Netsurion. EventTracker*

Integrate Zscaler ZPA EventTracker v9.2 and above

Publication Date: June 26, 2020

Abstract

This guide helps you in configuring **Zscaler ZPA** with EventTracker to receive **Zscaler ZPA** events. In this guide, you will find the detailed procedures required for monitoring **Zscaler ZPA**.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **Zscaler ZPA**.

Audience

Administrators, who are assigned the task to monitor and manage **Zscaler ZPA** events using **EventTracker**.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	C	Dverview	. 3
2	P	Prerequisites	. 3
3.	. Ir	ntegration of Zscaler ZPA with EventTracker	. 3
4.	Е 4.1	ventTracker Knowledge Pack Category	. 5 . 5
	4.2	Alert	. 5
	4.3	Report	. 6
	4.4	Dashboards	. 8
5.	lı 5.1	mporting Zscaler ZPA knowledge pack into EventTracker Category	12 12
	5.2	Alert	13
	5.3	Knowledge Object	14
	5.4	Report	17
	5.5	Dashboards	18
6	V 6.1	/erifying Zscaler ZPA knowledge pack in EventTracker Category	21 21
	6.2	Alert	22
	6.3	Knowledge Object	23
	6.4	Report	23
	6.5	Dashboards	24

Netsurion. EventTracker*

1. Overview

This guide helps you in configuring **Zscaler ZPA** with EventTracker to receive **Zscaler ZPA** events. In this guide, you will find the detailed procedures required for monitoring **Zscaler ZPA**.

EventTracker helps to monitor events from **Zscaler ZPA**. Its dashboard, alerts and reports help to detect authentication failure and other suspicious activities.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- EventTracker v9.2 or above should be installed.
- **Zscaler ZPA** should be configured.
- Port 514 should be open.

3. Integration of Zscaler ZPA with EventTracker

A. Configure a connector.

To configure a new Connector: https://help.zscaler.com/zpa/configuring-connectors.

B. Configure the log receiver.

To add a log receiver.

- 1. Go to Administration > Log Receivers.
- 2. Click Add Log Receiver.

The Add Log Receiver window appears.

In the Add Log Receiver window, configure the following tabs.

- a. In the Log Receiver tab:
 - Name: Enter a name for the log receiver. The name cannot contain special characters, except for periods (.), hyphens (-), and underscores (_).



- **Description**: (Optional)Enter a description.
- **Domain or IP Address**: Enter the fully qualified domain name (FQDN) or IP address of EventTracker Manager.

If the FQDN or IP address of the log receiver overlaps with or is as same as the wildcard domain or IP subnet defined in an application segment, the <u>Bypass setting</u> configured for the application segment takes precedence. As a result, if the FQDN or IP address is bypassed for a user on a trusted network, the user's device will not be able to communicate with the log receiver.

- **TCP Port**: Enter the TCP port number used by the EventTracker Manager.
- **Connector Groups**: Choose the Connector groups that can forward logs to the receiver and click **Done**. You can search for a specific group, click **Select All** to apply all groups, or click **Clear Selection** to remove all selections.

If you have a use case where the user's device needs to send logs to the log receiver using ZPA, configure an application segment with the log receiver domain or IP address and the port that the log receiver is listening on.

×

b. Click Next.



Netsurion. EventTracker

C. Configure Log stream

In the Log Stream tab, select a Log Type from the drop-down menu:

- User Activity: Information on end user requests to applications.
- User Status: Information related to an end user's availability and connection to ZPA.
- **Connector Status**: Information related to a Connector's availability and connection to ZPA.
- **Browser Access**: HTTP log information related to browser access.

Select Log Template from the drop-down menu as Json.

Click Next

Note: For any query regarding configuring log receiver and log stream, click on following link. <u>https://help.zscaler.com/zpa/configuring-log-receiver#Step1</u>

4. 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 to support Zscaler ZPA.

4.1 Category

- **Zscaler ZPA: User Authentication Failed** This category provides information related to any user authentication failure detected in Zscaler ZPA.
- **Zscaler ZPA: Connector Authentication Failed** This category provides information related to connector authentication failure in Zscaler ZPA.
- **Zscaler ZPA: Browser Activity** This category provides information related to all the browser activity in Zscaler ZPA.
- **Zscaler ZPA: Connector Status** This category provides information related to connector status in Zscaler ZPA.
- **Zscaler ZPA: User Activity** This category provides information related to user activities such as user performed in Zscaler ZPA
- Zscaler ZPA: User Status This category provides information related to user status in Zscaler ZPA.

4.2 Alert

• **Zscaler ZPA: User Authentication Failure** – This alert is generated when any user authentication failure is detected in Zscaler ZPA.



• **Zscaler ZPA: Connector Authentication Failure** – This alert is generated when any connector authentication failure is detected in Zscaler ZPA

4.3 Report

Zscaler ZPA: User Activity - This report gives the information related to user activities performed in Zscaler ZPA. Report contains connection status, IP address, port, application name, username, customer name and other fields which will be provide a detailed view about user activity.

LogTime	Customer	ConnectionID	ConnectionStatus	IPProtocol	SessionID	Username	ServicePort PrivatelP	Client IP	ConnectorIP
06/25/2020 12:46:03 PM	ANZ Team/zdemo in beta	SqyZIMkg0JTj7EABsvwA,Q+EjXG0 rvbF2lPiBbedm	1 active	6	SqyZIMkg0JTj7EABsvwA	ZPA LSS Client	10011	34.209.189.218	192.168.1.53
06/25/2020 12:46:03 PM	ANZ Team/zdemo in beta	SqyZIMkg0JTj7EABsvwA,Q+EjXGo rvbF2IPiBbedm	l open	6	SqyZIMkg0JTj7EABsvwA	ZPA LSS Client	" 10011	34.209.189.218	192.168.1.53
06/25/2020 12:46:03 PM	ANZ Team/zdemo in beta	SqyZIMkg0JTj7EABsvwA,Q+EjXGo rvbF2IPiBbedm	l closed	6	SqyZIMkg0JTj7EABsvwA	ZPA LSS Client	1 0011	34.209.189.218	192.168.1.53



• **Zscaler ZPA: Browser Activity** - This report gives the information about the HTTP log information related to browser access. Reports contains User email, HTTP method, protocol, request size, response size, user agent, URL, client IP, port and other details which can be used for investigation.

LogTime	ApplicationPort	Client IP	Customer	Exporter	Host	Method	Email ID	URL	UserAgent
06/24/2020 01:30:40 PM	443	139.216.128.195	ANZ Team/zdemo in beta	unset	portal.beta.zdemo.net	GET	admin@zdemo.net	/speeddial-18.0.99-82-gd7ba322- dirty/media/HelveticaNeueLTStd- Regular.762cbf85.woff	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKt/b05.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
06/24/2020 01:30:40 PM	443	139.216.128.195	ANZ Team/zdemo in beta	unset	portal beta.zdemo.net	POST	admin@zdemo.net	/speeddial-18.0.99-82-gd7ba322- dirty/media/HelveticaNeueLTStd- Regular.762cbf85.woff	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebK#/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safar/605.1.15
06/25/2020 12:46:03 PM	443	139.216.128.195	ANZ Team/zdemo in beta	unset	portal.beta.zdemo.net	GET	admin@zdemo.net	/speeddial-18.0.99-82-gd7ba322- dirty/media/HelveticaNeueLTStd- Regular.762cb185.woff	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKill605.1.15 (KHTML, like Gecko) Version/12.1.1 Safarl/605.1.15

Figure 3

• **Zscaler ZPA: Connector Status** – This report gives information about the connector status of Zscaler ZPA regarding management, data forwarding and configuration update. Reports contains session type, status, session ID, connector name and IP of connector and other useful details for investigation.

LogTime	Connector	Customer	Platform	PrivateIP	Client IP	SessionID	Session Status	Session Type	Session Edge
06/26/2020 03:04:36 PM	Seattle Connector 1	Safe March	el7	10.0.0.4	52.224.237.221	8A64Qwj9zCkfYDGJVoUZ	ZPN_STATUS_AUTHENTICATED	ZPN_ASSISTANT_BROKER_CONT ROL	US-NY-8179
06/26/2020 03:04:36 PM	Seattle Connector 1	Safe March	el7	10.0.0.4	52.224.237.221	8A64Qwj9zCkfYDGJVoUZ	ZPN_STATUS_AUTHENTICATED	ZPN_ASSISTANT_BROKER_DATA	US-NY-8179
06/26/2020 03:04:36 PM	Seattle Connector 1	Safe March	el7	10.0.0.4	52.224.237.221	8A64Qwj9zCkfYDGJVoUZ	ZPN_STATUS_AUTHENTICATED	ZPN_ASSISTANT_BROKER_CONFI G	US-NY-8179

F	igı	٦r	e	4
	ıgı	JI	e	4

Netsurion. EventTracker

• **Zscaler ZPA: User Status** – This report gives information about user status connected to Zscaler ZPA. Report contains IP address, username, email, session status as (connected, disconnected and authenticated) and other useful information.

LogTime	Cert Common Name	Client Type	Customer	Hostname	Email	SAML UserName	Platform	Client IP	SessionID	Session Status
06/26/2020 03:04:36 PM	slogger1b.pdx2.zpabeta.net	zpn_client_type_zapp	ANZ Team/zdemo in beta	DESKTOP-2K299HC	jdoe@zscaler.com	jdoe	windows	34.216.108.5	cKgzUERSLI09Y+ytH8v5	ZPN_STATUS_CONNECTED
06/26/2020 05:02:01 PM	slogger1b.pdx2.zpabeta.net	zpn_client_type_zapp	ANZ Team/zdemo in beta	DESKTOP-2K299HC	jenny@zscaler.com	jenny	windows	34.216.108.5	cKgzUERSLI09Y+ytH8v5	ZPN_STATUS_AUTHENTICATE
06/26/2020 05:02:01 PM	slogger1b.pdx2.zpabeta.net	zpn_client_type_zapp	ANZ Team/zdemo in beta	DESKTOP-2K299HC	william@zscaler.com	william	windows	3 <mark>4.216.108.5</mark>	cKgzUERSLI09Y+ytH8v5	ZPN_STATUS_DISCONNECTED

Figure 5

• **Zscaler ZPA: User Authentication Failure** - This report gives information regarding all the user authentication failure detected in Zscaler ZPA. Reports contains IP address, session ID, username, email, IP and other useful information for analysis.

LogTime	Cert Common Name	Client Type	Customer	Hostname	Email	SAML UserName	Platform	Client IP	SessionID	Username
06/26/2020 03:04:36 PM	slogger1b.pdx2.zpabeta.net	zpn_client_type_zapp	ANZ Team/zdemo in beta	DESKTOP-2K299HC	jdoe@zscaler.com	jdoe	windows	34.216.108.5	cKgzUERSLI09Y+ytH8v5	ZPA LSS Client
06/26/2020 03:04:36 PM	slogger1b.pdx2.zpabeta.net	web	ANZ Team/zdemo in beta	DESKTOP-2K299HC	jdoe@zscaler.com	jdoe	windows	34.216.108.5	cKgzUERSLI09Y+ytH8v5	ZPA LSS Client
06/26/2020 05:02:01 PM	slogger1b.pdx2.zpabeta.net	zpn_client_type_zapp	ANZ Team/zdemo in beta	DESKTOP-2K299HC	mark@zscaler.com	mark	windows	34.216.108.5	cKgzUERSL109Y+ytH8v5	ZPA LSS Client

Figure 6

Logs Considered

application_type	+- el7
attributes	+- Azure Connectors
category	+- Seattle Connector 1
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 6/26/2020 5:02:01 PM
event_datetime_utc	+- 1593171121
event_description	Jun 26 17:02:01 172:27.100.13 ("LogTimestamp": "Wed Jul 3 05:17:22 2019", "Customer": "Safe March", "SessionID": "8A64Qwj9zCkfYDGJVoUZ", "SessionTy
	pe": "ZPN_ASSISTANT_BROKER_DATA", "SessionStatus": "ZPN_STATUS_DISCONNECTED", "Version": "19.20.3", "Platform": "eI7", "ZEN": "US-NY-8179", "Conn
	ector": "Seattle Connector 1","ConnectorGroup": "Azure Connectors","PrivatelP": "10.0.0.4","PubliclP": "52.224.237.222","Latitude": 47.000000,"Longitud
	e": -122.000000, "CountryCode": "", "TimestampAuthentication": "2019-06-27T05:05:23.3482", "TimestampUnAuthentication": "", "CPUUtilization": 1, "Mem
	Utilization": 20, "ServiceCount": 2, "InterfaceDefRoute": "eth0", "DefRouteGW": "10.0.0.1", "PrimaryDNSResolver": "168.63.129.16", "HostUpTime": "15132299
	95", "ConnectorUpTime": "1555920005", "NumOfInterfaces": 2, "BytesRxInterface": 319831966346, "PacketsRxInterface": 1617569938, "ErrorsRxInterface":
	0, "DiscardsRxInterface": 0, "BytesTxInterface": 192958782635, "PacketsTxInterface": 1797471190, "ErrorsTxInterface": 0, "DiscardsTxInterface": 0, "TotalBytesR
	x": 10902554,"TotalBytesTx": 48931771}
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event user domain	+- N/A

Figure 7

Netsurion EventTracker[®]

4.4 Dashboards



• Zscaler ZPA: Authentication Failed by Username



• Zscaler ZPA: Authentication Success by Username









• Zscaler ZPA: Authentication Failed by Geolocation





• Zscaler ZPA: Connection Status by Username







• Zscaler ZPA: Application Name by Host



• Zscaler ZPA: Session Type by Session Status





Netsurion. EventTracker[®]



• Zscaler ZPA: Connector Authentication Failure by IP

Figure 14



• Zscaler ZPA: Session Type by IP





5. Importing Zscaler ZPA knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence.

- Category
- Alert
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.



Figure 16

3. Click the Import tab.

5.1 Category

1. Click **Category** option, and then click Browse

<u>ц</u>	Export Import Utility	-		x
Export Import	e of the Categories file. Use the '' button to browse and locate the import file. Location Source :			
	Import		Close	9

Figure 17

- 2. Locate Category_Zscaler ZPA.iscat file, and then click Open.
- 3. To import categories, click Import.

EventTracker displays success message.





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

5.2 Alert

1. Click Alert option, and then click Browse

ц. 1	Export Ir	Export Import Utility							
Export Import	Export Ir me of the Alerts file. Use the '' butt Location Import E-mail settings Set Active Only if notifications set By default Watchlist Configuration Import Watchlist configuration Import Watchlist configuration Intis setting is applicable only f Note: If this option is enabled t on the console where the alert Source : Tiset	nport Utility on to browse and locate the import file. This setting is applicable only for imports from Leg Alert files. For v7, the active status will be set base "Active" key available in the configuration section on or alerts which have Advanced watchlist configured he user should make sure the watchlist groups are a s are imported.	acy (v £x) ad on 						
		Import	Close						

Figure 19

- 2. Locate Alert_Zscaler ZPA.isalt file, and then click Open.
- To import alerts, click Import.
 EventTracker displays success message.



Figure 20

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

5.3 Knowledge Object

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.



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

Figure 21

2. Click **Import** \mathbb{T} as highlighted in the below image.

	Knowledge Ob	jects		↑ Admin / Knowledge Objects
Q. 	Search objects	Q	Q Activate Now	Objects 🕀 🇊 🏦 🇱
	Groups	🕀 🏈 🗓		٤.
	E Cylance			
	EventTracker			

Figure 22



- 4. Locate the file named **KO_Zscaler ZPA.etko**.
- 5. Now select the check box and then click \blacksquare Import.

3. Click Browse.

Netsurion. EventTracker

Import			×
Select fi	le		🗁 Browse Upload
	Object name	Applies to	Group name
	Zscaler	Zscaler ZPA	Zscaler ZPA
			Import Close

Figure 24

6. Knowledge objects are now imported successfully.

File imported successfully.
ОК
 Figure 25



5.4 Report

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

4	Export Import Utility	-		x
Export Import 1. Provide the path and file nam 2. Click the Import button Note : if report(s) contains temp Options Category Filters Alerts Systems and Groups Token Value Image: Reports Behavior Correlation	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility. Location C Legacy (*.issch) New (*.etcx) Source : *.issch			
	Import		Clos	e

Figure 26

2. Locate the file named **Reports_Zscaler ZPA.etcrx** and select the check box.

ailab	ole repo	ts						
le			Freq	uency Show al	•	QQ		
2		Title	S	lites		Groups	Systems	Frequency
3	EDIT	Zscaler ZPA - Browser Activity Log	R1S5-VM30					Undefined
3	EDIT	Zscaler ZPA - Connector Status logs	R1S5-VM30					Undefined
1	EDIT	Zscaler ZPA - User Activity Log	R1S5-VM30					Undefined
1	<u>EDIT</u>	Zscaler ZPA - User Authenticaion Failure	R1S5-VM30					Undefined
1	EDIT	Zscaler ZPA - User Status Logs	R1S5-VM30					Undefined
ote	e: Set ru	n time option is not applicable for Defined F	Reports and Houry	/ Reports				>

Figure 27



3. Click Import \mathbb{T} to import the report. EventTracker displays success message.





5.5 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.

	Home		
٩	My Dashboard		
R	Threats	1	
	Incidents	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation		
	Change Audit		-
	Compliance	The second s	



- 2. Navigate to My Dashboard option as shown above.
- 3. Click **Import** \blacksquare as show below.

Event Tracker ⊕	*	Admin→	Tools +	💽 ETAdmin 🔹
My Dashboard		A	/ Dashboar	d / My Dashboard
		÷	or 🕲 🖏	1 3 0
Fig	ure 30			

- 4. Import dashboard file Dashboard_Zscaler ZPA.etwd and select Select All checkbox.
- 5. Click Import as shown below.

		Browse	Upload
Available widgets			
Zscaler ZPA: Authenticati	Zscaler ZPA: Authenticati		
Zscaler ZPA: Authenticati	Zscaler ZPA: Connection s		
Zscaler ZPA: Application	Zscaler ZPA: Session Type		
Zscaler ZPA: Connector Au	Zscaler ZPA: Session Type		

Figure 31

6. Import is now completed successfully.





7. In **My Dashboard** page select to add dashboard.





8. Choose appropriate name for **Title** and **Description**. Click **Save**.

Netsurion. EventTracker

itle			
Zscaler ZPA			
escription			
Zscaler ZPA			
		1	7
	Save	Delete	Cancel

Figure 34

9. In **My Dashboard** page select (a) to add dashlets.

My Dash	board		👚 / Dashboard / My Dashboar					
			+ 🖉 🕲 🌣 主 🗊 🎯					
CheckPoi	nt Trend Micr	Microsoft	_					
	Figure 35							

10. Select imported dashlets and click Add.

scale			Q	
Zscaler ZPA: Application Name	Zscaler ZPA: Authentication Fail	Zscaler ZPA: Authentication Fail	Zscaler ZPA: Authentication Suc	
Zscaler ZPA: Connection status	Zscaler ZPA: Connector Authent	Zscaler ZPA: Session Type by IP	Zscaler ZPA: Session Type by Se	

Figure 36



6. Verifying Zscaler ZPA knowledge pack in EventTracker

6.1 Category

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

≡	Event Tracker ⊕					🐥 🛛 Admin 🗸	Tools -
	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	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	P Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			_



3. In **Category Tree** to view imported category, scroll down and expand **Zscaler ZPA** group folder to view the imported category.

Category Tree	Search
- All Categories	
La Ca EventTr	acker
	IP DNS
Zscaler	ZPA
- 🗐 Zso	caler ZPA: Broswer Activity
- 🗐 Zso	aler ZPA: Connector Authenticatio
- 🗐 Zso	aler ZPA: Connector Status
- 🗐 Zso	aler ZPA: User Activity
- 🗐 Zso	aler ZPA: User Authentication Faile

Figure 38

Netsurion EventTracker[®]

6.2 Alert

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

≡	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	_
s, ₿	O Potential Cyber Breaches Unsafe connections of processes, new TCP entry point	2 Indicators of Cc USB activities, New sen	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	T Weights	
			🍓 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
			Casebook Configuration	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker		- News				

Figure 39

 In the Search box, type 'Zscaler ZPA, and then click Go. Alert Management page will display the imported alert.

Ð	Ē	Activate Now Click 'Activate Now' after making	ng all changes	
		Alert Name 🔨	Threat	Active
	6-0	Zscaler ZPA: Connector Authentication Failed	•	
	6-0	Zscaler ZPA: User Authentication Failed	•	

Figure 40

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.



Figure 41

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

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

6.3 Knowledge Object

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

≡	Event Tracker ⊕					🔺 🗛 Admin -	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	QQ 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 Co USB activities, New sen	Casebook Configuration	Seventvault	D Parsing Rules		
			e Category	FAQ Configuration	Report Settings		
	Attacker			- News			



2. In the Knowledge Object tree, expand **Zscaler ZPA** group folder to view the imported knowledge object.

Netsurion EventTra	icker ⁻			
Duo Security	Rule	s		
EventTracker		Title	Event source	Source Type
	+	ZPA	syslog*	Zscaler ZPA
FS BIG IP		Message Signature:		
F5 Big IP DNS		Message Exception:		
G suite		Expressions		
E Linux OS		Expression type	Expression 1	
	_	Regular Expression	\"(? <key>[^"]+)\"\:(\s\" \")(?<val< td=""><td>ue>[^"]+)</td></val<></key>	ue>[^"]+)
Microsoft 365		Regular Expression	\"myname\:(? <name>[^,]+)my</name>	email\:(? <email>[^"]</email>
Sophos Central				
Sophos XG Firewall				
• Windows				
Zscaler ZPA				
Zscaler 🧭	Ē			



3. Click Activate Now to apply imported knowledge objects.

6.4 Report

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





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

epo	rt Configuration					
⊖ Scł	neduled 🔿 Queued 🧿 D	efined				
Repoi	rt Groups		(+)	Rep	orts conf	iguration: Zscalar ZPA
4	Security			Ð	1 2	
٩.	Compliance					Title
1	Operations					Zscaler ZPA - Browser Activity Log
٩.	Flex					Zscaler ZPA - User Activity Log
	F5 BIG IP DNS	Ē	Ø			Zscaler ZPA - Connector Status logs
	Zscalar ZPA		1			Zscaler ZPA - User Authenticaion Failur
					533	Zscaler ZPA - User Status Logs

Figure 45

6.5 Dashboards

1. In the EventTracker web interface, Click Home and select "My Dashboard".

Netsurion. EventTracker

	Home	
Dashb	My Dashboard	
	Threats	
	Incidents	



2. In the "Zscaler ZPA" dashboard you should be now able to see something like this.



Figure 47

