EventTracker

Actionable Security Intelligence

How to Configure Non-Reporting Systems Alert Report

Publication Date: October 05, 2015

Abstract

This document helps EventTracker Admin to configure Non-Reporting Systems Alert and report using Scheduled action script.

Scope

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

Audience

EventTracker Administrators.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

Table of Contents

Overview

EventTracker Agents are deployed to remote systems for collecting logs from remote windows machines. Syslog sources are configured to send logs to EventTracker servers. Many times it is observed that remote logs are not being received from remote log sources because of various reasons but EventTracker Admins are not aware of that. This guide helps EventTracker users to configure automated alerts and reports using Scheduled action scripts.

Prerequisites

- EventTracker v7.x should be installed.
- Go to **EventTracker web server> Admin>Systems**, and make sure that the **Asset Value** are put accordingly.

How it works?

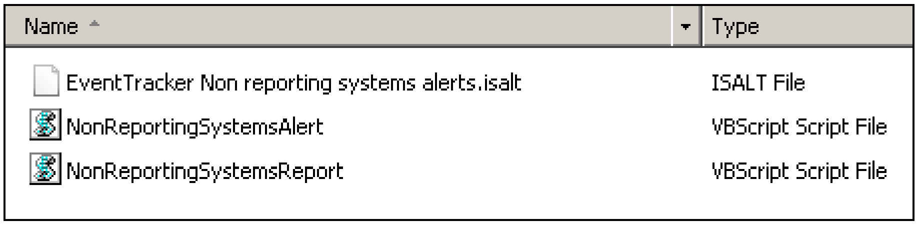
EventTracker Non-Reporting Systems Alert script queries the EventTracker database and checks whether LogRecievedTime for any managed systems are earlier than number of hours passed as parameter. If LogRecievedTime of any systems found older, then Event ID 8000 is generated with Source EventTracker.

EventTracker Non-Reporting Systems Report script queries the EventTracker database and checks whether LogRecievedTime for any managed systems are earlier than no of hours passed as parameter. If LogRecievedTime of any systems found older, then CSV file is generated.

Automating Non-Reporting Systems Alerts and Reports

Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the NonReportingSystemsScript pack.
- Save NonReportingSystemsScript.zip (saved to D:\NonReportingSystemsScript\ folder in the example below).
- Extract all files to D:\NonReportingSystemsScript\.
- Files in the package are shown below.



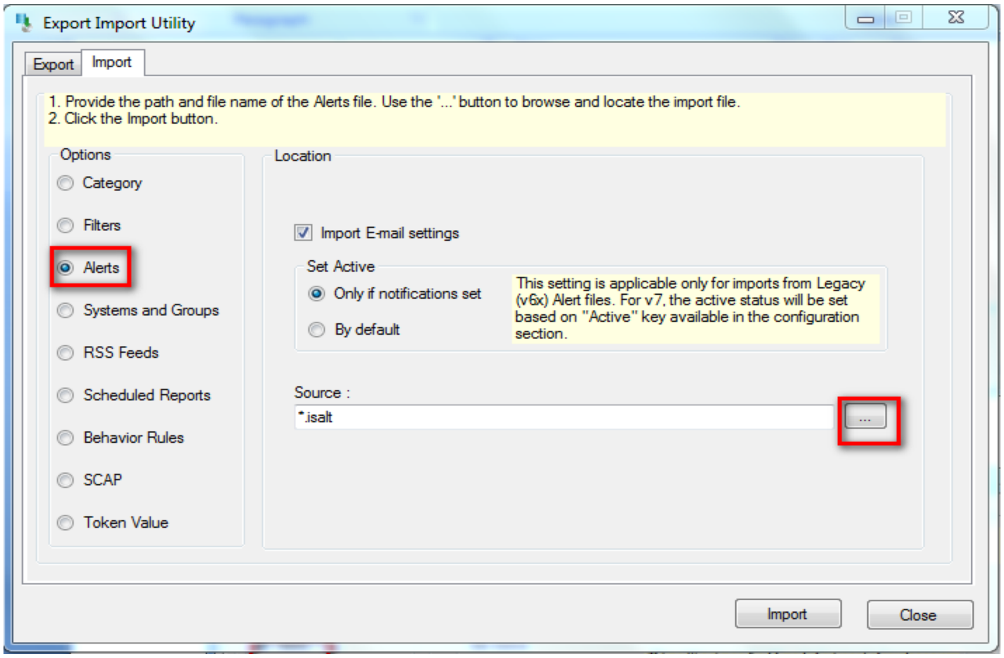
Name	Type
EventTracker Non reporting systems alerts.isalt	ISALT File
NonReportingSystemsAlert	VBScript Script File
NonReportingSystemsReport	VBScript Script File

Figure 1

- Copy both the scripts files inside the install path "..\EventTracker\ScheduledActionScripts" folder.

Import Alert

For importing the alert **EventTracker Non-Reporting Systems.isalt,** select the **Alerts** Option.



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

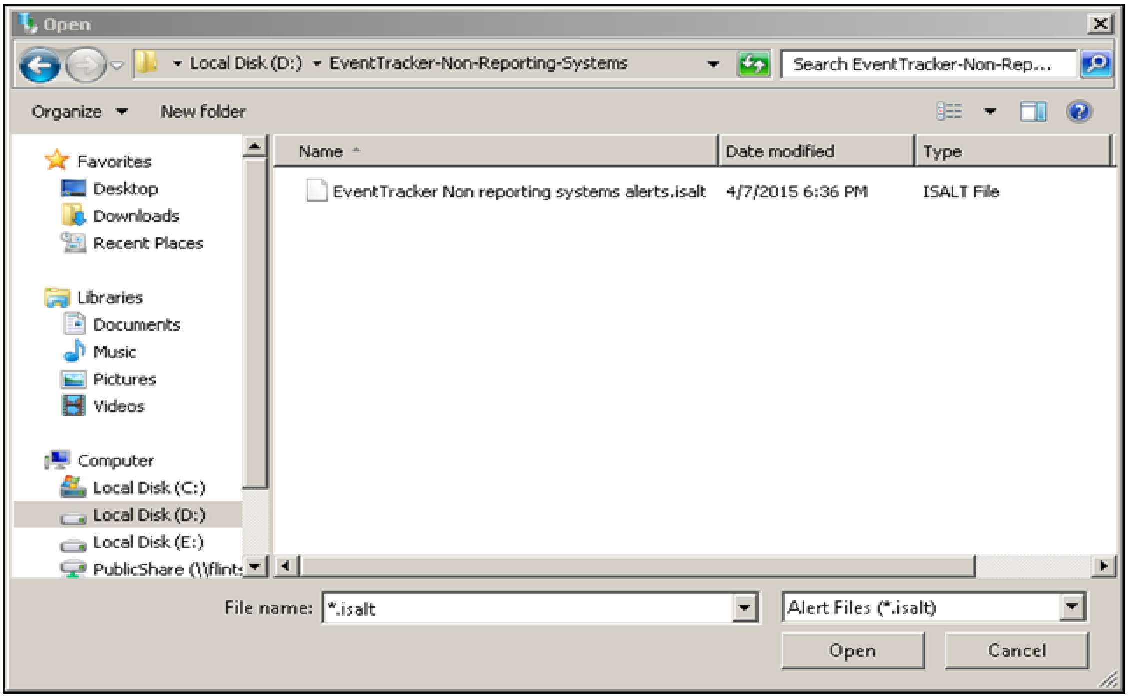
● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 2

- Provide the file name of the Alert file.
- For this, click the icon ... and browse the Alert File i.e**. EventTracker Non reporting systems alerts.isalt** from your system and click **Open.**



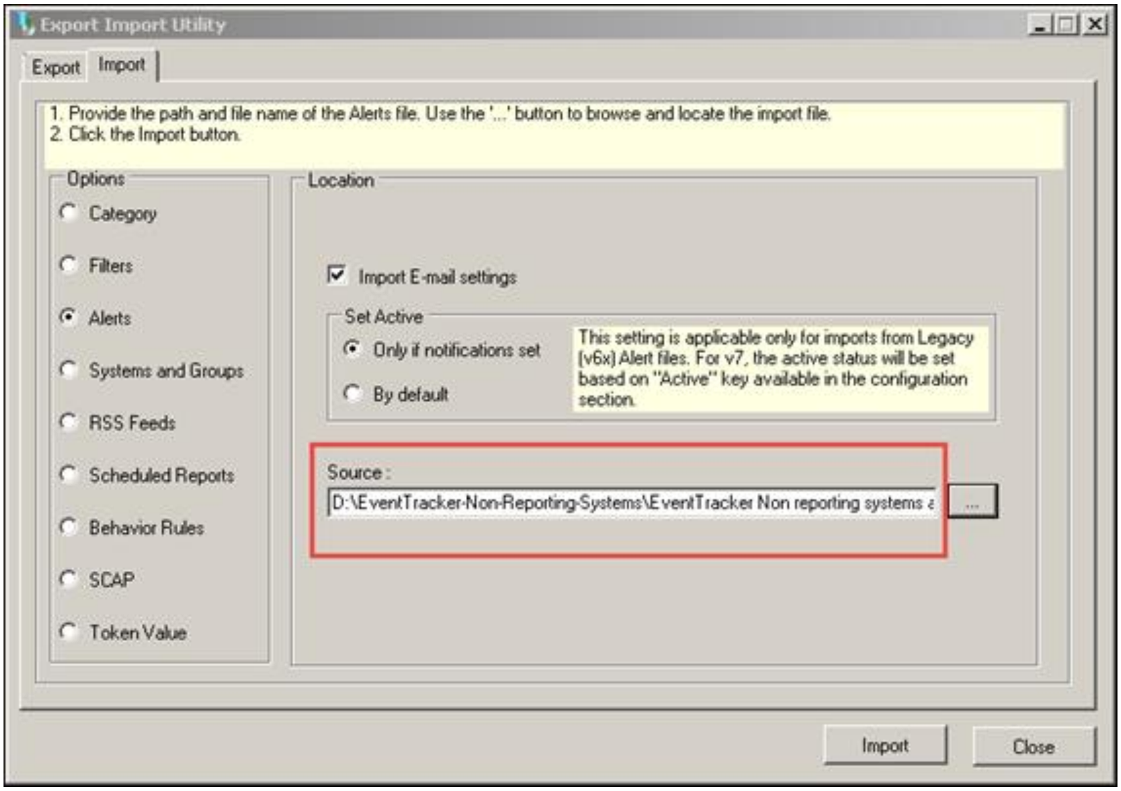
Name	Date modified	Type
EventTracker Non reporting systems alerts.isalt	4/7/2015 6:36 PM	ISALT File

File name: *.isalt

Alert Files (*.isalt)

Figure 3

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



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options: ○ Category ○ Filters ● Alerts ○ Systems and Groups ○ RSS Feeds ○ Scheduled Reports ○ Behavior Rules ○ SCAP ○ Token Value

☑ Import E-mail settings

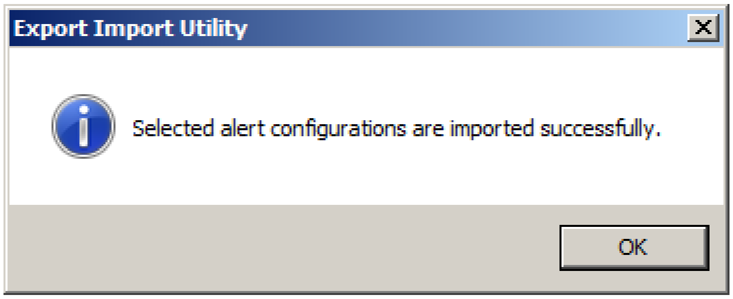
Set Active: ● Only if notifications set ○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : D:\EventTracker-Non-Reporting-Systems\EventTracker Non reporting systems a

Figure 4

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



Selected alert configurations are imported successfully.

Figure 5

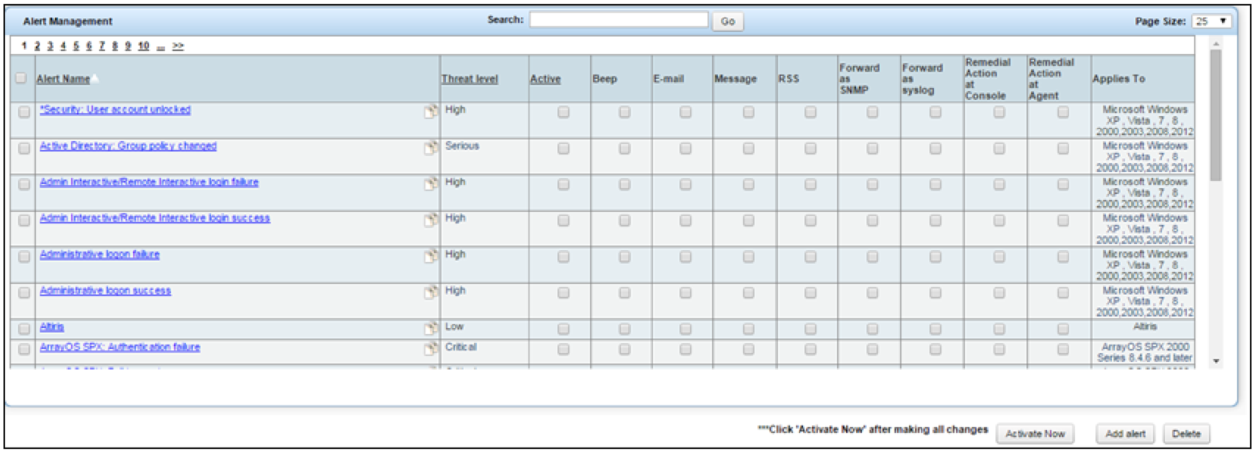
- Click **OK.**

The Alert **EventTracker Non reporting systems alerts.isalt,** gets successfully imported.

Configure Non-Reporting System Alert

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

EventTracker displays the **Alert Management** page.



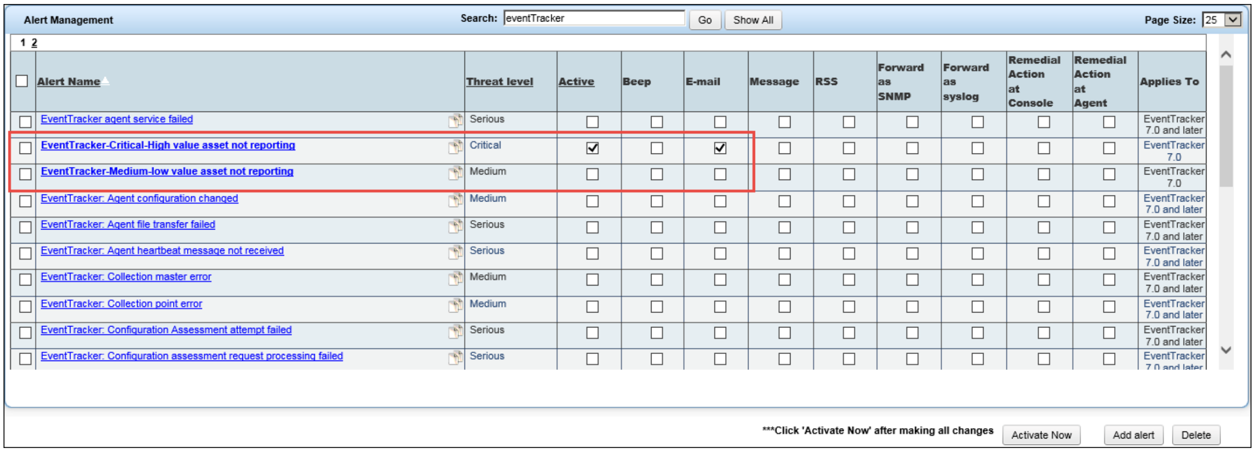
□	Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	*Security: User account unlocked	High	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Active Directory: Group policy changed	Serious	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Admin Interactive/Remote Interactive login failure	High	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Admin Interactive/Remote Interactive login success	High	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Administrative logon failure	High	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Administrative logon success	High	□	□	□	□	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
□	Altiris	Low	□	□	□	□	□	□	□	□	□	Altiris
□	ArrayOS SPX: Authentication failure	Critical	□	□	□	□	□	□	□	□	□	ArrayOS SPX 2000 Series 8.4.6 and later

***Click 'Activate Now' after making all changes

Figure 6

- Enter the Alert Name in the Search box.
- Click the **Go** button.

The two Alerts will be displayed.



Alert Management Search: eventTracker Go Show All Page Size: 25

1 2

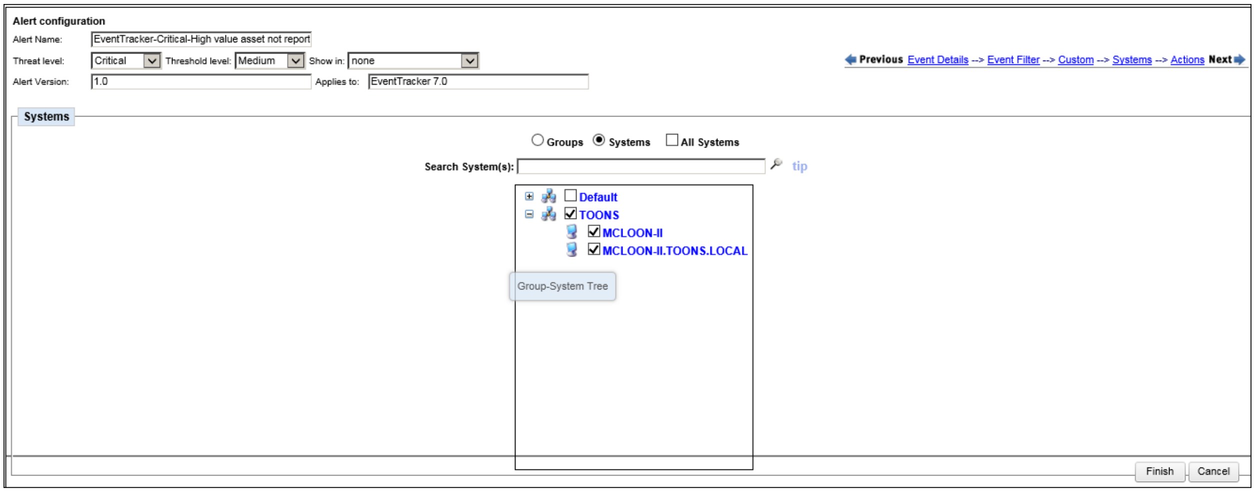
☐	Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
☐	EventTracker agent service failed	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	**EventTracker-Critical-High value asset not reporting**	Critical	☑	☐	☑	☐	☐	☐	☐	☐	☐	EventTracker 7.0
☐	**EventTracker-Medium-low value asset not reporting**	Medium	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0
☐	EventTracker: Agent configuration changed	Medium	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Agent file transfer failed	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Agent heartbeat message not received	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Collection master error	Medium	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Collection point error	Medium	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Configuration Assessment attempt failed	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later
☐	EventTracker: Configuration assessment request processing failed	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	EventTracker 7.0 and later

***Click 'Activate Now' after making all changes

Figure 7

NOTE: One Alert will not be Active by default. You need to enable it by clicking the checkbox.

- Click on the alert hyperlink to make changes in the Alert Configuration.
- Click the **System** hyperlink and select the Manager system as shown in the figure below:



Alert configuration

Alert Name: EventTracker-Critical-High value asset not report

Threat level: Critical Threshold level: Medium Show in: none

Alert Version: 1.0 Applies to: EventTracker 7.0

Previous Event Details --> Event Filter --> Custom --> Systems --> Actions Next

Systems

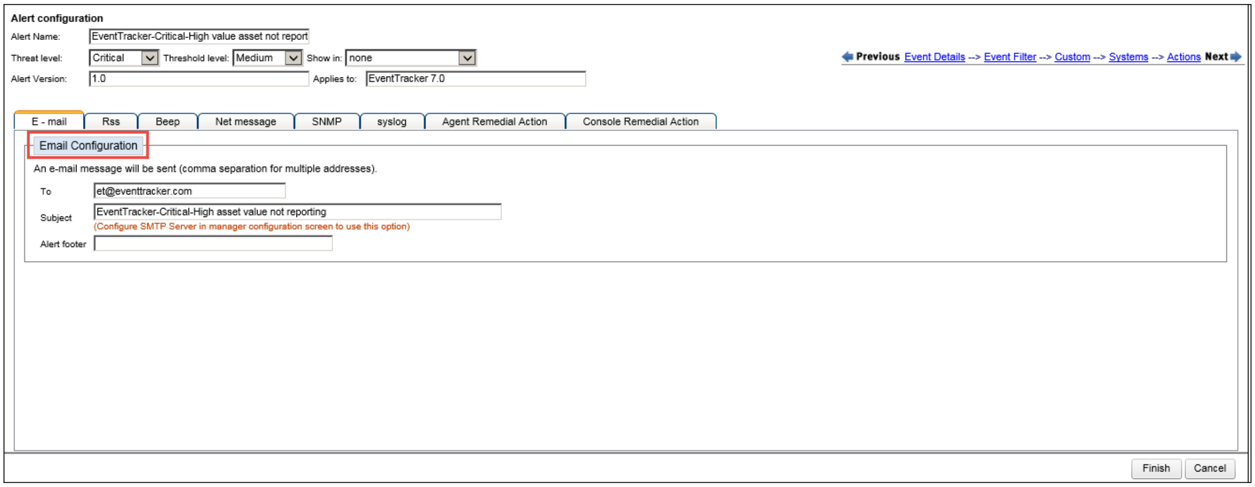
○ Groups ● Systems ☐ All Systems

Search System(s):

Figure 8

For assigning Action based on an Alert,

- Click the **Action** hyperlink and then click the **e-mail** option tab**.**
- Enter the required details.



Alert configuration

Alert Name: EventTracker-Critical-High value asset not report

Threat level: Critical Threshold level: Medium Show in: none

Alert Version: 1.0 Applies to: EventTracker 7.0

Email Configuration

An e-mail message will be sent (comma separation for multiple addresses).

To: et@eventtracker.com

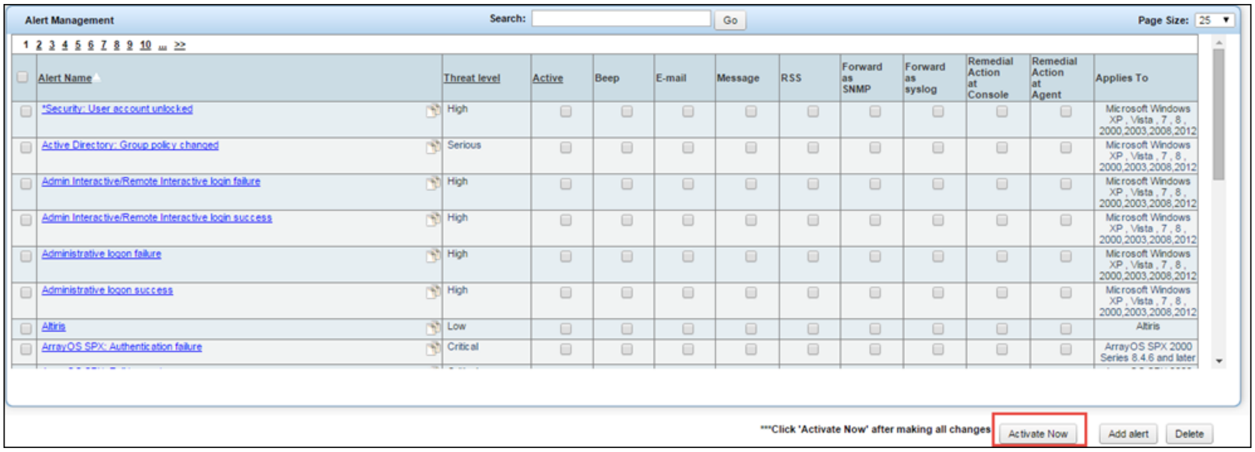
Subject: EventTracker-Critical-High asset value not reporting

(Configure SMTP Server in manager configuration screen to use this option)

Alert footer:

Figure 9

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



☐	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
☐	*Security: User account unlocked	High	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Active Directory: Group policy changed	Serious	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Admin Interactive/Remote Interactive login failure	High	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Admin Interactive/Remote Interactive login success	High	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Administrative logon failure	High	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Administrative logon success	High	☐	☐	☐	☐	☐	☐	☐	☐	☐	Microsoft Windows XP , Vista , 7 , 8 , 2000,2003,2008,2012
☐	Altiris	Low	☐	☐	☐	☐	☐	☐	☐	☐	☐	Altiris
☐	ArrayOS SPX: Authentication failure	Critical	☐	☐	☐	☐	☐	☐	☐	☐	☐	ArrayOS SPX 2000 Series 8.4.6 and later

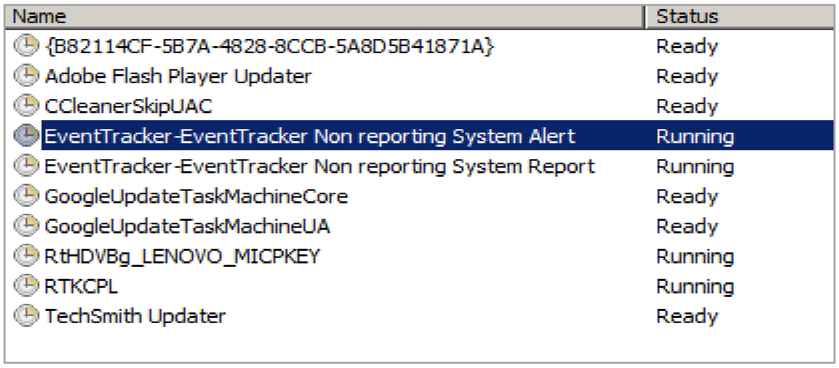
***Click 'Activate Now' after making all changes

Figure 10

Scheduling the scripts

Schedule Non-Reporting System Alert Script

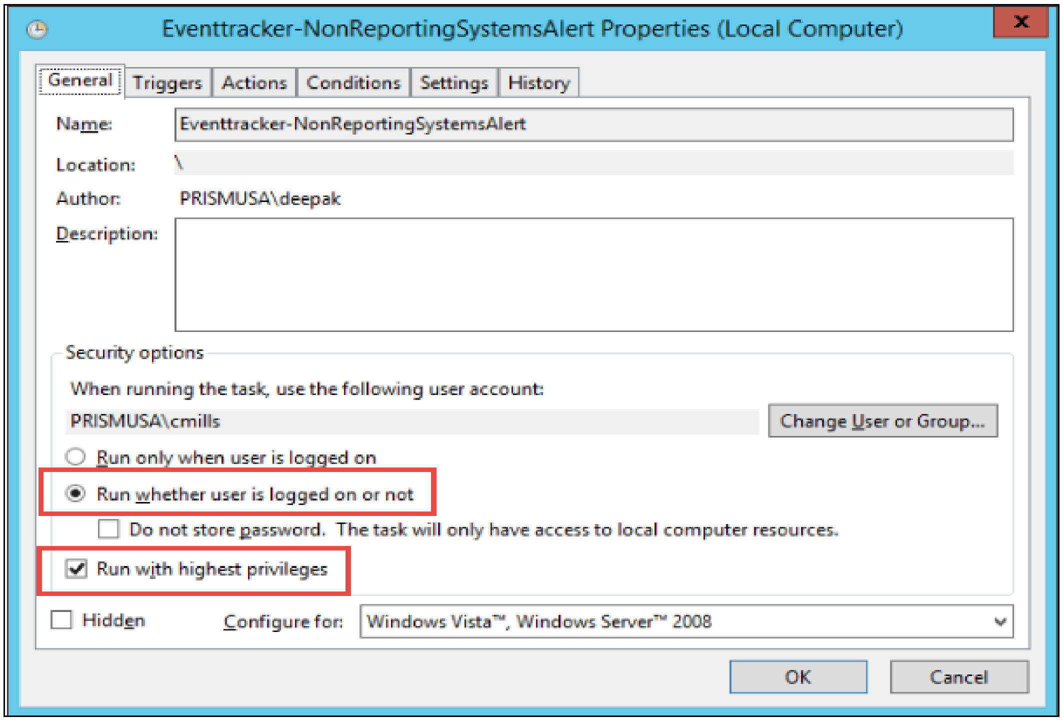
For scheduling, Non-Reporting System Alert Script, Go to **Task Scheduler** and create a new task with the same name.



Name	Status
{B82114CF-5B7A-4828-8CCB-5A8D5B41871A}	Ready
Adobe Flash Player Updater	Ready
CCleanerSkipUAC	Ready
EventTracker-EventTracker Non reporting System Alert	Running
EventTracker-EventTracker Non reporting System Report	Running
GoogleUpdateTaskMachineCore	Ready
GoogleUpdateTaskMachineUA	Ready
RtHDVBg_LENOVO_MICPKEY	Running
RTKCPL	Running
TechSmith Updater	Ready

Figure 11

Now, in the **General** tab, enter the name: EventTracker-EventTracker Non-reporting System Alert and select the check box as highlighted below in the figure:



Eventtracker-NonReportingSystemsAlert Properties (Local Computer)

Name: Eventtracker-NonReportingSystemsAlert

Location: \

Author: PRISMUSA\deepak

Description:

Security options

When running the task, use the following user account:

PRISMUSA\cmills

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

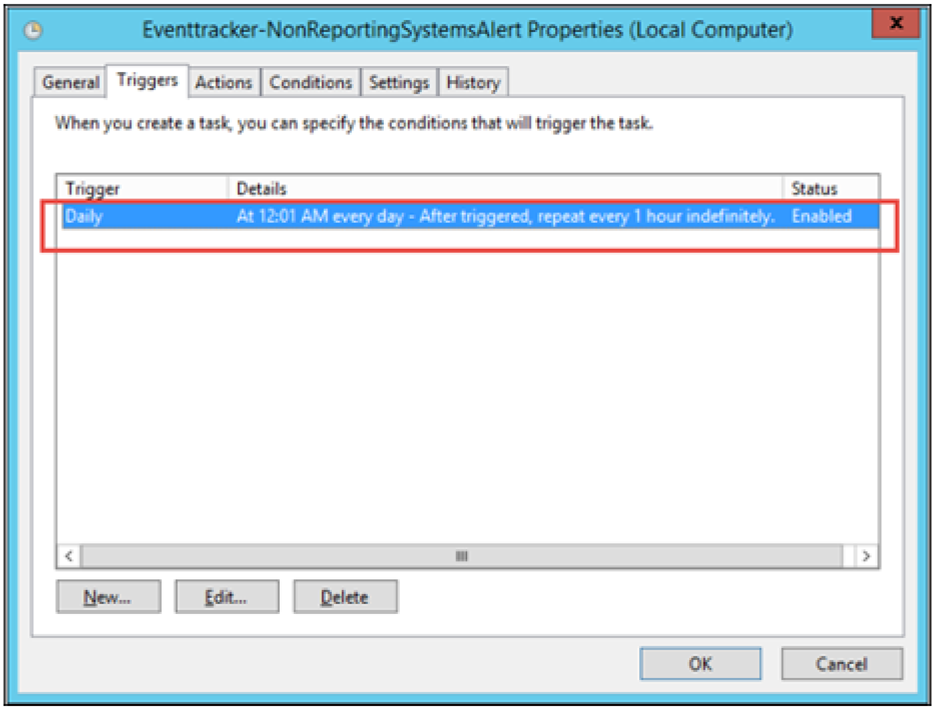
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

Figure 12

In the **Trigger** tab, select the time as 12:01 AM and the duration as “indefinitely”.

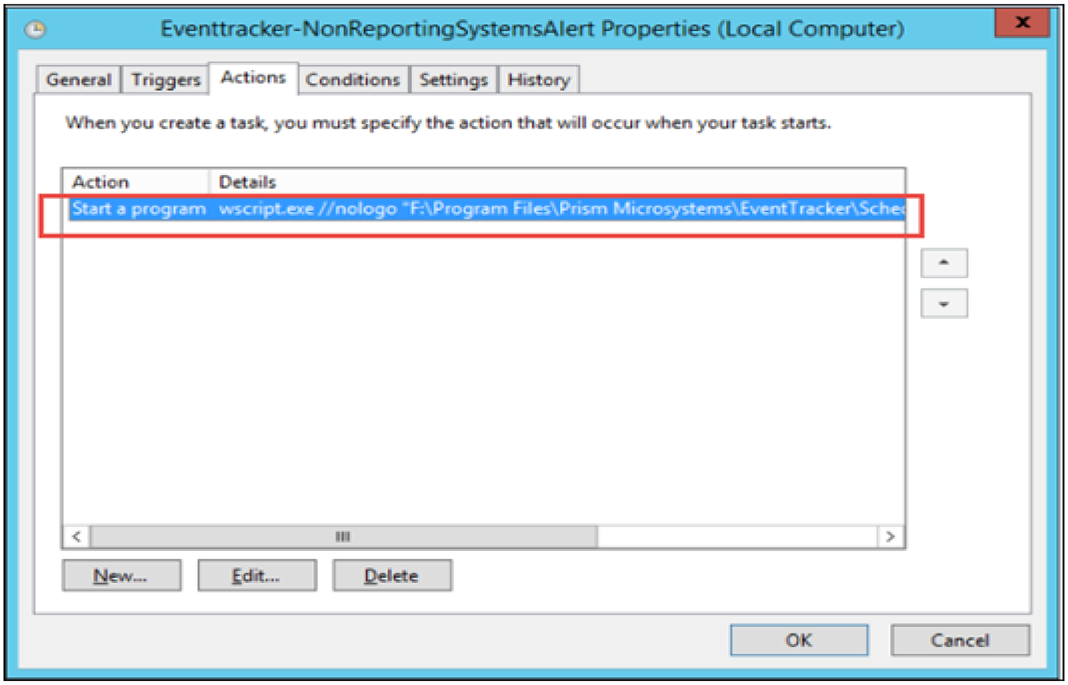


When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 12:01 AM every day - After triggered, repeat every 1 hour indefinitely.	Enabled

Figure 13

In the **Action** tab, browse the script file and click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

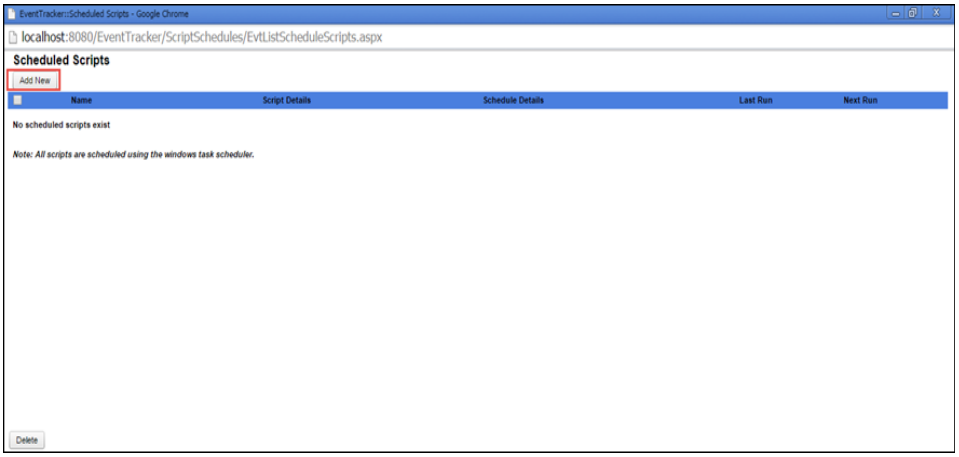
Action	Details
Start a program	wscript.exe //nologo "F:\Program Files\Prism Microsystems\EventTracker\Sche

Figure 14

Scheduling Non-Reporting System Report Script

- Go to **Tools** and select **Scheduled Scripts** from the drop-down list.

The Scheduled Scripts window displays.



EventTracker::Scheduled Scripts - Google Chrome

localhost:8080/EventTracker/ScriptSchedules/EvtListScheduleScripts.aspx

Scheduled Scripts

□	Name	Script Details	Schedule Details	Last Run	Next Run

No scheduled scripts exist

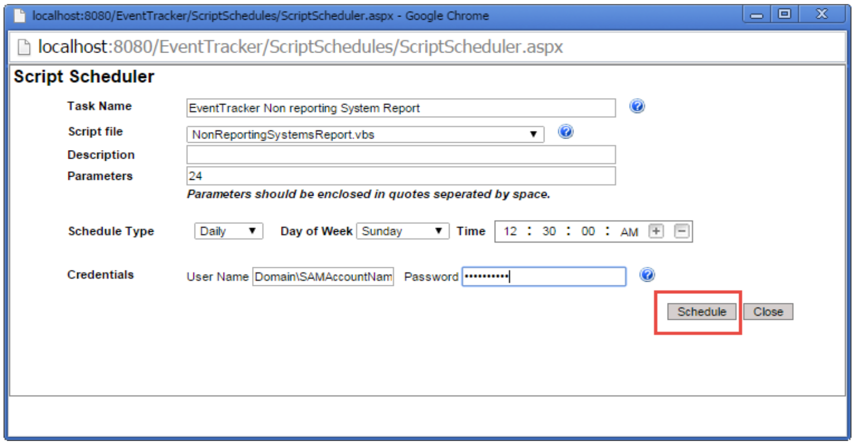
Note: All scripts are scheduled using the windows task scheduler.

Figure 15

- Click the **Add New** button.

The Script Scheduler page displays.

- Give the **Task Name** as “EventTracker Non-Reporting System Report” and select the **Script file** from the drop-down list.
- In the **Parameters** Field, put the duration of hours for which the report needs to be generated. Here, “24” is taken, i.e. 24 hours.
- Select the **Time** as: 12:30:00 AM.
- Put user credentials used for EventTracker configuration and click on **Schedule** button as shown in the figure below:



localhost:8080/EventTracker/ScriptSchedules/ScriptScheduler.aspx - Google Chrome

localhost:8080/EventTracker/ScriptSchedules/ScriptScheduler.aspx

Script Scheduler

Task Name: EventTracker Non reporting System Report

Script file: NonReportingSystemsReport.vbs

Description:

Parameters: 24

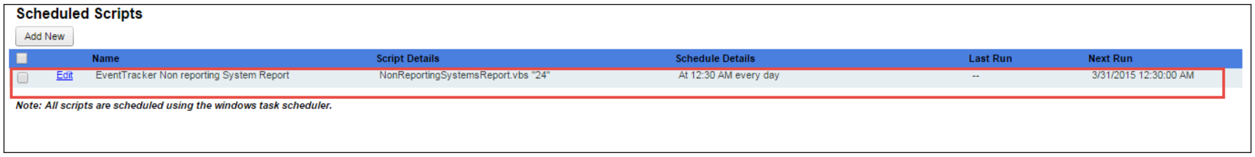
Parameters should be enclosed in quotes seperated by space.

Schedule Type: Daily Day of Week: Sunday Time: 12 : 30 : 00 : AM

Credentials: User Name: Domain\SAMAccountNam Password: ••••••••••

Figure 16

It gets displayed in the **Scheduled Script** window.



Scheduled Scripts

□		Name	Script Details	Schedule Details	Last Run	Next Run
□	Edit	EventTracker Non reporting System Report	NonReportingSystemsReport.vbs "24"	At 12:30 AM every day	--	3/31/2015 12:30:00 AM

Note: All scripts are scheduled using the windows task scheduler.

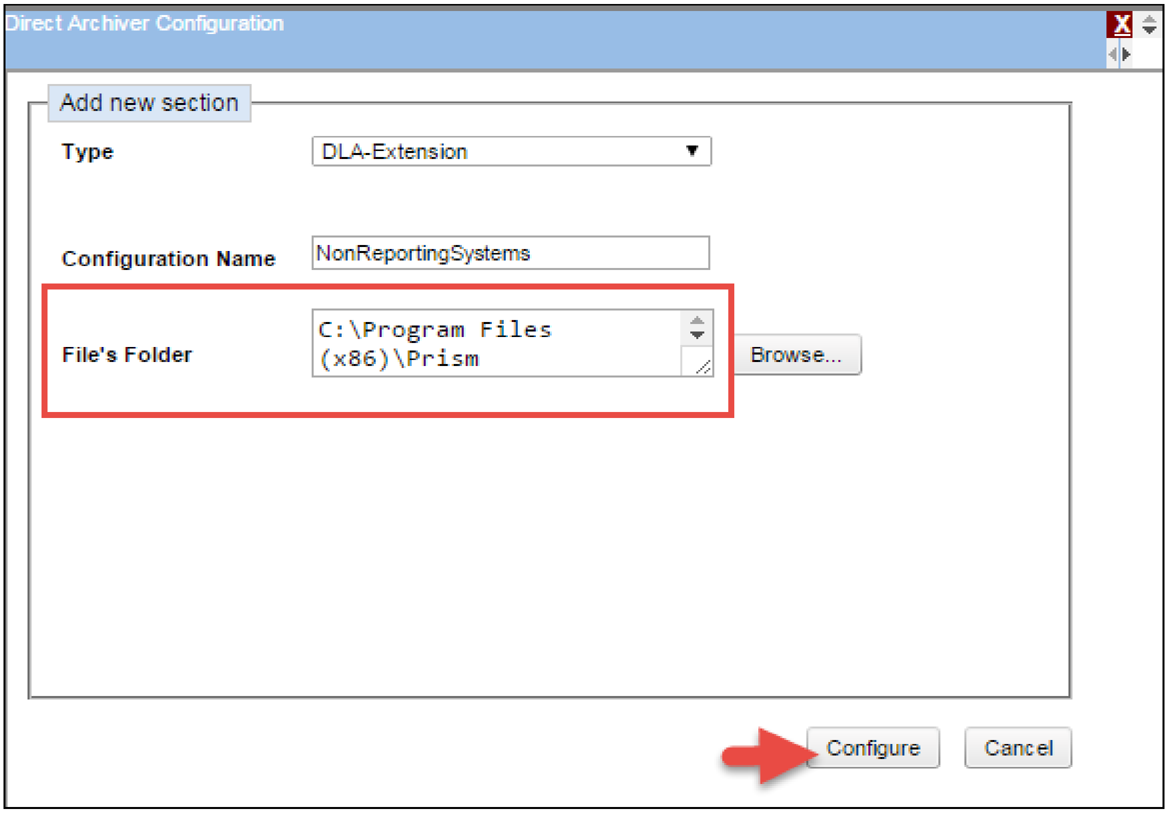
Figure 17

Configure DLA Extension for the Report

- Go to **Admin** and select **Manager** from the drop-down list.
- Select the **Direct Log Archiver/ Net Flow Receiver** and click the **Add** button.

The Direct Archiver Configuration page displays.

- In the **Type** field, select DLA Extension from the drop down list
- Give the Configuration name as **NonReportingSystems.**
- Browse the file's folder and click on the **Configure** button as shown in the figure below:



Direct Archiver Configuration

Add new section

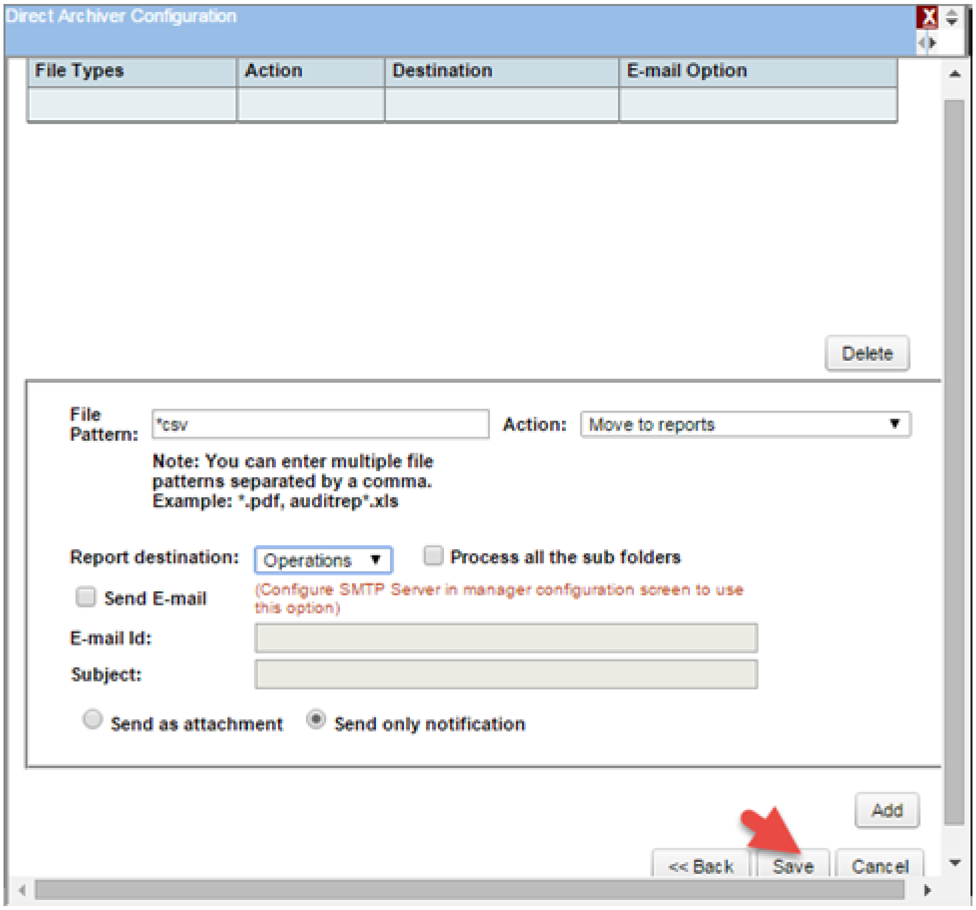
Type: DLA-Extension

Configuration Name: NonReportingSystems

File's Folder: C:\Program Files (x86)\Prism

Figure 18

- In the File Pattern, enter *csv and in the Action field, select ‘Move to reports’ from the drop-down box.
- In the **Report Destination** field, select ‘Operations’ and click on **Save** as shown below:



Direct Archiver Configuration

File Types	Action	Destination	E-mail Option

File Pattern: *csv

Action: Move to reports

Note: You can enter multiple file patterns separated by a comma. Example: *.pdf, auditrep*.xls

Report destination: Operations

□ Process all the sub folders

□ Send E-mail

(Configure SMTP Server in manager configuration screen to use this option)

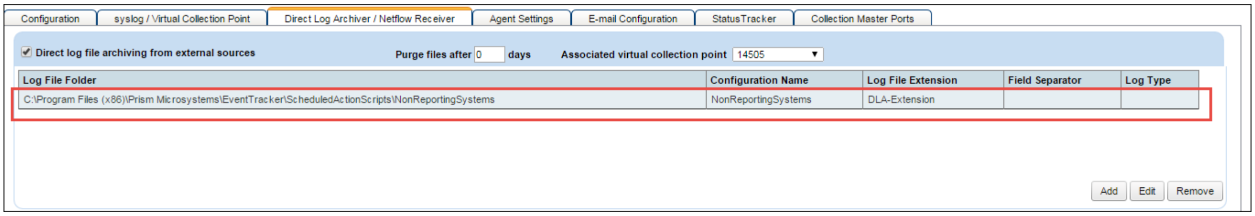
E-mail Id:

Subject:

○ Send as attachment ● Send only notification

Figure 19

It gets listed as shown in the figure below:



☑ Direct log file archiving from external sources

Purge files after 0 days

Associated virtual collection point 14505

Log File Folder	Configuration Name	Log File Extension	Field Separator	Log Type
C:\Program Files (x86)\Prism Microsystems\EventTracker\ScheduledActionScripts\NonReportingSystems	NonReportingSystems	DLA-Extension		

Figure 20

Verify Reports

For verifying the reports,

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

In the Graph page, the report gets displayed.

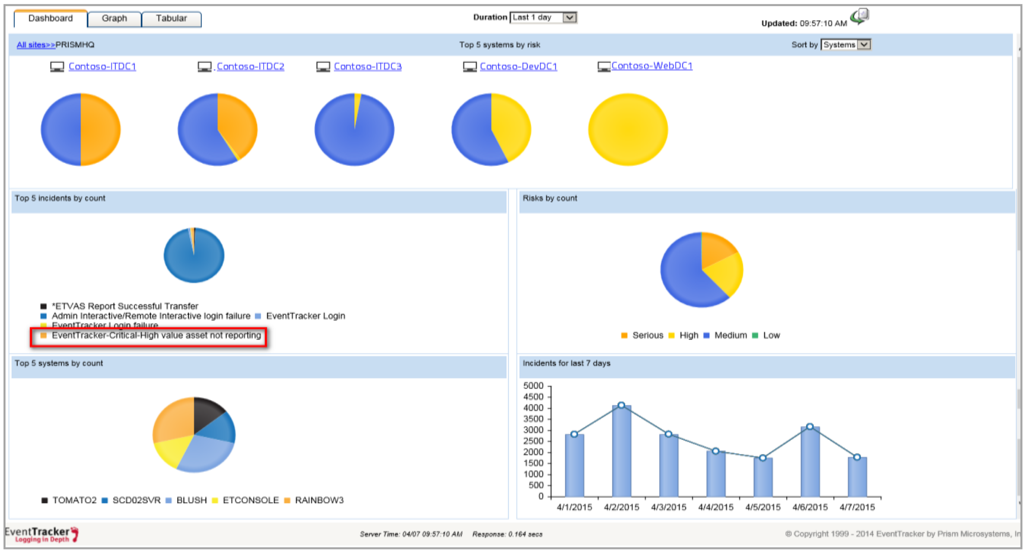
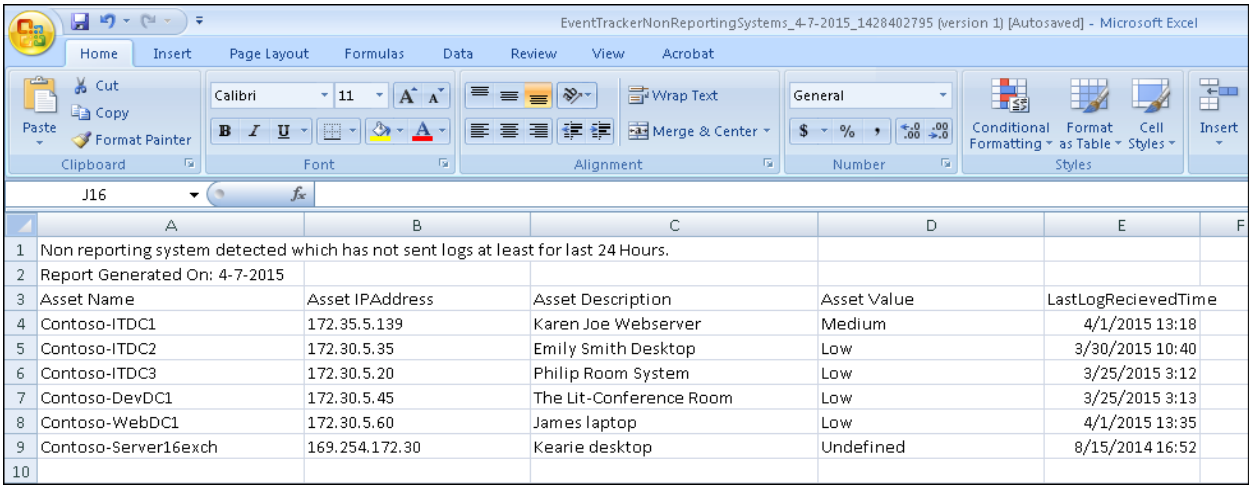


Figure 21

- For generating sample report based on the **EventTracker: Non-reporting systems detected, go to Report Dashboard and click on the report.**

The report gets exported as excel file as shown below:



Non reporting system detected which has not sent logs at least for last 24 Hours.

Report Generated On: 4-7-2015

Asset Name	Asset IPAddress	Asset Description	Asset Value	LastLogRecievedTime
Contoso-ITDC1	172.35.5.139	Karen Joe Webserver	Medium	4/1/2015 13:18
Contoso-ITDC2	172.30.5.35	Emily Smith Desktop	Low	3/30/2015 10:40
Contoso-ITDC3	172.30.5.20	Philip Room System	Low	3/25/2015 3:12
Contoso-DevDC1	172.30.5.45	The Lit-Conference Room	Low	3/25/2015 3:13
Contoso-WebDC1	172.30.5.60	James laptop	Low	4/1/2015 13:35
Contoso-Server16exch	169.254.172.30	Kearie desktop	Undefined	8/15/2014 16:52

Figure 22