Netsurion | EventTracker®

New System selection interface

EventTracker v9.3 and above

Publication Date: January 15, 2021

Abstract

This guide will help you to use the enhanced system selection interface in log search and report configuration in EventTracker. It helps in navigating through the system structure in an easier way to perform search.

For complete log search and report configuration kindly refer to the main user guide.

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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Advanced Search

Here search is performed using the **Elastic Search**.

- Enter a Lucene query for searching or select from the fields available in the **Search In** box.

For example, to search for event source and event id and filter event computer

- Write a Lucene query: "**event_source:(*EVENTTRACKER*) AND event_id:(3240 || 2040 || 2037) AND NOT event_computer:(*-DLA)**" to perform a search.
  or
- You can choose the **duration** and can also select from the **system selection interface** in the left pane.

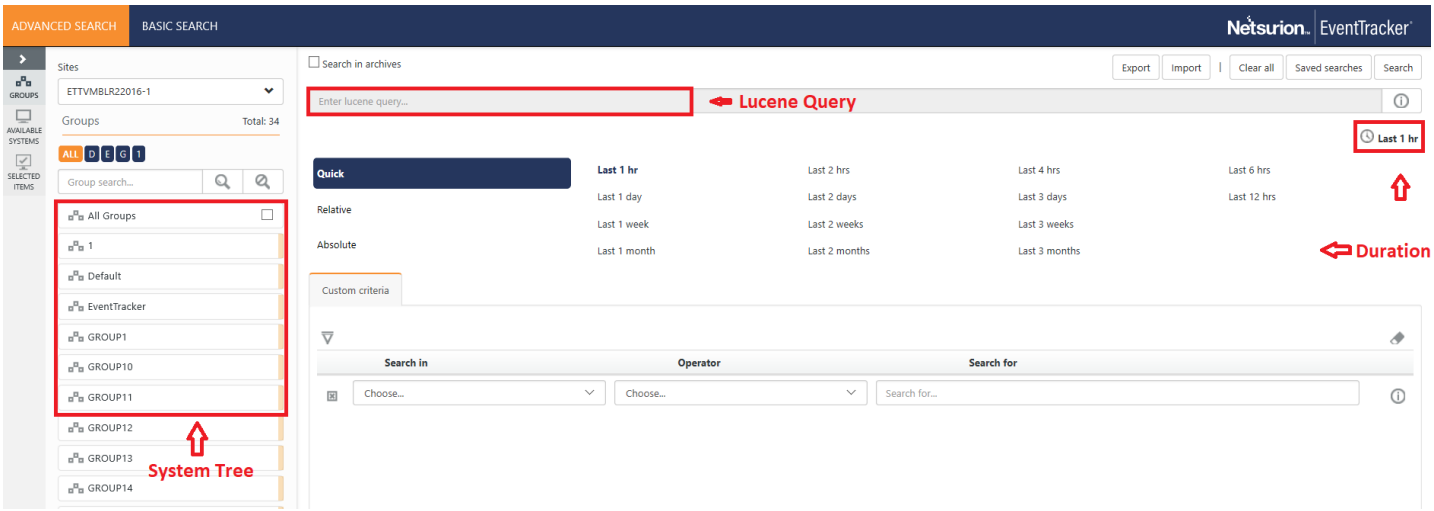

Figure 1

1.1 New System selection interface (System Tree) search

1. In the **Advanced search** page, in the left pane, click the **Sites** drop down arrow and choose the required Site, the respective groups present in the Sites appear.
2. Enter the group name in the Group search box to search the **Group** or
   Click the hotkeys to search the **Groups** in alphabetical order.

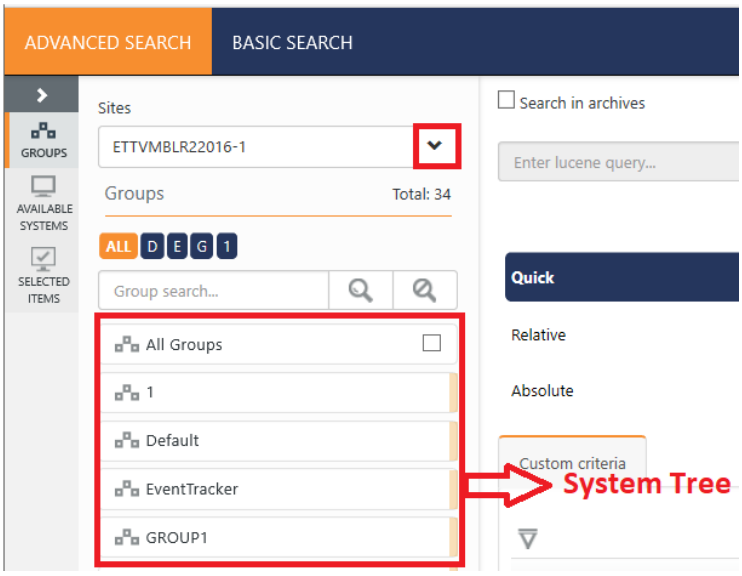

Figure 2

Note: "All Groups" will display all the systems across the groups of a specific site.

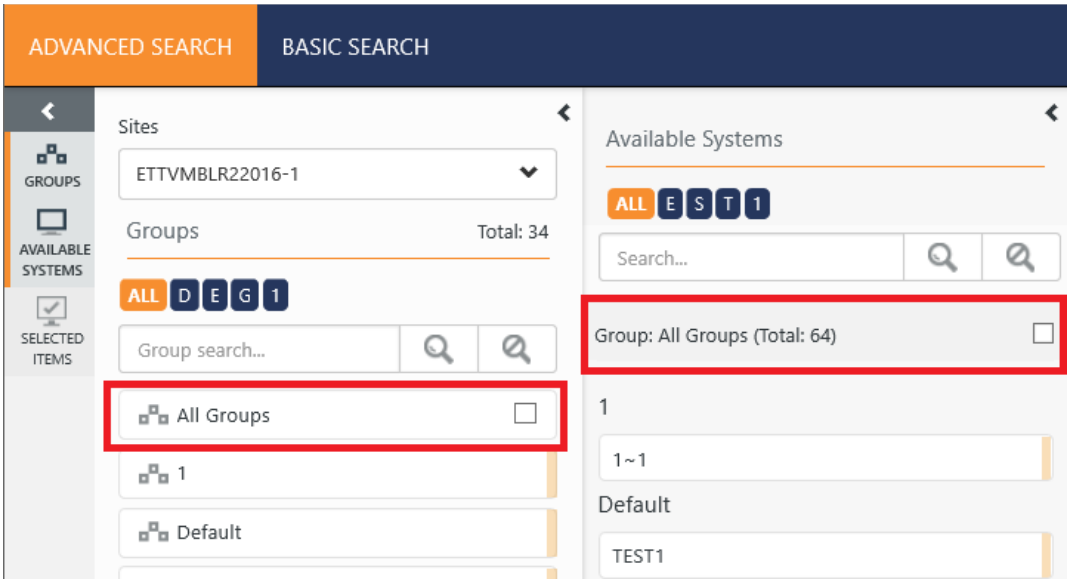

Figure 3

3. Click on any group to populate the systems available in the group.
   The available systems display in the **Available Systems** pane.
   You may also click the hotkeys to search the **systems** in alphabetical order.

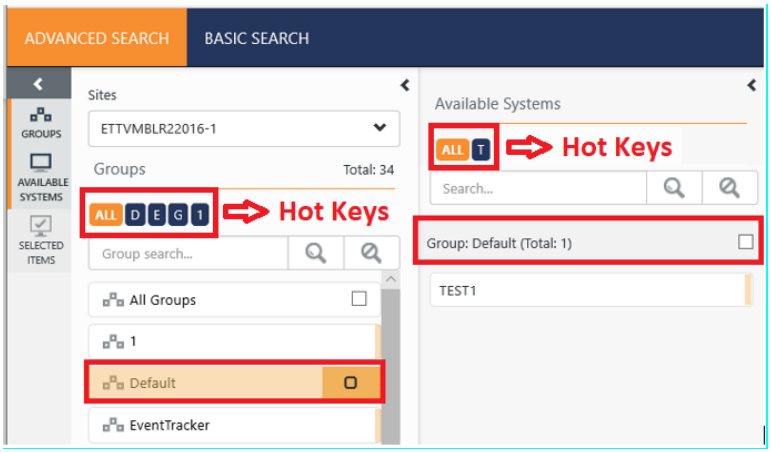

Figure 4

4. Select any group from the group pane. The selected Group is seen in Selected Items pane.
   The Groups turn orange when you hover the mouse and turns green when selected.
   Using the Collapse button on top right corner of each pane, the pane can be shown or hidden.
   We can also show or hide the panes by clicking on the respective section on the left most vertical bar.

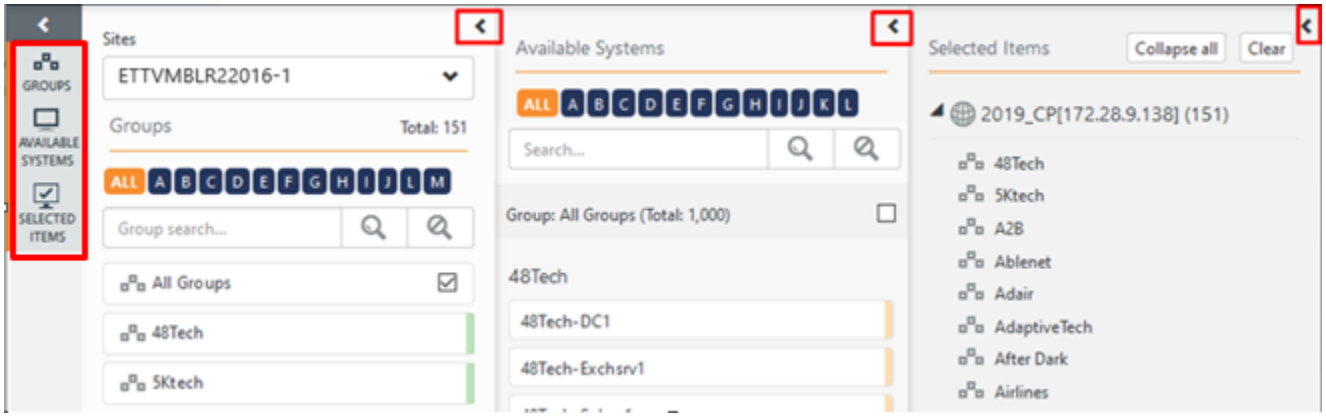

Figure 5

5. **Collapse all** and **Expand all** affect the occurrences of selected items.

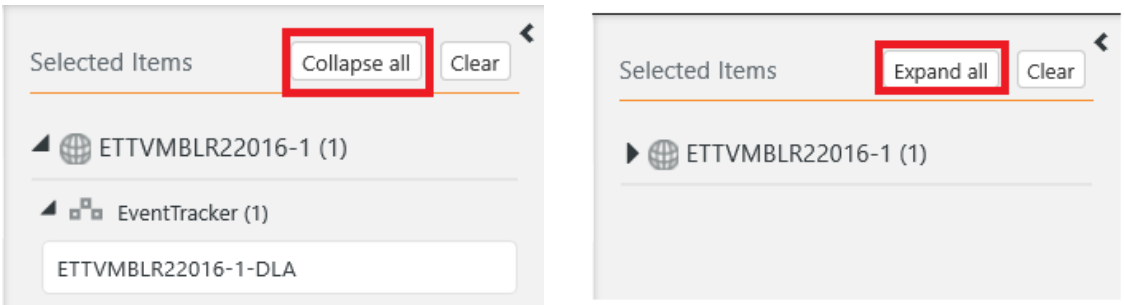

Figure 6

Note: Now we can click anywhere outside the system tree frame to use options like Lucene Query, Custom Criteria or to click on Search.

1.2 Group Based Search

1. Select any group from the group pane.
   Selected group displays in **Selected Items** pane and **Collapse All** button is enabled.
   The Groups turn orange when you hover the mouse and turns green when selected.

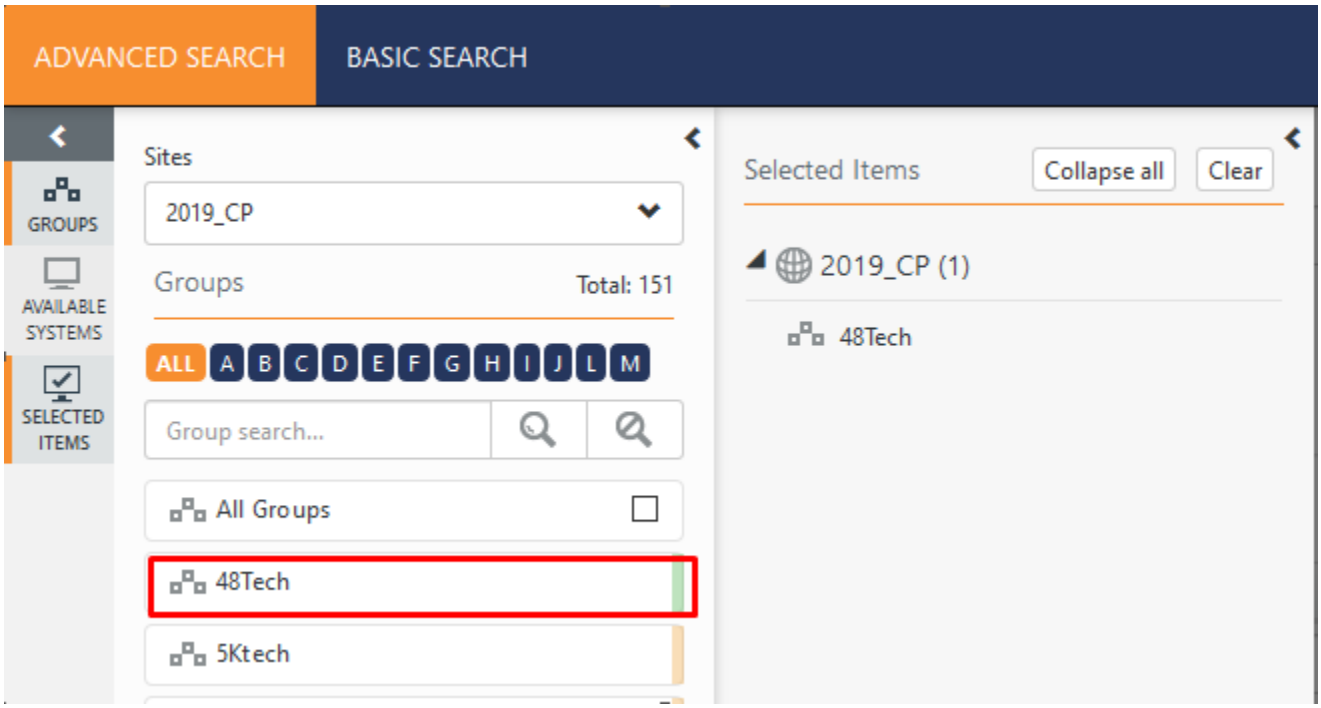

Figure 7

2. Click on the **Search** to perform group-based log search.

   Note: In Elastic group-based search the lucene query will go with group name Ex: event_group_name: ("48Tech") only if **Archiver at group level** is enabled.

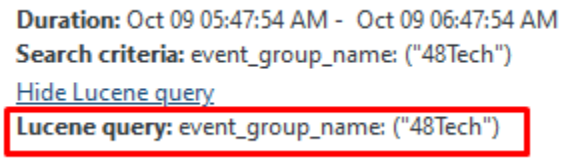

Figure 8

1.3 All Groups Selection search

1. Enable **All groups** check box, to select all the groups of a site.
   Selected groups are displayed in **Selected Items** pane.

   Note: Filtered group results can be selected in bulk by enabling the check box.

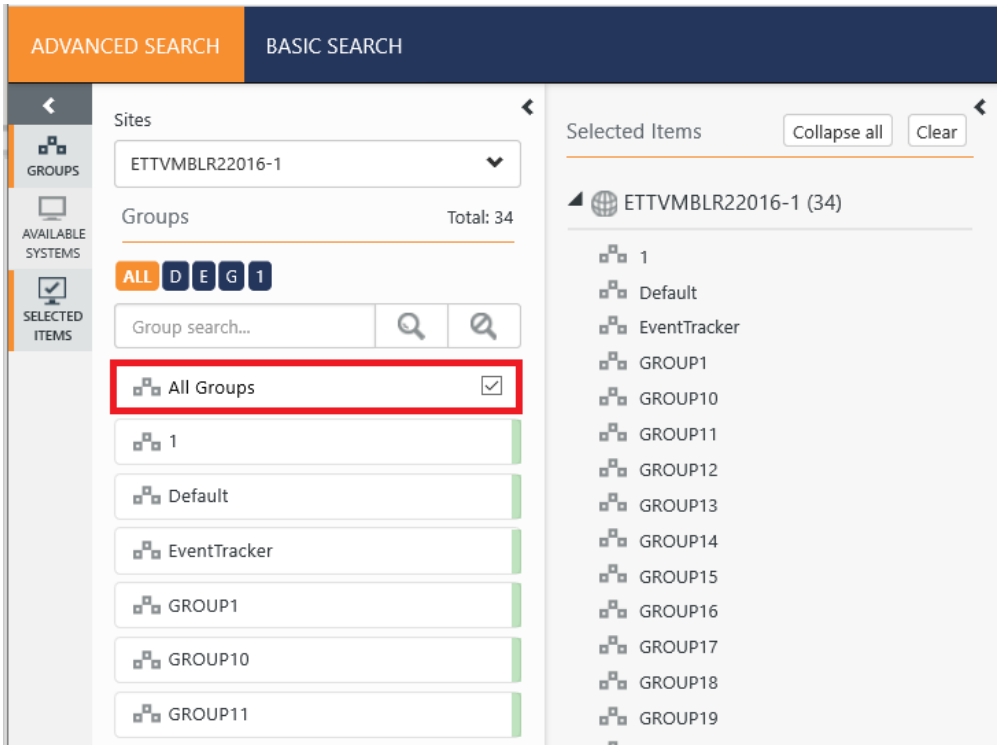

Figure 9

1.4 System Based Search

1. Select the required Group from the **Groups** Pane, available systems are displayed in the **Available Systems** pane.
2. Select any system, and the selected system displays in the **Selected Items pane**.
   The System turns orange when you hover the mouse and turns green when selected.
3. Click on **Collapse All/Expand All** button to hide or expand to view systems in bulk.

   Note: Individual Site/Group can also be collapsed and expanded by clicking on respective Site/Group name.

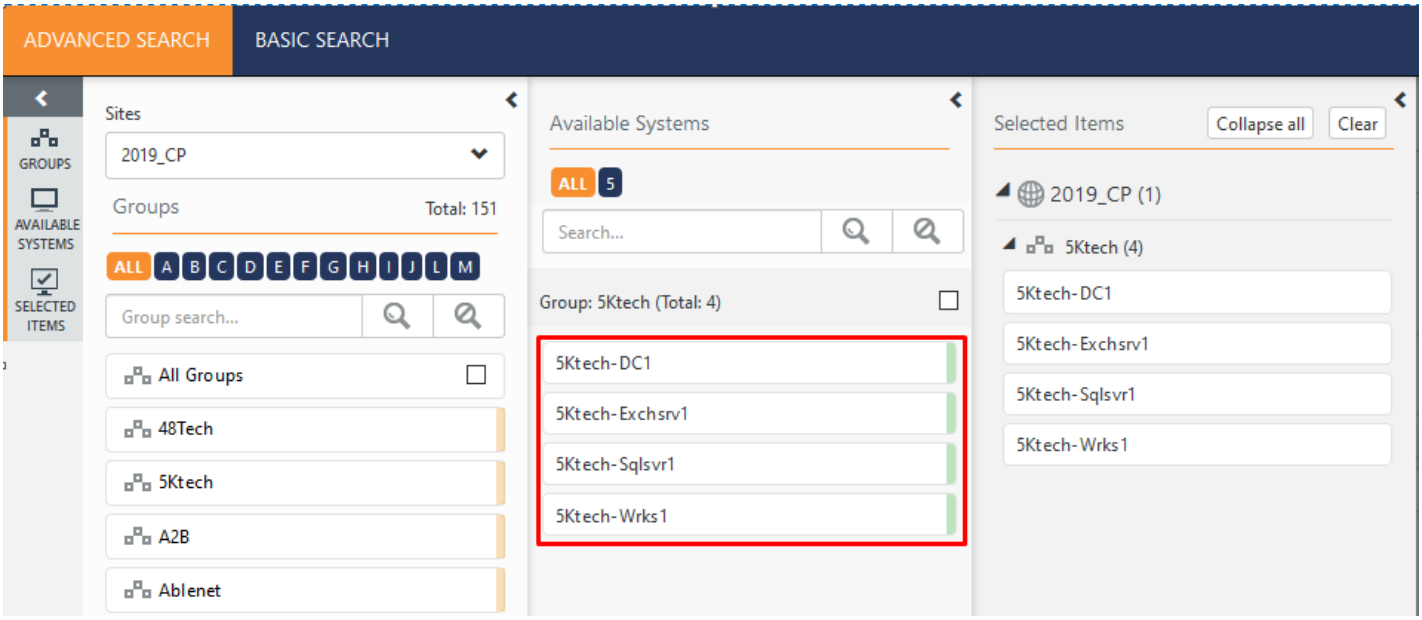

Figure 10

4. Click on the **Search** perform computer-based log search.
5. Click **'<'** button to collapse all the panes.

Note: To search a specific system, open the **Available Systems** pane directly and search systems across the groups of a specific site.

1.5 All Systems Selection Search

To select all the systems under a site

1. Click **All Groups** in Groups pane.
   All the systems display in **Available Systems** pane.
2. Select **Groups: All Groups** check box to select all the systems.

Note: Filtered results also can be selected in bulk using this check box.

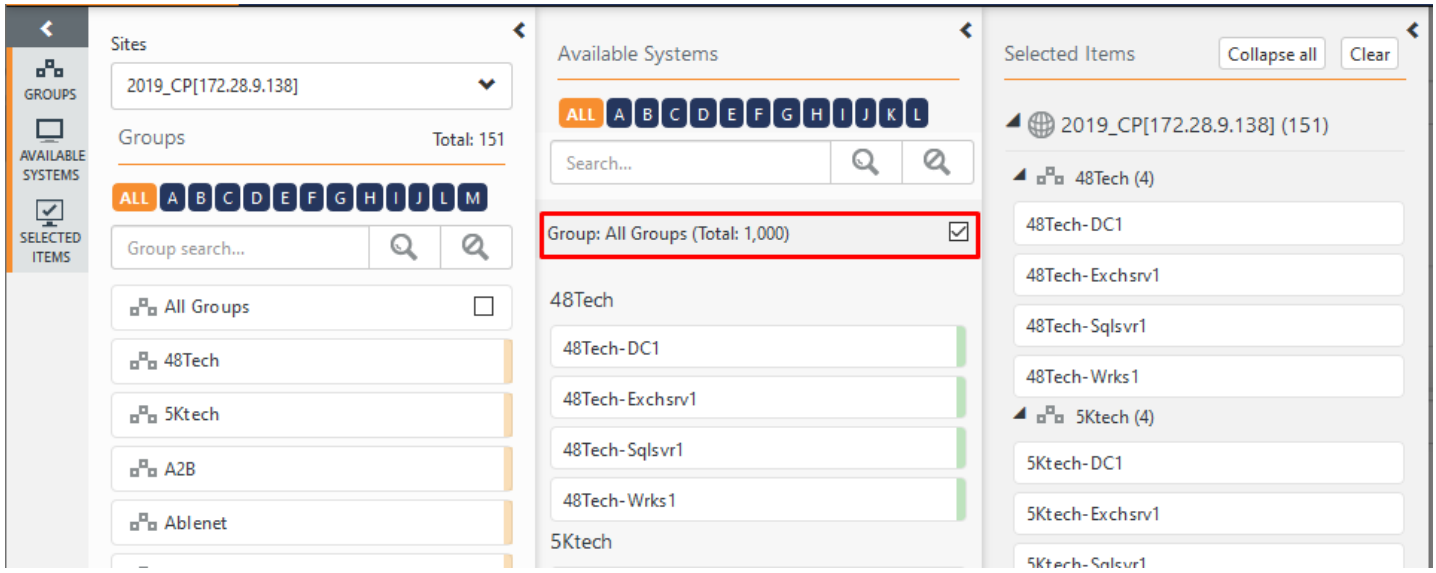

Figure 11

2. Importing the Saved Search Criteria

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

To import saved search criteria

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

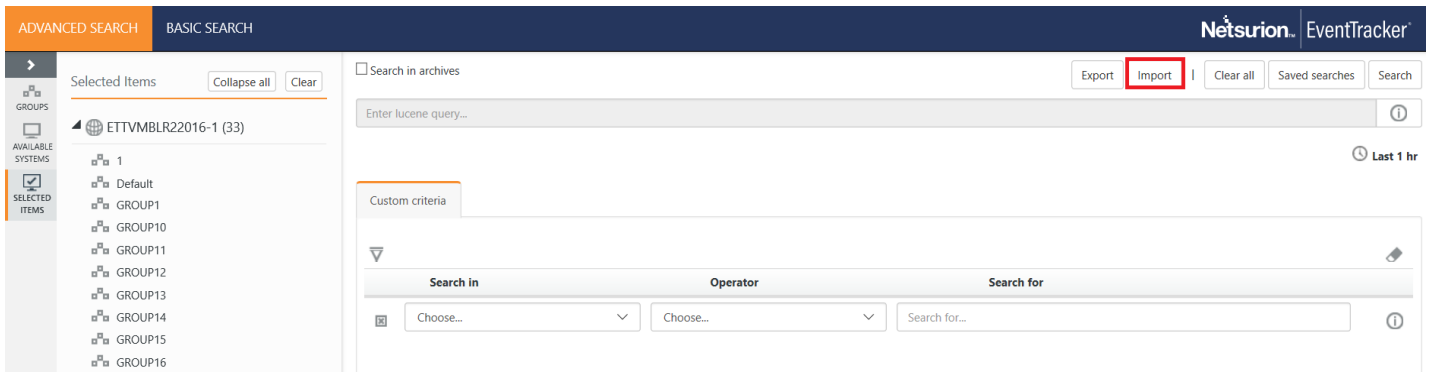

Figure 12

Import page opens

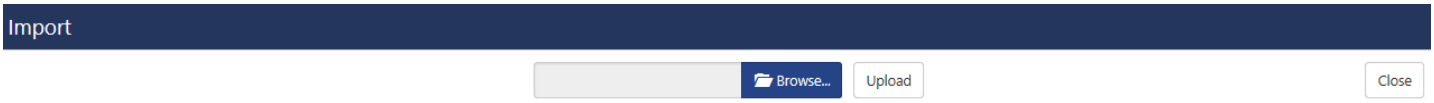

Figure 13

2. 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 available in the **Elastic** option or in the **Archive** option.

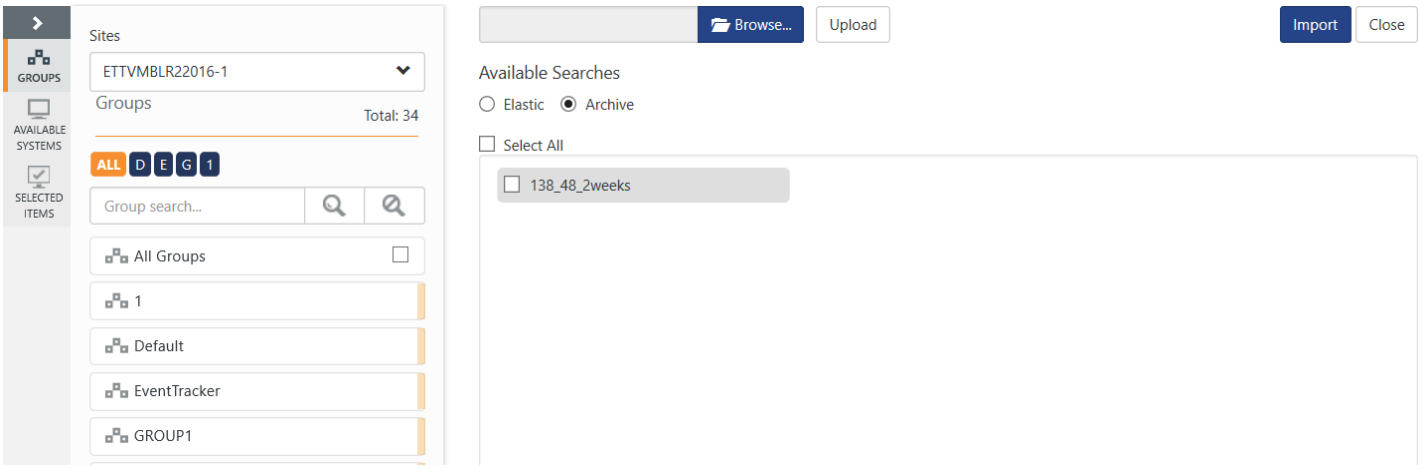

Figure 14

To apply the criteria for the selected groups/systems

3. Choose the saved search files (criteria) and select the required group and then click Import.

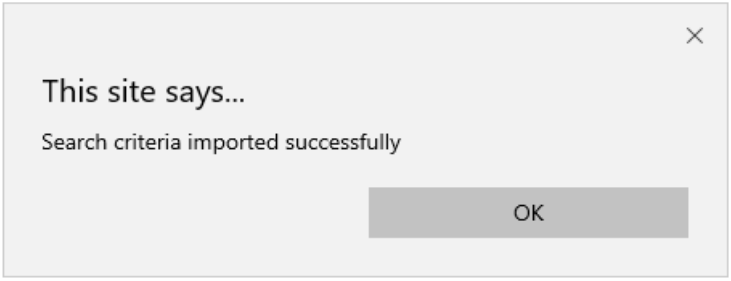

Figure 15

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.

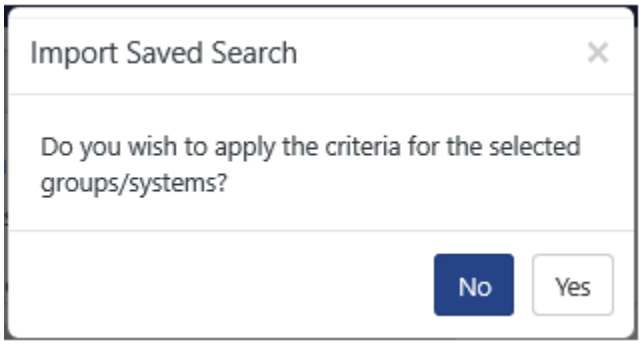

Figure 16

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 are 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.

The below section shows how to use new system tree interface during one of the report configurations. Refer 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. 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.**

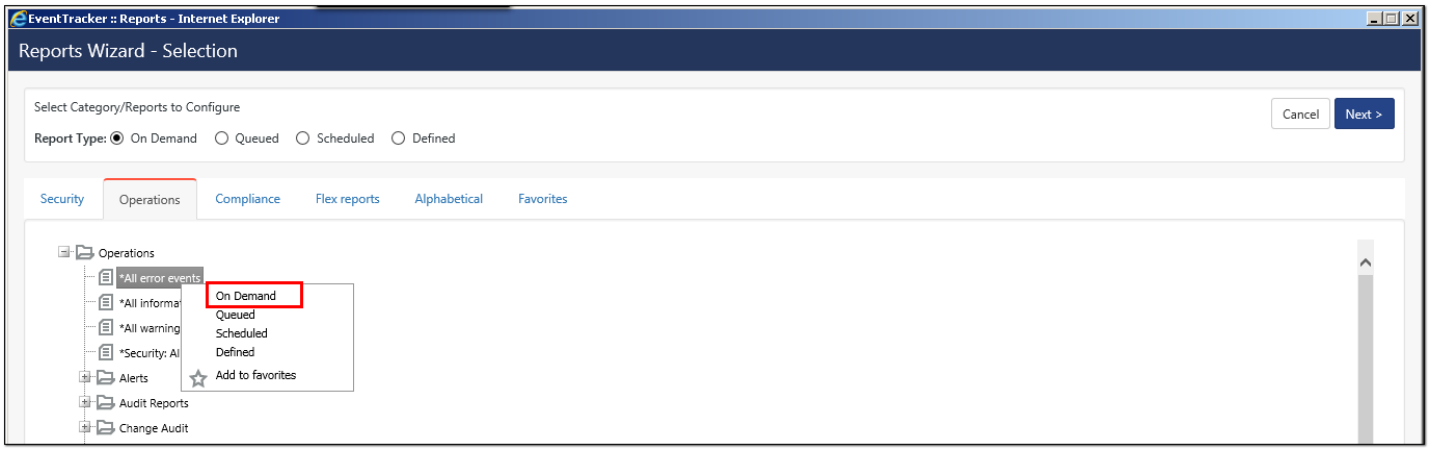

Figure 17

EventTracker opens the Reports Wizard.

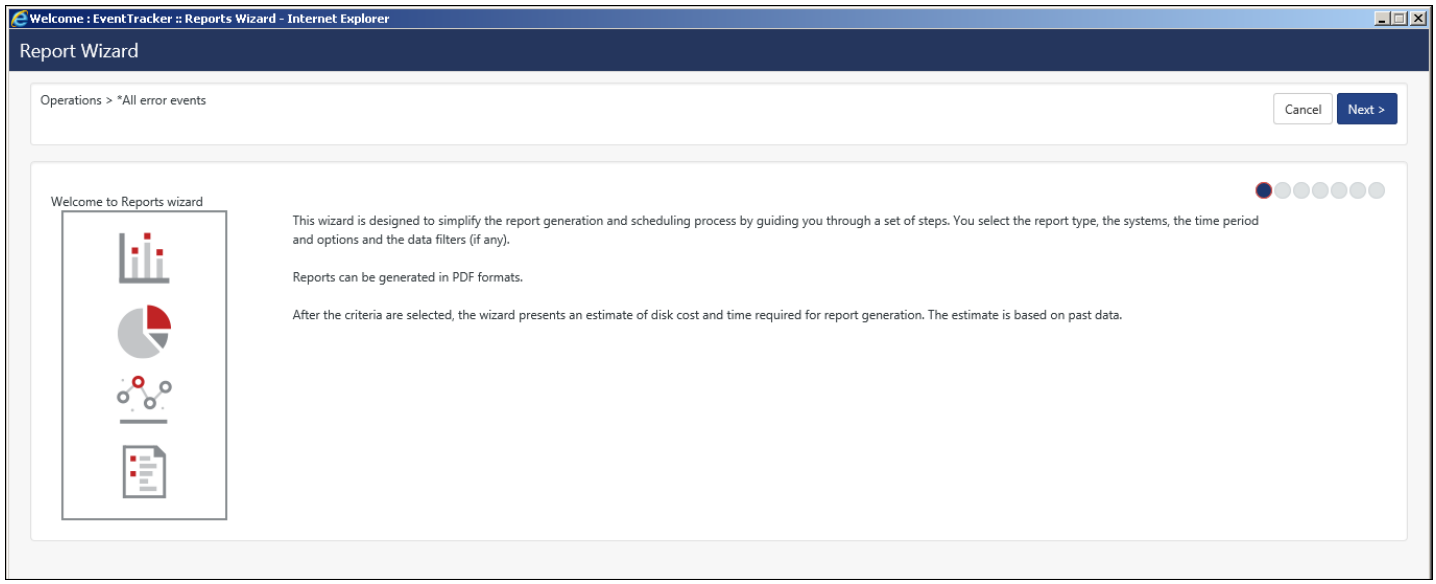

Figure 18

7 Click **Next >>.**

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

Note:

- Selecting the **Sites/Groups** option from the drop down enables 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.

9 You can select the required group directly or select the systems under the group.

- The Groups and systems turn orange when you hover the mouse and turns green when selected.

10 When a group or a system is selected, the selected group or system displays in the **Selected Items** pane and the **Collapse All button** is enabled.
To know more about System selection, refer System selection interface section.

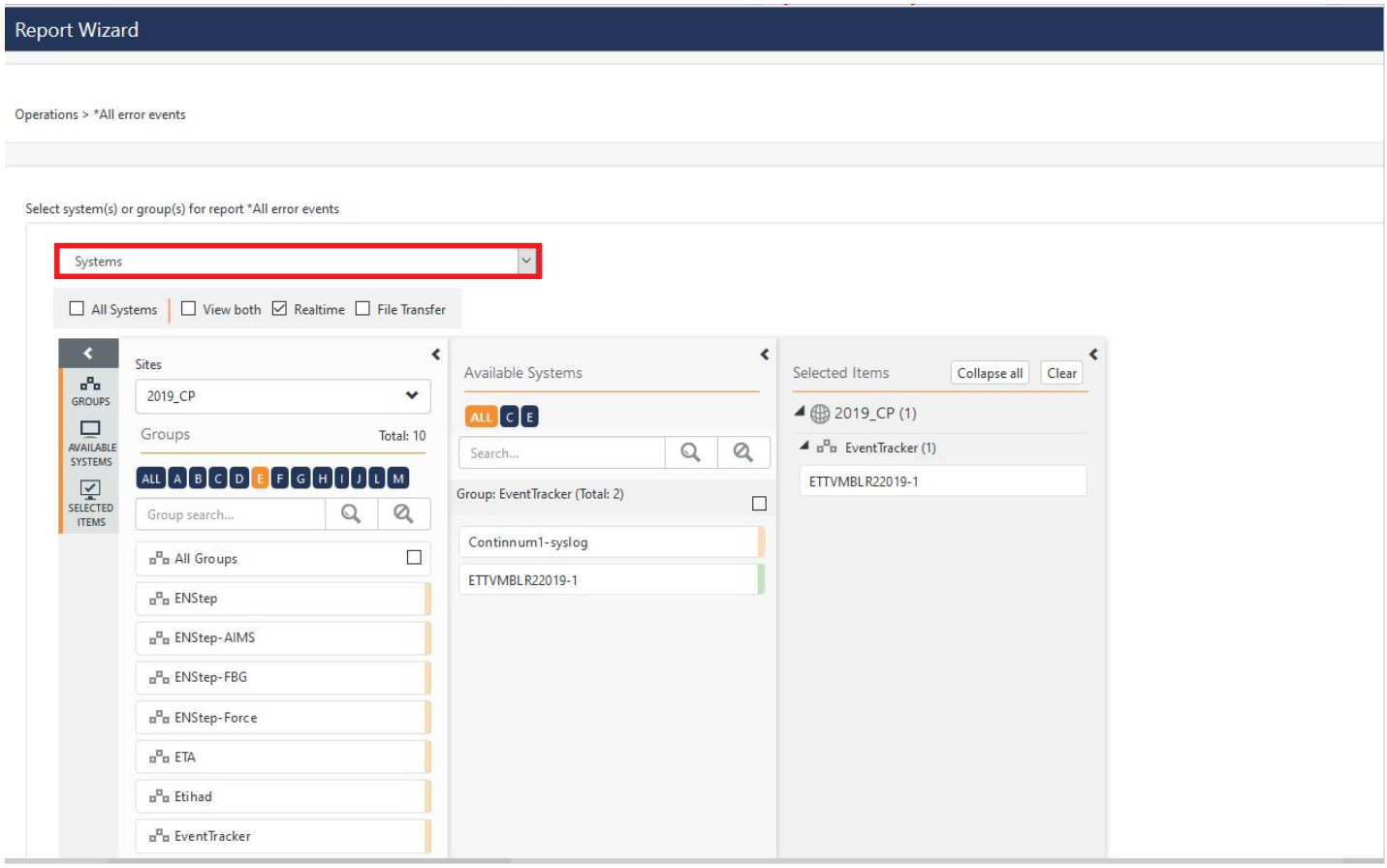

Figure 19

11 Click on **Collapse All/Expand All** button to hide or expand to view systems in bulk.

12 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).**

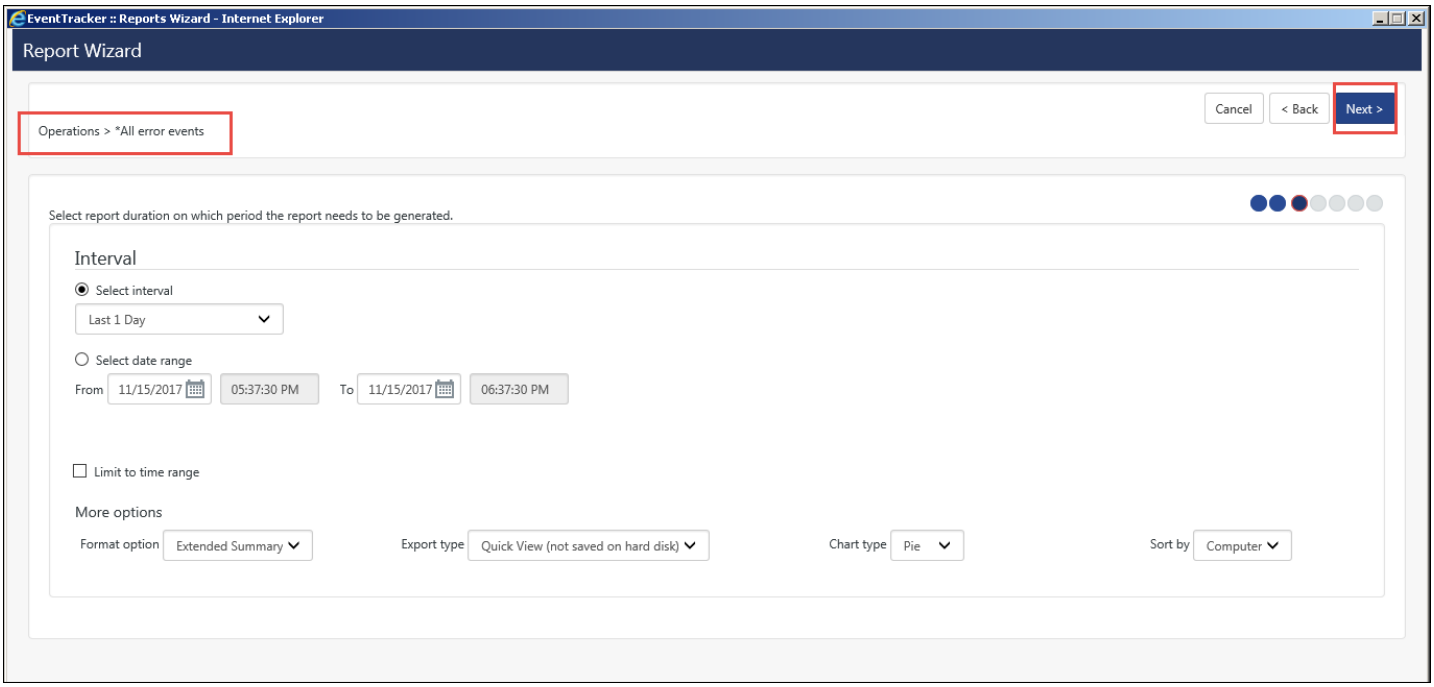

Figure 20

18 Click **Next>>**.

19 Enter the appropriate **Refine** and **Filter** details.

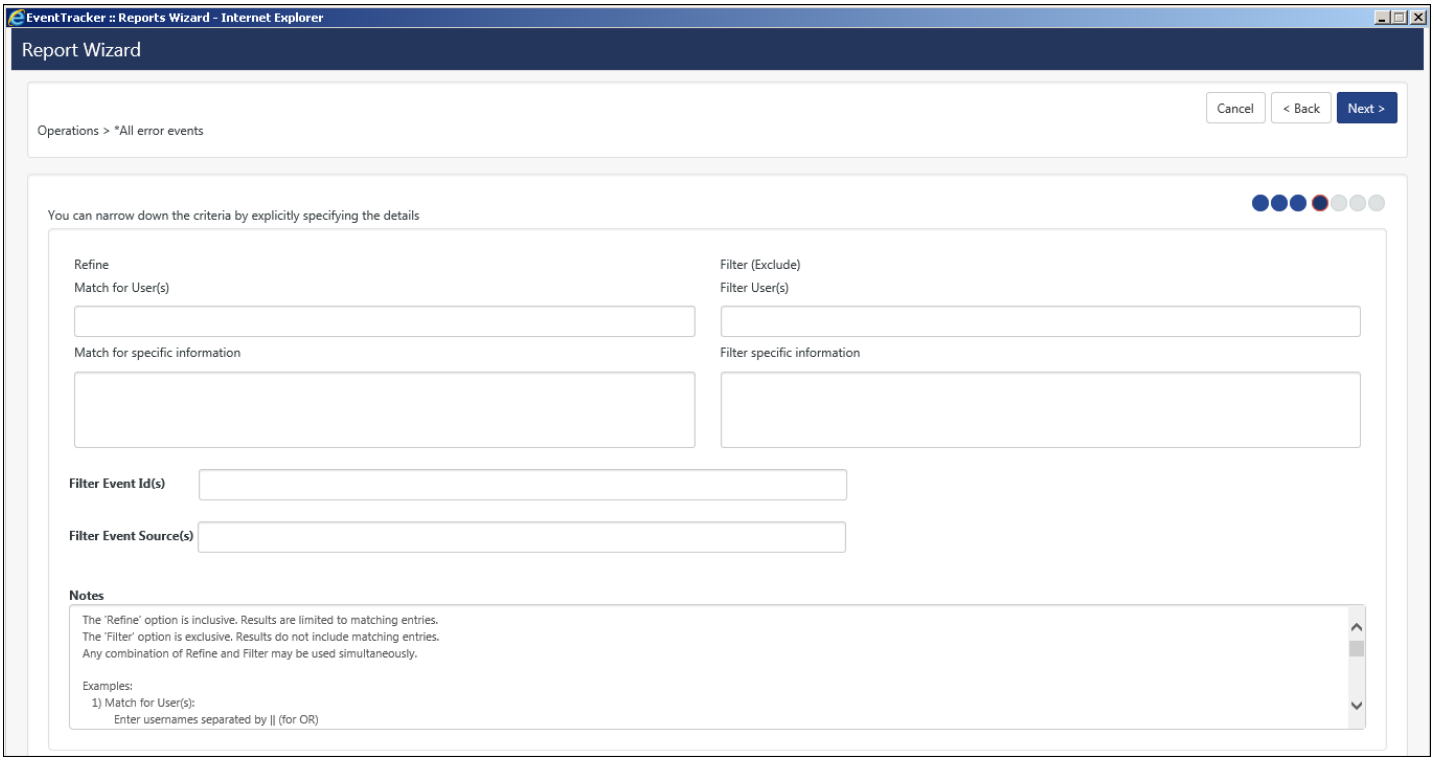

Figure 21

20 Click **Next>>**.

21 Enter the relevant **Title**, **Header**, **Footer**, and **Description** data.

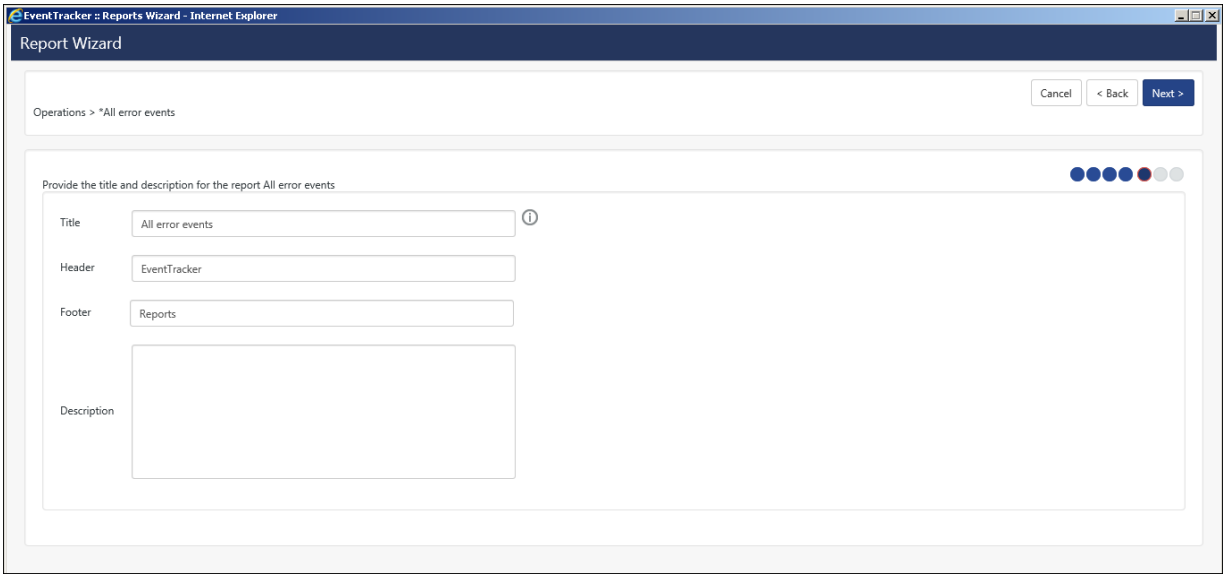

Figure 22

22 Click **Next>>**.

23 Review the cost details and configure.
The publishing options window opens.

NOTE

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

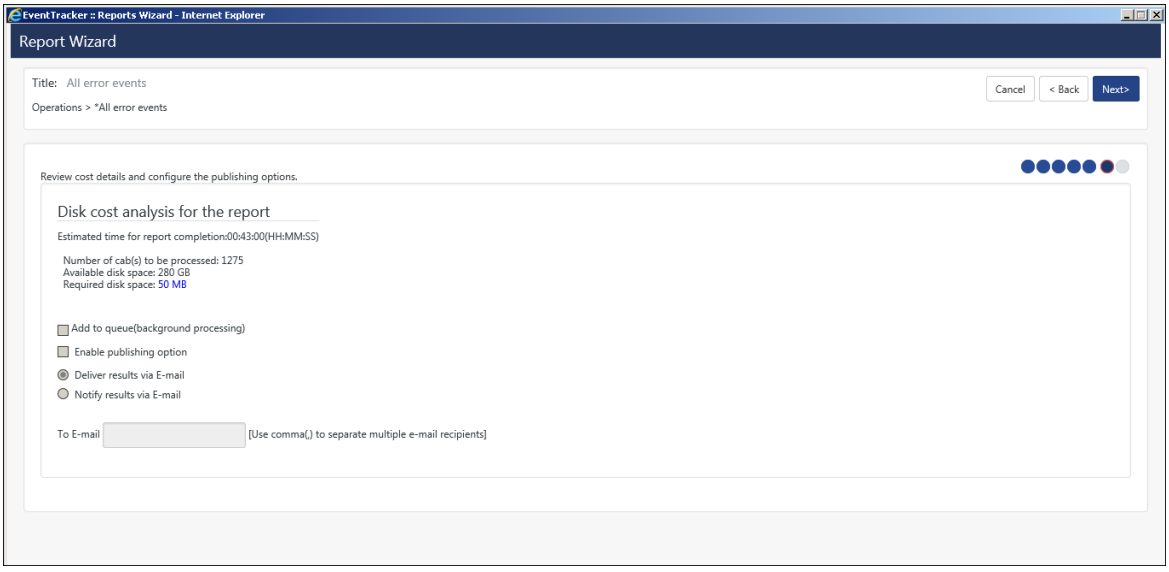

Figure 23

24 Click **Next>>**.
Completing Report Configuration Wizard opens.

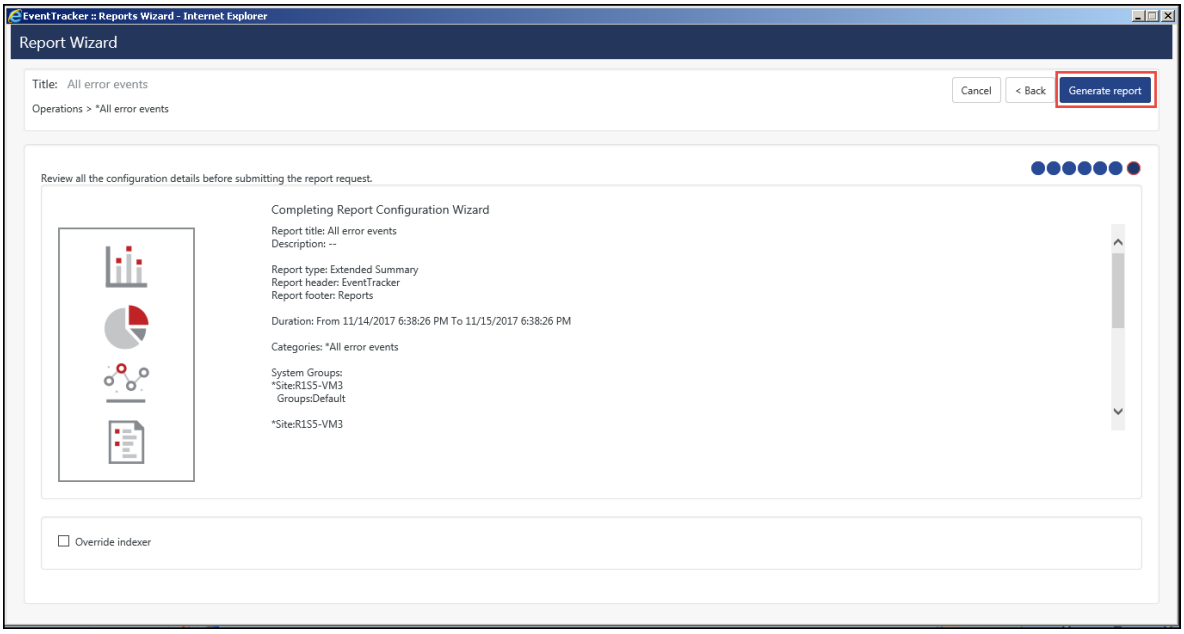

Figure 24

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