Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating TrapX DeceptionGrid with EventTracker

EventTracker v9.2x and above

Publication Date:

February 10, 2022

Abstract

This guide provides instructions to configure the **TrapX DeceptionGrid Syslog** to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with the EventTracker version v9.2x or above and TrapX DeceptionGrid v6.1.

Audience

The Administrators who are assigned the task to monitor the TrapX DeceptionGrid events using EventTracker.

Table of Contents

1. Overview

TrapX is a new generation of deception technology that provides real-time breach detection and prevention. Its field-proven solution deceives would-be attackers with turn-key decoys (traps) that imitate true assets. Traps can be deployed creating a virtual minefield for cyberattacks, alerting you to any malicious activity with actionable intelligence immediately.

EventTracker integrates with TrapX DeceptionGrid and helps you monitor crucial events such as threats detected and malicious traffic events.

EventTracker provides insights about the TrapX DeceptionGrid scan events and connection events. EventTracker reports TrapX DeceptionGrid scan events and connection events which provide a detailed summary for various events like the scan hosts, device connected, etc.

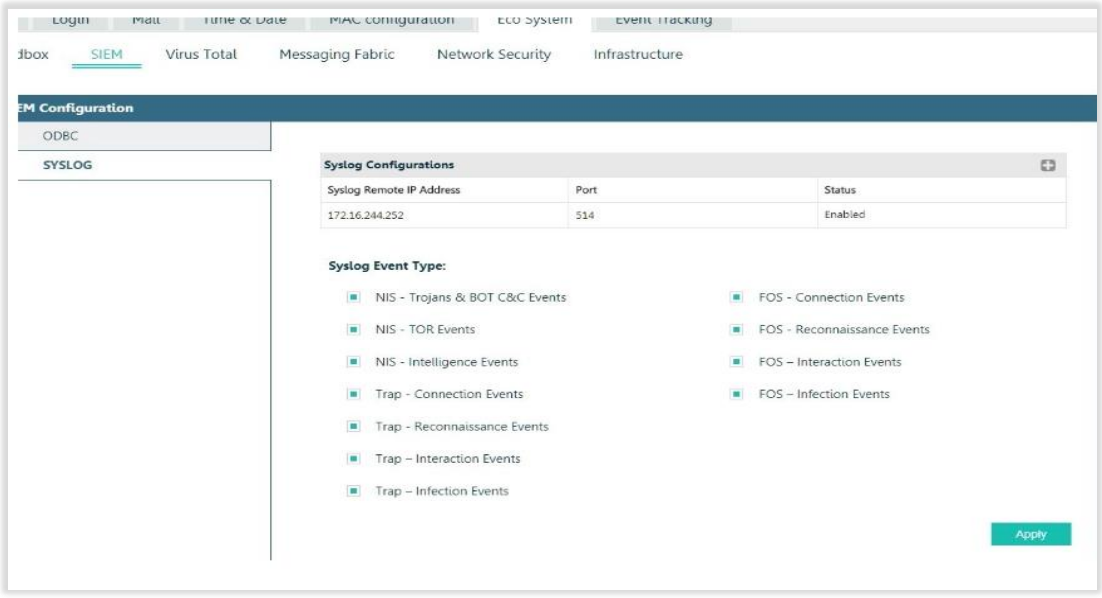
2. Prerequisites

- **Admin** access to the **TrapX DeceptionGrid** console.
- **EventTracker** Manager/Sensor should be installed and running.

3. Configuring TrapX DeceptionGrid Syslog Logging

Refer to the following steps to configure the TrapX DeceptionGrid Syslog to send the logs to EventTracker.

1. Go to the portal and navigate to **Settings** > **General** > **Eco System** > **SIEM** > **Syslog**.
2. Under the **Syslog** server, click **Remote IP address,** enter the **EventTracker** IP address and port number 514.
3. Click **Add**.
4. Check all the **Event** types.
5. Click **Apply**.



4. EventTracker Knowledge Packs

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

The following Knowledge Packs are available in EventTracker to support **TrapX DeceptionGrid**.

4.1 Categories

- **TrapX DeceptionGrid – Scan activities -** This category provides information related to the network scanning detected on their hosts.
- **TrapX DeceptionGrid – Connection activities -** This category provides information related to the device's connectivity on their hosts.
- **TrapX DeceptionGrid: Interaction trap has been detected -** This category provides information related to a host interacting and is involved in different suspicious operations.
- **TrapX DeceptionGrid: Reconnaissance trap has been detected –** This category provides information related to a host activity involved in collecting information.

4.2 Alerts

- **TrapX DeceptionGrid: Connection trap has been detected -** This alert generates whenever a host is successfully connected with another host.
- **TrapX DeceptionGrid: Interaction trap has been detected -** This alert generates whenever a host interacts and is involved in different suspicious operations.
- **TrapX DeceptionGrid: Reconnaissance trap has been detected –** This alert generates whenever a host activity is involved in collecting the information.
- **TrapX DeceptionGrid: Scan trap has been detected -** This alert generates whenever scan activities happen on their hosts.

4.3 Reports

- **TrapX DeceptionGrid – Scan activities -** This report gives information about network scanning to discover active hosts and detect vulnerabilities. It contains field information like the source IP address, hostname, source port, destination IP address, destination port, and protocol.

Sample Report

LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	Device Hostname	Device Facility
01/20/2022 03:47:29 AM	TRAPX-SYSLOG	192.168.10.14	28616	192.168.20.11	445	RST SCAN	ContosoWKS23_SR	ContosoWKS23
01/20/2022 03:47:29 AM	TRAPX-SYSLOG	192.168.10.14	28666	192.168.20.22	80	ACK SCAN	ContosoWKS24_SR	ContosoWKS24
01/20/2022 03:47:32 AM	TRAPX-SYSLOG	192.168.10.10	28516	192.168.20.10	445	SYN SCAN	ContosoWKS22_SR	ContosoWKS22
01/20/2022 03:47:32 AM	TRAPX-SYSLOG	192.168.10.14	28616	192.168.20.11	445	RST SCAN	ContosoWKS24_SR	ContosoWKS23

Sample Logs

```
Dec 01 19:44:02 ContosoWKS23 Dec  1 19:44:02 192.168.20.150
CEF:0|TrapX|TSOC|7.0|ID:8|Malware Trap - Scan Event|1|rt=Dec 01 2021
```

```
19:43:37 src=192.168.10.10 deviceNtDomain=ContosoWKS23_SR
deviceFacility=ContosoWKS23 dvchost=Contoso-WK-S23.com cs5Label=company
cs5=ADB proto=SYN SCAN spt=28516 cs8Label=OS Version cs8=Microsoft Windows
Server 2016 R2 deviceTranslatedAddress=192.168.20.10 cs7Label=Emulation Type
cs7=Windows Server deviceExternalId=1 cat=Scan devicePayloadId=NO dpt=445
externalId=430873 dst=192.168.20.10 cs4Label=PCAP cs4=NO
```

- **TrapX DeceptionGrid - connection activities -** This report gives information about the devices connected to their hosts. It contains fields information like the hostname, protocol, source IP address, source port, destination IP address, company name, operating system, operating system version, destination port, etc.

Sample Report

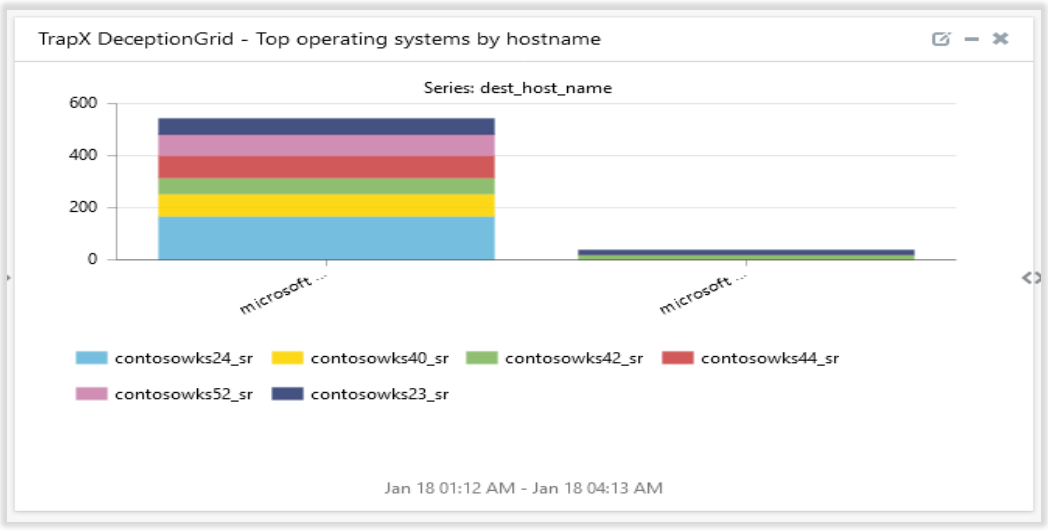
LogTime	Computer	Source IP Address	Source Port	Protocol	Destination IP Address	Destination Port	Device Hostname
01/18/2022 04:08:17 AM	TRAPX-SYSLOG	192.168.10.42	54230	SMB	192.168.20.142	445	ContosoWKS42
01/18/2022 04:08:17 AM	TRAPX-SYSLOG	192.168.10.52	54730	SMB	192.168.20.194	445	ContosoWKS52
01/18/2022 04:08:17 AM	TRAPX-SYSLOG	192.168.10.44	54620	FTP	192.168.20.192	445	ContosoWKS44
01/18/2022 04:08:17 AM	TRAPX-SYSLOG	192.168.10.40	54220	HTTP	192.168.20.120	80	ContosoWKS23

Sample Logs

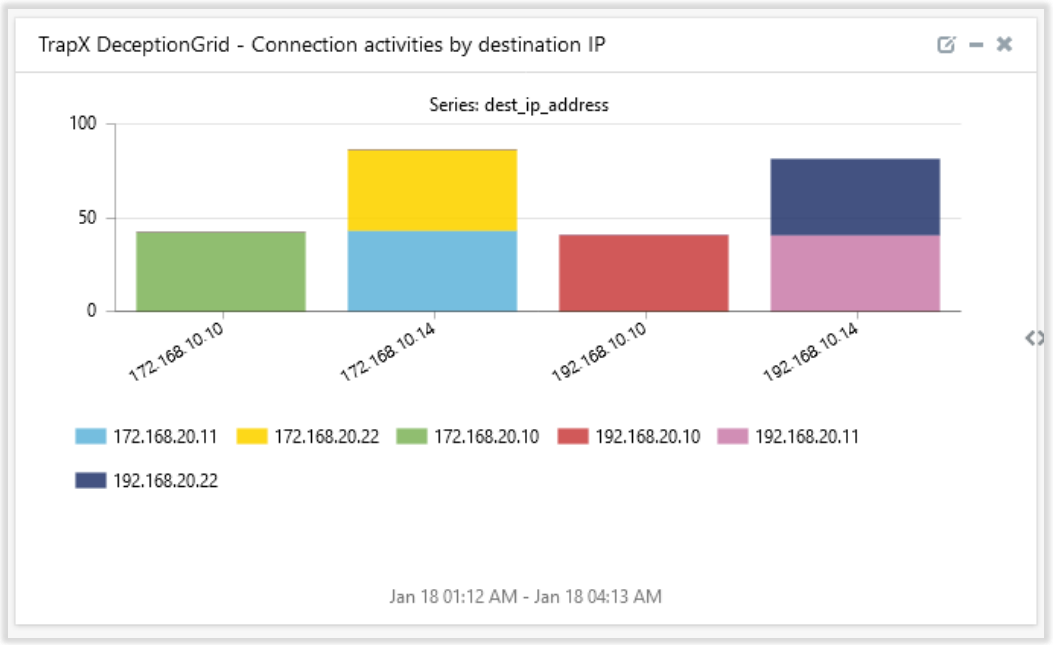
```
Dec 01 19:43:51 ContosoWKS23 Dec  1 19:43:51 192.168.20.150
CEF:0|TrapX|TSOC|7.0|ID:4|Malware Trap - Connection Event|1|rt=Dec 01 2021
19:43:49 src=192.168.10.52 deviceNtDomain=ContosoWKS52_SR
deviceFacility=ContosoWKS52 dvchost=Contoso-WK-S52.com.com cs5Label=company
cs5=ADB proto=SMB spt=54730 cs8Label=OS Version cs8=Microsoft Windows Server
2008 R2 deviceTranslatedAddress=192.168.20.194 cs7Label=Emulation Type
cs7=Windows Server deviceExternalId=1 cat=Connection cs3Label=Commands Used
cs3=Disconnected dpt=445 externalId=430872 dst=192.168.20.194 cs4Label=PCAP
cs4=YES
```

4.4 Dashboards

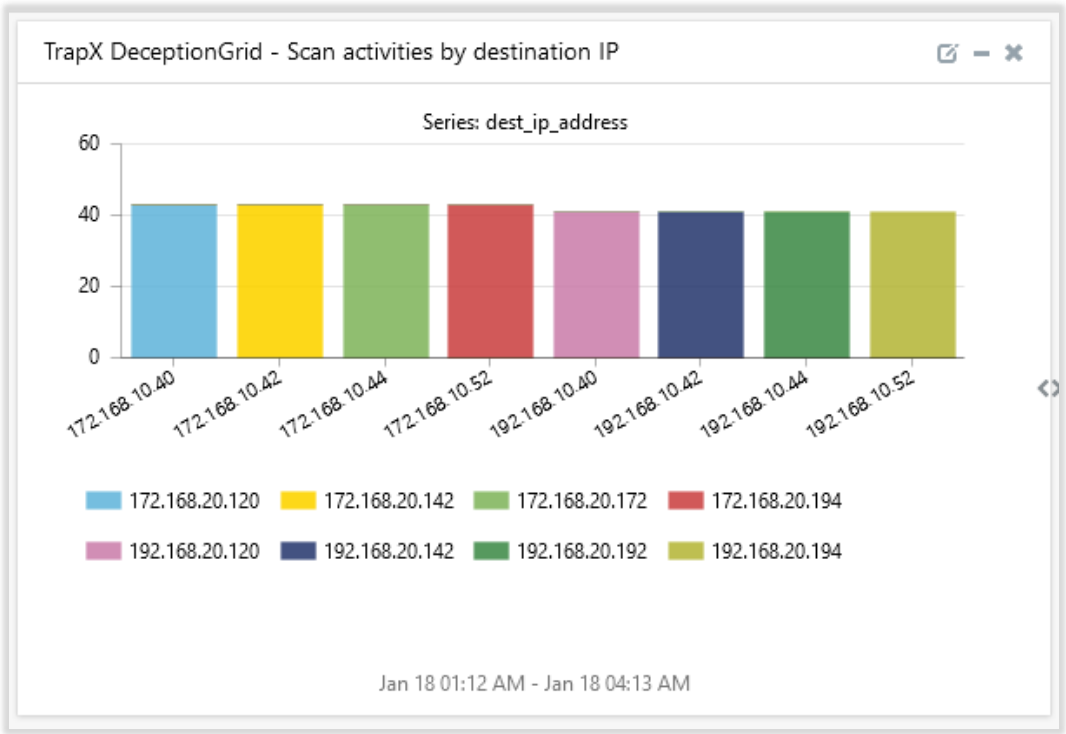
- **TrapX DeceptionGrid – Top operating systems by hostname**



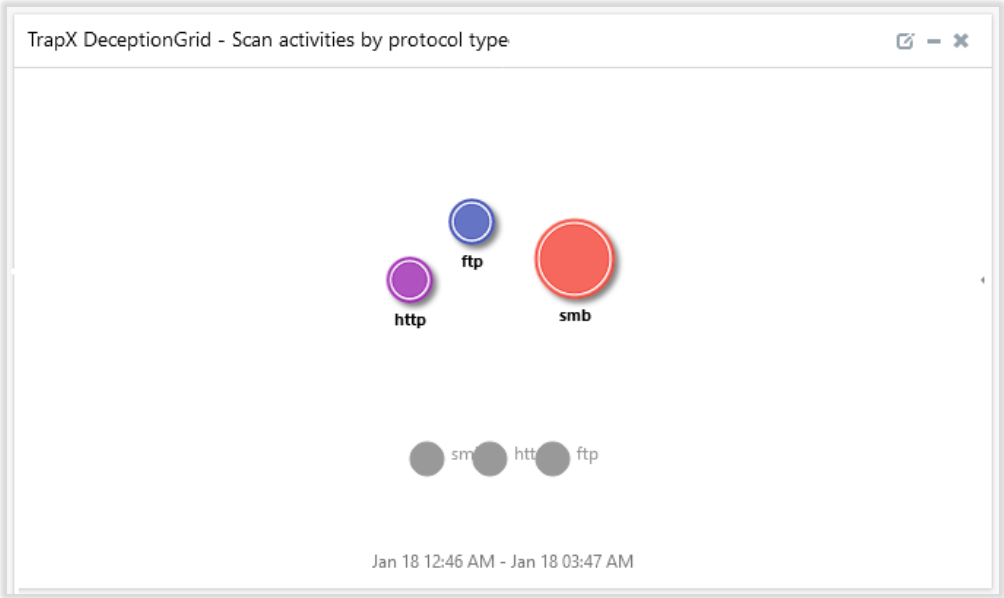
- **TrapX DeceptionGrid – Connection activities by destination IP address**



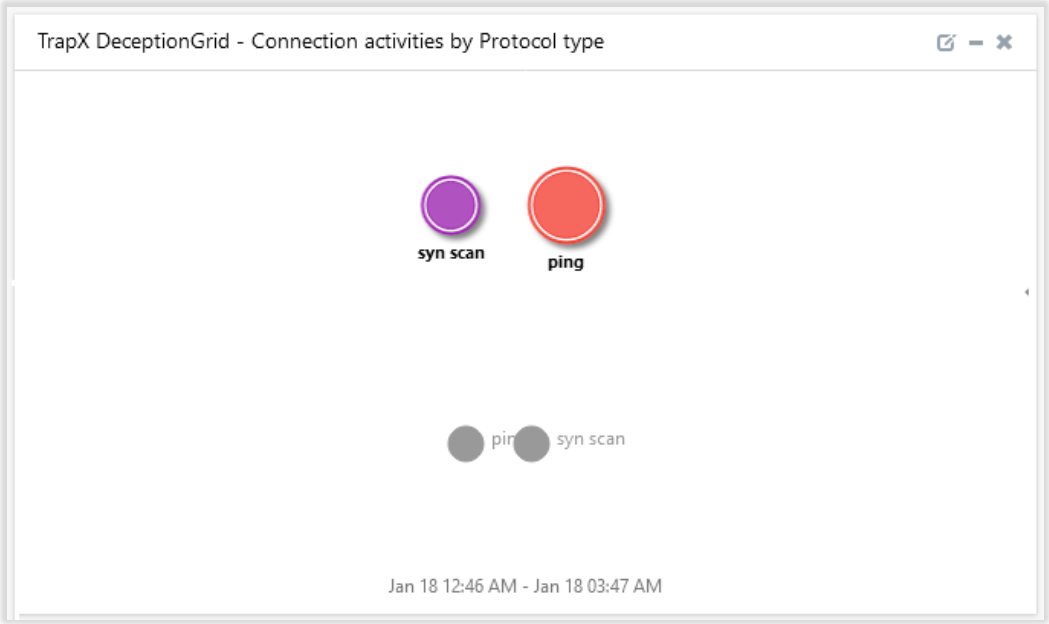
- **TrapX DeceptionGrid – Scan activities by destination IP address**



- **TrapX DeceptionGrid – Scan activities by protocol type**



- **TrapX DeceptionGrid – Connection activities by protocol type**

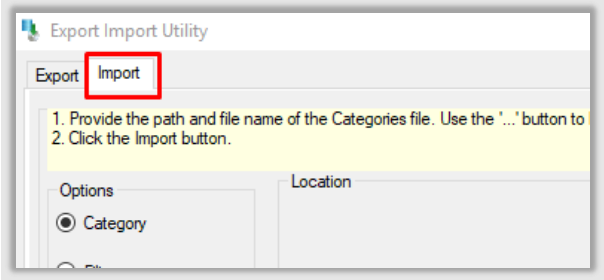


5. Importing TrapX DeceptionGrid Knowledge Pack into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

- Categories
- Alerts
- Knowledge Objects
- Flex Reports
- Dashboards

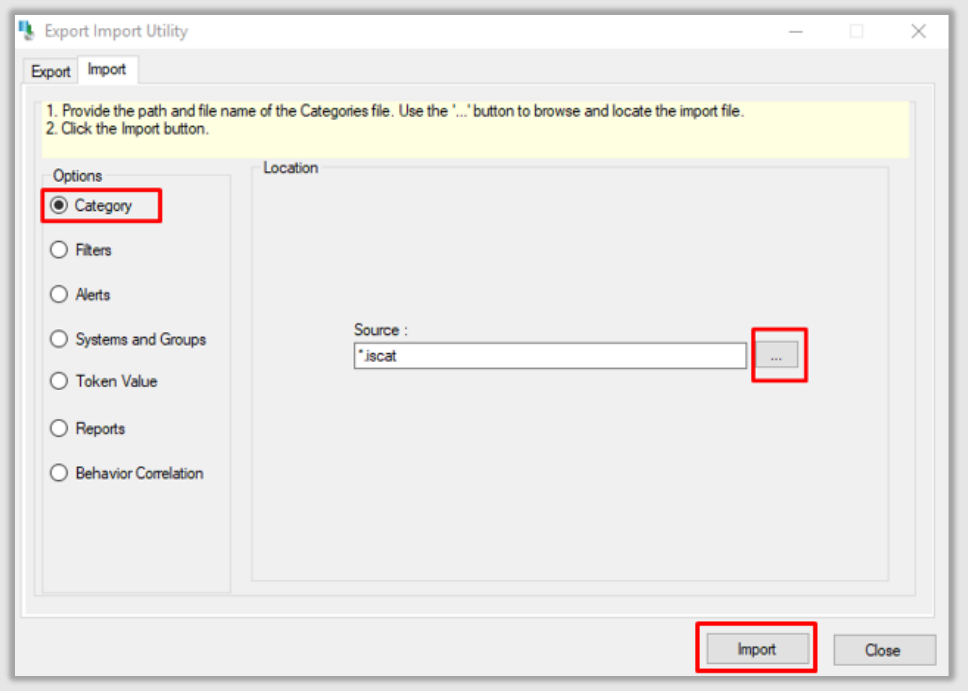
1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.



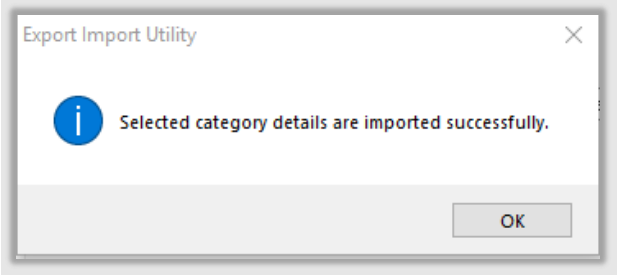
3. Click the **Import** tab.

5.1 Categories

1. After opening the **Export-Import Utility** via the **EventTracker Control Panel**, click the **Category** option, and then click **Browse** ... .
2. Navigate to the Knowledge Pack folder and select the file with the extension **".iscat", e.g., "Categories_TrapX DeceptionGrid.iscat"** and click the **Import** button.

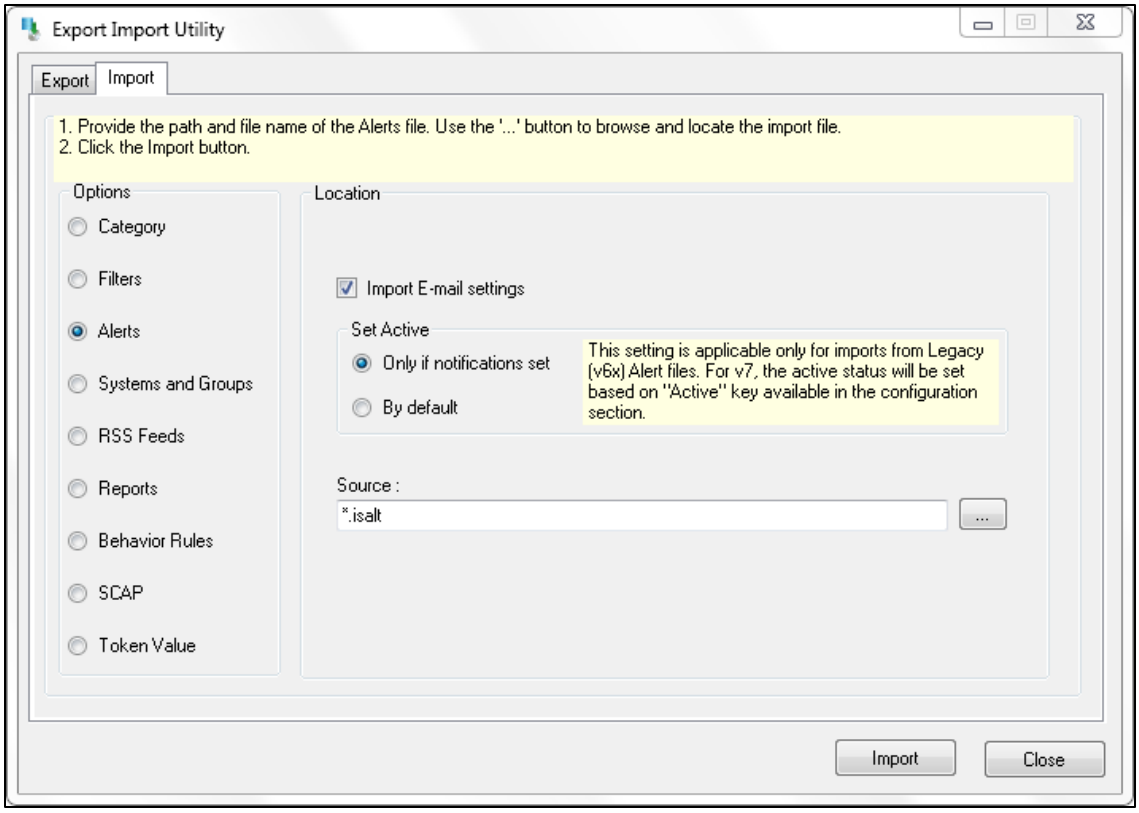


EventTracker displays a success message.

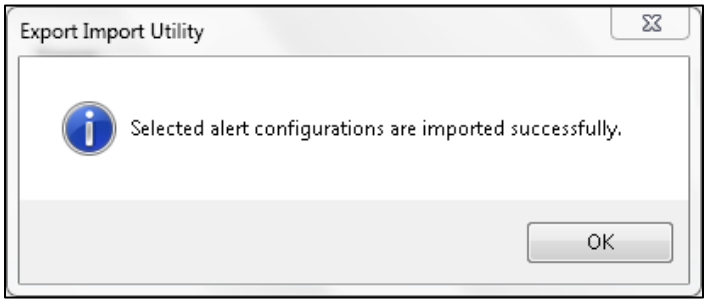


5.2 Alerts

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



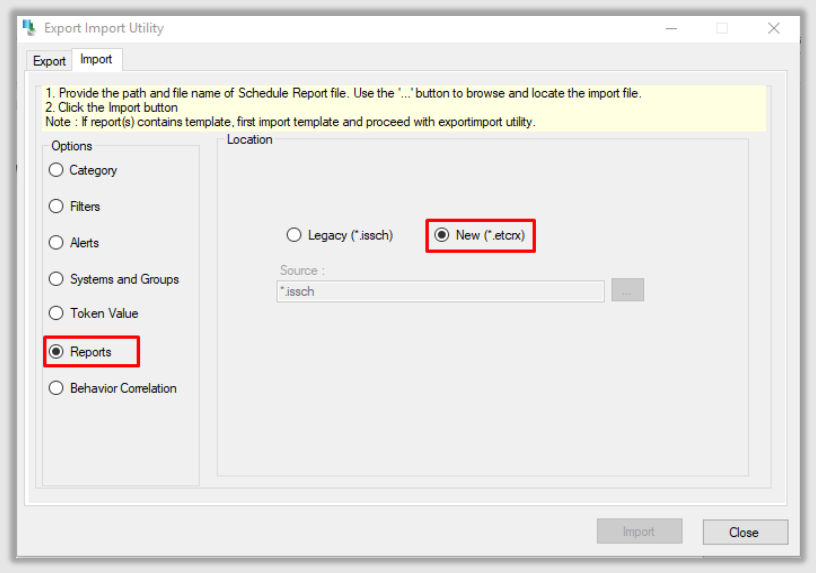
2. Locate the **Alerts_TrapX DeceptionGrid.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
4. EventTracker displays a success message.



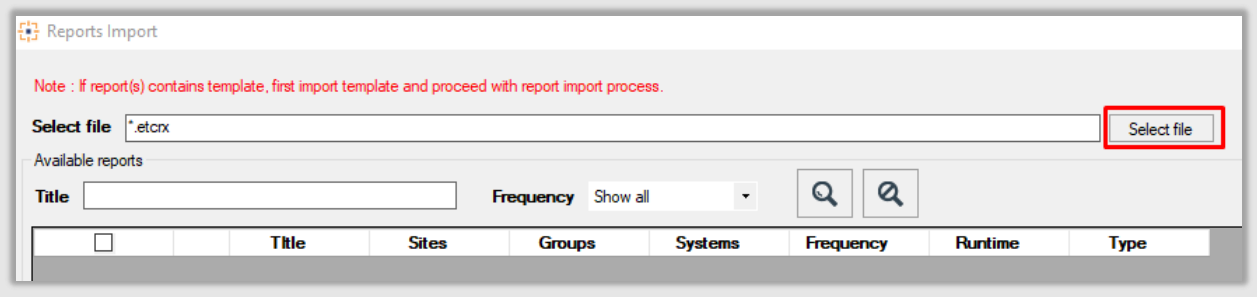
5. Click the **OK** button, and then click the **Close** button.

5.3 Reports

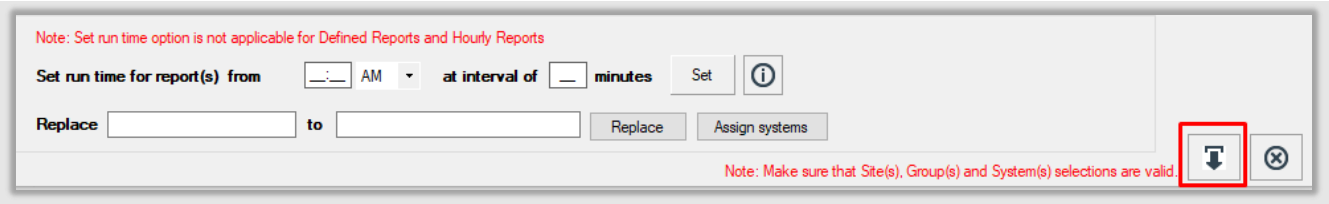
1. In the EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click the **Reports** option, and choose **New (*.etcrx)**.



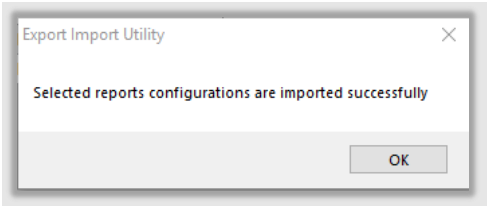
2. A new pop-up window appears. Click the **Select File** button and navigate to the file path with a file having the extension "**.etcrx", e.g., Reports_TrapX DeceptionGrid .etcrx.**



3. Wait while the reports populate in the below tables. Now, select all the relevant reports and then click the **Import** button.

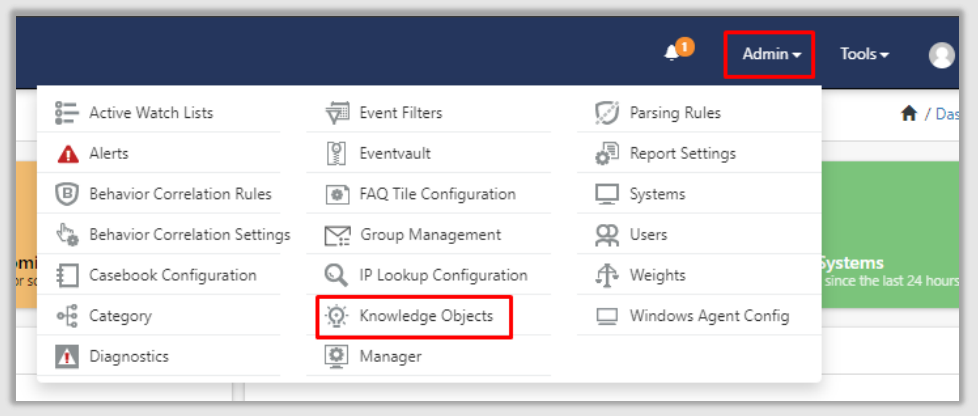


EventTracker displays a success message.

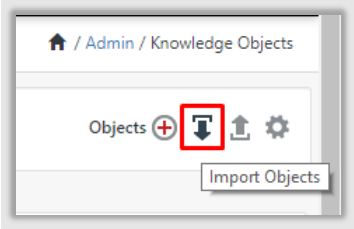


5.4 Knowledge Objects

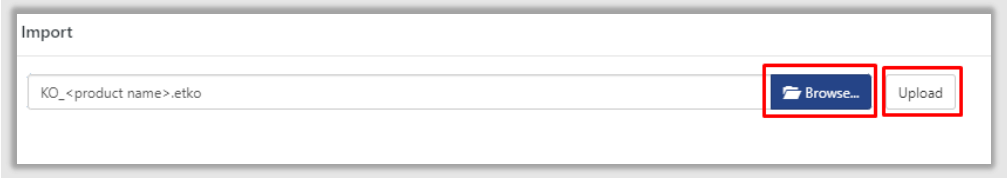
1. Click **Knowledge Objects** under the **Admin** option on the EventTracker page.



2. Click the **Import objects** icon.



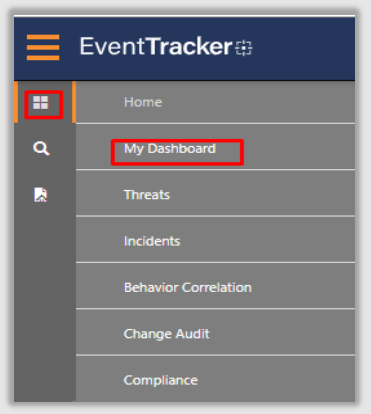
3. A pop-up box appears, click **Browse** and navigate to the Knowledge Packs folder (type **%et_install_path%\Knowledge Packs** in the navigation bar) with the extension **".etko", e.g., KO_TrapX DeceptionGrid.etko,** and then click **Upload**.



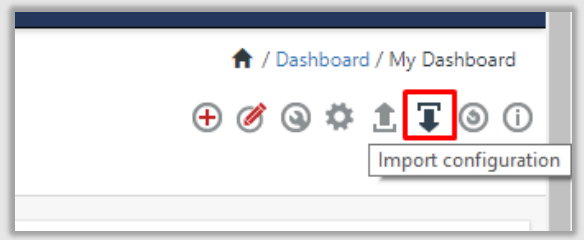
4. A list of available Knowledge Objects will appear. Select the relevant files and click the **Import** button.

5.5 Dashboards

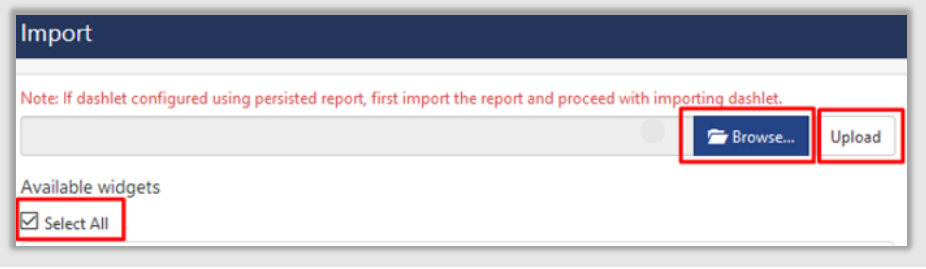
1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.

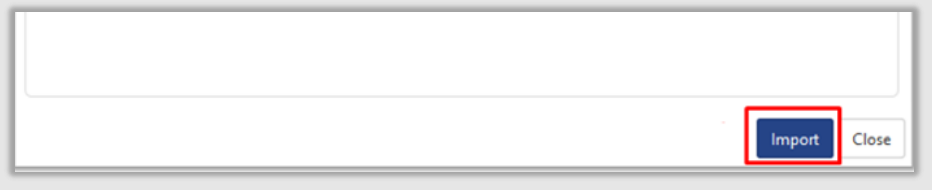


3. In **My Dashboard**, click the **Import** button.



4. Select the **Browse** button and navigate to the Knowledge Pack folder (type **%et_install_path%\Knowledge Packs** in the navigation bar) where the **.etwd** file is saved, **e.g., Dashboards_TrapX DeceptionGrid.etwd** and click **Upload**.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click the **Import** button.

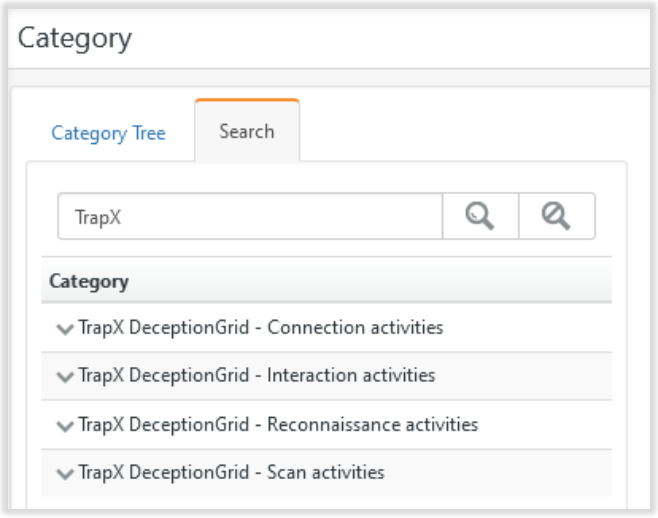




6. Verifying TrapX DeceptionGrid Knowledge Pack in EventTracker

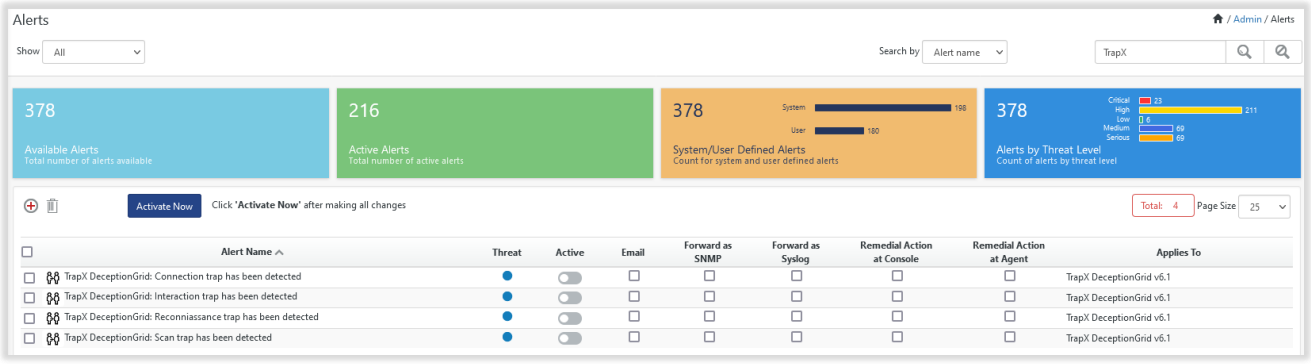
6.1 Categories

1. Login to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree** scroll down and expand the **TrapX DeceptionGrid** group folder to view the imported categories.



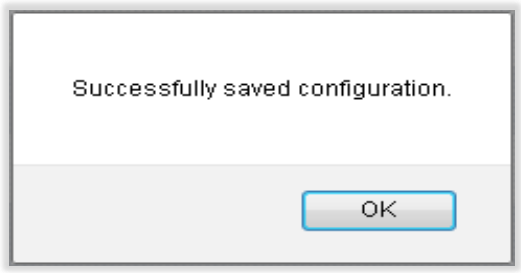
6.2 Alerts

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type **TrapX DeceptionGrid**, and then click the **Go** button.
   The **Alert Management** page will display all the imported alerts.



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

   EventTracker displays a success message.

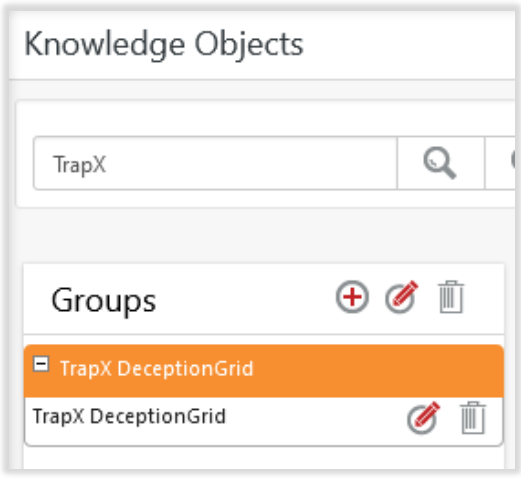


5. Click **OK**, and then click the **Activate Now** button.

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

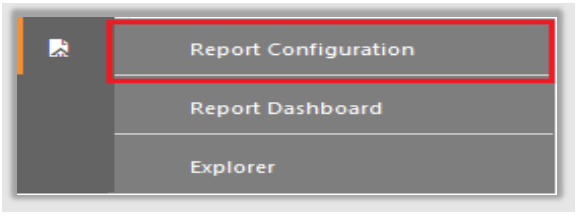
6.3 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Objects** tree, expand the **TrapX DeceptionGrid** group folder to view the imported Knowledge Objects.

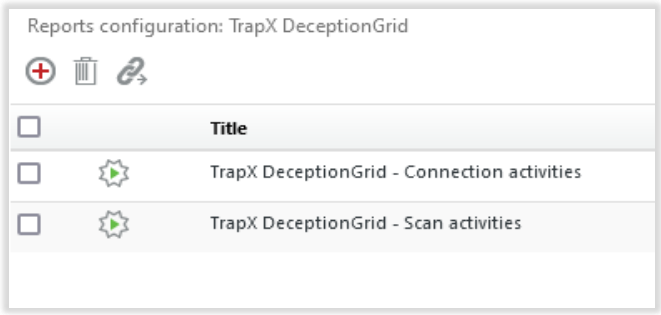


6.4 Reports

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

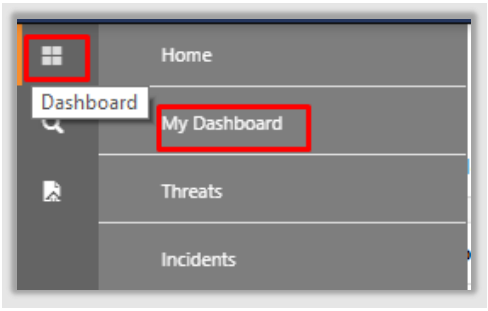


2. In the **Report Configuration** pane, select the **Defined** option.
3. Click the **TrapX DeceptionGrid** group folder to view the imported reports.

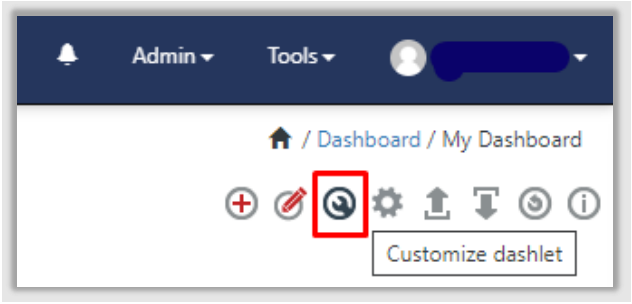


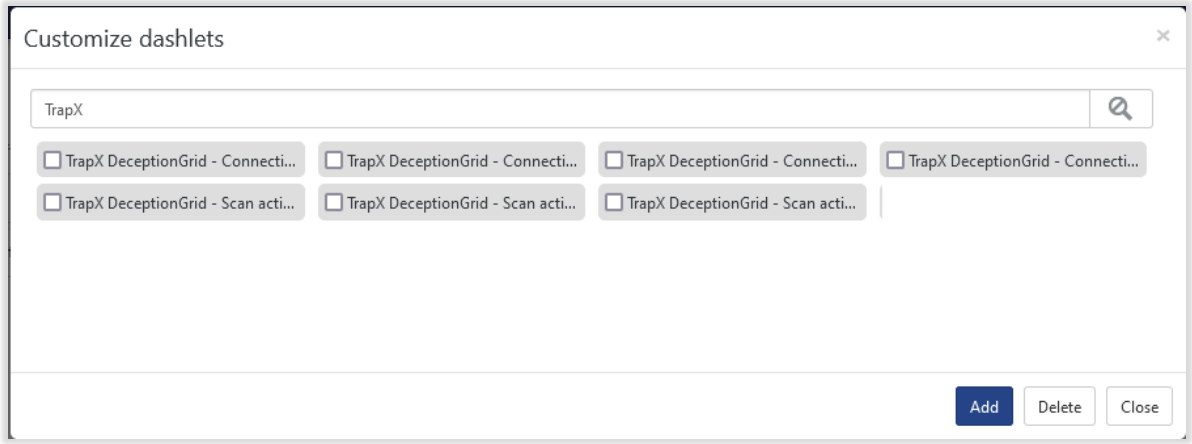
6.5 Dashboards

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



2. Select **Customize dashlets** and type **TrapX DeceptionGrid** in the search bar.





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