Integrate Trend Micro Deep Security

EventTracker v9.0 and above

Publication Date: November 5, 2019
Abstract

This guide will facilitate a Trend Micro Deep Security user to send logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker v9.x or later and Trend Micro Deep Security v9.5 and above.

Audience


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 laws 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

1. Introduction .................................................................................................................................................. 3  
2. Pre-requisites .................................................................................................................................................. 3  
3. DSM syslog configuration ................................................................................................................................. 3  
   3.1 DSM server configuration ............................................................................................................................ 3  
   3.2 Configure the Policy ................................................................................................................................... 4  
4. EventTracker Knowledge Pack .......................................................................................................................... 5  
   4.1 Categories .................................................................................................................................................. 5  
   4.2 Alerts ....................................................................................................................................................... 6  
   4.3 Flex Reports ............................................................................................................................................. 7  
   4.4 Dashboards ............................................................................................................................................. 11  
5. Importing knowledge pack into EventTracker .................................................................................................. 13  
   5.1 Categories ................................................................................................................................................ 14  
   5.2 Alerts ....................................................................................................................................................... 15  
   5.3 Token Templates ....................................................................................................................................... 16  
   5.4 Flex Reports ............................................................................................................................................. 18  
   5.5 Knowledge Objects .................................................................................................................................. 19  
   5.6 Dashboards ............................................................................................................................................. 21  
6. Verifying knowledge pack in EventTracker ...................................................................................................... 22  
   6.1 Categories ................................................................................................................................................ 22  
   6.2 Alerts ....................................................................................................................................................... 23  
   6.3 Token Templates ....................................................................................................................................... 23  
   6.4 Flex Reports ............................................................................................................................................. 24  
   6.5 Knowledge Objects .................................................................................................................................. 25  
   6.6 Dashboards ............................................................................................................................................. 25
1. Introduction

Trend Micro Deep Security delivers a comprehensive security platform optimized for virtual and cloud environments. Its comprehensive security capabilities include anti-malware with web reputation, host-based firewall, intrusion detection and prevention (IDS/IPS), integrity monitoring, and log inspection.

Trend Micro Deep Security can be integrated with EventTracker using syslog forwarding. Trend Micro Deep Security KP helps to monitor the malware detection, malicious sites visited by users, authentication failures, policy management, group management, device management, and firewall activities. EventTracker triggers the alert whenever any malware is detected, any action is taken on malware, failure to act on the malware and a malicious URL detection happens. EventTracker dashboard will help you to visualize the group management, policy management, device management, and user authentication failures.

2. Pre-requisites

- EventTracker 9.x or later should be installed.
- Users should have administrator privileges to Trend Micro Deep Security Manager (DSM) console.

3. DSM syslog configuration

Deep Security has the option that either an Agent can forward events to the syslog server or the DSM can collect the events on the Agent collection interval and forward the events from the DSM server to the syslog server.

3.1 DSM server configuration

1. Log in to the DSM console.
2. Click Administration -> System Settings -> SIEM in the main menu.
3. Under System Event Notification:
   a. Select Forward System Events to a remote computer checkbox to allow the DSM manager to send logs to EventTracker.
   b. Specify the EventTracker machine IP address.
   c. Specify the UDP Port Eg:514
   d. Select syslog facility as syslog.
   e. Specify the syslog format as Common Event Format (CEF).
4. Click Save.
3.2 Configure the Policy

Forward security events directly in real-time from agent computers to an EventTracker.

Now you must add the syslog source to your policy configuration. Set the integration details at the top (root/base) policy as follows:

1. Click on Policies.
2. Go to Settings > SIEM.
3. For Anti-Malware Event Forwarding, select Forward Events To: and Relay via the Manager.
   a. Specify the EventTracker machine IP address.
   b. Specify the UDP port Eg:514
   c. Select syslog facility as syslog.
   d. Specify the syslog format as Common Event Format (CEF).
4. For Web Reputation Event Forwarding, select Forward Events To and Relay via the Manager.
   a. Specify the EventTracker machine IP address.
   b. Specify the UDP port Eg:514
   c. Select syslog facility as syslog.
   d. Specify the syslog format as Common Event Format (CEF).
5. Click Save.
Once Trend Micro Deep Security events are enabled and Trend Micro Deep Security events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Trend Micro Deep Security monitoring.

4.1 Categories

- **Trend Micro Deep Security: Antimalware activity**: This category-based report provides information related to the agent that defends against physical servers and virtual desktops.
Integrate Trend Micro Deep Security

- **Trend Micro Deep Security: Computer management**: This category-based report provides information related to computer added, computer deleted, computer updated, computer moved, and policy assigned details.
- **Trend Micro Deep Security: File integrity monitoring**: This category-based report provides information related to unexpected changes to files and systems registry in real-time.
- **Trend Micro Deep Security: Firewall activity**: This category-based report provides information related to firewall activity which displays the list of most common source IPs of denied packets.
- **Trend Micro Deep Security: Group management**: This category-based report provides information related to group create, the group removed, and the group updated by the administrator.
- **Trend Micro Deep Security: Intrusion prevention**: This category-based report provides information related to intrusion prevention that prevents attacks by detecting malicious network traffic and dropping relevant packets.
- **Trend Micro Deep Security: Policy management**: This category-based report provides information related to the policy created, policy updated, and policy deleted details.
- **Trend Micro Deep Security: Roles management**: This category-based report provides information related to roles that have access rights and editing privileges that can be assigned to users.
- **Trend Micro Deep Security: System logs**: This category-based report provides information related to logs and events generated by operating systems and applications running on the computers.
- **Trend Micro Deep Security: User authentication failed**: This category-based report provides information related to users failing to logon due to wrong credentials.
- **Trend Micro Deep Security: User logon activity**: This category-based report provides information related to the user signed in and the user signed out activities on manager console.
- **Trend Micro Deep Security: User management**: This category-based report provides information related to user-created, user deleted, user updated, and user password reset by the administrator.
- **Trend Micro Deep Security: Active directory activity**: This category-based report provides information related to computers that are discovered using Microsoft active directory.

4.2 Alerts

- **Trend Micro Deep Security: User authentication failed**: This alert is generated when the user enters the wrong credentials while logging into the manager console.
- **Trend Micro Deep Security: Agent disk space low**: This alert is generated when agent disk space is low.
- **Trend Micro Deep Security: Duplicate computer**: This alert is generated by the manager when it finds the duplicate computer.
- **Trend Micro Deep Security: Manager clock changed**: This alert is generated when a clock is changed on the manager by the user.
- **Trend Micro Deep Security: Manager disk space low**: This alert is generated when disk space is low on a manager.
- **Trend Micro Deep Security: Manager shutdown**: This alert is generated when a manager goes offline and shutdown.
• **Trend Micro Deep Security: Action taken on malware:** This alert is generated when malware is detected and action was taken on malware like deleted, quarantined, access denied and cleaned.

• **Trend Micro Deep Security: No Action taken on malware:** This alert is generated when malware is passed, and no action is taken on that malware.

• **Trend Micro Deep Security: Malicious URL detected:** This alert is generated when a malicious URL is detected in a web reputation.

• **Trend Micro Deep Security: Intrusion prevention detected:** This alert is generated when the prevention rule is reset or blocked.

• **Trend Micro Deep Security: Action failed on malware:** This alert is generated when malware is detected and actions are failed on the malware like delete failed, quarantined failed, and clean failed.

### 4.3 Flex Reports

• **Trend Micro Deep Security- Antimalware activity:** This report provides information related to antimalware activity, where the malware found on the target computer and the action taken in real-time is reported to the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Target Computer</th>
<th>File Path</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 14:10:20</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm8</td>
<td>C:\Users\trend\Desktop\Eicar.exe</td>
<td>Pass</td>
<td>Realtime</td>
</tr>
<tr>
<td>Mar 17 14:10:20</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm8</td>
<td>C:\Users\trend\Desktop\eicar.txt</td>
<td>Delete</td>
<td>Realtime</td>
</tr>
</tbody>
</table>

Mar 17 14:10:27 esxwin2k12r2vm2 Mar 17 14:10:20 esxwin2k12r2vm2 CEF:0|Trend Micro|Deep Security Agent|9.5.2456|9001|Eicar_test_file|6|cn1=1|cn1Label=Host ID|dvchost=Esxwin7vm8|cn2=205|cn2Label=Quarantine|File Size|filePath=C:\Users\trend\Desktop\eicar.txt|act=Delete|msg=Realtime

• **Trend Micro Deep Security- Computer management:** This report provides information related to computer management where the action taken by the source user from source computer on a target computer is specified.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer Name</th>
<th>Target Computer Name</th>
<th>Source User Name</th>
<th>Source IP</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 11 14:11:04</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Computer Created</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 14:11:08</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm2</td>
<td>System</td>
<td>192.168.1.131</td>
<td>Computer Updated</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 16:38:33</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Policy Assigned to Computer</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 16:39:31</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Computer Moved</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 16:39:47</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Computer Deleted</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>

Mar 11 14:11:05 esxwin2k12r2vm2 Mar 11 14:11:04 esxwin2k12r2vm2 CEF:0|Trend Micro|Deep Security Manager|9.5.2456|250|Computer Created|3|src=192.168.1.131|suser=William|target=Esxwin7vm2|msg=Description Omitted|TrendMicroDsTenant=Primary|TrendMicroDsTenantId=0
• **Trend Micro Deep Security - File integrity monitoring:** This report provides information related to integrity monitoring where the file modified, and the action taken on the target computer is reported to the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Target Computer</th>
<th>File Path</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 14:10:20</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm7</td>
<td>c:\windows\message.dll</td>
<td>updated</td>
<td>lastModified,sha1.size</td>
</tr>
</tbody>
</table>

Mar 17 14:10:27 esxwin2k12r2vm2 Mar 17 14:10:20 esxwin2k12r2vm2 CEF:0|Trend Micro|Deep Security Agent|9.5.2456|8003|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvhost=Esxwin7vm7 act=updated filePath=c:\windows\message.dll msg=lastModified,sha1.size

• **Trend Micro Deep Security - Firewall activity:** This report provides the information related to firewall activity, where the agent accesses the destination network, finds that the traffic is suspicious and then performs the action and reports it to the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Target Computer</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source MAC</th>
<th>Destination MAC</th>
<th>Source Port Port</th>
<th>Protocol</th>
<th>Ethernet Frame Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 14:10:20</td>
<td>esxwin2k12r2vm2</td>
<td>Esxwin7vm9</td>
<td>192.168.126.150</td>
<td>72.14.204.147</td>
<td>00:0C:29:EB:35:DE</td>
<td>00:56:5F:56:47:4F</td>
<td>80</td>
<td>TCP</td>
<td>IP</td>
<td>Log</td>
</tr>
</tbody>
</table>

Mar 17 14:10:27 esxwin2k12r2vm2 Mar 17 14:10:20 esxwin2k12r2vm2 CEF:0|Trend Micro|Deep Security Agent|9.5.2456|106|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dv=Esxwin7vm9 act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cnt=1 cs2Label=TCP Flags TrendMicroDsPacketData=AFB..

• **Trend Micro Deep Security - Group management:** This report provides information related to group management, where the group added, updated or removed by the source computer is specified.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer Name</th>
<th>Source User Name</th>
<th>Source IP</th>
<th>Group Name</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 15 15:41:12</td>
<td>esxwin2k12r2vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Computing</td>
<td>Group Added</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 15 15:43:23</td>
<td>esxwin2k12r2vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Computing</td>
<td>Group Removed</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>

• **Trend Micro Deep Security-Intrusion prevention**: This report provides information related to intrusion prevention where the agent detects the threat from the traffic, takes the appropriate action and reports it to the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source MAC</th>
<th>Destination MAC</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Frame Type</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 14:10:20</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.126.150</td>
<td>72.14.204.108</td>
<td>00:50:56:F5:8F:47</td>
<td>48716</td>
<td>21</td>
<td>TCP</td>
<td>IP</td>
<td>Block</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• **Trend Micro Deep Security-Policy management**: This report provides information related to policy management, where the policy is added, deleted or updated by the source user on source computer is listed.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer Name</th>
<th>Source User Name</th>
<th>Source IP</th>
<th>Policy Name</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 11 16:23:16</td>
<td>esxwin2k12r2vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Windows 7 Desktop</td>
<td>Policy Deleted</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 16:22:23</td>
<td>esxwin2k12r2vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>Base Policy</td>
<td>Policy Deleted</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 17:43:56</td>
<td>esxwin2k12r2vm2</td>
<td>William</td>
<td>192.168.1.131</td>
<td>IT</td>
<td>Policy Updated</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>

• **Trend Micro Deep Security-Roles management**: This report provides information related to roles management where the roles created or deleted by the source name on source computer is specified.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer Name</th>
<th>Source IP</th>
<th>Source Name</th>
<th>Target Name</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 11 17:00:30</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>Human Resource</td>
<td>Role Created</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 11 17:52:52</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>Human Resource</td>
<td>Role Deleted</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>
• **Trend Micro Deep Security-System logs:** This report provides information related to system logs, where the target machine which generates an event related to an operating system that belongs to security, is reported to the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Target Computer</th>
<th>Target Name</th>
<th>Target Entity</th>
<th>Message</th>
</tr>
</thead>
</table>

• **Trend Micro Deep Security-User authentication failed:** This report provides information related to user authentication failure, where the target name fails to login on the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Source IP</th>
<th>Source Name</th>
<th>Target Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 20:26:04</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>System</td>
<td>William</td>
<td>User password incorrect for username 'William' on an attempt to sign in</td>
</tr>
<tr>
<td>Mar 18 12:12:45</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>System</td>
<td>William</td>
<td>User with username William was locked out on an attempt to sign in</td>
</tr>
</tbody>
</table>

• **Trend Micro Deep Security-User logon activity:** This report provides information related to user logon activity that the user signed in and signed out from the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Source IP</th>
<th>Source Name</th>
<th>Target Name</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 17 19:42:20</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>William</td>
<td>User Signed In</td>
<td>User signed in</td>
</tr>
<tr>
<td>Mar 17 19:42:29</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>System</td>
<td>William</td>
<td>User Signed Out</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>
• **Trend Micro Deep Security-User management**: This report provides information related to user management where the source name has taken action on the target name on the source computer.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Computer</th>
<th>Source IP</th>
<th>Source Name</th>
<th>Target Name</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 10 12:45:38</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>Ellen</td>
<td>User Created</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 10 13:02:33</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>Ellen</td>
<td>User Password Set</td>
<td>Description Omitted</td>
</tr>
<tr>
<td>Mar 10 13:02:58</td>
<td>esxwin2k12r2vm2</td>
<td>192.168.1.131</td>
<td>William</td>
<td>Ellen</td>
<td>User Deleted</td>
<td>Description Omitted</td>
</tr>
</tbody>
</table>

Mar 10 12:45:43 esxwin2k12r2vm2 Mar 10 12:45:38 esxwin2k12r2vm2 CEF:0|Trend Micro|Deep Security Manager|9.5.2456|650|User Created|3|src=192.168.1.131 suser=william target=Ellen msg=Description Omitted TrendMicroDsTenant=Primary TrendMicroDsTenantId=0

4.4 Dashboards

• **Trend Micro Deep Security-Computer management** – This dashboard will show information about device management like computer created, moved, and deleted.

![Figure 3](image-url)

• **Trend Micro Deep Security-Group management** – This dashboard will show information about group management like group added and group removed.
• **Trend Micro Deep Security-Policy management** – This dashboard will show information about policy management like policy deleted, updated and new policy created.

• **Trend Micro Deep Security – User authentication failed** – This dashboard will show information about which user authentication has failed.
5. Importing knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

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

5.1 **Categories**

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click the **Category** option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like the “All Trend Micro Deep Security category.iscat” and then click on the “**Import**” button:
EventTracker displays a success message:

![Success Message](image)

**Figure 9**

**5.2 Alerts**

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Alert option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “All Trend Micro Deep Security alerts.isalt” and then click on the “Import” button.
EventTracker displays a success message:

5.3 Token Templates

For importing "Token Template", navigate to the EventTracker web interface.

1. Click Parsing Rules under the Admin option in the EventTracker web interface.
2. Next, click the “Template” tab and then click the “Import Configuration” button.

3. Now, click the “Browse” button and navigate to the knowledge packs folder (type `C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs` in the navigation bar) where “.ettd”, e.g. “All Trend Micro Deep Security templates.ettd” file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click “Import” button:
5.4 Flex Reports

1. In the EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and choose “New (*.etcrx)”: 

2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click the “Select File” button and navigate to the knowledge pack folder and select file with the extension “.etcrx”, e.g. “All Trend Micro Deep Security flex reports.etcrx”.

![Figure 16 Import](image)

![Figure 17 Export/Import Utility](image)
3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Import** button.

EventTracker displays a success message:

![EventTracker success message](image)

**5.5 Knowledge Objects**

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.
2. Next, click the “import object” icon:

3. A pop-up box will appear, click “Browse” in that and navigate to knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “All Trend Micro Deep Security knowledge object.etko” and then click “Upload” button.

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the “Import” button:
5.6 Dashboards

1. Login to the EventTracker web interface.
2. Navigate to Dashboard → My Dashboard.
3. In “My Dashboard”, Click Import Button:
4. Select the **browse** button 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. "All Trend Micro Deep Security Dashboards.etwd" is saved and click on "Upload" button.

5. Wait while EventTracker populates all the available dashboards. Now, choose "Select All" and click on "Import" Button.

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand "**Trend Micro Deep Security**" group folder to view the imported categories:
6.2 Alerts

1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
2. In search box enter “Trend Micro” and then click the Search button.

EventTracker displays an alert related to the Trend Micro Deep Security:

6.3 Token Templates

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rule.
2. In the Template tab, click on the “Trend Micro” group folder to view the imported Token Values.
6.4 Flex Reports

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

2. In Reports Configuration pane, select the Defined option.
3. Click on the “Trend Micro Deep Security” group folder to view the imported reports.
6.5 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 “Trend Micro Deep Security” group folder to view the imported Knowledge objects.

6.6 Dashboards

1. In the EventTracker web interface, click on Home Button and select “My Dashboard”.

Figure 33

Figure 34
2. In “Trend Micro Deep Security” dashboard you should be able to see something like this: