Integrate Sophos Enterprise Console

EventTracker v8.x and above
Abstract

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

Audience

Sophos Enterprise console users, who wish to forward events to EventTracker Manager.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise, and Sophos Enterprise console 5.2 and later.

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

Audience .................................................................................................................................................................. 1

Scope ........................................................................................................................................................................ 1

Overview ...................................................................................................................................................................... 3

Pre-requisite................................................................................................................................................................. 3

Configure Sophos Enterprise Console ........................................................................................................................ 3

EventTracker Knowledge Pack (KP) .......................................................................................................................... 10
    Reports ................................................................................................................................................................... 10
    Alerts ...................................................................................................................................................................... 13

Import Sophos Enterprise Console Knowledge Pack into EventTracker ............................................................... 13
    To import Alerts ..................................................................................................................................................... 15
    To import Reports ................................................................................................................................................. 15
    To Import Knowledge Objects .............................................................................................................................. 16

Verify Sophos Enterprise Console Knowledge Pack in EventTracker ................................................................. 18
    Verify alerts ............................................................................................................................................................ 18
    Verify Reports ........................................................................................................................................................ 19
    Verify Knowledge Object ...................................................................................................................................... 20

Create Dashboards in EventTracker ......................................................................................................................... 21
    Schedule Reports ............................................................................................................................................... 21
    Create Dashlets .................................................................................................................................................... 24

Sample Dashboards ................................................................................................................................................... 27
Overview

Sophos Antivirus makes it simple to secure your Windows, Mac and Linux systems against malware and advanced threats, such as targeted attacks.

EventTracker collects and analyze events and enlightens an administrator about security violations, user behavior, and traffic anomalies.

Pre-requisite

- EventTracker Enterprise should be installed.
- Sophos Enterprise console 5.2 and later should be installed.

Configure Sophos Enterprise Console

Before configuring Sophos enterprise console, deploy the EventTracker agent on Sophos EC machine, please refer EventTracker Agent installation guide. After installation of the agent, follow below mentioned steps to configure Sophos enterprise console.

1. Contact EventTracker Support to download KP for Sophos Enterprise Console.

3. Then extract SophosIntegrator.zip

![Figure 1](image1.png)

![Figure 2](image2.png)
4. We need to schedule the above **SophosIntegrator.exe** utility in the task scheduler.
5. Click **Create Task** icon.
6. Enter the name and then click on the radio button (**Run whether user is logged on or not**)

![Sophos to EventTracker Reporting service Properties (Local Computer)](image)

**Figure 3**

7. Click on the **Triggers** Tab.
8. Click **New** button.
9. Create a **New Trigger** and schedule as shown above image and click **OK**.
10. Click the **Actions Tab**
11. Select the button **New**.
12. Browse the location at which the **SophosIntegrator.exe** file is located and click **OK**.
13. Click **OK** in the **Action** page.
14. Set the **user name** and **password** to run the selected task and **click OK**.
EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker Enterprise to support Sophos Enterprise Console monitoring:

Reports

- **Sophos EC - Application Control** - This report provides information related to application control module of Sophos enterprise console. It will give us the information about clients who are trying to access the application which is allowed or blocked through application policy.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>Client System</th>
<th>Application</th>
<th>Application Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>ContosoJohn</td>
<td>con-wks-01</td>
<td>Google Chrome</td>
<td>Internet browser</td>
<td>Blocked</td>
</tr>
</tbody>
</table>

- **Sophos EC - Audit events** - This report provides information related to configuration change in Sophos enterprise console like policy created, deleted and modified, computer added, group added, etc. It will provide us the information about the user who trying to change the configuration of Sophos enterprise console.

<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>09/20/2017 12:44:36 PM</td>
<td>3230</td>
<td>CONTOSO / SEC-SRV</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>EventTracker</td>
</tr>
</tbody>
</table>
Log Search:

- **Sophos EC – Tamper protection** - This report provides information related to devices on which user is trying to make agent configuration changes like Sophos Endpoint protection uninstallation or policy changes.

<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>9/18/2017 3:51:13 PM</td>
<td>3230</td>
<td>CONTOSO / SEC-SRV</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>EventTracker</td>
</tr>
</tbody>
</table>

**Sophos EC-Tamper protection**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client System</th>
<th>User Name</th>
<th>Event Type</th>
<th>Event Sub Type</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/18/2017 03:53:06 PM</td>
<td>SEC-SRV</td>
<td>con-wks-01</td>
<td>CONTOSO\John</td>
<td>Tamper protection</td>
<td>Successful authentication</td>
<td></td>
</tr>
<tr>
<td>09/18/2017 03:53:06 PM</td>
<td>SEC-SRV</td>
<td>con-wks-02</td>
<td>CONTOSO\Mike</td>
<td>Tamper protection</td>
<td>Successful authentication</td>
<td></td>
</tr>
</tbody>
</table>

Log Search:

- **Sophos EC – Threat detected** - This report provides information related to threats detected on systems. It will provide us information about systems on which threat is detected and give us the details of threat like threat name, threat type, etc.

<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>9/18/2017 3:51:13 PM</td>
<td>3230</td>
<td>CONTOSO / SEC-SRV</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>EventTracker</td>
</tr>
</tbody>
</table>

**Sophos EC-Threat detected**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client System</th>
<th>Threat type</th>
<th>Threat file path</th>
<th>File version</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/16/2017 3:23:13 PM</td>
<td>SEC-SRV</td>
<td>con-wks-01</td>
<td>Vircure spyware</td>
<td>C:\Windows\System32\winscript.exe</td>
<td>277413403</td>
</tr>
</tbody>
</table>
Log Search:

**Sophos EC – Firewall events** - This report provides information related to firewall activities happened on client systems. It will give us information about the allowed and blocked network activities on client system.

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-01</td>
<td>svchost.exe</td>
<td>10.0.15063.0 (WinBuild 160101.0800)</td>
<td>Outbound</td>
<td>TCP</td>
<td>55160</td>
<td>55160</td>
<td>122.188.1.22</td>
</tr>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-02</td>
<td>svchost.exe</td>
<td>10.0.15063.0 (WinBuild 160101.0800)</td>
<td>Outbound</td>
<td>UDP</td>
<td>58803</td>
<td>58803</td>
<td>239.255.255.250</td>
</tr>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-03</td>
<td>svchost.exe</td>
<td>10.0.15063.0 (WinBuild 160101.0800)</td>
<td>Outbound</td>
<td>UDP</td>
<td>54427</td>
<td>54427</td>
<td>239.255.255.250</td>
</tr>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-01</td>
<td>svchost.exe</td>
<td>10.0.15063.0 (WinBuild 160101.0800)</td>
<td>Outbound</td>
<td>TCP</td>
<td>55199</td>
<td>55199</td>
<td>192.168.1.11</td>
</tr>
<tr>
<td>09/15/2017 03:23:12 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-01</td>
<td>svchost.exe</td>
<td>10.0.15063.0 (WinBuild 160101.0800)</td>
<td>Outbound</td>
<td>TCP</td>
<td>54855</td>
<td>54855</td>
<td>111.221.20.253</td>
</tr>
</tbody>
</table>

---

Log Search:
Integrate Sophos Enterprise Console

- **Sophos EC - Device control** - This report provides information related to device control module of Sophos Enterprise console. This report will show the devices information which is being blocked or allowed by device control policy.

- **Sophos EC – Data control** - This report provides information related to DLP module of Sophos enterprise console. This will give us the information about sensitive data which the user is trying to send to other unauthorized user using USB transfer, file transfer, email transfer, etc.

- **Sophos EC – Web control** - This report provides information related to web control module of Sophos enterprise console. It will give us the information of users who are trying to access website, which is allowed or blocked by web filter and web control.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>ClientComputer</th>
<th>User Name</th>
<th>URL</th>
<th>Action</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/14/2017 04:40:30 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-01</td>
<td>TOONSjenny</td>
<td>sophostest.com/alcoholindex.html</td>
<td>Blocked</td>
<td>Category</td>
</tr>
<tr>
<td>09/14/2017 04:40:30 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-02</td>
<td>TOONSjon</td>
<td>sophostest.com/anonymizers/index.html</td>
<td>Blocked</td>
<td>Category</td>
</tr>
<tr>
<td>09/14/2017 04:40:30 PM</td>
<td>SEC-SRV</td>
<td>Con-wks-03</td>
<td>TOONSmike</td>
<td>sophostest.com/calhome/index.html</td>
<td>Warned</td>
<td>Category</td>
</tr>
<tr>
<td>09/14/2017 04:40:30 PM</td>
<td>SEC-SRV</td>
<td>Con-wks04</td>
<td>TOONShnn</td>
<td>sophostest.com/violence/index.html</td>
<td>Warned</td>
<td>Risk</td>
</tr>
</tbody>
</table>

**Log Search:**

**Alerts**

- **Sophos EC: Threat detected** - This alert is generated when threat is detected on client system.
- **Sophos EC: Configuration changes** - This alert is generated when configuration changes happen in policy, group, computer, etc. on Sophos Enterprise Console.

**Import Sophos Enterprise Console Knowledge Pack into EventTracker**

1. Launch EventTracker Control Panel.
2. Double click **Import Export Utility** icon, and then click the **Import** tab.
Import **Category/ Alert/ Flex Reports** as given below.

**To import Alerts**

1. Click **Alert** option, and then click the browse button.
2. Locate the **All Sophos EC group of alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
   
   EventTracker displays success message.

   ![Success Message](image12.png)

   Figure 12

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

**To import Reports**

1. Click **Report** option, and then click the browse button.
2. Locate **All Sophos EC defined analysis report.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports.
   
   EventTracker displays success message.

   ![Success Message](image13.png)

   Figure 13

4. Click the **OK** button, and then click the **Close** button.
To Import Knowledge Objects

1. Logon to EventTracker Enterprise.
2. Click the admin dropdown, and then click Knowledge Objects.

3. Click on Import button and browse for All KO group of Sophos Enterprise console.etko file.
4. Upload .etko file and Select all objects. Click on **OVERWRITE** button.

EventTracker Displays message box.
Verify Sophos Enterprise Console Knowledge Pack in EventTracker

Verify alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, enter ‘Sophos’, and then click the Go button.

Alert Management page will display all the imported Sophos EC alerts.

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

EventTracker displays message box.
5. 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.

**Verify Reports**

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Sophos Enterprise Console group folder.

   Scheduled Reports are displayed in the Reports configuration pane.
Verify Knowledge Object

1. Logon to EventTracker Enterprise.
2. Click the admin dropdown, and then click Knowledge Objects.
3. Select Sophos Enterprise Console group and check all the Knowledge object.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.
2. Navigate to Reports>Configuration.

3. Select Sophos Enterprise Console in report groups. Check defined dialog box.

4. Click on ‘schedule’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check Persist data in Eventvault explorer box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

### Create Dashlets

1. **EventTracker 8.x and later** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

![Figure 26](image)

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

![Figure 27](image)

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. Evaluated chart is shown.

![Figure 30](image-url)

16. If satisfied, click **Configure** button.
17. Click ‘customize’ to locate and choose created dashlet.
18. Click to add dashlet to earlier created dashboard.

Sample Dashboards

1. Sophos Antivirus- Data transfer allowed and blocked

![Sample Dashboard Image](image-url)
2. Sophos Antivirus - Virus removed

![Sophos Antivirus - Virus removed](image)

Figure 33