Remote Indexing Feature Guide

EventTracker Version 7.x
Abstract

The purpose of this document is to help users install, configure, and use EventTracker Indexer service on remote machines and index CAB files on the EventTracker Server machine.

Intended Audience

- Users of EventTracker v7.x who wish to deploy EventTracker Indexer service on remote machine to index CAB files on the EventTracker Server thus reducing the workload and improving the performance of the EventTracker Server.

- Technical evaluator of EventTracker who seeks to understand how the feature is implemented and its limitations.

The information contained in this document represents the current view of Prism Microsystems, Inc. on the issues discussed as of the date of publication. Because Prism Microsystems, Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, Inc. and Prism Microsystems, Inc. cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. Prism Microsystems, Inc. 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 Guide may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided. Prism Microsystems, Inc. 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 Prism Microsystems, Inc. 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. © 2014 Prism Microsystems, Inc. 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

Intended Audience ................................................................................................................................ 1

Keyword Indexing ........................................................................................................................................ 3

Pros........................................................................................................................................................... 3

Cons.......................................................................................................................................................... 3

Before You Begin..................................................................................................................................... 4

   To disable EventTracker Indexer Service in services.msc................................................................. 4

Configure Log on Account for EventTracker Services .......................................................................... 11

   Create and Share Archives Folder....................................................................................................... 11

   Enable Database Engine for Remote Connection in SQL 2005......................................................... 23

      To restart SQL Server (SQLEXPRESS) service .................................................................................. 26

   Enable SQL Server 2008/2012/2014 Remote Connections ............................................................... 28

   Synchronize EventTracker Server and Remote Machine ................................................................. 32

      Verify TCP/IP protocol status ........................................................................................................... 32

Steps to follow, when the Firewall is enabled in the EventTracker Server and Client machine: ........... 38

Remote System ......................................................................................................................................... 44

   Create EventTracker System DSN....................................................................................................... 44

   How to Apply the Update?....................................................................................................................... 52

   Manually Index CAB files .................................................................................................................... 55

Verify — EventTracker Server System .................................................................................................. 57
Keyword Indexing

Keywords are unique words or short phrases used to make searching easier. To make the most of this feature, you must know the unique Keyword associated with the logs. CAB files should be there in the server for the Keyword Indexer to index.

By default, Keyword Indexer

1. Indexes all unique words present in the CAB files that are generated. Keywords include unique words found in Event Properties (Standard Columns) and Description

2. Reduces the resource utilizations of the EventTracker Server

3. The Keyword Indexer helps us in speeding up the search results.

When you present search criteria, Reports/Log Search Utility verifies the XML files; if the search criteria are present in the indexed files it returns with the result set of cabs, which needs to be processed. If the cab file is not indexed, then the search happens in the un-indexed cabs along with the indexed cabs.

Pros

- Faster log search improves the performance significantly. Performance measurement depends upon search string too and on an average it can vary from 20% to 500%

Cons

- Indexing CAB files is a resource intensive task. It will take minimum 40 - 50% of CPU usage and minimum 50-60 MB of memory usage thus impacting the performance of the EventTracker Server
Before You Begin

By default, Keyword Indexing Service will be enabled. You need to disable the EventTracker Indexer service in services.msc.

To disable EventTracker Indexer Service in services.msc

1. Click the Start button. Type Run in the search option or select Run.

   Run window displays.

   ![Run window displaying services.msc](Figure 1)

2. In Open text box, enter Services.msc, click OK and then double click EventTracker Indexer.
3. Select **Startup Type** as **Disabled**.

![Figure 2](image-url)
4. Click **Stop**.

5. Click **Apply**, and then Click **OK**.

   The Startup Type for EventTracker Indexer is disabled. Refer Figure 4.
NOTE: Also ensure that the EventTracker Indexer is removed from agent configuration in EventTracker Control panel, before configuring Remote Indexing.

For this,

- Go to EventTracker Control Panel.
- Double click on EventTracker Agent Configuration.
• Click on the Services tab and select EventTracker Indexer from the list displayed.
Click the **Remove** button.
A pop-up confirmation message displays.
• Click **Yes**.

• For saving the changes, click the **Save** button in the Agent Configuration window.

![EventTracker Agent Configuration Window](image)

*Figure 8*
Configure Log on Account for EventTracker Services

EventTracker service account must be changed to user account that has been assigned permission on shared EventVault storage folder. For Example: `toons\Karen`

- Event Correlator (If it is Available)
- EventTracker EventVault
- EventTracker Reporter
- EventTracker Scheduler

After configuring the services, restart it using the User Credentials.

Create and Share Archives Folder

**NOTE:** Creating and Sharing Archives folder steps can be skipped if EventVault Storage folder is already configured to use UNC path.

- For users who wants to share the existing Archive folder in `...\Program Files\Prism Microsystems\EventTracker\Archives`.

1. Right-click on the existing archive folder, and then select **Properties**.

2. Click the **Sharing** tab to share the existing **Archives** folder (`\systemname\Archives`).
3. Click the **Security** tab to grant **Full Control** permission to the remote user.

**NOTE:**

You are requested to share it with relevant users only.
Verification: Go to remote machine and verify if the user is able to access the shared folder created in the EventTracker Server machine or not.

1. Set the Archives path as UNC (Uniform Naming Convention) path.

   **NOTE:** Follow the below mentioned steps -
   
   a) Double click and open **EventTracker Control Panel**, select **EventVault**.
   
   b) Select **Configuration** on the EventVault Warehouse Manager console.
c) Click the **Browse** button.

Choose Directory window displays.

Type the correct UNC path (i.e. `\systemname\Archives`) of the existing Archives folder in the **Vault Storage Folder** field.

(OR)

d) Click the **Network** button.
Select the event vault storage folder.

Click OK.

NOTE:

The number of archives may vary.

Click NO.
NOTE: As the path remains the same and only we have configured it as a UNC path, so it is not required to move the cab files.

Once the archive path is changed, you will get the following message.

![Figure 14](image)

If you click on Yes, as per the Figure 13, and then Click Move, you will get the following screen:

![Figure 15](image)

NOTE: In this case, the cab status fails, as the cabs are already present in the existing path.
h) Click **Close**.

5. Click the **Close** button in *EventVault Warehouse Manager* window.

**NOTE:**

As per the above example, the cab files were stored in the following path, i.e. ...
\Program Files\Prism Microsystems\EventTracker\Archives..

After sharing the Archives (UNC path), whenever a new cab file gets created, it gets stored in the same location but it is represented as \systemname\Archives. (For example: \MCLOON\Archives)

- For user who wants to create a New Archives Folder in the custom path-

  1. Create a folder on local drive, right-click the folder, and then select **Properties**.

     For example: 'New Archives'.

  2. Click the **Sharing** tab to share the **New Archives** folder.
3. Click the **Security** tab to grant **Full Control** permission to the remote user.

**NOTE:**

You are requested to share it with relevant users only.
Verification: Go to remote machine and verify if the user is able to access the shared folder created in the EventTracker Server machine or not.

4. To create a new Archive folder, set the Archives path as UNC (Uniform Naming Convention) path.

**NOTE:** Follow the below mentioned steps, if you are creating a new Archive folder.

a) Double click and open EventTracker Control Panel, select EventVault.

b) Select Configuration on the EventVault Warehouse Manager console.
c) Click the **Browse** button.

Choose Directory window displays.

Type the correct UNC path of the Archives folder in the **Vault Storage Folder** field.

(OR)

**Figure 19**

(OR)

d) Click the **Network** button.
e) Select the event vault storage folder.

f) Click OK.

NOTE:

The number of archives may vary.

g) Click Yes.
h) Click **Move**.
i) Click Close.

5. Click the Close button in EventVault Warehouse Manager window.

Enable Database Engine for Remote Connection in SQL 2005

SQL Server Browser Service must be running and Database Engine must support Remote Connection

1. Select the Start button, select All Programs, and then select Microsoft SQL Server 2005.
2. Select Configuration Tools, and then select SQL Server Surface Area Configuration.
3. Select Surface Area Configuration for Services and Connections.
4. Expand the **SQLEXPRESS** node, select **Database Engine**, and then select **Remote Connections**.

4. Expand the **SQLEXPRESS** node, select **Database Engine**, and then select **Remote Connections**.

![Surface Area Configuration for Services and Connections](image)

Figure 25

5. Select **Local and remote connections**, select **Using TCP/IP only**.
6. Select the **Apply** button. The **Connection Settings Change Alert** window displays.
7. Select the **Apply** button, and then select **OK**.

**NOTE:** Make sure that the SQL Server browser service is **Started**.

**To restart SQL Server (SQLEXPRESS) service**

2. Click the **Start** button. Type **Run** in the search option or select **Run**.

Run window displays.
3. Enter ‘Services.msc’ and then click **OK**.

4. Select **SQL Server (SQLEXPRESS)** and the **SQL Browser**, and then select **Restart** the service.
Enable SQL Server 2008/2012/2014 Remote Connections

1. Select the **Start** button, select **All Programs**, and then select **Microsoft SQL Server 2008/2012/2014**.

2. Select **SQL Server Management Studio Express**.

3. Right click the server name, and then click **Properties**.

![Figure 31](image_url)
SQL server displays **Server Properties** window.
4. In ‘Select a page’ pane, click Connections.
5. Ensure that 'Allow remote connections to this server' checkbox is selected. If not then select the checkbox to enable remote connections.
Synchronize EventTracker Server and Remote Machine

Verify TCP/IP protocol status

- For Windows Server 2008/2008 R2/Windows 7

1. Select the **Start** button, select **All Programs**, and then select **Microsoft SQL Server <Version>**.

![Figure 35](image)

OR

- For Windows 8/8.1/2012 R2, Click on Windows key and Search- **SQL Server Configuration Manager**.

**NOTE**: If the search does not show any result, the SQL server configuration Manager can be found in the following location:

`C:\Windows\System32 \ SQLServerManager10.msc`
The SQL server manager number can vary depending upon the version of SQL installed. For Example: It can be SQLServerManager12.msc also.

Figure 36

2. With respect to the operating system selected, the below window is displayed when you click on the Configuration Manager.

Figure 37

3. Expand SQL Server Network Configuration node, right click on Protocols for SQLEXPRESS, and then click Open.

(OR)
Double click on **Protocols for SQLEXPRESS**.

![Figure 38](image1)

Right pane displays protocol name and their status.

![Figure 39](image2)

4. After Remote Indexing is configured, TCP/IP protocol status should be **Enabled**. If it is disabled, then right click **TCP/IP**, and then click **Enable**.

   SQL server displays a Warning message.
5. Click OK.

Depending on the operating system, follow the above steps mentioned as per Figure 35 and Figure 36.

For Example-

1. Click on Configuration tool and select SQL Server Configuration Manager.
2. Expand the SQL Native Client 10.0 Configuration (32 bit).

- Select Client Protocol.
• Double click the TCP/IP option.
• Enter the Port number.
  In this example, the Port used is ‘1433’
• Select ‘Yes’ for Enabled option (if not selected).
• Click OK.

Now, expand the **SQL Server Network Configuration** option and select the Protocols for SQL on which EventTracker is running, as shown in the figure below:

![Figure 44](image)

• Double click the **TCP/IP** option and select ‘Yes’ for **Enabled** option (if not selected).

![Figure 45](image)
- In the **IP Address** tab, go to the **IP All** section and make sure the TCP port is same i.e. ‘1433’.

![TCP/IP Properties](image)

- Click the **OK** button.

**Steps to follow, when the Firewall is enabled in the EventTracker Server and Client machine:**

For creating an inbound rule for TCP port:

- Go to **Start > Control Panel > Windows Firewall.**
• Click on Advanced Settings.

The Windows Firewall with Advanced Security page displays.

• Select the Inbound Rules option, go to the Action pane and select New Rule.
The **New Inbound Rule Wizard** displays.

- Select the **Port** option and click **Next**.
• Select the TCP option (if not selected) and click on ‘Specific local ports’.
• Enter the port number – ‘1433’ and click Next.

Figure 50

• In the Action pane, select ‘Allow the connection’ (if not selected) and click Next.
• In the Profile section, enable all the options i.e., Domain/Public/Private and click Next.
In the Name section, the user can enter the **Name** and **Description** (as per preference) and click **Finish**.

![Figure 53](image)

The TCP port gets displayed in the Windows Firewall and Advanced Security page.
Remote System

Create EventTracker System DSN

1. Click the **Start button**, select **All Programs**, and then select **Settings**.

2. Select **Control Panel**, select **Administrative Tools**, and then select **Data Sources (ODBC)**.

   **NOTE:**
   
   In case of 64 bit operating system launch `odbcad32.exe` available in `%windir%\SysWOW64\` folder.

3. Click the **System DSN** tab, and then click **Add**.
5. Scroll-down and select **SQL Server**.
**Verification:** Make sure SQL Browser service is running in the EventTracker server machine.

6. Click **Finish**.

7. Enter/select appropriately as shown below.

   ![Create a New Data Source to SQL Server](image)

   If the system name alone is displayed in the Server drop-down list, for example, ESXWEBDOC then append `\SQLEXPRESS` with the server name.

   **Verification:** From Remote machine, user should be allowed to access EventTracker server SQL databases and tables.

8. Click **Next**.
NOTE: For users, who have enabled firewall on both the EventTracker server machine and client machine, click the Client Configuration... option.

The Edit Network Library Configuration page displays.

- Select TCP/IP option and uncheck the dynamically determine port option.
- Enter Port number as “1433”.

Figure 58

Figure 59
9. Now, proceed from *Figure 58* and click **Next >**.

10. Select the **Change the default database to** drop-down, and then select **EventTracker** from the drop-down list.

11. Click **Next >**, and then click **Finish**.
NOTE: While creating EventTrackerData System DSN, select EventTrackerData from the Change the default database to drop-down list.
12. Click the **Test Data Source** button to display the test Results.

![Test Data Source Result](image)

*Figure 63*

13. Click **OK**.

Similarly to create **EventTrackerData** System DSN,

All the steps remain same from Figure 55- Figure 63 except Figure 57 and Figure 60 wherein we need to mention the name as EventTrackerData and select the default database to EventTrackerData. The changes are displayed below:

![Microsoft SQL Server DSN Configuration](image)

*Figure 64*
And also select the ‘**EventTracker data**’ from the dropdown list as per Figure 60. The Figure is displayed below:

![Figure 65](image)

After the configuration process gets complete, ‘**EventTracker**’ as well as the ‘**EventTracker data**’ will be displayed as per the figure below:

![Figure 66](image)

14. Click **OK**.
How to Apply the Update?

Please contact Prism Office-Sales department to get Remote Indexer Update.

1. Click the Contact hyperlink on the EventTracker Enterprise login page.

   EventTracker redirects to the Prism Contact Us page.

2. From Location/Direction pane, note the Product Sales contact number.
3. Please contact Sales office and place your request of **Remote Indexer Update**. The Sales team will send you the patch file on your registered Email ID.

4. Save the update file in a system wherein you want to install the Remote Indexer.

5. Launch **RemotelIndexer.exe** from saved path.

   You will get a confirmation message.

   ![Figure 68](image)

6. Click **Yes**.

   Successful installation of EventTracker Indexer service is displayed.

   ![Figure 69](image)

7. Open the `services.msc` to check if the **EventTracker Indexer** service is running.
Indexer Console runs with logged in user credentials. Therefore, the logged in user must have full access (read/write) to the shared folder (Archive Path and Keyword Index Directory) and EventTracker Server database (EventTracker, EventTrackerData)

Indexer Service account must be changed to user credentials which has been given permission to shared folders and database

8. Right-click the service and change the user credentials.

9. Click Apply and then OK.
10. Restart the service as advised on the message box.

**Mandatory steps to be followed:**

In 64 bit system, create a folder in the registry in the following path

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Prism Microsystems\EventTracker\Manager

In 32 bit system, create a folder in the registry in the following path

HKEY_LOCAL_MACHINE\SOFTWARE\Prism Microsystems\EventTracker\Manager

In Manager Folder, create a new ‘String Value’ key as ‘SQLINSTANCENAME’. Provide the EventTracker Server’s SQL instance name as the value. The SQL instance name should be same as on EventTracker Server. This can be found under EventTracker manager path.

Ex: From EventTracker Server machine, if you have copied /SQLEXPRESS as the instance name, please remove (.) DOT and replace it by the EventTracker Server machine name or EventTracker Server IP address.

**Manually Index CAB files**

If there are existing un-indexed CAB files, you need to index them manually.

1. In Keyword Indexer, select the **Start Time** and **End Time**, and then select **Index Now**.

Keyword Indexer displays confirmation message.
NOTE:
The number of cab files may vary.

2. Click Yes.

Keyword Indexer enables 'Stop Indexing' button.

NOTE:
Click Stop Indexing to stop the indexing process

3. Click the Save button to save the configuration.
Verify – EventTracker Server System

1. Open the Keyword Indexes folder \<installed path>\EventTracker\Archives\<port>\<year>\<month>\index\<CabName>.xml
   
   For Example: \<systemname>\NewArchives\14505\2011\8\Index

2. Check if index files are being created.

   ![Cab file folder](image)

   **Figure 75: Cab file folder**

   **NOTE:**

   If EventTracker Server machine is in domain 1 and Remote Indexer machine is in Domain 2, remote indexing will not work.