Setup User Location affinity

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 setup User Location Affinity Monitoring for windows users based on windows interactive logins.

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
Setting up User Location Affinity 5
Preparing Scripts for use as per your environment 5
Import Alert 5
Import Scheduled Reports 7
Import Behavior Rule 10
Configure User Interactive Login Alert 13
Verify Behavior Rules 16

Introduction

Microsoft windows operating system generates event id 528 or 4624 depending on OS version with Logon Type 2, 10 and 11.It is important to monitor user logins to the workstations and the source from where they are logging in to systems. Sometimes it might be internal intrusion user may be trying to login to the other user systems to get access to sensitive information or user password is stolen and hacker logs in to the system from different geographical location.

EventTracker monitors the Interactive and remote interactive logins and extract Username, Target computer and source network address from where user is logged in and it alerts and provides reports if any user logs in to the system other than the regular workstations which is allocated to her or him. It also alerts when user logs in to his/her regular workstations but from different source network address.

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 deployed to remote windows systems.

Setting up User Location Affinity

Preparing Scripts for use as per your environment

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

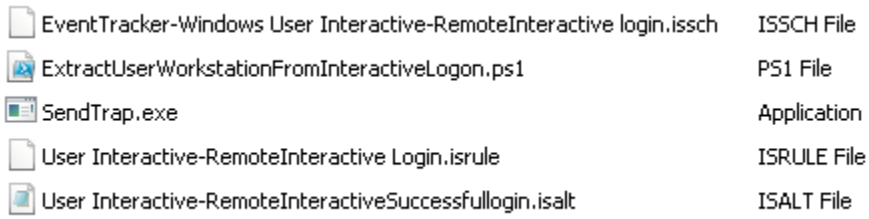

Figure 1

Import Alert

For importing the alert **User Interactive/Remote Interactive login success,** select the **Alerts** Option.

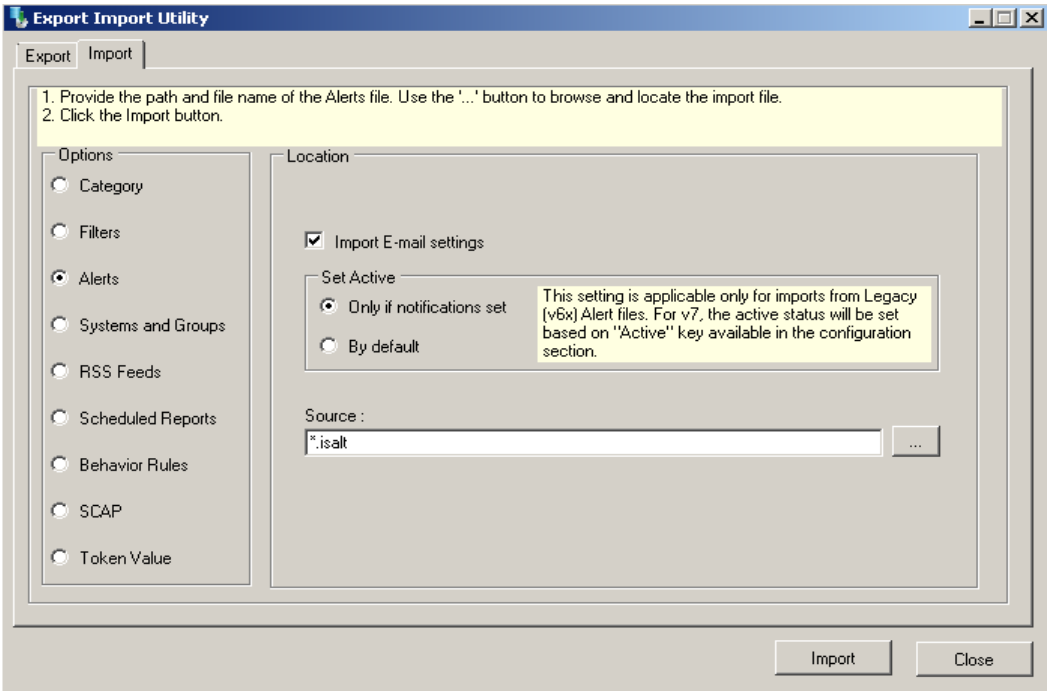

Figure: 2

- Provide the file name of the Alert file.
- For this, click the icon  and browse the Alert File i.e**. User Interactive-RemoteInteractiveSuccessfullogin.isalt** from your system and click **Open.**

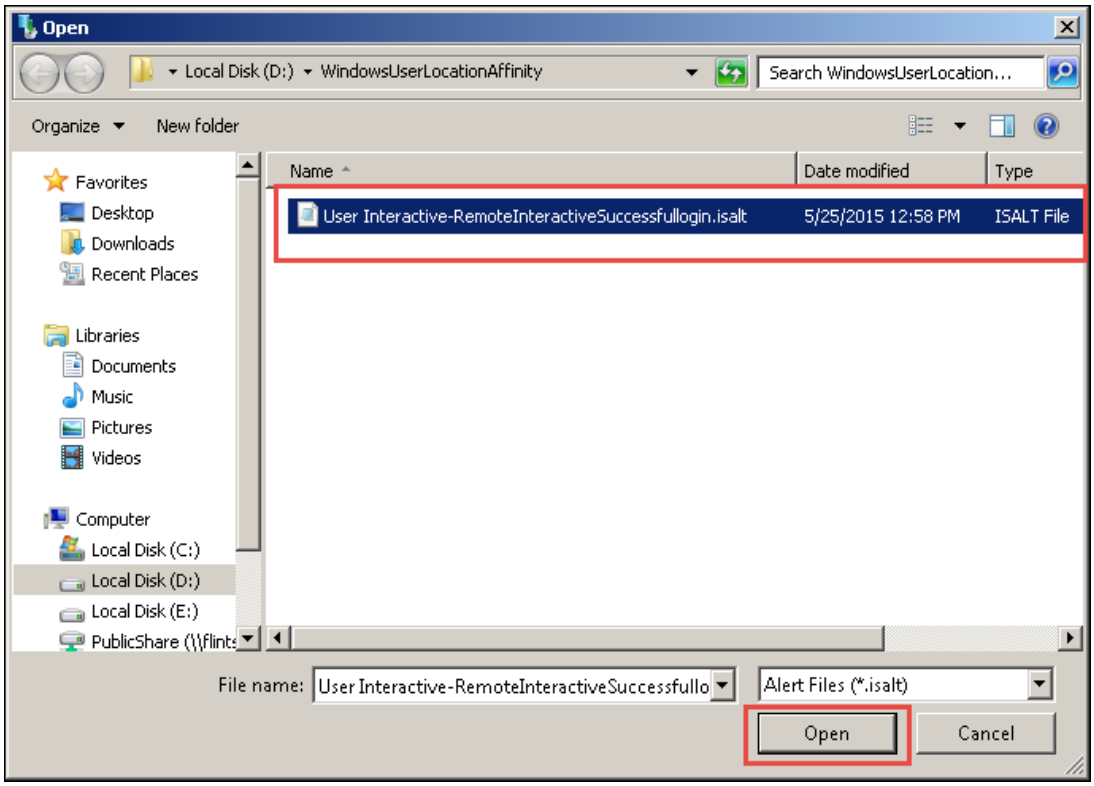

Figure: 3

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

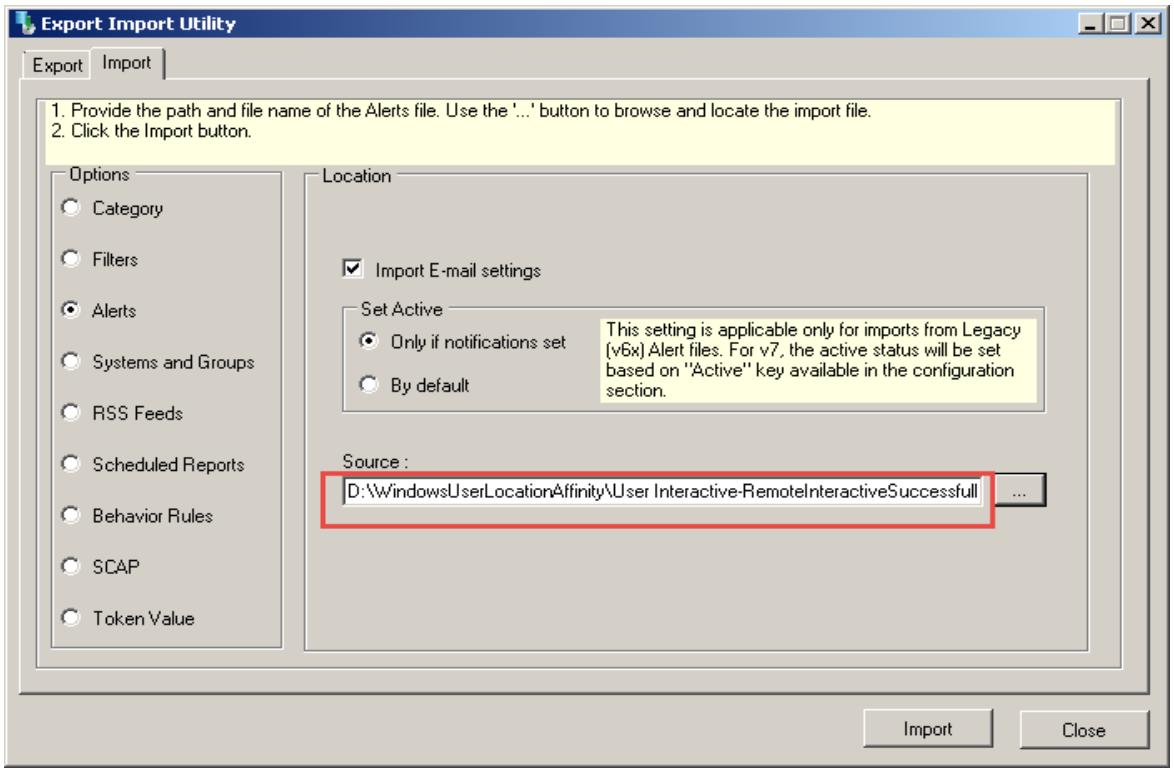

Figure: 4

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

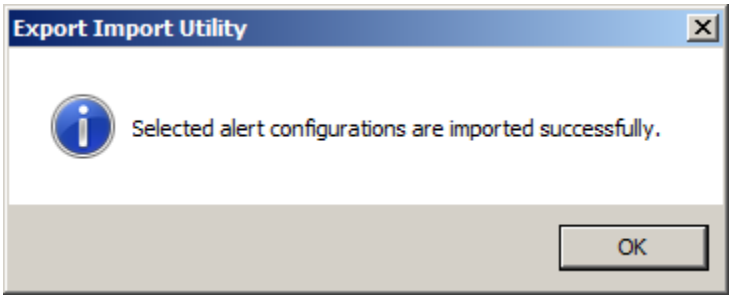

Figure 5

- Click **OK.**

The Alert **User Interactive/Remote Interactive login success** gets successfully imported.

Import Scheduled Reports

For importing the report **EventTracker-Windows User Interactive-RemoteInteractive login,** select the **Report** Option.

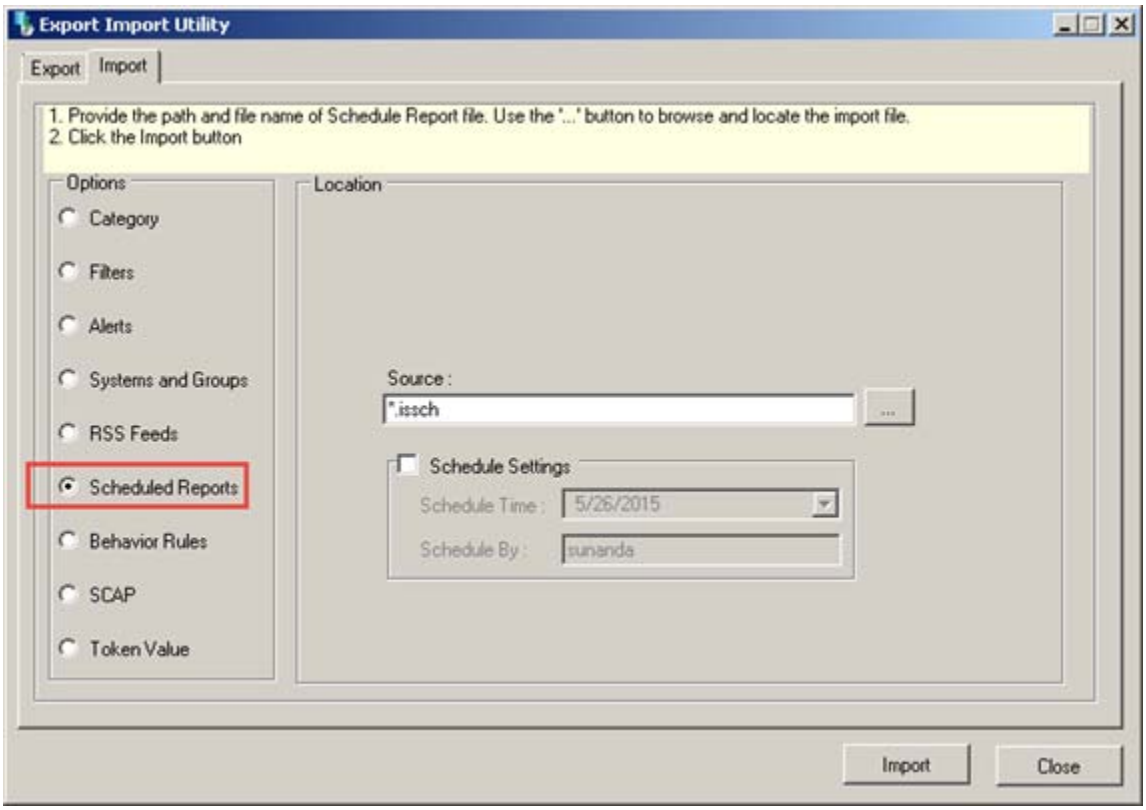

Figure: 6

- Provide the file name of the Report file.
- For this, click the icon  and browse the Report File i.e**. EventTracker-Windows User Interactive-RemoteInteractive login.issch** from your system and click **Open.**

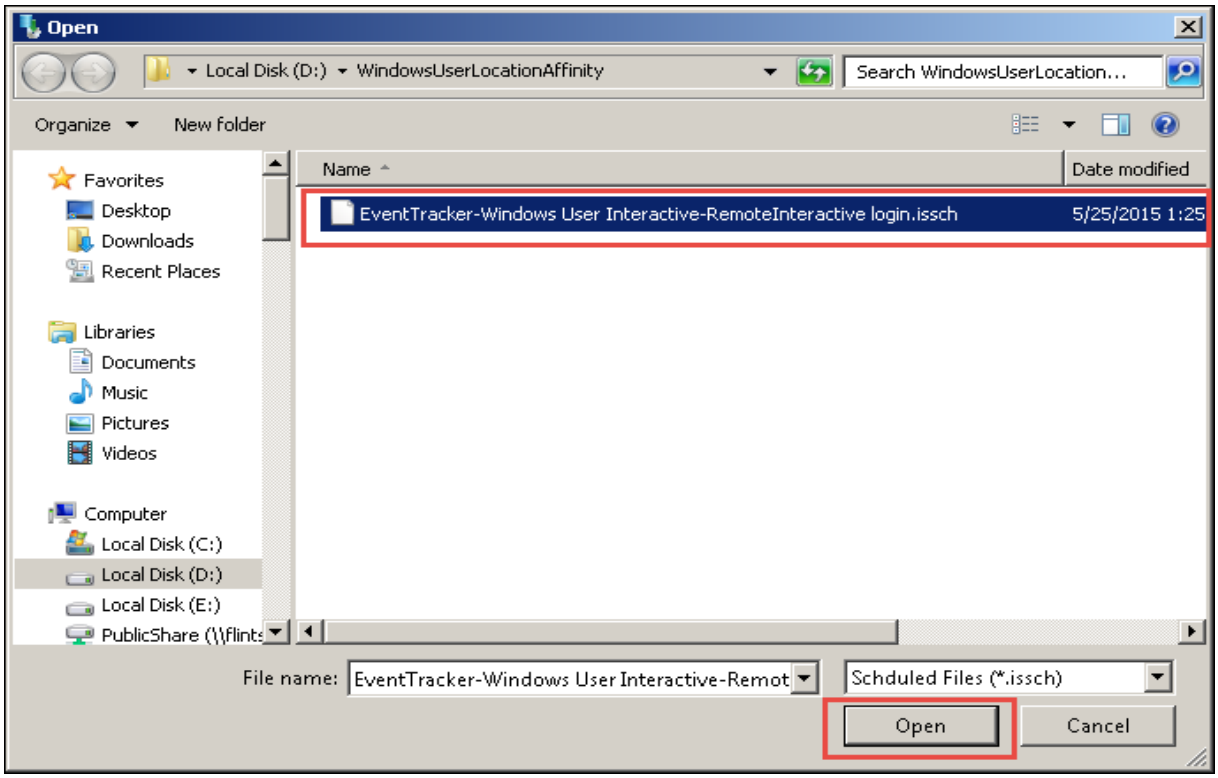

Figure: 7

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

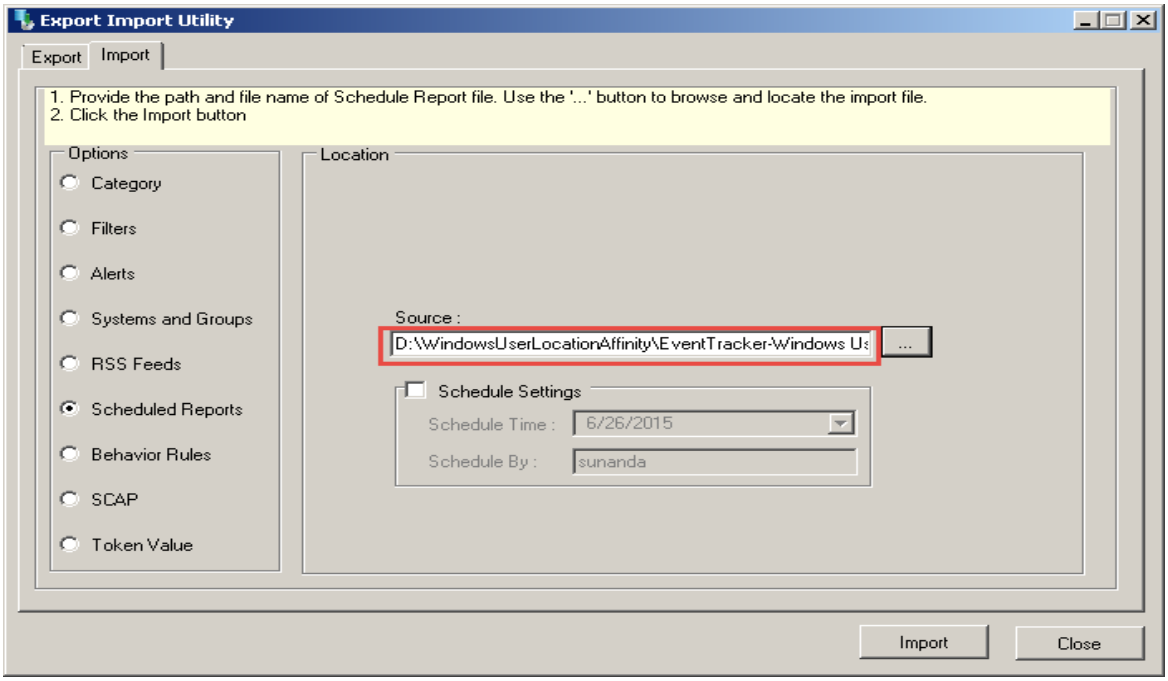

Figure: 8

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

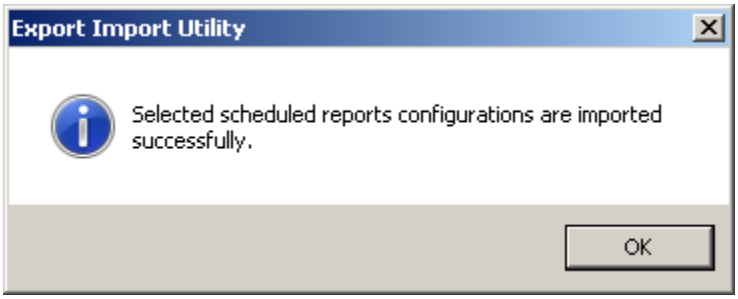

Figure 9

- Click **OK.**

The Report file **EventTracker-Windows User Interactive-RemoteInteractive login.issch,** gets successfully imported.

Import Behavior Rule

For importing the Behavior Rule, **User Interactive-RemoteInteractive Login,** select the **Behavior Rules** Option.

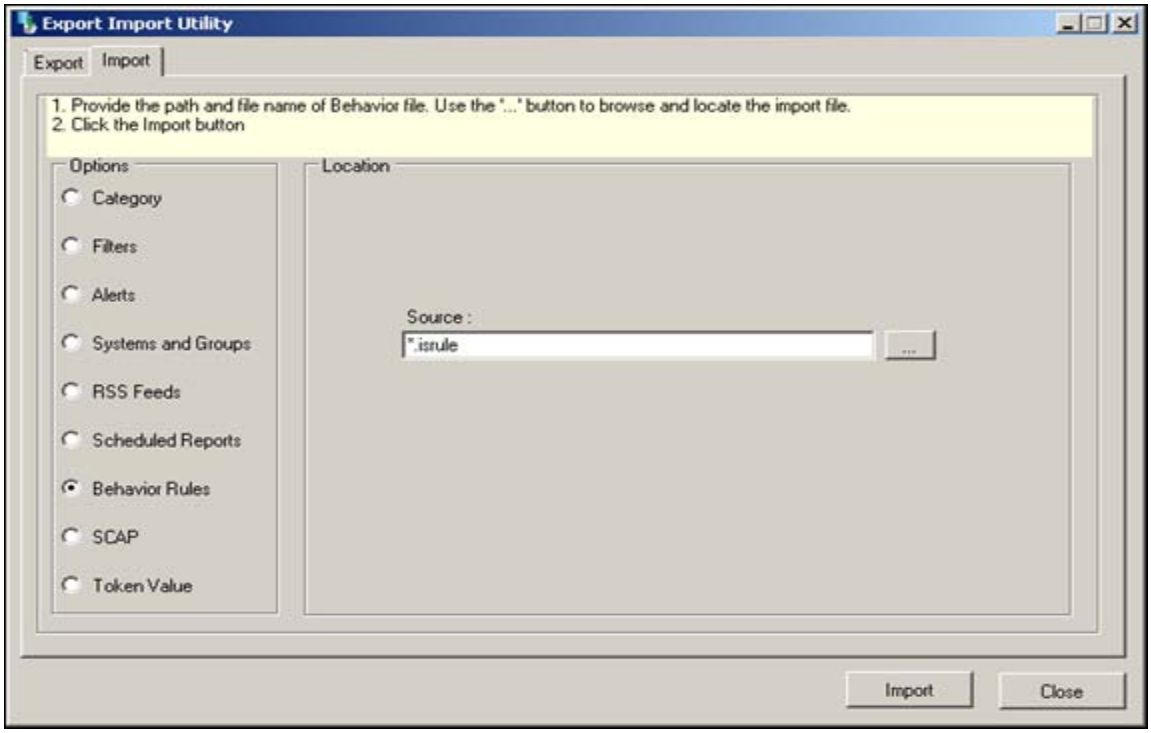

Figure: 10

- Provide the file name of the Behavior Rule file.
- For this, click the icon  and browse the Behavior Rule File i.e**. User Interactive-RemoteInteractive Login.isrule** from your system and click **Open.**

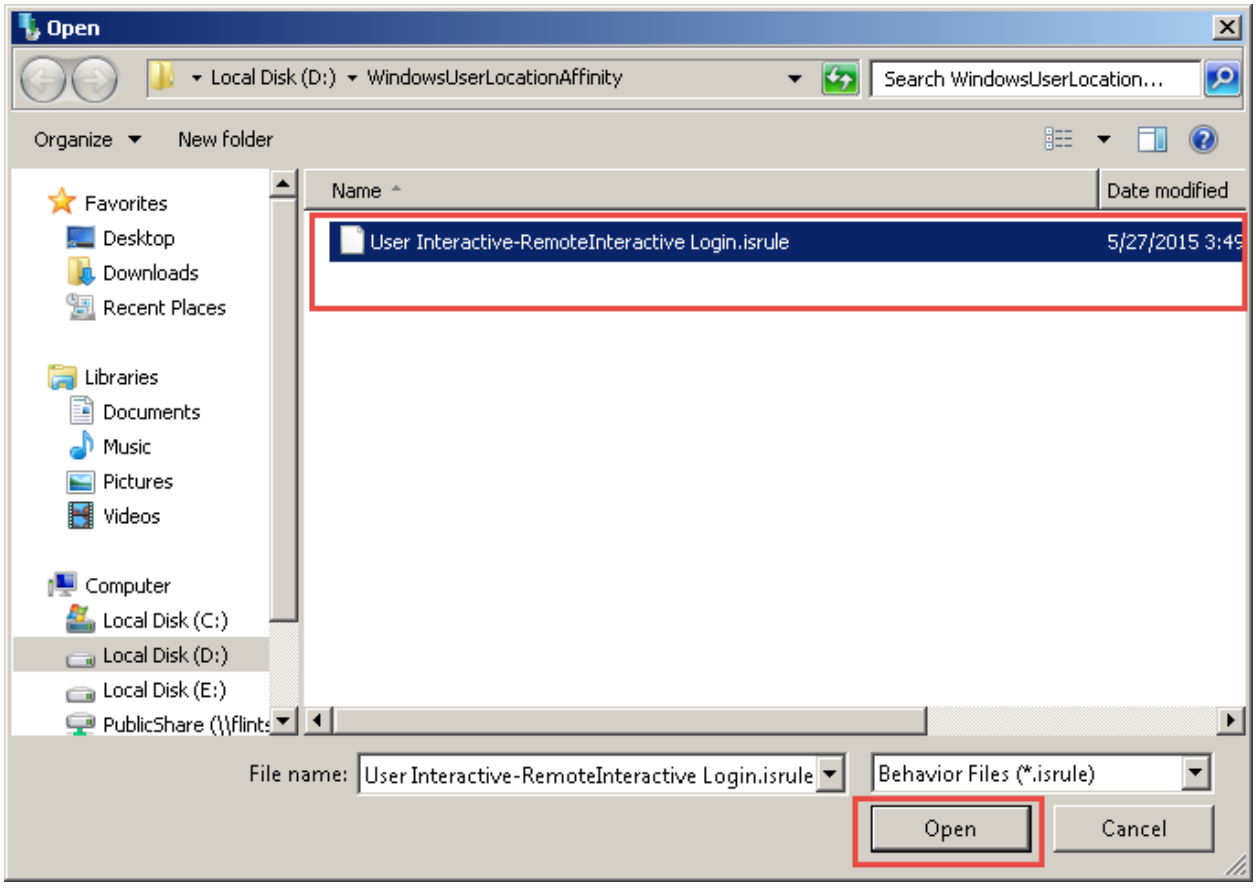

Figure: 11

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

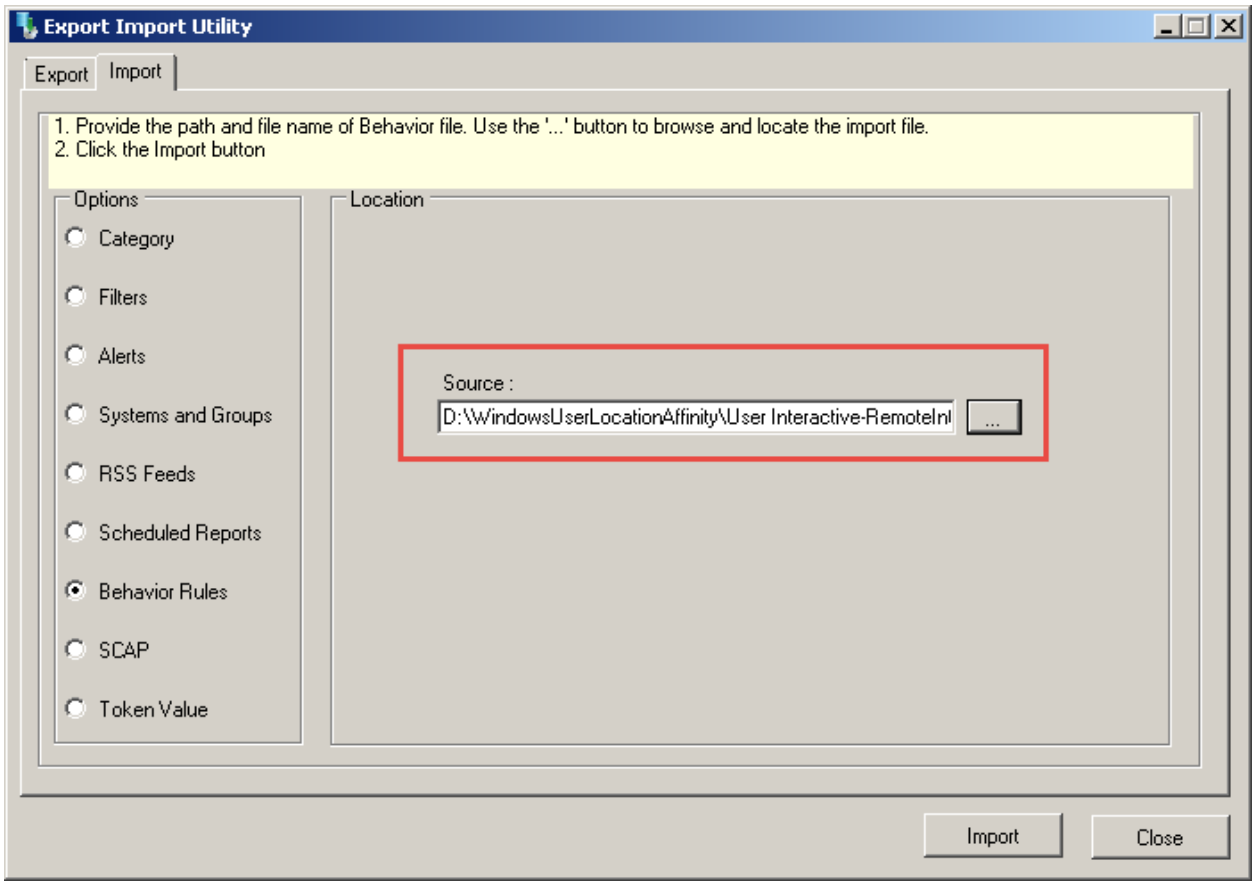

Figure: 12

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

Figure: 13

- Click **OK.**

The Behavior Rule file **User Interactive-RemoteInteractive Login.isrule,** gets successfully imported.

Configure User Interactive Login Alert

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

EventTracker displays the **Alert Management** page.

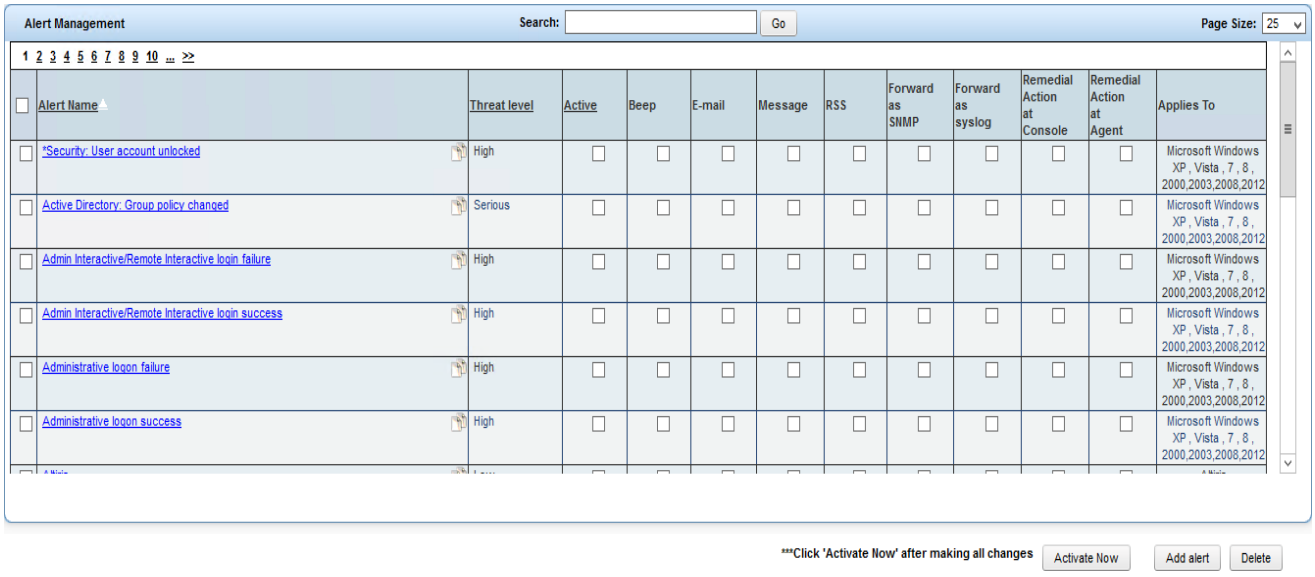

Figure: 14

- Enter the Alert Name **User Interactive/Remote Interactive login success** in the Search box.
- Click the **Go** button.

The Alert will be displayed.

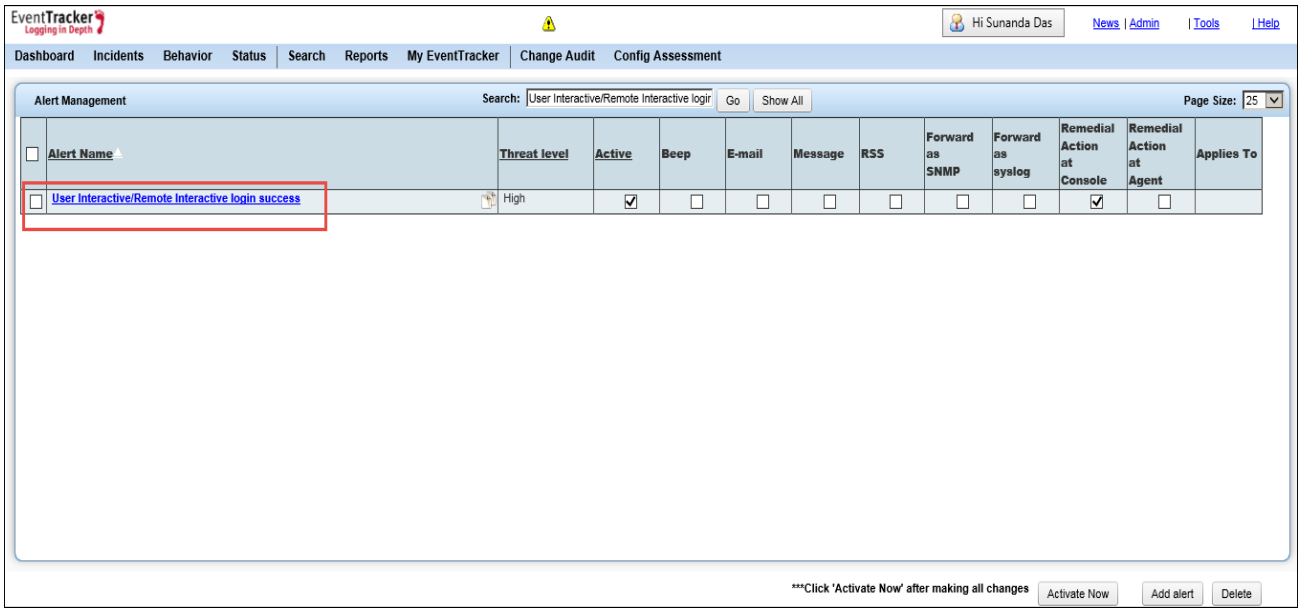

Figure: 15

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

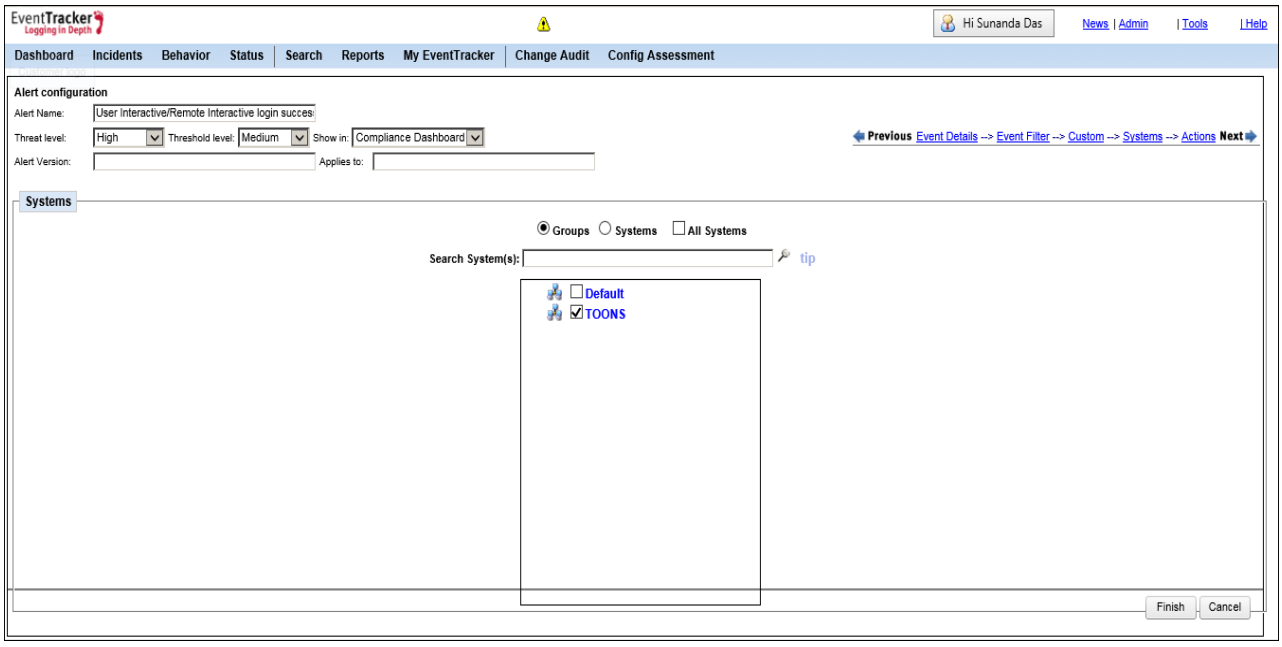

Figure: 16

For assigning Action based on a particular Alert,

- Click the **Action** hyperlink and then click the **Console Remedial Action** option tab.
- Enter the file name with the mentioned path as shown below:

"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe"–File"D:\Scripts\ExtractUserWorkstationFromInteractiveLogon\ExtractUserWorkstationFromInteractiveLogon.ps1"

NOTE: Please replace the install path with the path where the script has been stored.

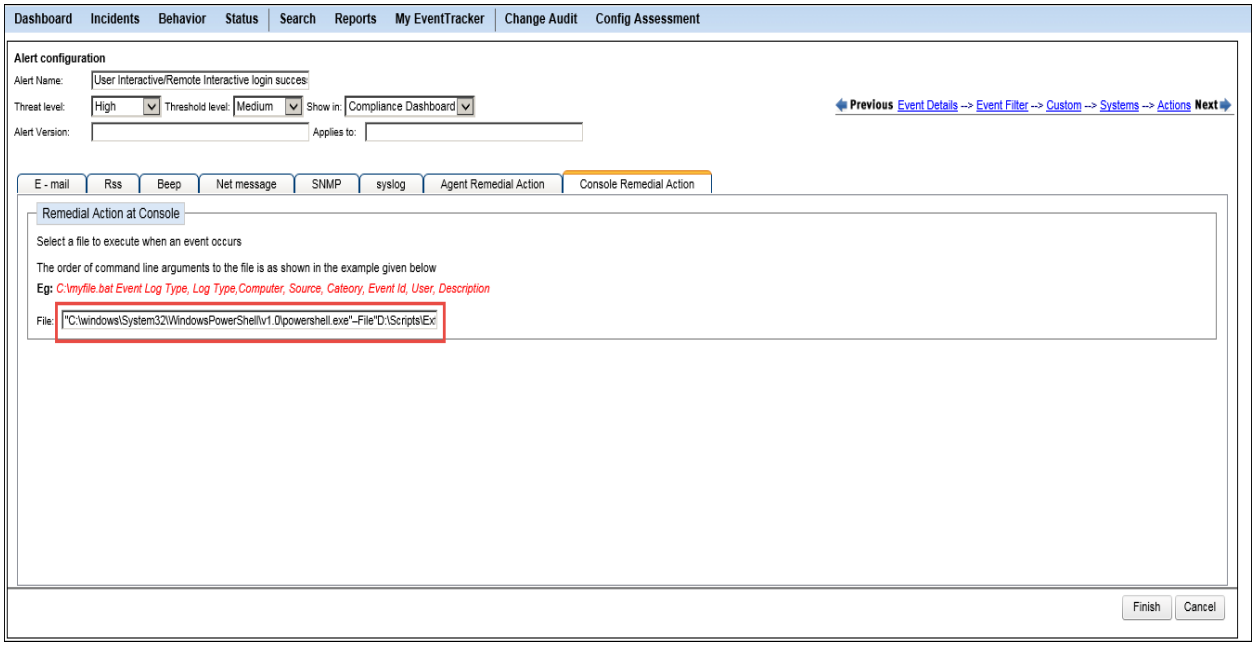

Figure: 17

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

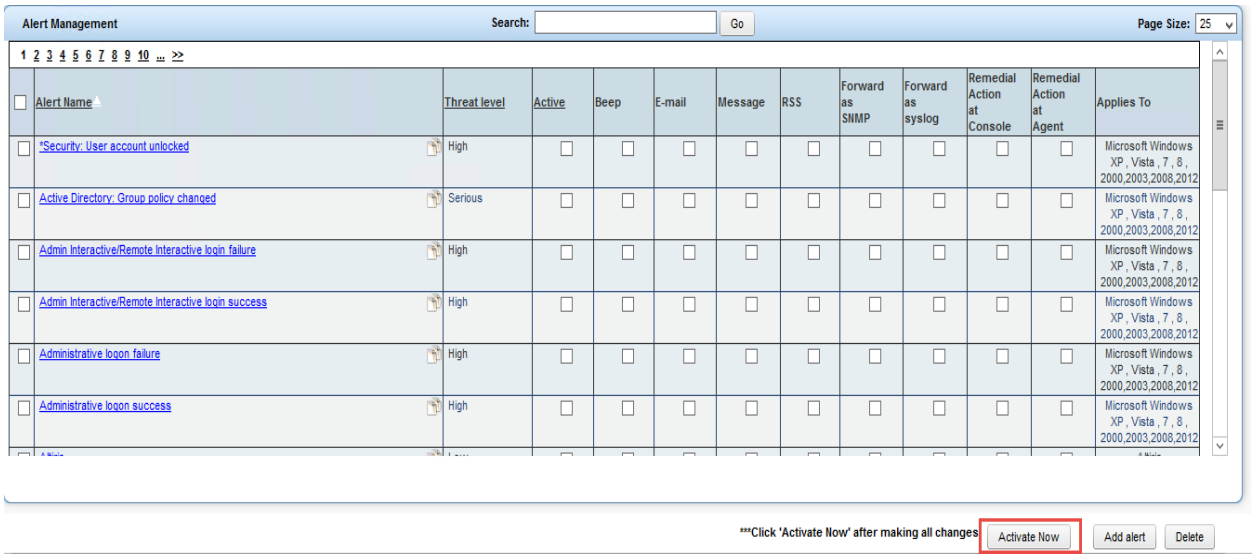

Figure: 18

Verify Behavior Rules

For verifying the Behavior Rules,

- Go to **Behavior** tab and click on the **Dashboard** from the dropdown box**.**
- Select the Behavior rule and click the **Go** button.

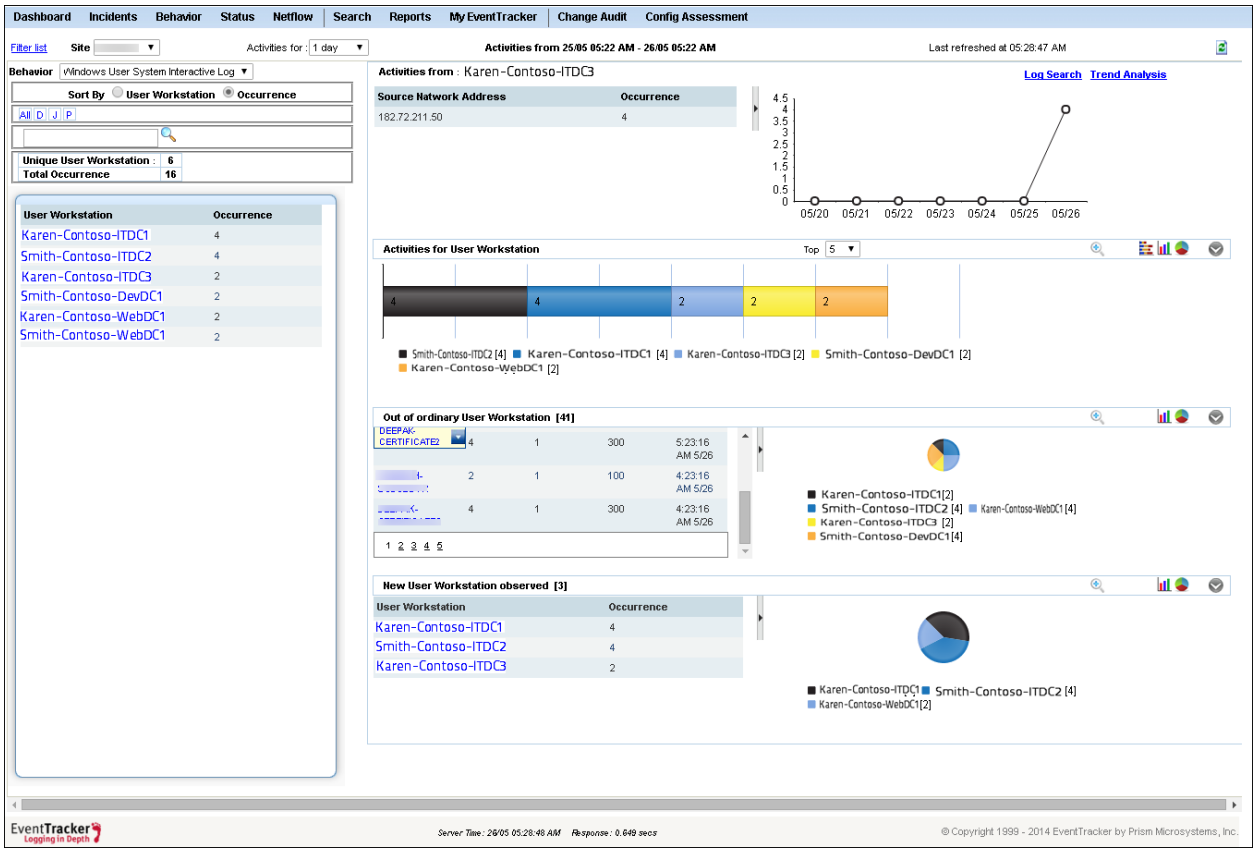
Dashboard
Incidents
Behavior
Status
Netflow
Search
Reports
My EventTracker
Change Audit
Config Assessment
Filter list
Site
Activities for : 1 day
Activities from 25/05 05:22 AM - 26/05 05:22 AM
Last refreshed at 05:28:47 AM
Behavior
Windows User System Interactive Log
Sort By
User Workstation
Occurrence
Unique User Workstation : 6
Total Occurrence 16
User Workstation
Occurrence
Karen-Contoso-ITDC1 4
Smith-Contoso-ITDC2 4
Karen-Contoso-ITDC3 2
Smith-Contoso-DevDC1 2
Karen-Contoso-WebDC1 2
Smith-Contoso-WebDC1 2
Activities from : Karen-Contoso-ITDC3
Log Search
Trend Analysis
Source Network Address
Occurrence
182.72.211.50 4
05/20 05/21 05/22 05/23 05/24 05/25 05/26
Activities for User Workstation
Top 5
Smith-Contoso-ITDC2 [4]
Karen-Contoso-ITDC1 [4]
Karen-Contoso-ITDC3 [2]
Smith-Contoso-DevDC1 [2]
Karen-Contoso-WebDC1 [2]
Out of ordinary User Workstation [41]
DEEPAK-CERTIFICATE2
5:23:16 AM 5/26
4:23:16 AM 5/26
4:23:16 AM 5/26
1 2 3 4 5
Karen-Contoso-ITDC1[2]
Smith-Contoso-ITDC2 [4]
Karen-Contoso-WebDC1 [4]
Karen-Contoso-ITDC3 [2]
Smith-Contoso-DevDC1[4]
New User Workstation observed [3]
User Workstation
Occurrence
Karen-Contoso-ITDC1 4
Smith-Contoso-ITDC2 4
Karen-Contoso-ITDC3 2
Karen-Contoso-ITDC1
Smith-Contoso-ITDC2 [4]
Karen-Contoso-WebDC1[2]
EventTracker
Logging in Depth
Server Time : 26/05 05:28:48 AM
Response : 0.649 secs
© Copyright 1999 - 2014 EventTracker by Prism Microsystems, Inc.

Figure: 19