

How To-Configure Alerts with Active WatchList

EventTracker Enterprise

Abstract

This update will allow the user(s) to configure alerts by extracting the values from the event and compare it against the Active Watch List.

Who should read this document?

Customers who use v 8.2 Build 14.

Why to apply this update?

If the admin maintains a local black/white list data, he/she can configure the alerts and compare it with Active Watch list, based on which the alert will be triggered.

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

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

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Process to be followed after applying the update

- Go to **Admin-> Alerts**. In the Alert Management page, click the Add Alert icon.
- Enter the Alert name and the other required fields.

NOTE: Follow the steps in the document “**BDS Alert Configuration**” for extracting values.

In the below example, we have taken the extraction method as “**Regular Expression**” for Alert “**EventTracker: Critical Potential Breach from low reputation IP**”.

- Configure the alert using Event level configuration or Alert level configuration.

The screenshot displays the 'ALERT CONFIGURATION' page in the EventTracker interface. The top navigation bar includes 'Dashboard', 'Incidents', 'Behavior', 'Search', 'Reports', 'My EventTracker', 'Change Audit', and 'Config Assessment'. The main content area has a breadcrumb trail: '< Back | Event Details | Event Filter | Custom | Systems | Actions | Next >'. A gear icon in the top right corner is highlighted with a red box. Below the breadcrumb, the 'ALERT CONFIGURATION' section contains several input fields and dropdown menus: 'Alert name' (EventTracker: Critical potential breach from), 'Threat level' (Undefined), 'Threshold level' (Medium), 'Applies to' (empty), 'Alert version' (empty), and 'Show in' (None). A table below the configuration fields has a red plus icon to its left. The table has columns: LOG TYPE, EVENT TYPE, CATEGORY, EVENT ID, SOURCE, USER, MATCH IN DESCRIPTION, and DESCRIPTION EXCEPTION. A single row is visible with values: 0, 8010, EventTracker. A gear icon in the rightmost column of this row is also highlighted with a red box. At the bottom right of the table area are 'FINISH' and 'CANCEL' buttons. The footer includes the EventTracker logo, 'Server Time: Apr 17 01:00:30 PM', 'Response: 0.35 secs', and '© 1999 - 2017 EventTracker'.

Figure 1

- Select the **Token Type** as Regular Expression.
- Enter the Sample Description, Regular Expression and a Short Description.

Here we have extracted the values “**ProcessName**” and “**RemoteHostName**”.

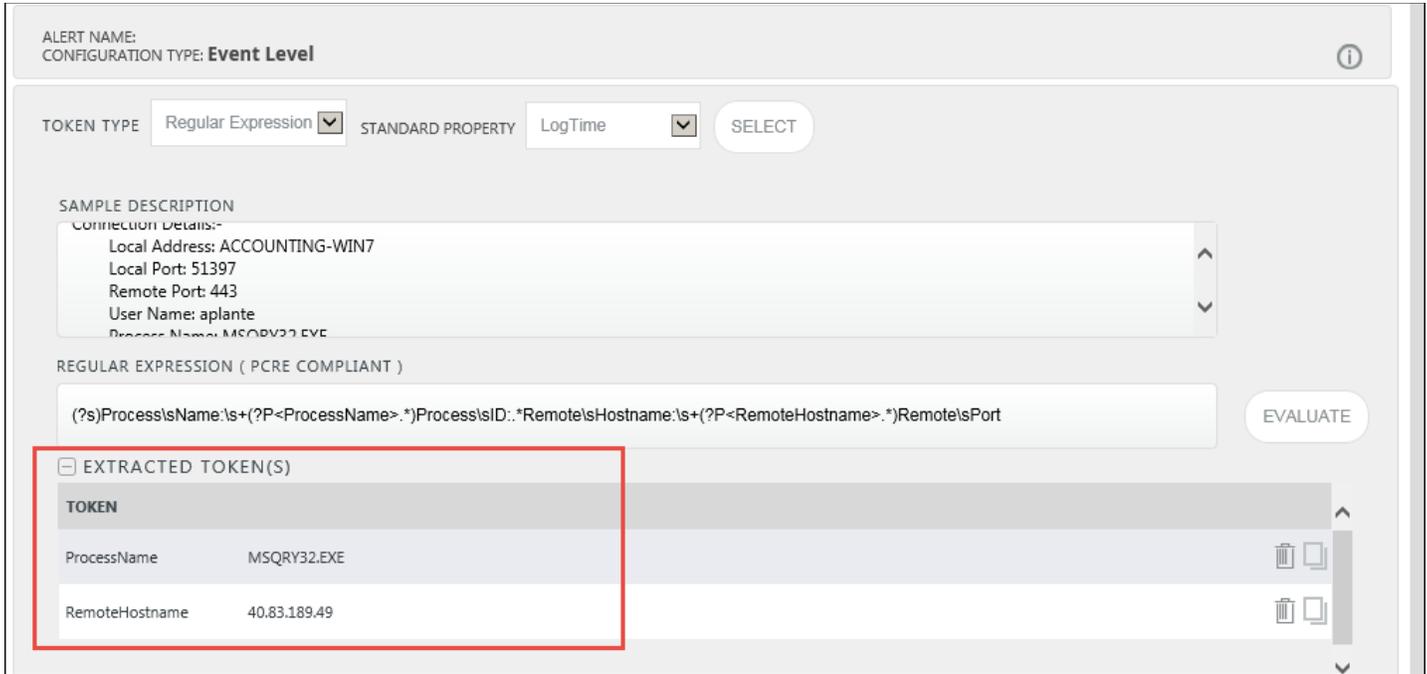


Figure 2

The extracted values will be displayed in the Watch List Lookup pane.

- Click the lookup icon  to add data class and watch list.

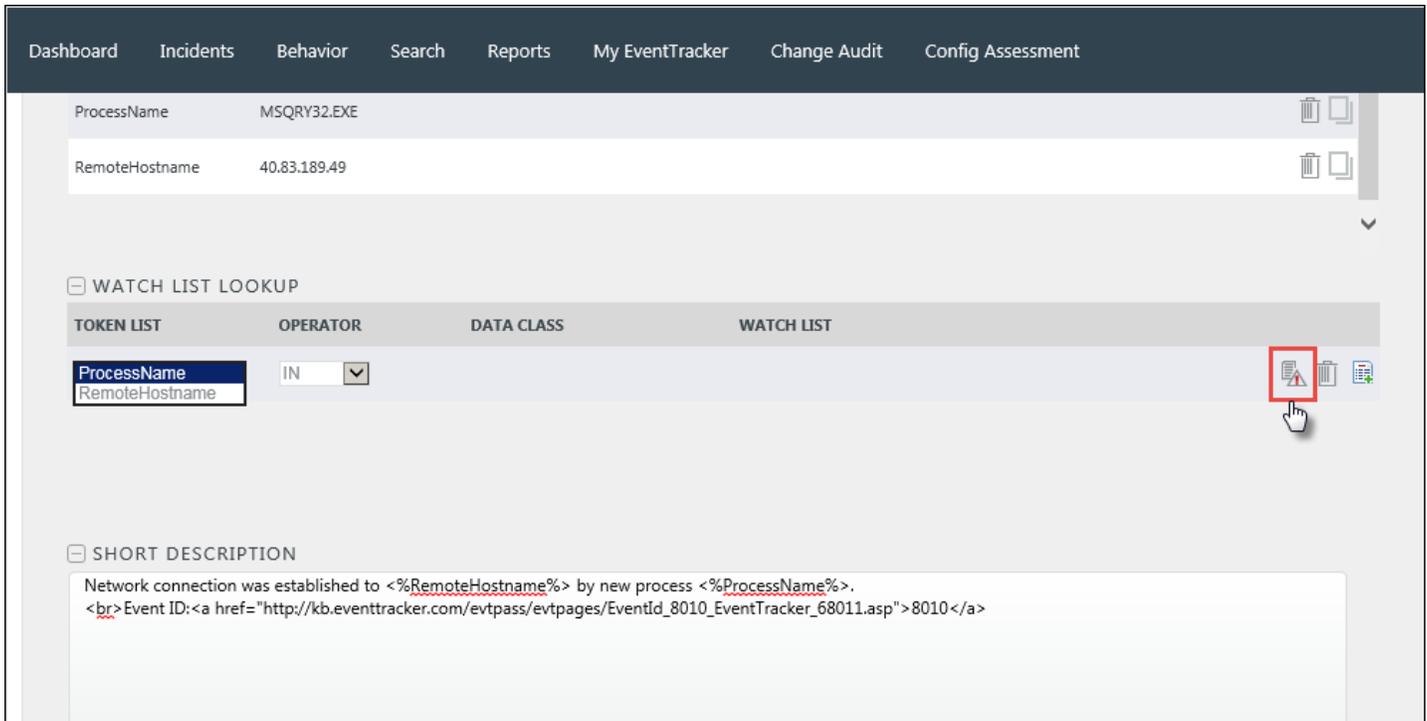


Figure 3

From the Watch List tree, select the class or group to add to the watch list.

Figure 4

In the below example, for “**ProcessName**” we have added the Group “**KnownExeWhitelist**”. It will display the Data Class and the watch list which gets added.



Figure 5

The user can also select Operator as IN or NOT IN as per the user preference.



Figure 6

To add multiple lookup for the extracted token, click the clone icon , to duplicate the record. Now the user can change the duplicated records as per requirement.

For example, we have taken the extracted token “**RemoteHostName**” and added the watch list “**EmergingThreatsBlockedIPList**” by selecting it from the watch list tree.

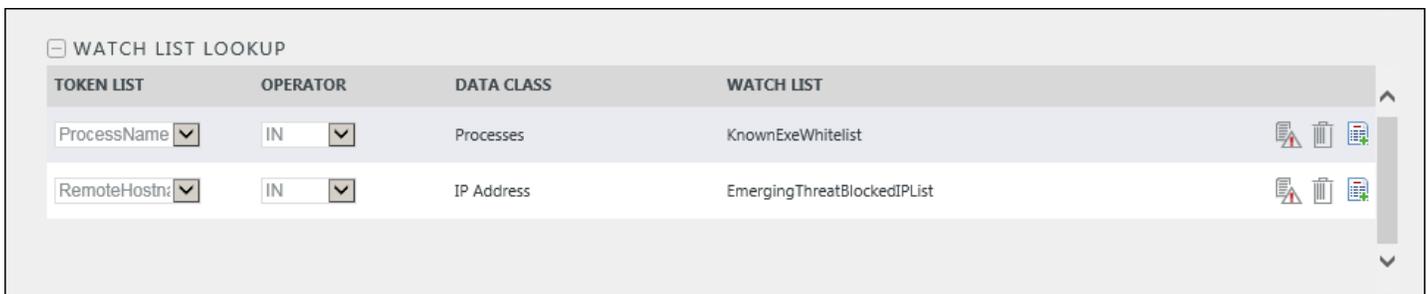


Figure 7

- To save the configuration, click **Save** and **Finish**.