Netsurion®
Powering Secure and Agile Networks

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 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 **How-To guide** 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

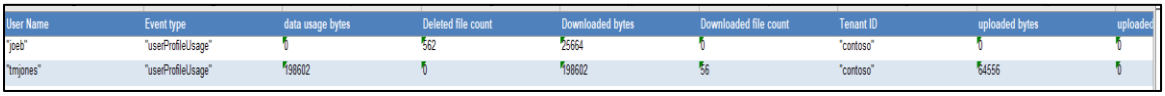
- **Citrix Cloud Analytics - User riskscore activities -** Provides information related to user riskScore.
- **Citrix Cloud Analytics - User profile usage activities -** Provides information related to user data usage.
- **Citrix Cloud Analytics - Risk indicator Summary -** Provides information related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

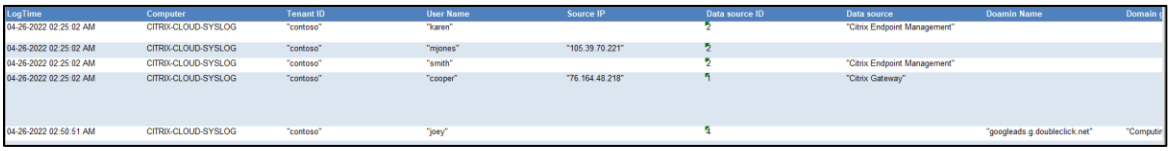
LogTime	Computer	Tenant ID	User Name	Current Riskscore	Change In riskscore	Alert Type	Alert Message	Timestamp
04-26-2022 02:25:02 AM	CITRIX-CLOUD-SYSLOG	"contoso	"calvin	18	-2.173913	"riskscore_large_drop_pct	"Large risk score drop percent since last check	"2021-02-11T05:45:00Z

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



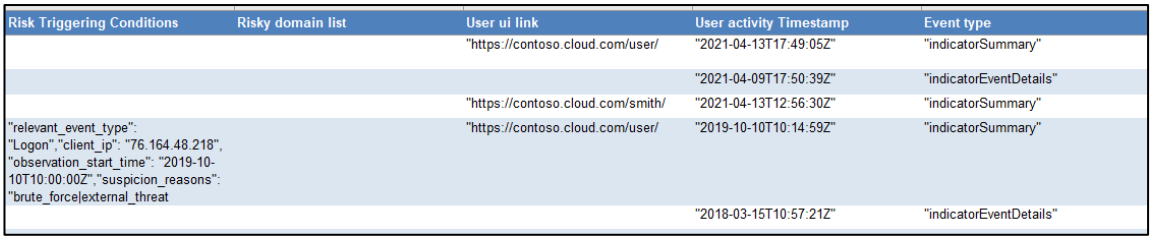
User Name	Event type	data usage bytes	Deleted file count	Downloaded bytes	Downloaded file count	Tenant ID	uploaded bytes	uploaded
"jpeb"	"userProfileUsage"	0	562	25664	0	"contoso"	0	0
"tmjones"	"userProfileUsage"	198602	0	198602	56	"contoso"	64566	0

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
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"		4		"googleads.g.doubleclick.net"	"Computer

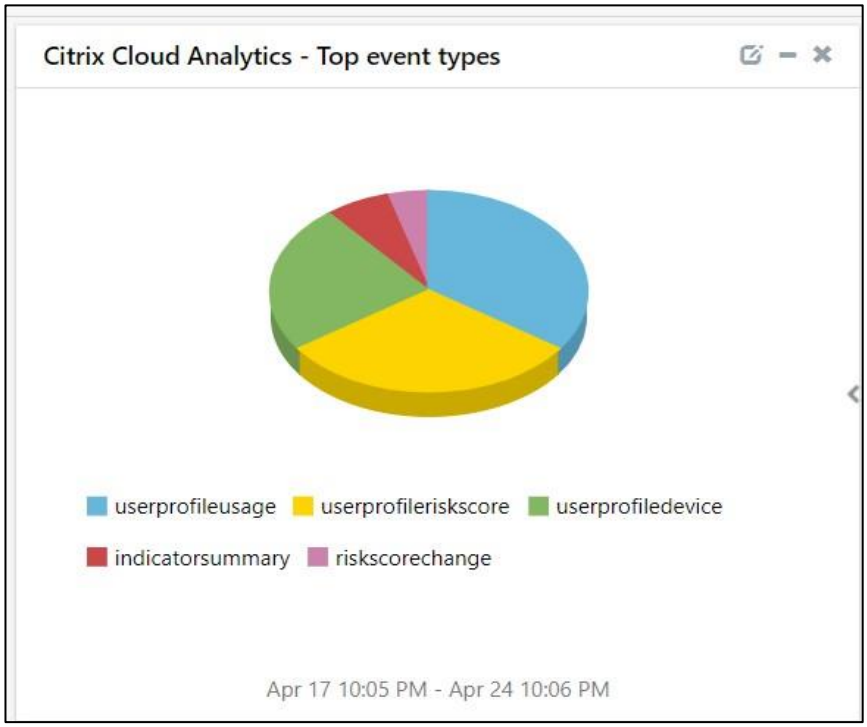
Domain Category	Risk indicator id	Risk indicator name	Risk category	Risk probability	Risk severity	Action Taken	Reason for action	Other Ris
	200	"Jailbroken / Rooted Device Detected"	"Compromised endpoints"	1.0	"high"			
	201							
	203	"Unmanaged Device Detected"	"Compromised endpoints"	1.0	"high"			
	102	"Logon from suspicious IP"	"Compromised users"	0.91	"medium"			
"Advertisements/Banners"	401					"blocked"	"URL Category match"	



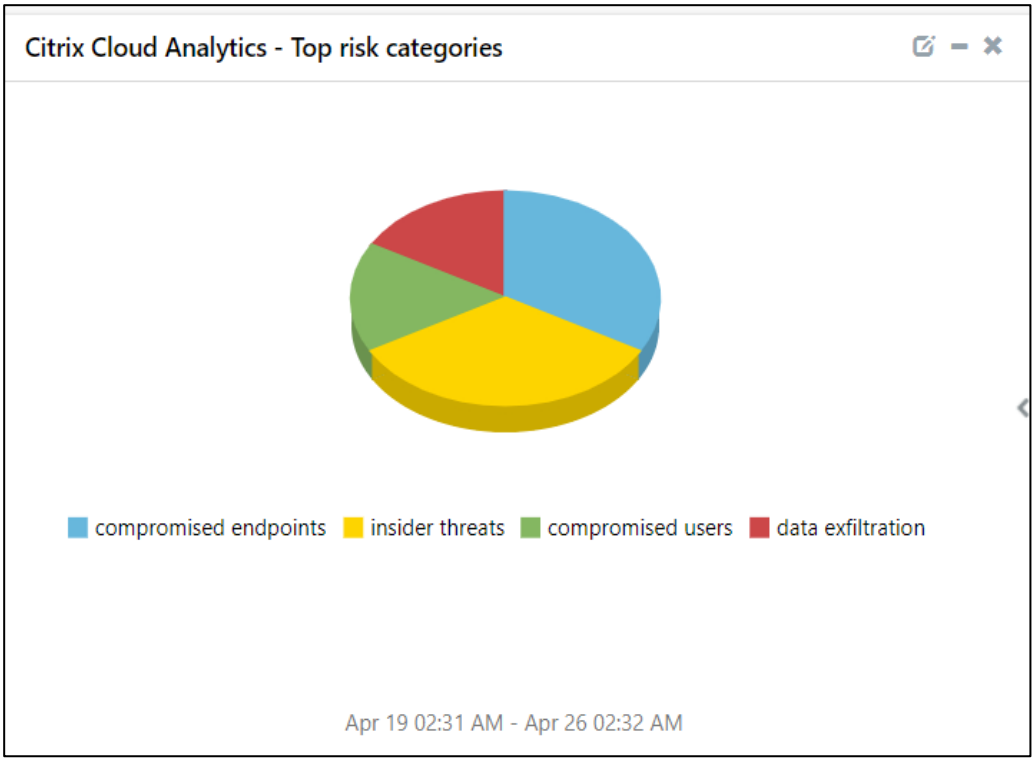
Risk Triggering Conditions	Risky domain list	User ui link	User activity Timestamp	Event type
		"https://contoso.cloud.com/user/	"2021-04-13T17:49:05Z"	"indicatorSummary"
			"2021-04-09T17:50:39Z"	"indicatorEventDetails"
		"https://contoso.cloud.com/smith/	"2021-04-13T12:56:30Z"	"indicatorSummary"
"relevant_event_type":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

3.4 Dashboards

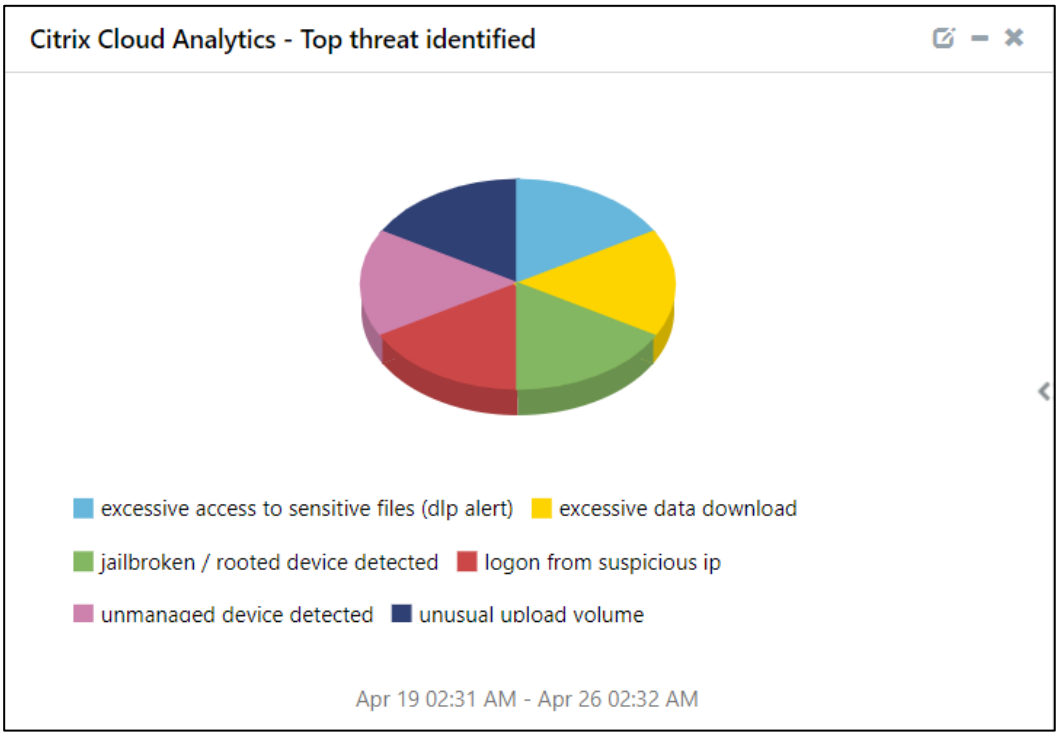
- **Citrix Cloud Analytics - Top event types**



- **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.

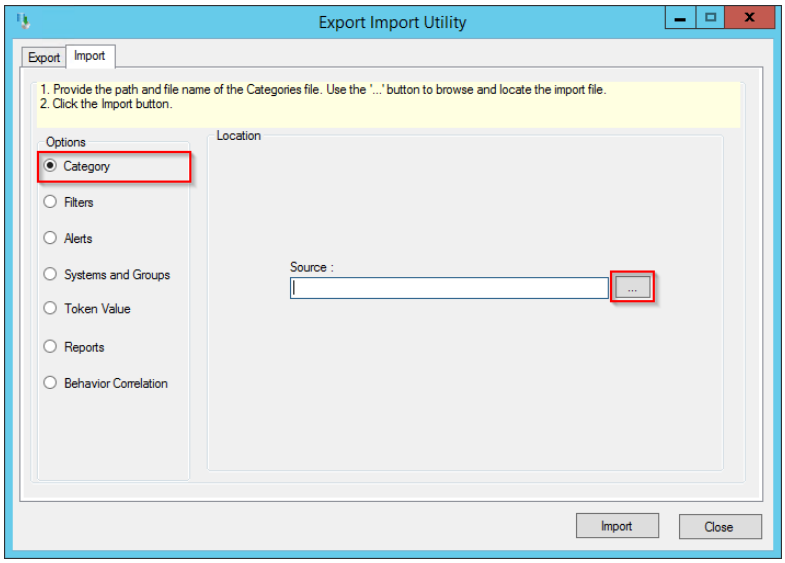
- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

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

3. Click **Import**.

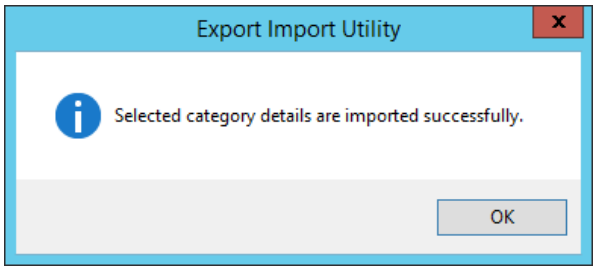
4.1 Categories

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



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.

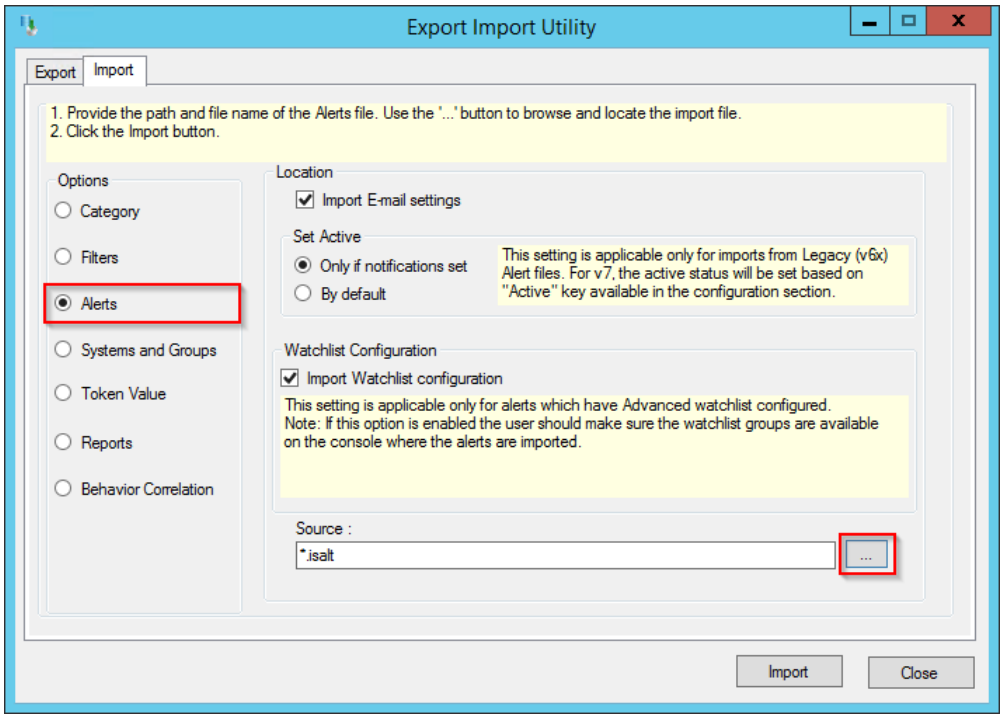
4. EventTracker displays a success message.



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

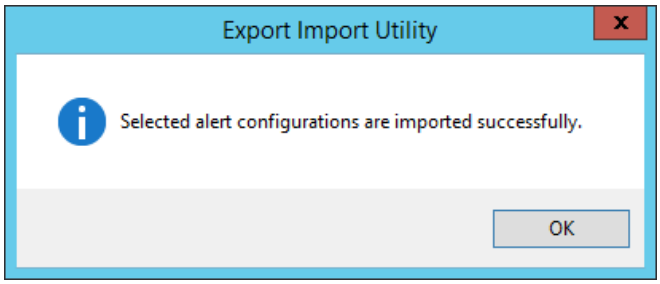
4.2 Alerts

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



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.

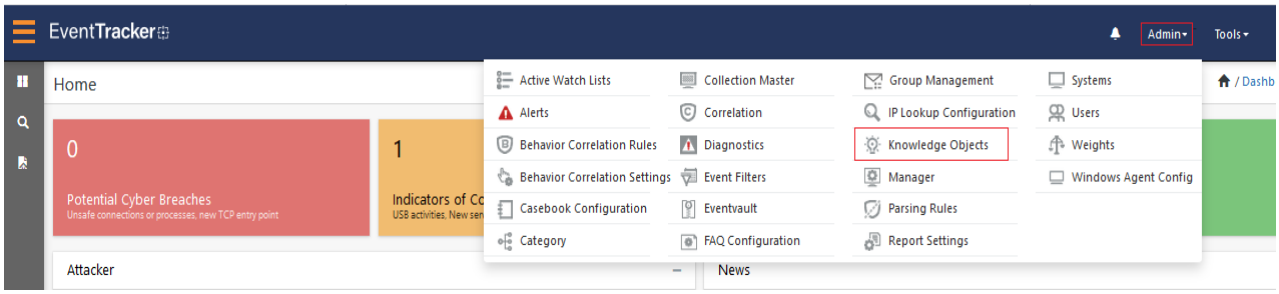
4. EventTracker displays a success message.



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**.

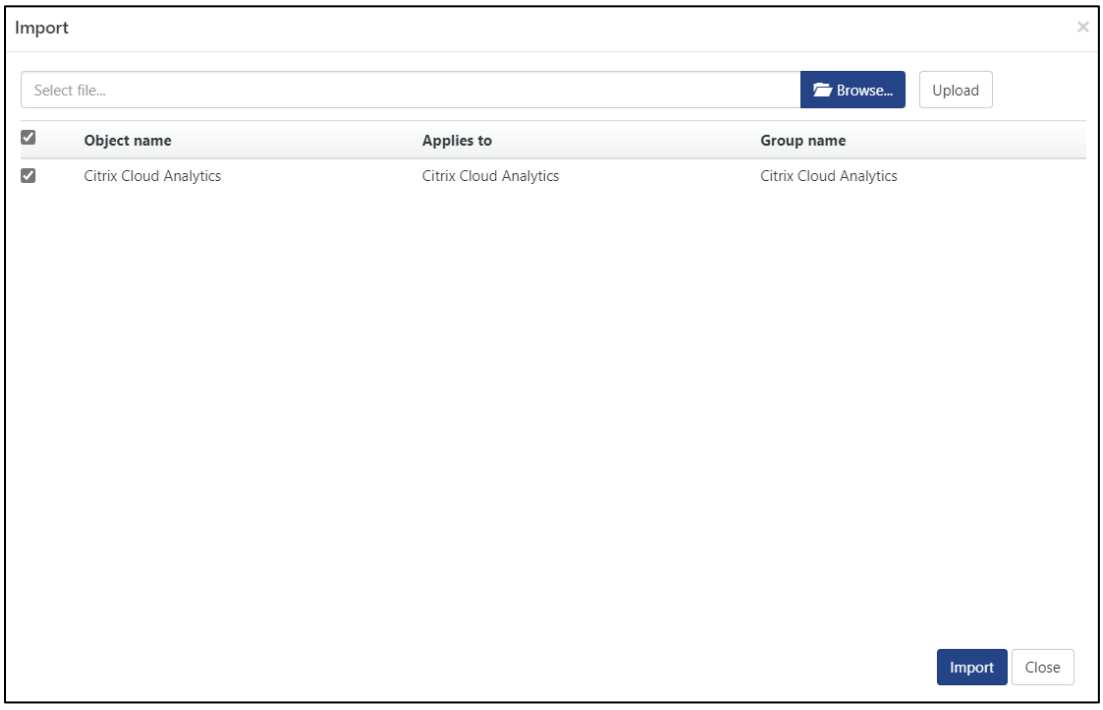


2. In the **Knowledge Objects** interface, click on the **Import** button as highlighted in the below image:

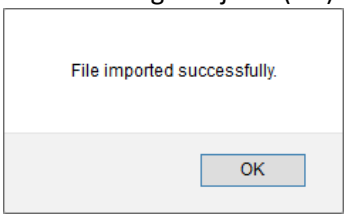
3. Then click **Browse**.

4. Locate the file named **KO_Citrix Cloud Analytics.etko**.

5. Select the **Citrix Cloud Analytics** check box and then click on the **Import** option.

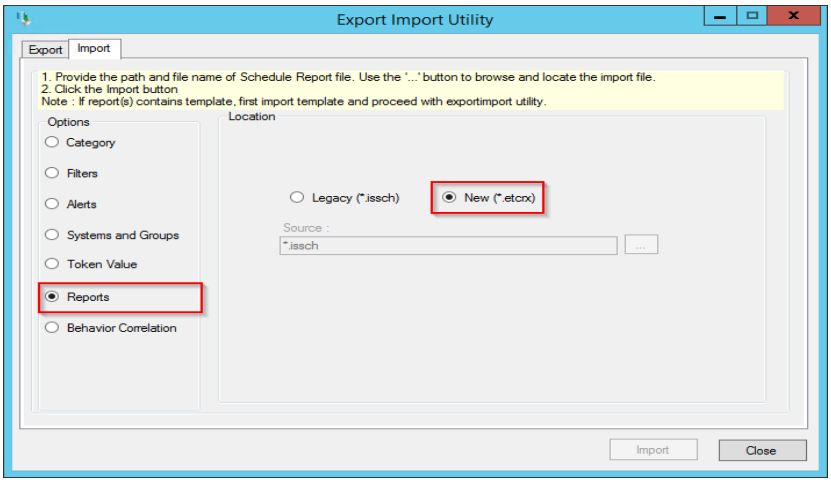


6. The Knowledge Objects (KO) are now imported successfully.

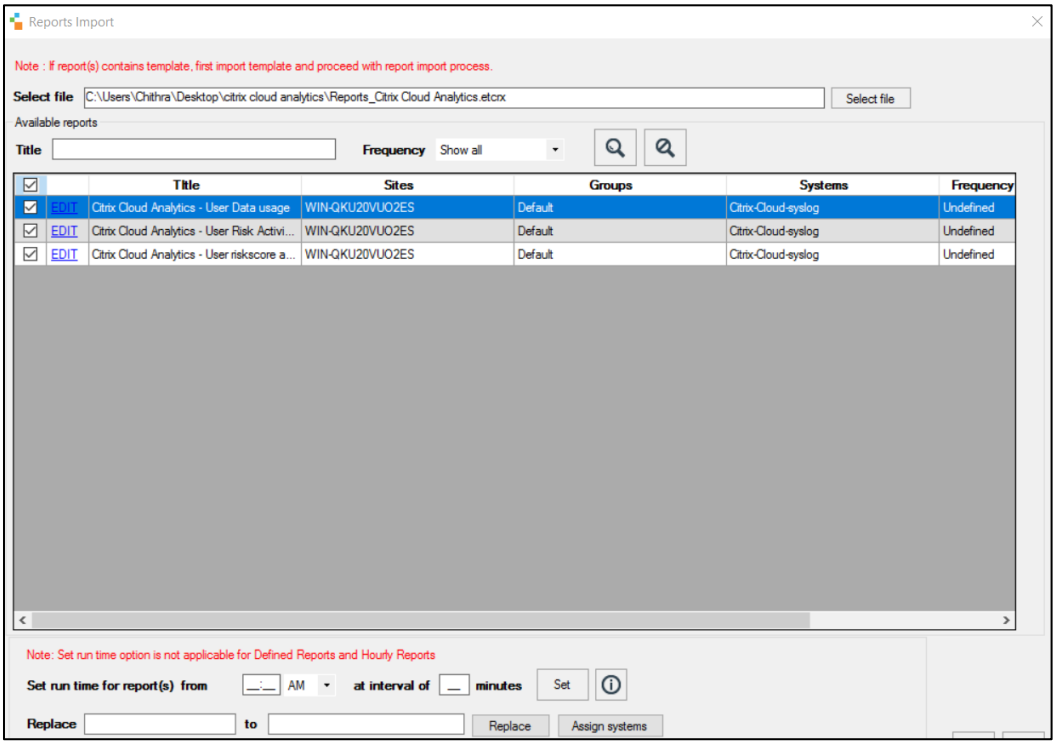


4.4 Reports

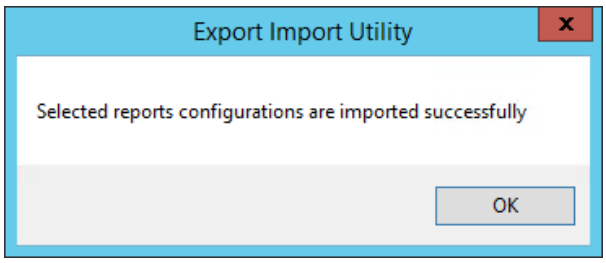
1. In the **Import** tab, choose the **Reports** option and then select **New (*. etcrx)**.



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



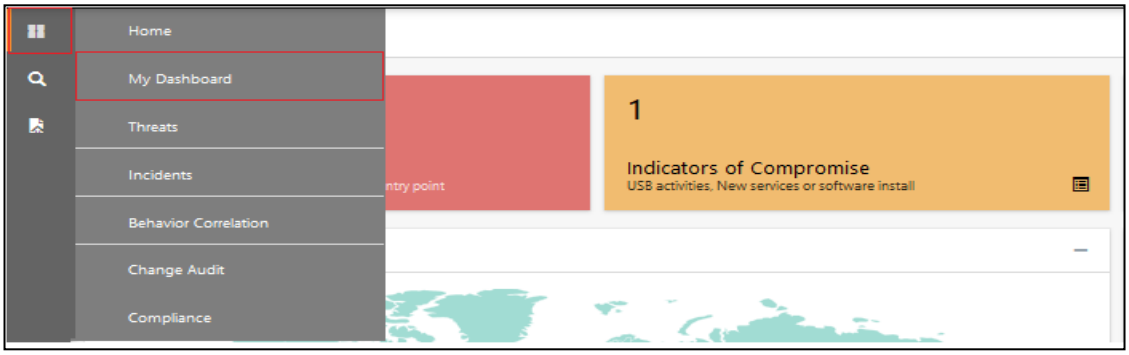
1. Click on the **Import** button to import the report. EventTracker displays a success message.



4.5 Dashboards

The following steps are specific to EventTracker 9 and later.

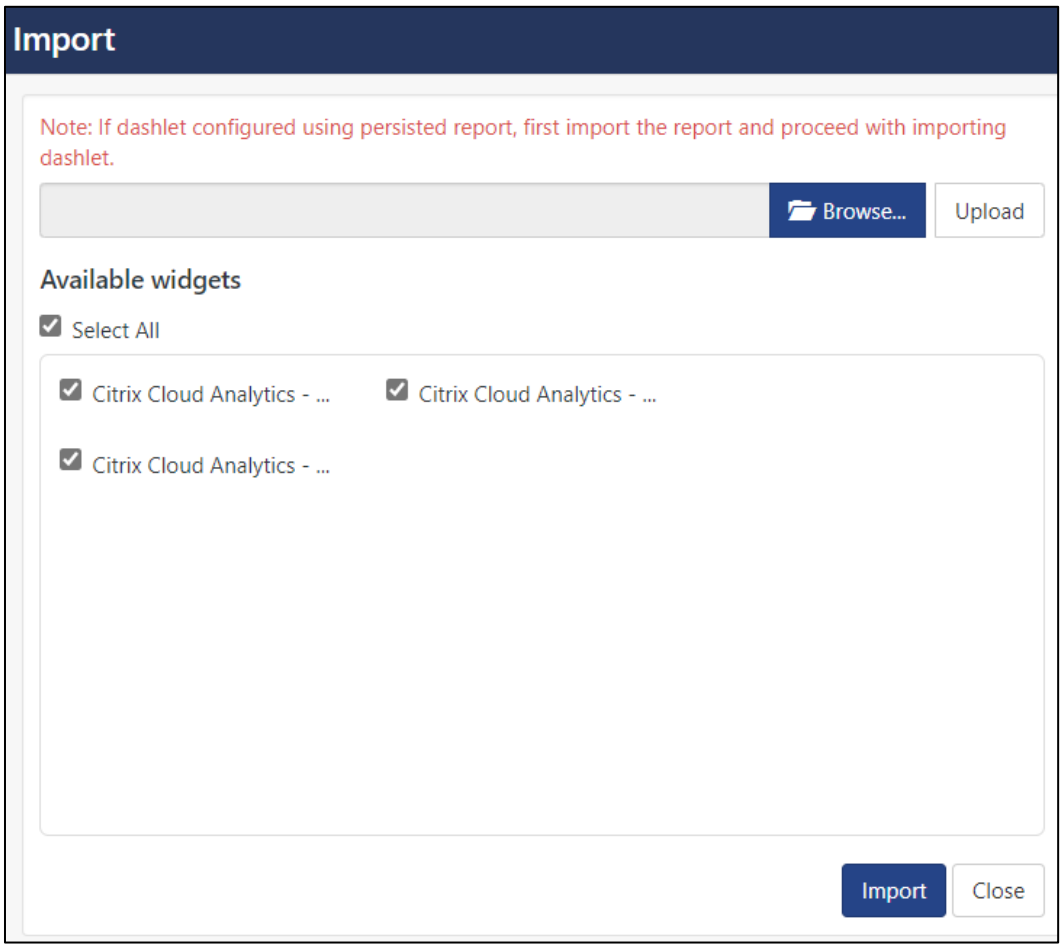
1. Open the **EventTracker** application in a browser and **Log-in**.



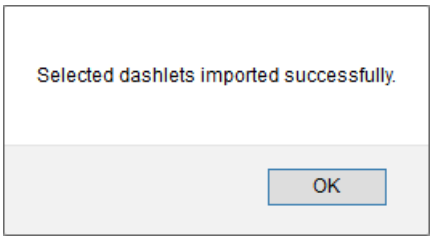
2. Navigate to **My Dashboard**.
3. On the **My Dashboard** interface, click on the **Import** button as shown below.

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

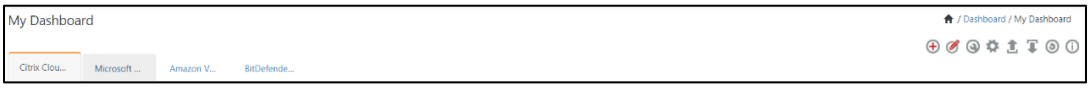
5. Click **Import** as shown below.



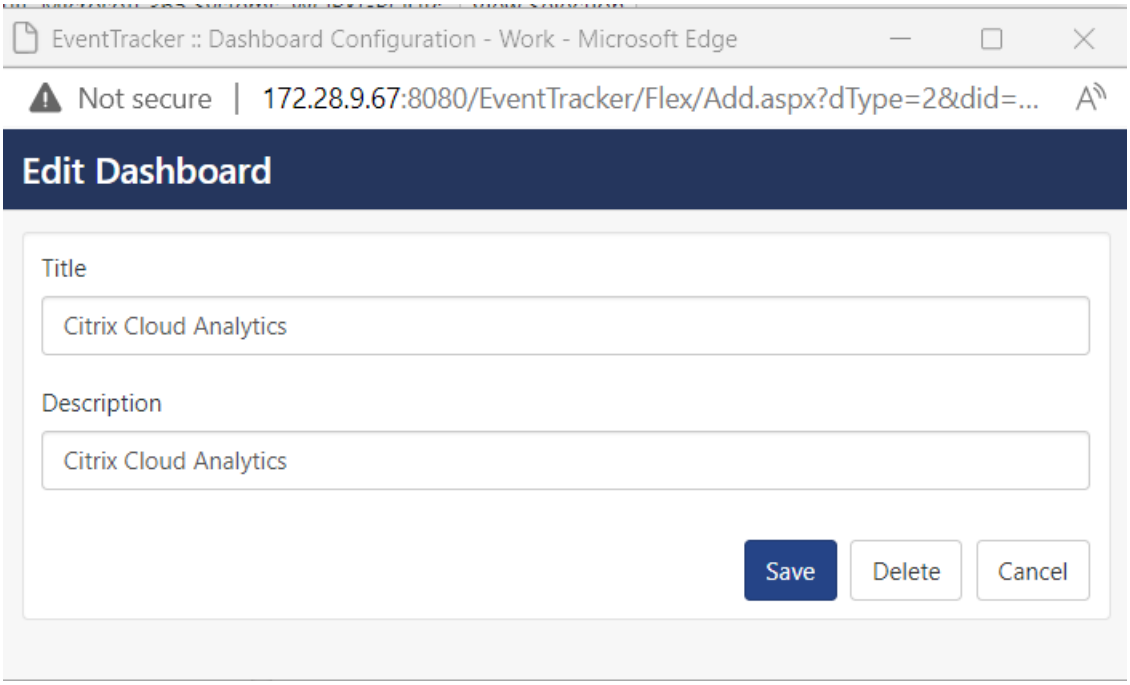
6. Import is now completed successfully.



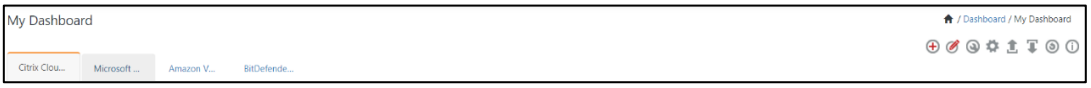
7. In the **My Dashboard** interface click on the **Add** ⊕ button to add dashboard.



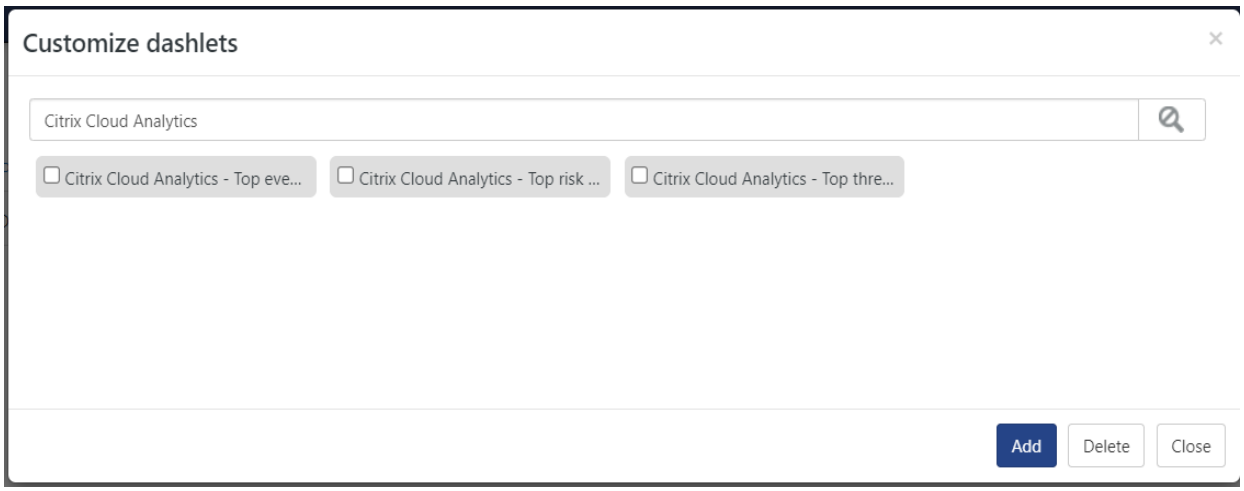
8. Choose the appropriate name for the **Title** and **Description**, and then click **Save**.



9. In the **My Dashboard** interface, click to customize dashlets.



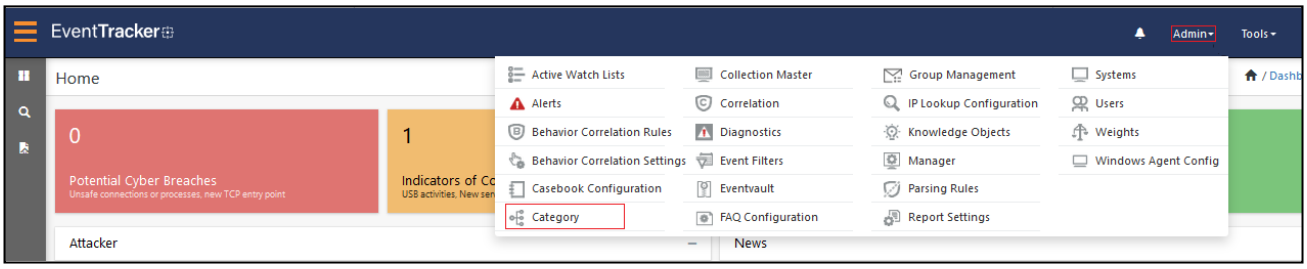
10. In the **Customize dashlets** window, select the imported dashlets and click **Add**.



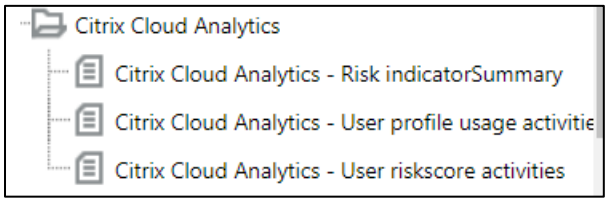
5 Verifying Citrix Cloud Analytics Knowledge Packs in EventTracker

5.1 Categories

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

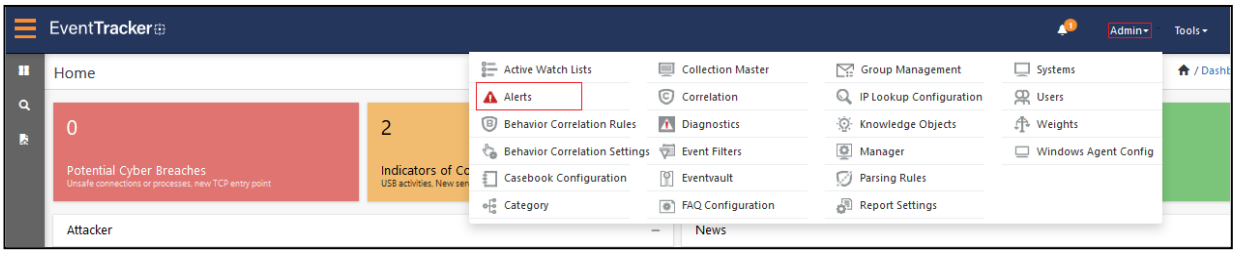


3. In the **Category** tree, scroll down and expand the **Citrix Cloud Analytics** group folder to view the imported category.



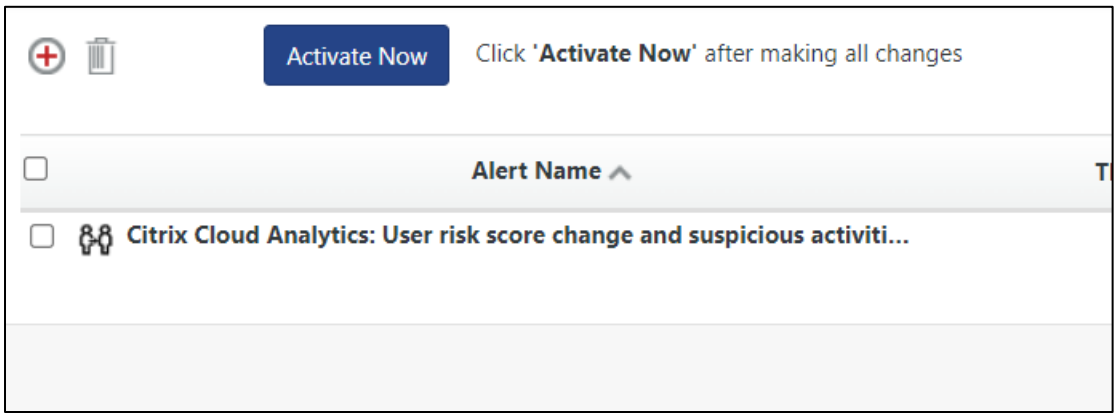
5.2 Alerts

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

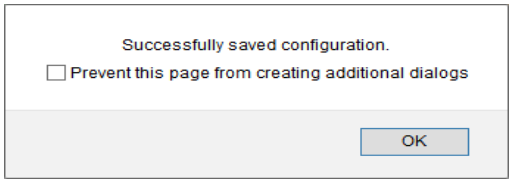


3. In the **Search** field type **Citrix Cloud Analytics**, and then click on the **Search** button.

4. The **Alerts** management page displays the imported alert.



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

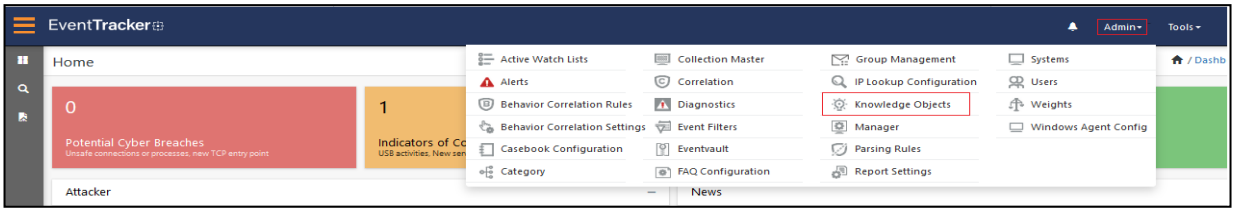


7. Click **OK**, and then click on the **Activate Now** button.

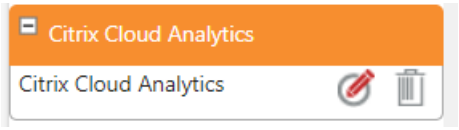
NOTE: Specify the appropriate **System** in **Alerts** configuration for better performance.

5.3 Knowledge Objects

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



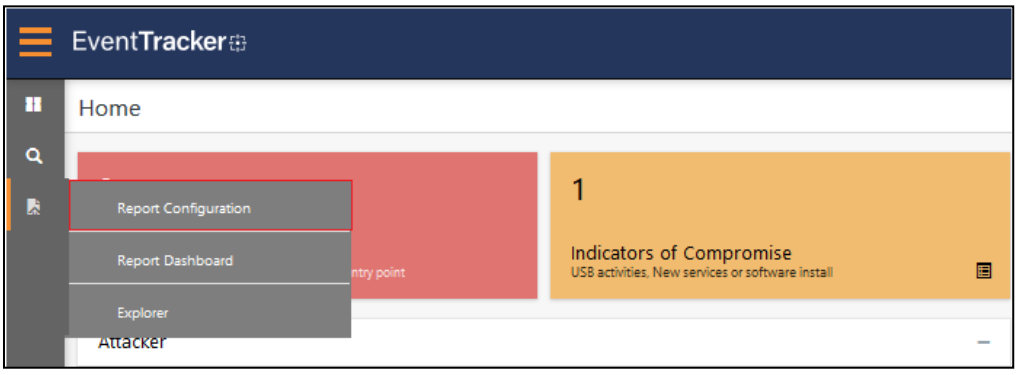
2. In the **Knowledge Object** tree, expand the **Citrix Cloud Analytics** folder to view the imported Knowledge Objects.



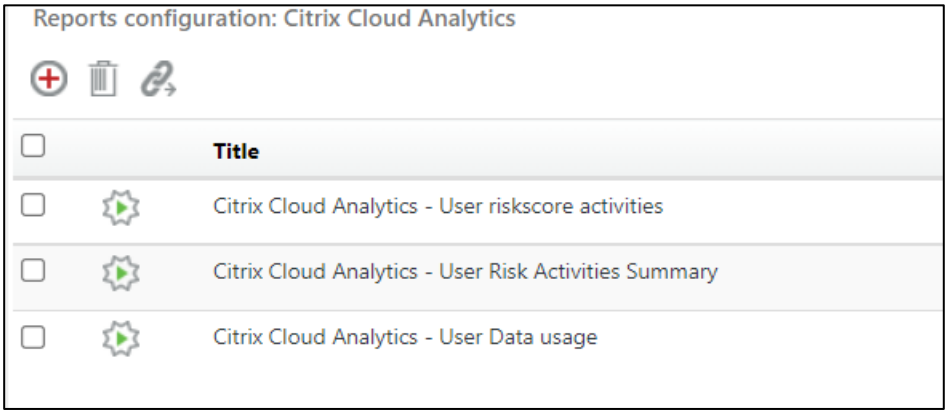
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.4 Reports

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

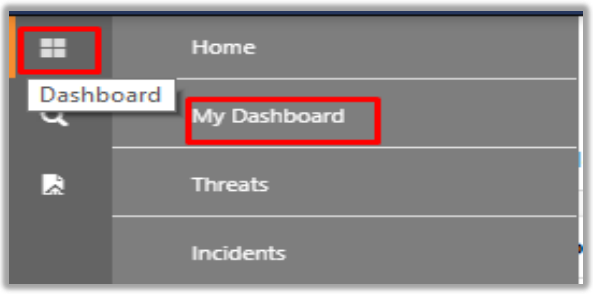


2. In the **Reports Configuration** interface, choose the **Defined** option.
3. Select the **Citrix Cloud Analytics** group folder to view the imported reports.

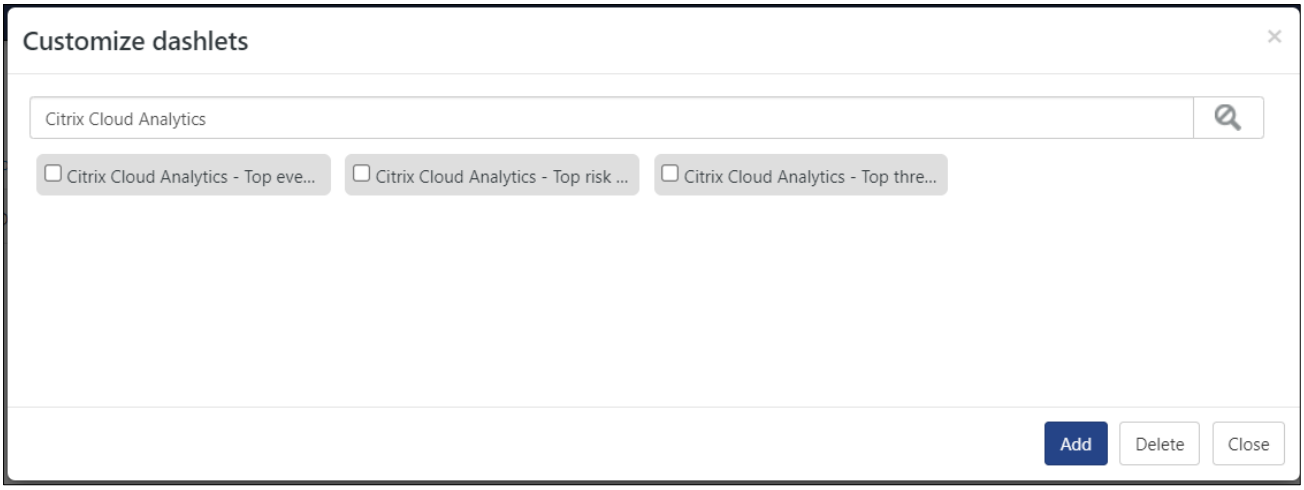


5.5 Dashboards

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



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



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