

Integration Guide

Integrating Citrix Cloud Analytics with EventTracker

Publication Date:

June 06, 2022

Abstract

This guide provides instructions to configure the Knowledge Pack in EventTracker to receive the logs from the Citrix Cloud Analytics service. The Knowledge Pack contains the reports, dashboard, alerts, and saved searches.

Scope

The configuration details in this guide are consistent with the EventTracker version 9.3 or later and Citrix Cloud Analytics.

Audience

This guide is for the Administrators responsible to configure the Knowledge Packs to EventTracker.



Table of Contents

1	Ove	erview	4
2	Pre	requisites	4
3	Eve	entTracker Knowledge Packs	4
	3.1	Alerts	4
	3.2	Categories	5
	3.3	Reports	5
	3.4	Dashboards	6
4	Imp	oorting Citrix Cloud Analytics Knowledge Packs into EventTracker	7
	4.1	Categories	8
	4.2	Alerts	9
	4.3	Knowledge Objects (KO)	. 10
	4.4	Reports	. 12
	4.5	Dashboards	. 13
5	Ver	ifying Citrix Cloud Analytics Knowledge Packs in EventTracker	.16
	5.1	Categories	. 16
	5.2	Alerts	. 16
	5.3	Knowledge Objects	. 17
	5.4	Reports	. 18
	5.5	Dashboards	. 19

1 Overview

Citrix Cloud Analytics solutions facilitate organizations to detect and deflect potential threats and instantly address performance issues long before security incidents occur, or employees begin to submit help desk tickets. Citrix Analytics for Security continuously assesses the behavior of Citrix Virtual Apps and Desktops users, Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) users, and Citrix Workspace users. It applies actions to protect sensitive corporate information.

EventTracker dashboard and reports will provide information about possible attacks, suspicious activities, or any other threat noticed in user activities based on the user's risk score.

2 Prerequisites

Refer to <u>How-To guide</u> to see the process of configuring Citrix Cloud Analytics to forward logs to EventTracker.

3 EventTracker Knowledge Packs

Once the Event Tracker Manager receives the logs, configure the Knowledge Packs into EventTracker. The following Knowledge Packs (KPs) are available in EventTracker to support the Citrix Cloud Analytics.

3.1 Alerts

Citrix Cloud Analytics: User riskscore change and Suspicious activities detected - This alert is triggered when the following events occur.

- Change in User's risk score If there is a change in a user's risk score (that is, an increase or decrease in the risk score) based on user activity.
- Detection of Suspicious activities If there is a summary of the event that indicates a threat or risk based on user activity.

3.2 Categories

- Citrix Cloud Analytics User riskscore activities Provides information related to user riskScore.
- Citrix Cloud Analytics User profile usage activities Provides information related to user data usage.
- Citrix Cloud Analytics Risk indicator Summary Provides information related to user suspicious activities.

3.3 Reports

Citrix Cloud Analytics - User riskscore activities: This report delivers detailed information on the increase and decrease of the user risk scores. It includes username, risk score value changes (difference between earlier and current risk score), and more.

А	D	L L	U	L	r r	0		1
LogTime	Computer	Tenant ID	User Name	Current Riskscore	Change In riskscore	Alert Type	Alert Message	Timestamp
04-26-2022 02:25/02 AM	CITRIX-CLOUD-SYSLOG	"contoso	"calvin	1 8	-21,73913	"riskscore_large_drop_pct	"Large risk score drop percent since last check	*2021-02-11T05:45:002

Citrix Cloud Analytics – User profile summary: This report provides a detailed summary of user data usage, user location, and device access information.

User Name	Event type	data usage bytes	Deleted file count	Downloaded bytes	Downloaded file count	Tenant ID	uploaded bytes	uploaded
"joeb"	"userProfileUsage"	5	562	25664	5	"contoso"	5	0
"tmjones"	"userProfileUsage"	198602	5	198602	56	"contoso"	64556	0

Citrix Cloud Analytics – User risk activities summary: This report summarizes any suspicious activities or threats linked to a user. It comprises user details, threat type, the severity of the threat, risk probability, and other events occurrence details.

LogTime	Computer	Tenant ID	User Name	Source IP	Data source ID	Data source	Doamin Name	Domain d
04-26-2022 02:25:02 AM	CITRIX-CLOUD-SYSLOG	"contoso"	"karen"		2	"Citrix Endpoint Management"		
04-26-2022 02:25:02 AM	CITRIX-CLOUD-SYSLOG	"contoso"	"mjones"	"105.39.70.221"	2			
04-26-2022 02:25:02 AM	CITRIX-CLOUD-SYSLOG	"contoso"	"smith"		2	"Citrix Endpoint Management"		
04-26-2022 02:25:02 AM	CITRIX-CLOUD-SYSLOG	"contoso"	"cooper"	"76.164.48.218"	1	"Citrix Gateway"		
04-26-2022 02:50:51 AM	CITRIX-CLOUD-SYSLOG	"contoso"	"joey"		2		"googleads.g.doubleclick.net"	"Computir

Domain Category	Risk indicator id	Risk indicator name	Risk category	Risk probability	Risk severity	Action Taken	Reason for action	Other Ris
	200	"Jailbroken / Rooted Device Detected"	"Compromised endpoints"	1.0	"high"			
	201							
	203	"Unmanaged Device Detected"	"Compromised endpoints"	1 .0	"high"			
	102	"Logon from suspicious IP"	"Compromised users"	0.91	"medium"			
"Advertisements/Banners"	\$ 01					"blocked"	"URL Category match"	

Risk Triggering Conditions	Risky domain list	User ui link	User activity Timestamp	Event type
		"https://contoso.cloud.com/user/	"2021-04-13T17:49:05Z"	"indicatorSummary"
			"2021-04-09T17:50:39Z"	"indicatorEventDetails"
		"https://contoso.cloud.com/smith/	"2021-04-13T12:56:30Z"	"indicatorSummary"
"relevant_event_type": "Logon","client_ip": "76.164.48.218", "observation_start_time": "2019-10- 10T10:00:002","suspicion_reasons": "brute_forceJexternal_threat		"https://contoso.cloud.com/user/	"2019-10-10T10:14:59Z"	"indicatorSummary"
			"2018-03-15T10:57:21Z"	"indicatorEventDetails"



3.4 Dashboards



Citrix Cloud Analytics - Top event types

Citrix Cloud Analytics - Top risk categories







Citrix Cloud Analytics - Top threat identified

4 Importing Citrix Cloud Analytics Knowledge Packs into EventTracker

NOTE: Import the Knowledge Packs in the following sequence.

- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.





3. Click Import.

4.1 Categories

1. In the Import tab, choose the Category option, and then click on the Browse button.

9	Export Import Utility	□ X
Export Import Provide the path and file name Click the Import button. Options Category Filters Alerts Systems and Groups Token Value Reports	Export Import Utility of the Categories file. Use the "" button to browse and locate the import file. Location Source :	
Behavior Correlation	Import	Close

- 2. Locate the Categories_Citrix Cloud Analytics.iscat file, and then click on the Open button.
- **3.** To import the categories, click on the **Import** button.

4. EventTracker displays a success message.



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

4.2 Alerts

 1. In the Import tab, choose the Alerts option, and then click on the Browse
 button.

 It
 Export Import Utility

Reports on the console where the alerts are imported. Behavior Correlation Behavior Correlation	
O Behavior Correlation Source :	

- 2. Locate the Alerts_Citrix Cloud Analytics.isalt file, and then click on the Open button.
- **3.** To import the alerts, click on the **Import** button.

4. EventTracker displays a success message.



5. Click OK, and then click Close.

4.3 Knowledge Objects (KO)

1. In the EventTracker Manager application, go to the Admin menu and click Knowledge Objects.

≡	Event Tracker @					🐥 🛛 Admin 🗸	Tools -
	Home		🚰 Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	▲ Diagnostics	· 🔆 Knowledge Objects		
N.			🇞 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		
	Attacker		e Category	FAQ Configuration	Report Settings		
				- News			

2. In the Knowledge Objects interface, click on the Import I button as highlighted in the below image:





3. Then click Browse.



- 4. Locate the file named KO_Citrix Cloud Analytics.etko.
- 5. Select the Citrix Cloud Analytics check box and then click on the \blacksquare Import option.

Impor	t			×
Sele	ct file		🗁 Browse Uploa	ıd
	Object name	Applies to	Group name	
	Citrix Cloud Analytics	Citrix Cloud Analytics	Citrix Cloud Analytics	
			Imp	port Close

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



4.4 Reports

1. In the Import tab, choose the Reports option and then select New (*. etcrx).

3	Export Import Utility
Export Import Provide the path and file nam Callick the import button Note: if report(s) contains tempt Options Category Filters Alerts Systems and Groups Token Value Reports	Export Import Utility C X
Reports Behavior Correlation	Import Close

2. Locate the file named Reports_Citrix Cloud Analytics.etcrx and select all the check boxes.

۹.	Reports	Import				×					
			a de constante de la constante								
Not	e : It rep	iort(s) contains template, first import template a	and proceed with report import process.								
Sel	ielect file C:\Users\Chithra\Desktop\citrix cloud analytics\Reports_Citrix Cloud Analytics.etcrx Select file										
Ava	ilable re	ports									
Tit	e		Frequency Show all	· & &							
	3	Title	Sites	Groups	Systems	Frequency					
	EDI	Citrix Cloud Analytics - User Data usage	WIN-QKU20VUO2ES	Default	Citrix-Cloud-syslog	Undefined					
		Citrix Cloud Analytics - User Risk Activi	WIN-QKU20VUO2ES	Default	Citrix-Cloud-syslog	Undefined					
E	EDI	Citrix Cloud Analytics - User riskscore a	WIN-QKU20VUO2ES	Default	Citrix-Cloud-syslog	Undefined					
<						>					
1	lote: Set	run time option is not applicable for Defined f	Reports and Hourly Reports								
5	iet run	time for report(s) from	• at interval of minute	es Set ()							
F	Replace	e to	Rep	lace Assign systems							



1. Click on the Import I button to import the report. EventTracker displays a success message.



4.5 Dashboards

The following steps are specific to EventTracker 9 and later.

1. Open the EventTracker application in a browser and Log-in.

88	Home			
٩	My Dashboard			
R	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			_
	Compliance		Carton Carton	

- 2. Navigate to My Dashboard.
- 3. On the My Dashboard interface, click on the Import I button as shown below.

Event Tracker ⊕	ø	Admin -	Tools -	💽 ETAdmin 🝷
My Dashboard		A	/ Dashboar	d / My Dashboard
		(+)	🧭 🎱 🎝	1 3 0

4. Import the dashboard file named Dashboards_Citrix Cloud Analytics.etwd and check-in the Select All checkbox.



5. Click Import as shown below.

lr	nport
	Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
	🗁 Browse Upload
	Available widgets Select All
	Citrix Cloud Analytics
	Citrix Cloud Analytics
	Import Close

6. Import is now completed successfully.



7. In the My Dashboard interface click on the Add ⊕ button to add dashboard.



8. Choose the appropriate name for the **Title** and **Description**, and then click **Save**.

BeventTracker :: Dashboard Configuration - Work - Microsoft Edge	_		\times
▲ Not secure 172.28.9.67:8080/EventTracker/Flex/Add.aspx?dT	ype=28	ιdid=	A»
Edit Dashboard			
Title			
Citrix Cloud Analytics			
Description			
Citrix Cloud Analytics			
Save	Delete	Cance	el

9. In the **My Dashboard** interface, click ^(a) to customize dashlets.

My Dashboar	d						🔒 / Dashb	oard / My Das	ashboard
							🕂 🧭 🕀	0 1 T	() ()
Citrix Clou	Microsoft	Amazon V	BitDefende						

10. In the **Customize dashlets** window, select the imported dashlets and click **Add**.

Customize dashlets				×
Citrix Cloud Analytics				Q
Citrix Cloud Analytics - Top eve	Citrix Cloud Analytics - Top risk	Citrix Cloud Analytics - Top thre		
			Add Delete	Close

Netstrion

5 Verifying Citrix Cloud Analytics Knowledge Packs in EventTracker

5.1 Categories

- 1. Log in to EventTracker.
- 2. Navigate to the Admin menu and click Category.

≡	Event Tracker ⊕					🔶 Admin-	Tools •										
-	Home		Active Watch Lists	Collection Master	Croup Management	Systems	🕈 / Dash										
a			Alerts	Correlation	🔍 IP Lookup Configuration	🙊 Users											
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	1 Weights											
		Indicators of Co USB activities, New sen	🗞 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	Indicators of Co USB activities, New sen	Indicators of Cc USB activities, New sen	Indicators of Co USB activities, New sen	Indicators of C USB activities, New se	USB activities, New sen	Indicators of Cc USB activities, New sen	Casebook Configuration	🛐 Eventvault	🧭 Parsing Rules					
			📲 Category	FAQ Configuration	Report Settings												
	Attacker		- News														

3. In the **Category** tree, scroll down and expand the **Citrix Cloud Analytics** group folder to view the imported category.

- 🔁 Citr	Citrix Cloud Analytics								
E	Citrix Cloud Analytics - Risk indicatorSummary								
E	Citrix Cloud Analytics - User profile usage activiti $\boldsymbol{\varepsilon}$								
E	Citrix Cloud Analytics - User riskscore activities								

5.2 Alerts

- 1. Log in to EventTracker.
- 2. Navigate to the Admin menu and click Alerts.

Ξ	Event Tracker ⊕					🔎 🛛 Admin 🕶	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashl
٩			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	Diagnostics	Knowledge Objects	1 Weights	
			🗞 Behavior Correlation Settings	😨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	🖉 Eventvault	🧭 Parsing Rules		
			o-Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the Search field type Citrix Cloud Analytics, and then click on the Search button.



4. The Alerts management page displays the imported alert.

÷	Click 'Activate Now' after making all changes						
	Alert Name 🔨 T						
	유유 Citrix Cloud Analytics: User risk score change and suspicious activiti						

- 5. To activate the imported alert, toggle the **Active** button.
- 6. EventTracker displays a message box as shown below.



7. Click OK, and then click on the Activate Now button.

NOTE: Specify the appropriate System in Alerts configuration for better performance.

5.3 Knowledge Objects

1. In the EventTracker web interface, navigate to the Admin menu, and click Knowledge Objects.

≡	Event Tracker ⊕					🐥 🛛 Admin-	To ols -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	🔍 IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r 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		
			● Category	FAQ Configuration	Report Settings		
	Attacker		- News				

2. In the Knowledge Object tree, expand the Citrix Cloud Analytics folder to view the imported Knowledge Objects.



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

5.4 Reports

1. In the EventTracker web interface, go to Reports, and click Report Configuration.

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

- 2. In the Reports Configuration interface, choose the Defined option.
- 3. Select the Citrix Cloud Analytics group folder to view the imported reports.



5.5 Dashboards

1. In the EventTracker web interface, navigate to the Home Button and click My Dashboard.

		Home
Dashb	oard	My Dashboard
		Threats
		Incidents

In the Customize daslets window, type Citrix Cloud Analytics in the Search field, and click Search
 You will see the following screen.

C	ustomize dashlets				×
[Citrix Cloud Analytics			ସ	
	Citrix Cloud Analytics - Top eve	Citrix Cloud Analytics - Top risk	Citrix Cloud Analytics - Top thre		
				Add Delete C	lose



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 <u>Managed Threat Protection</u> 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 <u>Secure Edge Networking</u> 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</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 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