Check Point Guide
Configure ETAgent to read CheckPoint Logs
Abstract

The purpose of this document is to help users configure EventTracker™ Agent to read Check Point Log files.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise v7x and later, Check Point R75.40 and later.
# Table of Contents

Abstract ........................................................................................................................................................ 1  
Scope ........................................................................................................................................................ 1  
Check Point – Mandatory Configurations ................................................................................................. 3  
  Set the Rule.............................................................................................................................................. 3  
  Register OPSEC Application – get Client DN ....................................................................................... 12  
  Get Server DN ........................................................................................................................................ 18  
    To get Server DN on Checkpoint R75 ............................................................................................... 19  
  Configure Check Point to track Log ..................................................................................................... 20  
  Install Policy........................................................................................................................................... 21  
Configure Event Tracker – the Check Point Certificate .......................................................................... 23  
  Configure EventTracker Agent ............................................................................................................. 25  
  Authenticated SSL CA connections ..................................................................................................... 31  
    Checkpoint device configuration ...................................................................................................... 31  
Appendix A: Alternative OPSEC SIC Connection Methods ..................................................................... 33
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 Event Tracker host to pull the certificate from the Check Point SmartCenter server, TCP port 18210, and that allows the LEA (Log Event API) connection from Event Tracker 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. Event Tracker 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 SmartDashboard.
You need to add a rule in ‘Security’. For Checkpoint server R70 and later same steps have to 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.

![SmartDashboard displays the newly added Rule.](image)
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)

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.

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.
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.

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_url)

17. Right-click the **TRACK** column.
   Check Point displays the shortcut menu.
18. From the shortcut menu, choose **Account**.

![Figure 10](image_url)

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.
ET Agent and Check Point installed on the same system

Figure 12
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.

![OPSEC Application Properties window](image)

**Figure 17**

You need this name to get the certificate as an object name.

This string is called Client DN and you need this to configure EventTracker Agent.

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.
How to – Configure Check Point Logs for EventTracker

Get Server DN

1. Expand the **Check Point** node on the tree pane.
   
   Event Tracker 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.

   ![Figure 19](image)

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 Checkpoint R75

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.

   
   [cpmodule]# cpca_client lscert -kind SIC
   Operation succeeded. rc=0.
   7 certs found.

   Subject = CN=ETAgent,O=cpmodule..4acdd4
   Status = Revoked Kind = SIC Serial = 4726 DP = 0

   Subject = CN=cpmodule,O=cpmodule..4acdd4
   Status = Valid Kind = SIC Serial = 52105 DP = 0
   Not_Before: Tue Mar 19 02:44:36 2013 Not_After: Mon Mar 19 02:44:36 2018

   Subject = CN=ETAgent,O=cpmodule..4acdd4
   Status = Revoked Kind = SIC Serial = 54347 DP = 0
   Not_Before: Tue Mar 19 06:58:58 2013 Not_After: Mon Mar 19 06:58:58 2018

   Subject = CN=ETAgent,O=cpmodule..4acdd4
   Status = Revoked Kind = SIC Serial = 78016 DP = 0
   Not_Before: Tue Mar 19 06:27:42 2013 Not_After: Mon Mar 19 06:27:42 2018

   Subject = CN=ETAgent,O=cpmodule..4acdd4
   Status = Valid Kind = SIC Serial = 81684 DP = 0
   Not_Before: Tue Mar 19 08:10:34 2013 Not_After: Mon Mar 19 08:10:34 2018

   Subject = CN=ETAgent,O=cpmodule..4acdd4
   Status = Revoked Kind = SIC Serial = 85711 DP = 0
   Not_Before: Tue Mar 19 03:41:42 2013 Not_After: Mon Mar 19 03:41:42 2018

   Subject = CN=cp_mgmt,O=cpmodule..4acdd4
   Status = Valid Kind = SIC Serial = 86923 DP = 0
   Not_Before: Tue Mar 19 02:44:30 2013 Not_After: Mon Mar 19 02:44:30 2018

   [cpmodule]#

   Figure 20

   Management server certificate will be the one with CN=cp_mgmt.

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.
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.

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

   Check Point displays the SmartDashboard Warning message.

   ![Figure 22]

2. Click the OK button.

   Check Point displays the Install Policy window.

   ![Figure 23]

3. Click the OK button.
Check Point displays a successful message.

![Installation Process - Standard](image)

Figure 24

4. Click the **Close** button.
Configure Event Tracker – 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).
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 Event Tracker 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 Event Tracker reset and then initialize to create a new certificate. Refer step 8 to Register the OPSEC Application Object section.

c) On the Event Tracker 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.

   ![EventTracker Agent Configuration](image)

   **Figure 26**

3. Select the **Add File Name** button.

   EventTracker displays the ‘Enter File Name’ window.
How to – Configure Check Point Logs for EventTracker

4. Select **CHECKPOINT** from the **Select Log File Type** drop-down list.
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 Compressed: No</td>
</tr>
<tr>
<td>OPSEC_SSLCA_COMP</td>
<td>Encryption Method: 3DES 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. Event Tracker 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.
How to – Configure Check Point Logs for EventTracker

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>This option is selected by default. Select this option to receive live Check Point logs when the configuration takes effect.</td>
</tr>
</tbody>
</table>
| Historical | 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. |

5. Click the **OK** button.

![Figure 31](image-url)
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:

HKLM\SOFTWARE\Prism Microsystems\EventTracker\Agent\CheckPoint

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)

Figure 32

6. Click the **Save** button.
NOTE: If the EventTracker Agent is unable to receive events from Checkpoint server then, please check the authenticated SSL CA is available or not. If not, please enable by following the below steps:

Authenticated SSL CA connections

Checkpoint device configuration

1. Modify $FWDIR/conf/fwopsec.conf, where Checkpoint Server is installed.
2. Go to $FWDIR/conf location. See the below screen

![Figure 33](image)

3. Enter `vi fwopsec.conf` to make the changes and then click Enter.
4. Define the port to be used for authenticated LEA connections (e.g. 18184):

**NOTE**: If the below mentioned entries are commented, please make sure that they are uncommented in the `fwopsec.conf` file.

```
lea_server port 0
lea_server auth_port 18184
lea_server auth_type sslca
```
How to – Configure Check Point Logs for EventTracker

Figure 35

NOTE: If the entry (lea_server auth_type sslca) is not there, please add it and then Save the configuration.

5. Restart in order to activate changes:
   cpstop; cpstart

Appendix A: Alternative OPSEC SIC Connection Methods

It may be necessary to use a connection between EventTracker and the Check Point device that is not one of the defaults. If this is needed to help debug a problem or to use as a work-a-round please use the instructions below.

Configure the Check Point Device

Edit the file $FWDIR/conf/fwopsec.conf. Find the following lines;

    # lea_server auth_port 18184
# lea_server port 0

Change the lines to look like this;

lea_server auth_port 0

lea_server port 18184

Restart the LEA server on the Check Point device for the change to take effect by executing the following command;

# fw kill fwd

The Check Point watchdog process will restart it. This can be monitored with the command;

# cpwd_admin list

**Configure Event Tracker**

- In the Event Tracker Agent Configuration set the Communication Method to OPSEC_NONE and save the Configuration to restart the Agent. To see if the connection is successful monitor the file \Program Files\Prism Microsystems\Event Tracker\Agent\etalog.txt file.