

EventVault explorer, Behavior and Tile Dashboard enhancement

EventTracker Enterprise v8.2

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

Abstract	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**.

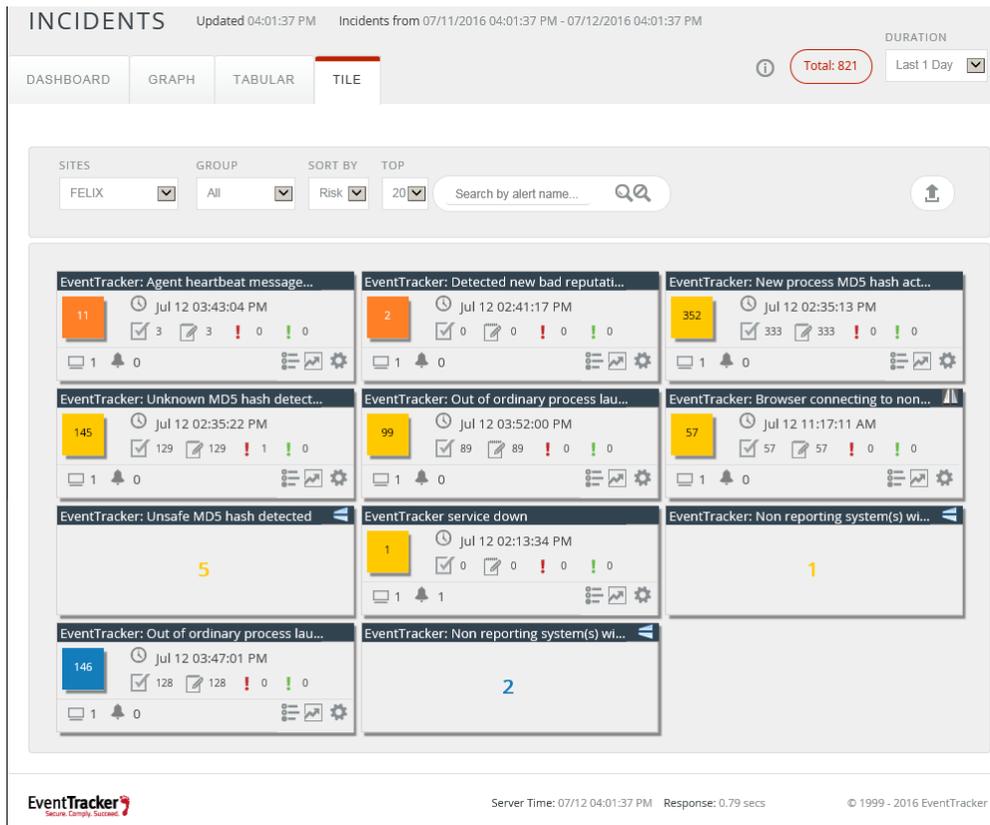


Figure: 1

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.

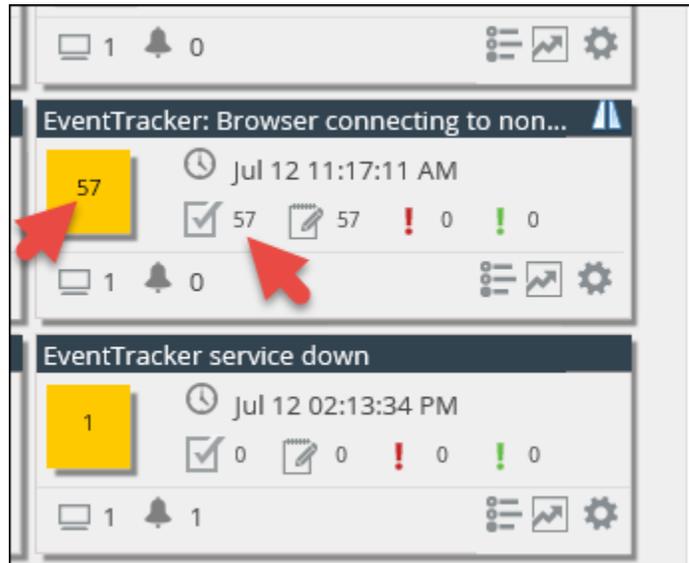


Figure: 2

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.

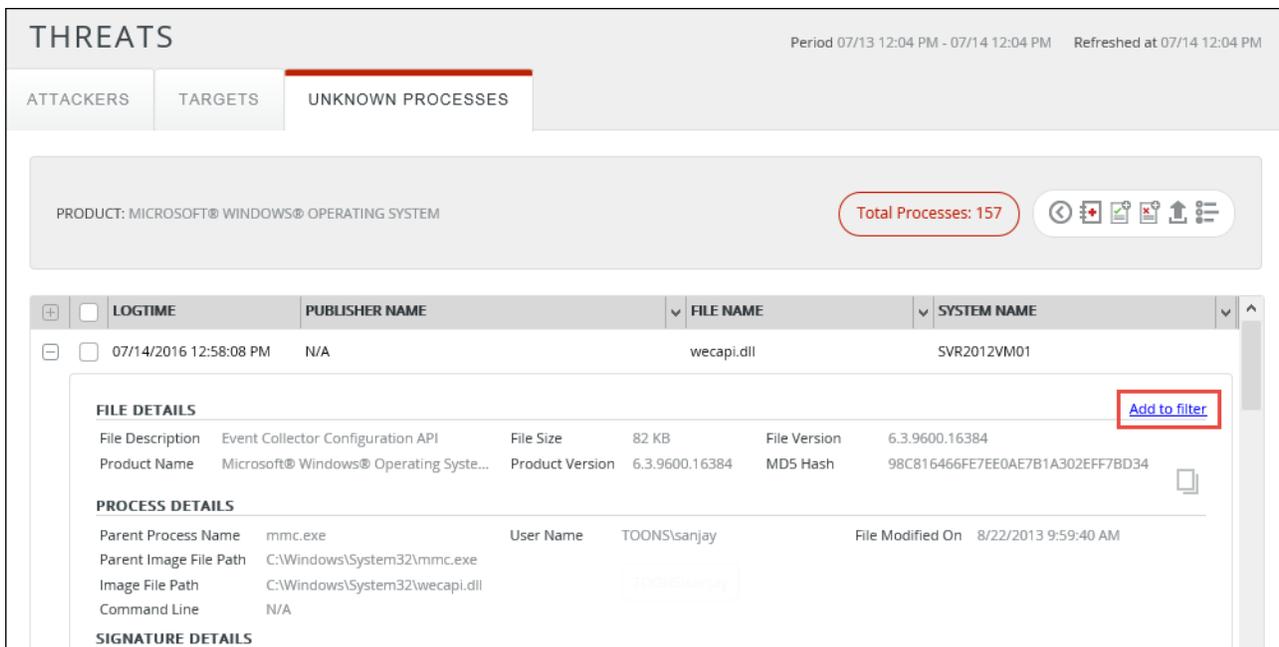


Figure: 4

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

Field	Value	Checked
<input type="checkbox"/> SELECT ALL		Unchecked
<input checked="" type="checkbox"/> Signed By	N/A	Checked
<input checked="" type="checkbox"/> Product Name	Microsoft® Windows® Operating System	Checked
<input type="checkbox"/> Product Version	6.3.9600.16384	Unchecked
<input checked="" type="checkbox"/> File Name	wecapi.dll	Checked
<input type="checkbox"/> Image File Path	C:\Windows\System32\wecapi.dll	Unchecked
<input checked="" type="checkbox"/> Parent Process Name	mmc.exe	Checked
<input checked="" type="checkbox"/> Parent Image File Path	C:\Windows\System32\mmc.exe	Checked
<input type="checkbox"/> File Version	6.3.9600.16384	Unchecked

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 PROCESS FILTERS

RULE NAME	DESCRIPTION	ADD TO RULE GROUP	
<input type="text"/>	<input type="text"/>	Default <input type="checkbox"/>	<input checked="" type="checkbox"/> ACTIVE 🗑️ ↩️

	OPERATOR	VALUE
SIGNED BY	Equals <input type="checkbox"/>	N/A
SIGNED	Select <input type="checkbox"/>	
PRODUCT NAME	Equals <input type="checkbox"/>	Microsoft® Windows® Operating System
PRODUCT VERSION	Select <input type="checkbox"/>	
FILE NAME	Equals <input type="checkbox"/>	wecapi.dll
IMAGE FILE PATH	Select <input type="checkbox"/>	
PARENT PROCESS NAME	Equals <input type="checkbox"/>	mmc.exe
PARENT IMAGE FILE PATH	Equals <input type="checkbox"/>	C:\Windows\System32\mmc.exe
FILE VERSION	Select <input type="checkbox"/>	

EventTracker Secure. Comply. Succeed.
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:

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**.

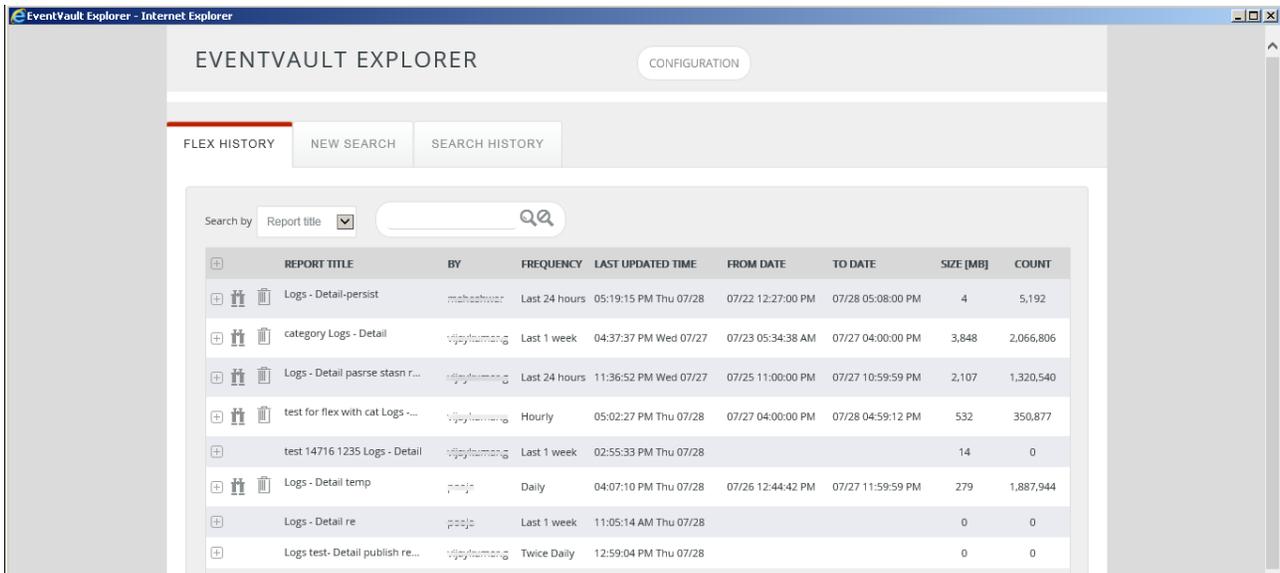
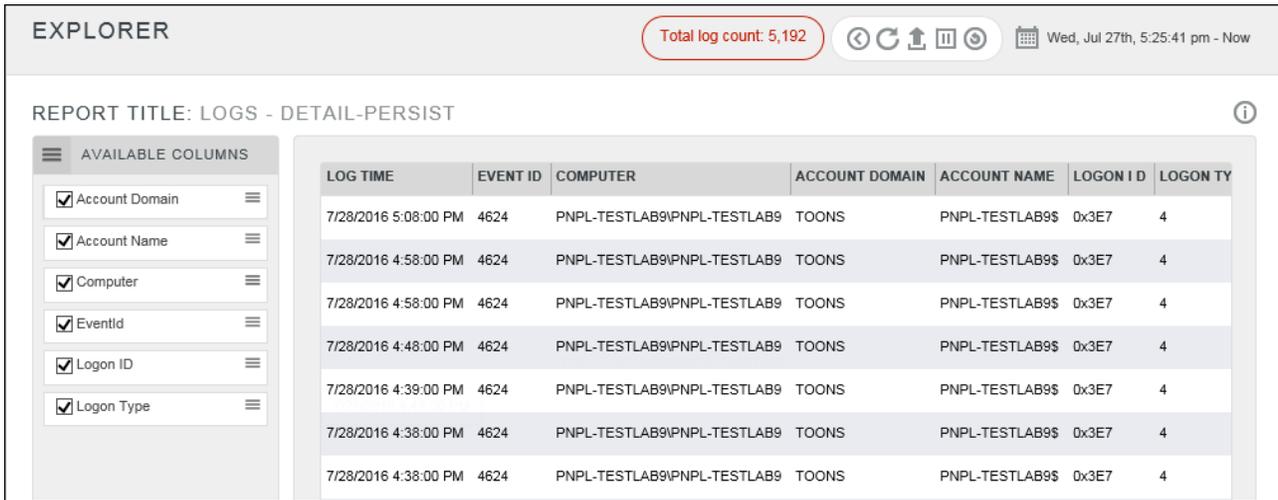


Figure: 8

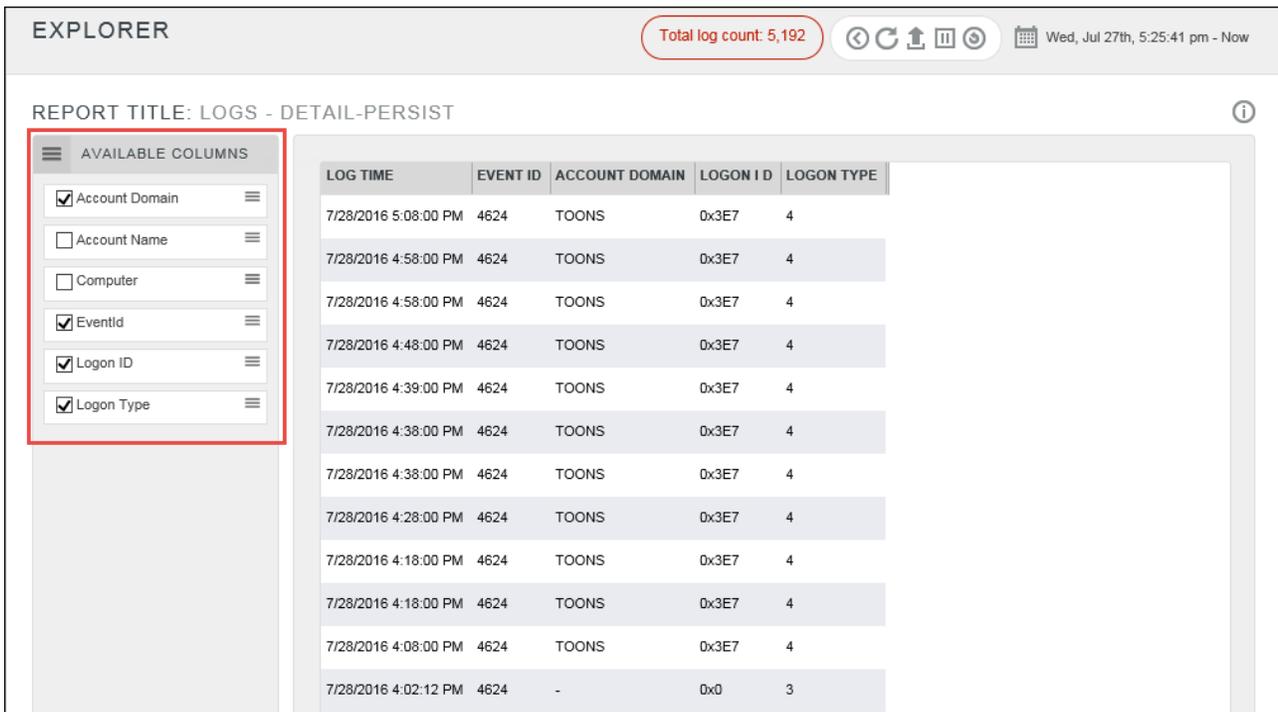
- 2. Click the **Explore** icon  for a particular report.



The screenshot shows the 'EXPLORER' interface with a 'Total log count: 5,192' indicator. The report title is 'LOGS - DETAIL-PERSIST'. On the left, the 'AVAILABLE COLUMNS' sidebar is expanded, showing checkboxes for 'Account Domain', 'Account Name', 'Computer', 'EventId', 'Logon ID', and 'Logon Type', all of which are checked. The main table displays log entries with the following columns: LOG TIME, EVENT ID, COMPUTER, ACCOUNT DOMAIN, ACCOUNT NAME, LOGON I D, and LOGON TY. The data rows show logon events for 'TOONS' on 'PNPL-TESTLAB9\PNPL-TESTLAB9' with event ID 4624 and logon type 4.

Figure: 9

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



This screenshot is similar to Figure 9, but the 'AVAILABLE COLUMNS' sidebar is highlighted with a red border. In this view, the 'Account Name' and 'Computer' checkboxes are unchecked, while 'Account Domain', 'EventId', 'Logon ID', and 'Logon Type' remain checked. The main table columns are updated to reflect these selections: LOG TIME, EVENT ID, ACCOUNT DOMAIN, LOGON I D, and LOGON TYPE. The data rows show logon events for 'TOONS' on 'PNPL-TESTLAB9\PNPL-TESTLAB9' with event ID 4624 and logon type 4.

Figure: 10

- 4. For selecting the time interval, click the calendar icon  .

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

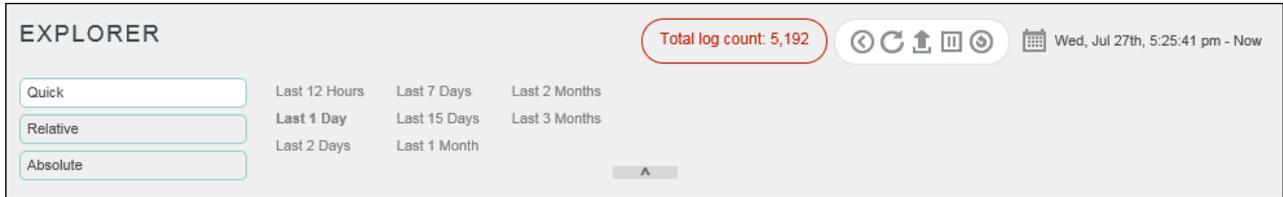
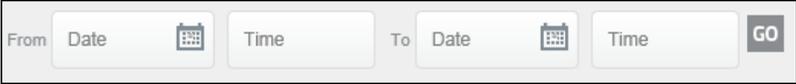


Figure: 11

Click	To
Quick	<p>Select from any listed time frequency.</p>  <p>Quick access to the frequency links for fast browsing</p>
Relative	<p>Select time frequency 'From' and 'To: Now'.</p>  <p>Enter custom values from the available options.</p>
Absolute	<p>Select Date and time for both 'From' and 'To'.</p>  <p>For being more specific, select from the time controls.</p>

- Click the Expand/Collapse icon  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.

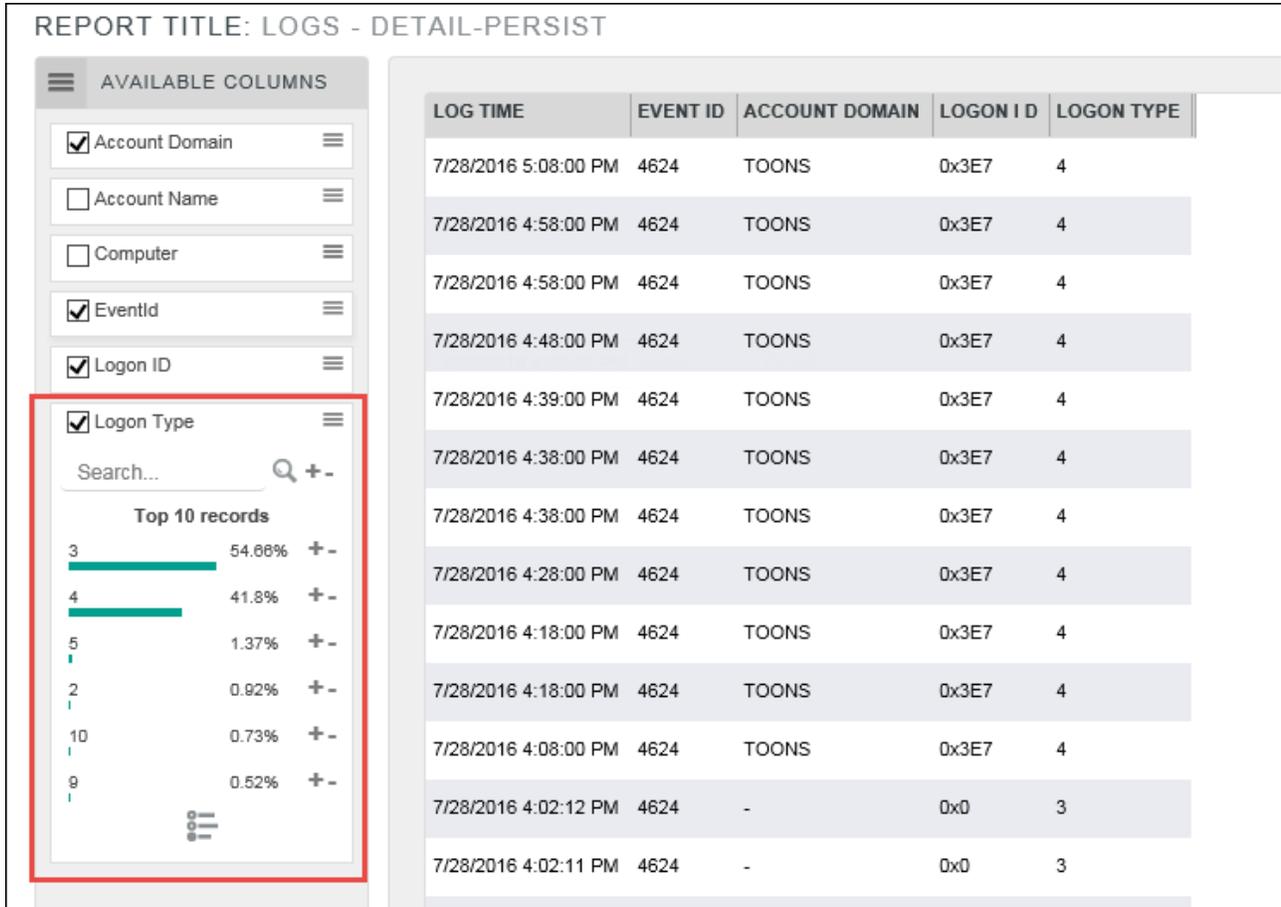


Figure: 12

- Click the icon '+' to include and '-' to exclude the records.
- If the user wants to view all the distinct records (Metadata) for a particular column, click the Analyze all Data icon .

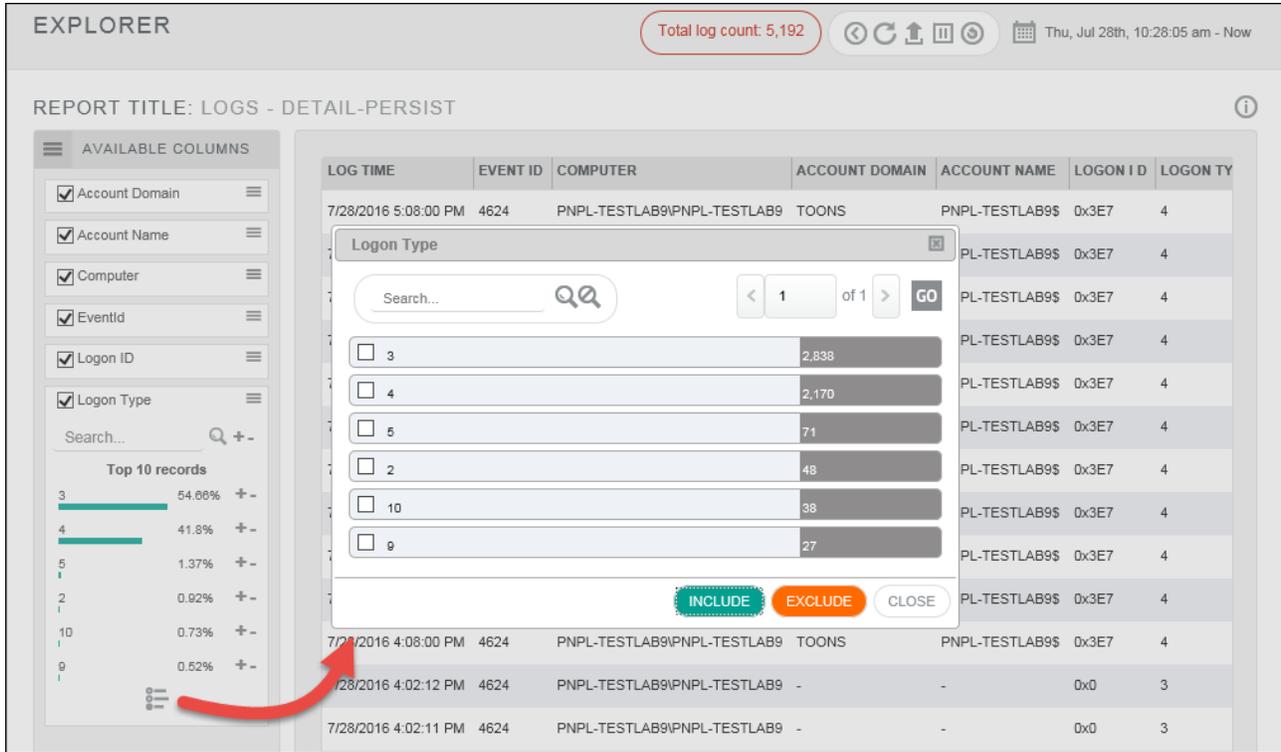


Figure: 13

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

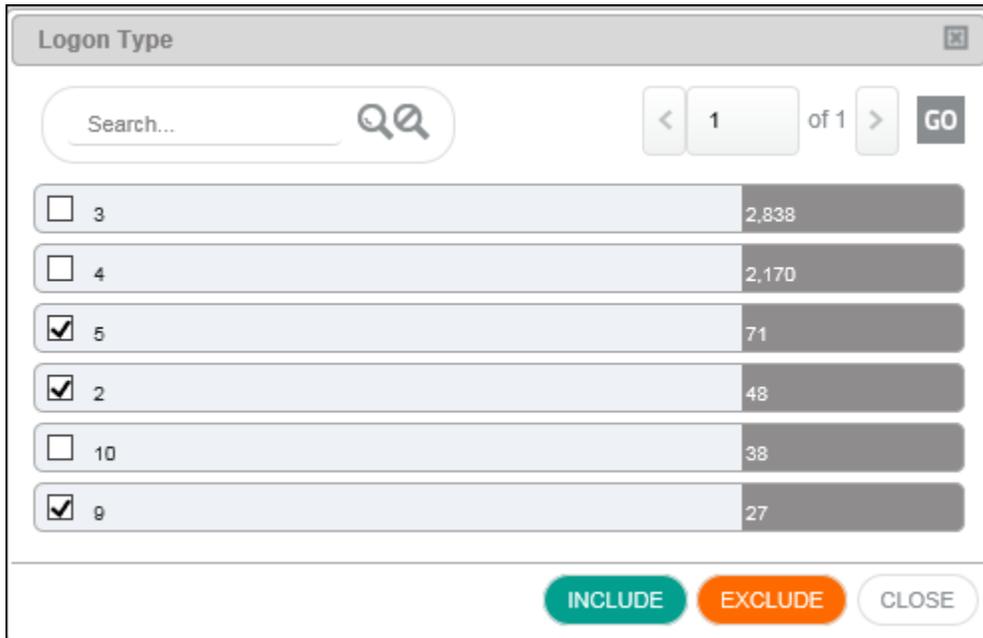


Figure: 14

The Excluded/Included values get displayed.

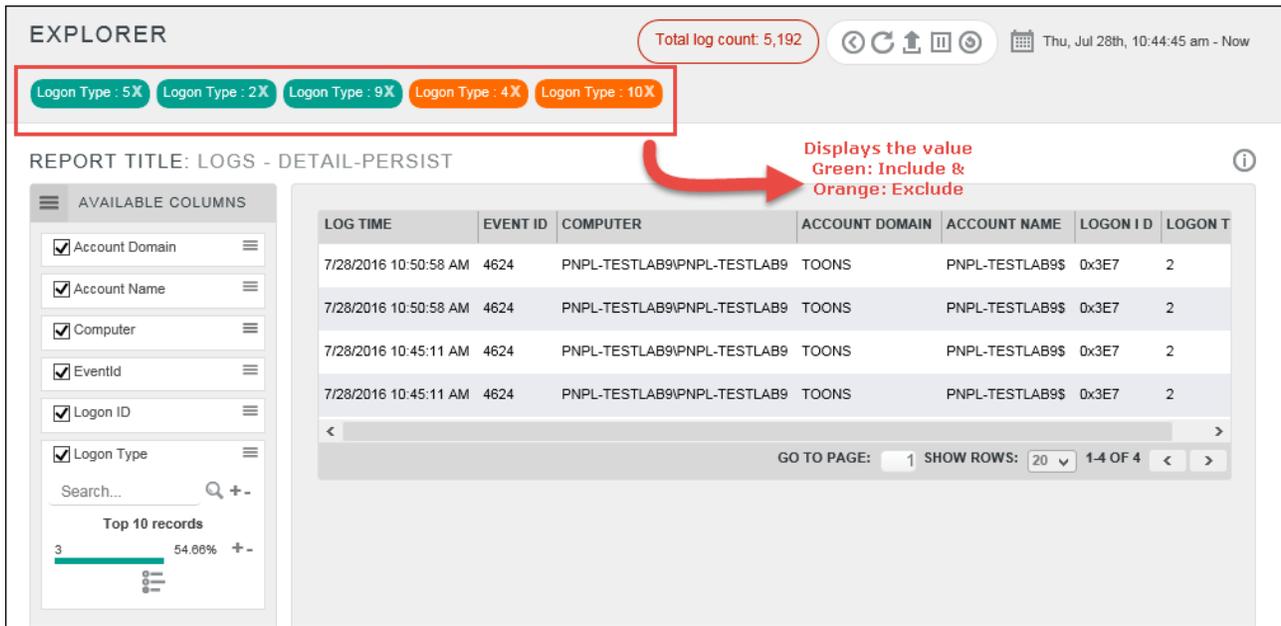


Figure: 15

Click	To
	Go back to Flex History
	Refresh data
	Export the search result
	Pause the auto show data
	Play the auto show data
	Reset the values

- Click the information icon  , 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	ACCOUNT DOMAIN	ACCOUNT NAME	LOGON I D	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.

LOG TIME	EVENT ID	COMPUTER	LOGON I D	ACCOUNT DOMAIN	ACCOUNT NAME	LOGON I D	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	

Figure: 17

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



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.

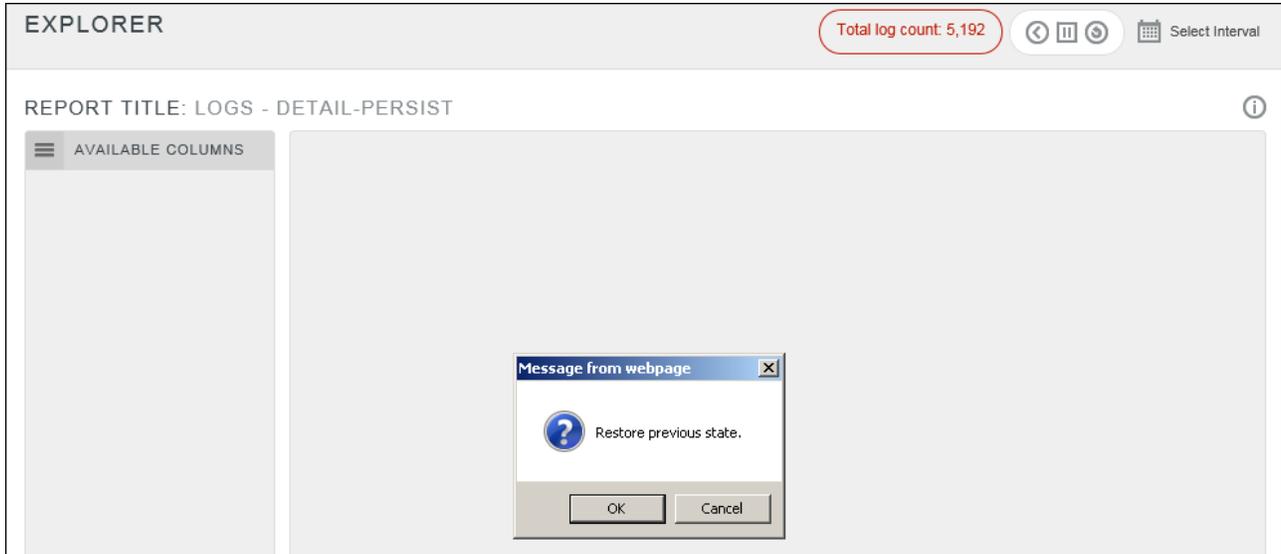


Figure: 19

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.

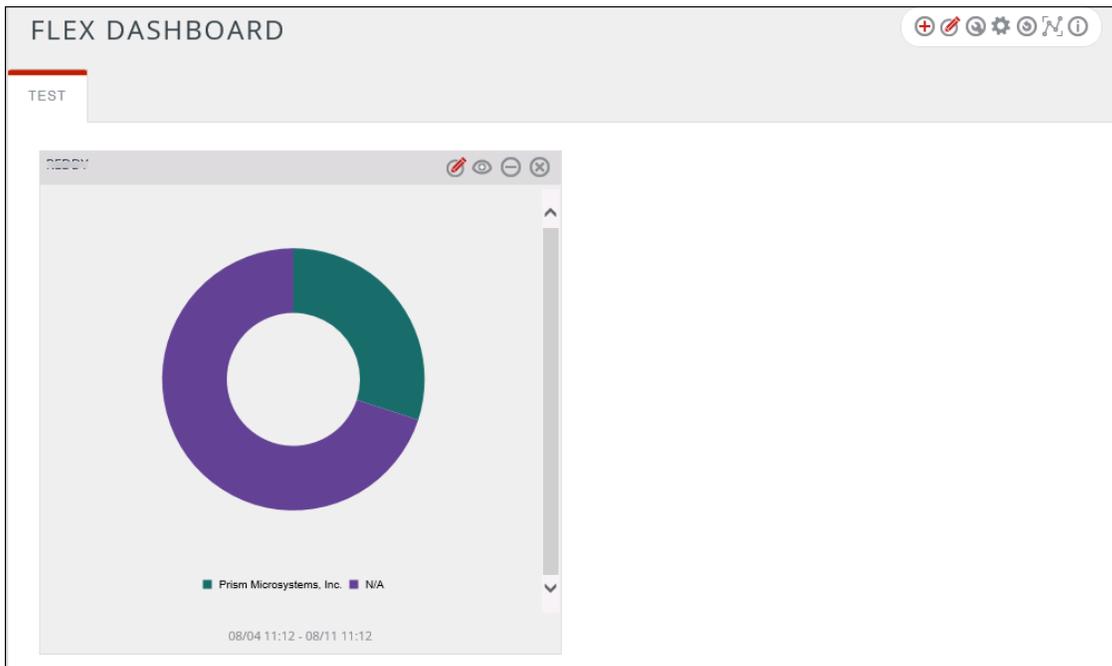


Figure: 20

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

The screenshot displays the 'EXPLORER' interface. At the top, it shows 'Total log count: 10' and a date range from 'Thu, Aug 4th, 11:12:27 am' to 'Thu, Aug 11th, 11:12:27 am'. The user is identified as 'Prism Microsystems, Inc. X'. The report title is 'EVENTTRACKER-UNKNOWN MD5 HASH DETECTED'. On the left, there is a list of 'AVAILABLE COLUMNS' with checkboxes for Creator Process Name, Creator Process Path, File Description, File Name, File Path, File Version, Product Name, Signer, Suspicious Hash, System Name, and User Name. The main area contains a table with the following data:

LOG TIME	SYSTEM NAME	USER NAME	FILE NAME	FILE PATH
8/10/2016 6:32:52 PM	PNPL-TEST4	NT AUTHORITY\SYSTEM	Prism.Reports.TLSReporter.exe	C:\Program F
8/9/2016 6:29:53 PM	PNPL-TEST4	NT AUTHORITY\NETWORK SERVICE	App_Web_siemreport.aspx.59b6e57e.dll	C:\Program F
8/9/2016 6:29:52 PM	PNPL-TEST4	NT AUTHORITY\NETWORK SERVICE	App_Web_tlsgeneratedinfo.aspx.59b6e57e.dll	C:\Program F

Below the table, there is a pagination control showing 'GO TO PAGE: 1 SHOW ROWS: 20 1-3 OF 3'.

Figure: 21