Setup User Location affinity
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.

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
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-ExecutionPolicy Unrestricted`.
  - Make sure you do this for both x86 and x64 versions.
- EventTracker Agent must be deployed to remote windows systems.
How to – Setup User Location Affinity Monitoring

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:

  - EventTracker-Windows User Interactive-RemoteInteractive login.issch  ISSCH File
  - ExtractUserWorkstationFromInteractiveLogon.ps1  PS1 File
  - SendTrap.exe  Application
  - User Interactive-RemoteInteractive Login.isrule  ISRULE File
  - User Interactive-RemoteInteractiveSuccessfulLogin.isalt  ISALT File

![](image1.png)

Figure 1

Import Alert

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

![](image2.png)

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**.

![Image of file selection process]

**Figure: 3**

• Now, click the **Import** button.
How to – Setup User Location Affinity Monitoring

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

![Figure: 7](image)

![Figure: 8](image)
The success message box of 'Selected reports configurations are imported ' will be displayed.

![Image of Export Import Utility dialog box]

- Click OK.


**Import Behavior Rule**

For importing the Behavior Rule, User Interactive-RemoteInteractive Login, select the Behavior Rules Option.
• 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](image)

• Now, click the **Import** button.
How to – Setup User Location Affinity Monitoring

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.
How to – Setup User Location Affinity Monitoring

Configure User Interactive Login Alert

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

EventTracker displays the **Alert Management** page.

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

The Alert will be displayed.
• Click on the alert hyperlink to make changes in the Alert Configuration.
• Click the **System** hyperlink and select all the Windows system.

For assigning Action based on a particular Alert,
How to – Setup User Location Affinity Monitoring

- 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.
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.
How to – Setup User Location Affinity Monitoring

Figure: 19