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.
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**.
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.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Host Name</th>
<th>User Name</th>
<th>User Domain</th>
<th>Source IP Address</th>
<th>Action</th>
<th>Severity</th>
<th>Occurred Time</th>
<th>Action Detail</th>
<th>Action Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/17/2017 09:47:50 PM</td>
<td>LRK-CSET</td>
<td>Administrator</td>
<td>Native user</td>
<td>10.47.45.111</td>
<td>Login attempt</td>
<td>Information</td>
<td>10-Aug-2017 11:47:27</td>
<td>Authenticating native user &quot;Administrator&quot;</td>
<td>Success</td>
</tr>
</tbody>
</table>

Logs Considered:

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

### Log Time | Event ID | Site/Computer | User | Domain | Source
---|---|---|---|---|---
8/23/2017 6:37:13 PM | 5555 | NTPLD7BLR8 | N/A | N/A | Syslog

**Event Type:** Information  
**Log Type:** Application  
**Category Id:** 0

**Description:**

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

Logs Considered:

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

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/23/2017 6:37:14 PM</td>
<td>5555</td>
<td>NTPLDTRL38 / ESET</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Description:**
Aug 08 22:44:49 10.1.1.10 Aug 8 22:39:17 LRX ESET ERServer[5371]: {"event_type":"FirewallAggregated_Event","hostname":"acme.len3 61","source_uid":"f5bbea9-7624-492-482-168-e821-6ead84f30d","occurred":"2018-08-09 12:35:03","severity":"Critical","Event Name":"Filter","source_address":"192.168.33.33","source_port":"2222","target_address":"11.2.15.120","status":"info","target_port":543,"protocol":"tcp","account":"acme.s4.tratt","process_name":"FireSignature","rule_name":"Passed packets","rule_id":"G-4896-888WDR-3569-2478-2FE9-81177EE77","inbound":true,"threat_name":"maliciousvirus.org/login class=download","aggregate_count":"3"}

---

Logs Considered:

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

---

**EventTracker**

Actionable Security Intelligence
Integrate ESET Antivirus

Logs Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/23/2017 8:37:15 PM</td>
<td>S555</td>
<td>NTPLDTBLR38 / ESRT</td>
<td>N/A</td>
<td>N/A</td>
<td>Systlog</td>
</tr>
</tbody>
</table>

Event Type: Information

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.
3. Click the **Import** tab.

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **ESET Antivirus alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button. EventTracker displays success message.

![Selected alert configurations are imported successfully.](image)

**Figure 5**

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

### Knowledge Objects

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

![EventTracker manager page with Admin option highlighted](image)

**Figure 6**

2. Locate the **ESET Antivirus knowledge objects.etko**, and then click **Import** button.
3. Choose the Knowledge objects that needs to be imported and click on **upload**.
4. Knowledge objects are now imported successfully.

Figure 9

Token Template

1. Click **Token Value** option, and then click the browse button.
2. 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](image11.png)

**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](image12.png)
3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.
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.

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

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.

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’
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.

2. Navigate to Reports>Configuration.

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

![Figure 22](image)

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

**Create Dashlets**

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

![Figure 23](image)
2. Navigate to Dashboard > Flex. 
Flex Dashboard pane is shown.

3. Fill suitable title and description and click Save button.
4. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.
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.

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

![ESET AV-HIPS Alerts Chart](chart.png)

- **Action: blocked**
- **Target Applications:**
  - HKEY_USERS\S-1-5-21-1945282642-56334563-200145766-1000\Software\Microsoft\Windows\CurrentVersion\Run:
  - C:\Windows\System32\winlogon.exe

08/22 18:37 - 08/23 18:37
• 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 Accesssed