Configure Critical Service Lookup

Publication Date: May 27, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

About this Guide:

This document helps EventTracker Admin to maintain the list of Non Critical service running on monitored windows systems in EventTracker List Group and get alerted when these critical services are stopped.

Scope:

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later and Windows Operating systems.

Audience:

EventTracker Administrators.

Table of Contents:

About this Guide: 1
Scope: 1
Audience: 1
Introduction 3
Pre-requisite 4
How it works? 5
Setting up Critical Service lookup: 6
Preparing Scripts for use as per your environment 6
Create group in List Management 6
Import Alert 7
Import Scheduled Reports: 10
Configuring Remedial Action for Critical service Alert 13
Verify Reports 16

Introduction

EventTracker Agent has service monitoring feature which generates an event when any of the services running on the system is observed 'stopped'. On windows operating system many service might be not that critical than the one which causes immediate application outage or problem. EventTracker List management feature can be used to maintain the list of known Non critical services and can be looked up when EventTracker Agent detects any service not running.

Pre-requisite

- EventTracker v7.x should be installed.
- Windows PowerShell 3.0 or later must be installed.
  To check the PowerShell version:
  - Launch Windows PowerShell as Administrator.
  - Run command $PSVersionTable.PSVersion
- Script Execution policy must be set to Unrestricted.
  To change PowerShell execution policy,
  - Launch Windows PowerShell as Administrator.
  - Run command 'Set-Execution Policy Unrestricted".
  - Make sure you do this for both x86 and x64 versions.
- EventTracker Agent must be configured to monitor service status on monitored systems.
  For this go to **EventTracker Control Panel**-
  - Click on EventTracker Agent Configuration.
  - Select the **Services** tab and enable the option **Services monitoring**.

How it works?

EventTracker launches Critical service lookup script when event id 3202 is generated. Script queries the EventTracker NonCriticalService list and checks whether service name extracted from description of event ID 3202 is part of part of it or not. If service name is not part of NonCriticalServices list then it generates event id 8003 is generated.

Setting up Critical Service lookup:

Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the Critical service lookup script pack.
- Save Critical service lookup script.zip (saved to d:\CriticalServiceLookupScript\folder in the example below).
- Extract .ps1 file to d:\CriticalServiceLookupScript\.
- Files in the package are shown below:

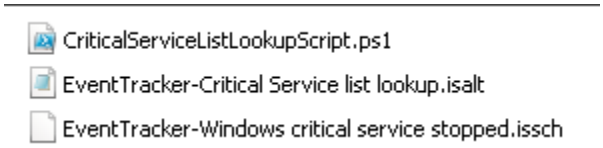


Figure 1

Create group in List Management

- Go to **Admin>List Management**.
- Click the add icon to create a new group.
- In the Class field, select Services from the dropdown list.
- Give the group name as '**Non Critical Services**".

Figure 2

- Click the **Save** button.

Now, add the Non critical services name under the group created, as shown in the figure below:

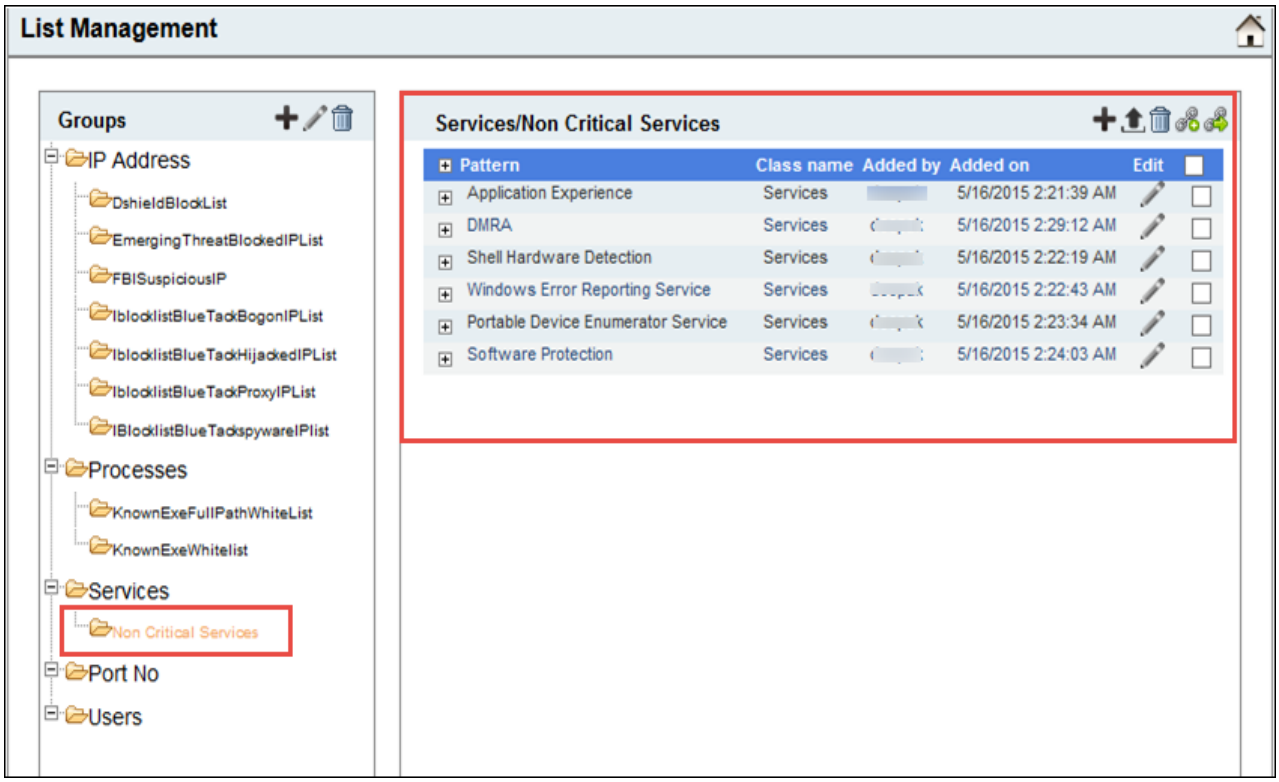


Figure 3

Import Alert

For importing the alert file **EventTracker-Critical Service list lookup.isalt,** select the **Alerts** Option.

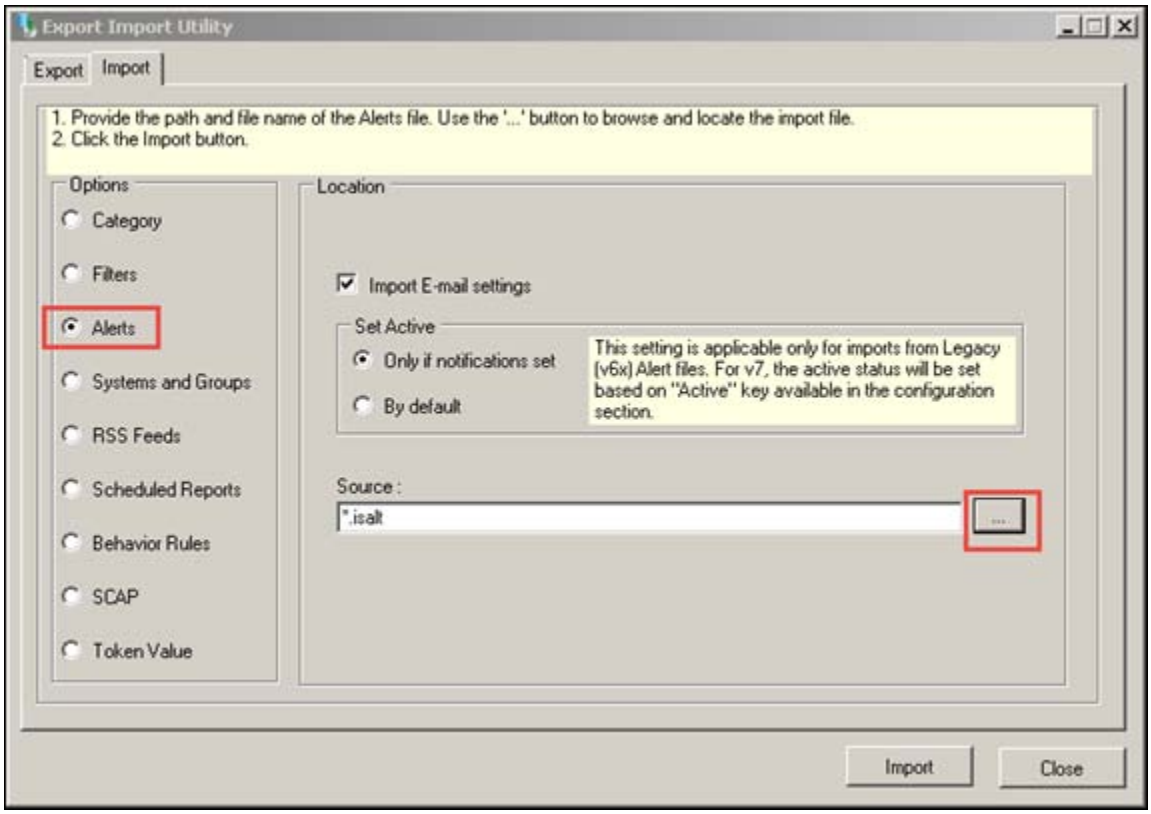


Figure: 4

- Provide the path name and file name of the Alert file.
- For this, click the icon  and browse the Alert File i.e**. EventTracker-Critical Service list lookup.isalt** from your system and click **Open.**

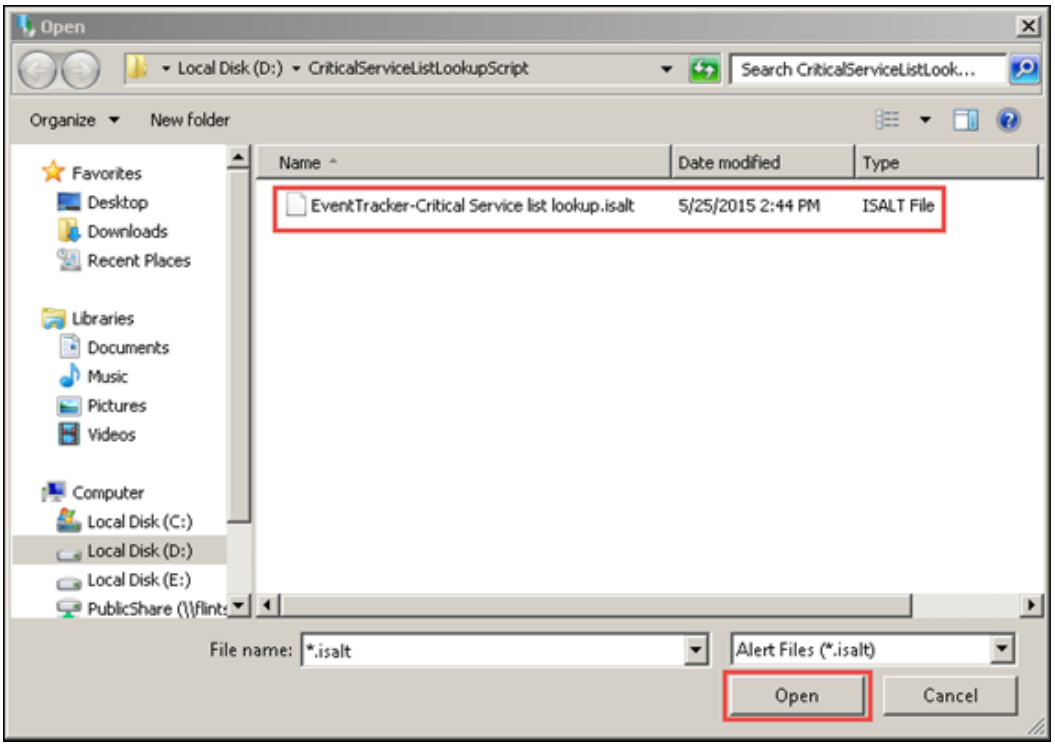


Figure: 5

- Now, click the **Import** button.

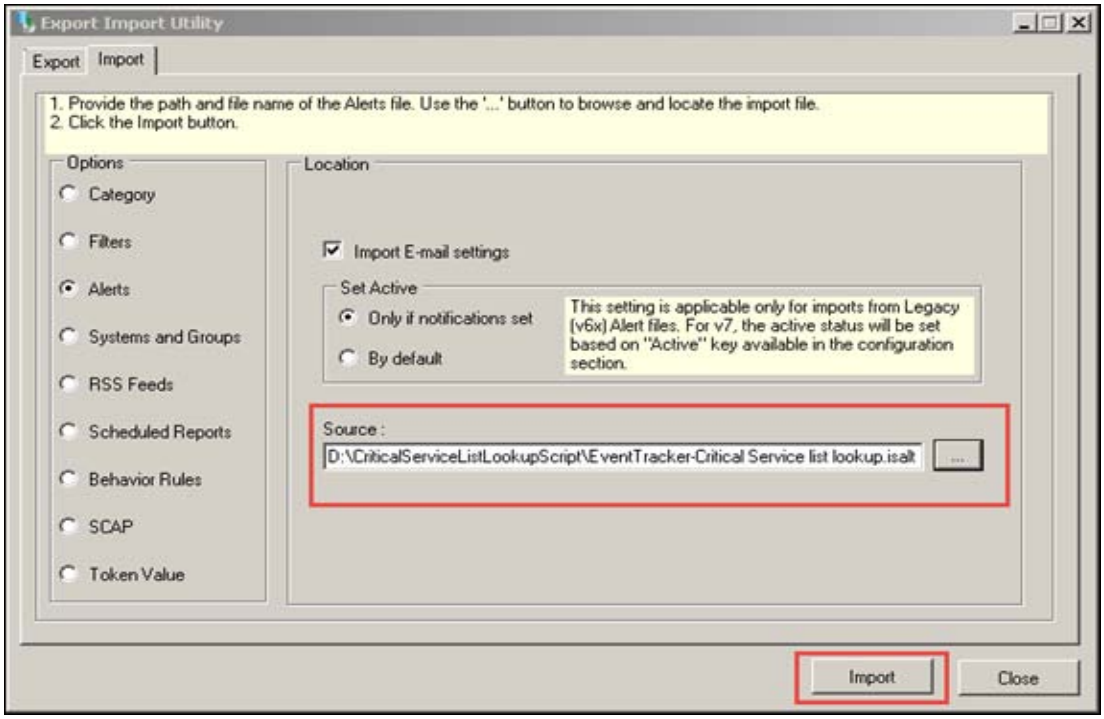


Figure: 6

The success message box of 'Selected alert configurations are imported 'will be displayed.

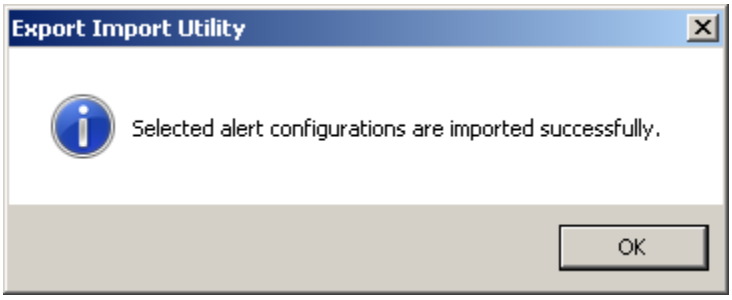


Figure 7

- Click **OK.**

Thus, the two alerts **EventTracker: Critical windows service not running** and **EventTracker: Service list lookup** gets successfully imported.

Import Scheduled Reports:

To Import Scheduled Reports,

- Select **Scheduled Report** from the Export Import Utility Window.

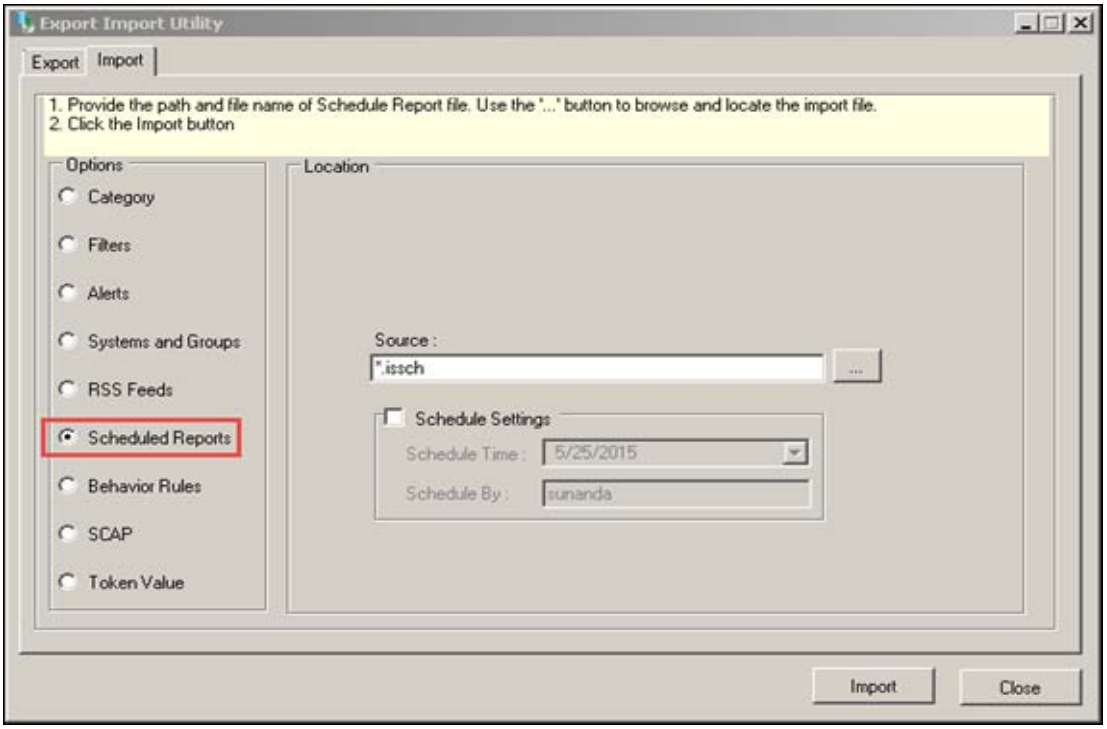


Figure: 8

- Browse the path and file name of the scheduled report file i.e. **EventTracker-Windows critical service stopped.issch**, by browsing the Report file from your system.

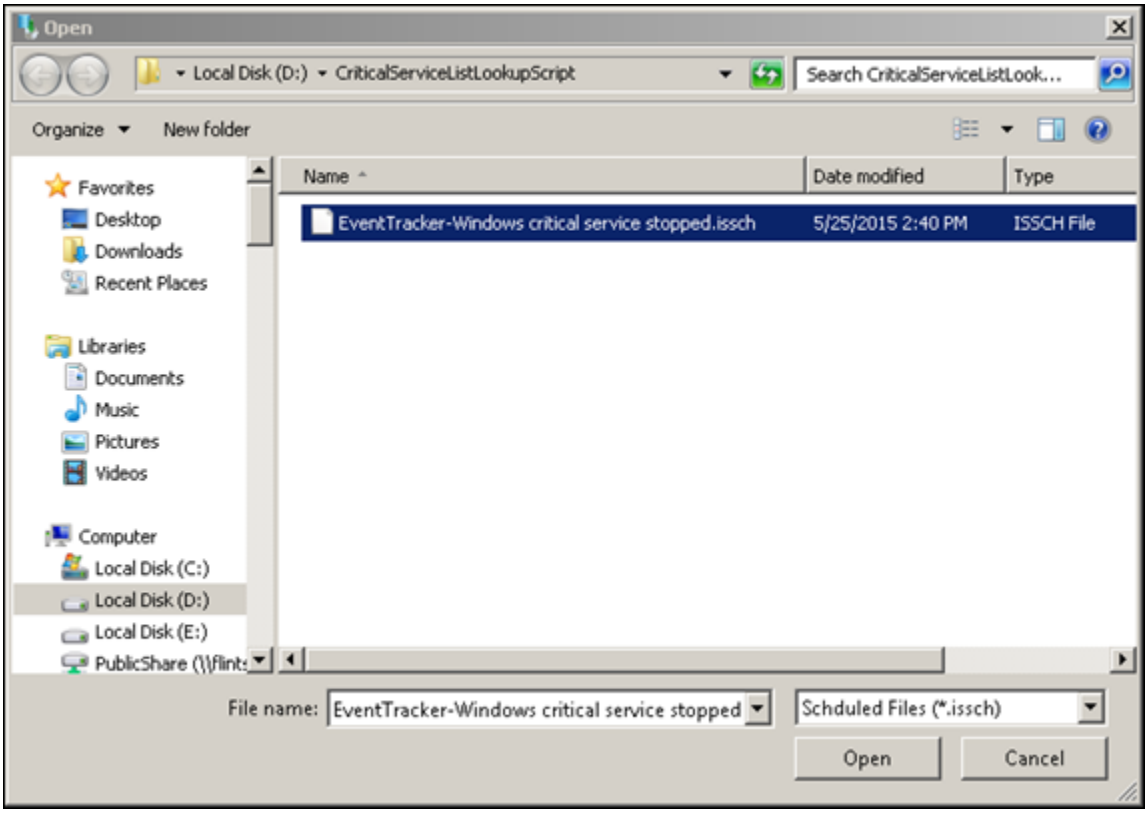


Figure: 9

- Open the Report file and click the **Import** button.

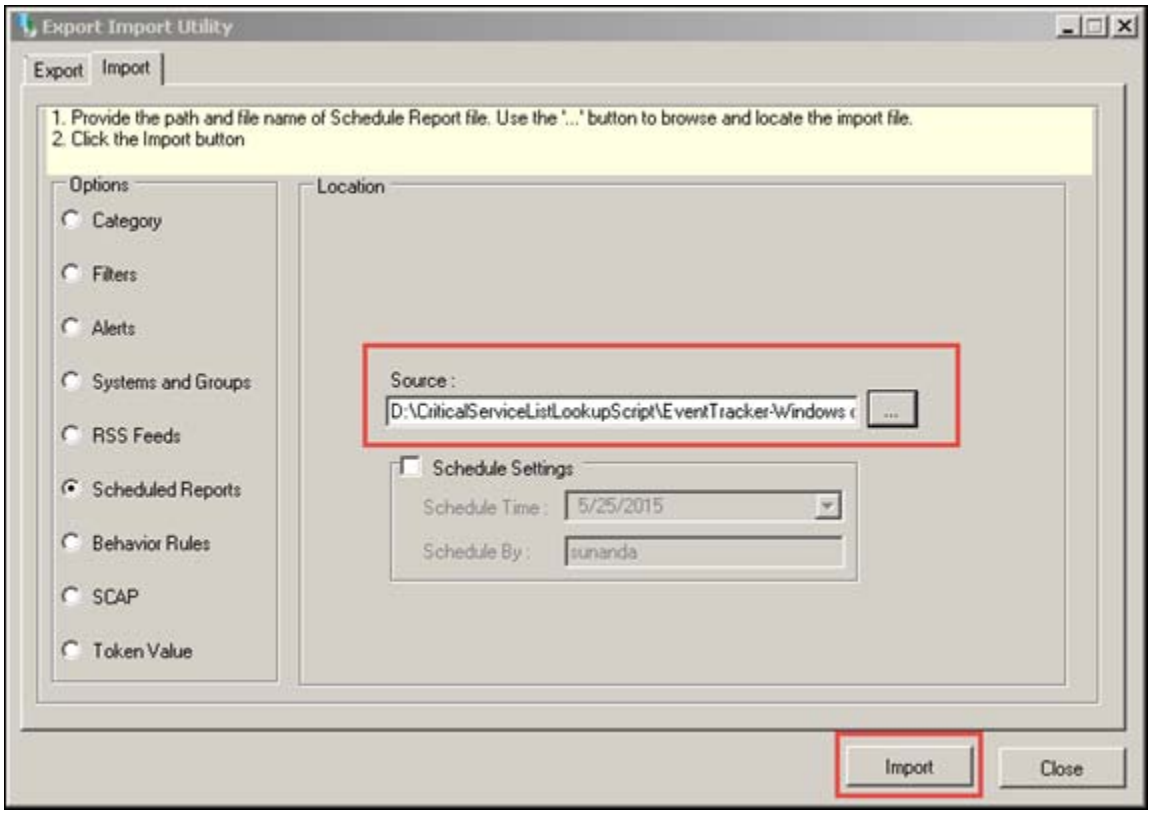
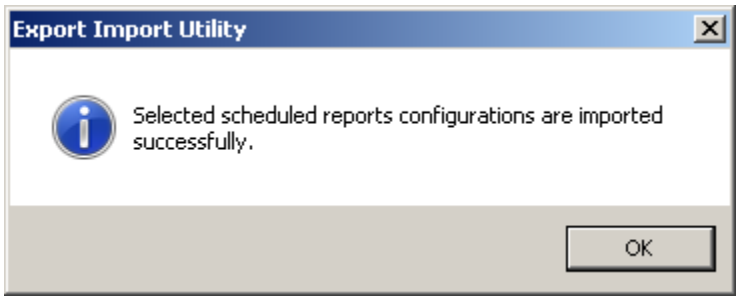


Figure: 10

The report file **EventTracker-Windows critical service stopped** will be successfully imported, with the below message:



Configuring Remedial Action for Critical service Alert

- Login to EventTracker Enterprise Web Console.
- Click **Admin** dropdown and click **Alerts**.

EventTracker displays the **Alert Management** page.

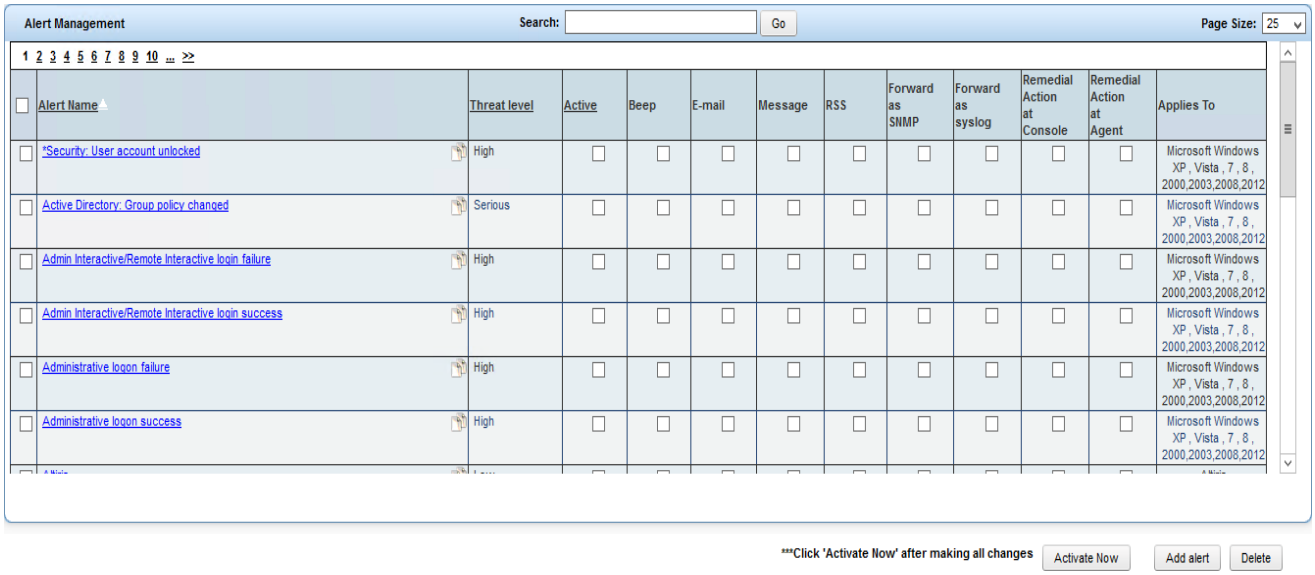


Figure: 11

- Enter the Alert Name i.e. **EventTracker: Service list lookup** in the Search box.
- Click the **Go** button.

The Alert will be displayed.

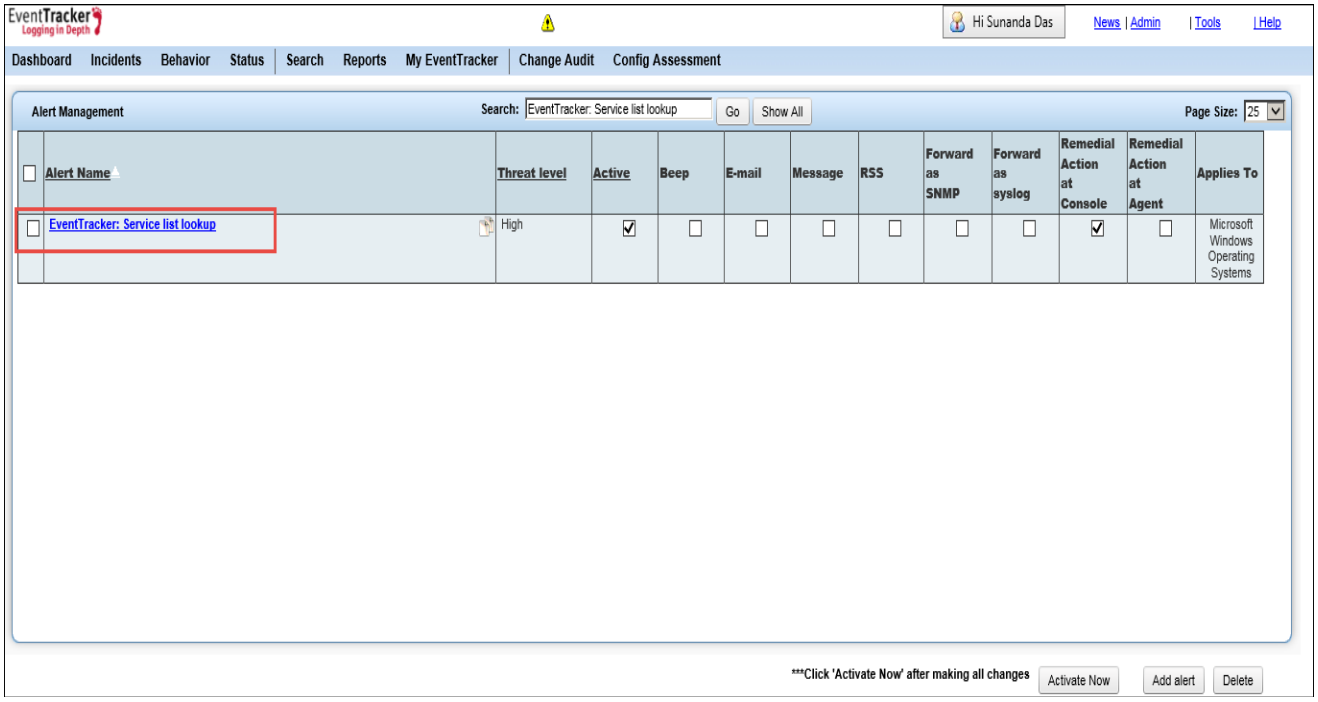


Figure: 12

- Click on the alert hyperlink to make changes in the Alert Configuration.
- Click the **System** hyperlink and select all the Windows system.

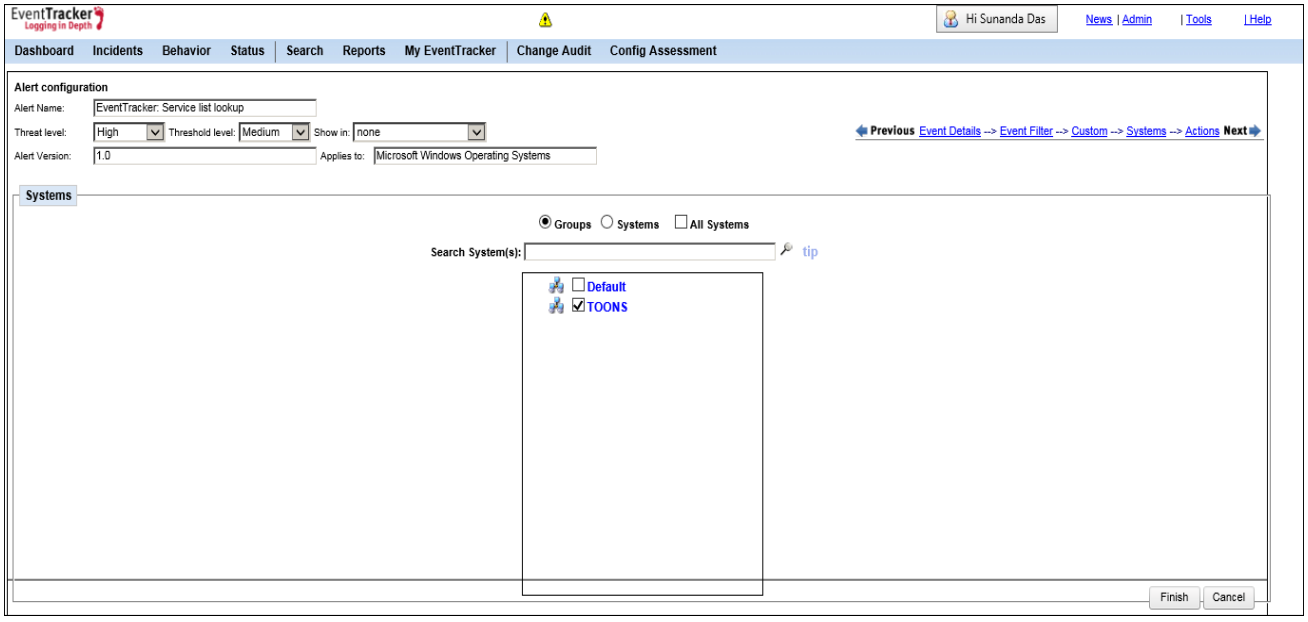


Figure: 13

For assigning Action based on the Alert, **EventTracker: Service list lookup:**

- Click the **Action** hyperlink and then click the **Console Remedial Action** option tab.
- Enter the file path to execute when an event occurs.

For example:

"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" -File "F:\Scripts\CriticalServiceListLookup\CriticalServiceListLookupScript.ps1"

NOTE: Please enter the install path where you have stored the script.

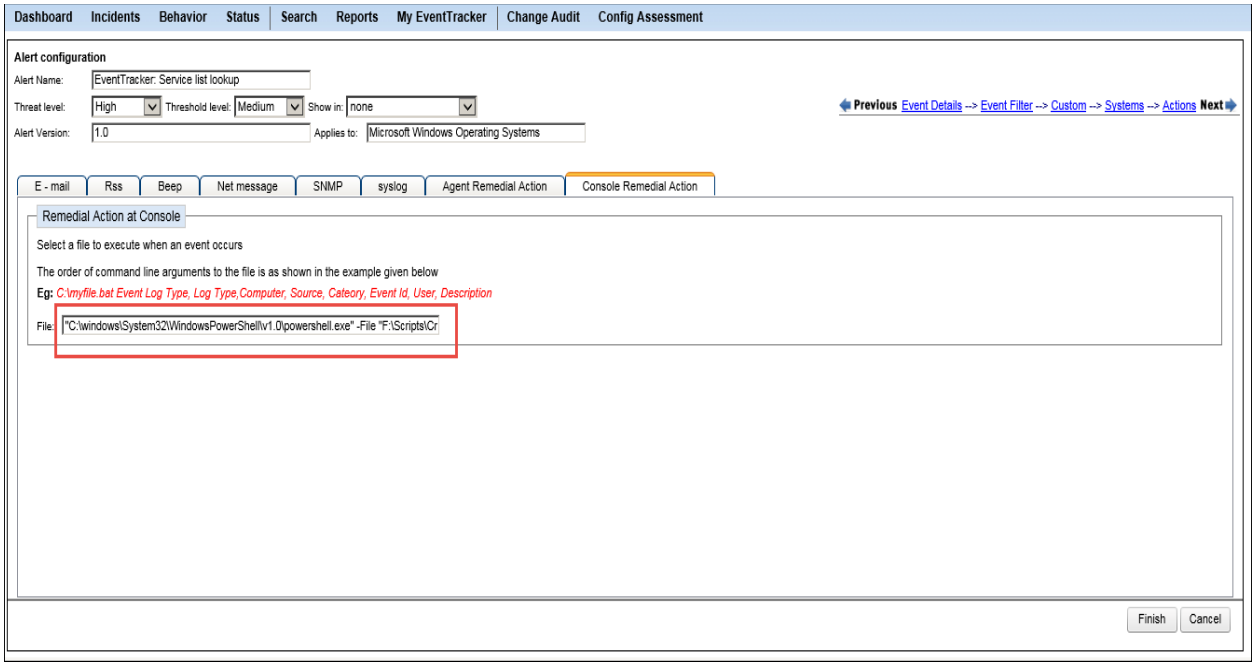


Figure: 14

- Click the **Finish** button.
- Now click the **Activate Now** button after confirming all the changes made and activate the Alerts.

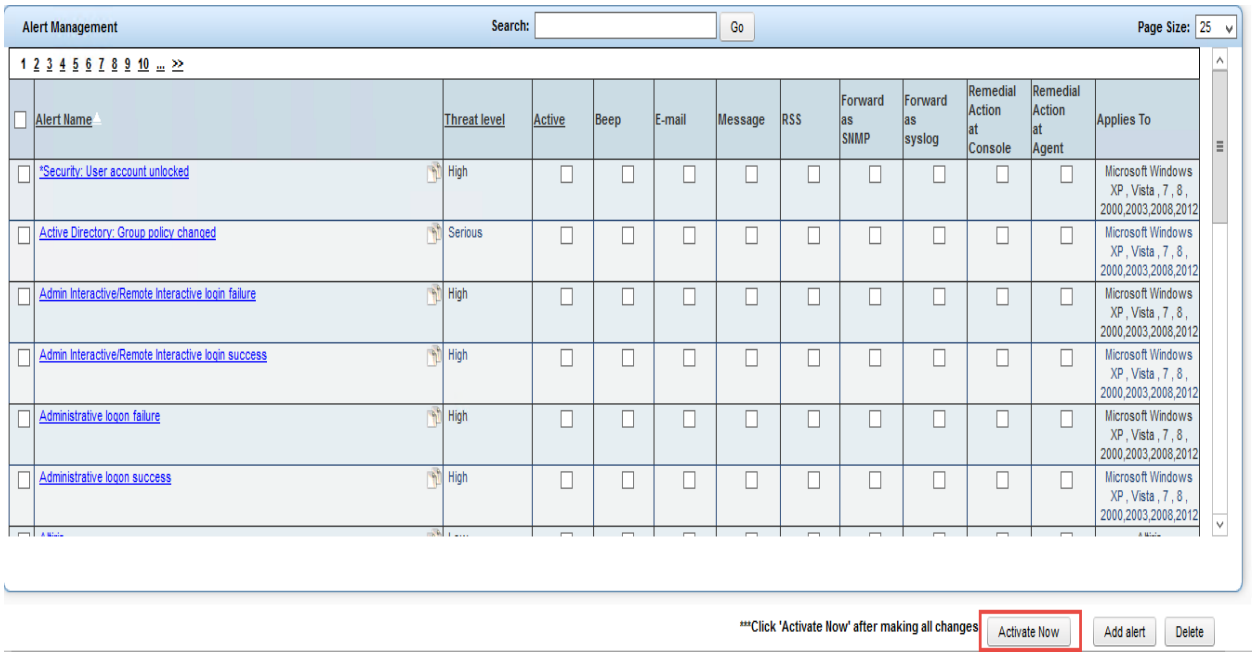


Figure: 15

Verify Reports

For verifying the reports,

- Go to **Incidents** tab and click on the **Dashboard** from the dropdown box.

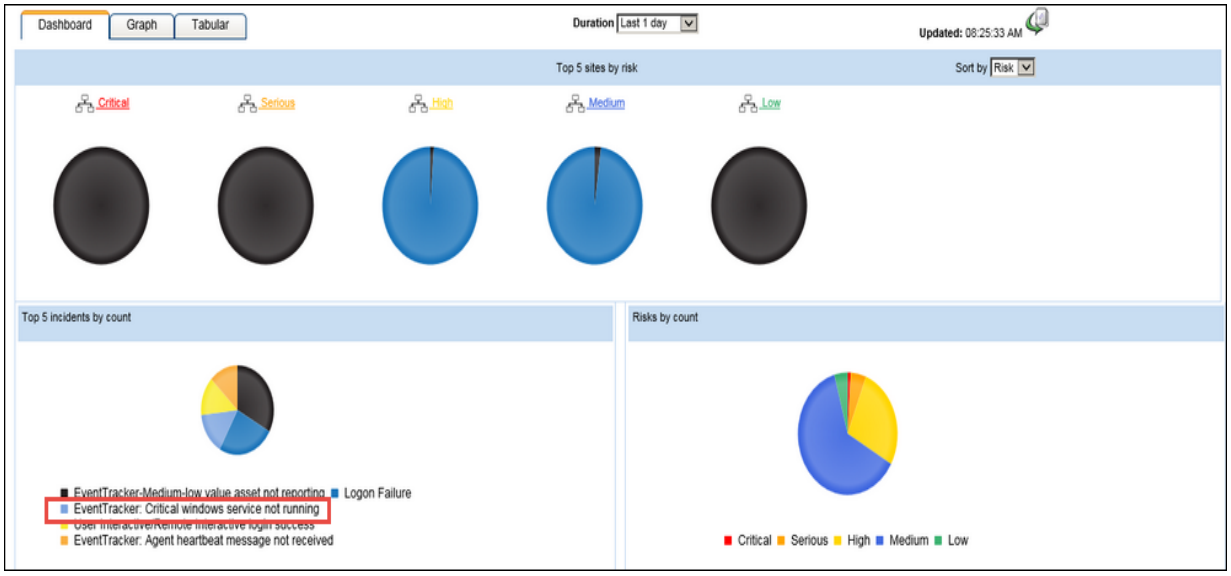


Figure: 16

- For viewing the graph, click the **Graph** tab.

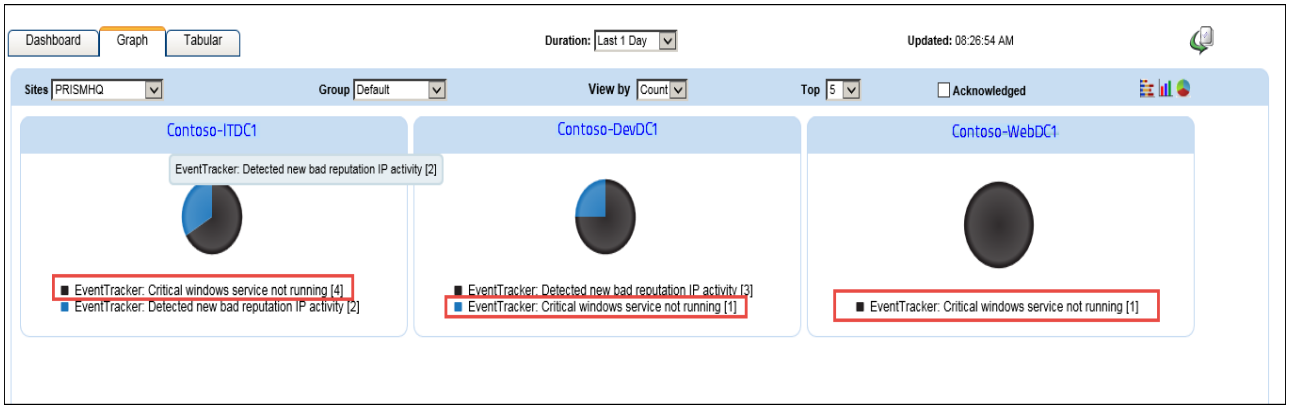


Figure: 17

- For Tabular view, click the **Tabular** tab.

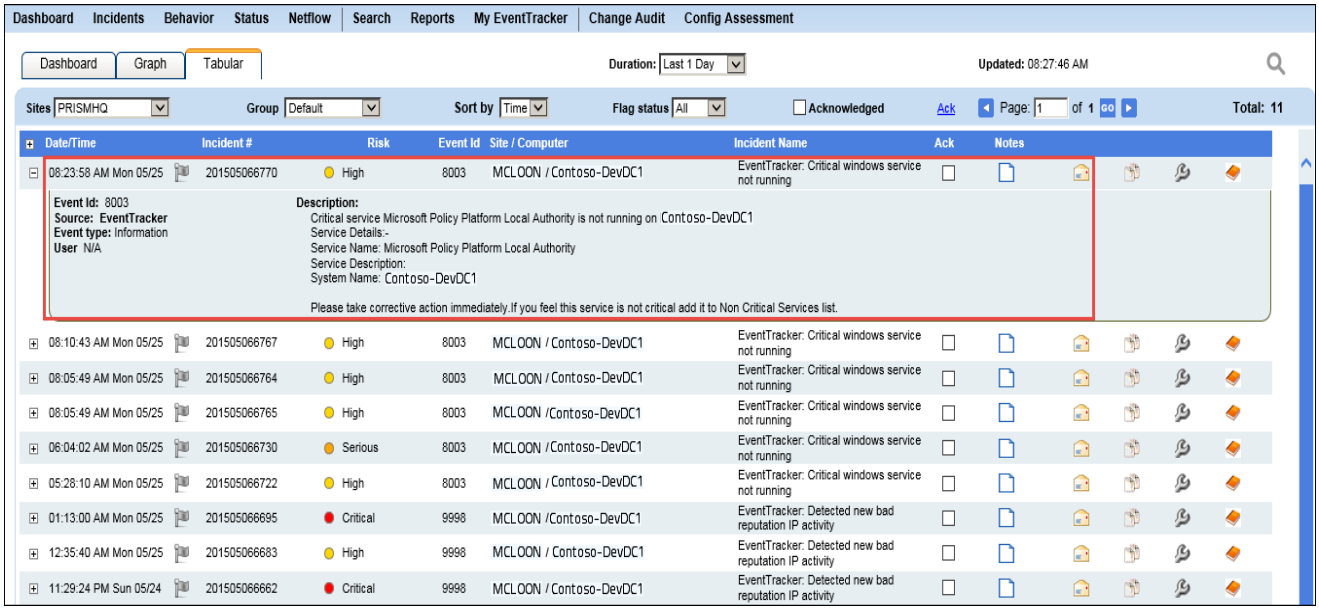


Figure: 18