Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Symantec Endpoint Protection Cloud with EventTracker

Publication Date:
October 28, 2021

Abstract

This guide helps you configure the Symantec Endpoint Protection Cloud (SEPC) with EventTracker to receive the Symantec Endpoint Protection Cloud events. In this guide, you will find the detailed procedures required for monitoring the Symantec Endpoint Protection Cloud.

Audience

Administrators who are assigned the task to monitor and manage the Symantec Endpoint Protection Cloud events using the EventTracker.

Table of Contents

1. Overview

The Symantec Endpoint Protection Cloud is a cloud-based security solution tailored for small and medium-sized businesses.

The EventTracker Knowledge Pack (KP) for Symantec Endpoint Protection Cloud provides insight into Threat Detection, Device Management, and other critical events.

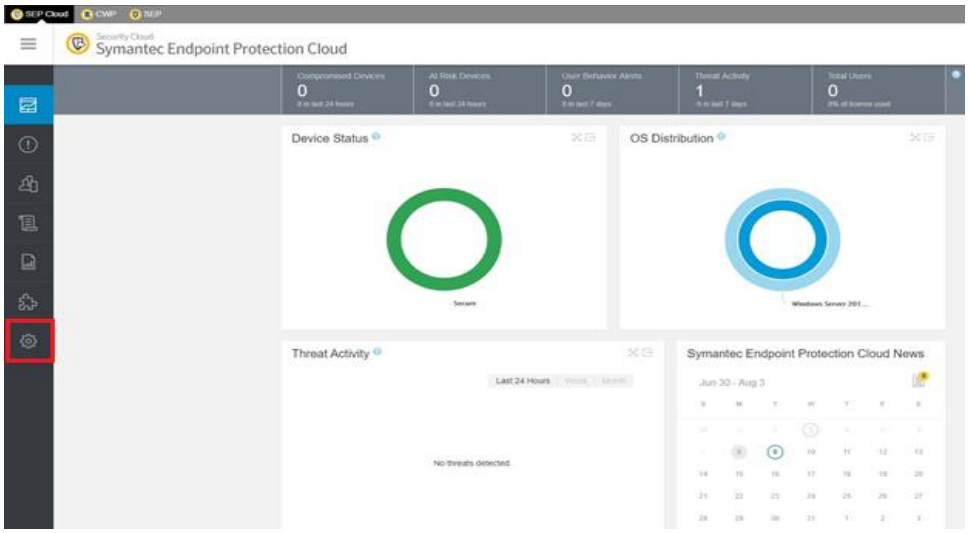
2. Prerequisites

- EventTracker 9.0 and later should be installed.
- Install the integrator on the machine where the EventTracker Agent/Manager is installed.
- The users should have the administrative credentials for the Symantec Endpoint Protection Cloud console.

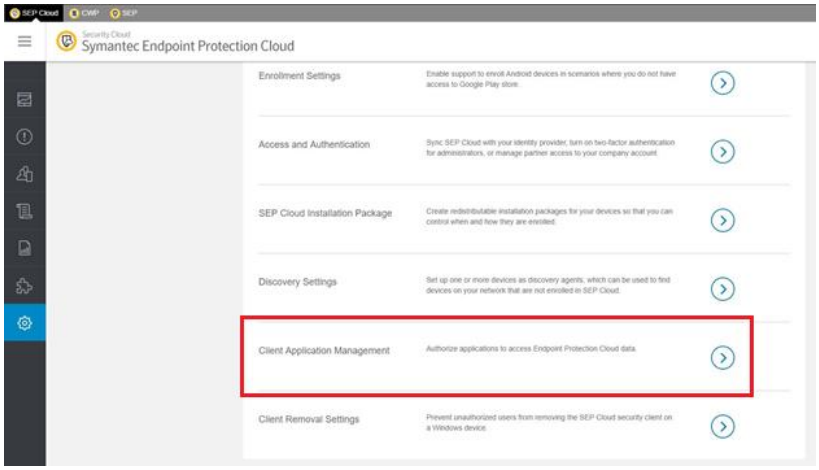
3. Obtaining Symantec Endpoint Protection Cloud Credentials

To obtain the **Symantec Endpoint Protection Cloud** API credentials, follow these steps:

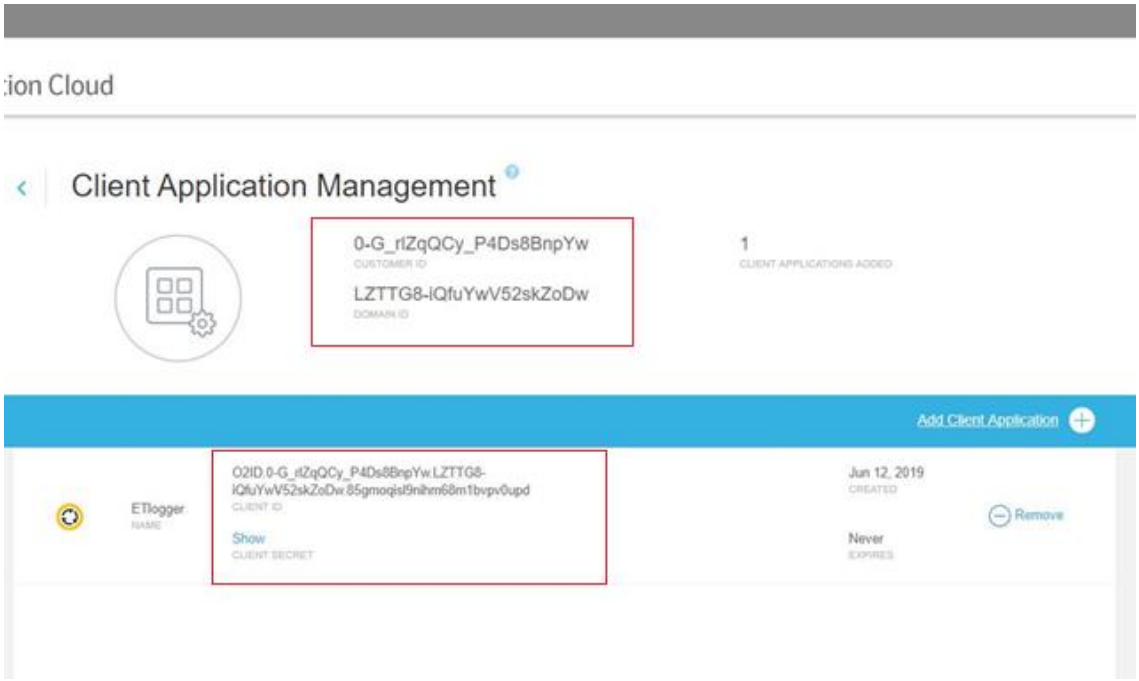
1. Go to the **Settings**.



2. Select **Client Application Management**.



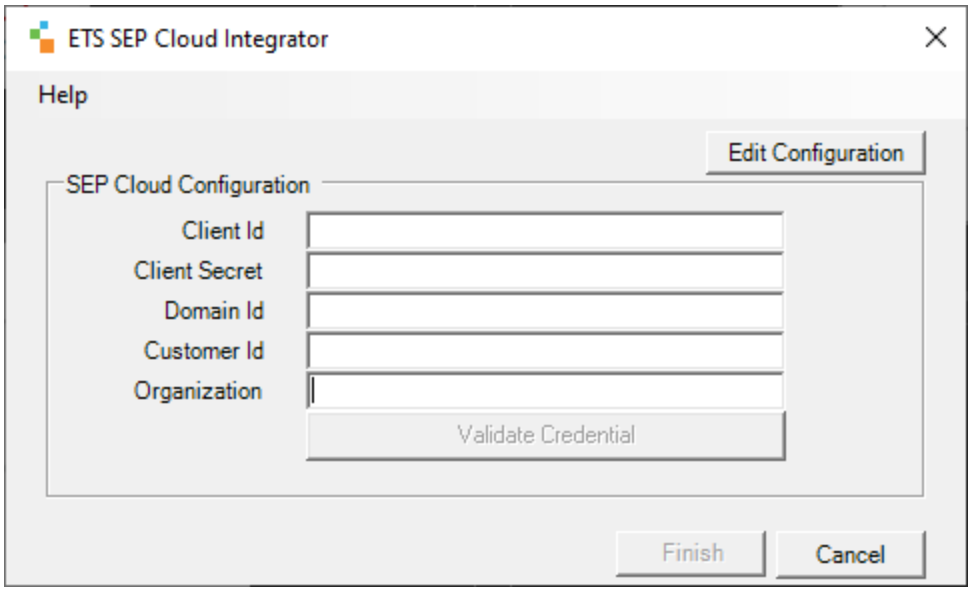
3. Click the **Add Client Application** and create the **API** keys.



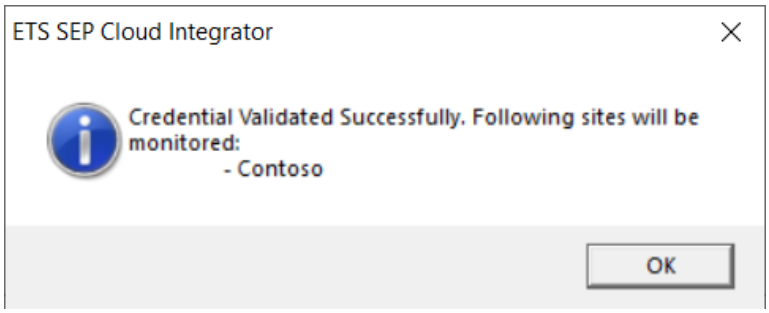
4. Copy the **Client ID, Client Secret, Customer ID,** and the **Domain ID**.

4. Integrating Symantec Endpoint Protection Cloud to EventTracker

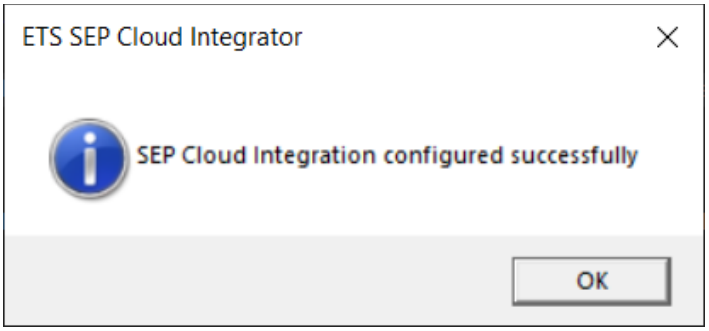
1. Download the Integrator for the Symantec Endpoint Protection Cloud.
2. Save the **.exe** file and run the executable file **ETS_SEP_Integrator.exe**. It will launch the **ETS SEP Cloud Integrator** window.
3. Enter the **Details** and click the **Validate Credential** button.



It will validate the credentials and the following message appears if the credentials are successfully validated and also enables the **Finish** button.



4. Click the **Finish** button to complete the integration.
   You will get a success message.



5. EventTracker Knowledge Packs

After the logs are received in the EventTracker, the Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Microsoft Windows.

5.1 Category

- **SEP Cloud - Threat Detection:** This category provides information related to all the threats that are detected by the Symantec Endpoint Protection Cloud.
- **SEP Cloud - Audit Events:** This category provides information related to all the audit-related activities.
- **SEP Cloud - Management Events:** This category provides information related to all the device and client management-related activities.
- **SEP Cloud - Security Events:** This category provides information related to all the security activities such as enabled critical features, disabled critical features, scan details, etc.
- **SEP Cloud - System Events:** This category provides information related to all the system-related activities.

5.2 Alerts

- **SEP Cloud - Threat detection:** This alert generates when the Symantec Endpoint Protection Cloud detects any malware or threats.
- **SEP Cloud - Scan aborted:** This alert generates when the Symantec Endpoint Protection scan aborts.
- **SEP Cloud - Definition update failed:** This alert generates when the Symantec Endpoint Protection Cloud detects any failed definition update.
- **SEP Cloud - Critical Feature disabled:** This alert generates when the Symantec Endpoint Protection Cloud detects any disabled critical feature.

5.3 Reports

- **SEP Cloud - Threat detection -** This report provides details about the threat detected by the SEPC on the endpoint. This report contains information about the threat and the endpoint on which it occurs.

Address	Device Type	Source Port	Threat Level	Target Resource	Target Service	Signature	Signature Properties	Target Folder	Threat md5	Threat sha2	Threat id	Threat Name	Message
213.211.198.58	Server	443	2	https://secure.eicar.org/eicar.com	C:\Program Files (x86)\Internet	Diagnostic: EICAR Standard	0x0000000000001214						Detected: low-risk intrusion attempt
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILES\MICROSOFT SECURITY CLIENT\MSMPENG.EXE
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILES\MICROSOFT SECURITY CLIENT\MSMPENG.EXE
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILES (X86)\WEBROOT\WRSA.EXE
127.163.118.133	Server	443	2	https://secure.eicar.org/eicar.com	C:\Program Files\Mozilla	Diagnostic: EICAR Standard	0x0000000000001214						Detected: low-risk intrusion attempt
	Server							C:\Users\Pratik.k\Desktop\eicar_com\	44D88612FEA8A8F36DE82E1278ABB02F	275A021BBFB6489E54D471899F7DB9D1663FC695	5F28383E-C3DA-416F-824E-	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\Desktop\eicar_com\	44D88612FEA8A8F36DE82E1278ABB02F	275A021BBFB6489E54D471899F7DB9D1663FC695	1027F027-85FD-4043-802A-	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\$RECYCLE.BIN\S-1-5-21-117257714-2094817907-3186505446-	44D88612FEA8A8F36DE82E1278ABB02F	275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538	01382E2E-D244-472D-ACDA-36DE1E67FE6	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\Desktop\eicar_com.zip	44D88612FEA8A8F36DE82E1278ABB02F	275A021BBFB6489E54D471899F7DB9D1663FC695	41D40989-D470-4CBD-B673-	EICAR Test String	Threat detected: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\AppData\Local\Mozilla\Firefox\Profiles\sw7qzhxa.default\cache2\entries\787F9B10F6FDEFC7173	44D88612FEA8A8F36DE82E1278ABB02F	275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F	03917B82-ADE7-41F1-BAA2-072C76E28310	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\AppData\Local\Mozilla\Firefo	44D88612FEA8A8F36DE82E12	275A021BBFB6489E54D471899F7	03917B82-ADE7-41F1-	EICAR Test String	Threat detected: Malware - EICAR Test String

- **SEP Cloud - Scan details –** This report provides detailed information about the Antivirus (AV) scan on the endpoints, along with the statistical details of the files, process, the registry and the folders which it scans.

Event Type	Source Host Name	Scan Start Time	Device Type	Scan End Time	Risks Detected	Files	Folders	Network	Processes	Registry	Skipped	Total	Message
Quick Scan	R1S5-VM30	2019-06-25T20:41:53.760Z	Server	2019-06-25T20:44:43.760Z	0	595	6588	596	1772	404	0	9996	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-26T02:42:16.881Z	Server	2019-06-26T02:44:57.881Z	0	595	6588	596	1772	404	0	9996	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-26T02:42:16.881Z	Server	2019-06-26T02:44:57.881Z	0	595	6588	596	1772	404	0	9996	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-26T18:48:23.294Z	Server	2019-06-26T18:51:16.294Z	0	598	7048	596	1998	404	0	10685	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-26T18:48:23.294Z	Server	2019-06-26T18:51:16.294Z	0	598	7048	596	1998	404	0	10685	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T00:50:43.524Z	Server	2019-06-27T00:53:33.524Z	0	598	7048	596	1992	404	0	10679	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T00:50:43.524Z	Server	2019-06-27T00:53:33.524Z	0	598	7048	596	1992	404	0	10679	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T06:30:19.904Z	Server	2019-06-27T06:33:42.904Z	0	598	7048	596	1992	404	0	10679	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T06:30:19.904Z	Server	2019-06-27T06:33:42.904Z	0	598	7048	596	1992	404	0	10679	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T11:24:23.461Z	Server	2019-06-27T11:24:23.461Z	0	2	0	0	0	0	0	2	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T11:24:23.461Z	Server	2019-06-27T11:24:23.461Z	0	2	0	0	0	0	0	2	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T11:08:39.092Z	Server	2019-06-27T11:11:34.092Z	0	585	7048	596	1932	404	30	10606	Scan completed on R1S5-VM30
Quick Scan	R1S5-VM30	2019-06-27T11:08:39.092Z	Server	2019-06-27T11:11:34.092Z	0	585	7048	596	1932	404	30	10606	Scan completed on R1S5-VM30

- **SEP Cloud - Console login logout details -** This report provides details about the login and logout activities along with its user details, their roles and their IP address and from where these activities occur.

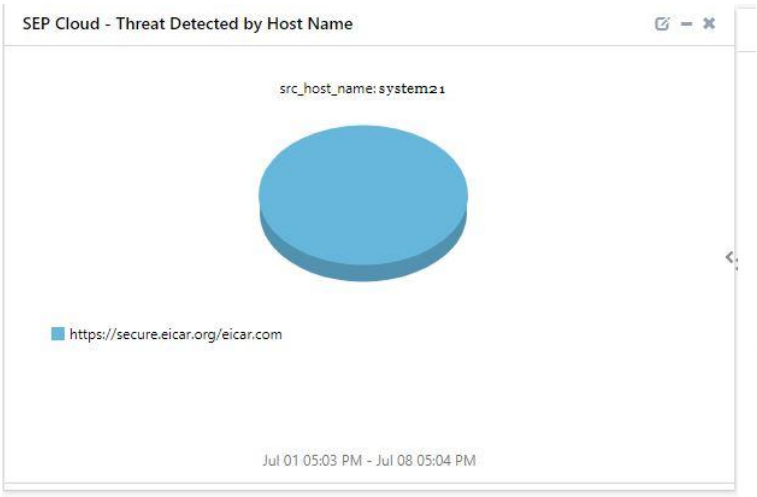
LogTime	User UID	Source User Name	Source IP Address	User Role	Message
06/12/2019 12:57:11 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.145.29	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 01:07:14 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.165.3	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 01:08:36 PM		John			User 'John' logged on.
06/12/2019 01:08:46 PM		John			User 'John' logged off.
06/12/2019 01:11:17 PM		John			User 'John' logged on.
06/12/2019 01:13:38 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 03:10:33 PM		John			User 'John' logged off.
06/12/2019 03:20:04 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 04:22:39 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 04:26:43 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 04:31:12 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.145.29	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in
06/12/2019 04:34:48 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINISTRATOR	User 'John' logged in

- **SEP Cloud - Management activities -** This report provides details about any changes (like policy changes, exceptions, and many more.) done by the administrator using the SEPC console.

LogTime	Device Type	Source Host Name	Device OS Name	Source IP Address	Message
06/10/2019 03:58:44 PM					Policy group 'Symantec Default Policy Group : UNIX' created by SYMANTEC.
06/10/2019 03:59:10 PM					Policy group 'Symantec Default Antimalware Policy Group : UNIX' created by SYMANTEC.
06/11/2019 03:05:06 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/11/2019 03:05:06 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/11/2019 10:56:10 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/12/2019 05:11:06 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/12/2019 05:11:06 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/12/2019 11:12:21 PM		R1S5-VM30		172.28.9.137	'ReactivationCommand' is completed on device 'R1S5-VM30'.
06/15/2019 01:09:02 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/17/2019 09:09:16 AM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy
06/18/2019 05:09:33 PM	Server	R1S5-VM30	Windows Server 2012 R2 Datacenter		Successfully applied Management policy

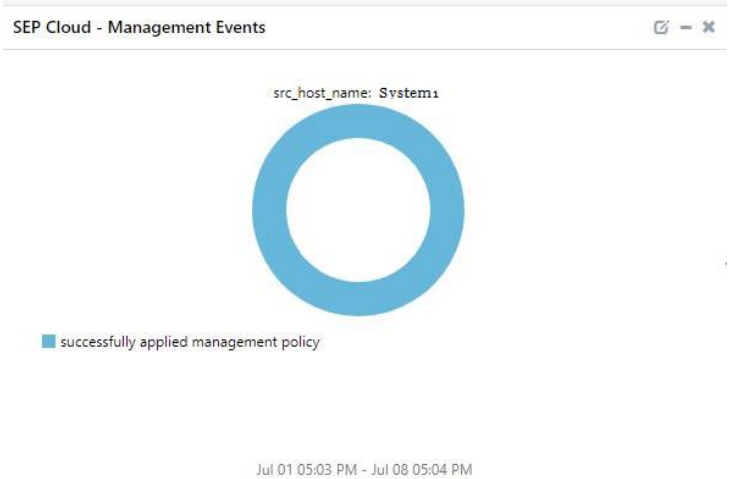
5.4 Dashboards

- **SEP Cloud – Threats Detected by the Host Name**



- **SEP Cloud – Login Details by the Source IP Address**

- **SEP Cloud – Management Events**

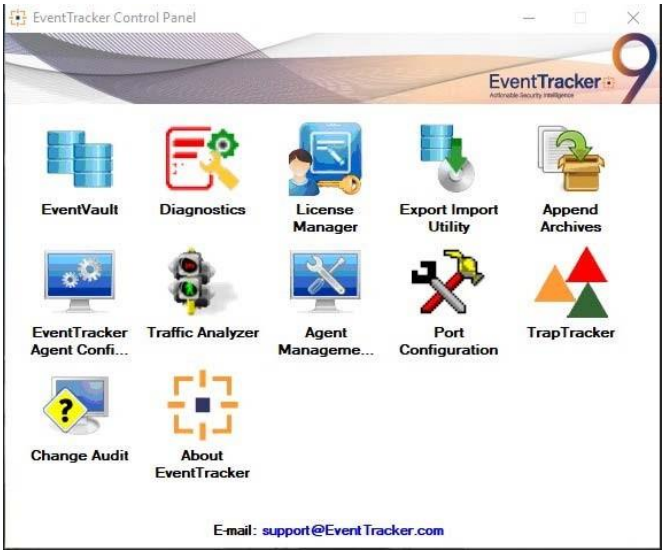


6. Importing the Knowledge Pack

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

- Category
- Alerts
- Knowledge Objects
- Reports
- Dashboards

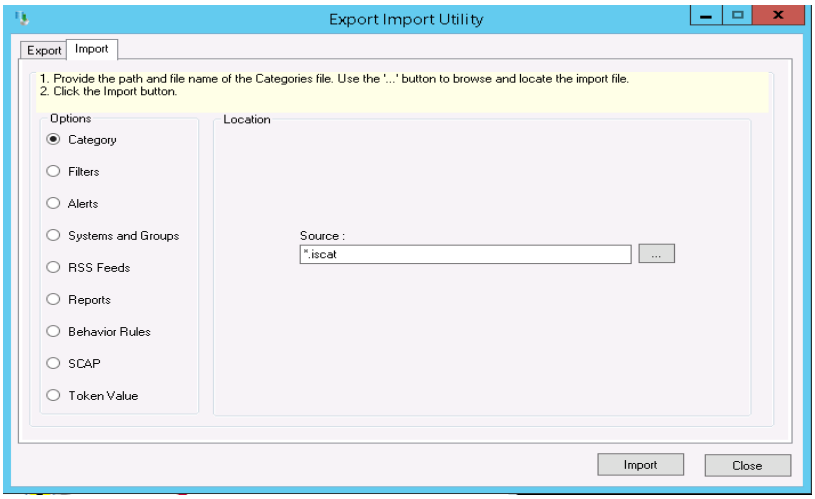
1. Launch the **EventTracker Control Panel.**
2. Double click Export-Import Utility.



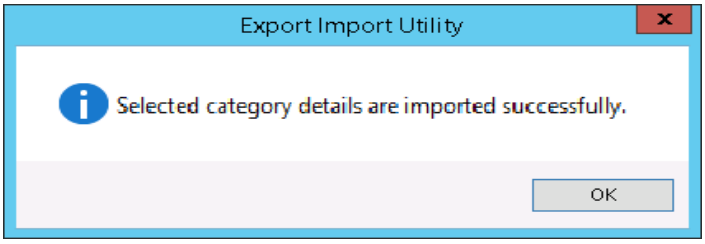
3. Click the **Import** tab.

6.1 Category

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



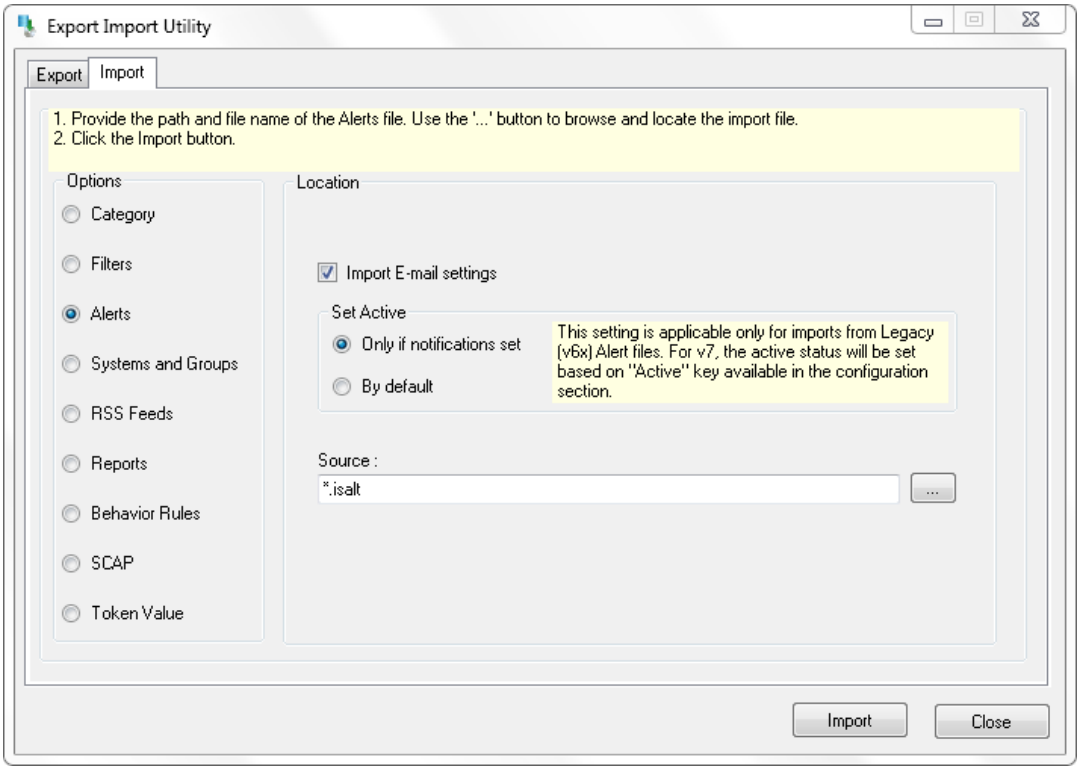
2. Locate the **.iscat** file, and then click the **Open** button.
3. To import the **Categories**, click the **Import** button.
4. EventTracker displays a success message.



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

6.2 Alerts

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

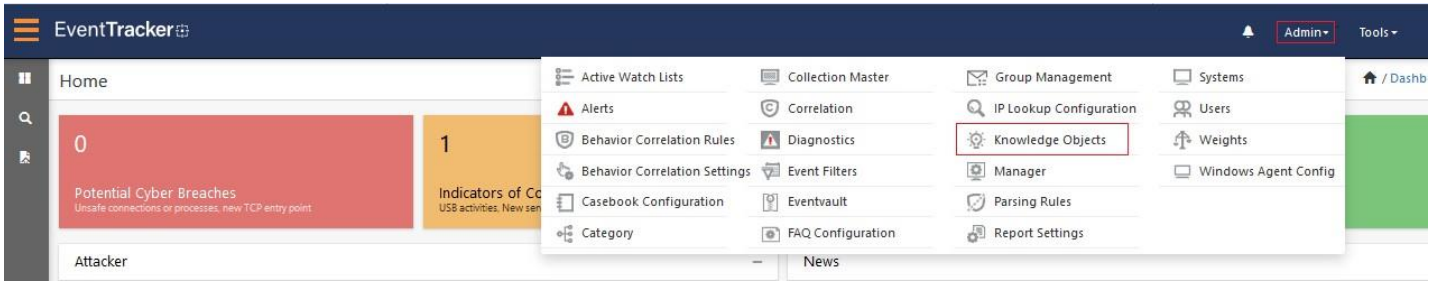


2. Locate the **.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
4. EventTracker displays a success message.

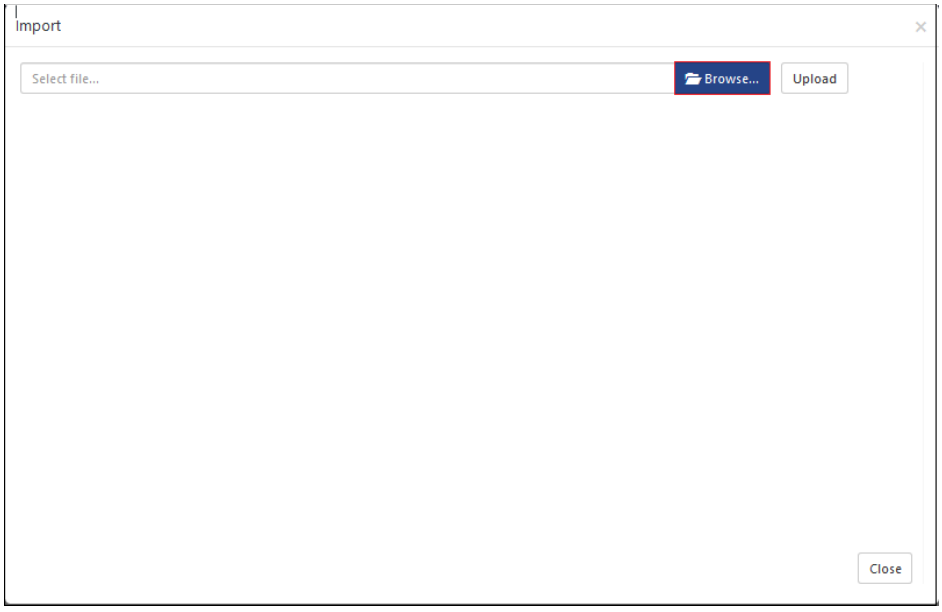
5. Click the **OK** button, and then click the **Close** button.

6.3 Knowledge Objects

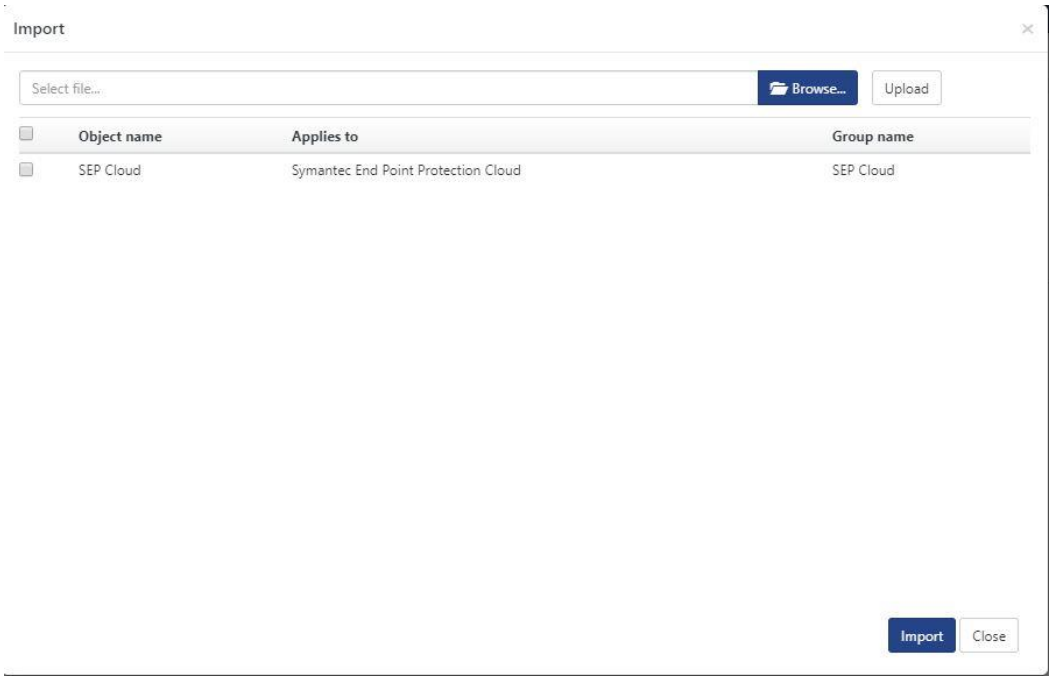
1. Click the **Knowledge Objects** under the **Admin** option in the **EventTracker Manager** page.



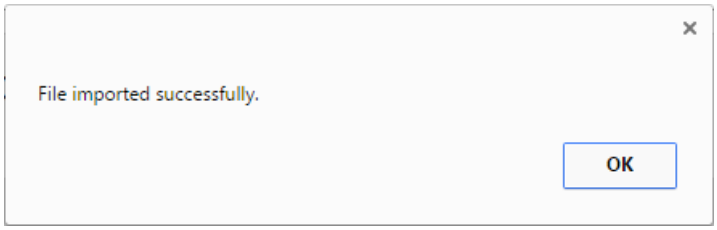
2. Click the **Import** button.



3. Click **Browse**.
4. Locate the file named .**etko**.
5. Select all the checkboxes and then click the **Import** option.



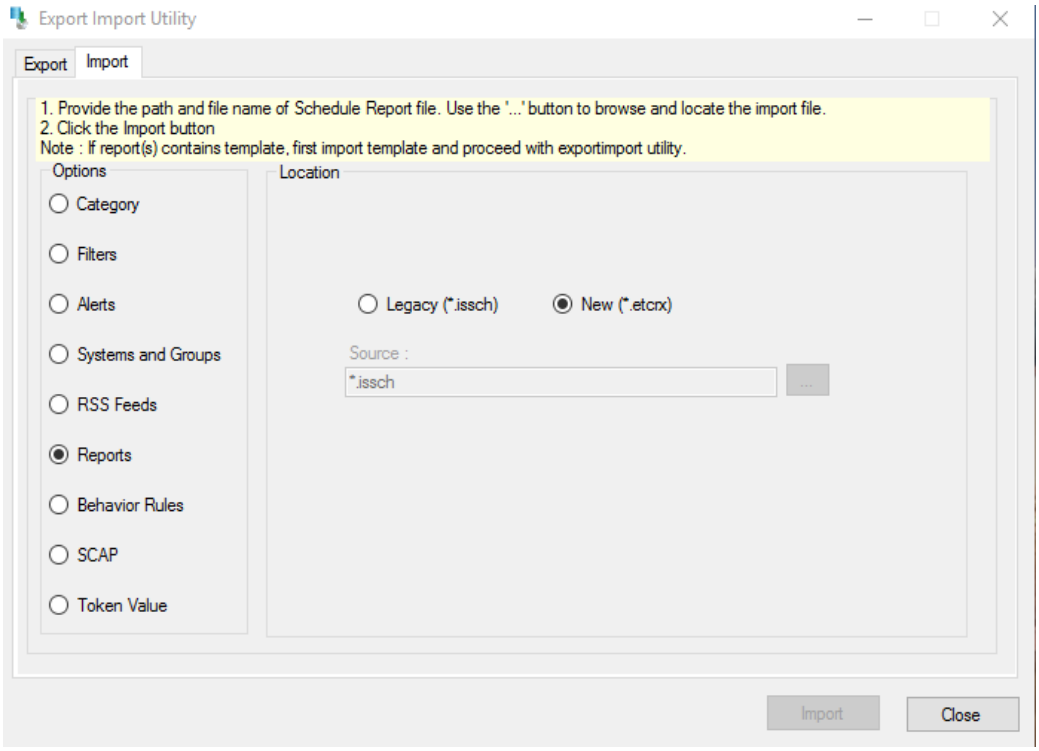
6. Knowledge Objects are now imported successfully.



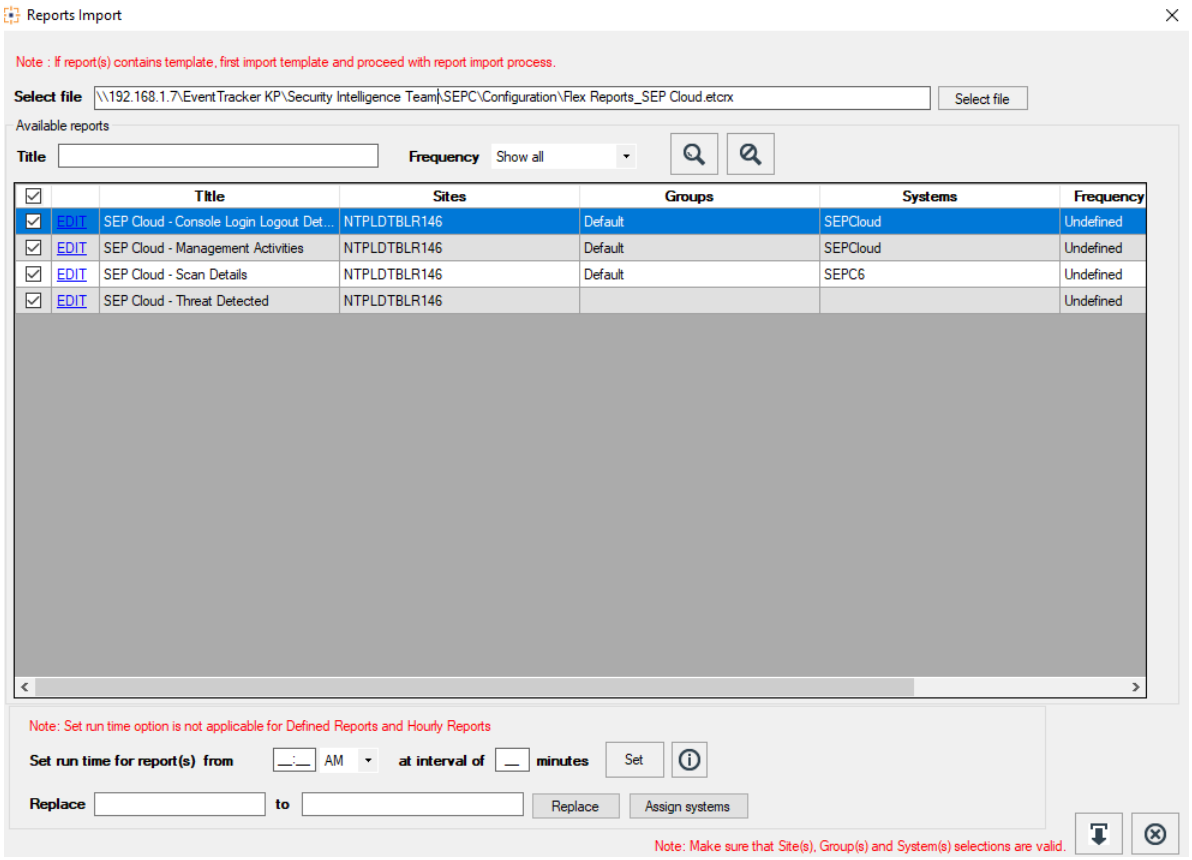
6.4 Flex Reports

On the EventTracker Control Panel,

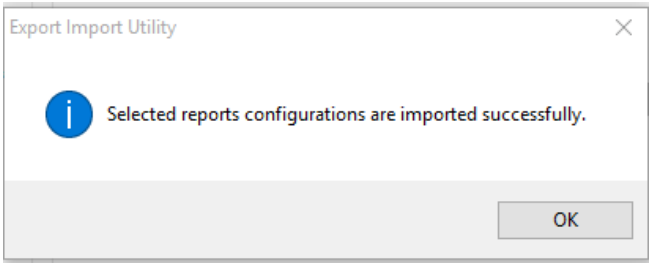
1. Click the **Reports** option and select the **New** (*.etcrx) option.



2. Locate the file named **.etcrx** and select all the checkboxes.



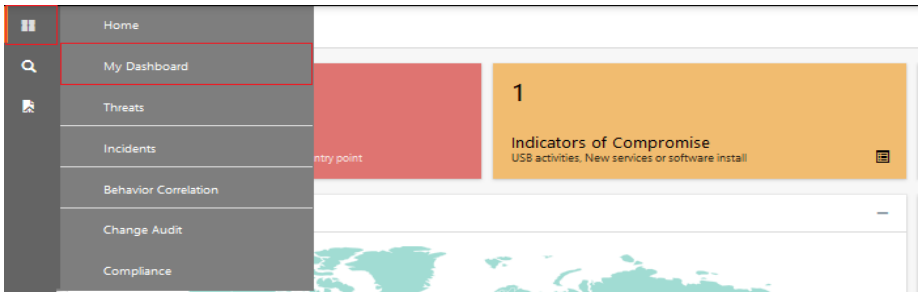
3. Click the **Import** button to import the reports. EventTracker displays a success message.



6.5 Dashboards

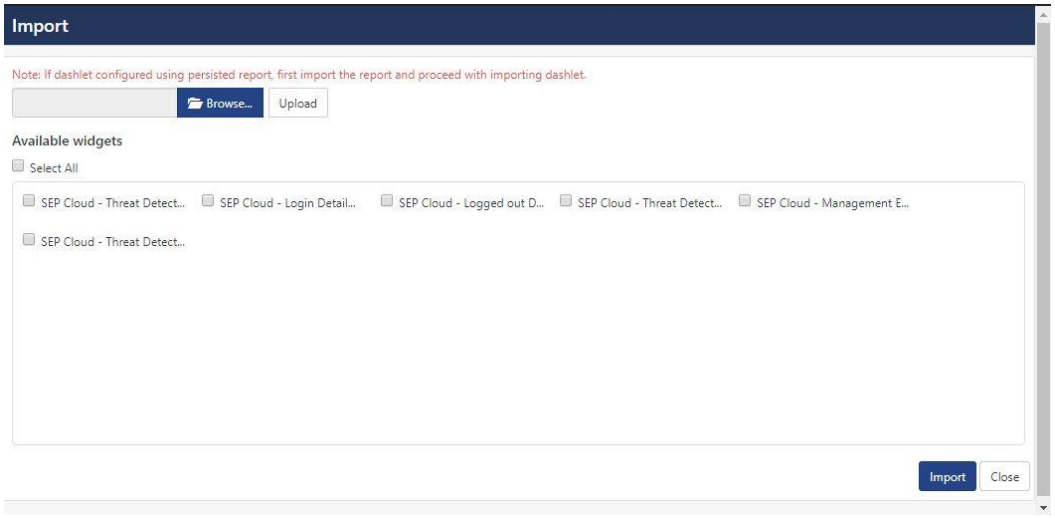
NOTE: The following steps given are specific to EventTracker v9.2 and later.

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

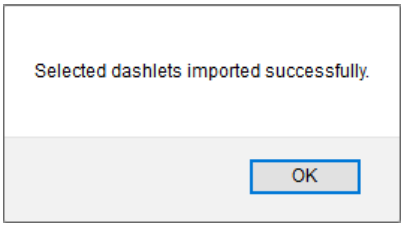


2. Navigate to the **My Dashboard** option.
3. Click the **Import** button.

4. Import the dashboard file **.etwd** and click the **Import** button to import the **Dashlets** into the EventTracker Dashboard.
   You have an option to enable the **Available widgets** for the required Dashboard.



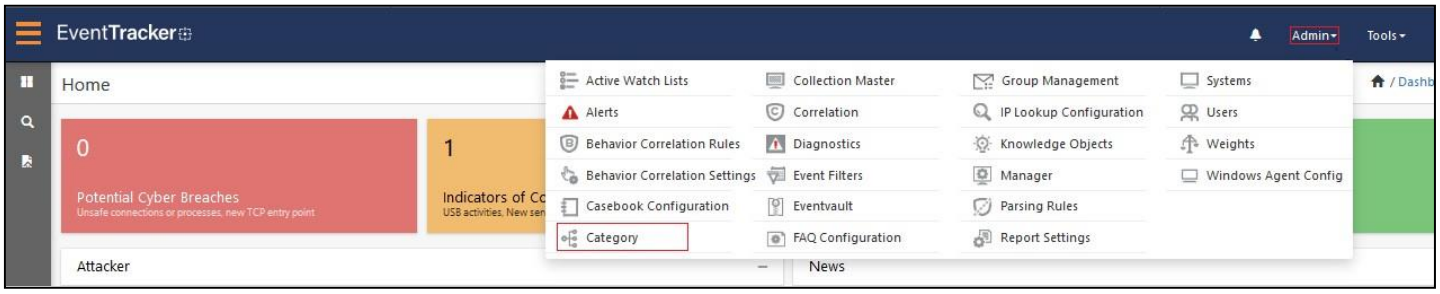
5. Import is now completed successfully.



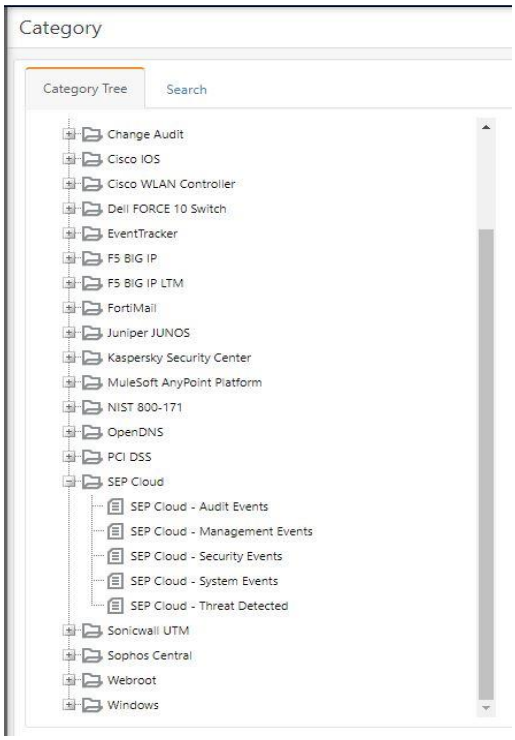
7. Verifying the Knowledge Pack

7.1 Category

1. Logon to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Categories**.

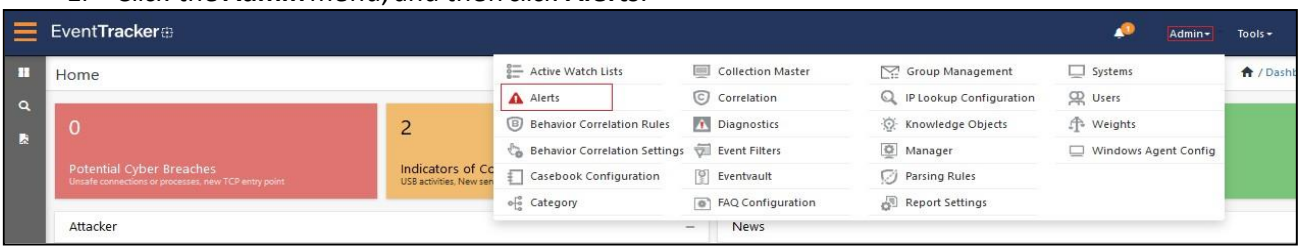


3. In the **Category Tree**, scroll down and expand the **SEP Cloud** group folder to view the imported categories.

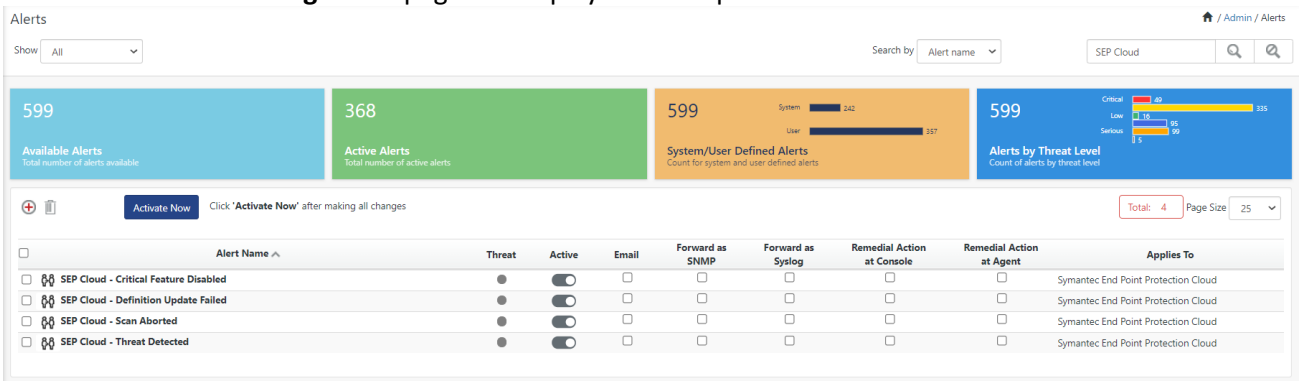


7.2 Alerts

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

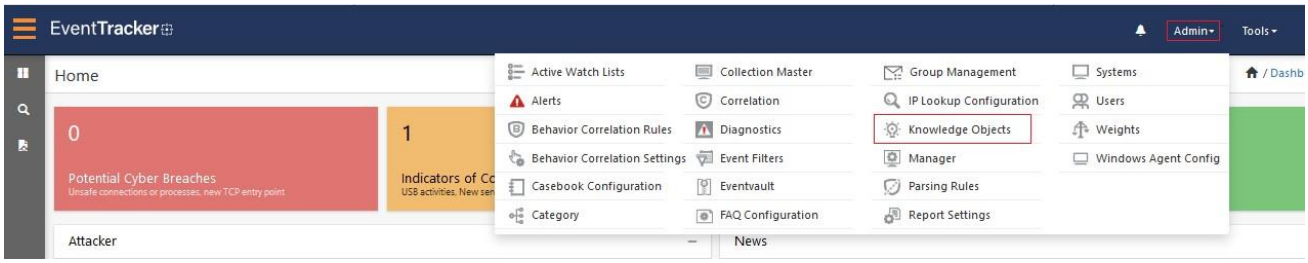


3. In the **Search** box, type **SEP Cloud**, and then click the **Go** button.
   The **Alert Management** page will display all the imported alerts.

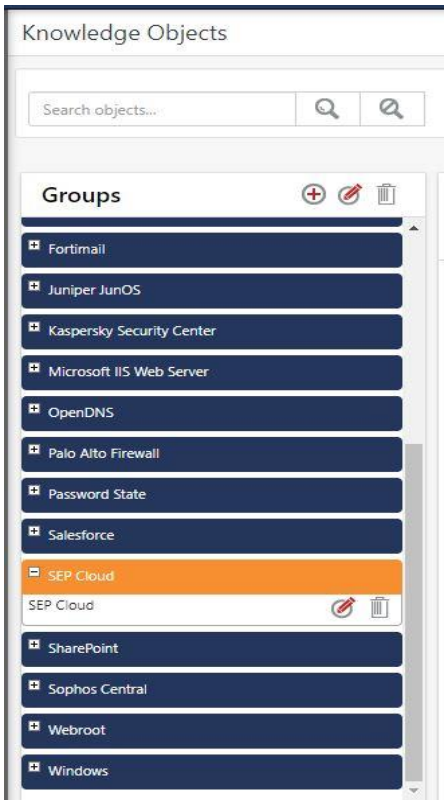


7.3 Knowledge Objects

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

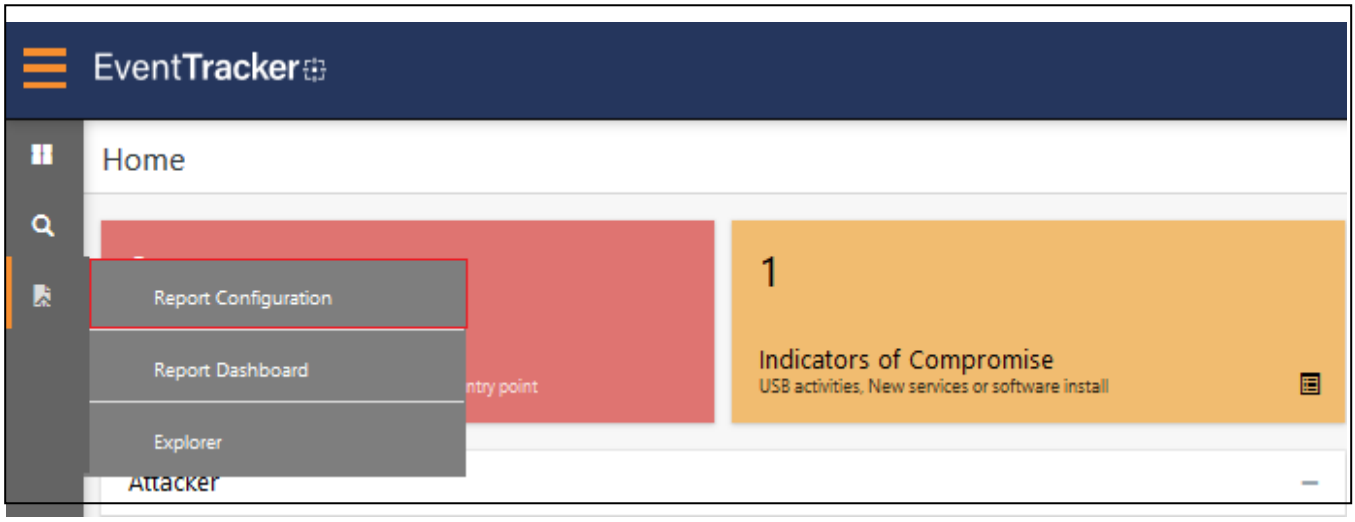


2. In the Knowledge Object tree, expand the **SEP Cloud** group folder to view the imported Knowledge Objects.

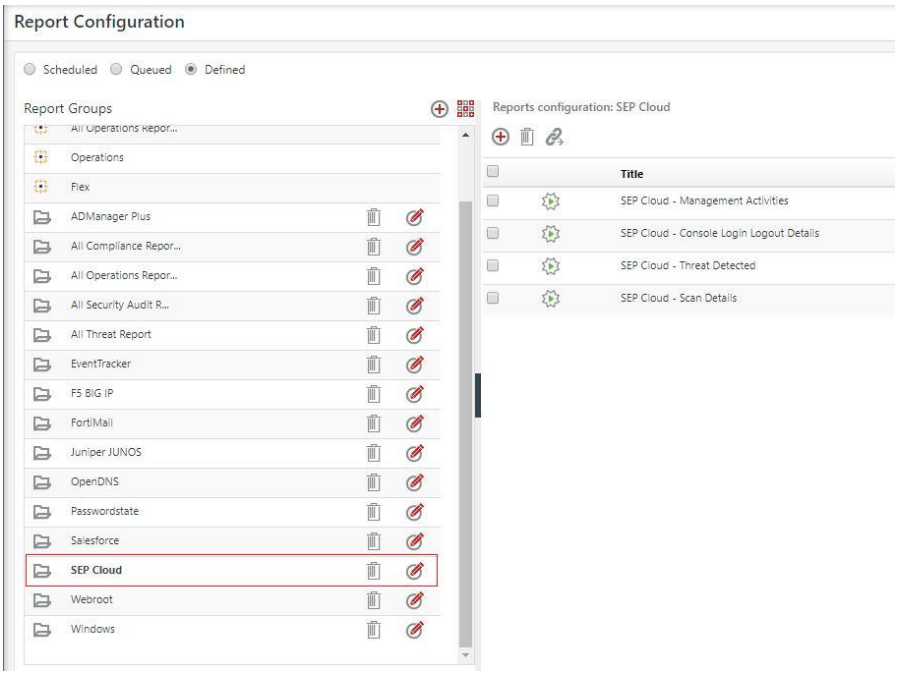


7.4 Flex Reports

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

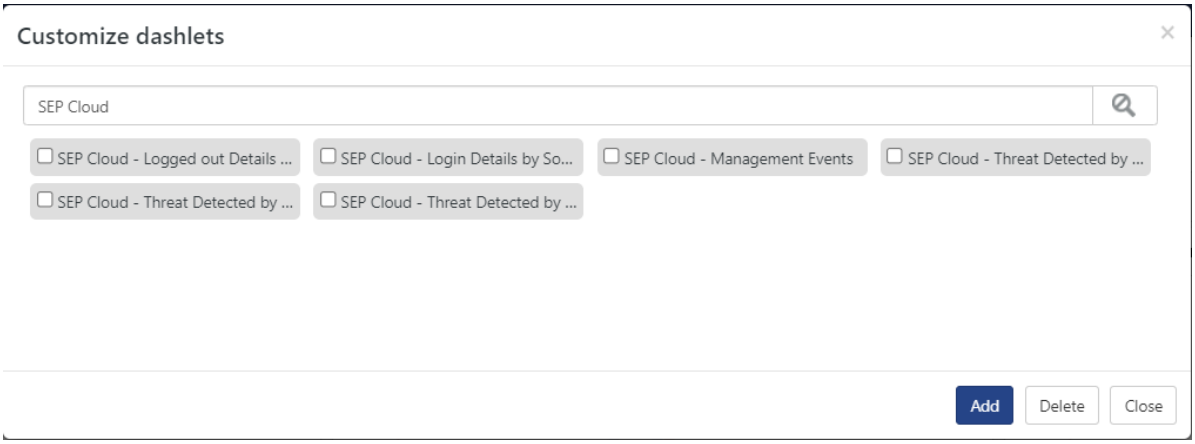


2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **SEP Cloud** group folder to view the imported SEP Cloud reports.



7.5 Dashboards

1. In the EventTracker web interface, click the **Home** button and select **My Dashboard**.
2. Click the **Customize dashlets** icon and search for the **SEP Cloud** and verify the following dashlet.



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