

# Enhancement in Log Search and System Manager

## Abstract

This document provides enhancements in EventTracker v9.0 log search result and system manager.

## Audience

EventTracker v9.0 user(s) who wish to refine the log search result by selecting multiple normalized data and also given an option to pivot the log search results, by selecting multiple CIM fields.

*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.*

*© 2019 Netsurion. 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
Audience.....	1
Options to add multiple CIM fields for pivoting.....	3
Option to add multiple normalized data by using include/exclude options in log search. ....	5
Option to move systems from one group to other in System Manager.....	8

# Options to add multiple CIM fields for pivoting

After performing log search, the user can see new enhancements in the log search result window.

User is provided with an option to filter multiple interesting fields for pivoting the log search results.

To perform multiple CIM field for pivoting.

1. Click **“Add multiple fields for Pivoting”**  icon in the **Interesting** field tab.

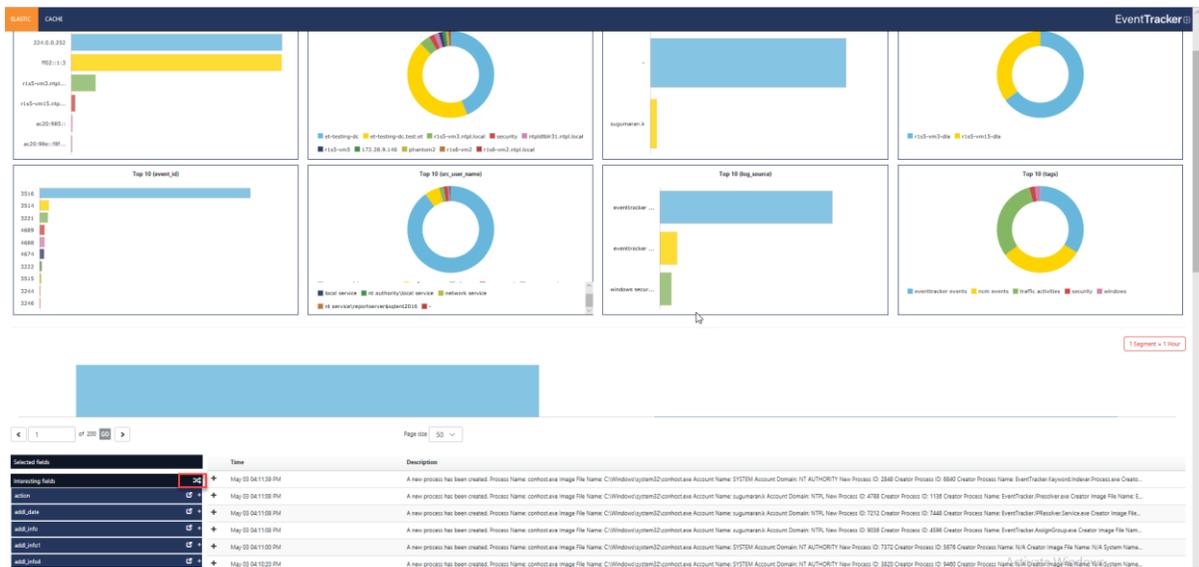


Figure 1

2. **“Add multiple fields for pivoting”** dialog box appears.

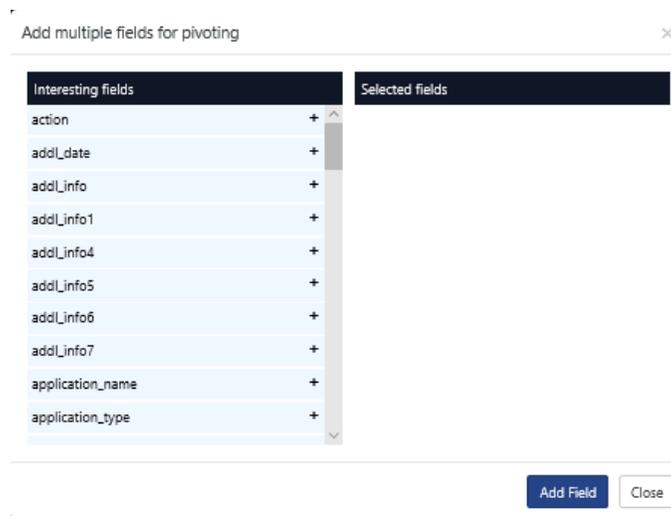


Figure 2

- Select the CIM fields by clicking **Add field (+ sign)** icon and click **Add Field** button to add multiple fields for pivoting.

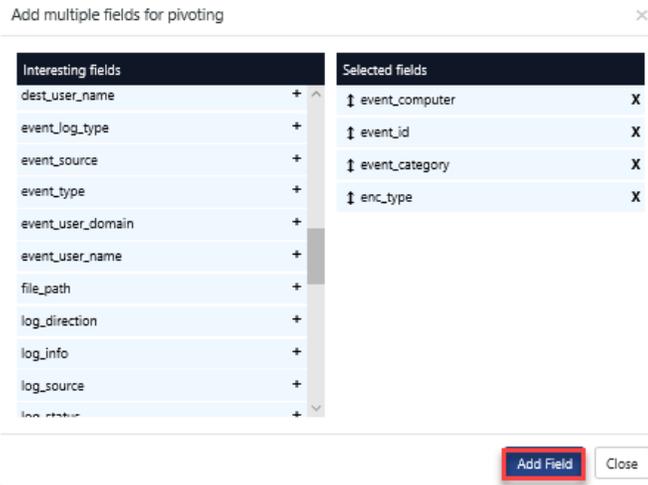


Figure 3

- The selected fields are displayed in the tabular form as a pivot column as well as under the **Selected field** tab.

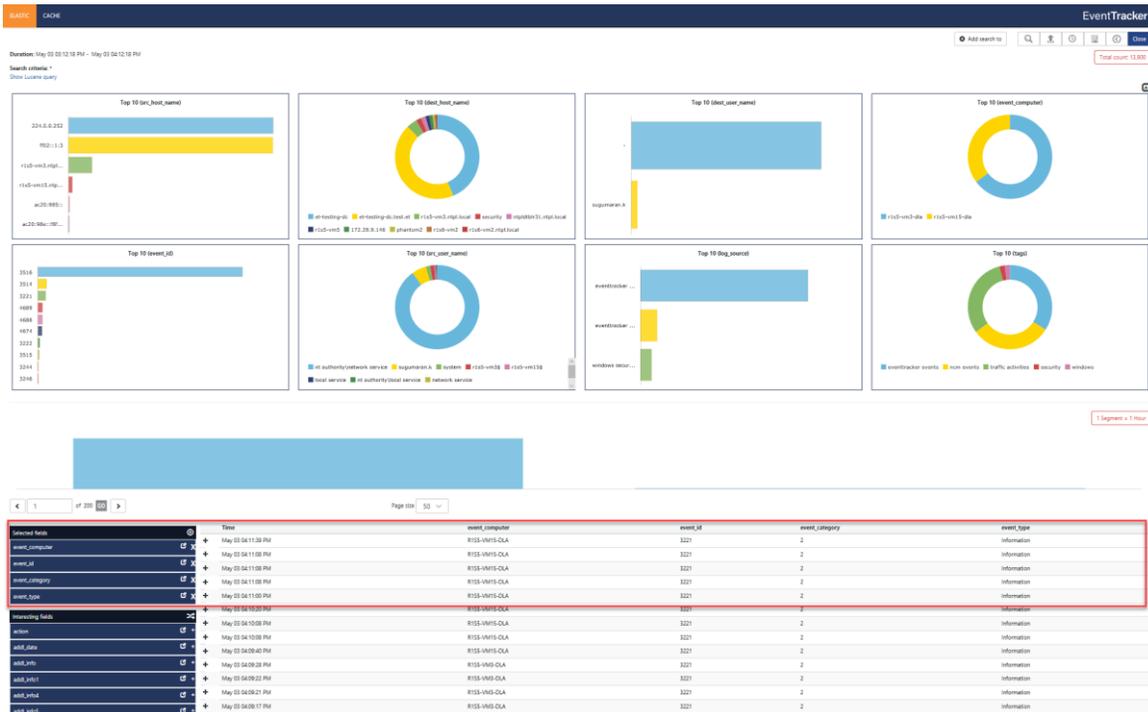


Figure 4

**NOTE:** The exported log search result file will contain pivoted columns with respect to columns selected for pivoting.

# Option to add multiple normalized data by using include/exclude options in log search.

To add the multiple CIM field values or data and get the results based on it

1. Click the **View field values**  icon for the respective CIM field. In this example “event\_id” is chosen.

Selected fields	Time	Description
Interesting fields	+	May 06 11:30:17 AM
action	+	May 06 11:30:17 AM
addl_date	+	May 06 11:30:17 AM
addl_info	+	May 06 11:30:16 AM
addl_info1	+	May 06 11:30:16 AM
addl_info4	+	May 06 11:30:16 AM
addl_info5	+	May 06 11:30:16 AM
addl_info6	+	May 06 11:30:16 AM
addl_info7	+	May 06 11:30:16 AM
application_name	+	May 06 11:30:16 AM

Figure 5

2. Choose the required values to be displayed from the “Values for event\_id” dialog box window that appears and click **Include**.

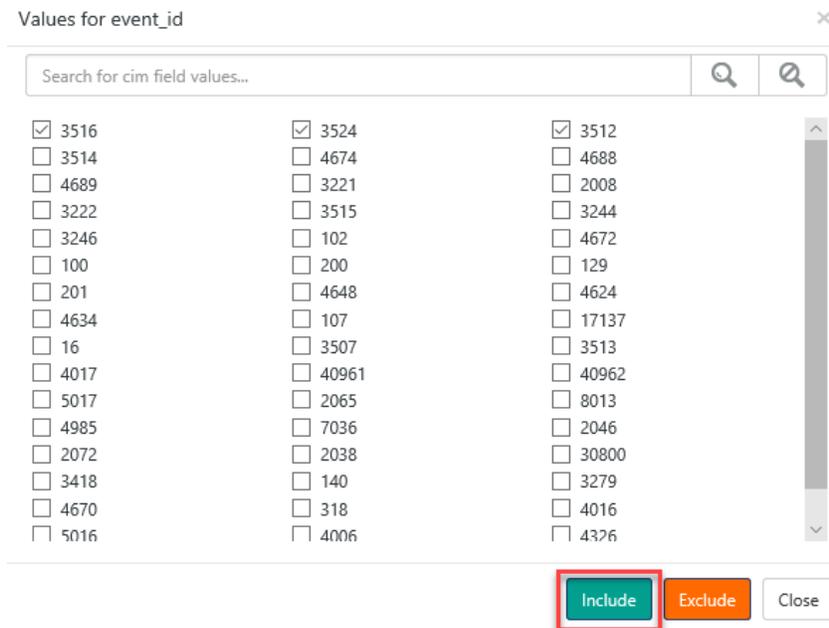


Figure 6

3. The search criteria result displays depending on the values that are selected.

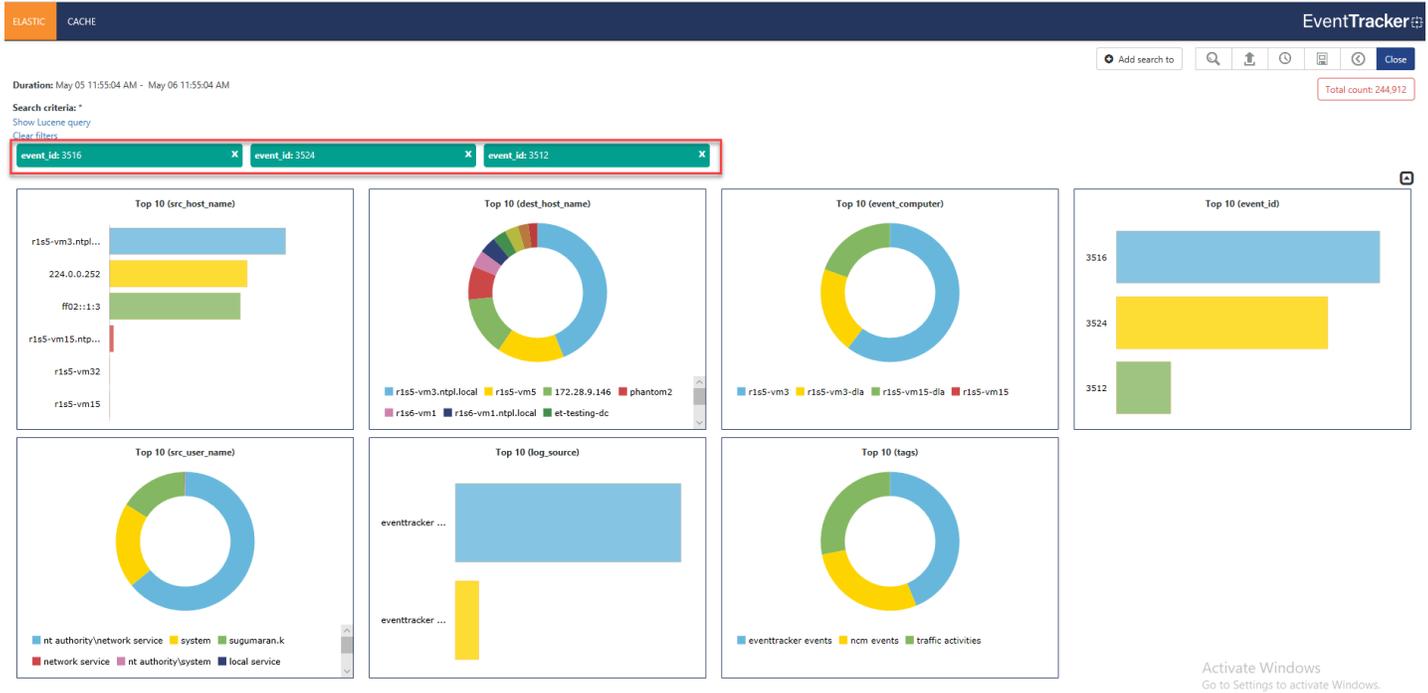


Figure 7

To exclude the values, in the result page.

1. Click the **View field values** icon for the “event\_id” CIM field.



Figure 8

2. Choose the values from the “Values for event\_id” dialog box window and click **Exclude** option.

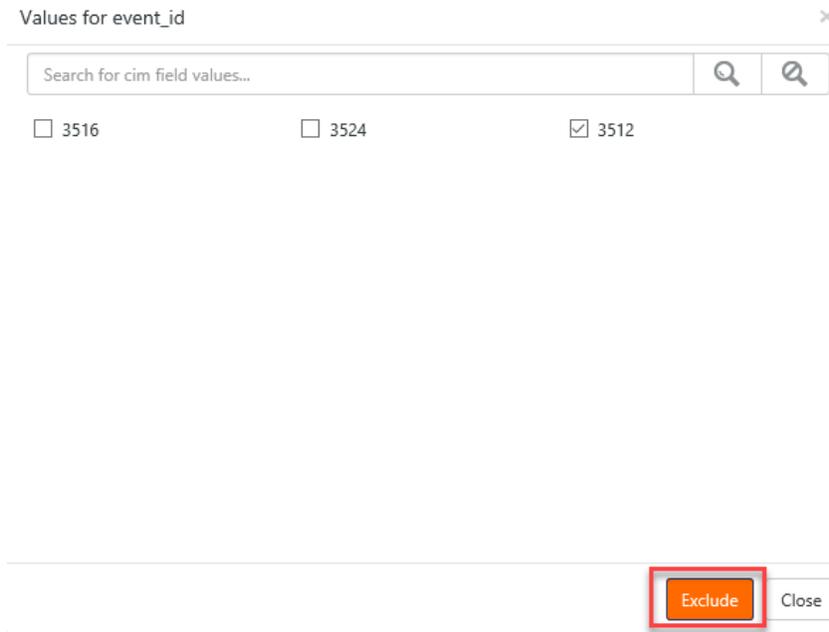


Figure 9

3. The excluded value is highlighted in orange color.

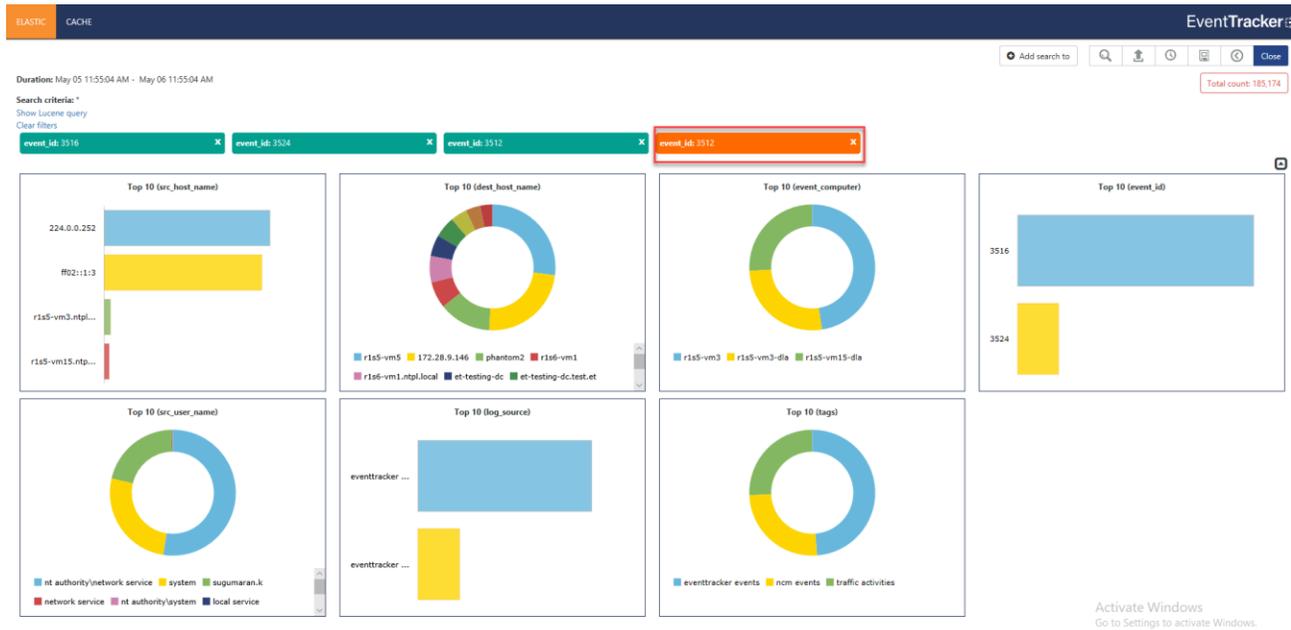


Figure 10

**NOTE: The same changes apply for both Cache Search and Archive search.**

# Option to move systems from one group to other in System Manager.

User is provided with an option to select the system and move to any other groups.

To move the system to other groups.

1. Click **Admin** option from the Home page and choose Systems.

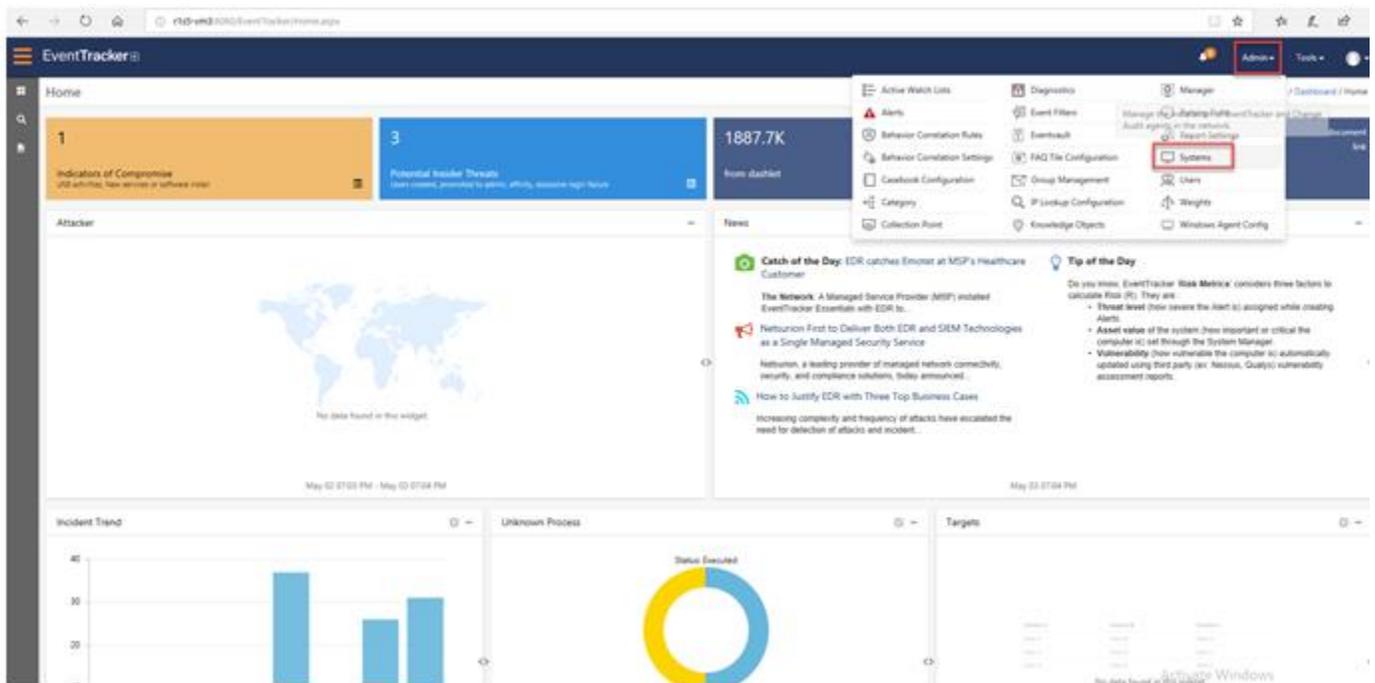


Figure 11

2. In the Systems Manager Page, click  **Groups** icon.

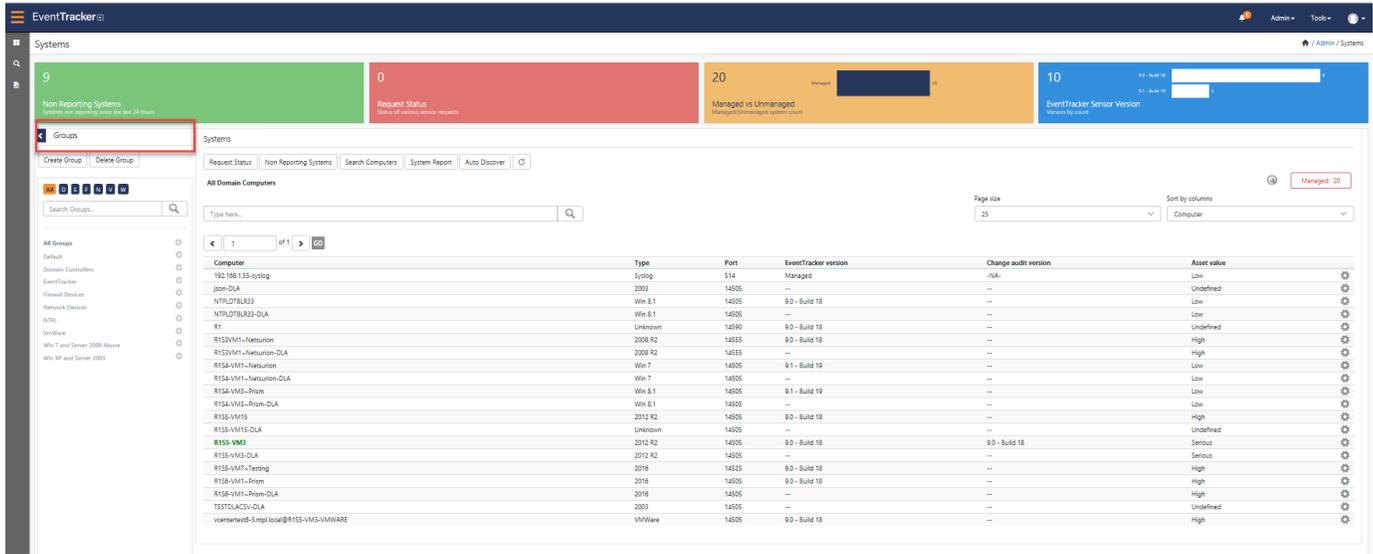


Figure 12

3. Click  **Tools** icon and choose **Move System** option.

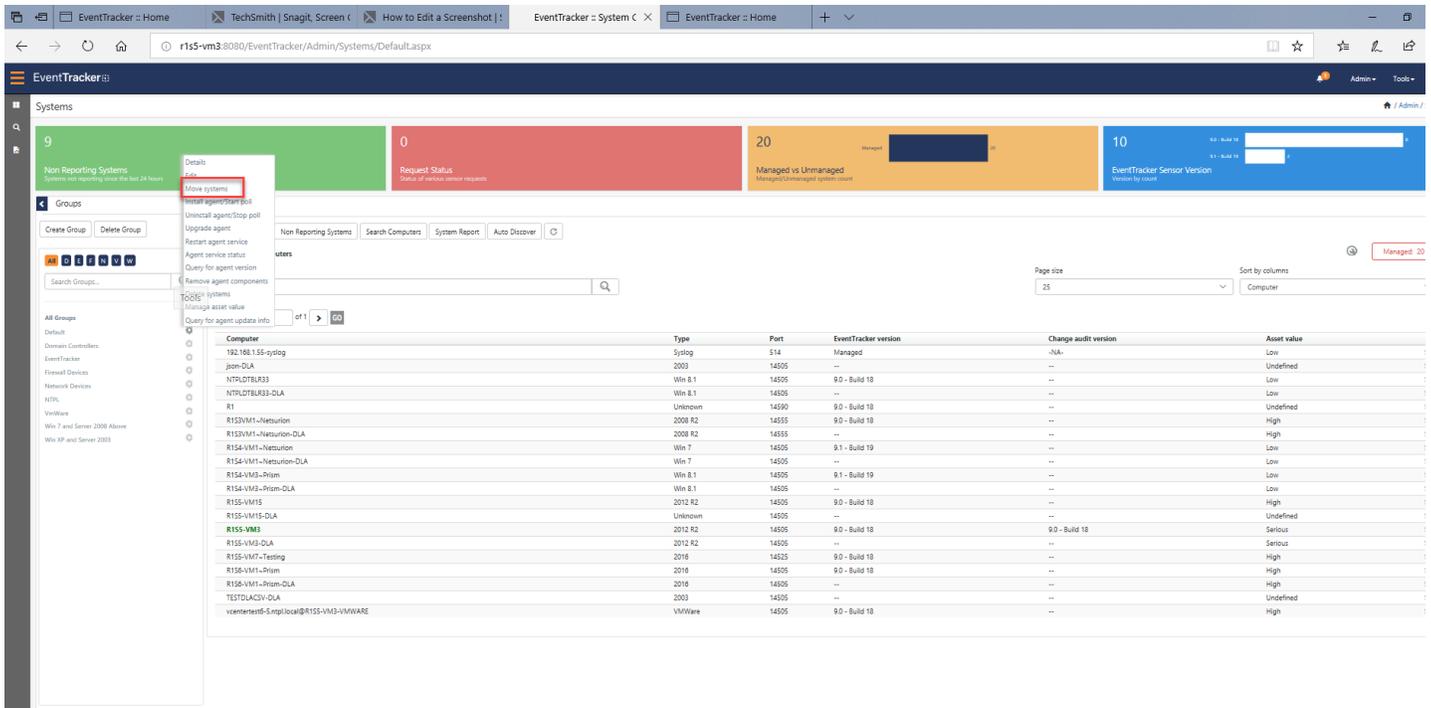


Figure 13

4. **“Move Systems from group”** window opens.

Move systems from group: Default

Select group

Domain Controllers

Select Systems

Search...

192.168.1.55-syslog

json-DLA

NTPDTPBLR33

NTPDTPBLR33-DLA

R1

R153VM1~Netsurion

R153VM1~Netsurion-DLA

R154-VM1~Netsurion

Move Cancel

Figure 14

5. **Select Group** from the drop-down option you want to move from and **Select Systems** from the list.
6. Click **Move** button to move the systems from the selected group.