Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating DarkTrace Intrusion Detection System (IDS)

EventTracker v9.x and above

Publication Date:

August 3, 2021

Abstract

This guide provides instructions to configure DarkTrace IDS to generate logs for critical events. After EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor networks and systems.

Scope

The configuration details in this guide are consistent with EventTracker version 8.x and later, and DarkTrace IDS.

Audience

Administrators who are assigned the task to monitor DarkTrace IDS events using EventTracker.

Table of Contents

1. Overview

DarkTrace Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator.

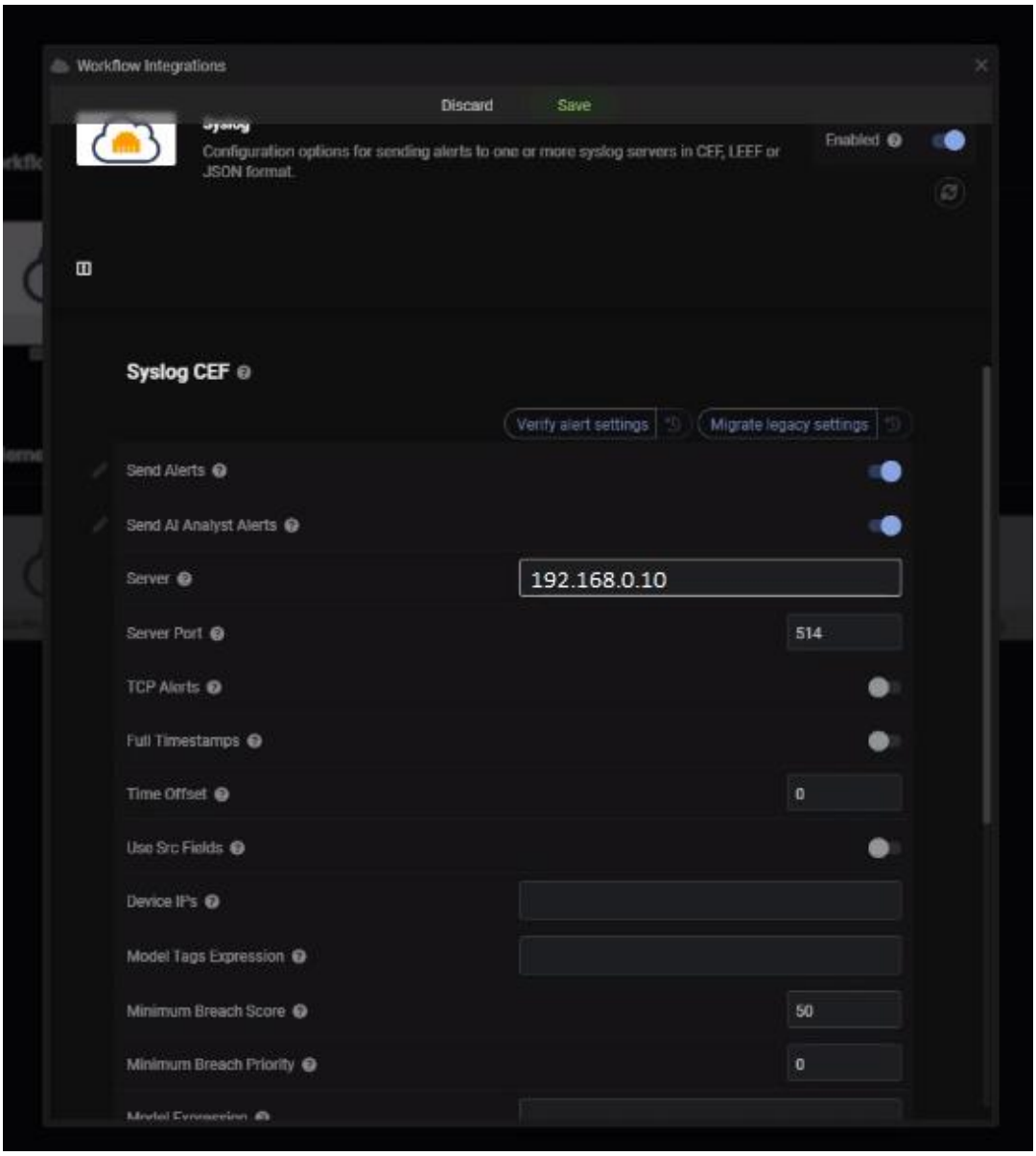
DarkTrace IDS can be integrated with EventTracker using syslog. With the help of DarkTrace IDS KP items, we can monitor the intrusion happening inside the network and trigger the alert whenever any high server intrusion is detected. EventTracker dashboard will help you to view the intrusion happening inside the network by its source IP address as well as based on categories. It can even create the report which helps to collect intrusion happening on the network on time bases which assist you to review the intrusion. EventTracker CIM will help you to correlate the intrusion with other log sources like firewall, OS events, etc.

2. Prerequisites

- EventTracker v9.x or above should be installed.
- **DarkTrace IDS** V3.0.10 or latest version should be installed.

3. Configuring DarkTrace IDS Syslog

1. Within the Threat Visualizer, navigate to the **System Config** page in the main menu under **Admin**.
2. From the left-hand menu, select **Modules** and choose **syslog** from the available **Workflow Integrations**.
3. A configuration window will open. Select the relevant form of syslog - here, syslog CEF - and click **New** to reveal the configuration settings.



4. Complete the **Server** location and optionally modify the communication port. Ensure that the port selected is allowed by any intermediary firewalls.
5. Review any additional configuration options you may wish to enable that alter the syslog syntax or connection mode. A full list is available below.
6. Finally, enable **Send Alerts** and save your changes.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker , Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support **DarkTrace IDS**.

4.1 Alerts

- **DarkTrace IDS – Intrusion Detected –** This alert will trigger for all DarkTrace IDS logs.

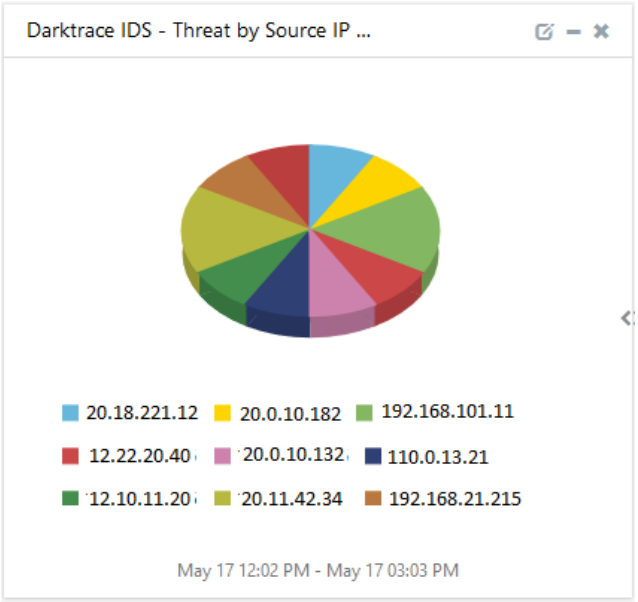
4.2 Reports

- **DarkTrace IDS – Activities –** This report provides information related to possible unencrypted password storage.

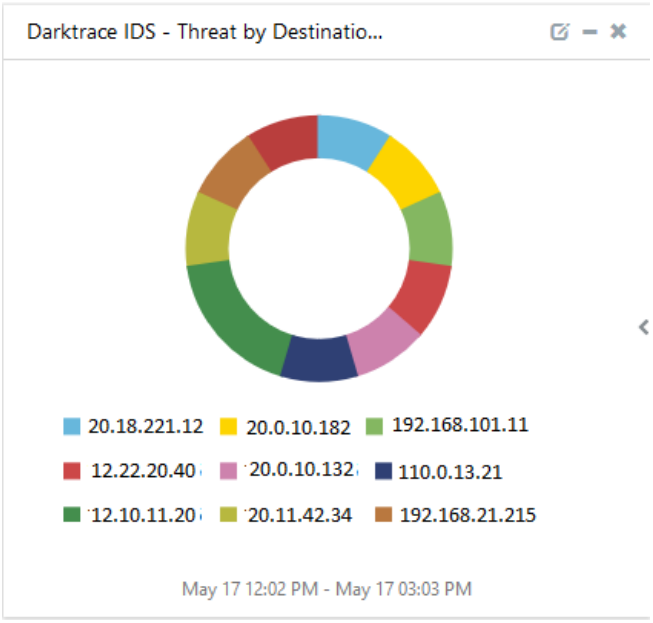
LogTime	Computer	Category	Priority	Device Host Name	Source IP Address	Source MAC Address	Destination IP Address	Destination Port Number	Message
05/17/2019 01:01:16 PM	DARKTRACE IDS	Anomalous Connection	6	contoso-work1.corp.net	40.20.10.34	b0:c8:dd:6f:5f:cd	30.10.23.224	4302	Multiple Connections to New External UDP Port
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	5	contoso-work12.corp.net	28.10.11.3		20.11.45.23	1265	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	4	contoso-work18.corp.net	30.10.23.224	b0:c8:dd:6f:5f:cd	11.21.1.23	2121	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	3	contoso-work21.corp.net	20.11.45.23		28.10.11.3	2222	Sensitive Terms in Unusual SMB Connection
05/17/2019 01:01:16 PM	DARKTRACE IDS	Compliance	3	contoso-work11.corp.net	11.21.1.23	b0:c8:dd:6f:5f:cd	40.20.10.34	2324	Sensitive Terms in Unusual SMB Connection

4.3 Dashboards

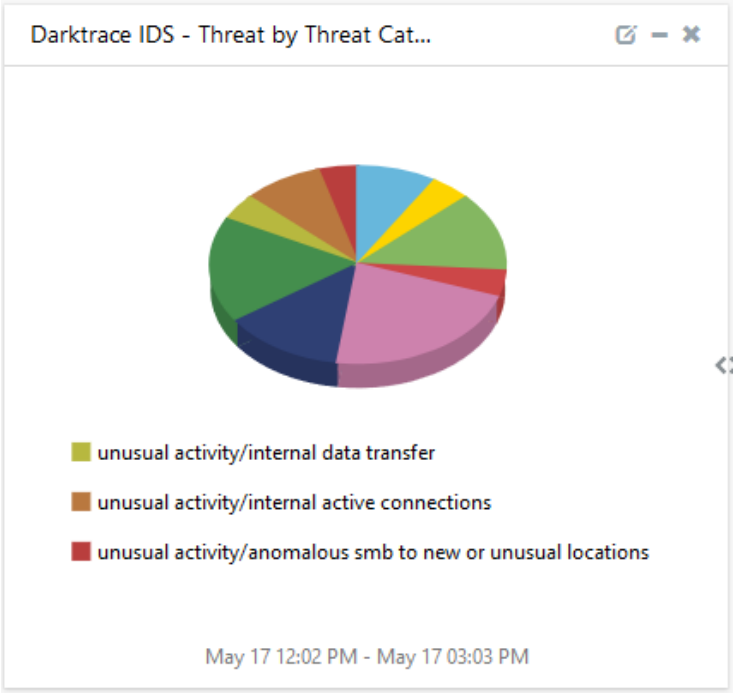
- **DarkTrace IDS – Threat by Source IP Address** – This dashboard shows information about the threat by source IP address.



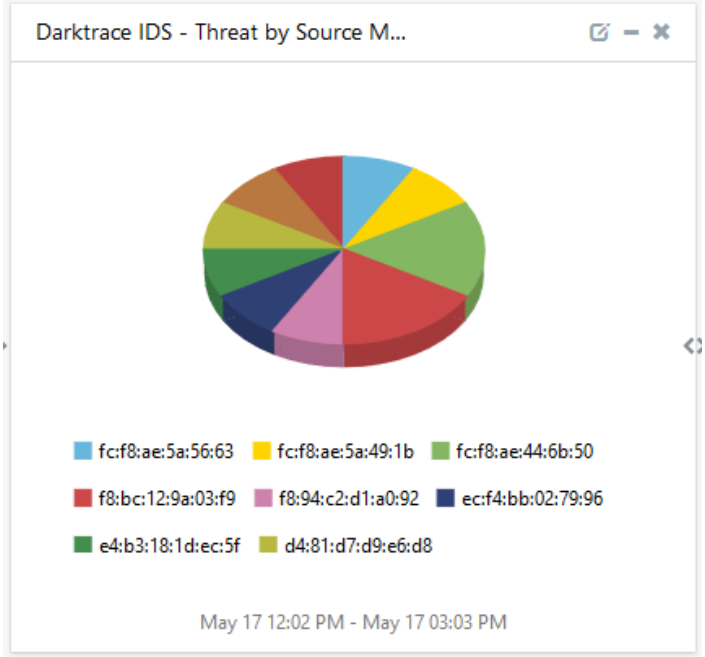
- **DarkTrace IDS – Threat by Destination IP Address** – This dashboard shows information about which threat by what are the destination IP addresses.



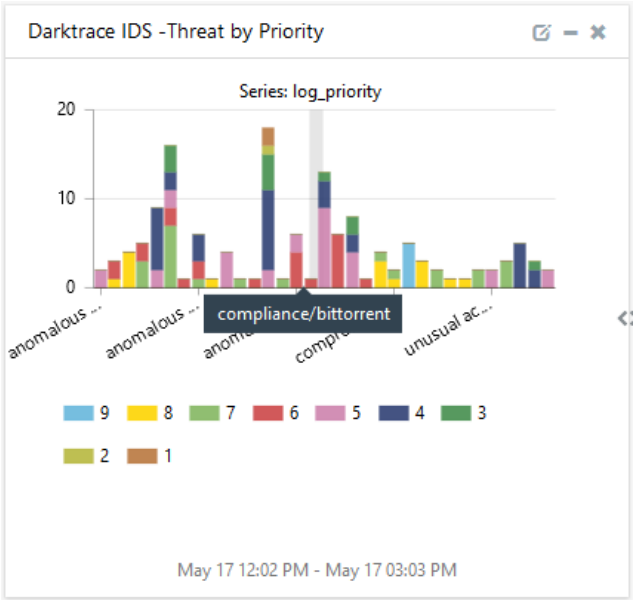
- **DarkTrace IDS – Threat by Threat Category** – This dashboard shows information about threat categories like possible unencrypted password storage.



- **DarkTrace IDS – Threat by Source MAC Address** – This dashboard shows information threat by source MAC address.

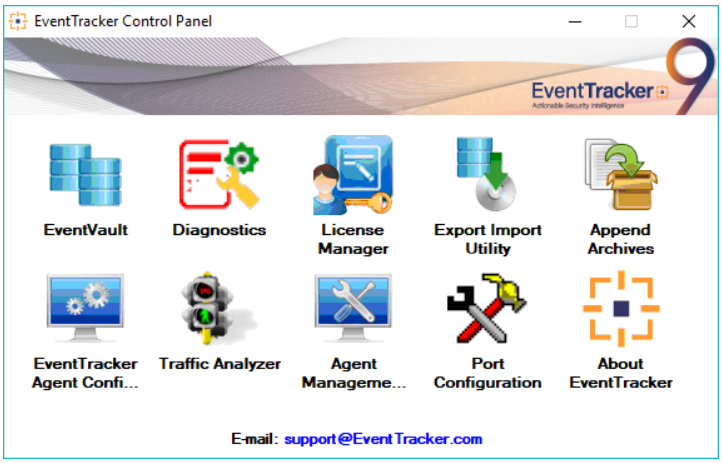


- **DarkTrace IDS – Threat by Priority** – This dashboard shows information based on threat priority.



5. Importing Extreme Network Access Control Knowledge Pack into EventTracker

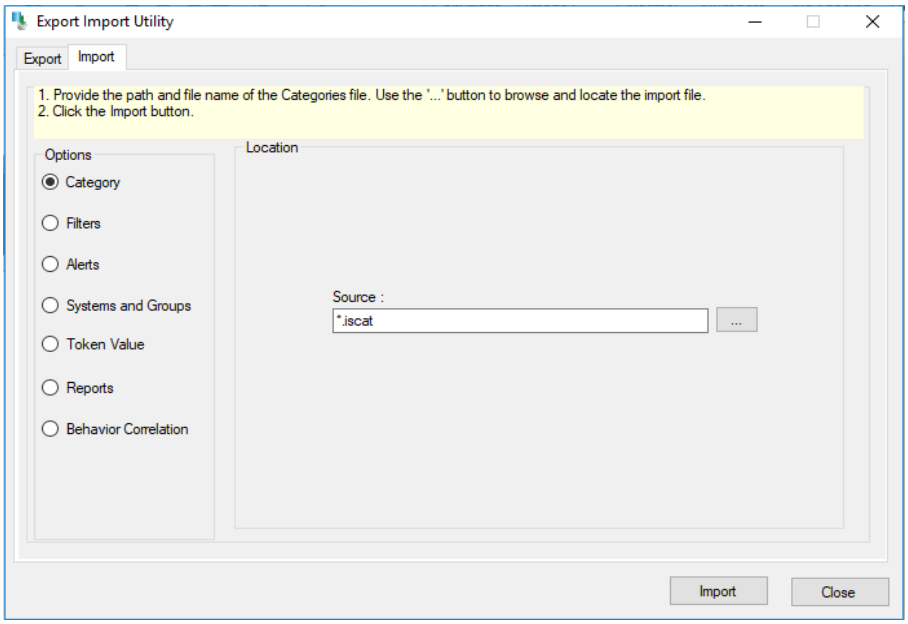
1. Launch the **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.



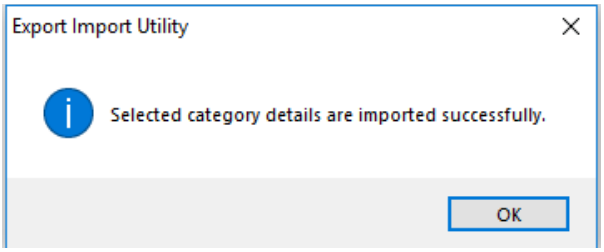
3. Import **Tokens/Flex Reports** as given below.

5.1 Category

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



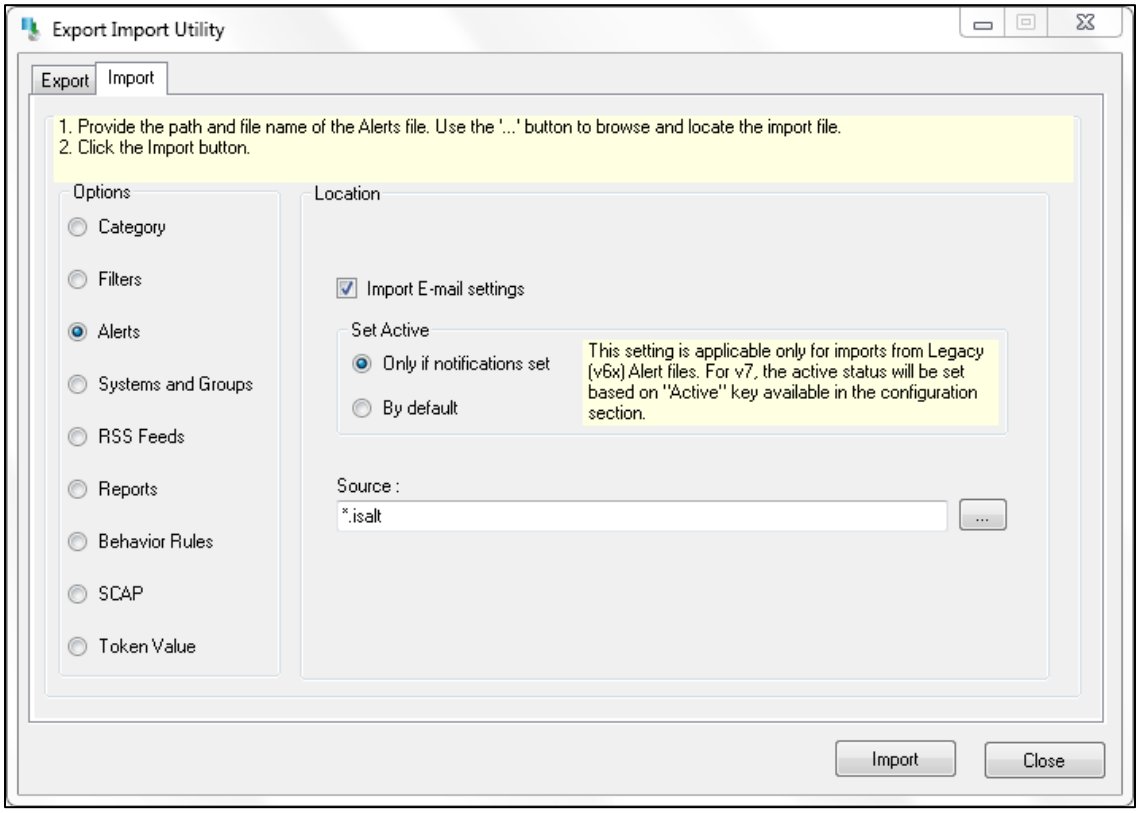
2. Locate **Category_Darktrace IDS.iscat** file, and then click the open button.
3. To import category, click the **Import** button.
4. EventTracker displays a success message.



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

5.2 Alerts

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

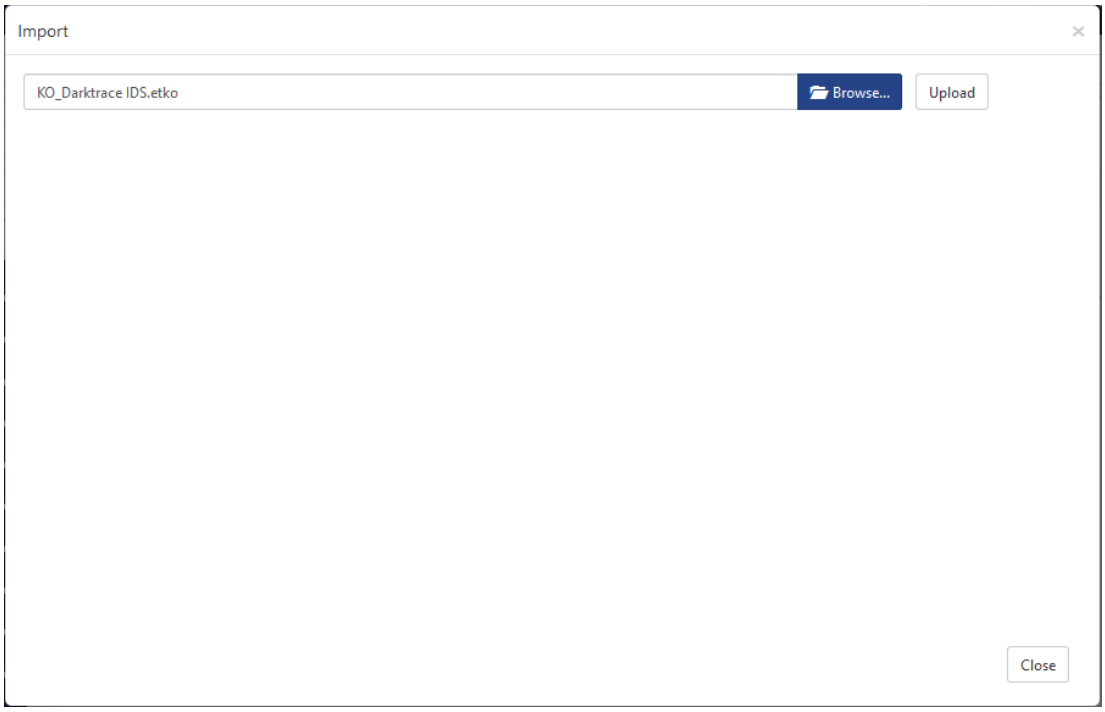


2. Locate **Alerts_DarkTrace IDS.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
4. EventTracker displays a success message.

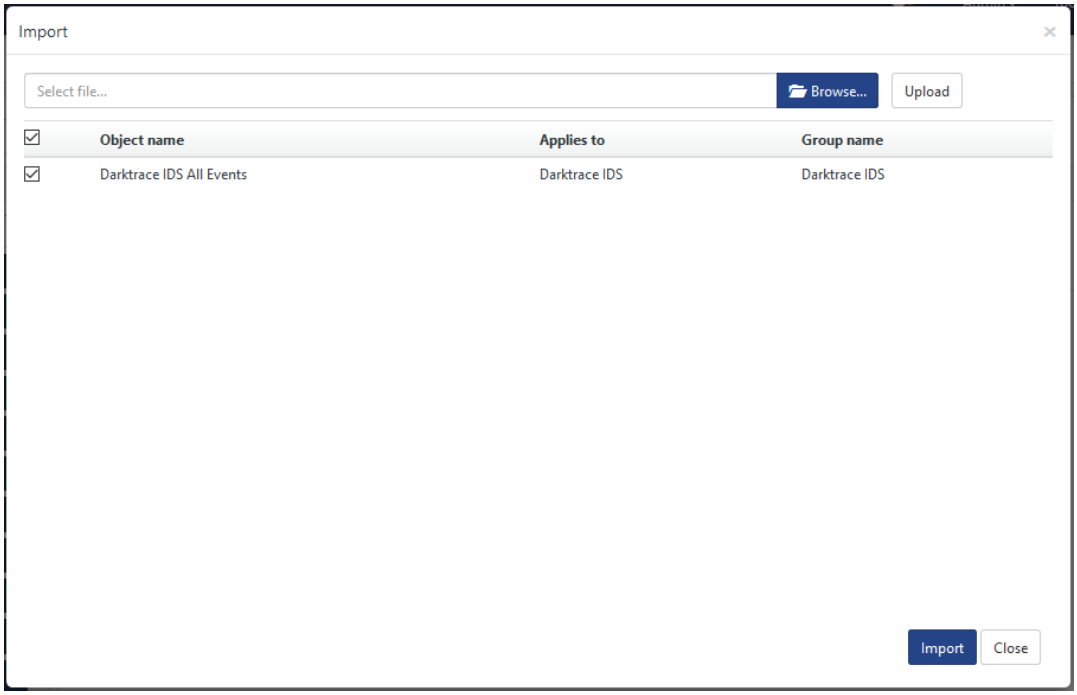
5. Click the **OK** button, and then click the **Close** button.

5.3 Knowledge Objects

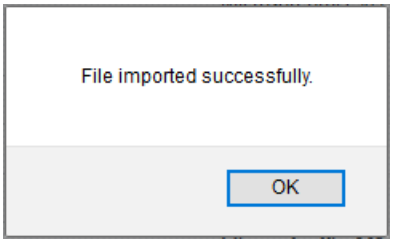
1. Click **Knowledge objects** under the admin option in the EventTracker page.
2. Locate the file named **KO_DarkTrace IDS.etko**.



3. Select all the checkbox and then click on the ‘**Import**’ option.

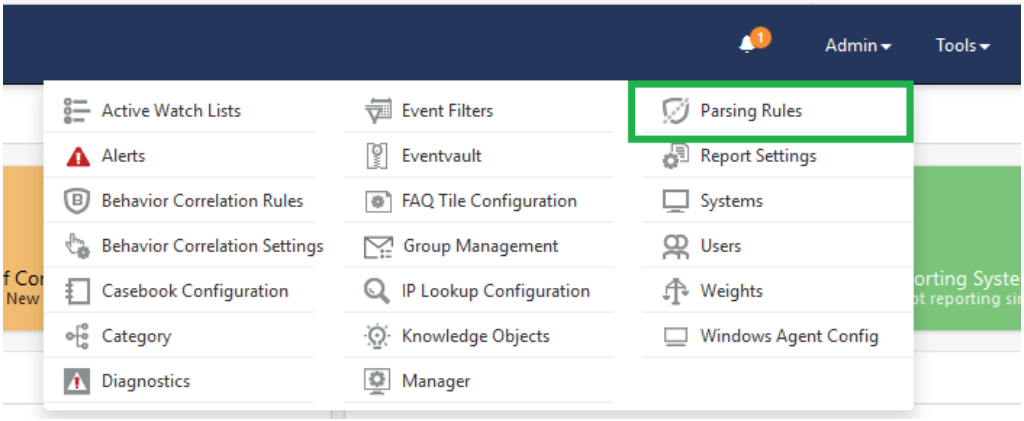


4. Knowledge objects are now imported successfully.

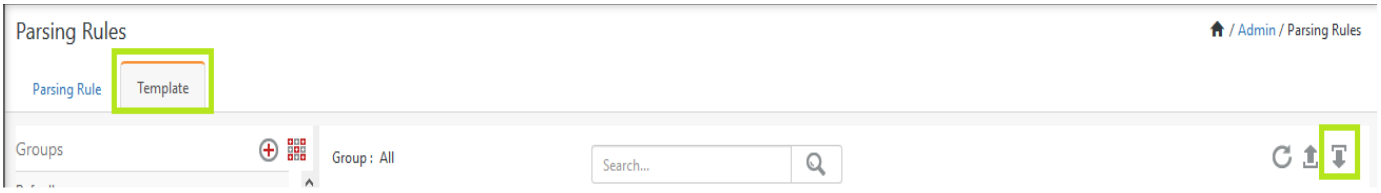


5.4 Token Template

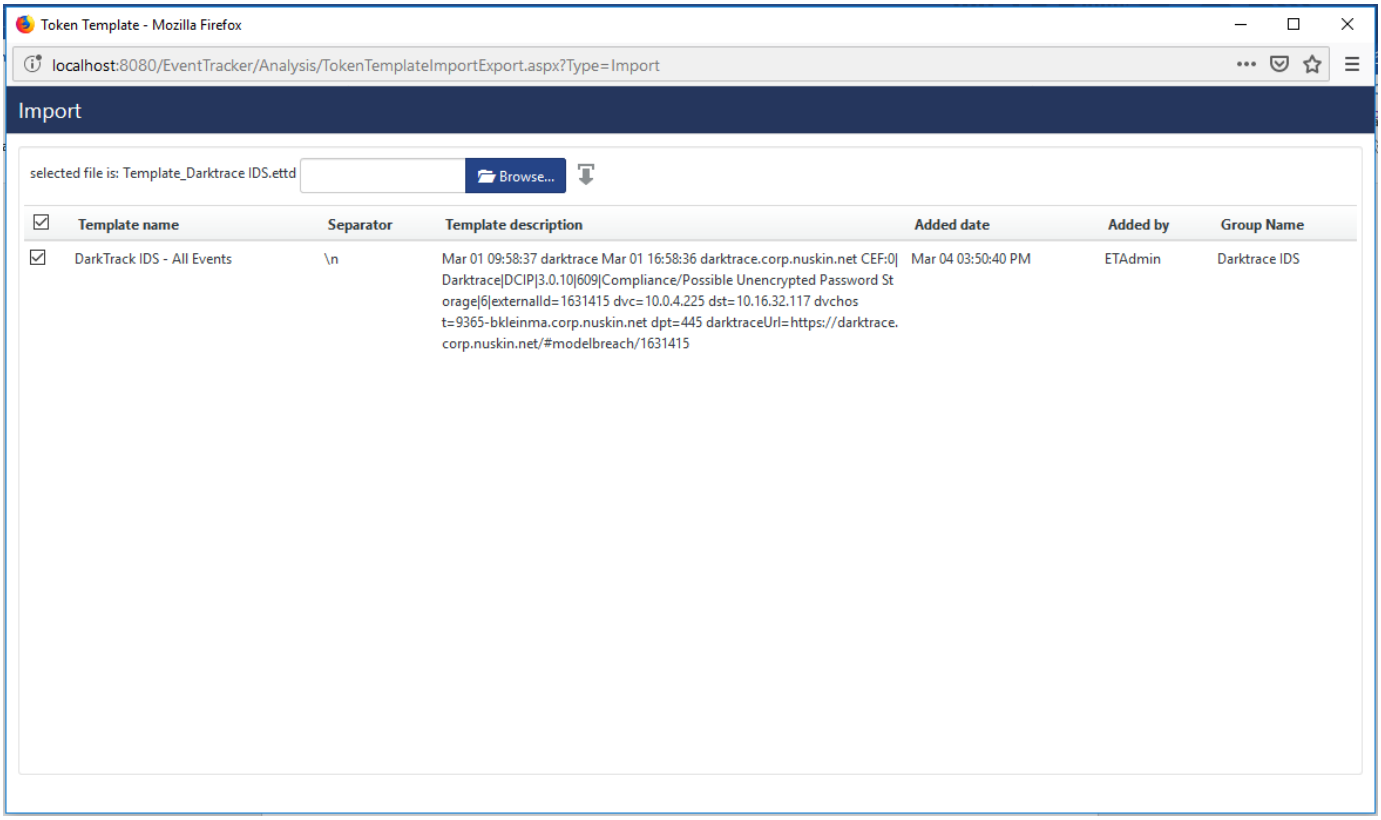
1. Login to the **EventTracker**.
2. Click on **Admin >> Parsing Rules**.



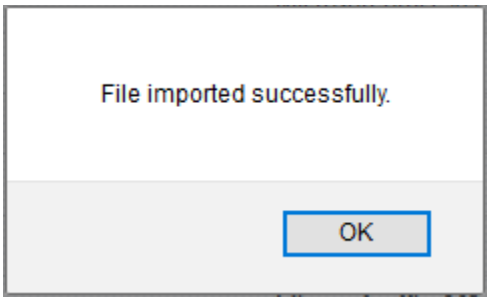
3. Click on **Template** and click **import configuration** symbol.



4. Locate the **Template_Darktrace IDS.ettd** file and click on **import**.

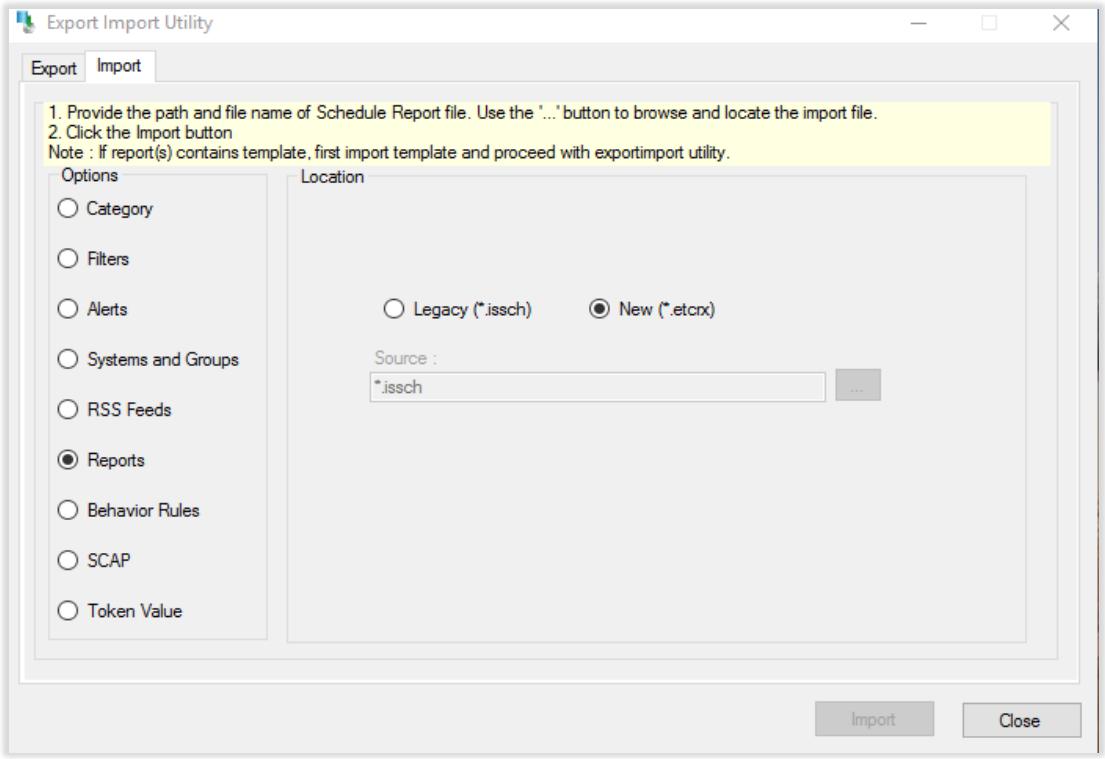


5. Templates are imported now successfully.

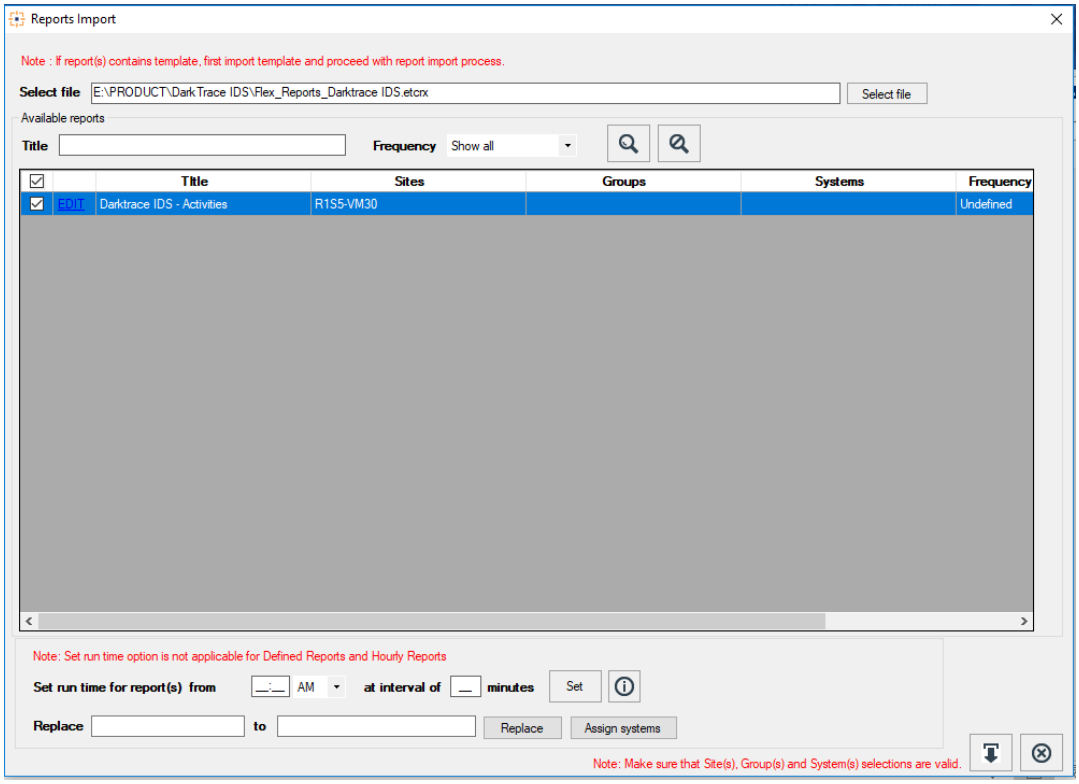


5.5 Flex Reports

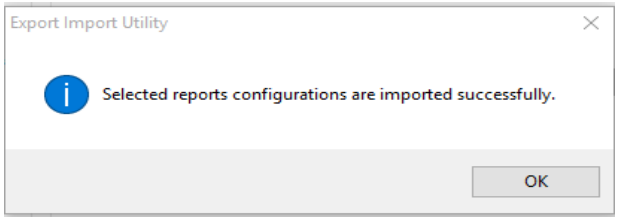
1. Click **Reports** option and select new (.etcrx) from the option.



2. Locate the file named **Flex_Reports_Darktrace IDS.etcrx** and select all the checkbox.



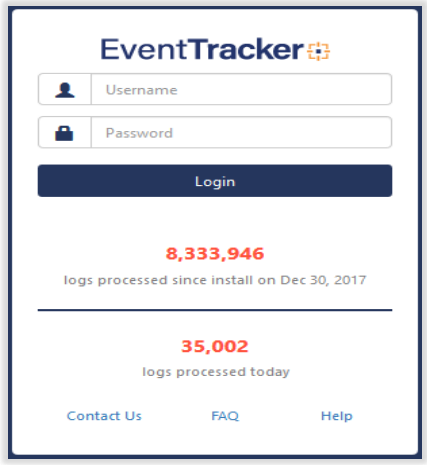
3. Click the **Import** button to import the reports. EventTracker displays a success message.



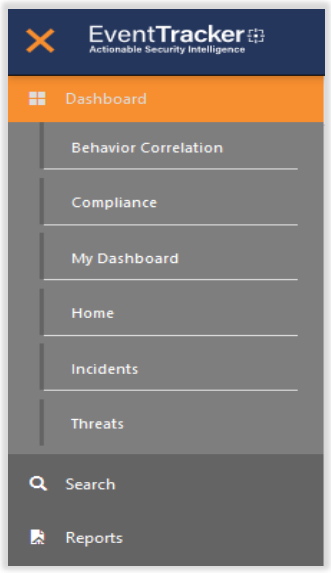
5.6 Dashlets

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

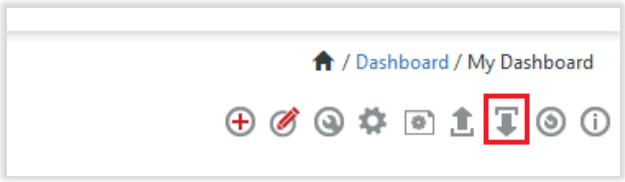
1. Login into EventTracker Web console.

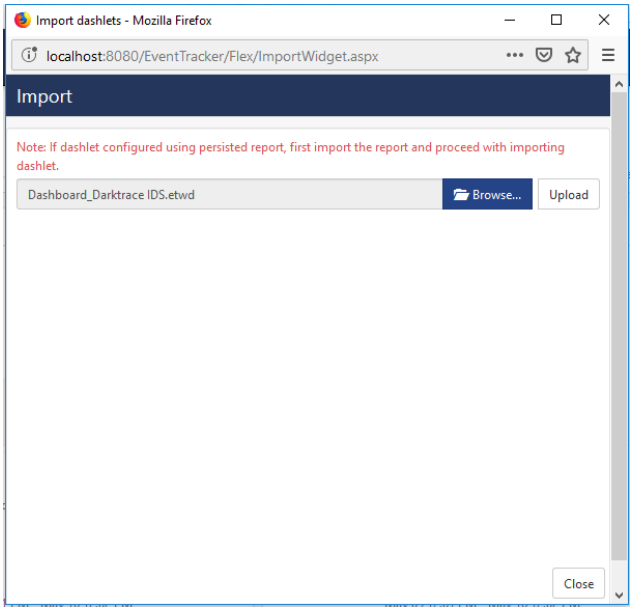


2. Go to **My Dashboard** option.

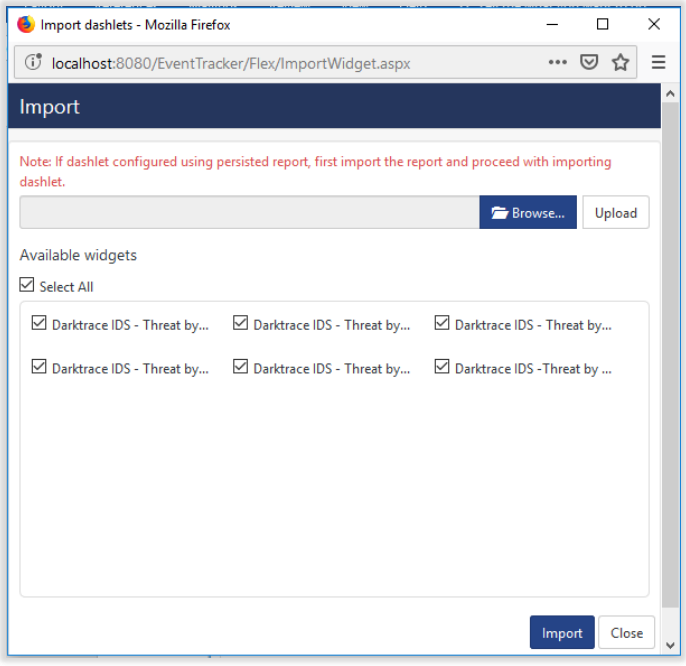


3. Click on the import button and select **.etwd** File.





4. Click upload and select **Dashboard** which you want to import.

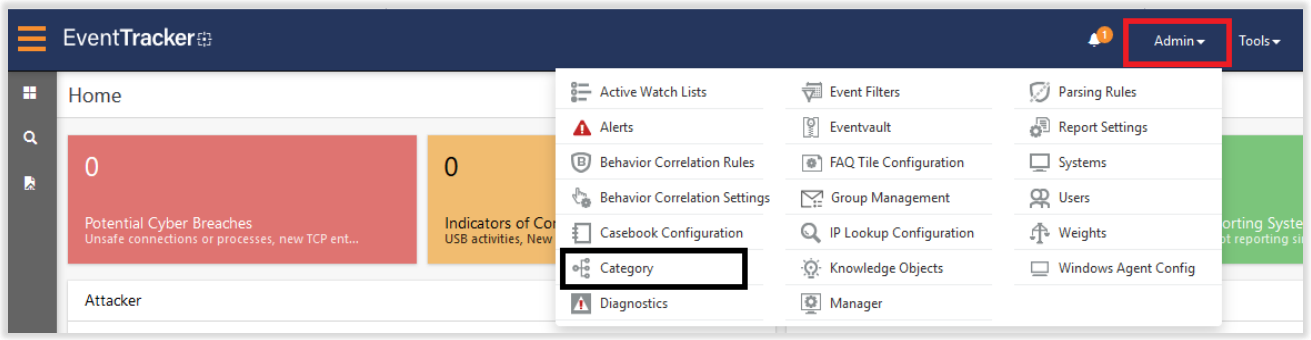


5. Click on the **Import** button. It will upload all selected dashboards.

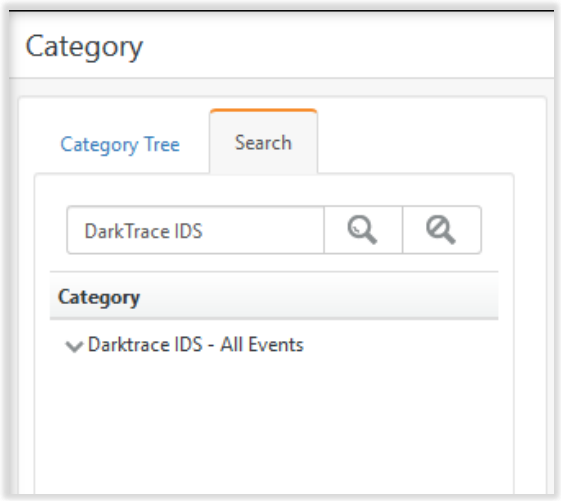
6. Verifying Knowledge Pack in EventTracker

6.1 Category

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Category**.

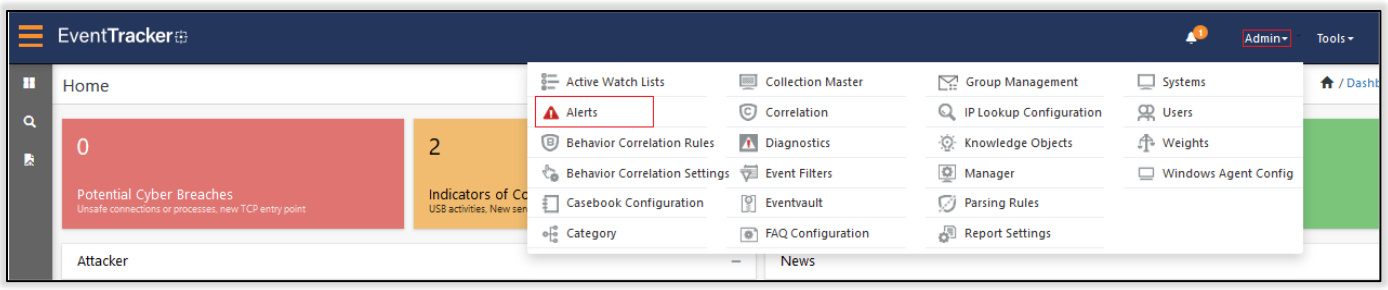


3. Click the **search**, and then **search** with **DarkTrace IDS**.

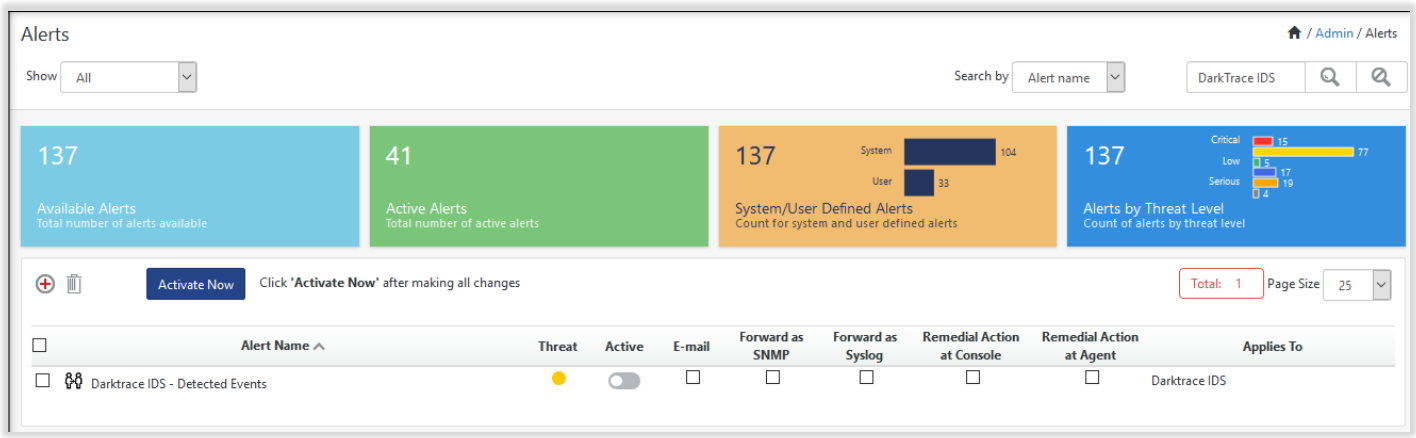


6.2 Alerts

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

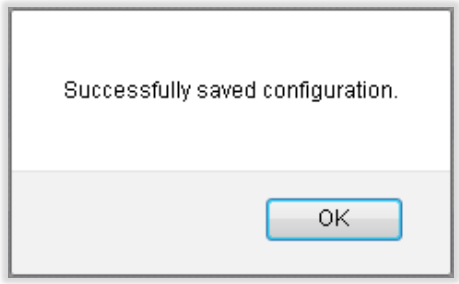


3. In the **Search** box, type **'DarkTrace IDS'**, and then click the **Go** button.
   Alert Management page will display all the imported alerts.



4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays a message box.



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

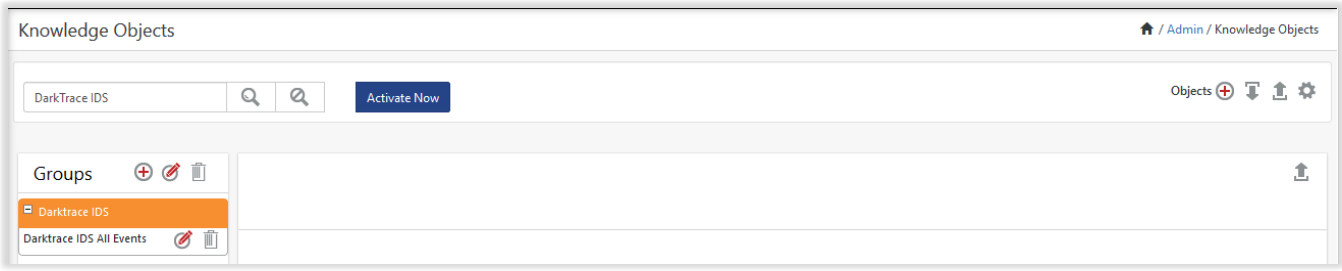
Note: Specify appropriate **systems** in the **alert configuration** for better performance.

6.3 Knowledge Object

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click the **Knowledge Object**.

3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click the **DarkTrace IDS** group folder.

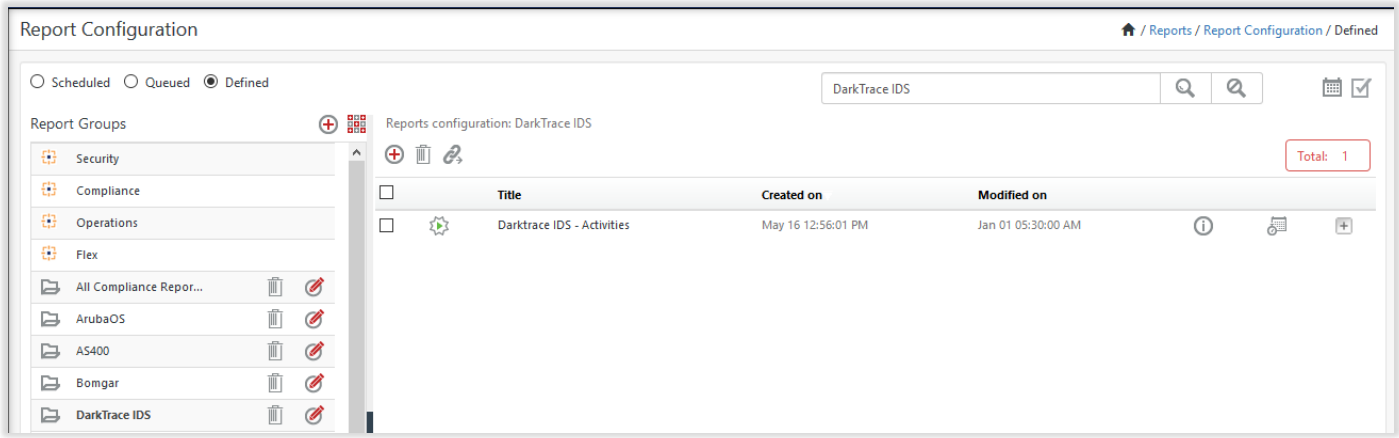
4. Knowledge Object is displayed in the pane.



6.4 Flex Reports

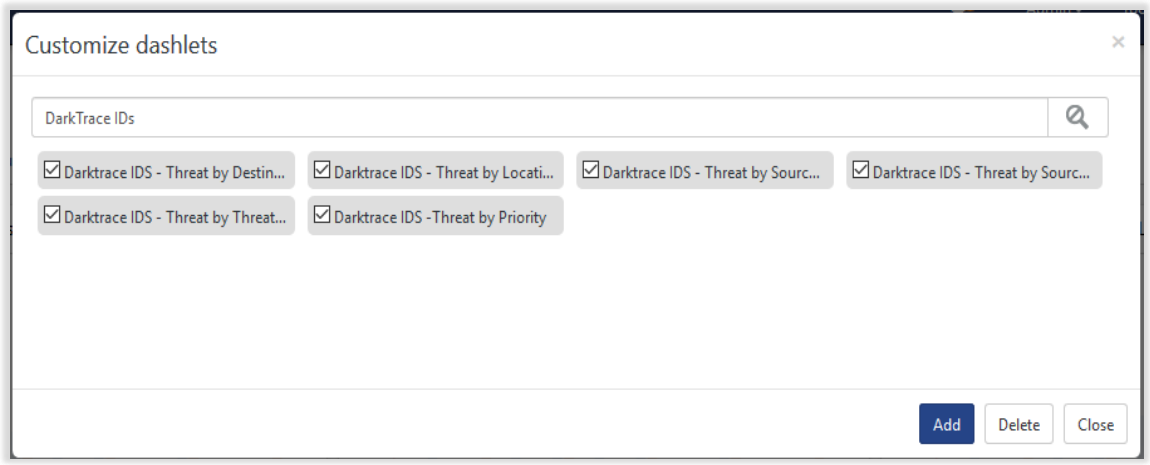
1. Login to **EventTracker**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click the **DarkTrace IDS** group folder.

5. Reports are displayed in the Reports configuration pane.



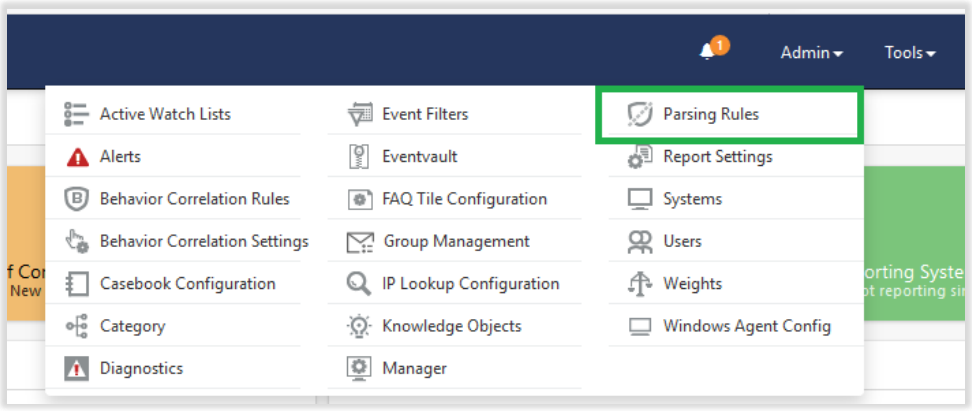
6.5 Dashlets

1. Login to **EventTracker**.
2. Click the **Dashboard** menu, and then **My Dashboard.**
3. Then click on **Customize Dashlet** button and search for **"DarkTrace IDS"**

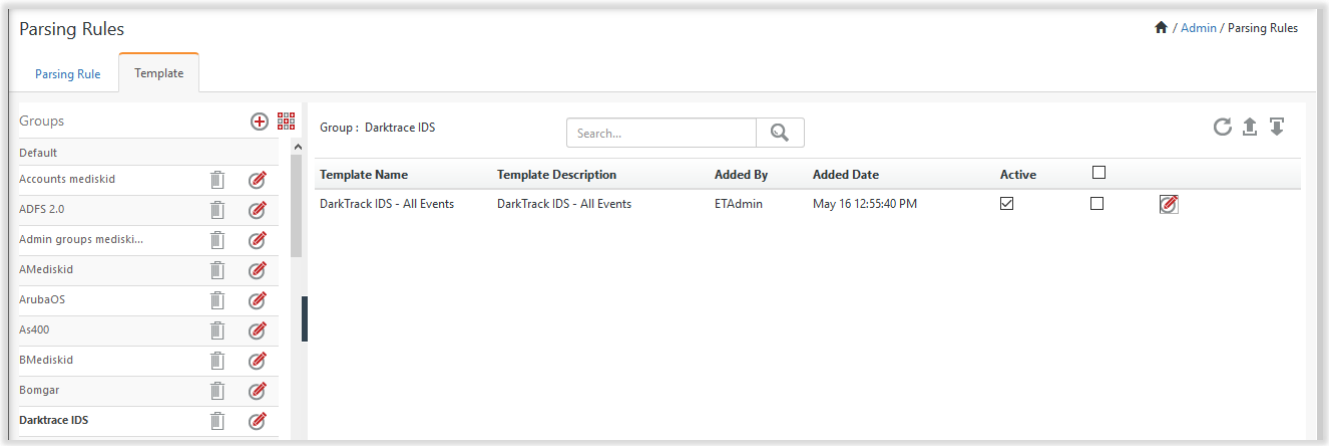


6.6 Token Template

1. Login to the **EventTracker**.
2. Click on **Admin >> Parsing Rules**.



3. Click on **Template** and search for **DarkTrace IDS.**



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, end 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