Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate Sophos Web Appliance with EventTracker

Publication Date:

July 6, 2021

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

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:

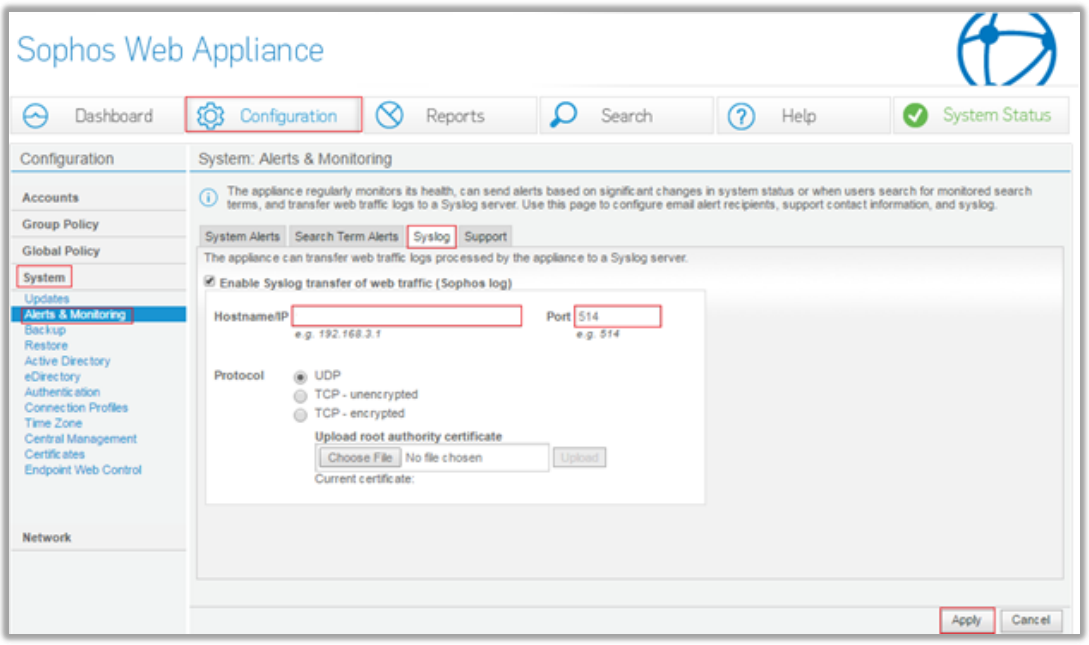
- EventTracker v9.3 or above should be installed.
- Admin role on Sophos Web Appliance to make configuration changes.
- Administrative access on the EventTracker.
- EventTracker IP and port need to add in firewall allowed list.

3. Configuring Sophos Web Appliance to forward logs to EventTracker

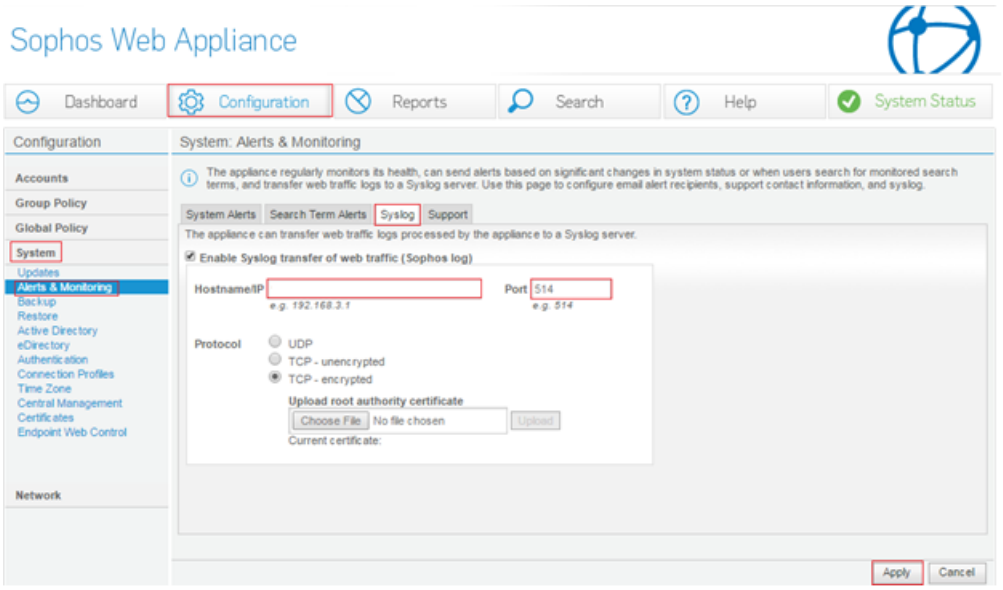
The steps provided below will help to configure the EventTracker to receive Sophos Web Appliance events via Syslog.

1. On the **Configuration > System > Alerts & Monitoring** page, select the **Syslog** tab.
2. Select the **Enable syslog transfer of web traffic** check box.
3. 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**.

- UDP

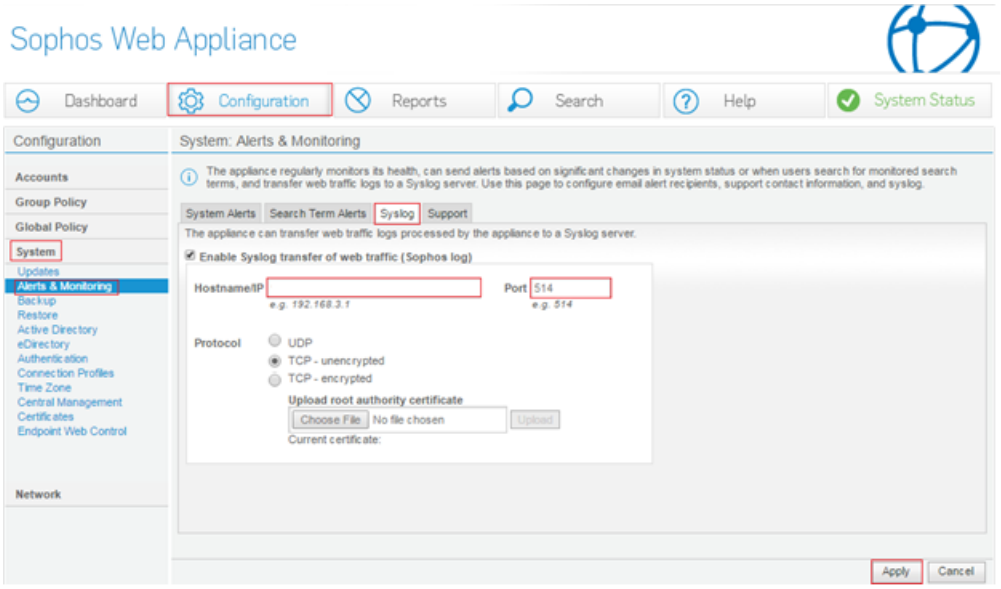


- TCP-encrypted



Note: - Attach the valid signing certificate

- TCP-Unencrypted



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.

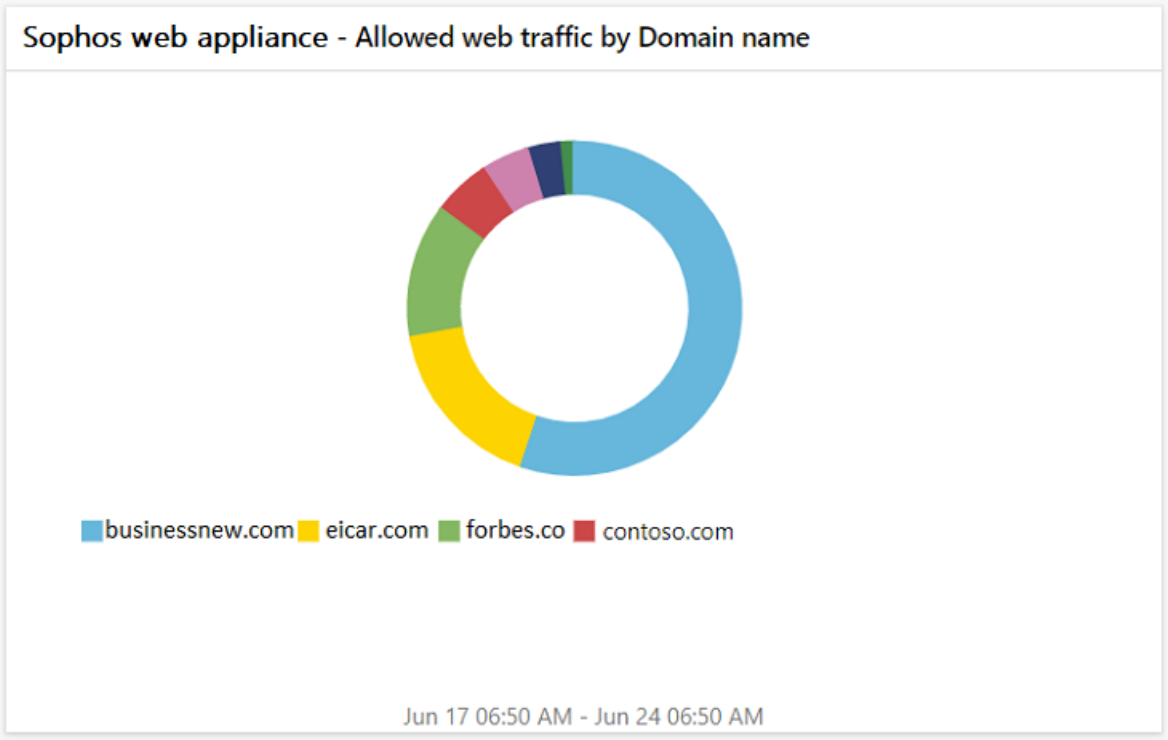
LogTime	Computer	User	Sender IP Address	Domain portion	Http Request	Http respose code	Received Bytes	Sent Bytes	File type	File size
06-08-2021 01:42:10 PM	SOPHOS	Jake	1xx.xx.33.123	contoso.com	GET http://request xx	200	427	692	-	-
06-08-2021 01:42:10 PM	SOPHOS	John	1xx.xx.xx.123	contoso.com	HEAD http:requestxxx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

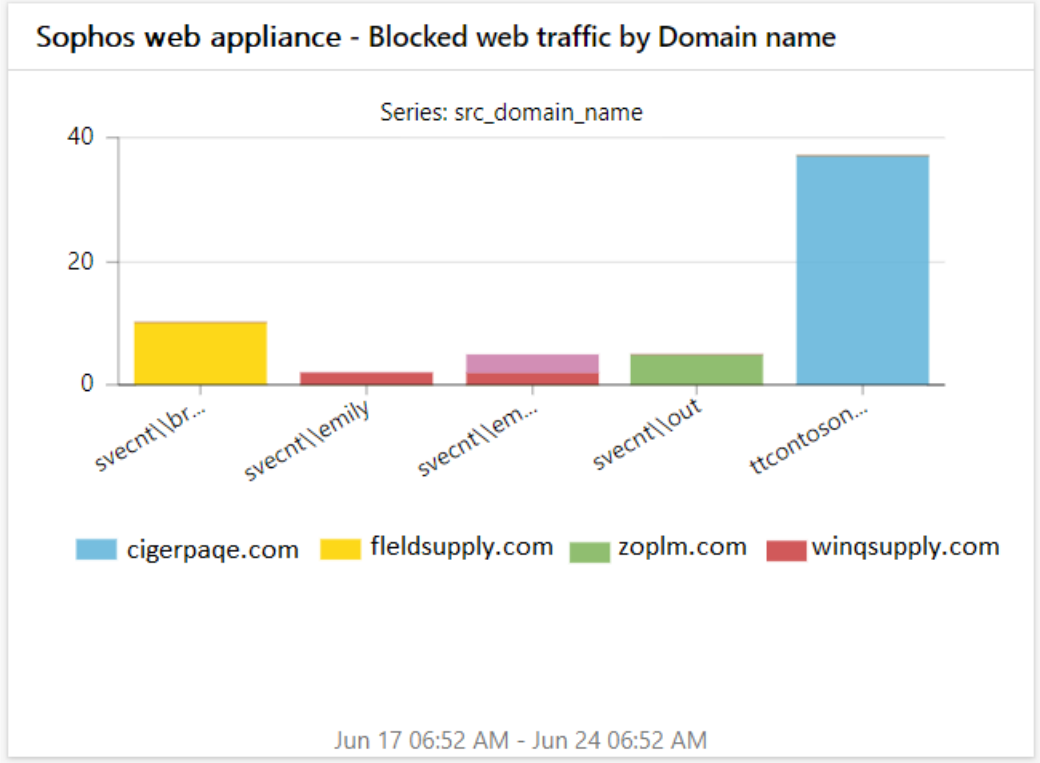
LogTime	Computer	User	Sender IP Address	Domain portion	Http Request	Http respose code	Received Bytes	Sent Bytes	File type	File size
06-08-2021 01:42:10 PM	SOPHOS	John	1xx.xx.33.123	zoplm.com	GET http://request xx	-	427	-	-	-
06-08-2021 01:42:10 PM	SOPHOS	Jake	1xx.xx.xx.123	zoplm.com	HEAD http:requestxxx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

4.4 Dashboards

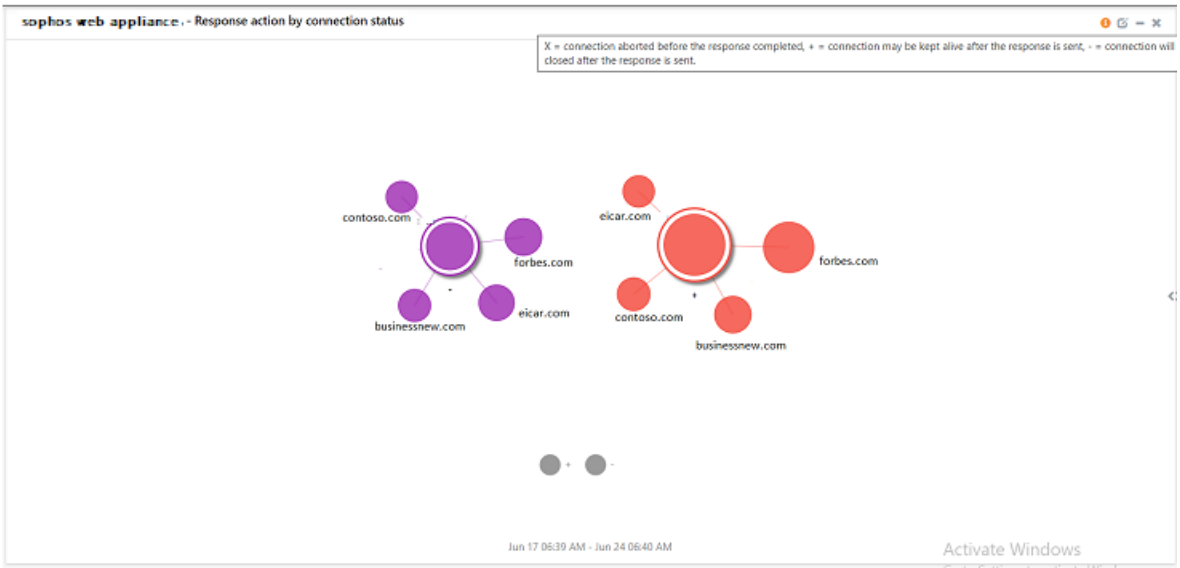
- **Sophos Web Appliance - Allowed web traffic by Domain name**



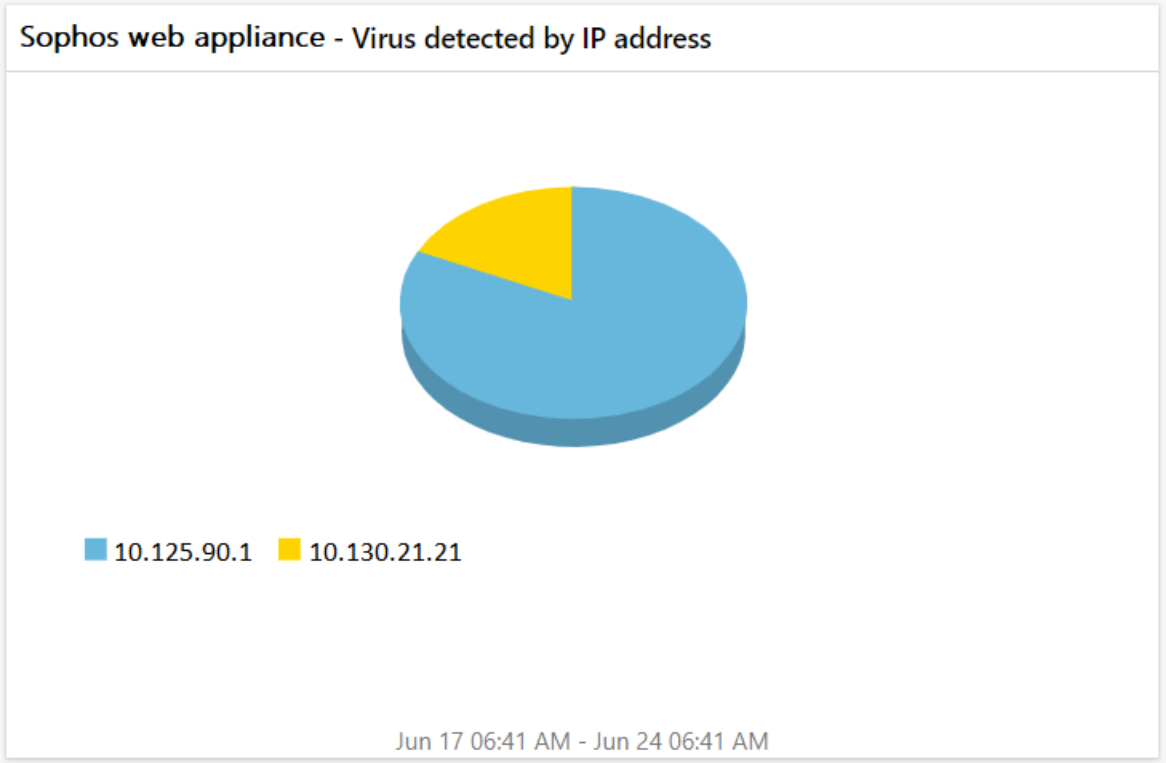
- **Sophos Web Appliance - Blocked web traffic by Domain name**



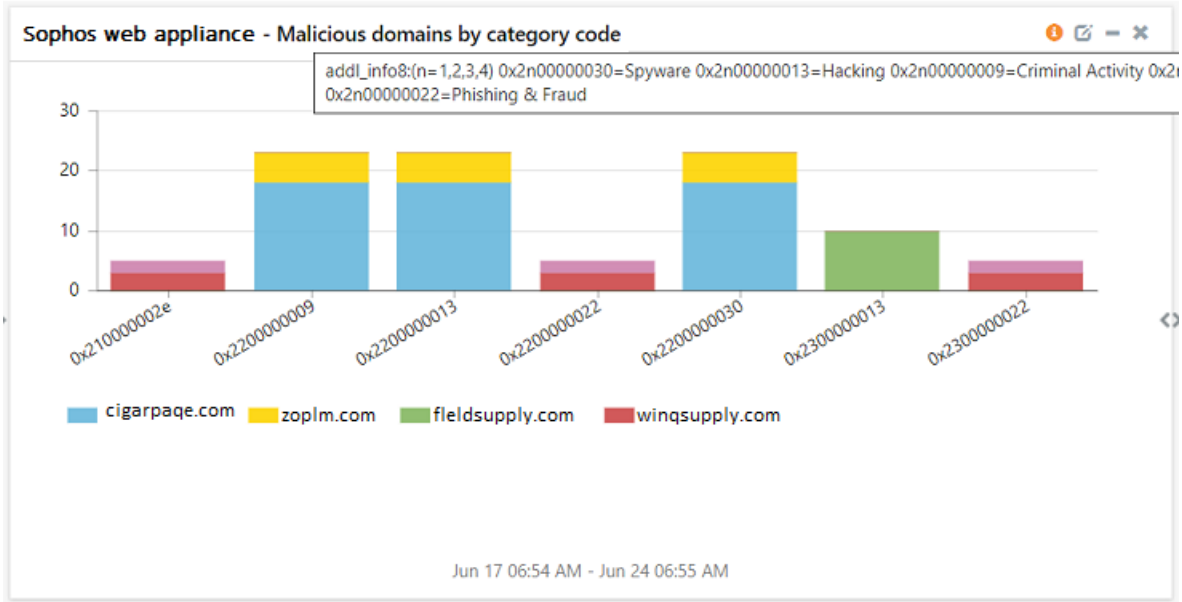
- **Sophos Web Appliance - Response action by connection status**



- **Sophos Web Appliance – Virus detected by IP address**



- **Sophos Web Appliance – Malicious domains by category code**



5. Importing Sophos Web Appliance Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

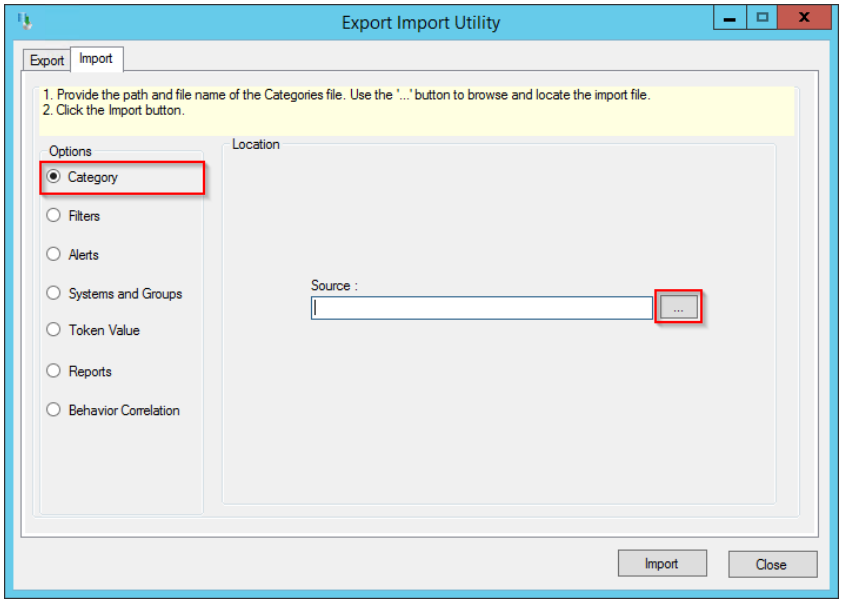
- Category
- Alert
- Knowledge Object
- Report
- Dashboard

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

3. Click the **Import** tab.

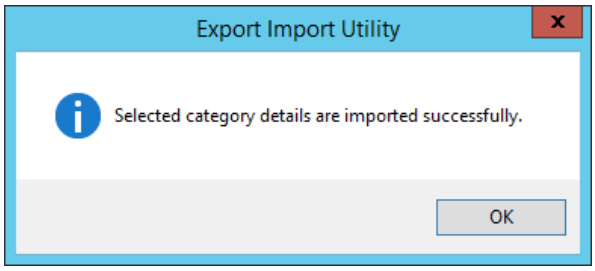
5.1 Category

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



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

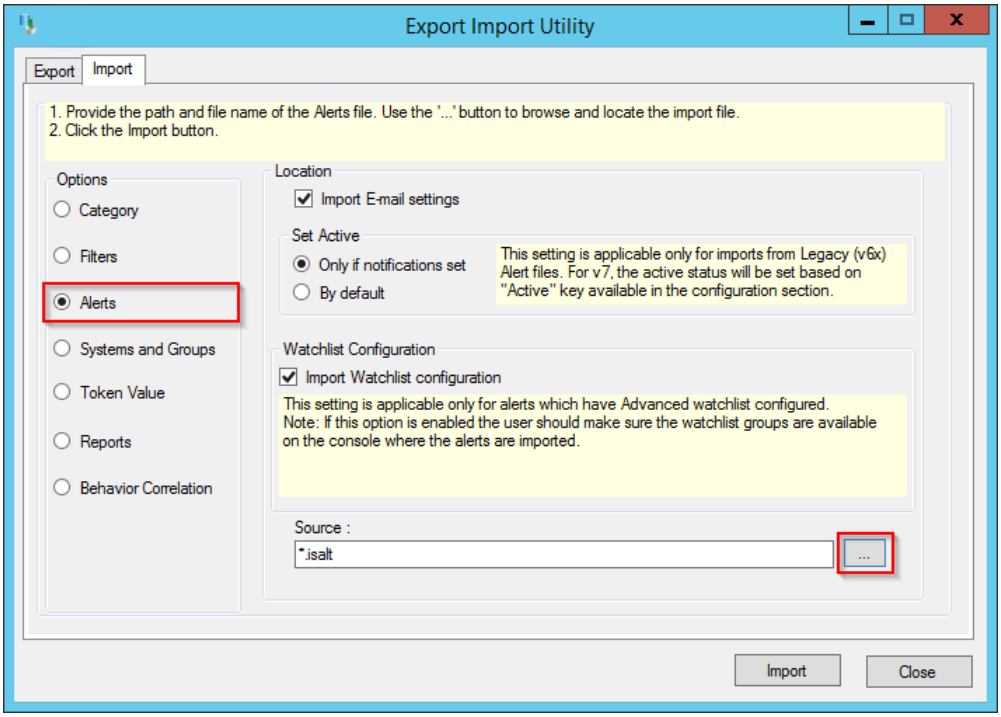
EventTracker displays success message.



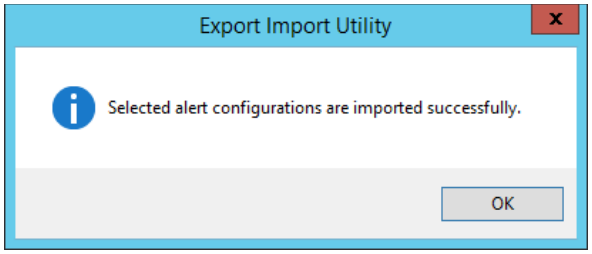
4. Click **OK,** and then click the **Close** button.

5.2 Alert

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



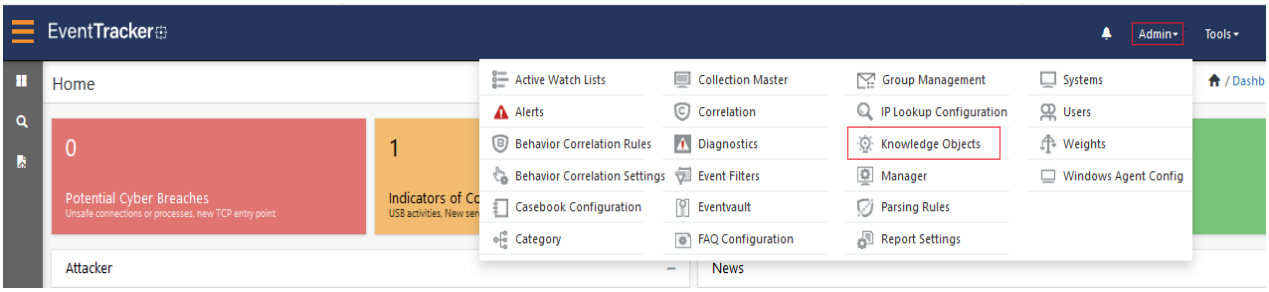
2. Locate **Alert_Sophos web appliance.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.



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

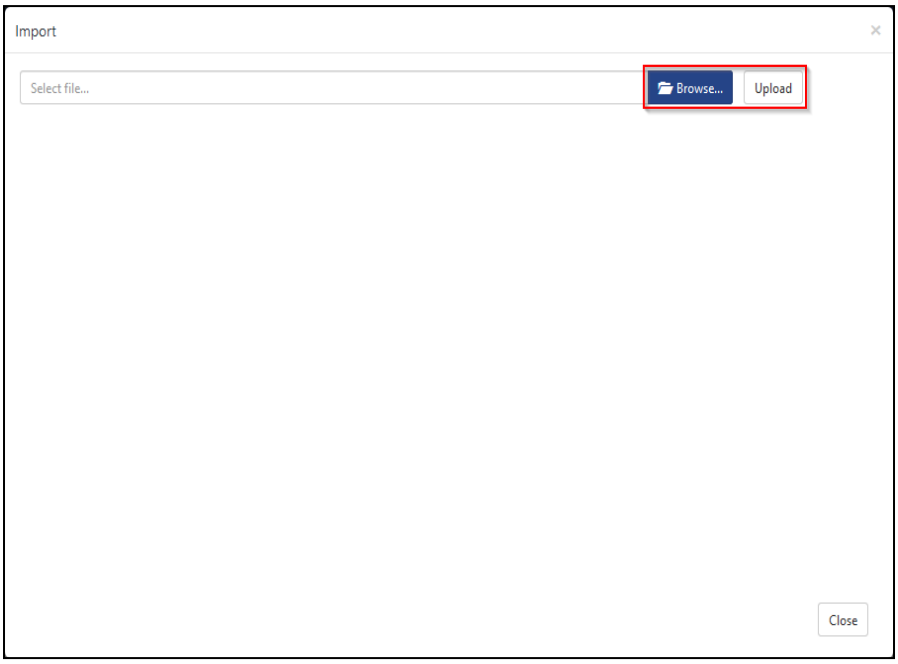
5.3 Knowledge Object

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

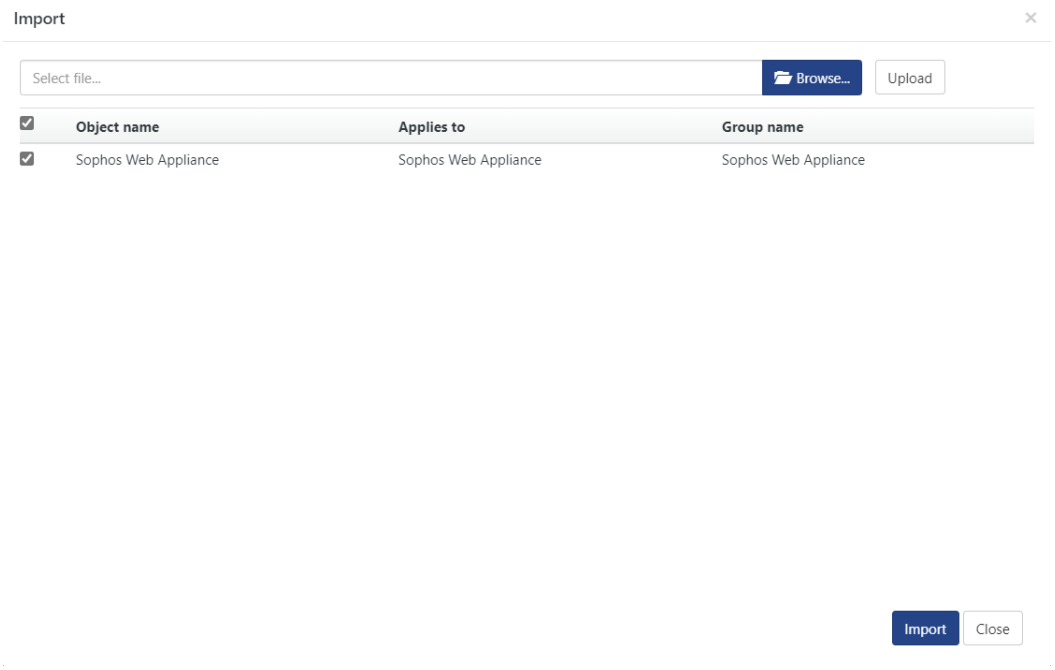


2. Click on **Import** button as highlighted in the below image:

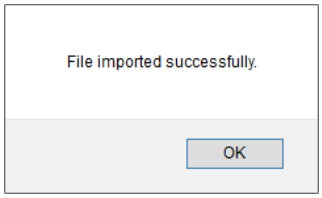
3. Click on **Browse**.



4. Locate the file named **KO_Sophos web appliance.etko**.
5. Select the check box and then click on **Import** option.

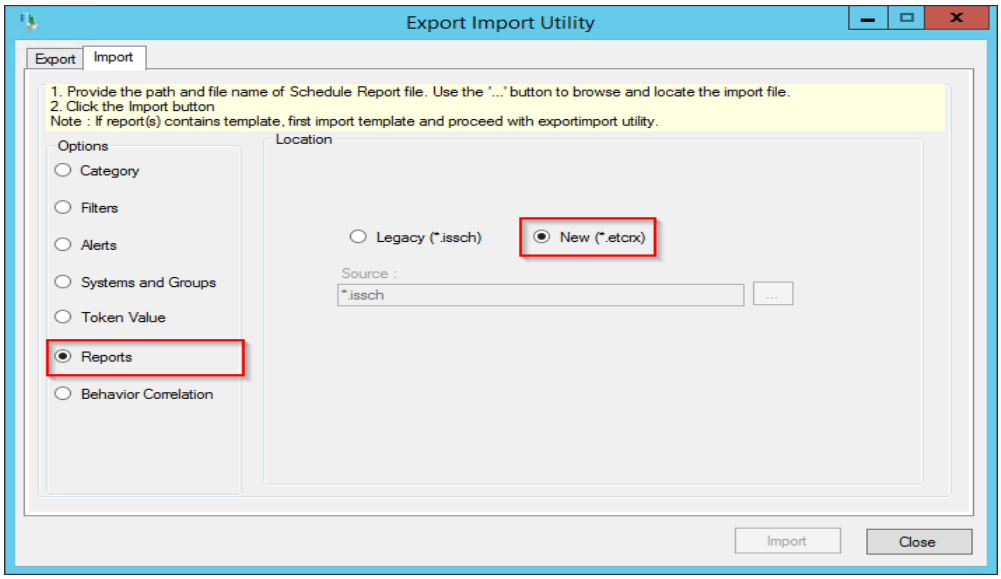


6. Knowledge objects are now imported successfully.

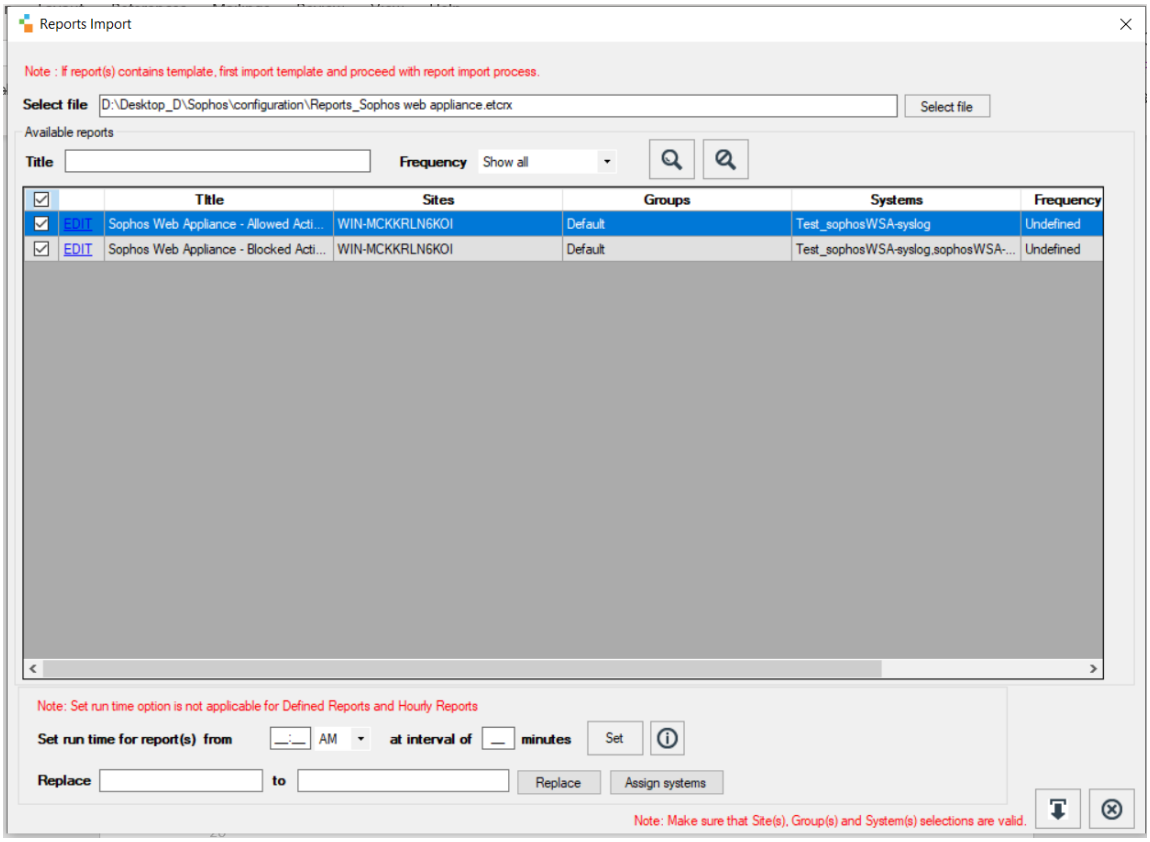


5.4 Report

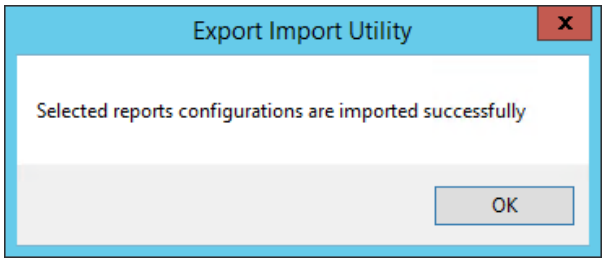
1. Click **Reports** option and select **New (*.etcrx)** option.



2. Locate the file named **Reports_ Sophos web appliance.etcrx** and select all the check box.



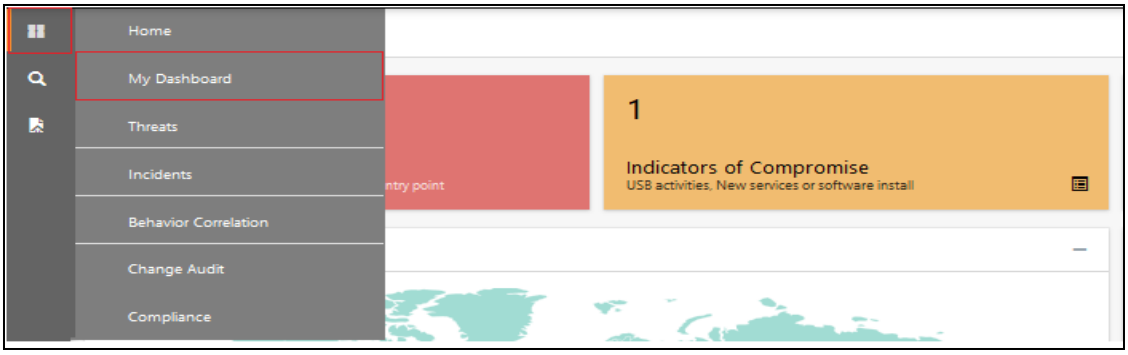
3. Click the **Import** button to import the report. EventTracker displays success message.



5.5 Dashboards

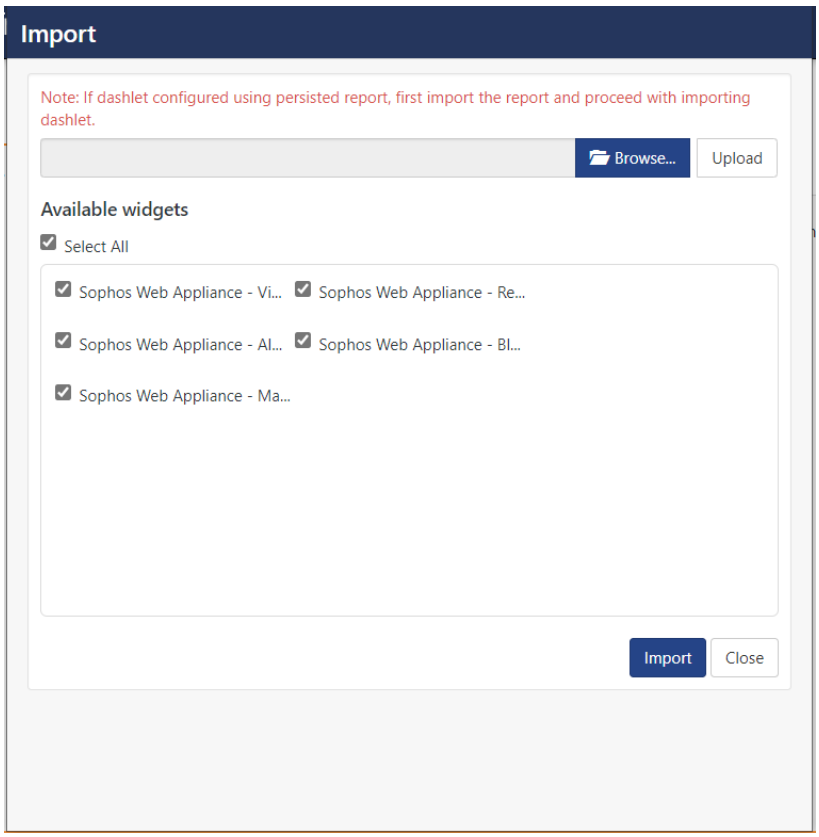
NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.

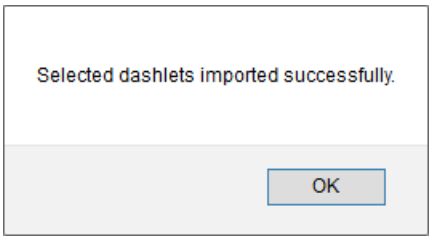


2. Navigate to **My Dashboard** option as shown above.
3. Click on the **Import** button as show below.

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

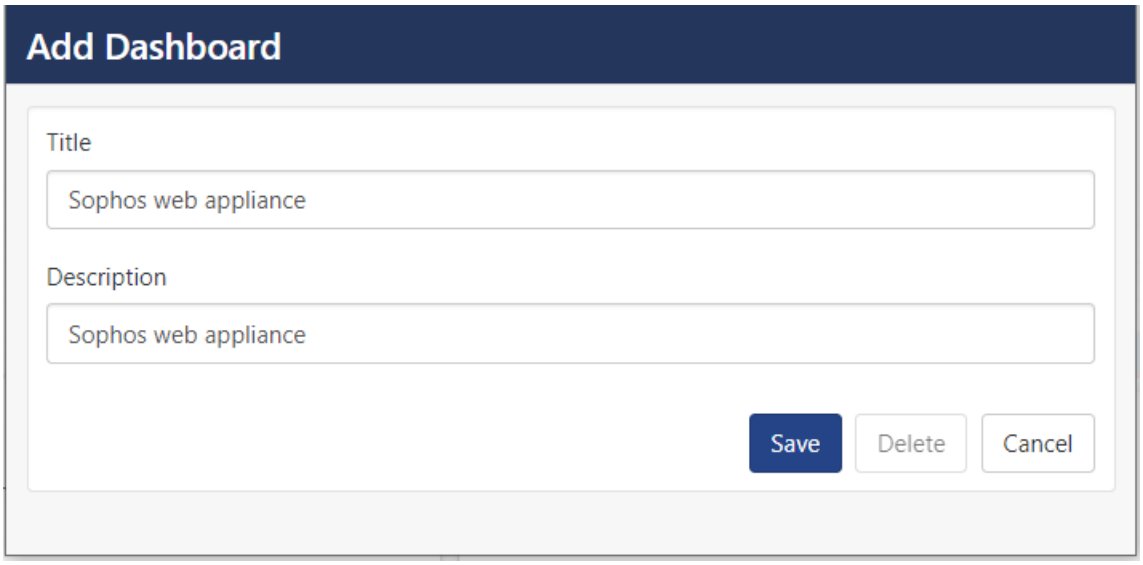


6. Import is now completed successfully.

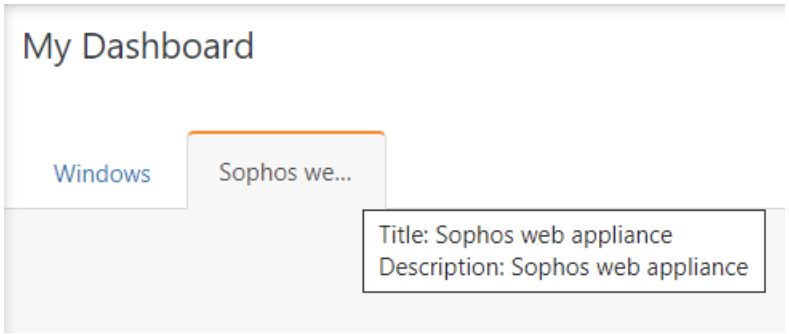


7. In **My Dashboard** page select ⊕ to add dashboard.

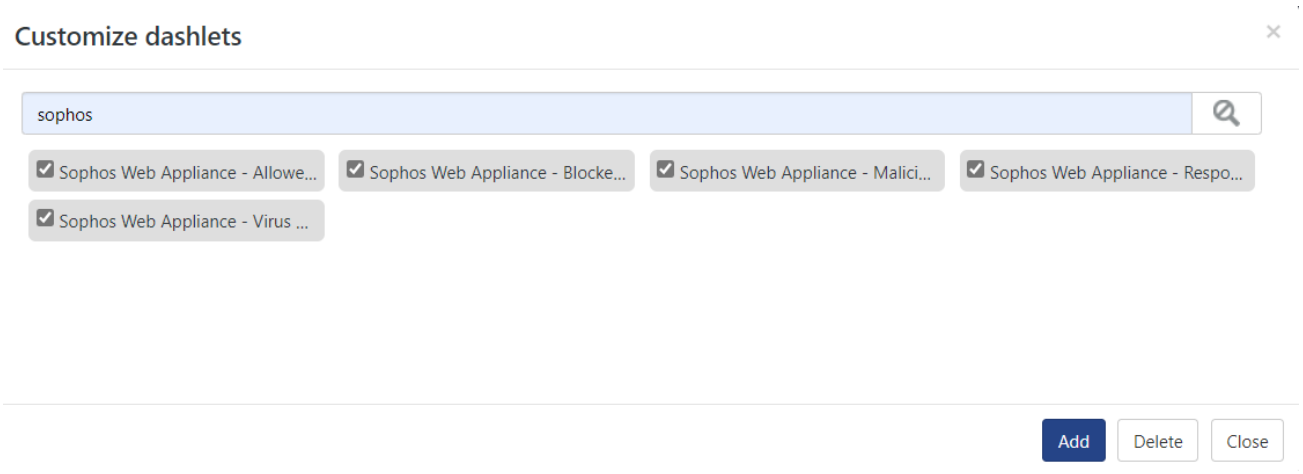
8. Choose appropriate name for **Title** and **Description**. Click **Save**.



9. In **My Dashboard** page select to add dashlets.



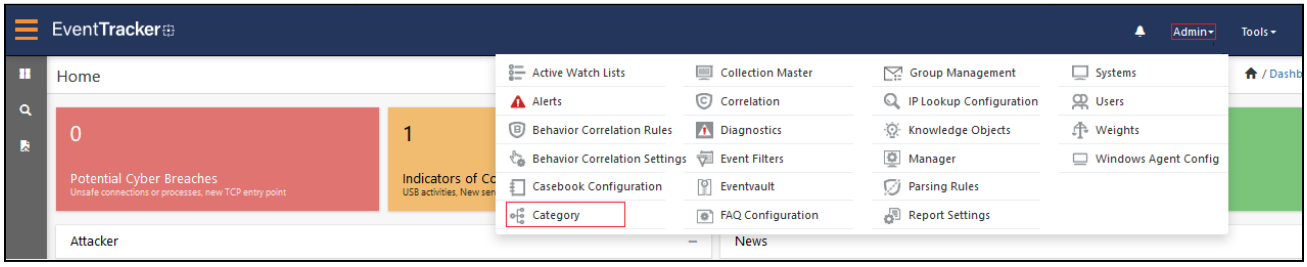
10. Select imported dashlets and click **Add**.



6. Verifying Sophos Web Appliance Knowledge Pack in EventTracker

6.1 Category

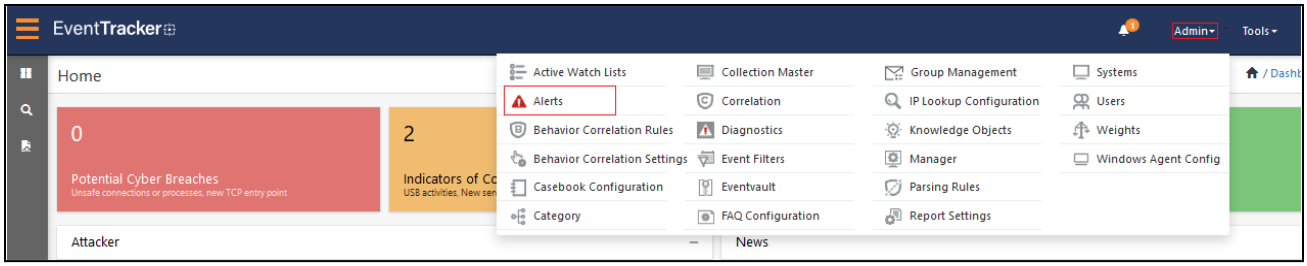
1. Logon to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.



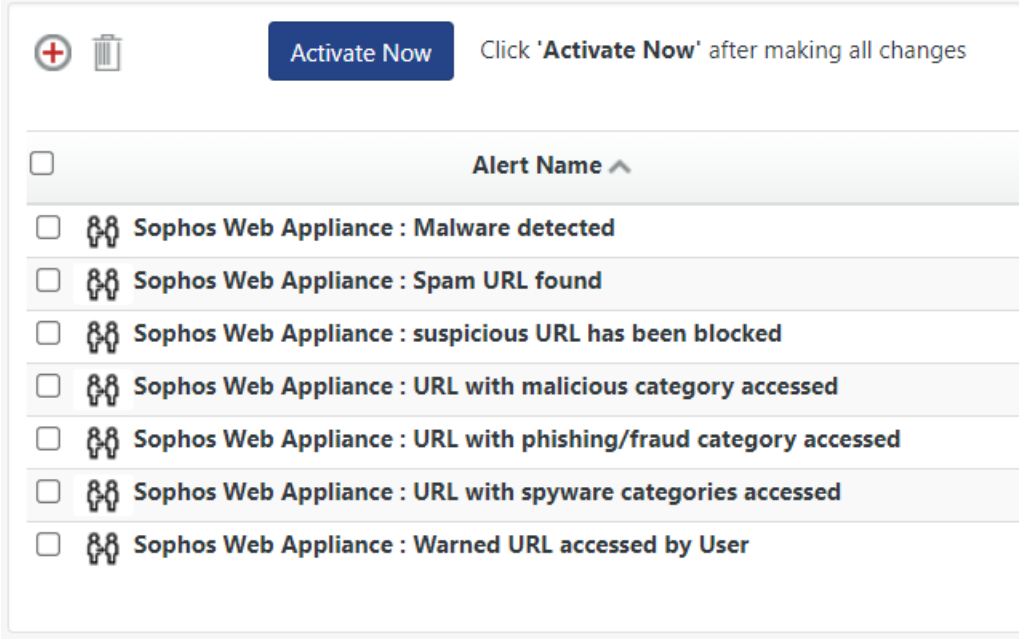
3. In **Category Tree** to view imported category, scroll down and expand **Sophos Web Appliance** group folder to view the imported category.

6.2 Alert

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

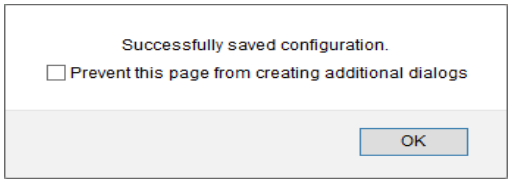


3. In the **Search** box, type **Sophos Web Appliance**, and then click **Go**.
   Alert Management page will display the imported alert.



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

   EventTracker displays message box.

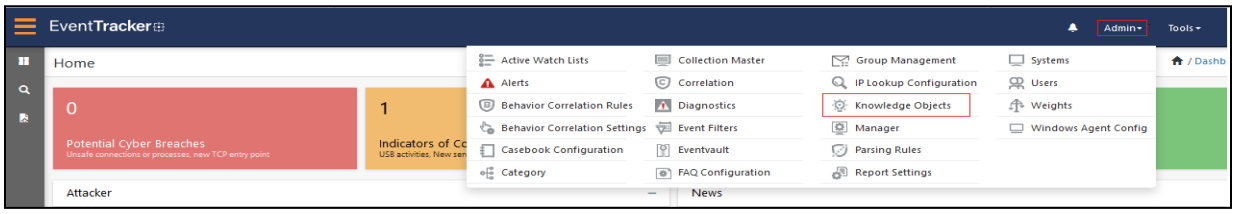


5. Click **OK**, and then click **Activate Now**.

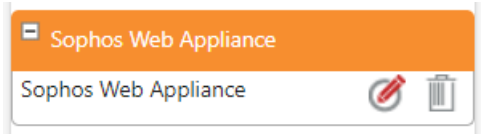
NOTE: Specify appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Object

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



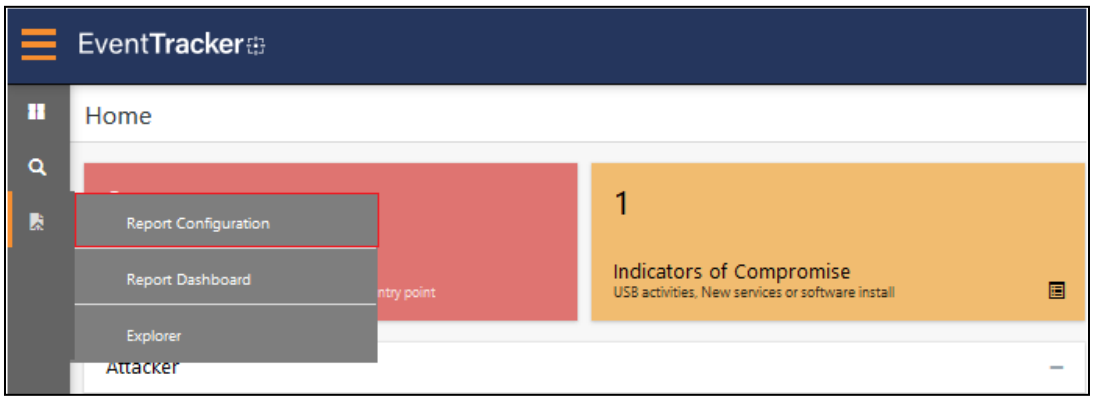
2. In the Knowledge Object tree, expand **Sophos Web Appliance** group folder to view the imported knowledge object.



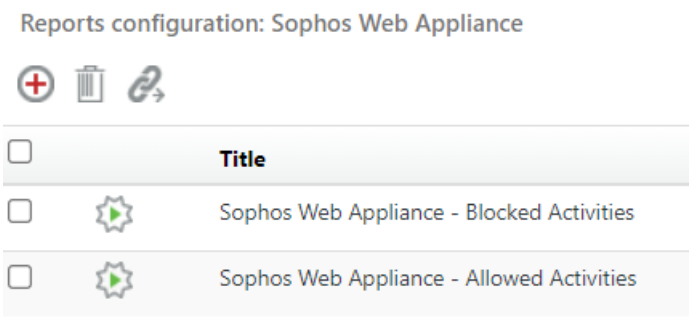
3. Click **Activate Now** to apply imported knowledge objects.

6.4 Report

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

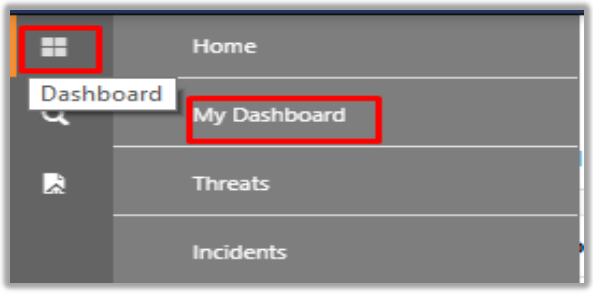


2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Sophos Web Appliance** group folder to view the imported reports.

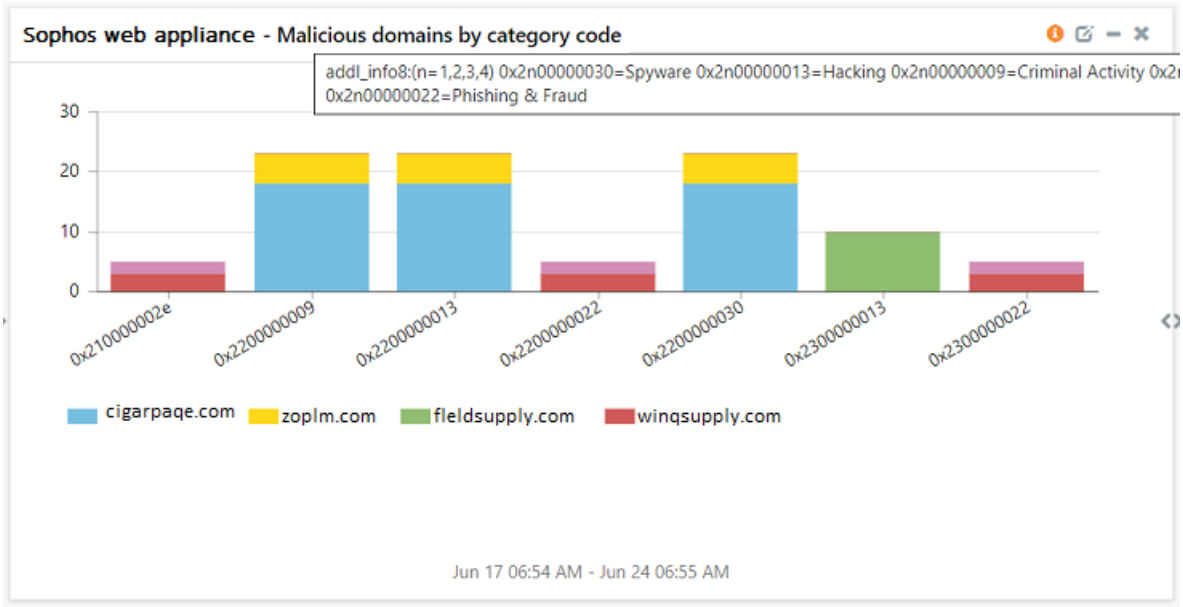


6.5 Dashboards

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 EventTracker 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 BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location 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 netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

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