EventVault explorer, Behavior and Tile Dashboard enhancement

EventTracker Enterprise v8.2

Publication Date: Aug.1, 2016

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

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.

Table of Contents

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**.

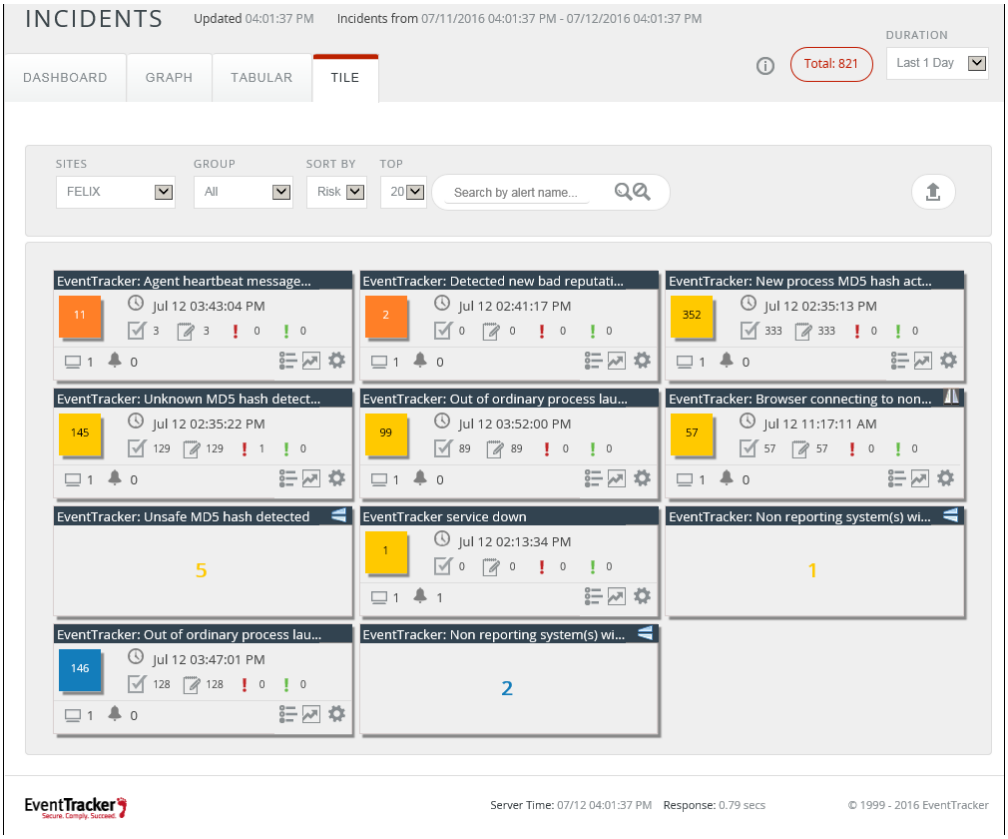


Figure: 1

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.

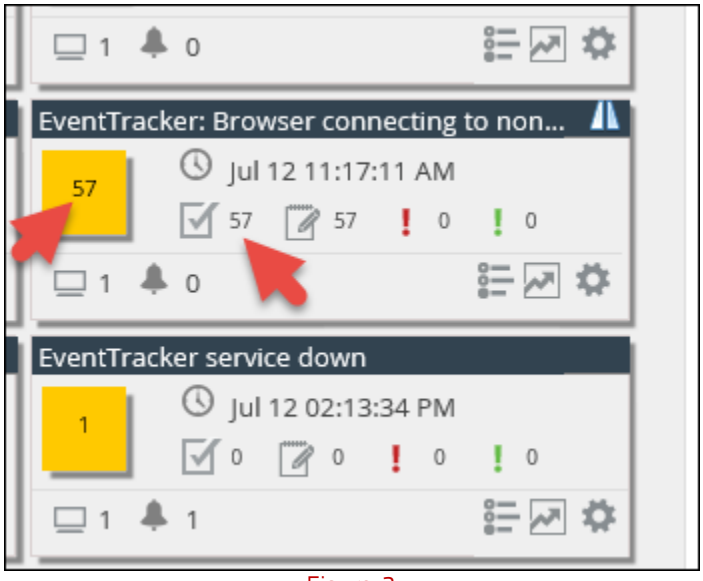


Figure: 2

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.

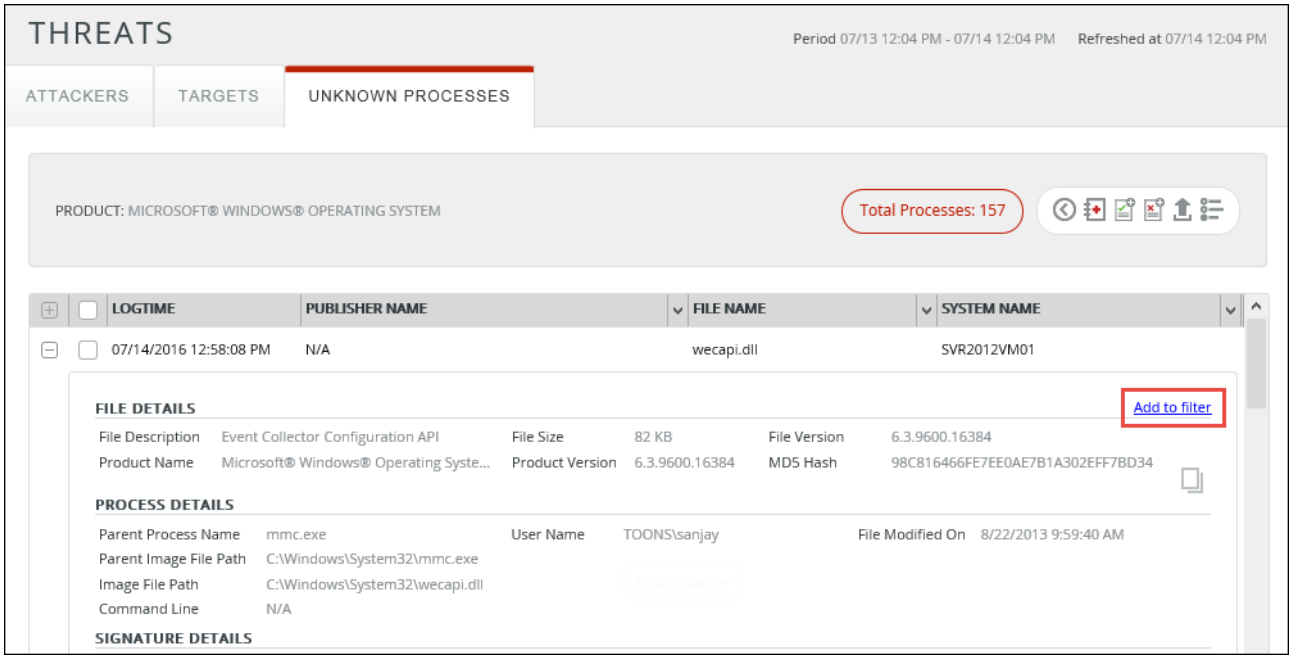


Figure: 4

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

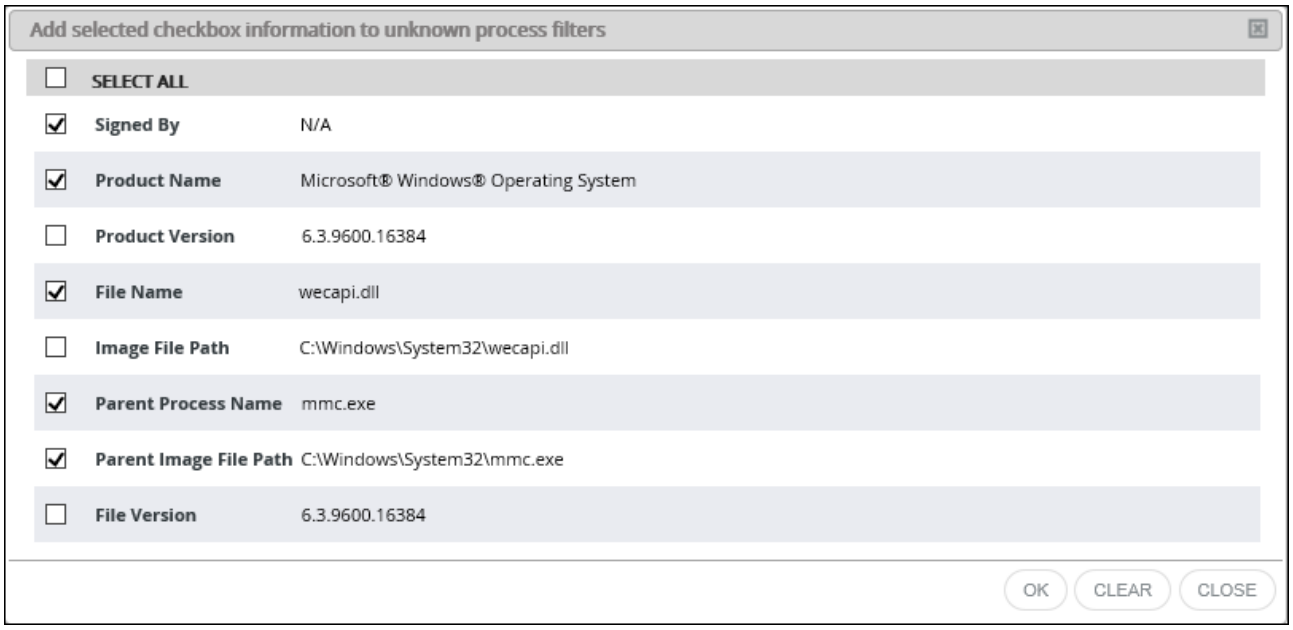


Figure: 5

- 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**.

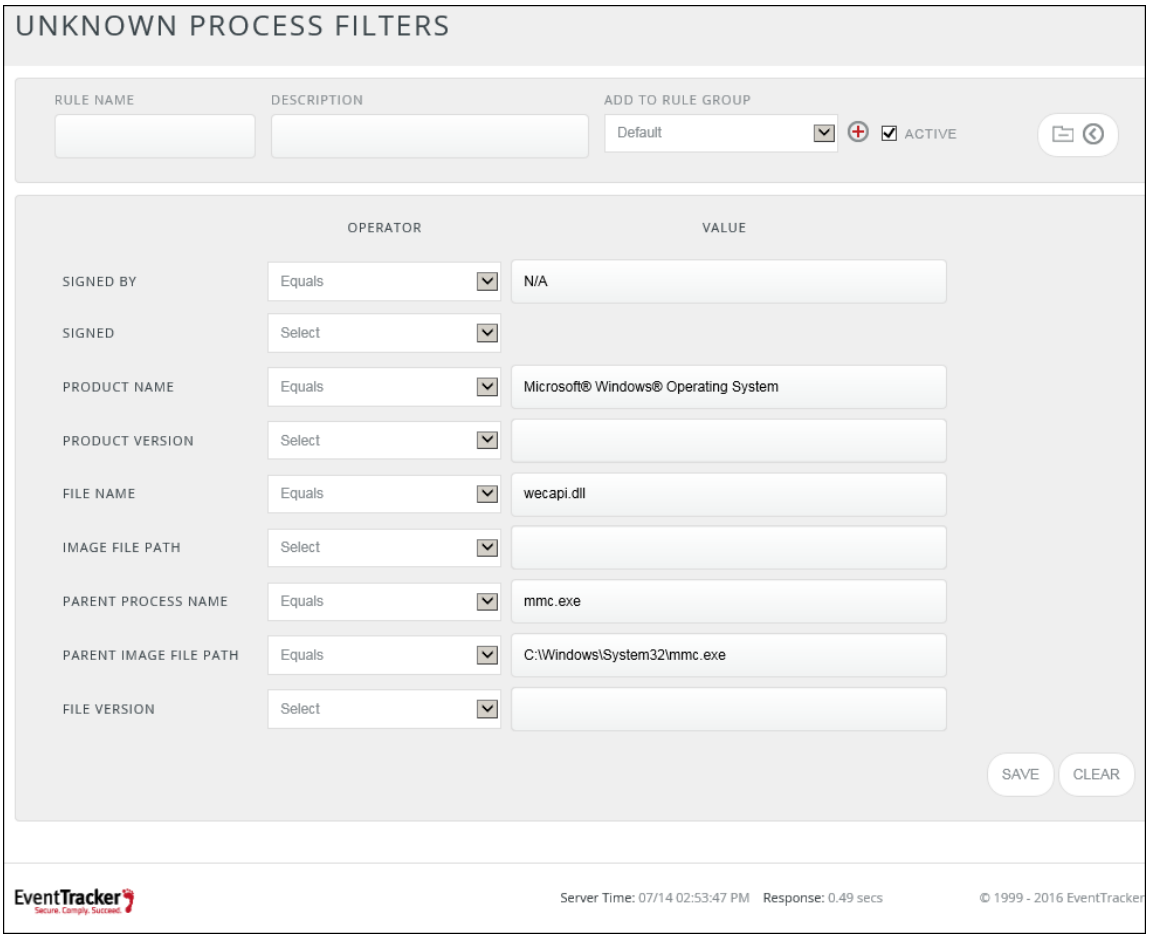


Figure: 6

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**.

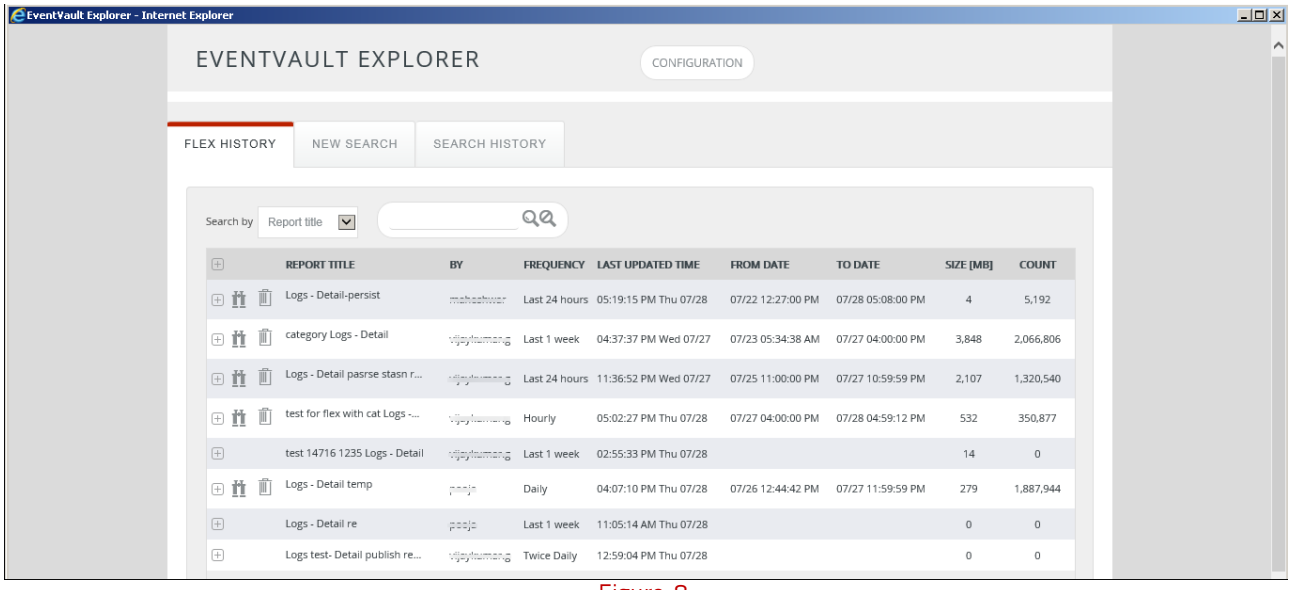


Figure: 8

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

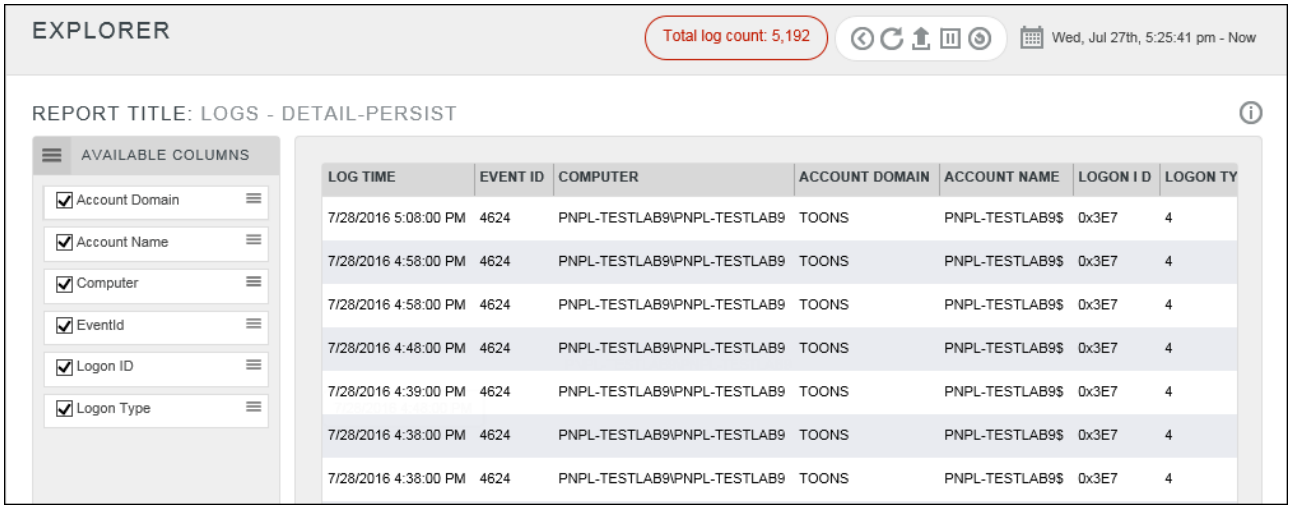


Figure: 9

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

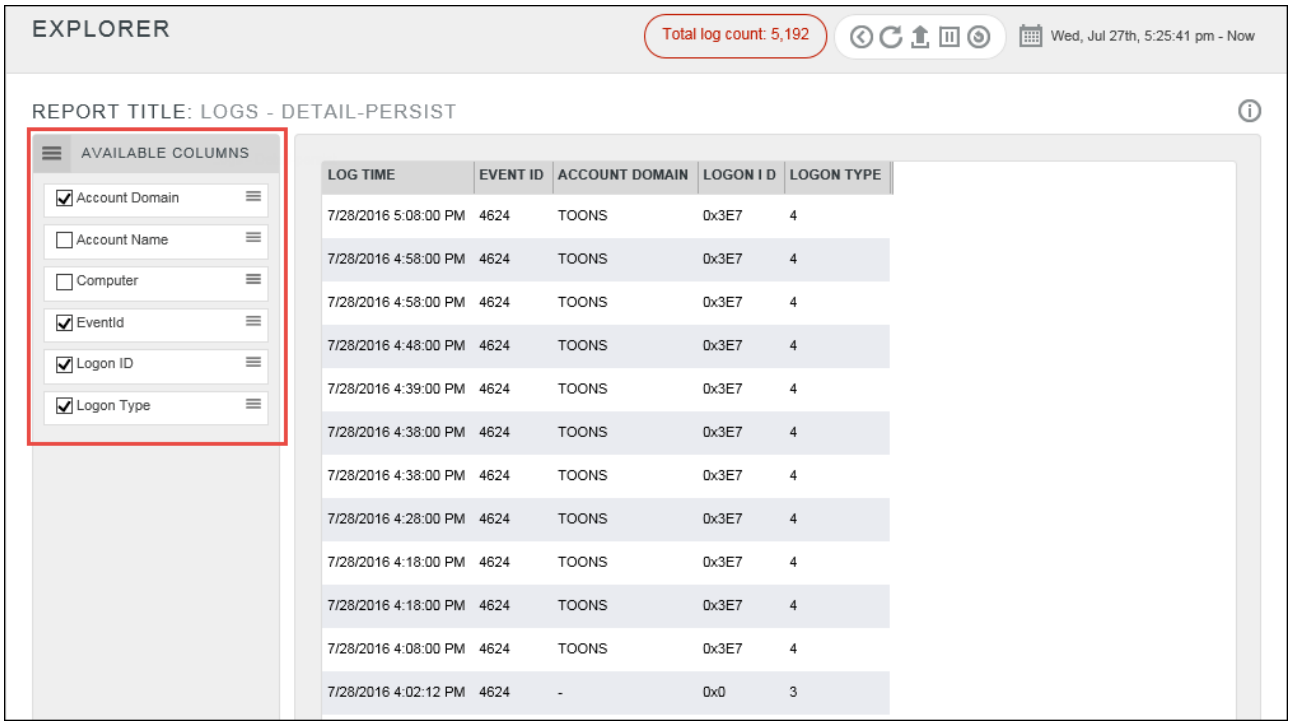


Figure: 10

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

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

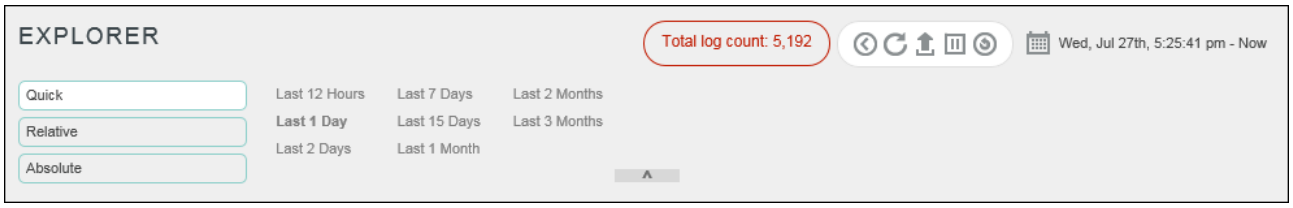
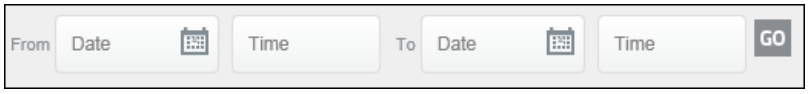


Figure: 11

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

5. 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.

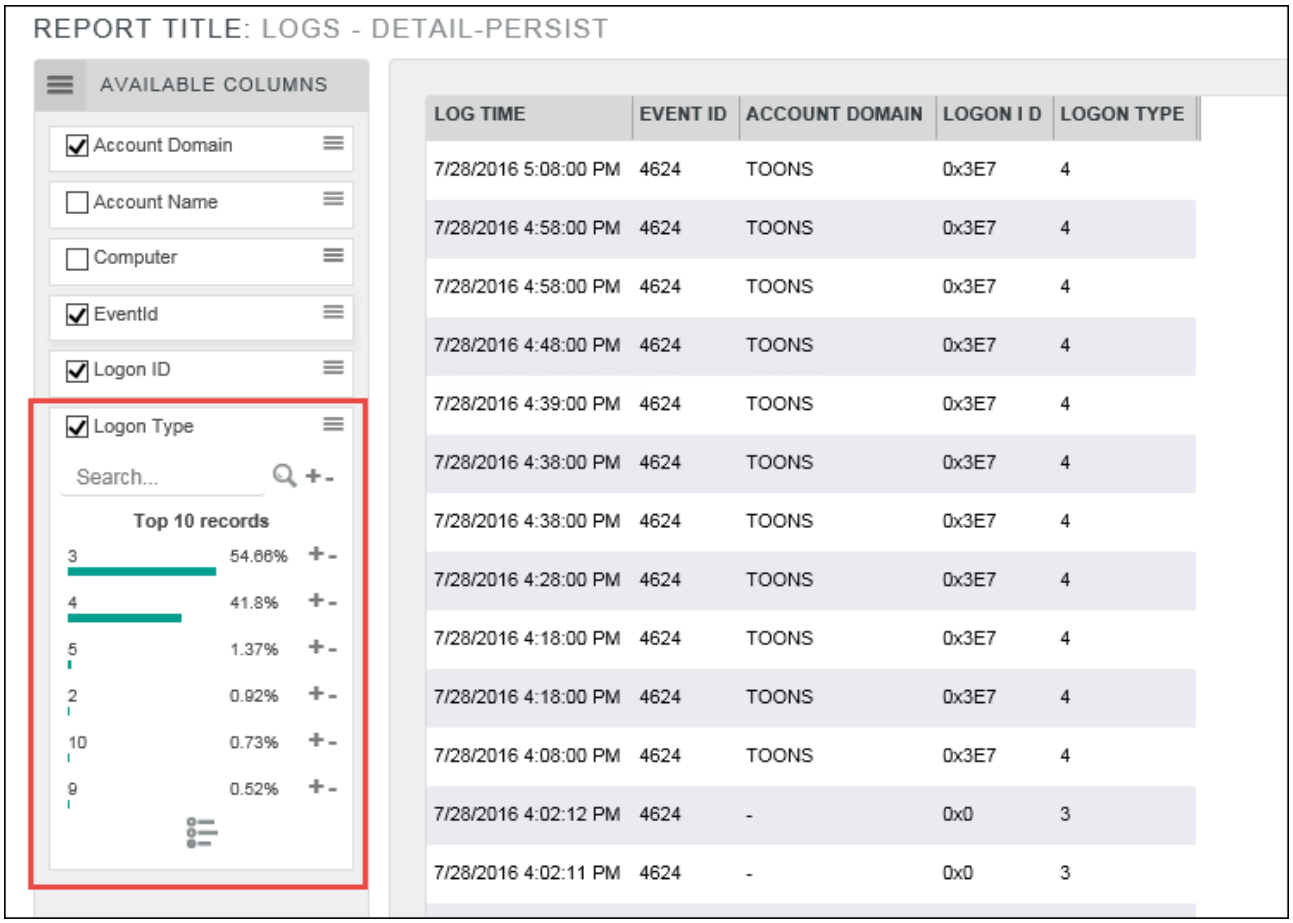


Figure: 12

6. Click the icon '+" to include and '- '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 .

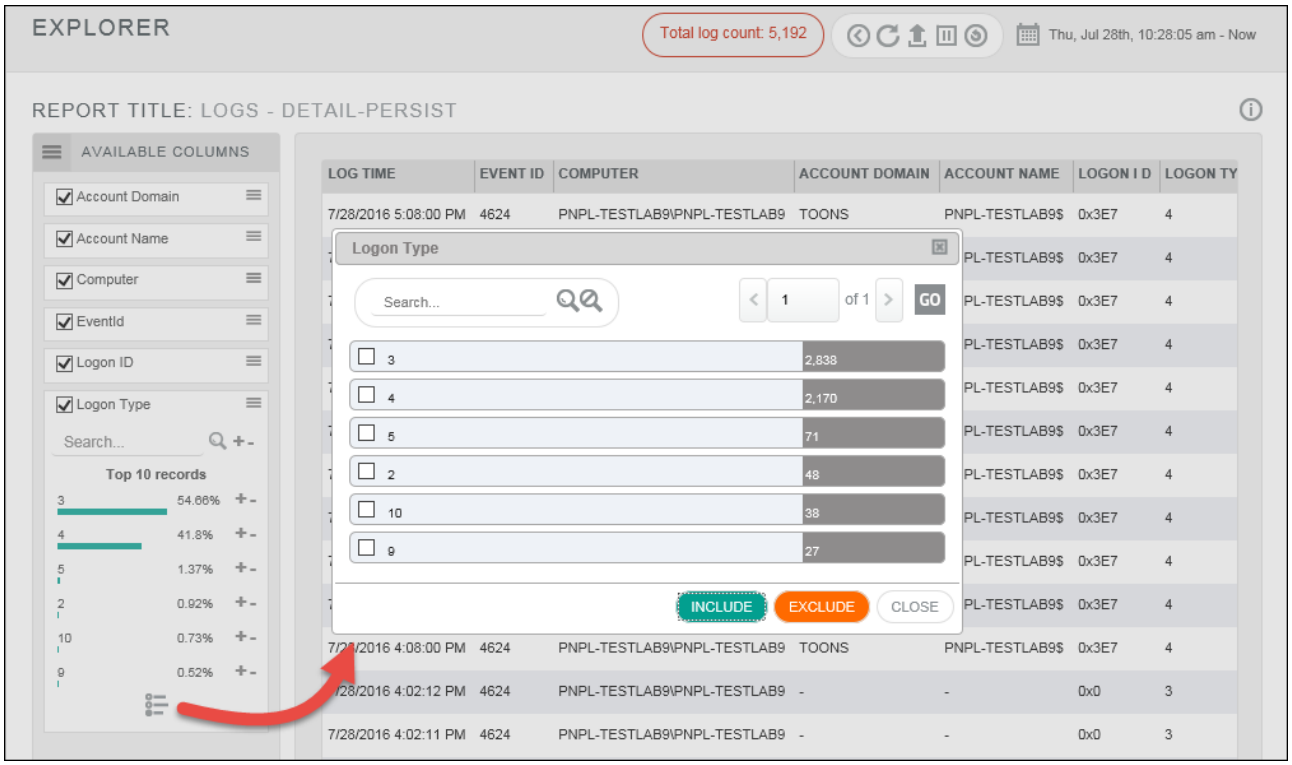


Figure: 13

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

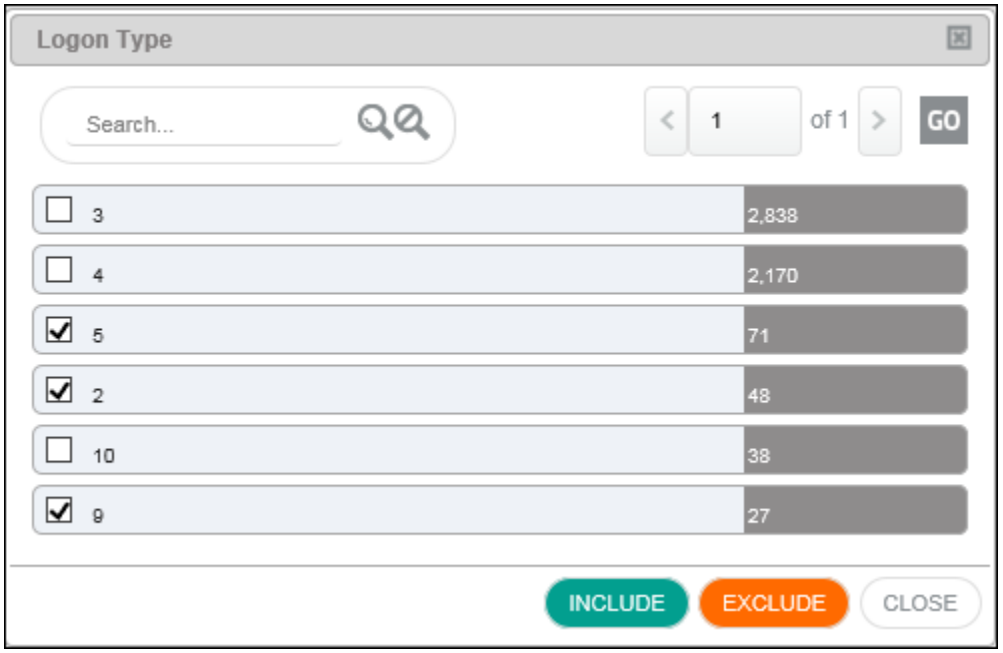


Figure: 14

The Excluded/Included values get displayed.

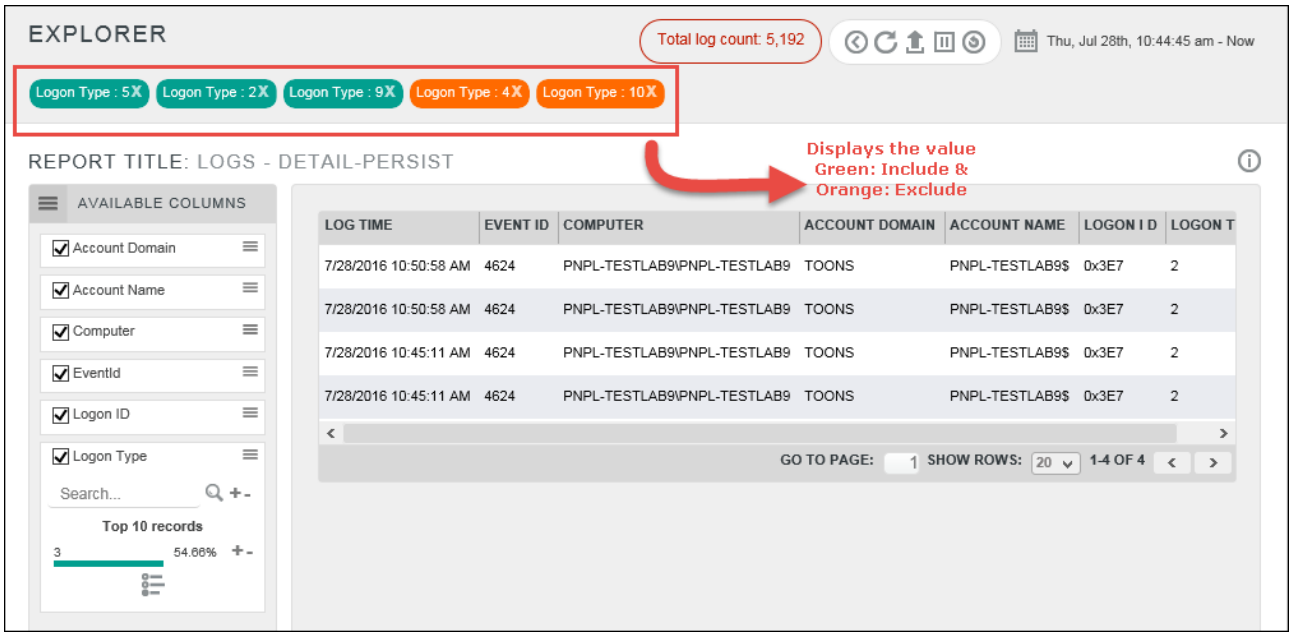
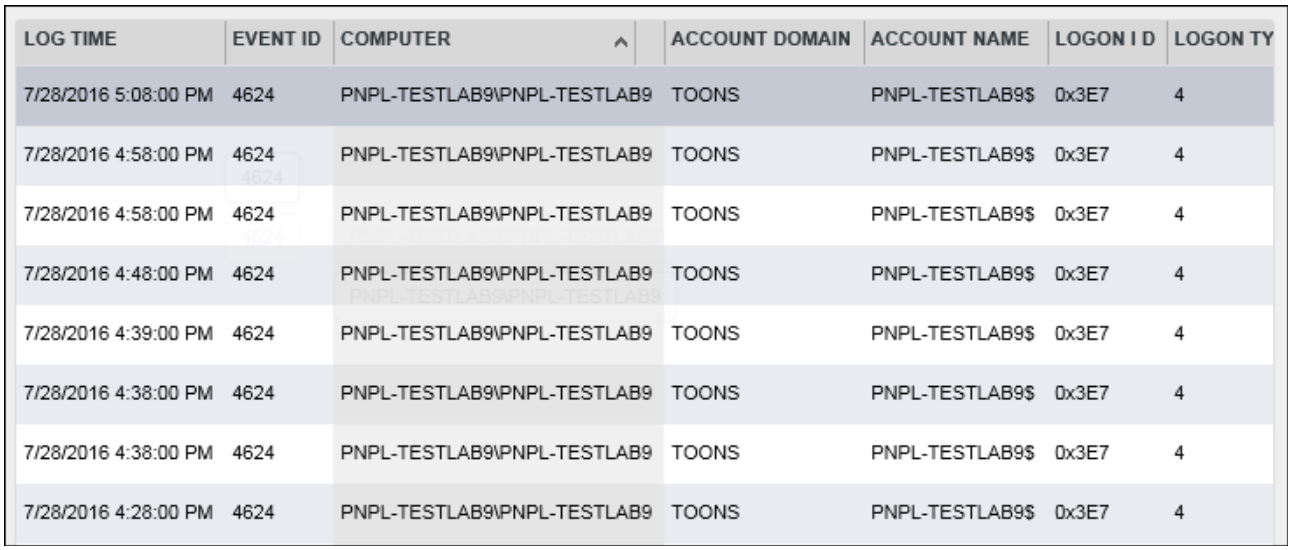


Figure: 15

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

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

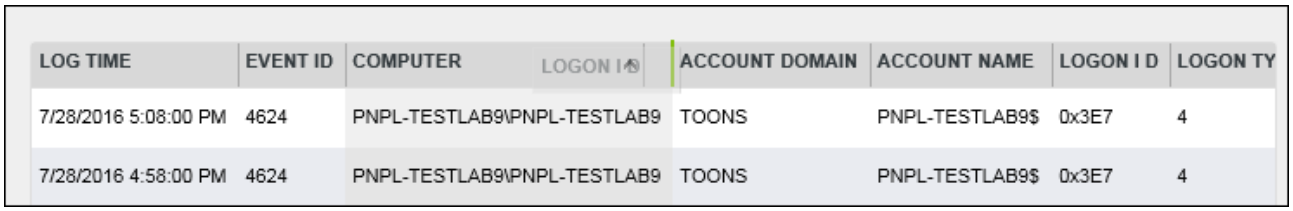
NOTE: The search result will display only top 10000 record values as per the search criteria.



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	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.

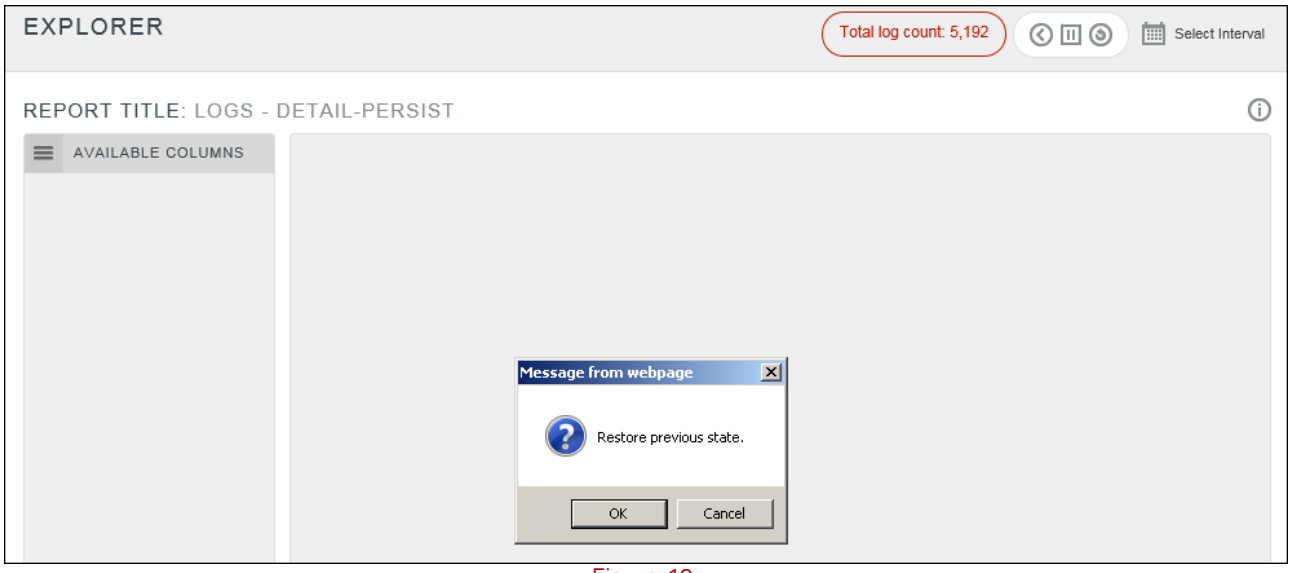


Figure: 19

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.

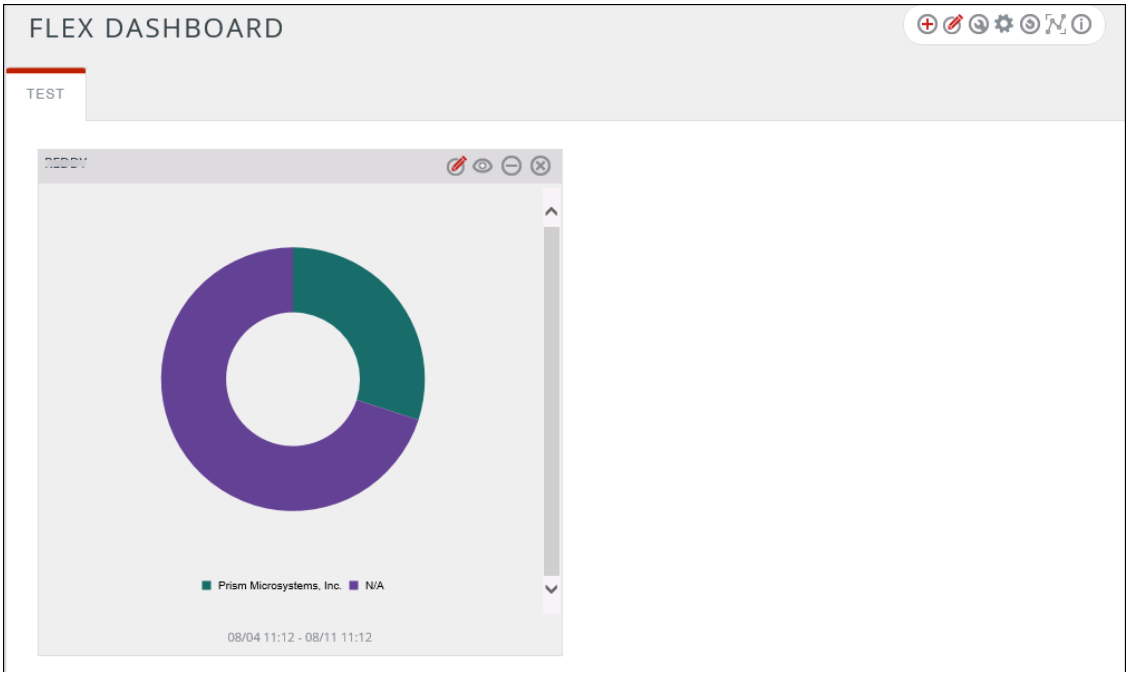


Figure: 20

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

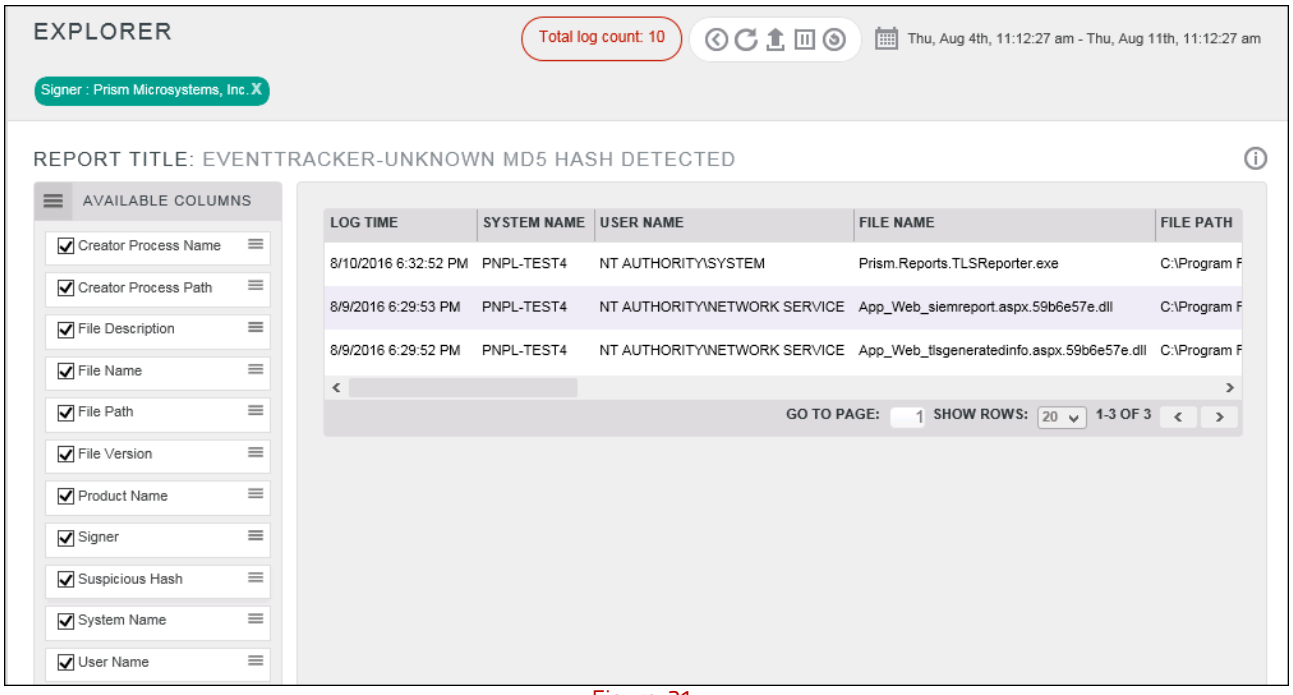


Figure: 21