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	
1.1 New System selection interface (System Tree) search	3
1.2 Group Based Search	6
1.3 All Groups Selection search	7
1.4 System Based Search	7
1.5 All Systems Selection Search	8
2. Importing the Saved Search Criteria	9
3. Reports Configuration	12
3.1 Generating on Demand Reports	12



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.

ADVAN	CED SEARCH	BASIC SEARCH					Netsurion. EventTracker	r'
>	Sites		Search in archives				Export Import I Clear all Saved searches Searc	ch
GROUPS	ETTVMBLR220	16-1 👻	Enter lucene query		 Lucene Query 		G)
AVAILABLE	Groups	Total: 34					() Last 1	l br
	ALL D E G	0	Quick	Last 1 hr	Last 2 hrs	Last 4 hrs	Last 6 hrs	
ITEMS	Group search	ର୍ ଷ୍	quick	Last 1 day	Last 2 days	Last 3 days	Last 12 hrs	1
	a ⁿ a All Group	s 🗌	Relative	Last 1 week	Last 2 weeks	Last 3 weeks		
	a¶a 1		Absolute	Last 1 month	Last 2 months	Last 3 months	🗢 Durati	ion
	📲 Default		Custom criteria					
	e ⁿ e EventTrac	ker						
	∎ [®] ∎ GROUP1		$\overline{\nabla}$				Å	,
	_B GROUP10		Search in		Operator	Search for		
	∎ª GROUP11		E Choose	∽ Choose	~	Search for	0	t
	B GROUP12							
	∎ [®] ∎ GROUP13	System Tree						
	B ^B B GROUP14	5,51011100						



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.



ADVAN	ICED SEARCH	BASIC SEAR	СН			
CROUPS GROUPS AVAILABLE SYSTEMS SELECTED ITEMS	Sites ETTVMBLR220 Groups ALL D E G Group search.	116-1 1 	Q	Image: Search in archives Image: Search in archives Image: Enter lucene query Total: 34 Image: Quick Image: Relative		
	Bang Default Bang EventTrac	:ker			Absolute Custom criteria System Tree V	



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

ADVAN	ICED SEARCH BASIC SEARCH	
CROUPS	Sites ETTVMBLR22016-1	Available Systems ALL E S T 1 Search
SELECTED ITEMS	ALL D E G Group search Q Q	Group: All Groups (Total: 64)
	All Groups	1 1~1
	 Default	Default TEST1



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.



ADVAN	CED SEARCH	BASIC SEARCH				
<	Sites			<	Available Systems	<
GROUPS	ETTVMBLR220	~				
AVAILABLE SYSTEMS SELECTED ITEMS	Groups		Total: 34		Sarch	0
	ALL DEG	🛛 🖚 Но	t Keys	ł	Searchin	~
	Group search.		Q Q	L	Group: Default (Total: 1)	
	📲 All Group)S			TEST1	
	a ⁿ a 1					
	∎ [∎] ∎ Default		0			
	∎∎ EventTrac	:ker				
			Figure	e 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.

<	Sites	<	Available Systems	<	Selected Items	Collapse all Cl	lear
	ETTVMBLR22016-1			0	4 () 2019_CP[172.2	28.9.138] (151)	
AILABLE		-	Search Q	Q	a ⁰ a 48Tech		
ECTED TEMS	Group search Q. Q.		Group: All Groups (Total: 1,000)		a ⁿ a SKtech a ⁿ a A2B		
	a ⁿ a All Groups		48Tech		a ⁿ a Ablenet a ⁿ a Adair		
	u ^u u 48Tech	48Tech-DC1		a ⁰ a AdaptiveTech			
	u ⁿ u SKtech	i l	48Tech-Exchsrv1		o ⁿ o After Dark		
					a a Airlines		

Figure 5

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

Selected Items Collapse all Clear	Selected Items Expand all Clear
▲ () ETTVMBLR22016-1 (1)	ETTVMBLR22016-1 (1)
🖌 📲 EventTracker (1)	
ETTVMBLR22016-1-DLA	



Netsurion. EventTracker[®]

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

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.

ADVAN	CED SEARCH	BASIC SEARCH			
CROUPS	Sites 2019_CP Groups ALL A B C Group search Group search All Groups All Groups All Groups Group Search	To DEEGHOOL Q	< tal: 151	Selected Items 2019_CP (1) 48Tech	Collapse all Clear



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.

Duration: Oct 09 05:47:54 AM - Oct 09 06:47:54 AM
Search criteria: event_group_name: ("48Tech")
Hide Lucene query
Lucene query: event_group_name: ("48Tech")

Figure 8



1.3 All Groups Selection search

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.

ADVAN	ICED SEARCH	BASIC SEARCH			
AVAILABLE SYSTEMS SELECTED ITEMS	Sites ETTVMBLR22C Groups ALL D E G Group search. Group search. All Group B All Group B GROUP1 G GROUP1	116-1 1 	< Total: 34	Selected Items Collapse all Cl Collapse all Cl Collapse all Cl Cl Collapse all Cl Cl Cl Cl Cl Cl Cl Cl Cl Cl	lear

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.
- 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.







- 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

- 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.



<	Sites	Available Systems	Selected Items Collapse all Clear
GROUPS	2019_CP[172.28.9.138]		
Ē	Groups Total: 151	ALL A B C D E F G H I J K L	4 🌐 2019_CP[172.28.9.138] (151)
AVAILABLE SYSTEMS		Search Q	⊿ 📲 48Tech (4)
		Group: All Groups (Total: 1 000)	48Tech-DC1
ITEMS	Group search Q Q		48Tech-Exchstv1
	💾 All Groups	48Tech	
		48Tech-DC1	48Tech-Sqlsvr1
			48Tech-Wrks1
	∎¶∎ 5Ktech	48 lech-Exchsrv1	▲ 📲 5Ktech (4)
	A2B	48Tech- Sqlsvr1	5Ktech-DC1
		48Tech-Wrks1	5Ktech-Evchsp/1
	∎"∎ Ablenet	5Ktech	
	_		5Ktech-Salsvr1

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.

ICED SEARCH	BASIC SEARCH				Netsurion EventTrac	cker®
Selected Item	Collapse all Clear	Search in archives			Export Import I Clear all Saved searches	Search
▲	BLR22016-1 (33)	Enter lucene query				(i)
-1					() L	Last 1 hr
📲 Default	t					
GROUF	P1	Custom criteria				
GROUF	P10					
GROUF	P11	$\overline{\nabla}$				۲
GROUF	P12 P13	Search in	Operator	Search for		
🖷 GROUF	P14	Choose	✓ Choose	Search for		(i)
GROUP	P15					0
🖷 GROUP	P16					
	Selected Item Selected Item Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison	ACED SEARCH BASIC SEARCH Selected Items Collapse all Clear Image: Selected Items Collapse all Image: Selected Items Selected Items Image: Selecte	Selected Items Collapse all Clear Image: Search in archives Enter lucene query Image: Search in archives Image: Search in archives Image: Searc	Selected Items Collapse all Clear Image: Selected Items Collapse all Enter lucene query Image: Selected Items Custom criteria Image: Selected Items Search in Image: Selected Items Custom criteria Image: Selected Items Search in Image: Selected Items Custom criteria Image: Selected Items Search in Image: Selected Items Choose Image: Selected Items Choose Image: Selected Items Choose	Selected Items Collapse all Clear Image: Selected Items Clear Enter lucene query Image: Selected Items Custom criteria Custom criteria Image: Selected Items Search in Operator Image: Selected Items Search in Operator Image: Search In Operator Search for Image: Search In Choose Search for Image: Search In Choose Search for	Selected Items Collapse all Clear all Saved searches Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import Import





Import page opens		
Import		
	🖆 Browse Upload	Close

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.

>	Sites	🗁 Browse Upload	nport	Close
GROUPS	ETTVMBLR22016-1	Available Searches		
	Groups Total: 34	◯ Elastic ● Archive		
SYSTEMS		Select All		
<u>_</u>		138_48_2weeks		
ITEMS	Group search Q			
	All Groups			
	n 1			
	📲 Default			
	- EventTracker			
	GROUP1			
		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.

		\times
This site says		
Search criteria imported successf	ully	
	ОК	





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

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





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 \oplus 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.

e Event Tracker :: Reports - Internet Explorer	
Reports Wizard - Selection	
Select Category/Reports to Configure Report Type: On Demand Queued Scheduled Defined	Cancel Next >
Security Operations Compliance Flex reports Alphabetical Favorites	^
Image: Stream of the stream	
Alerts Add to favorites	

Figure 17



EventTracker opens the Reports Wizard.

Welcome : EventTracker :: Reports Wiza	nd - Internet Explorer	
Report Wizard		
Operations > *All error events		Cancel Next >
Welcome to Reports wizard	This wizard is designed to simplify the report generation and scheduling process by guiding you through a set of steps. You select the report type, the systems, the time period and options and the data filters (if any). Reports can be generated in PDF formats. After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.	



- 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.



rt Wizar	d								
ons > *All er	rror events								
system(s) o	or group(s) for report *All err	or events							
Systems	stems 🗌 View both 🗹	Realtime 🗌	File Transfe	r					
× ۵۵	Sites		<	Available Systems		<	Selected Items	Collapse all	Clear
GROUPS	2019_CP		*	ALLCE		4 @ 2019_CP (1)			
AVAILABLE	Groups		Total: 10	Search	Q	Q	▲ o ⁿ o EventTracker (1)	
SELECTED ITEMS	ALL A B C D B F	LL A B C D 📴 F G H I J L M Group search			Group: EventTracker (Total: 2)			ETTVMBLR22019-1	
	and All Groups			Continnum1-syslog					
				ETTVMBLR22019-1					
	=== ENSten-AIMS		-						
	ENStep-FBG		_						
	B ENStep-Force		1						
	a ⁿ a ETA		-i						
	∎ ⁿ ∎ Etihad		1						
	- EventTracker								



- 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).



Report Wizard Cancel < Back Next >
Cancel < Back Next >
Select report duration on which period the report needs to be generated.
INTERVAI Select interval
Last 1 Day 🗸
O Select date range From 11/15/2017 Ⅲ 05:37:30 PM To 11/15/2017 Ⅲ 06:37:30 PM
Limit to time range
More options
Format option Extended Summary Export type Quick View (not saved on hard disk) Chart type Pie Sort by Computer

Figure 20

- 18 Click Next>>.
- 19 Enter the appropriate Refine and Filter details.

Tracker :: Reports Wizard - Internet Explorer		_
ort Wizard		
rations > *All error events	Cano	el < Back Next >
u can narrow down the criteria by explicitly specifying the details		••••
Refine Match for User(s)	Filter (Exclude) Filter User(s)	
Match for specific information	Filter specific information	
Filter Event Id(s)		
Filter Event Source(s) Notes		
The 'Refine' option is inclusive. Results are limited to matching entries. The 'Filter' option is exclusive. Results do not include matching entries. Any combination of Refine and Filter may be used simultaneously. Examples: 1) Match for User(s): Enter usernames separated by (for OR)		<



- 20 Click Next>>.
- 21 Enter the relevant Title, Header, Footer, and Description data.

entTracker :: Reports Wizard - Internet Explorer			
ort Wizard			
erations > *All er	rror events		Cancel < Back Nex
rovide the title a	nd description for the report All error events		•••••
Title	All error events	0	
Header	EventTracker		
Footer	Reports		
Description			

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.

EventTracker :: Reports Wizard - Internet Explorer	_ 🗆 🗙
Report Wizard	
Title: All error events Operations > "All error events	ancel < Back Next>
Review cost details and configure the publishing options.	•••••
Disk cost analysis for the report	
Estimated time for report completion:00:43:00(HH:MM:SS)	
Number of cab(s) to be processed: 1275 Available diak space: 280 GB Required disk space: 50 MB	
Add to queue(background processing)	
Enable publishing option	
Deliver results via E-mail	
Notify results via E-mail	
To E-mail [Use comma() to separate multiple e-mail recipients]	

Netsurion. EventTracker

24 Click Next>>.

Completing Report Configuration Wizard opens.

e: All error events		Cancel < Back Generate rep
erations > *All error events		
eview all the configuration details	before submitting the report request.	••••••
	Completing Report Configuration Wizard	
	Report title: All error events Description:	^
	Report type: Extended Summary	
	Report header: EventTracker Report footer: Reports	
	Duration: From 11/14/2017 6:38:26 PM To 11/15/2017 6:38:26 PM	
	Categories: "All error events	
: <u></u> ••	- System Groups:	
°, ö.	*Šite:R1S5-VM3 Groups:Default	
	*Site:R1S5-VM3	~
Override indexer		

Figure 24

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

