

# Integrate Bluecoat Content Analysis

EventTracker v9.x and above

## Abstract

This guide provides instructions to configure a **Bluecoat Content Analysis** to send its syslog to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v9.x or above and Bluecoat Content Analysis 1.3 or above.

## Audience

Administrators who are assigned the task to monitor Bluecoat Content Analysis events using EventTracker.

*The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.*

*EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

Abstract .....	1
Scope .....	1
Audience .....	1
Overview .....	3
Prerequisites .....	3
Integration of Bluecoat Content Analysis with EventTracker manager .....	3
Configuring Log Delivery .....	3
EventTracker Knowledge Pack .....	4
Alerts .....	4
Flex Reports .....	4
Categories .....	5
Knowledge Objects .....	5
Import Bluecoat Content Analysis knowledge pack into EventTracker .....	6
Alerts .....	7
Category .....	7
Knowledge Objects .....	9
Token Templates .....	10
Flex Reports .....	10
Dashlets .....	12
Verify Bluecoat Content Analysis knowledge pack in EventTracker .....	15
Alerts .....	15
Categories .....	16
Knowledge Objects .....	16
Token Template .....	17
Flex Reports .....	18
Sample Flex Dashboards .....	19

## Overview

Bluecoat Content Analysis is a next-generation anti-virus, malware, and spyware detection system. Content Analysis includes the features such as Malware and Antivirus scanning, Static Analysis services from Cylance, File Reputation Service, Manual File Blacklist and Whitelist, Sandbox integration with Blue Coat's Malware Analysis.

EventTracker helps to monitor events from Bluecoat Content Analysis. Its knowledge objects and flex reports will help you to analyze file scanning activity and threat detection.

## Prerequisites

- EventTracker v9.x or above should be installed.
- Bluecoat Content Analysis 1.3 or above should be configured for forwarding logs.
- Please add exception for port 514 in firewall and EventTracker Manager.

## Integration of Bluecoat Content Analysis with EventTracker manager

### Configuring Log Delivery

To configure a Bluecoat Content Analysis to forward logs to a syslog server,

1. Logon to Bluecoat appliance.
2. Navigate to **Settings > Alerts > Syslog**. Configuring options are provided below:
  - **Server:** IP address or hostname of EventTracker Manager
  - **Port:** 514
  - **Protocol:** UDP
  - **Facility:** Information
3. Click **Save Changes**.

## EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Bluecoat Content Analysis.

### Alerts

- **Bluecoat Content Analysis: Threat detected** – This alert generates when threats are detected while scanning.
- **Bluecoat Content Analysis: File blocked** – This alert generates when the files are blocked by inbuilt anti-virus.

### Flex Reports

- **Bluecoat Content Analysis - File activity** – This report gives the information about file scan result, reputation and the action taken.

LogTime	Computer	Machine IP Address	Machine Name	Server IP Address	Client IP Address	Action	Reason	URL	Antivirus Vendor	Pattern File Version	Scan Engine Version
05/08/2018 05:51:02 PM	BLUECOAT CAS	10.226.72.29	Etmachine-cas1	100.11.56.44	10.11.12.22	File has been dropped.	File decompression/decode error	http://1b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/521b2fcc-5ebb-4fac-b349-a561b78eb9d4?P1=152525595	Symantec	20180501.016. (Pattern date: 2018/05/01)	2.0.1.4
05/08/2018 05:51:02 PM	BLUECOAT CAS	10.226.72.29	Etmachine-cas1	100.11.56.44	10.11.12.22	File has been dropped.	Maximum file size exceeded	http://officecdn.microsoft.com.edgesuite.net/sg/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.9226.2114/stream.x86.x-none.dat	Symantec	20180501.016. (Pattern date: 2018/05/01)	2.0.1.4
05/08/2018 05:51:02 PM	BLUECOAT CAS	10.226.72.29	Etmachine-cas1	100.11.56.44	10.11.12.22	File has been dropped.	File decompression/decode error	http://1b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/521b2fcc-5ebb-4fac-b349-a561b78eb9d4?P1=152525595	Symantec	20180501.016. (Pattern date: 2018/05/01)	2.0.1.4
05/08/2018 05:51:02 PM	BLUECOAT CAS	10.226.72.29	Etmachine-cas1	100.11.56.44	10.11.12.22	File has been dropped.	File reputation service identified a "known bad" file	hxxp://download.winzip.com/gi/gad/winzip22.exe	Symantec	20180501.006. (Pattern date: 2018/05/01)	2.0.1.4

Figure 1

### Sample logs:

LogTime	Computer	Machine IP Address	Machine Name	Server IP Address	Client IP Address	Action	Reason	URL	Antivirus Vendor	Pattern File Version	Scan Engine Version
May 08 05:51:04 PM	BLUECOAT CAS	10.226.72.29	Etmachine-cas1	100.11.56.44	10.11.12.22	File has been dropped.	Maximum file size exceeded.	http://www.symantec.com	Pre AV call, no vendor data	Unknown	Unknown

```

event_log_type      +- Application
event_type          +- Information
event_id            +- 3333
event_source        +- syslog
event_user_domain   +- N/A
event_computer      +- Bluecoat CAS
event_user_name     +- N/A
event_description    May 01 07:01:06 vxdc-cas1 1 2018-05-01T11:01:06.747Z avservice 4381 - Maximum file size exceeded., File has been dropped., 2018-05-01 07:01:06 (EDT), Hardware serial number: 0216320083, CAS (Version 2.3.1.1(213733)) - http://www.symantec.com, Antivirus Vendor: Pre AV call, no vendor data, Scan Engine Version: Unknown, Pattern File Version: Unknown (Pattern date: Unknown), Machine name: cas, Machine IP address: 10.34.20.32, Server: 6.61.16 122, Client: Unknown., URL: http://officecdn.microsoft.com.edgesuite.net/pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.9226.2114/stream.x86.x-none.dat
  
```

Figure 2

- **Bluecoat Content Analysis- Threat detected** – This report gives the information about threats detected while scanning.

LogTime	Computer	Serial Number	Machine IP Address	Machine Name	Server IP Address	Client IP Address	Antivirus Vendor	Pattern File Version	Threat Detail	URL
05/08/2018 05:51:04 PM	BLUECOAT CAS	0515320030	10.34.8.32	Etmachine-cas1	10.11.12.22	100.11.56.44	Kaspersky Labs	180504 (Pattern date: 2018/05/04)	"Suspicious:Trojan.Script.Miner.gen" found!	hxxp://www.umbertospizzaria.com/
05/08/2018 05:51:04 PM	BLUECOAT CAS	0515320030	10.34.8.32	Etmachine-cas1	10.11.12.22	100.11.56.44	Kaspersky Labs	180504 (Pattern date: 2018/05/04)	"Suspicious:Trojan.Script.Miner.gen" found!	hxxp://umbertospizzaria.com/
05/08/2018 05:51:04 PM	BLUECOAT CAS	0515320030	10.34.8.32	Etmachine-cas1	10.11.12.22	100.11.56.44	Kaspersky Labs	180504 (Pattern date: 2018/05/04)	"Suspicious:Trojan.Script.Miner.gen" found!	hxxp://umbertospizzaria.com/
05/08/2018 05:51:04 PM	BLUECOAT CAS	0515320030	10.34.8.32	Etmachine-cas1	10.11.12.22	100.11.56.44	Kaspersky Labs	180504 (Pattern date: 2018/05/04)	"Suspicious:Trojan.Script.Miner.gen" found!	hxxp://umbertospizzaria.com/

Figure 3

### Sample logs:

Time	Description
May 08 05:51:04 PM	May 04 10:50:30 iodc-cas1 1 2018-05-04T14:50:30.578Z 10.34.8.32 avservice 10890 - 2018-05-04 14:50:30 (UTC), Hardware serial number: 0515320030, C...
<i>event_log_type</i>	+ Application
<i>event_type</i>	+ Information
<i>event_id</i>	+ 3333
<i>event_source</i>	+ syslog
<i>event_user_domain</i>	+ N/A
<i>event_computer</i>	+ Bluecoat CAS
<i>event_user_name</i>	+ N/A
<i>event_description</i>	May 04 10:50:30 iodc-cas1 1 2018-05-04T14:50:30.578Z 10.34.8.32 avservice 10890 - 2018-05-04 14:50:30 (UTC), Hardware serial number: 0515320030, C AS (Version 2.3.1.1(213733)) - http://www.symantec.com, Antivirus Vendor: Kaspersky Labs, Scan Engine Version: 8.2.5.17, Pattern File Version: 180504 (Pattern date: 2018/05/04), Machine name: iodc-cas1, Machine IP address: 10.34.8.32, Server: 107.180.40.34, Client: 10.226.77.186, Virus/PUS: ""Suspicious:Trojan.Script.Miner.gen"" found!, URL: hxxp://umbertospizzaria.com/

Figure 4

### Categories

- **Bluecoat Content Analysis: File Activity** - This category provides information related to file scan result, reputation and the action taken.
- **Bluecoat Content Analysis: Threat Detected** – This category provides information related to the threats detected while scanning.

### Knowledge Objects

- **Bluecoat Content Analysis File Activity** – This knowledge object will help us to analyze logs related to file scan result, reputation and the action taken.
- **Bluecoat Content Analysis Threat Detected** – This knowledge object will help us to analyze logs related to the threats detected while scanning.

# Import Bluecoat Content Analysis knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Alerts
- Categories
- Knowledge Objects
- Token Template
- Flex Reports
- Dash lets

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

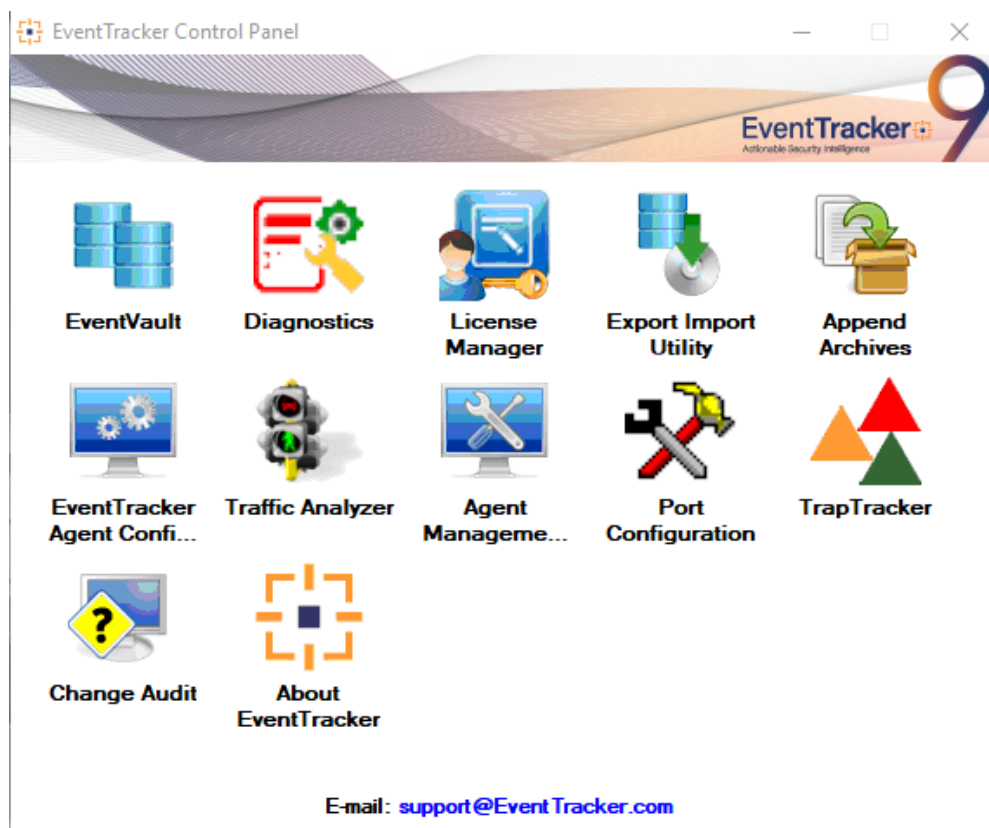


Figure 5

3. Click the **Import** tab.

## Alerts

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

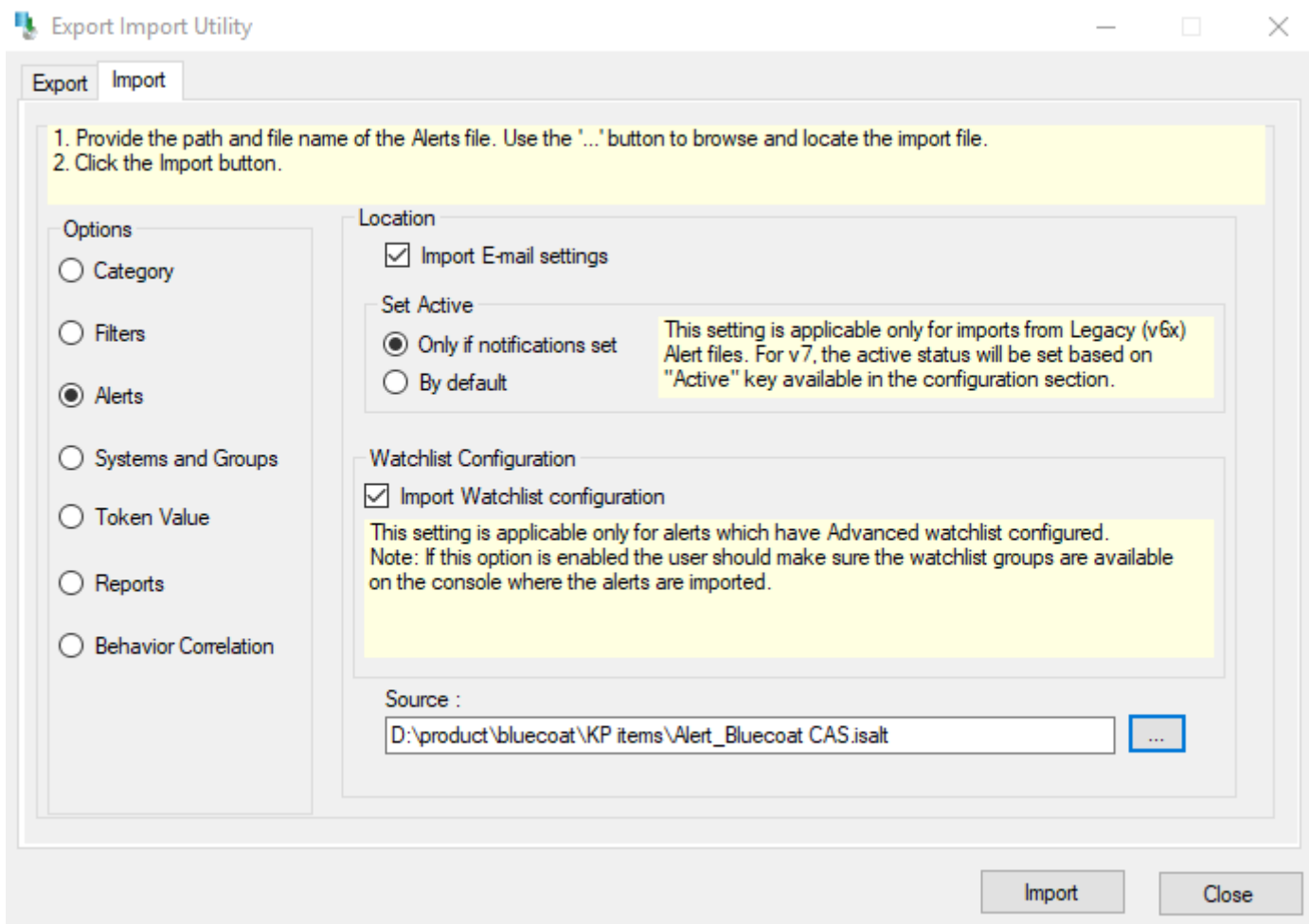


Figure 6

2. Locate **Alert\_Bluecoat CAS. Isalt** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

## Category

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



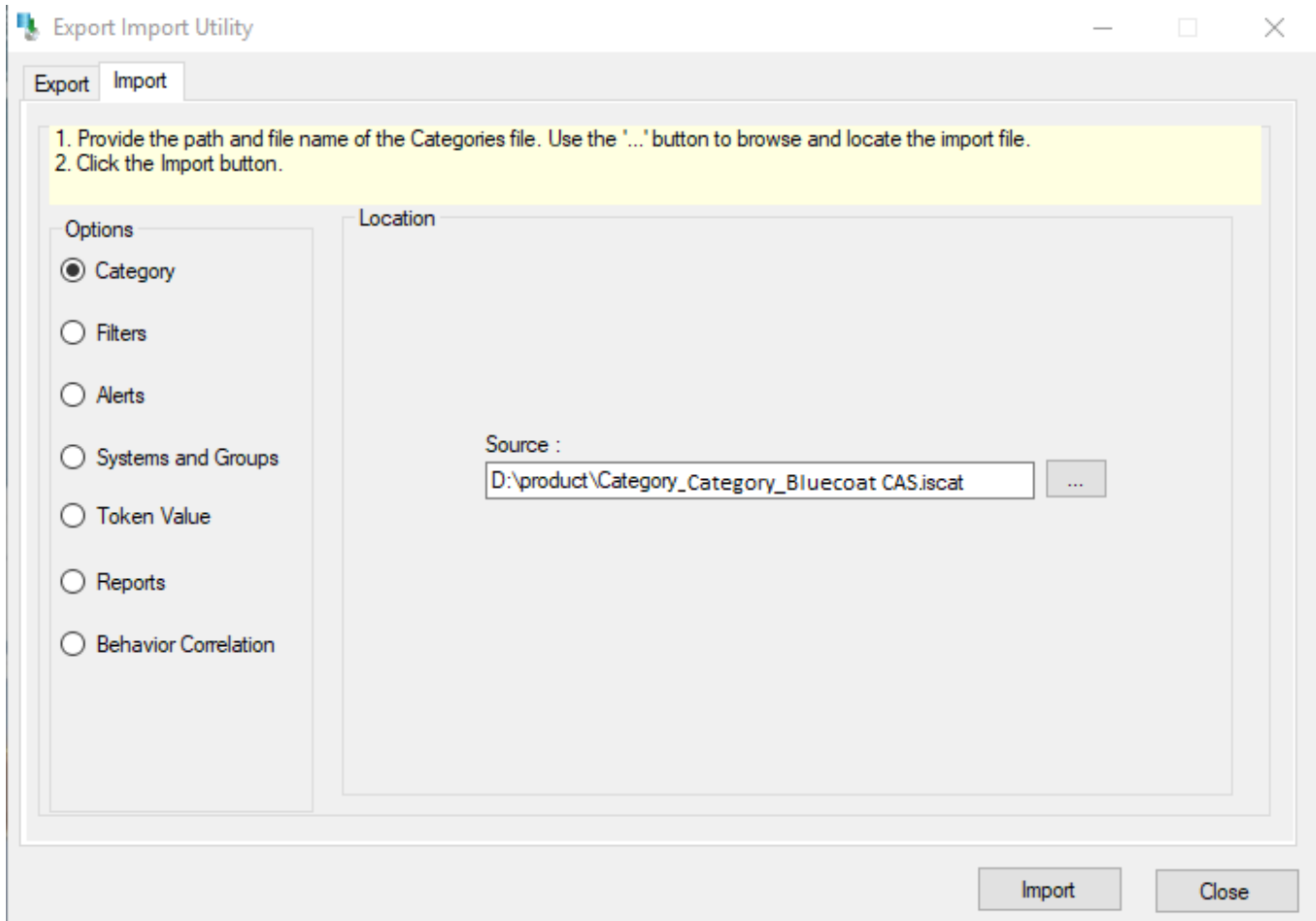


Figure 7

2. Locate **Category\_Bluecoat CAS.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

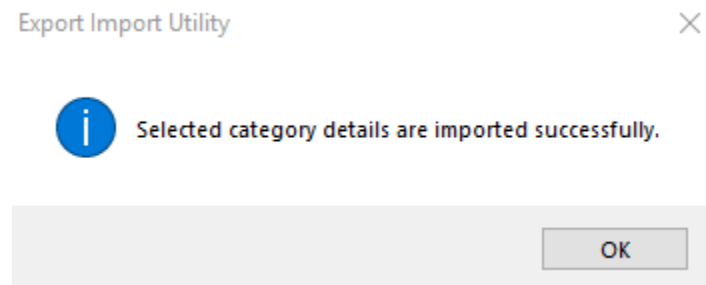


Figure 8

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

## Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named **KO\_Bluecoat CAS.etko**.

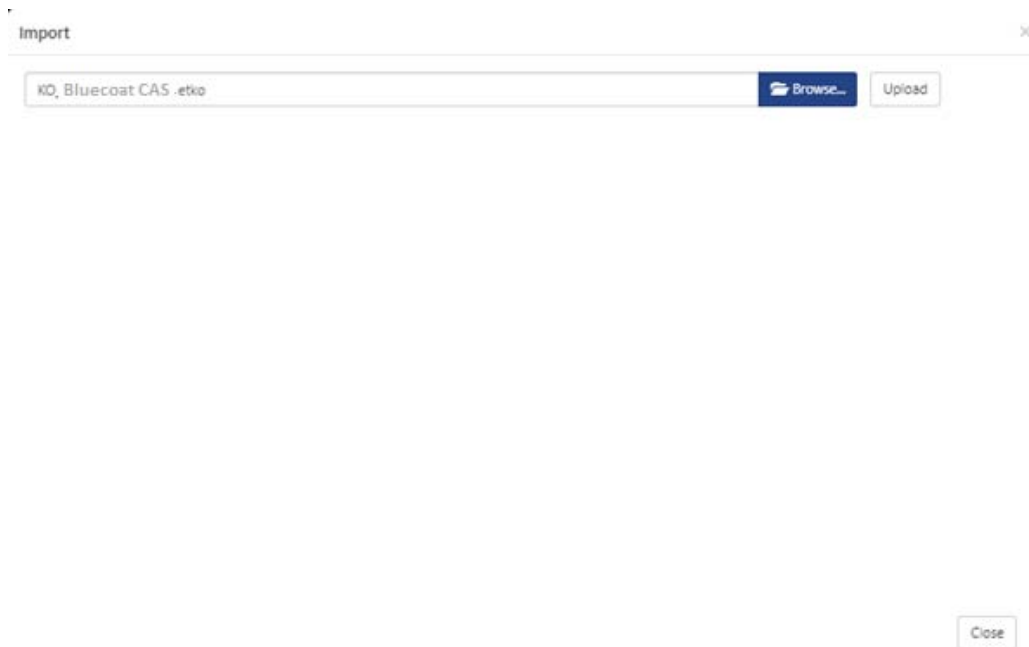


Figure 9

3. Now select all the check box and then click on **'Import'** option.

<input checked="" type="checkbox"/>	Object name	Applies to	Group name
<input checked="" type="checkbox"/>	Bluecoat Content Analysis File Activity	Bluecoat Content Analysis 1.3.x	Bluecoat Content Analysis
<input checked="" type="checkbox"/>	Bluecoat Content Analysis Threat Detected	Bluecoat Content Analysis 1.3.x	Bluecoat Content Analysis

Figure 10

4. Knowledge objects are now imported successfully.

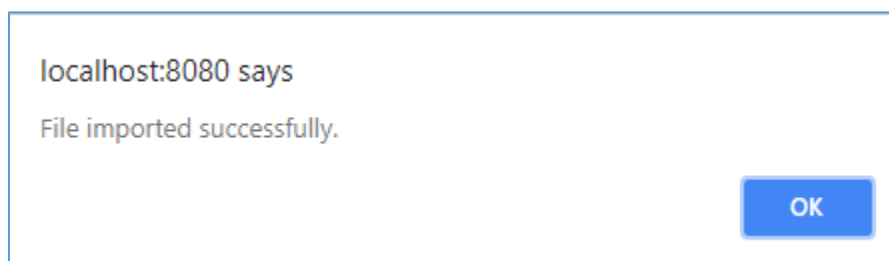


Figure 11

## Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.

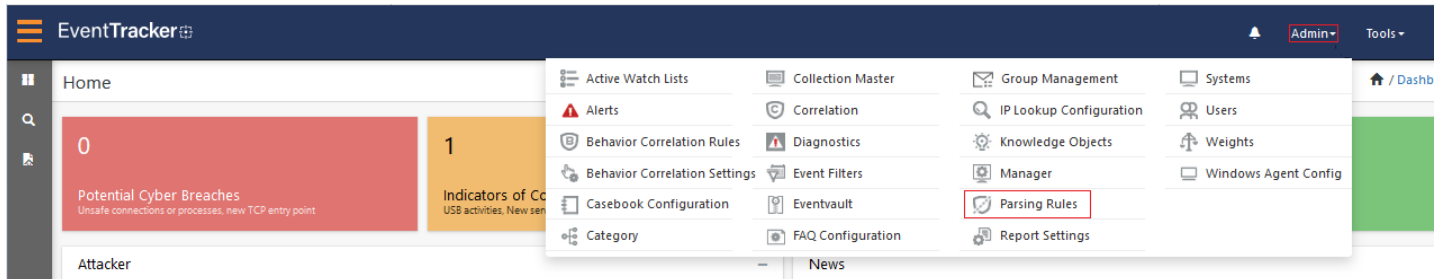



Figure 12

2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file named **token\_Bluecoat CAS.ettid**.

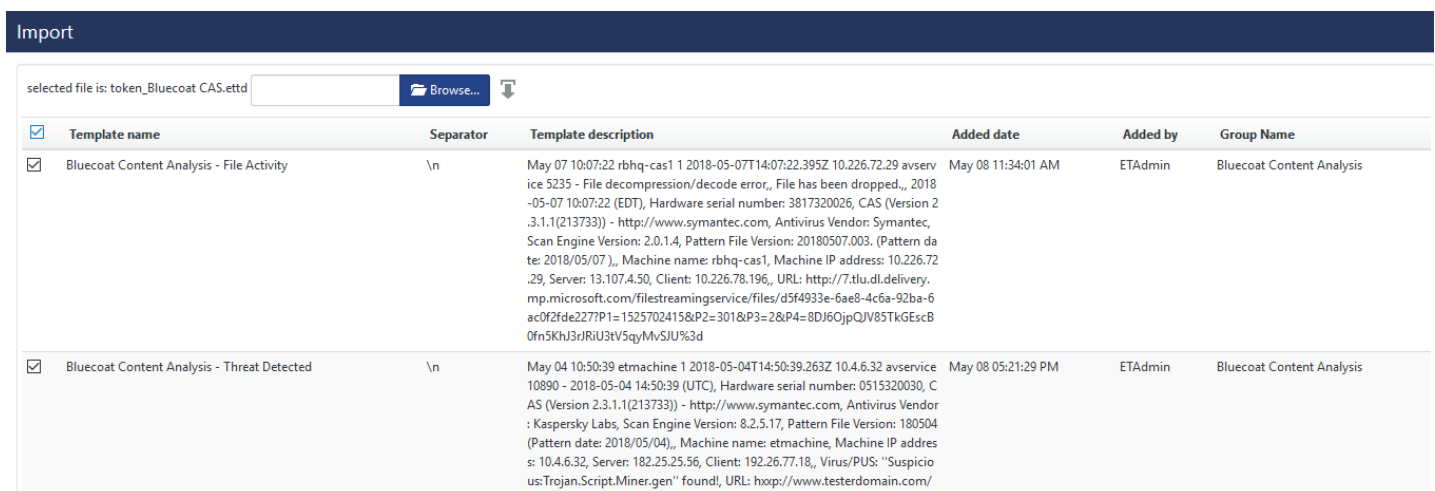



Figure 13

4. Now select all the check box and then click on  Import option.

## Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new(etcrx) from the option.

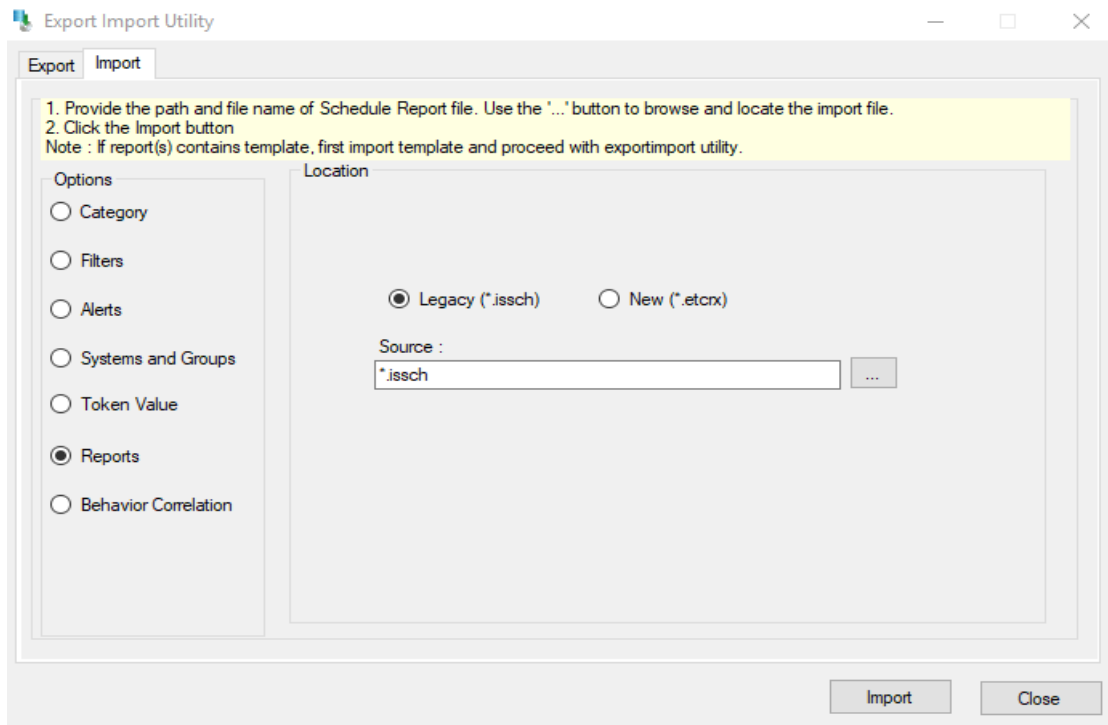


Figure 14

2. Locate the file named **Reports\_Bluecoat CAS.etcrx**, and select all the check box.

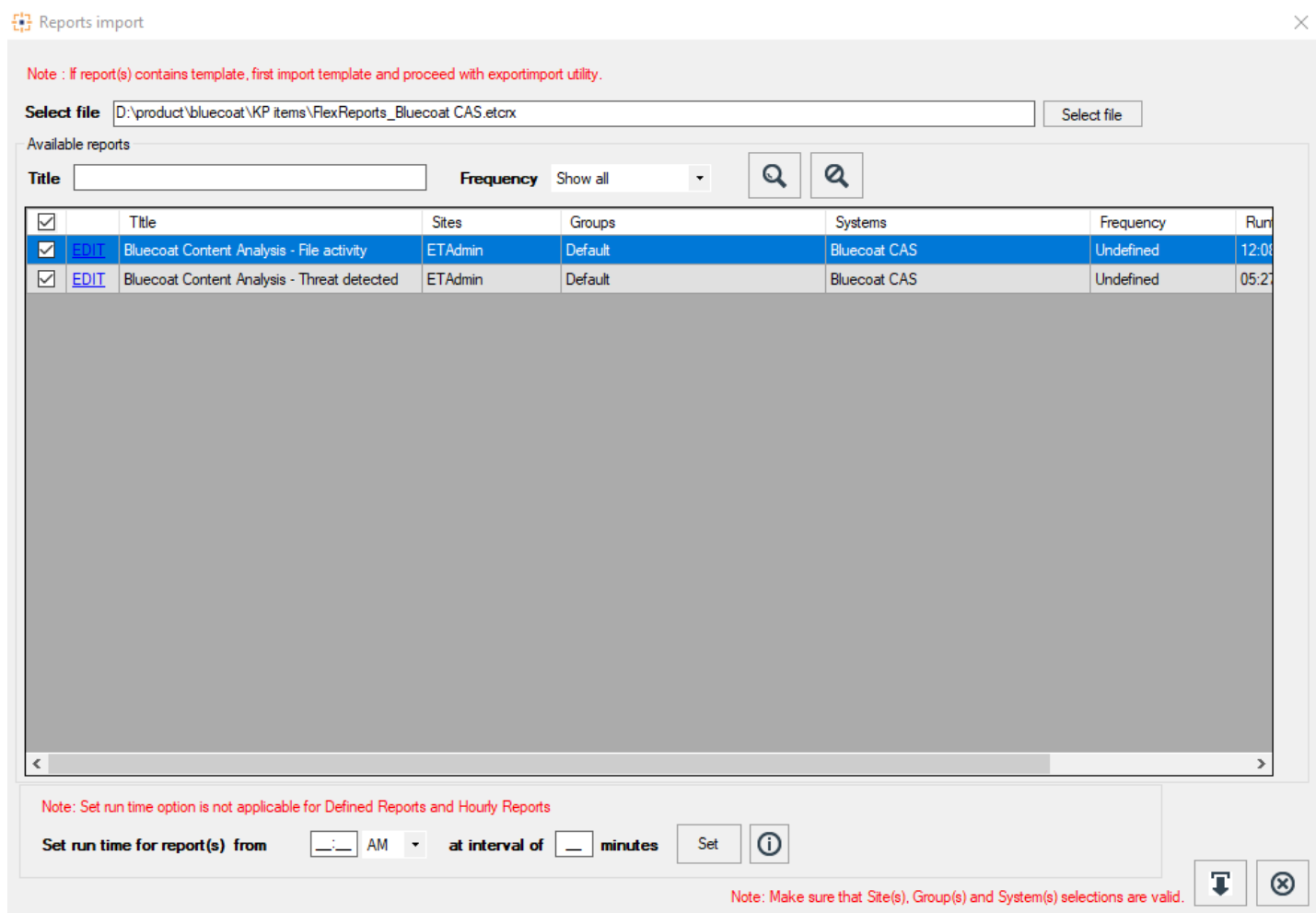


Figure 15

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

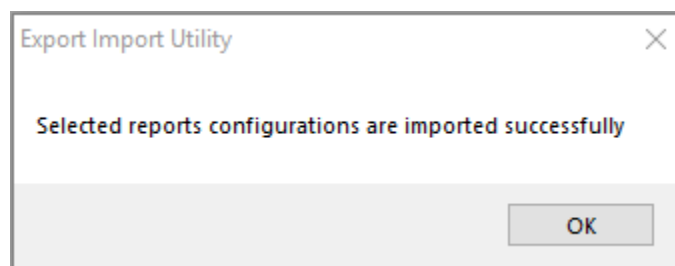


Figure 16

## Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

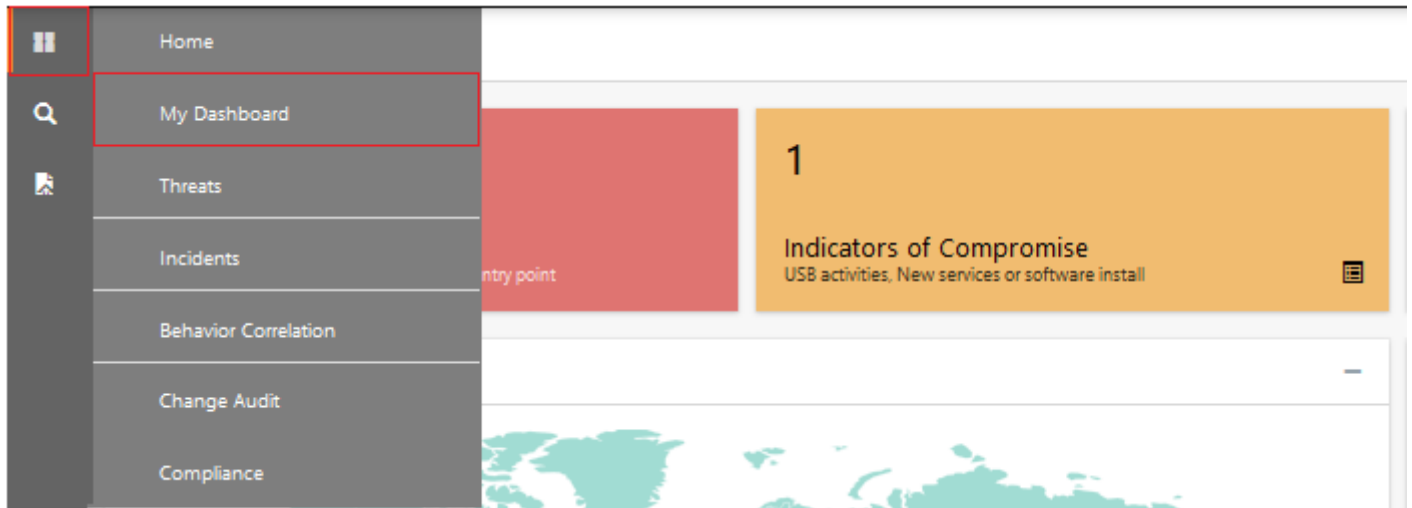



Figure 17

2. Navigate to **My Dashboard**
3. Click on import configuration  icon on the top right corner.
4. In the popup window browse the file named **Dashboard\_Bluecoat CAS.etwd**.

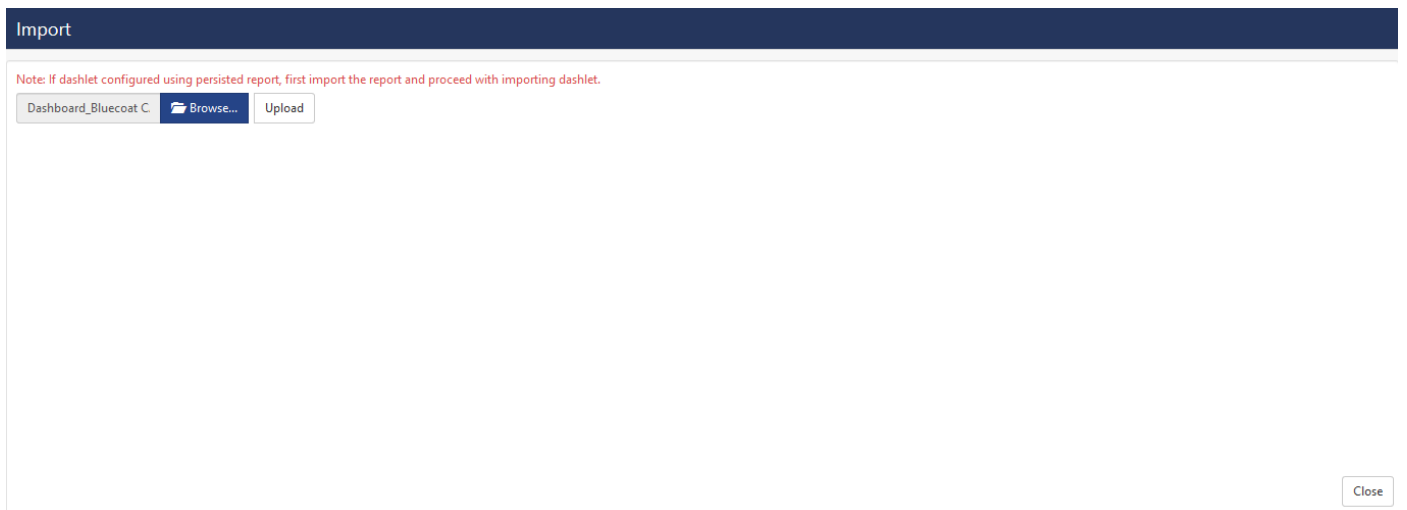


Figure 18

5. Now select all the check box and then click on **Import** option.

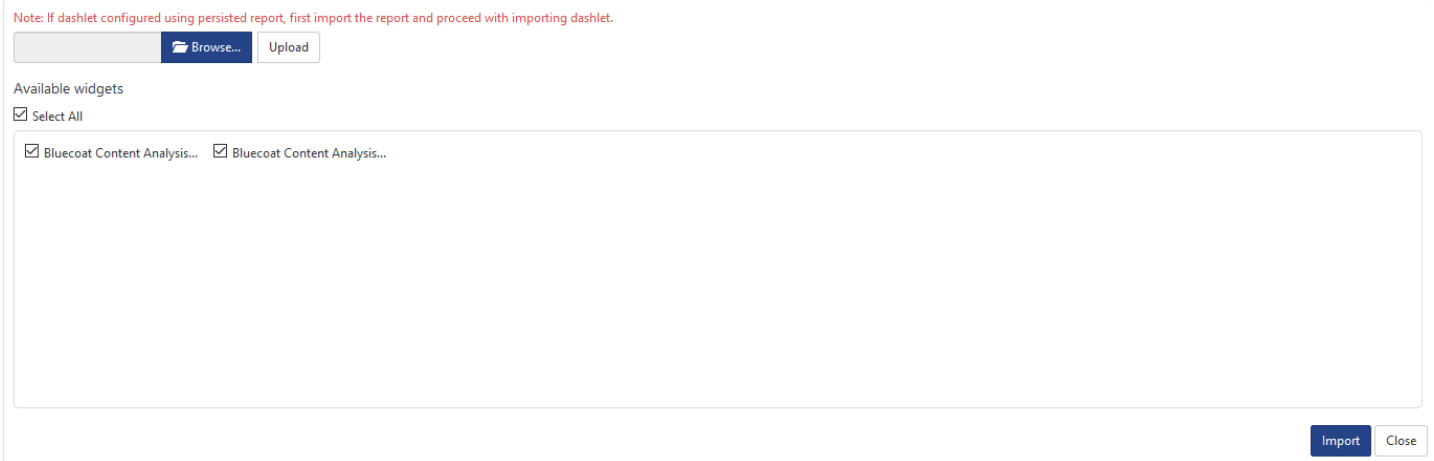



Figure 19

6. Click 'customize'  to locate and choose created dashlet.

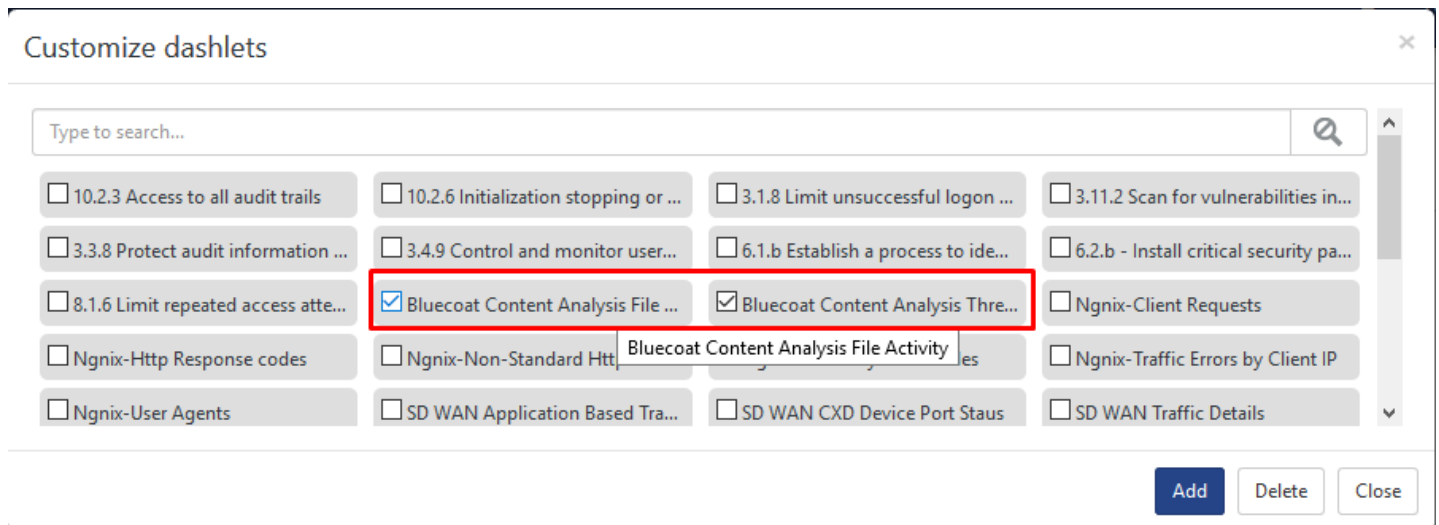


Figure 20

7. Click **Add** to add dashlet to dashboard.

# Verify Bluecoat Content Analysis knowledge pack in EventTracker

## Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.

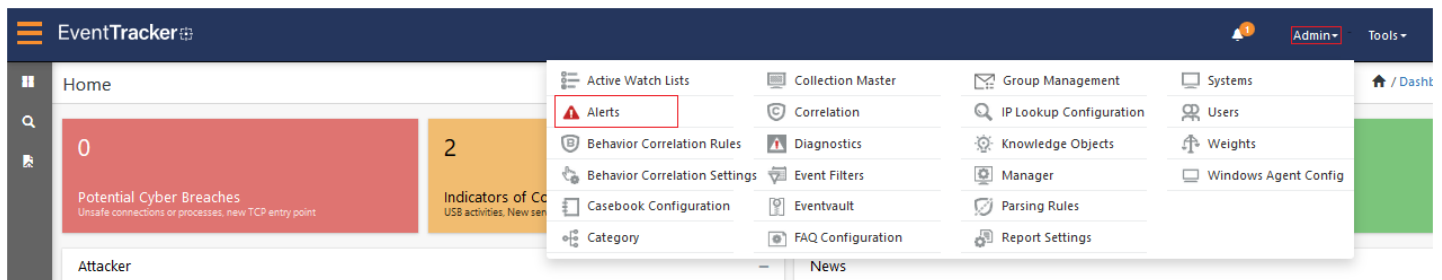


Figure 21

3. In the **Search** box, type **Bluecoat Content Analysis**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alert Name ^	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
<input type="checkbox"/> Bluecoat Content Analysis: File Blocked	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bluecoat Content Analysis 1.3x or above
<input type="checkbox"/> Bluecoat Content Analysis: Threat Detected	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bluecoat Content Analysis 1.3x or above

Figure 22

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.



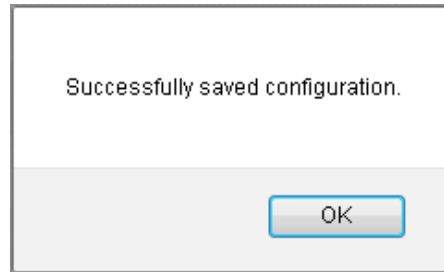


Figure 23

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

**NOTE:** Please specify appropriate **systems** in **alert configuration** for better performance.

## Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand Bluecoat Content Analysis group folder to view the imported categories.

Category

Category Tree Search

- All Categories
  - \*All error events
  - \*All information events
  - \*All warning events
  - \*Security: All security events
  - Bluecoat Content Analysis
    - Bluecoat Content Analysis File Activity
    - Bluecoat Content Analysis Threat Detect
  - Change Audit
  - Cisco ASA Firewall
  - EventTracker
  - Fortigate Firewall
  - Nginx Web Server
  - NIST 800-171
  - PCI DSS
  - Riverbed SteelHead
  - SDWAN

Category Details

Parent Group: Bluecoat Content Analysis

Event Category Name: Bluecoat Content Analysis File Activity

Description: [Empty text area]

Applies to: Bluecoat Content Analysis 1.3x or abo Category version: [Empty text area]

Show In:  Operations  Compliance  Security

Event Rule

Log Type	Event Type	Event Category Id	Source	User	Match in Description	Description Exception	Lucene Query
0	0	0	syslog		Hardware\sserial\snumber:.*?Machine\sname:.*? Machine\sIP\saddress:.*?Server:.*?Client:.*?+.*?URL:		log_source:"Bluecoat Content Analysis File Activity"

Save Cancel

Figure 24

## Knowledge Objects

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

- In the **Knowledge Object** tree, expand **Bluecoat Content Analysis** group folder to view the imported Knowledge objects.

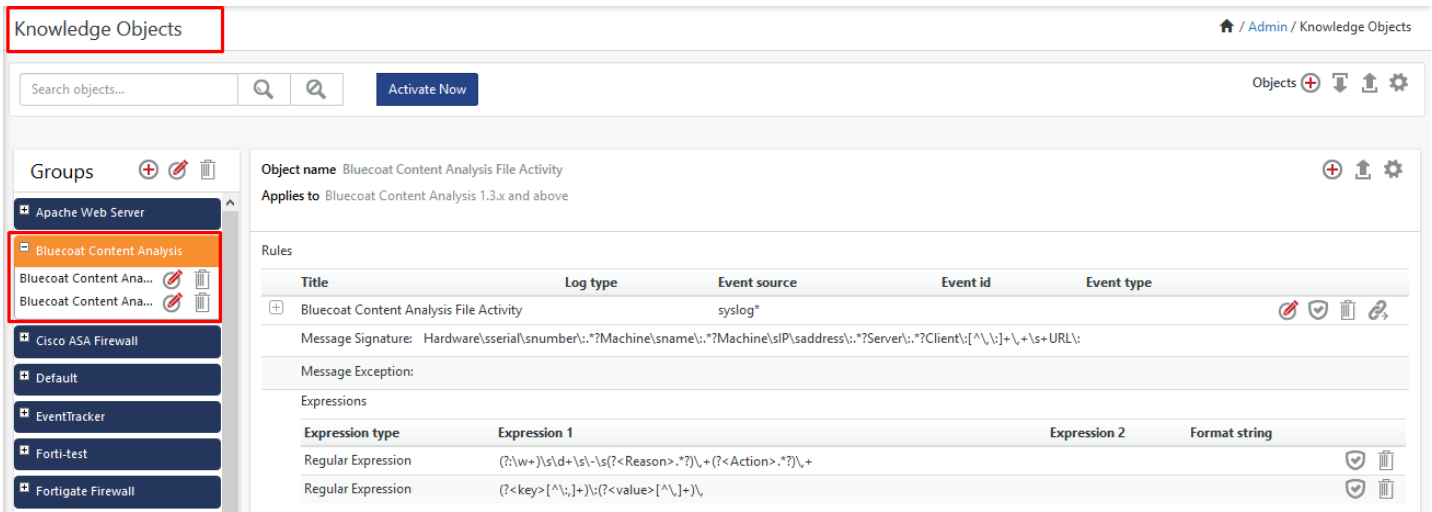


Figure 25

## Token Template

- In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

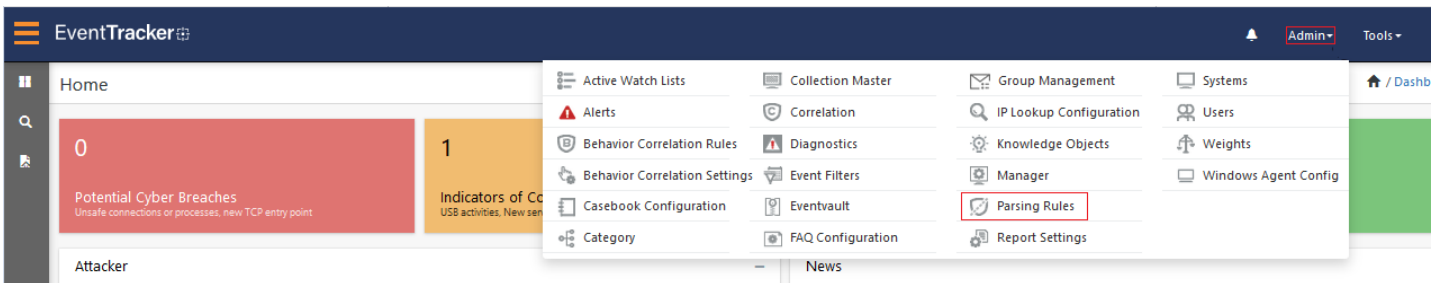


Figure 26

- On **Template** tab, click on the **Bluecoat Content Analysis** group folder to view the imported Templates.

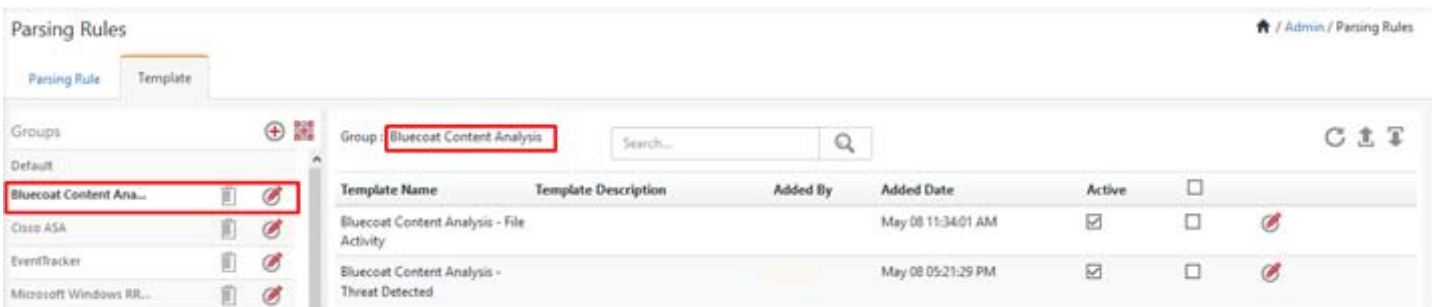


Figure 27

## Flex Reports

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

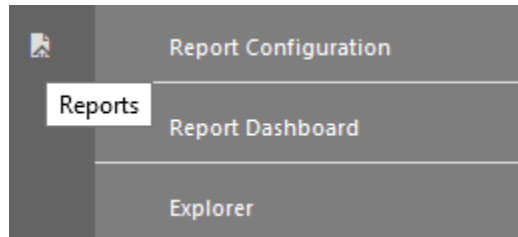


Figure 28

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Bluecoat Content Analysis** group folder to view the imported Bluecoat Content Analysis reports.

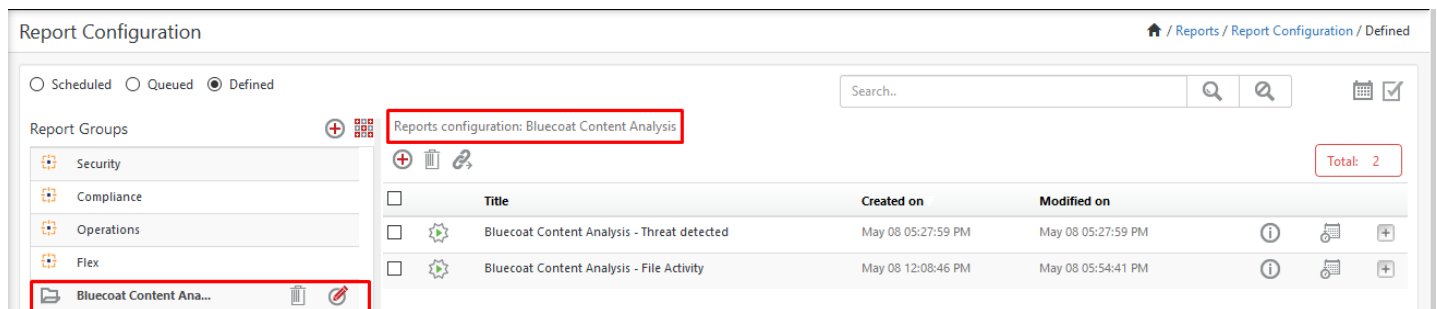


Figure 29

## Sample Flex Dashboards

Title: Bluecoat Content Analysis File Activity

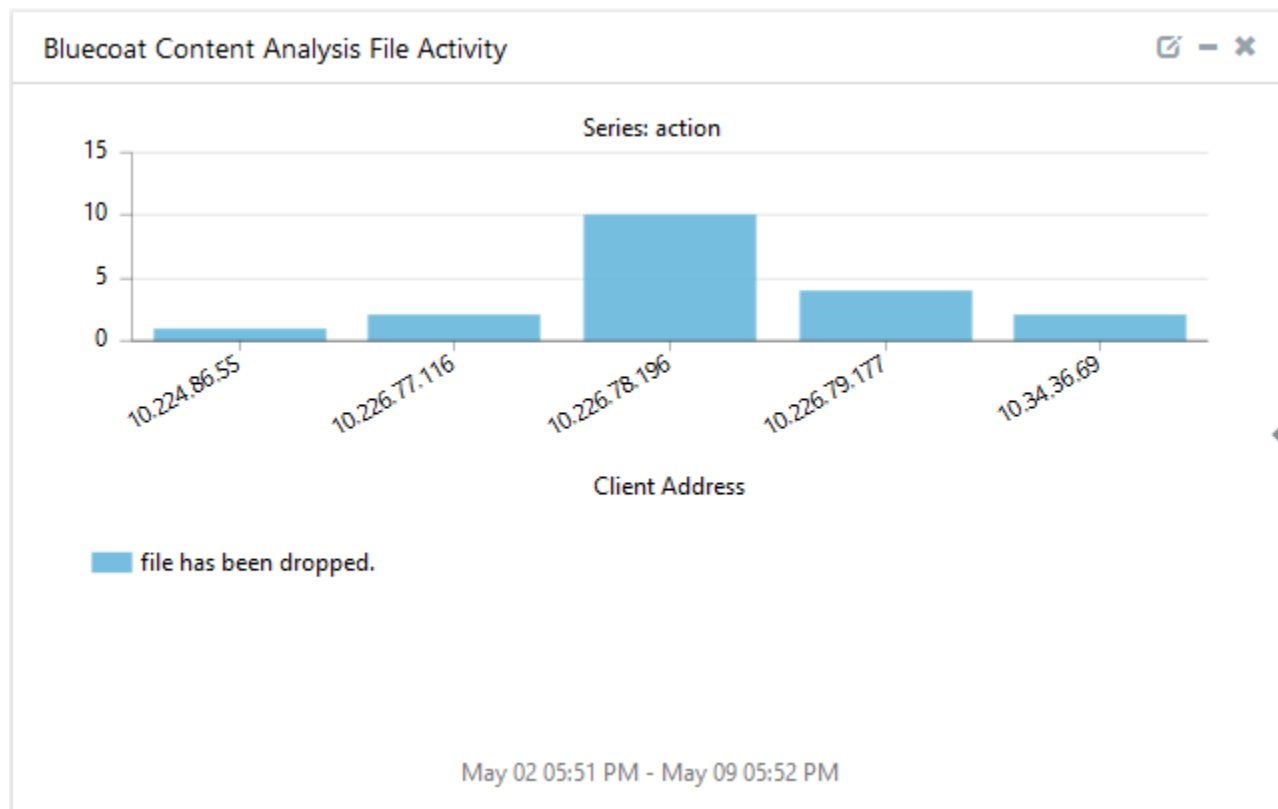


Figure 30

**Title: Bluecoat Content Analysis Threat Detected**

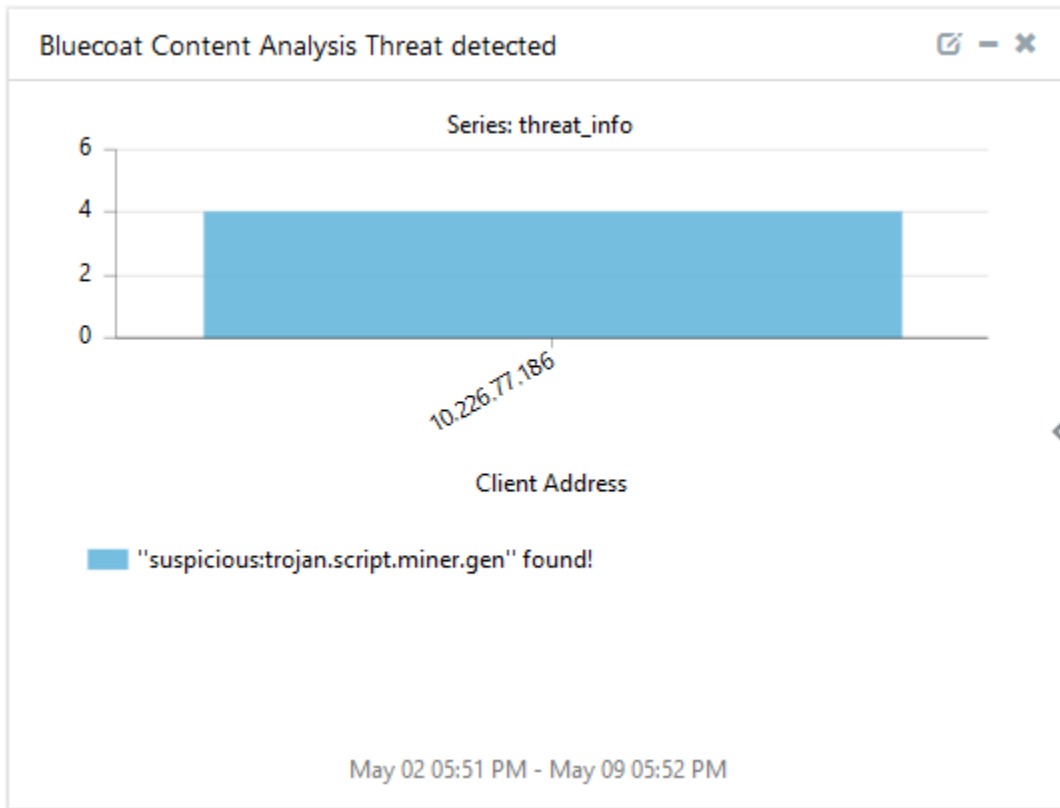


Figure 31