Integration Guide

Integrate Barracuda Sentinel with EventTracker

Publication Date:

October 25, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Barracuda Sentinel (Impersonation Protection). The Knowledge Pack contains alerts, reports, dashboards, and knowledge objects.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later, and Barracuda Sentinel (Impersonation Protection).

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.

Table of Contents

1 Overview

Barracuda Impersonation Protection (formerly Sentinel) combines artificial intelligence, deep integration with Microsoft Office 365, and brand protection into a comprehensive cloud-based solution that guards against business email compromise, account takeover, spear phishing and other cyber fraud.

Netsurion, the Managed Threat Protection platform facilitates monitoring events retrieved from Barracuda Sentinel and seamlessly consolidates SIEM, Log Management, File Integrity Monitoring, machine analytics, and user behavior details.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Barracuda Sentinel (Impersonation Protection) to forward logs to EventTracker.

Note

Refer to How-To guide to configure Barracuda Sentinel (Impersonation Protection) to forward logs to EventTracker.

3 EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, configure the Knowledge Packs into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker.

3.1 Category

Barracuda Sentinel - Spear phishing threat activities: This category shows the spear phishing threat related activities performed by the users.

Barracuda Sentinel - Account takeover attack activities: This category shows the account takeovers threat activities performed by the users.

3.2 Alerts

Barracuda Sentinel: Threat detected: This alert is triggered when potentially malicious content or threat like spear phishing or account takeover are detected.

Barracuda Sentinel: Suspicious user login detected: This alert is triggered when a suspicious user logon is detected based on the geo location logon patterns.

3.3 Reports

Barracuda Sentinel - Spear phishing threat activities: This report provides a detailed summary of all the Barracuda Sentinel events related to spear phishing threat activities. The report includes sender details, recipient address, and more.

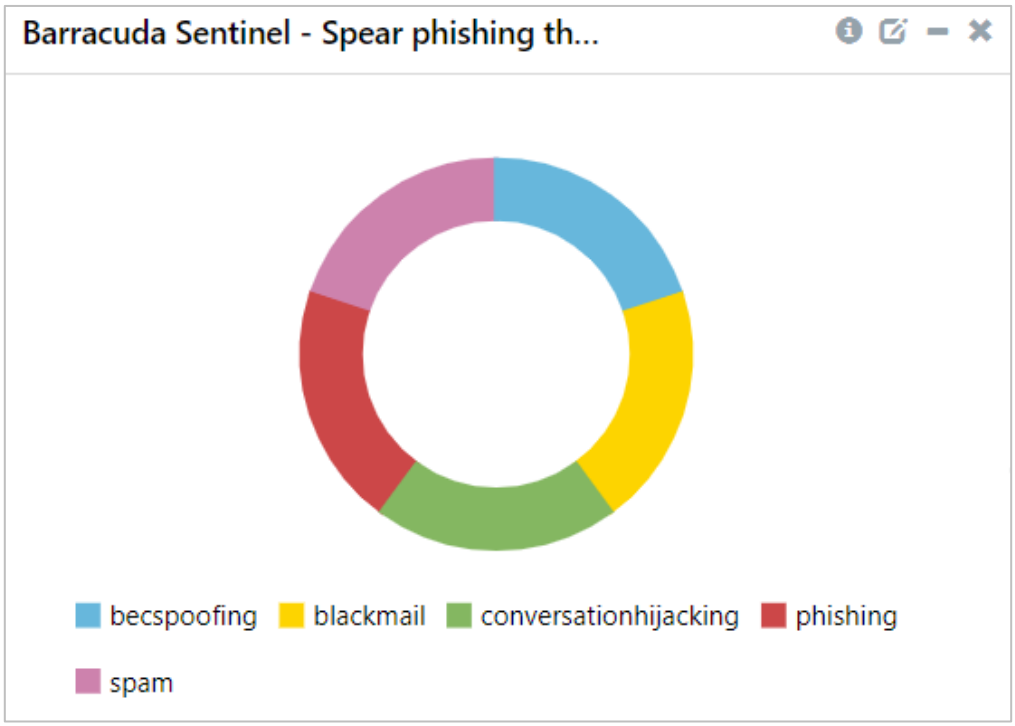
Log time	Threat type	Sender address	Email subject	Recipient address	Access token ID	Account ID
2022-06-25 - 12:11:50	becSpoofing	user@example.com	One more question	jack@contoso.com	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-18 - 22:10:55	blackmail	jeremyanapophysial1993@yahoo.com	Jonathan david	jonathan@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-19 - 07:02:20	spam	copydb@initweb.net	Re: Hello	Jacob@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-21 - 01:45:17	phishing	info@ravintitle.com	contoso Docusign-M JF839-0139-M-S39-6, Contract No. 39-g	cole@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d
2022-09-26 - 11:52:01	conversationHijacking	sglickman@chmsgroups.com	New Castle	samuel@contoso.com	dd55-4a24-be9d-6e1bae264e96	b117-4c79-b825-df1793d7f46d

Barracuda Sentinel: Account takeover attack activities: This report provides a detailed summary of all the account takeover alerts like suspicious login activities performed by the users, any inbox rule changes, and more. The report includes User information, IP address details, Logon location, and so on.

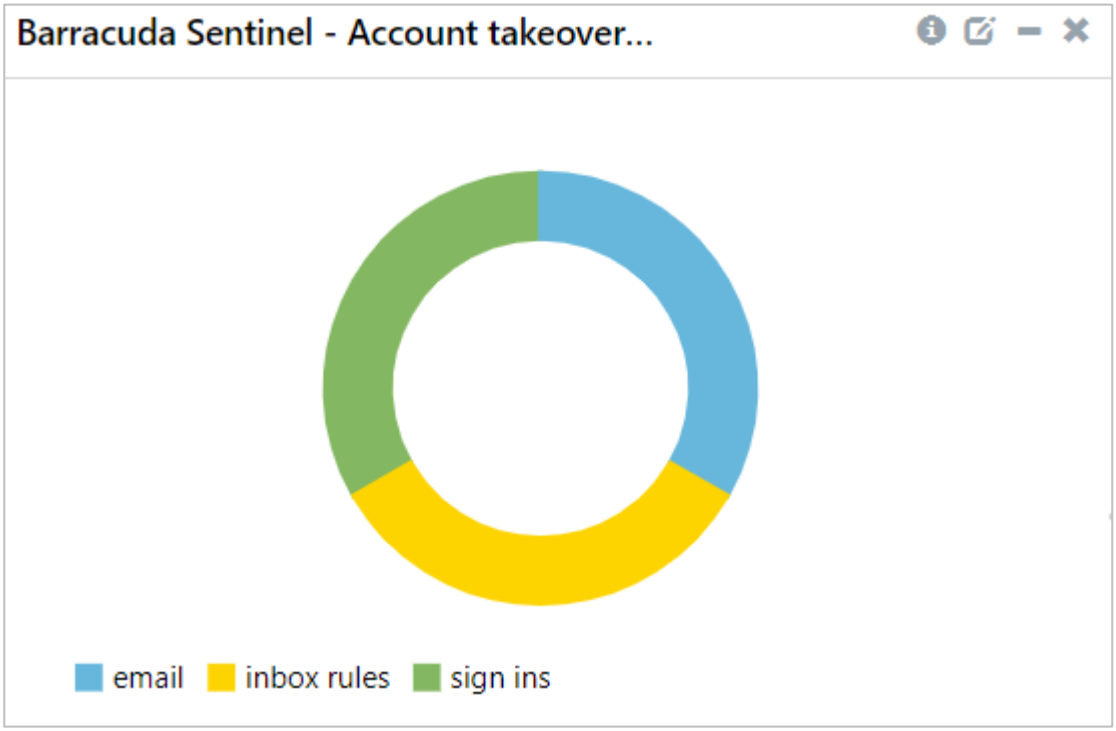
Log time	Threat type	Sender name	Sender details	Email subject	User Info	User name	Login agent	Login IP address	Location	Rule name	Access token ID	Account ID
2020-06-21 - 00:40:00	Inbox Rules				johnathan@contoso.com	Internal, User				Forward mail to John	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00	Sign Ins				mark@contoso.com	Internal, User	Windows/10 - Chrome	142.250.138.101	Mexico		dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00	Inbox Rules				johnathan@contoso.com	Internal, User				Forward mail to John	dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-21 - 00:40:00	Sign Ins				mark@contoso.com	Internal, User	Windows/10 - Chrome	142.250.138.101	Mexico		dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-23 - 21:45:27	Email	John, User	John@contso.com	HW#22.pdf	user@contoso.com	Internal, User					dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d
2020-06-23 - 21:45:27	Email	John, User	John@contso.com	HW#22.pdf	user@contoso.com	Internal, User					dd55-4a24-be9d6e1bae264e96	b117-4c79-b825-df1793d7f46d

3.4 Dashboard

Barracuda Sentinel: Spear phishing threats: This dashlet displays the different types of phishing threats detected related to spear phishing.



Barracuda Sentinel: Account takeover attacks related events: This dashlet displays the different types of threat detected related to account takeover alerts.

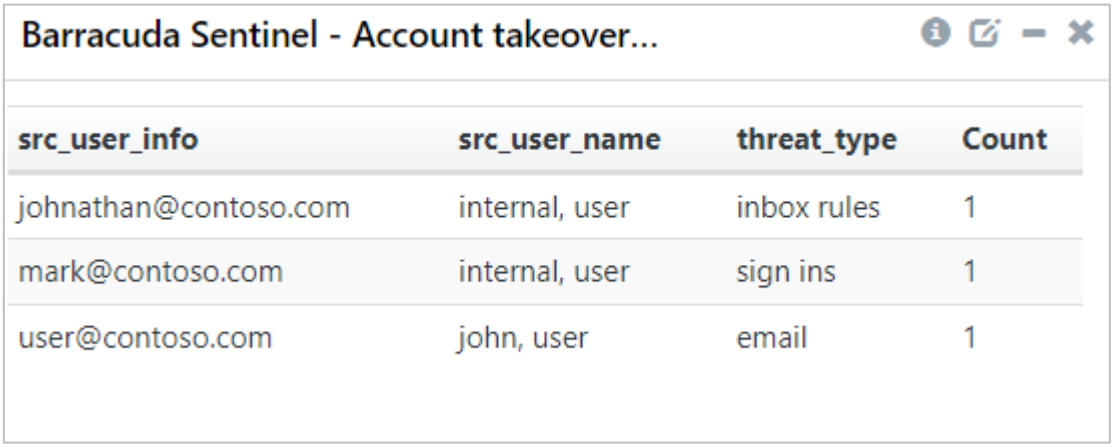


Barracuda Sentinel: Spear phishing detected on users: This dashlet displays the list of user information according to the threat attack detected.

Barracuda Sentinel - Spear phishing detected on ...

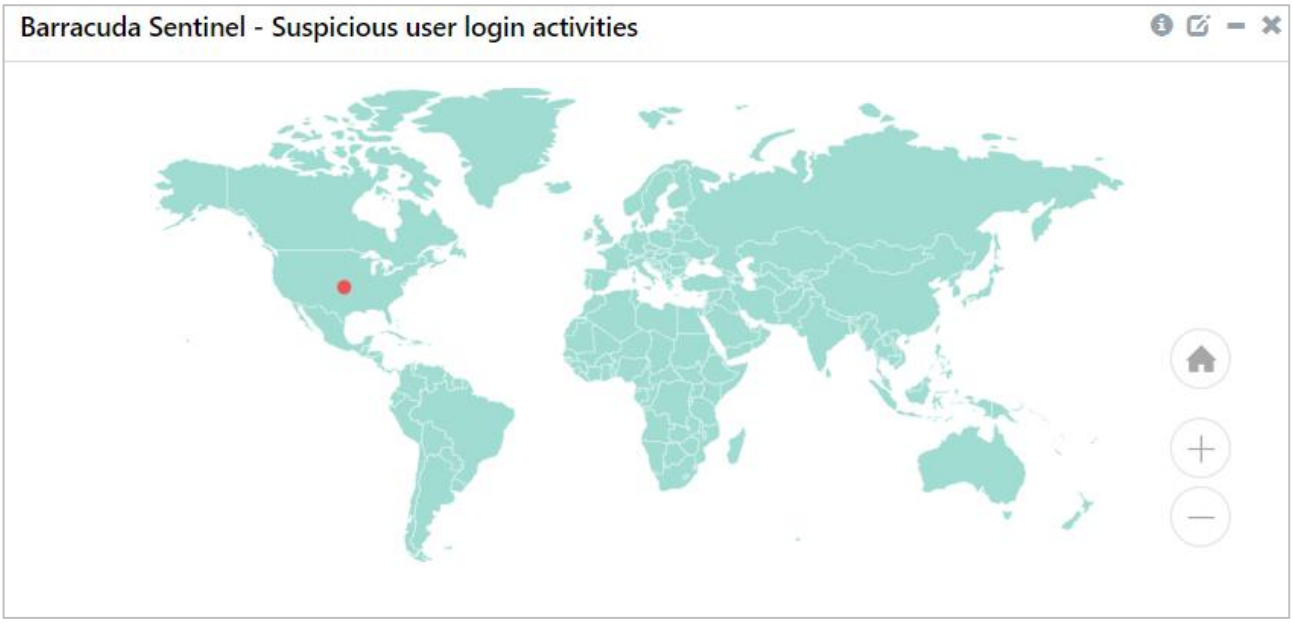
recipient_address	sender_address	threat_type	Count
cole@contoso.com	info@ravintitle.com	phishing	1
jack@contoso.com	user@example.com	becspoofing	1
jacob@contoso.com	copydb@initweb.net	spam	1
jonathan@contoso.com	jeremyanapophysial1993@yahoo.com	blackmail	1
samuel@contoso.com	sglickman@chmsgroups.com	conversationhijacking	1

Barracuda Sentinel: Account takeover alert detected on users: This dashlet displays the list of users with information according to the threat type detected for account takeover.



src_user_info	src_user_name	threat_type	Count
johnathan@contoso.com	internal, user	inbox rules	1
mark@contoso.com	internal, user	sign ins	1
user@contoso.com	john, user	email	1

Barracuda Sentinel: Suspicious user login activities: This dashlet displays the suspicious login activities performed by users according to their geo location.

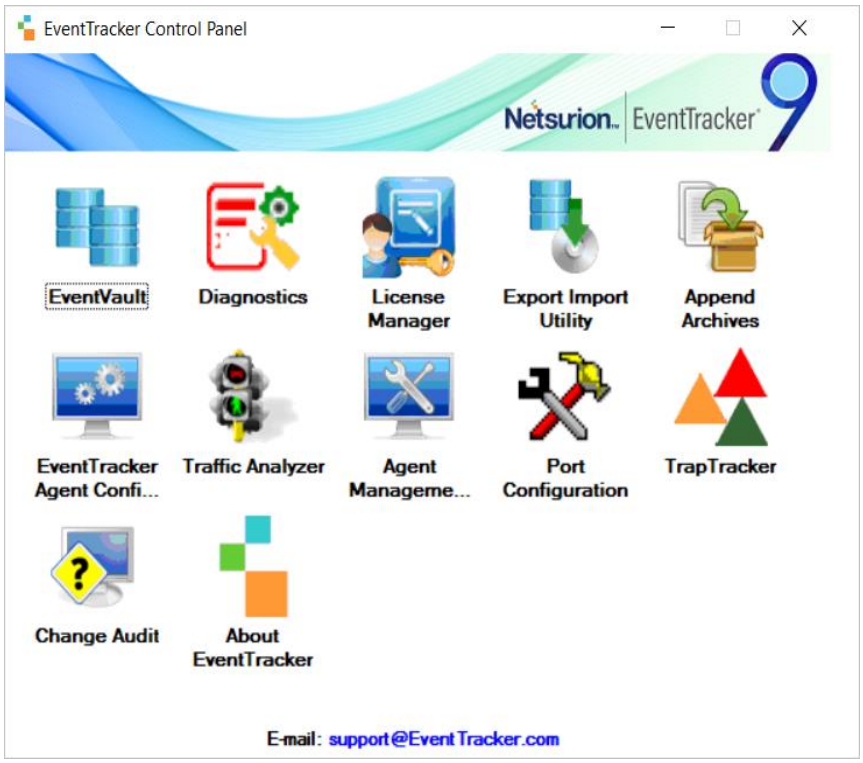


4 Importing Barracuda Sentinel Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

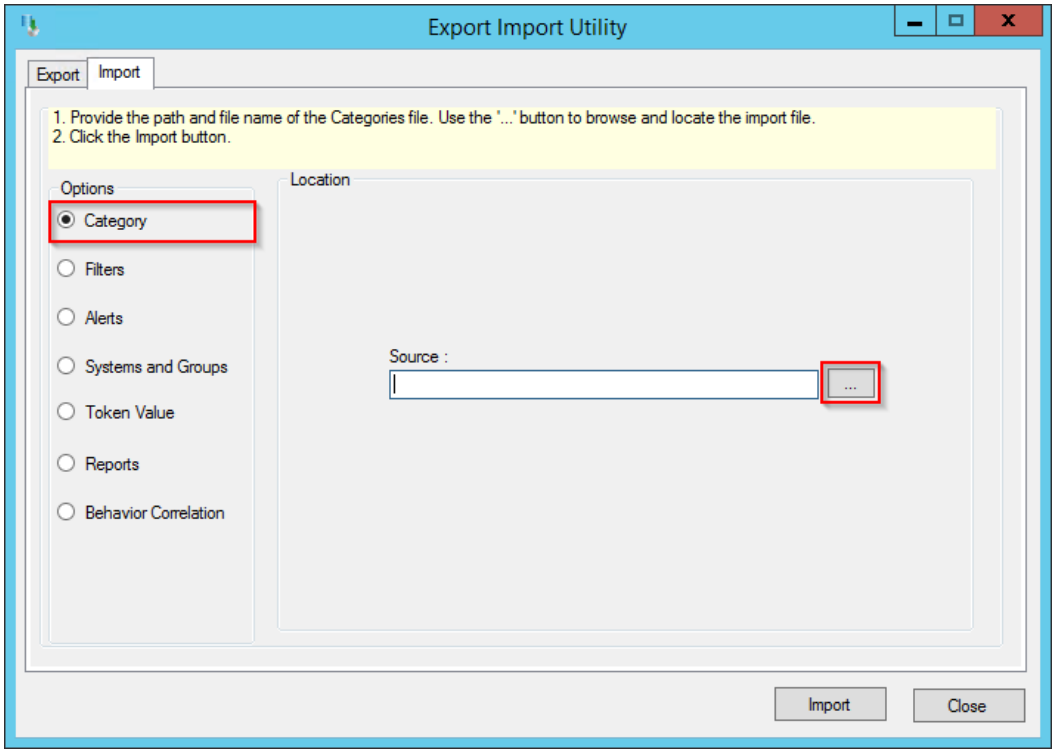
- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

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

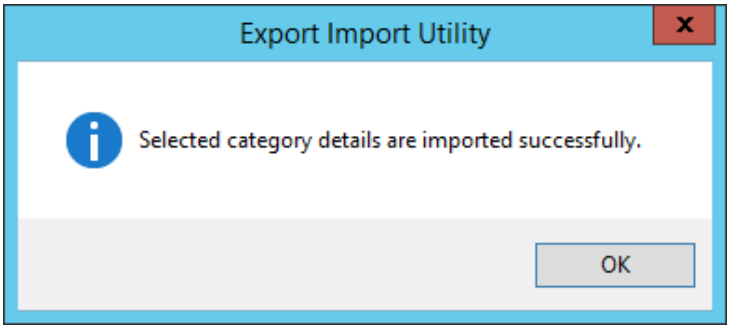


4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



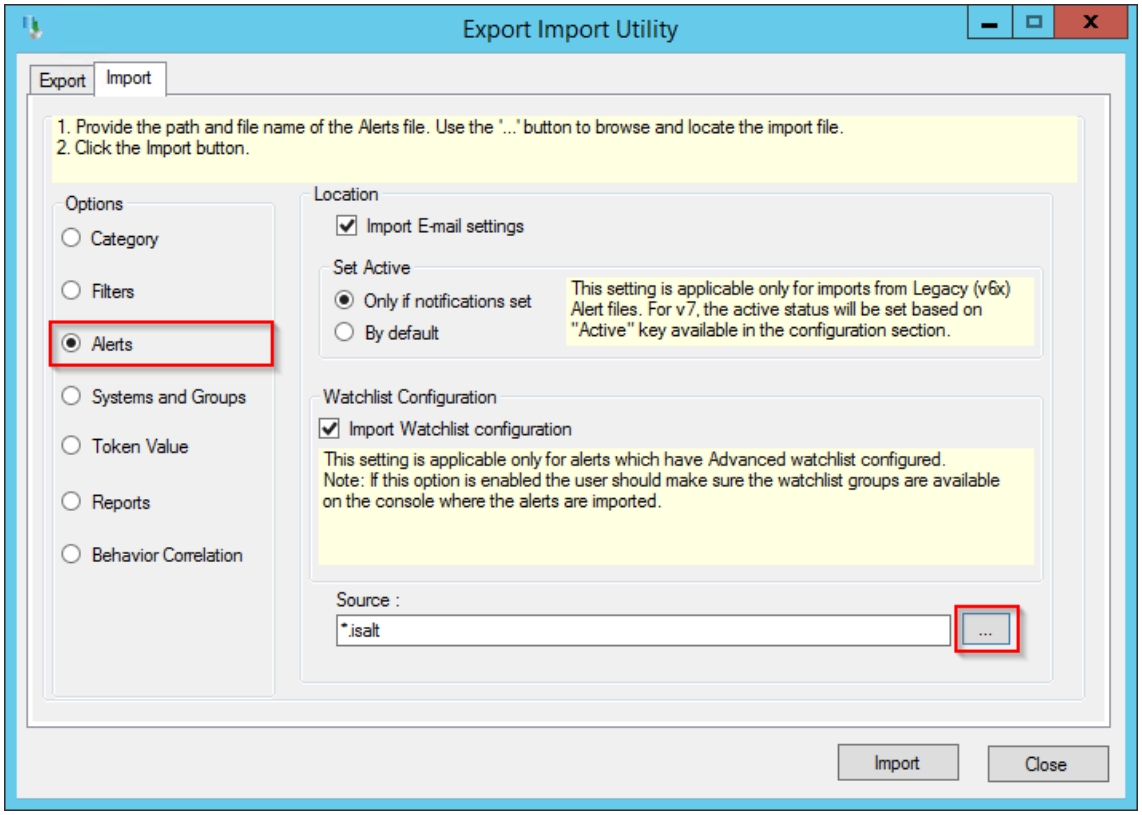
2. In the **Browse** window, locate the **Categories_ Barracuda Sentinel.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



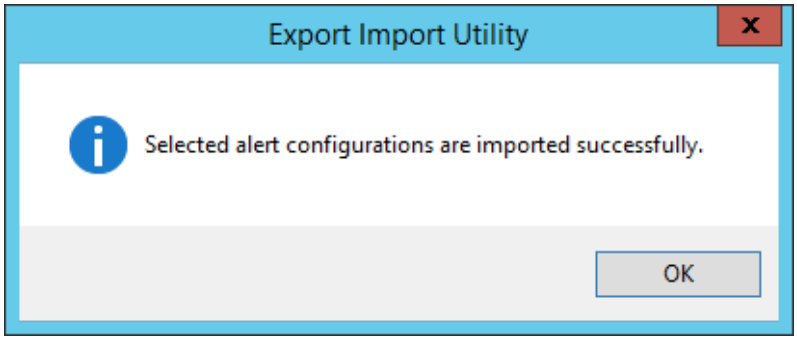
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** button to locate the file.



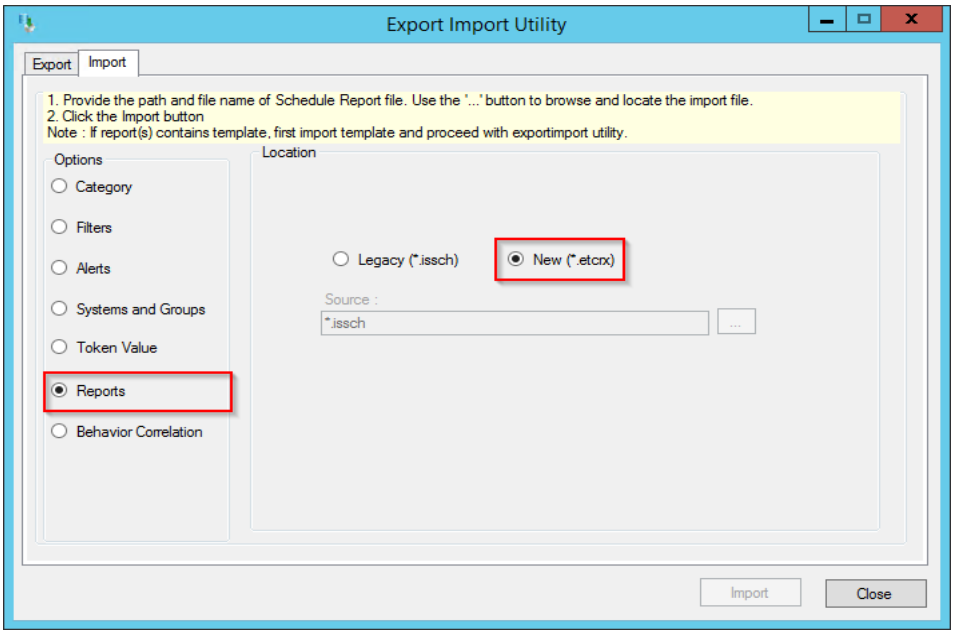
2. In the **Browse** window, locate the **Alerts_ Barracuda Sentinel.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



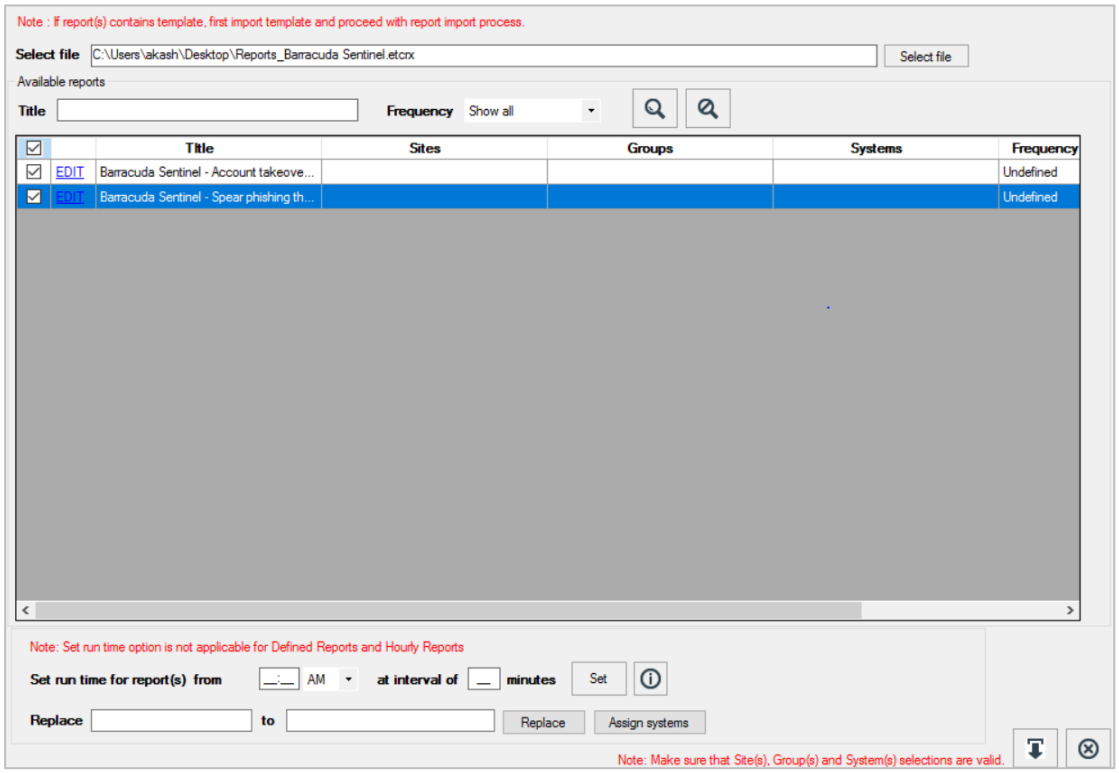
5. Click **OK** or the **Close** button to complete the process.

4.3 Reports

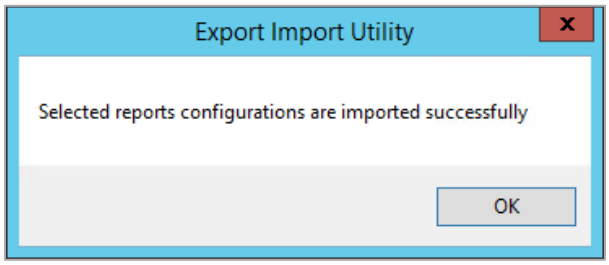
1. In the **Import** tab, click **Reports** and then click **New (*.etcrx)**.



2. In the **Reports Import** window, click **Select file** to locate **Reports_ Barracuda Sentinel.etcrx** file.
3. Select the check box of all the files and click the **Import** button to import the selected files



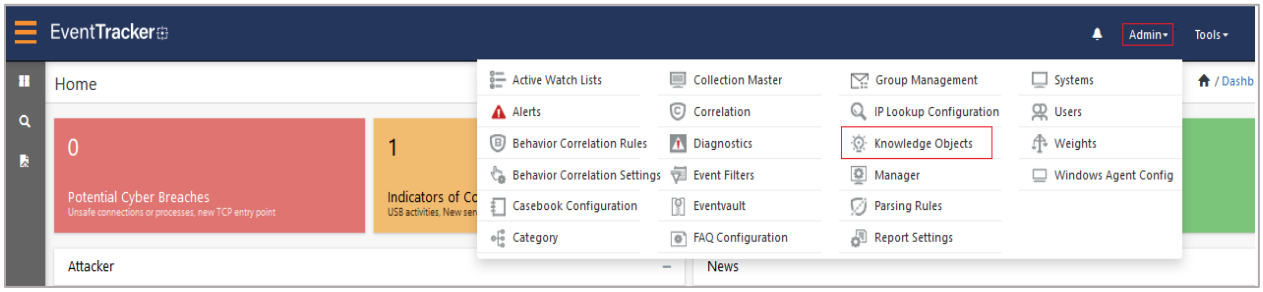
4. EventTracker displays a success message on successful importing of the selected file in **Reports**.



5. Click **OK** or the **Close** button to complete the process.

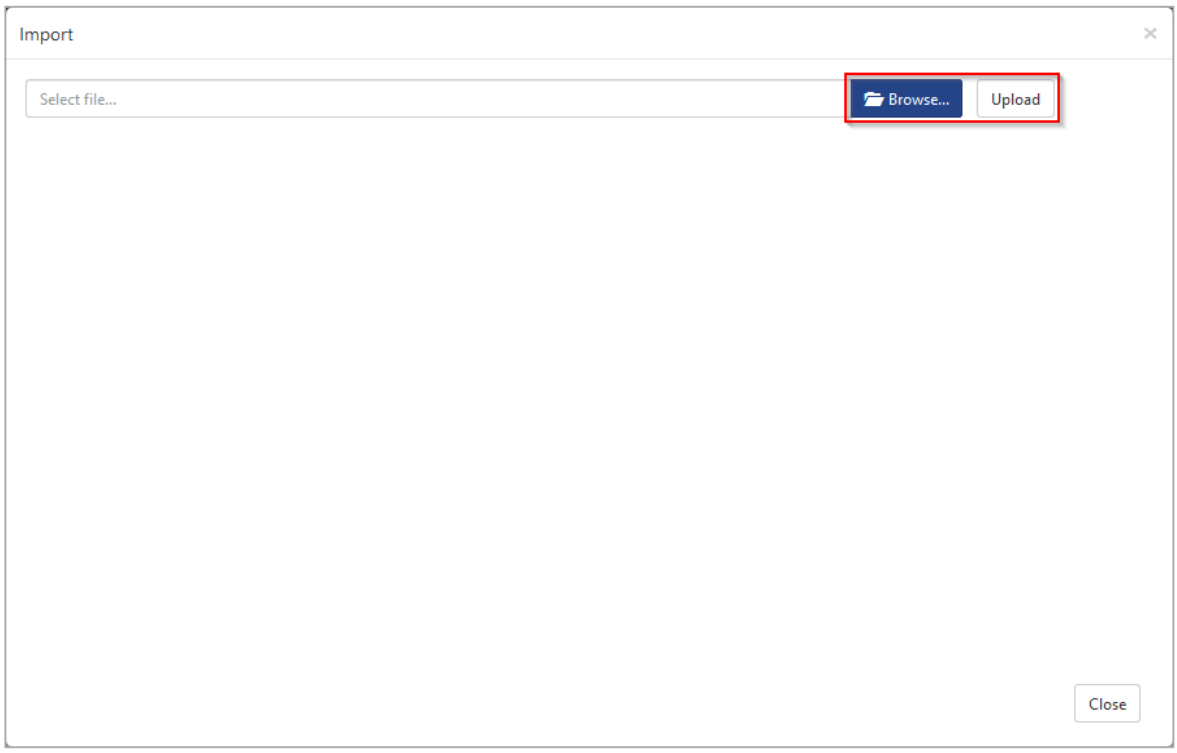
4.4 Knowledge Objects (KO)

1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.

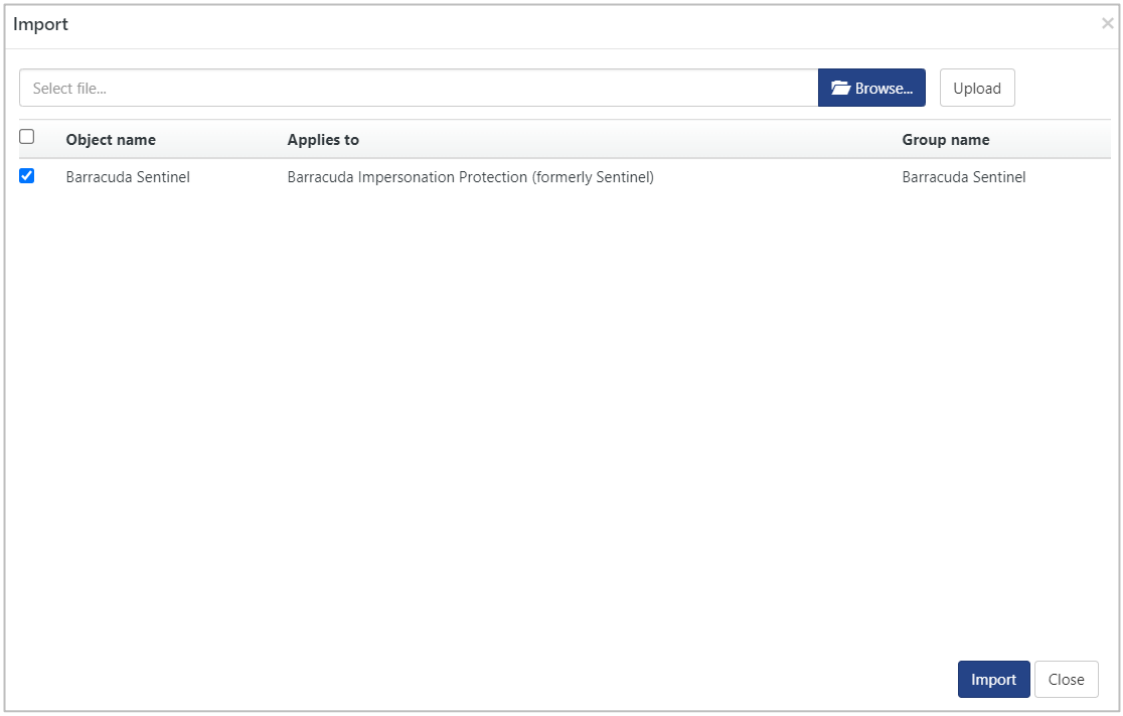


2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.

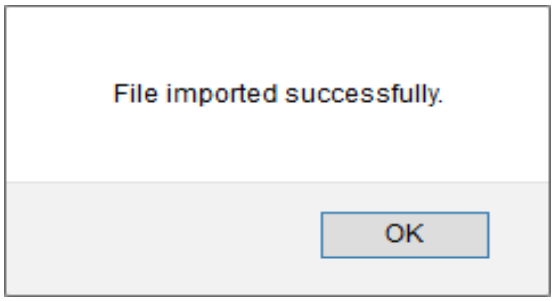
3. In the **Import** window, click **Browse** and locate the **KO_ Barracuda Sentinel.etko** file.



4. Select the check box next to the browsed KO file and then click the **Import** button.



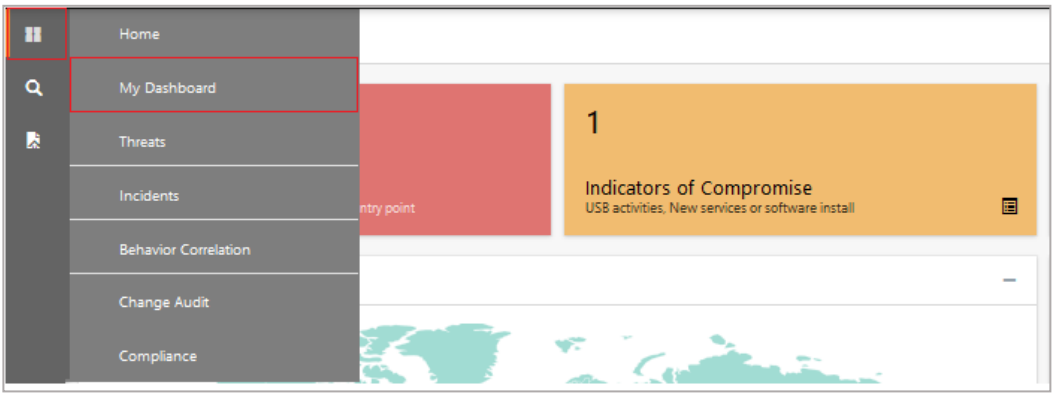
5. EventTracker displays a successful message on successfully importing the selected file in **Knowledge Objects**.



6. Click **OK** or the **Close** button to complete the process.

4.5 Dashboard

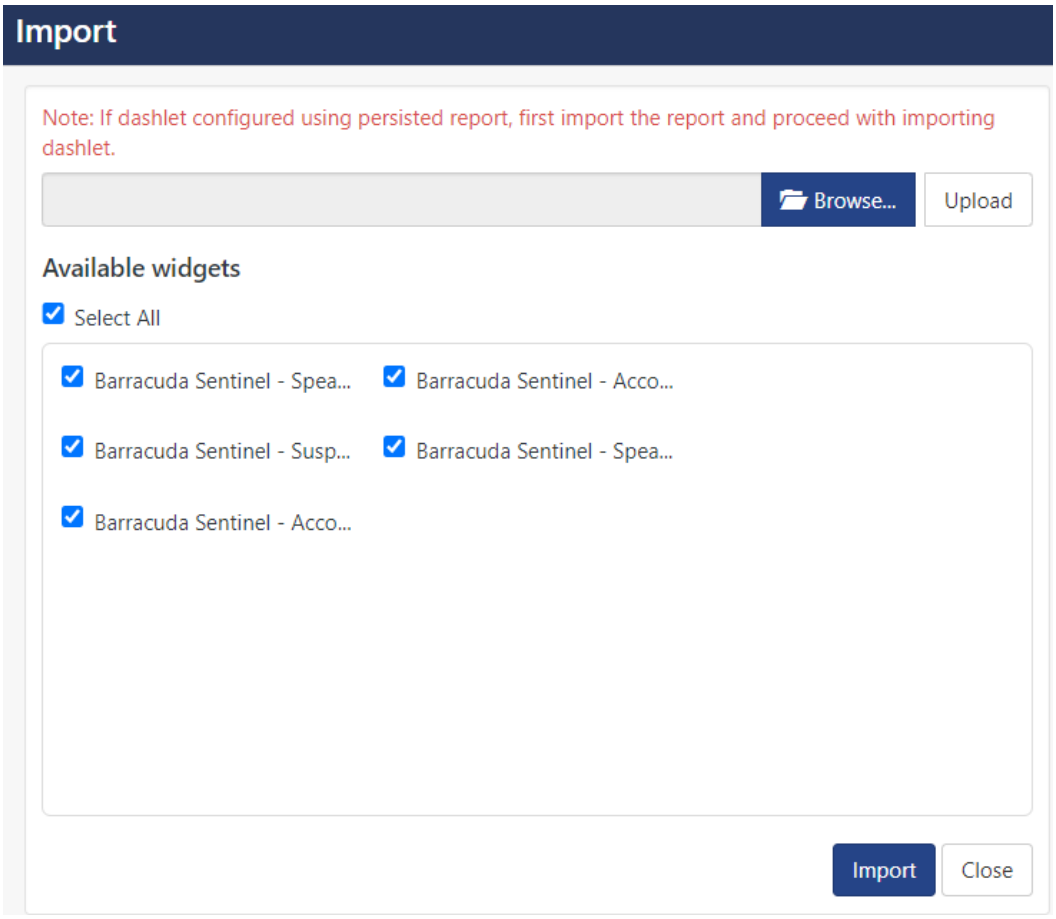
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



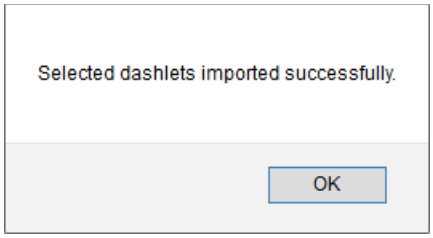
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_ Barracuda Sentinel.etwd** file and then click **Upload.**

4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

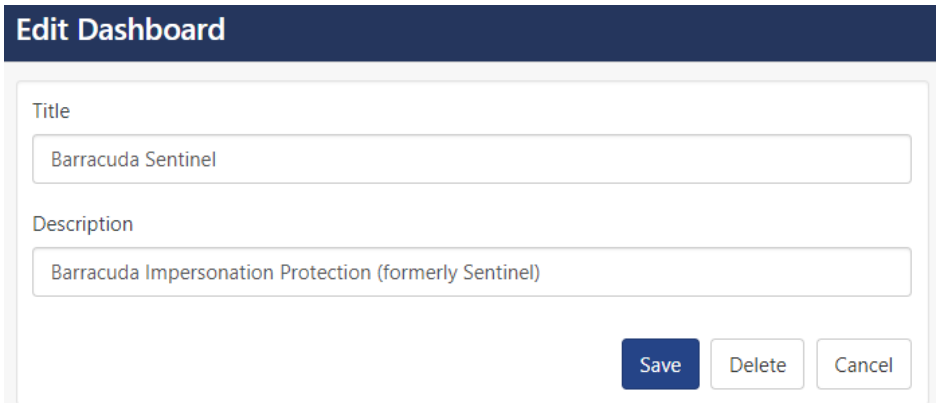


5. EventTracker displays the success message on successful import of the dashlet files.

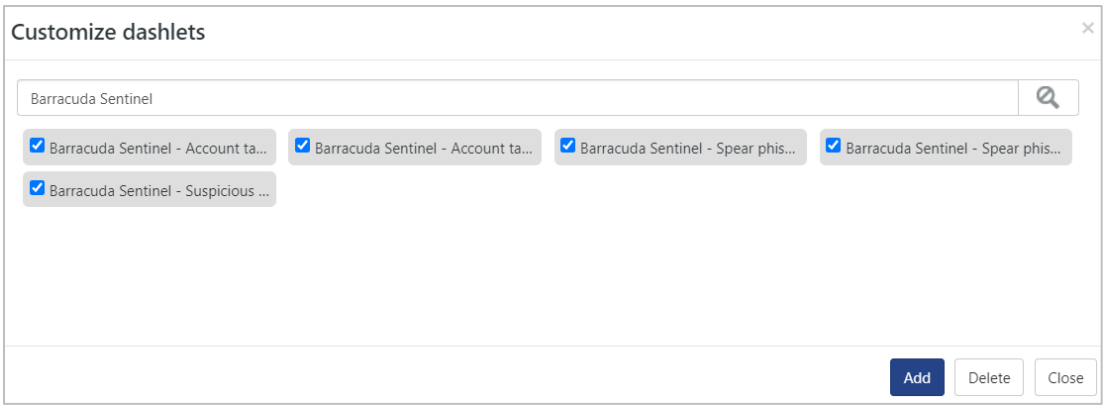


6. Then, in the **My Dashboard** interface click the **Add** ⊕ button to add dashboard.

7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



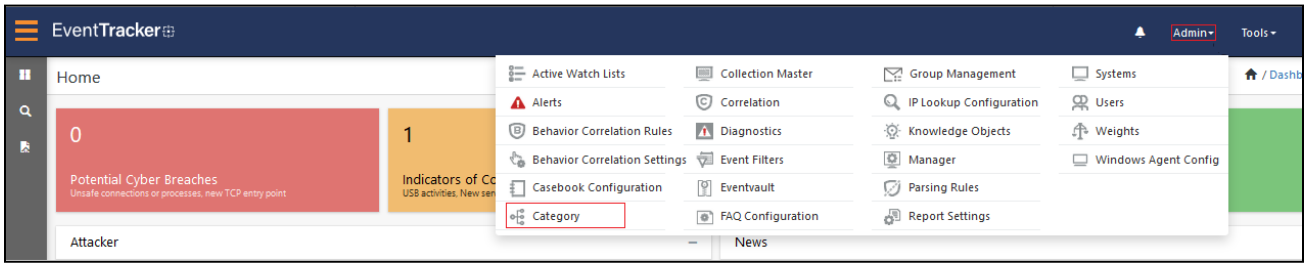
8. From the newly created dashboard interface (for example, **Barracuda Sentinel**), click the **Configuration** button to add the Barracuda Sentinel dashlets.
9. Search and select the newly imported dashlets and click **Add**.



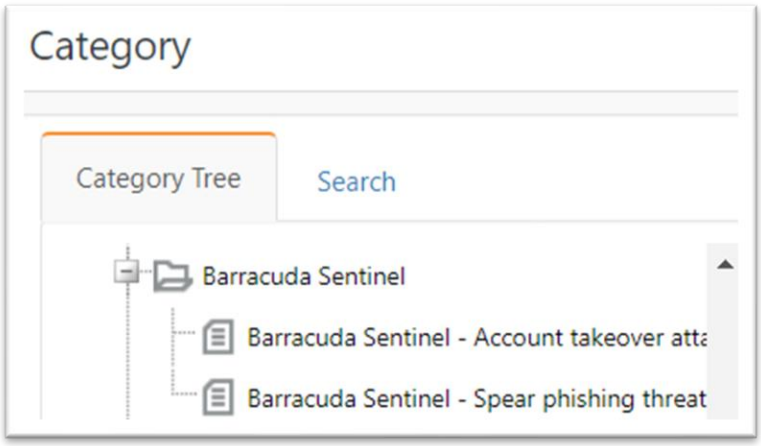
5 Verifying Barracuda Sentinel Knowledge Packs in EventTracker

5.1 Category

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Category**.

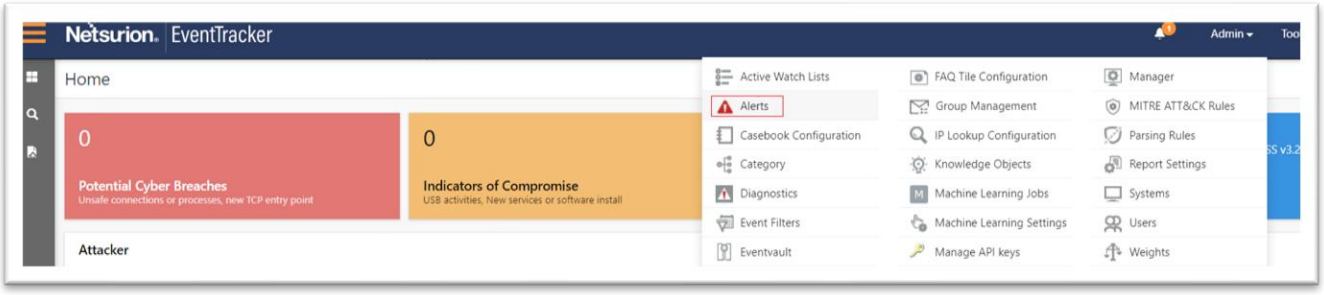


2. In the **Category** interface, under the **Category Tree** tab, click the **Barracuda Sentinel** group folder to expand and see the imported categories.



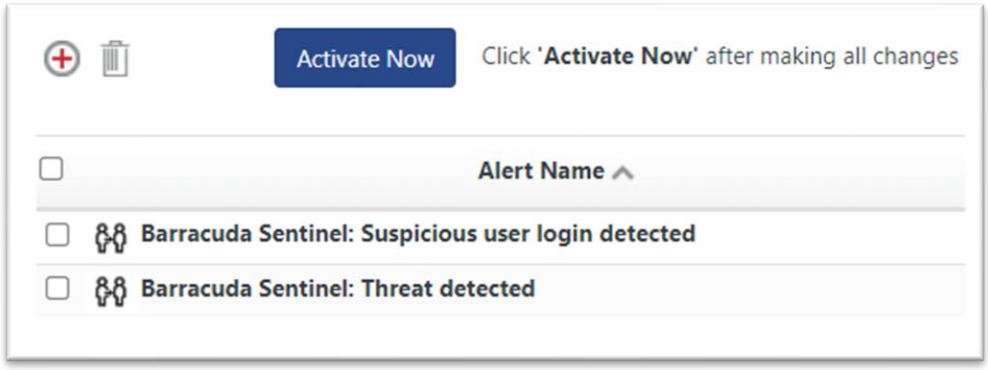
5.2 Alert

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Alerts**.

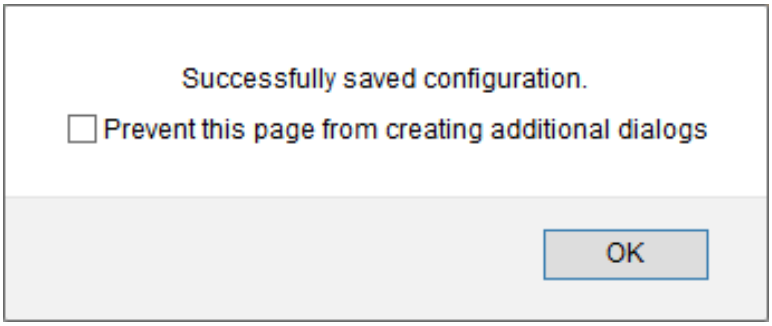


2. In the **Alerts** interface, type **Barracuda Sentinel** in the **Search** field and click the **Search** button.

3. The **Alerts** interface will display all the imported **Barracuda Sentinel** alerts.



4. To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.
5. EventTracker displays a success message on successfully configuring the alerts.



6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

Note

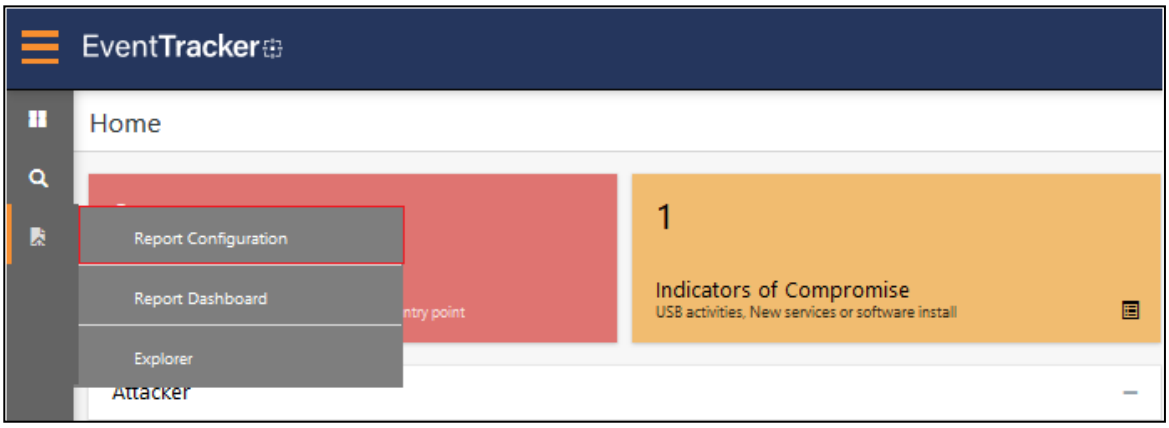
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

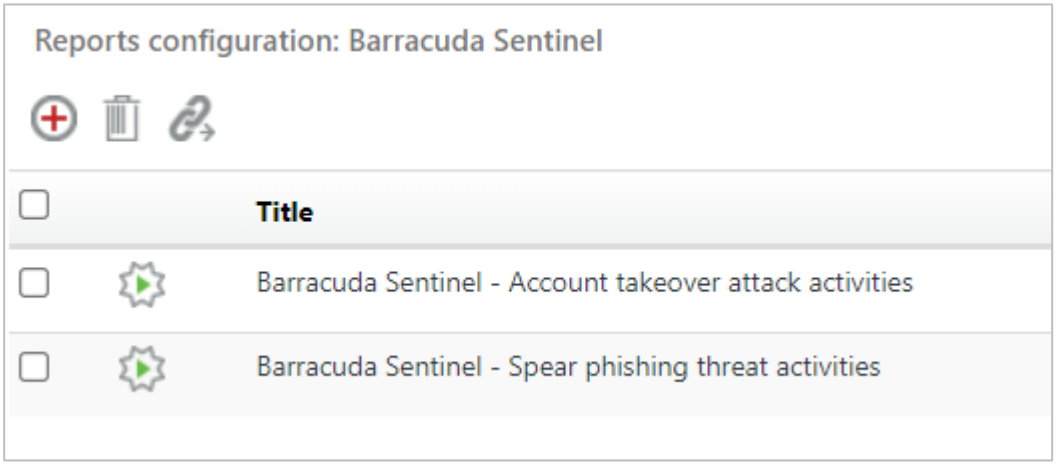
In the **Alert Configuration** interface, specify the appropriate **System** for better performance.

5.3 Reports

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

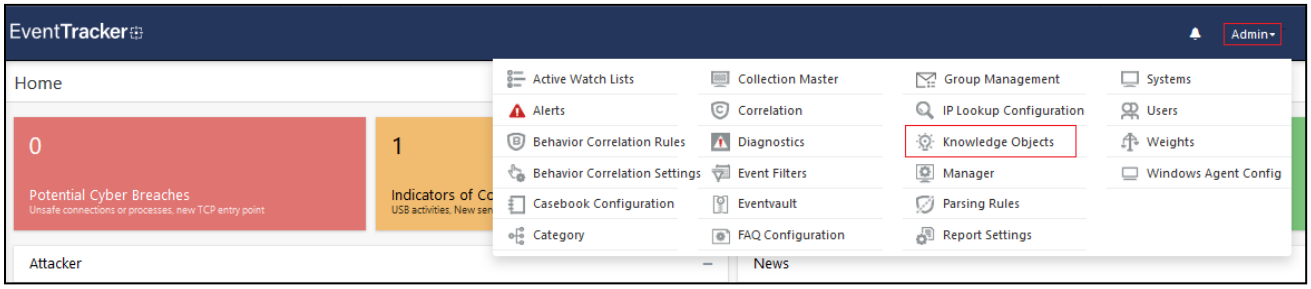


2. In the **Reports Configuration** interface, select the **Defined** option.
3. In the search field, type **Barracuda Sentinel** and click **Search** to search for the Barracuda Sentinel files.
4. EventTracker displays the reports for Barracuda Sentinel.

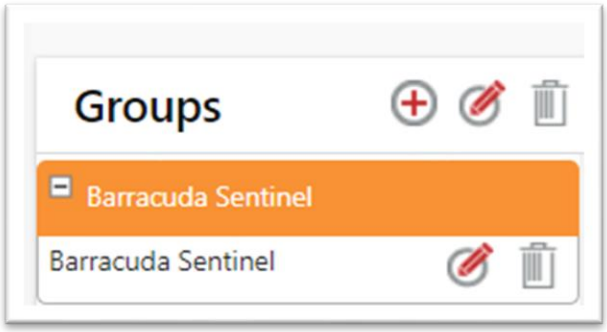


5.4 Knowledge Objects (KO)

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Knowledge Objects.**



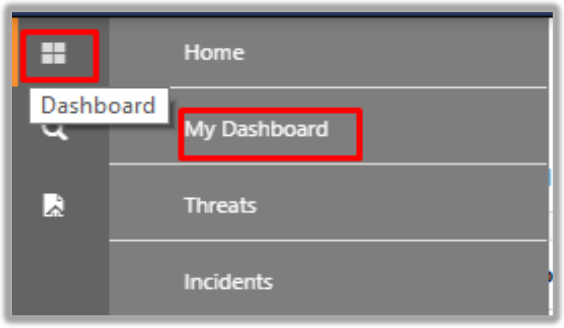
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Barracuda Sentinel** group to expand and view the imported Knowledge objects.



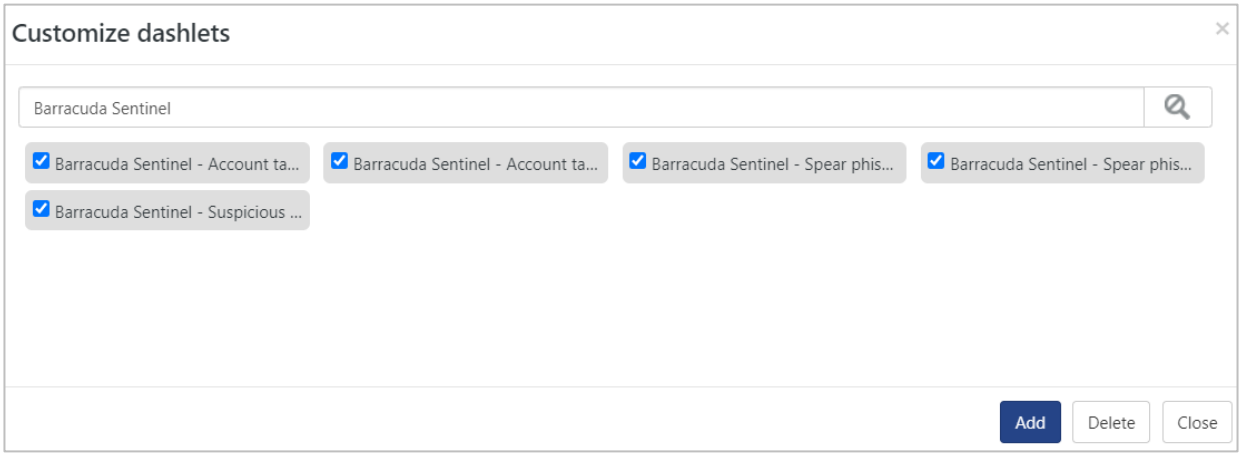
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.5 Dashboard

1. In the **EventTracker** web interface, go to **Home** > **My Dashboard**, and click the **Customize dashlets** button.



2. In the **Customize dashlets** interface, search for **Barracuda Sentinel** in the search field.
3. The following Barracuda Sentinel dashlet files will get displayed.



About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

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 MSPs 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