EventTracker:

Actionable Security Intelligence

Service Pack ET90U18-025

Feature Document

Publication Date: September 12, 2018

Abstract

This Guide will guide you with the enhancements added in the Service Pack (ET90U18-025).

Audience

User(s) who are using Service Pack (ET90U18-025) for EventTracker v9.0.

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

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

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	1
Audience	1
Support for GeoIP plugin in the Elastic search Resolve Hostname through Elasticsearch	3 5
Support for Extracting device id from relay devices Enhancement in Agent LFM	6 6
Specifying the System Name & Event Source for LFM logs	6
Extract Device ID from syslog devices	7
FAQ tiles enhancements	8
Permalink	9
How to configure a permalink in FAQ tile configuration?	9
Compliance Dashboard	12
Three tabs - Elastic, Cache and Archives in Log search result window	12
Support for Transport Layer Security 1.2	13
Supported Environment Details	13
Operating Systems:	13
SQL Versions	13
Prepare EventTracker for TLS 1.2	14
Steps to create EventTracker DSN with ODBC SQL Driver 11	15
Steps to enable TLS 1.2	20
How to enable TLS 1.2 manually without using IIS Crypto	23



Support for GeoIP plugin in the Elastic search.

The GeoIP plugin gets installed for Elasticsearch and uses Maxmind DB to fetch the Geolocation details of the Public IP addresses.

So, whenever a public IP address is encountered in EventTracker console, the Elasticsearch fetches details of the IP address. If Elasticsearch identifies a public IP address in any of the below mentioned CIM fields i.e.

- src_ip_address
- dest_ip_address
- dest_dns_address
- device_address

then, the geolocation details will be fetched and added to the newly introduced CIM fields.

For example, if the Public IP address is identified in **dest_ip_address** during elastic index then the geolocation details will be fetched and will be added the below CIM fields.

- dest_ip_address_geoip.city_name
- dest_ip_address_geoip.continent_name
- dest_ip_address_geoip.country_iso_code
- dest_ip_address_geoip.location.lat
- dest_ip_address_geoip.location.lon
- dest_ip_address_geoip.region_name

The above-mentioned details will be shown whenever user performs a logsearch

ELASTIC	CACHE		Event Tracker ⊕
Selected fi	elds	Time	Description
Interesting) fields	+ May 08 12:45:13 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR13 Time: 2018-05-08 00:39:32 Source IP: 192.168.4.38 Source Port: 50117 Destination I
addl_info		+ + May 08 12:43:32 AM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpl.local Local Port: 50117 Remote Addr
applicatio	n_name ·	+ May 08 12:39:32 AM	Network connection opened. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpl.local Local Port: 50117 Remote Add
attributes		+ May 07 12:44:13 PM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR13 Time: 2018-05-07 12:38:47 Source IP: 192.168:4.38 Source Port: 38691 Destination I
dest_host	name	+ May 07 12:44:13 PM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR13 Time: 2018-05-07 12:38:47 Source IP: 192.168.4.38 Source Port: 38690 Destination I
dest_ip_a	ldress ·	+ May 07 12:44:13 PM	New activity found: Rule Name: IP Pair Activity System: NTPLDT8LR13 Time: 2018-05-07 12:38:47 Source IP: 192.168:4.38 Source Port: 38689 Destination I
dest_ip_ac	ldress_geoip.city_n	+ May 07 12:38:58 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpl.local Local Port: 38691 Remote Addr
dest_ip_ac	ldress_geoip.conti	+ May 07 12:38:58 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpLlocal Local Port: 38689 Remote Addr
dest_ip_ac	ldress_geoip.count	+ May 07 12:38:58 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDT8LR13.ntpl.local Local Port: 38690 Remote Addr
dest_ip_ac	ldress_geoip.locati	+ May 07 12:38:47 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpl.local Local Port: 38675 Remote Addr
dest_ip_ac	ldress_geoip.locati	+ May 07 12:38:47 PM	Network connection opened. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDT8LR13.ntpl.local Local Port: 38691 Remote Add
dest_ip_ac	ldress_geoip.regio	+ May 07 12:38:47 PM	Network connection opened. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDT8LR13.ntpl.local Local Port: 38689 Remote Add
dest_port_	no	+ May 07 12:38:47 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpLlocal Local Port: 38674 Remote Addr
device_na	me ·	+ May 07 12:38:47 PM	Network connection closed. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDTBLR13.ntpl.local Local Port: 38676 Remote Addr
event_cate	≥gory	+ May 07 12:38:47 PM	Network connection opened. Type: TCP IP Version: 4 Local Address: 192.168.4.38 Local Hostname: NTPLDT8LR13.ntpl.local Local Port: 38690 Remote Add
event con	nputer	+	

Figure 1



In the same way, for other CIM fields, the geolocation details will be suffixed.

For src_ip_address,

- src_ip_address_geoip.city_name
- src_ip_address_geoip.continent_name
- src_ip_address_geoip.country_iso_code
- src_ip_address_geoip.location.lat
- src_ip_address_geoip.location.lon
- src_ip_address_geoip.region_name

For dest_dns_address,

- dest_ dns _address_geoip.city_name
- dest_dns _address_geoip.continent_name
- dest_dns_address_geoip.country_iso_code
- dest _dns _address_geoip.location.lat
- dest_ dns _address_geoip.location.lon
- dest_dns_address_geoip.region_name

For device_address,

- device_address_geoip.city_name
- device_address_geoip.continent_name
- device_address_geoip.country_iso_code
- device_address_geoip.location.lat
- device_address_geoip.location.lon
- device_address_geoip.region_name

The user can use these same newly introduced Geolocation details CIM Fields to configure dashlet in My dashboard, using Map chart type. See the below screen.



Dashlet configuration	
Dashlet title ()	public IP activity
Note ①	
Use SQL database Duration	ê eren de la companya
Lucene Query ①	
Saved searches Get CIM Fields	
Chart Type Value field setting Map Value field setting COUNT V	
Show ① Top 10 Records	
View CIM field mapping Select geo-location details	7
dest_ip_address_geoip.continent_name	
Select Columns ☑ North America ☑ Asia ☑ Europe	
Test Configure Cancel	

Figure 2

Resolve Hostname through Elasticsearch

After applying the Service pack, by default the "**Resolve Hostname**" option will be disabled. In this case, the hostname for the IP addresses will not be resolved (Local or Public IP). User can enable this option by navigating to Admin--> Manager--> Elasticsearch tab, under DNS configuration.

anager							🔒 / Admin / Ma
Configuration syslog / Virtual Co	Illection Point Direct Log Archiver	Agent Settings	E-mail	Collection Master Ports	Elasticsea	rch	
Elasticsearch Configuration							
Server address		Server port				Purge Indexes older than (days)	
localhost		9200				365	
Maximum degree of parallelism		Log level				Request time out (in seconds)	
2		Information			٣	120	
Minimize CPU Usage							
DNS Configuration							
✓ Resolve hostname	Resolve time out (in seconds)		Resolve retry			DNS Server IP	
Resolve local IP only	1	*	1		•	192.168.1.5	
							Save C

Figure 3



On enabling Resolved hostname option, the alert message will get display.

Ξ	Event Tracker ⊕		📣 Admin = Tools = 🛞 EventTrackerAdmin =
	Manager Configuration systeg / Virtual Collection Point Direct Log Archiver Direct Log Archiver	Agent Settings L-mail Collection Master Ports Electrometer	🕅 / främm / Manager
	Server address Incadrost Maximum degree of parallelism 2 2 Minimite CPU Usage	Caution! Enabling "Resolve hostname" feature may slow down the elastic indexing performance.	Purge Indexes older than (days) 7 Request time out (in seconds) 120
	DNS Configuration Resolve histoare Resolve local P only) Decoherentry	DES Seren P
	EventTracker @	Server Time: May 08 07:34 PM	ere : © 1999 - 2018 Freed Fucker

Figure 4

After enabling this option Resolved hostname the DNS server IP address will be fetched automatically. By default, it is set to Resolve local IP only.

The user can also provide the DNS Server IP manually.

Whenever a local IP address is identified in **src_ip_address** or **dest_ip_address** during elastic index, Elasticsearch service will resolves the hostname for IP address and puts the same hostname in the associated CIM fields, i.e. **src_host_name** or **dest_host_name** respectively.

When the **"Resolve local IP only**" option is unchecked, then Elasticsearch will resolve both Public and Local IP addresses.

Support for Extracting device id from relay devices

Enhancement in Agent LFM

Specifying the System Name & Event Source for LFM logs

At present, in Agent Log file monitoring, the event source and computer are default for the log source i.e. **Source**: "EventTracker" and **System**: "LocalComputer" where agent is running.

In this update, an option is provided to get the log source and computer name from user(s) for all supported format.



Event id 3230 will get generated based on this property. If user does not give any value then by default it will consider Source as "EventTracker" and System Name as "Local computer name"

- 1. In EventTracker Control Panel, double-click EventTracker Agent Configuration.
- 2. Click on Logfile Monitor tab and select Add File Name.

NOTE: System name allowed special characters are "-"and "_".

2	EventTracker Agent Configuration	ĸ
File	Help	
Sele	ct Systems	1
NTF	PLDTBLR103 Agent based system	
	Apply the following settings to specified Agents	
Manag	ger destinations:	
NTF	🖙 Enter File name	x
	You can configure the complete path of the log file or folder that needs to be mo along with the strings that need to be searched.	nitored
M	Get All Existing Log Files	
	Select Log File Type IIS	•
s	This is the Microsoft IIS log file format generated by IIS. Provided event source system name will be reflected as event computer name and event source in the property.	and event
e	Enter File name	
Г	D:\IIS*.iis	<u></u>
	Event Source IIS	
	System Name NTPLDTBLR16	
	OK Cance	
	Add File Name View File Details Delete File Name Search Strings	
	<u>S</u> ave <u>C</u> lose	



3. In the Enter File Name window, enter the file path, the Event Source and the System name and click **OK**.

NOTE: For VMware, Checkpoint, Evt and syslog, this new option will not be available.

Extract Device ID from syslog devices

Another enhancement is extracting the device ID from syslog device while it is relaying. It will extract the Device ID from event description by using regular expression. After extracting the value from description it assigns it to "Computer Name" standard property.

Example: FG1K5D3I14802285@ntpldtblr104-syslog



록 Enter File name		×
Configure EventTracker	Agent to receive syslog messages.	
Select <u>L</u> og File Type	syslog	+
messages from various A valid port which is no Based on provided reg description and add the Example : .*devid=(?P< description and use it a 'Computer' for any field	devices and forwarding them to configured managers t used by any other process should be configured. ular expression agent will extract the particular value fi e extracted value into computer name property of the Computer>[\w]+).* expression will extract devid from t s computer name.Please provide Named Capture gro name, as shown in example.	rom event event. he event up as
🔽 Regular express	ion .*devid=(?P <computer>[\w]+).*</computer>	
Protocol	UDP	-
Port	519	
	Can	cel

Figure 6

NOTE: The allowed special characters for system name are ".", "_" and "-"

FAQ tiles enhancements

Now the FAQ Tile option has been included in the Admin Dropdown.

		🔎 Admin -
Active Watch Lists	Diagnostics	Manager
Alerts	Event Filters	🧭 Parsing Rules
Behavior Correlation Rules	Eventvault	Report Settings
🗞 Behavior Correlation Settings	FAQ Configuration	Systems
Casebook Configuration	Group Managemeenhiguring F	AQ tiles. Users
● Category	Q IP Lookup Configuration	reights
Collection Point	· 🔆 Knowledge Objects	Windows Agent Config

Figure 7

FAQ tiles count for report dashboard:

- 1. Report Status for generated reports
- 2. Review Status for generated reports
- 3. Generated Type

NOTE: FAQ tiles count will be based on user permissions for non-admin user



4. Bookmarks links

Bookmark link can be any of the following:

- ✓ Website URL
- ✓ Application web page URL
- ✓ Documents like pdf/excel/word etc.

NOTE: Links can be configured in FAQ tiles configuration by Admin user only.

Report Dashboard									A / Reports / Rep	ort Dashboard
4 Succes 4 Report Status Generated report status	4 Review Status Review status for gene	Unflagged rated reports	s	·	4 Generation Type Generated reports by (Schedule 4 Generation types		Bookmarks References	Solutior PCI DSS v3.2 Solutior	brief document brief document
Reports Top Level Summary				Duration: Mar 29 04	:19 PM - Mar 30 04:19	PM				
Search Q Q Q	2							÷	1 C □ □ Page size 25 ∨	Total: 4
Title				Туре		Generation Type	Generate	d On	Size (KB)	
Unknown Processes - Executed20180330-1522400	580.xlsx		1	Unknown Processes -	Executed	None	Mar 30 0	2:33:01 PM	13	\$
TargetsReport20180330-1522400580.xlsx			1	Targets report		None	Mar 30 0	2:33:00 PM	17	\$
AttackersReport20180330-1522400520.xlsx			1	Attackers report		None	Mar 30 0	2:32:01 PM	49	\$
Logs - Detail	B	1	1	Logs		Schedule	Mar 30 0	2:30:03 PM	18,882	\$

Figure 8

Permalink

User(s) can use this option to provide Useful links like Solution brief link, Compliance mapping document, PCI DSS requirement link etc. which is useful for reference.

How to configure a permalink in FAQ tile configuration?

In v9.0, the user can configure FAQ tiles which will be displayed in modules like Home, Alerts, Reports and Systems.

To configure FAQ tile,

• Click the FAQ configuration option in Admin dropdown. The FAQ tile configuration window gets displayed.



FAQ tile configu	uration						
A	vailable FAQ tiles			ŧ	€	Module	
_						Select Page	~
	Non Reporting Systems	Ø	Potential Cyber Breaches	Ø		Configured FAQ tiles A maximum of 4 FAQ tiles can be displayed.	
	Indicators of Compromise	Ø	Potential Insider Threats	۲			
	Available Alerts	Ø	Active Alerts	0		Move FAQ tile up or down to reorder.	
	System/User Defined Alerts	Ø	Alerts by Threat Level	۲			
	Request Status	Ø	Managed vs Unmanaged	Ø			
	EventTracker Sensor Version	Ø	Report Status	Ø			
	Review Status	Ø	Generation Type	0			
	Bookmarks	1	wqwsas	Ø İ			
							Ok

Figure 9

• In the right pane, the user can select from the modules, where they want to display the tiles.

Aodule							
Select Page							
Reports							
Home							
Systems							
Alerts							

Figure 10

• The left pane displays the available list of FAQ tiles.

To add a link to a particular FAQ Tile, click the add icon and check **Use Link** option.

• Click the Add Link button to add URL or Documents, as per requirement.



FAQ tile configuration			
	Title		Description
	Data source	~	
	Background color		
	Use Link Add Link		Title
		ſ	© URL ○ Doc
			Permalink
			Link nline-help/eventtracker-v9.x/index.htm#t=Chapter_2_Dashboard.htm
			Ok Cancel
			Configure

Figure 11

- Give a suitable title and click OK. It will be listed in the left pane.
- And then click the **Configure** button.

FAQ tile configuration			
Tit	le	Description	
	FAQ tile		
Da	ata source		
	Select	~	
Ва	ckground color		permalink
\checkmark	Use Link Add Link		
		FAQ tile Description	
	permalink Ø 🗓 T.	st	
	v9.x/index.htm#t=Chapter_2_Dashboard.htm		
		Co	nfigure Cancel

Figure 12

In the same way, the user can also add documents and configure a FAQ tile, as per needs.



NOTE:

- 1. The supported document extensions are (.txt,.pdf,.doc,.docx,.rtf,.xlsx,.xls).
- 2. The maximum size of the document is 2MB.

Compliance Dashboard

The Compliance Dashboard has been updated with changes where user will now be able to view compliance summary reports details. If the user has configured compliance summary report, then only the below screen will be displayed:

	ventTracker⊕		Admin -	Tools +	Shankar pabt
-	Compliance			÷.	Dashboard / Compl
а. В	Dashbaard PCIDSS NST 800 171				
	Date Mar 29 12:00:00 AM to Mar 29 11:59:59 PM This report is based on guidance from the PCI Standards Council. For security logs to be useful in the defense of information assets, they must be monitored and analyzed. To generate this report, EventTracker receives, processes, alerts and summarizes log data from a	Published	Report Ac	me PCI-DSS (Com Print • Iy to satisfy the Log
	Monitoring requirements of PCI-DSS. If you would like to get more information or have questions regarding PCI DSS, email us at essentials-support@eventtracker.com				
	Requirement 10.2.1				
	All individual user accesses to cardholder data.				
	Windows User Logon or Logoff Success.				
	Descriptions perior must use a contract were operated. Recommendation: Review the user activities listed below and confirm if they are legitimate.				
	4 INCIDENTS: SHOW				
	Requirement 10.2.1 and 10.2.4				
	All individual user accesses to cardholder data and Invalid logical access attempts.				

Figure 13

If no Compliance summary report is configured, the Dashboard will be displayed as shown below:

Compliance	1 / Dashboard / Compliance
	\oplus
Dashboard PCI DSS NIST 800 1	
Published Report	✓ Print
No Report is configured	

Figure 14

Three tabs - Elastic, Cache and Archives in Log search result window

When log volume is more and the data is not indexed in the selected duration, the 3 tabs in search helps to show the entire data without any miss.



For example: Suppose the elastic purge is set to 7 days and if user try to do elastic search for last 2 weeks data, then 1 week data will be shown Elastic tab, the mdb's which are available in cache folder and are not indexed cabs data will be shown in the Cache tab and second week cabs data will be shown in Archives tab.





Support for Transport Layer Security 1.2

Supported Environment Details

The following combinations of Operating System and MS SQL Server has been tested and supported.

Please make sure when you are installing EventTracker, the TLS 1.2 is not enabled. This is applicable for EventTracker pre-requisites and SQL as well.

NOTE: User(s), who wish to use the TLS, please enable the TLS 1.2 option, if not checked.

Operating Systems:

- 1. Windows Server 2016
- 2. Windows Server 2012 R2
- 3. Windows 10

SQL Versions

- 1. SQL Server 2016 (Express and Enterprise Edition)
- 2. SQL Server 2017 (Express and Enterprise Edition)



NOTE: If EventTracker server is running with SQL server 2014 or below versions then first upgrade to SQL Server 2016 or SQL Server 2017 before using this Guide.

Web server: IIS

Supported ODBC Driver: ODBC Driver 11 for SQL Server

The below steps can be followed after the EventTracker Installation is complete.

Prepare EventTracker for TLS 1.2

- 1) Apply the Windows Updates (Up to date).
- 2) Stop and disable all EventTracker services.
- 3) Install the "ODBC Driver 11 for SQL Server" using below path.

https://www.microsoft.com/en-in/download/confirmation.aspx?id=36434

4) Rename existing EventTracker DSN entries by using below system utility

C:\Windows\SysWOW64\odbcad32.exe

An example of renaming the existing EventTracker DSN is shown below:



Figure 16

After renaming the DSN from EventTracker to "EventTracker_old", click on Finish.

NOTE: In the similar way, also the rename the EventTrackerAlerts and EventTrackerData.

5) Create new DSN with ODBC driver "ODBC Driver 11 for SQL Server"



- ✓ EventTracker
- ✓ EventTrackerData
- ✓ EventTrackerAlerts

Steps to create EventTracker DSN with ODBC SQL Driver 11

1. Create EventTracker DSN entries by using below system utility.

C:\Windows\SysWOW64\odbcad32.exe

ODBC Data Source Administrator (32-bit)							
User DSN System DSN	File DSN	Drivers Tracing Connection Pooling About					
System Data Sources:							
Name EventTracker old	Platform	Driver Add					
Event TrackerAlerts_old	32-bit	SQL Server Remove					
EventTrackerData_old	32-bit	SQL Server					
		Conngure					
An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users of this computer, including NT services.							
OK Cancel Apply Help							



An example of Creating the EventTracker DSN is shown below:

2. Click on Add and it will populate the below window:



Create New Data Source		×
	Select a driver for which you want to set up a data se Name Microsoft Paradox-Treiber (*.db) Microsoft Text Driver (*.txt; *.csv) Microsoft Text-Treiber (*.txt; *.csv) ODBC Driver 11 for SQL Server ODBC Driver 13 for SQL Server SQL Server SQL Server Native Client 11.0	Durce.
	< <p>Konstant</p>	> ancel



3. Select ODBC Driver 11 and click on Finish. It will populate the below window.

Create a New Data Sour	ce to SQL Server	×
SQL Server	This wizard will help you create an ODBC data source that you can use to connect SQL Server. What name do you want to use to refer to the data source? Name:	t to
	How do you want to describe the data source? Description:	
	Which SQL Server do you want to connect to?	
	<u>S</u> erver:	~
	Finish <u>N</u> ext > Cancel Help	



4. Provide the DSN name and SQL server instance name like ".\sqlExpress", and then move to the **Next** window.



Microsoft SQL Server DS	N Configuration				×
SQL Server	This wizard will help y SQL Server. What name do you w Name: How do you want to Description: Which SQL Server d Server:	vou create an (vant to use to r Event Tracke describe the d describe the d R1S5-VM9\S	DDBC data source efer to the data so d ata source? connect to? iQLEXPRESS	e that you can use	e to connect to
	[Finish	Next >	Cancel	Help

Figure 20

- 5. Click **Next** to proceed.
- 6. Check "Change the default database to" and select the "EventTracker" database.

Microsoft SQL Server DSN Configuration X						
SQL Server	Change the default database to: Contractor Mirror server: SPN for mirror server (Optional): Attach database filename: Vuse ANSI quoted identifiers. Vuse ANSI nulls, paddings and warnings. Application intent: READWRITE Multi-subnet failover.					
	< Back Next > Cancel Help					

Figure 21

7. Click **Next** and then select **Finish**.



Microsoft SQL Server D	5N Configuration	×		
	Change the language of SQL Server system messages to:	~		
SQL Server	Use strong encryption for data			
	Save long running queries to the log file: C:\Users\chethan\AppData\Local\Temp\QUERY.Ll Browse			
	Long query time (milliseconds): 30000			
Federal Contra	C:\Users\chethan\AppData\Local\Temp\STATS.LC Browse			
	Connect Retry Count: 1			
	Connect Retry Interval (seconds): 10			
	< Back Finish Cancel Help			

Figure 22

NOTE: After click the finish button, it will populate the Test window. Click on Test DSN Source....

This will help the users to ensure whether the Test connection status is successful or not.

ODBC Microsoft SQL Server Setup	\times
A new ODBC data source will be created with the following configuration	i:
Microsoft ODBC Driver for SQL Server Version 12.00.5543	\sim
Data Source Name: EventTracker Data Source Description: Server: R1S5-VM9\SQLEXPRESS Use Integrated Security: Yes Database: EventTracker Language: (Default) Data Encryption: No Trust Server Certificate: No Multiple Active Result Sets(MARS): No Mirror Server: Translate Character Data: Yes Log Long Running Queries: No Log Driver Statistics: No Use Regional Settings: No Use ANSI Quoted Identifiers: Yes Use ANSI Null, Paddings and Warnings: Yes	*
Test Data Source OK Cancel	

Figure 23

In case of success it will populates below window.



SQL Server ODBC Data Source Test	×
Test Results	
Microsoft ODBC Driver for SQL Server Version 12.00.5543	^
Running connectivity tests	
Attempting connection Connection established Verifying option settings Disconnecting from server	
TESTS COMPLETED SUCCESSFULLY!	
	~
ОК	



NOTE: In the similar way, you can a Create the EventTrackerAlerts and EventTrackerData.

8. Now, Create registry string value under:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\Manager

- Enter the Value name: "SQLODBCDrv" of type String
- And Enter the Value: ODBC Driver 11 for SQL Server



📑 Registry Editor — 🗆 🗙								
File	File Edit View Favorites Help							
Com	nputer\	HKE	Y_	LOCAL_MACHINE\SOFT	WAI	RE\WOW6432Node\Prism Microsyste	ms\EventTracker\N	Manager
		>		JavaSoft	^	Name	Туре	Data
				JreMetrics		ab (Default)	REG SZ	(value not set)
		>		Khronos			REG_SZ	C:\Program Files (x86)\Prism Mi
		>		Macromedia			REG_DWORD	0-00000000 (0)
		>		Macrovision			REG_DWORD	0.00000000 (0)
		>		Martin Prikryl			REG_DWORD	0x0000000 (0)
		>		Microsoft		EA_KeloadLocalHashUnsafeList	REG_DWORD	0x0000000 (0)
		>		Microsoft Corporation		EA_ReloadProcessFilterRule	REG_DWORD	0x0000000 (0)
		>		Mozilla		esinstallPath	REG_SZ	C:\Program Files\Elasticsearch-
		>		mozilla.org		ab EsVersion	REG_SZ	5.5.2
		>		MozillaPlugins		100 ETConsoleType	REG_DWORD	0x0000001 (1)
		>		Nuance		80 ETCorrelator	REG_DWORD	0x00000000 (0)
		>		NuGet		ab INSTALLPATH	REG_SZ	C:\Program Files (x86)\Prism Mi
		>		ODBC		👪 InstallTime	REG_DWORD	0x5ae2ff43 (1524825923)
		>		Policies		KO_ReloadObjects	REG_DWORD	0x00000000 (0)
		>		PreEmptive Solutions		LastCabProcessedTime	REG_DWORD	0x5b33368d (1530082957)
		~		Prism Microsystems		LastCabProcessedTime_disable	REG DWORD	0x5b221259 (1528959577)
			~	EventTracker		ab SOLINSTANCENAME	REG SZ	\EventTracker0
				> Agent		ab SOLNativeDry	REG SZ	SOL Server Native Client 11.0
				ASPNET_SETREG			REG SZ	ODBC Driver 11 for SOL Server
				Manager		1 TranTracker	REG DWORD	0x00000000 (0)
				iSMARTset		abWebServer	PEG S7	
				PrivateTunnel		Tel Menselvel	NEG_3Z	113
	Registered Applications *							

Figure 25

Steps to enable TLS 1.2

Enable the TLS 1.2 using IIS Crypto

1. Download the IIS Crypto tool from the below link:

https://www.nartac.com/Products/IISCrypto/Download

2. After downloading the IIS Crypto Tool, please ensure that the tool is digitally signed. Below figure shows the verification screen for IIS Crypto.



IISCrypto Properties					
Security Details Previous Versi	ons				
General Compatibility Digital Signatures					
Signature list					
Name of signer: Digest algorit Timestamp					
Nartac Software Inc. sha1 Saturday, July 1	6, 20				
Nartac Software Inc. sha256 Saturday, July 1	6, 20				
Details					
OK Cancel	Apply				

Figure 26

3. Once the download is complete, run the exe as administrator.



E.		IIS Crypto		_ _ X
📕 IIS (Crypto 2.0			NARTAC SOFTWARE
Schannel	Schannel These settings enable or disable v default for the operating system	various options system wide. When will be used. Click the Apply button	the checkbox is grey it means r to save changes.	10 setting has been specified and the
0	Protocols	Ciphers	Hashes	Key Exchanges
Cipher Suites Templates Site Scanner	☐ Multi-Protocol Unified Hello ☐ PCT 1.0 ☐ SSL 2.0 ☐ SSL 3.0 ☐ TLS 1.0 ☐ TLS 1.1 ☑ TLS 1.2	 ✓ NULL ✓ DES 56/56 ✓ RC2 40/128 ✓ RC2 56/128 ✓ RC4 128/128 ✓ RC4 56/128 ✓ RC4 56/128 ✓ RC4 128/128 ✓ Triple DES 168 ✓ AES 128/128 ✓ AES 256/256 	 ✓ MD5 ✓ SHA ✓ SHA 256 ✓ SHA 384 ✓ SHA 512 	 ✓ Diffie-Hellman ✓ PKCS ✓ ECDH
About	✓ Set Client Side Protocols			
	Best Practices			Apply

Figure 27

Select TLS 1.2 from the protocol section which is highlighted in the figure above. Click on Apply.
 A pop-up window displays to restart.



Figure 28

- 5. Delete the IIS Crypto exe from the server.
- 6. Restart the server.
- 7. Enable and start all the **EventTracker services**.

NOTE: Ensure that the SQL service is running



How to enable TLS 1.2 manually without using IIS Crypto

- 1. Start the registry editor by clicking on **Start** and **Run**. Type in "regedit" into the **Run** field (without quotations).
- Highlight Computer at the top of the registry tree. Backup the registry first by clicking on File and then on Export. Select a file location to save the registry file.

Note: You will be editing the registry. This could have detrimental effects on your computer if done incorrectly, so it is strongly advised to make a backup.

- Browse to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
- 4. Right click on the Protocols folder and select New and then Key from the drop-down menu. This will create new folder. Rename this folder to TLS 1.2.
- 5. Right click on the TLS 1.2 key and add two new keys underneath it.
- 6. Rename the two new keys as:
 - ✓ Client
 - ✓ Server
- 7. Right click on the Client key and select New and then DWORD (32-bit) Value from the drop-down list.
- 8. Rename the DWORD to DisabledByDefault.
- 9. Right-click the name DisabledByDefault and select Modify... from the drop-down menu.
- 10. Ensure that the Value data field is set to 0 and the Base is Hexadecimal. Click on OK.
- 11. Create another DWORD for the Client key as you did in Step 7.
- 12. Rename this second DWORD to Enabled.
- 13. Right-click the name Enabled and select Modify... from the drop-down menu.
- 14. Ensure that the Value data field is set to 1 and the Base is Hexadecimal. Click on OK.
- 15. Repeat steps 7 to 14 for the Server key (by creating two DWORDs, DisabledByDefault and Enabled, and their values underneath the Server key).
- 16. Reboot the server. **NOTE:** Your server should now support TLS 1.2.

