

# Configure Critical Service Lookup

Publication Date: May 27, 2015

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://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.

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

*This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems 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 Prism Microsystems, 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. © 2015 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# 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:

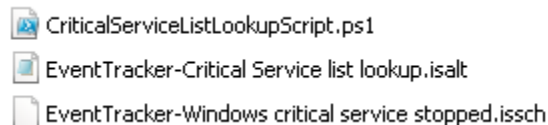


Figure 1

## 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**'.

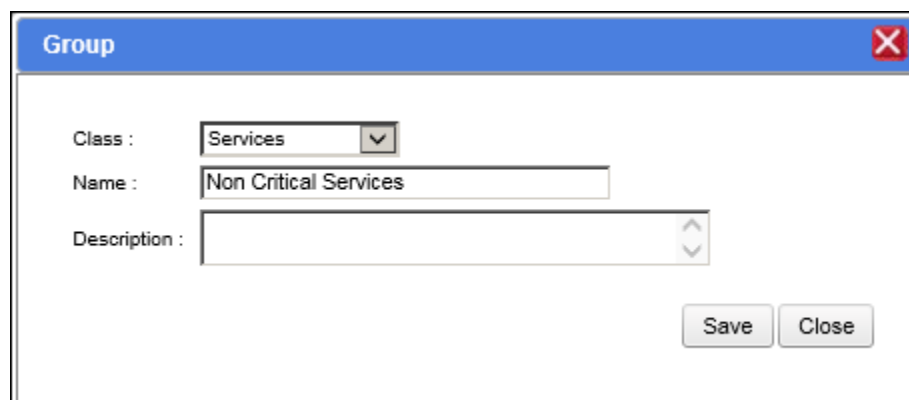


Figure 2

- Click the **Save** button.

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

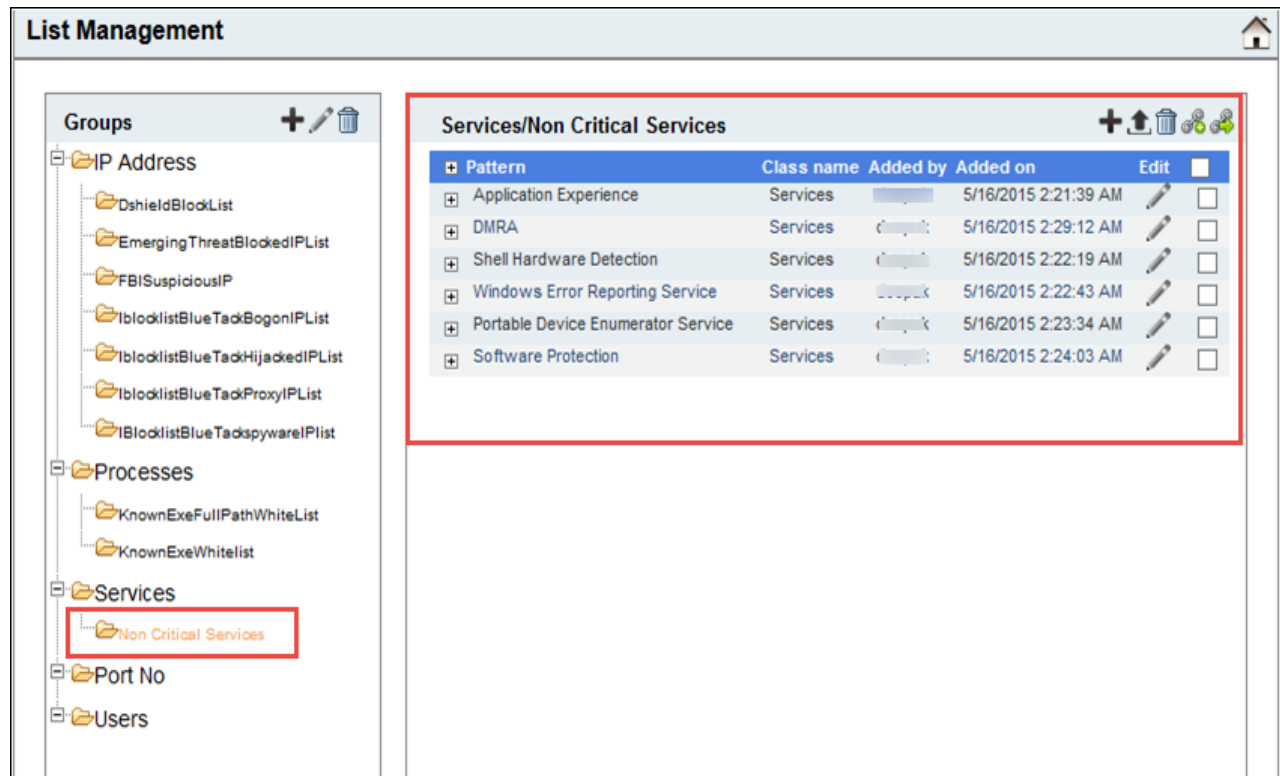


Figure 3

## Import Alert

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



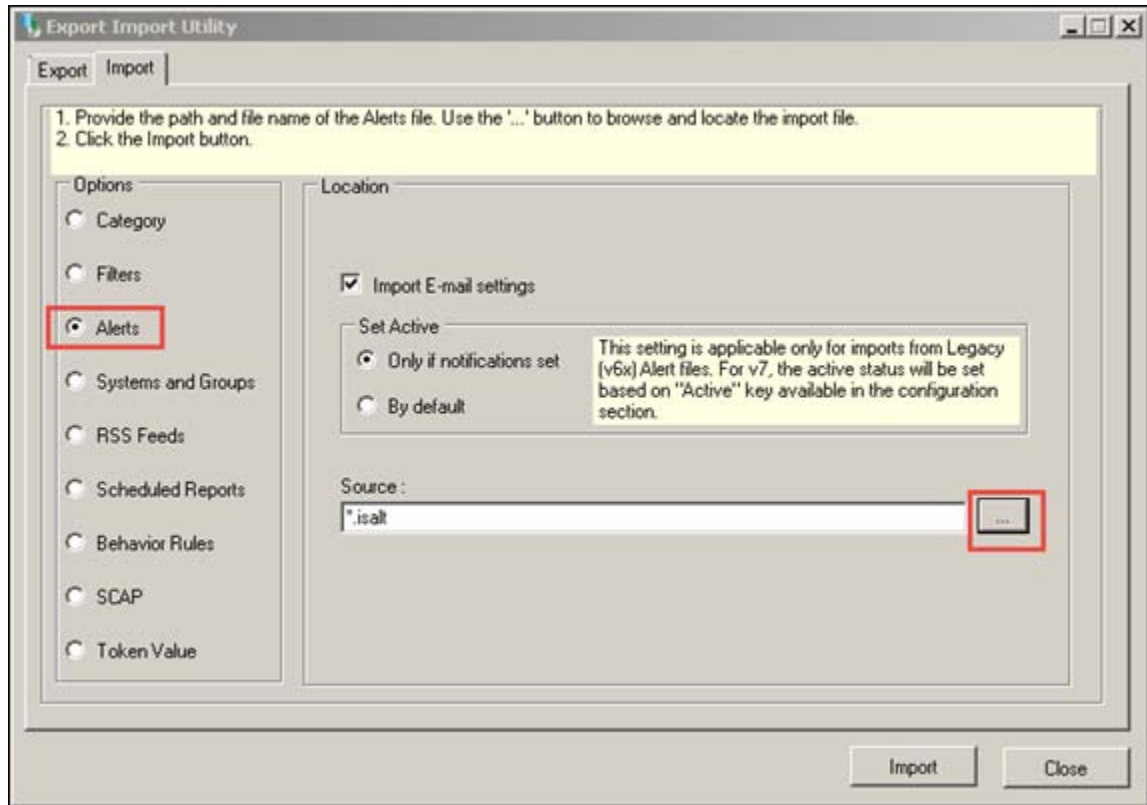



Figure: 4

- 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**.

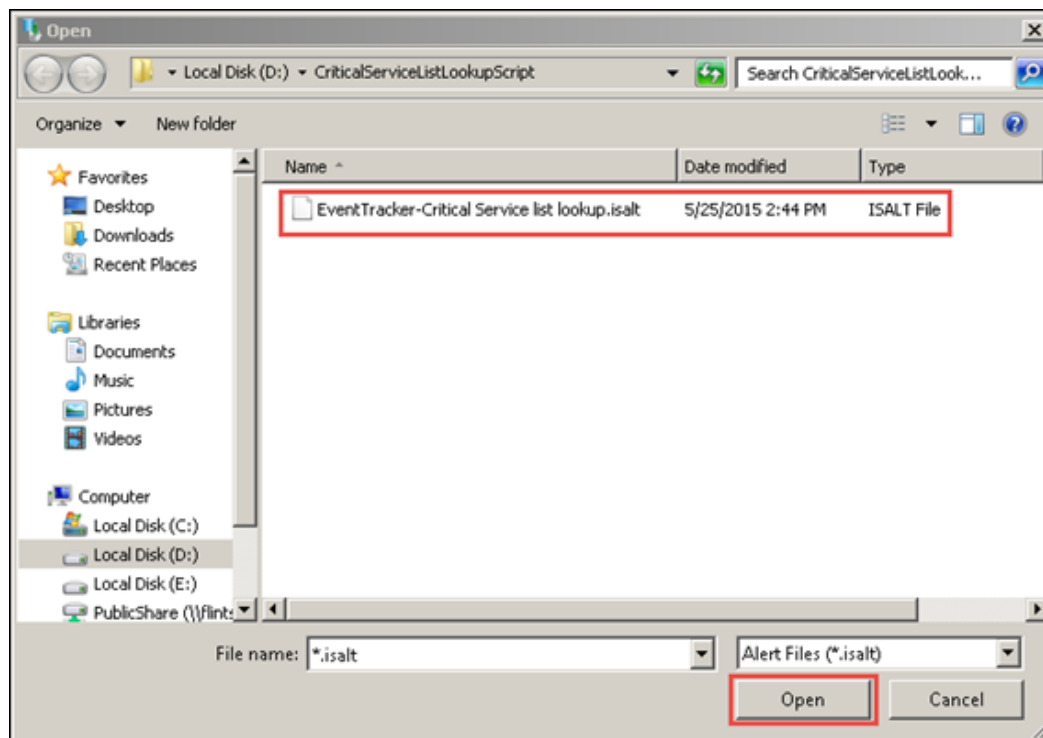


Figure: 5

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

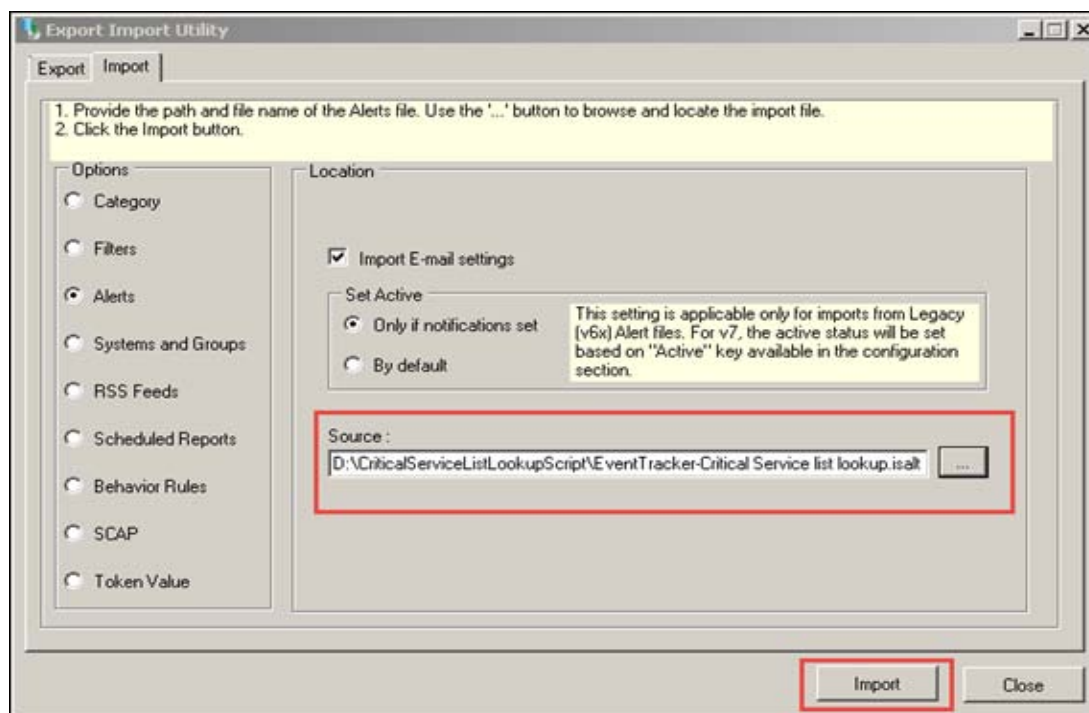


Figure: 6

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

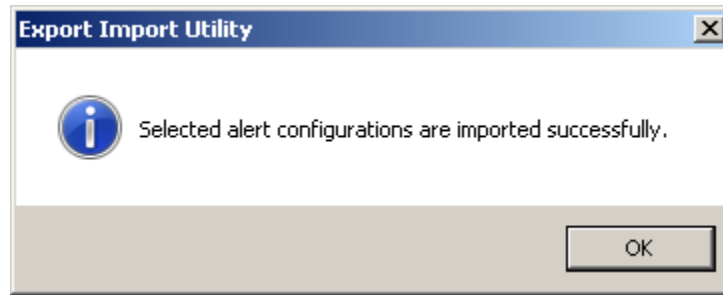


Figure 7

- 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.

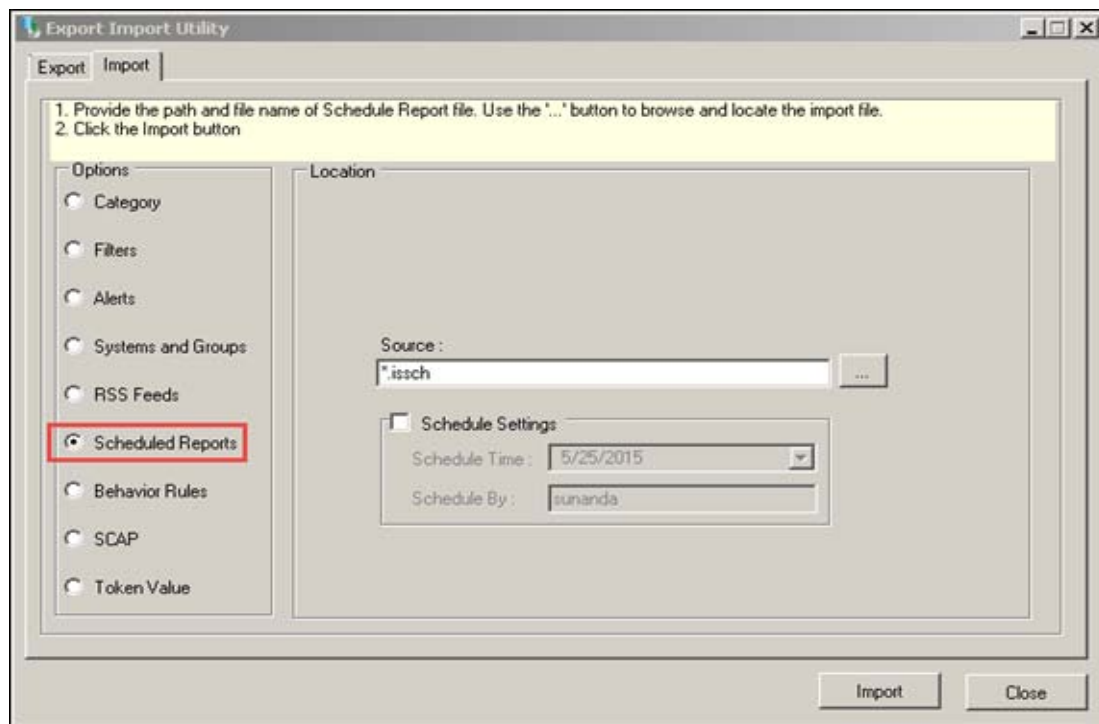


Figure: 8

- 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.

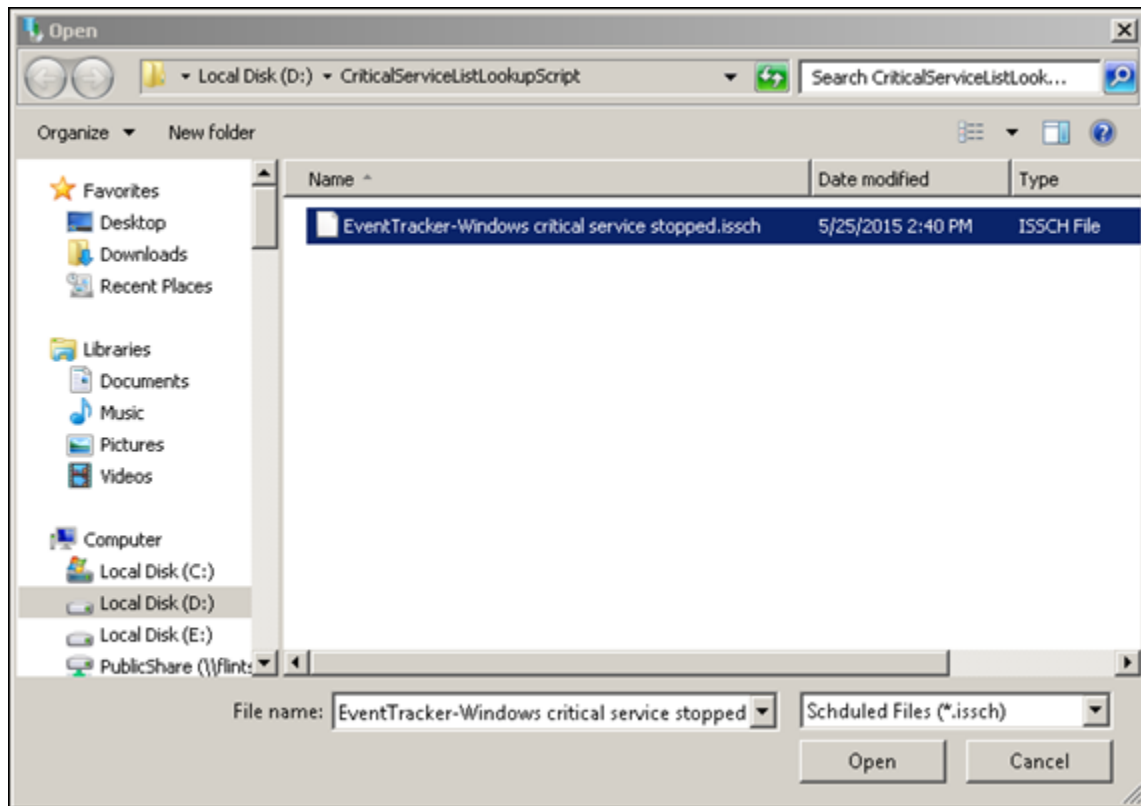


Figure: 9

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

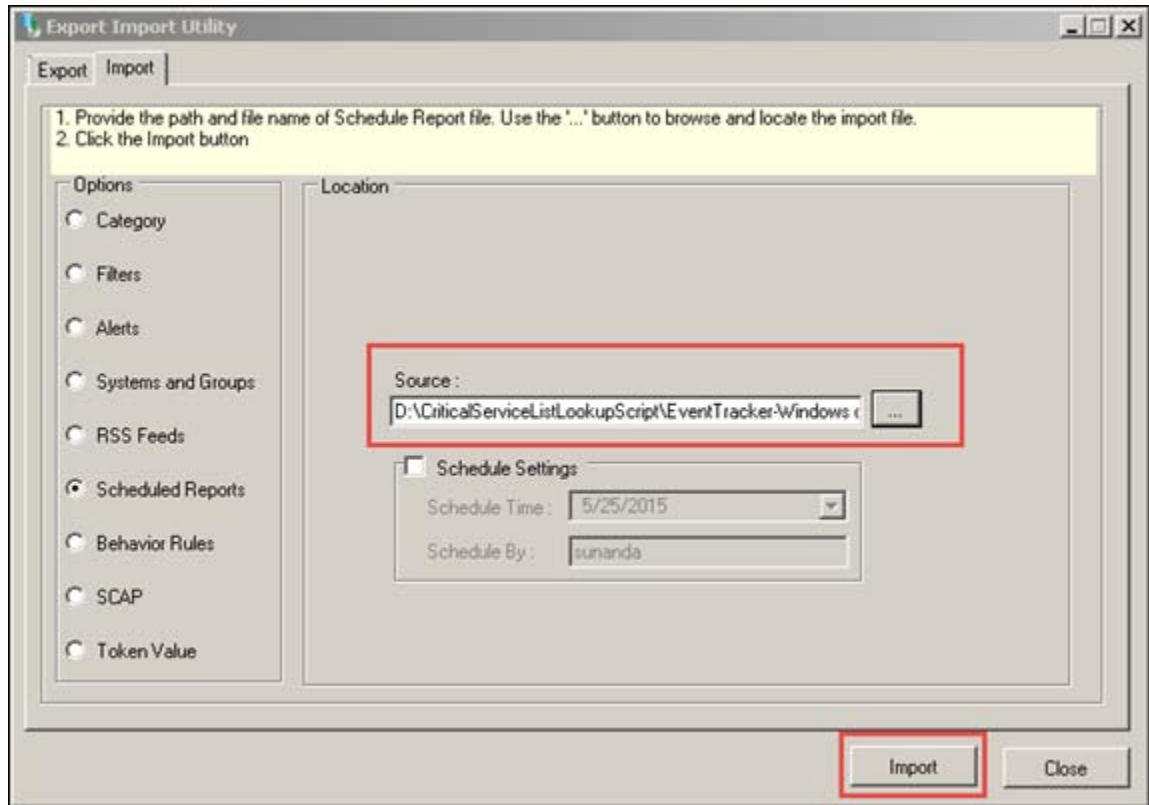
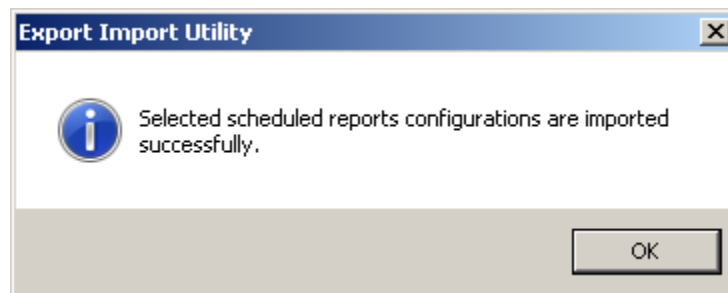


Figure: 10

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.

The screenshot shows the 'Alert Management' interface. At the top, there is a search bar with the text 'Search:' and a 'Go' button. To the right, the 'Page Size' is set to '25'. Below the search bar is a table with the following columns: Alert Name, Threat level, Active, Beep, E-mail, Message, RSS, Forward as SNMP, Forward as syslog, Remedial Action at Console, Remedial Action at Agent, and Applies To. The table contains several rows of alerts, including 'Security: User account unlocked', 'Active Directory: Group policy changed', 'Admin Interactive/Remote Interactive login failure', 'Admin Interactive/Remote Interactive login success', 'Administrative login failure', and 'Administrative login success'. At the bottom right of the table, there are three buttons: 'Activate Now', 'Add alert', and 'Delete'. A note below the buttons reads: '\*\*\*Click 'Activate Now' after making all changes'.

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.

## How to – Configure Critical Service Lookup

The screenshot shows the EventTracker Alert Management interface. At the top, there is a navigation bar with 'Dashboard', 'Incidents', 'Behavior', 'Status', 'Search', 'Reports', 'My EventTracker', 'Change Audit', and 'Config Assessment'. Below this is a search bar with the text 'EventTracker: Service list lookup' and a 'Go' button. A 'Page Size' dropdown is set to '25'. The main area contains a table with the following columns: Alert Name, Threat level, Active, Beep, E-mail, Message, RSS, Forward as SNMP, Forward as syslog, Remedial Action at Console, Remedial Action at Agent, and Applies To. The first row of the table is highlighted with a red box and contains the following data: Alert Name: EventTracker: Service list lookup, Threat level: High, Active: checked, Beep: unchecked, E-mail: unchecked, Message: unchecked, RSS: unchecked, Forward as SNMP: unchecked, Forward as syslog: unchecked, Remedial Action at Console: checked, Remedial Action at Agent: unchecked, Applies To: Microsoft Windows Operating Systems. At the bottom right, there are buttons for 'Activate Now', 'Add alert', and 'Delete', along with a note: '\*\*\*Click 'Activate Now' after making all changes'.

Figure: 12

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

The screenshot shows the EventTracker Alert configuration interface. At the top, there is a navigation bar with 'Dashboard', 'Incidents', 'Behavior', 'Status', 'Search', 'Reports', 'My EventTracker', 'Change Audit', and 'Config Assessment'. Below this is a search bar with the text 'EventTracker: Service list lookup' and a 'Go' button. The main area contains a form for alert configuration. The 'Alert Name' field is 'EventTracker: Service list lookup'. The 'Threat level' is 'High', 'Threshold level' is 'Medium', and 'Show in' is 'none'. The 'Alert Version' is '1.0' and 'Applies to' is 'Microsoft Windows Operating Systems'. Below the form is a section titled 'Systems' with a search bar and a list of systems. The 'Systems' section has radio buttons for 'Groups', 'Systems', and 'All Systems'. The search bar contains the text 'Search System(s):'. The list of systems includes 'Default' and 'TOONS', with 'TOONS' selected. At the bottom right, there are buttons for 'Finish' and 'Cancel'.

Figure: 13

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

## How to – Configure Critical Service 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.

The screenshot shows the 'Alert configuration' window in EventTracker. The 'Alert Name' is 'EventTracker: Service list lookup'. The 'Threat level' is 'High', 'Threshold level' is 'Medium', and 'Show in' is 'none'. The 'Alert Version' is '1.0' and it 'Applies to' 'Microsoft Windows Operating Systems'. The 'Console Remedial Action' tab is selected, showing a text area for the remedial action command. The command is: `"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" -File "F:\Scripts\Cr`. A red box highlights the file path portion of the command. The 'Finish' and 'Cancel' buttons are at the bottom right.

Figure: 14

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



Alert Management Search:  Go Page Size: 25

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
<a href="#">*Security: User account unlocked</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012
<a href="#">Active Directory: Group policy changed</a>	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012
<a href="#">Admin Interactive/Remote Interactive login failure</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012
<a href="#">Admin Interactive/Remote Interactive login success</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012
<a href="#">Administrative logon failure</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012
<a href="#">Administrative logon success</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Windows XP, Vista, 7, 8, 2000, 2003, 2008, 2012

\*\*\*Click 'Activate Now' after making all changes Activate Now Add alert Delete

Figure: 15

## Verify Reports

For verifying the reports,

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

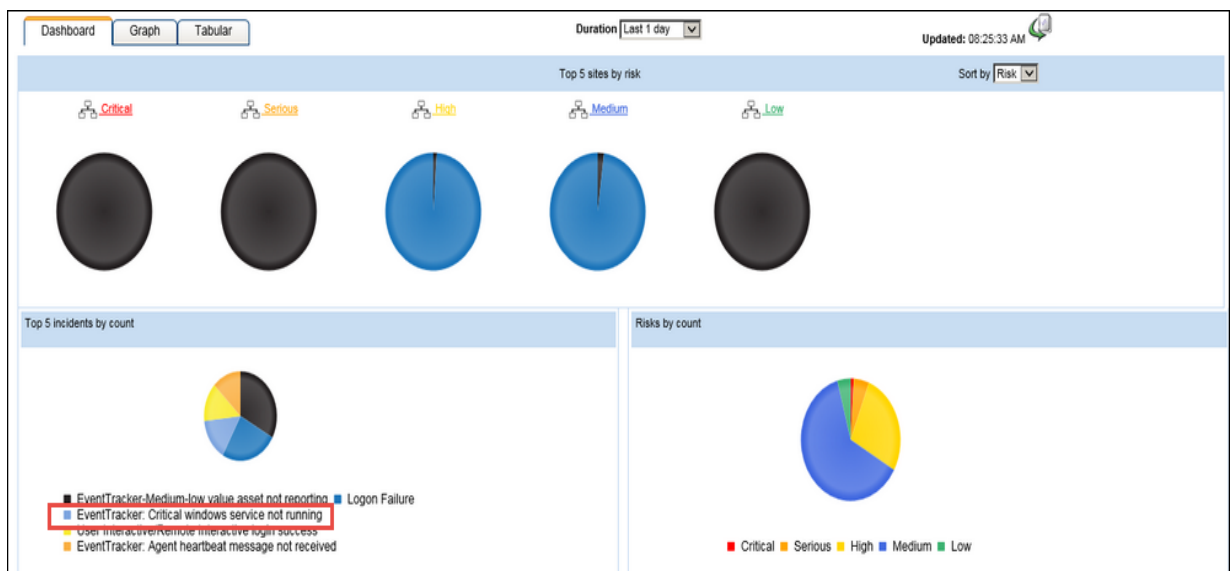


Figure: 16

## How to – Configure Critical Service Lookup

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

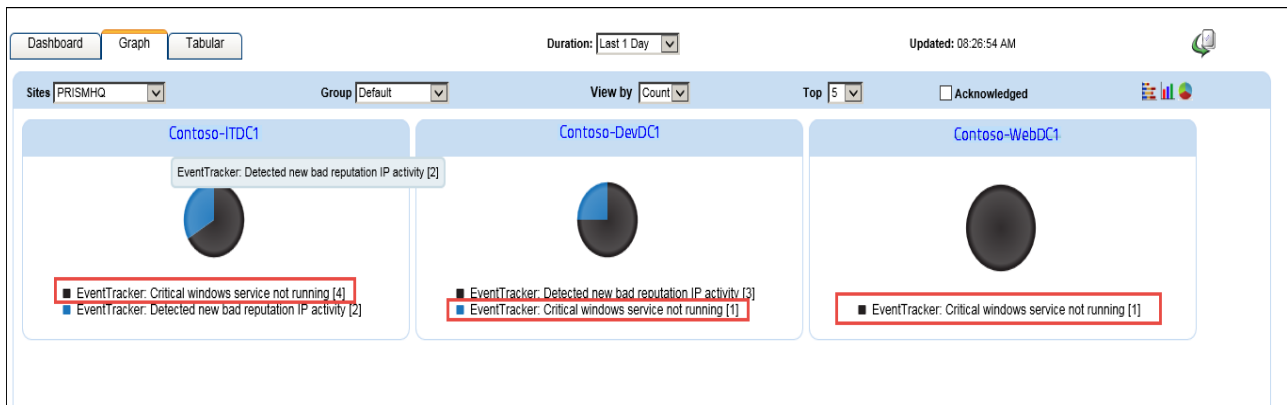


Figure: 17

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

The screenshot shows the EventTracker dashboard in Tabular view. The dashboard displays a table of incidents with the following columns: Date/Time, Incident #, Risk, Event Id, Site / Computer, Incident Name, Ack, and Notes. The table contains 11 rows of incident data. The first row is highlighted, and its details are shown in a pop-up window. The details window shows the following information:

- Event Id:** 8003
- Source:** EventTracker
- Event type:** Information
- User:** N/A
- Description:** Critical service Microsoft Policy Platform Local Authority is not running on Contoso-DevDC1
- Service Details:** Service Name: Microsoft Policy Platform Local Authority, Service Description: System Name: Contoso-DevDC1
- Note:** Please take corrective action immediately. If you feel this service is not critical add it to Non Critical Services list.

Figure: 18