Integration Guide

Integrating Cisco® Secure Endpoint with EventTracker

Publication Date:

May 17, 2022

Abstract

This guide provides instructions to retrieve the **Cisco® Secure Endpoint** events via remote syslog. Once the logs start coming into EventTracker, then reports, dashboards, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Cisco® Secure Endpoint.**

Audience

Administrators who are assigned the task to monitor the **Cisco® Secure Endpoint** events using EventTracker.

Table of Contents

Table of Contents 3
1. Overview 4
2. Prerequisites 4
3. Integration of Cisco® Secure Endpoint events to EventTracker 4
4. EventTracker Knowledge Packs 8
4.1 Category 8
4.2 Alerts 8
4.3 Reports 8
5. Importing Cisco® Secure Endpoint Knowledge Pack into EventTracker 8
5.1 Category 9
5.2 Alerts 10
5.3 Knowledge Objects (KOs) 11
5.4 Reports 12
6. Verifying Cisco® Secure Endpoint Knowledge Pack in EventTracker 14
6.1 Category 14
6.2 Alerts 14
6.3 Knowledge Objects 15
6.4 Report 16
About Netsurion 17
Contact Us 17

1. Overview

Cisco® Secure Endpoint (formerly AMP for Endpoints) integrates prevention, detection, threat hunting, and response capabilities in a single solution, leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through public or private cloud deployment.

EventTracker helps to monitor events from Cisco® Secure Endpoint. Its knowledge objects and flex reports will help you to analyse scanning details, threat detection and quarantine details, vulnerable application details, as well as suspicious and system activities.

2. Prerequisites

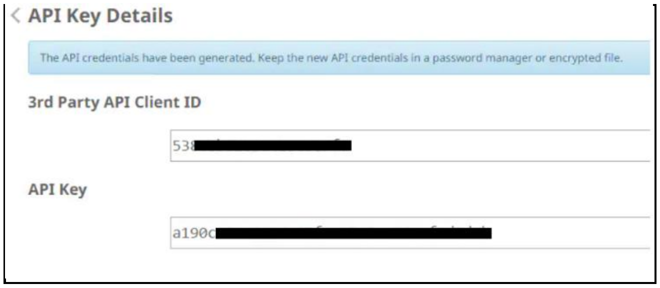
- **EventTracker v9.x or above** should be installed.
- A user with global administrator access of Cisco® Secure Endpoint.
- Administrative access on EventTracker.

3. Integration of Cisco® Secure Endpoint events to EventTracker

To configure the Cisco® Secure Endpoint integration.

Generating Client ID and API Key:

1. Log into https://console.amp.cisco.com/ (N.A.) or https://console.eu.amp.cisco.com/ (E.U.)
2. Go to the **Business Page** from the **Accounts** dropdown menu.
3. Click the **Edit** button.
4. Under features, click the **Regenerate** button beside **3rd Party API Access** to generate the **Client ID** and **secure API Key**
5. Once you have the **API client ID** and **API key**, you can get the logs as follows:



< API Key Details

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

3rd Party API Client ID

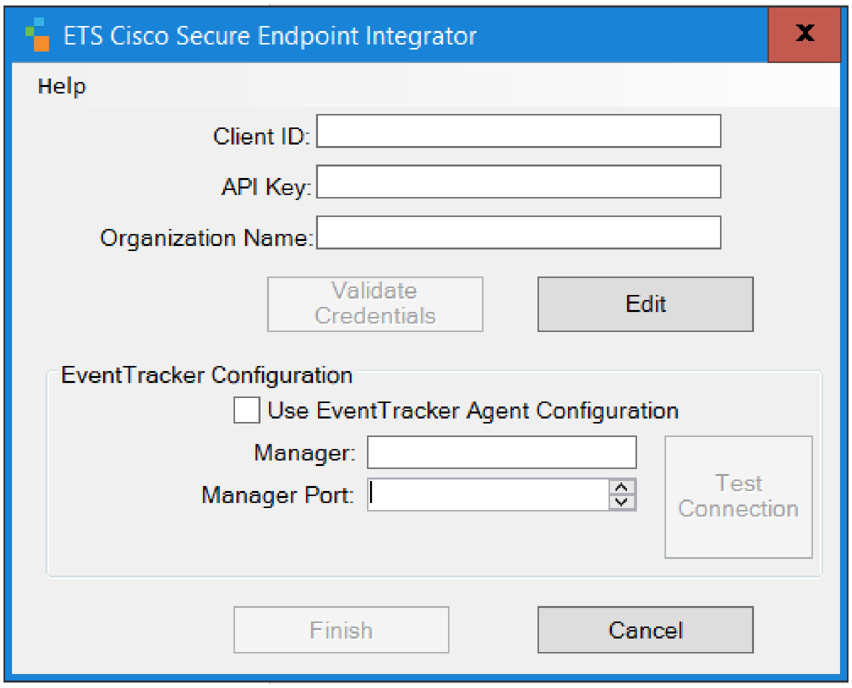
53[redacted]

API Key

a190c[redacted]

Following are the steps to integrate Cisco Secure Endpoint into EventTracker.

1. Get the **Cisco® Secure Endpoint** executable file:
   https://downloads.eventtracker.com/kp-integrator/ETS_Cisco Secure Endpoint_Integrator.exe
2. Once the executable application is received, click the file **ETS_Cisco Secure Endpoint_Configure**.



Client ID:

API Key:

Organization Name:

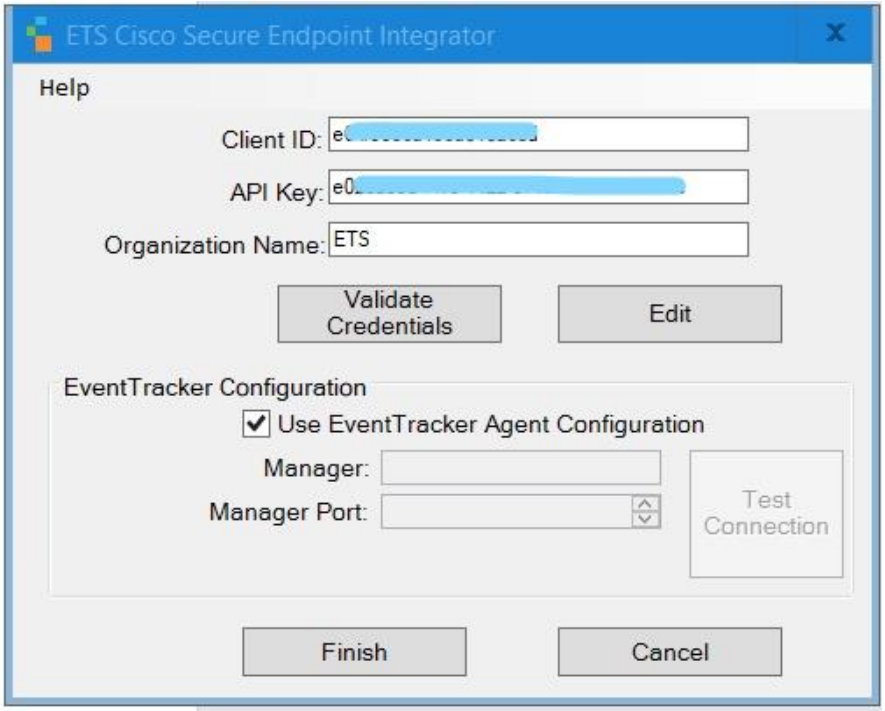
EventTracker Configuration

☐ Use EventTracker Agent Configuration

Manager:

Manager Port:

3. **Cisco® Secure Endpoint Integrator** window is displayed. Fill in the **Client ID**, and **API Key** as received from the web interface of Cisco® Secure Endpoint, and provide the **Organization Name**.



Client ID: e[redacted]

API Key: e0[redacted]

Organization Name: ETS

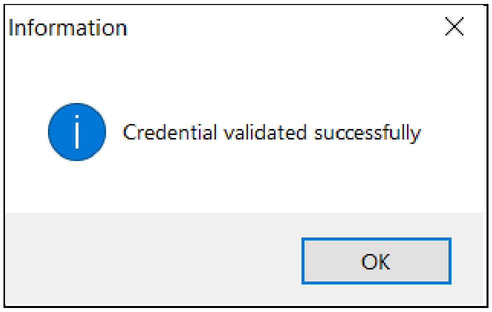
EventTracker Configuration

☑ Use EventTracker Agent Configuration

Manager:

Manager Port:

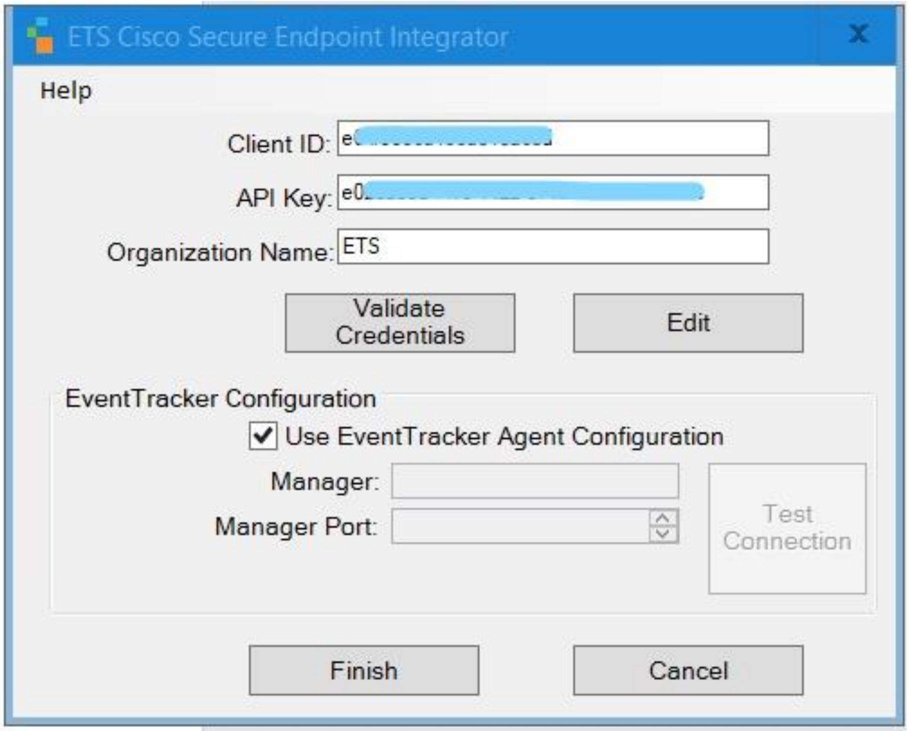
4. Once you have filled out the fields, click the **Validate** button to check if the credentials are correct and working properly.



Information

Credential validated successfully

5. If the **Agent** is installed on the server where the program is launching, the **EventTracker Agent Configuration** check box is enabled to use the Agent machine **etaconfig.ini** file manager details to send the logs.



ETS Cisco Secure Endpoint Integrator

Client ID: e[redacted]

API Key: e0[redacted]

Organization Name: ETS

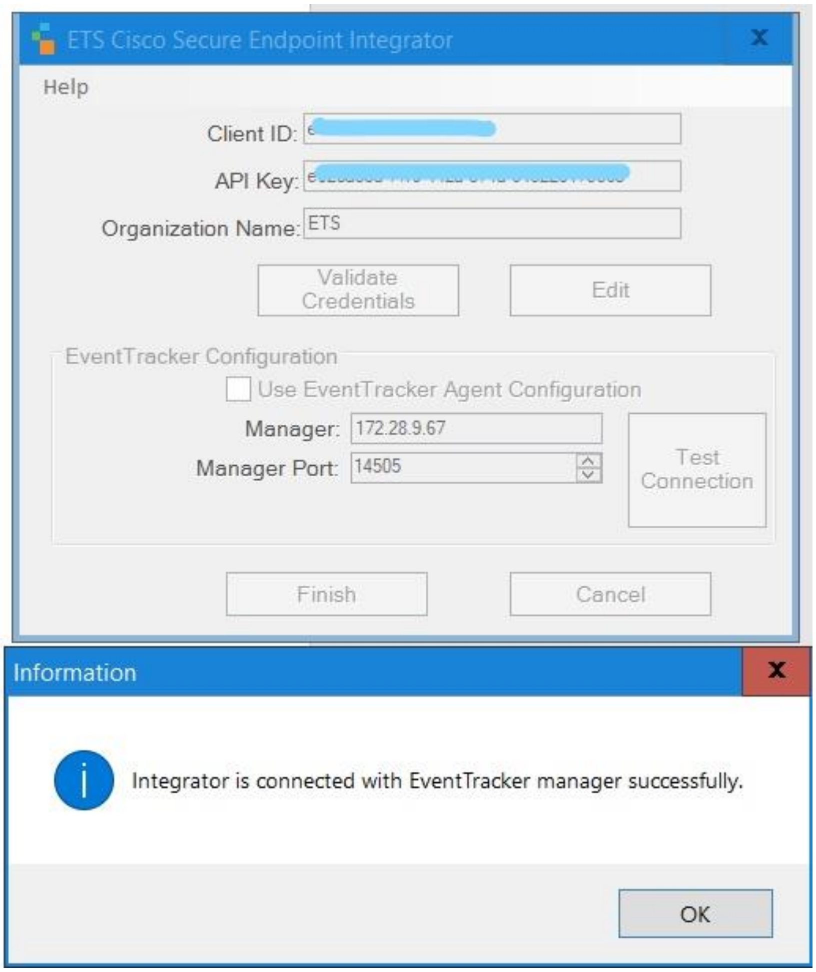
EventTracker Configuration

☑ Use EventTracker Agent Configuration

Manager:

Manager Port:

6. If the user wants to send the logs to specific EventTracker, then the user needs to mention EventTracker **Manager IP** and **Manager Port** to send the logs and click **Test Connection** to check the connectivity.



Client ID: [redacted]

API Key: [redacted]

Organization Name: ETS

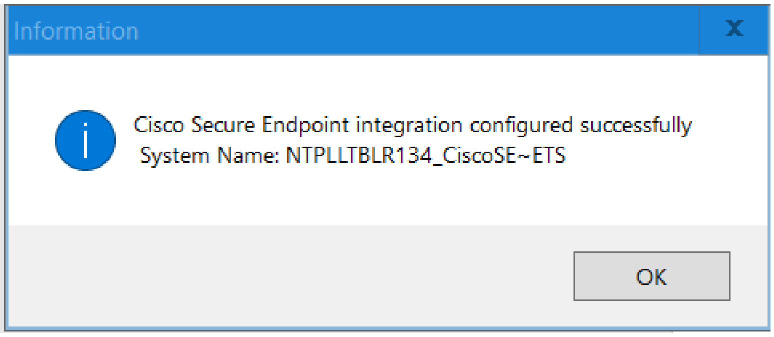
□ Use EventTracker Agent Configuration

Manager: 172.28.9.67

Manager Port: 14505

Integrator is connected with EventTracker manager successfully.

7. Once everything verified, click the **Finish** button to complete the Integration.



Cisco Secure Endpoint integration configured successfully
System Name: NTPLLTBLR134_CiscoSE~ETS

8. Run **ETS_Cisco Secure Endpoint_LogForwarder** exe to get the logs into EventTracker.

4. EventTracker Knowledge Packs

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

The following Knowledge Packs (KPs) are available in EventTracker to support Cisco® Secure Endpoint.

4.1 Category

- **Cisco® Secure Endpoint - Events -** This category provides information about all the events such as scan details, Threat Detected and Quarantine Details, Vulnerable Application and Fault Detected, Suspicious Activity Detected, System Activity, File activity.

4.2 Alerts

- **Cisco® Secure Endpoint – Risk Detected** – This alert generates when any risk is detected for the event_type_id like 1091567628, 1090519054, 1005, 1090524040 etc.

4.3 Reports

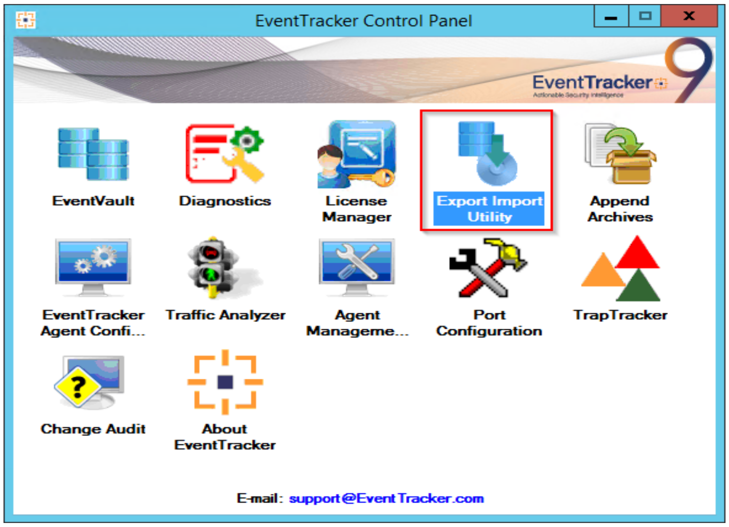
- **Cisco® Secure Endpoint – Events** – This report gives information about all the events which are generated from Cisco® Secure Endpoint.

5. Importing Cisco® Secure Endpoint Knowledge Pack into EventTracker

NOTE: Import Knowledge Pack items in the following sequence:

- Category
- Alerts
- Knowledge Objects
- Reports
- Dashboards

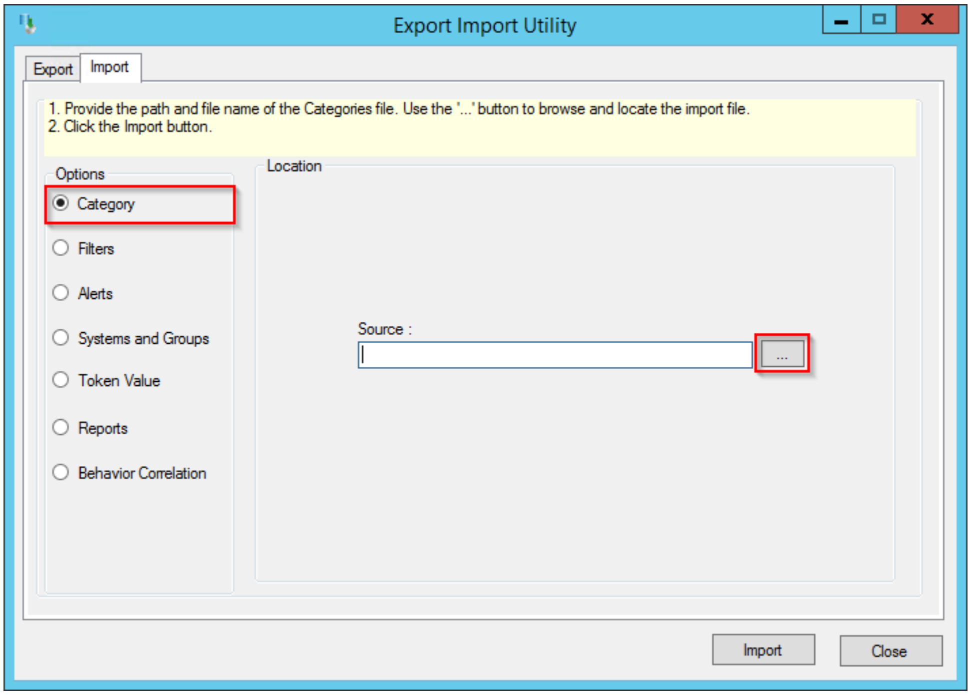
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

5.1 Category

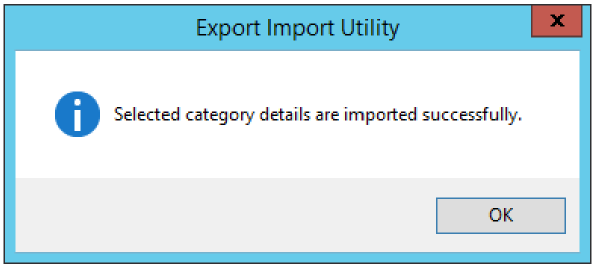
1. Click the **Category** option, and then click the browse ... button.



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.

2. Locate the **Categories_Cisco Secure Endpoint.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays a success message.

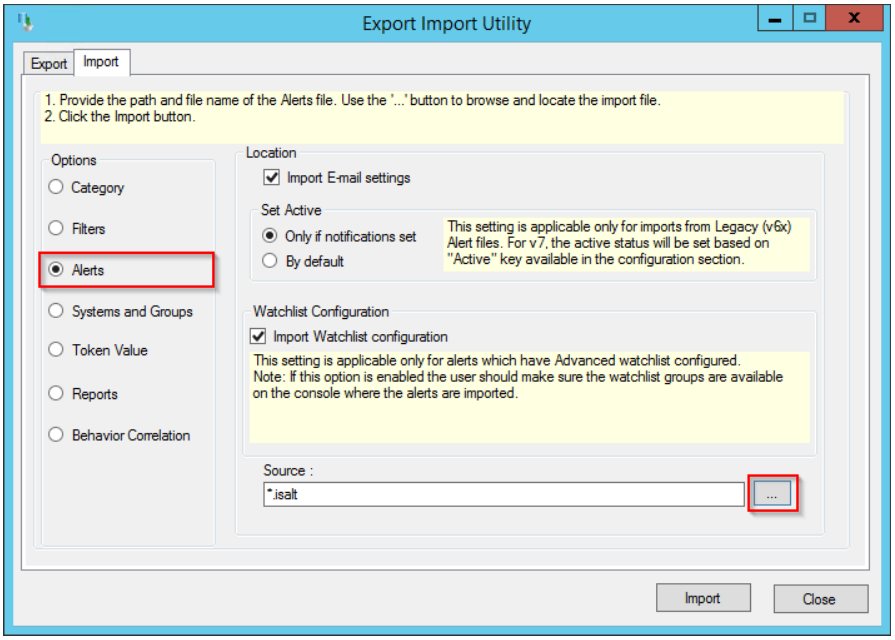

Export Import Utility

Selected category details are imported successfully.

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

5.2 Alerts

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


Export Import Utility

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.

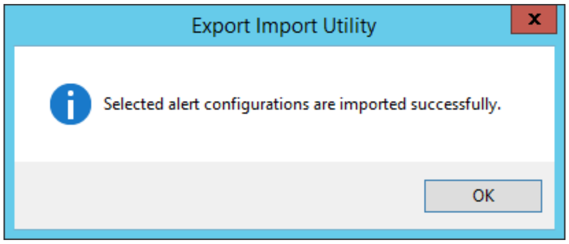
Watchlist Configuration

☑ 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

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

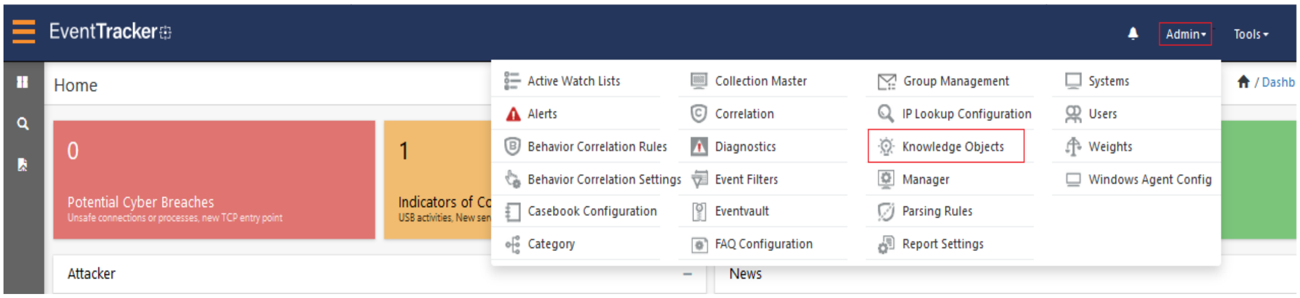

Export Import Utility

Selected alert configurations are imported successfully.

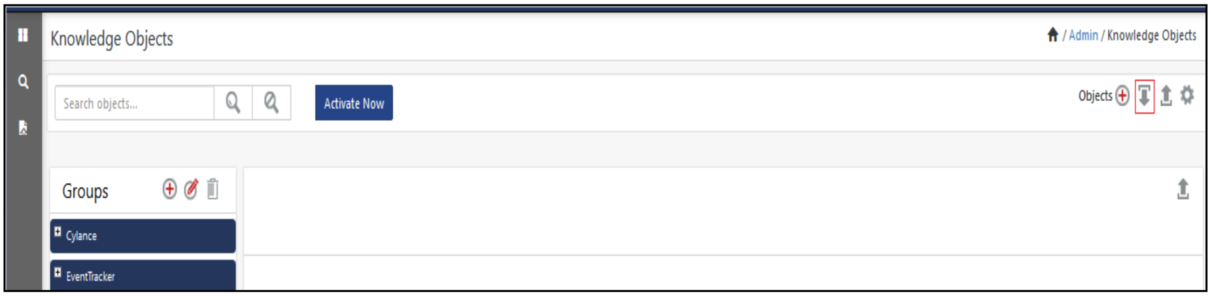
4. Click **OK**, and then click **Close**.

5.3 Knowledge Objects (KOs)

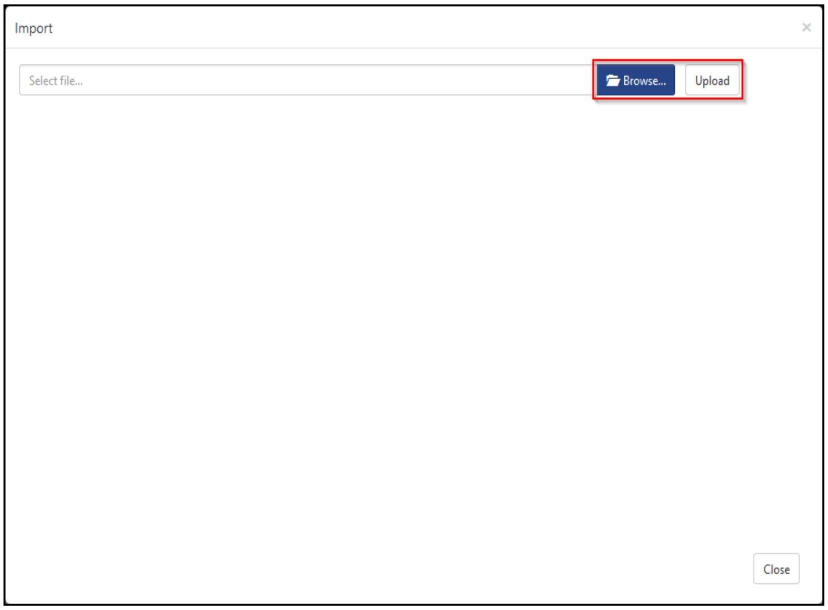
1. Click **Knowledge Objects** under the **Admin** option in the EventTracker Manager page.



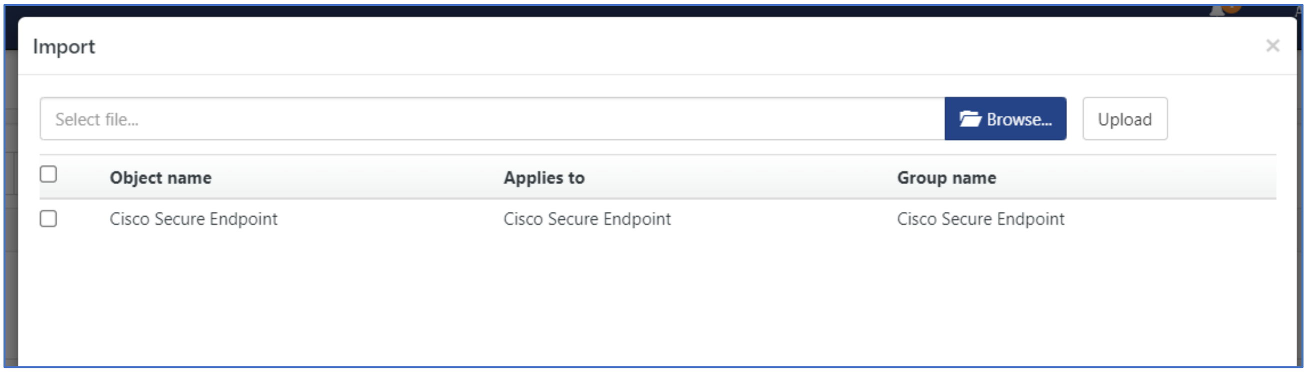
2. Click the **Import** button as highlighted in the below image:



3. Click **Browse**.



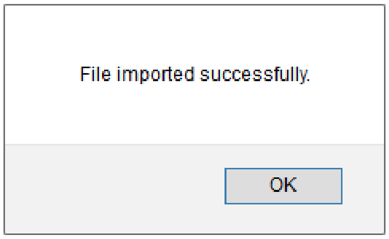
4. Locate the file named **KO_Cisco Secure Endpoint.etko**.
5. Select the check box and then click the **Import** option.



Import

□	Object name	Applies to	Group name
□	Cisco Secure Endpoint	Cisco Secure Endpoint	Cisco Secure Endpoint

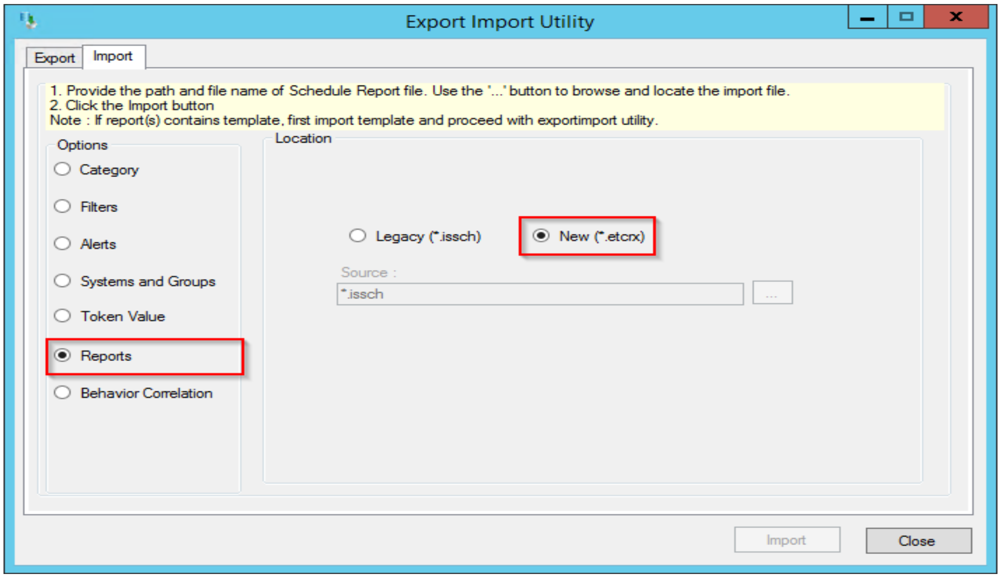
6. Knowledge Objects are now imported successfully.



File imported successfully.

5.4 Reports

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



Export Import Utility

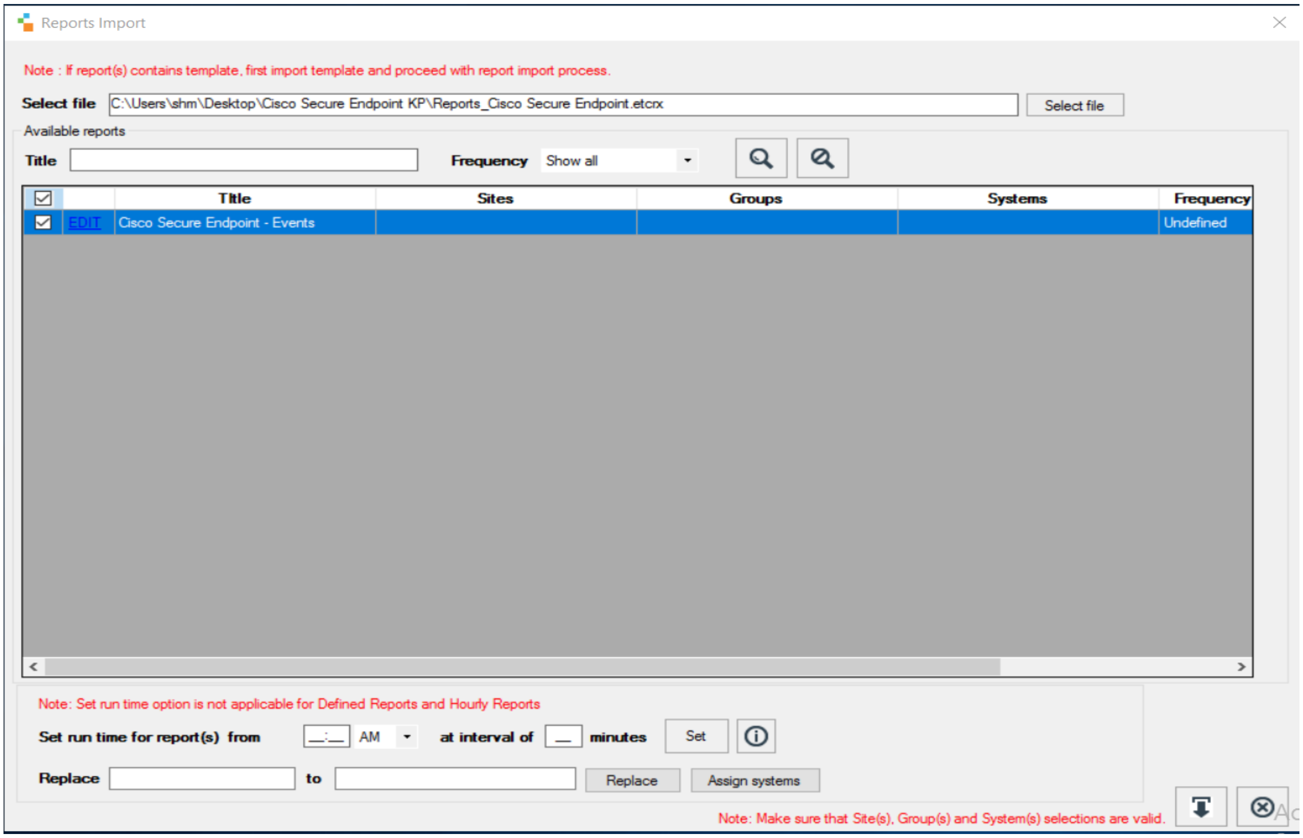
1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

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_Cisco Secure Endpoint.etrcx** and select all the check box.



Reports Import

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

Select file C:\Users\shm\Desktop\Cisco Secure Endpoint KP\Reports_Cisco Secure Endpoint.etcrx

Available reports

Title **Frequency** Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Cisco Secure Endpoint - Events				Undefined

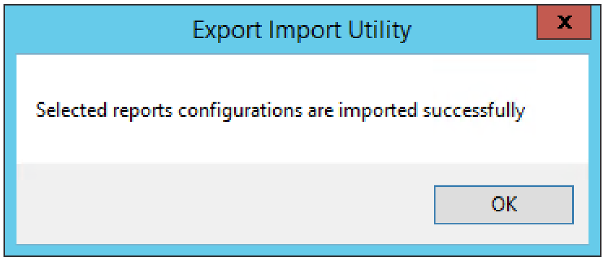
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM **at interval of** __ **minutes**

Replace **to**

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.



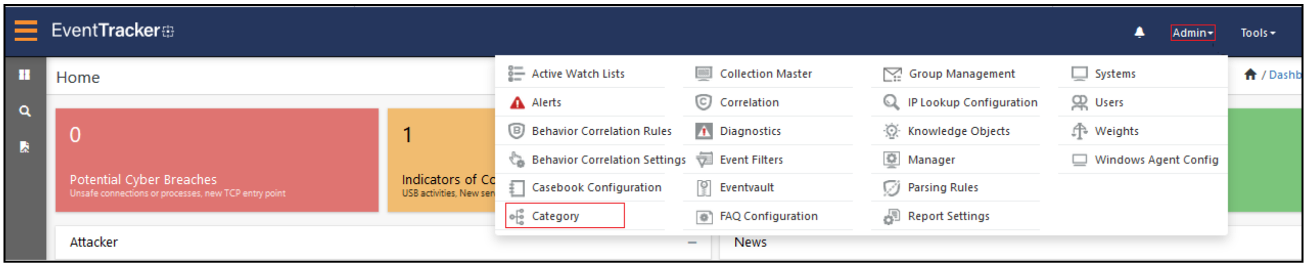
Export Import Utility

Selected reports configurations are imported successfully

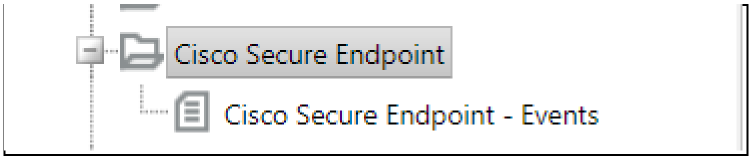
6. Verifying Cisco® Secure Endpoint Knowledge Pack in EventTracker

6.1 Category

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

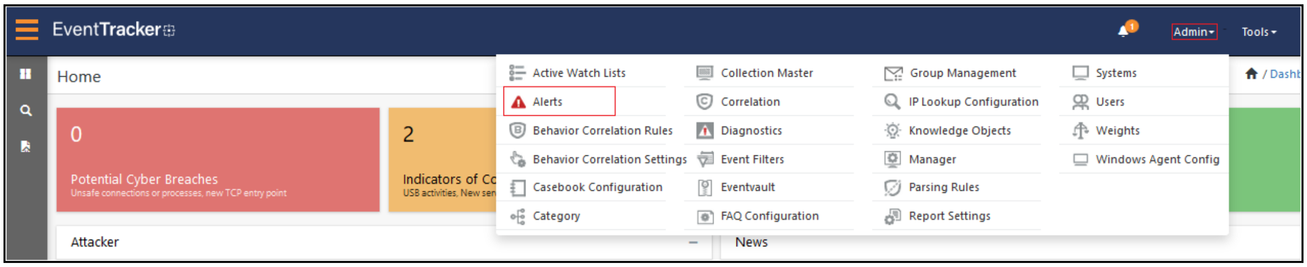


3. In the **Category Tree** to view the imported category, scroll down and expand the **Cisco® Secure Endpoint** group folder to view the imported category.

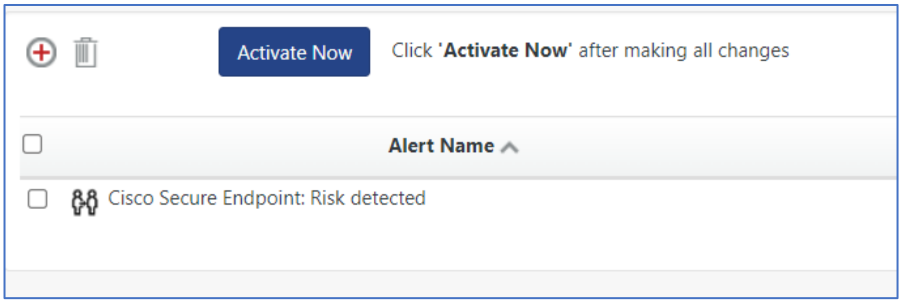


6.2 Alerts

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



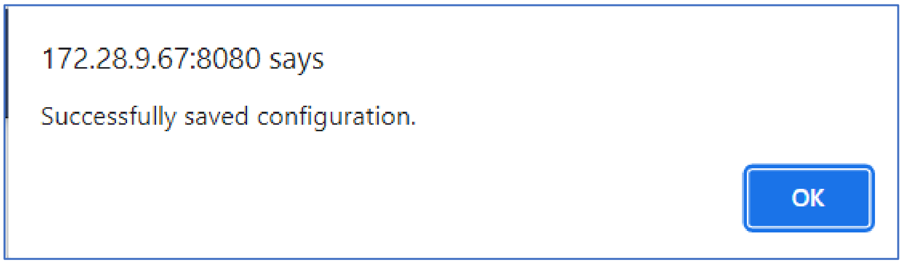
3. In the **Search** box, type **Cisco® Secure Endpoint,** and then click the **Go** button.
   The Alert Management page will display the imported alert.



□	Alert Name
□	Cisco Secure Endpoint: Risk detected

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

   EventTracker displays a message box.



172.28.9.67:8080 says

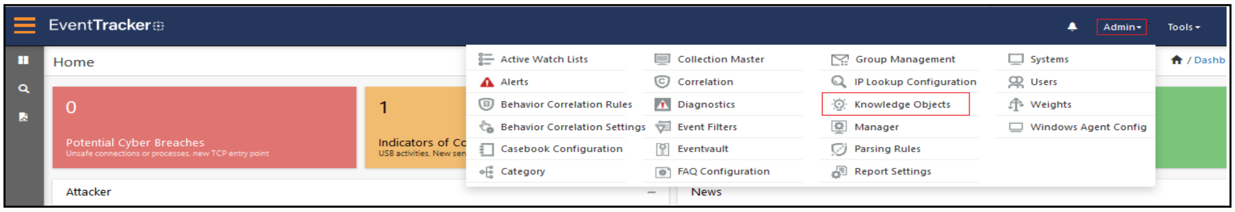
Successfully saved configuration.

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

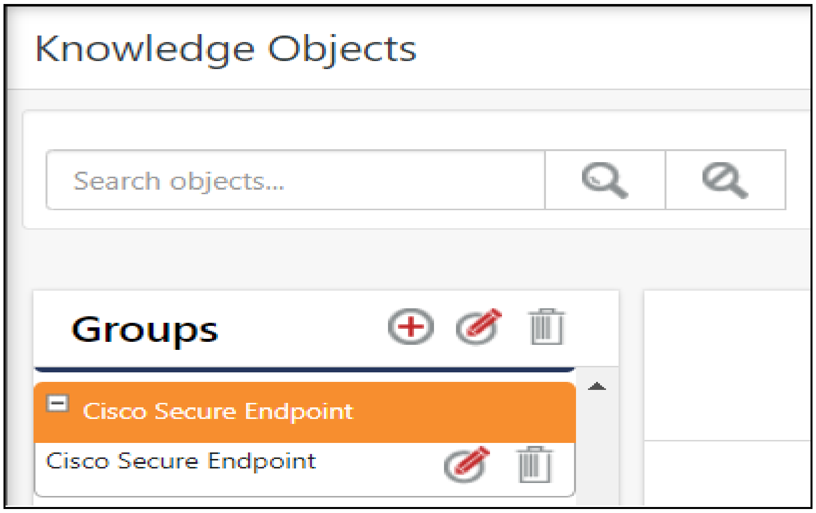
NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

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



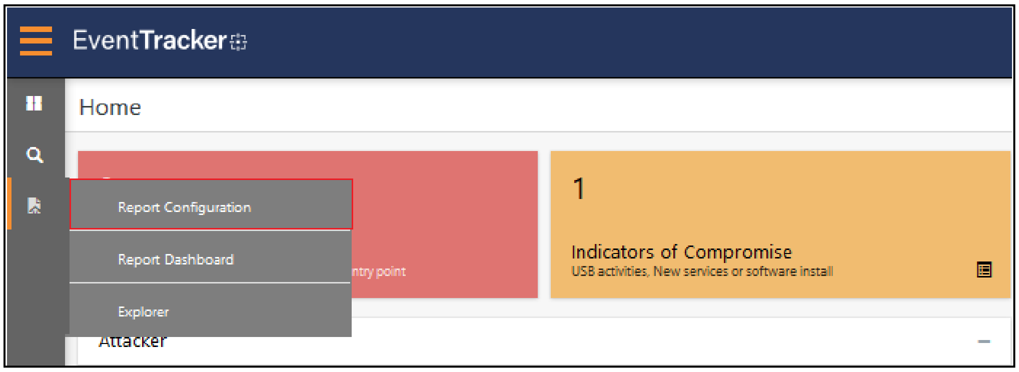
2. In the Knowledge Object tree, expand the **Cisco® Secure Endpoint group** folder to view the imported knowledge object.



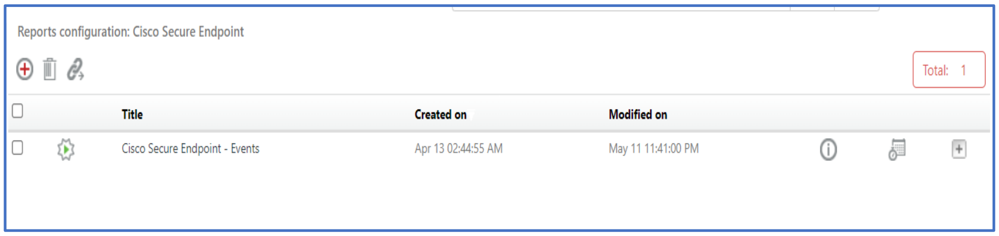
3. Click **Activate Now** to apply imported knowledge objects.

6.4 Report

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



2. In **Reports Configuration** pane, select the **Defined** option.
3. Click the **Cisco® Secure Endpoint** group folder to view the imported reports.


Reports configuration: Cisco Secure Endpoint

Total: 1

□		Title	Created on	Modified on
□		Cisco Secure Endpoint - Events	Apr 13 02:44:55 AM	May 11 11:41:00 PM

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, endpoint 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 #23 among MSSP Alert's 2021 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