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.**

Table of Contents

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 Bypass setting 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**.

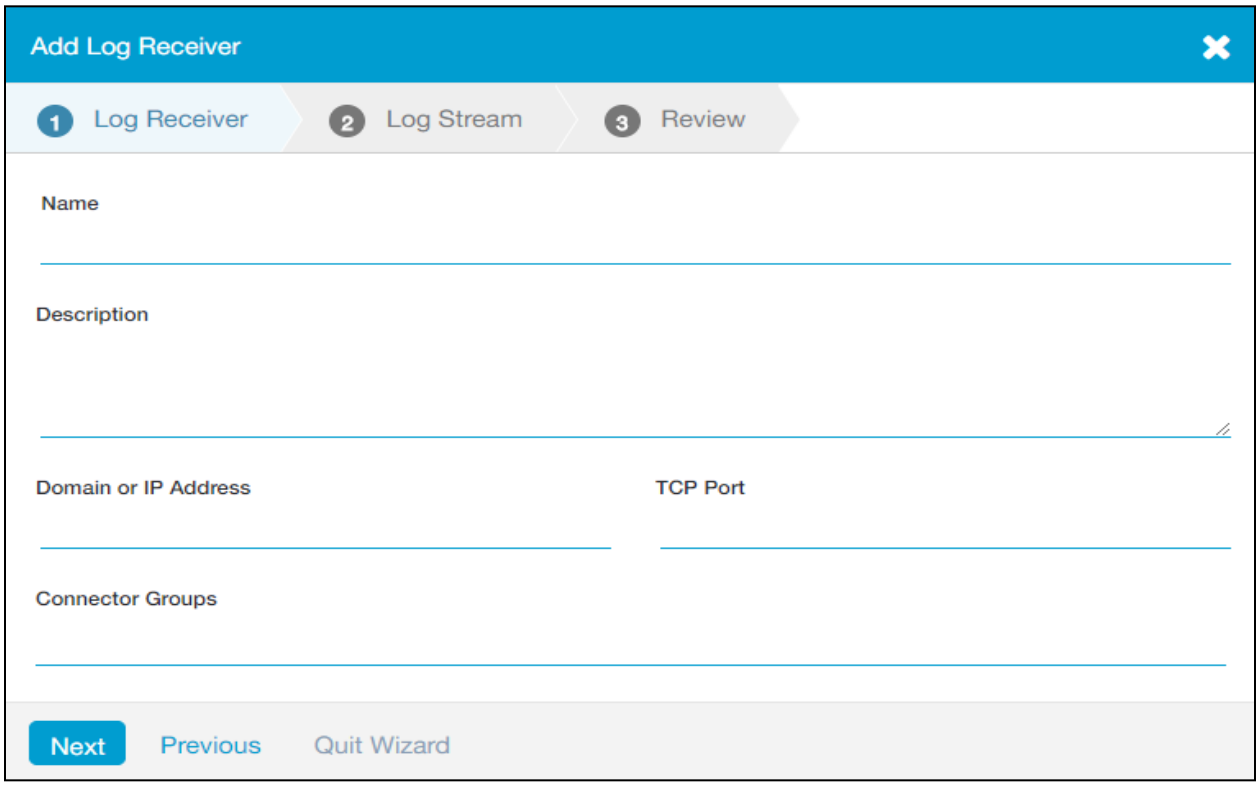

Figure 1

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.
https://help.zscaler.com/zpa/configuring-log-receiver#Step1

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	PrivateIP	Client IP	ConnectorIP
06/25/2020 12:46:03 PM	ANZ Team/zdemo in beta	SqyZIMkg0JTj7EABsvwA,Q+EjXGd rvbF2lPlBbedm	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+EjXGd rvbF2lPlBbedm	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+EjXGd rvbF2lPlBbedm	closed	6	SqyZIMkg0JTj7EABsvwA	ZPA LSS Client	10011		34.209.189.218	192.168.1.53

Figure 2

- **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	St
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) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	30
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) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	30
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.762cbf85.woff	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	30

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	8A64QwjθzCkfYDGJVoUZ	ZPN_STATUS_AUTHENTICATED	ZPN_ASSISTANT_BROKER_CONTROL	US-NY-8179
06/26/2020 03:04:36 PM	Seattle Connector 1	Safe March	el7	10.0.0.4	52.224.237.221	8A64QwjθzCkfYDGJVoUZ	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	8A64QwjθzCkfYDGJVoUZ	ZPN_STATUS_AUTHENTICATED	ZPN_ASSISTANT_BROKER_CONFIG	US-NY-8179

Figure 4

- **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	34.216.108.5	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	cKgzUERSLI09Y+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","SessionType": "ZPN_ASSISTANT_BROKER_DATA","SessionStatus": "ZPN_STATUS_DISCONNECTED","Version": "19.20.3","Platform": "el7","ZEN": "US-NY-8179","Connector": "Seattle Connector 1","ConnectorGroup": "Azure Connectors","PrivateIP": "10.0.0.4","PublicIP": "52.224.237.222","Latitude": 47.000000,"Longitude": -122.000000,"CountryCode": "","TimestampAuthentication": "2019-06-27T05:05:23.348Z","TimestampUnAuthentication": "","CPUUtilization": 1,"Mem Utilization": 20,"ServiceCount": 2,"InterfaceDefRoute": "eth0","DefRouteGW": "10.0.0.1","PrimaryDNSResolver": "168.63.129.16","HostUpTime": "1513229995","ConnectorUpTime": "1555920005","NumOfInterfaces": 2,"BytesRxInterface": 319831966346,"PacketsRxInterface": 1617569938,"ErrorsRxInterface": 0,"DiscardsRxInterface": 0,"BytesTxInterface": 192958782635,"PacketsTxInterface": 1797471190,"ErrorsTxInterface": 0,"DiscardsTxInterface": 0,"TotalBytesRx": 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

4.4 Dashboards

- **Zscaler ZPA: Authentication Failed by Username**

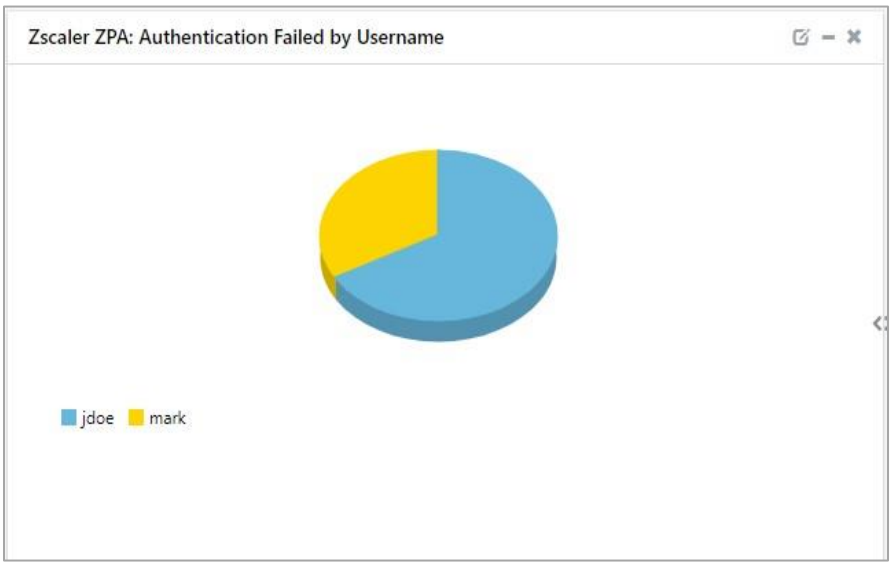

Figure 8

- **Zscaler ZPA: Authentication Success by Username**

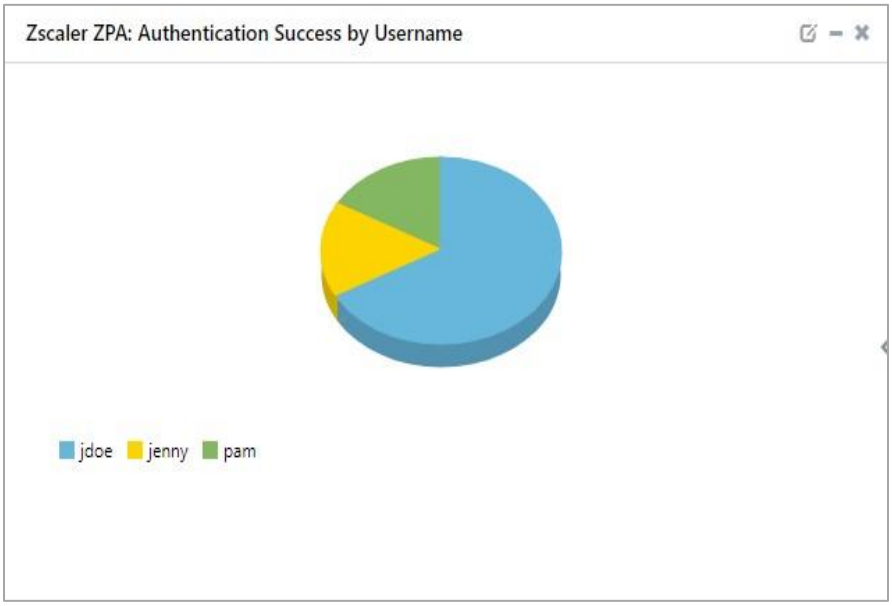

Figure 9

- **Zscaler ZPA: Authentication Failed by Geolocation**

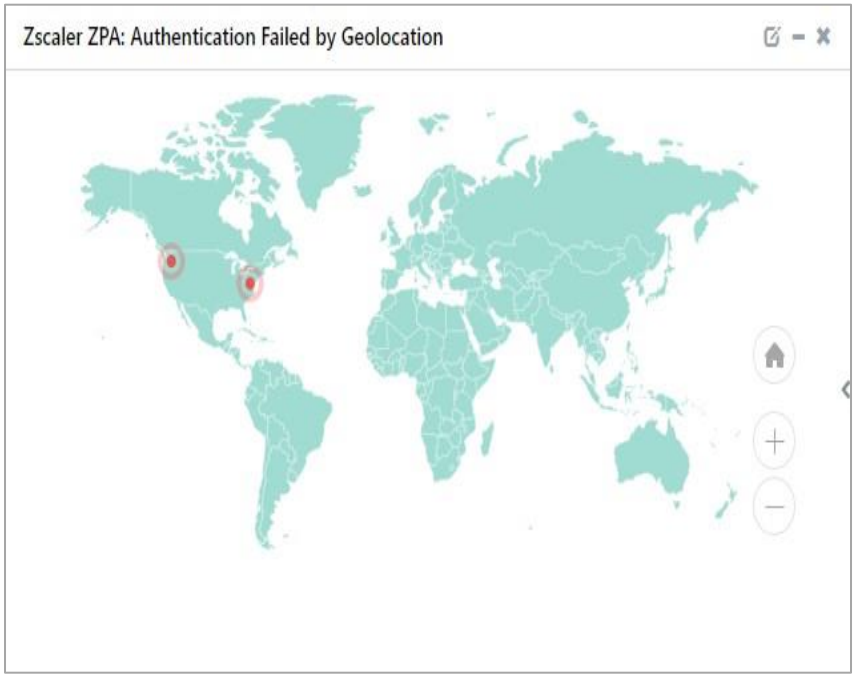

Figure 10

- **Zscaler ZPA: Connection Status by Username**

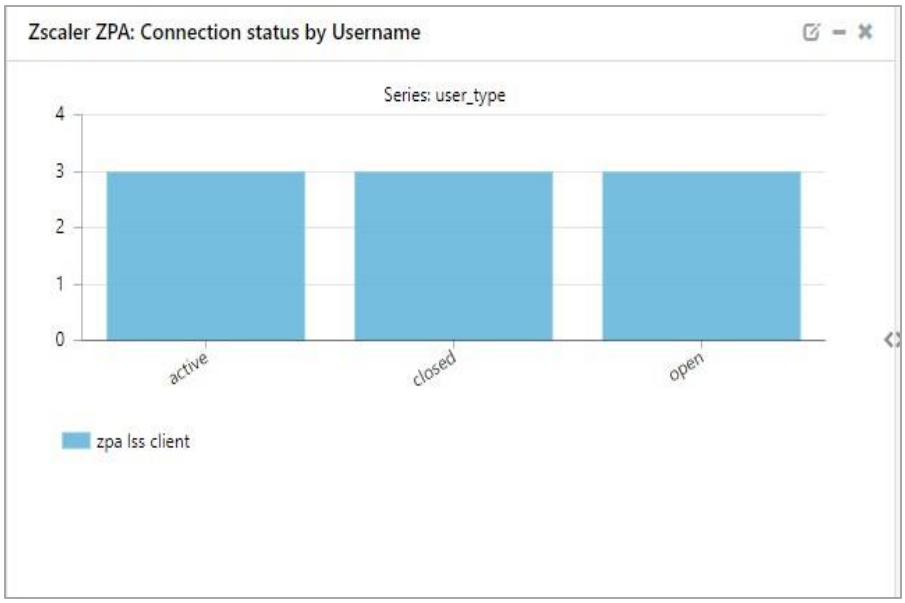

Figure 11

- **Zscaler ZPA: Application Name by Host**

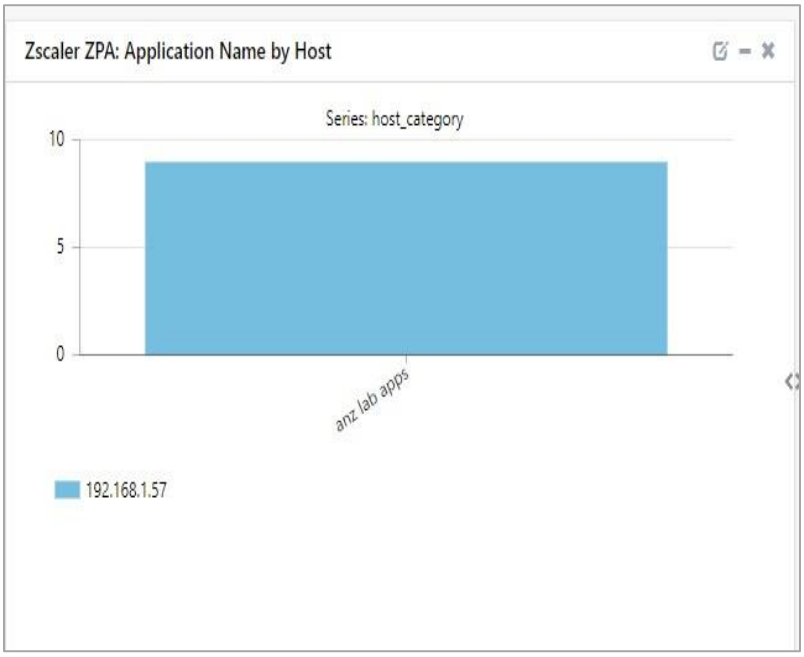

Figure 12

- **Zscaler ZPA: Session Type by Session Status**

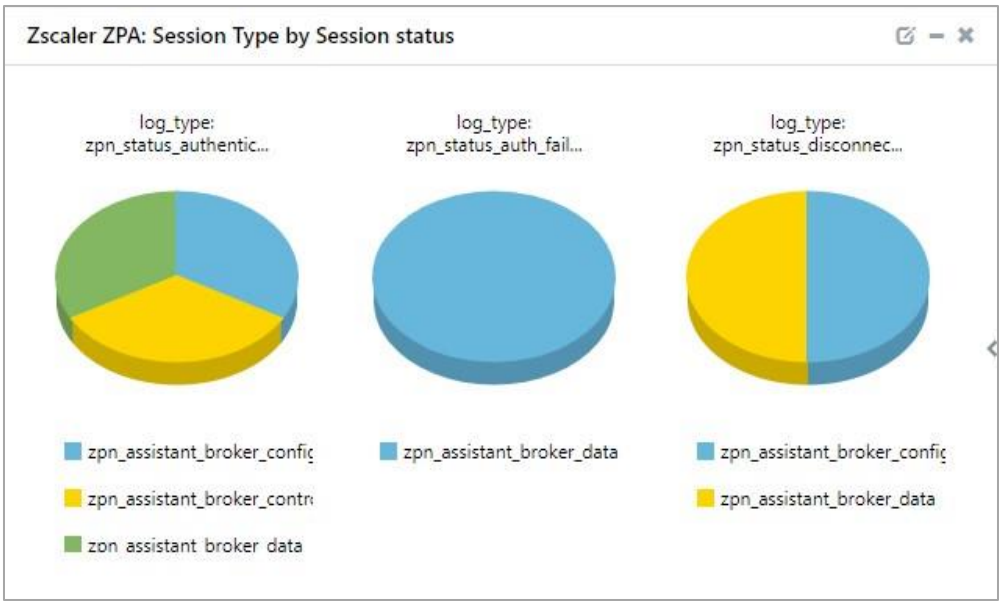

Figure 13

- **Zscaler ZPA: Connector Authentication Failure by IP**

Figure 14

- **Zscaler ZPA: Session Type by IP**

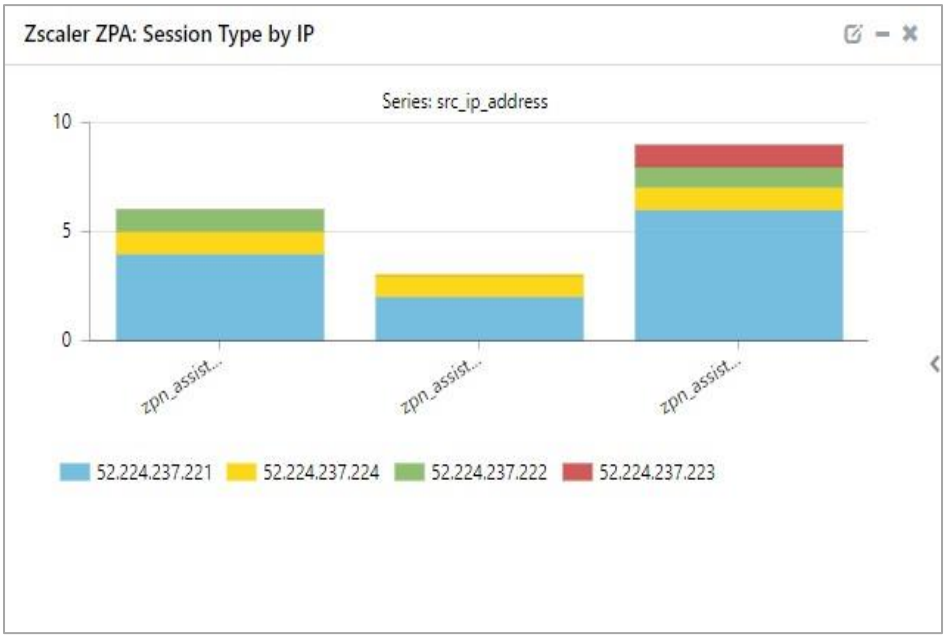

Figure 15

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**.

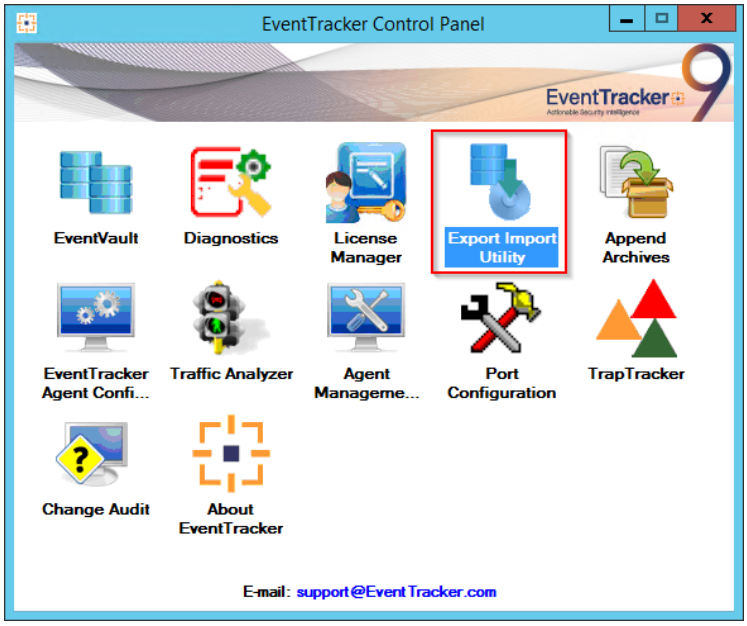

Figure 16

3. Click the **Import** tab.

5.1 Category

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

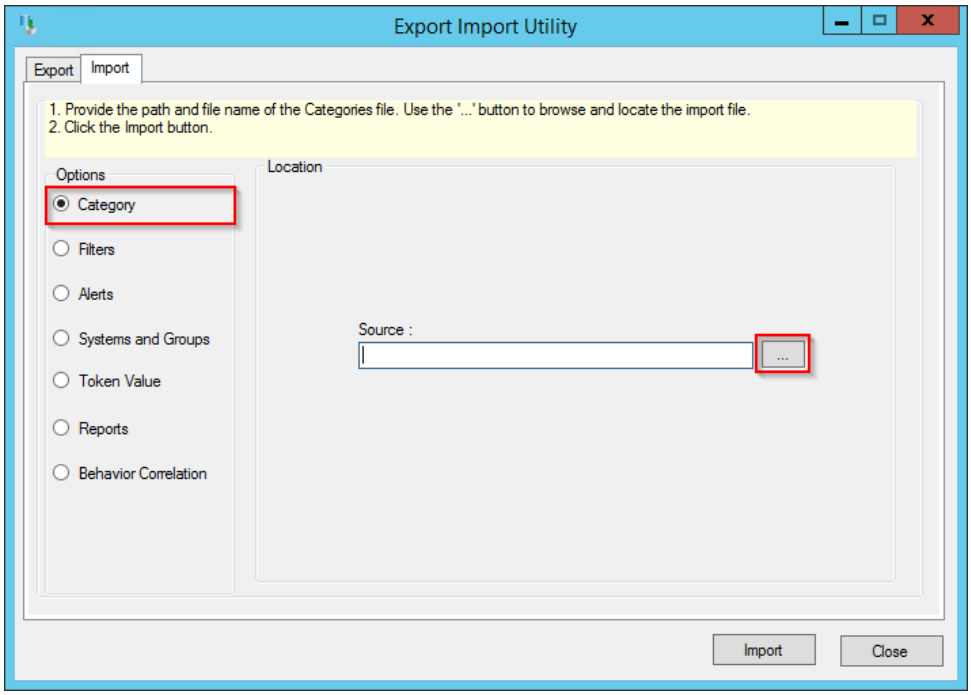

Figure 17

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

EventTracker displays success message.

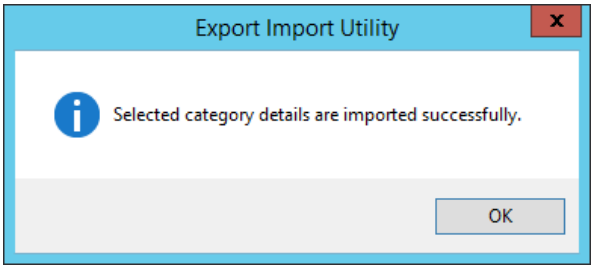

Figure 18

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

5.2 Alert

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

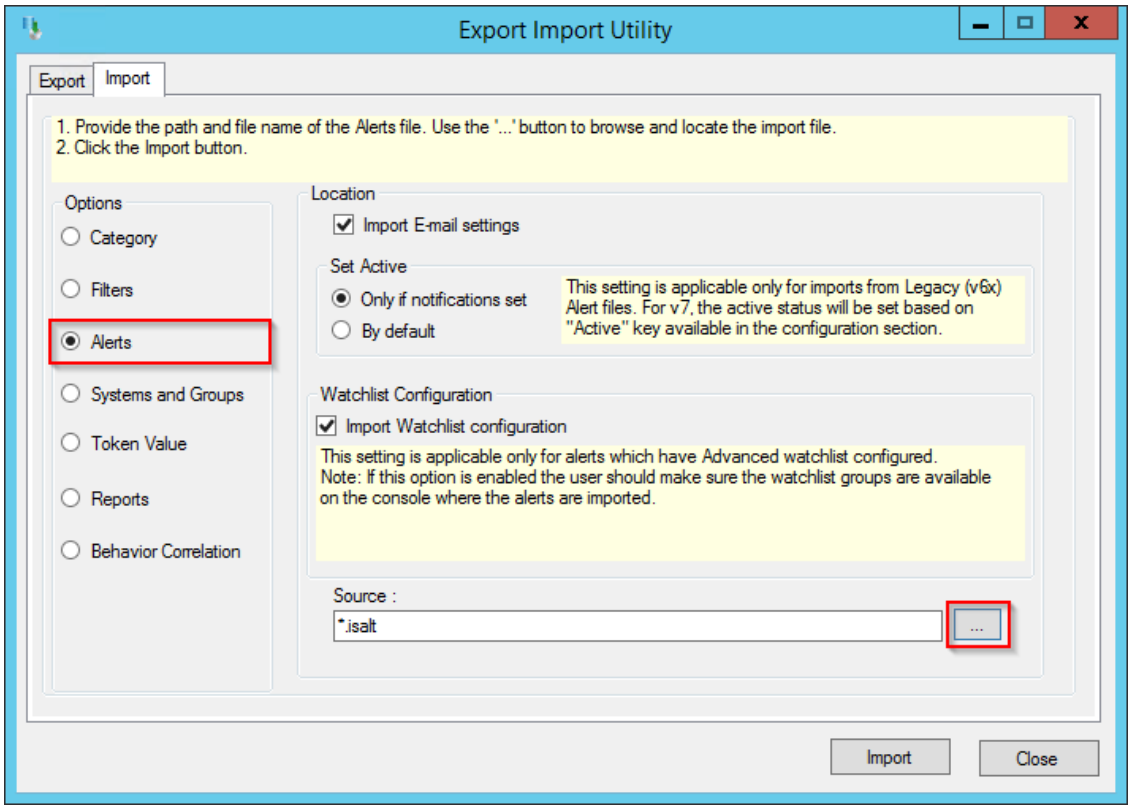

Figure 19

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

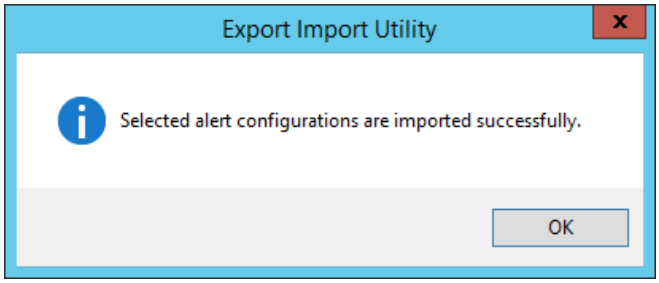

Figure 20

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

5.3 Knowledge Object

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

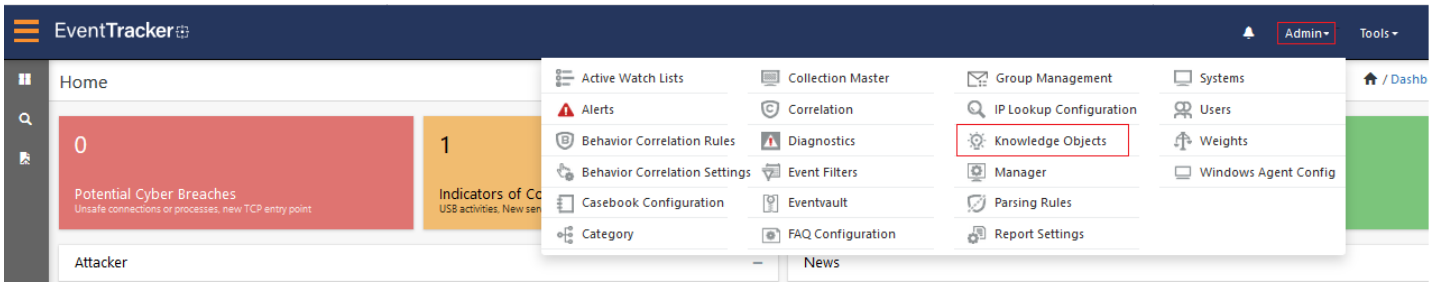

Figure 21

2. Click **Import** as highlighted in the below image.

Figure 22

3. Click **Browse**.

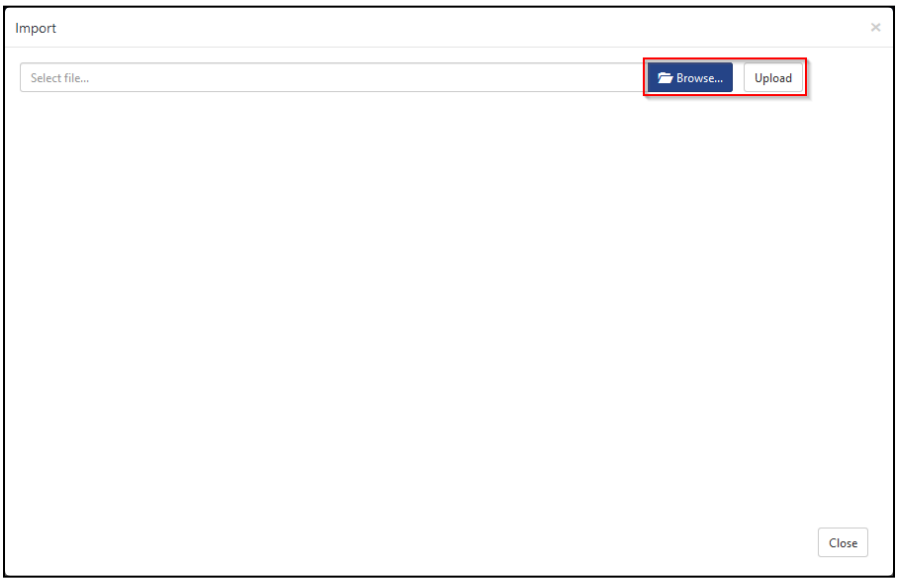

Figure 23

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

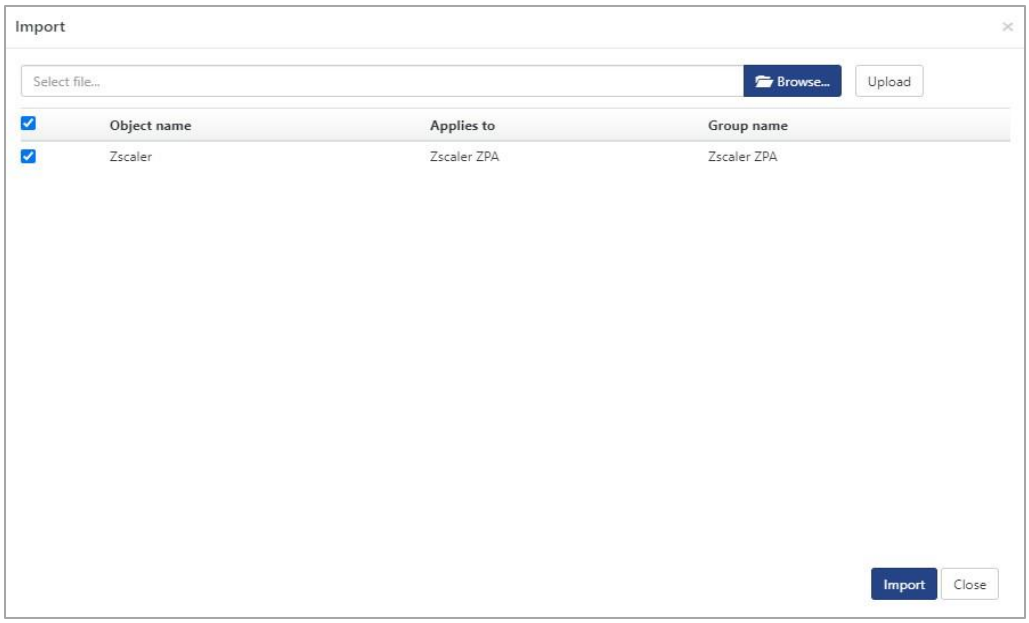

Figure 24

6. Knowledge objects are now imported successfully.

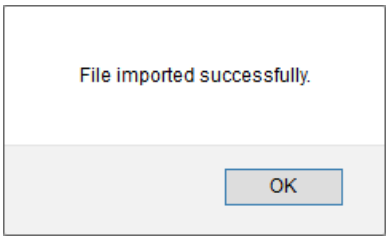

Figure 25

5.4 Report

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

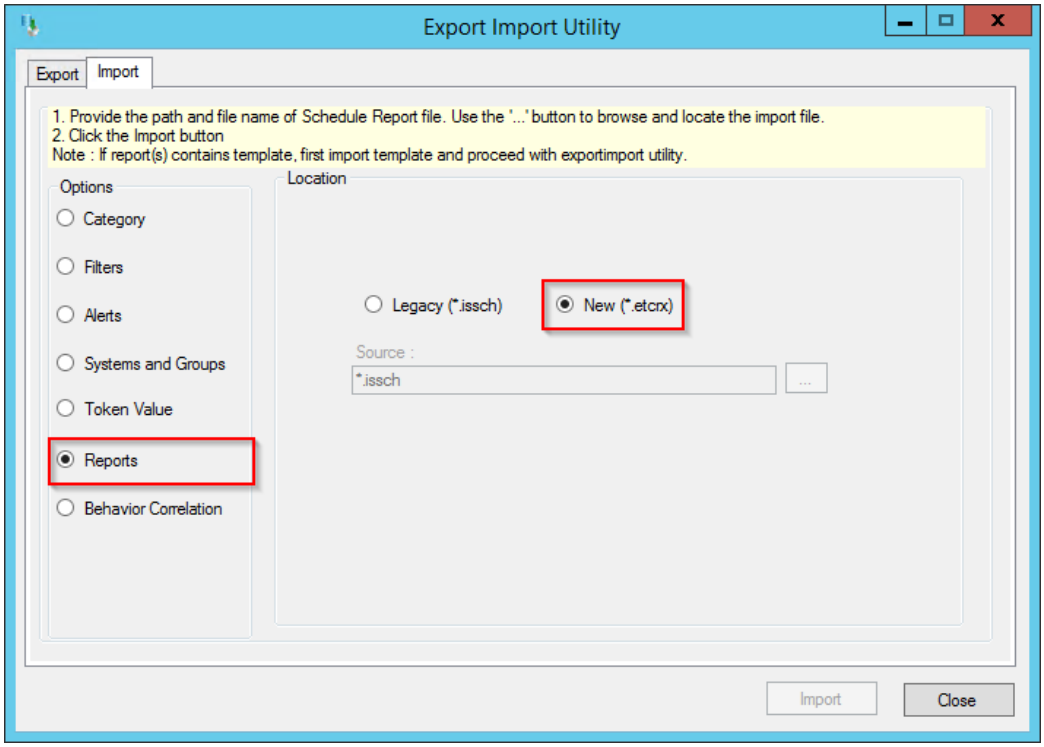

Figure 26

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

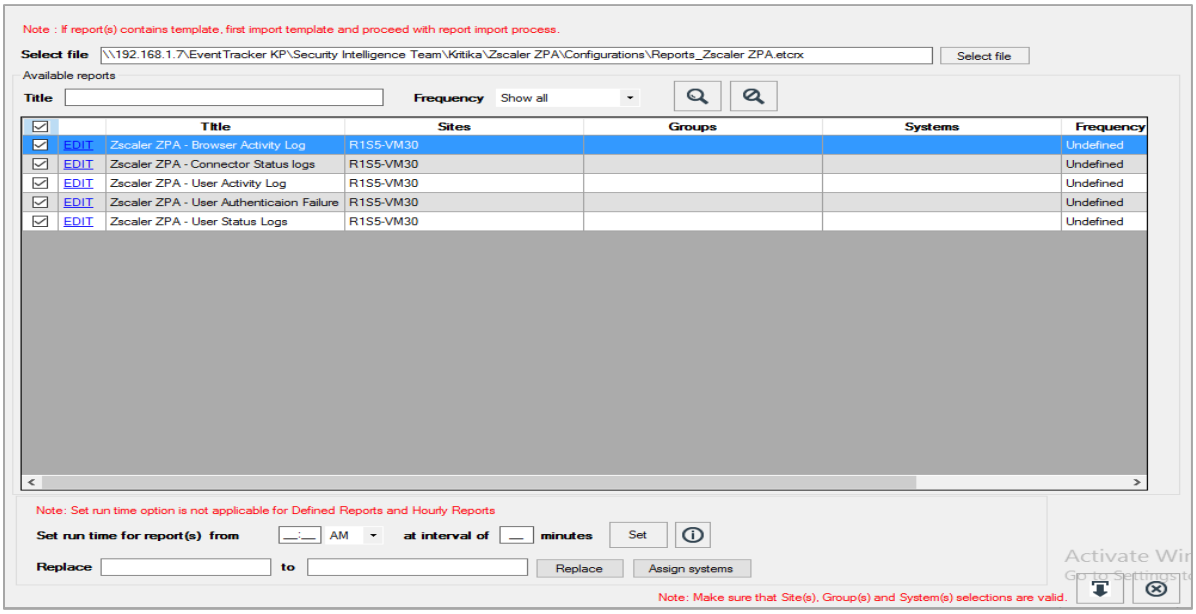

Figure 27

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

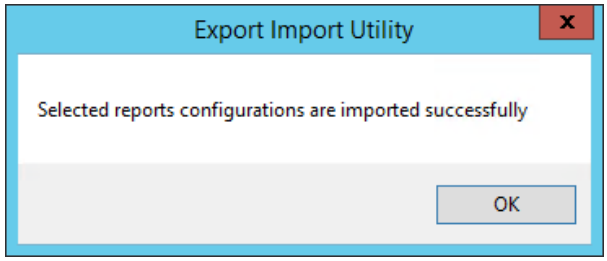

Figure 28

5.5 Dashboards

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

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

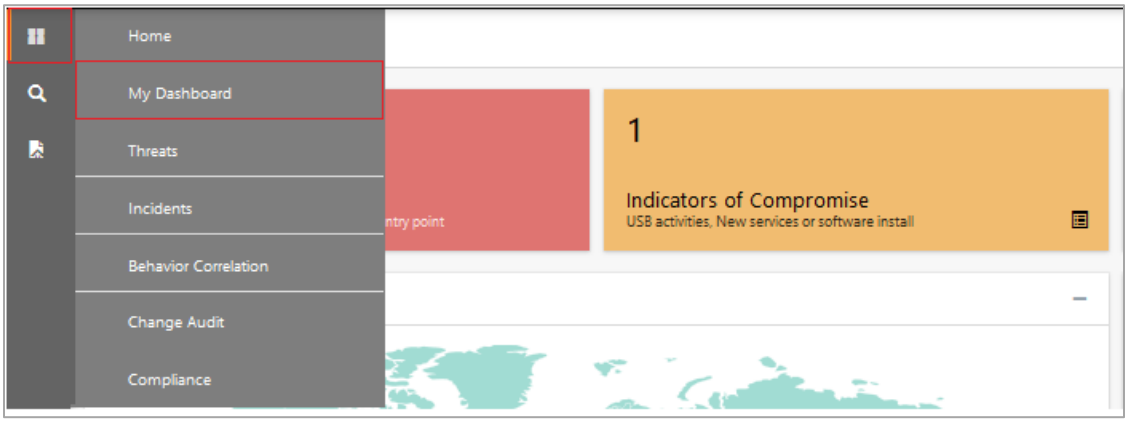

Figure 29

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

Figure 30

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

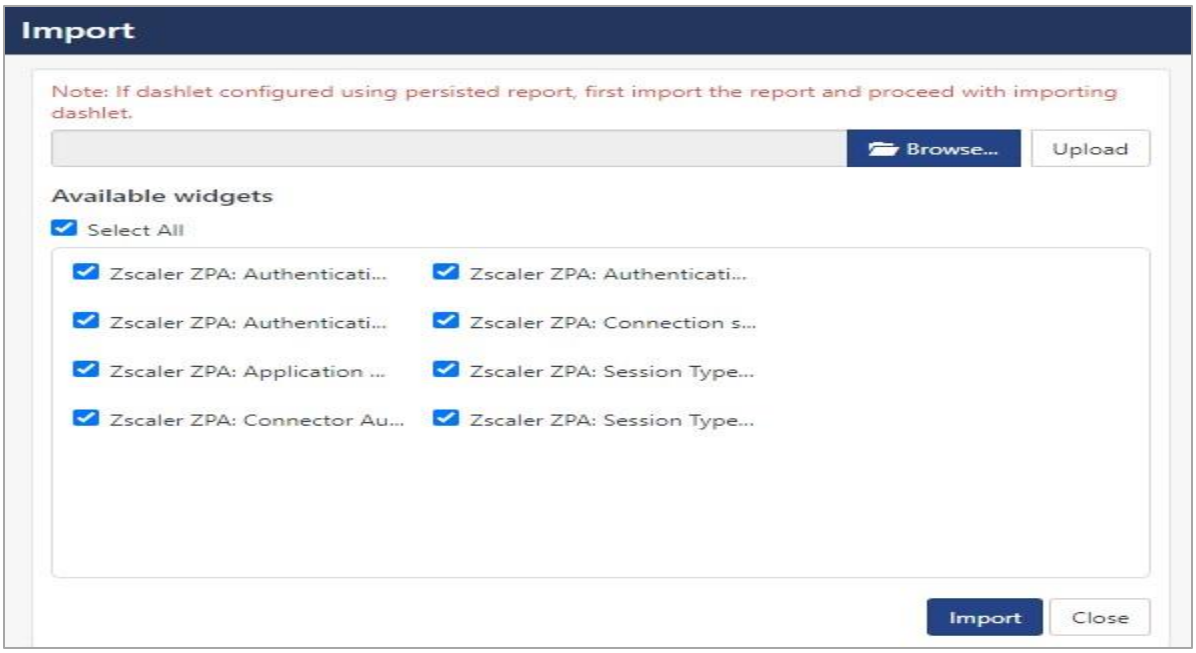

Figure 31

6. Import is now completed successfully.

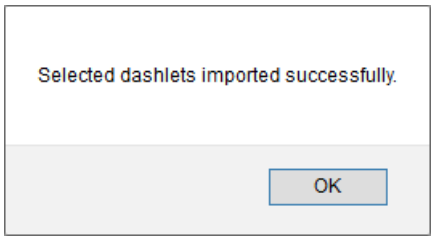

Figure 32

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

Figure 33

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

Figure 34

9. In **My Dashboard** page select to add dashlets.

Figure 35

10. Select imported dashlets and click **Add**.

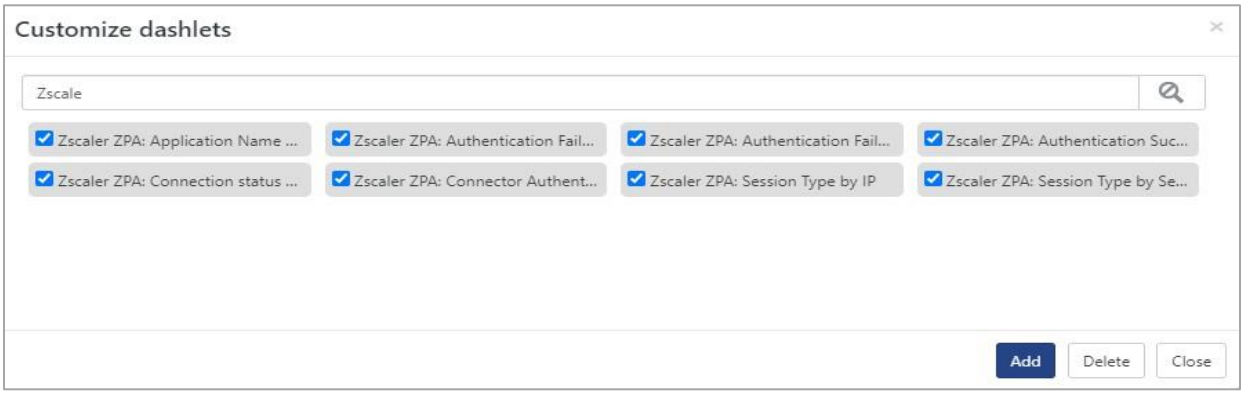

Figure 36

6. Verifying Zscaler ZPA knowledge pack in EventTracker

6.1 Category

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

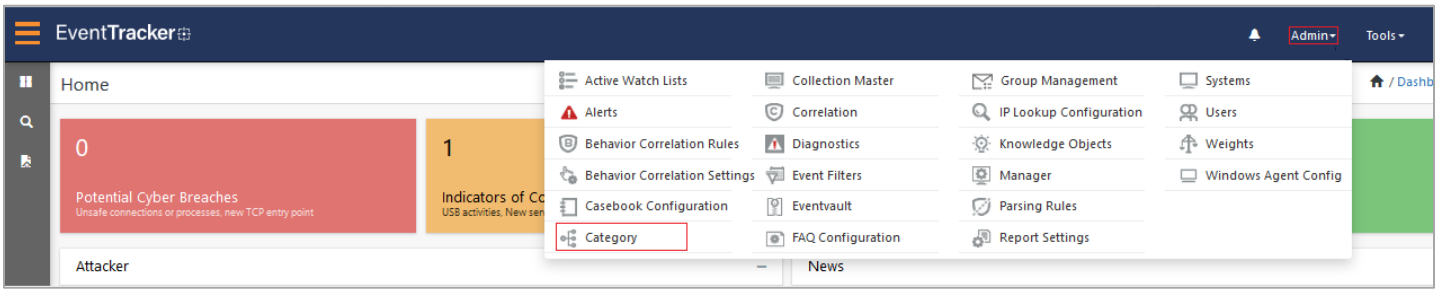

Figure 37

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

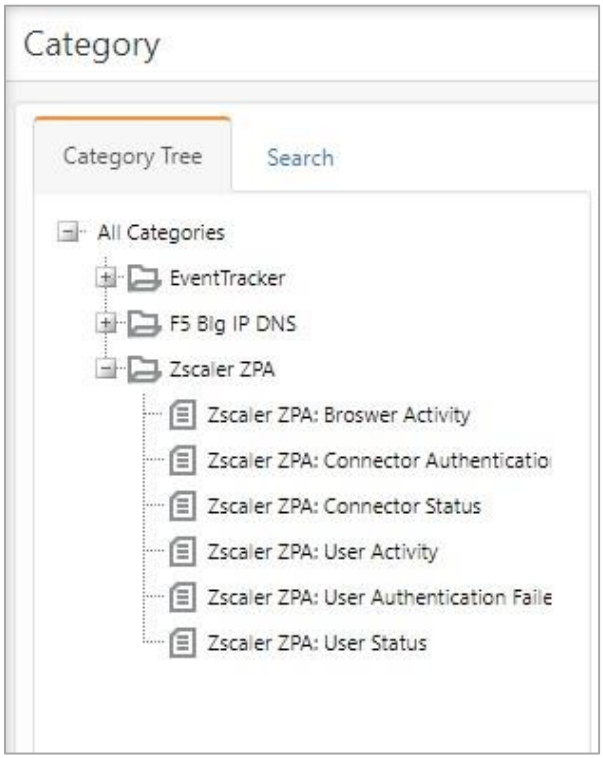

Figure 38

6.2 Alert

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

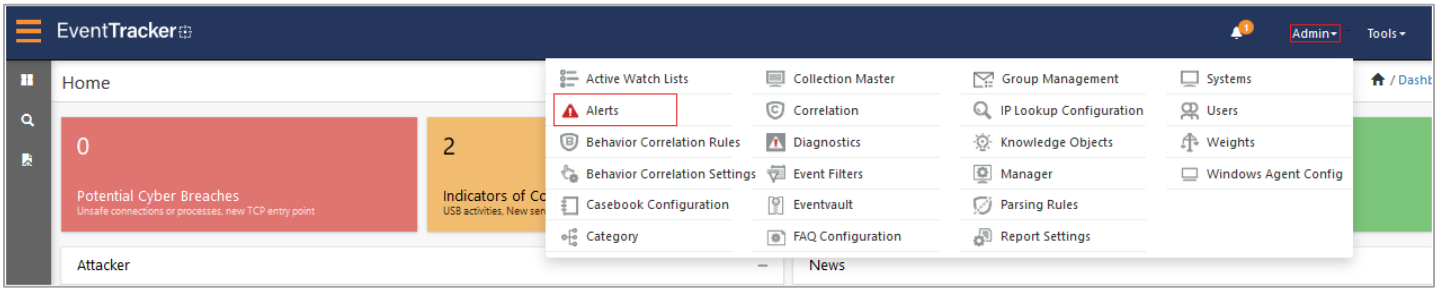

Figure 39

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

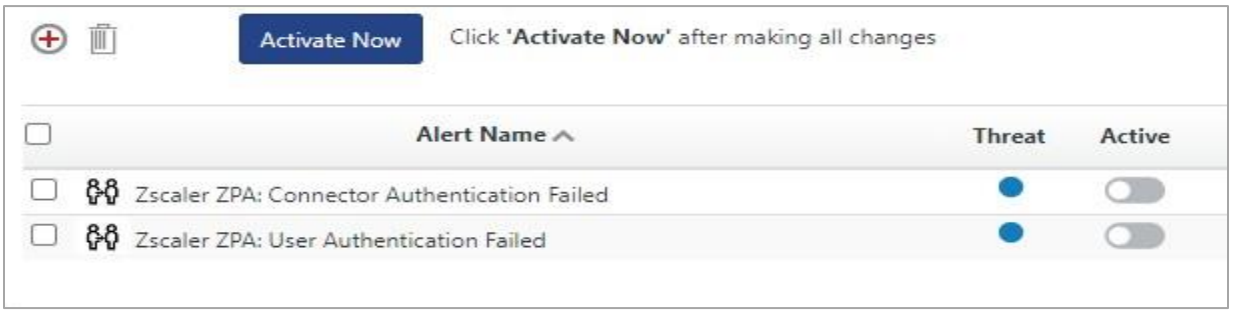

Figure 40

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

   EventTracker displays message box.

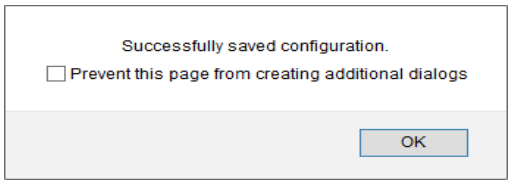

Figure 41

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.**

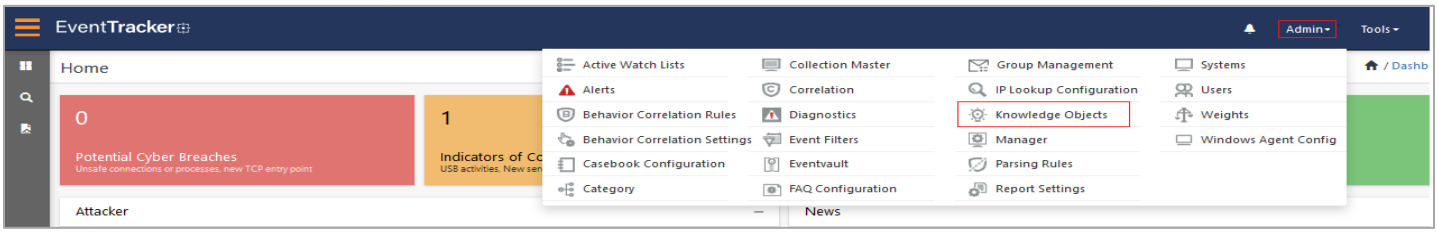

Figure 42

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

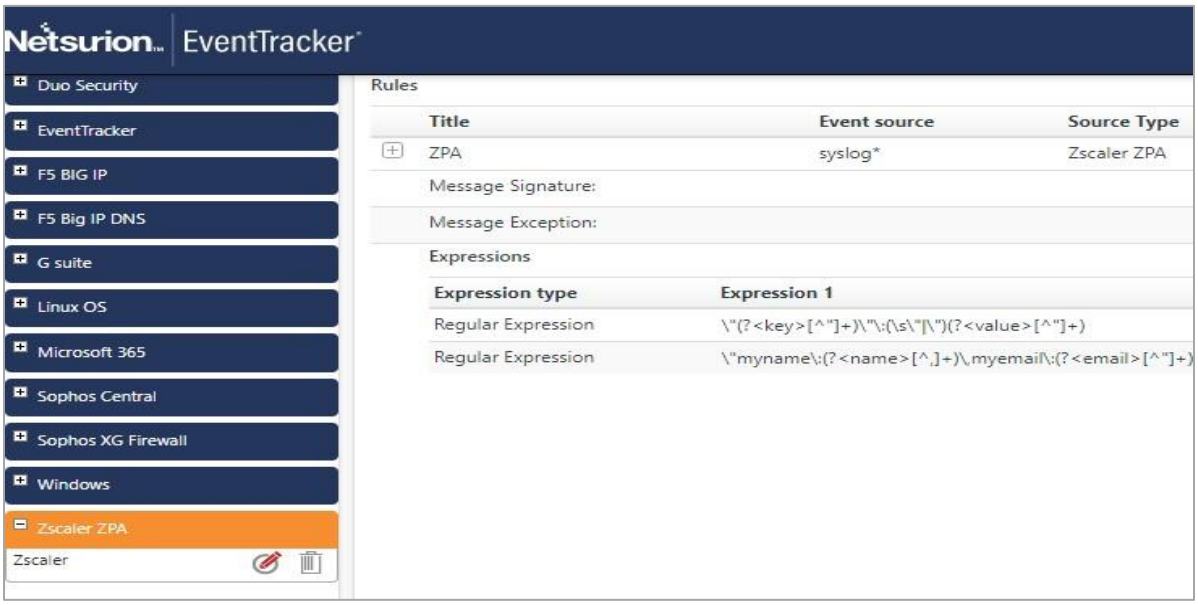

Figure 43

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**.

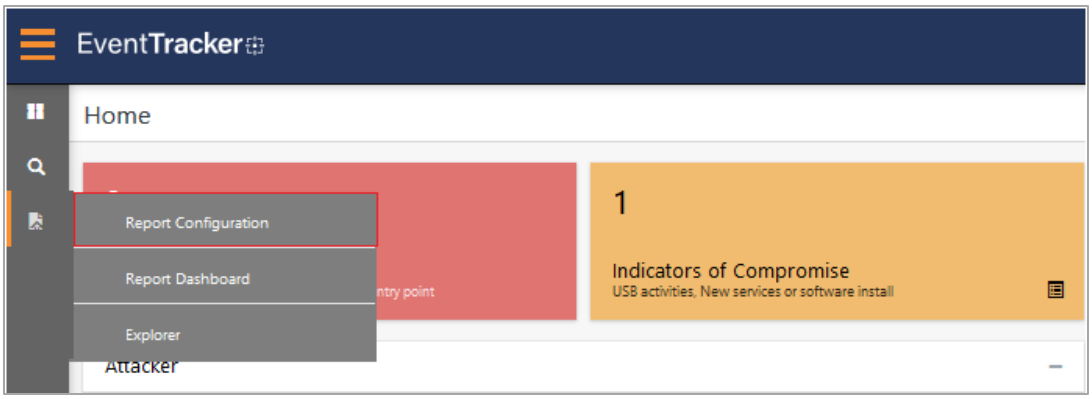

Figure 44

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

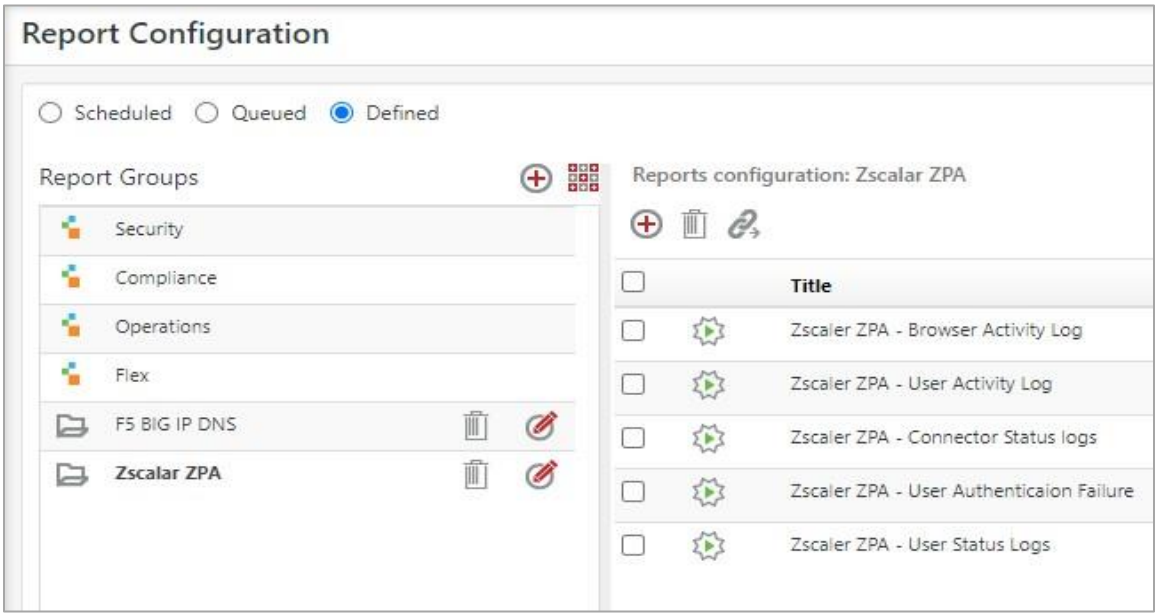

Figure 45

6.5 Dashboards

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

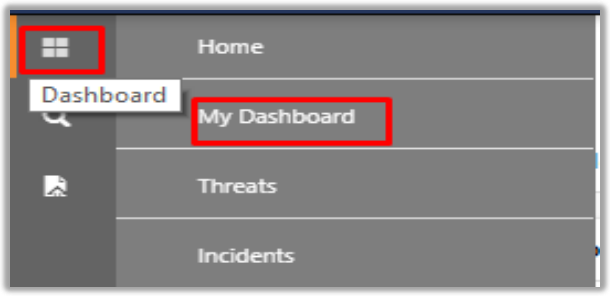

Figure 46

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

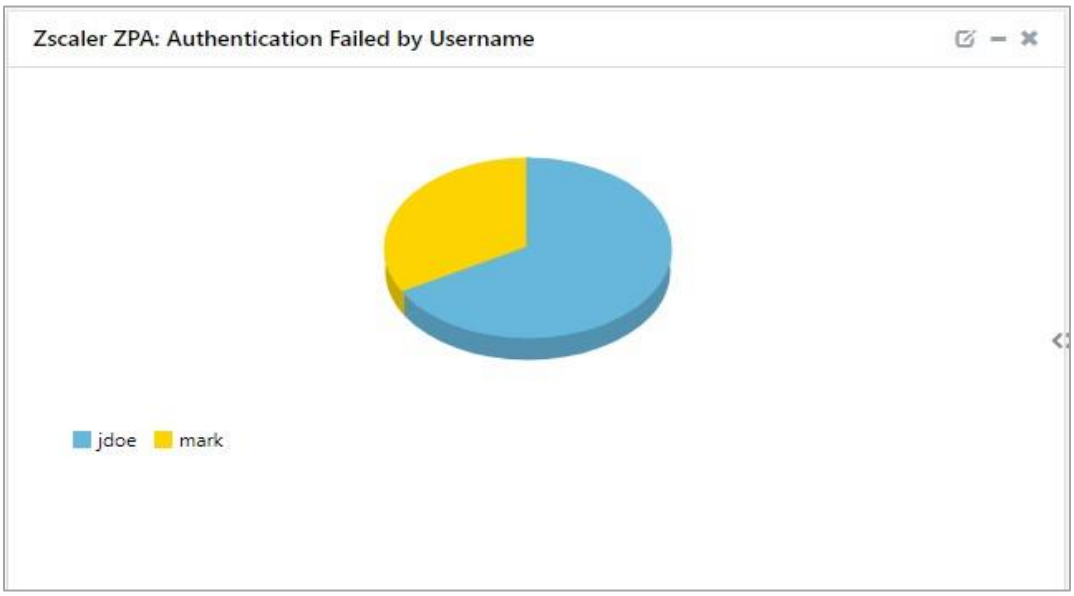

Figure 47