Integration Guide

Integrating Azure Kubernetes Service with EventTracker

Publication Date:

March 28, 2022

Abstract

This guide provides instructions to retrieve the **Azure Kubernetes Service** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Azure Kubernetes Service.**

Audience

The Administrators who are assigned the task to monitor the **Azure Kubernetes Service** events using EventTracker.

Table of Contents

1. Overview

Azure Kubernetes Service (AKS) deploys and manages the containerized applications easily with a fully-managed Kubernetes service. It offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver, and scale the applications with confidence.

EventTracker helps to monitor events from the Azure Kubernetes Service. Its dashboard and reports will help you track, delete and update action for the Azure Kubernetes instances, unauthorized deletion could lead to data loss and/or potential denial of service or potentially compromised credentials, and create an action that helps you understand the cluster building with resources.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.

3. Configuring Azure Kubernetes Service to Forward Logs to EventTracker

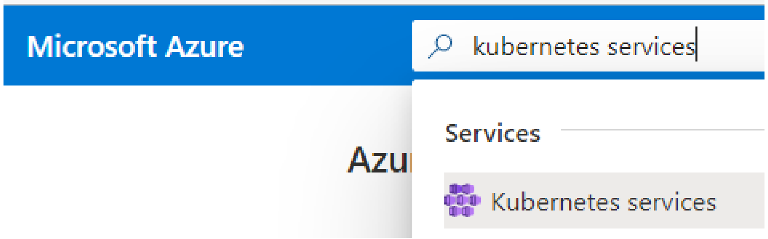
Azure Kubernetes Service can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

Refer to the configuration of Azure function app to forward logs to EventTracker.

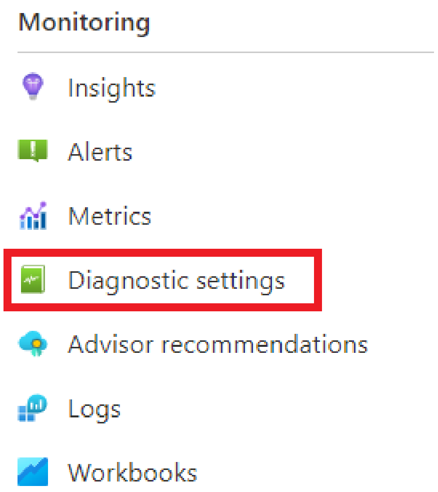
3.2 Configuring Azure Kubernetes Service to stream events to Event Hub

1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **Azure Kubernetes Service** from **All services**.



kubernetes services

3. From the left panel under **Monitoring**, select **Diagnostics settings**.



Monitoring

Insights

Alerts

Metrics

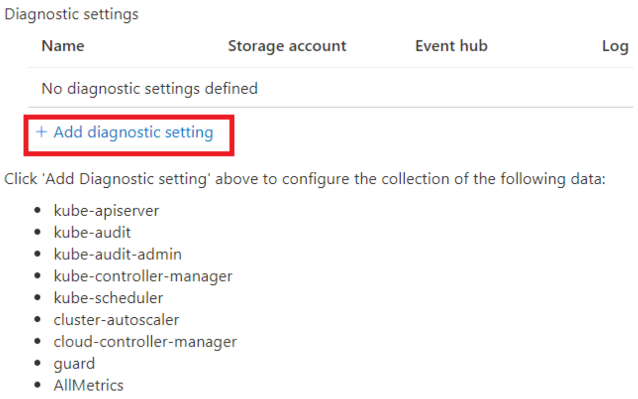
Diagnostic settings

Advisor recommendations

Logs

Workbooks

4. Click **Add diagnostics settings**.



Diagnostic settings

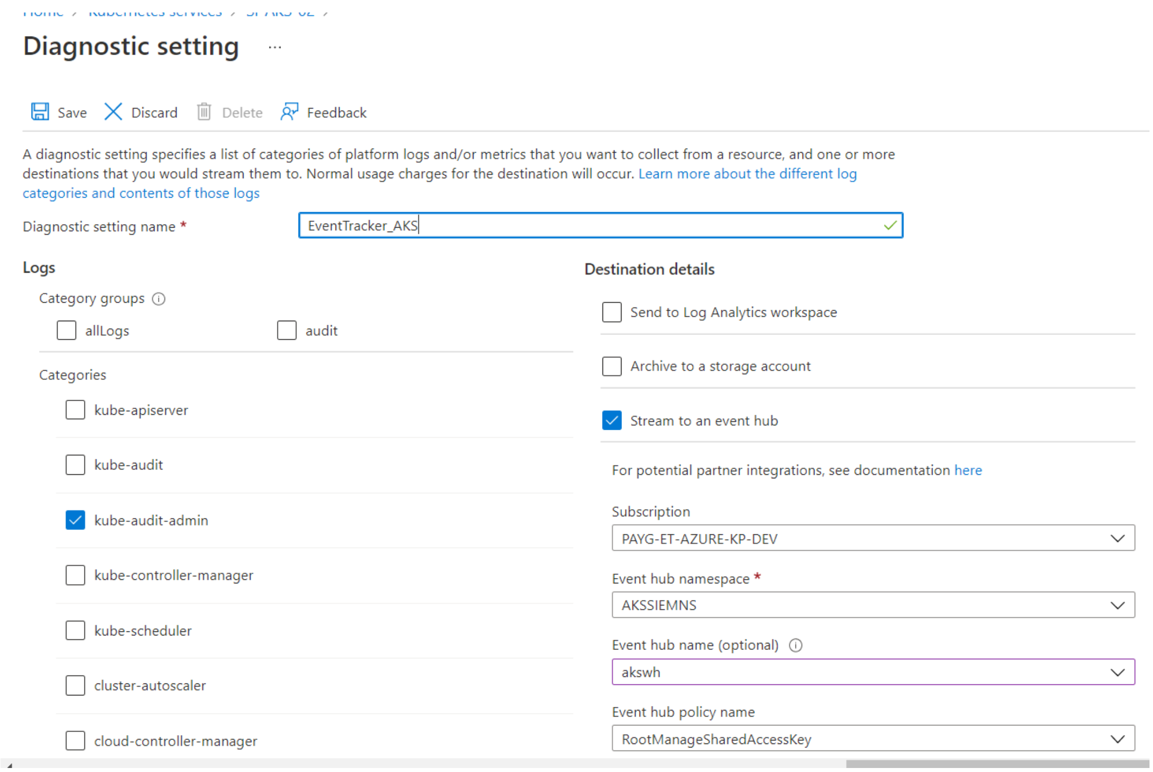
Name	Storage account	Event hub	Log
No diagnostic settings defined			

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- kube-apiserver
- kube-audit
- kube-audit-admin
- kube-controller-manager
- kube-scheduler
- cluster-autoscaler
- cloud-controller-manager
- guard
- AllMetrics

5. Provide the inputs.
   Diagnostics settings name, such as **EventTracker_AKS**.
   Select all **log** types, i.e., kube-audit-admin
   In the **Destination details** section, select **stream to an Event Hub** and then choose the following options.
   - **Subscription:** Select the desired Azure subscription.
   - **Event Hub namespace:** Select the Event Hub namespace.
   - **Event Hub name:** Select the Event Hub created under Event Hub namespace.
   - **Event Hub policy name:** Select the Event Hub policy.
6. Click **OK/Save.**



Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * EventTracker_AKS ✓

Logs

Category groups ⓘ

□ allLogs □ audit

Categories

□ kube-apiserver

□ kube-audit

☑ kube-audit-admin

□ kube-controller-manager

□ kube-scheduler

□ cluster-autoscaler

□ cloud-controller-manager

Destination details

□ Send to Log Analytics workspace

□ Archive to a storage account

☑ Stream to an event hub

For potential partner integrations, see documentation here

Subscription: PAYG-ET-AZURE-KP-DEV

Event hub namespace *: AKSSIEMNS

Event hub name (optional) ⓘ: akswh

Event hub policy name: RootManageSharedAccessKey

4. EventTracker Knowledge Packs

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

The following Knowledge Packs (KPs) are available in EventTracker to support the Azure Kubernetes Service.

4.1 Alerts

- **Azure Kubernetes Service: Deployment deleted -** Containerized applications can be deployed in the Azure Kubernetes Service cluster to render the services. When the deployments delete action is performed, the host will no longer be found. A malicious attempt to delete a deployment could lead to operational issues or potential denial of service. This alert indicates that a delete action was successful on the Azure Kubernetes Deployments.
- **Azure Kubernetes Service: Indication of Cluster deletion -** Azure Kubernetes Service cluster has instances such as nodes, pods, deployments, namespaces, etc. Deleting a cluster leads to the deletion of all the dependencies of the cluster. Unauthorized cluster deletions could lead to the data loss and operational issues for the services it was rendering. This alert indicates that a cluster deletion has occurred on the Azure Kubernetes Service.
- **Azure Kubernetes Service: Node deleted-** Azure Kubernetes Service cluster which has nodes (which run applications), are mapped grouped into node pools. There are no recovery options for the data loss that may occur when a node pool is deleted. This alert indicates that an Azure Kubernetes node deletion has occurred on the Azure Kubernetes Service.

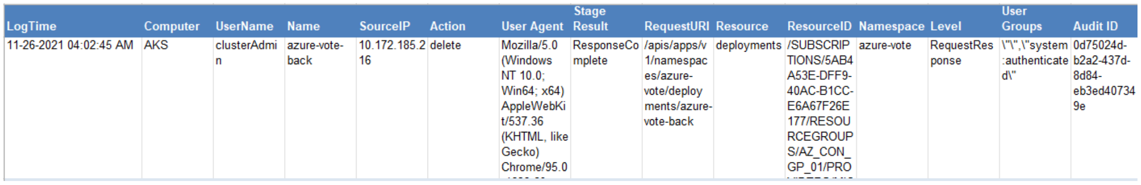
- **Azure Kubernetes Service: Pods deleted -** Azure Kubernetes Service cluster is an instance Pods subset of namespace; Pods contain container image which is used to deploy the end-user applications on the node. This alert indicates successful deletion action on the Azure Kubernetes node.
- **Azure Kubernetes Service: Successful node update -** Azure Kubernetes Service cluster is an instance Node, which was mapped to node pool, when the node pool update action is performed by a user, mapped nodes will get updated. This alert indicates that an Azure Kubernetes node is updated on the Azure Kubernetes Service.
- **Azure Kubernetes Service: Unsuccessful deletion action -** This alert indicates an unsuccessful deletion action performed on the Azure Kubernetes instance/resource.
- **Azure Kubernetes Service: Pod created on kube system:** This alert indicates that a pod was created under the kube system namespace in the Azure Kubernetes Service.

4.2 Categories

- **Azure Kubernetes Service - Successful Update action-** This category of the saved search will allow users to parse events that are specific to the successful update action on the Azure Kubernetes Service.
- **Azure Kubernetes Service - Successful delete action-** This category of the saved search will allow users to parse events specific to the successful deletion action on the Azure Kubernetes Service.

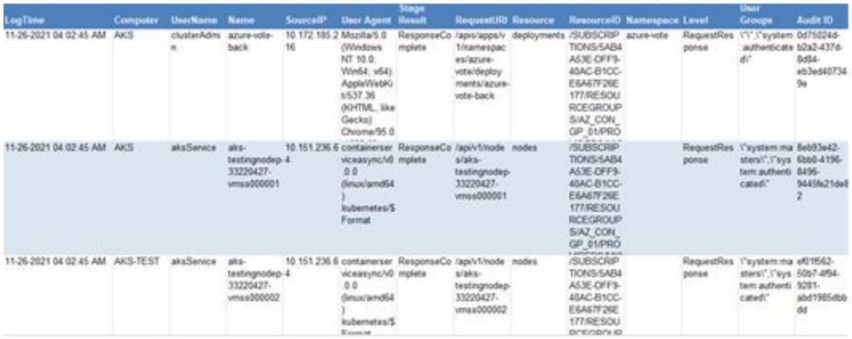
4.3 Reports

- **Azure Kubernetes Service – Cluster activity:** This report provides a detailed summary of create actions, delete actions performed /triggered on the cluster instance in the Azure Kubernetes Service. It contains a source IP address, username, request URL, resource, user groups, action, and more.



LogTime	Computer	UserName	Name	SourceIP	Action	User Agent	Stage Result	RequestURI	Resource	ResourceID	Namespace	Level	User Groups	Audit ID
11-26-2021 04:02:45 AM	AKS	clusterAdmin	azure-vote-back	10.172.185.216	delete	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0	ResponseComplete	/apis/apps/v1/namespaces/azure-vote/deployments/azure-vote-back	deployments	/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PRO	azure-vote	RequestResponse	\"\",\"system:authenticated\"	0d75024d-b2a2-437d-8d84-eb3ed407349e

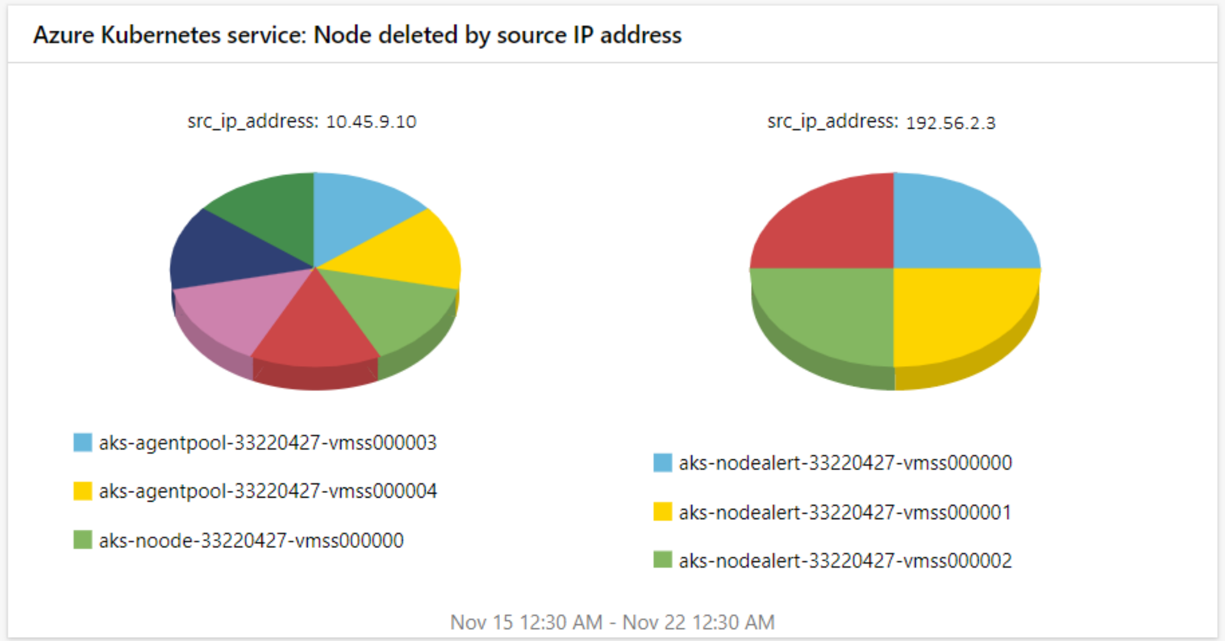
- **Azure Kubernetes Service – Cluster update activity:** This report provides a detailed summary of update actions performed /triggered on the cluster instance in the Azure Kubernetes Service. It contains a source IP address, username, request URL, resource, user groups, and more.



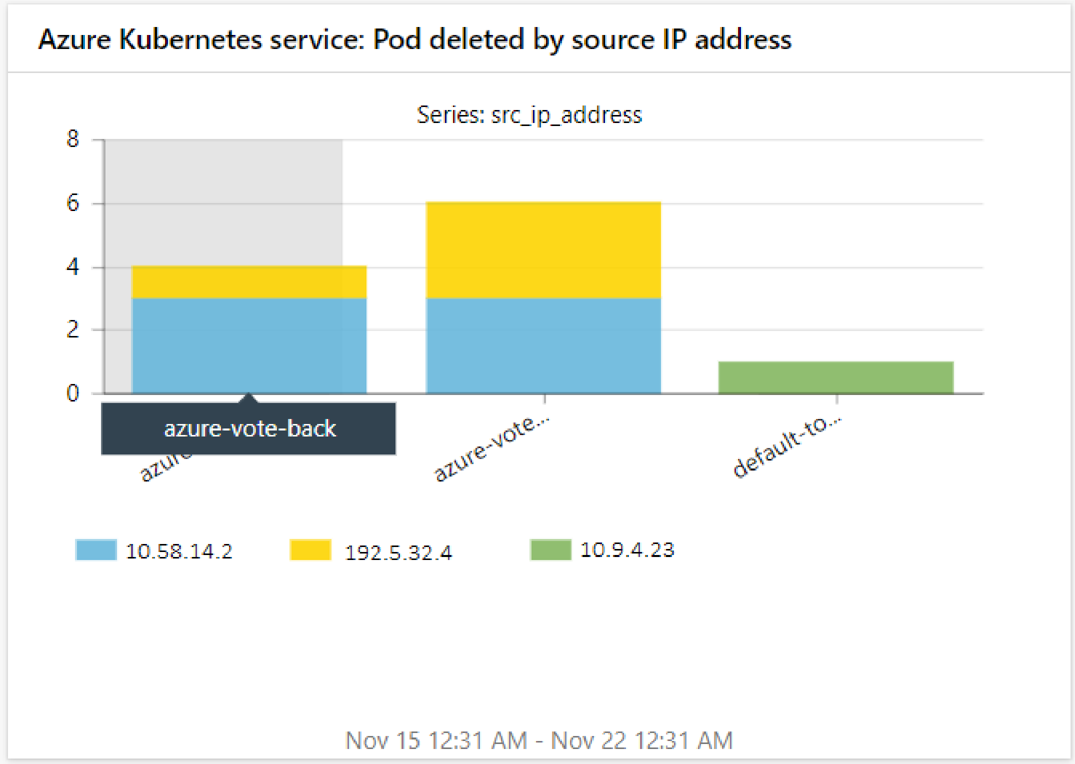
LogTime	Computer	UserName	Name	SourceIP	User Agent	Stage Result	RequestURI	Resource	ResourceID	Namespace	Level	User Groups	Audit ID
11-26-2021 04:02:45 AM	AKS	clusterAdmin	azure-vote-back	10.172.185.216	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0	ResponseComplete	/apis/apps/v1/namespaces/azure-vote/deployments/azure-vote-back	deployments	/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PRO	azure-vote	RequestResponse	\"\",\"system:authenticated\"	0d75024d-b2a2-437d-8d84-eb3ed407349e
11-26-2021 04:02:45 AM	AKS	aksService	aks-testingnodep-33220427-vmss000001	10.151.236.64	containerserviceasync/v0.0.0 (linux/amd64) kubernetes/$Format	ResponseComplete	/api/v1/nodes/aks-testingnodep-33220427-vmss000001	nodes	/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PRO		RequestResponse	\"system:masters\",\"system:authenticated\"	8eb93e42-6bb0-4196-8496-9445fe21de82
11-26-2021 04:02:45 AM	AKS-TEST	aksService	aks-testingnodep-33220427-vmss000002	10.151.236.64	containerserviceasync/v0.0.0 (linux/amd64) kubernetes/$	ResponseComplete	/api/v1/nodes/aks-testingnodep-33220427-vmss000002	nodes	/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOU		RequestResponse	\"system:masters\",\"system:authenticated\"	ef01f562-50b7-4f94-9281-abd1985dbbdd

4.4 Dashboards

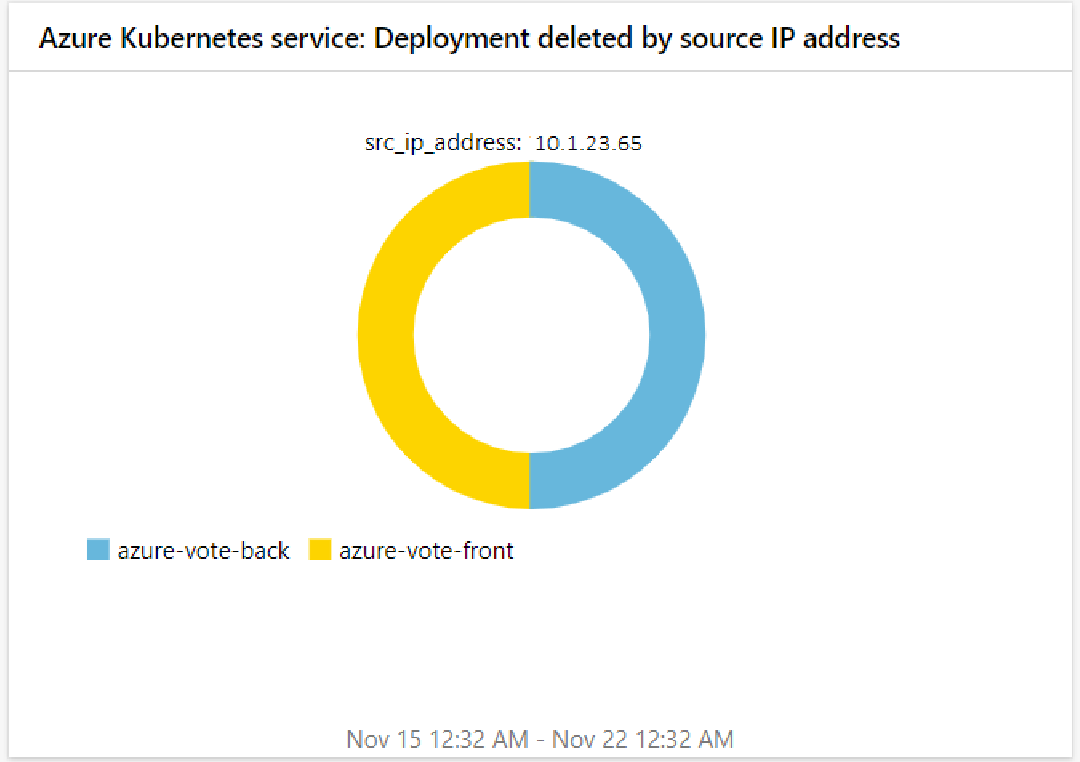
- **Azure Kubernetes Service: Node deleted by the source IP Address**


Azure Kubernetes service: Node deleted by source IP address
src_ip_address: 10.45.9.10
src_ip_address: 192.56.2.3
aks-agentpool-33220427-vmss000003
aks-agentpool-33220427-vmss000004
aks-noode-33220427-vmss000000
aks-nodealert-33220427-vmss000000
aks-nodealert-33220427-vmss000001
aks-nodealert-33220427-vmss000002
Nov 15 12:30 AM - Nov 22 12:30 AM

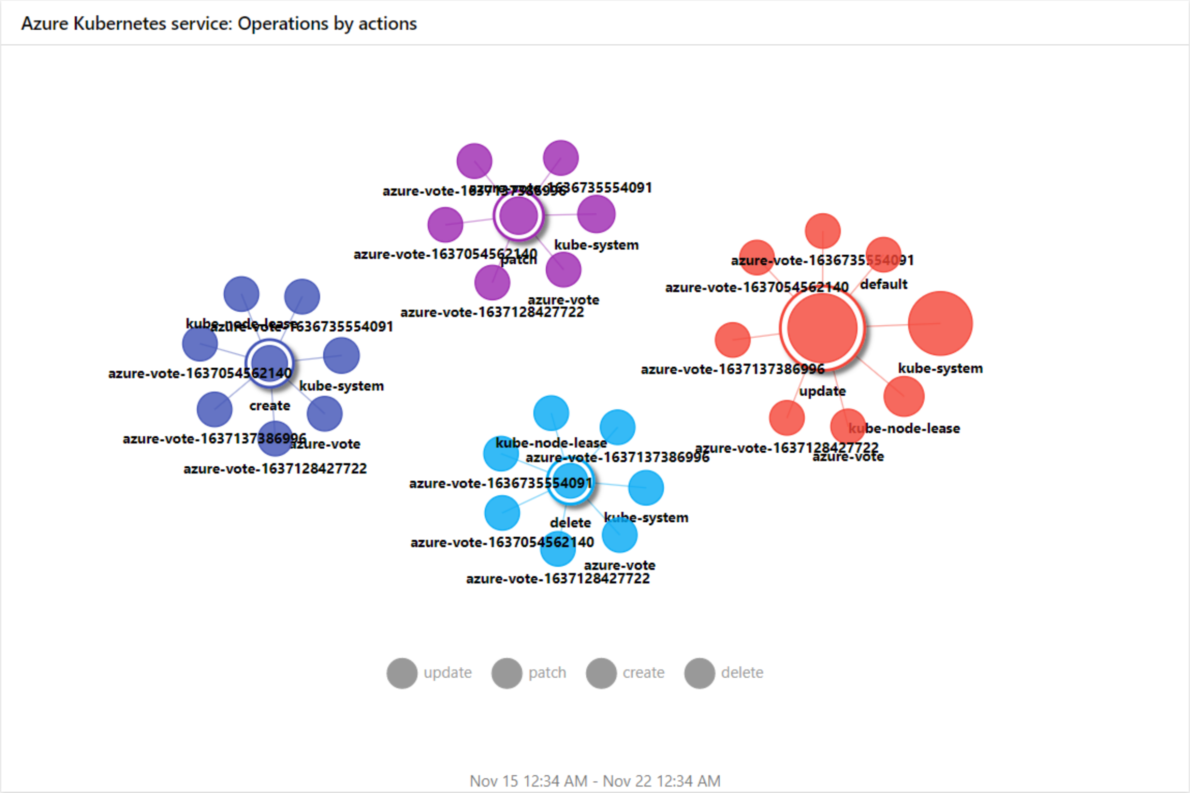
- **Azure Kubernetes Service: Pod deleted by the source IP Address**



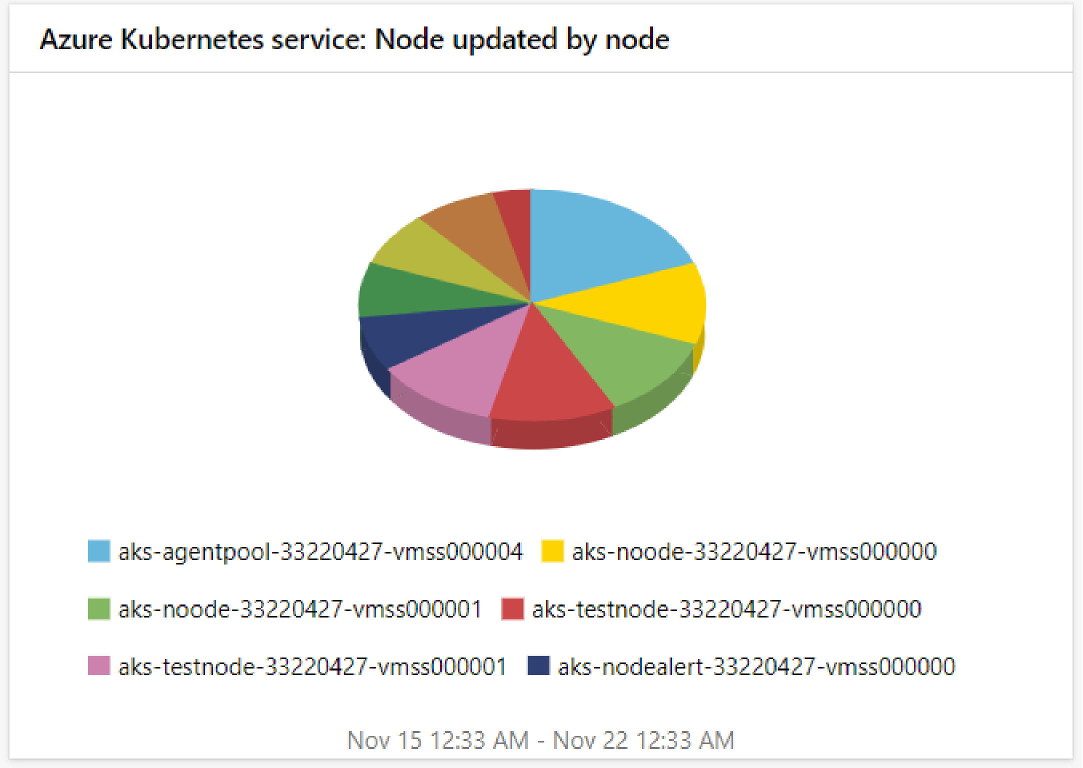
- **Azure Kubernetes Service: Deployment deleted by the source IP Address**



- **Azure Kubernetes Service: Operations by actions**



- **Azure Kubernetes Service: Node updated by node**



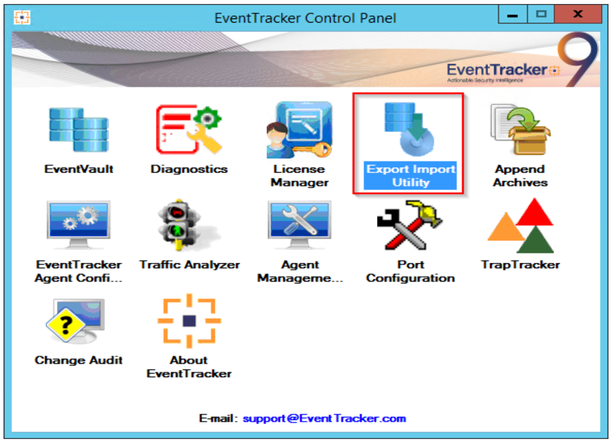
Azure Kubernetes service: Node updated by node

5. Importing Azure Kubernetes Service Knowledge Packs into EventTracker

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

- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

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

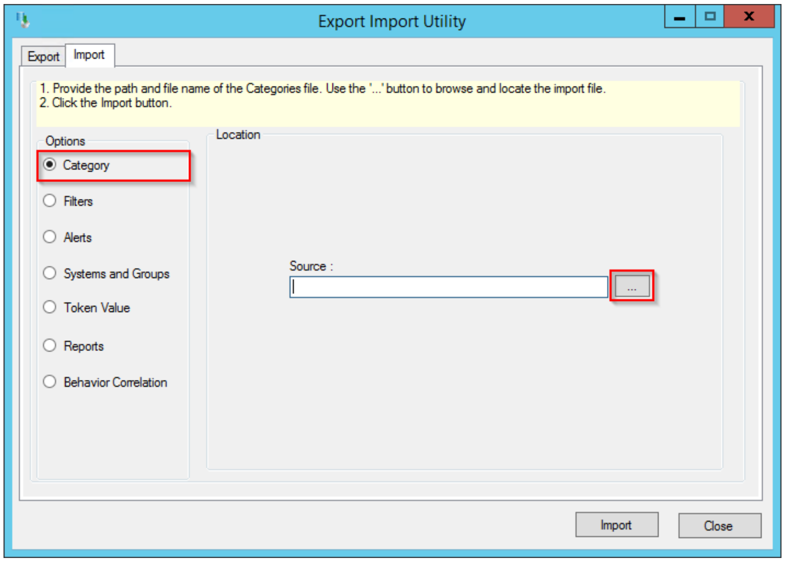


E-mail: support@EventTracker.com

3. Click the **Import** tab.

5.1 Categories

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

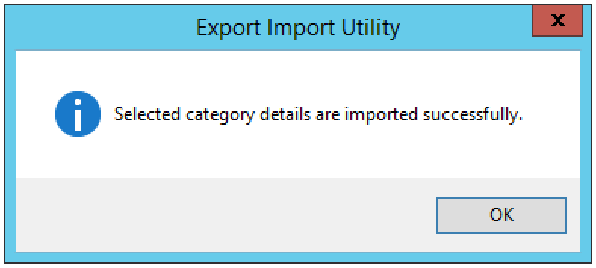


1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

2. Locate the **Categories_Microsoft AKS.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

EventTracker displays a success message.

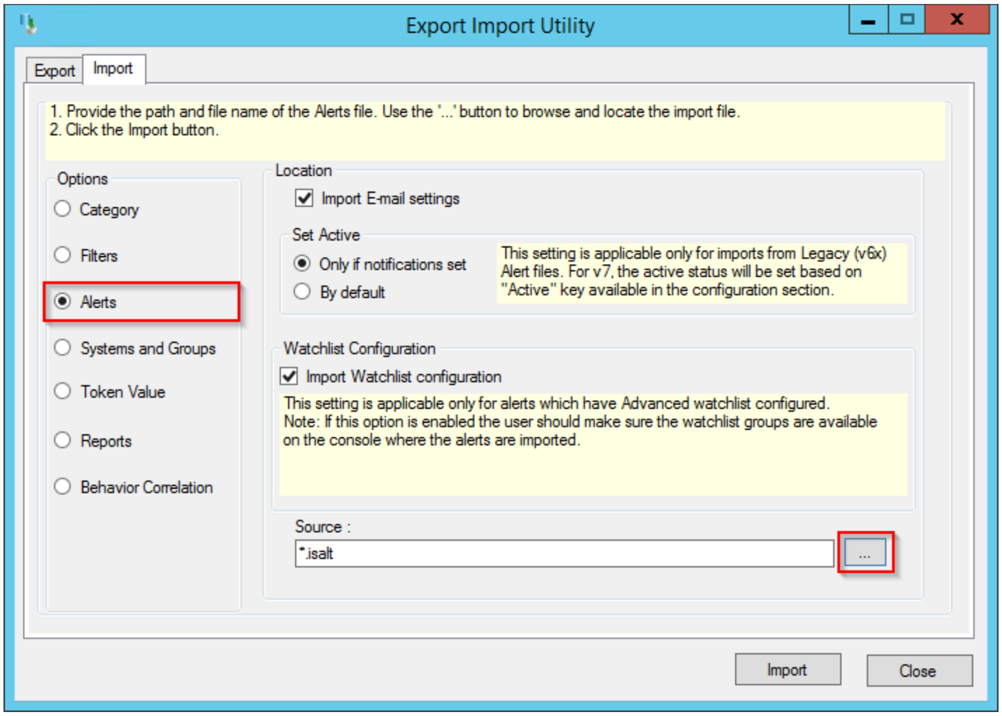


Selected category details are imported successfully.

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

5.2 Alerts

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



Export Import Utility

Export | Import

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options
- ○ Category
- ○ Filters
- ● Alerts
- ○ Systems and Groups
- ○ Token Value
- ○ Reports
- ○ Behavior Correlation

Location

☑ Import E-mail settings

Set Active
- ● Only if notifications set
- ○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration

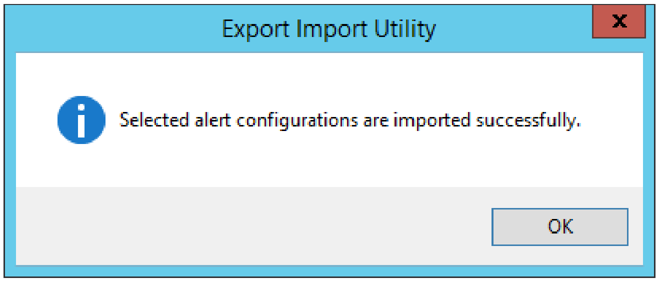
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt ...

Import | Close

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



Export Import Utility

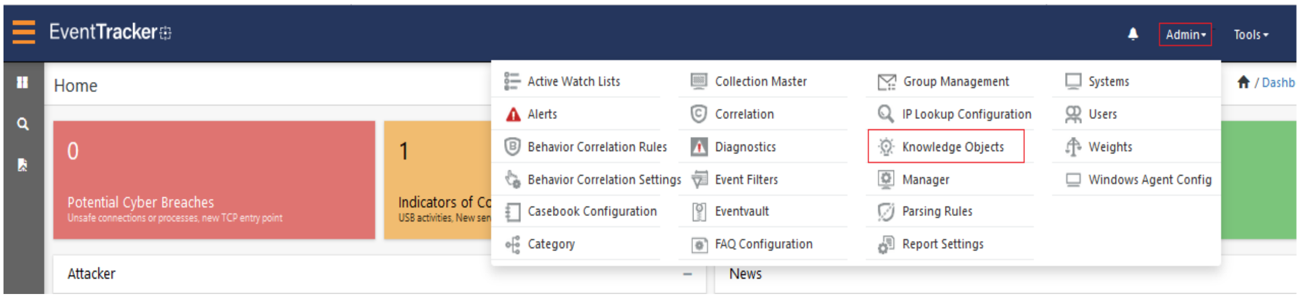
Selected alert configurations are imported successfully.

OK

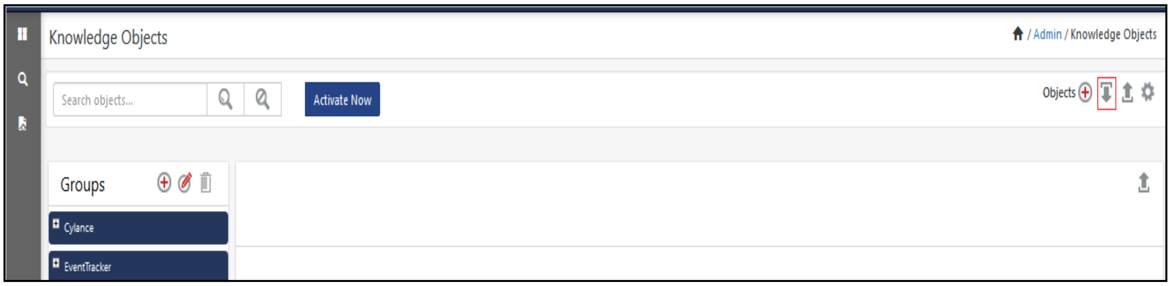
4. Click **OK**, and then click **Close**.

5.3 Knowledge Objects (KO)

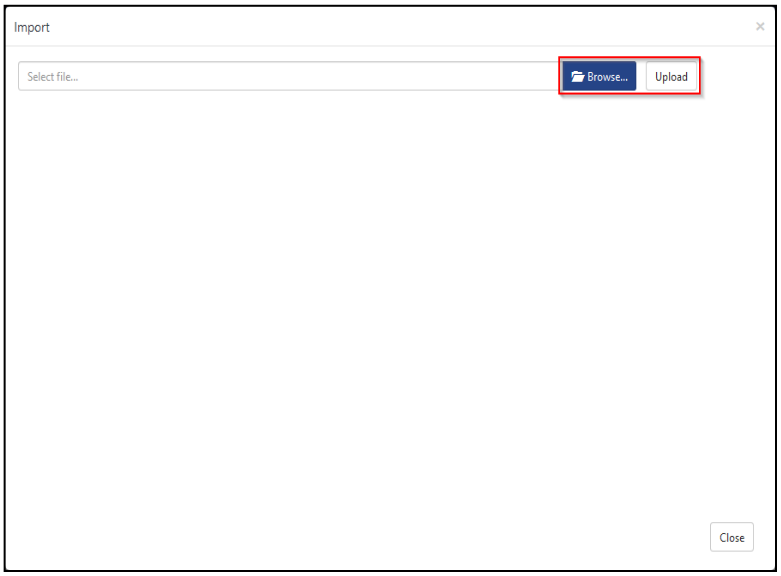
1. Click **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.



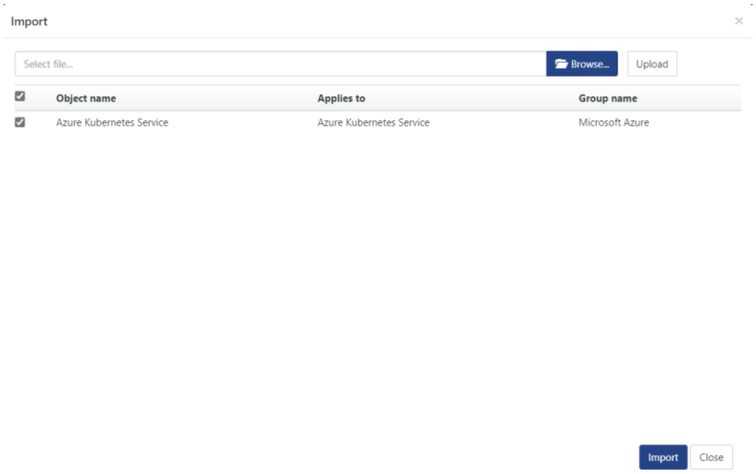
2. Click the **Import** button as highlighted in the below image:



3. Click **Browse**.



4. Locate the file named **KO_Microsoft AKS.etko**.
5. Select the check box and then click the **Import** option.

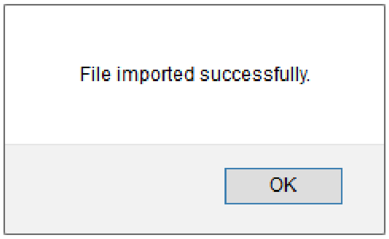


Import

Select file... | Browse... | Upload

☑	Object name	Applies to	Group name
☑	Azure Kubernetes Service	Azure Kubernetes Service	Microsoft Azure

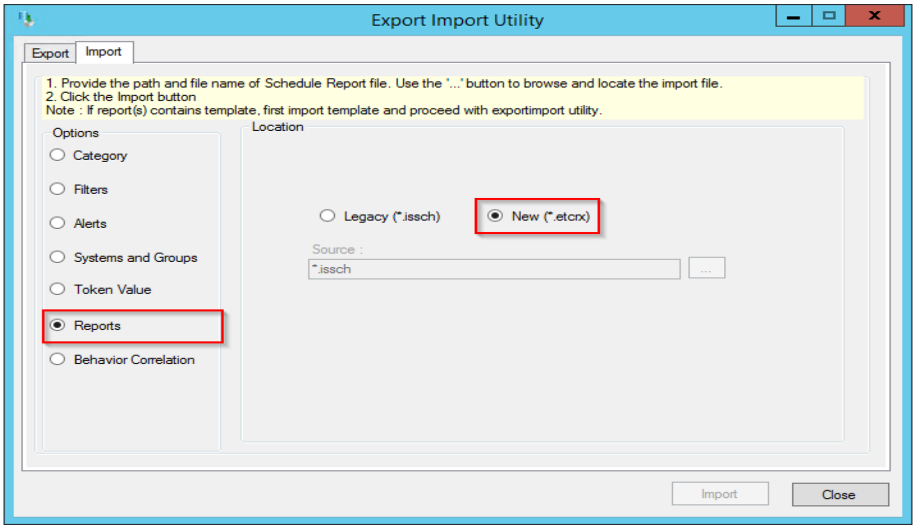
6. The Knowledge Objects (KO) are now imported successfully.



File imported successfully.

5.4 Reports

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



Export Import Utility

Export | Import

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

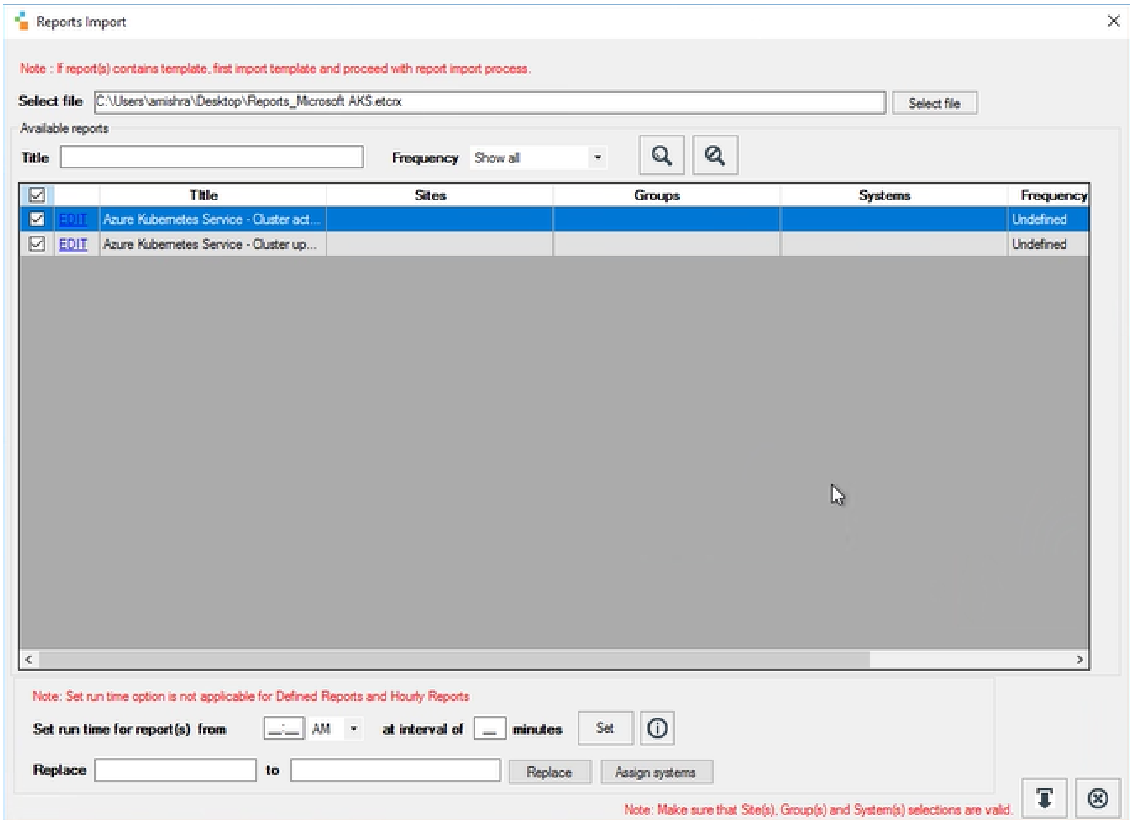
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

2. Locate the file named **Reports_ Microsoft AKS.etcrx** and select all the check boxes.



Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

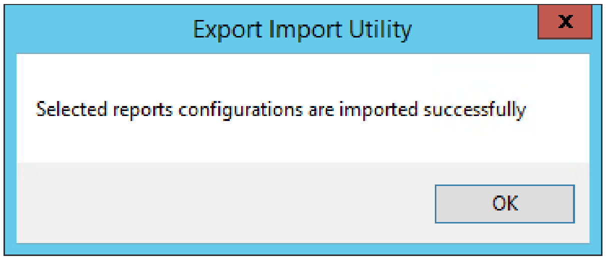
Select file C:\Users\amishra\Desktop\Reports_Microsoft AKS.etcrx

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Azure Kubernetes Service - Cluster act...				Undefined
☑	EDIT	Azure Kubernetes Service - Cluster up...				Undefined

Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

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



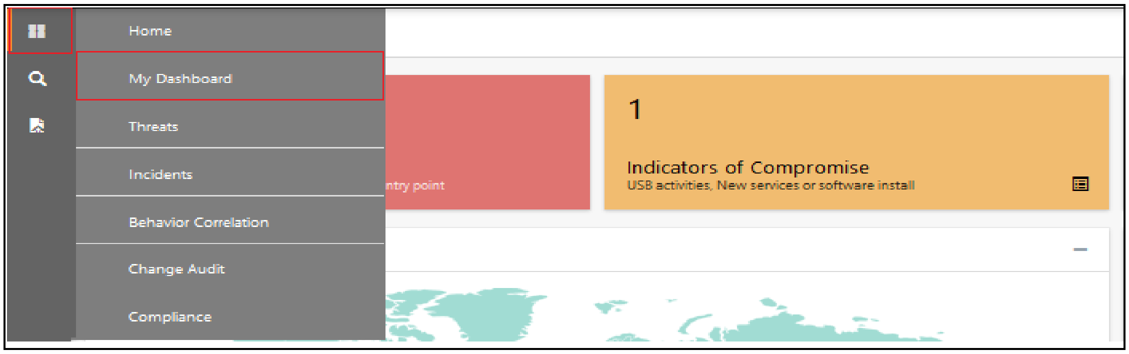
Export Import Utility

Selected reports configurations are imported successfully

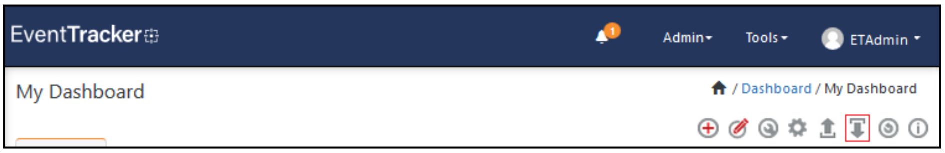
5.5 Dashboards

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

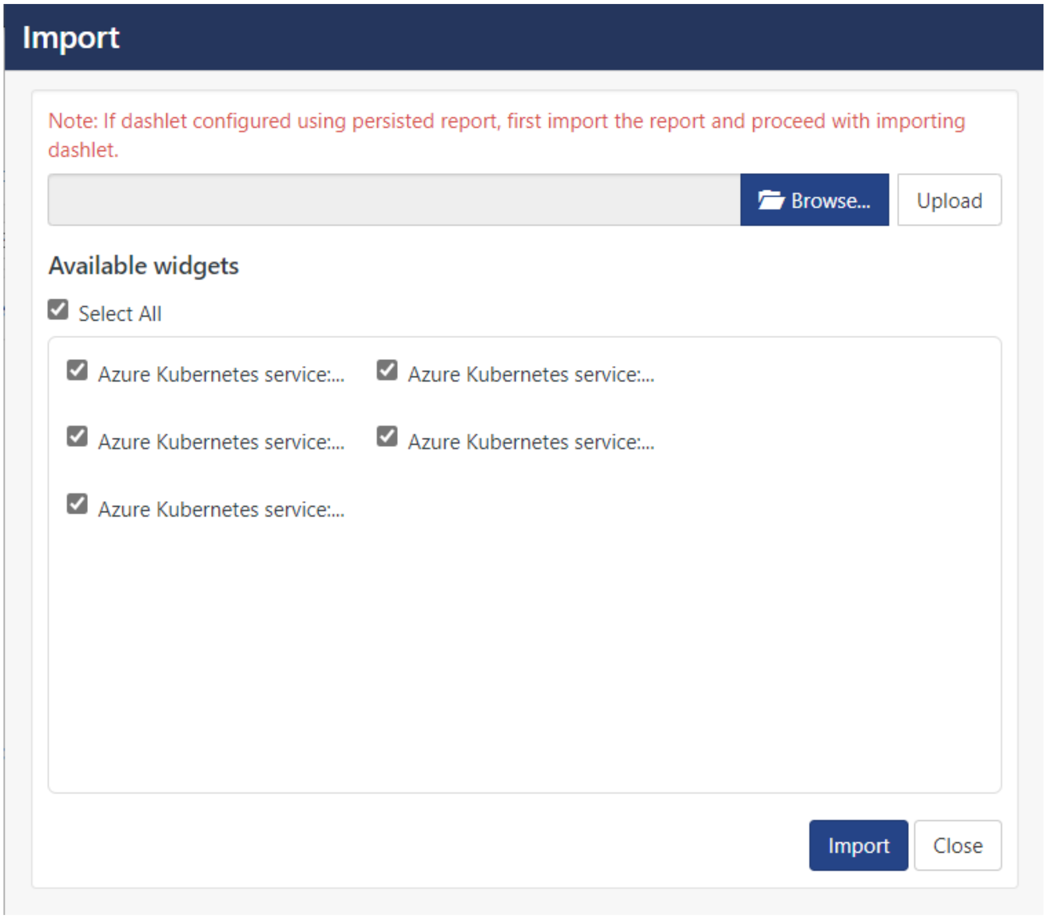
1. Open **EventTracker** in a browser and log on.



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



4. Import the dashboard file **Dashboards_Microsoft AKS.etwd** and select the **Select All** checkbox**.**
5. Click **Import** as shown below.



Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Available widgets

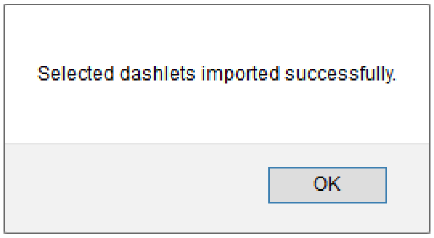
☑ Select All

☑ Azure Kubernetes service:... ☑ Azure Kubernetes service:...

☑ Azure Kubernetes service:... ☑ Azure Kubernetes service:...

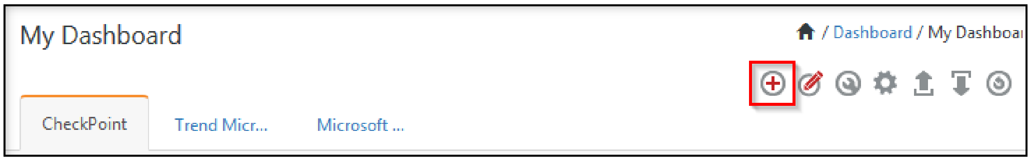
☑ Azure Kubernetes service:...

6. Import is now completed successfully.

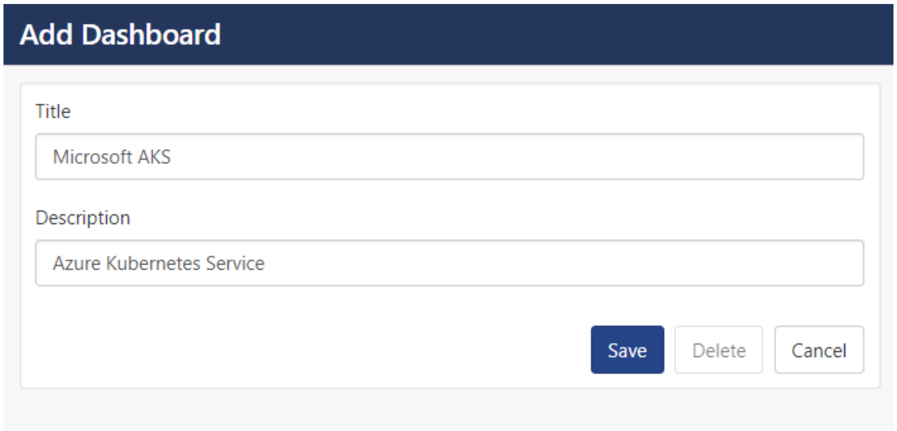


Selected dashlets imported successfully.

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



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

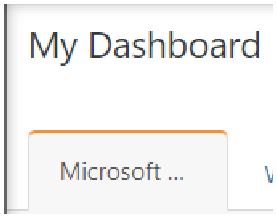


Add Dashboard

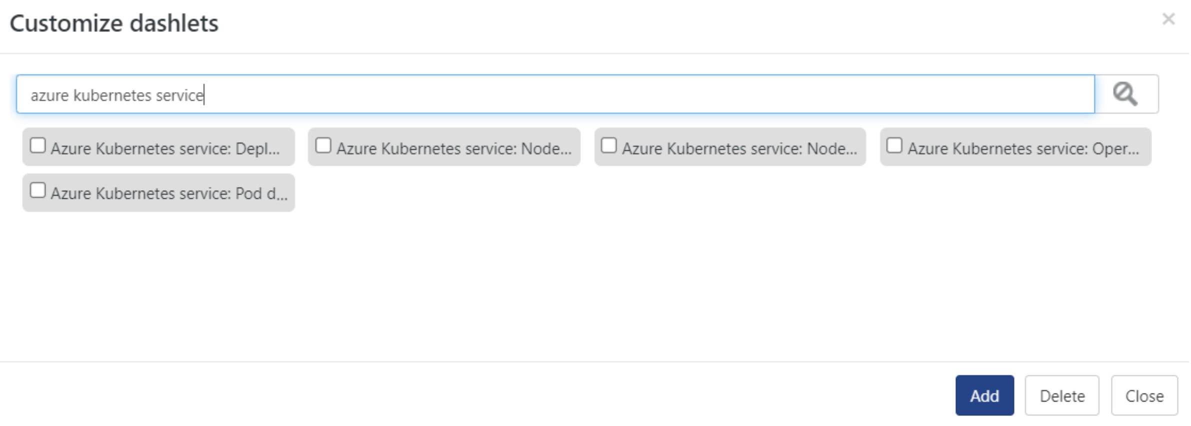
Title: Microsoft AKS

Description: Azure Kubernetes Service

9. On the **My Dashboard** page select ◔ to add dashlets.



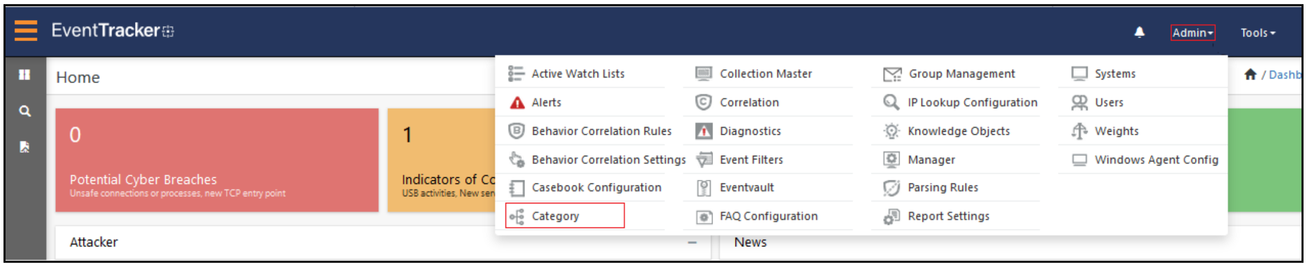
10. Select the imported dashlets and click **Add**.


Customize dashlets
azure kubernetes service
☐ Azure Kubernetes service: Depl...
☐ Azure Kubernetes service: Node...
☐ Azure Kubernetes service: Node...
☐ Azure Kubernetes service: Oper...
☐ Azure Kubernetes service: Pod d...
Add
Delete
Close

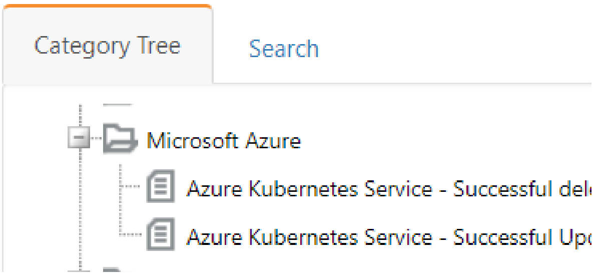
6. Verifying Azure Kubernetes Service Knowledge Packs in EventTracker

6.1 Categories

1. Log onto **EventTracker**.
2. Click the **Admin** dropdown, and then click **Category**.

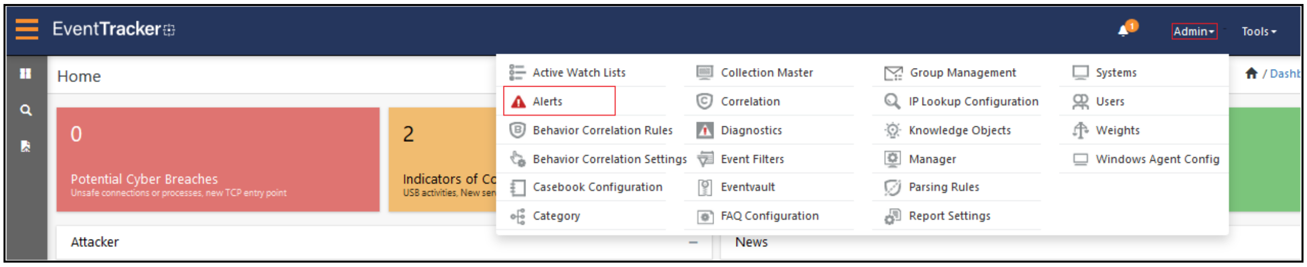


3. In the **Category Tree**, scroll down and expand the **Microsoft Azure** group folder to view the imported category.

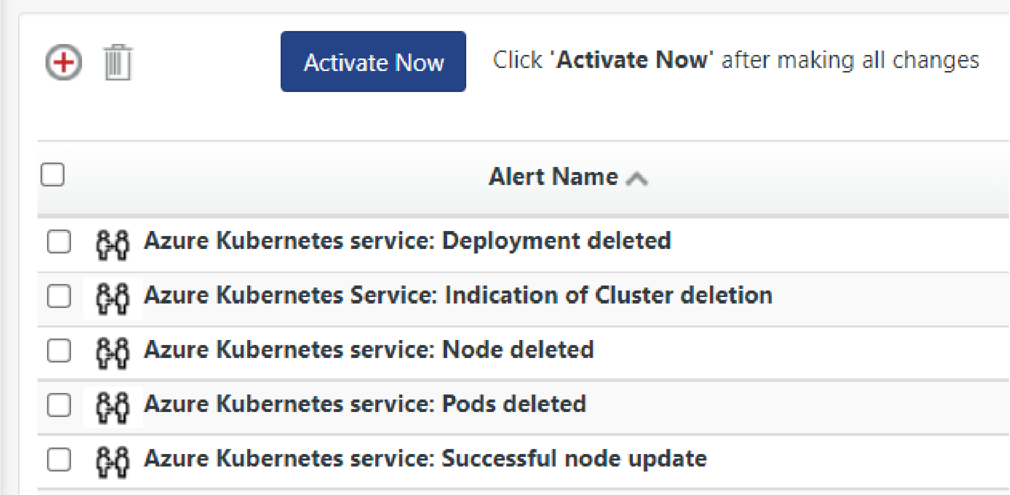

Category Tree
Search
Microsoft Azure
Azure Kubernetes Service - Successful del
Azure Kubernetes Service - Successful Upd

6.2 Alerts

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



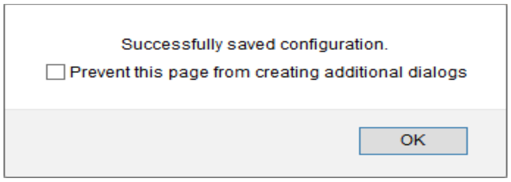
3. In the **Search** box, type **Azure Kubernetes Service**, and then click the **Go** button.
   The Alert Management page will display the imported alert.



□	Alert Name
□	Azure Kubernetes service: Deployment deleted
□	Azure Kubernetes Service: Indication of Cluster deletion
□	Azure Kubernetes service: Node deleted
□	Azure Kubernetes service: Pods deleted
□	Azure Kubernetes service: Successful node update

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

   EventTracker displays a message box.



Successfully saved configuration.

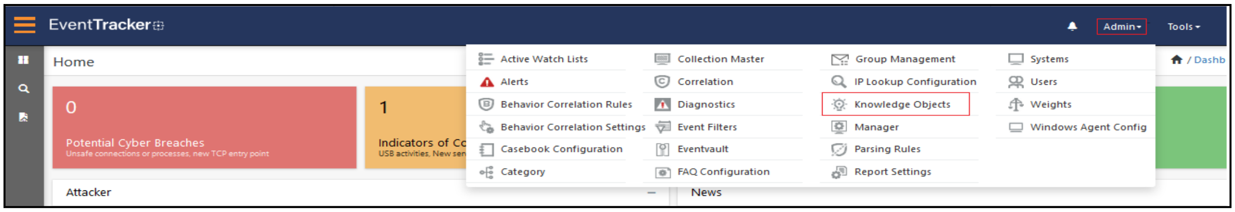
□ Prevent this page from creating additional dialogs

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

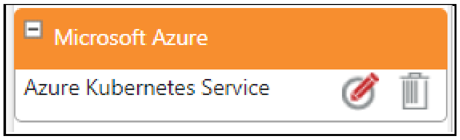
NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

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



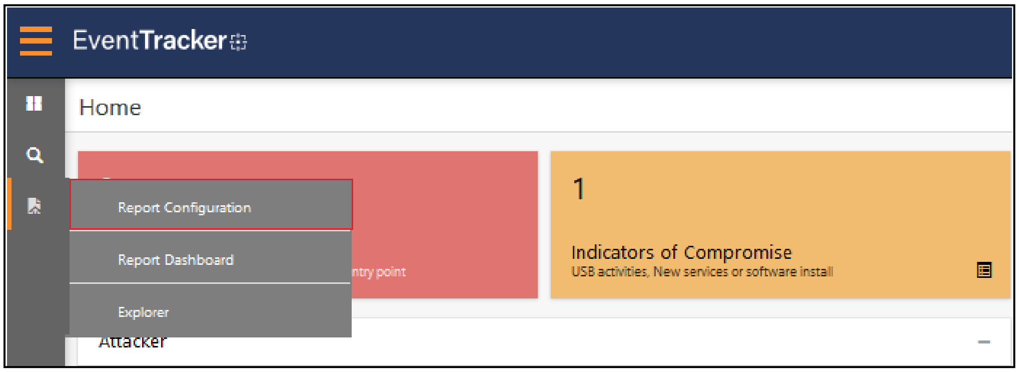
2. In the Knowledge Object tree, expand the **Microsoft Azure group** folder to view the imported Knowledge Objects.



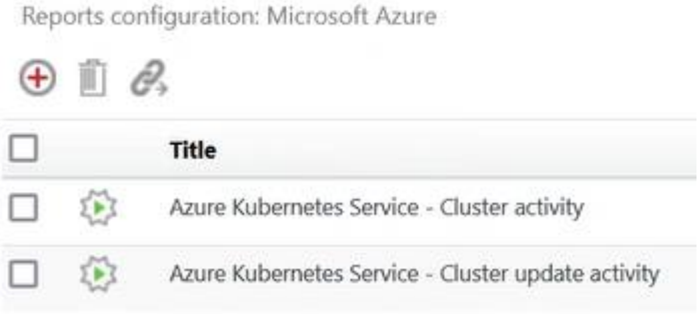
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.4 Reports

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



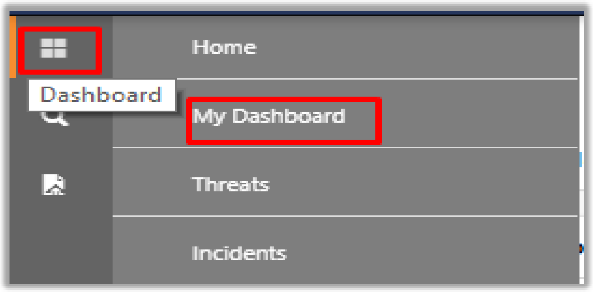
2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Microsoft Azure** group folder to view the imported reports.


Reports configuration: Microsoft Azure

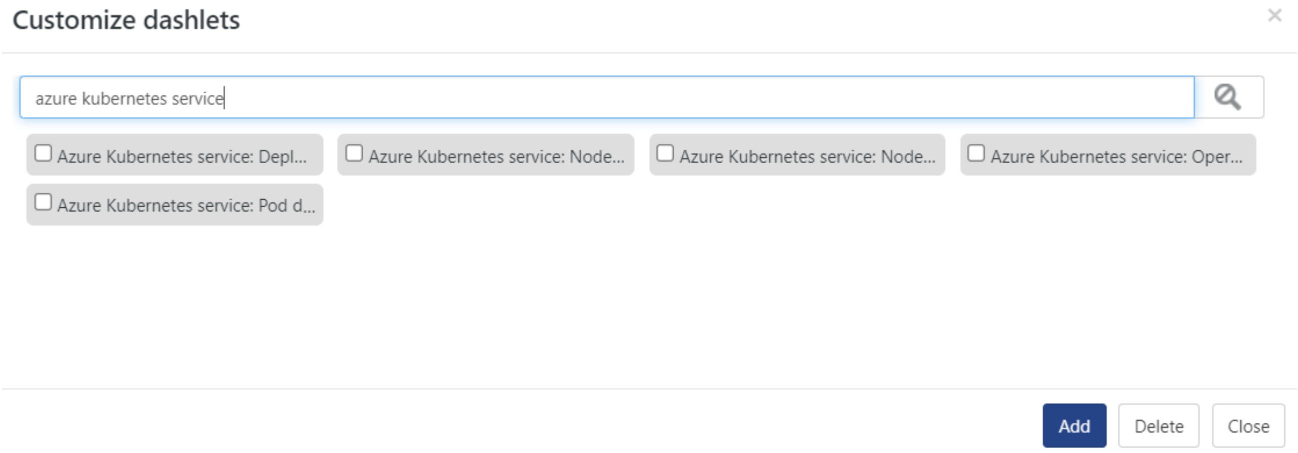
□		Title
□		Azure Kubernetes Service - Cluster activity
□		Azure Kubernetes Service - Cluster update activity

6.5 Dashboards

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



2. Click **Search** for the **Azure Kubernetes Service.** You will see the following screen.


Customize dashlets

azure kubernetes service

□ Azure Kubernetes service: Depl...
□ Azure Kubernetes service: Node...
□ Azure Kubernetes service: Node...
□ Azure Kubernetes service: Oper...
□ Azure Kubernetes service: Pod d...

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