

EventVault explorer, Behavior and Tile Dashboard enhancement

EventTracker Enterprise v8.2

EventTracker 8815 Centre Park Drive Columbia MD 21045 www.eventtracker.com

Publication Date: Aug.1, 2016

Abstract

This document is to guide you with the enhancements given in the Product Update: **ET82U16-014**, for the various modules.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.2.

Audience

EventTracker v8.2 users.

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.

© 2016 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

| \bstract | 1 |
|-----------------------------|---|
| Scope | 1 |
| Audience | 1 |
| Tiles Dashboard | 3 |
| Tiles Flip | 3 |
| Unknown Process Dashboard | 5 |
| Add to Filter | 5 |
| Top Level Summary Dashboard | 7 |
| EventVault Explorer | 8 |



Tiles Dashboard

Tiles Flip

If total incident count is equal to the acknowledged count then tile will be flipped informing that this tile is of least importance.

A user visiting Tiles dashboard will be interested to know incidents which are important to him and needs attention. In the current scenario, such incident might be scattered and difficult to find.

Tile Flip for those tile(s) will make the process hassle-free so that other incidents get noticed.

NOTE: The auto refresh time for tiles is set to 120 seconds, by default.

To use Tile Flip,

- Login to EventTracker web.
- Navigate to Incidents > Tile View.

| INCIDENTS Updated 04:01:37 PM Inc | i dents from 07/11/2016 04:01:37 PM - 07/12/2016 04:0 | 1:37 PM DURATION |
|---|--|--|
| DASHBOARD GRAPH TABULAR TIL | E | (i) Total: 821 Last 1 Day |
| | | |
| SITES GROUP SORT BY | TOP 20 Search by alert name QQ | t |
| Subscription Subscription< | EventTracker: Detected new bad reputati 2 ③ Jul 12 02:41:17 PM ④ ② ③ ② ● ③ ③ ● ③ □ 1 ♣ ○ ● ③ ● ③ ● ③ | EventTracker: New process MD5 hash act 352 ③ Jul 12 02:35:13 PM ③ 333 ③ 333 ● 0 □ 1 ▲ 0 第二 Ø |
| EventTracker: Unknown MDS hash detect 145 ③ Jul 12 02:35:22 PM 145 ☑ 129 ☑ 129 Ⅰ 1 Ⅰ 0 □ 1 ♣ 0 플 27 🚰 40 🎽 | EventTracker: Out of ordinary process lau 99 ○ Jul 12 03:52:00 PM ✓ 89 ? 0 ! 0 ✓ 89 ? 89 ! 0 ! 0 □ 1 ♣ 0 : : . . . | EventTracker: Browser connecting to non 小 57 ③ Jul 12 11:17:11 AM ✓ 57 ☑ 57 I 0 □ 1 ♣ 0 플 27 🔅 |
| EventTracker: Unsafe MD5 hash detected | EventTracker service down 0 Jul 12 02:13:34 PM ✓ ✓ ● ! ● ✓ ✓ ✓ ● ! ● ✓ ✓ ✓ ● ! ● ✓ ✓ ✓ ● ! ● | EventTracker: Non reporting system(s) wi 4 |
| EventTracker: Out of ordinary process lau 146 Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" Image: Colspan="2">Image: Colspan="2" Image: Colspan="2" Image | EventTracker: Non reporting system(s) wi 4 | |
| EventTracker | Server Time: 07/12 04:01:37 PM | Response: 0.79 secs © 1999 - 2016 EventTracker |
| | Figure: 1 | |



When the incident count becomes equal to the acknowledged count, the tile gets flipped. In the below displayed example, the total incident count is equal to the acknowledged count i.e. 57.



Thus, the tile gets flipped displaying the count. This is shown below:



Figure: 3

Click the 📶 icon to unflip and see the incident detail.



Unknown Process Dashboard

Add to Filter

'**Add to filter**" option has been provided in unknown process dashboard under details window which allows the user to select Signed by, Product name, Product version, File name, File version, Image file path, Parent Process name, Parent image file path, which will get displayed in the unknown process filter page for respected text box, with the editing option. Thus, the users' job of manually entering the particulars gets minimized.

NOTE: The 'Add to filter" option is available only for Console types.

To use this option,

- Login to EventTracker web.
- Select the **Dashboard** option in the menu bar and click **Threats** from the dropdown list.
- Select the Unknown Processes tab.
- Select a process name and expand the process detail. The '**Add to filter**" option gets displayed at the right hand side corner. This is shown in the figure below.

| THREATS | | | Period 07/13 12:04 PM - 07/14 12:04 PM Refreshed a | t 07/14 12:04 PM |
|--|-----------------------------|-------------------|--|------------------|
| ATTACKERS TARGETS UNKNOWN | PROCESSES | | | |
| PRODUCT: MICROSOFT® WINDOWS® OPERATING SY | STEM | | Total Processes: 157 | 1 := |
| E LOGTIME PUBLISHER NA | ME | ✓ FILE NAME | ✓ SYSTEM NAME | ~ ^ |
| - 07/14/2016 12:58:08 PM N/A | | wecapi.dll | SVR2012VM01 | |
| FILE DETAILS | | | Add | I to filter |
| File Description Event Collector Configuration | n API File Size | 82 KB File | Version 6.3.9600.16384 | |
| Product Name Microsoft® Windows® Oper | ating Syste Product Version | 6.3.9600.16384 MD | 5 Hash 98C816466FE7EE0AE7B1A302EFF7BD34 | |
| PROCESS DETAILS | | | | |
| Parent Process Name mmc.exe | User Name | TOONS\sanjay | File Modified On 8/22/2013 9:59:40 AM | |
| Parent Image File Path C:\Windows\System3. | 2\mmc.exe | | | |
| Command Line N/A | zwecapi.dii | | | |
| SIGNATURE DETAILS | | | | |

Figure: 4

• Click the 'Add to filter' hyperlink. The below window gets displayed.



| \dd s | elected checkbox infor | mation to unknown process filters | X |
|-------|------------------------|--------------------------------------|---|
| | SELECT ALL | | |
| ✓ | Signed By | N/A | |
| ✓ | Product Name | Microsoft® Windows® Operating System | |
| | Product Version | 6.3.9600.16384 | |
| ✓ | File Name | wecapi.dll | |
| | Image File Path | C:\Windows\System32\wecapi.dll | |
| ✓ | Parent Process Name | mmc.exe | |
| ✓ | Parent Image File Path | C:\Windows\System32\mmc.exe | |
| | File Version | 6.3.9600.16384 | |
| | | OK CLEAR CLOS | E |

Figure: 5

- The Product Version, File Version and Image File path are dynamic fields, so the fields are kept unchecked, by default.
- Select the respective check boxes as per requirement and click **OK**.



| UNKNOWN PRO | CESS FILTERS | | | |
|------------------------|--------------|---|--|----------------------------|
| RULE NAME | DESCRIPTION | | ADD TO RULE GROUP Default 🕑 🗹 ACTI | VE 🕒 🕑 |
| | OPERATOR | | VALUE | |
| SIGNED BY | Equals | ~ | N/A | |
| SIGNED | Select | ~ | | |
| PRODUCT NAME | Equals | ~ | Microsoft® Windows® Operating System | |
| PRODUCT VERSION | Select | ~ | | |
| FILE NAME | Equals | ~ | wecapi.dll | |
| IMAGE FILE PATH | Select | ~ | | |
| PARENT PROCESS NAME | Equals | ~ | mmc.exe | |
| PARENT IMAGE FILE PATH | Equals | ~ | C:\Windows\System32\mmc.exe | |
| FILE VERSION | Select | ~ | | |
| | | | | SAVE CLEAR |
| EventTracker | | | Server Time: 07/14 02:53:47 PM Response: 0.49 secs | © 1999 - 2016 EventTracker |

Figure: 6

NOTE: The operator for each component or field is set to 'Equals" by default. The user can change the operator as per his requirement.

- The selected fields gets added automatically which can further be edited.
- Edit the changes, if required and click the **Save** button.

Top Level Summary Dashboard

Previously, the TLS summary, Log Volume report only displayed the Event Count and Computer column. Once the **Product Update-ET82U16-014** is applied by the user, the TLS report will have Real Time and File Transfer columns for Event count and Computer count. A sample report is shown below:



| Log Volume | | | | | | |
|------------------------|-------------------------|-----------------------------|----------------|----------------------------|--------------------------------|-------------------|
| Report Date 🛛 🔽 | Real time event count 💌 | File transfer event count 💌 | Total events 💌 | Real time computer count 🔽 | File transfer computer count 💌 | Total computers 💌 |
| 07/25/2016 11:59:59 PM | 39015 | 90977 | 129992 | 1 | 1 | 2 |
| 07/25/2016 11:59:59 PM | 39015 | 90977 | 129992 | 1 | 1 | 2 |
| 07/25/2016 11:59:59 PM | 39015 | 90977 | 129992 | 1 | 1 | 2 |
| | | | | | | |
| | | | Figure: 7 | | | |

NOTE: After applying the Update, the TLS Report will display no data until the earlier configured reports are generated, at least once.

EventVault Explorer

With the new User Interface enhancement provided in **Product Update-ET82U16-014**, the EventVault Explorer will now support the following changes:

- Faster Data loading
- Quick access to columns with the top records.
- Time Selection options (Quick, Relative and Absolute).
- Expand and Collapse for the available column option.
- Include/Exclude metadata from available columns.

To use the new enhancement in EventTracker Explorer,

1. Navigate to **Reports > Explorer**.

| Event¥ault Explorer - Inter | net Explorer | | | | | | | | | |
|-----------------------------|---------------|-------------------------------|--------------|---------------|-----------------------|-------------------|-------------------|-----------|-----------|--|
| | EVENT | VAULT EXPLO | RER | | CONFIGURAT | TION | | | | |
| | FLEX HISTOR | Y NEW SEARCH | SEARCH HIST | ORY | | | | | | |
| | Search by | Report title | | ۹۹ | | | | | | |
| | + | REPORT TITLE | ВҮ | FREQUENCY | LAST UPDATED TIME | FROM DATE | TO DATE | SIZE [MB] | COUNT | |
| | + <u>11</u> Û | Logs - Detail-persist | mahaabooar | Last 24 hours | 05:19:15 PM Thu 07/28 | 07/22 12:27:00 PM | 07/28 05:08:00 PM | 4 | 5,192 | |
| | ÷ <u>†</u> | category Logs - Detail | | Last 1 week | 04:37:37 PM Wed 07/27 | 07/23 05:34:38 AM | 07/27 04:00:00 PM | 3,848 | 2,066,806 | |
| | ⊕ <u>†</u> 1 | Logs - Detail pasrse stasn r | | Last 24 hours | 11:36:52 PM Wed 07/27 | 07/25 11:00:00 PM | 07/27 10:59:59 PM | 2,107 | 1,320,540 | |
| | ÷ <u>†</u> 1 | test for flex with cat Logs | · | Hourly | 05:02:27 PM Thu 07/28 | 07/27 04:00:00 PM | 07/28 04:59:12 PM | 532 | 350,877 | |
| | + | test 14716 1235 Logs - Detail | -ijeyharrang | Last 1 week | 02:55:33 PM Thu 07/28 | | | 14 | 0 | |
| | ÷ 👖 🗓 | Logs - Detail temp | <u>i</u> - | Daily | 04:07:10 PM Thu 07/28 | 07/26 12:44:42 PM | 07/27 11:59:59 PM | 279 | 1,887,944 | |
| | ÷ | Logs - Detail re | peojo | Last 1 week | 11:05:14 AM Thu 07/28 | | | 0 | 0 | |
| | ÷ | Logs test- Detail publish re | | Twice Daily | 12:59:04 PM Thu 07/28 | | | 0 | 0 | |





2. Click the **Explore** icon **II** for a particular report.

| EXPLORER | | Total log count: 5, | 192 OC 1 | 11 (3) 11 We | ed, Jul 27th, 5: | 25:41 pm - Now |
|-------------------------|---------------------------|-----------------------------|----------------|------------------|------------------|----------------|
| REPORT TITLE: LOGS - DE | TAIL-PERSIST | | | | | () |
| AVAILABLE COLUMNS | LOG TIME EVENT | ID COMPUTER | ACCOUNT DOMAIN | ACCOUNT NAME | LOGONID | LOGON TY |
| | 7/28/2016 5:08:00 PM 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| Computer = | 7/28/2016 4:58:00 PM 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| EventId = | 7/28/2016 4:58:00 PM 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| ☑ Logon ID | 7/28/2016 4:48:00 PM 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| ☑ Logon Type 🛛 🚍 | 7/28/2016 4:39:00 PM 4624 | PNPL-TESTLAB9/PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| | 7/20/2010 4:36:00 PM 4624 | | TOONS | DNDL TESTLABO | UX3E7 | 4 |
| | 7720/2010 4.36:00 PM 4624 | | TUUNS | PINPL-IESTLAB9\$ | UX3E/ | 4 |

3. Check/Uncheck from the available list of columns in the left pane, to view in the result set.

| EXPLORER | | | Total | log count: 5, | ,192 🔇 🔇 | CIIO | Wed, Jul 27th, 5:25:41 pm - N | low |
|--|---|--|---|--|---|------|-------------------------------|-----|
| EXPLORER REPORT TITLE: LOGS - DET AVAILABLE COLUMNS Account Domain = Account Name = Computer = EventId = Logon ID = Logon Type = | AIL-PERSIST LOG TIME 7/28/2016 5:08:00 PM 7/28/2016 4:58:00 PM 7/28/2016 4:58:00 PM 7/28/2016 4:39:00 PM 7/28/2016 4:38:00 PM 7/28/2016 4:38:00 PM | EVENT ID 4624 4624 4624 4624 4624 4624 4624 462 | Toons Toons Toons Toons Toons Toons Toons Toons Toons Toons Toons | log count: 5, LOGON I D 0x3E7 0x3E7 0x3E7 0x3E7 0x3E7 0x3E7 0x3E7 0x3E7 | 192 (C) | | Wed, Jul 27th, 5:25:41 pm - N | () |
| | 7/28/2016 4:18:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| | 7/28/2016 4:18:00 PM 7/28/2016 4:08:00 PM | 4624 4624 | TOONS | 0x3E7 0x3E7 | 4 | | | |
| | 7/28/2016 4:02:12 PM | 4624 | - | 0x0 | 3 | | | |

Figure: 10

4. For selecting the time interval, click the calendar icon \overline{IIII} .

It will display three different options for Time selection: (Quick, Relative and Absolute).



| EXPLORER | | | | Total log count: 5,192 |
|----------|---------------|--------------|---------------|------------------------|
| Quick | Last 12 Hours | Last 7 Days | Last 2 Months | |
| Relative | Last 1 Day | Last 15 Days | Last 3 Months | |
| Absolute | Last 2 Days | Last 1 Month | | ٨ |



| Click | То |
|----------|---|
| | Select from any listed time frequency. |
| Quick | |
| | Last 12 Hours Last 7 Days Last 2 Months |
| | Last 1 Day Last 15 Days Last 3 Months |
| | Last 2 Days Last 1 Month |
| | |
| | |
| | Quick access to the frequency links for fast browsing |
| Relative | Select time frequency 'From" and 'To: Now". |
| | |
| | Hour(s) ago |
| | From Day(s) ago To Now GO |
| | Month(s) ago |
| | |
| | Enter custom values from the available ontions |
| | |
| Absolute | Select Date and time for both 'From" and 'To". |
| | |
| | From Date 🔛 Time To Date 🖽 Time GO |
| | |
| | For being more specific, select from the time controls. |
| | |

5. Click the Expand/Collapse icon \equiv against the columns to view the top 10 records for that particular column. It will also display the graph for record occurrence in percentage out of the total distinct records.



| REPORT TITLE: LOGS - DETAIL-PERSIST | | | | | | | | |
|-------------------------------------|-----------------------|---------|----------------|---------|------------|--|--|--|
| AVAILABLE COLUMNS | 100 7745 | | | | | | | |
| Account Domain = | LOG TIME | EVENTID | ACCOUNT DOMAIN | LOGONTD | LOGON TYPE | | | |
| | 7/28/2016 5:08:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| Account Name = | 7/28/2016 4:58:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| □ Computer | 7/28/2016 4:58:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| ✓ EventId | 7/28/2016 4:48:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| ☑ Logon ID | 7/28/2016 4:30:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 🖌 Logon Type 🛛 🗮 | 7202010 4.33.00 PM | 4024 | 100103 | 0,527 | 4 | | | |
| Search Q +- | 7/28/2016 4:38:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| Top 10 records | 7/28/2016 4:38:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 3 54.66% +- | 7/28/2016 4:28:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 4 41.8% +- | 7/28/2016 4:18:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 2 0.92% +- | 7/28/2016 4:18:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 10 0.73% + - | 7/28/2016 4:08:00 PM | 4624 | TOONS | 0x3E7 | 4 | | | |
| 9 0.52% + - | 7/28/2016 4:02:12 PM | 4624 | | 0x0 | 3 | | | |
| 0 | 172012010 4.02.12 F W | | | | - | | | |
| | 7/28/2016 4:02:11 PM | 4624 | - | 0x0 | 3 | | | |

- 6. Click the icon ' \bullet " to include and ' \Box 'to exclude the records.
- 7. If the user wants to view all the distinct records (Metadata) for a particular column, click the Analyze all Data icon 📒.



| EXPLORER | Total log count: 5,192 🔇 🕻 🔟 🌀 🛗 Thu, Jul 28th, 10:28:05 am - Now |
|------------------------|---|
| REPORT TITLE: LOGS - D | ETAIL-PERSIST ① |
| AVAILABLE COLUMNS | |
| 🖌 Account Domain 🛛 🗮 | LOG TIME EVENT ID COMPUTER ACCOUNT DOMAIN ACCOUNT NAME LOGON ID LOGON TY |
| Account Name = | 7/28/2016 5:08:00 PM 4624 PNPL-TESTLAB9\PNPL-TESTLAB9 TOONS PNPL-TESTLAB9\$ 0x3E7 4 |
| | Logon Type PL-TESTLAB9\$ 0x3E7 4 |
| | Search QQ < 1 of 1 > G0 PL-TESTLAB9\$ 0x3E7 4 |
| ✓ EventId | PL-TESTLAB9\$ 0x3E7 4 |
| ✓ Logon ID 📃 | |
| 🖌 Logon Type 🛛 🔤 | 2,170 |
| Search Q, +- | 7 U 5 PL-TESTLAB9S 0x3E7 4 |
| Top 10 records | 1 2 48 PL-TESTLAB9\$ 0x3E7 4 |
| 3 54.00% T = | 7 0 10 38 PL-TESTLAB9\$ 0x3E7 4 |
| 5 1.37% +- | PL-TESTLAB9\$ 0x3E7 4 |
| 2 0.92% +- | INCLUDE EXCLUDE CLOSE PL-TESTLAB9\$ 0x3E7 4 |
| 10 0.73% +- | |
| 9 0.52% +- | TUTIZUTO 4.00.00 FM 4024 PNPL-TESTLADSVENPL-TESTLADS TOURS PNPL-TESTLADS 0X3E/ 4 |
| 0 <u></u> | 28/2016 4:02:12 PM 4624 PNPL-TESTLAB9\PNPL-TESTLAB9 0x0 3 |
| | 7/28/2016 4:02:11 PM 4624 PNPL-TESTLAB9/PNPL-TESTLAB9 0x0 3 |

Figure: 13

8. Use the search icon Q to search the records and select from the listed records to **Include** or **Exclude** from the search result.

| Logon Type | | | X |
|------------|-------|--------|--------------|
| Search | QQ | < 1 | of 1 > GO |
| а з | | | 2,838 |
| 4 | | | 2,170 |
| 5 | | | 71 |
| 2 | | | 48 |
| 10 | | | 38 |
| 9 | | | 27 |
| | | | XOLUDE CLOSE |
| | Figur | re: 14 | |



The Excluded/Included values get displayed.

| EXPLORER | | | | Total log count: 5,19 | 2 001 | 11 🕥 🗮 Thu, | Jul 28th, 10:4 | 4:45 am - Now |
|-------------------------|----------|--------------------------|----------|-----------------------------|--|--------------------|----------------|-------------------|
| Logon Type : 5X Logon T | ype : 2X | ogon Type : 9X Logon Typ | e:4X La | ogon Type : 10X | | | | |
| REPORT TITLE: L | DGS - DF | ETAIL-PERSIST | | | Displays the va Green: Include Orange: Exclu | alue e & ide | | () |
| AVAILABLE COLU | MNS | LOG TIME | EVENT ID | COMPUTER | ACCOUNT DOMAIN | ACCOUNT NAME | LOGONID | LOGON T |
| Account Domain | = | 7/28/2016 10:50:58 AM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 2 |
| Account Name | = | 7/28/2016 10:50:58 AM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 2 |
| Computer | = | 7/28/2016 10:45:11 AM | 4624 | | TOONS | | 0×3E7 | 2 |
| EventId | = | 7/20/2010 10.43.11 AW | 4024 | | | FINEL-TESTERDS\$ | 0,527 | 2 |
| Logon ID | = | 7/28/2016 10:45:11 AM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 2 |
| Logon Type | = | < | | G | TO PAGE: 1 SH | IOW ROWS: 20 V | 1-4 OF 4 | $\langle \rangle$ |
| Search | λ+- | | | | | | | |
| Top 10 records | | | | | | | | |
| 3 54.88% | , +- | | | | | | | |

Figure: 15

| Click | То |
|---------|--------------------------|
| \odot | Go back to Flex History |
| C | Refresh data |
| t | Export the search result |
| | Pause the auto show data |
| ► | Play the auto show data |
| 0 | Reset the values |

9. Click the information icon (1), to know about how to use wild card character(s) in search column.

NOTE: The search result will display only top 10000 record values as per the search criteria.



| LOG TIME | EVENT ID | COMPUTER A | ACCOUNT DOMAIN | ACCOUNT NAME | LOGONID | LOGON TY |
|----------------------|----------|-----------------------------|----------------|-----------------|---------|----------|
| 7/28/2016 5:08:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:58:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:58:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:48:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:39:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:38:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:38:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |
| 7/28/2016 4:28:00 PM | 4624 | PNPL-TESTLAB9\PNPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 |

Figure: 16

10. The columns can be re-arranged by dragging and dropping, as per requirement.

| LO | DG TIME | EVENT ID | COMPUTER | LOGON I 🕭 | ACCOUNT DOMAIN | ACCOUNT NAME | LOGONID | LOGON TY | |
|----|--------------------|----------|------------------|--------------|----------------|-----------------|---------|----------|--|
| 7/ | 28/2016 5:08:00 PM | 4624 | PNPL-TESTLAB9\PN | IPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 | |
| 7/ | 28/2016 4:58:00 PM | 4624 | PNPL-TESTLAB9\PN | IPL-TESTLAB9 | TOONS | PNPL-TESTLAB9\$ | 0x3E7 | 4 | |
| | Figure 47 | | | | | | | | |

Figure: 17

11. To sort by Ascending/Descending, click the arrow icon 🛽 against the column.

| COMPUTER | |
|------------|--|
| | |
| | |
| Figure: 18 | |

If a same report was opened earlier on the same browser, it will display a confirmation message asking whether the user wants to restore the previous state.



| EXPLORER | Total log count: 5,192 (III (S) III Select Interval |
|--|---|
| REPORT TITLE: LOGS - DETAIL-PERSIST | 0 |
| AVAILABLE COLUMNS Message from webpage Restore previous stat OK Can | e. |

Figure: 19

12. Click **OK** to confirm.

NOTE: Please apply the **Update ET82U16-017**, to view the new designed explorer search result from the Flex Dashboard.

- In **EventTracker** web, click **Dashboard**.
- Select **Flex** from dropdown list.
- Click the configured dashlet.





• Click the graph and it will open the search result in Explorer.

| EXPLORER | | Total lo | og count: 10 🔇 🕻 🗓 🏵 | Thu, Aug 4th, 11:12:27 am - Thu, Aug | 11th, 11:12:27 am |
|-------------------------------------|---------------------|--------------|------------------------------|--|-------------------|
| Signer : Prism Microsystems, Inc. X | | | | | |
| REPORT TITLE: EVENT | RACKER-UNKNO | WN MD5 HA | SH DETECTED | | (i) |
| AVAILABLE COLUMNS | LOC TIME | SYSTEM NAME | | | |
| ☑ Creator Process Name 🛛 ≡ | 8/10/2016 6:32:52 P | M PNPL-TEST4 | NT AUTHORITY\SYSTEM | Prism.Reports.TLSReporter.exe | C:\Program F |
| ✓ Creator Process Path | 8/9/2016 6:29:53 PM | PNPL-TEST4 | NT AUTHORITY/NETWORK SERVICE | App_Web_siemreport.aspx.59b6e57e.dll | C:\Program F |
| ✓ File Description | 8/9/2016 6:29:52 PM | PNPL-TEST4 | NT AUTHORITY/NETWORK SERVICE | App_Web_tisgeneratedinfo.aspx.59b6e57e.dll | C:\Program F |
| ✓ File Name | < | | | | > |
| ✓ File Path | | | GO TO P | AGE: 1 SHOW ROWS: 20 V 1-3 OF | 3 < > |
| File Version | | | | | |
| Product Name = | | | | | |
| Suspicious Hash | | | | | |
| System Name | | | | | |
| User Name | | | | | |

Figure: 21

