

**Integration Guide** 

## Integrate Sophos Web Appliance with EventTracker

**Publication Date:** 

July 6, 2021

© Copyright Netsurion. All Rights Reserved.

### Abstract

This guide helps you in configuring **Sophos Web Appliance** with EventTracker to receive **Sophos Web Appliance** web traffic events via syslog integration. In this guide, you will find the detailed procedures required for monitoring **Sophos Web Appliance**.

### Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and **Sophos Web Appliance.** 

### Audience

Administrators, who are assigned the task to monitor and manage **Sophos Web Appliance** events using **EventTracker.** 

## Table of Contents

Та	ble o	f Contents	3
1.	٥v	verview	4
2.	Pr	erequisites	4
3.	Со	nfiguring Sophos Web Appliance to forward logs to EventTracker	4
4.	Εv	entTracker Knowledge Pack	6
	4.1	Category	6
	4.2	Alert	6
	4.3	Report	7
	4.4	Dashboards	7
5.	Im	porting Sophos Web Appliance Knowledge Pack into EventTracker	10
	5.1	Category	10
	5.2	Alert	11
	5.3	Knowledge Object	12
	5.4	Report	14
	5.5	Dashboards	15
6.	Ve	rifying Sophos Web Appliance Knowledge Pack in EventTracker	18
	6.1	Category	18
	6.2	Alert	18
	6.3	Knowledge Object	20
	6.4	Report	20
	6.5	Dashboards	21
	Abou	ut Netsurion	22
	Cont	act Us	22

### 1. Overview

Sophos is a Web Security Application (web appliance), built to secure web gateway that makes web protection simple. It provides advanced protection from today's sophisticated web malware and gives user full control over their employees' online activity. User can easily create policies for individuals or groups while gaining important insights into user activity on their network.

EventTracker helps to monitor events from Sophos web appliance. Its dashboard, alerts and reports will help you track allowed and blocked traffic activities. It will trigger alert such as, 'Warned URL accessed by User or any 'URL with malicious category accessed'.

This guide helps you in configuring **Sophos Web Appliance** with EventTracker to receive **Sophos Web Appliance** events. In this guide, you will find the detailed procedures required for monitoring **Sophos Web Appliance**.

## 2. Prerequisites

Prior to configuring Sophos Web Appliance and the EventTracker, ensure that you meet the following prerequisites:

- EventTracker v9.3 or above should be installed.
- Admin role on Sophos Web Appliance to make configuration changes.
- Administrative access on the EventTracker.
- EventTracker IP and port need to add in firewall allowed list.

## 3. Configuring Sophos Web Appliance to forward logs to EventTracker

The steps provided below will help to configure the EventTracker to receive Sophos Web Appliance events via Syslog.

- 1. On the Configuration > System > Alerts & Monitoring page, select the Syslog tab.
- 2. Select the Enable syslog transfer of web traffic check box.
- In the Hostname/IP text box, enter the address of the EventTracker Manager IP/EventTracker Agent Syslog relay to which the appliance will send logs.
   Note: If the Syslog server becomes unavailable to the appliance, it is possible that some log information may be dropped before the server becomes available again. The amount of information dropped depends on the duration that the server is unavailable.
- 4. In the **Port** text box, enter the port number that EventTracker Agent Syslog relay uses. Eg.,514(UDP port)
- 5. Select a **Protocol** option button to select whether the appliance will send Syslog data using UDP and TCP (encrypted/unencrypted).(Note: If on-premises solution, select UDP protocol)
- 6. Click **Apply**.

•	U	DΡ
•		υг

Sophos Wel	o Appliance
🔿 Dashboard	🔅 Configuration 🚫 Reports 🔎 Search 🕜 Help 🥑 System Status
Configuration Accounts Group Policy Global Policy System Updates Active Directory Correction Profes Time Zone Control Management Certificates Endpoint Web Control Network	System: Alerts & Monitoring  The applance regularly monitors its health, can send alerts based on significant changes in system status or when users search for monitored search terms, and transfer web traffic logs to a Systog server. Use this page to configure email alert recipients, support contact information, and systog.  System Alerts Search Term Alerts Systog Support  The applance can transfer web traffic logs processed by the applance to a Systog server.  E Enable Systog transfer of web traffic (Sophos log)  HostnamellP  e.g. 192.168.3.1  Protocol  UDP  TCP- unencrypted Upload root authority certificate Current certificate:  Upload  Do file chosen  Upload  Current certificate:
	Apply Cancel

• TCP-encrypted

🔿 Dashboard	🔅 Config	guration	$\otimes$	Reports	Q	Search	?	Help	0	System Status
Configuration Accounts Group Policy Global Policy Updates Averse & Montor og Backup Restore Active Directory eDirectory Authentic ation Connection Profiles Time Zone Certific atios Endpoint Web Control	System: Ale The applia System Alerts The appliance Enable System Hostname/II Protocol	rts & Monito nce regularly in i transfer web to Search Term can transfer we log transfer or e.g. 192.168 UDP TCP- un TCP- un Upload Current to Current to	nonitors its h raffic logs to Alerts Sy eb traffic log d web traffic log d web traffic a.t encrypted root author is File. No	health, can send a Syskog server (slog) Support is processed by ic (Sophos log)	Alerts based o Use this pag he appliance t Port 51 e g	n significant change to configure email o a Syslog server. 4 2. 314	es in system s il alert recipient	tatus or when u	sers search for	r monitored search and syslog.
Network										

#### Note: - Attach the valid signing certificate

• TCP-Unencrypted

<ul> <li>Dashboard</li> </ul>	😥 Config	uration	Ø F	Reports	Q	Search	?	Help	System Statu
Configuration	System: Aler	rts & Monitor	ing						
Group Policy Global Policy System Updates Arbit & Montoring Bestsp Restore Restore Restore Softectory Softectory Softectory Connection Profiles Time Zone Connet Gion Profiles Time Zone Central Management Certificates Endpoint Web Control	System Alerts The applance Problem System Hostname II Protocol	Search Term / can transfer well log transfer of e.g. 192.168.3 UDP TCP - une TCP - une TCP - une Choose Current ce	Alerts Sys b traffic logs web traffic web traffic ncrypted not authorit File No fil ertificate:	log Support processed by the (Sophos log) ty certificate le chosen	Port 51 e.g	o a Syslog server.			
letwork									

### 4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Sophos web appliance.

#### 4.1 Category

- Sophos Web Appliance All allowed activities This category provides information related to all allowed requests detected in Sophos Web Appliance.
- Sophos Web Appliance All blocked activities This category provides information related to all blocked requests created in Sophos Web Appliance.

#### 4.2 Alert

- **Sophos Web Appliance: URL with malicious category accessed-** This alert is triggered when a URL with criminal and hacking category matched in Sophos Web Appliance.
- **Sophos Web Appliance: Spam URL found -** This alert is triggered when a Potential Spam URL detected in Sophos Web Appliance.
- Sophos Web Appliance: URL with spyware categories accessed This alert is triggered when a potential spyware detected in Sophos Web Appliance.
- Sophos Web Appliance: URL with phishing/fraud category accessed This alert is triggered when a Potential Phishing and Fraud activity detected in Sophos Web Appliance.
- Sophos Web Appliance: suspicious URL has been blocked This alert is triggered when a suspicious web traffic has been detected in Sophos Web Appliance.
- Sophos Web Appliance: Warned URL accessed by User This alert is triggered when a User decided to proceed with warned web traffic detected in Sophos Web Appliance.

#### 4.3 Report

• Sophos Web Appliance - Allowed Activities - This report gives information about all allowed activities detected in Sophos web appliance. Report contains user detail, source IP address, domain name, and other useful information.

LogTime	Computer	User	Sender IP Address	Domain portion	Http Request	Http respose code	Received Bytes	Sent Bytes	File type	File size
06-08-2021 01:42:10 PM	SOPHOS	Jake	1xx.xx.33.123	contoso.com	GET http://request xx	200	427	692	-	-
06-08-2021 01:42:10 PM	SOPHOS	John	1xx.xx.xx.123	contoso.com	HEAD http:requestxxx	401	279	657	-	-

• Sophos Web Appliance - Blocked Activities - This report gives information about all allowed activities detected in Sophos web appliance. Report contains user detail, source IP address, domain name, and other useful information.

	LogTime	Computer	User	Sender IP Address	Domain portion	Http Request	Http respose code	Received Bytes	Sent Bytes	File type	File size
ĺ	06-08-2021 01:42:10 PM	SOPHOS	John	1xx.xx.33.123	zoplm.com	GET http://request xx		427	-	-	-
ĺ	06-08-2021 01:42:10 PM	SOPHOS	Jake	1xx.xx.xx.123	zoplm.com	HEAD http:requestxxx		279	1 C		÷

### 4.4 Dashboards

- Sophos web appliance Allowed web traffic by Domain name
- Sophos Web Appliance Allowed web traffic by Domain name

• Sophos Web Appliance - Blocked web traffic by Domain name



• Sophos Web Appliance - Response action by connection status





• Sophos Web Appliance – Virus detected by IP address



- Sophos web appliance Malicious domains by category code 0 🖸 – 🗙 addl\_info8:(n=1,2,3,4) 0x2n00000030=Spyware 0x2n00000013=Hacking 0x2n00000009=Criminal Activity 0x2i 0x2n00000022=Phishing & Fraud 30 20 10 0 0x2200000009 0x2200000013 0x2200000022 0x2200000030 0x2300000013 0x2300000022 0x210000002e <0 💼 cigarpaqe.com 📩 zoplm.com 📰 fleldsupply.com winqsupply.com Jun 17 06:54 AM - Jun 24 06:55 AM
- Sophos Web Appliance Malicious domains by category code



## 5. Importing Sophos Web Appliance Knowledge Pack into EventTracker

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

- Category
- Alert
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.



3. Click the **Import** tab.

#### 5.1 Category

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

4	Export Import Utility
Export       Import         1. Provide the path and file name         2. Click the Import button.         Options         Octaegory         Filters         Alerts         Systems and Groups         Token Value         Reports         Behavior Correlation	e of the Categories file. Use the '' button to browse and locate the import file.  Location  Source :
	Import Close

- 2. Locate Category\_Sophos web appliance.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays success message.



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

#### 5.2 Alert

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

internet Import	Export Ir	
1. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' but	ton to browse and locate the import file.
Options O Category	Import E-mail settings	
⊖ Filters	Only if notifications set     By default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the confinuation section
<ul> <li>Alerts</li> <li>Systems and Groups</li> </ul>	Watchlist Configuration	
Token Value	<ul> <li>Import Watchlist configurat</li> <li>This setting is applicable only f Note: If this option is enabled t</li> </ul>	ion for alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are available
Reports     Behavior Correlation	on the console where the alert	is are imported.
	Source : *isalt	
		Import Close

- 2. Locate Alert\_Sophos web appliance.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 **Close**.

#### 5.3 Knowledge Object

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.

≡	EventTracker					🐥 🛛 Admin-	Tools 🕶
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	🔍 IP Lookup Configuration	🙊 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	·@ Knowledge Objects		
<b>A</b>			🗞 Behavior Correlation Settings	⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			– News			

2. Click on **Import**  $\mathbb{T}$  button as highlighted in the below image:

■ Kn	Knowledge Ob	jects		🕈 / Admin / Knowledge Objects
Q 	Search objects	Q	Q Activate Now	Objects 🕀 📳 🏦 🌣
	Groups	🕀 🗷 🗓		1
	• Cylance			
	• EventTracker			

3. Click on **Browse**.

Import			×
Select file	🗁 Browse	Upload	
			Close

- 4. Locate the file named **KO\_Sophos web appliance.etko**.
- 5. Select the check box and then click on  $\mathbb{T}$  Import option.

Import					
Selec	t file		Browse Upload		
~	Object name	Applies to	Group name		
~	Sophos Web Appliance	Sophos Web Appliance	Sophos Web Appliance		



6. Knowledge objects are now imported successfully.



### 5.4 Report

1. Click **Reports** option and select **New (\*.etcrx)** option.

<u>Ф</u>	Export Import Utility	-		x	5
Export       Import         1. Provide the path and file name.         2. Click the import button         Note : If report(s) contains templ.         Options         Category         Filters         Alerts         Systems and Groups         Token Value                 Behavior Correlation	Export Import Utility	-		~	
	Import		Close	e	

2. Locate the file named **Reports\_Sophos web appliance.etcrx** and select all the check box.

E Rep	eports Import				
Note :	: If report(s) contains template, first import template a	nd proceed with report import process.			
Select	ct file D:\Desktop_D\Sophos\configuration\Rep	orts_Sophos web appliance.etcrx		Select file	
Availat	able reports				
Title	2	Frequency Show all	- Q Q		
	Title	Sites	Groups	Systems	Frequency
	EDIT Sophos Web Appliance - Allowed Acti	WIN-MCKKRLN6KOI	Default	Test_sophosWSA-syslog	Undefined
	EDIT Sophos Web Appliance - Blocked Acti	WIN-MCKKRLN6KOI	Default	Test_sophosWSA-syslog,sophosWSA	. Undefined
2					>
_					,
Note	te: Set run time option is not applicable for Defined F	Reports and Hourly Reports			
Set	et run time for report(s) from	• at interval of minut	es Set (i)		
Rep	eplace to	Rep	olace Assign systems		
			Note: Make sure that Site	s), Group(s) and System(s) selections are va	id. 耳 🧕 🧕

3. Click the Import  $\mathbb{T}$  button to import the report. EventTracker displays success message.



#### 5.5 Dashboards

**NOTE:** Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.



	Home			
٩	My Dashboard			
R	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			-
	Compliance		The second second	

- 2. Navigate to **My Dashboard** option as shown above.
- 3. Click on the **Import**  $\blacksquare$  button as show below.

Event <b>Tracker</b> ⊕	<b>"</b>	Admin <del>-</del>	Tools <del>-</del>	💽 ETAdmin 🔹
My Dashboard		A	/ Dashboar	d / My Dashboard
		÷	🧭 🎱 🎝	1 3 0

- 4. Import dashboard file Dashboard\_Sophos web appliance.etwd and select Select All checkbox.
- 5. Click on **Import** as shown below.

						🗁 Browse	Upload
Availat	le widgets						
Selec	t All						
So So	phos Web Appli	ance - Vi	Sophos W	leb Appliance	e - Re		
🗹 So	phos Web Appli	ance - Al	Sophos W	/eb Appliance	e - Bl		
So So	phos Web Appli	ance - Ma					
						Import	Close

6. Import is now completed successfully.



7. In **My Dashboard** page select ⊕ to add dashboard.



8. Choose appropriate name for **Title** and **Description**. Click **Save**.

Add Dashboard	
Title	
Sophos web appliance	
Description	
Sophos web appliance	
Save Delete Cancel	
	_

9. In **My Dashboard** page select (a) to add dashlets.

My Dashb	oard	
Windows	Sophos we	
		Title: Sophos web appliance Description: Sophos web appliance

10. Select imported dashlets and click Add.

Customize dashlets				×
sophos			୍	
Sophos Web Appliance - Allowe	Sophos Web Appliance - Blocke	Sophos Web Appliance - Malici	Sophos Web Appliance - Respo	
Sophos Web Appliance - Virus				
			Add Delete Clos	e

## 6. Verifying Sophos Web Appliance Knowledge Pack in EventTracker

#### 6.1 Category

- 1. Logon to EventTracker.
- 2. Click Admin dropdown, and then click Category.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin 🗸	Tools <del>-</del>
	Home		artive Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	1 Weights	
			🗞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	🧭 Parsing Rules		
			oloo⊂ Category	FAQ Configuration	Report Settings		
	Attacker			<ul> <li>News</li> </ul>			

3. In **Category Tree** to view imported category, scroll down and expand **Sophos Web Appliance** group folder to view the imported category.



### 6.2 Alert

- 1. Logon to **EventTracker**.
- 2. Click the Admin menu, and then click Alerts.

≡	Event <b>Tracker</b> ⊕						🔑 🛛 Admin 🗸	Tools <del>-</del>
	Home		Active Watch Lists		Collection Master	Group Management	Systems	🕈 / Dash
a			Alerts		Correlation	🔍 IP Lookup Configuration	🙊 Users	_
	0	2	Behavior Correlati	on Rules	Diagnostics	· Knowledge Objects	1 Weights	
			🍓 Behavior Correlation Settings		⊽ Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configu	uration	Eventvault	🧭 Parsing Rules		
			₀ Category		FAQ Configuration	Report Settings		
	Attacker				- News			

 In the Search box, type Sophos Web Appliance, and then click Go. Alert Management page will display the imported alert.

÷	Activate Now Click 'Activate Now' after making all changes
	Alert Name 🔨
	ဇူနို Sophos Web Appliance : Malware detected
	နိုဂ္ဂို Sophos Web Appliance : Spam URL found
	နူန္မိ Sophos Web Appliance : suspicious URL has been blocked
	နူရို Sophos Web Appliance : URL with malicious category accessed
	နူရို Sophos Web Appliance : URL with phishing/fraud category accessed
	နူရို Sophos Web Appliance : URL with spyware categories accessed
	ဇူရို Sophos Web Appliance : Warned URL accessed by User

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

Succ	essfully saved configuration. s page from creating additional dialogs
	ОК

5. Click **OK**, and then click **Activate Now**.

**NOTE:** Specify appropriate **system** in **alert configuration** for better performance.

#### 6.3 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects.** 

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin -	Tools <del>-</del>
	Home		🚰 Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
0			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	_
	0	1	Behavior Correlation Rules	1 Diagnostics	Knowledge Objects	⊕ Weights	
<b>*</b>			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			o-[o Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Object tree, expand **Sophos Web Appliance** group folder to view the imported knowledge object.



3. Click Activate Now to apply imported knowledge objects.

#### 6.4 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

≡	Event <b>Tracker</b> ⊕			
	Home			
Q R	 Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer Attacker			-

- 2. In Reports Configuration pane, select Defined option.
- 3. Click on the Sophos Web Appliance group folder to view the imported reports.

Reports configuration: Sophos Web Appliance

<b>+</b>	Î <b>2</b> ,	
		Title
	£\$3	Sophos Web Appliance - Blocked Activities
	(i)	Sophos Web Appliance - Allowed Activities

#### 6.5 Dashboards

1. In the EventTracker web interface, click on the Home Button and select My Dashboard.



2. In the Sophos Web Appliance dashboard you will see the following screen.



### **About Netsurion**

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

#### **Contact Us**

#### **Corporate Headquarters**

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support