How-To Guide

Configuring Zix Email Threat Protection to Forward Logs to 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.

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.

2. Prerequisites

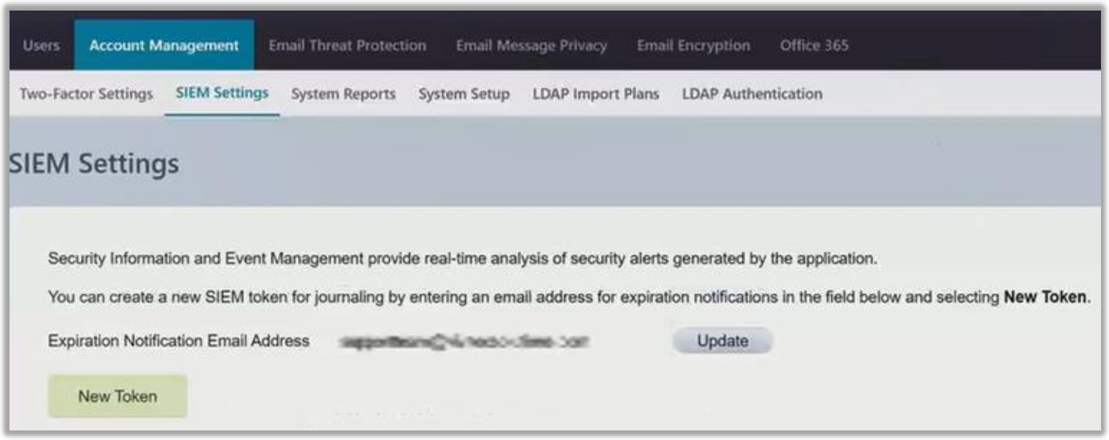
- EventTracker agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run powershell.
- Admin access to Zix/AppRiver Email Threat Protection platform.

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**.



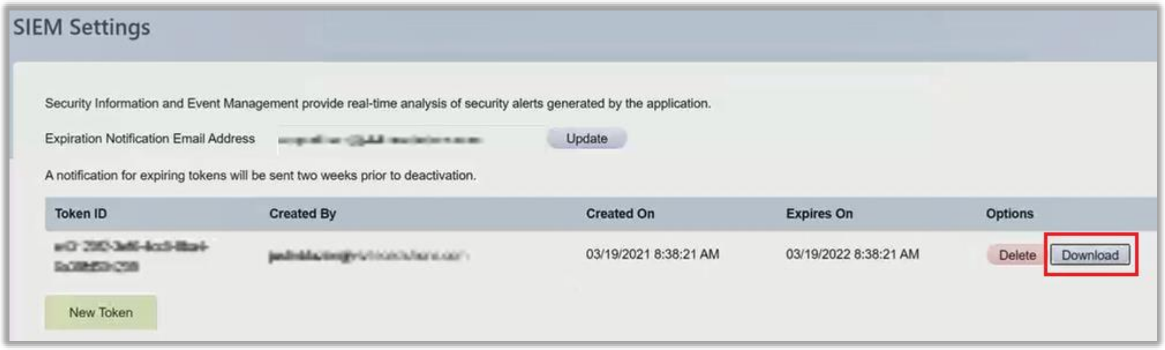
SIEM Settings

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] Update

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

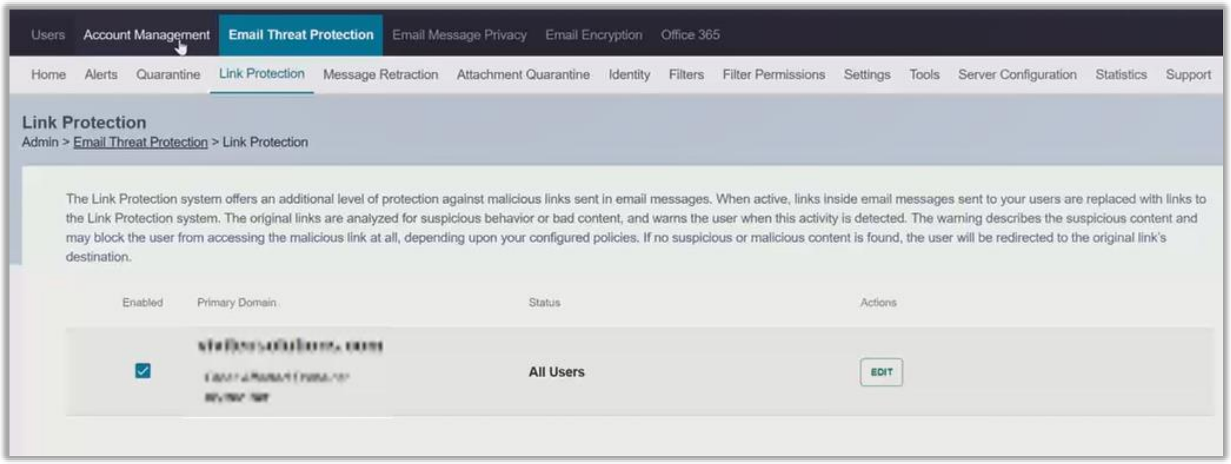
Token ID	Created By	Created On	Expires On	Options
[redacted]	[redacted]	03/19/2021 8:38:21 AM	03/19/2022 8:38:21 AM	Delete Download

New Token

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

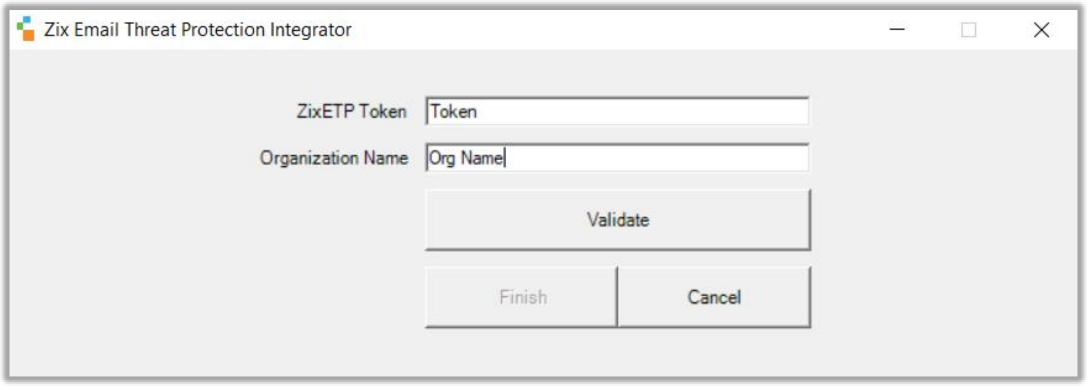
Admin > Email Threat Protection > Link Protection

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.

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