Integrate EventTracker Honeynet

EventTracker v8.x and above

Publication Date: May 15, 2017
Abstract

This guide provides instructions to configure EventTracker Honeynet to send the events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and EventTracker Honeynet: Nova 13.10.0 by Datasoft.

Audience

EventTracker Honeynet users, who wish to forward events to EventTracker Enterprise.

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

Introduction ................................................................................................................................................................. 3
Pre-requisites ............................................................................................................................................................... 3

EventTracker (ET) Honeynet (Integrated with Nova by Datasoft) ................................................................. 3  
  - Configure rsyslog to send Honeynet logs to EventTracker Enterprise .......................................................... 3  
  - Enable syslog setting on Nova GUI .................................................................................................................. 4  
  - Import ET Honeynet logs in EventTracker .................................................................................................... 5  
  - Schedule logs transfer of cron jobs to EventTracker Enterprise .............................................................. 6  
  - Configuring DLA for ET Honeynet logs ......................................................................................................... 7

EventTracker Knowledge Pack (KP) .......................................................................................................................... 11  
  - Categories ......................................................................................................................................................... 11  
  - Alerts ................................................................................................................................................................. 11  
  - Flex Reports ..................................................................................................................................................... 11

Import ET Honeynet knowledge pack into EventTracker .................................................................................. 13  
  - Category .......................................................................................................................................................... 14  
  - Alerts ................................................................................................................................................................. 15  
  - Parsing Rules .................................................................................................................................................. 16  
  - Flex Reports .................................................................................................................................................. 17  
  - To import Knowledge Object ......................................................................................................................... 18

Verify ET Honeynet knowledge pack in EventTracker ....................................................................................... 20  
  - Categories ......................................................................................................................................................... 20  
  - Alerts ................................................................................................................................................................. 21  
  - Parsing Rules .................................................................................................................................................. 22  
  - Flex Reports .................................................................................................................................................. 23  
  - Verifying Knowledge Object .......................................................................................................................... 24

Create Flex Dashboards in EventTracker ............................................................................................................ 25  
  - Schedule Reports .......................................................................................................................................... 25  
  - Create Dashlets ............................................................................................................................................ 28  
  - Sample Flex Dashboards ............................................................................................................................... 31
Introduction

A Honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker’s activities and methods can be studied and that information can be used to increase network security. A Honeynet contains one or more honeypots which are computer systems on the internet expressly set up to attract and trap people who attempt to penetrate other people’s computer systems.

EventTracker Honeynet provides an additional level of support by enabling you to generate reports and run searches on data to improve your ability to manage networks.

Pre-requisites

- EventTracker should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- FTP server must be installed on EventTracker machine.
- EventTracker Honeynet should be deployed.

NOTE: To deploy ET Honeynet, please contact support team for the download link to ET Honeynet OVA package and the installation guide.

EventTracker (ET) Honeynet (Integrated with Nova by Datasoft)

Configure rsyslog to send Honeynet logs to EventTracker Enterprise

1. Open rsyslog.conf in VI Editor.
2. Using following command, add an entry to the EventTracker Enterprise.

   `Syslogfacility.priority<tab>@ ip of the EventTracker Enterprise`

   For example: If Honeynet logs were sent as local1 and to collect all logs it will be mentioned as log_info , then the following entry can be made in-

   `local1.info @@RemotehostIPADDRESS: Port_No`

NOTE: Use ‘@@’ for TCP and ‘@’ for UDP to forward logs to Remote host.
3. Save and restart the rsyslog service.

Enable syslog setting on Nova GUI

1. Log into Nova Web user interface.
2. Select Settings from Configuration.

3. Enable Rsyslog.
4. Specify the Remote log server IP address i.e. **10.50.81.23** address of EventTracker Enterprise.
5. Specify Remote Log Server Port i.e. **514**.
6. Select UDP Port.
7. Select configured Ethernet interfaces.
8. Click on Save Changes.
**Integrate EventTracker Honeynet**

**Figure 2**

**Import ET Honeynet logs in EventTracker**

1. Open ET Honeynet system via **SSH (Secure Shell)**.
2. Go to the path `/ethoneynetreport/script/`.
3. Open file `ethoneynetreports.sh` in VI Editor.

To go into edit mode, press ESC and enter I

4. Modify relevant parameters as per the requirements and then follow the steps mentioned below:

**NOTE:** The parameters that have to be modified are:
Integrate EventTracker Honeynet

**Figure 3**

- **$HOST** – IP Address of EventTracker Manager
- **$USER** – FTP username (ETAdmin)
- **$PASSWD** – Password for relevant FTP user in base64 encoded form

For encoding password in base64 format, use following command:

```
[root@etvas8r3 ~]# echo P@ssword | base64
UEBzc3dvcmQK
```

Schedule logs transfer of cron jobs to EventTracker Enterprise

1. Open ET Honeynet system via **SSH (Secure Shell)**.
2. Go to the path `/ethoneynetreport/script/`.
3. Open file `ethoneynetreporttransfer.sh` in VI Editor.
4. Modify relevant parameters as per the requirements.
5. Enter the command `crontab -e`.
6. Press ‘i’ to insert a command.
7. Enter the time of schedule (i.e. Minute, Hour, Day, Month, and Day of Week).
8. We can schedule the script on daily as well as hourly basis.

   **For example,**

   Scheduling of script on daily basis:
   ```
   0 0 * * * /ethoneynetreport/script/ethoneynetreports.sh daily
   ```
   Scheduling of script on hourly basis:
   ```
   0 * * * * /ethoneynetreport/script/ethoneynetreports.sh hourly
   ```

   **NOTE:** It is mandatory to provide parameter with script as **(daily or hourly)**, otherwise script will send whole report again and again to EventTracker manager.

   The report scans once in a day or every hour as per schedule.
For verification of crontab, run the following command:

```
[root@etvas8r3 script]# crontab -l
0 0 * * * /ethoneynetreport/script/ethoneynetreports.sh daily
0 * * * * /ethoneynetreport/script/ethoneynetreports.sh hourly
```

Figure 4

9. Press **Escape** key on keyboard, type **:wq**, and then press the **Enter** button.
10. Restart the service using the following command ‘**service crond restart**’.

```
[root@etvas8r3 script]# service crond restart
Redirecting to /bin/systemctl restart crond.service
```

Figure 5

Once the schedule action runs, it will send csv reports to EventTracker manager machine.

**Configuring DLA for ET Honeynet logs**

Once .csv files are received, below mentioned procedure can be followed, that helps to configure DLA for consuming ET Honeynet logs.

1. Logon to EventTracker.
2. Navigate to **Admin>Manager**.
3. Select **Direct Log Archiver / NetFlow Receiver** tab, enable “Direct log file archiving from external sources”.
4. Enter appropriate purge frequency and click **Add**.
5. Configure DLA options as shown below:

### Figure 6

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>DROP RATE</th>
<th>DECODE PACKET</th>
<th>RECORD BINARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>9991</td>
<td>0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9992</td>
<td>0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9993</td>
<td>0</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
6. Configure ET Honeynet log file as shown above. Compose log file path as given below: i.e. FTP folder where all ET Honeynet CSV files are received.
7. Select Log Source as “ET Honeynet”. Enter ET Honeynet server’s IP Address and Name in respective fields.

**NOTE:** it is mandatory to provide Log Source as “ETHoneynet”.

8. Scroll down and click Save and Close to apply.

9. Click Save on DLA pane to complete configuration.
Integrate EventTracker Honeynet

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker; alerts and reports can be configured into EventTracker.

The following Knowledge Packs are applicable in EventTracker v8.x and later to support ET Honeynet:

Categories

- **ET Honeynet: Suspect hostile activity** - This category provides information related to suspect hostile activity which has protected IPs contacted, distinct TCP ports contacted, distinct UDP ports contacted and suspect IP address details.
- **ET Honeynet: Connections from suspect** - This category provides information related to connections from suspect displays that suspect IP touching the configured honeypot IPs.
- **ET Honeynet: Packet count summaries** - This category provides information related to packet count summaries for TCP, UDP, ICMP ports contacted by the suspect IP address.
- **ET Honeynet: Packet size Summaries** - This category provides information related to packet sizes received from suspect IP to the honeynet IP’s.

Alerts

- **ET Honeynet: Suspect hostile activity** - This alert is generated when suspect hostile activity occurs.

Flex Reports

- **ET Honeynet: Connections from suspect**

This report provides the information related to connections from suspect which displays suspect IP contacting the honeypot IPs through the protocols via the configured interface.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Suspect IP Address</th>
<th>Interface</th>
<th>Protocol Type</th>
<th>Honeypot IP</th>
<th>Port</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/07/2016 06:54:45 PM</td>
<td>Honeynet</td>
<td>42.51.30.22</td>
<td>ens160</td>
<td>icmp</td>
<td>10.30.72.98</td>
<td>8</td>
<td>39</td>
</tr>
<tr>
<td>06/07/2016 06:54:56 PM</td>
<td>Honeynet</td>
<td>42.51.30.22</td>
<td>ens160</td>
<td>icmp</td>
<td>10.30.65.11</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>06/07/2016 07:01:22 PM</td>
<td>Honeynet</td>
<td>60.104.112.210</td>
<td>ens160</td>
<td>tcp</td>
<td>10.42.51.121</td>
<td>23</td>
<td>6</td>
</tr>
<tr>
<td>06/07/2016 07:08:30 PM</td>
<td>Honeynet</td>
<td>29.10.36.54</td>
<td>ens160</td>
<td>tcp</td>
<td>10.35.22.122</td>
<td>80</td>
<td>8</td>
</tr>
<tr>
<td>06/07/2016 07:10:12 PM</td>
<td>Honeynet</td>
<td>29.10.36.54</td>
<td>ens160</td>
<td>tcp</td>
<td>10.54.32.27</td>
<td>23</td>
<td>4</td>
</tr>
<tr>
<td>06/07/2016 07:12:25 PM</td>
<td>Honeynet</td>
<td>29.10.36.54</td>
<td>ens160</td>
<td>tcp</td>
<td>10.55.25.32</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>06/07/2016 07:15:35 PM</td>
<td>Honeynet</td>
<td>68.54.36.20</td>
<td>ens160</td>
<td>udp</td>
<td>10.36.42.58</td>
<td>53</td>
<td>12</td>
</tr>
<tr>
<td>06/07/2016 07:20:36 PM</td>
<td>Honeynet</td>
<td>160.139.50.103</td>
<td>ens160</td>
<td>tcp</td>
<td>10.38.43.55</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>06/07/2016 07:20:48 PM</td>
<td>Honeynet</td>
<td>187.172.89.190</td>
<td>ens160</td>
<td>tcp</td>
<td>10.38.43.58</td>
<td>445</td>
<td>9</td>
</tr>
<tr>
<td>06/07/2016 07:20:59 PM</td>
<td>Honeynet</td>
<td>187.172.89.190</td>
<td>ens160</td>
<td>icmp</td>
<td>10.36.43.55</td>
<td>8</td>
<td>5</td>
</tr>
</tbody>
</table>

Figure 9
Integrate EventTracker Honeynet

Logs Considered:

- **ET Honeynet: Packet count summaries**

This report provides information related to packet count summaries that counts TCP, UDP and ICMP packets received from the suspect IP to the honeypot IPs.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Suspect IP Address</th>
<th>Interface</th>
<th>Count TCP</th>
<th>Count UDP</th>
<th>Count ICMP</th>
<th>Count Other</th>
<th>Count TCPACK</th>
<th>Count TCPPFIN</th>
<th>Count TCPReset</th>
<th>Count TCPSYN</th>
<th>Count TCPSYNACK</th>
<th>Count Total</th>
<th>Count Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00/04/2016 03:17:48 AM</td>
<td>Honeynet</td>
<td>169.125.215.30</td>
<td>ens180</td>
<td>1417</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1173</td>
<td>204</td>
<td>12</td>
<td>244</td>
<td>0</td>
<td>1417</td>
<td>78395</td>
</tr>
<tr>
<td>00/04/2016 03:22:39 AM</td>
<td>Honeynet</td>
<td>165.154.71.12</td>
<td>ens180</td>
<td>582</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>471</td>
<td>69</td>
<td>33</td>
<td>111</td>
<td>0</td>
<td>582</td>
<td>28671</td>
</tr>
<tr>
<td>00/04/2016 03:33:49 AM</td>
<td>Honeynet</td>
<td>222.102.12.15</td>
<td>ens180</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>145</td>
<td>145</td>
</tr>
<tr>
<td>00/04/2016 03:40:12 AM</td>
<td>Honeynet</td>
<td>66.49.52.96</td>
<td>ens180</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>145</td>
<td>145</td>
</tr>
<tr>
<td>00/04/2016 03:45:28 AM</td>
<td>Honeynet</td>
<td>179.125.111.82</td>
<td>ens180</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>00/04/2016 03:49:35 AM</td>
<td>Honeynet</td>
<td>211.36.51.133</td>
<td>ens180</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>156</td>
</tr>
<tr>
<td>00/04/2016 03:52:40 AM</td>
<td>Honeynet</td>
<td>123.142.23.213</td>
<td>ens180</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>360</td>
<td>360</td>
</tr>
</tbody>
</table>

- **ET Honeynet-Packet size summaries**
This report provides information related to packet size summaries i.e the size of packets received from the suspect IP to the honeypot IPs.

<table>
<thead>
<tr>
<th>Event Date</th>
<th>Suspect IP</th>
<th>Interface</th>
<th>Packet Size</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>665</td>
<td>1</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>664</td>
<td>1</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>657</td>
<td>1</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>639</td>
<td>1</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>611</td>
<td>1</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>473</td>
<td>2</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>52</td>
<td>11</td>
</tr>
<tr>
<td>Thu Aug 4 20:04:12 IST 2016</td>
<td>207.250.200.166</td>
<td>ens160</td>
<td>40</td>
<td>102</td>
</tr>
</tbody>
</table>

**Figure 13**

**Logs Considered:**

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/10/2016 2:21:51 PM</td>
<td>3330</td>
<td>enobi-0104</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>ET Honeynet</td>
</tr>
</tbody>
</table>

**Event Type:** Information  
**Log Type:** System  
**Category Id:** 2  
**Description:**  
ip: 192.168.25.185  
interface: ens160  
packetSize: 57  
count: 60  

**Figure 14**

### Import ET Honeynet knowledge pack into EventTracker

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

- Categories  
- Alerts  
- Parsing Rules  
- Flex Reports  
- Knowledge object

1. Launch **EventTracker Control Panel**.  
2. Double click **Export Import Utility**.
3. Click the **Import** tab.
4. Import knowledge pack as specified in the sequence.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate the **All ET Honeynet group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

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

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the All ET Honeynet group of alerts.isalt file, and then click the Open button.

![Figure 18](image1)

2. To import alerts, click the Import button.

EventTracker displays success message.

![Figure 19](image2)

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

**Parsing Rules**

1. Click Token value option, and then click the browse button.
2. Locate the **All ET Honeynet group of parsing rules.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button.

   EventTracker displays success message.

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

**Flex Reports**

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

2. Locate the **All ET Honeynet group of flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.

![Figure 23](image-url)

**To import Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **‘Import’** icon.
3. In **IMPORT** pane click on **Browse** button.

4. Locate **All ET Honeynet group of knowledge object. etko** file, and then click the **UPLOAD** button.
Verify ET Honeynet knowledge pack in EventTracker

Categories

1. In the EventTracker Enterprise, web interface, click the Admin dropdown, and then click Categories.
2. In the Category Tree, expand ET Honeynet group folder to see the imported categories.
Integrate EventTracker Honeynet

Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type 'ET Honeynet', and then click Go button.

    Alert Management page will display all the imported ET Honeynet alert
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 28](image.png)

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.

**Parsing Rules**

1. In the **EventTracker Enterprise** web interface, click the **Admin** menu, and then click **Parsing Rules**.
2. Select **ET Honeynet**.
In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.

In Reports Configuration pane, select Defined option.

EventTracker displays Defined page.

In search box enter ‘ET Honeynet’, and then click the Search button.

EventTracker displays Flex reports of ET Honeynet
Verifying Knowledge Object

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Knowledge Objects.
3. In Objects Tree, select ET Honeynet group folder.

Imported ET Honeynet objects are shown on the right pane.
Integrate EventTracker Honeynet

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.

Figure 34


4. Click on ‘schedule’ to plan a report for later execution.
Integrate EventTracker Honeynet

Figure 35

**REPORT WIZARD**

**TITLE:** ET HONEYNET CONNECTIONS FROM SUSPECT LOGS

Review cost details and configure the publishing options.

**DISK COST ANALYSIS**

Estimated time for completion: 02:20:32 (H:MM:SS)
Number of cases to be processed: 1
Available disk space: 256 GB
Required disk space: 30 MB

Enable publishing option [Configure SMTP Server in manager configuration screen to use this option]
- Delivery results via E-mail
- Notify results via E-mail

To Email: [Enter email(s) separated by a comma]

Update status via RSS: Select Fixed

Persist data in EventVault Explorer

Figure 36

**REPORT WIZARD**

**TITLE:** ET HONEYNET CONNECTIONS FROM SUSPECT DATA PERSIST DETAIL

Select columns to persist

**RETENTION SETTING**

Retention period: 7 days

Persist in database only

**SELECT COLUMNS TO PERSIST**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PERSIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>☑</td>
</tr>
<tr>
<td>Suspect IP Address</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>☑</td>
</tr>
<tr>
<td>Protocol Type</td>
<td></td>
</tr>
<tr>
<td>Honeypot IP</td>
<td>☑</td>
</tr>
<tr>
<td>Port</td>
<td>☑</td>
</tr>
</tbody>
</table>
5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
6. Proceed to next step and click **Schedule** button.
7. Wait till the reports get generated.

Create Dashlets

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

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

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

5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
6. Proceed to next step and click **Schedule** button.
7. Wait till the reports get generated.
4. Fill suitable title and description and click **Save** button.
5. Click to configure a new flex dashlet. Widget configuration pane is shown.

![Widget Configuration](image)

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

16. Click ‘customize’ 🕵️ to locate and choose created dashlet.

17. Click  🔗 to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard DATA SOURCE: ET Honeynet-Connections from suspect

1. ET Honeynet: Suspect TCP Connections by IP

WIDGET TITLE: ET Honeynet Suspect TCP connections by IP

CHART TYPE: Stacked Column

AXIS LABELS [X-AXIS]: Suspect IP Address

Label Text: Suspect IP

FILTER: Protocol Type

FILTER Values: tcp

Figure 42
2. **ET Honeynet: Suspect TCP Connections by Port**

**WIDGET TITLE:** ET Honeynet Suspect TCP connections by Port

**CHART TYPE:** Stacked Column

**AXIS LABELS [X-AXIS]:** Port

**Label Text:** Port Number

**FILTER:** Protocol Type

**FILTER Values:** tcp

![ET HONEYPOT SUSPECT TCP CONNECTIONS BY PORT](image)

*Figure 43*
3. **ET Honeynet: Honeypot TCP Connections by IP**

**WIDGET TITLE:** ET Honeynet Suspect TCP connections by Port

**CHART TYPE:** Stacked Column

**AXIS LABELS [X-AXIS]:** Honeypot IP

**Label Text:** Honeypot IP

**FILTER:** Protocol Type

**FILTER Values:** tcp

![ET Honeynet Honeypot TCP Connections by IP Chart](image)

*Figure 44*
4. **ET Honeynet: Suspect ICMP Connections by IP**

**WIDGET TITLE:** ET Honeynet Suspect TCP connections by Port  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** Suspect IP Address  
**Label Text:** Suspect IP  
**FILTER:** Protocol Type  
**FILTER VALUES:** icmp

![ET Honeynet Suspect ICMP Connection by IP](image)

*Figure 45*
5. **ET Honeynet: Suspect UDP Connections by IP**

**WIDGET TITLE:** ET Honeynet Suspect UDP connections by IP

**CHART TYPE:** Stacked Column

**AXIS LABELS [X-AXIS]:** Suspect IP Address

**Label Text:** Suspect IP

**FILTER:** Protocol Type

**FILTER Values:** udp

![Figure 46](image-url)
6. **ET Honeynet: Honeypot UDP Connections from IP**

**WIDGET TITLE:** ET Honeynet Honeypot UDP connections by IP

**CHART TYPE:** Stacked Column

**AXIS LABELS [X-AXIS]:** Honeypot IP

**Label Text:** Honeypot IP

**FILTER:** Protocol Type

**FILTER VALUES:** udp

![ET HONEYPOT HONEYPOT UDP CONNECTIONS...](image)

Figure 47
7. **ET Honeynet: Suspect UDP Connections from Port**

   **WIDGET TITLE:** ET Honeynet Suspect UDP connections by Port

   **CHART TYPE:** Stacked Column

   **AXIS LABELS [X-AXIS]:** Suspect IP

   **Label Text:** Honeypot IP

   **FILTER:** Protocol Type

   **FILTER Values:** udp

   ![Graph showing ET Honeynet Suspect UDP Connections by Port](image)

   **Figure 48**