

Integrate Palo Alto Traps

EventTracker v8.x and above

Abstract

This guide provides instructions to configure **Palo Alto Traps** to send its syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and **Palo Alto Traps**.

Audience

Administrators who are assigned the task to monitor Palo Alto Traps events using EventTracker.

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

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

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

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Scope	1
Audience.....	1
Overview.....	3
Prerequisites.....	3
Integration of Palo Alto Traps with EventTracker Manager	3
EventTracker Knowledge Pack	4
Category	4
Alerts	4
Knowledge Object	5
Flex Reports	5
Import Palo Alto Traps knowledge pack into EventTracker	11
Category	12
Alerts	13
Token Templates	14
Knowledge Object	15
Flex Report.....	17
Dashboard	19
Verify Palo Alto Traps knowledge pack in EventTracker	20
Category	20
Alerts	21
Token Template.....	22
Knowledge Object	23
Flex Report.....	23
Dashboard	25

Overview

Palo Alto Traps advanced endpoint protection stops threat on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. Traps stands apart in its ability to protect endpoints. It blocks security breaches and successful ransomware attacks that leverage malware and exploits, known or unknown, before they can compromise endpoints.

EventTracker helps to monitor events from **Palo Alto Traps**. It's knowledge object and flex reports will help you to analyze file threats detected, ESM activities, and agent activities and to monitor policy or configuration changes.

Prerequisites

- **EventTracker v8.x or above** should be installed.
- **Palo Alto Traps** should be configured.
- Create a **rule** in **EventTracker Manager Workstation** firewall for inbound and outbound to allow **UDP** port **514**.

Integration of Palo Alto Traps with EventTracker Manager

To configure Palo Alto Traps to forward logs to a syslog server,

1. Enable log forwarding.
 - From the ESM Console, select **Settings -> ESM -> Syslog**, and then **Enable Syslog**.
2. Configure the settings to send logs from ESM components to an external logging platform.

Configure the following settings:

- **Syslog Server**—Enter the IP address of **EventTracker Manager**.
 - **Syslog Port**—Set port as **514(UDP)**.
 - **Syslog Protocol**—Set the format to **CEF**.
 - **Keep-alive Timeout**—Period (in minutes) in which Traps sends a keep-alive message to the external logging platform (default is 0; range is 0 to 2,147,483,647). A value of 0 specifies that you do not want to send a keep-alive message to the external logging platform.
 - **Communication Protocol**—Set as **UDP**.
3. Select the events that you want to send to the external logging platform.

- In the **Logging Events** area, select one or more of the events. Scroll through the list to see additional types of events you can send.
- 4. Save your settings.
 - Click **Save**.
- 5. Verify the configuration of your settings.
 - Click **Check Connectivity**. The ESM Console sends a test communication to the external logging platform using the settings you configured. If you do not receive the test message, confirm that your settings are correct and then try again.

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Palo Alto Traps Business.

Category

- **Palo Alto Traps- Agent activity-** This category provides information related to all the agent activities such as agent content update, agent policy change and so on.
- **Palo Alto Traps- Agent status-** This category provides information related to all the agent status such as client license invalid, client license request, enabled protection and so on.
- **Palo Alto Traps- ESM configuration change-** This category provides information related to all the ESM configuration changes that are done.
- **Palo Alto Traps- ESM policy change-** This category provides information related to all the ESM policy changes that are done.
- **Palo Alto Traps- ESM system activity-** This category provides information related to all the system activities such as archived preventions, archived preventions failure, file upload failure and so on.
- **Palo Alto Traps- ESM user logon-** This category provides information related to all the user logon activities.
- **Palo Alto Traps- Threats detected-** This category provides information related to all the threats that are detected by Palo Alto Traps.

Alerts

- **Palo Alto Traps: Critical agent activity:** This alert is generated when any critical agent activity is done.
- **Palo Alto Traps: Critical license usage:** This alert is generated when any critical license usage is tracked.
- **Palo Alto Traps: Policy changed:** This alert is generated when any policy is changed.
- **Palo Alto Traps: Threats detected:** This alert is generated when any threat is detected.

- **Palo Alto Traps: User logins:** This alert is generated when any user logon occurs.

Knowledge Object

- **Palo Alto Traps All knowledge objects-** This knowledge object will help us to analyze every type of logs of Palo Alto Traps differentiated by respective categories.

Flex Reports

- **Palo Alto Traps- Threats detected-** This report gives the information about all the threats that are detected by Palo Alto Traps.

LogTime	Computer	Source Device Name	Destination Host Name	Destination User Name	Module Name	Event Name	File Hash	Event Priority	Event Details
08/09/2018 05:34:17 PM	ContosoR80	112.1.144.12	Contoso-12	Janet	EPM1.1	Access Violation		5	
08/09/2018 05:34:17 PM	ContosoR80	10.163.15.14	Contoso-144	Xavier	EPM1.2	Notification Event	5D785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473	4	New notification event. Prevention Key: w9gh4gh4r54g6wg496g49
08/09/2018 05:34:17 PM	ContosoR80	127.12.13.11	ACME-RS1	Brenda	EPM1.1	Post Detection Event	6A785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473	4	New post detection event. Prevention Key: d64bgweg7eg6ege9g256
08/09/2018 05:34:17 PM	ContosoR80	110.12.36.25	Contoso-124	Janet	EPM1.0.1	Prevention Event	9A785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473	5	New prevention event. Prevention Key: e7gfgth5tjkl98oi899
08/09/2018 05:34:17 PM	ContosoR80	114.1.4.43	ACME-RSVM	Leo	EPM1.1	Provisional Event	4B785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473	5	New provisional event. Prevention Key: o6nt7k9965h623g2bm9u
08/09/2018 05:34:17 PM	ContosoR80	127.12.13.11	Contoso-12	Albert	EPM1.0.1	Service Warning		5	Warning- Java sandboxed file access to 164.45.1.13

Figure 1

Logs Considered

Aug 09 05:34:17 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0(Palo Alto Networks)Traps Agent(3.4.1.16709)Service Warning(Threat)5[rt=Aug 08 2017 21:18:25 dhost=Contoso-12 duser=Albert cs2Label=Module cs2=EPM1.0.1 dvc=...
add_info	+ 3.4.1.16709
add_info8	+ EPM1.0.1
dest_host_name	+ Contoso-12
dest_user_name	+ Albert
device_name	+ 127.12.13.11
event_category	+ 0
event_computer	+ Samplelogs
event_datetime	+ 8/9/2018 5:34:17 PM
event_datetime_utc	+ 1533816257
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0(Palo Alto Networks)Traps Agent(3.4.1.16709)Service Warning(Threat)5[rt=Aug 08 2017 21:18:25 dhost=Contoso-12 duser=Albert cs2Label=Module cs2=EPM1.0.1 dvc=...=127.12.13.11 msg=Warning- Java sandboxed file access to 164.45.1.13
event_id	+ 3333
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_category	+ Threat
log_datetime	+ Aug 08 2017 21:18:25
log_info	+ Warning- Java sandboxed file access to 164.45.1.13
log_priority	+ 5
log_source	+ Palo Alto Traps All knowledge objects
log_type	+ Service Warning
tags	+ User Logon
tags	+ Palo Alto Traps
tags	+ Threats detected
tags	+ configuration and policy change
tags	+ agent activities

Figure 2

- Palo Alto Traps- ESM configuration changes**– This report gives the information about all the ESM configuration changes that are done.

LogTime	Computer	Source Host Name	Source User Name	Destination Host Name	Event Name	Event Priority	Event Details
08/09/2018 05:34:18 PM	ContosoR80	Contoso-13	peter	ACME-11	Condition Deleted	5	Condition ID: 1459876 was deleted
08/09/2018 05:34:18 PM	ContosoR80	Contoso-47	susan		User Edited	5	User edward was added/changed.
08/09/2018 05:34:18 PM	ContosoR80	Contoso-46	Wendy		User Deleted	5	User wendy was deleted.
08/09/2018 05:34:18 PM	ContosoR80	Contoso-45	victoria	ACME-15	Sending License To Client	5	New license sent
08/09/2018 05:34:18 PM	ContosoR80	Contoso-44	Wendy		Role Status Changed	5	Secure11 status was changed to operational
08/09/2018 05:34:18 PM	ContosoR80	Contoso-40	lucy		Role Edited	5	Role operator was added/changed
08/09/2018 05:34:18 PM	ContosoR80	Contoso-40	salah		Role Deleted	5	Role security admin was deleted
08/09/2018 05:34:18 PM	ContosoR80	Contoso-40	Wendy		Restriction Settings Edited	5	Restriction Settings were added/changed

Figure 3

Logs Considered

addl_info	+• 4.0.2.1
event_category	+• 0
event_computer	+• Samplelogs
event_datetime	+• 8/9/2018 5:34:18 PM
event_datetime_utc	+• 1533816258
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 Restriction Settings Edited(Config 3 rt=Aug 08 2017 21:18:25 shost=Contoso-40 suser=Wendy msg=Restriction Settings were added/changed
event_id	+• 3333
event_log_type	+• Application
event_source	+• syslog
event_type	+• Information
event_user_domain	+• N/A
event_user_name	+• N/A
log_category	+• Config
log_datetime	+• Aug 08 2017 21:18:25
log_info	+• Restriction Settings were added/changed
log_priority	+• 3
log_source	+• Palo Alto Traps All knowledge objects
log_type	+• Restriction Settings Edited
src_host_name	+• Contoso-40
src_user_name	+• Wendy
tags	+• User Logon
tags	+• Palo Alto Traps
tags	+• Threats detected
tags	+• configuration and policy change
tags	+• agent activities

Figure 4

- Palo Alto Traps- ESM policy changes**–This report gives information about all the ESM policy changes that are done.

LogTime	Computer	Source Host Name	Source User Name	Event Name	Event Type	Event Priority	Event Details
08/09/2018 05:34:18 PM	ContosoR80	Contoso-43	su	Server Content Update Success	Policy	3	Content version was updated to 3.21.1 successfully
08/09/2018 05:34:18 PM	ContosoR80	Contoso-46	hazard	Verdict Reverted To WildFire	Policy	3	Hash verdict reverted to WildFire. Oldhash11 -> Newhash12
08/09/2018 05:34:18 PM	ContosoR80	Contoso-41	watson	New Hash Added	Policy	3	New hash added
08/09/2018 05:34:18 PM	ContosoR80	Contoso-41	penny	Trusted Signer Changed	Policy	3	Hash 6A785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9064F1BE1C1B473 trusted signer changed automatically from SignedX1 to SignedX4
08/09/2018 05:34:18 PM	ContosoR80	Contoso-41	xander	Rule Deleted	Policy	3	Rule M469: Deleted
08/09/2018 05:34:18 PM	ContosoR80	Contoso-44	corrie	Rule Edited	Policy	3	Rule 9599vi Edited

Figure 5

Logs Considered

Aug 09 05:34:18 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 Server Content Update Failed Policy 3 rt=Aug 08 2017 21:18:25 shost=Contoso-45 suser=naoimi msg=Content version failed to ...
addl_info	+ 4.0.2.1
event_category	+ 0
event_computer	+ Samplelogs
event_datetime	+ 8/9/2018 5:34:18 PM
event_datetime_utc	+ 1533816258
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 Server Content Update Failed Policy 3 rt=Aug 08 2017 21:18:25 shost=Contoso-45 suser=naoimi msg=Content version failed to ... o update to 3.21.1. Error: Failed to update xx01g0
event_id	+ 3333
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_category	+ Policy
log_datetime	+ Aug 08 2017 21:18:25
log_info	+ Content version failed to update to 3.21.1. Error: Failed to update xx01g0
log_priority	+ 3
log_source	+ Palo Alto Traps All knowledge objects
log_type	+ Server Content Update Failed
src_host_name	+ Contoso-45
src_user_name	+ naoimi
tags	+ User Logon
tags	+ Palo Alto Traps
tags	+ Threats detected
tags	+ configuration and policy change
tags	+ agent activities

Figure 6

- Palo Alto Traps- Agent status**-This report gives information about all the agent status such as client license invalid, client license request, enabled protection and so on.

LogTime	Computer	Destination Host Name	Destination User Name	Event Name	Event Priority	Event Details
08/09/2018 05:34:17 PM	ContosoR80	Contoso-11	Janet	Agent Content Update	3	Contoso-11 received new content-version 4.21.3.0
08/09/2018 05:34:17 PM	ContosoR80	Contoso-13	Eric	Agent Policy Changed	3	Policy changed
08/09/2018 05:34:17 PM	ContosoR80	Contoso-14	Brian	Agent Install	3	Agent installed
08/09/2018 05:34:17 PM	ContosoR80	AcmeCM	edward	Agent Uninstall	3	Agent uninstalled
08/09/2018 05:34:17 PM	ContosoR80	AcmeCM	lily	Agent Upgrade	3	Agent upgraded
08/09/2018 05:34:47 PM	ContosoR80	Contoso-11	Janet	Agent Content Update	3	Contoso-11 received new content-version 4.21.3.0

Figure 7

Logs Considered

Aug 09 05:34:17 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0(Palo Alto Networks)Traps Agent(4.0.2.1)Quarantine Failed(Agent)3(rt=Aug 08 2017 21:18:25 dhost=Contoso-11 duser=varan msg=File eicar.php could not be quarantined, reason: Manual cleanup required.
addl_info	+ 4.0.2.1
dest_host_name	+ Contoso-11
dest_user_name	+ varan
event_category	+ 0
event_computer	+ Samplelogs
event_datetime	+ 8/9/2018 5:34:17 PM
event_datetime_utc	+ 1533816257
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0(Palo Alto Networks)Traps Agent(4.0.2.1)Quarantine Failed(Agent)3(rt=Aug 08 2017 21:18:25 dhost=Contoso-11 duser=varan msg=File eicar.php could not be quarantined, reason: Manual cleanup required.
event_id	+ 3333
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_category	+ Agent
log_datetime	+ Aug 08 2017 21:18:25
log_info	+ File eicar.php could not be quarantined, reason: Manual cleanup required.
log_priority	+ 3
log_source	+ Palo Alto Traps All knowledge objects
log_type	+ Quarantine Failed
tags	+ User Logon
tags	+ Palo Alto Traps
tags	+ Threats detected
tags	+ configuration and policy change
tags	+ agent activities

Figure 8

- Palo Alto Traps- Agent activities**-This report gives information about all the agent activities such as agent content update, agent policy change and so on.

LogTime	Computer	Destination Host Name	Destination User Name	Event Name	Event Priority	Event Details
08/09/2018 05:34:17 PM	ContosoR80	Contoso-14	Janet	Quarantine Quota Exceeded	3	File eicr.php was permanently removed from the quarantine folder because quota was exceeded
08/09/2018 05:34:17 PM	ContosoR80	AcmeCM1	edward	Traps Service Status Change	3	Agent Service Status Changed: Stopped -> Started
08/09/2018 05:34:17 PM	ContosoR80	Contoso-11	Janet	Local Analysis Extraction Failed	3	Local Analysis Feature Extraction Failed
08/09/2018 05:34:17 PM	ContosoR80	AcmeCM	lily	Local Analysis Module Failed	3	Add new module into Local Analysis- Failed
08/09/2018 05:34:17 PM	ContosoR80	Contoso-14	varan	Local Analysis Module Succeeded	3	Add new module into Local Analysis- Succeeded
08/09/2018 05:34:17 PM	ContosoR80	Contoso-11	lily	One Time Action Complete	3	One Time Action completed. Action Type: uninstall. Action ID: 4785423
08/09/2018 05:34:17 PM	ContosoR80	Contoso-11	Janet	One Time Action Failed	3	One Time Action failed to run. Action Type: modify
08/09/2018 05:34:17 PM	ContosoR80	Contoso-11	lily	Process Crashed	3	Process TLms45-err had crashed

Figure 9

Logs Considered:

Aug 09 05:34:17 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps Agent 4.0.2.1 Agent Uninstall Agent 3 rt=Aug 08 2017 21:18:25 dhost=AcmeCM duser=edward msg=Agent uninstalled
add_info	+ 4.0.2.1
dest_host_name	+ AcmeCM
dest_user_name	+ edward
event_category	+ 0
event_computer	+ Samplelogs
event_datetime	+ 8/9/2018 5:34:17 PM
event_datetime_utc	+ 1533816257
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps Agent 4.0.2.1 Agent Uninstall Agent 3 rt=Aug 08 2017 21:18:25 dhost=AcmeCM duser=edward msg=Agent uninstalled
event_id	+ 3333
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_category	+ Agent
log_datetime	+ Aug 08 2017 21:18:25
log_info	+ Agent uninstalled
log_priority	+ 3
log_source	+ Palo Alto Traps All knowledge objects
log_type	+ Agent Uninstall
tags	+ User Logon
tags	+ Palo Alto Traps
tags	+ Threats detected
tags	+ configuration and policy change
tags	+ agent activities

Figure 10

- Palo Alto Traps- ESM system activities**-This report gives information about all the system activities such as archived preventions, archived preventions failure, file upload failure and so on.

LogTime	Computer	Source Host Name	Source User Name	Destination Host Name	Destination User Name	Event Name	Event Priority	Event Details
08/09/2018 05:34:17 PM	ContosoR80	Contoso11	Kim	Acme11	Jannet	Preventions Archived	3	Detailed description here
08/09/2018 05:34:18 PM	ContosoR80	Contoso-12	john	ACME-15		Machine License Validation Failed	3	License Validation Failed
08/09/2018 05:34:18 PM	ContosoR80	Contoso-13	Wendy	ACME-15		Local Analysis Model Unavailable	3	Local Analysis Model Unavailable
08/09/2018 05:34:18 PM	ContosoR80	Contoso-19	fiona	ACME-15		License Quantity	3	Agent Licenses are running low
08/09/2018 05:34:18 PM	ContosoR80	Contoso-19	Wendy	ACME-15		License Pool Added	3	A pool of 45 licenses of type enroll have been added
08/09/2018 05:34:18 PM	ContosoR80	Contoso-19	miller	ACME-45	ivin	License Expiration	3	mempool licenses will expire in 15 days
08/09/2018 05:34:18 PM	ContosoR80	Contoso-13	susan	ACME-11	kelly	File Upload Failure	3	File failed to upload
08/09/2018 05:34:18 PM	ContosoR80	Contoso-13	eric	ACME-12		ESM Status Change	3	ESM status changed
08/09/2018 05:34:18 PM	ContosoR80	Contoso-15	ivin	ACME-15		ESM Configuration Change	3	Multi ESM configurations has changed
08/09/2018 05:34:18 PM	ContosoR80	Contoso-11	eric	ACME-15		Preventions Archived Failed	3	Archived preventions failed

Figure 11

Logs Considered:

Aug 09 05:34:18 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 Communications Check With Proxy[System]3 rt=Aug 08 2017 21:18:25 shost=Contoso-11 suser=Wendy dhost=ACME-14 msg=C...
addl_info	+• 4.0.2.1
dest_host_name	+• ACME-14
event_category	+• 0
event_computer	+• Samplelogs
event_datetime	+• 8/9/2018 5:34:18 PM
event_datetime_utc	+• 1533916258
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 Communications Check With Proxy[System]3 rt=Aug 08 2017 21:18:25 shost=Contoso-11 suser=Wendy dhost=ACME-14 msg=Communications check with Proxy on host 'ACME-15'. Status: Successfully completed
event_id	+• 3333
event_log_type	+• Application
event_source	+• syslog
event_type	+• Information
event_user_domain	+• N/A
event_user_name	+• N/A
log_category	+• System
log_datetime	+• Aug 08 2017 21:18:25
log_info	+• Communications check with Proxy on host 'ACME-15'. Status: Successfully completed
log_priority	+• 3
log_source	+• Palo Alto Traps All knowledge objects
log_type	+• Communications Check With Proxy
src_host_name	+• Contoso-11
src_user_name	+• Wendy
tags	+• User Logon
tags	+• Palo Alto Traps
tags	+• Threats detected
tags	+• configuration and policy change
tags	+• agent activities

Figure 12

- **Palo Alto Traps- ESM user logon activities**-This report gives information about all the user logon activities.

LogTime	Computer	Source Host Name	Source User Name	Event Name	Event Priority	Event Details
08/09/2018 05:34:18 PM	ContosoR80	Contoso-15	albert	User Login	3	User janet logged in to ESM console
08/09/2018 05:34:48 PM	ContosoR80	Contoso-15	albert	User Login	3	User janet logged in to ESM console

Figure 13

Logs Considered:

Aug 09 05:34:18 PM	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 User Login System 3 rt=Aug 08 2017 21:18:25 shost=Contoso-15 user=albert msg=User janet logged in to ESM console
addl_info	+ 4.0.2.1
event_category	+ 0
event_computer	+ Samplelogs
event_datetime	+ 8/9/2018 5:34:18 PM
event_datetime_utc	+ 1533816258
event_description	Aug 01 10:57:58 traps Aug 08 2017 21:18:25 10.8.4.225 CEF:0 Palo Alto Networks Traps ESM 4.0.2.1 User Login System 3 rt=Aug 08 2017 21:18:25 shost=Contoso-15 user=albert msg=User janet logged in to ESM console
event_id	+ 3333
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_category	+ System
log_datetime	+ Aug 08 2017 21:18:25
log_info	+ User janet logged in to ESM console
log_priority	+ 3
log_source	+ Palo Alto Traps All knowledge objects
log_type	+ User Login
src_host_name	+ Contoso-15
src_user_name	+ albert
tags	+ User Logon
tags	+ Palo Alto Traps
tags	+ Threats detected
tags	+ configuration and policy change
tags	+ agent activities

Figure 14

Import Palo Alto Traps knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Token Templates
- Knowledge Objects
- Flex Reports

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.

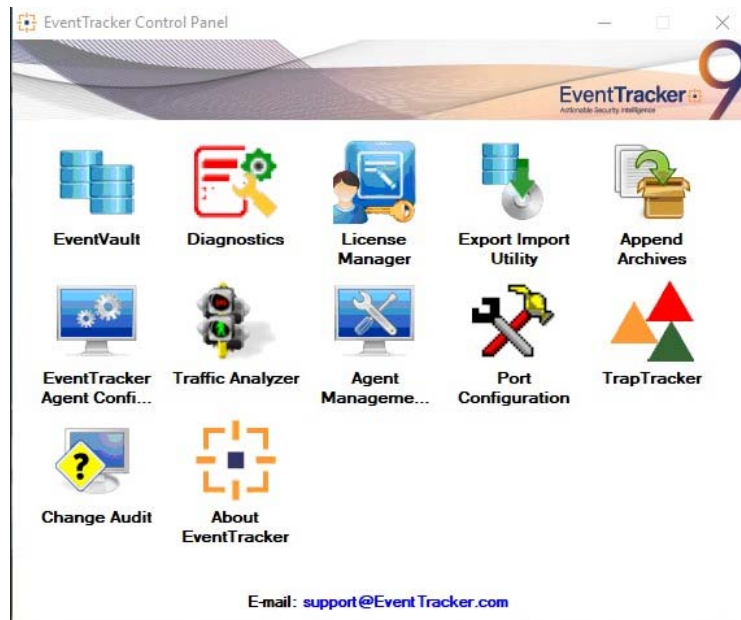



Figure 15

3. Click the **Import** tab.

Category

1. Click **Category** option, and then click the browse  button.

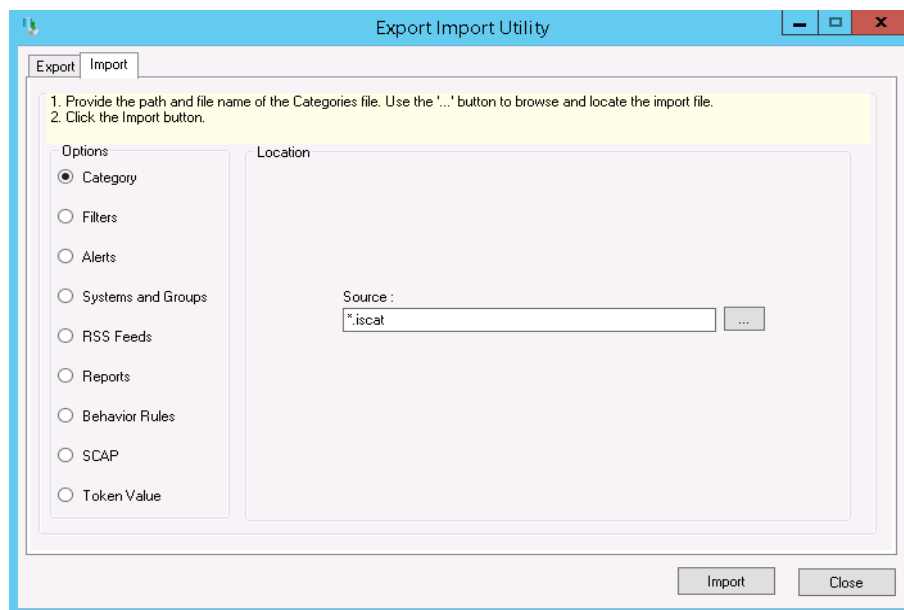


Figure 16

2. Locate **Category_PaloAlto_Traps.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

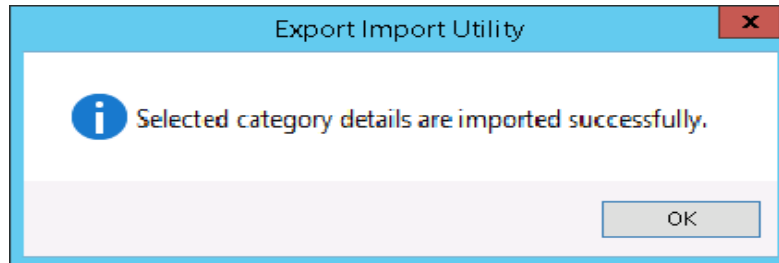



Figure 17

4. Click **OK**, and then click the **Close** button.

Alerts

1. Click **Alert** option, and then click the **browse**  button.

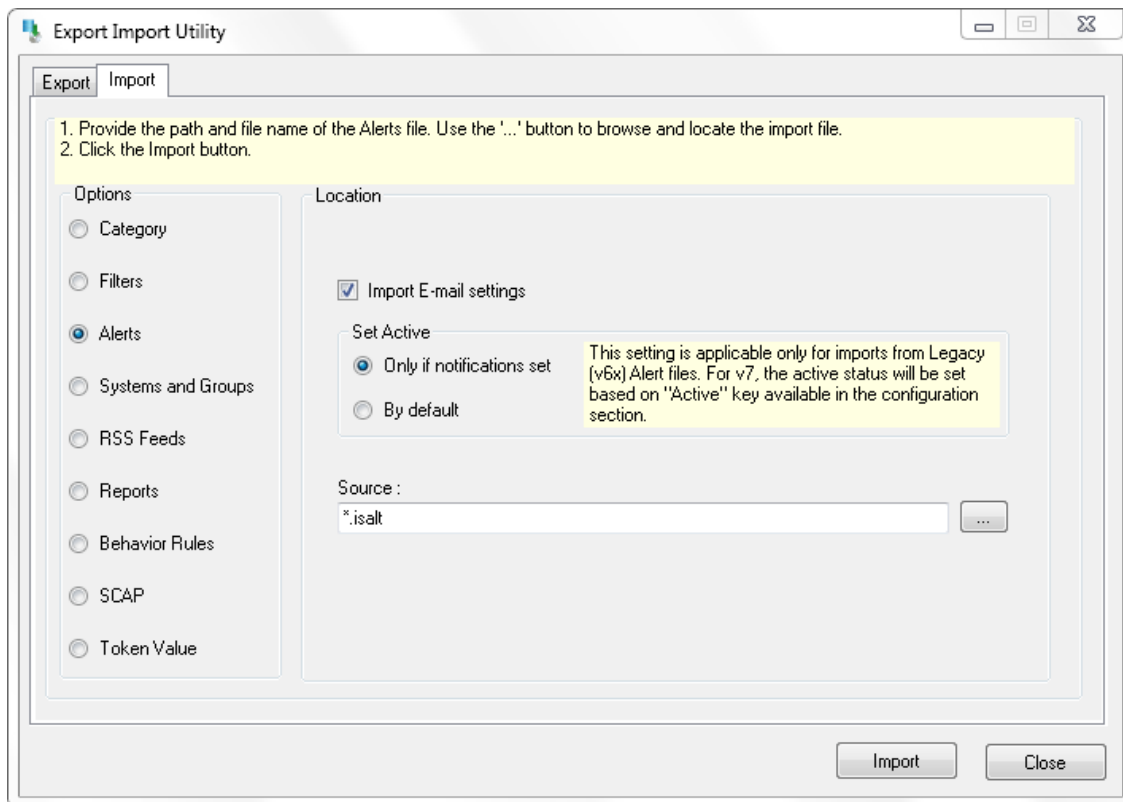


Figure 18

2. Locate **Alerts_PaloAlto_Traps.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
4. EventTracker displays success message.

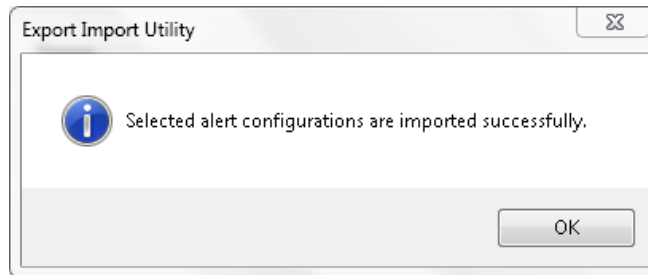


Figure 19

Click the **OK** button, and then click the **Close** button.

Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.

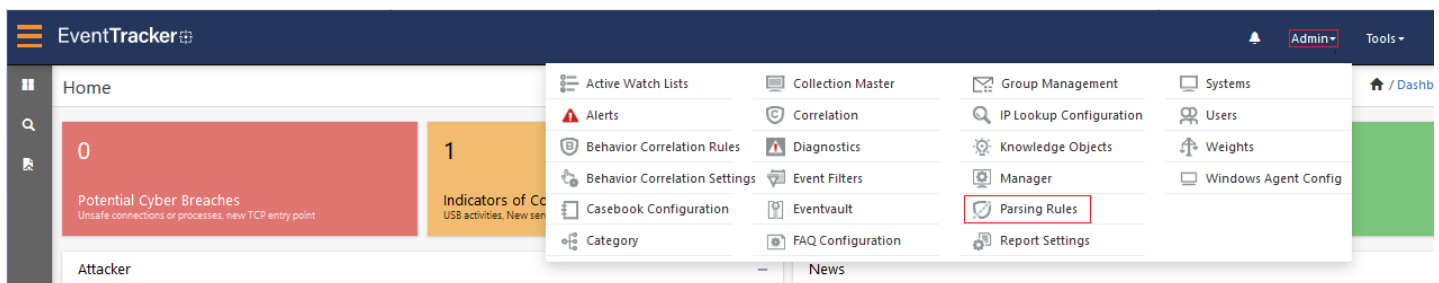



Figure 20

2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file named **Template_PaloAlto_Traps.ettd**.

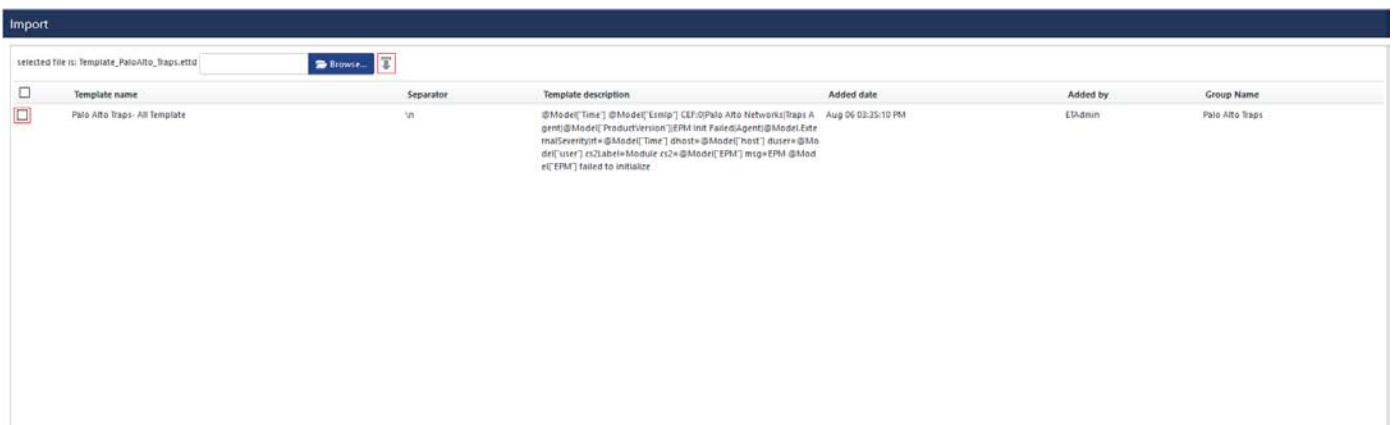



Figure 21

4. Now select all the check box and then click on  Import option.

Knowledge Object

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

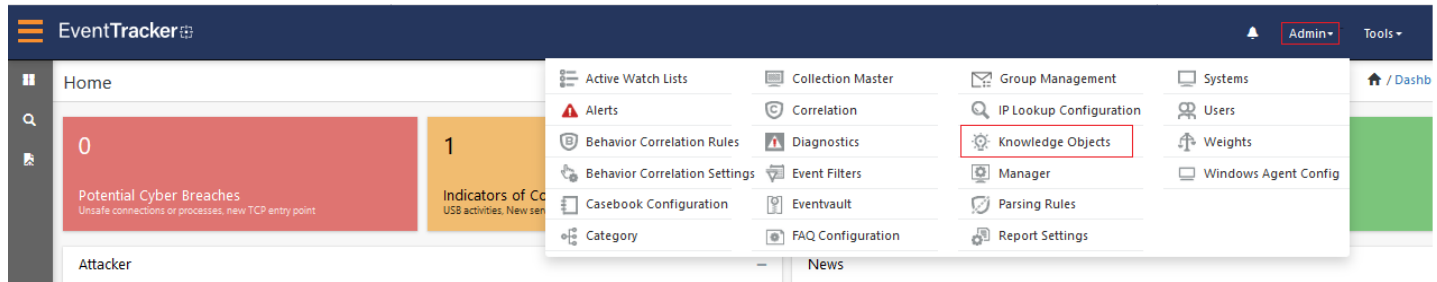


Figure 22

2. Click on **Import** button as highlighted in the below image.



Figure 23

3. Click on **Browse**.

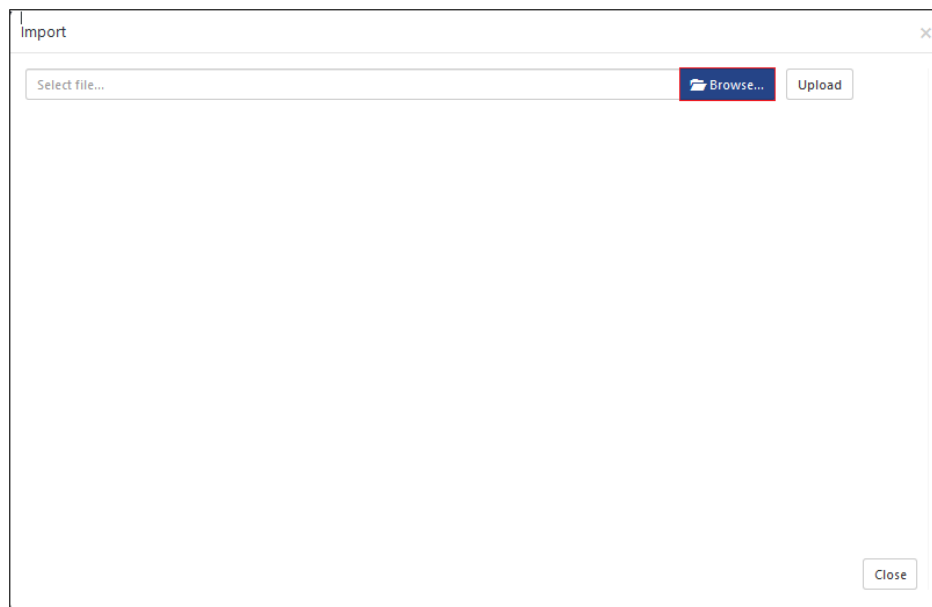



Figure 24

4. Locate the file named **KO_PaloAlto_Traps.etko**.
5. Now select all the check box and then click on  'Import' option.

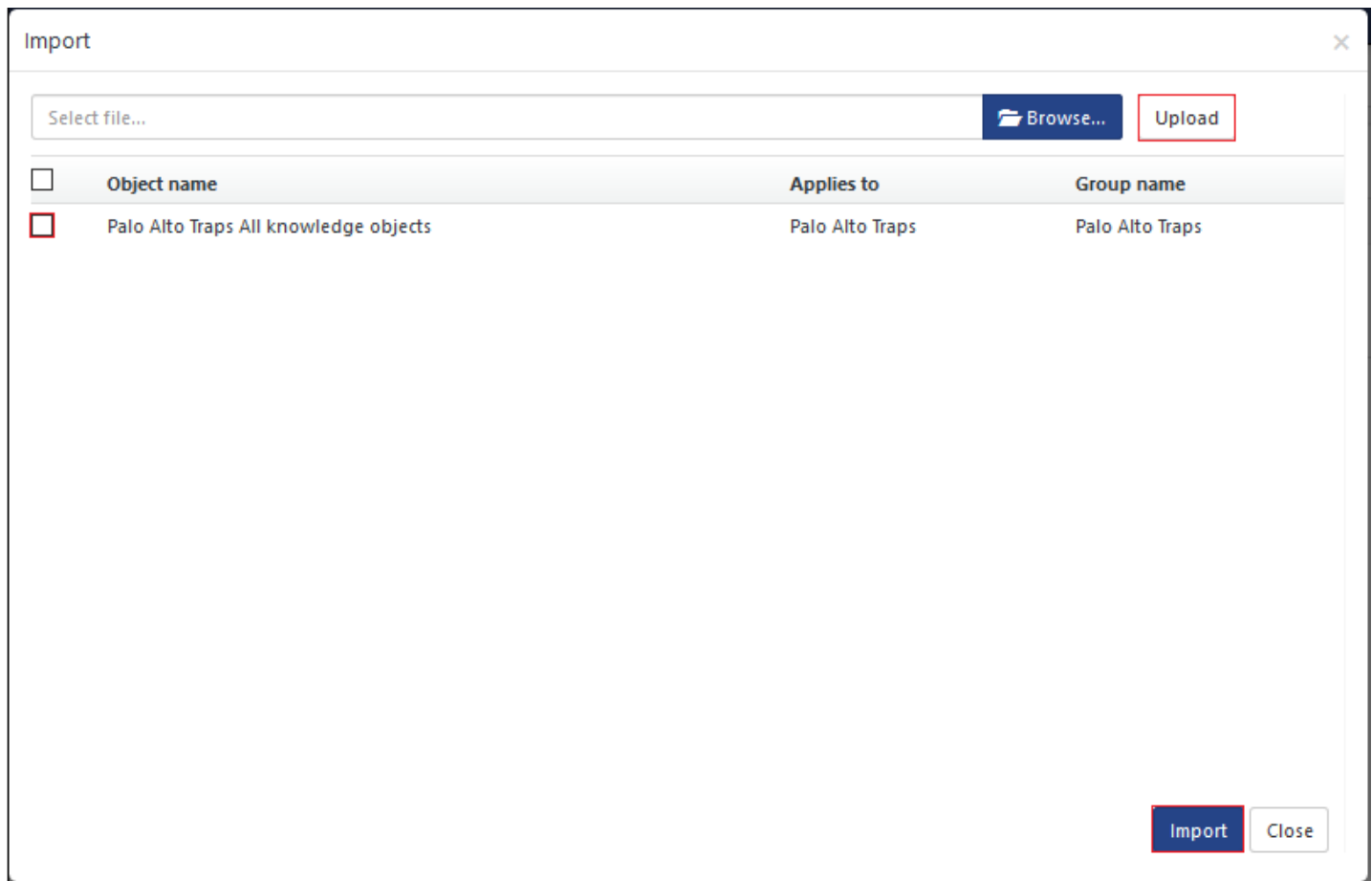


Figure 25

6. Knowledge objects are now imported successfully.

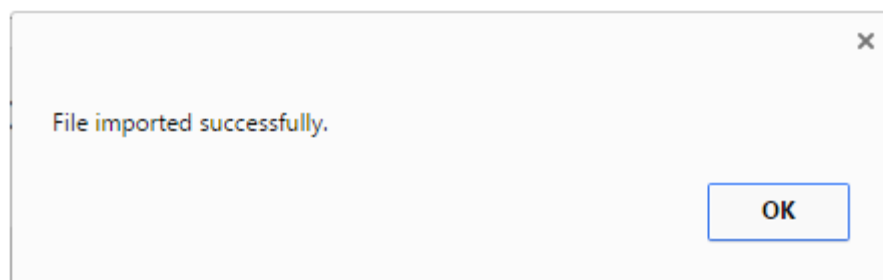


Figure 26

Flex Report

On **EventTracker Control Panel**,

1. Click **Reports** option, and select **New (*.etcrx)** option.

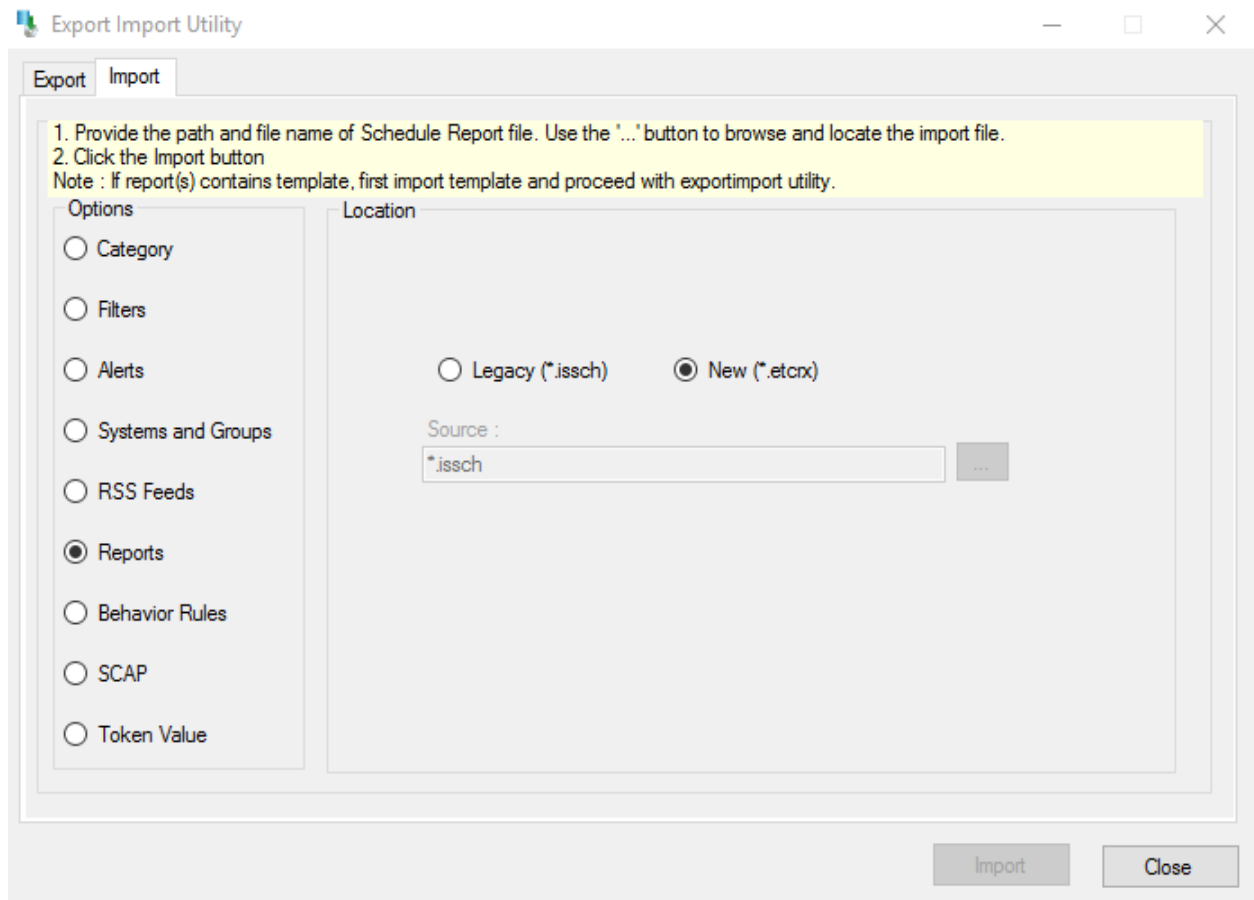


Figure 27

2. Locate the file named **Reports_PaloAlto_Traps.etcrx** and select all the check box.

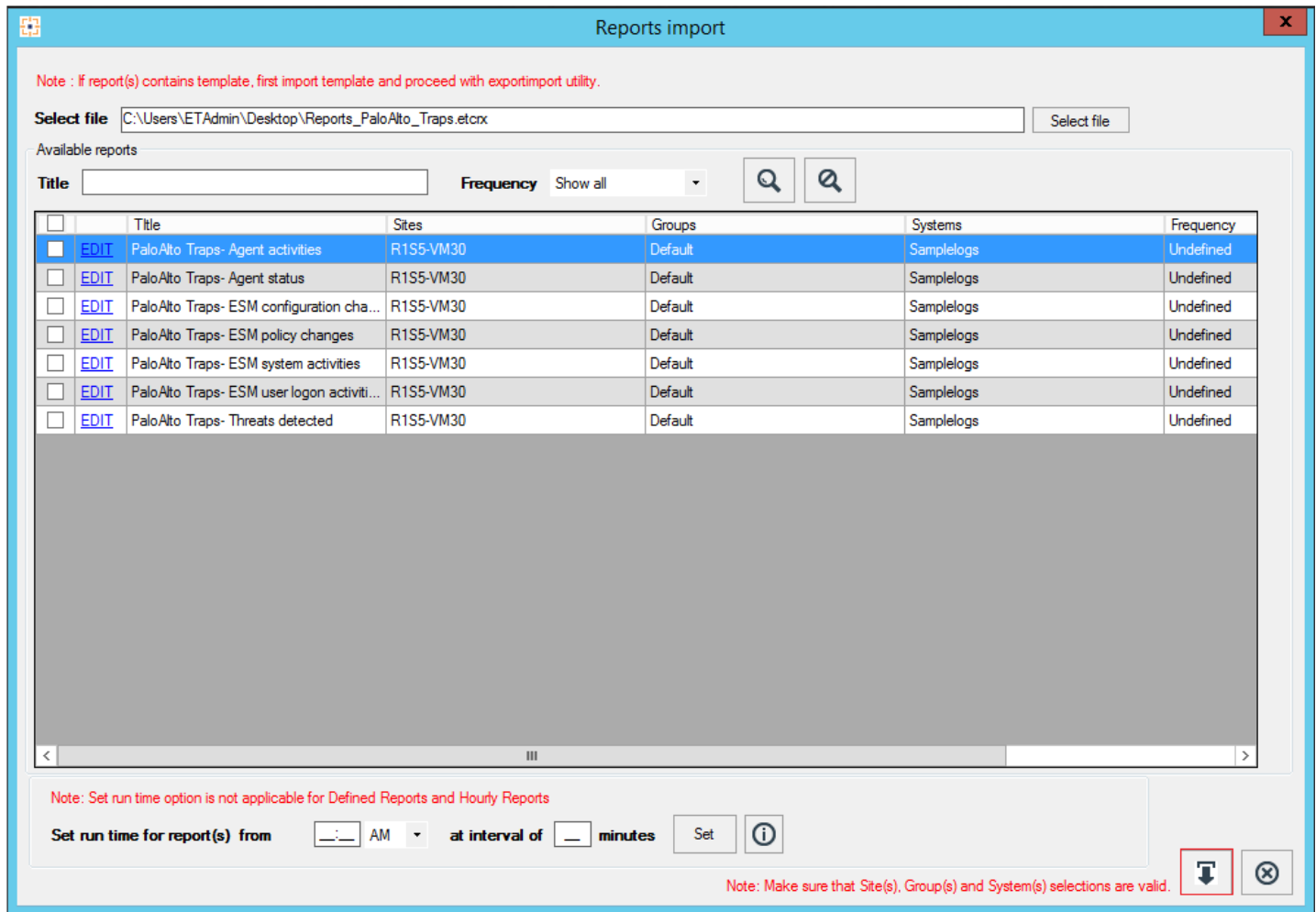


Figure 28

- Click the **Import** button to import the reports. EventTracker displays success message.

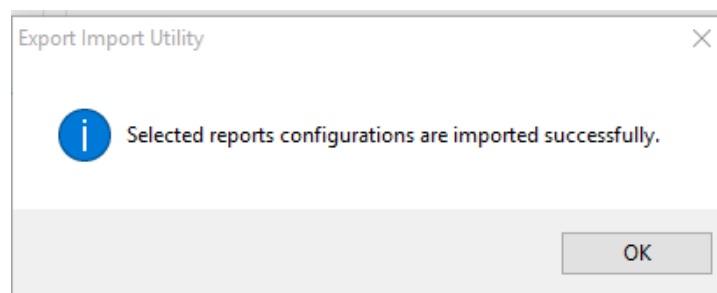


Figure 29

Dashboard

NOTE- Below steps given are specific to EventTracker 9 and later.

- Open **EventTracker Enterprise** in browser and login.

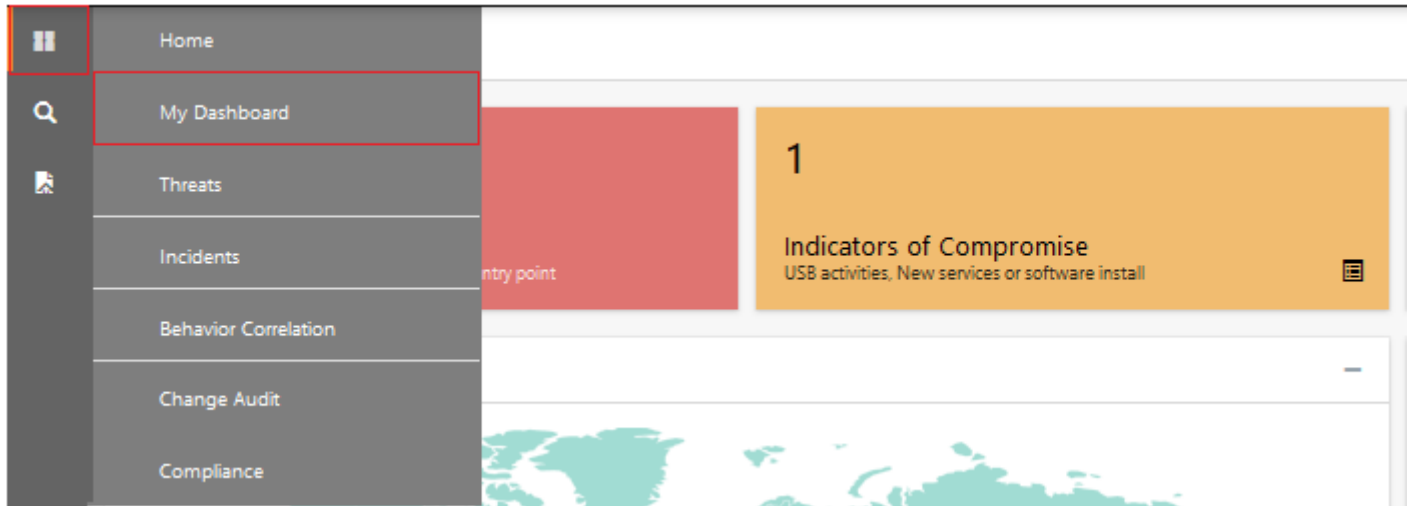


Figure 30

- Navigate to **My Dashboard** option as shown above.
- Click on the **Import** button as show below:



Figure 31

- Import dashboard file **Dashboard_PaloAlto_Traps.etwd** and select the dashlets that you require and click on **Import** as shown below:

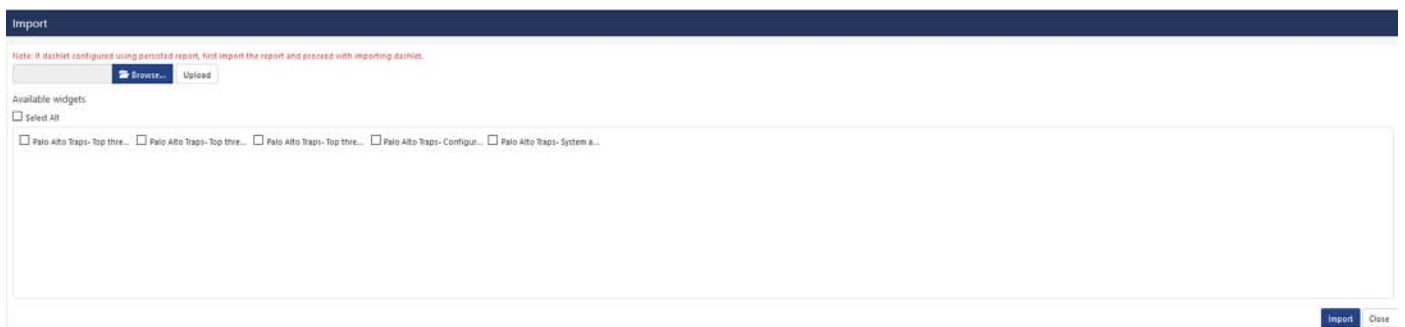


Figure 32

- Import is now completed successfully.

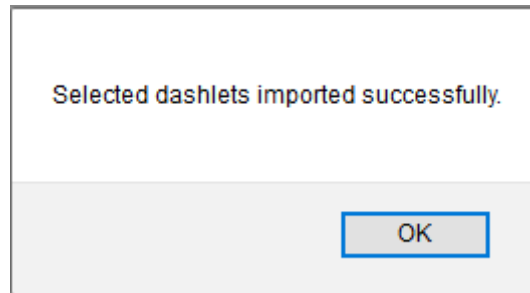


Figure 33

Verify Palo Alto Traps knowledge pack in EventTracker

Category

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.

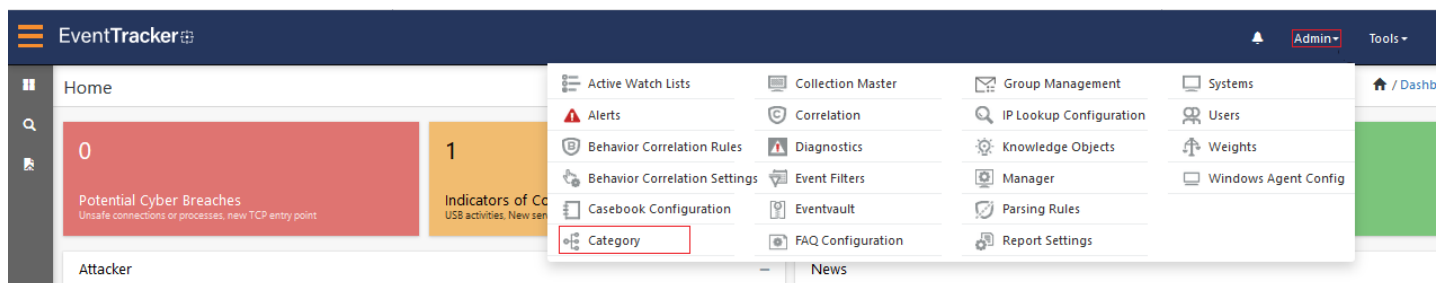


Figure 34

3. In **Category Tree** to view imported categories, scroll down and expand Palo Alto Traps Business group folder to view the imported categories.

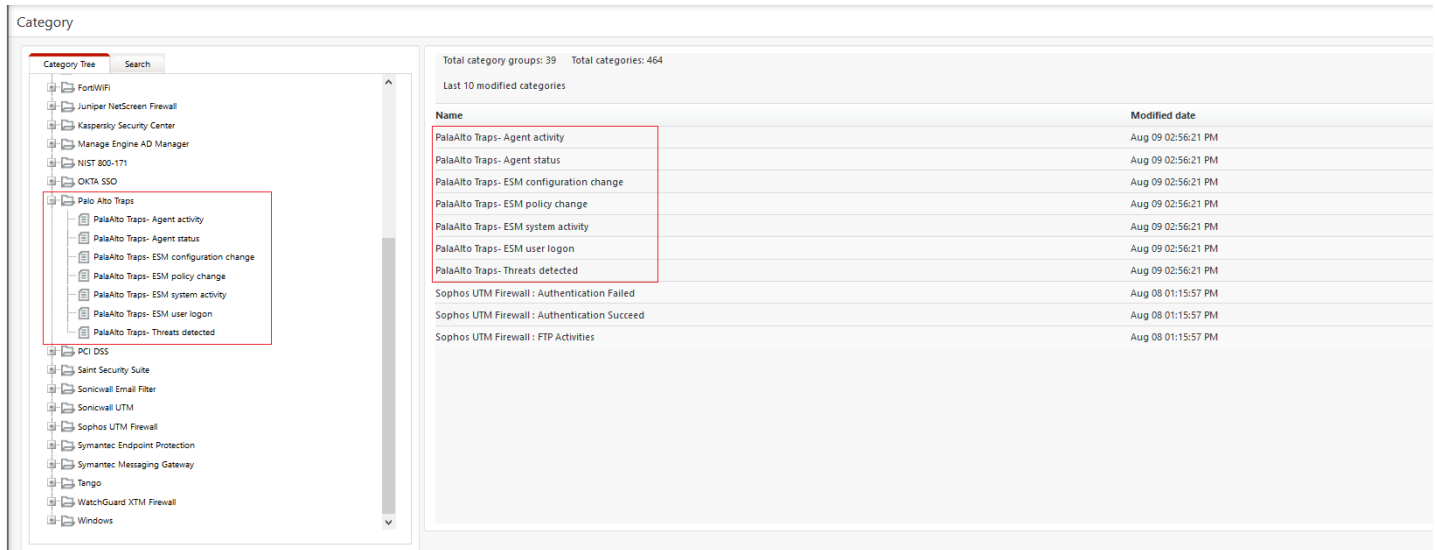


Figure 35

Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.

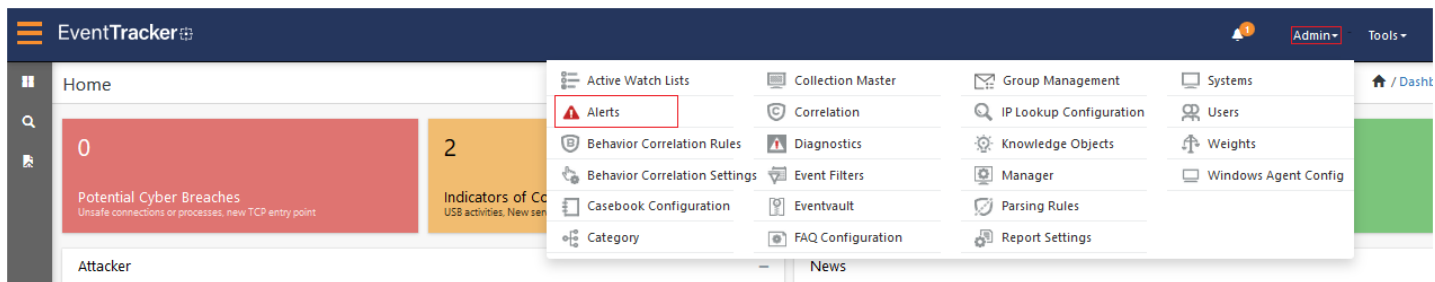


Figure 36

3. In the **Search** box, type '**Traps**', and then click the **Go** button.
Alert Management page will display all the imported alerts.

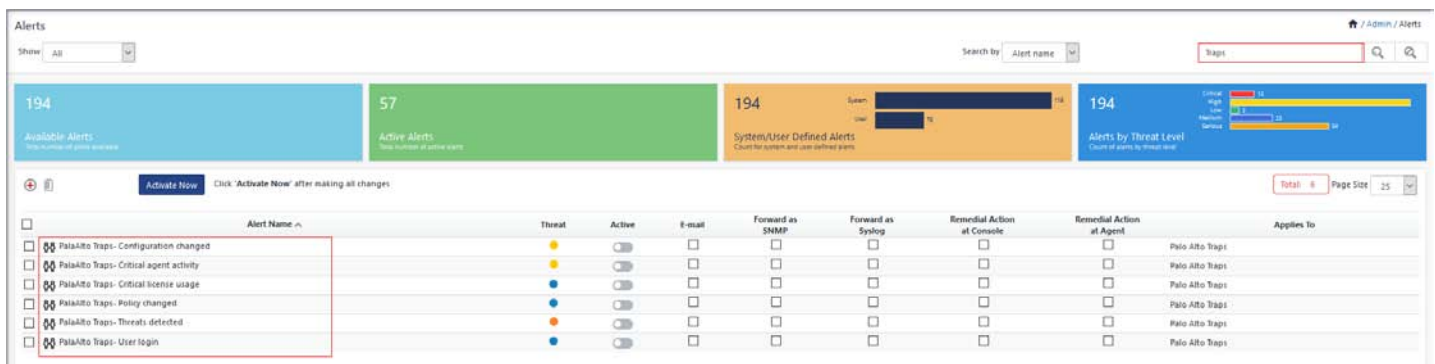


Figure 37

- To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

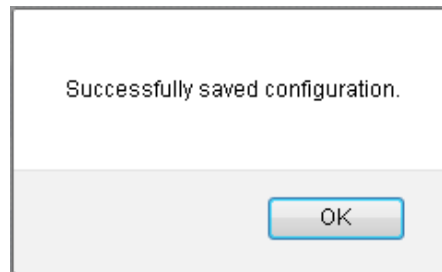


Figure 38

- Click **OK**, and then click the **Activate Now** button.

NOTE: Please specify appropriate **systems** in **alert configuration** for better performance.

Token Template

- In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

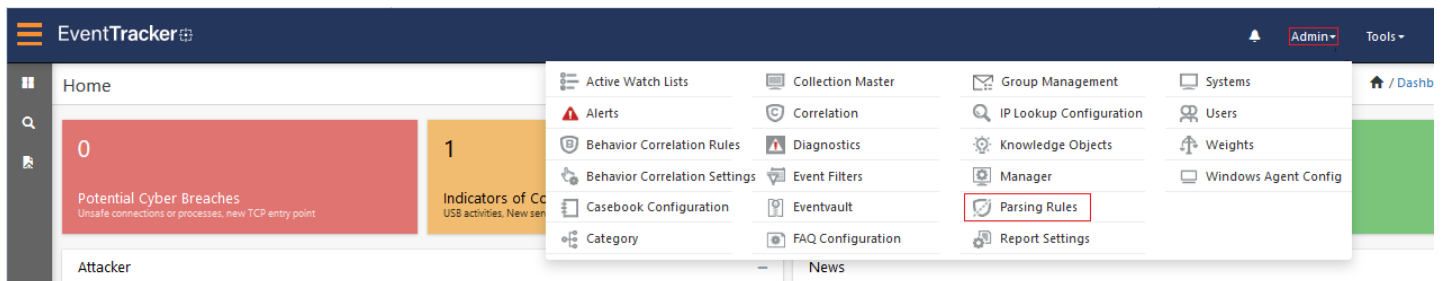


Figure 39

- On **Template** tab, click on the **Palo Alto Traps** group folder to view the imported Templates.

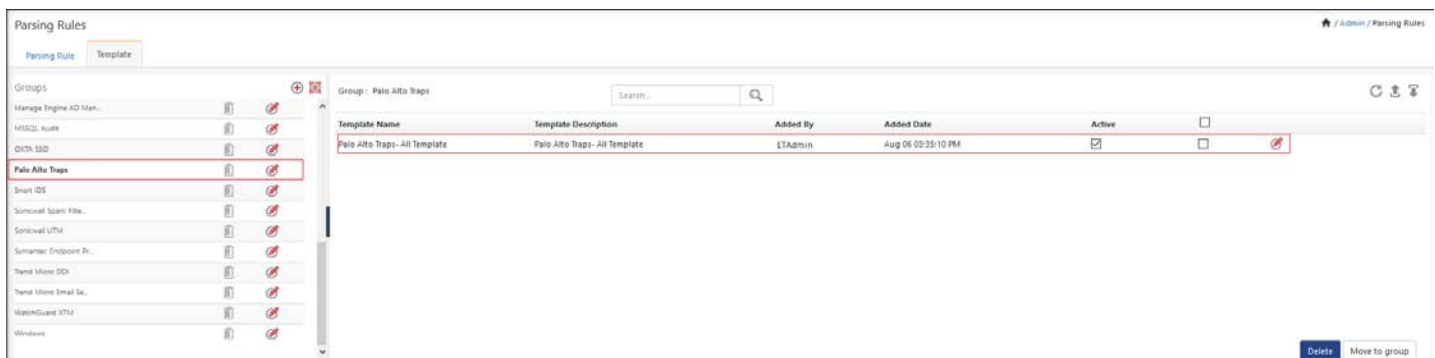


Figure 40

Knowledge Object

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

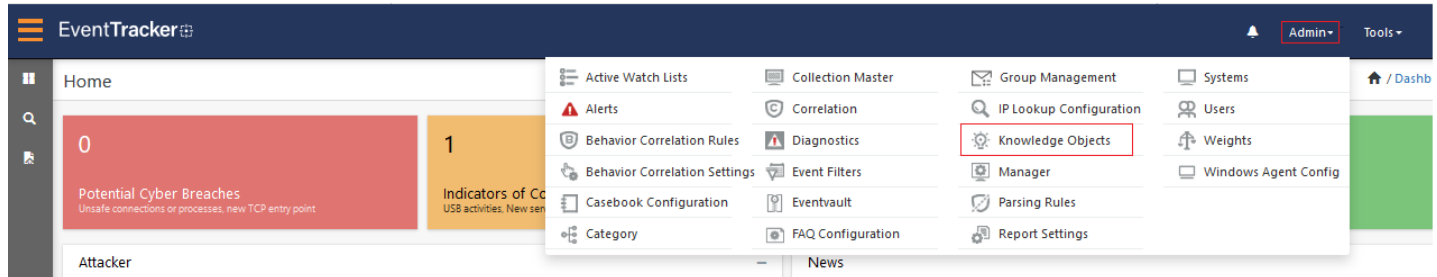


Figure 41

2. In the Knowledge Object tree, expand **Palo Alto Traps** group folder to view the imported Knowledge objects.

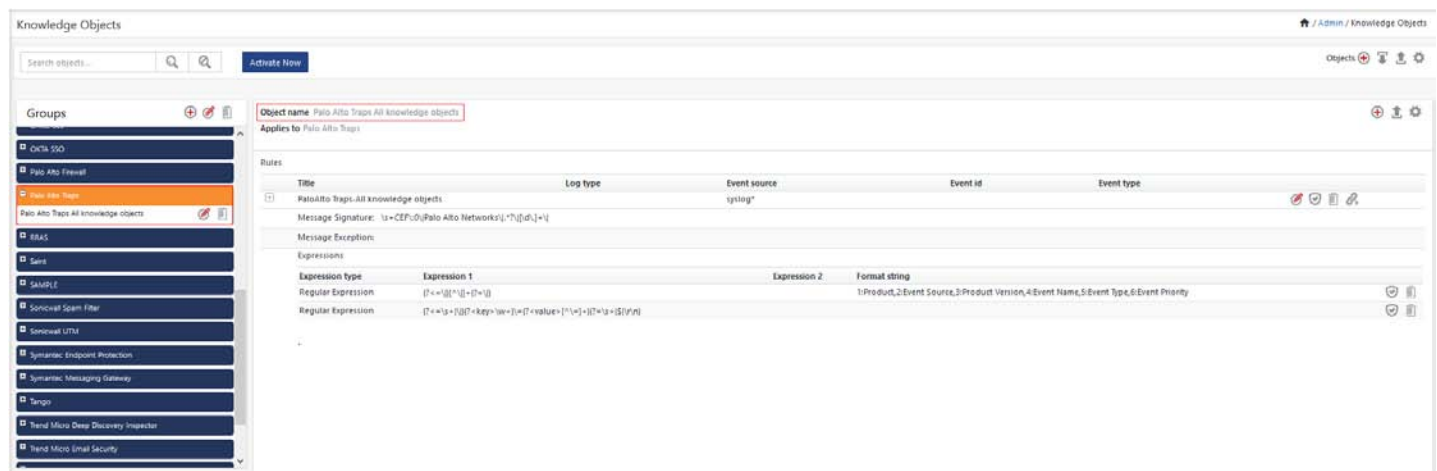


Figure 42

Flex Report

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

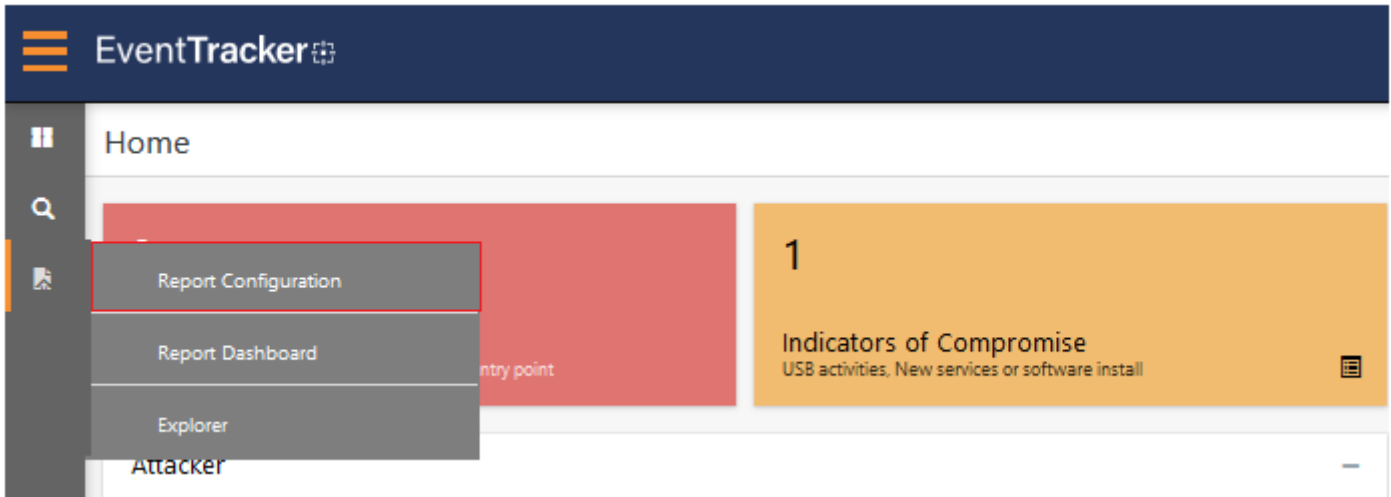


Figure 43

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the Palo Alto Traps group folder to view the imported Palo Alto Traps reports.

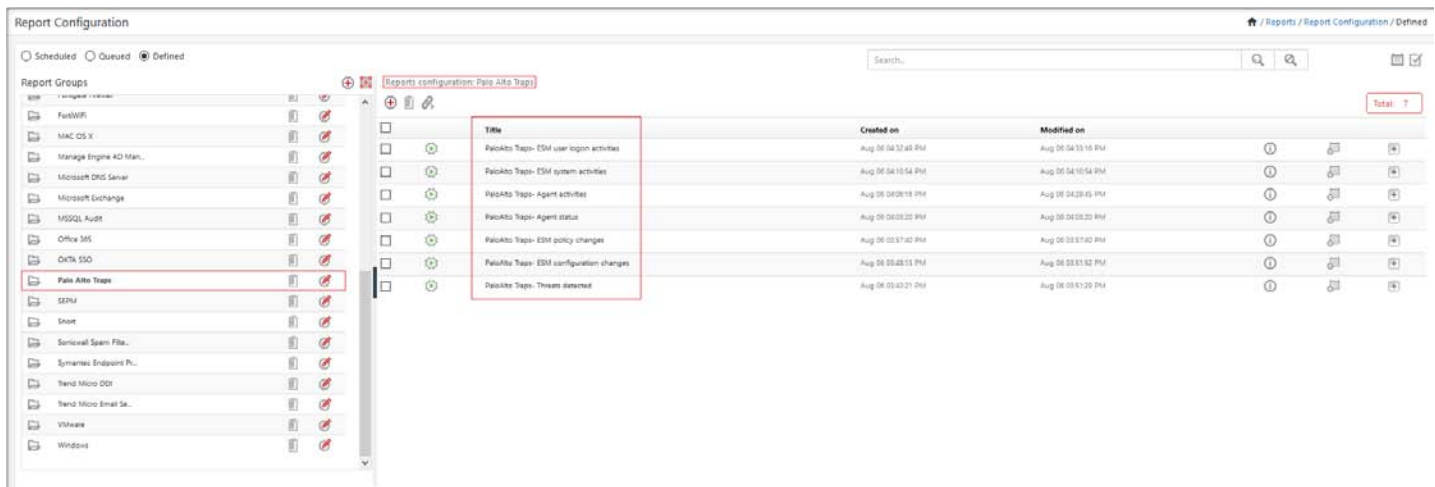


Figure 44

Dashboard

- **WIDGET TITLE:** Palo Alto Traps- Top threats detected by destination hostname

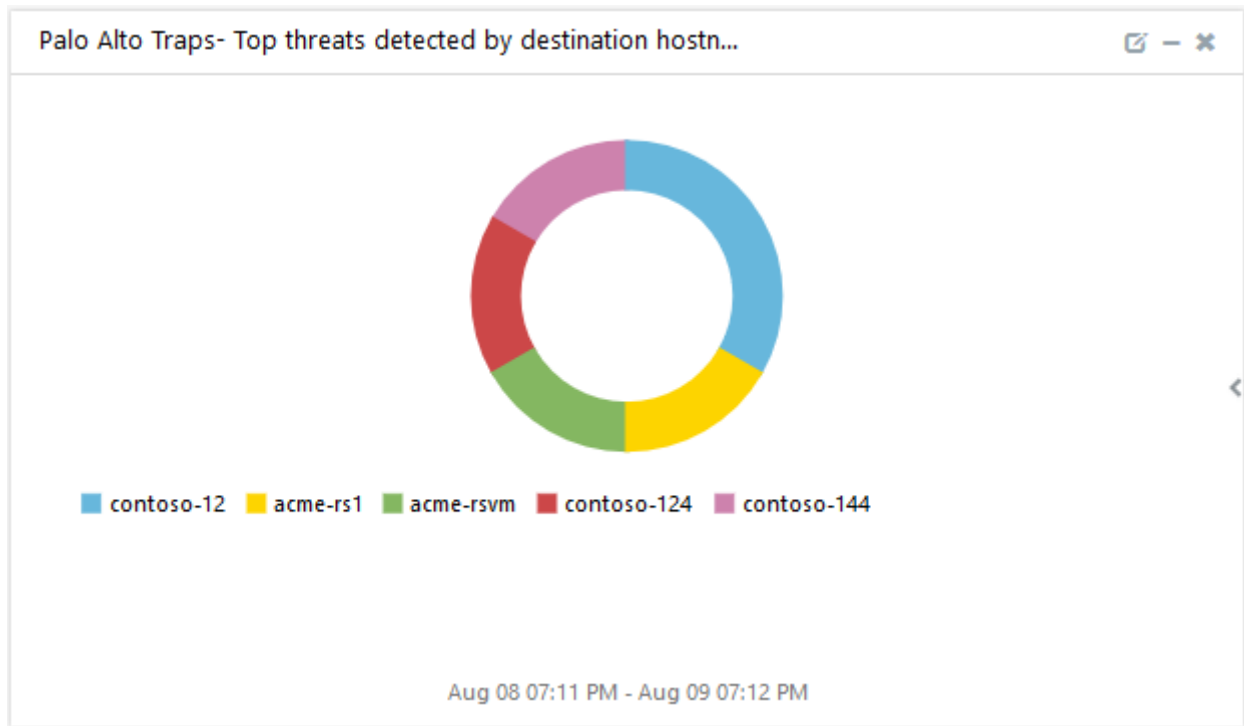


Figure 45

- **WIDGET TITLE:** Palo Alto Traps- Top threats detected by process name

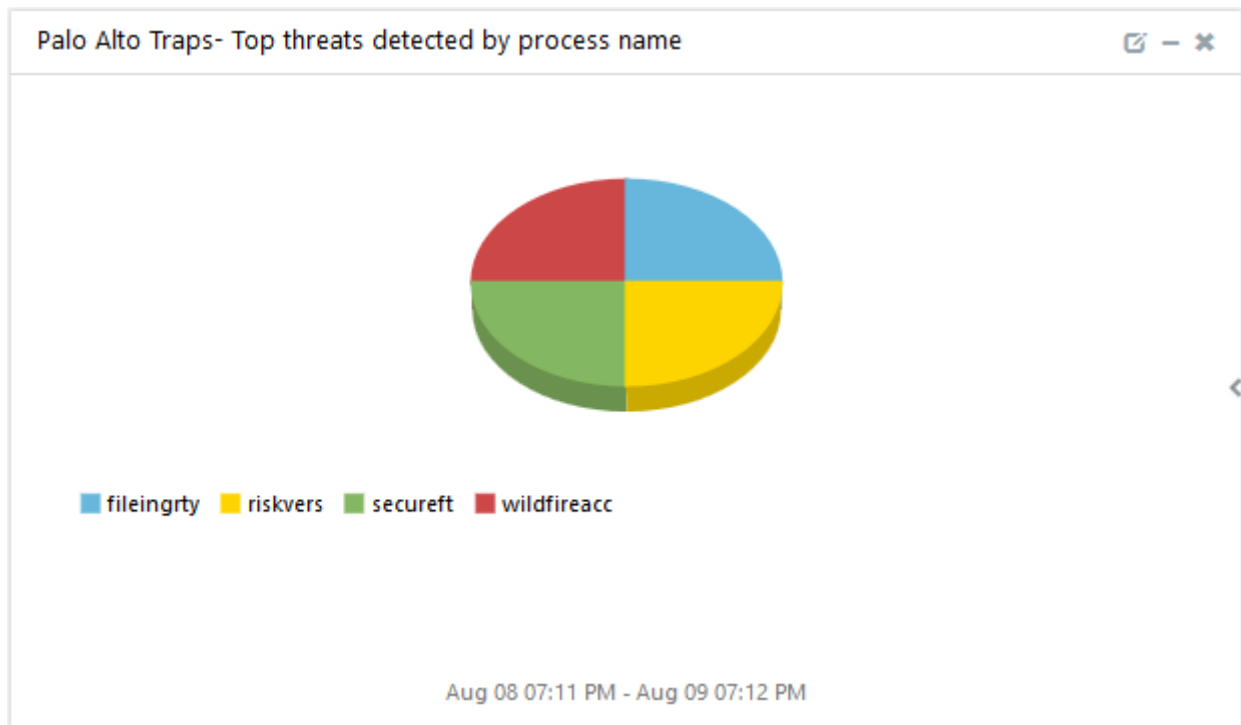


Figure 46

- **WIDGET TITLE:** Palo Alto Traps- Top threats detected by category

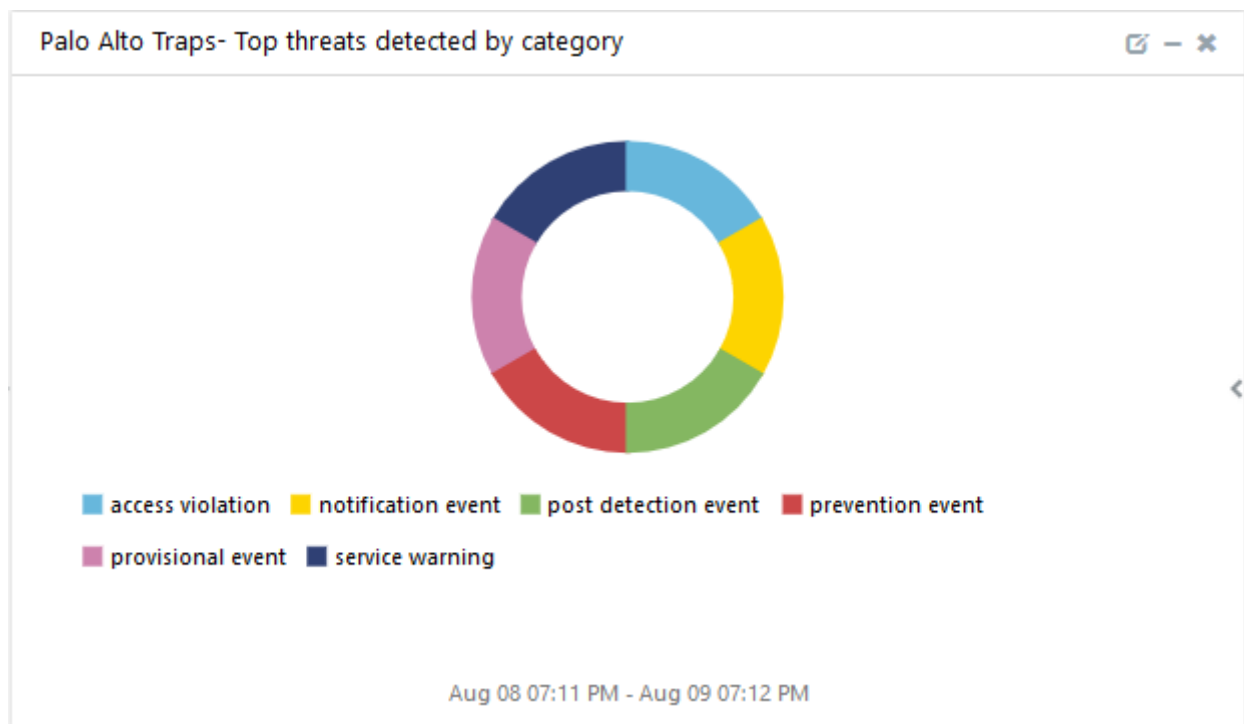


Figure 47

- **WIDGET TITLE:** Palo Alto Traps- Configuration changes

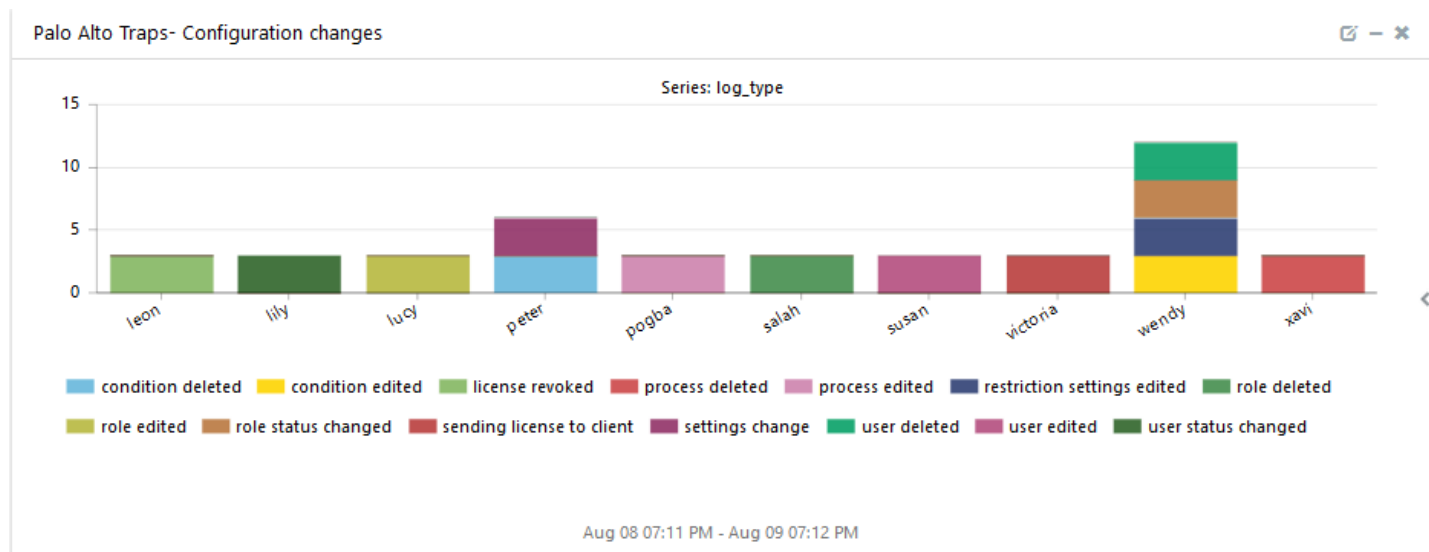


Figure 48

- **WIDGET TITLE:** Palo Alto Traps- System activities by destination hostnames

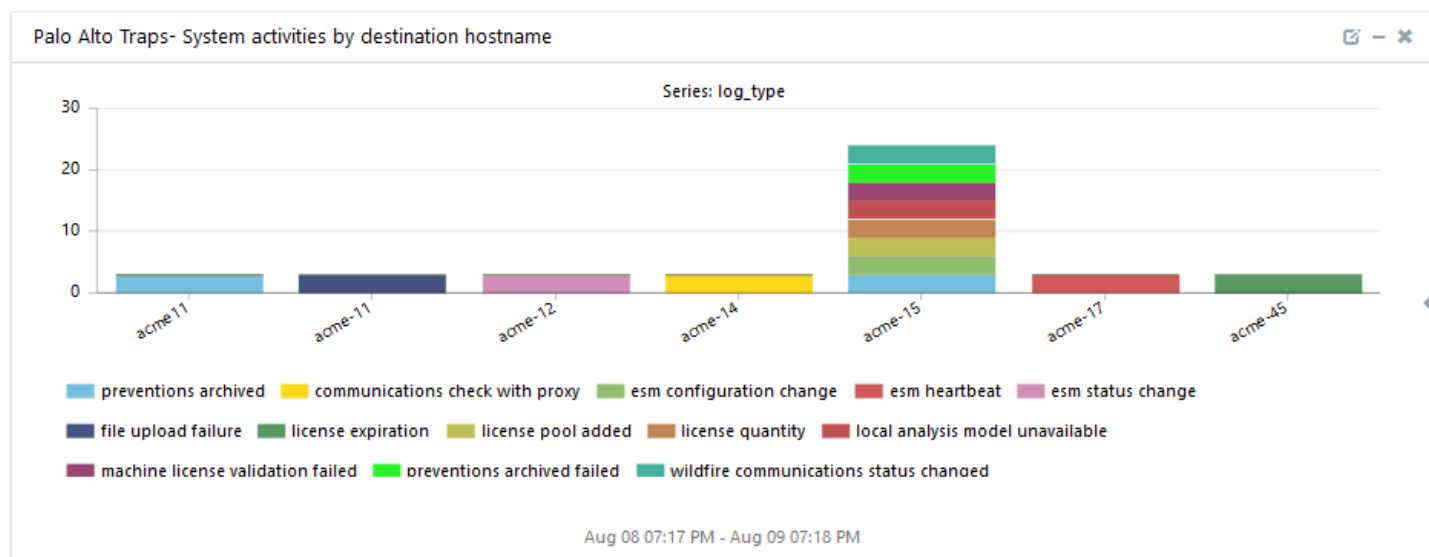


Figure 49