New System selection interface

EventTracker v9.3.3

Publication Date: July 14, 2020
Abstract

This guide will help you use the enhanced system selection interface in log search and report configuration in EventTracker. Please refer to main user guide for complete log search and report configuration.

Audience

This guide is intended for use by all EventTracker users responsible for investigating and managing network security. This guide assumes that you have EventTracker access and understanding of networking technologies.
# Table of Contents

1. Advanced Search ........................................................................................................................................... 3  
   1.1 New System selection interface (System Tree) ......................................................................................... 3  
2. Importing the saved search criteria ................................................................................................................. 7  
3. Reports Configuration ..................................................................................................................................... 10  
   3.1 Generating on Demand Reports ................................................................................................................. 10
1. Advanced Search

Here the search result is performed using the Elastic Search. The user can write a lucene query for searching or can select from the fields available in the “Search In” box.

For example, if the user wants to search for event source and event id and filter event computer. They can either write a lucene query such as: “event_source:(EVENTTRACKER) AND event_id:(3240 || 2040 || 2037) AND NOT event_computer:D-LA” to perform a search.

The user can choose the duration and can also select from the system selection interface in the left pane.

![Advanced Search Page](image1.jpg)

**Figure 1**

1.1 New System selection interface (System Tree)

**Note:** This is applicable from “Feature update 9.3.3 (ET93U20-031)” onwards

1. In the Advanced search page, in the left pane, click the Sites drop down arrow to choose the required Site, the respective groups present in the Sites appears.
2. Enter the group name in the Group search box to search the group.
Note: “All Groups” will display all systems across the groups of a specific site.

3. Click on any group to populate the systems present in the group. The systems present in the Group populates in the Available Systems pane.
New System selection interface

Group based search

1. Select any group from the group pane. **Update selected** button is enabled in the selection pane. The Groups turn orange while hovering the mouse and turns green when selected.
2. Click on **Update selected** button to view the selected item.

![Figure 6](image)

3. Click on search to perform group-based log search.

**System based search**

1. Select Group from the Group Pane, Systems available in that group is seen in the Available Systems pane.
2. Select any system, **Update selected** button is enabled.
   
   The System turn orange while hovering the mouse and turns green when selected.

![Figure 7](image)

3. Click on **Update selected** button to view the selected item.
4. Click on search to perform computer-based log search.
5. Click ‘<’ button to collapse all the panes.

**Note:** In order to search a specific system, you can open the Available Systems pane directly and search systems across the groups of a specific site.

### 2. Importing the saved search criteria

The saved search criteria can be imported to the selected site, group, system based on their requirement.

To do that

1. Click **Import** in the **Advanced Search** page.
2. Import page opens

![import](image)

**Figure 10**

3. Click **Browse** and navigate to the location and select the saved search files (.etss files) and click **Upload**.

The saved search files are uploaded in the **Available Searches**.

**Note**: Based on the saved search type the saved search files are either available in the **Elastic** option or in the **Archive** option.

![Import](image)

**Figure 11**

To apply the criteria for the selected groups/systems.

4. Choose the saved search files (criteria) and the specific group you want to apply and click **Import**.

![This site says](image)

**Figure 12**
To apply the criteria on the system and groups present in the exported (.etss) file.

1. Choose the criteria and click Import.
   The following message appears.

![Import Saved Search](image)

**Figure 13**

a. Click **No**
   - To only import the search criteria.
     **Note:** When the imported saved search is opened in edit mode, user can make the selection from the system tree.

b. Click **Yes**
   - If the saved search file is of the same environment, then both the search criteria and the group/system is imported.
   - If the saved search file is of the different environment, then only the search criteria is imported.
3. Reports Configuration

While configuring a report, new system selection interface (system tree) is displayed.

Note: This is applicable from “Feature update 9.3.3 (ET93U20-031)” onwards.

The below section shows how to use new system tree interface during one of the report configurations. Please refer to main user guide for the rest of the report configuration information.

3.1 Generating on Demand Reports

On Demand reports can be generated in the foreground and background as well. Reports that are generated in the foreground are called On Demand reports. Reports that are generated in the background are called Queued reports (explained in the next section).

1. Log on to EventTracker, click the Reports menu, and then select Dashboard or Configuration.
2. Click New in Dashboard / Configuration.
3. Select any one of the Compliance / Security / Operations / Flex reports/Alphabetical tab.
4. Expand the Report Tree node and select any report.
5. Select Report Type as On Demand.
   (OR)
   Right click the respective report and then select On Demand.
6. Click Next.
   For Example: In Security menu, select All error events, right-click On Demand.
EventTracker opens the Reports Wizard.

7 Click **Next >>**.
8 Select **Realtime** or **File Transfer** and then click **Next>>**.
9 New system selection interface (system tree) is displayed.

**Note:**
- Selecting the **Sites/Groups** option from the drop down enables the two panes the **Sites/Groups** pane and the **Selected Items** pane.
- Selecting the **Systems** option from the drop down enables all the three panes **Sites/Groups** pane, **Available Systems** pane and **Selected Items** pane.

10 You can select the required group directly or select the systems under the group.
   - The Groups and systems turn orange while hovering the mouse and turns green once when selected.

11 The **Update selected** button is enabled, when a group or a system is selected.
   To know more about System selection kindly refer **System selection interface** section.
12 Click **Update selected** to view the selected items and click **Next**.
13 Select the required **Interval** and **Limit to time Range option**.
14 Select the required **Format option** (i.e. Summary, Extended Summary, Detail, Trend Report).
15 Select the required **Export Type** (i.e. PDF file, Word Document, HTML file, Quick View (not saved on hard disk)).
16 Select the required **Chart Type** (i.e. Donut, Bar, Line graph).
17 Select **Sort by** (Computer or User).
18 Click **Next>>**.

19 Enter the appropriate **Refine** and **Filter** details.
20 Click Next>>.
21 Enter the relevant Title, Header, Footer, and Description data.

![Figure 19]

22 Click Next>>.
Review cost details and configure the publishing options window opens.

**NOTE**

Publishing options are disabled because On Demand (foreground processing) has been selected.

![Figure 20]
23 Click **Next>>**.

The last step of **Completing Report Configuration Wizard** opens.

24 Select **Override indexer** if required, and then select **Generate Report**.