# EventTracker:

Actionable Security Intelligence

# Integrate Bluecoat Content Analysis

# EventTracker v9.x and above

Publication Date: June 8, 2018

### 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 Configuring Log Delivery	3 3
EventTracker Knowledge Pack Alerts	4 4
Flex Reports	4
Categories	5
Knowledge Objects	5
Import Bluecoat Content Analysis knowledge pack into EventTracker Alerts	6 7
Category	7
Knowledge Objects	9
Token Templates	10
Flex Reports	10
Dashlets	12
Verify Bluecoat Content Analysis knowledge pack in EventTracker Alerts	15 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 antivirus.

### **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.micro soft.com/filestreamingservice/fi les/521b2fcc-56bb-4fac-b349- a561b76eb9d4?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.micro soft.com/filestreamingservice/fi les/521b2fcc-56bb-4fac-b349- a561b76eb9d4?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/gl /gad/winzip22.exe	Symantec	20180501.006. (Pattern date: 2018/05/01)	2.0.1.4

Figure 1

#### Sample logs:

- May 08 05:51:04 PM	May 01 07:01:06 vxdc-cas1 1 2018-05-01T11:01:06.747Z 10:34.20	0.32 avservice 4381 - Maximum file size exceeded, File has been dropped, 2018-05-01 0
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 0
	7:01:06 (EDT), Hardware serial number: 0216320083, CAS (Versio	n 2.3.1.1(213733)) - http://www.symantec.com, Antivirus Vendor: Pre AV call, no vendor d
	ata, Scan Engine Version: Unknown, Pattern File Version: Unknow	vn (Pattern date: Unknown),, Machine name: cas, Machine IP address: 10.34.20.32, Se
	rver: 6.61.16 122, Client: Unknown, URL: http://officecdn.micro	osoft.com.edgesuite.net/pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.92

Figure 2

26.2114/stream.x86.x-none.dat



• 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.co m/
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
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 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 (Pat
	tern 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:Tr
	ojan.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.

Export Import Utility			-		$\times$
Export Import					
1. Provide the path and file nar 2. Click the Import button.	me of the Alerts file. Use the '' butt	on to browse and locate the import file.			
Options	Location				
<ul> <li>Category</li> </ul>	Import E-mail settings				
⊖ Filters	Set Active Only if notifications set	This setting is applicable only for imports from Alert files. For v 7, the active status will be set	Legacy ( based on	v6x)	
Alerts	<ul> <li>By default</li> </ul>	"Active" key available in the configuration se	ction.		
<ul> <li>Systems and Groups</li> <li>Token Value</li> </ul>	Watchlist Configuration	on			
<ul> <li>Reports</li> </ul>	This setting is applicable only f Note: If this option is enabled t on the console where the alert	or alerts which have Advanced watchlist config he user should make sure the watchlist groups a s are imported.	ured. are availat	ble	
O Behavior Correlation					
	Source :				
	D:\product\bluecoat\KP ite	ms\Alert_Bluecoat CAS.isalt			
		Impo	rt	Clos	e

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.



٩	💺 Export Import Utility		_		$\times$
	Export Import				
	1. Provide the path and file name 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.			
	Options	Location			
	Category				
	⊖ Filters				
	◯ Alerts				
	O Systems and Groups	Source : D:\product\Category_Category_Rtuescat_CAS isoat			
	O Token Value	D. product roalogory_caregory_braccoar choiacar			
	◯ Reports				
	O Behavior Correlation				
			ort	Class	
		ini	JOIL	Close	e



- 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.



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**.

KO, Bluecoat CAS .etko	🖀 Browse	Upload	

Close

#### Figure 9

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

•	Object name	Applies to	Group name
	Bluecoat Content Analysis File Activity	Bluecoat Content Analysis 1.3.x	Bluecoat Content Analysis
	Bluecoat Content Analysis Threat Detected	Bluecoat Content Analysis 1.3.x	Bluecoat Content Analysis



4. Knowledge objects are now imported successfully.







## **Token Templates**

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

≡	Event <b>Tracker</b> ⊕						Tools <del>•</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a			🛕 Alerts	Correlation	🔍 IP Lookup Configuration	🙊 Users	
	0	1	Behavior Correlation Rules	Diagnostics	Knowledge Objects	1 Weights	
<b>~</b>			🇞 Behavior Correlation Settings	🔁 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			📲 Category	FAQ Configuration	Report Settings		
	Attacker			<ul> <li>News</li> </ul>			

Figure 12

- 2. Move to **Template** and click on import configuration  $\mathbb{F}$  icon on the top right corner.
- 3. In the popup window browse the file named token\_Bluecoat CAS.ettd.

Impo	ort					
selec	ted file is: token_Bluecoat CAS.ettd	🗃 Browse Ҭ				
	Template name	Separator	Template description	Added date	Added by	Group Name
	Bluecoat Content Analysis - File Activity	\n	May 07 10:07:22 rbhq-cas1 1 2018-05-07T14:07:22.395Z 10.226.72.29 avserv ice 5235 - File decompression/decode error,, File has been dropped.,, 2018 -05-07 10:07:22 (EDT), Hardware serial number: 3817320026, CAS (Version 2 .3.1.1(213733)) - http://www.symantec.com, Antivirus Vendor: Symantec, Scan Engine Version: 2.0.1.4, Pattern File Version: 20180507.003. (Pattern da te: 2018/05/07),, Machine name: rbhq-cas1, Machine IP address: 10.226.72 .29, Server: 13.107.4.50, Client: 10.226.78.196, URL: http://7.tlu.dl.delivery. mp.microsoft.com/filestreamingservice/files/d5f4933e-6ae8-4c6a-92ba-6 ac0f2fde2277P1=1525702415&P2=301&P3=2&P4=8DJ6OjpQJV85TKG5scB 0fn5KhJ3rJRiU3tVSqVMvSJU%3d	May 08 11:34:01 AM	ETAdmin	Bluecoat Content Analysis
	Bluecoat Content Analysis - Threat Detected	\n	May 04 10:50:39 etmachine 1 2018-05-04T14:50:39.263Z 10.4.6.32 avservice 10890 - 2018-05-04 14:50:39 (UTC), Hardware serial number: 0515320030, C AS (Version 2.3.1.1(213733)) - http://www.symantec.com, Antirirus Vendor : Kaspersky Labs, Scan Engine Version: 8.2.5.17, Pattern File Version: 180504 (Pattern date 2018/05/04), Machine name: etmachine, Machine IP addres s: 10.4.6.32, Server: 182.25.25.56, Client: 192.26.77.18, Virus/PUS: "Suspicio us:Trojan.Script.Miner.gen" found!, URL: hxxp://www.testerdomain.com/	May 08 05:21:29 PM	ETAdmin	Bluecoat Content Analysis

Figure 13

4. Now select all the check box and then click on  $\ensuremath{\mathbb{T}}$  Import option.

# Flex Reports

On EventTracker Control Panel,



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

lote : If report(s) contains templa Options	ate, first import template and proceed with exportimport utility. Location
) Filters	
Alerts	Legacy (*.issch)     New (*.etcnx)
Systems and Groups	Source : *issch
) Token Value	
Reports	
Behavior Correlation	



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



- Repo	orts import						×
Note : I	If report(s) contains template, first import template and p	roceed with exportimp	ort utility.				
Select	t file D:\product\bluecoat\KP items\FlexReports_Blue	iecoat CAS.etcrx				Select file	
Availab	ble reports	_					
Title		Frequency	Show all	- Q	a		
$\checkmark$	Title	Sites	Groups		Systems	Frequency	Run
	EDIT Bluecoat Content Analysis - File activity	ETAdmin	Default		Bluecoat CAS	Undefined	12:08
	EDIT Bluecoat Content Analysis - Threat detected	ETAdmin	Default		Bluecoat CAS	Undefined	05:27
/						_	
Note	e: Set run time option is not applicable for Defined Repo	rts and Hourly Reports	1				
Set	run time for report(s) from	<ul> <li>at interval of</li> </ul>	_ minutes	Set ()			
				Note: Make s	ure that Site(s), Group(s) and System	(s) selections are valid.	• 0

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.



88	Home		
۹	My Dashboard		
2	Threats	1	
	Incidents	ntry point USB activities, New services or software install	
	Behavior Correlation		
	Change Audit		-
	Compliance		

Figure 17

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

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.         Dashboard_Bluecoat C	
	Close

Figure 18

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



Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
Department Upload	
Available widgets	
Select All	
🗹 Bluecoat Content Analysis 🗹 Bluecoat Content Analysis	
	Import Close

#### Figure 19

### 6. Click 'customize' (a) to locate and choose created dashlet.

С	ustomize dashlets				×
	Type to search			Q	^
	10.2.3 Access to all audit trails	10.2.6 Initialization stopping or	3.1.8 Limit unsuccessful logon	3.11.2 Scan for vulnerabilities in	
	3.3.8 Protect audit information	3.4.9 Control and monitor user	6.1.b Establish a process to ide	6.2.b - Install critical security pa	
	8.1.6 Limit repeated access atte	Bluecoat Content Analysis File	Bluecoat Content Analysis Thre	□ Ngnix-Client Requests	
	□ Ngnix-Http Response codes	Ngnix-Non-Standard Htt, Bluecoat	Content Analysis File Activity	□ Ngnix-Traffic Errors by Client IP	
	Ngnix-User Agents	SD WAN Application Based Tra	SD WAN CXD Device Port Staus	SD WAN Traffic Details	~
				Add Delete C	lose



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.

≡	Event <b>Tracker</b> ⊕					🔎 Admin-	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
q		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q 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 Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
		● Category	FAQ Configuration	Report Settings			
	Attacker		- News				



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

Alerts Alerts										
Show All 🗸						Search by	Alert name 🗸	bluecoat content 🔍 🔍		
124	14				124	System User	111	124	Critical 10 High Low 4 15 Senous 24	
Available Alerts Total number of alerts available	Active Alerts Total number of active alert		System/User Defined Alerts         Alerts by Threat Level           Count for system and user defined alerts         Count of alerts by threat level			Threat Level lerts by threat level				
Activate Now Click 'Activate No	ow' after making all changes								Total: 2 Page Size 25 🗸	
Alert Name A		Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To	
🔲 🚱 Bluecoat Content Analysis: File Blocked		•							Bluecoat Content Analysis 1.3x or above	
Bluecoat Content Analysis: Threat Detected		•							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		🕈 / Admin / Category
Category Tree Search	Category Details	
· All Categories	Parent Group Bluecoat Content Analysis	
-	Event Category Name Bluecoat Content Analysis File Activity	
	Description	
Bluecoat Content Analysis      Bluecoat Content Analysis File Activity      Bluecoat Content Analysis File Activity      Bluecoat Content Analysis Theat Detect	Applies to Bluecoat Content Analysis 1.3x or abo Category version	
	Show In Compliance Security	
Cisco ASA Firewall	Event Rule	Add Edit Delete
Fortigate Firewall     Joginx Web Server	Log         Event         Description           Type         Type         Category         Id         Source         User         Match in Description         Exception	on n Lucene Query
IST 800-171	0 0 syslog Hardware\sserial\snumber\*?Machine\sname\*? Machine\sIP\saddress\*?Client\[^\\]+\+\s+URL\:	log_source:"Bluecoat Content Analysis File Activity"
Riverbed SteelHead		
SDWAN		Save

Figure 24

### Knowledge Objects

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



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

Knowledge Objects						📌 / Admin / Knowledge Objects
Search objects	Q Q Activa	e Now				Objects 🕂 ፒ 🏦 🇱
Groups 🕀 🧭 🗓	Object name Bluecoat Conte	nt Analysis File Activity				+ <u>1</u> 🌣
Apache Web Server	Applies to Bluecoat Content	Analysis 1.3.x and above				
Bluecoat Content Analysis	Rules					
Bluecoat Content Ana 🧭 🏢	Title	Log type	Event source	Event id	Event type	
Bluecoat Content Ana 🧭 📗	🗄 Bluecoat Content Ana	lysis File Activity	syslog*			🧭 记 🗓 🔗
E Cisco ASA Firewall	Message Signature:	lardware\sserial\snumber\:.*?Machine\	sname\:.*?Machine\sIP\saddress\:.'	*?Server\:.*?Client\:[^\:]++	\s+URL\:	
Default	Message Exception:					
E EventTracker	Expressions					
-	Expression type	Expression 1			Expression 2	Format string
	Regular Expression	(?:\w+)\s\d+\s\-\s(? <reaso< td=""><td>on&gt;.*?)+(?<action>.*?)+</action></td><td></td><td></td><td></td></reaso<>	on>.*?)+(? <action>.*?)+</action>			
Fortigate Firewall	Regular Expression	(? <key>[^\;,]+)\;(?<value></value></key>	[^]+)			



## Token Template

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

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin 🗸	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	© Correlation	🔍 IP Lookup Configuration	🛱 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	1 Weights	
<u>~</u>			🇞 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 ser	Casebook Configuration	Seventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker		- News				



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

Parsing Rules									🕈 / Admin / Parsing Rules
Parsing Rule Templ	late								
Groups		⊕ 101	Group : Bluecoat Conten	t Analysis Search_	Q				CII
Default.		^							
Bluecoat Content Ana	直	1	Template Name	Template Description	Added By	Added Date	Active		
Cisco ASA	前	Ø	Bluecoat Content Analysi Activity	u - File		May 08 11:34:01 AM			Ø
EventTracker	前	1	Bluecost Content Analysi	ā -		May 08 0521-29 PM	R		Ø
Microsoft Windows RR 📋 🧭		1	Threat Detected					-	10 A





### **Flex Reports**

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



- 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.

Report Configuration A / Reports / Report Configuration / D								
○ Scheduled ○ Queued   Defined		Search	Q Q					
Report Groups 🕀 🏭	Reports configuration: Bluecoat Content Analysis			T-t-b 2				
Compliance	Title	Created on	Modified on	Iotai: 2				
Operations	Kit Bluecoat Content Analysis - Threat detected	May 08 05:27:59 PM	May 08 05:27:59 PM	- +				
🔁 Flex	Bluecoat Content Analysis - File Activity	May 08 12:08:46 PM	May 08 05:54:41 PM	÷				
🔁 Bluecoat Content Ana 🏢 🧭								

Figure 29



# Sample Flex Dashboards

#### **Title: Bluecoat Content Analysis File Activity**



Figure 30







Figure 31

