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.

Table of Contents

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

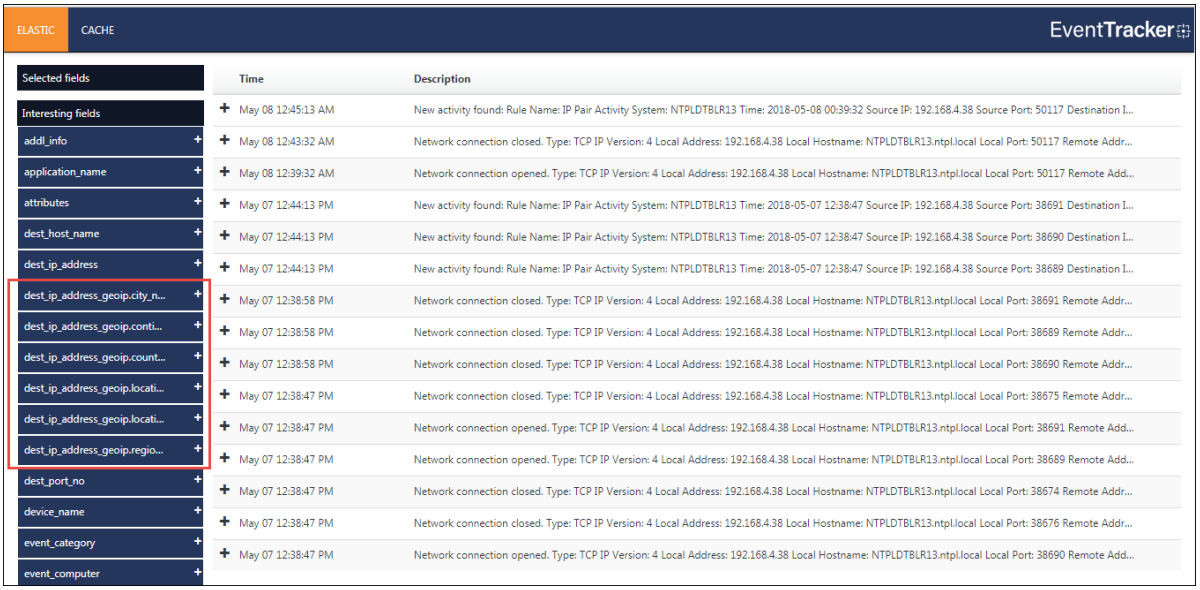

Figure 1

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.

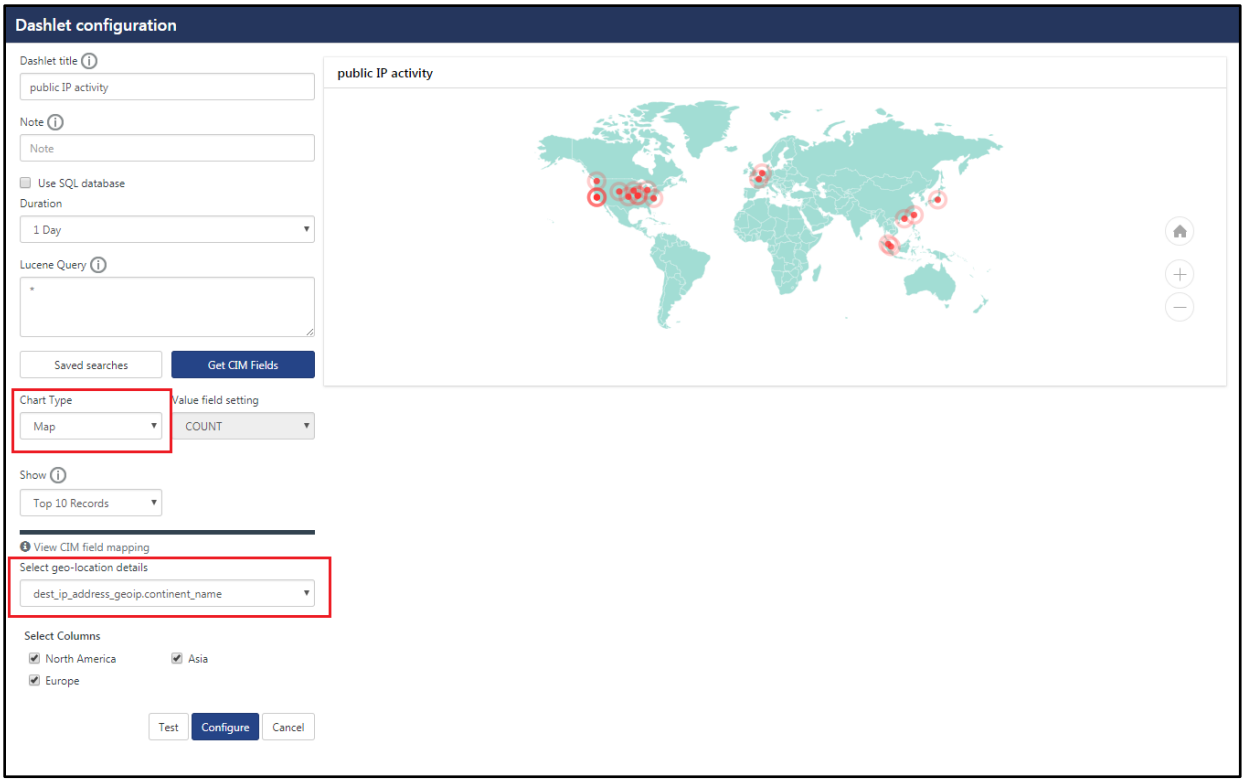

Figure 2

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.

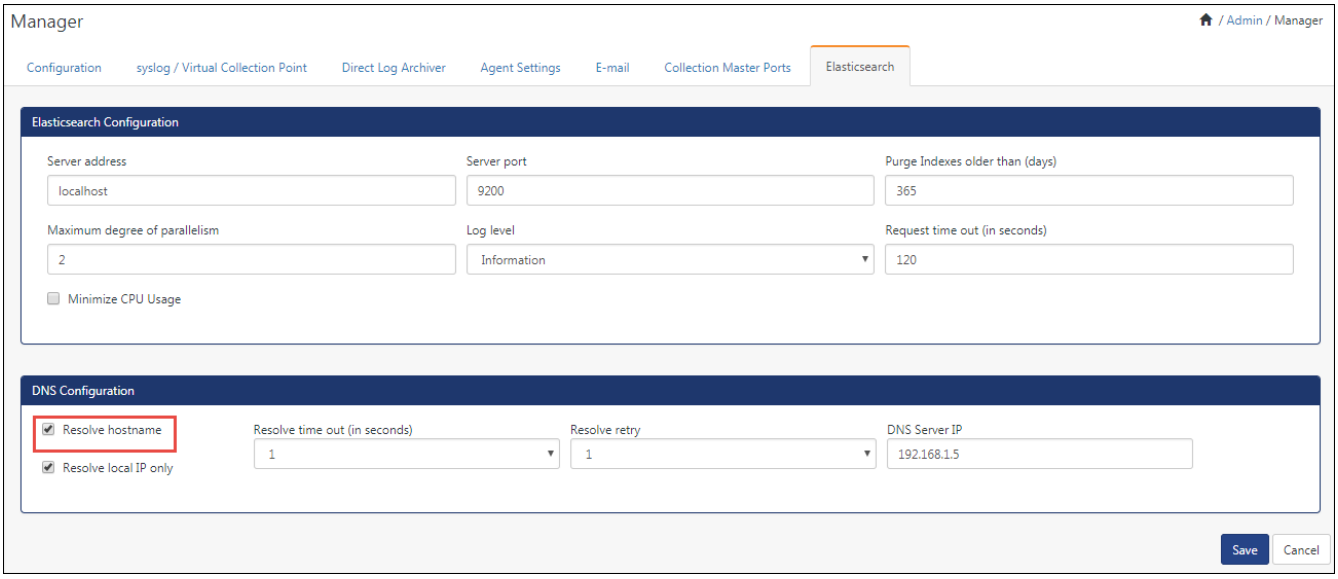

Figure 3

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

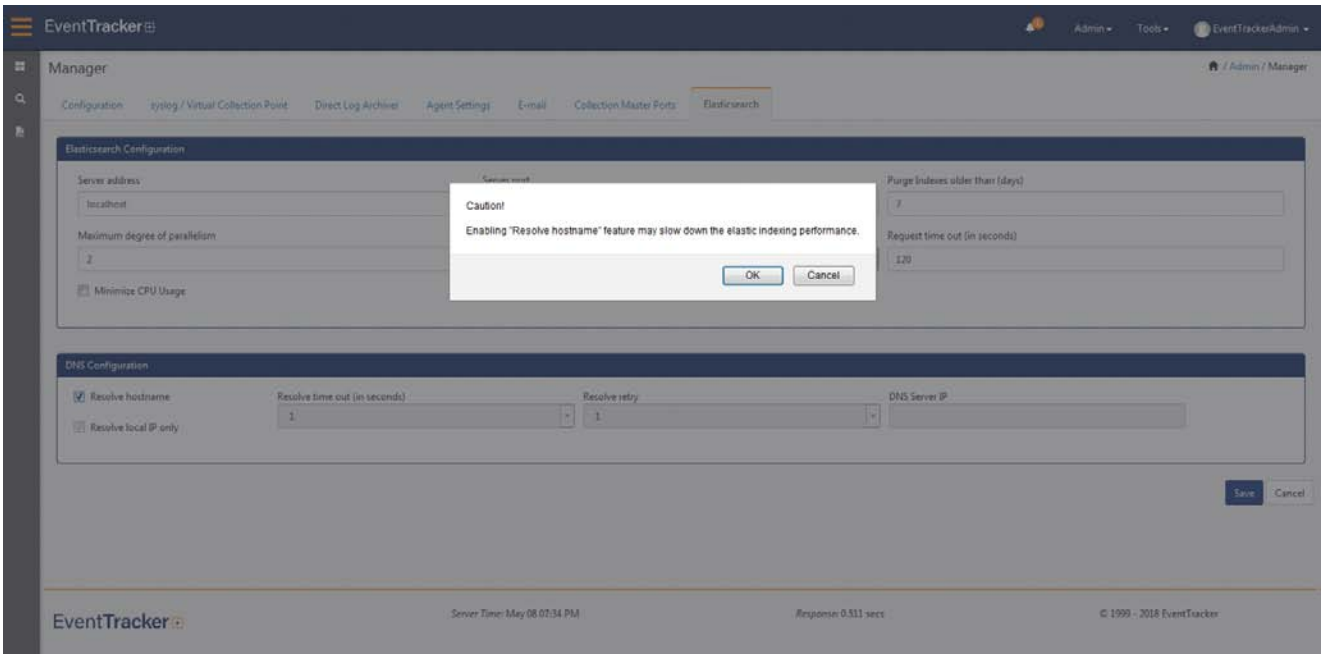

Figure 4

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 "**_**".

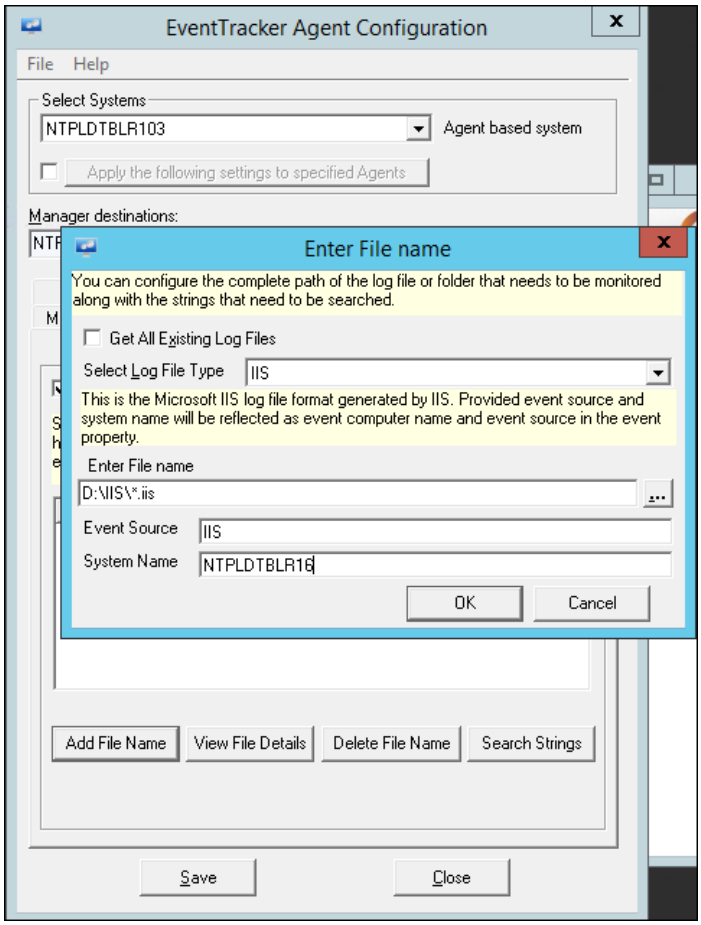

Figure 5

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

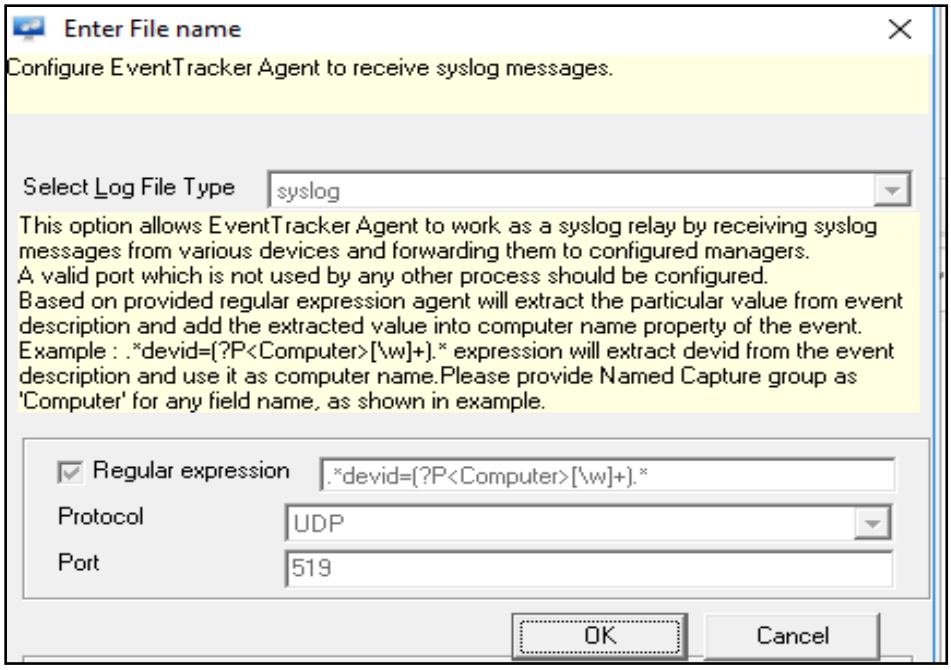

Figure 6

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.

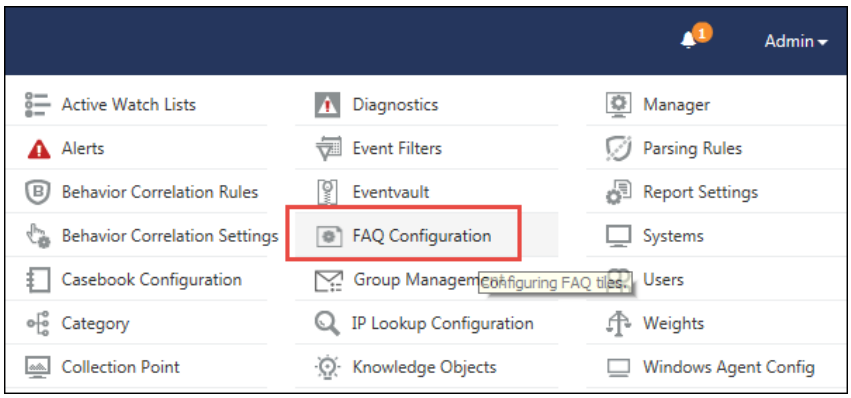

Figure 7

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.

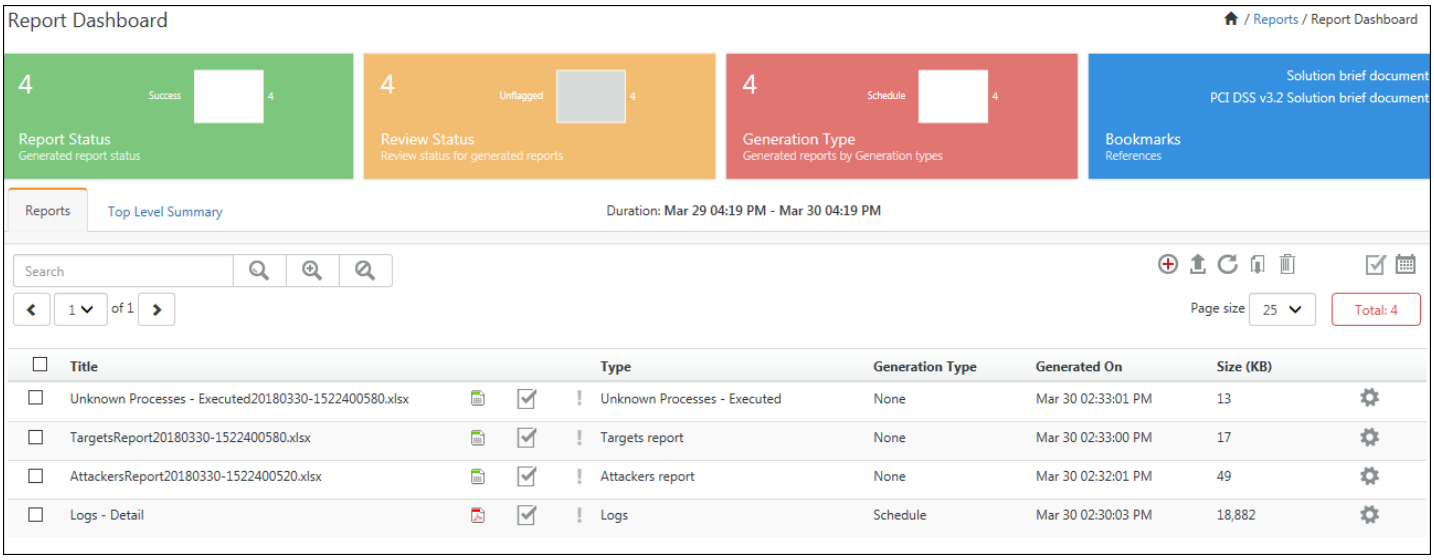

Figure 8

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.

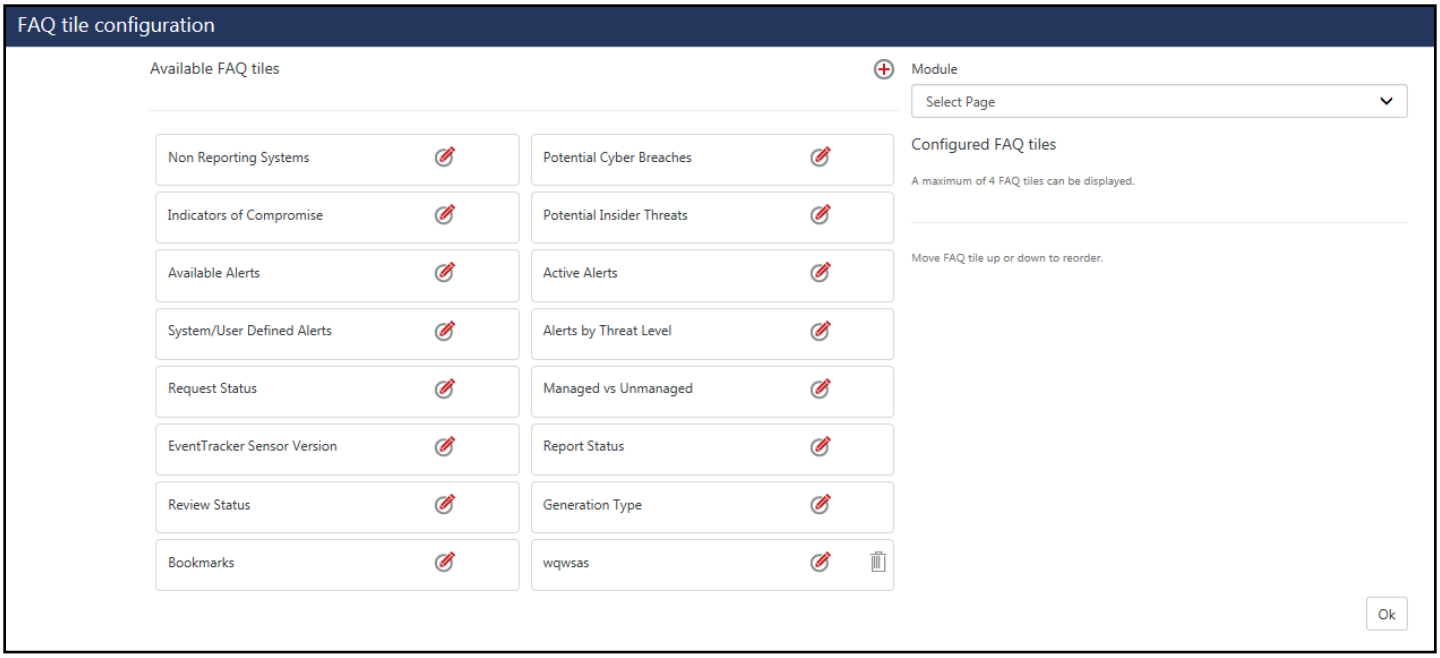

Figure 9

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

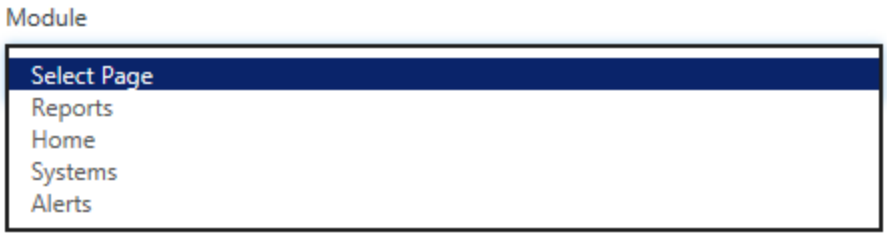

Figure 10

- 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.

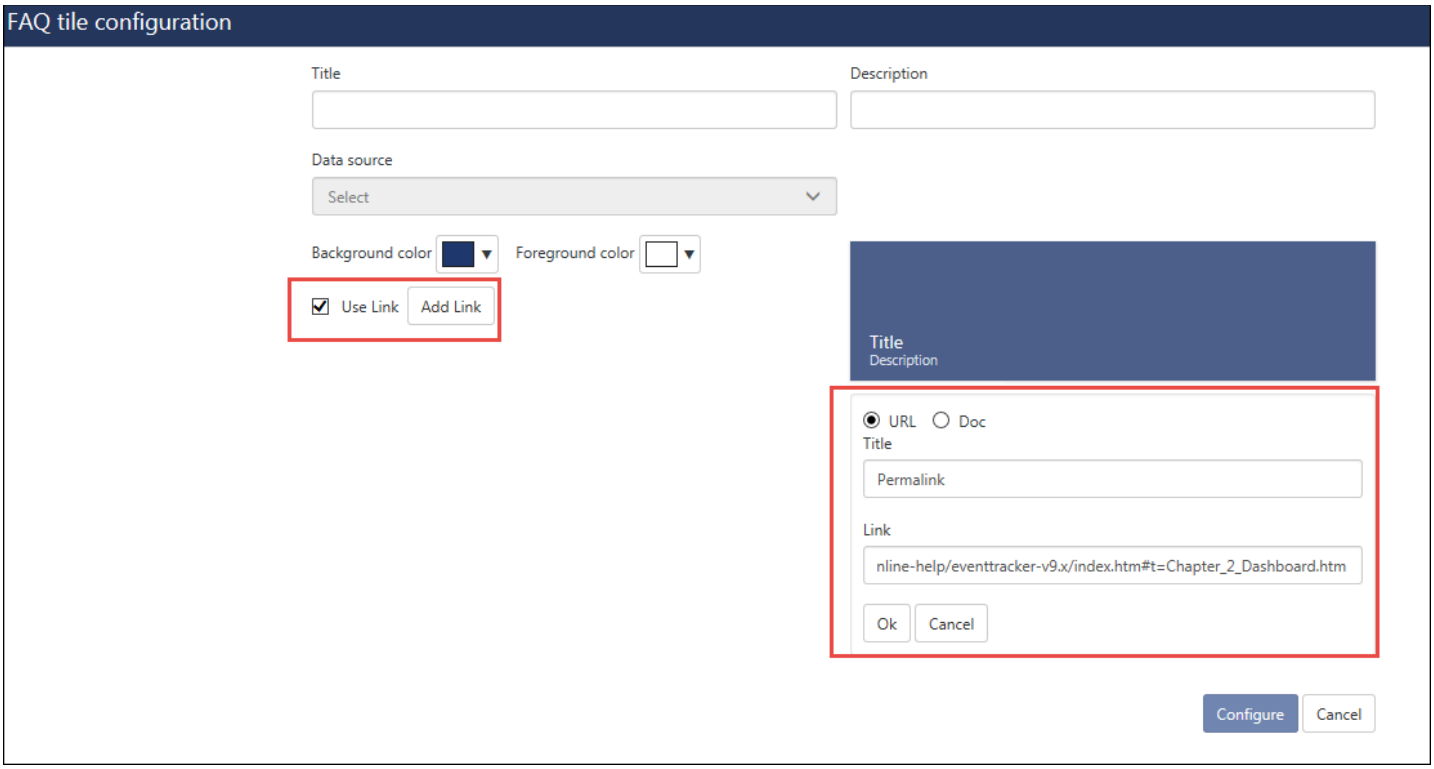

Figure 11

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

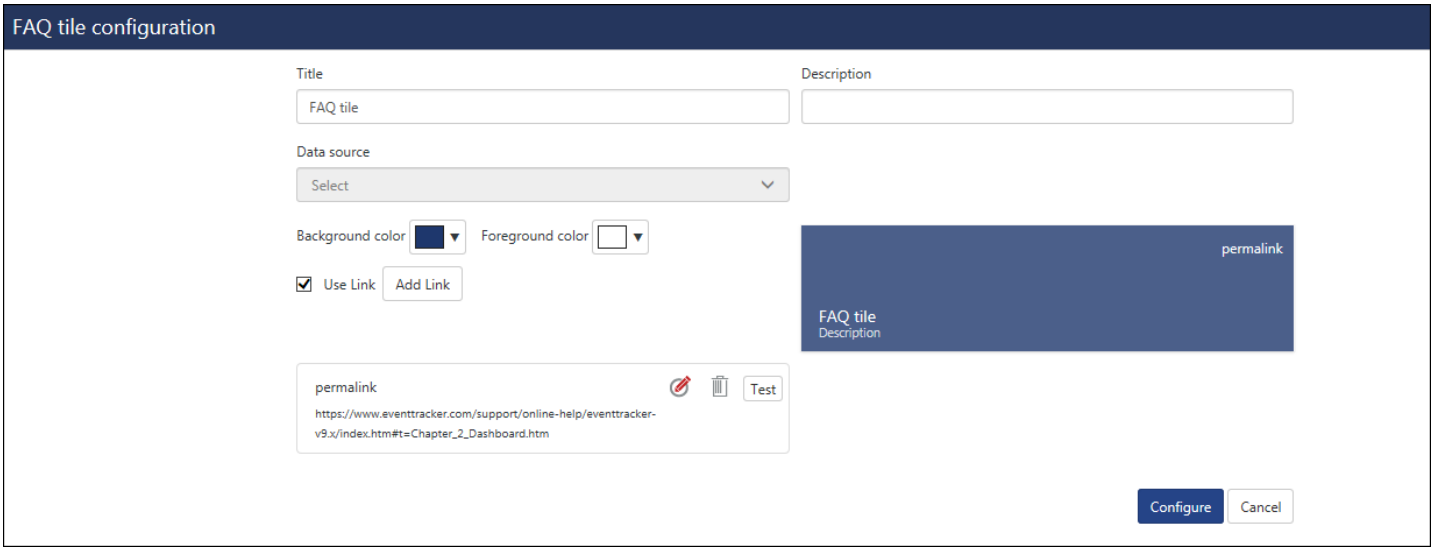

Figure 12

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:

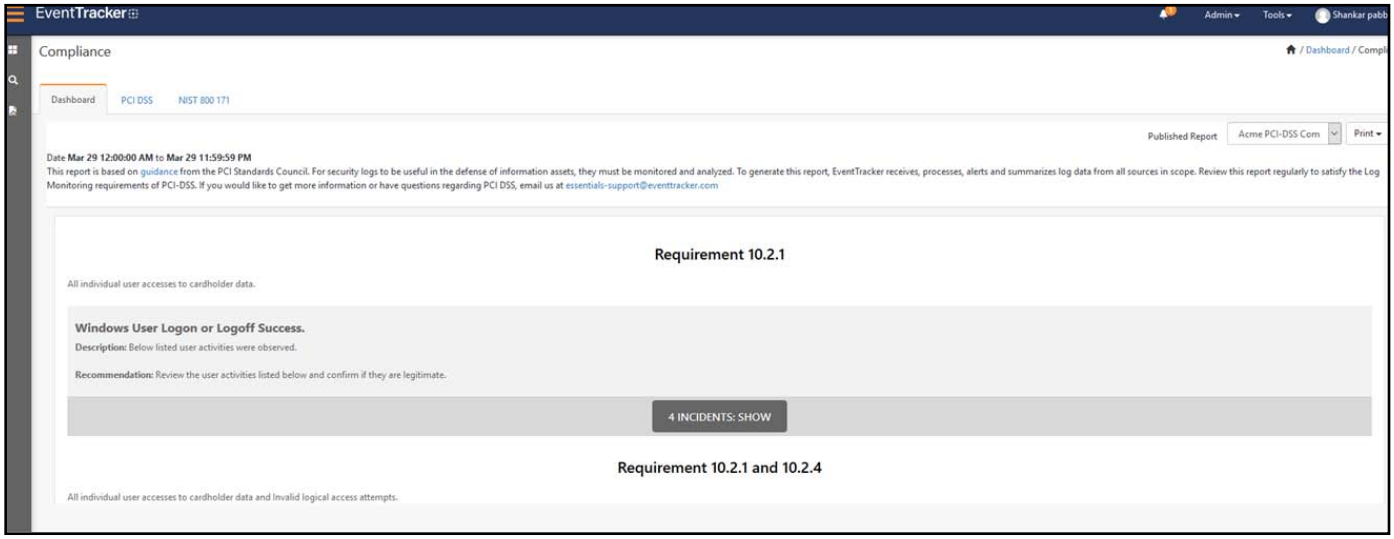

Figure 13

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

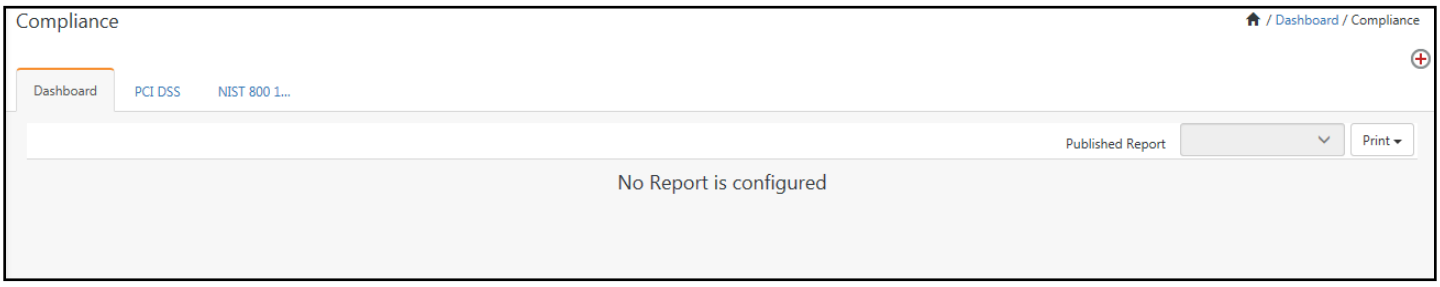

Figure 14

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.

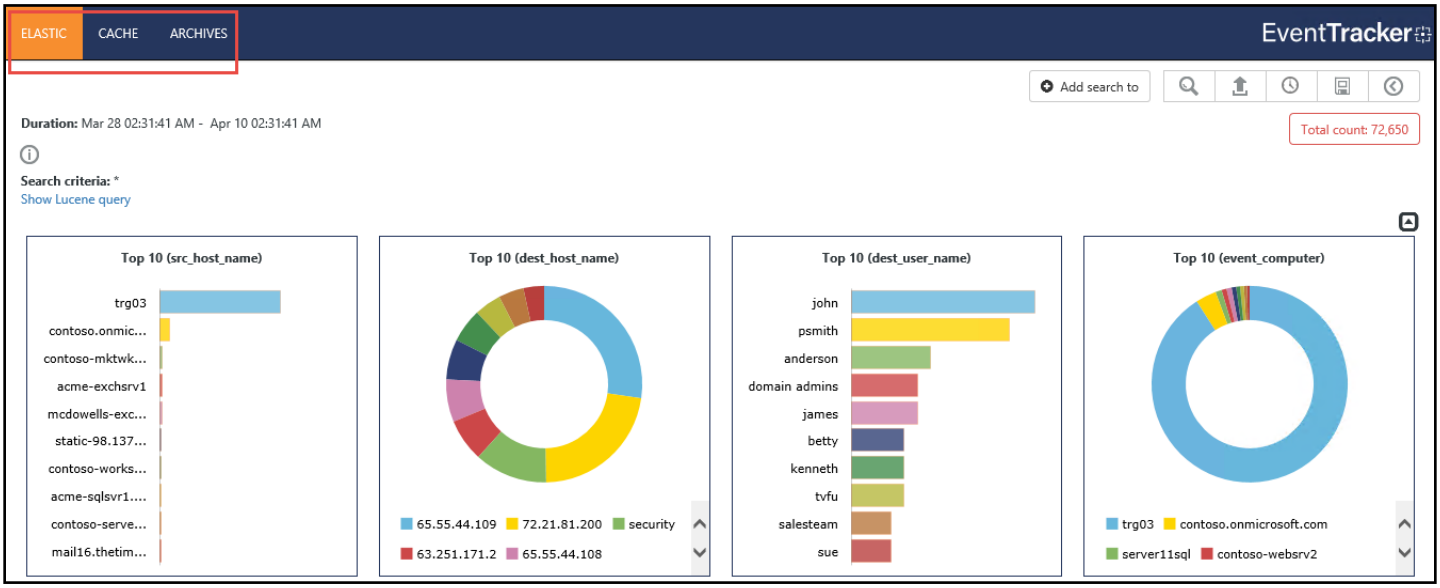

Figure 15

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:

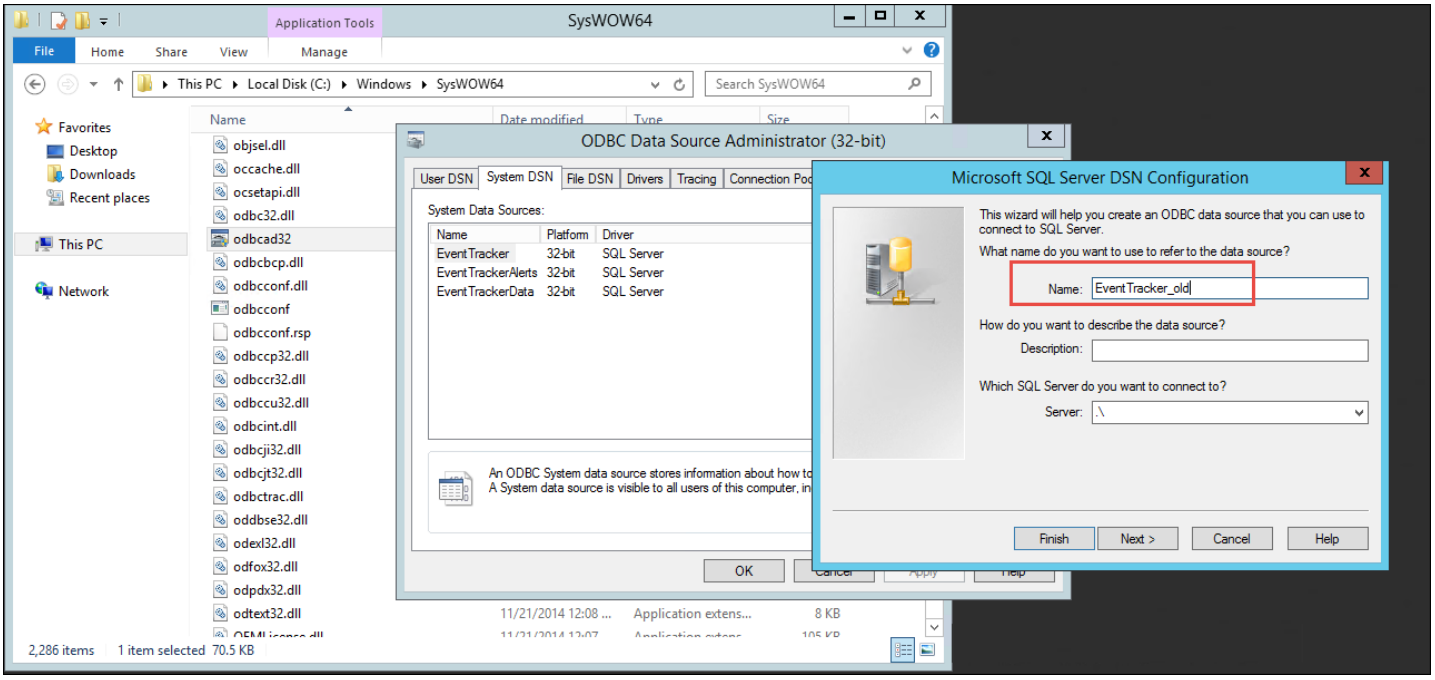

Figure 16

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

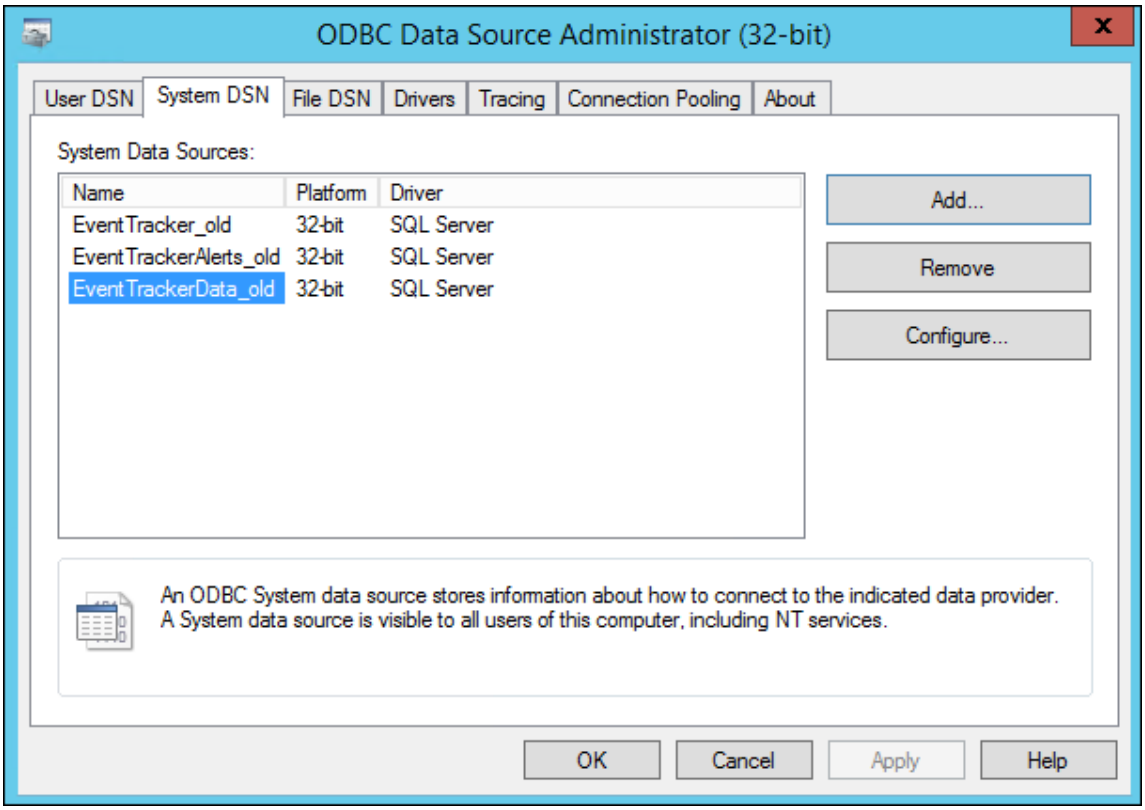

Figure 17

An example of Creating the EventTracker DSN is shown below:

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

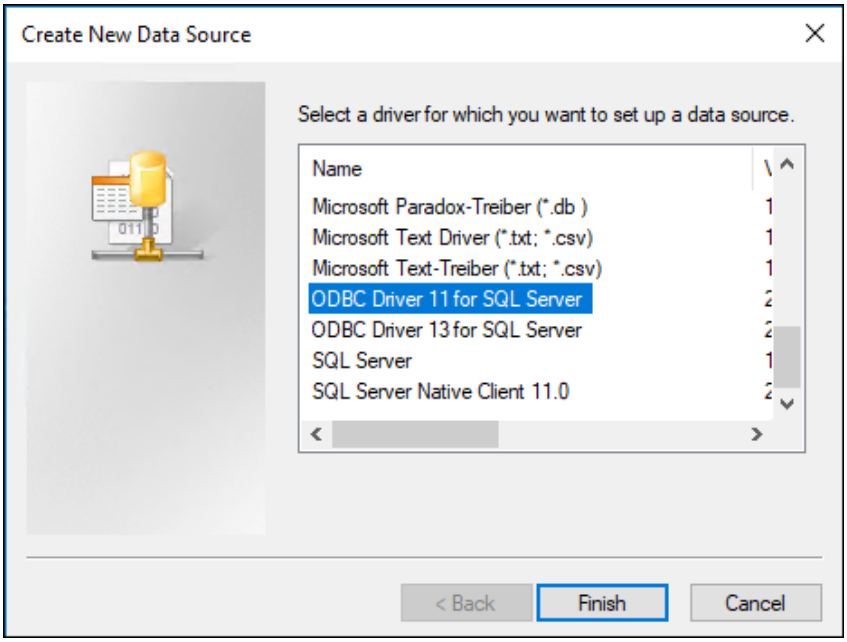

Figure 18

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

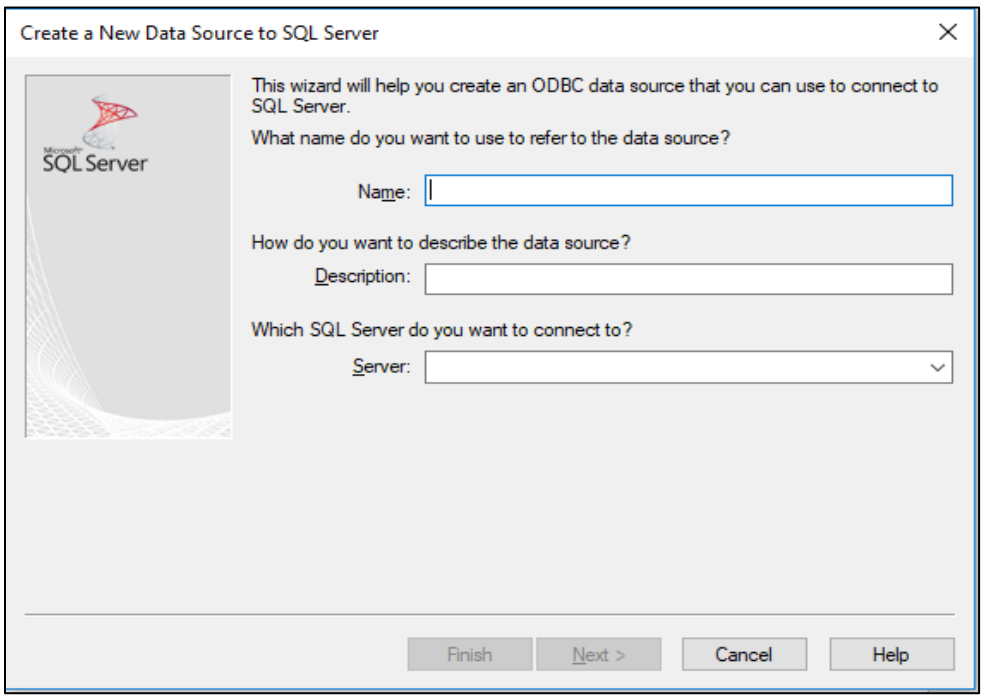

Figure 19

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

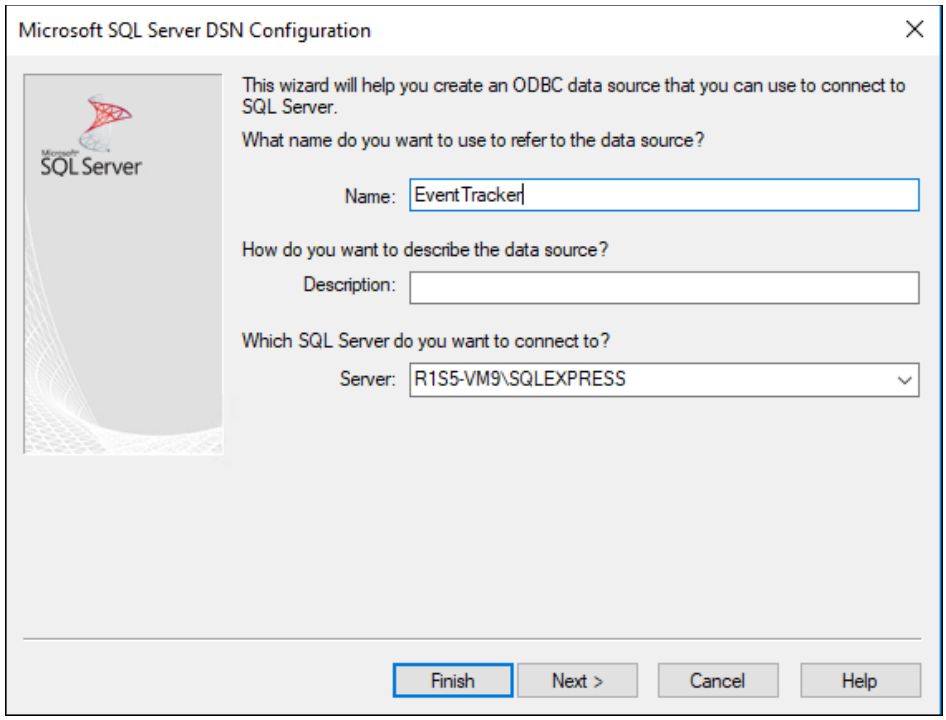

Figure 20

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

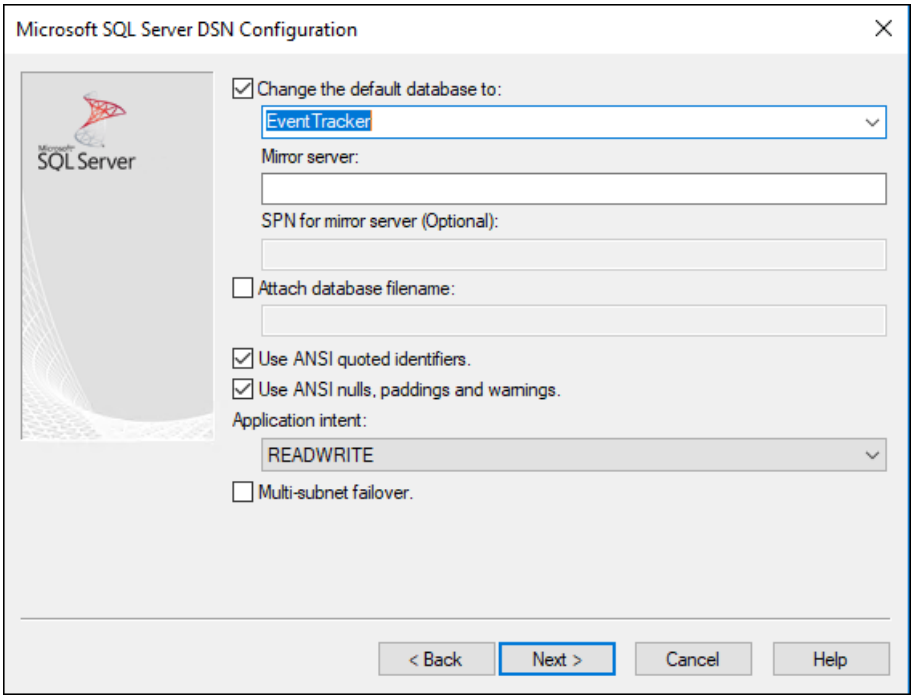

Figure 21

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

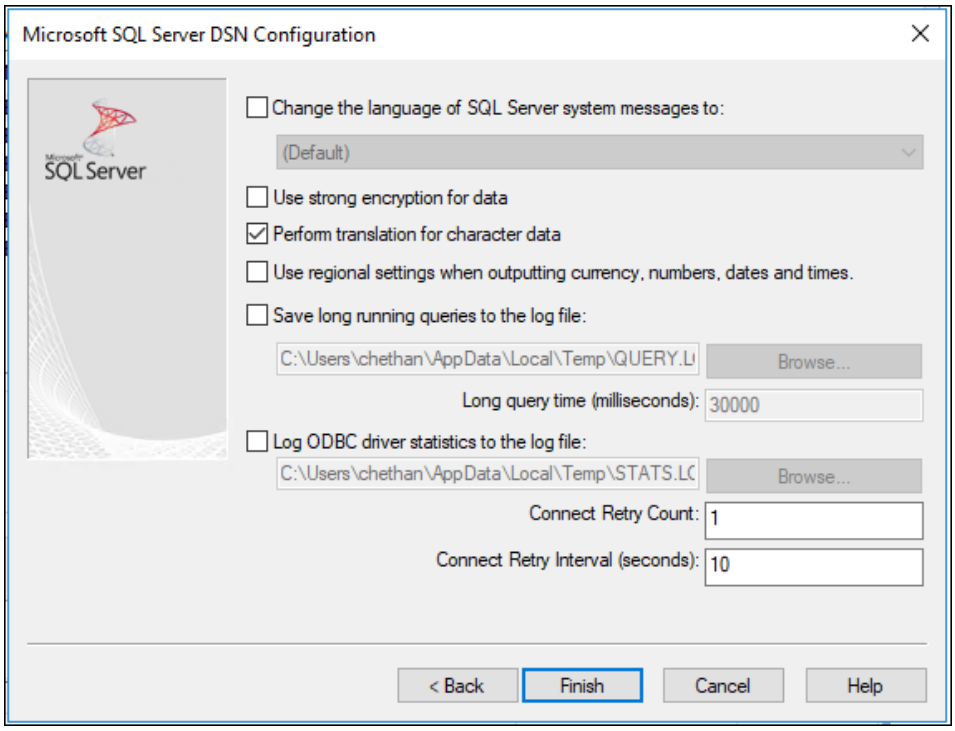

Figure 22

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.

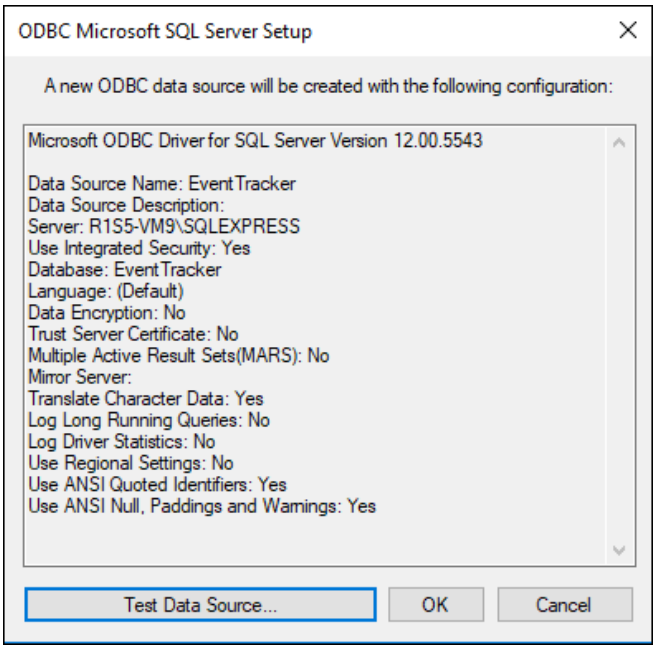

Figure 23

In case of success it will populates below window.

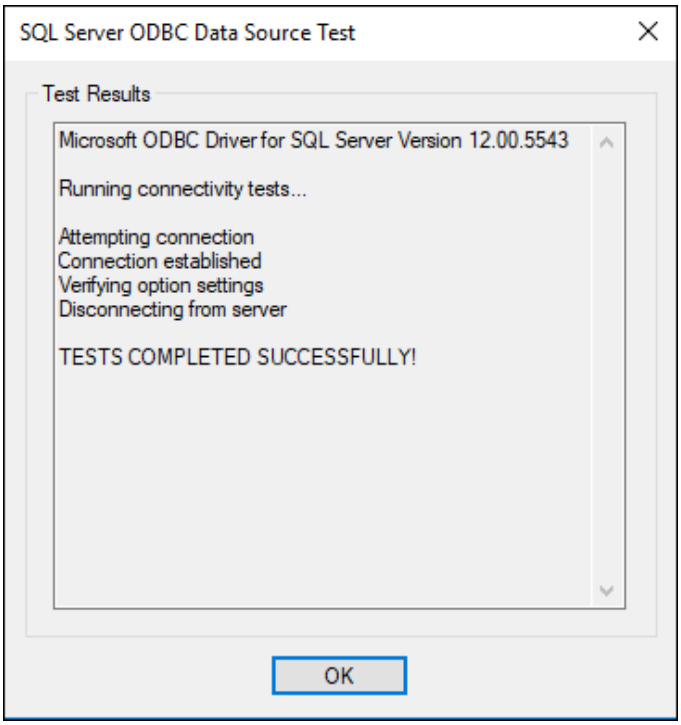

Figure 24

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**

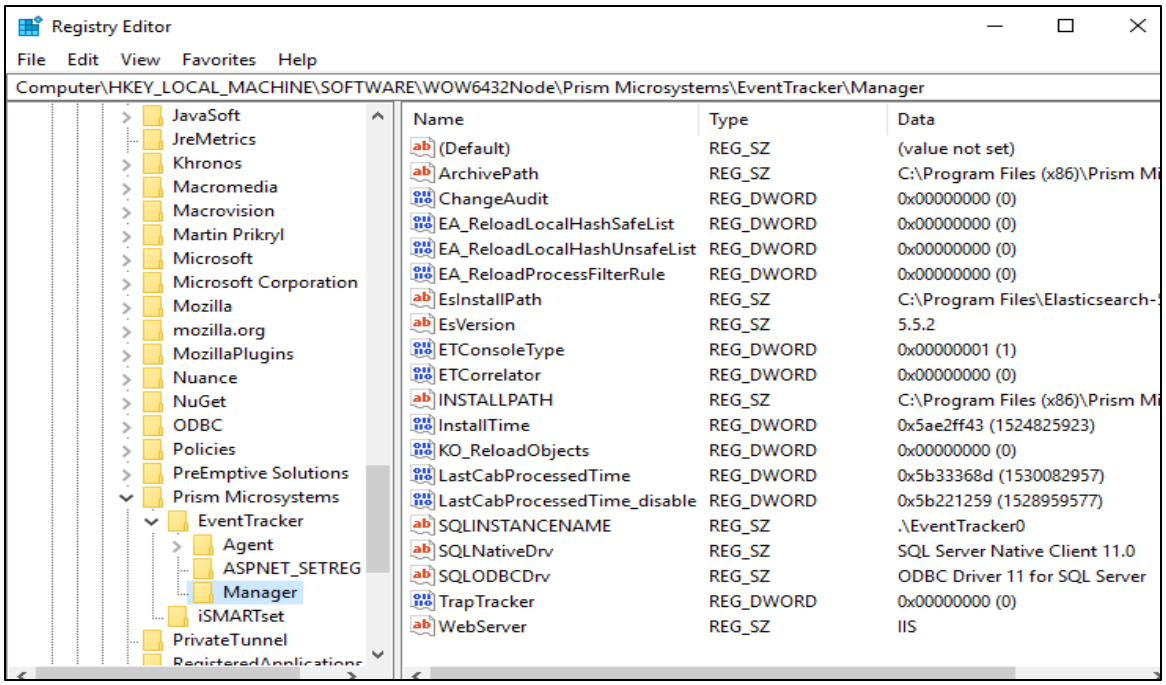

Figure 25

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.

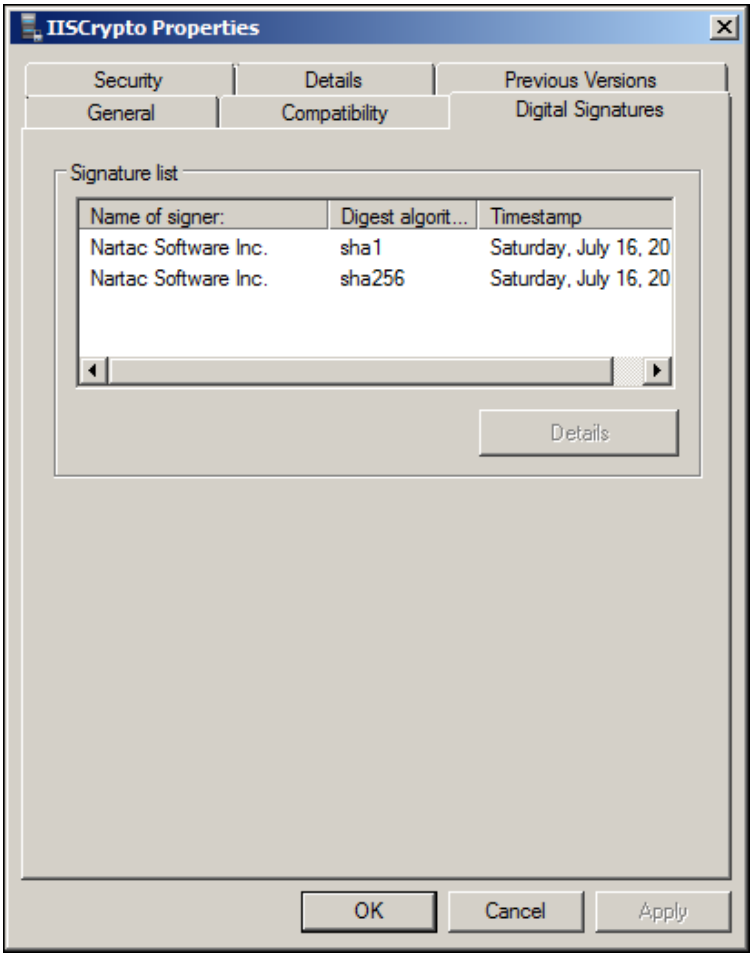

Figure 26

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

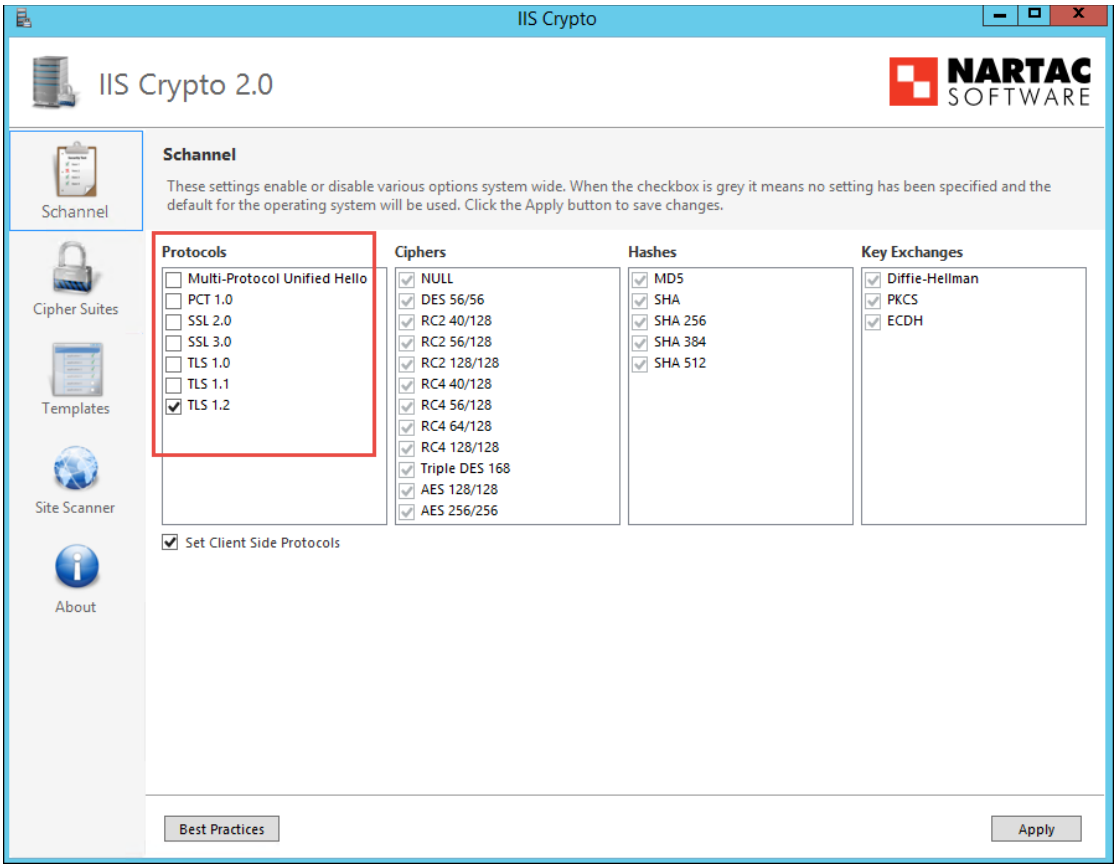

Figure 27

4. 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.

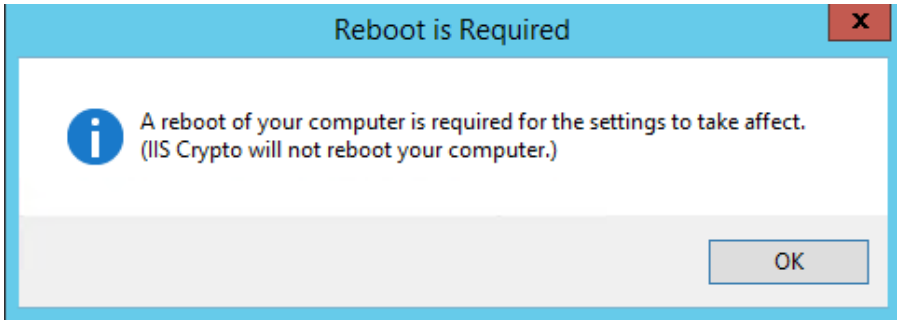

Figure 28

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).

2. 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.

3. 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.