevention system activities 				
 Comodo EDR: Unknown or potentially unsafe application 				

Figure 39



Q

Q

~

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.

Alerts 🕈 / Admin / Alerts Search by Alert name 🗸 Show All ~ comodo 216 216 System/User Defined Alerts Alerts by Threat Level 🕀 🗓 Activate Now Click 'Activate Now' after making all changes Total: 3 Page Size 25 Remedial Remedial Forward as Forward as Alert Name ٨ Active Email Action Action Applies To Threat SNMP Syslog at Agent at Console □ 🖗 Comodo EDR: Configuration changes Comodo EDR 🗆 🖗 Comodo EDR: Threat detected Comodo EDR Comodo EDR: Unrecognized files removed Comodo EDR 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.



Report Configuration				
○ Scheduled ○ Queued ● Defined	ł			
Report Groups	æ			
heport oroups		000		
Comodo EDR	Ø	-		
	<u> </u>			
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.

Knowledge Objects				
comodo	Q	Q		
Groups 🕀 🧭 🗓				
Comodo EDR				
Comodo EDR 🧭 📋				

Figure 43

6.5 Dashboards

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







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

Customize dashlets			×
Comodo			Q
Comodo EDR - Autorunning pr	Comodo EDR - Configuration c	Comodo EDR - File management	Comodo EDR - Intrusion detect
Comodo EDR - IPS detected ma	Comodo EDR - Threat detected	Comodo EDR - Threat detected	Comodo EDR - Threat detected
Comodo EDR - Threat detected			
			Add Delete Close

Figure 45

