Integration Guide

Integrating Zix Email Threat Protection with EventTracker

EventTracker v9.x and above

Publication Date:

April 9, 2021

Abstract

This guide provides instructions to configure/ retrieve Zix Email Threat Protection activity logs via REST API method. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Zix Email Threat Protection.

Scope

The configuration details in this guide are consistent with EventTracker version v 9.x or above and Zix Email Threat Protection.

Audience

Administrators who are assigned the task to monitor Zix Email Threat Protection events using EventTracker.

Table of Contents

1. Overview

Zix/AppRiver Email Threat Protection (Zix ETP) provides multi-layered filtering that permits legitimate email while keeping out malicious threats such as phishing, impersonation, malware, ransomware, and spam-type messages.

EventTracker helps to monitor events from Zix Email Threat Protection. EventTracker reports, alerts, and dashboards will help you to analyze the activity logs such as, email traffic, or links clicked by users. Reports are provided to get a detailed summary of events during specific time. This contains critical information such as time of occurrence of events, user source IP and action taken on those events by Zix ETP.

Dashboards are basically a graphical representation of the events, which allows administrators to take an overview of key information found such as total number or percentage of traffic events or link protection events. And most importantly Alerts, such as, suspicious links clicked by user, will be triggered in real time to let administrators know of such foul activity performed within their networks.

2. Prerequisites

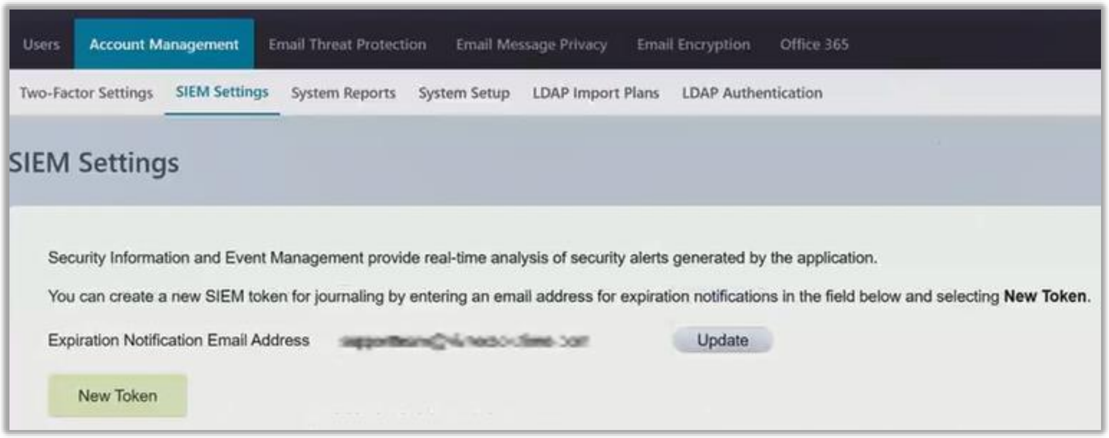
- EventTracker agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run powershell.
- Admin access to Zix/AppRiver Email Threat Protection platform.

3. Configuring Zix ETP to forward logs to EventTracker

The steps provided below will help to configure the EventTracker to receive specific events related to email traffic and links clicked by using Zix Email Threat Protection REST API.

3.1 Collecting Token

1. Login into your Zix management platform using admin account.
2. Navigate to **Account Management.** This contains **SIEM settings** and click **New Token**.



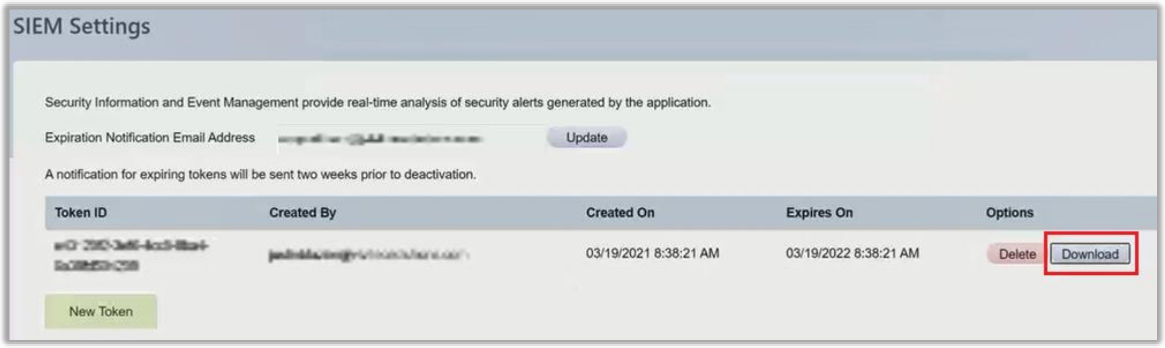
SIEM Settings

Security Information and Event Management provide real-time analysis of security alerts generated by the application.

You can create a new SIEM token for journaling by entering an email address for expiration notifications in the field below and selecting **New Token**.

Expiration Notification Email Address [redacted]

3. Once you have generated a new token, **Download** it.



SIEM Settings

Security Information and Event Management provide real-time analysis of security alerts generated by the application.

Expiration Notification Email Address [redacted]

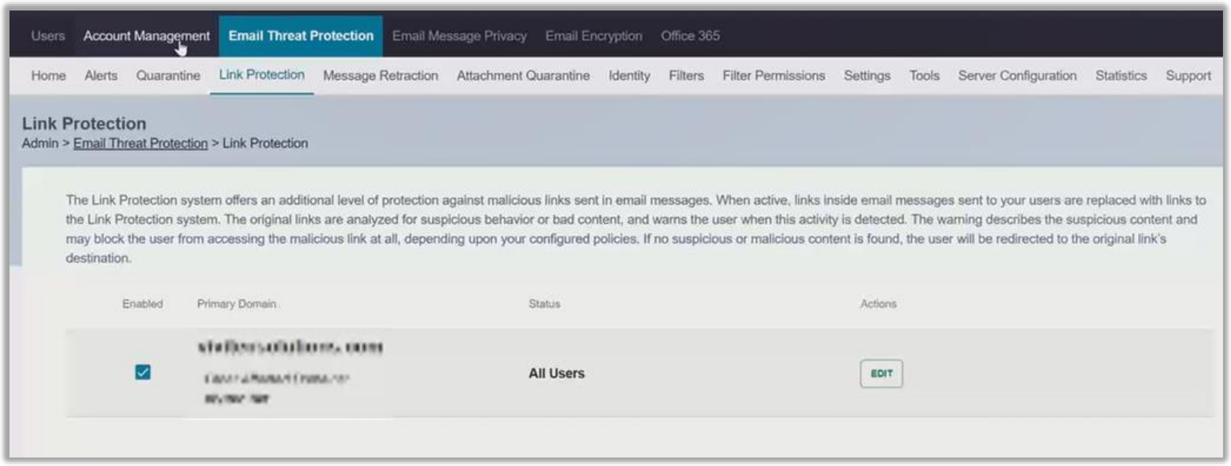
A notification for expiring tokens will be sent two weeks prior to deactivation.

Token ID	Created By	Created On	Expires On	Options
[redacted]	[redacted]	03/19/2021 8:38:21 AM	03/19/2022 8:38:21 AM	Delete Download

4. Collect/Save the newly created **Token**, you will need this token for later use.

3.2 Enabling Link Protection

1. In your Zix portal, navigate to **Email Threat Protection > Link Protection**.
2. Put a check on the **Enable** button.



Link Protection

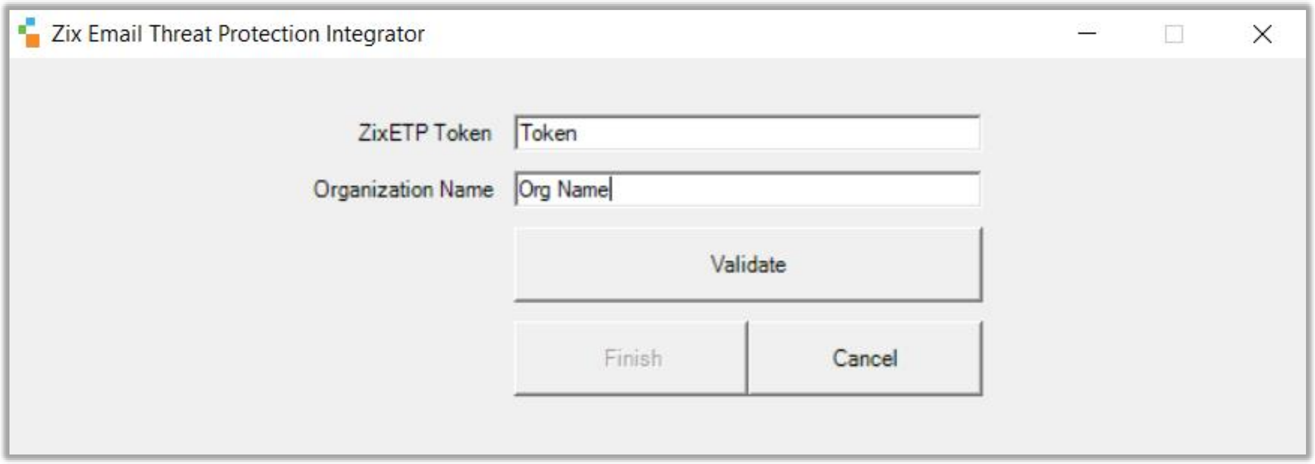
Admin > Email Threat Protection > Link Protection

The Link Protection system offers an additional level of protection against malicious links sent in email messages. When active, links inside email messages sent to your users are replaced with links to the Link Protection system. The original links are analyzed for suspicious behavior or bad content, and warns the user when this activity is detected. The warning describes the suspicious content and may block the user from accessing the malicious link at all, depending upon your configured policies. If no suspicious or malicious content is found, the user will be redirected to the original link's destination.

Enabled	Primary Domain	Status	Actions
☑	[redacted]	All Users	EDIT

3.3 Configuring EventTracker Zix Email Threat Protection Integrator

1. Get the **Zix Email Threat Protection Integrator** executable file: https://downloads.eventtracker.com/kp-integrator/ZixETPIntegrator.exe
2. Once the executable application is received, right click on the file, and select **Run as Administrator**.
3. In the dialog box, enter your Zix **Token** (as created in previous steps), and your **organization name** and click on the **Validate** button to verify the credentials.



Zix Email Threat Protection Integrator

ZixETP Token: Token

Organization Name: Org Name

4. On successful verification, a pop window will appear with a message: **Credential Validated Successfully**.
5. Click on the **Finish** button to complete the integration process.

3.4 Error Codes

The API has a few different errors that a customer may come across, all of which are documented in the SIEM API document. Here are some errors that may occur:

- **Token has been deleted**: This occurs when the token provided in the request header is no longer active. Log into HSP and create a new one to use with the request.
- **Client is not active**: The Client referenced in the token provided in the request header has been cancelled. This should not happen unless the customer was cancelled in HSP.
- **Begin time is too old**: The epoch value for “from=” in the request is more than 7 days in the past.
- **Range too wide**: The difference between the “from=” value and the “to=” value if the request is more than 24 hours apart.
- **403 Forbidden**: No token was used or in the request or it has been tampered with.
- **Invalid Request**: Syntax of the request URL is likely bad.
- **404 – Not Found**: This can be due to an invalid format for the “from” or “to” parameters.
- **End Time before begin time**: Indicates the “From=” value is greater than the “to=” value.

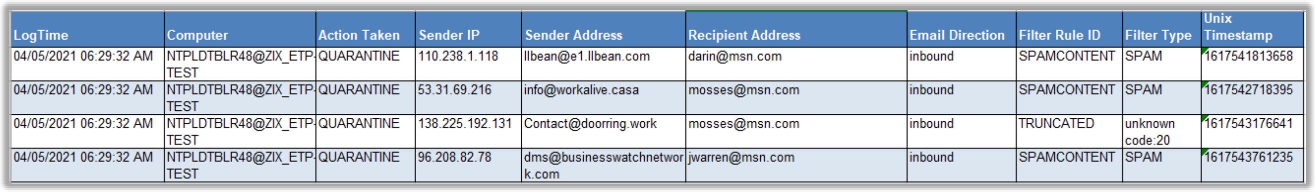
4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support **Zix ETP**.

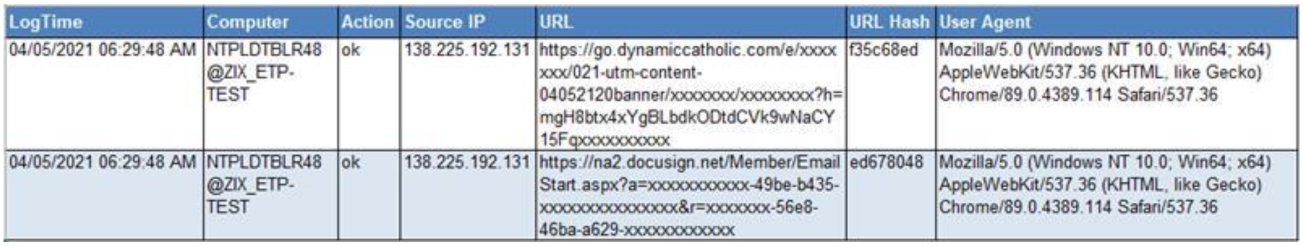
4.1 Reports

- **Zix ETP - Threat Protection Activities** – This report contains a detailed overview of email traffic events or threat protection events. This includes key information such as email direction, action the filter takes when triggered, source IP, sender, and recipient address.



LogTime	Computer	Action Taken	Sender IP	Sender Address	Recipient Address	Email Direction	Filter Rule ID	Filter Type	Unix Timestamp
04/05/2021 06:29:32 AM	NTPLDTBLR48@ZIX_ETP-TEST	QUARANTINE	110.238.1.118	llbean@e1.llbean.com	darin@msn.com	inbound	SPAMCONTENT	SPAM	1617541813658
04/05/2021 06:29:32 AM	NTPLDTBLR48@ZIX_ETP-TEST	QUARANTINE	53.31.69.216	info@workalive.casa	mosses@msn.com	inbound	SPAMCONTENT	SPAM	1617542718395
04/05/2021 06:29:32 AM	NTPLDTBLR48@ZIX_ETP-TEST	QUARANTINE	138.225.192.131	Contact@doorring.work	mosses@msn.com	inbound	TRUNCATED	unknown code:20	1617543176641
04/05/2021 06:29:32 AM	NTPLDTBLR48@ZIX_ETP-TEST	QUARANTINE	96.208.82.78	dms@businesswatchnetwork.com	jwarren@msn.com	inbound	SPAMCONTENT	SPAM	1617543761235

- **Zix ETP - Link Protection Activities** - This report contains a detailed overview of link protection events or events related to suspicious links clicked by user. This includes key information such as user source IP, the suspicious URL/ IOC, the user agent used, event datetime.



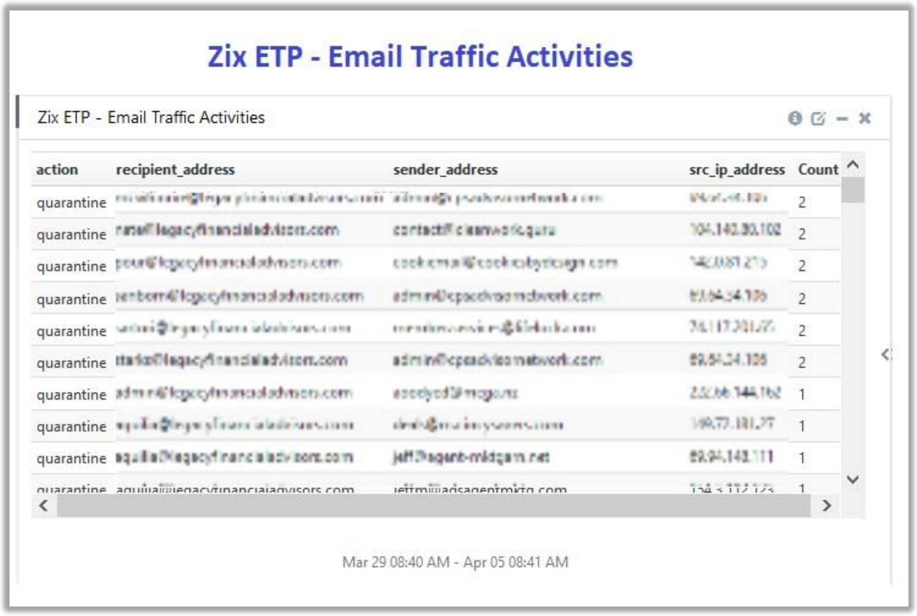
LogTime	Computer	Action	Source IP	URL	URL Hash	User Agent
04/05/2021 06:29:48 AM	NTPLDTBLR48@ZIX_ETP-TEST	ok	138.225.192.131	https://go.dynamiccatholic.com/e/xxxxxxx/021-utm-content-04052120banner/xxxxxxx/xxxxxxxx?h=mgH8btx4xYgBLbdkODtdCVk9wNaCY15Fqxxxxxxxxxxx	f35c68ed	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
04/05/2021 06:29:48 AM	NTPLDTBLR48@ZIX_ETP-TEST	ok	138.225.192.131	https://na2.docusign.net/Member/EmailStart.aspx?a=xxxxxxxxxxxx-49be-b435-xxxxxxxxxxxxxxx&r=xxxxxxx-56e8-46ba-a629-xxxxxxxxxxxx	ed678048	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36

4.2 Alerts

- **Zix ETP: A suspicious link or URL has been identified -** This alert is triggered when a user clicks any link or URL which turns out to be a source of suspicious activity.

4.3 Dashboards

- **Zix ETP - Email Traffic Activities**



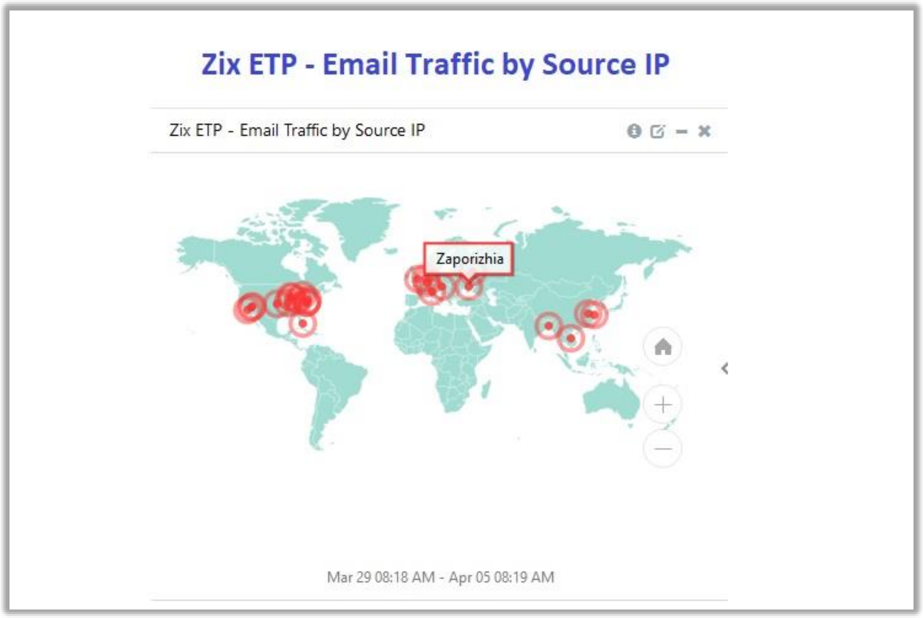
Zix ETP - Email Traffic Activities

Zix ETP - Email Traffic Activities

action	recipient_address	sender_address	src_ip_address	Count
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	2
quarantine	[redacted]	[redacted]	[redacted]	1
quarantine	[redacted]	[redacted]	[redacted]	1
quarantine	[redacted]	[redacted]	[redacted]	1
quarantine	[redacted]	[redacted]	[redacted]	1

Mar 29 08:40 AM - Apr 05 08:41 AM

- **Zix ETP - Email Traffic by Source IP**

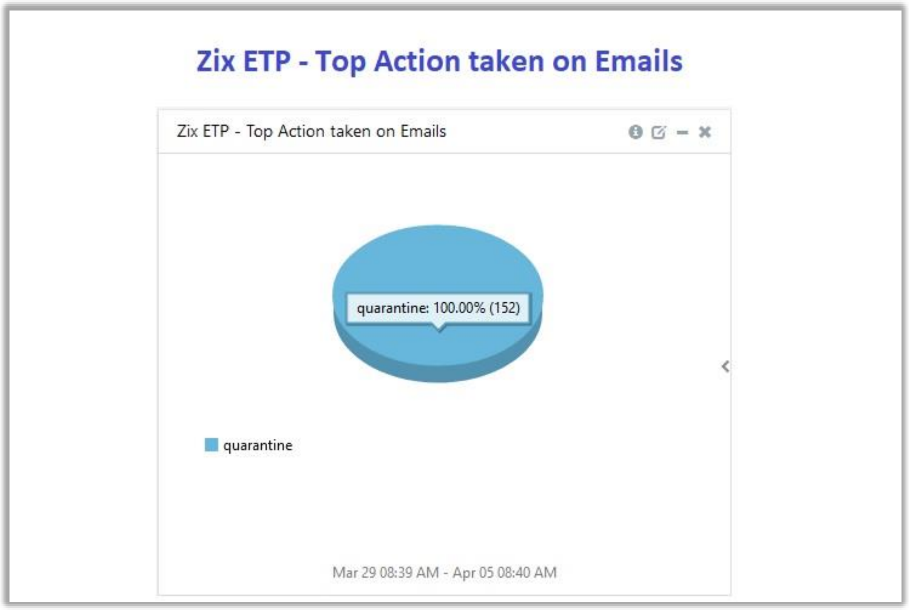


Zix ETP - Email Traffic by Source IP

Zix ETP - Email Traffic by Source IP

Mar 29 08:18 AM - Apr 05 08:19 AM

- **Zix ETP - Top Action taken on Emails**

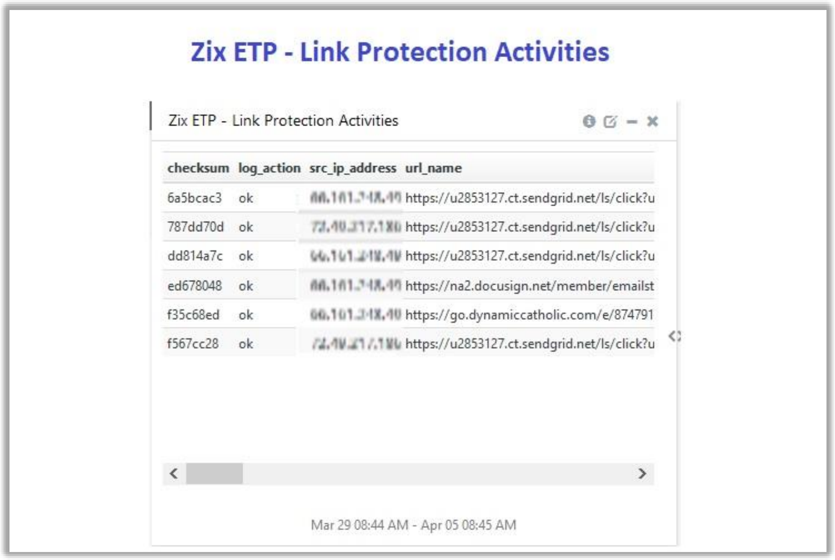


Zix ETP - Top Action taken on Emails

Zix ETP - Top Action taken on Emails

Mar 29 08:39 AM - Apr 05 08:40 AM

- **Zix ETP - Link Protection Activities**



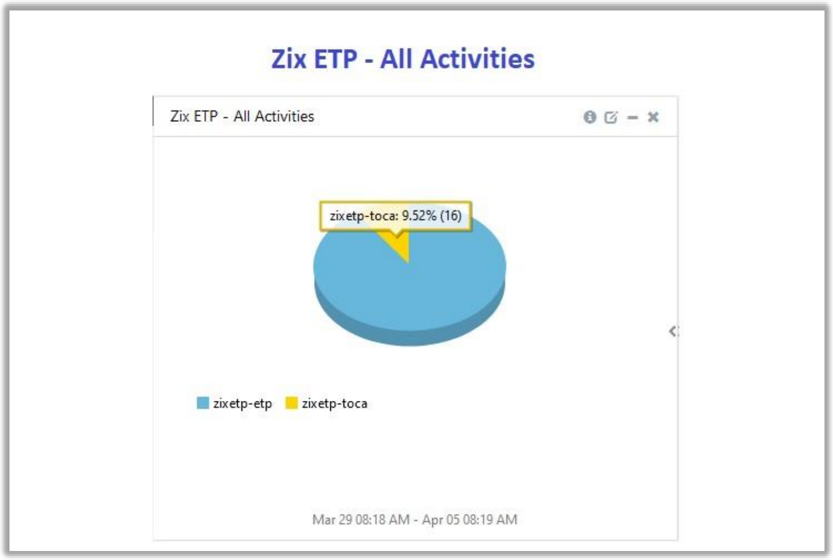
Zix ETP - Link Protection Activities

Zix ETP - Link Protection Activities

checksum	log_action	src_ip_address	url_name
6a5bcac3	ok	[redacted]	https://u2853127.ct.sendgrid.net/ls/click?u
787dd70d	ok	[redacted]	https://u2853127.ct.sendgrid.net/ls/click?u
dd814a7c	ok	[redacted]	https://u2853127.ct.sendgrid.net/ls/click?u
ed678048	ok	[redacted]	https://na2.docusign.net/member/emailst
f35c68ed	ok	[redacted]	https://go.dynamiccatholic.com/e/874791
f567cc28	ok	[redacted]	https://u2853127.ct.sendgrid.net/ls/click?u

Mar 29 08:44 AM - Apr 05 08:45 AM

- **Zix ETP - All Activities**



Zix ETP - All Activities

Zix ETP - All Activities

Mar 29 08:18 AM - Apr 05 08:19 AM

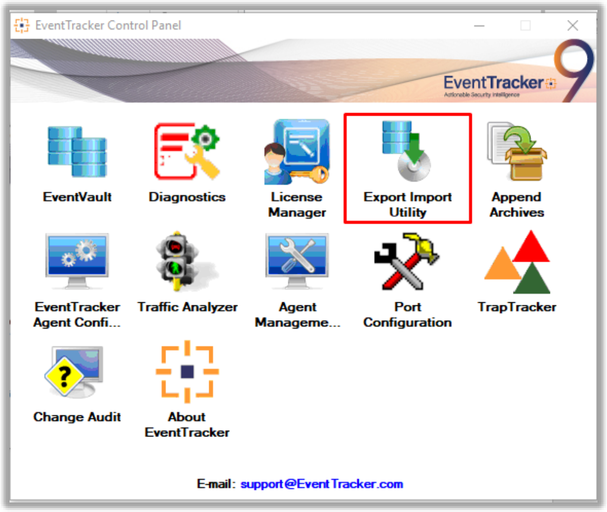
5. Importing Zix ETP Knowledge Pack into EventTracker

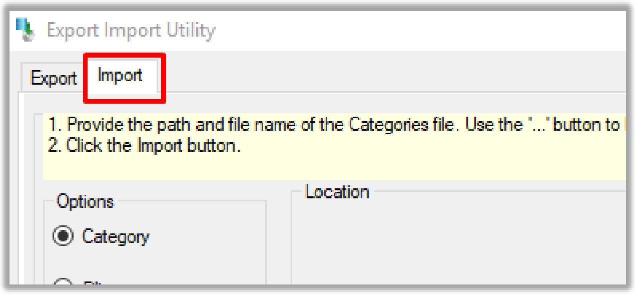
NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template
- Knowledge Objects
- Flex Reports
- Dashboard

1. Launch the **EventTracker Control Panel**.

2. Double click **Export-Import Utility**.





1. Provide the path and file name of the Categories file. Use the "..." button to
2. Click the Import button.

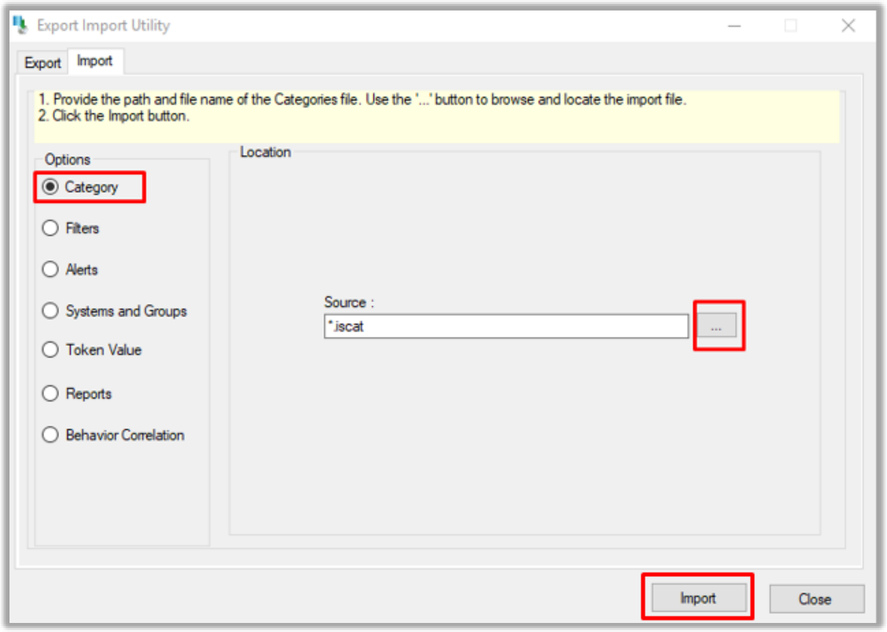
Options

● Category

3. Click the **Import** tab.

5.1 Categories

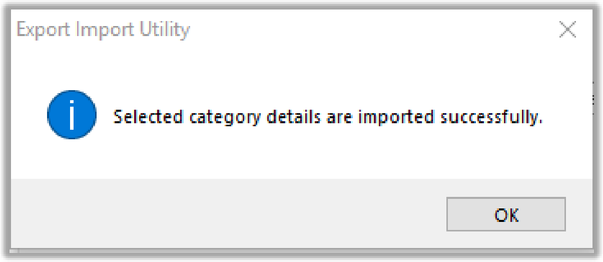
1. Once you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click Browse. ...
2. Navigate to the knowledge pack folder and select the file with extension **".iscat", e.g., "Categories_ZixETP.iscat"** and then click on the **Import** button.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Source : *.iscat

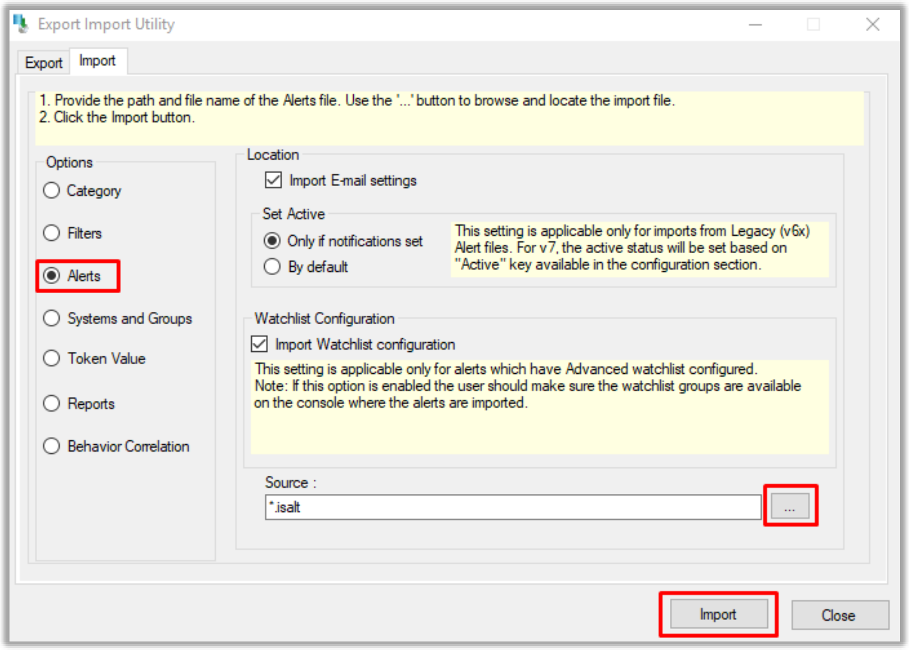
EventTracker displays a success message:



Selected category details are imported successfully.

5.2 Alerts

1. Once you have opened **Export Import Utility** via **EventTracker Control Panel**, click **Alert** option, and then click Browse. ...
2. Navigate to the knowledge pack folder and select the file with extension "**.isalt**", **e.g.**, **Alerts_ZixETP.isalt** and then click on the **Import** button.

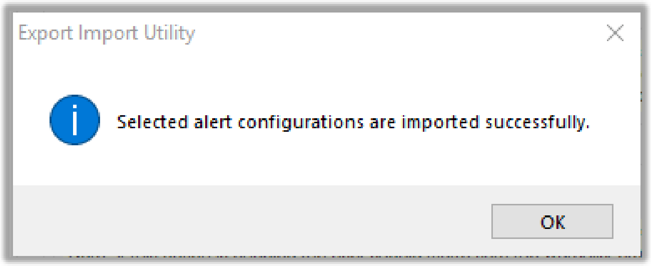


1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

EventTracker displays a success message:

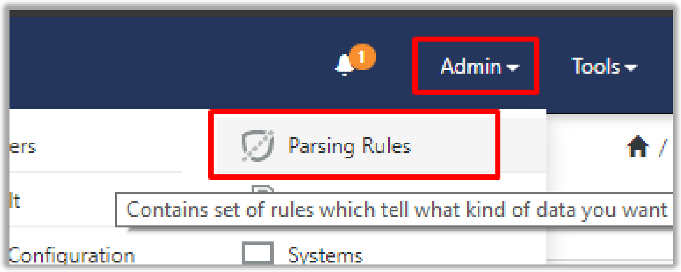


Selected alert configurations are imported successfully.

5.3 Token Template

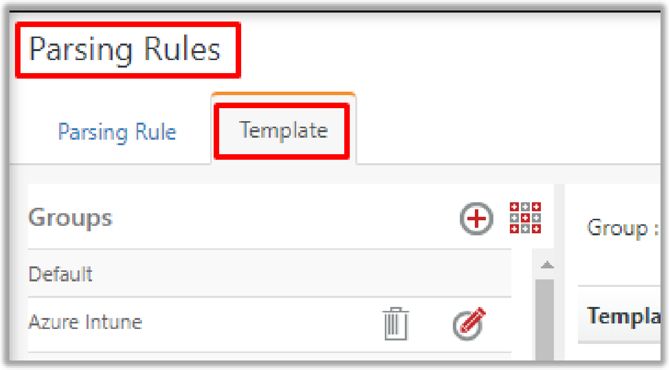
For importing **Token Template**, navigate to **EventTracker manager** web interface.

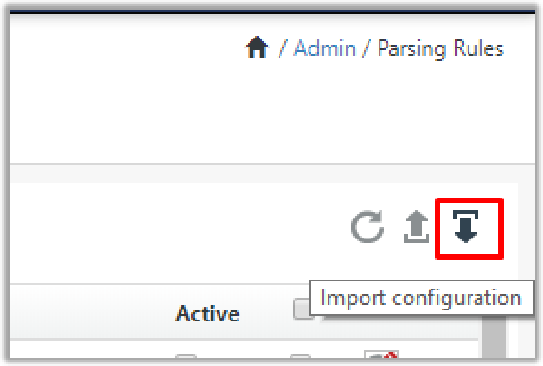
1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface:



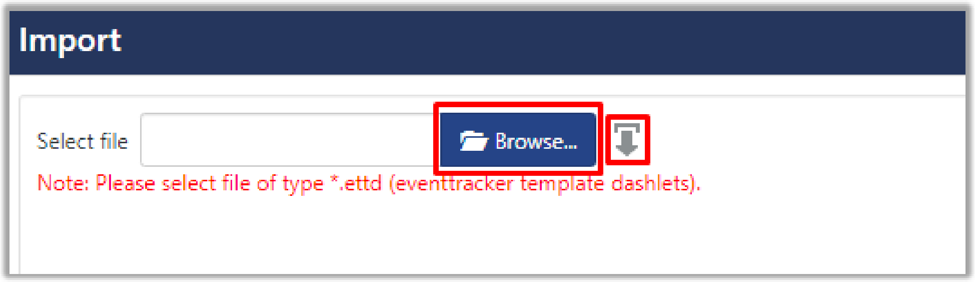
Contains set of rules which tell what kind of data you want

2. Click the **Template** tab and then click the **Import Configuration** button.





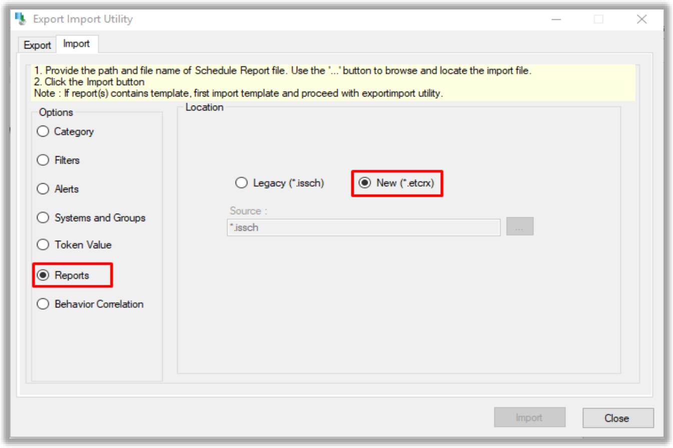
3. Click **Browse** button and navigate to the knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where "**.ettd**", **e.g.,** "**Token Templates_ZixETP.ettd** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired template, and click **Import** button.



Note: Please select file of type *.ettd (eventtracker template dashlets).

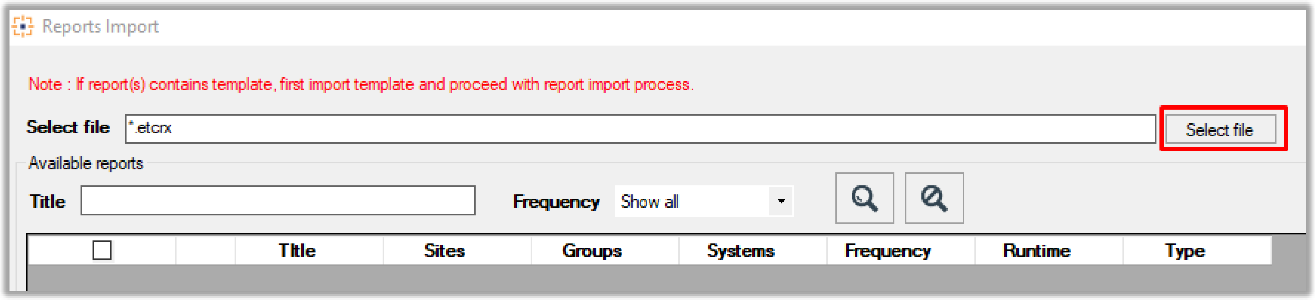
5.4 Reports

1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click **Reports** option, and Choose **New (*.etcrx)**:



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

2. Once you have selected **New (*.etcrx)**, a new pop-up window will appear. Click on the **Select File** button and navigate to the file path with a file having the extension "**.etcrx**", **e.g., Reports_ ZixETP.etcrx.**



Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file *.etcrx

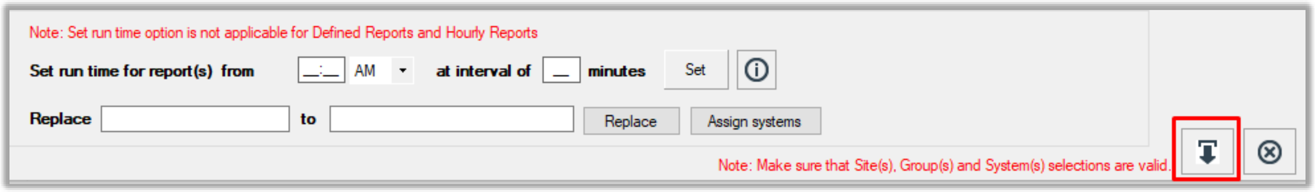
Available reports

Title

Frequency Show all

☐	Title	Sites	Groups	Systems	Frequency	Runtime	Type

3. Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import** button:

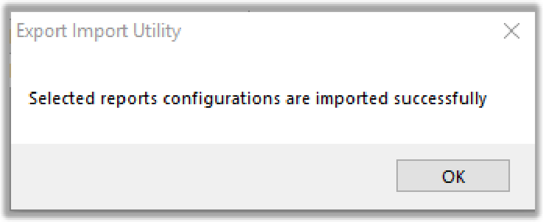


Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

4. EventTracker displays a success message:

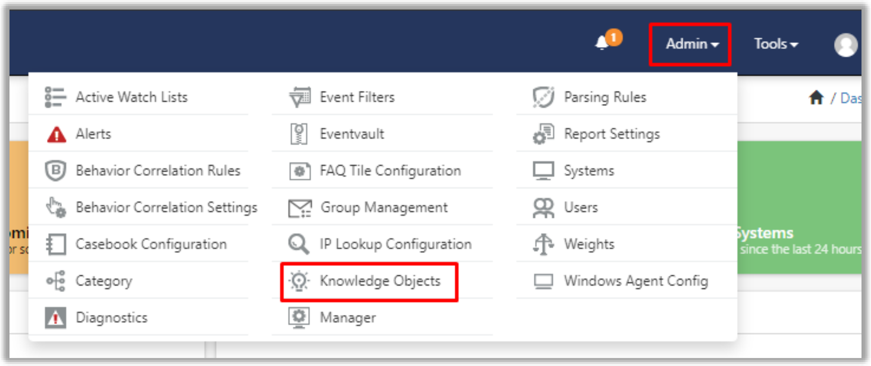


Export Import Utility

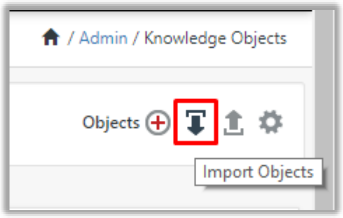
Selected reports configurations are imported successfully

5.5 Knowledge Object

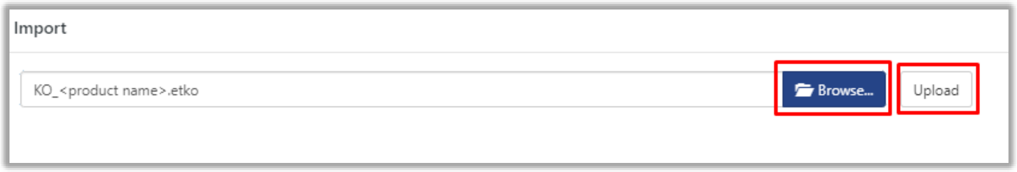
1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager page.



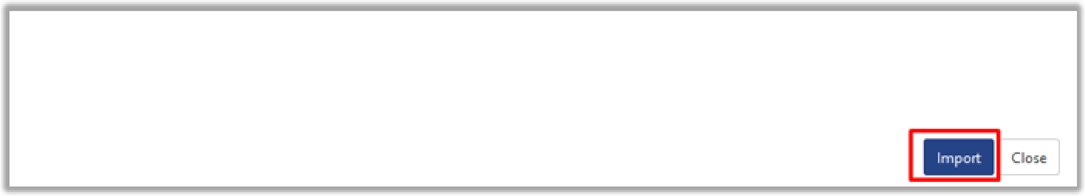
2. Click on the **import object** icon:



3. A pop-up box appears, click Browse in that and navigate to knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) with the extension **".etko", e.g., KO_ZixETP.etko** and then click **Upload**.

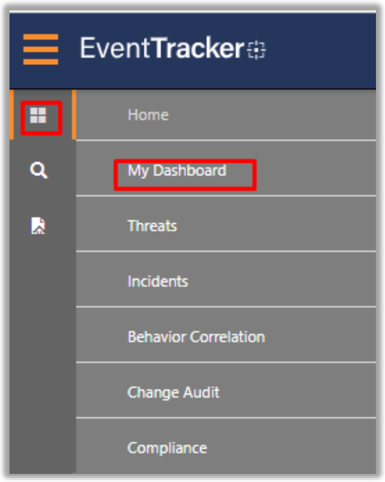


4. List of available knowledge object will appear. Select the relevant files and click on **Import** button:

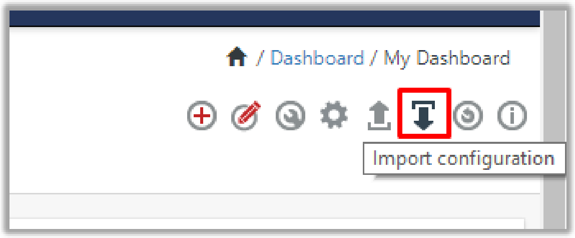


5.6 Dashboard

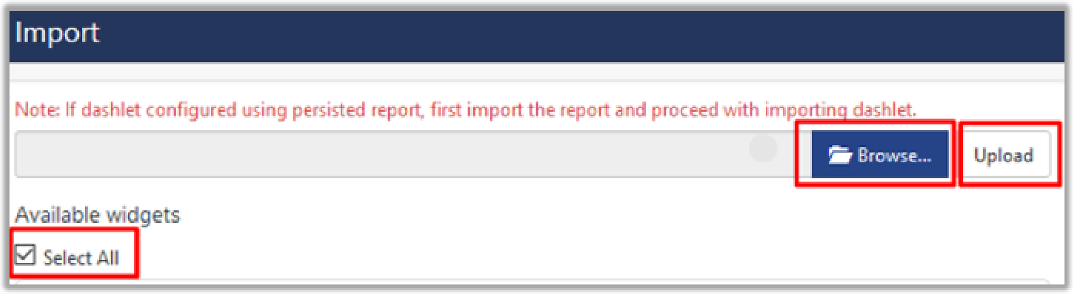
1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.



3. In **My Dashboard**, Click on **Import Button**:

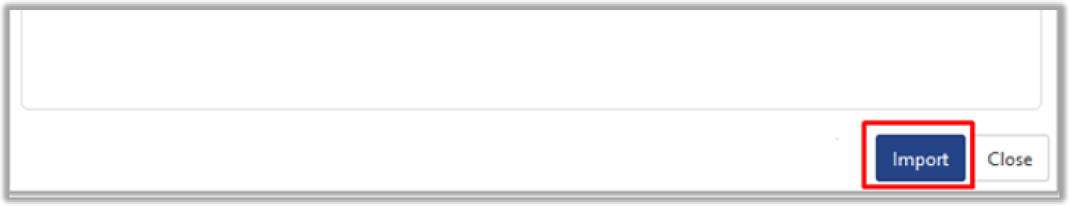


4. Select the **browse** button and navigate to knowledge pack folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where **.etwd, e.g., Dashboards_ZixETP.etwd** is saved and click on **Upload** button.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click on **Import** Button.



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

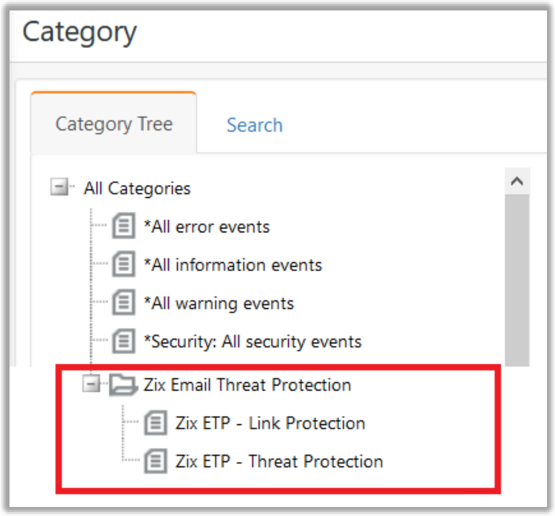
☑ Select All



6. Verifying Zix ETP Knowledge Pack in EventTracker

6.1 Categories

1. Login to **EventTracker**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Zix Email Threat Protection** group folder to view the imported categories.



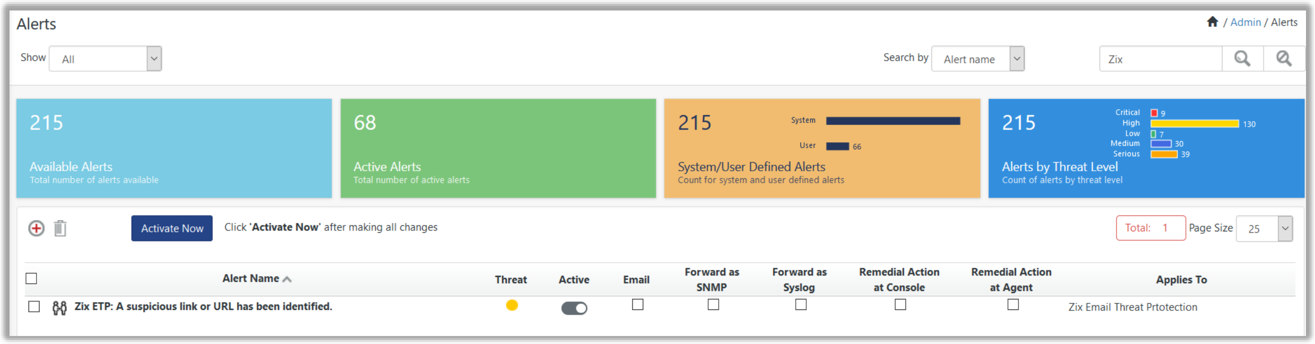
Category

- All Categories
  - *All error events
  - *All information events
  - *All warning events
  - *Security: All security events
  - Zix Email Threat Protection
    - Zix ETP - Link Protection
    - Zix ETP - Threat Protection

6.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **Zix** and then click the **Search** button.

   EventTracker displays an alert of **Zix ETP.**



Alerts

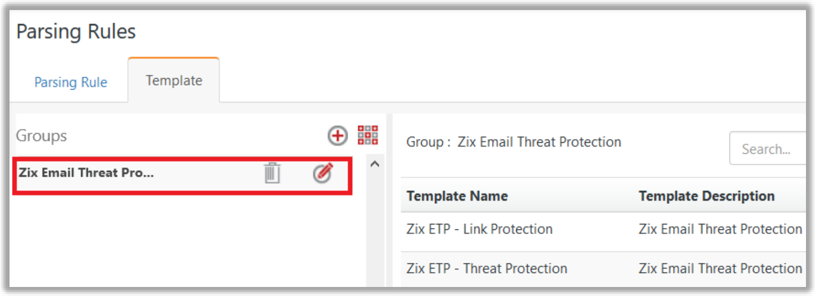
Click '**Activate Now**' after making all changes

Total: 1 Page Size 25

□	Alert Name	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Zix ETP: A suspicious link or URL has been identified.	●		□	□	□	□	□	Zix Email Threat Prtotection

6.3 Token Value

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Template.**
2. In the **Template** tab, click on the **Zix Email Threat Protection** group folder to view the imported Token Values.



Parsing Rules

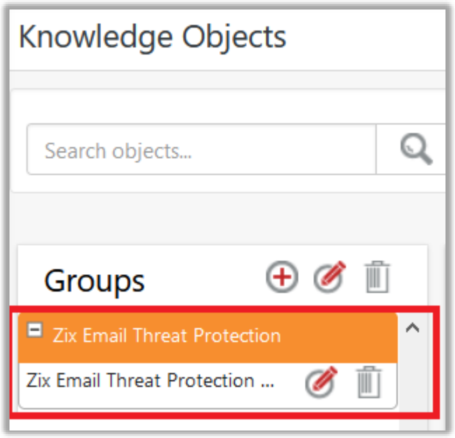
Group : Zix Email Threat Protection

Template Name	Template Description
Zix ETP - Link Protection	Zix Email Threat Protection
Zix ETP - Threat Protection	Zix Email Threat Protection

6.4 Knowledge Objects

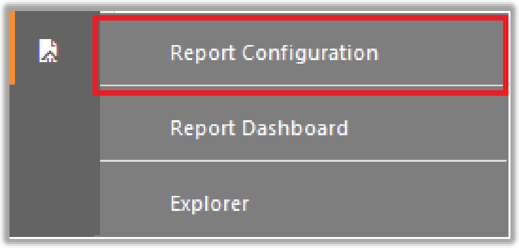
1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**

2. In the **Knowledge Object** tree, expand the **Zix Email Threat Protection Events** group folder to view the imported Knowledge objects.

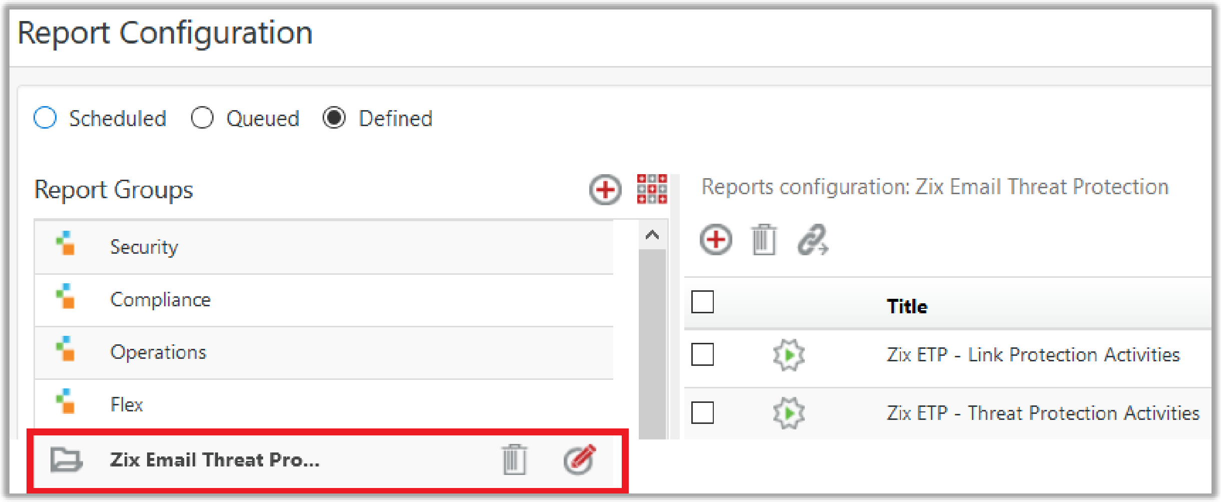


6.5 Reports

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



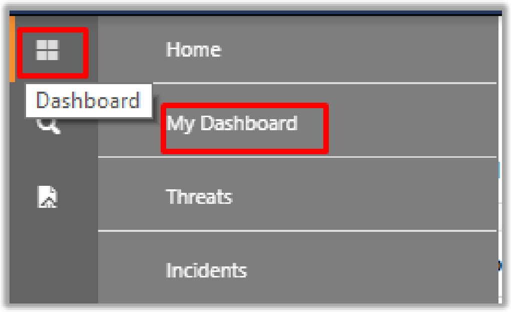
2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Zix Email Threat Protection** group folder to view the imported reports.



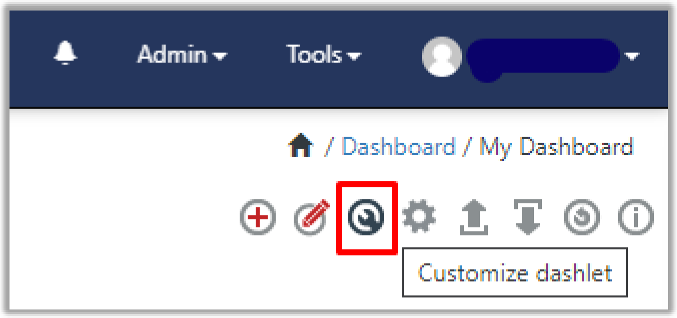
□	Title
□	Zix ETP - Link Protection Activities
□	Zix ETP - Threat Protection Activities

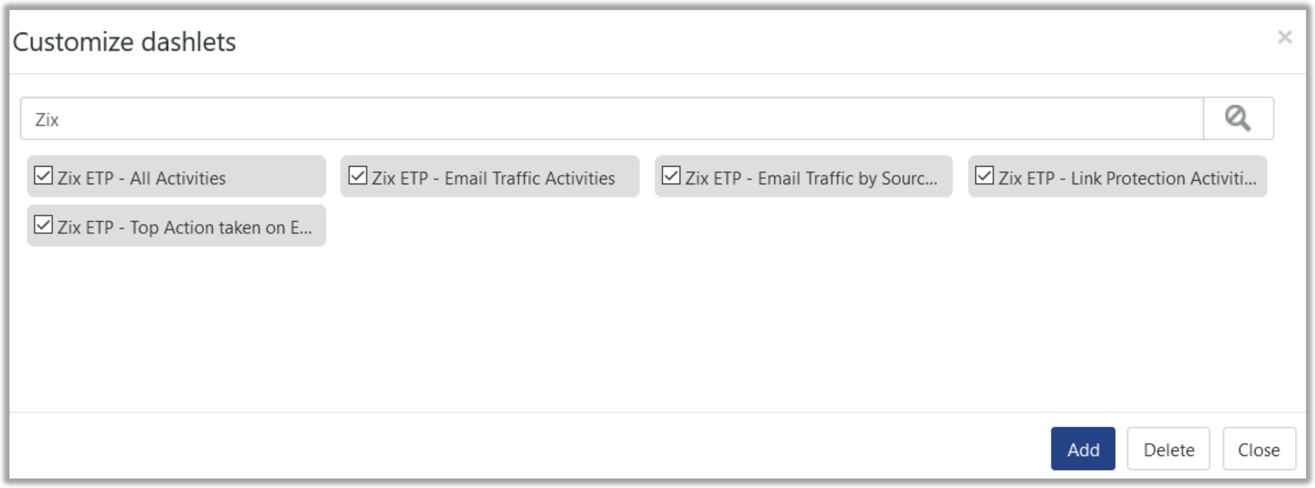
6.6 Dashboard

1. In the EventTracker web interface, Click on Home Button ⊞ and select **My Dashboard**.



2. Select **Customize daslets** button and type **Zix** in the search bar.




Customize dashlets

Zix

☑ Zix ETP - All Activities
☑ Zix ETP - Email Traffic Activities
☑ Zix ETP - Email Traffic by Sourc...
☑ Zix ETP - Link Protection Activiti...
☑ Zix ETP - Top Action taken on E...

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)

EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)

EventTracker Essentials SOC: 877-333-1433 (Option 4)

EventTracker Software Support: 877-333-1433 (Option 5)

https://www.netsurion.com/eventtracker-support