Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate InQuest with EventTracker

Publication Date:

August 01, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from InQuest. The Knowledge Pack contains alerts, reports, dashboards, categories, and the knowledge object.

Scope

The configuration detailed in this guide is consistent with EventTracker version 9.3 or later and InQuest manager version 3.87.x or later.

Audience

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

Table of Contents

1 Overview

InQuest focuses its analysis on identifying, processing, and inspecting files downloaded over the web or received via email to detect malicious code in transit. In addition to threat detection, InQuest encounters sensitive data in motion like confidential documents and personally identifiable information.

Netsurion facilitates monitoring events retrieved from the InQuest. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking possible attacks, suspicious activities, or any other threat noticed.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure InQuest to forward logs to EventTracker.

> **Note**
>
> Refer to How-To guide to configure InQuest to forward logs to EventTracker.

3 EventTracker Knowledge Packs

Configure categories and reports in EventTracker once the logs are available in EventTracker.

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

3.1 Category

InQuest - C2 engine: This category aids in finding and parsing the logs relevant to risky IP connections and DNS.

InQuest - Malware detection engine: This category aids in finding and parsing the logs related to the detection of potential malware on systems.

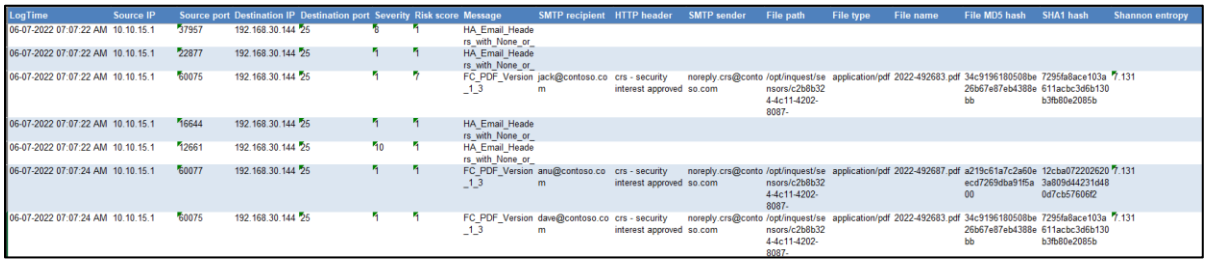
InQuest - Threat detection engine: This category aids in finding and parsing the logs related to risky SMTP transfers and malicious file attachments on emails.

3.2 Alerts

InQuest: Suspicious file detected: This alert gets triggered when the InQuest Malware detection engine detects a suspicious file with a high-risk score and a reasonably high Shannon entropy.

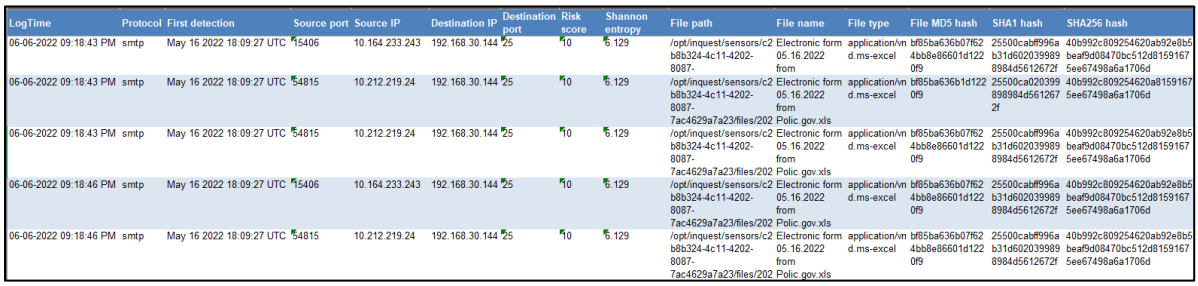
3.3 Reports

InQuest - Potential SMTP threats: This report provides details of emails or SMTP transfers that are potentially risky and may have malicious file attachments.



LogTime	Source IP	Source port	Destination IP	Destination port	Severity	Risk score	Message	SMTP recipient	HTTP header	SMTP sender	File path	File type	File name	File MD5 hash	SHA1 hash	Shannon entropy
06-07-2022 07:07:22 AM	10.10.15.1	57957	192.168.30.144	25	6	1	HA_Email_Headers_with_None_or_									
06-07-2022 07:07:22 AM	10.10.15.1	22877	192.168.30.144	25	1	1	HA_Email_Headers_with_None_or_									
06-07-2022 07:07:22 AM	10.10.15.1	50075	192.168.30.144	25	1	7	FC_PDF_Version_1_3	jack@contoso.com	crs - security interest approved	noreply.crs@contoso.com	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-	application/pdf	2022-492683.pdf	34c9196180508be26b67e87eb4388ebb	7295fa8ace103a611acbc3d6b130b3fb80e2085b	7.131
06-07-2022 07:07:22 AM	10.10.15.1	16644	192.168.30.144	25	1	1	HA_Email_Headers_with_None_or_									
06-07-2022 07:07:22 AM	10.10.15.1	12661	192.168.30.144	25	10	1	HA_Email_Headers_with_None_or_									
06-07-2022 07:07:24 AM	10.10.15.1	50077	192.168.30.144	25	1	1	FC_PDF_Version_1_3	anu@contoso.com	crs - security interest approved	noreply.crs@contoso.com	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-	application/pdf	2022-492687.pdf	a219c61a7c2a60eecd7269dba91f5a00	12cba072202620a809d44231d480d7cb57606f2	7.131
06-07-2022 07:07:24 AM	10.10.15.1	50075	192.168.30.144	25	1	1	FC_PDF_Version_1_3	dave@contoso.com	crs - security interest approved	noreply.crs@contoso.com	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-	application/pdf	2022-492683.pdf	34c9196180508be26b67e87eb4388ebb	7295fa8ace103a611acbc3d6b130b3fb80e2085b	7.131

InQuest - Malware and suspicious files: This report provides details related to potential malware on systems based on the InQuest Malware Detection Engine.



LogTime	Protocol	First detection	Source port	Source IP	Destination IP	Destination port	Risk score	Shannon entropy	File path	File name	File type	File MD5 hash	SHA1 hash	SHA256 hash
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	15406	10.164.233.243	192.168.30.144	25	10	5.129	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-	Electronic form from 05.16.2022	application/vnd.ms-excel	bf85ba636b07f624bb8e86601d1220f9	25500cabff996ab31d602039989 8984d5612672f	40b992c809254620ab92e8b5beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	10	5.129	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-7ac4629a7a23/files/202	Electronic form from 05.16.2022 Polic.gov.xls	application/vnd.ms-excel	bf85ba636b1d1220f9	25500ca020399898984d5612672f	40b992c809254620a8159167 5ee67498a6a1706d
06-06-2022 09:18:43 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	10	5.129	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-7ac4629a7a23/files/202	Electronic form from 05.16.2022 Polic.gov.xls	application/vnd.ms-excel	bf85ba636b07f624bb8e86601d1220f9	25500cabff996ab31d602039989 8984d5612672f	40b992c809254620ab92e8b5beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:46 PM	smtp	May 16 2022 18:09:27 UTC	15406	10.164.233.243	192.168.30.144	25	10	5.129	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-7ac4629a7a23/files/202	Electronic form from 05.16.2022 Polic.gov.xls	application/vnd.ms-excel	bf85ba636b07f624bb8e86601d1220f9	25500cabff996ab31d602039989 8984d5612672f	40b992c809254620ab92e8b5beaf9d08470bc512d8159167 5ee67498a6a1706d
06-06-2022 09:18:46 PM	smtp	May 16 2022 18:09:27 UTC	54815	10.212.219.24	192.168.30.144	25	10	5.129	/opt/inquest/sensors/c2b8b324-4c11-4202-8087-7ac4629a7a23/files/202	Electronic form from 05.16.2022 Polic.gov.xls	application/vnd.ms-excel	bf85ba636b07f624bb8e86601d1220f9	25500cabff996ab31d602039989 8984d5612672f	40b992c809254620ab92e8b5beaf9d08470bc512d8159167 5ee67498a6a1706d

InQuest - C2 engine detections: This report provides details of suspicious detections by the InQuest C2 engine.

LogTime	C2 category	C2 hit	Destination IP	Destination port	Source IP	Source port	Risk score
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53975	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52745	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53393	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56450	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53426	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53521	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56497	10
06-24-2022 04:33:24 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53422	10
06-24-2022 04:33:25 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	10
06-24-2022 04:33:25 AM	C2_IP_Alert	192.168.98.124	192.168.30.114	22	192.168.98.14	16869	10
06-24-2022 04:33:25 AM	C2_IP_Alert	192.168.98.124	192.168.30.118	22	192.168.98.12	33772	10
06-24-2022 04:33:25 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52835	9
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	56457	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	53336	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	54132	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	55970	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	10.191.99.254	53	10.191.98.67	52805	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	10
06-24-2022 04:33:26 AM	C2_DNS_Alert	contoso.com	8.8.8.8	53	10.191.98.66	2891	10

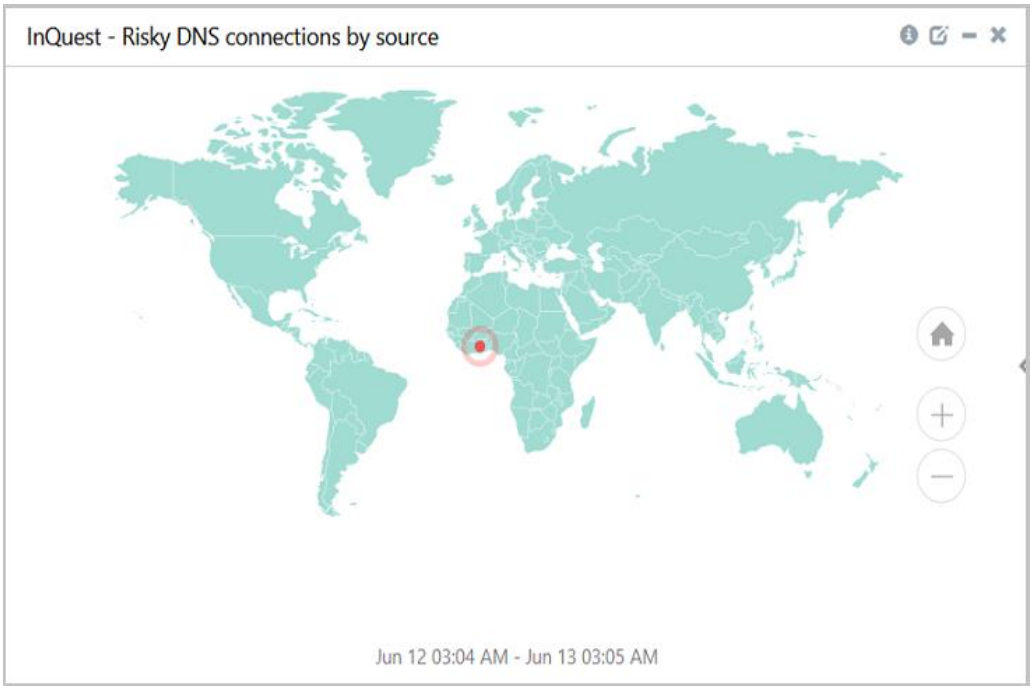
3.4 Dashboard

InQuest - Threats by geolocation: This dashlet displays the details of the active threat detected by InQuest based on the geolocation.

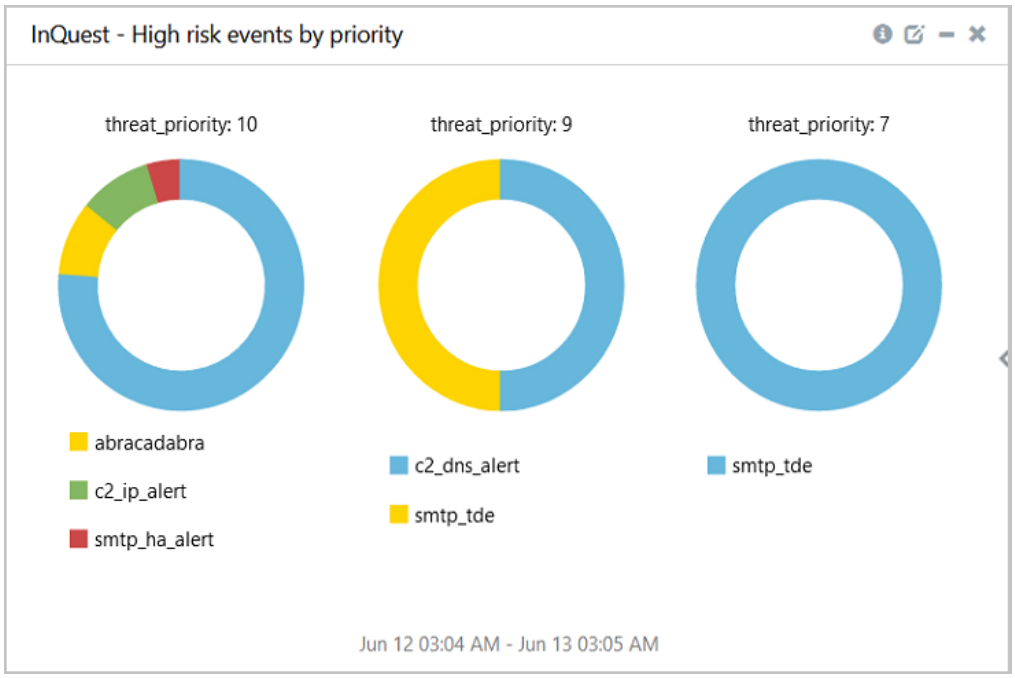
InQuest - Risky DNS connections by source: This dashlet displays the log information for risky DNS connections based on the Shannon entropy risk score.

Note

The higher the risk score, the higher the risk associated with a particular DNS connection.



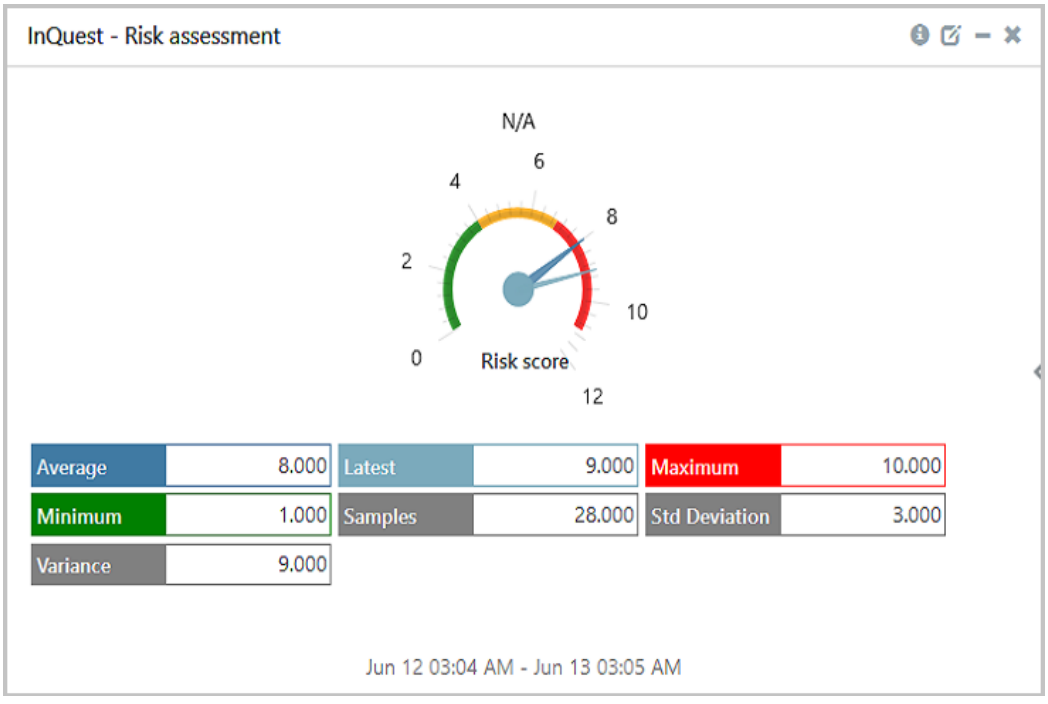
InQuest - High risk events by priority: This dashlet displays the high-risk alert details detected by the malware detection engine.



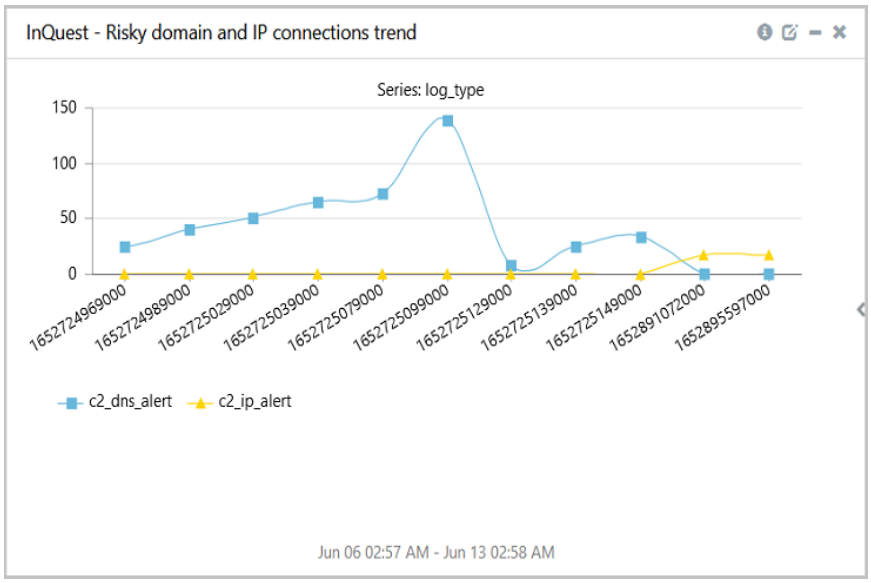
InQuest - Risk assessment: This dashlet displays the average risk score of all the alerts associated with InQuest. The **Average** displays the average risk score of all the alerts, and the **Latest** displays the current risk score of the latest alert.

Note

A risk score above 8 must be reported.



InQuest - Risky domain and IP connections trend: This dashlet displays the risk status of the DNS and the IP alert traffic.

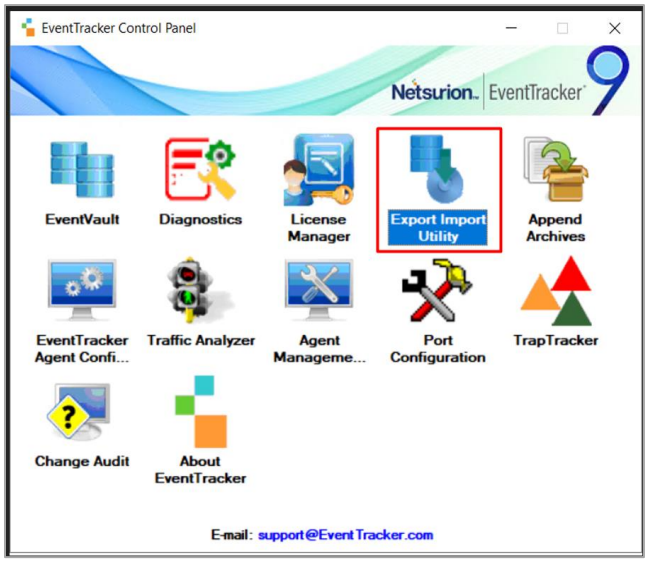


4 Importing InQuest Knowledge Packs into EventTracker

Import the InQuest Knowledge Pack items in the following sequence.

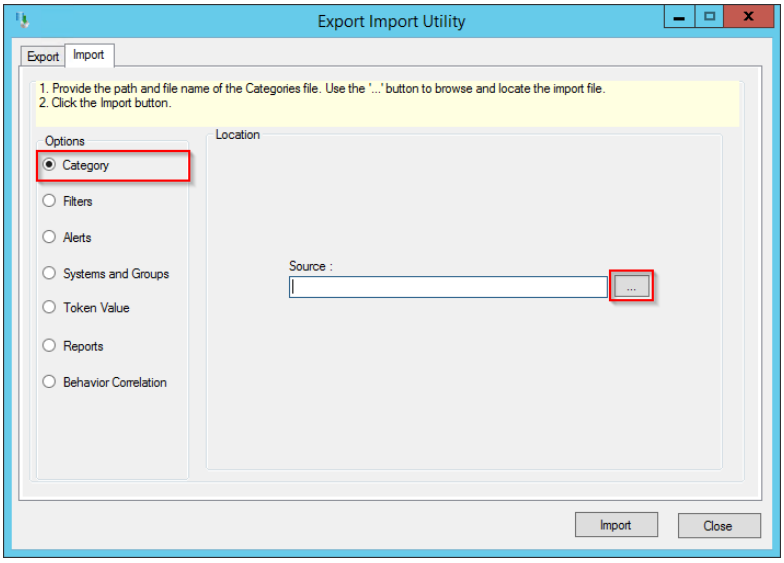
- Category
- Alerts
- Reports and templates
- Knowledge Objects
- Dashboards

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



4.1 Category

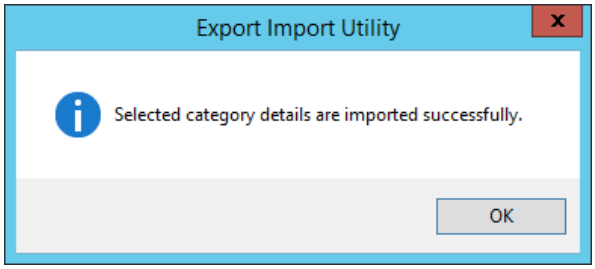
1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



2. In the **Browse** window, locate the **Categories_InQuest.iscat** file and click **Open**.

3. To import the categories, click **Import**.

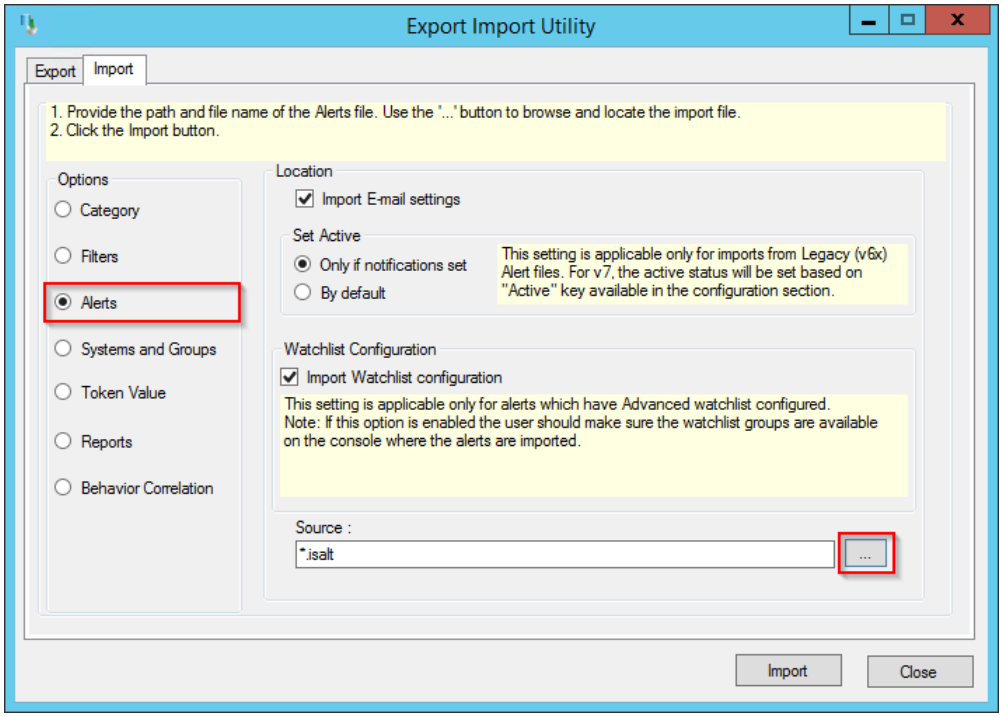
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



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

4.2 Alerts

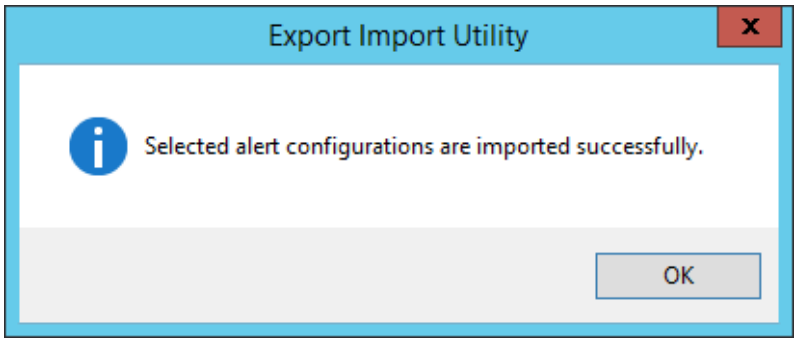
1. In the **Import** tab, click **Alerts**, and then click the **Browse** button to locate the file.



2. In the **Browse** window, locate the **Alerts_InQuest.isalt** file, and then click **Open**.

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

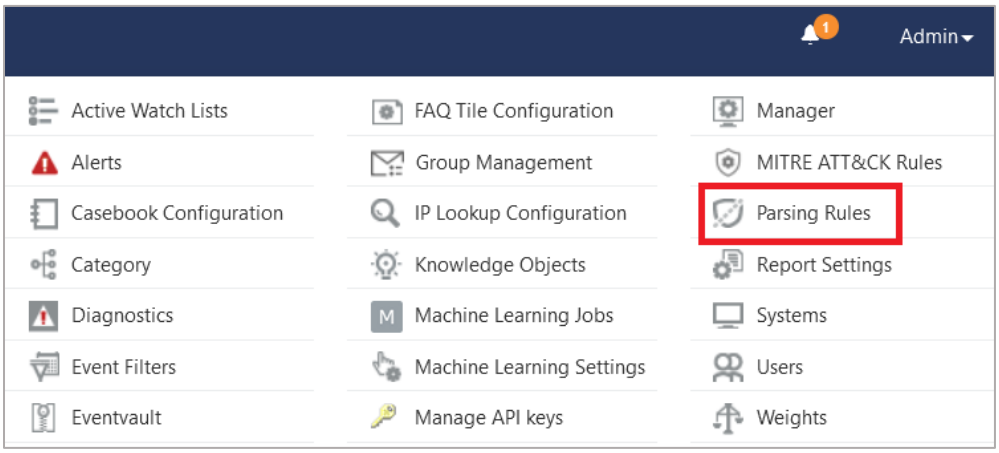
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



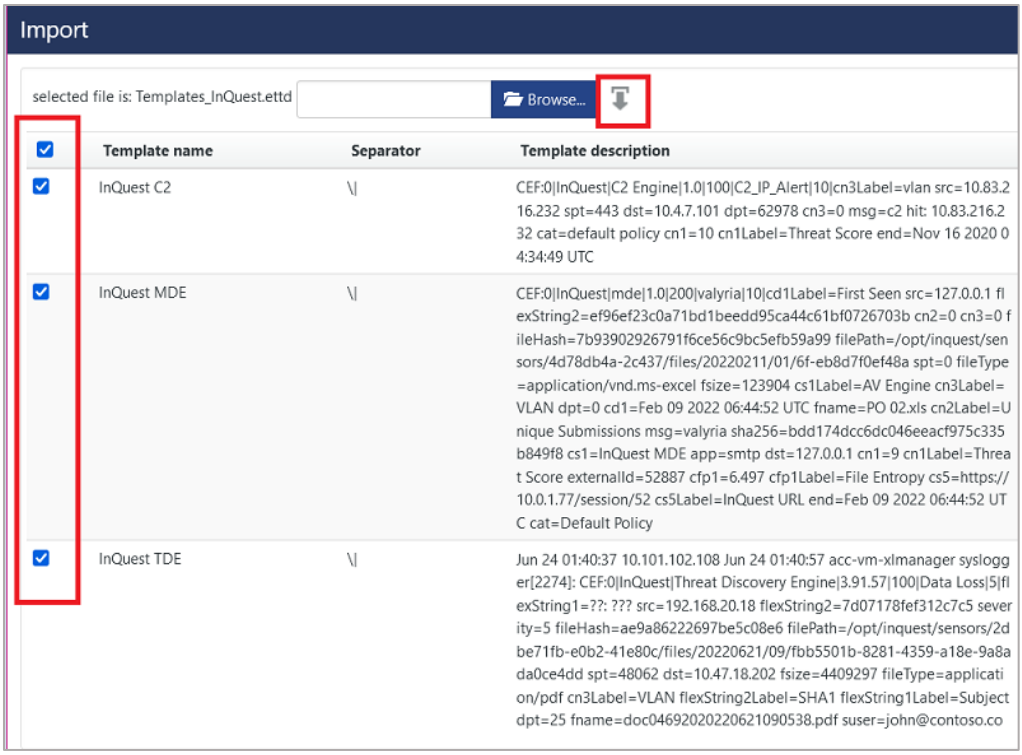
5. Click **OK** or the **Close** button to complete the process.

4.3 Token Template

1. In the **EventTracker Web** interface, hover over the **Admin** menu and click **Parsing Rules**.



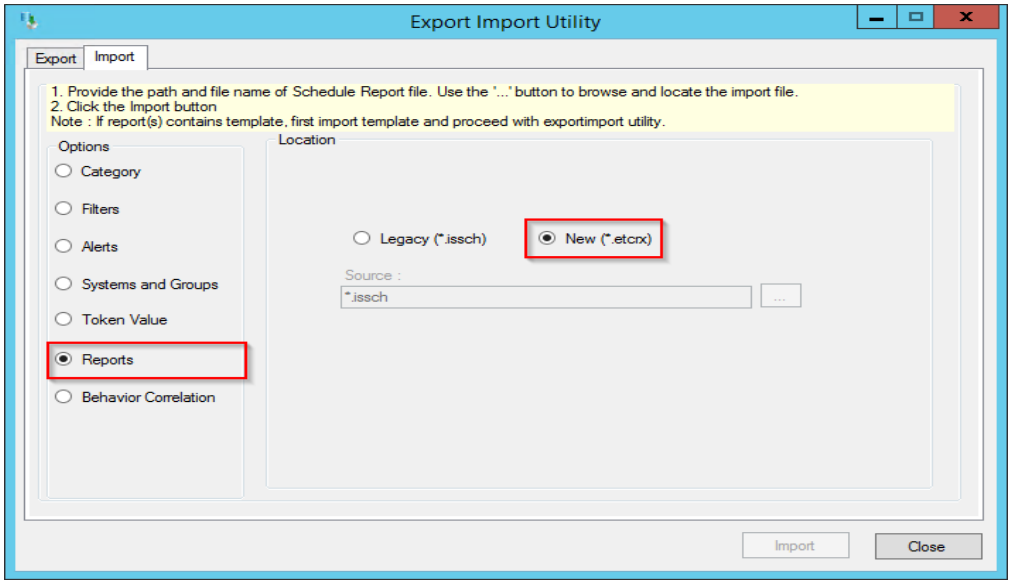
2. In the **Parsing Rules** interface, click the **Template** tab and then click the **Import Configuration** button**.**
3. In the **Import** window, click **Browse** to search and locate for the **Templates_InQuest.ettd** file.
4. It takes few seconds to load the templates and once you see the list of templates, select the appropriate templates, and click **Import**.



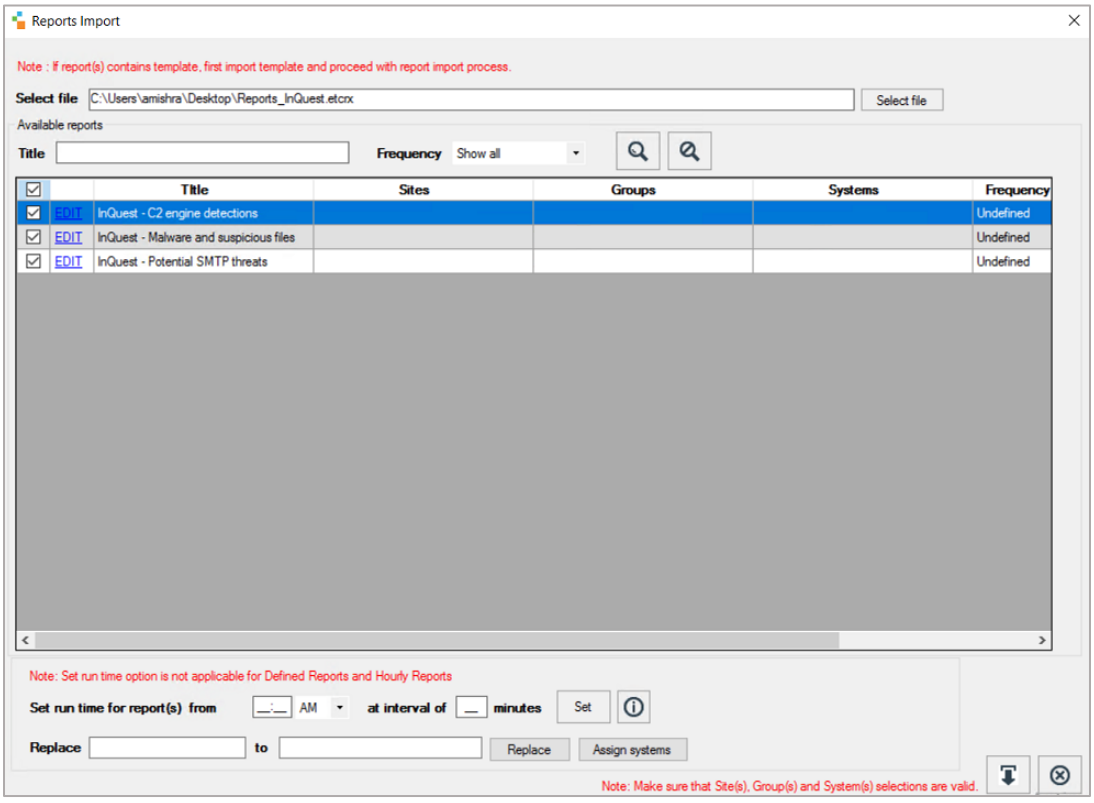
5. EventTracker displays a success message on successfully importing the selected file in **Template**.

4.4 Reports

1. In the **EventTracker Control Panel** > **Export-Import Utility** > **Import** tab, click **Reports**, and then click **New (*.etcrx)**.

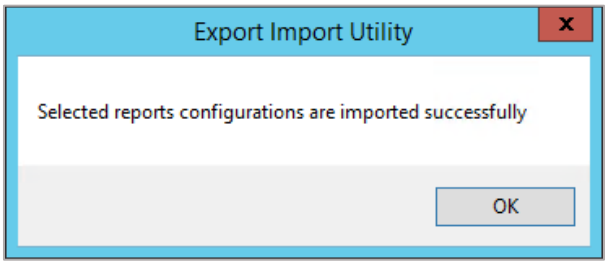


2. In the **Reports Import** window, click **Select file** to locate the **Reports_InQuest.etcrx** file.



3. Select the check box of all the files and click the **Import** button to import the selected files.

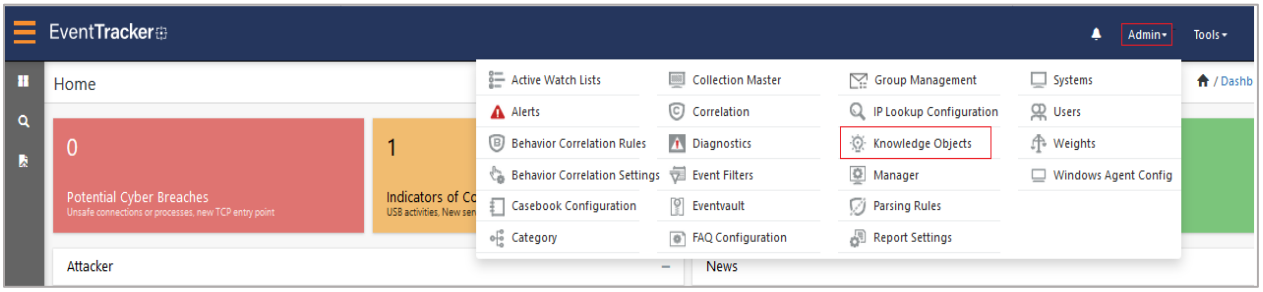
4. EventTracker displays a success message on successful importing of the selected files in **Reports.**



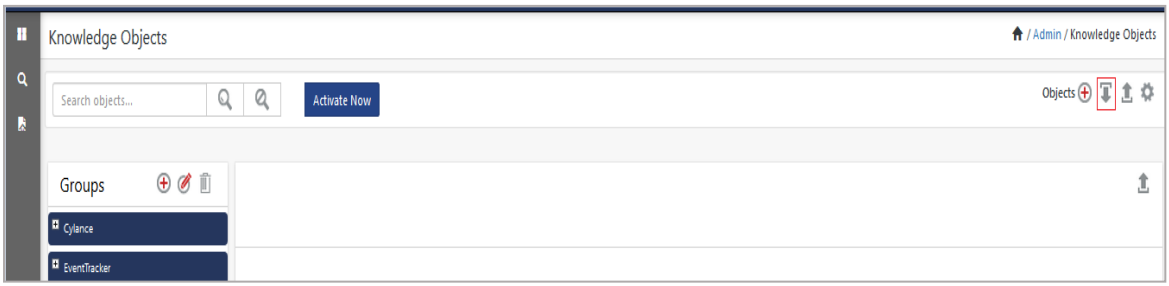
5. Click **OK** or the **Close** button to complete the process.

4.5 Knowledge Objects (KO)

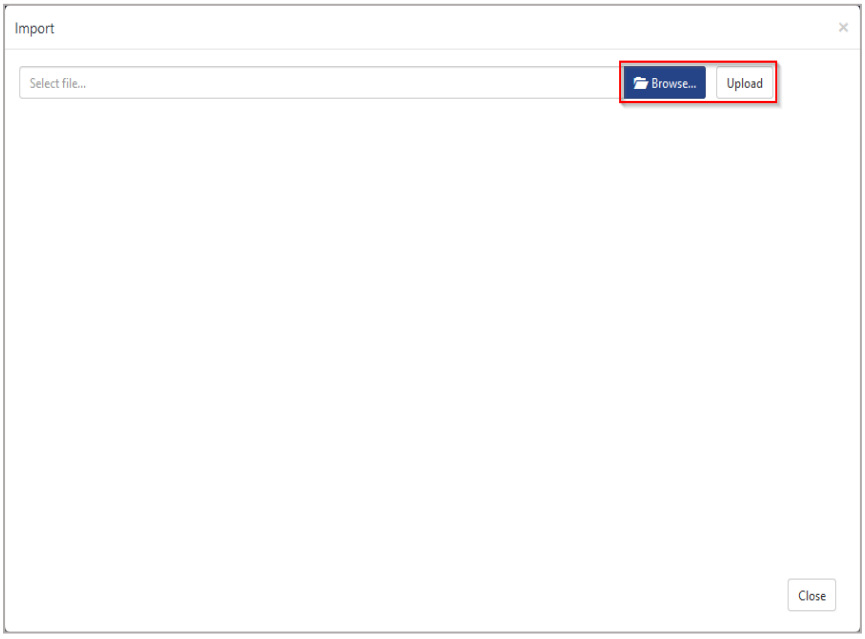
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



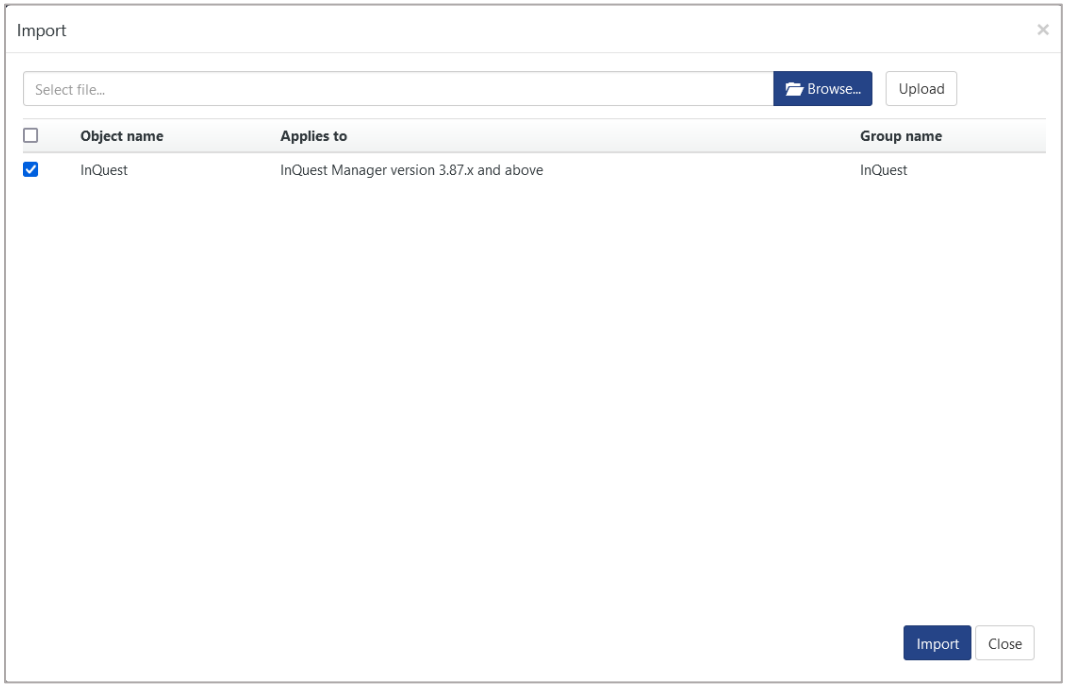
2. In the **Knowledge Objects** interface, click the **Import** button as shown in the below image.



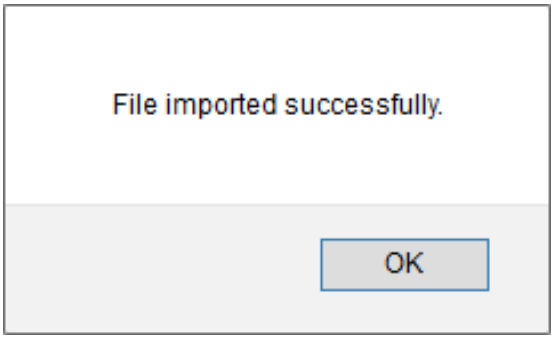
3. In the **Import** window, click **Browse** and locate the **KO_InQuest.etko** file.



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

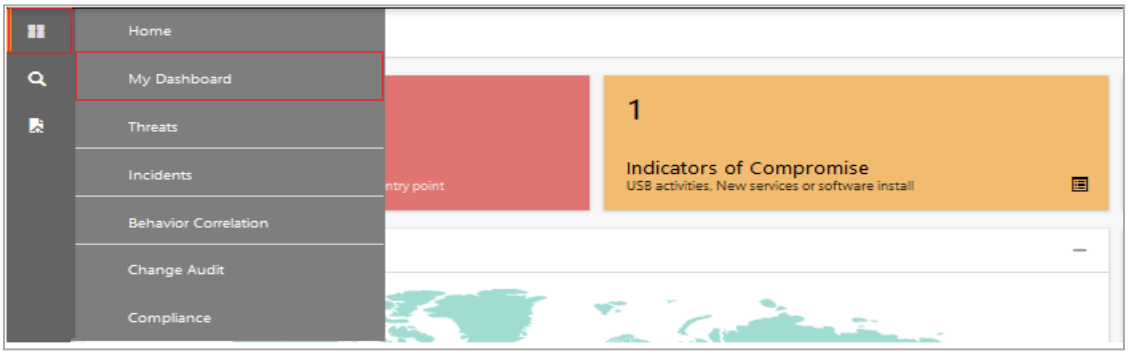


5. EventTracker displays a success message on successfully importing the selected file in **Knowledge Objects**.



4.6 Dashboard

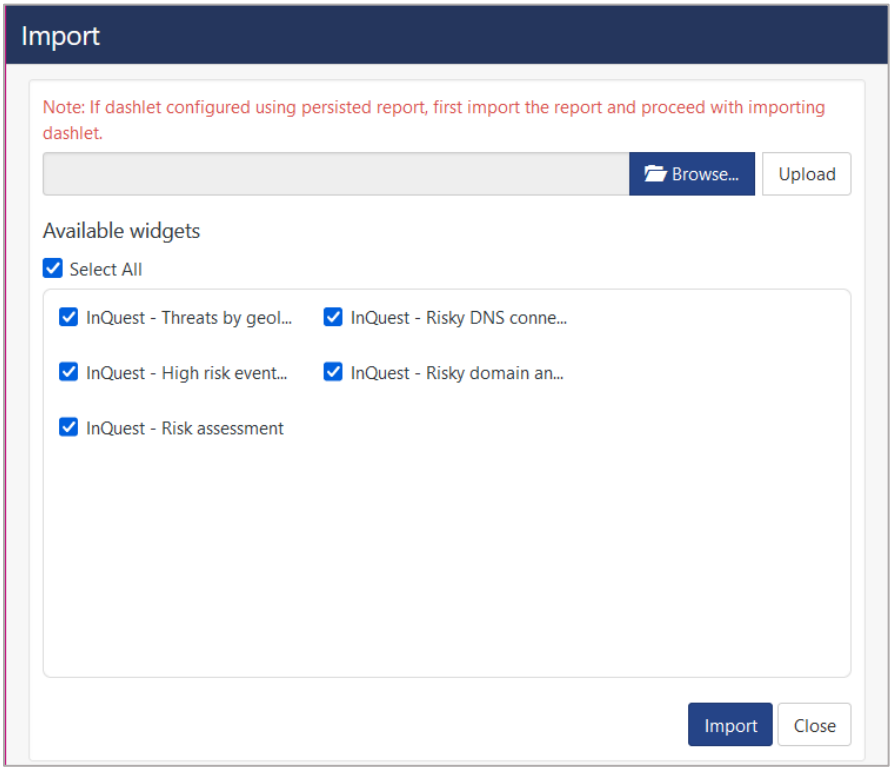
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



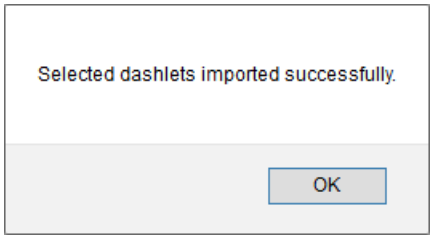
2. In the **My Dashboard** interface, click the **Import** button to import the InQuest files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_InQuest.etwd** dashboard file, and then click **Upload**.

4. Select the **Select All** checkbox for all the dashlet files and click **Import** to import the InQuest dashlet files.

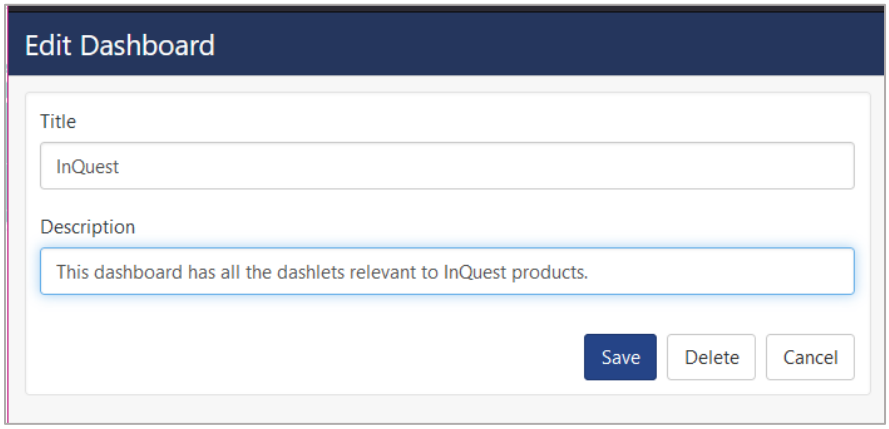


5. The EventTracker displays a success message on successful import of the dashlet files.

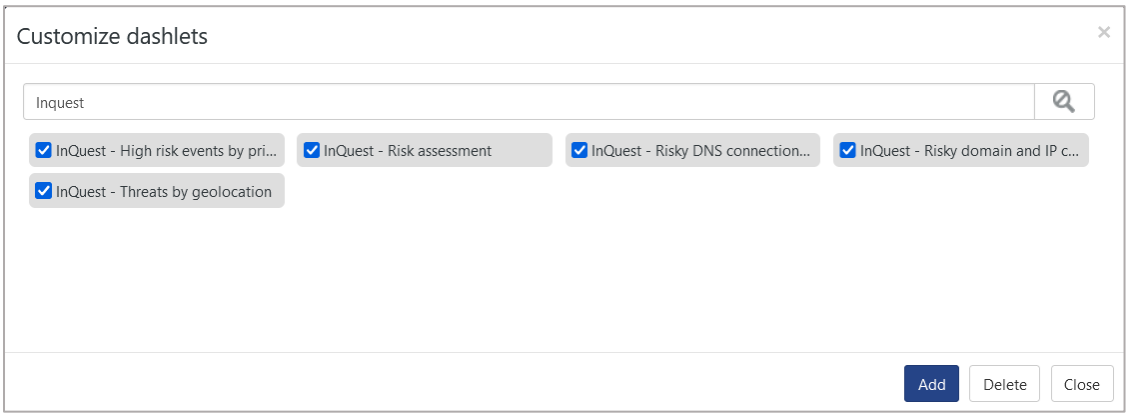


6. Then, in the **My Dashboard** interface, click the **Add** button to add the dashboard.

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



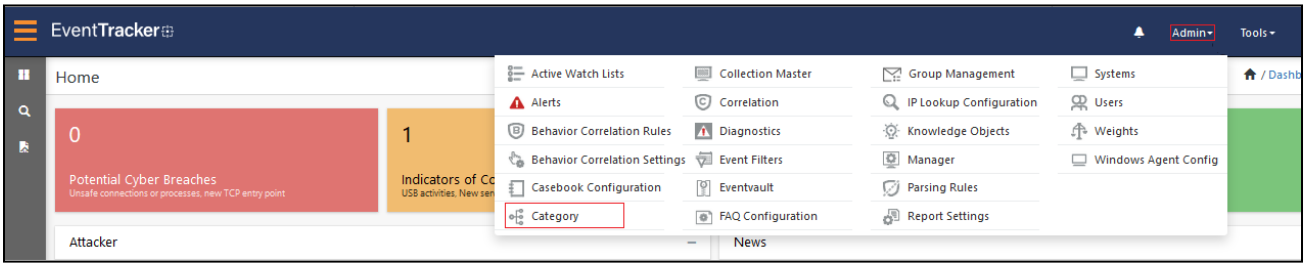
8. From the newly created dashboard interface (for example, **InQuest**), click the **Configuration** button to add the InQuest dashlets.
9. Search and select the newly imported dashlets and click **Add**.



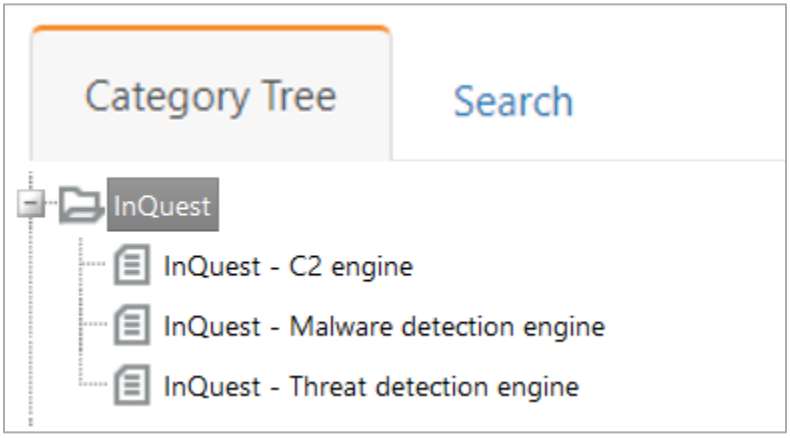
5 Verifying InQuest Knowledge Packs in EventTracker

5.1 Category

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

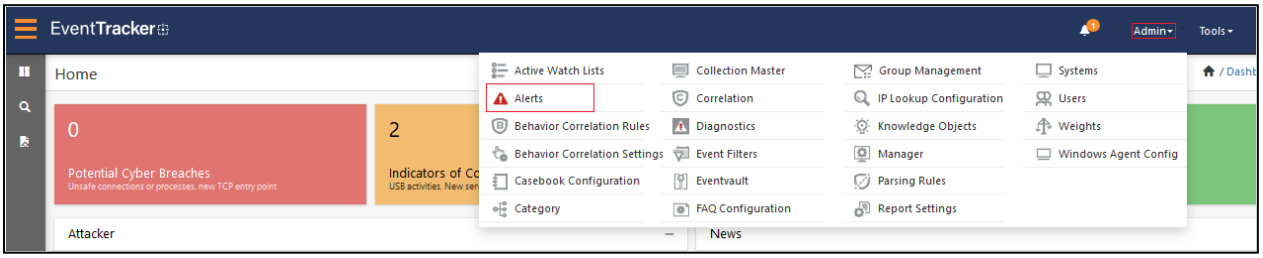


2. In the **Category** interface, under the **Category Tree** tab, click the **InQuest** group folder to expand and see the imported categories.



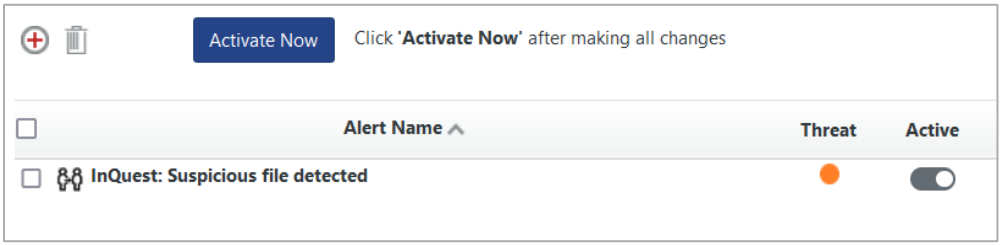
5.2 Alerts

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

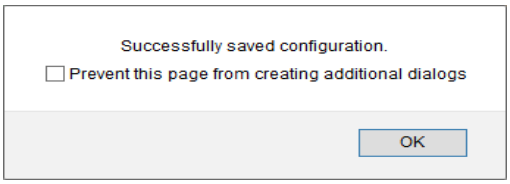


2. In the **Alerts** interface, type **InQuest** in the search field, and click the **Search** button.

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



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



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

Note

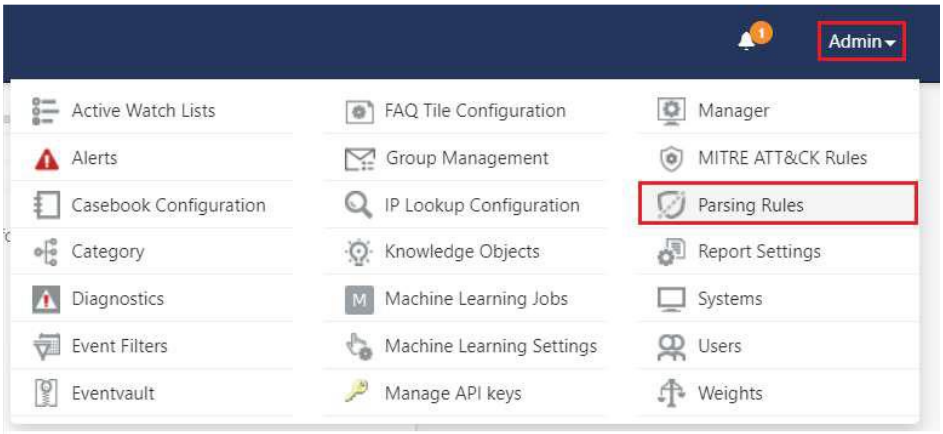
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In **Alert configuration** interface, select the appropriate **System** name for better performance.

5.3 Token Template

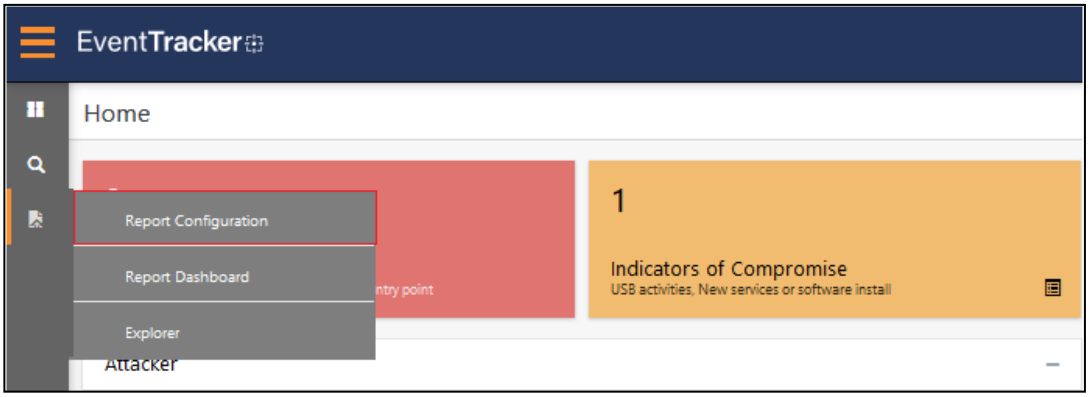
1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Parsing Rules.**



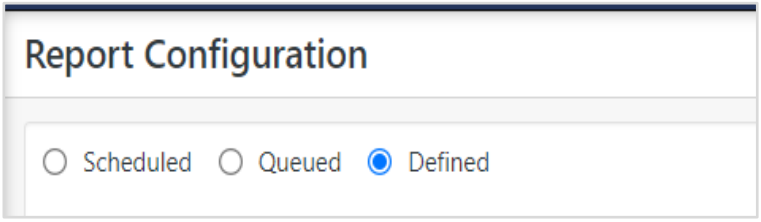
2. Go to the **Template** tab and click the **InQuest** group folder to view the imported Token template.

5.4 Reports

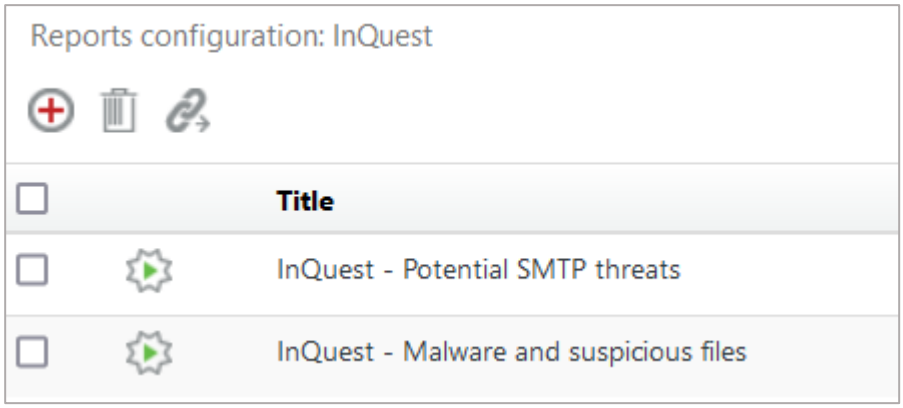
1. In the **EventTracker** web interface, click the **Reports** menu, and then click **Report Configuration**.



2. In the **Report Configuration** interface, click **Defined**.

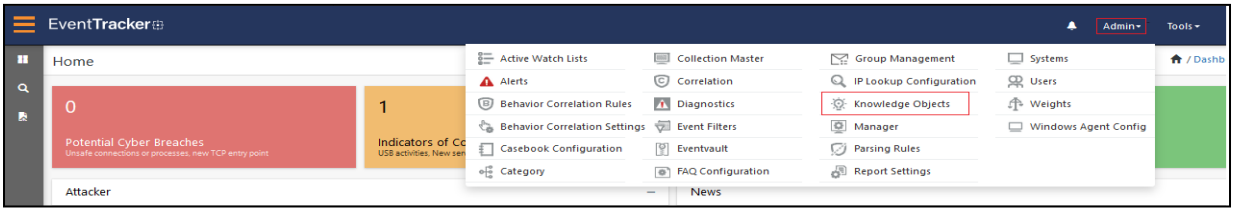


3. In the search field, type **InQuest** and click **Search** to search for the InQuest files.
4. EventTracker displays the reports for InQuest.



5.5 Knowledge Objects (KO)

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

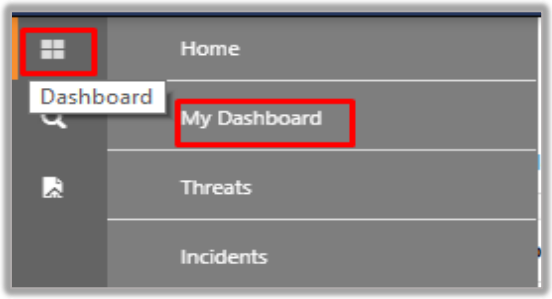


2. In the **Knowledge Object** interface, under **Groups** tree, expand the **InQuest** group to view the imported Knowledge objects.

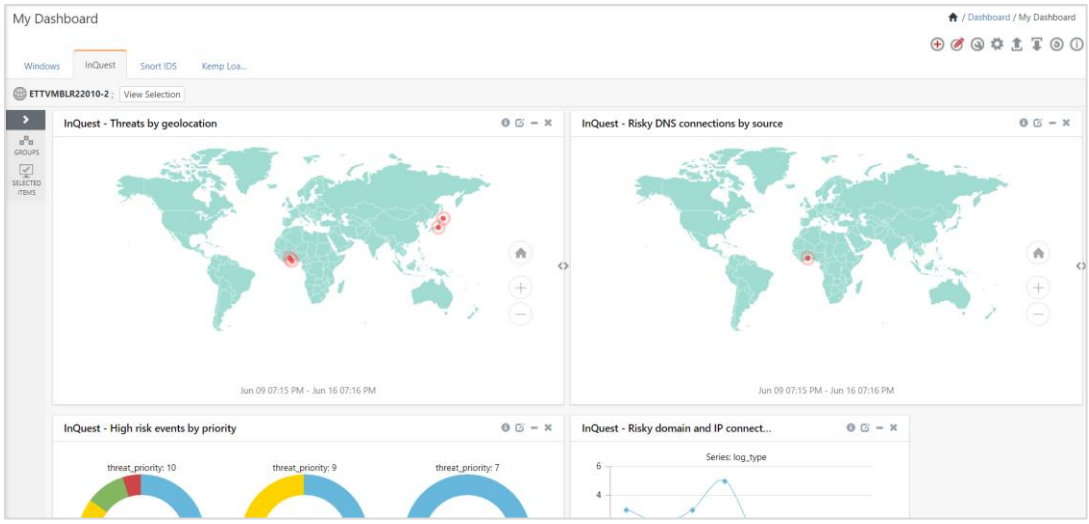
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.6 Dashboard

1. In the **EventTracker** web interface, go to **Home** > **My Dashboard**.



2. The **My Dashboard** interface displays all the dashlets related to **InQuest.**



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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.

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