Integrate Sophos UTM

*EventTracker v7.x*
Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, and Sophos UTM 9 and later.

Audience

Sophos UTM users, who wish to forward Syslog events to EventTracker Manager.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2014 Prism Microsystems Corporation. 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
Prerequisites .......................................................................................................................................... 3
Integrate EventTracker with Sophos UTM ............................................................................................ 3
EventTracker Knowledge Pack (KP) ....................................................................................................... 5
Import Sophos UTM Knowledge Pack into EventTracker ..................................................................... 6
  Import Category .................................................................................................................................. 6
  Import Alerts .................................................................................................................................... 7
  Import Tokens ................................................................................................................................... 8
  Import Flex Reports ........................................................................................................................... 9
Verify Sophos UTM knowledge pack in EventTracker ......................................................................... 10
  Verify Sophos UTM Categories ......................................................................................................... 10
  Verify Sophos UTM Alerts .................................................................................................................. 11
  Verify Sophos UTM Tokens ................................................................................................................ 12
  Verify Sophos UTM Flex Reports ....................................................................................................... 13
Sample Reports ................................................................................................................................... 14
Prerequisites

- EventTracker should be installed
- Sophos UTM 9 and later should be installed and configured

Integrate EventTracker with Sophos UTM

To configure logging for Sophos UTM proceed as follows:

- Logon to the WebAdmin of the UTM
- Navigate to **Logging & Reporting > Log Settings > Remote Syslog Server**
- Activate the Remote Syslog status
- Configure a Syslog server
  - **Name**: freely selectable
  - **Server**: IP or hostname of your Syslog server EventTracker Enterprise
  - **Port**: UDP 514
- Click on Apply

![Figure 01](image)

If syslog messages cannot be delivered, they will be buffered, and re-send when possible. By default, up to 1000 logs will be buffered.
Once Syslog targets have been configured the logs to send via syslog must also be selected on the same screen. By default, none are selected. Select the desired logs, and click 'Apply'.

To determine which logs are desired, you can view complete log contents and watch logs in real-time, under 'Logging & Reporting' > 'View Log Files'.
EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker v7.x to support Sophos UTM monitoring:

Alerts:-

- **Sophos UTM: User authentication failure** - This alert is generated when user authentication failure occurs.
- **Sophos UTM: Shell password changed** - This alert is generated when shell password has been changed.
- **Sophos UTM: Object changed** - This alert is generated when object changed.
- **Sophos UTM: Object deleted** - This alert is generated when object deleted.
- **Sophos UTM: Node changed** - This alert is generated when node changed.

Reports:-

- **Sophos UTM: User Authentication Success** - This flex report provides information related to user authentication success.
- **Sophos UTM: Shell Password Changed** - This flex report provides information related to shell password changed by someone.
- **Sophos UTM: Packet Dropped** - This flex report provides information related to packet data dropped. It gives the information on which interface packet dropped.
- **Sophos UTM: Packet Accepted** - This flex report provides information related to packet data accepted. It gives the information on which interface packet accepted.
- **Sophos UTM: Object Created** - This flex report provides information related to object created. It gives the object name which has been created and who has created.
- **Sophos UTM: Object Changed** - This flex report provides information related to object changed. It gives information which object has been changed by who.
- **Sophos UTM: Object Deleted** - This flex report provides information related to object deleted. It gives information which object has been deleted by who.
- **Sophos UTM: Node Changed** - This flex report provides information related to node changed. It gives information what node has been changed by who.

**Import Sophos UTM Knowledge Pack into EventTracker**

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**, and then click the **Import** tab.

   Import **Category, Alert, Tokens** and **Flex Reports** as given below.

**Import Category**

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

![Figure 03](image.png)
2. Locate All Sophos UTM group of Categories.iscat file, and then click the **Open** button.

3. To import the categories, click the **Import** button. EventTracker displays success message.

![Figure 04](image)

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

**Import Alerts**

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

![Figure 05](image)
2. Locate **All Sophos UTM group of Alerts.isalt** file, and then click the **Open** button.

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

   EventTracker displays success message.

   ![Figure 06](image)

   **Figure 06**

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

**Import Tokens**

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

   ![Figure 07](image)

   **Figure 07**
2. Locate **All Sophos group of Tokens.istoken** file, and then click the **Open** button.

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

   EventTracker displays success message.

   ![Image](image08.png)

   **Figure 08**

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

**Import Flex Reports**

1. Click **Scheduled Report** option, and then click the **browse** button.
2. Locate All Sophos UTM group of Flex Report.issch file, and then click the Open button.

3. To import scheduled reports, click the Import button.

   EventTracker displays success message.

   ![Export Import Utility]

   Figure 10

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

Verify Sophos UTM knowledge pack in EventTracker

Verify Sophos UTM Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In the Category Tree, expand Sophos UTM group folder to view the imported categories.
Verify Sophos UTM Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search field, type ‘Sophos UTM’, and then click the Go button.
   Alert Management page will display all the imported Sophos UTM alerts.
4. To activate the imported alerts, select the respective checkbox in the Active column.
EventTracker displays message box.

![Image of Successfully saved configuration message box]

Figure 13

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 Sophos UTM Tokens

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** menu, and then click **Parsing rules**.

   The imported Sophos UTM tokens are added in Token-Value Groups list. Please refer Figure 14.
Verify Sophos UTM Flex Reports

1. Logon to EventTracker Enterprise.
2. Select the Reports menu, and then select Configuration.
3. In Reports Configuration, select Defined option.
   EventTracker displays Defined page.
4. In search box enter ‘Sophos UTM’.
   EventTracker displays Flex reports of Sophos UTM.

Figure 15
Sample Reports

Some sample reports are given below.

### Sophos UTM User Authentication Failure

<table>
<thead>
<tr>
<th>LogTime</th>
<th>UserName</th>
<th>Source IP</th>
<th>Logon Type</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/30/2015 11:16:18 AM</td>
<td>chef</td>
<td>192.168.1.95</td>
<td>webadmin</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/30/2015 11:16:22 AM</td>
<td>chef</td>
<td>192.168.1.95</td>
<td>webadmin</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:20:52 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:20:59 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:21:03 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:26:47 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:28:59 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:27:04 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:29:56 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:51:34 AM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 11:54:50 AM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 12:03:44 PM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 12:04:00 PM</td>
<td>loginuser</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:11:50 PM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:11:52 PM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:14:05 PM</td>
<td>admin</td>
<td>192.168.1.95</td>
<td>webadmin</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:14:05 PM</td>
<td>admin</td>
<td>192.168.1.95</td>
<td>webadmin</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:17:17 PM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
<tr>
<td>03/31/2015 04:17:19 PM</td>
<td>root</td>
<td>192.168.1.94</td>
<td>sshd</td>
<td>192.168.1.38-SYSLOG</td>
</tr>
</tbody>
</table>

Figure 16

### Sophos UTM Shell Terminal Password Changed

<table>
<thead>
<tr>
<th>LogTime</th>
<th>UserName(Changed By)</th>
<th>Source IP</th>
<th>UserName(Changed for)</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/17/2015 03:22:37 PM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>root</td>
</tr>
<tr>
<td>03/17/2015 03:45:37 PM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>root</td>
</tr>
<tr>
<td>03/23/2015 05:37:39 PM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>root</td>
</tr>
<tr>
<td>03/23/2015 05:50:28 PM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>root</td>
</tr>
<tr>
<td>03/23/2015 05:50:28 PM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>loginuser</td>
</tr>
<tr>
<td>03/21/2015 11:23:29 AM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>root</td>
</tr>
<tr>
<td>03/31/2015 11:28:29 AM</td>
<td>admin</td>
<td>192.168.1.94</td>
<td>loginuser</td>
</tr>
</tbody>
</table>

Figure 17