

Integration Guide

Integrating Zix Email Threat Protection with EventTracker

EventTracker v9.x and above

Publication Date:

April 9, 2021

© Copyright Netsurion. All Rights Reserved.

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

Τa	ble o	of Contents
1.	Ov	verview4
2.	Pro	erequisites4
3.	Со	onfiguring Zix ETP to forward logs to EventTracker4
	3.1	Collecting Token4
	3.2	Enabling Link Protection5
	3.3	Configuring EventTracker Zix Email Threat Protection Integrator
	3.4	Error Codes6
4.	Ev	entTracker Knowledge Pack6
	4.1	Reports6
	4.2	Alerts7
	4.3	Dashboards7
5.	Im	porting Zix ETP Knowledge Pack into EventTracker9
	5.1	Categories10
	5.2	Alerts11
	5.3	Token Template12
	5.4	Reports13
	5.5	Knowledge Object14
	5.6	Dashboard15
6.	Ve	erifying Zix ETP Knowledge Pack in EventTracker16
	6.1	Categories16
	6.2	Alerts17
	6.3	Token Value17
	6.4	Knowledge Objects17
	6.5	Reports
	6.6	Dashboard18
	Abou	ut Netsurion

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.

Users	Account Manageme	ent Email Th	ireat Protectio	n Email Me	ssage Privacy Em	ail Encryption	Office 365	
Two-Fa	ctor Settings SIEM S	iettings Syste	em Reports	System Setup	LDAP Import Plans	LDAP Authe	ntication	
SIEM	Settings							
Sec	curity Information and	Event Manage EM token for je	ement provide ournaling by e	real-time ana	lysis of security aler all address for expir	s generated by ation notification	the applications in the field b	n. below and selecting New Token .
Exp	piration Notification E	mail Address	seportes	n@%neacc	Sime-cont	Update		
	New Token							

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

Security Information and Event M	anagement provide real-time analysis of security ale	erts generated by the application.		
Expiration Notification Email Addr	ess مرد ما المرود الملي: ما المرود م	Update		
A notification for expiring tokens v	vill be sent two weeks prior to deactivation.			
		Created On	Expires On	Options
Token ID	Created By	Created On		
Token ID #IO 2310-3a61-4aa3-8ba+	Created By	03/19/2021 8-38-21 AM	03/19/2022 8·38·21 AM	Delete

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.

	Account	Management	Email Threat F	Protection	Email Me				Office 36						
Home	Alerts	Quarantine	Link Protection	Message R	Retraction	Attachment	Quarantine	Identity	Filters	Filter Permissions	Settings	Tools	Server Configuration	Statistics	Support
Link P Admin >	rotectio Email Thre	n at Protection	Link Protection												
ti d	The Link Pro he Link Pro nay block th lestination.	otection syster tection system ne user from a	n offers an addition. The original link ccessing the mali	onal level of p s are analyze clous link at a	protection a ed for susp all, depend	gainst malicio Iclous behavio Ing upon your	us links sen or or bad cor configured (t in email r itent, and v policies. If	nessages. warns the i no suspicio	When active, links in user when this activity ous or malicious cont	side email i y is detecte ent is found	nessage d. The wa , the use	s sent to your users are aming describes the sus r will be redirected to the	replaced wit picious cont e original link	h links to ent and 's
	En	abled Prin	nary Domain				Status				Actions				
		**	ritersolute	125.0011											
			ant different (na Visio fair	64.19 ²			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** (<u>as created in previous steps</u>), and your **organization name** and click on the **Validate** button to verify the credentials.

🛓 Zix Email Threat Protection Integrator			<u></u>	×
ZixETP Token	Token			
Organization Name	Org Name			
	Vali	date		
	Finish	Cancel		

- 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.

									Unix
LogTime	Computer	Action Taken	Sender IP	Sender Address	Recipient Address	Email Direction	Filter Rule ID	Filter Type	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@businesswatchnetwor k.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/xxxx xxx/021-utm-content- 04052120banner/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	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/Email Start.aspx?a=xxxxxxxxxx49be-b435- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	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			90-	- >
action	recipient_address	sender_address	src_ip_address	Count	^
quarantine	nishiningtypeyininintations and	allen alige possible constraints a con-	9904.01.191	2	
quarantine	rate/Flagacyfinancialadvizors.com	contactifi cleanwork.guru	104.140.80.102	2	
quarantine	peur@kgacyfmanciolad/moni.com	cook email@cook.cobysicsgn.com	142.087.215	2	
quarantine	tenborn@logecyfmancialadva.com	admin@cpacelvoorndovork.com	63.64.34.106	2	
quarantine	seturi@legeryliserriekoloises.com	mentessesiaes@filelada.um	76117.201.65	2	
quarantine	statio@legacyfinancialadvisors.com	admin@cpeadvicometwork.com	69.51.34.105	2	
quarantine	admin@log.cominancialadvisors.com	ecodycd18mcgo.m.	202,66,144,162	1	
quarantine	ngalla@legn.ylinarcialadeinas.com	deals@mainsystems.com	199.77.131.27	1	
quarantine	equile Dispect nancialedvicers.com	jeff Diagent-midgam.net	69.94.142.111	1	
uarantine K	ลตมนั้นสมับเคตลดงทั่งกลุกตาลโลตับปรดกร com	ieftmīlijadsanentmirtn com	1443112123	1	~

• Zix ETP - Email Traffic by Source IP



• Zix ETP - Top Action taken on Emails

Zix ETP - Top Action taken on Emails	0 🗹 – x
quarantine: 100.00% (152)	
quarantine	

• Zix ETP - Link Protection Activities

hecksum log_action src_ip_address url_name a5bcac3 ok minitian https://u2853127.ct.sendgrid.net/ls/cl 87dd70d ok 77.00000000000000000000000000000000000	
a5bcac3 ok mm.101.41.419 https://u2853127.ct.sendgrid.net/ls/cl 87dd70d ok 77.40.317.410 https://u2853127.ct.sendgrid.net/ls/cl d81da7cc ok 60.411.410 https://u2853127.ct.sendgrid.net/ls/cl	
87dd70d ok 71,49,317,180 https://u2853127.ct.sendgrid.net/ls/cl d814a7c ok 64,141,419,419 https://u2853127.ct.sendgrid.net/ls/cl	ick?u
d814a7c ok 66.161.218.49 https://u2853127.ct.sendgrid.net/ls/cl	ick?u
	ick?u
d678048 ok 66.161.748.49 https://na2.docusign.net/member/en	nailst
35c68ed ok 66,161.34X.49 https://go.dynamiccatholic.com/e/87	4791
567cc28 ok 72.49.217.196 https://u2853127.ct.sendgrid.net/ls/cl	ick?u
aoroves ox https://nac.docusign.net/member/en 35c6Sed ok 567cc28 ok	479 ick?

• Zix ETP - All Activities

<

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.

EventTracker Con	trol Panel		Eve	entTracker
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives
EventTracker	Traffic Analyzer	Agent	Port	TrapTracker
Agent Conti	53	Manageme	Configuration	
Change Audit	About EventTracker			

🥾 Expo	🐁 Export Import Utility							
Export	Import							
1. Pr 2. Cli	ovide the p ck the Imp	ath and file nam ort button.	e of the Categories file. Use the '' button to					
Opt	ions Category		Location					

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.

💺 Export Import Utility	-	- 🗆	\times
Export Import 1. Provide the path and file na 2. Click the Import button.	me of the Categories file. Use the '' button to browse and locate the import file.		
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location Source :]	
	Import	Clo	se

EventTracker displays a success message:

Export Import Utility Selected category details are imported successfully.	
Selected category details a	re imported successfully.
	ОК

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.

Export Import Utility		- 0
1. Provide the path and file na 2. Click the Import button.	me of the Alerts file. Use the '' butt	ton to browse and locate the import file.
Options Category Filters (a) Alerts	Location Import E-mail settings Set Active Only if notifications set By default	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.
 Systems and Groups Token Value Reports 	Watchlist Configuration Import Watchlist configurat This setting is applicable only f Note: If this option is enabled t on the console where the alert	ion or alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are available s are imported.
Behavior Correlation	Source : *isalt	
		Import

EventTracker displays a success message:

Export Import Utility		
Selected alert configurations are imported	ed successfully.	
	ОК	

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:

	" D	Admin	- Tools •	
ers	🧭 Parsing Rules		1	n /
lt Conta	ins set of rules which tell	what kind	l of data you v	vant
Configuration	Systems			

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



Parsing Rules			🔒 / Admin / Parsi	ng Rules	
Parsing Rule Template					
Groups		+	Group :	Ci	Ŧ
Default	-			Import cor	figuration
Azure Intune		0	lempla	Active	

 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.

Import	
Select file Note: Please select	t 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)**:

2. Click the Import button Note : If report(s) contains tem	plate, first import template and proceed with exportimport utility.	
Options	Location	
Category		
 Filters 		
O Alerts	O Legacy (*.issch) New (*.etcrx)	
Sustana and Ground	Source :	
 Systems and Groups 	*issch	
 Token Value 		
Reports		
Behavior Correlation		
- benavior correlation		

 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.

ŧ	Reports Import								
l	Note : If report(s) contains template, first import template and proceed with report import process.								
l	Select file *.etcrx	Select file *.etcrx Select file							
ľ	Available reports								-
l	Title		Fi	requency Show al	•	aa			
L		Title	Sites	Groups	Systems	Frequency	Runtime	Туре	

3. Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import t** 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	Set 🛈				
Replace	to Replace	Assign systems				
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.				

4. EventTracker displays a success message:

I	Export Import Utility	×
	Selected reports configurations are imported successfully	
	ОК	

5.5 Knowledge Object

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

		🔎 🛛 Admin 🗸	Tools 🗸 (
Active Watch Lists	Event Filters	🧭 Parsing Rules	📌 / D
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
ni sc 🚺 Casebook Configuration	Q IP Lookup Configuration	r Weights	since the last 24 hou
କଟ୍ଟି Category	·☆ Knowledge Objects	Windows Agent Config	_
Diagnostics	Manager		

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



Admin / Knowledge Objects
Objects 🕀 丁 🏦 🌣
Import Objects

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.

Import	
KO_ <product name="">.etko</product>	🗲 Browse Upload

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

Import Close

5.6 Dashboard

- 1. Login to EventTracker.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.



3. In My Dashboard, Click on Import Button:

👚 / Dashboard / My Dashboard
+ 🖉 @ 🌣 1 🗐 🛈
Import configuration

- 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.

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
🗁 Browse	Upload
Available widgets	

Import

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	
Category Tree Search	
All Categories All error events All information events All warning events All warning events Security: All security events	^
Zix Email 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								🔒 / Admin	/ Alerts
Show All						Search by Alert n	ame ~	Zix	Q
215	68			215	System	66	215	Critical 9 High 130 Loow 7 Medium 130	
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts			System/User D Count for system an	efined Alerts ad user defined alerts		Alerts by T Count of alert	Serious 39 Threat Level Is by threat level	
Activate Now Click 'Activate Now' aft	er making all changes							Total: 1 Page Size 25	~
Alert Name A	Th	hreat Ac	tive Email	Forward as SNMP	Forward as Syslog	Remedial Action F at Console	temedial Action at Agent	Applies To	
ි දිරි 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			
Parsing Rule Template			
Groups	+ III	Group : Zix Email Threat Protection	Search
		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.

Knowledge Ob	jects
Search objects	Q
Groups	🕀 🧭 🗓
Zix Email Threat Prot	tection
Zix Email Threat Protect	tion 🧭 📋

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.

Repor	t Configuration						
O Sch	neduled 🔿 Queued 🔘 Defined						
Repor	t Groups		÷		Repo	orts configu	uration: Zix Email Threat Protection
S.,	Security			^	÷	Ē 2,	
S .	Compliance						Title
S.,	Operations					223	Zix ETP - Link Protection Activities
S .	Flex					2.23	Zix ETP - Threat Protection Activities
	Zix Email Threat Pro	Ē	Ø				

6.6 Dashboard

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



	Home
Dashb	My Dashboard
R	Threats
	Incidents

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



Customize dashlets			×
Zix			Q
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			
			Add Delete Close



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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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