



Actionable Security Intelligence

Integrate ESET Antivirus

EventTracker v8.x and above

Abstract

This guide provides instructions to configure **ESET Antivirus** to send logs to EventTracker Enterprise. Once logs are being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.X and later, and **ESET Antivirus**.

Audience

Administrators who are responsible for monitoring **ESET Antivirus** which are running using EventTracker Manager.

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.

© 2017 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 ESET Antivirus events to EventTracker server	3
EventTracker Knowledge Pack.....	5
Alerts	6
Flex Reports	6
Import ESET Antivirus knowledge pack into EventTracker.....	9
Alerts	10
Knowledge Objects.....	11
Token Template	13
Flex Reports	14
Verify ESET Antivirus knowledge pack in EventTracker	16
Alerts	16
Token Templates	17
Flex Reports	17
Create Flex Dashboards in EventTracker	18
Schedule Reports	18
Create Dashlets.....	20
Sample Flex Dashboards	23

Overview

ESET Antivirus is the most effective protection you can find to combat today's huge volumes of Internet and email threats. It provides comprehensive antivirus and anti-spyware protection without affecting your computer's performance. Using advanced ThreatSense technology, ESET Antivirus proactively protects you from new attacks, even during the critical first hours when other vendors' products are not aware the attack even exists. ESET Antivirus detects and disables both known and unknown viruses, trojans, worms, adware, spyware, rootkits and other Internet threats.

EventTracker integrates ESET Antivirus and provides reports, knowledge objects and dashboards for all generated events including attacks, configuration changes etc. EventTracker will also monitor antivirus sensors and process execution statuses for all workstations in the network.

Prerequisites

- EventTracker v8.x should be installed.
- Latest business version of ESET Antivirus (Endpoint Protection).

Integration of ESET Antivirus events to EventTracker server

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Click **Admin → Server Settings** and expand **Advanced Settings**.

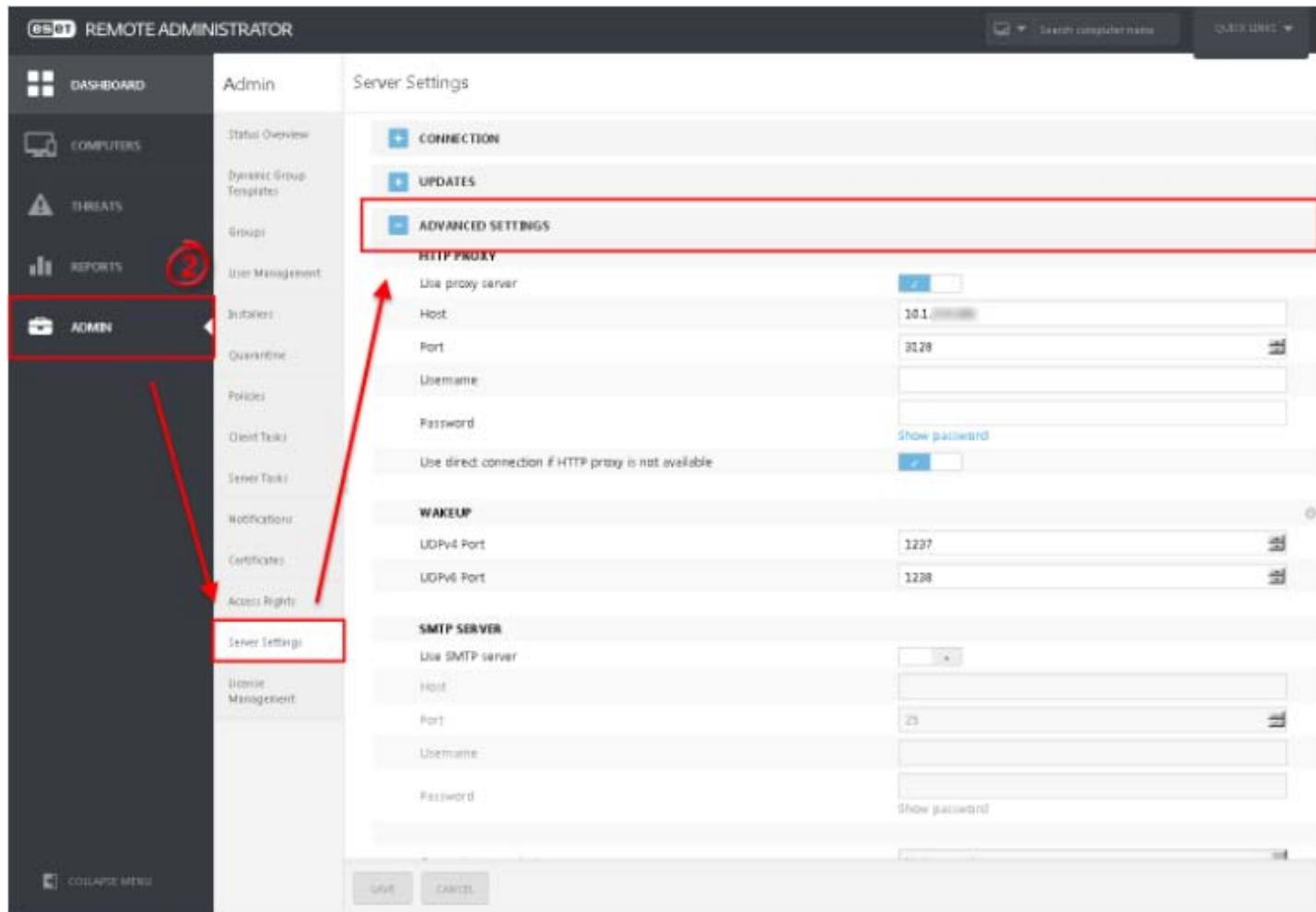


Figure 1

3. In the Syslog Server section, complete the following steps:
 - Click the slider bar next to **Use Syslog server**
 - **Host:** Type the IP address or hostname for the destination of Syslog messages.
 - **Port:** Default value is 514.

4. In the **Logging** section, click the slider bar next to **Export logs to Syslog** and click **Save**.

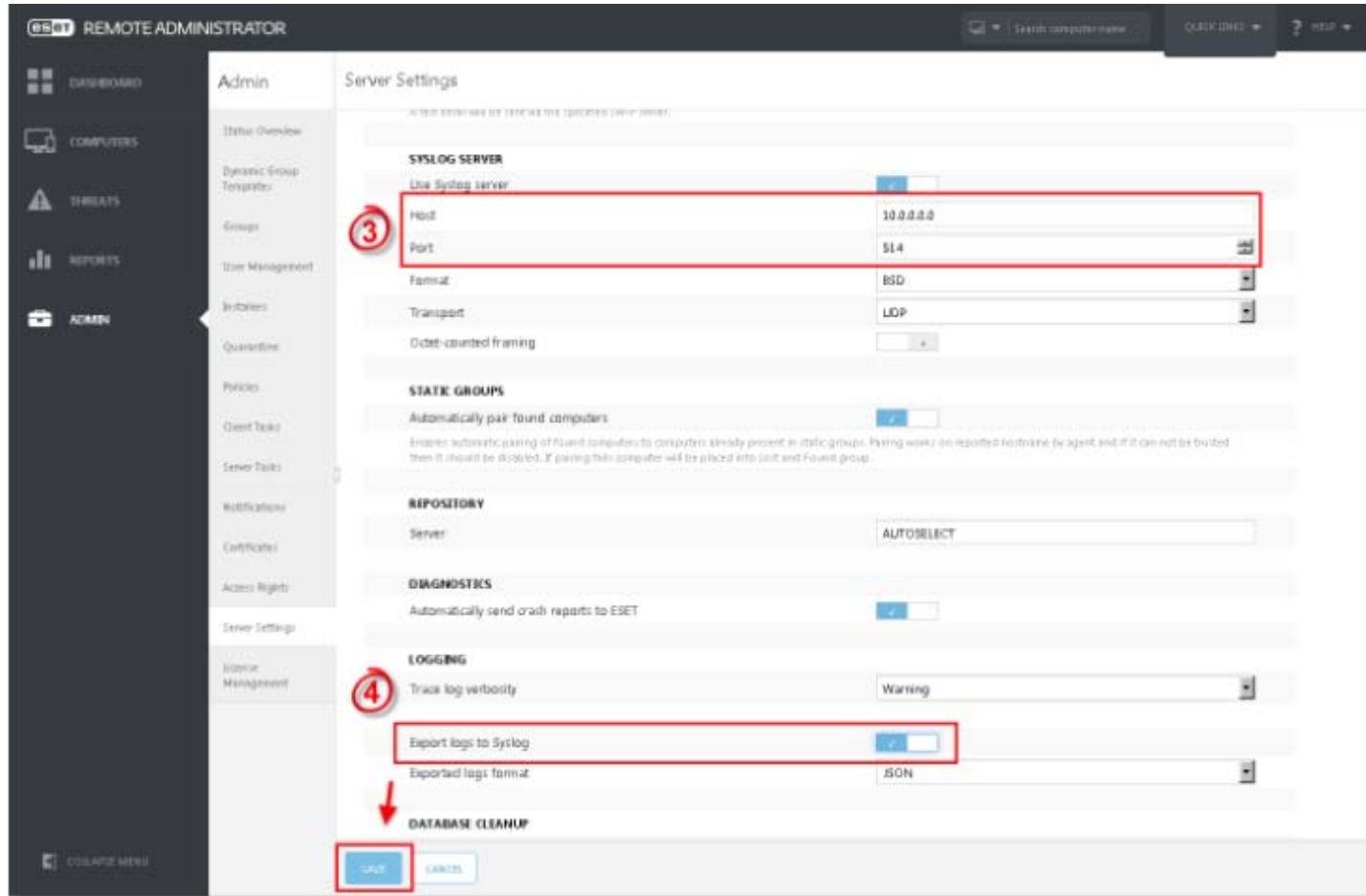


Figure 2

NOTE: - ESET Remote Administrator can export certain logs/events and send them to your Syslog server. Events such as **ThreatEvent**, **Firewall Aggregated Event**, **HIPS Aggregated Event** etc. are generated on a managed client computer running ESET security product (for example ESET Endpoint security). These events can be processed by EventTracker which can import events from a Syslog server. Events are written to the Syslog server by ESET Remote Administrator.

After you have enabled Syslog server, navigate to **Admin > Server Settings > Syslog Server > Logging** and enable **Export logs to Syslog**. Event messages are formatted in **JSON** (JavaScript Object Notation) format.

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories and Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Alerts

- ESET AV- Threat activities:** This alert is generated when a threat is detected by the ESET Endpoint Protection.
- ESET AV-HIPS alerts:** This alert is generated when any IPS alert is detected by ESET Endpoint Protection.
- ESET AV-Quarantined events:** This alert is generated when ESET Endpoint Protection quarantines any detected malware.

Flex Reports

- ESET AV- Login and logout activity-** This report provides details about all the login and logout activities.

LogTime	Host Name	User Name	User Domain	Source IP Address	Action	Severity	Occurred Time	Action Detail	Action Result
08/17/2017 05:47:00 PM	LRX-ESET	Administrator	Native user	10.25.161.14	Logout	Information	10-Aug-2017 11:47:27	Logging out native user "Administrator".	Success
08/17/2017 05:47:00 PM	LRX-ESET	Administrator	Native user	10.47.45.111	Login attempt	Information	10-Aug-2017 11:47:27	Authenticating native user "Administrator".	Success

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/23/2017 6:37:12 PM	5555	NTPLDTBLR38 / ESET	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Aug 10 07:47:43 10.0.2.13 Aug 10 07:47:27 LRX-ESET ERA Server[3936]: {"event_type":"Audit_Event","ipv4":"10.25.161.14","hostname":"LRX-ESET","source_uuid":"0bcbb1cf-7776-4717-85c7-5255646e2fef","occurred":"10-Aug-2017 11:47:27","severity":"Information","domain":"Native user","action":"Logout","target":"Administrator","detail":"Logging out native user \"Administrator\".","user":"00000000-0000-0000-7002-000000000002","result":"Success"}			

- ESET AV- Threat activities-** This report provides details about all the threat that are detected by ESET Endpoint Protection.

LogTime	Host Name	Source IP Address	Threat Name	Threat Type	Severity	Occurred Time	Uri Accessed	Object Type	Threat Hash	Action Taken	Threat Handled	First Discovered	Restart Needed
08/18/2017 04:23:10 PM	Contoso.lan	192.171.12.148	Win32/Adware.Coupons.AA	application	Critical	08-Aug-2017 20:35:03	file:///C:/Users/mroth/Downloads/CouponPrinterCPS.exe	file	AAFE7B9C941	cleaned by deleting	true	02-Aug-2016 14:52:44	false
08/18/2017 04:23:10 PM	Contoso.lan	192.162.32.15	Win32/Adware.Coupons.adwareexec	application	Fatal	08-Aug-2017 20:33:16	file:///C:/Users/mroth/AppData/Local/Temp/Low/cpnprt2win32.cid	file	4F09A3AD90	cleaned by deleting	true	15-Oct-2015 17:20:47	false
08/18/2017 04:23:10 PM	Contoso.eth1	172.151.14.19	Win32/Deceptor.OptiSpeed.C	application	Fatal	08-Aug-2017 20:35:09	file:///C:/Users/mroth/Downloads/optispeed-setup.exe	file	B920F5DA1F8	cleaned by deleting	true	02-Dec-2016 14:20:53	TRUE

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/23/2017 6:37:13 PM	5555	NTPLDTBLR38 / ESET	N/A	N/A	Syslog
Description:					
Aug 08 18:50:00 10.0.2.13 Aug 8 18:49:42 LRX-ESET ERAServer[3936]: {"event_type":"Threat_Event","ipv4":"172.14.23.111","hostname":"mroth.avita.lan","source_uuid":"b5bbaaa9-762e-4f62-a821-faade848fd0d","occurred":"08-Aug-2017 20:35:17","severity":"Warning","threat_type":"application","threat_name":"Win32/Adware.Coupons-AA","threat_flags":"Variant","scanner_id":"First scan scanner","scan_id":"ndl16774.dat","engine_version":"15577 (20170613)","object_type":"file","object_uri":"file:///C:/Windows/CouponPrinter.ocx","action_taken":"cleaned by deleting","threat_handled":true,"need_restart":false,"firstseen":"01-Oct-2014 21:33:20","hash":"8CE421A6A18623292CBC8713DA9B6777C1FA56E2"}					
Event Type: Information Log Type: Application Category Id: 0					

- ESET AV-Firewall aggregated event-** This report provides details on all the firewall aggregated events including traffic allowed and denied activities.

LogTime	Host Name	Process Name	Source IP Address	Source Type	Source Port	Target Address	Target Type	Target Port	Protocol	User Account	Threat name	Severity	Rule Name	Inbound	Count	Occurred Time
08/23/2017 02:12:48 PM	contoso.lan	Esetaction.exe	192.168.13.10	unicast	4812	172.168.9	multicast	145	tcp	contoso.vm1	Win32/Skype. Information	Allowed	0	27	08-Aug-2017 20:35:03	
					9.10					2	plugins.e12sd	Comms				
08/23/2017 02:12:48 PM	contoso.eth1	GQconho.st.exe	87.86.189.66	local	2556	192.168.9	broadcast	2556	udp	contoso.S1	eicar.org/cls/ addin	Critical	Denied	1	1	08-Aug-2017 20:35:03
08/23/2017 02:12:48 PM	contoso.emc.h1	HB1assy metric.exe	192.168.1.111	broadcast	1492	121.227.1	local	4155	tcp	VM12wer15	Microsoft/fmb .css/adobe-flash/rogues.jss	Warning	Blocked packets	0	2	08-Aug-2017 20:35:03
08/23/2017 02:12:48 PM	acme.lan36	Esetoverri de.exe	211.99.188.37	unicast	1554	172.15.12	multicast	453	tcp	acme.s4.traffic	malwarebyte s.org/loginclash/recurse	Critical	Passed packets	1	3	08-Aug-2017 20:35:03
					9.54											Activ

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/23/2017 6:37:14 PM	5555	NTPLDTBLR38 / ESET	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0					
Description: Aug 08 22:44:49 10.1.10.1 Aug 8 22:39:17 LRX-ESET ERA Server[5371]: {"event_type": "FirewallAggregated_Event", "hostname": "acme.lan36", "source_uuid": "b5bbaaa9-762e-4f62-a821-faade848fd0d", "occurred": "08-Aug-2017 20:35:03", "severity": "Critical", "Event Name": "P9 Filter", "source_address": "211.99.188.37", "source_address_type": "unicast", "source_port": "1554", "target_address": "172.15.129.54", "target_address_type": "multicast", "target_port": "453", "protocol": "tcp", "account": "acme.s4.traffic", "process_name": "FFq.45rg.new", "rule_name": "Passed packets", "rule_id": "G4986288WGR-3569-2478-2FE9-8HJ77EE7J", "inbound": "1", "threat_name": "malwarebytes.org/login.class.recurse", "aggregate_count": "3"}					

- ESET AV-HIPS alerts-** This report provides details about all the IPS alerts that are detected by the ESET Endpoint Protection.

LogTime	Host Name	Source IP Address	Occured Time	Application Accessed	Operation	Severity	Target Application	Action	Rule Name	Rule Id	Count
08/21/2017 03:45:02 PM	contoso.lan	192.168.1.105	08-Aug-2017 20:35:03	C:\Windows\System32\csrss.exe	Get access to another application	Critical	C:\Program Files\ESET\Smart Security\ekern.exe	blocked	Self-Defense: Protect ekern and egui processes	15577 (20170613)	2
08/21/2017 03:45:02 PM	contoso.eth1	172.163.14.78	08-Aug-2017 20:35:03	C:\Windows\System32\svchost.exe	Get access to file	Error	C:\Windows\System32\winlogon.exe	blocked	Self-Defense: Do not allow modification of system processes	156478 (20170412)	1
08/21/2017 03:45:02 PM	contoso.emc.h1	10.45.16.141	08-Aug-2017 20:35:03	C:\Program Files\CCleaner\CCleaner.exe	Start new application	Critical	C:\Program Files\Internet Explorer\explore.exe	blocked	User rule: Block CCleaner application from execution	73159 (20174441)	2
08/21/2017 03:45:02 PM	acme.lan36	172.19.133.45	08-Aug-2017 20:35:03	C:\Program Files\CCleaner\CCleaner64.exe	Change startup parameters	Fatal	HKEY_USERS\S-1-5-21-194528642-56334563-200145766-1000\Software\Microsoft\Windows\CurrentVersion\Run\ccleaner	blocked	User rule: Block CCleaner application from execution	73159 (20174441)	3

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/23/2017 6:37:13 PM	5555	NTPLDTBLR38 / ESET	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0					
Description: Aug 08 18:50:00 192.168.1.105 Aug 8 18:49:42 LRX-ESET ERA Server[1249]: {"event_type": "HipsAggregated_Event", "ipv4": "192.168.1.105", "hostname": "contoso.lan", "source_uuid": "b5bbaaa9-762e-4f62-a821-faade848fd0d", "occurred": "08-Aug-2017 20:35:03", "severity": "Critical", "application": "C:\Windows\System32\csrss.exe", "operation": "Get access to another application", "target": "C:\Program Files\ESET\Smart Security\ekern.exe", "action": "blocked", "rule_name": "Self-Defense: Protect ekern and egui processes", "rule_id": "15577 (20170613)", "aggregate_count": "2"}					

- ESET AV-Quarantined events:** This report provides details about all the detected malware when they are quarantined by the ESET Endpoint Protection.

LogTime	Host Name	Quarantine ID	Threat Name	Severity	File Name	Extension	Threat Details	Size	Threat Hits	Hash	Occurred Time	Occurred Last
08/23/2017 04:00:44 PM	contoso.lan	HAU08Q87T5I P42T3	C:\Flamer\advnetcfg.o cr_installer.pkg	Critical	C:\Users\lmroth\Downloads\CouponPrinterCPS.exe	exe	Probably a variant of Flamer trojan	256889	3	AAFE7B9C9410C060 484070EDA6CC6225 15AD03EC	08-Aug-2017 20:35:03	Aug 8 18:49:42
08/23/2017 04:00:44 PM	contoso.eth1	P95D1D5WQ63 ST	http://www.eicar.org/download/eicar.com	Critical	C:\Documents and Setting\User\Download\	exe	Eicar test file	74236	15	8CE421A6A1862329 2CBC8713DA9B6777 C1FA56E2	08-Aug-2017 20:35:03	Aug 8 11:21:39
08/23/2017 04:00:44 PM	acme.lan36	RYU7K4D3897 JWL8	http://www.eicar.petk.org/download/26D5.t	Critical	C:\Users\Petko\Downloads\	exe	Eicar test file	68	6	4F09A3AD90A07C18 AF485D6373772F2F5 FBEFEC1	08-Aug-2017 20:35:03	Aug 9 10:54:19

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/23/2017 6:37:15 PM	5555	NTPLDTBLR38 / ESET	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0					
Description: Aug 08 18:50:00 10.1.10.1 Aug 8 20:33:15 LRX-ESET ERAServer[1579]: {"event_type":"Threat_Event","hostname":"contoso.eth1","source_guid":"hr9h9hrh5-7y52e-rhy4-d5hw-faade848fd0d","occurred":"08-Aug-2017 20:35:03","severity":"Fatal","quarantine_id":"P95D1D5WQ63 ST","Hash":"8CE421A6A18623292CBC8713DA9B6777C1FA56E2","Date_received":"Aug 8 11:21:39","Occurred_last":"Aug 8 11:21:39","Object_name":"http://www.eicar.org/download/eicar.com","File_name":"C:\Documents and Setting\User\Download\eicar.exe","Extension":"exe","Size":74236,"Reason":"Eicar test file","Client_count":15,"Hits":15}					

Import ESET Antivirus knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

NOTE: Export knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

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



Figure 3

- Click the **Import** tab.

Alerts

- Click **Alerts** option, and then click the browse button.
- Locate the **ESET Antivirus alerts.isalt** file, and then click the **Open** button.

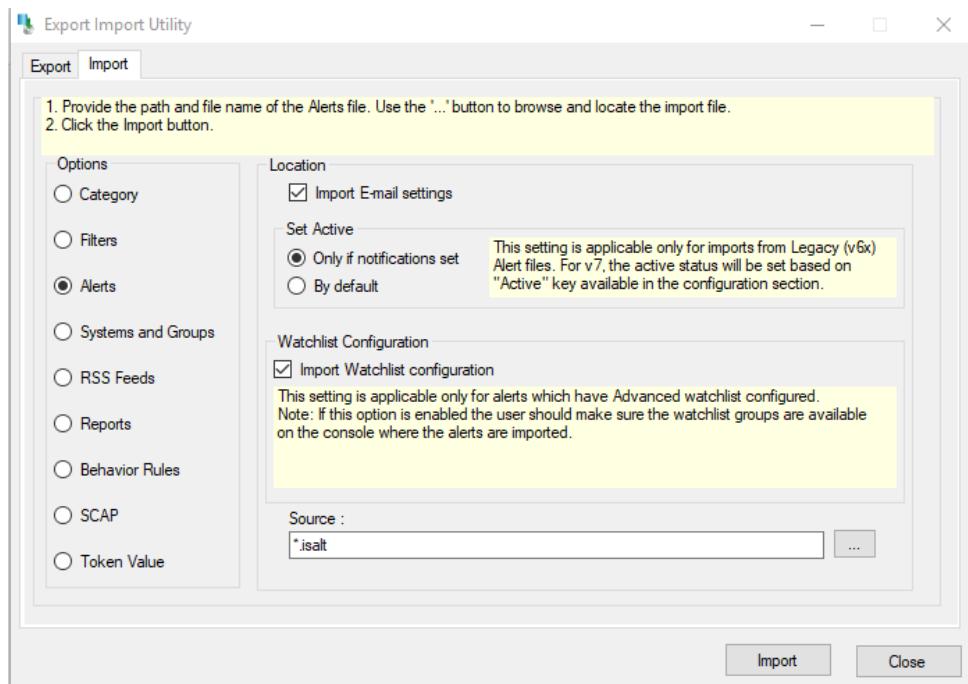


Figure 4

- To import alerts, click the **Import** button.

EventTracker displays success message.

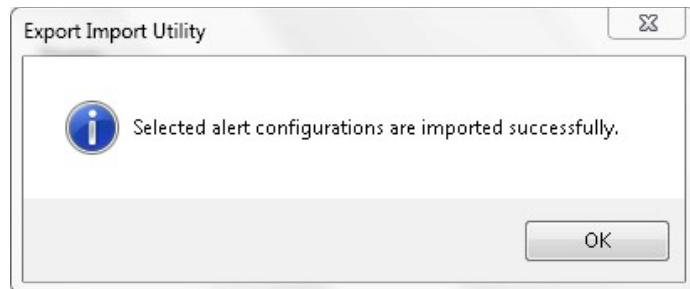


Figure 5

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

Knowledge Objects

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

The screenshot shows the EventTracker manager interface. At the top, there's a navigation bar with links for Dashboard, Incidents, Behavior, Search, Reports, My EventTracker, Change Audit, and Config. The Config link is currently active, as indicated by a blue background. A dropdown menu for 'Admin' is open, listing various configuration options: Active Watch Lists, Alerts, Behavior Rules, Behavior Settings, Category, Event Filters, Eventvault, IP Lookup Configuration, Knowledge Objects (which is highlighted with a red box), Logbook Configuration, Manager, Parsing Rules, Report Settings, RSS, Systems, Users, Weights, and Windows Agent Config. Below the navigation bar, there are sections for NEWS and ANNOUNCEMENTS. The NEWS section contains a 'Latest Knowledge Packs' card with a gear icon and text about using Knowledge Packs to assign meaning and severity to log messages. It includes a 'Learn more' link. The ANNOUNCEMENTS section shows a message: 'No Announcements'. To the right, there's a sidebar with a 'Knowledgeable browser' section and a note about supporting over 150 operators.

Figure 6

- Locate the **ESET Antivirus knowledge objects.eko**, and then click **Import** button

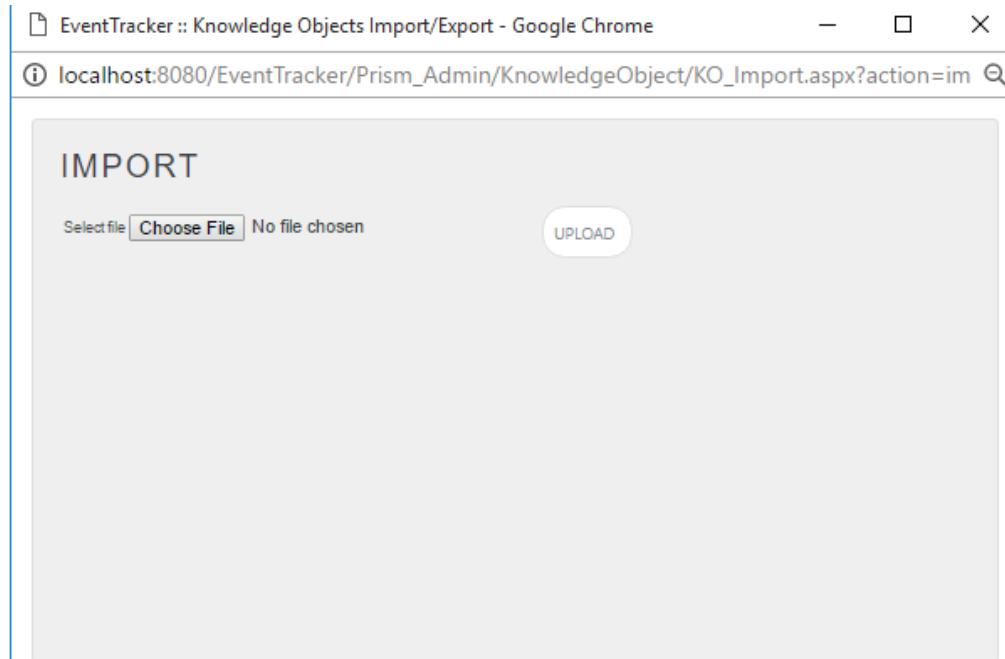


Figure 7

3. Choose the Knowledge objects that needs to be imported and click on **upload**.

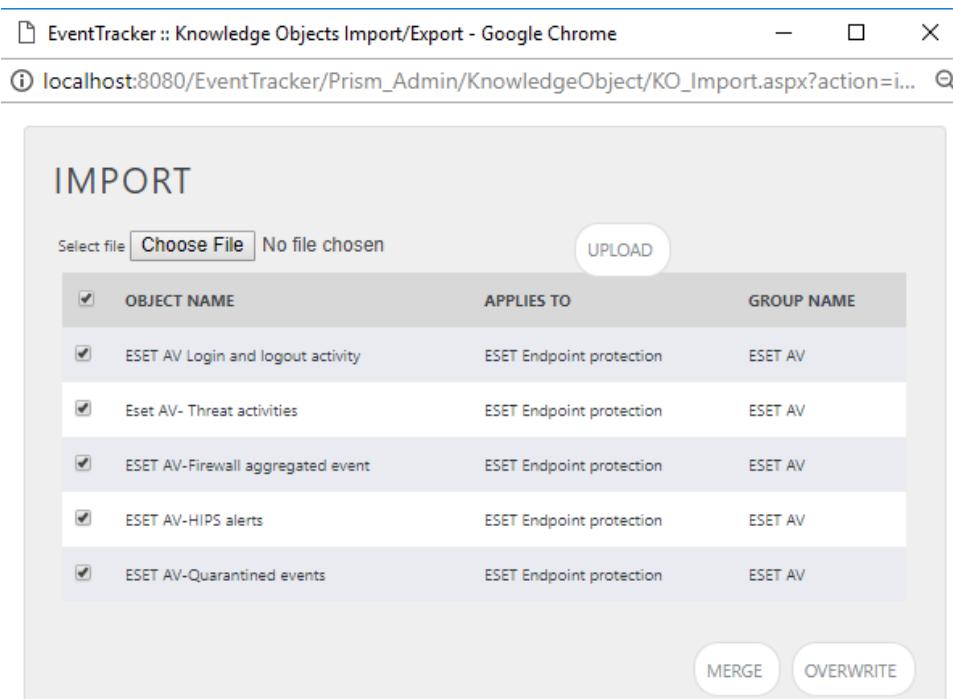


Figure 8

- Knowledge objects are now imported successfully.



Figure 9

Token Template

- Click **Token Value** option, and then click the browse  button.
- Locate the **ESET Antivirus Token Templates.ettd** file, and then click the **Open** button.

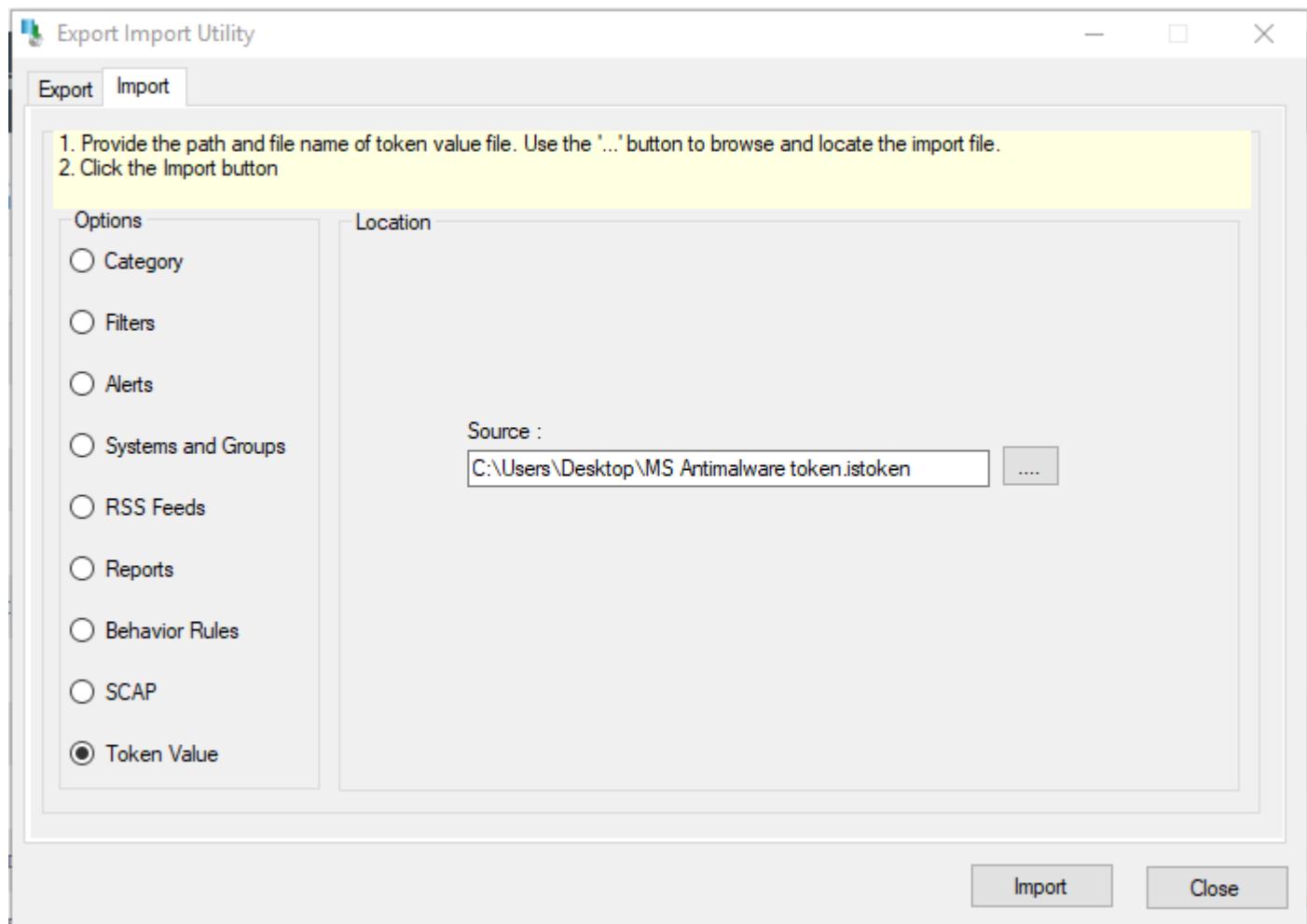


Figure 10

3. Click the **Import** button to import the tokens. EventTracker displays success message.

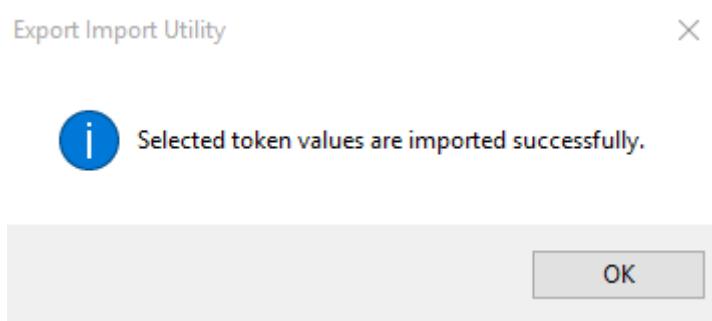


Figure 11

Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **ESET Antivirus reports.etcrx** file, and then click the **Open** button.

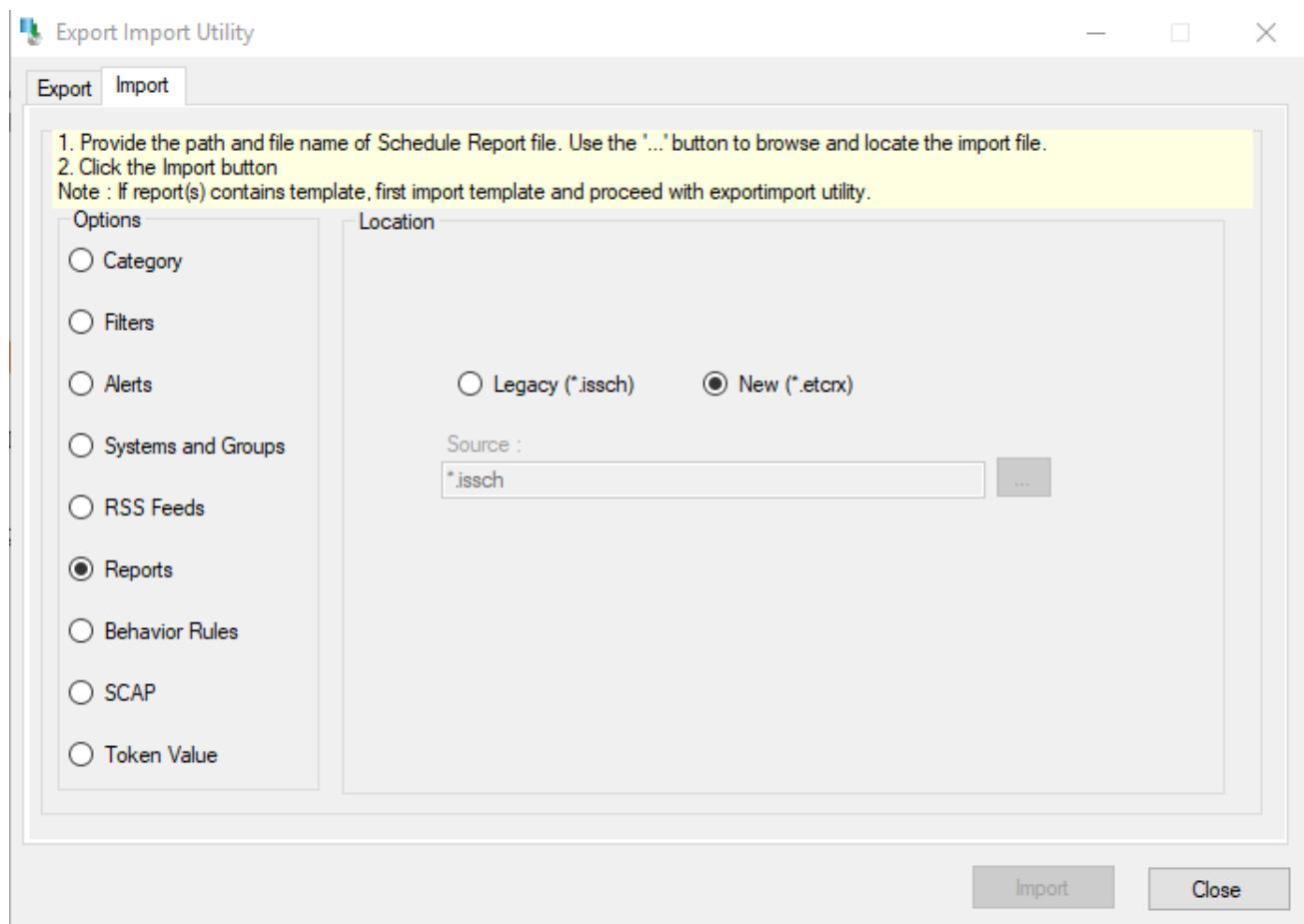


Figure 12

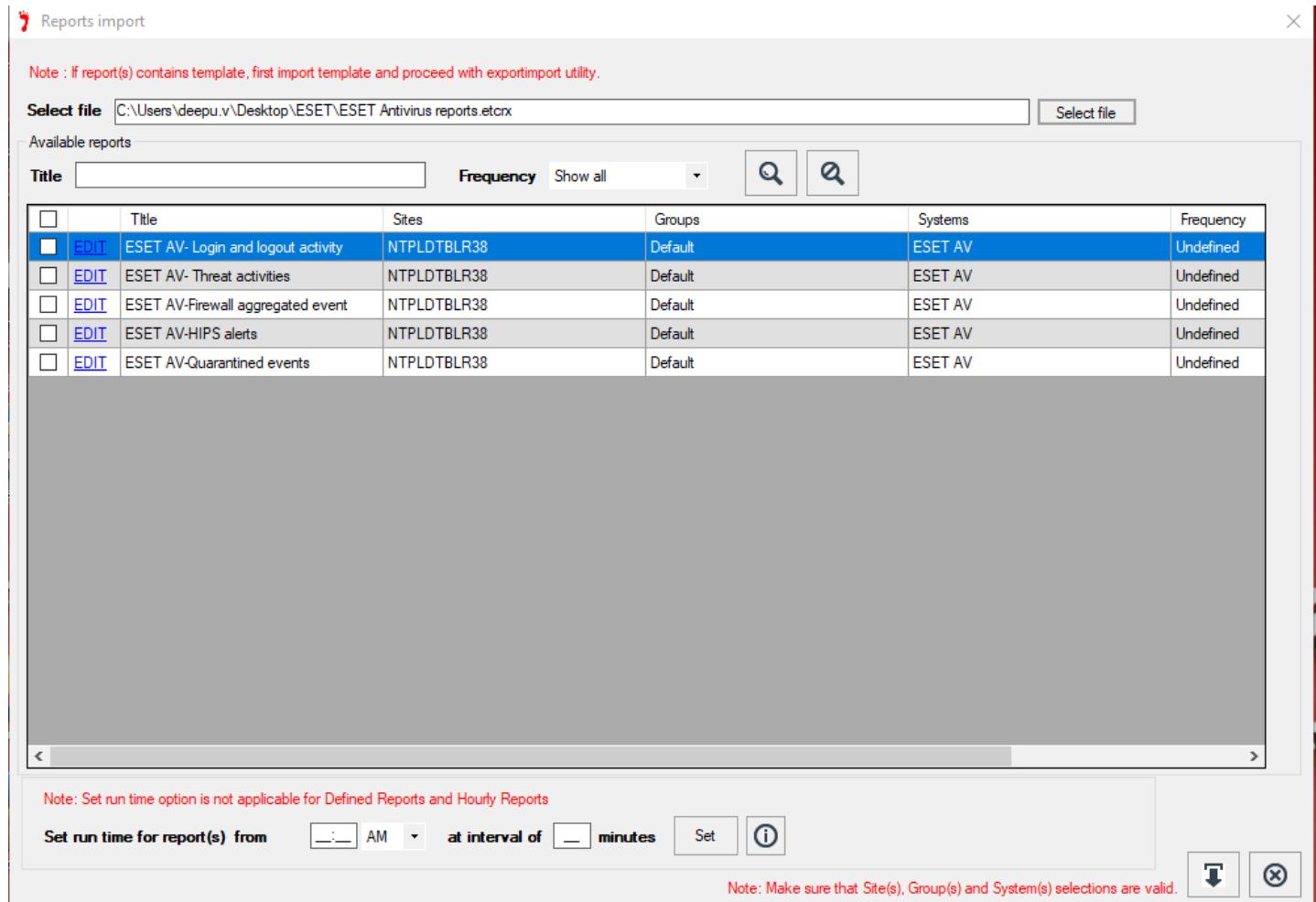


Figure 13

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

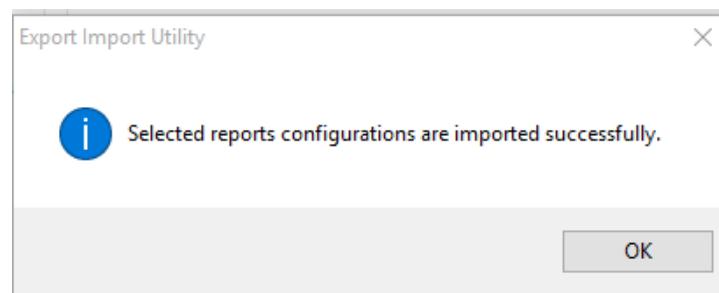


Figure 14

Verify ESET Antivirus knowledge pack in EventTracker

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **ESET Antivirus**, and then click **Go** button.

Alert Management page will display the imported **ESET Antivirus** alert.

The screenshot shows the 'ALERT MANAGEMENT' page. At the top, there is a search bar with 'ESET AV' and a magnifying glass icon. Below the search bar, there is a button labeled 'ACTIVATE NOW' and a note: 'Click 'Activate Now' after making all changes'. On the right side, there are buttons for 'Total: 3' and 'Page Size 25'. The main table has columns: ALERT NAME, THREAT, ACTIVE, E-MAIL, MESSAGE, RSS, FORWARD AS SNMP, FORWARD AS SYSLOG, REMEDIAL ACTION AT CONSOLE, REMEDIAL ACTION AT AGENT, and APPLIES TO. Three rows are listed, each corresponding to an ESET AV alert: 'ESET AV : HIPS alerts', 'ESET AV : Quarantined events', and 'ESET AV : Threat activities'. The first row is highlighted with a red border. A 'DELETE' button is located at the bottom left of the table area.

ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
ESET AV : HIPS alerts	<input type="checkbox"/> High	<input type="checkbox"/>	<input type="checkbox"/>	ESET Endpoint pro...						
ESET AV : Quarantined events	<input type="checkbox"/> High	<input type="checkbox"/>	<input type="checkbox"/>	ESET Endpoint pro...						
ESET AV : Threat activities	<input type="checkbox"/> High	<input type="checkbox"/>	<input type="checkbox"/>	ESET Endpoint pro...						

Figure 15

3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

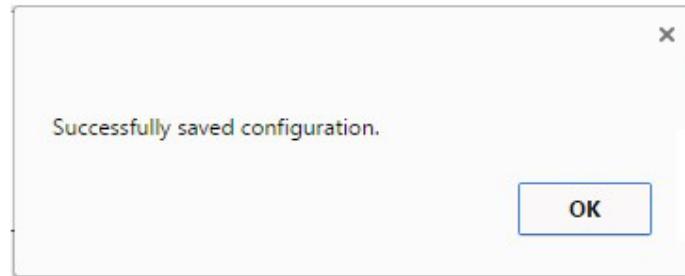


Figure 16

4. Click the **OK** button, and then click the **Activate now** button.

NOTE:

- You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Token Templates

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and the **Template** tab.
3. Click on **ESET AV** group option.

The screenshot shows the 'PARSING RULE' interface with the 'Template' tab selected. On the left, a sidebar lists various parsing rules, with 'ESET AV' highlighted by a red box. The main area displays a table of templates under the heading 'Group : ESET AV'. The table columns are: TEMPLATE NAME, TEMPLATE DESCRIPTION, ADDED BY, ADDED DATE, ACTIVE, and EDIT. The data rows are:

TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE	EDIT	
ESET AV-Firewall aggre...	ESET AV-Firewall aggregated...	ETAdmin	8/23/2017 2:35:24 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
ESET AV-HIPS alerts	ESET AV-HIPS alerts	ETAdmin	8/21/2017 3:57:07 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Eset AV-Login and log...	Eset AV-Login and logout ac...	ETAdmin	8/17/2017 5:40:33 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
ESET AV-Quarantined e...	ESET AV-Quarantined events	ETAdmin	8/23/2017 4:16:07 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Eset AV-Threat activities	Eset AV-Threat activities	ETAdmin	8/18/2017 4:01:57 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Figure 17

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**ESET AV**', and then click the **Search** button.

EventTracker displays Flex reports of '**ESET Antivirus**'

The screenshot shows the 'REPORTS CONFIGURATION' section of the EventTracker interface. On the left, a sidebar lists 'REPORT GROUPS' with items like Cyberoam UTM, Dell FORCE 10 Switch, Duo Security, eDirectory, Eset AV (which is highlighted with a red box), EventTracker, and EZproxy. Each item has edit and delete icons. On the right, a main panel titled 'REPORTS CONFIGURATION : ESET AV' displays a table of five reports. The table columns are 'TITLE', 'CREATED ON', and 'MODIFIED ON'. Each row contains a small gear icon and edit/delete icons. The first four rows are grouped together with a red box, indicating they belong to the selected 'Eset AV' report group.

TITLE	CREATED ON	MODIFIED ON
ESET AV-Quarantined events	8/23/2017 4:19:45 PM	8/23/2017 4:19:45 PM
ESET AV-Firewall aggregated event	8/23/2017 2:41:25 PM	8/23/2017 2:41:25 PM
ESET AV-HIPS alerts	8/21/2017 4:00:54 PM	8/21/2017 4:00:54 PM
ESET AV- Threat activities	8/18/2017 4:37:46 PM	8/23/2017 4:41:23 PM
ESET AV- Login and logout activity	8/17/2017 5:56:08 PM	8/23/2017 4:41:41 PM

Figure 18

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.

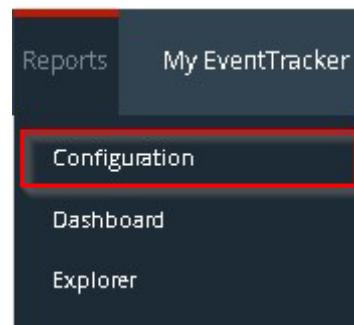


Figure 19

2. Navigate to **Reports>Configuration**.
3. Select **ESET Antivirus** in report groups. Check **Defined** dialog box.

The screenshot shows the 'REPORTS CONFIGURATION' screen. On the left, a sidebar lists 'REPORT GROUPS' with items like Cyberoam UTM, Dell FORCE 10 Switch, Duo Security, eDirectory, Eset AV (which is selected and highlighted with a red border), EventTracker, and EZproxy. Each item has edit and delete icons. On the right, a main panel titled 'REPORTS CONFIGURATION : ESET AV' displays a table of five reports. The table columns are 'TITLE', 'CREATED ON', and 'MODIFIED ON'. Each row contains a green gear icon, a link to the report title, and creation/modification dates/times. A 'Total: 5' button is in the top right corner.

TITLE	CREATED ON	MODIFIED ON
ESET AV-Quarantined events	8/23/2017 4:19:45 PM	8/23/2017 4:19:45 PM
ESET AV-Firewall aggregated event	8/23/2017 2:41:25 PM	8/23/2017 2:41:25 PM
ESET AV-HIPS alerts	8/21/2017 4:00:54 PM	8/21/2017 4:00:54 PM
ESET AV- Threat activities	8/18/2017 4:37:46 PM	8/23/2017 4:41:23 PM
ESET AV- Login and logout activity	8/17/2017 5:56:08 PM	8/23/2017 4:41:41 PM

Figure 20

4. Click on 'schedule' to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

The screenshot shows the 'REPORT WIZARD' step 8 of 10. The title is 'TITLE: ESET AV- THREAT ACTIVITIES'. The 'LOGS' section is visible. Below it, a note says 'Review cost details and configure the publishing options.' A progress bar shows Step 8 of 10. The main area is titled 'DISK COST ANALYSIS' and contains the following information:

- Estimated time for completion: 00:00:40(HH:MM:SS)
- Number of cab(s) to be processed: 5
- Available disk space: 163 GB
- Required disk space: 50 MB

Under 'UBLISHING OPTIONS', there are three radio buttons:

- Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
- Deliver results via E-mail
- Notify results via E-mail

Below these are fields for 'To E-mail' (with placeholder '[Use comma(,) to separate multiple e-mail recipients]'), 'Update status via RSS' (with 'Select Feed' dropdown), 'Show in' (with 'none' dropdown), and a checked checkbox for 'Persist data in EventVault Explorer'.

Figure 21

- In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

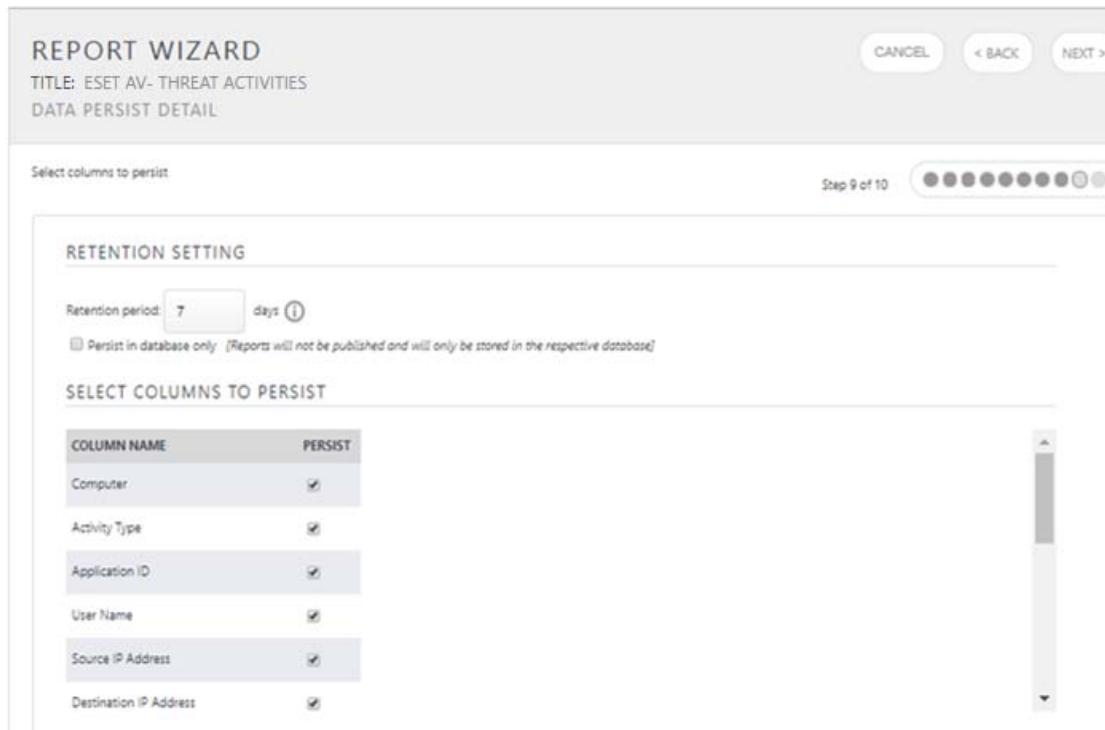


Figure 22

- Proceed to next step and click **Schedule** button.
- Wait till the reports get generated.

Create Dashlets

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

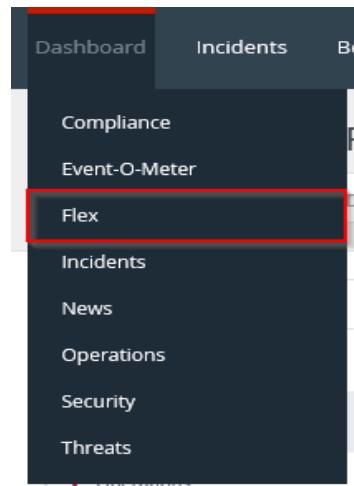


Figure 23

2. Navigate to Dashboard>Flex.

Flex Dashboard pane is shown.

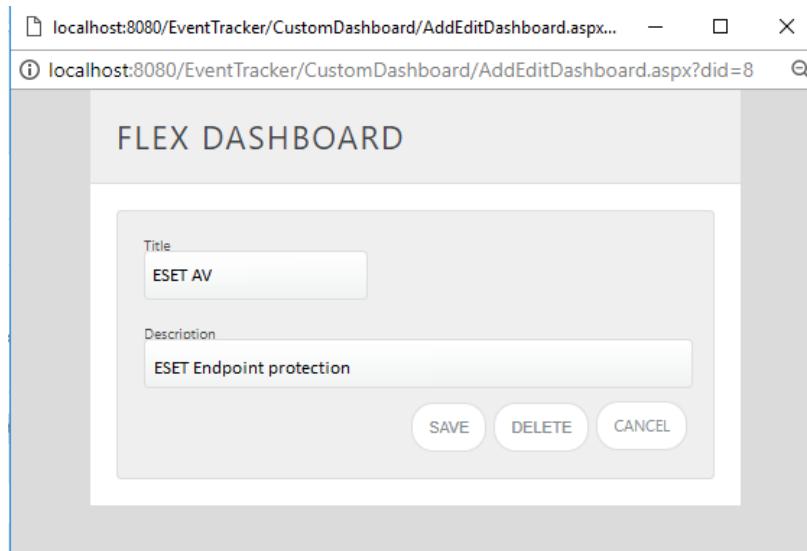


Figure 24

3. Fill suitable title and description and click **Save** button.

4. Click to configure a new flex dashlet. Widget configuration pane is shown.

Figure 25

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

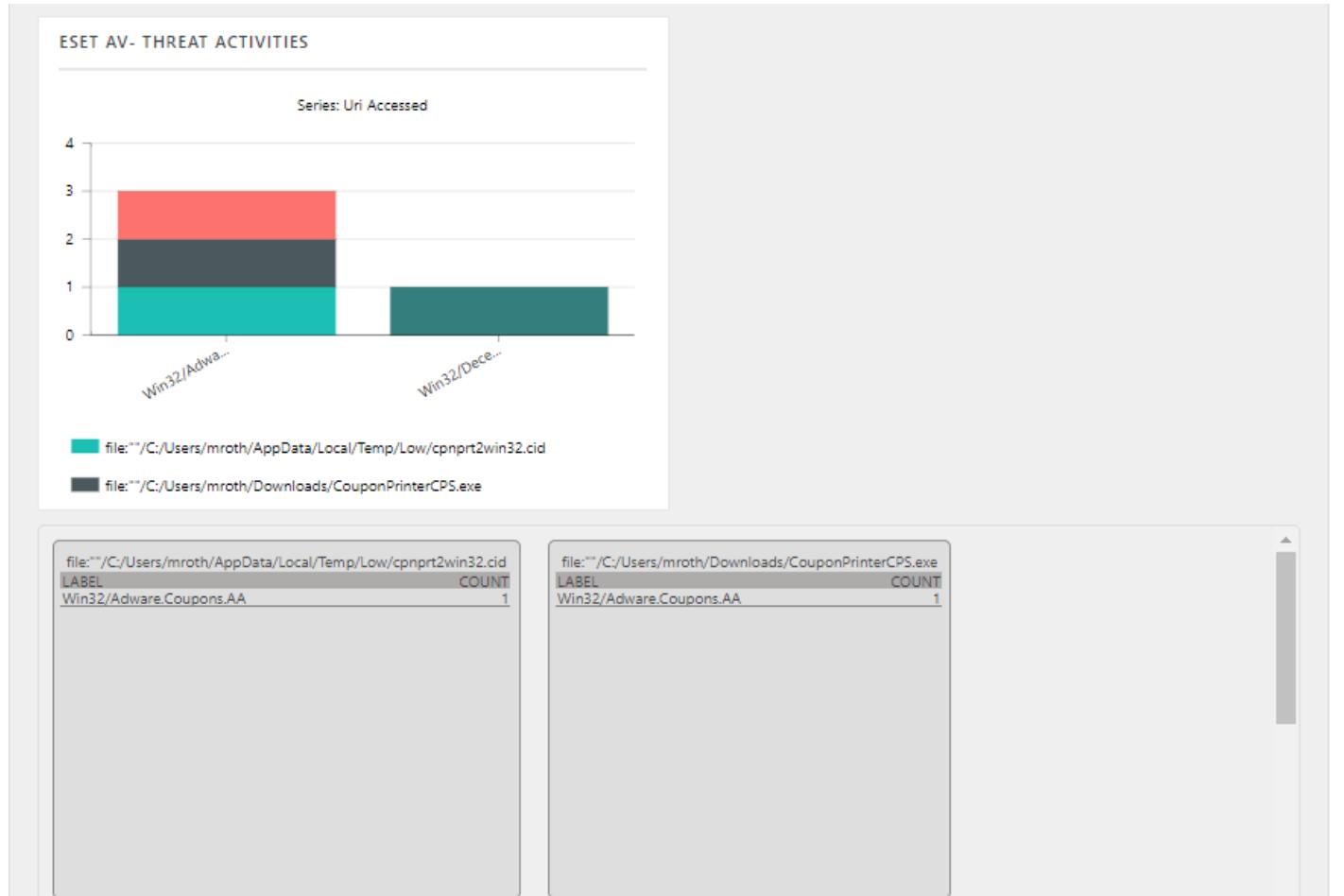


Figure 26

14. If satisfied, click **Configure** button.

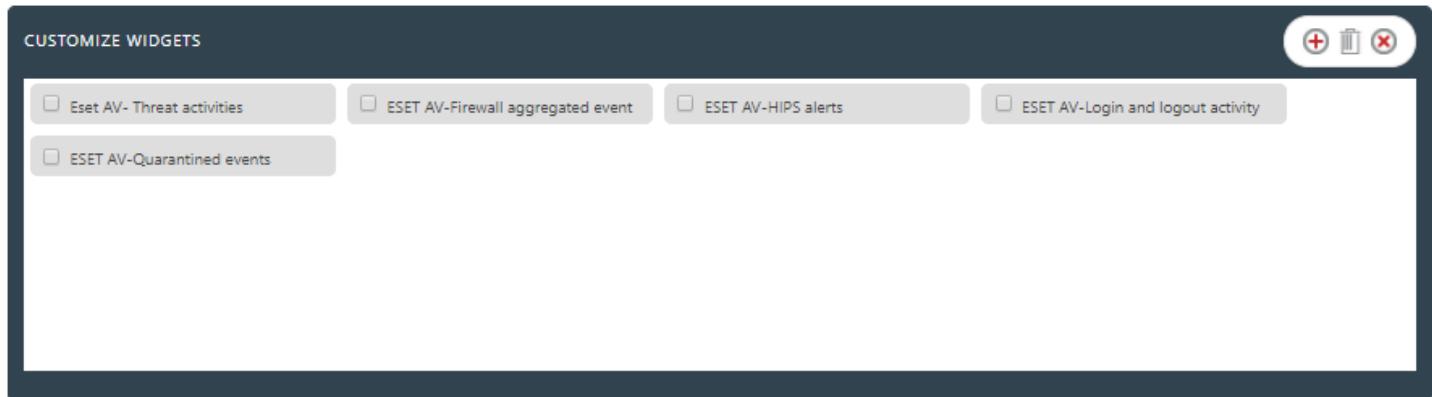
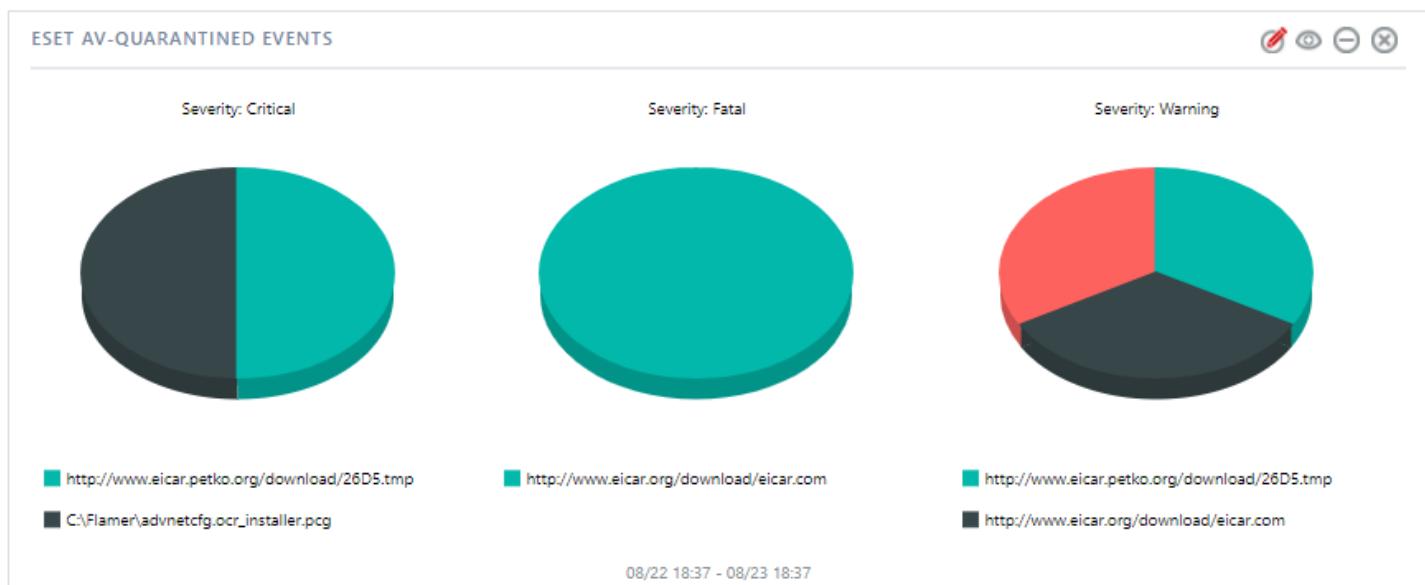


Figure 27

15. Click 'customize'  to locate and choose created dashlet.
16. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- **REPORT: ESET AV-Quarantined events**
WIDGET TITLE: ESET AV-Quarantined events
CHART TYPE: Pie
AXIS LABELS [X-AXIS]: Threat Name
LEGEND [SERIES]: Severity



- **REPORT: ESET AV-HIPS alerts**

WIDGET TITLE: ESET AV-HIPS alerts

CHART TYPE: Donut

AXIS LABELS [X-AXIS]: Target Application

LEGEND[SERIES]: Action



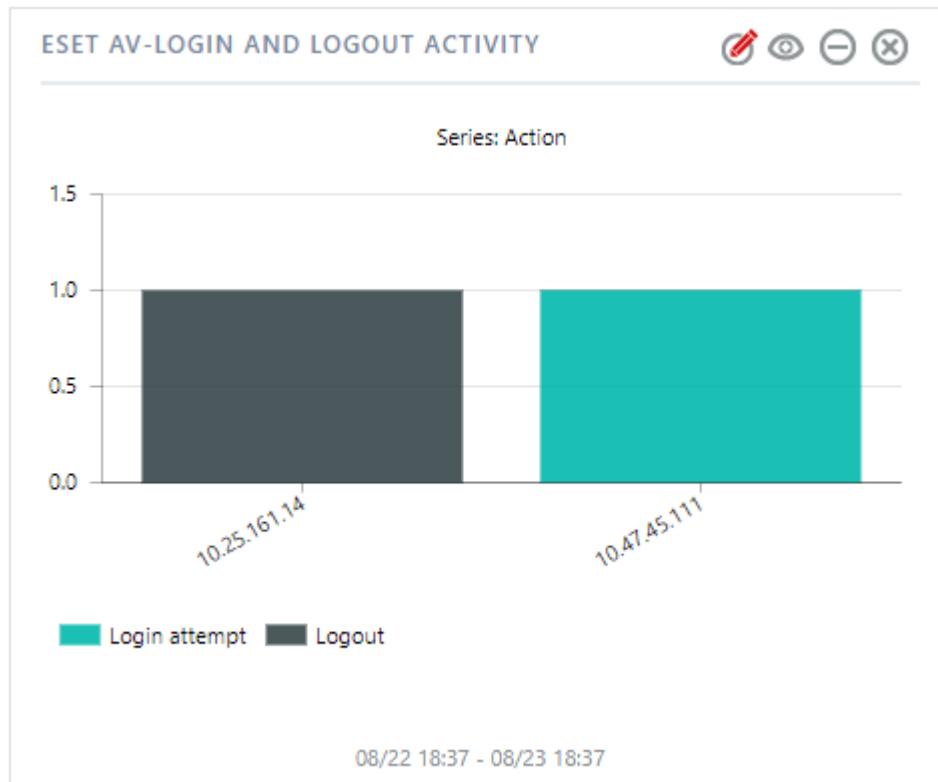
- **REPORT: Eset AV- Login and logout activity**

WIDGET TITLE: Eset AV- Login and logout activity

CHART TYPE: Stacked Column

AXIS LABELS [X-AXIS]: Source IP Address

LEGEND[SERIES]: Action



- **REPORT: ESET Antivirus-Service stopped**
WIDGET TITLE: ESET Antivirus-Service stopped
CHART TYPE: Pie
AXIS LABELS [X-AXIS]: Scan Id
LEGEND [SERIES]: User Name



- REPORT: Eset AV- Threat activities
WIDGET TITLE: Eset AV- Threat activities
CHART TYPE: Stacked Column
AXIS LABELS [X-AXIS]: Threat Name
LEGEND: Uri Accessed

