EventTracker

Actionable Security Intelligence

How To-Configure Alerts with Active WatchList

EventTracker Enterprise

Publication Date: April 17, 2017

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.

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.

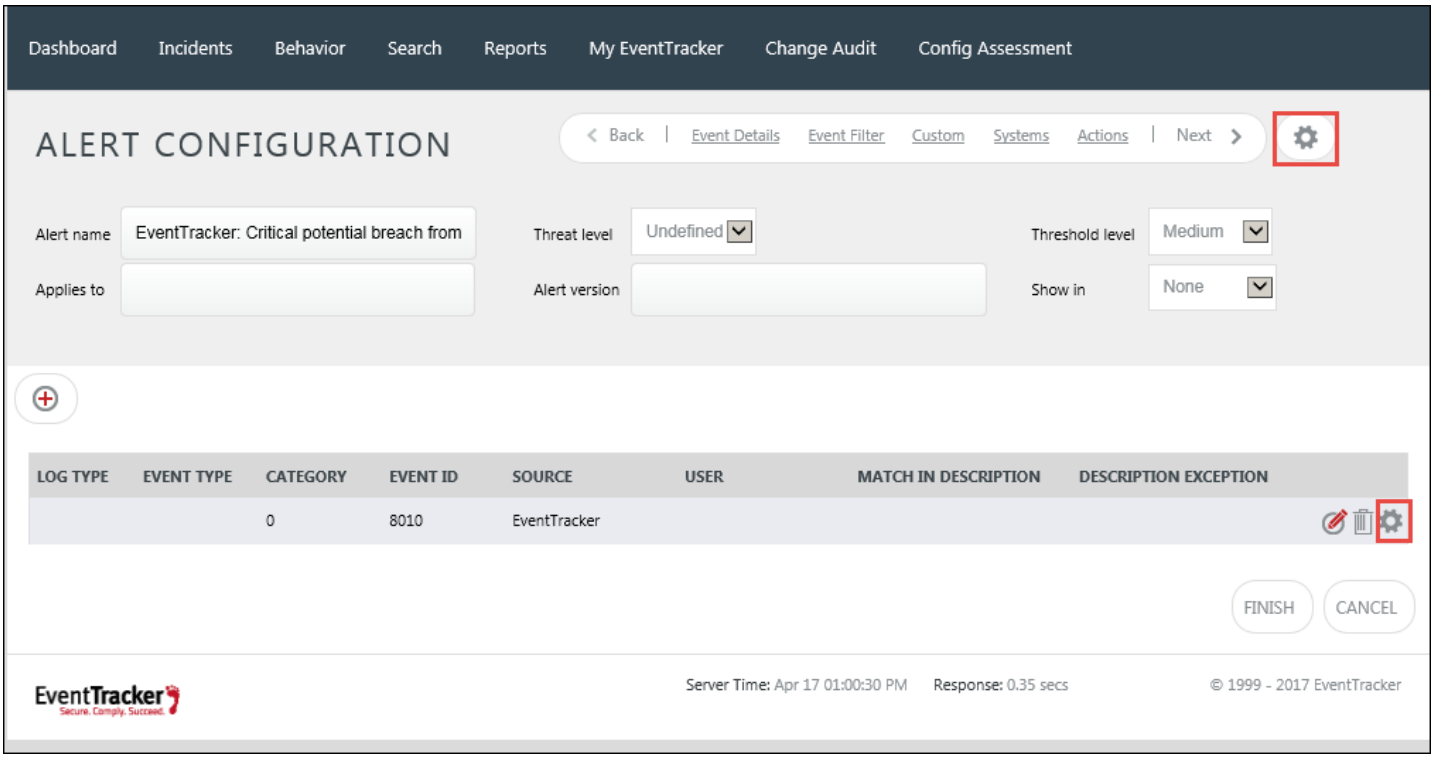

Figure 1

- 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**".

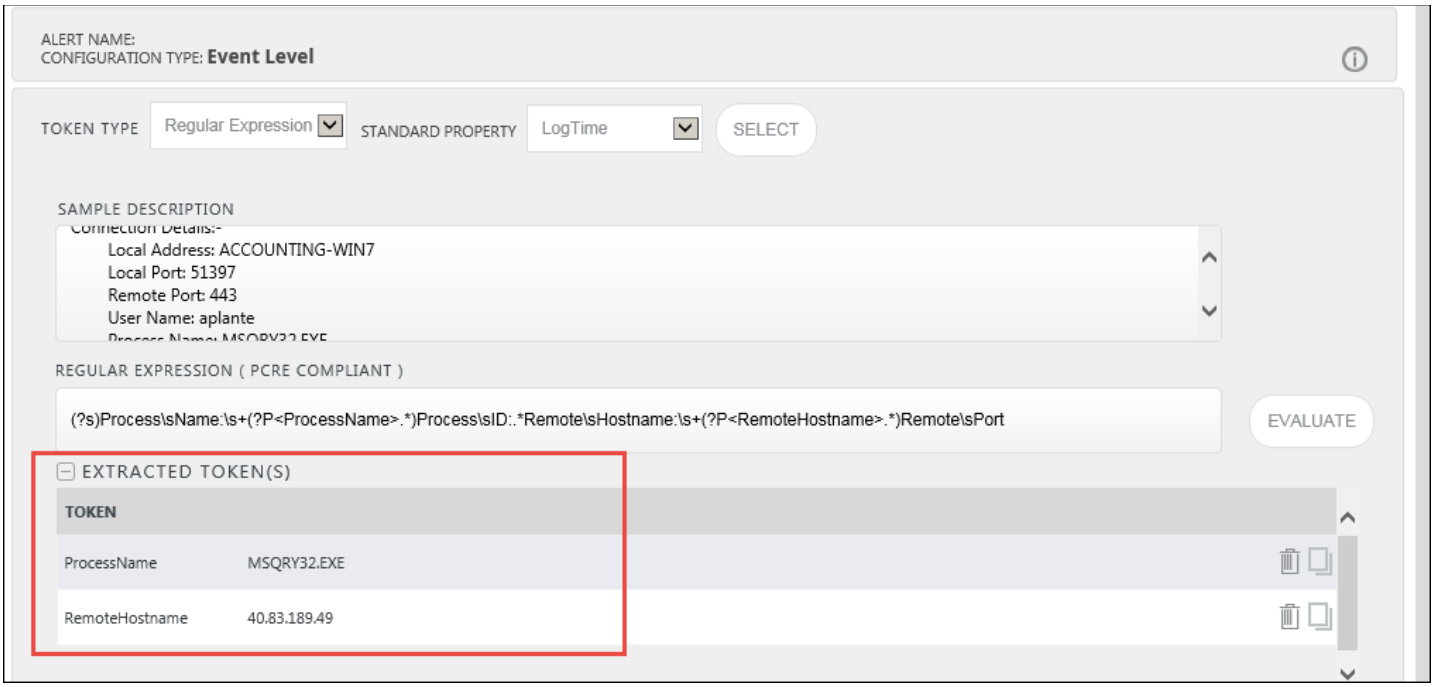

Figure 2

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

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

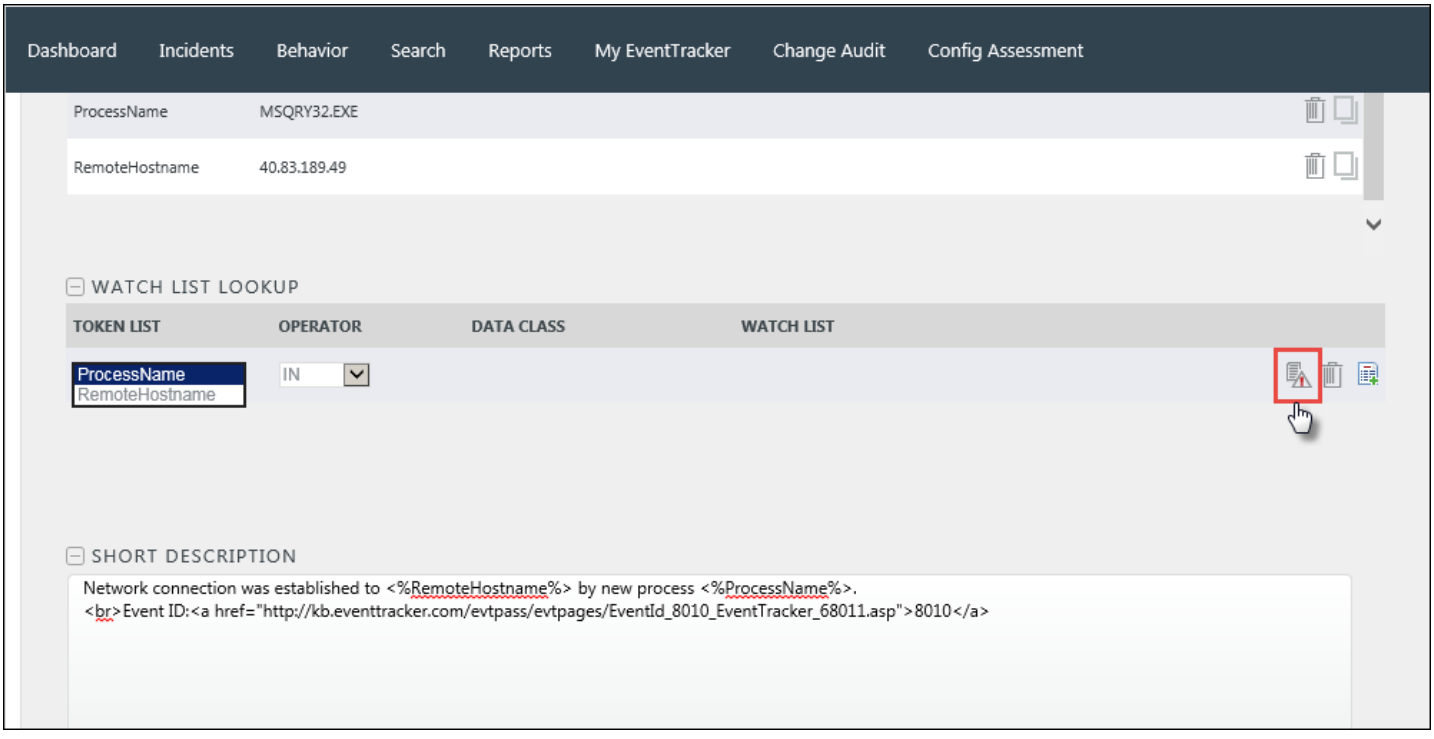

Figure 3

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

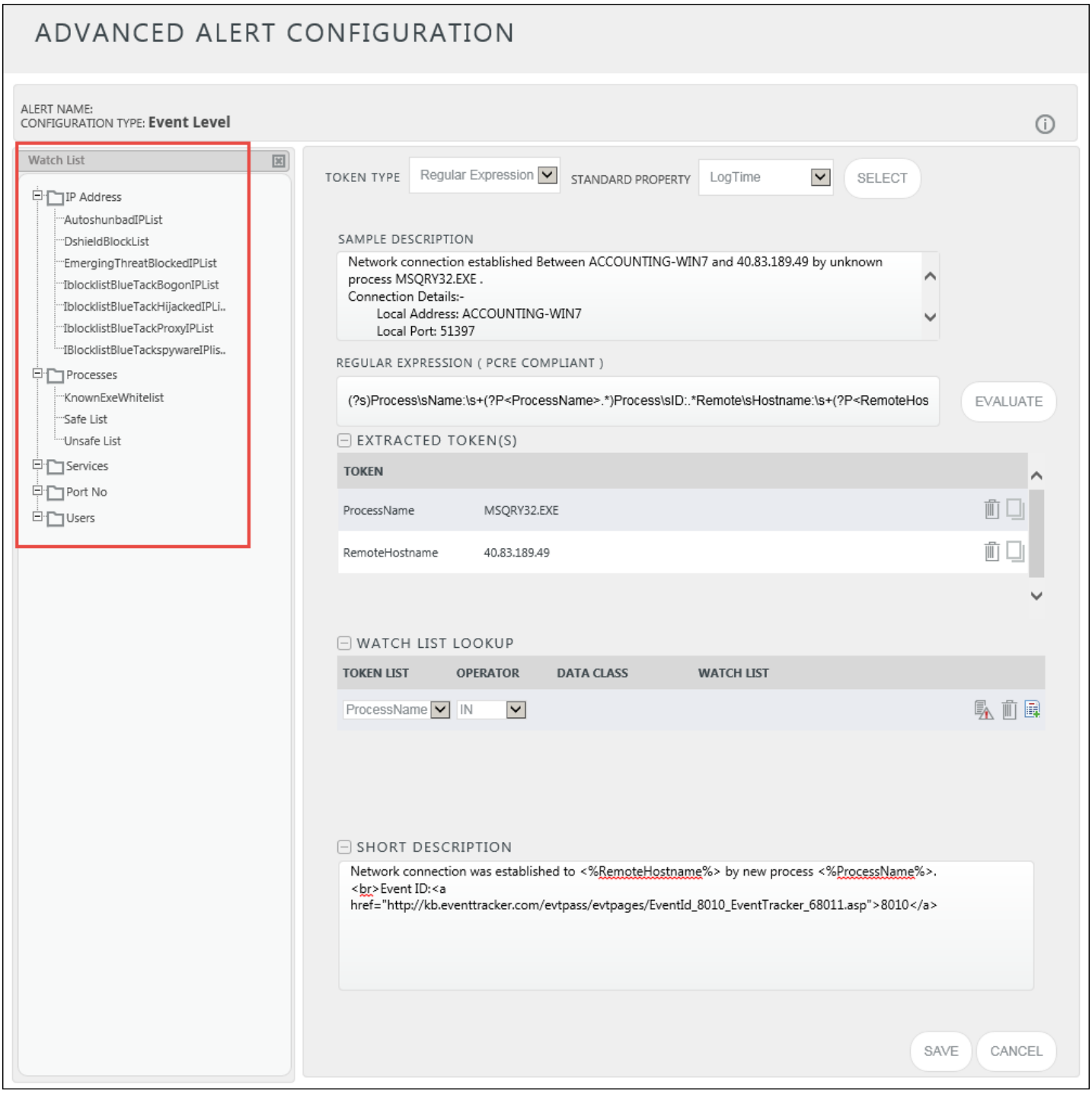

Figure 4

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**.