Integrate Check Point Firewall

EventTracker v8.x and above

Publication Date: January 11, 2018
Abstract

This guide helps you in configuring Check Point and EventTracker to receive Check Point events. You will find the detailed procedures required for monitoring Check Point.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise v8.x and later, Check Point R75.40 and later.

Audience

Check Point users, who wish to forward Events to EventTracker Manager and monitor events using 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

Abstract .................................................................................................................................................................... 1  
Scope ...................................................................................................................................................................... 1  
Audience ............................................................................................................................................................... 1  
Overview .............................................................................................................................................................. 4  
Integration of Check Point with EventTracker using API ....................................................................................... 4  
  Prerequisites for API .............................................................................................................................................. 4  
  Check Point – Mandatory Configurations ............................................................................................................. 4  
  Set the Rule ............................................................................................................................................................ 4  
  Register OPSEC Application – get Client DN ....................................................................................................... 12  
  Get Server DN ........................................................................................................................................................ 17  
  To get Server DN on Check Point R75.XX and later ............................................................................................. 18  
  Configure Check Point to track Log ...................................................................................................................... 19  
  Install Policy ........................................................................................................................................................ 20  
  Configure EventTracker – the Check Point Certificate ....................................................................................... 22  
  Configure EventTracker Agent ............................................................................................................................. 23  
Integration of Check Point with EventTracker using Syslog .................................................................................. 30  
  Prerequisites for Checkpoint Syslog ...................................................................................................................... 30  
  Check Point –Mandatory Configuration ............................................................................................................... 30  
EventTracker Knowledge Pack .................................................................................................................................. 31  
  Categories ............................................................................................................................................................ 31  
  Alerts .................................................................................................................................................................. 32  
  Reports ................................................................................................................................................................. 33  
Import knowledge pack into EventTracker ............................................................................................................ 40  
  To import Alerts .................................................................................................................................................. 41  
  To import Token Templates ................................................................................................................................. 43  
  To import Flex Reports ...................................................................................................................................... 44  
Verify knowledge pack in EventTracker .................................................................................................................. 45  
  Verify Alerts ........................................................................................................................................................... 45  
  Verify Token Templates ....................................................................................................................................... 46  
  Verify Flex Reports .............................................................................................................................................. 46
Create Dashboards in EventTracker ................................................................. 47
Schedule Reports .......................................................................................... 47
Create Dashlets .......................................................................................... 49
Sample Flex Dashboards ............................................................................ 54
Overview

Check Point offer the perfect combination of proven security, easy deployment and effective management by consolidating key security applications (firewall, VPN, intrusion prevention, and antivirus and more) into the same single, efficiently managed solution.

EventTracker’s built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

Note: - Check Point logs can be integrated by using Syslog as well as by API. Below guide gives both the Integration methods. You can choose the preferred integration method as per your architecture requirement.

Integration of Check Point with EventTracker using API

Prerequisites for API

- EventTracker v8.x and later should be installed.
- Administrative access to Check Point Smart Console.

Check Point – Mandatory Configurations

There are certain configuration settings you ought to do in the Check Point before you attempt to configure ET Agent to read the Check Point logs.

Set the Rule

Begin by adding a rule that allows the EventTracker host to pull the certificate from the Check Point SmartCenter server, TCP port 18210, and that allows the LEA (Log Event API) connection from EventTracker as the LEA Client and the Check Point LEA Server, TCP port 18184.

NOTE:

The port 18210 connection is only needed during the configuration of the OPSEC connection.

EventTracker can receive logs from the Check Point Management system; SmartCenter, Customer Management Add-on (CMA) in a Provider-1 environment, or from a Customer Log Module (CLM), a dedicated Check Point log server. This example uses a SmartCenter server.
1. Open the Smart Dashboard.

![Figure 1](image)

You need to add a rule in ‘Security’.

For Check Point server R70 and later same steps should be followed but in **Firewall** tab.

2. Select the **Security** tab, if it is not selected.
3. Select the **Rules** menu, select **Add Rule**, and then select **Top** option.
Integrate Check Point Firewall

Figure 2

SmartDashboard displays the newly added Rule.
The newly added Rule is a very generic rule. Edit each field as per your requirement.

4. Double-click the **NAME** column.
   Check Point displays the Rule Name dialog box.
5. Enter an appropriate name in the **Rule Name** field (example: EventTracker) and then click the **OK** button.

![Figure 4](image)

![Rule Name](image)

**Figure 4**

**Figure 5**

**NOTE:**

SOURCE is the system where EventTracker Agent is installed and DESTINATION is the system where Check Point is installed. Check Point and EventTracker Agent may co-exist on the same system or on two different systems.

6. Right-click the **SOURCE** column
   Check Point displays the shortcut menu.
7. From the shortcut menu, choose **Add...** Check Point displays the Add Object window.

![Add Object Window](image1.png)

**Figure 6**

8. Select the source and then click the **OK** button.

*(Example: Toons)*

9. Right-click the **DESTINATION** column.

Check Point displays the shortcut menu.

10. From the shortcut menu, choose **Add...**

    Check Point displays the Add Object window.

![Add Object Window](image2.png)

**Figure 7**

11. Select the destination and then click the **OK** button. *Example: pnpl-123-mar_mgmt*
12. Right-click the **SERVICE** column.
   Check Point displays the shortcut menu.

13. From the shortcut menu, select **Add...** Check Point displays the Add Object window.

   ![Figure 8](image)

14. Select the **FW1_ica_pull & FW1_lea** Services and then click the **OK** button.

15. Right-click the **ACTION** column.

   Check Point displays the shortcut menu.

16. From the shortcut menu, select **accept**.

   ![Figure 9](image)

17. Right-click the **TRACK** column.

   Check Point displays the shortcut menu.

18. From the shortcut menu, choose **Account**.
19. Configure **VPN, Install on** and **Time** as per policy.

Check Point displays the new configuration settings as shown below.

20. Click **Save** on the toolbar to save the settings.
Register OPSEC Application – get Client DN

Now you need to add an OPSEC application object for EventTracker LEA Client i.e. register/activate the OPSEC Application.

1. Click the **Manage** menu and then select the **Servers and OPSEC Applications…** option.

   **NOTE:**
   Select this option to add OPSEC Application server to the Check Point server.

2. Check Point displays the Servers and OPSEC Applications dialog box.
3. Click the **New** button. Check Point displays the shortcut menu.
4. From the shortcut menu, select **OPSEC Application...**

Check Point displays the OPSEC Application Properties window.
5. Enter appropriate details in the relevant fields.

Example:

**Name** = etagent

**Host** = pnpl testlab1 (name of the system where Check Point is installed)

**Vendor** = User Defined  **Client Entities**

= LEA
6. Click the **Communication** button.  
Check Point displays the Communication window.

7. Enter the Activation Key in the **Activation key** and **Confirm Activation Key** fields.

**NOTE:**  
Remember the key to get the certificate. This key may be of any value. (Example: 9794)

8. Click **Initialize**.  
After initializing, Check Point will display a string in the **Trust state** field.

9. Click the **Close** button.  
Check Point displays the OPSEC Application Properties window.
Copy the Client DN string to a safer location.

10. Click the **OK** button.

Check Point displays the Servers and OPSEC Application window.
11. Click the **Close** button.

**Get Server DN**

1. Expand the **Check Point** node on the tree pane.
   
   EventTracker can receive logs from the Check Point Management system; SmartCenter, Customer Management Add-on (CMA) in a Provider-1 environment, or from a Customer Log Module (CLM).

2. Double-click the system where the Check Point logs will be stored. In this example, it is the SmartCenter server.
3. Copy the Server DN string to a safer location.
4. Click the OK button.
5. To save the settings, click the Save button on the toolbar.

To get Server DN on Check Point R75.XX and later

Please follow the steps mentioned below.

1. Run the `cpca_client lscert -kind SIC` command on the Security Management Server.

   It will list all SIC certificates.
Integrate Check Point Firewall

2. Copy the server DN.

Configure Check Point to track Log

In the Check Point rules the Track column defines the Tracking option for connections that match the rule. In addition, there are log settings for the SmartDefense protections.

1. Click the system where Check Point is installed.

2. Click the **SmartDefense** tab.

Management server certificate will be the one with CN=cp_mgmt.
3. Expand all the nodes and then select **Log** from the **Track** drop-down list.

4. To save the settings, click the **Save** button on the toolbar.

**Install Policy**

You need to install the policy to implement newly created Rule on Firewall.

1. Click the **Policy** menu and then select the **Install...** option.

   Check Point displays the SmartDashboard Warning message.
2. Click the **OK** button.

Check Point displays the Install Policy window.

3. Click the **OK** button.

Check Point displays a successful message.
4. Click the **Close** button.

**Configure EventTracker – the Check Point Certificate**

To get the certificate, you need to execute the command-line utility `opsec_pull_cert.exe`. You can find this in the folder `\<INSTALLDIR>\EventTracker\Agent`.

1. Run the command prompt.
2. Go to the directory where `opsec_pull_cert.exe` exists.
3. Run the following command:

   ```
   ```

**NOTE:**

All the parameters are as we used while registering the application in the Smart Dashboard.

19.14.1.14 is the IP of the Check Point SmartCenter server or CMA which is also an Internal Certificate Authority in the Check Point architecture. etagent is the name of the OPSEC Application.

9794 is the Activation Key/Password we used to initialize the connection.

etagent.p12 is the name of the output (this could be any name, but the extension should be p12).
Integrate Check Point Firewall

Figure 25

You will find the certificate (etagent.p12) in the directory where the ‘opsec_pull_cert.exe’ is located typically `\<INSTALLDIR>\EventTracker\Agent`.

NOTE:

Once the certificate is pulled from the Check Point SmartCenter server, then status in the OPSEC Application object changes to Trust Established. If for some reason it is necessary to pull the certificate again follow these steps;

a) On the EventTracker host delete the certificate file; for instance etagent.p12.

b) Using a SmartDashboard connection to the SmartCenter server in the Communication window of the OPSEC Application object for EventTracker reset and then initialize to create a new certificate. Refer step 8 to Register the OPSEC Application Object section.

c) On the EventTracker host repeat step 3 above using the ‘opsec_pull_cert’ command to pull create the certificate file.

Now Check Point is configured.

Configure EventTracker Agent

1. Double click Control Panel, double click EventTracker Agent Configuration.

2. Click Log File Monitor tab, select Logfile Monitor, if not selected.
3. Select the **Add File Name** button.

EventTracker displays the ‘Enter File Name’ window.
4. Select **CHECK POINT** from the Select **Log File Type** drop-down list.
Integrate Check Point Firewall

EventTracker displays the Enter File Name window with new fields to fill-in.

a. Communication Method - select an option from the drop-down list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC_SSLCA</td>
<td>Encryption Method: 3DES</td>
</tr>
<tr>
<td></td>
<td>Compressed: No</td>
</tr>
<tr>
<td>OPSEC_SSLCA_COMP</td>
<td>Encryption Method: 3DES</td>
</tr>
<tr>
<td></td>
<td>Compressed: Yes</td>
</tr>
</tbody>
</table>

b. LEA Server Name - Enter a name for the LEA server.

c. Client DN - refer to Figure 16 OPSEC Application Properties – Client DN.

d. Server DN - refer to Figure 18 Check Point Gateway – General Properties – Server DN.

e. SSLCA file - Click the button. EventTracker displays the Open window.

- Go to the Agent folder, typically ...\Program Files\Prism Microsystems\EventTracker\Agent.
- Select the SSLCA file (etagent.p12) and then click the Open button.
EventTracker populates the SSLCA file field

f. Server IP - 19.14.1.14 is the IP where the Check Point logs are stored. EventTracker can receive logs from the Check Point Management system; SmartCenter, Customer Management Add-on (CMA) in a Provider-1 environment, or from a Customer Log Module (CLM). In this example it is the SmartCenter server.

g. Server Port – Enter 18184, which is the default port for the Check Point LEA server.

EventTracker displays the Agent Configuration window as shown below.
Integrate Check Point Firewall

Figure 31

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td>This option is selected by default. Select this option to receive live Check Point logs when the configuration takes effect.</td>
</tr>
<tr>
<td><strong>Historical</strong></td>
<td>Select this option to read from previous logs and the current logs as well. This option has two modes namely Current Logs and All Logs. Select the Current Logs option to read from the first record of the current log. This mode is selected by default. Select the All Logs option to read from all the backed up logs and the current logs.</td>
</tr>
</tbody>
</table>

5. Click the **OK** button.
NOTE:

When the Agent starts reading log records it records the file id and position read in the registry. If you change to read historical – all, then it may not update the registry entry. This can be monitored by looking at the registry entries in;

\texttt{HKLM\SOFTWARE\Prism Microsystems\EventTracker\Agent\Check Point}

and comparing the security log file values with entries in the Check Point LEA server \$FWDIR/log/fw.logtrack file.

EventTracker displays the Logfile Monitor tab with the new configuration settings.

![EventTracker Agent Configuration](image)

6. Click the **Save** button.
Integration of Check Point with EventTracker using Syslog

Prerequisites for Checkpoint Syslog

- EventTracker v8.x should be installed.
- Administrative access to Check Point Smart Console
- Checkpoint version R75 and later
- Windows Version 7 or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Check Point -Mandatory Configuration

To enable syslog reporting on your Check Point Gaia Portal UI:

- Click System Management in the main menu, and click the System Logging tab.
- The Logging page appears.

![Figure 33](image)

- Click on Add tab, and complete the fields using the information in the following table.
Integrate Check Point Firewall

- Click **Apply**.
- Logs will now be forwarded to the IP address of the syslog server that is provided.

### EventTracker Knowledge Pack

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

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

#### Categories

- **Check Point: Alerts**- All events logged by Check Point when any alert is issued by the Security Gateway.
- **Check Point: All firewall events**- All events generated by Check Point firewall.
- **Check Point: FTP activity**- All events generated by Check Point firewall related to FTP traffic passing through security gateway.
- **Check Point: IMAP/POP3 activity**- All events generated by Check Point related to IMAP/POP3 traffic passing through security gateway.
- **Check Point: Login failure**- All logs generated by Check Point related to all login failures that were reported by firewall and/or Connectra.
- **Check Point: Network activity**- All events generated by Check Point related to traffic accepted by firewall.
- **Check Point: Peer to peer activity**- All events logged by Check Point related to Peer to Peer.
- **Check Point: SMTP activity**- All events generated by Check Point firewall related to SMTP mail traffic passing through security gateway.
- **Check Point: Traffic allowed**- All events generated by Check Point when traffic is allowed by firewall.
- **Check Point: Traffic Blocked**- All events generated by Check Point when network traffic is blocked.
- **Check Point: Web activity**- All events generated by Check Point related to the web traffic passing through the security gateway.
- **Check Point: All identity awareness**- All Identity awareness events logged by Check Point.
• **Check Point: Failed login** - All identity awareness events logged by Check Point related to failed login.

• **Check Point: Login activity** - All events logged by Check Point identity awareness related to user login, logout and failed login.

• **Check Point: All IPS events** - All events generated by Check Point related to IPS.

• **Check Point: application control intrusion** - All logs generated by Check Point IPS application control protection.

• **Check Point: Critical intrusion not prevented** - All events generated by Check Point when any critical intrusion detected but not prevented.

• **Check Point: Protocol anomaly intrusion** - All logs generated by Check Point IPS Protocol anomaly protection.

• **Check Point: Administrator login** - All events logged by Check Point when administrator logs in to Check Point smartcenter server.

• **Check Point: All Check Point management events** - All Check Point management events.

• **Check Point: Audit activities** - All Check Point Audit logs.

• **Check Point: Object manipulation** - All events logged by Check Point when any object manipulation is done.

• **Check Point: Policy installation** - All events logged by Check Point when policy installation is performed.

• **Check Point: All VPN activity** - All events logged by Check Point IPSec VPN.

• **Check Point: Successful VPN login** - All events logged by Check Point VPN after successful VPN connection.

• **Check Point: VPN login failure** - All events logged by Check Point when login fails to VPN server.

**Alerts**

• **Check Point: Configuration changes** - This alert is generated when any configuration changes are done.

• **Check Point: Interface status changed** - This alert is generated when the interface status is changed.

• **Check Point: Logon failure** - This alert is generated when an identity awareness event is logged related to login failure.

• **Check Point: Upgrade and downgrade activity** - This alert is generated when any upgrade or downgrade checkpoint hotfixes or patches is done.

• **Check Point: User management activity** - This alert is generated when any user related changes are done for (e.g. user added to group, user deleted)

• **Check Point: Critical attack not prevented** - This alert is generated when any critical intrusion is detected but not prevented.

• **Check Point: IPS alerts** - This alert is generated when any alert is generated related to IPS.

• **Check Point: Successful VPN login** - This alert is generated when successful VPN connection is established.
Reports

- **Check Point-Login and logout activity:** This report provides us the information related to logon and logout activities which includes username, system name, source address and method when logon and logout happens on Check Point firewall.

  ![Figure 34](image)

  **Logs Considered:**

  ![Figure 35](image)

- **Check Point-Logon failure:** This report provides us the information related to logon failure which includes username, system name, source address and reason when logon fails on Check Point firewall.
Logs Considered:

- **Check Point-Allowed traffic:** This report provides us the information related to firewall allowed traffic which includes source address, source port, destination address, destination port and service name, when connection is accepted by Check Point firewall between source and destination.
Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>PNPL 6-KP</th>
<th>PNPL 6-K...</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/10/2017 4:32:27 PM</td>
<td>5555</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: Application
category id: 0

Description:

Logs Considered:

**Check Point- Denied traffic:** This report provides us the information related to firewall denied traffic which includes source address, source port, destination address, destination port and service name, when connection is denied by Check Point firewall between source and destination.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Firewall IP</th>
<th>Interface</th>
<th>Rule Id</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source port</th>
<th>Source port</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/06/2017 05:10:01 PM</td>
<td>192.168.99.1</td>
<td>eth0</td>
<td>34</td>
<td>192.168.99.105</td>
<td>192.168.99.10</td>
<td>tcp</td>
<td>47703</td>
<td></td>
</tr>
<tr>
<td>03/06/2017 05:20:44 PM</td>
<td>192.168.11.7</td>
<td>eth0</td>
<td>13</td>
<td>192.168.11.34</td>
<td>6.255.17.254</td>
<td>tcp</td>
<td>2050</td>
<td></td>
</tr>
<tr>
<td>03/08/2017 05:54:12 PM</td>
<td>192.168.11.7</td>
<td>eth8</td>
<td>13</td>
<td>192.168.99.11</td>
<td>4.23.34.126</td>
<td>tcp</td>
<td>2854</td>
<td></td>
</tr>
<tr>
<td>03/08/2017 01:54:17 PM</td>
<td>192.168.11.7</td>
<td>eth8</td>
<td>34</td>
<td>192.168.99.11</td>
<td>192.149.252.44</td>
<td>tcp</td>
<td>57172</td>
<td></td>
</tr>
<tr>
<td>03/06/2017 05:54:17 PM</td>
<td>192.168.11.7</td>
<td>eth5</td>
<td>34</td>
<td>192.168.99.11</td>
<td>172.16.40.250</td>
<td>udp</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

Logs Considered:
• **Check Point-Configuration changes:** This report provides us the information related to any configuration changes that are done e.g. trapstate on or off, interface changes etc.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client IP Address</th>
<th>Username</th>
<th>Object changed</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>183.162.1.140</td>
<td>Penny</td>
<td>p-hosts</td>
<td>test.checkpoint.com</td>
</tr>
<tr>
<td>03/07/2017 05:58:00 PM</td>
<td>CONTOSO-CP</td>
<td>192.168.1.226</td>
<td>Harris</td>
<td>p-dhcp</td>
<td>dhcpd:dynamic:192.168.192.0 max lease 86400</td>
</tr>
<tr>
<td>03/07/2017 07:45:13 PM</td>
<td>CONTOSO-CP</td>
<td>192.201:20.1</td>
<td>Merlin</td>
<td>1-if/phys</td>
<td>eth0-s2p5c0 speed 100M.</td>
</tr>
<tr>
<td>03/07/2017 08:06:00 PM</td>
<td>CONTOSO-CP</td>
<td>172.168.5.100</td>
<td>Dennis</td>
<td>1+snmp</td>
<td>eth1-s3p1c2 trapstate off.</td>
</tr>
<tr>
<td>03/07/2017 08:38:39 PM</td>
<td>CONTOSO-CP</td>
<td>192.237.1.222</td>
<td>Jacob</td>
<td>1+ip</td>
<td>arp keep time 50</td>
</tr>
<tr>
<td>03/07/2017 10:25:57 PM</td>
<td>CONTOSO-CP</td>
<td>192.237.2.112</td>
<td>Rose</td>
<td>1-resolv</td>
<td>domain:1</td>
</tr>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>192.237.1.222</td>
<td>Jacob</td>
<td>1+interface</td>
<td>eth-s1p1c0 ipaddr:1.1.1.1 mask:24</td>
</tr>
</tbody>
</table>

**Figure 42**

**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>3/10/2017 4:10:57 PM</td>
<td>'555'</td>
<td>PNPL-6-KP / PNPL-6-K_</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event Type: Information</td>
<td>Log Type: Application</td>
<td>Category Id: 0</td>
<td>Description: Mar 6 12:07:15 CONTOSO-CP xpcandy[7452]: Penny 183.162.1.140 p-hosts:test.checkpoint.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<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>3/10/2017 4:10:57 PM</td>
<td>'555'</td>
<td>PNPL-6-KP / PNPL-6-K_</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event Type: Information</td>
<td>Log Type: Application</td>
<td>Category Id: 0</td>
<td>Description: Mar 6 12:07:15 CONTOSO-CP xpcandy[3974]: Rose 192.237.2.112 t-resolv:resolver:3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 43**

• **Check Point-Device maintenance messages:** This report provides us the information related to device maintenance messages such as shutting down for system reboot, boot image information, backup operations etc.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Device messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>Shutting down for system reboot</td>
</tr>
<tr>
<td>03/07/2017 05:58:00 PM</td>
<td>CONTOSO-CP</td>
<td>Configuration changed from 192.168.3.140 by Mike</td>
</tr>
<tr>
<td>03/07/2017 06:24:19 PM</td>
<td>CONTOSO-CP</td>
<td>Processing: set time 12:00:00</td>
</tr>
<tr>
<td>03/07/2017 07:45:13 PM</td>
<td>CONTOSO-CP</td>
<td>Boot image will be myinitrd.img</td>
</tr>
<tr>
<td>03/07/2017 08:00:00 PM</td>
<td>CONTOSO-CP</td>
<td>Reboot with image kubectli.ing</td>
</tr>
<tr>
<td>03/07/2017 08:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>Server listening on 172.163.21.10 port 22.</td>
</tr>
<tr>
<td>03/07/2017 10:29:57 PM</td>
<td>CONTOSO-CP</td>
<td>BACKUP operation started.</td>
</tr>
</tbody>
</table>

**Figure 44**
Logs Considered:

![Table of DHCP server activity logs]

- **Check Point-DHCP server activity**: This report provides us the information related to DHCP server activity.

![Table listing DHCP requests and responses]

*Figure 45*

*Figure 46*
### Logs Considered:

**Check Point-Interface status changed**: This report provides us the information related to the interface status whether it is Up or Down.

![Table of interface status](image)

---

---

---
• **Check Point-Upgrade and downgrade activity:** This report provides us the information related to the upgrade or downgrade activity that is done. For e.g. checkpoint hotfixes or patches are upgraded to remove.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Patch details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>installer:available_install_packages_number 1</td>
</tr>
<tr>
<td>03/07/2017 05:56:00 PM</td>
<td>CONTOSO-CP</td>
<td>installer:packages:Check_Point_Hotfix_R77.20_sk104443.tgz:tag:importance</td>
</tr>
<tr>
<td>03/07/2017 07:45:13 PM</td>
<td>CONTOSO-CP</td>
<td>installer:packages:Check_Point_SmartConsole_R77.20_T124_Auto_Update.tgz 3</td>
</tr>
<tr>
<td>03/07/2017 08:00:00 PM</td>
<td>CONTOSO-CP</td>
<td>upgrade:package: 6.7.11 t</td>
</tr>
<tr>
<td>03/07/2017 08:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>Gaia DB Upgrade successful</td>
</tr>
<tr>
<td>03/07/2017 10:29:57 PM</td>
<td>CONTOSO-CP</td>
<td>upgrade:package: 6.7.11 t</td>
</tr>
<tr>
<td>03/07/2017 10:51:05 PM</td>
<td>CONTOSO-CP</td>
<td>installer:available_install_packages_number 1</td>
</tr>
</tbody>
</table>

Figure 50

**Logs Considered:**

![Logs Considered](image)

Figure 51

• **Check Point-User management activity:** This report provides us the information related to user management activity, which is any user-related changes done e.g. user added to group, user deleted.
4.0 Integrate Check Point Firewall

Figure 52

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Activity</th>
<th>Changed object type</th>
<th>Activity By</th>
<th>Changed object</th>
<th>Activity for</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>Delete group</td>
<td>Brad</td>
<td>UFC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03/07/2017 05:56:00 PM</td>
<td>CONTOSO-CP</td>
<td>Add user</td>
<td>homodir</td>
<td>Admin</td>
<td>Local\Conicco</td>
<td>Jerry</td>
</tr>
<tr>
<td>03/07/2017 07:37:22 PM</td>
<td>CONTOSO-CP</td>
<td>User entry</td>
<td></td>
<td>password database</td>
<td>Scarlett</td>
<td></td>
</tr>
<tr>
<td>03/07/2017 07:45:15 PM</td>
<td>CONTOSO-CP</td>
<td>Delete group</td>
<td>member</td>
<td>Jim</td>
<td>Barracuda news</td>
<td>Amy</td>
</tr>
<tr>
<td>03/07/2017 08:00:00 PM</td>
<td>CONTOSO-CP</td>
<td>Add user</td>
<td>homodir</td>
<td>Admin</td>
<td>Admin\Security</td>
<td>Mick</td>
</tr>
<tr>
<td>03/07/2017 08:30:30 PM</td>
<td>CONTOSO-CP</td>
<td>Add group</td>
<td>member</td>
<td>Robert</td>
<td>EcoSpace</td>
<td>Megan</td>
</tr>
<tr>
<td>03/07/2017 19:29:57 PM</td>
<td>CONTOSO-CP</td>
<td>Add group</td>
<td>Casey</td>
<td>Global Summit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logs Considered:

Figure 53

**Import knowledge pack into EventTracker**

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility. Click Import tab.
   - Import Alerts/Category/Tokens/ Flex Reports as given below.
To import Alerts

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

4. Click OK, and then click the Close button.
To import Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab, and then click on ‘Import’ option.
3. Click on Browse button.

![Figure 57]

4. Locate Check Point group of Token templates.ettd file, and then click the Open button

![Figure 58]

5. Now select the check box and then click on ‘Import’ option.
   EventTracker displays success message.

![Figure 59]

6. Click on OK button.
To import Flex Reports

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

   ![Figure 60](image)

2. Locate the **Check Point group of Reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.

   ![Figure 61](image)

4. Click the **OK** button. Click the **Close** button.
Verify knowledge pack in EventTracker

Verify Alerts

1. Logon to EventTracker Enterprise.

2. Click Admin dropdown, and then click Alert

3. In Search field, type ‘Check Point’, and then click the Go button.

Alert Management page will display all the imported Check Point alerts.

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

EventTracker displays message box.

Figure 62

Figure 63
5. Click OK, 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.

**Verify Token Templates**

1. Logon to **EventTracker Enterprise** web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.

![Figure 64](image)

**Verify Flex Reports**

1. Logon to **EventTracker Enterprise**.
2. Click the Reports.
3. Select the Configuration.
   In the Reports Configuration, select Defined from radio button. EventTracker displays Defined page.
4. Select Check Point folder from Reports Groups.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. During scheduling, please check **Persist data in EventVault Explorer** option.
4. Check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
5. Proceed to next step and click Schedule button.
6. Wait for scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to Dashboard>Flex.
   Flex Dashboard pane is shown.

4. Click to add a new dashboard.
   Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.
6. Click to configure a new flex dashlet. Widget configuration pane is shown.
7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.
16. If satisfied, click **Configure** button.
Integrate Check Point Firewall

Figure 73
Sample Flex Dashboards

- **WIDGET TITLE**: Check Point-Configuration changes
- **DATA SOURCE**: Check Point-Configuration changes
- **CHART TYPE**: Donut
- **AXIS LABELS [X-AXIS]**: Client IP address

![Check Point-Configuration changes chart](image)

*Figure 74*
- **Widget Title**: Check Point-Logon failure
- **Data Source**: Check Point-Logon failure
- **Chart Type**: Donut
- **Axis Labels [X-Axis]**: Activity

*Figure 75*
• **WIDGET TITLE:** Check Point-Interface status changed  
**DATA SOURCE:** Check Point-Interface status changed  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Interface Id  
**LEGEND [SERIES]:** Interface state

![Check Point-Interface status changed chart](image)

Figure 76
• **WIDGET TITLE**: Check Point-Device maintenance messages

**DATA SOURCE**: Check Point-Device maintenance messages

**CHART TYPE**: Donut

**AXIS LABELS [X-AXIS]**: Device messages.

![Check Point-Device Maintenance Messages Chart](image)

*Figure 77*
• WIDGET TITLE: Check Point-DHCP server activity
DATA SOURCE: Check Point-DHCP server activity
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Dhcp messages.

Figure 78
- **WIDGET TITLE**: Check Point-Upgrade and downgrade activity
- **DATA SOURCE**: Check Point-Upgrade and downgrade activity
- **CHART TYPE**: Donut
- **AXIS LABELS [X-AXIS]**: Patch details
• **WIDGET TITLE:** Check Point-User management activity  
**DATA SOURCE:** Check Point-User management activity  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Patch details

![Check Point-User Management Activity Chart](image-url)  
*Figure 80*
• **WIDGET TITLE:** Check Point-Traffic allowed  
  **DATA SOURCE:** Check Point-Denied Traffic  
  **CHART TYPE:** Donut  
  **AXIS LABELS [X-AXIS]:** Source IP address

![Check Point-Firewall Allowed Traffic](image)

*Figure 81*
- **WIDGET TITLE:** Check Point-Denied Traffic  
**DATA SOURCE:** Check Point-Denied Traffic  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Source IP address  

![Check Point-Firewall Denied Traffic Chart](image)

*Figure 82*