Alert Configuration

Contents

Introduction

An Alert is defined as being a set conditions along with a set of actions that are executed when the conditions are met. This tutorial shows how to configure such alerts by creating a set of conditions or filters and by configuring built-in executors such as *send mail* or *append to file.* The tutorial also shows how to create your own custom executors.

Get started with filters

1. Launch the PI Engine
2. Click on the configuration dashboard icon
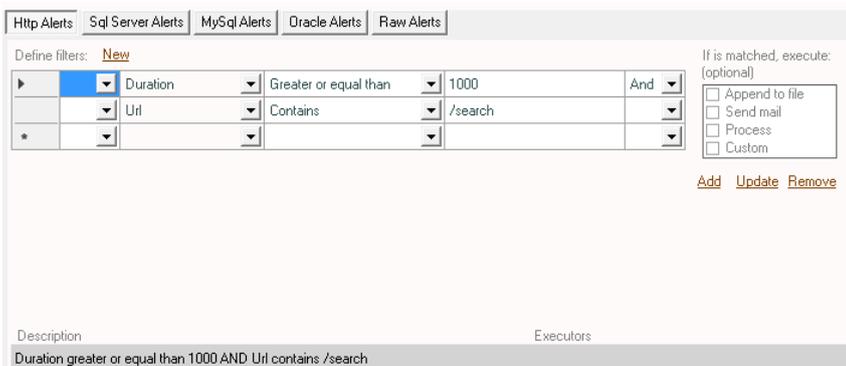3. All the filtering configuration is found here:

4. Select the desired tab in order to create your filters.
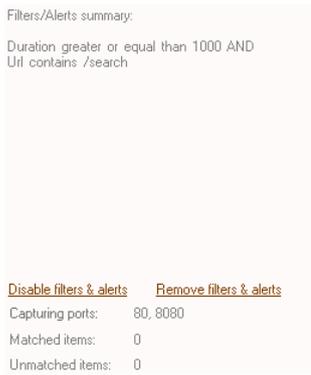5. Create your filter by setting each dropdown and click on "*Add*". This is an example of filter:

6. To update an existing filter, you have to select it from below grid where you have the filter description, then modify accordingly the dropdowns and click on "Update".
7. To remove a filter, you have to select it from below grid where you have the filter description and then click on "Remove"
8. Once you have finished creating your filters, you have to save the configuration dashboard.
9. In this example, a filter has been set for HTTP captures. You can see a filter summary on the "HTTP traffic" tab page:

```
Filters/Alerts summary:

Duration greater or equal than 1000 AND
Url contains /search




Disable filters & alerts    Remove filters & alerts
Capturing ports:      80, 8080
Matched items:        0
Unmatched items:      0
```

10. When you start capturing HTTP traffic, filters will be applied. You will see only the data that matches your filter.
11. The "Matched items" and "Unmatched items" are indicators that show the number of matched and unmatched data during the capture session. You can disable filters by clicking on the "*Disable filters & alerts*". This will not delete the filter. If you click on the "*Remove filters & alerts*" this will delete them.
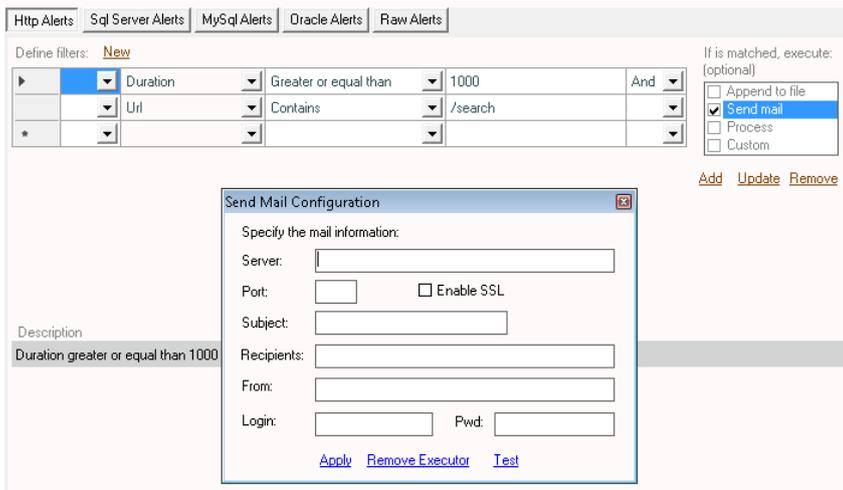
Creating an Alert

Alert creation is a two steps process. The first step is to create a filter (also called condition). Then you have to specify the action that has to be executed once the filter or condition is met.

1. Create a filter as per the above steps:
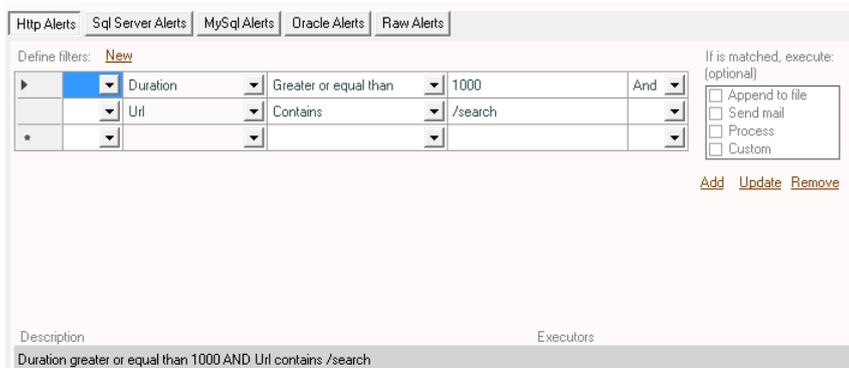
2. On the right side, check the desired action. The first three actions are built-in:
   a. Append to file
      This will write to a file all requests that match your filters
   b. Send mail
      This will send an email for <u>each request</u> that matches your filter
   c. Process
      This will execute the specified local process with the specified arguments
   d. Custom
      This will execute your own custom executor. Please refer to the end of this document on how to implement your own executor.

3. You can setup more than one executors. Once your are done, click on "Add" or "Update" if you are modifying an existing entry:
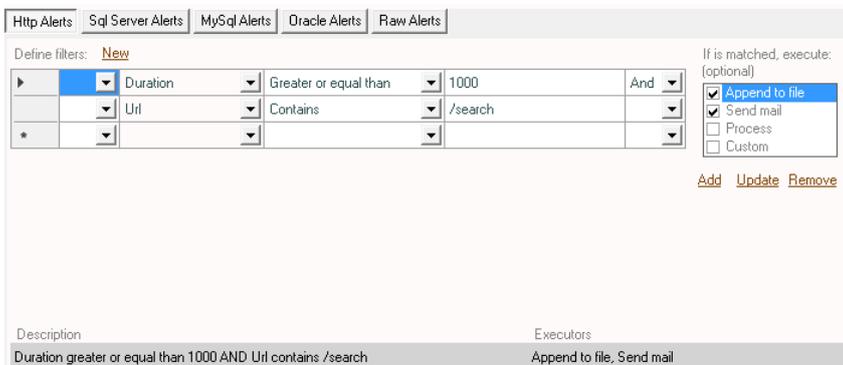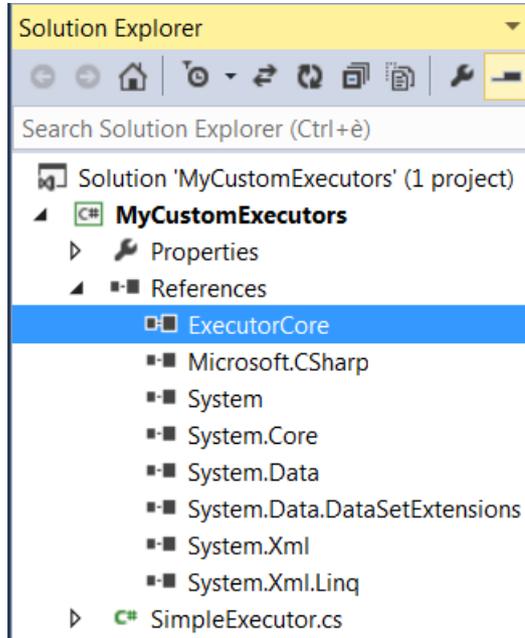

Create a custom Executor

As mentionned above, an alert is defined as being a set of filters or conditions along with a set of executors. Above you can see the built-in executors. If you want to create your executor, those are the steps to follow:

1. Use Visual Studio to create a Class Library project with .Net 4.0
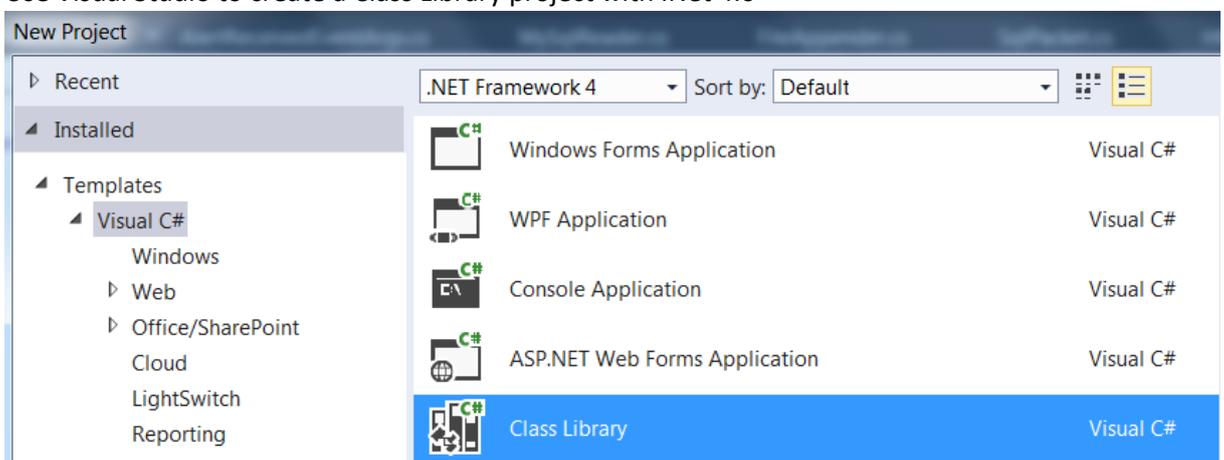
You can use C#.Net of VB.Net with Framework 4.0. You cannot use version 4.5 or higher so far (this will change with the future compilations of PI Engine)

2. Add a reference to the *ExecutorCore.dll* file which is located in the installation directory of PI Engine:

Solution Explorer

Search Solution Explorer (Ctrl+è)

- Solution 'MyCustomExecutors' (1 project)
  - C# **MyCustomExecutors**
    - Properties
    - References
      - ExecutorCore
      - Microsoft.CSharp
      - System
      - System.Core
      - System.Data
      - System.Data.DataSetExtensions
      - System.Xml
      - System.Xml.Linq
    - C# SimpleExecutor.cs

3. Create a class that inherits from Alerts.Actions.ActionItem class and implement the Execute method:

```csharp
using Alerts.Actions;
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Text;

namespace MyCustomExecutors
{
    public class SimpleExecutor : ActionItem
    {
        public override void Execute(Alerts.AlertReceivedEventArgs area)
        {
            //Do your custom code here.
            //You can use the AlertReceivedEventArgs to get all the captured data
        }
    }
}
```

4. Compile your project
5. Copy your DLL into the installation folder of PI Engine
6. In the configuration dashboard, select your filter and in the executors checkbox list, click on "*Custom*". This will open a popup where you can set your assembly and class information:
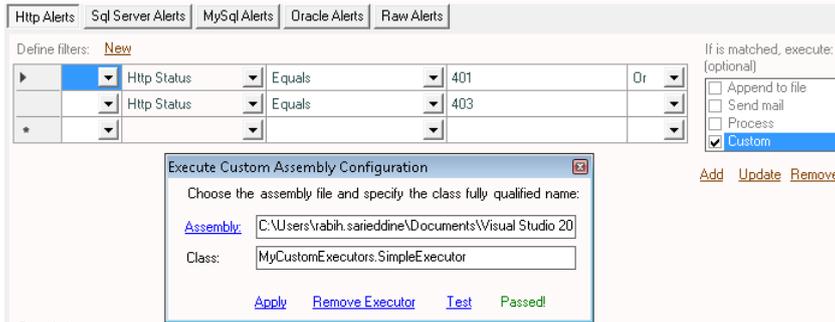
Click on the "*Test"* to check that your assembly and class are found and that your class inherits from *ActionItem.*

7. Click on *"Add"* to insert your alert or "Update" if you are updating an existing entry:
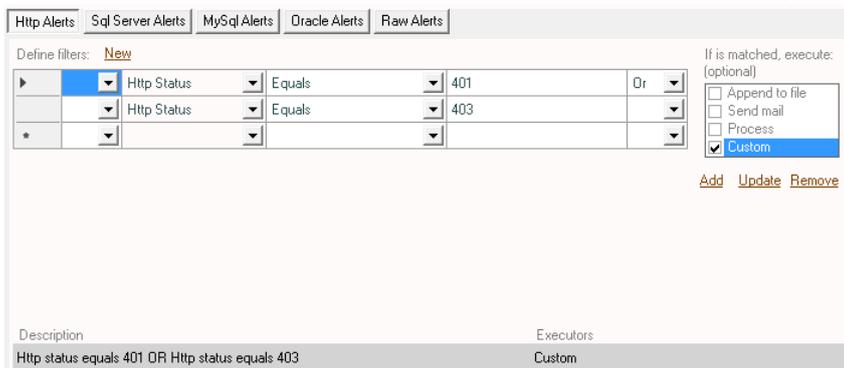
8. Save the configuration dashboard
9. When the captured data matches your filter then your custom class will be executed