

Command Line Log Search

EventTracker
Version 7.x

ABSTRACT

This document describes how to perform log search from Command prompt for EventTracker v7.x versions. Command line log search is an excellent tool to generate ad-hock reports for specific needs. Presently it generates a report and intermediate database is deleted. This database is retained at specific location and it can be used for analytic purpose.

AUDIENCE

EventTracker users who wish to perform log search via command line.

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 must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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, 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.

© 2013 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Command Line Log Search 3
 Examples for command line log search 5

Command Line Log Search

1. Click the **Start** button; enter **Run** in **Search** window to navigate to the command prompt.
2. Type **cmd**, and then click **OK**.
3. Navigate to the folder where EventTracker is installed i.e. EventTracker\AdvancedReports folder.

For example:

\\<<systemname>>\Program Files\Prism Microsystems\EventTracker\AdvancedReports folder.

4. Run the **Prism.Reports.ServiceProcessor.exe** with an appropriate search string.

Command line log search statement format is mentioned below:

Prism.Reports.ServiceProcessor.exe <from date time> <to date time> <search criteria> <is export to pdf > <is persist the temp data> <temp db retain path> <records limit>

<from date time>: from date time

<to date time>: to date time

<search criteria>: search criteria to process

<is export to pdf>: if set to true then pdf file will generate of searched data

<is persist temp data>: if set to true then temp access database file will retain

<temp database retain path>: file path where to retain the temp access database file

<records limit>: if this count is mentioned then processing will stop after processing this much records.

The process will not stop immediately as process will check this count after each cab is processed. So this count may vary.

NOTE:

- **All the parameters must be placed within double quotes**
- **First two parameters are mandatory**

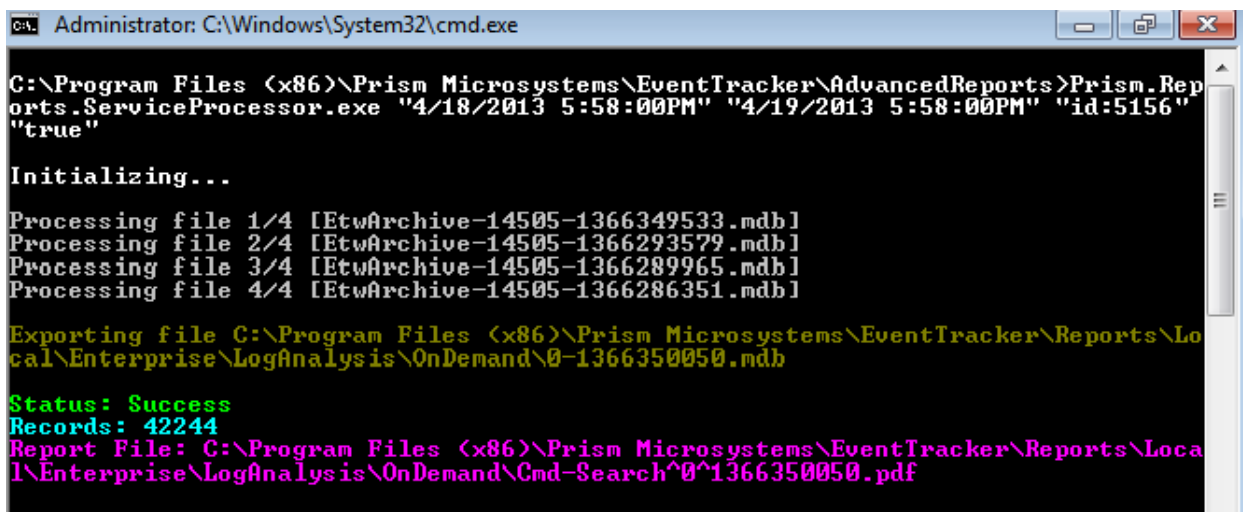
- **Parameters sequence must be maintained in order** i.e. From Date, To Date, Search String and Export (false/ true)
- Search string and Export is optional. If search string is absent then it will consider all the events within the specified time range. If export value is absent then by default it's false.
- Processing is interactive. During each cab file processing it will indicate the status
- After processing is over output is written to the console. It will contain the following keys
 - ❖ **Status:** It can contain any of the following values: **Success, NoRecordFound, Failed, Cancelled**
 - ❖ **Records:** Total no of records found
 - ❖ **Report Database:** If export is false then it will contain the database path with file name
 - ❖ **Report File:** If export is true then it will contain exported file path with name
 - ❖ **Exception:** If any error comes during processing then it will be present under this section

Examples for command line log search

Example 1:

```
Prism.Reports.ServiceProcessor.exe "4/18/2013 5:58:00 PM" "4/19/2013 5:58:00 PM" "id:5156" "true"
```

The corresponding output is



```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files (x86)\Prism Microsystems\EventTracker\AdvancedReports>Prism.Reports.ServiceProcessor.exe "4/18/2013 5:58:00PM" "4/19/2013 5:58:00PM" "id:5156" "true"

Initializing...

Processing file 1/4 [EtwArchive-14505-1366349533.mdb]
Processing file 2/4 [EtwArchive-14505-1366293579.mdb]
Processing file 3/4 [EtwArchive-14505-1366289965.mdb]
Processing file 4/4 [EtwArchive-14505-1366286351.mdb]

Exporting file C:\Program Files (x86)\Prism Microsystems\EventTracker\Reports\Local\Enterprise\LogAnalysis\OnDemand\0-1366350050.mdb

Status: Success
Records: 42244
Report File: C:\Program Files (x86)\Prism Microsystems\EventTracker\Reports\Local\Enterprise\LogAnalysis\OnDemand\Cmd-Search^0^1366350050.pdf
```

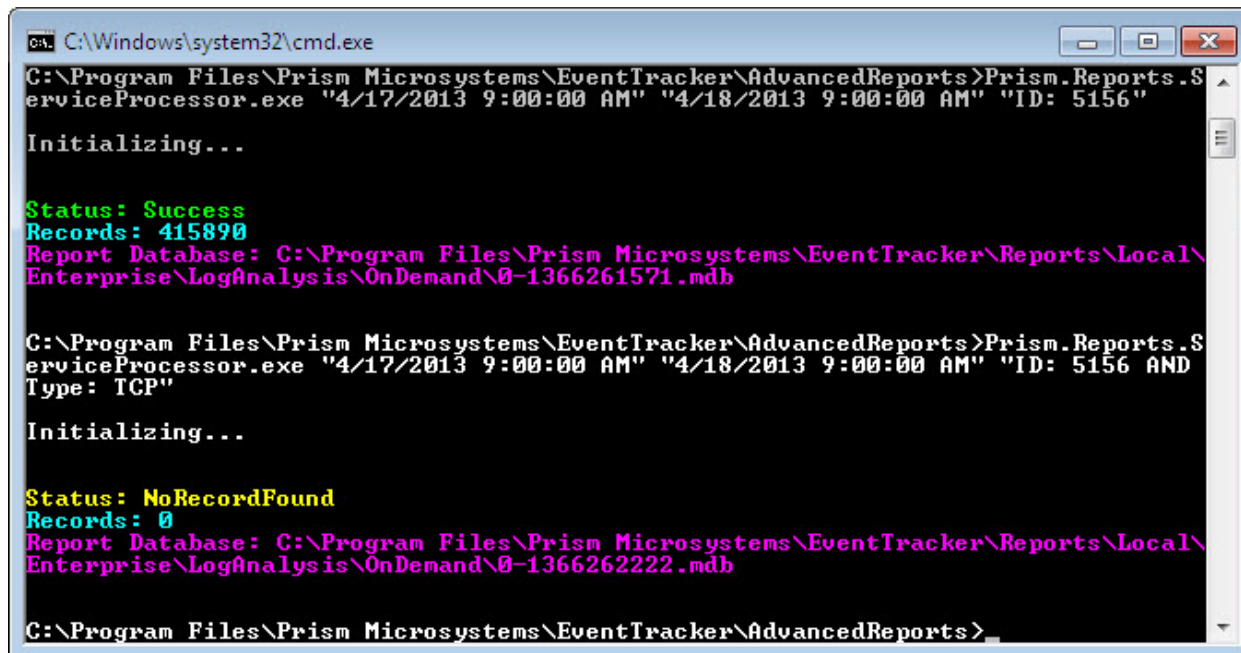
Figure 1

You can view the output in corresponding path/location in PDF or .mdb format. Refer Figure 1.

Example 2:

```
Prism.Reports.ServiceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID:5156 AND Type: TCP"
```

The corresponding output is



```
C:\Windows\system32\cmd.exe
C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>Prism.Reports.ServiceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156"
Initializing...
Status: Success
Records: 415890
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\Enterprise\LogAnalysis\OnDemand\0-1366261571.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>Prism.Reports.ServiceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 AND Type: TCP"
Initializing...
Status: NoRecordFound
Records: 0
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\Enterprise\LogAnalysis\OnDemand\0-1366262222.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>
```

Figure 2

Example 3:

Prism.Reports.ServiceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 OR Type: TCP"

The corresponding output is

```

C:\Windows\system32\cmd.exe
erviceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 AND
Type: TCP"

Initializing...

Status: NoRecordFound
Records: 0
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\
Enterprise\LogAnalysis\OnDemand\0-1366262222.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>Prism.Reports.S
erviceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 OR T
ype: TCP"

Initializing...

Status: Success
Records: 466116
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\
Enterprise\LogAnalysis\OnDemand\0-1366263494.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>
    
```

Figure 3

Example 4:

Prism.Reports.ServiceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 OR Type: TCP" "false"

The corresponding output is

```

C:\Windows\system32\cmd.exe
erviceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 OR T
ype: TCP"

Initializing...

Status: Success
Records: 466116
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\
Enterprise\LogAnalysis\OnDemand\0-1366263494.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>Prism.Reports.S
erviceProcessor.exe "4/17/2013 9:00:00 AM" "4/18/2013 9:00:00 AM" "ID: 5156 OR T
ype: TCP" "false"

Initializing...

Status: Success
Records: 466116
Report Database: C:\Program Files\Prism Microsystems\EventTracker\Reports\Local\
Enterprise\LogAnalysis\OnDemand\0-1366264223.mdb

C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports>
    
```

Figure 4