

Integration Guide

Integrating Symantec Endpoint Protection Cloud with EventTracker

Publication Date: October 28, 2021

© Copyright Netsurion. All Rights Reserved.

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

Tak	ole o	f Contents	3				
1.	Overview						
2.	Pr	erequisites	4				
3.	Oł	otaining Symantec Endpoint Protection Cloud Credentials	4				
4.	In	tegrating Symantec Endpoint Protection Cloud to EventTracker	5				
5.	Ev	entTracker Knowledge Packs	7				
5	5.1	Category	7				
5	5.2	Alerts	7				
5	5.3	Reports	7				
5	5.4	Dashboards	9				
6.	Im	porting the Knowledge Pack	10				
6	5.1	Category	11				
6	5.2	Alerts	12				
6	5.3	Knowledge Objects	13				
6	5.4	Flex Reports	14				
6	5.5	Dashboards	16				
7.	Ve	rifying the Knowledge Pack	17				
7	7.1	Category	17				
7	7.2	Alerts	18				
7	7.3	Knowledge Objects	18				
7	7.4	Flex Reports	19				
7	7.5	Dashboards	20				
A	٩po	utNetsurion	21				
(Cont	act Us	21				

1. Overview

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

SEP Cloud 🔒 CWP 👩 NOP									
≡ ® Scorty Could Symantec Endp	point Protection Cloud								
	Compromised Devices 0 3 is set 24 lesses	At Rose Develops. 0 8 in Indi 34 Maart	Unter Elefundor Alexta O Biologia 7 dege	Thereaf 1 - the task	Activity 1.1 mps		botal O oficial	Diere kommenset	•
0	Device Status 9		×@ OS Di	stribution	>				80
ය									
1					(
					1	_			
ప		Jacoure				- week	tawa Server J	101	
0	Threat Activity		хœ	Syma	ntec Endp	oint Pr	rotection	1 Cloud	News
		Last 24	Hours : Week (Menti	Jun	20 - Aug 3				12
						e - 1	ж. – з	5 - K	
		No tweats detected					17. 11 17. 14	1.000	1
				39	32 3	6	14 14	- 20	14
				- 34	3		11 X	- 2	10

2. Select Client Application Management.

Enrolment Settings	Enable support to erroll Android devices in scenarios where yes do not have access to Google Play store.	\bigcirc
Access and Authentication	Sync SEP Cloud will your klenitry provider, turn on two factor authentication for administrations, or manage partner access to your company account	\odot
SEP Cloud Installation Package	Create redshifts/date installation packages for your devices so that you can control when and how they are enclosed.	\odot
Discovery Settings	Set up one or more devices as discovery agents, which can be used to find devices on your network that are not enrolled in SEP Cloud.	\odot
Client Application Management	Authorize applications to access Engineer Protection Dowd data	\odot
Client Removal Settings	Prevent unauthorized users from removing the SEP Cloud security client on	0

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

Client	Applicati	on Management [●]	
		0-G_rlZqQCy_P4Ds8BnpYw costcater io LZTTG8-IQfuYwV52skZoDw DOMARID	1 CLIENT APPLICATIONS ADDED
	O2ID.0	G_rtZqQCy_P4Ds8BepYwLZTTG8- V52skZoDw85gmoqisI9nihm68m1bvpv0upd	Jun 12, 2019 CREATED

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.

ETS SEP Cloud Integrat	or	×
Help		
SEP Cloud Configuration	ı ————	Edit Configuration
Client Id		
Client Secret		
Domain Id		
Customer Id		
Organization		
	Validate Credential	
	Fi	nish Cancel

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.

ETS SEP Cloud Integrator	×
SEP Cloud Integration configured successfully	
ОК	

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	0x000000000001214						Detected: low-risk intrusion attempt
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILESIMICROSOFT SECURITY CLIENTMISMPENG.EXE
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILESIMICROSOFT SECURITY CLIENTIMISMPENG.EXE
	Server												Symantec Product Tamper Protection has blocked unauthorized access from file: C:\PROGRAM FILES (X86)WEBROOTWRSA.EXE
127.163.118.133	Server	443	2	https://secure.eicar. org/eicar.com	C:\Program Files\Mozilla	Diagnostic: EICAR Standard	0x000000000001214						Detected: low-risk intrusion attempt
	Server							C:\Users\Pratik.k\Deskt op\eicar_com\	44D88612FEA8 A8F36DE82E12 78ABB02F	275A021BBFB64 89E54D471899F7 DB9D1663FC695	5F28383E- C3DA-416F- 824E-	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik_k\Deskt op\eicar_com\	44D88612FEA8 A8F36DE82E12 78ABB02F	275A021BBFB64 89E54D471899F7 DB9D1663FC695	1027F027- 85FD-4043- 802A-	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\\$RECYCLE.BIN\S-1- 5-21-117257714- 2094817907- 3186505446-	44D88612FEA8 A8F36DE82E12 78ABB02F	275A021BBFB64 89E54D471899F7 DB9D1663FC695 EC2FE2A2C4538	01382E2E- D244-472D- ACDA- 36DE1E67FE6	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\Deskt op\eicar_com.zip	44D88612FEA8 A8F36DE82E12 78ABB02F	275A021BBFB64 89E54D471899F7 DB9D1663FC695	41D40989- D470-4CBD- B873-	EICAR Test String	Threat detected: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\AppD ata\LocalMozilla\Firefo x\Profiles\sw7qzhxa.d efault\cache2\entries\7 87F9B10F6FDEFC7173	44D88612FEA8 A8F36DE82E12 78ABB02F	275A021BBFB64 89E54D471899F7 DB9D1663FC695 EC2FE2A2C4538 AABF651FD0F	03917B82- ADE7-41F1- BAA2- 072C76E2831 0	EICAR Test String	Threat remediated: Malware - EICAR Test String
	Server							C:\Users\Pratik.k\AppD ata\LocaMozilla\Firefo	44D88612FEA8 A8F36DE82E12	275A021BBFB64 89E54D471899F7	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.

5-VM30 5-VM30	2019-06-25T20:41:53.760Z	Server					NCLIFOIR	FIOCESSES	Regiatly	Skipped	TOtal	message
5-V/M30		361 461	2019-06-25T20:44:43.760Z	10	595	6588	596	1772	404	б	9996	Scan completed on R1S5-VM30
	2019-06-26T02:42:16.881Z	Server	2019-06-26T02:44:57.881Z	б	595	6588	596	1772	404	ъ	9996	Scan completed on R1S5-VM30
5-VM30	2019-06-26T02:42:16.881Z	Server	2019-06-26T02:44:57.881Z	ъ	595	6588	596	1 772	404	5	5996	Scan completed on R1S5-VM30
5-VM30	2019-06-26T18:48:23.294Z	Server	2019-06-26T18:51:16.294Z	б	598	7048	596	1998	404	ъ	10685	Scan completed on R1S5-VM30
5-VM30	2019-06-26T18:48:23.294Z	Server	2019-06-26T18:51:16.294Z	ъ	598	7048	596	1 998	404	5	10685	Scan completed on R1S5-VM30
5-VM30	2019-06-27T00:50:43.524Z	Server	2019-06-27T00:53:33.524Z	б	598	7048	596	1992	404	ъ	10679	Scan completed on R1S5-VM30
5-VM30	2019-06-27T00:50:43.524Z	Server	2019-06-27T00:53:33.524Z	ъ	598	7048	596	1 992	404	б	10679	Scan completed on R1S5-VM30
5-VM30	2019-06-27T06:30:19.904Z	Server	2019-06-27T06:33:42.904Z	б	598	7048	596	1992	404	ъ	10679	Scan completed on R1S5-VM30
5-VM30	2019-06-27T06:30:19.904Z	Server	2019-06-27T06:33:42.904Z	ъ	598	7048	596	1 992	404	ъ	10679	Scan completed on R1S5-VM30
5-VM30	2019-06-27T11:24:23.461Z	Server	2019-06-27T11:24:23.461Z	б	2	ъ	б	ъ	ъ	ъ	2	Scan completed on R1S5-VM30
5-VM30	2019-06-27T11:24:23.461Z	Server	2019-06-27T11:24:23.461Z	Ю	2	5	ъ	ъ	ъ	б	2	Scan completed on R1S5-VM30
5-VM30	2019-06-27T11:08:39.092Z	Server	2019-06-27T11:11:34.092Z	б	585	7048	596	1932	404	30	10606	Scan completed on R1S5-VM30
5-VM30	2019-06-27T11:08:39.092Z	Server	2019-06-27T11:11:34.092Z	ъ	585	7048	596	1 932	404	50	10606	Scan completed on R1S5-VM30
5-V 5-V 5-V 5-V 5-V 5-V 5-V 5-V 5-V 5-V	M30 M30 M30 M30 M30 M30 M30 M30 M30 M30	M30 2019-08-267102-42,16,8812 M30 2019-06-26718,48,23,2942 M30 2019-06-26718,48,23,2942 M30 2019-06-27106,30,43,5242 M30 2019-06-277106,30,43,5242 M30 2019-06-277106,30,19,9042 M30 2019-06-277106,30,19,9042 M30 2019-06-27711,24,23,4612 M30 2019-06-27711,24,23,4612 M30 2019-06-27711,24,23,4612 M30 2019-06-27711,24,23,4612 M30 2019-06-27711,24,23,4612 M30 2019-06-27711,08,39,0922 M30 2019-06-27711,08,39,0922	M30 2019-06-26712-42-16.881Z Server M30 2019-06-26718.48.23.294Z Server M30 2019-06-26718.48.23.294Z Server M30 2019-06-2706.94.3.524Z Server M30 2019-06-27106.30.19.904Z Server M30 2019-06-27106.30.19.904Z Server M30 2019-06-27101.30.19.904Z Server M30 2019-06-27111.24.23.461Z Server M30 2019-06-27111.24.23.461Z Server M30 2019-06-27111.24.23.461Z Server M30 2019-06-27711.24.39.092Z Server M30 2019-06-27711.24.39.092Z Server	M30 2019-06-26712:42:16.881Z Server 2019-06-26712:44:57.881Z M30 2019-06-26718:46:23.294Z Server 2019-06-26718:51:16.294Z M30 2019-06-26718:46:23.294Z Server 2019-06-26718:51:16.294Z M30 2019-06-2710:50:43.524Z Server 2019-06-2710:53:33.524Z M30 2019-06-27706:30:19:904Z Server 2019-06-27706:33:42.904Z M30 2019-06-27706:30:19:904Z Server 2019-06-27706:33:42.904Z M30 2019-06-27706:30:19:904Z Server 2019-06-27706:33:42.904Z M30 2019-06-27706:30:19:904Z Server 2019-06-27706:33:42:904Z M30 2019-06-27711:24:23:461Z Server 2019-06-27711:24:23:461Z M30 2019-06-27711:24:23:461Z Server 2019-06-27711:24:23:461Z M30 2019-06-27711:24:23:461Z Server 2019-06-27711:24:23:461Z M30 2019-06-27711:08:39:092Z Server 2019-06-27711:1:4:092Z M30 2019-06-27711:08:39:092Z Server 2019-06-277111:1:4:092Z	M30 2019-06-26T02-42:16.8812 Server 2019-06-26T18-44:57.8812 % M30 2019-06-26T18-48:23.2942 Server 2019-06-26T18:16.2942 % M30 2019-06-26T18-48:23.2942 Server 2019-06-26T18:16.2942 % M30 2019-06-27T08:33.2942 Server 2019-06-27T06:33.35.242 % M30 2019-06-27T06:30.19.9042 Server 2019-06-27T06:33.35.242 % M30 2019-06-27T06:30.19.9042 Server 2019-06-27T06:33.42.9042 % M30 2019-06-27T06:30.19.9042 Server 2019-06-27T11.24.23.4612 % M30 2019-06-27T11:24.23.4612 Server 2019-06-27T11:24.23.4612 % M30 2019-06-2	M30 2019-06-26702-42:16.8312 Server 2019-06-26712:457.8312 % %55 M30 2019-06-26718:48:23.294Z Server 2019-06-26718:51:16.294Z % %58 M30 2019-06-26718:48:23.294Z Server 2019-06-26718:51:16.294Z % %58 M30 2019-06-27706:33.3524Z Server 2019-06-27706:33.3524Z % %58 M30 2019-06-27706:30:19.904Z Server 2019-06-27706:33.42.904Z % %58 M30 2019-06-27706:30:19.904Z Server 2019-06-27706:33.42.904Z % %58 M30 2019-06-27706:30:19.904Z Server 2019-06-27706:33.42.904Z % % %58 M30 2019-06-277106:30:19.904Z Server 2019-06-27711:42.42.461Z %	M30 2019-06-267102:42:16.881Z Server 2019-06-267102:44:57.881Z % %588 %588 M30 2019-06-26718:48:23.294Z Server 2019-06-26718:51:16.294Z % %98 %048 M30 2019-06-26718:48:23.294Z Server 2019-06-26718:51:16.294Z % %98 %048 M30 2019-06-27108:50:13.524Z Server 2019-06-27108:53:35.24Z % % % % M30 2019-06-27106:30:19.904Z Server 2019-06-27108:33:42.904Z %	M30 2019-08-26702 42:16.8812 Server 2019-06-26712:45:78812 % %56 %588 %586 M30 2019-06-26718:48:23:294Z Server 2019-06-26718:51:16:294Z % %588 %048 %596 M30 2019-06-26718:48:23:294Z Server 2019-06-26718:51:16:294Z % %588 %048 %596 M30 2019-06-27106:30:43:524Z Server 2019-06-27106:33:3524Z % %58 %048 %596 M30 2019-06-27106:30:19:904Z Server 2019-06-27106:33:42:904Z % %58 %048 %596 M30 2019-06-27106:30:19:904Z Server 2019-06-27106:33:42:904Z % %58 %048 %596 M30 2019-06-27110:42:3461Z % %596 %048 %596 M30 2019-06-27110:42:3461Z % %0 %58 %048 %596 M30 2019-06-27111:42:33:461Z % %0 %0 %0 %0 %0 %0 %0 %0 %0 %0 %0	M30 2019-06-26702-42:16.8312 Server 2019-06-26712:457.8612 %	M30 2019-06-267102:42:16.881Z Server 2019-06-267102:44:17.881Z 5 588 586 1772 404 M30 2019-06-267102:42:16.881Z Server 2019-06-267103:512:42 598 7048 596 1998 404 M30 2019-06-26718:46:23.294Z Server 2019-06-26718:51:16:294Z 6 598 7048 596 1998 404 M30 2019-06-2718:46:23.294Z Server 2019-06-2718:51:16:294Z 6 598 7048 596 1992 404 M30 2019-06-27105:043:524Z Server 2019-06-27105:33:524Z 6 598 7048 596 1992 404 M30 2019-06-27105:30:19:904Z Server 2019-06-27105:33:42:904Z 6 598 7048 596 1992 404 M30 2019-06-27105:30:19:904Z Server 2019-06-27110:34:23:461Z 6 5 6 6 5 6 6 6 6 6 6 6 6 6 6 6	M30 2019-06-267102:42:16.8312 Server 2019-06-267102:44:57.8812 % %95 %86 %96 %772 %04 %0 M30 2019-06-267118:46:23.294Z Server 2019-06-267118:51:16:294Z % %98 %96 %986 %992 %044 %	M30 2019-06-26702-42:16.881Z Server 2019-06-26712:45:7812 % <

 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.

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_ADMINI STRATOR	User 'John' logged in
06/12/2019 01:07:14 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.165.3	ROLE_SCSEM_ACCOUNT_ADMINI STRATOR	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_ADMINI STRATOR	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_ADMINI STRATOR	User 'John' logged in
06/12/2019 04:22:39 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.1 <mark>3</mark> 0.57	ROLE_SCSEM_ACCOUNT_ADMINI STRATOR	User 'John' logged in
06/12/2019 04:26:43 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINI STRATOR	User 'John' logged in
06/12/2019 04:31:12 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.145.29	ROLE_SCSEM_ACCOUNT_ADMINI STRATOR	User 'John' logged in
06/12/2019 04:34:48 PM	C5n-s8KYT46NUcVflOdcgg	John	10.33.130.57	ROLE_SCSEM_ACCOUNT_ADMINI STRATOR	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

© Copyright Netsurion. All Rights Reserved.



5.4 Dashboards

• SEP Cloud – Threats Detected by the Host Name



• SEP Cloud – Login Details by the Source IP Address

SEP Cloud - Login Details by Source IP Address src_ip_address: 10.33.145.27 John

• 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.

	Export Import Utility
xport Import 1. Provide the path and file na 2. Click the Import button.	me of the Categories file. Use the '' button to browse and locate the import file.
Options	Location
 Category 	
O Filters	
 Alerts 	
O Systems and Groups	Source :
O RSS Feeds	
O Reports	
 Behavior Rules 	
O SCAP	
O Token Value	
	Import
	Side Close

- 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.

1. Provide the path and file na 2. Click the Import button. Options	ame of the Alerts file. Use the '' button	to browse and locate the import file.
 Category Filters Alerts Systems and Groups 	 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.
RSS Feeds	Source :	
Behavior Rules SCAP	*.isalt	
🔘 Token Value		

- 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.

=	Event Tracker ⊕					🐥 🛛 Admin •	Tools -
-	Home		Active Watch Lists	Collection Master	Group Management	Systems	🔒 / Dashb
٩		-	Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	M Diagnostics	💮 Knowledge Objects	The Weights	
~			🍓 Behavior Correlation Settings	😴 Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			of Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. Click the **Import** button.

l Import		×
Select file	🗁 Browse	Upload
		Close

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

Impoi	rt		×
Sele	ect file		🗁 Browse Upload
	Object name	Applies to	Group name
	SEP Cloud	Symantec End Point Protection Cloud	SEP Cloud
			Import Close

6. Knowledge Objects are now imported successfully.

	×
File imported successfully.	
	1
ОК	

6.4 Flex Reports

On the EventTracker Control Panel,

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

ote : if report(s) contains tem Options) Category	Date, first import template and proceed with exportimport utility.	
) Filters		
Alerts	O Legacy (*.issch) New (*.etcrx)	
Systems and Groups	Source :	
RSS Feeds	JSSCN	
Reports		
Behavior Rules		
) SCAP		
) Token Value		

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

anabic	a reporte				
tle		Frequency Show a	- ର୍ ଝ୍		
2	Title	Sites	Groups	Systems	Frequency
	EDIT SEP Cloud - Console Login Logout D	et NTPLDTBLR146	Default	SEPCloud	Undefined
2 E	EDIT SEP Cloud - Management Activities	NTPLDTBLR146	Default	SEPCloud	Undefined
2 <u>E</u>	EDIT SEP Cloud - Scan Details	NTPLDTBLR146	Default	SEPC6	Undefined
2 <u>E</u>	EDIT SEP Cloud - Threat Detected	NTPLDTBLR146			Undefined
					>
lote: \$	Set run time option is not applicable for Defi	ed Reports and Hourly Reports			>

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.

	Home			
٩	My Dashboard			
R	Threats	-	1	
		ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			-
	Compliance		Contraction of the second	

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

EventTracker⊕	*	Admin•	Tools •	💽 ETAdmin *
My Dashboard		1	/Dashboar	rd / My Dashboard
		Ð	or (a) 🖏	; 1 🖡 🖲 🛈

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.

Import		
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.		
Available widgets		
SEP Cloud - Threat Detect SEP Cloud - Login Detail SEP Cloud - Logged out D SEP Cloud - Threat Detect SEP Cloud - Threat Detect SEP Cloud - Threat Detect SEP Cloud - Threat Detect		
	Import Cle	ose

5. Import is now completed successfully.

s	elected dashlets imported successfully.
	ОК

7. Verifying the Knowledge Pack

7.1 Category

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

=	Event Tracker ⊕					🐥 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	Correlation	🔍 IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	Diagnostics	😥 Knowledge Objects	The Weights	
<u>~</u>			🗞 Behavior Correlation Settings	対 Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	D Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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.

Ξ	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
0			Alerts	Correlation	Q IP Lookup Configuration	Q Users	
	0	2	Behavior Correlation Rules	A Diagnostics	💮 Knowledge Objects		
~			behavior Correlation Settings	觉 Event Filters	Manager	Uindows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
		-	₀[^e _a Category	FAQ Configuration	Report Settings		_
	Attacker			- News			

3. In the **Search** box, type **SEP Cloud**, and then click the **Go** button.

Alerts								🕇 / Admin / Alerts
Show All 🗸						Search by Alert	name 🖌	SEP Cloud Q Q
599 Available Alerts Total number of skets available	368 Active Alerts Total number of active alerts			599 System/User D Count for system an	System User efined Alerts d user defined alerts	242	599 Alerts by Th Count of alerts	Critical and State
Activate Now Click 'Activate Now' after	naking all changes							Total: 4 Page Size 25 V
Alert Name A	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
📄 Ĝỗ SEP Cloud - Critical Feature Disabled	•							Symantec End Point Protection Cloud
βδ SEP Cloud - Definition Update Failed	•							Symantec End Point Protection Cloud
🗋 ββ SEP Cloud - Scan Aborted	•							Symantec End Point Protection Cloud
ි රිරි SEP Cloud - Threat Detected	•							Symantec End Point Protection Cloud

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.

Ξ	EventTracker 🕀					🐥 Admin-	Tools -
	Home		San Active Watch Lists	Collection Master	Group Management	Systems	🔒 / Dashb
٥		_	Alerts	Correlation	Q IP Lookup Configuration	Q Users	
	0 1		Behavior Correlation Rules	1 Diagnostics	💮 Knowledge Objects	A Weights	
2°			🗞 Behavior Correlation Settings	🛱 Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Ind Unsafe connections or processes, new TCP entry point USB	dicators of Cc activities, New sen	Casebook Configuration	🔮 Eventvault	🧭 Parsing Rules		
			erenter of the second	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Knowledge Objects	
Search objects	Q Q
Groups	🕀 🧭 🗓
Fortimail	
Juniper JunOS	
Kaspersky Security Center	
Microsoft IIS Web Server	
OpenDNS	
Palo Alto Firewall	
Password State	
E Salesforce	
SEP Cloud	
SEP Cloud	<u>í</u> (
E SharePoint	
Sophos Central	
Webroot	
Windows	

7.4 Flex Reports

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

≡	Event Tracker ⊕			
	Home			
Q R	 Report Configuration]	1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer Attacker			-

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

Sch	neduled 🔘 Queued 💿 Defined					
Repor	t Groups		(+)	Repor	ts configura	tion: SEP Cloud
1,5	All Operations Repor			(+) [Ĩ 2,	
63	Operations					Title
£3	Flex				~	CED Cloud Management Activities
	ADManager Plus	Ĩ	1		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	aut cloud - management Activities
	All Compliance Repor	Ē	1		523	SEP Cloud - Console Login Logout Details
	All Operations Repor	Ē	0		1	SEP Cloud - Threat Detected
	All Security Audit R	1	0			SEP Cloud - Scan Details
Ð	All Threat Report	Ĩ	0			
	EventTracker	Ĩ	0			
	F5 BIG IP	Ē	1			
	FortiMail	Ē	1			
	Juniper JUNOS	Ē	0			
۵	OpenDNS	Ĩ	0			
	Passwordstate	Ē	0			
	Salesforce	Ē	1			
	SEP Cloud	Ē	۲			
	Webroot	Ű	1			
	Windows	Ĩ	Ø			

7.5 Dashboards

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

Customize dashlets			×
SEP Cloud			Q
SEP Cloud - Logged out Details	SEP Cloud - Login Details by So	SEP Cloud - Management Events	SEP Cloud - Threat Detected by
SEP Cloud - Threat Detected by	SEP Cloud - Threat Detected by		
			Add Delete Close

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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #23 among <u>MSSP Alert's 2021 Top 250 MSSPs</u>.

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