

Enhancement in LFM to consider the  
date and time mentioned in the log file  
*EventTracker Enterprise*

## Enhancement in LFM to consider the date and time mentioned in the log file

---

**Update:** ET82U16-022/ ET82UA16-022

**Abstract:** This update will offer Enhancement in LFM to consider the date and time mentioned in the log file.

### Who should read this document?

Customers who use v 8.2 Build 14.

### Why to use this Update?

The earlier Agent LFM configuration always considered current system date and time after parsing the records. To overcome this, we have provided standard and custom date and time formats to configure Agent LFM.

Now the configured files in the Agent LFM will be parsed as per the selected date and time formats.

*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.*

*© 2016 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

Process to be followed after applying the Update: ET82U16-022 .....	3
For Standard Date & Time format.....	5
For Custom Date & Time format.....	10
For EPOCH Date & Time format.....	14

# Process to be followed after applying the Update

## **\*\*Important Note:**

Before configuring a file in agent LFM, please open the file and check which date and time format (Standard or Custom) will apply.

1. New Enhancement in LFM, date and time formats are not applicable for below mentioned log files.
  - Check Point
  - VMware
  - syslog
  - EVT
  - IISMSID (Current date-time applicable)
  - TEXTWORD (Current date-time applicable)
  
2. New Enhancement in LFM, Custom and Current date-time formats are applicable only for below mentioned log files (Standard date-time formats are not applicable).
  - IISW3C
  - NCSA
  - BIN
  - URLSCAN
  - HTTPERR
  - W3C
  - IIS
  
3. New Enhancement in LFM, Standard, Custom and Current date-time formats are applicable for below mentioned the log files.
  - TEXTLINE
  - MULTILINE
  - CSV
  - XML
  - LOG4XML
  - JSON

## Enhancement in LFM to consider the date and time mentioned in the log file

---

- Open **EventTracker Control Panel**.
- Double-click **EventTracker Agent Configuration**.
- Click **LogFile Monitor** tab.
- Check the **Logfile Monitor** option and click **Add File Name**.

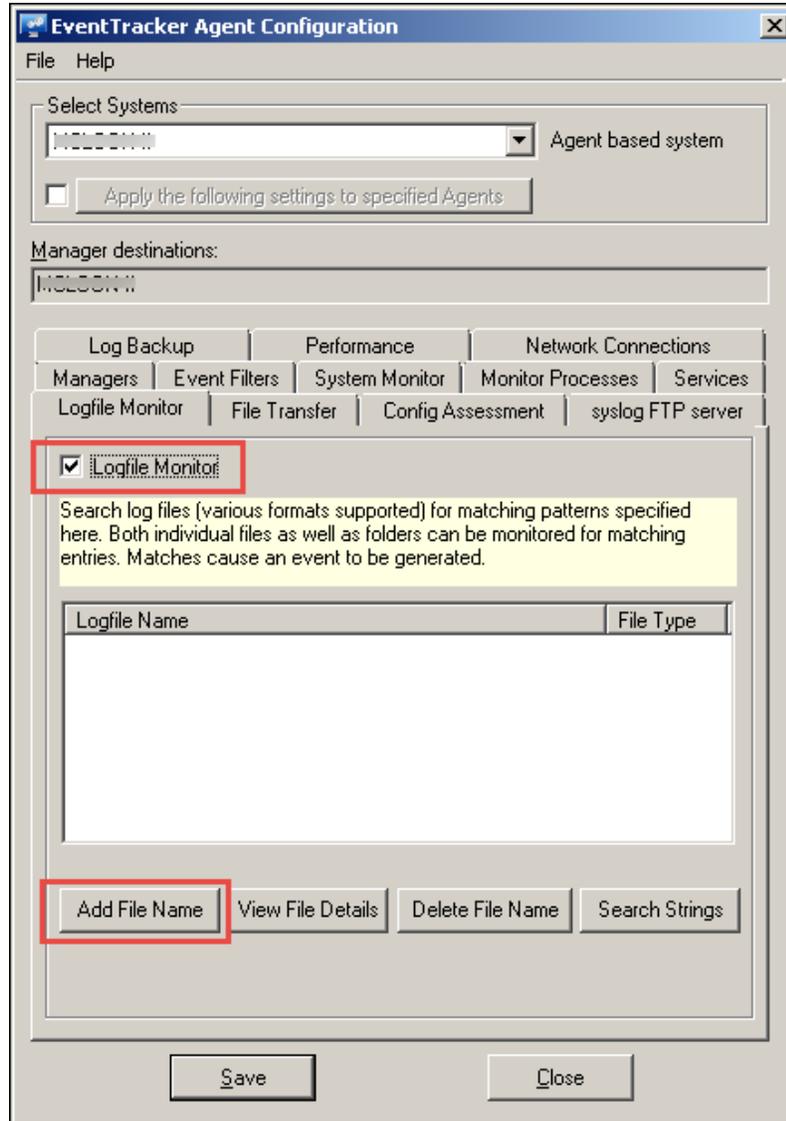


Figure: 1

The **Enter File Name** window displays.

- Select the file type from the drop down option.

## For Standard Date & Time format

The below example will provide details of how to configure standard date and time formats for CSV type. For other types also the same standard date and time format will apply.

- We have selected **File Type** as **CSV**.

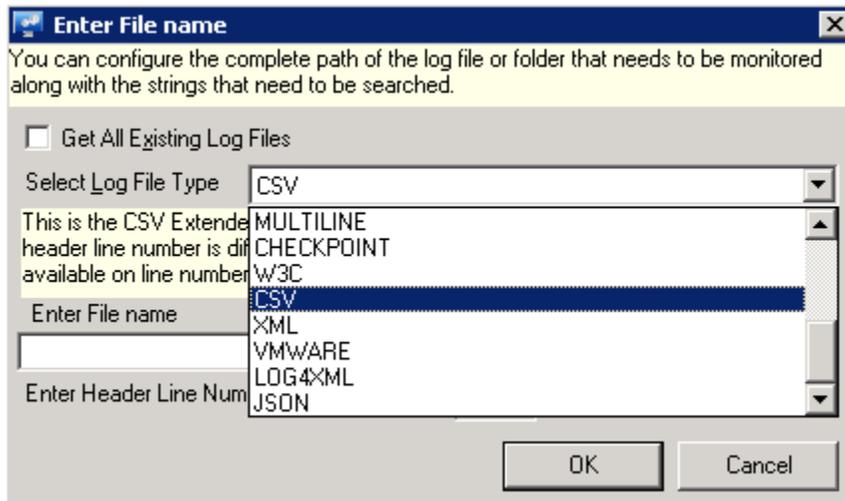


Figure: 2

- Browse the file path by clicking  and click the **OK** button.

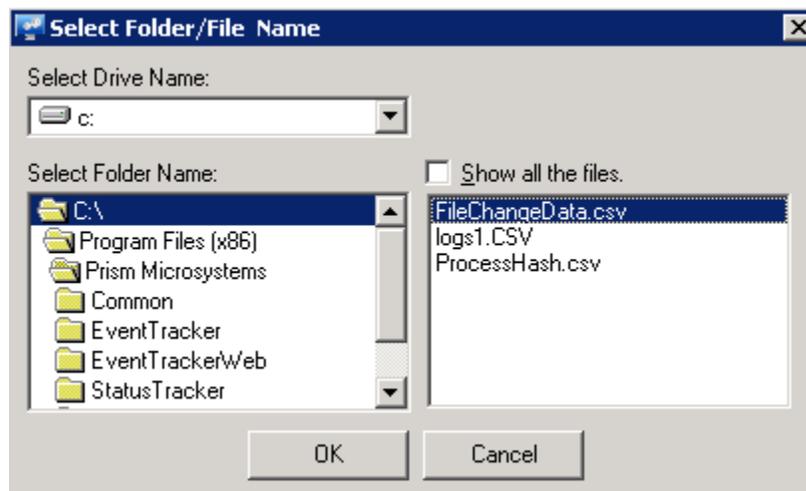


Figure: 3

The selected file path gets displayed. Click **OK**.

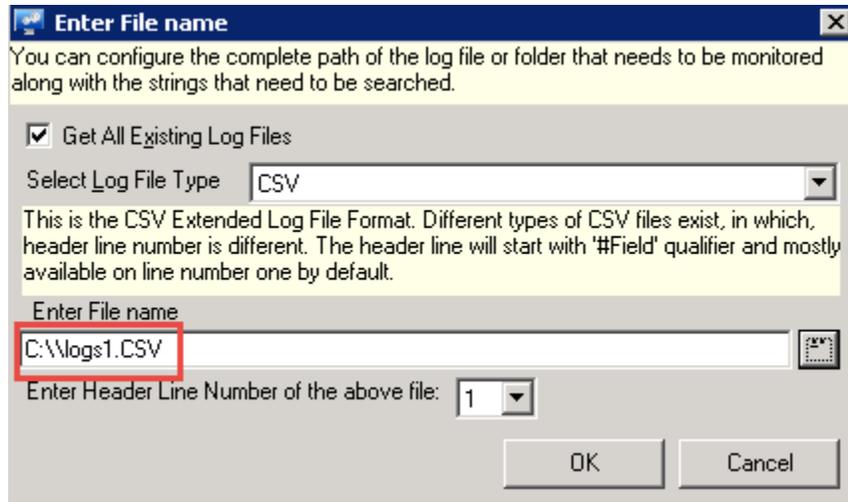


Figure: 4

The below message gets displayed. Click **Yes**.

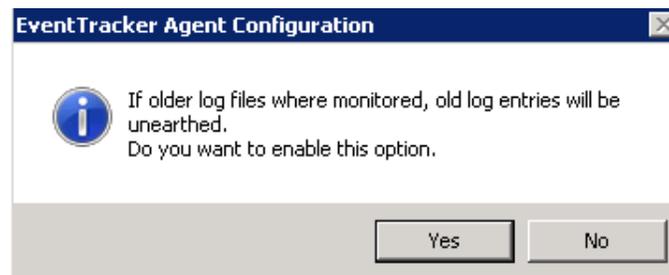


Figure: 5

- In the Search String window, click the **Add String** option.

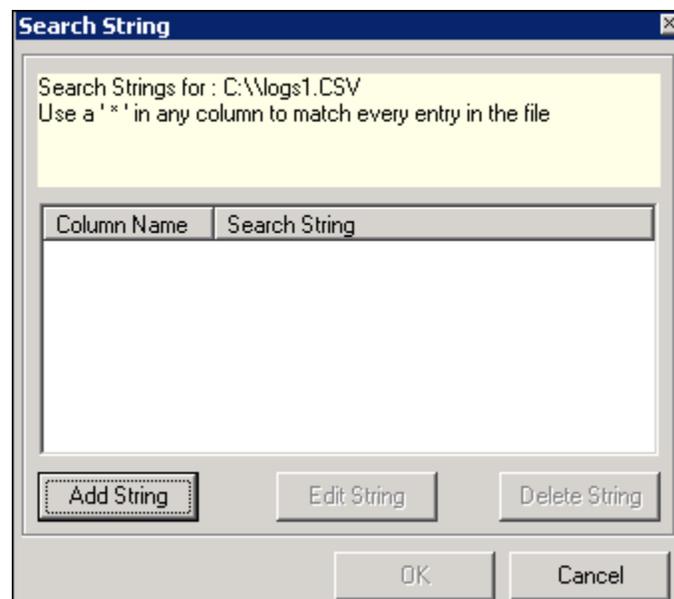


Figure: 6

The **Enter Search String** window displays.

**NOTE:** Check the **Current Date Time** option, if you want to parse the records with the present system's date and time.

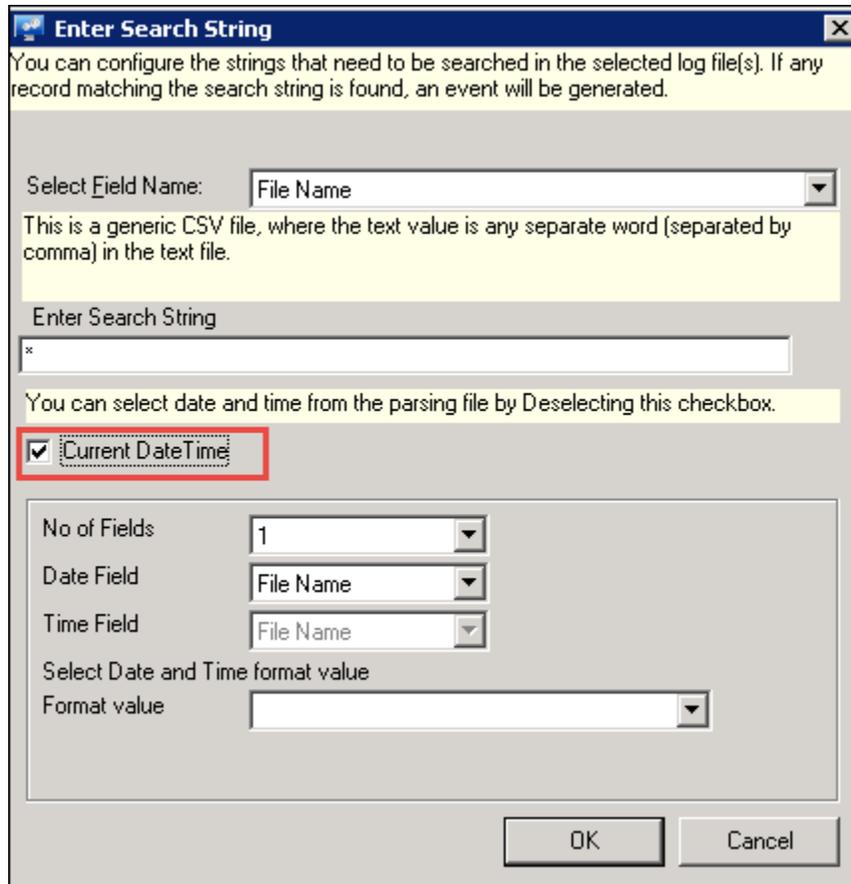


Figure: 7

OR,

- Select the No. of fields 1 or 2 based on the log file.
- Enter the Date Field and Time Field from the dropdown list.
- Select the Format Value from the available options which matches the configured file date and time format.

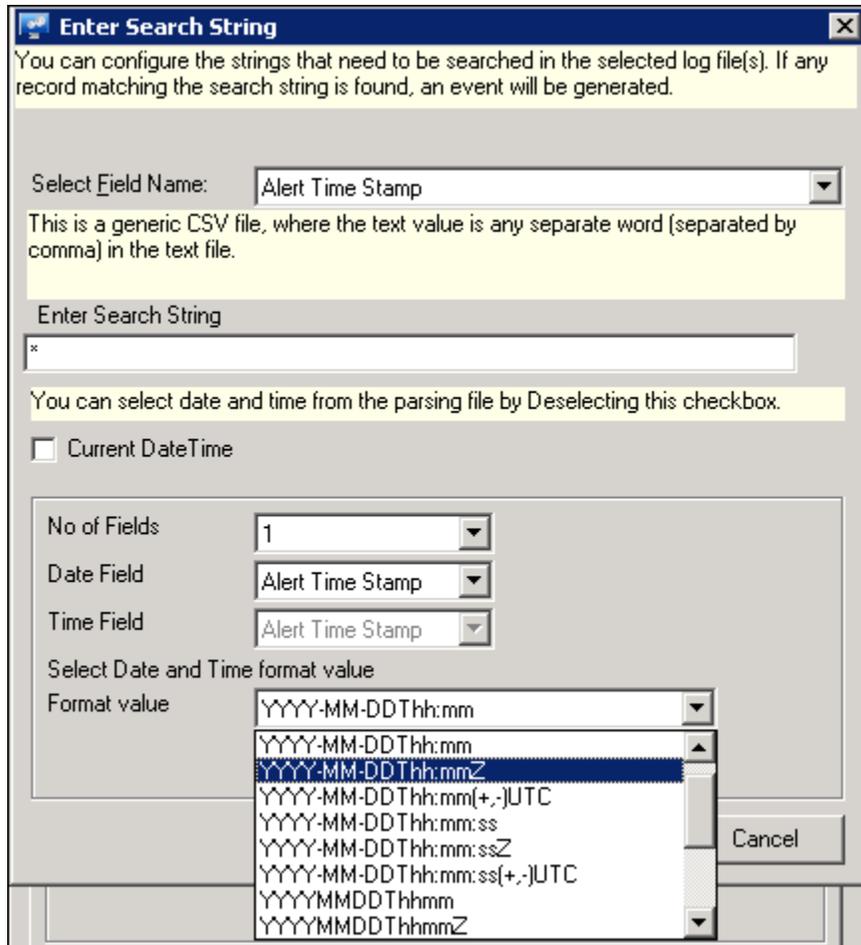


Figure: 8

- Click OK.

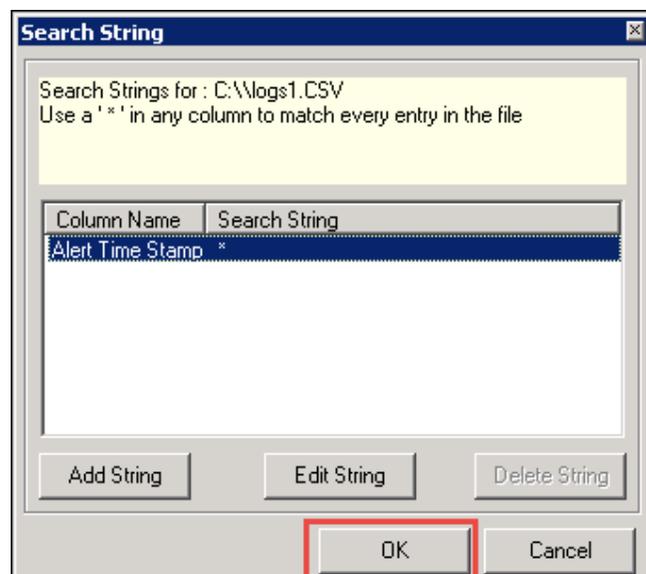


Figure: 9

## Enhancement in LFM to consider the date and time mentioned in the log file

---

The log file gets added and is displayed.

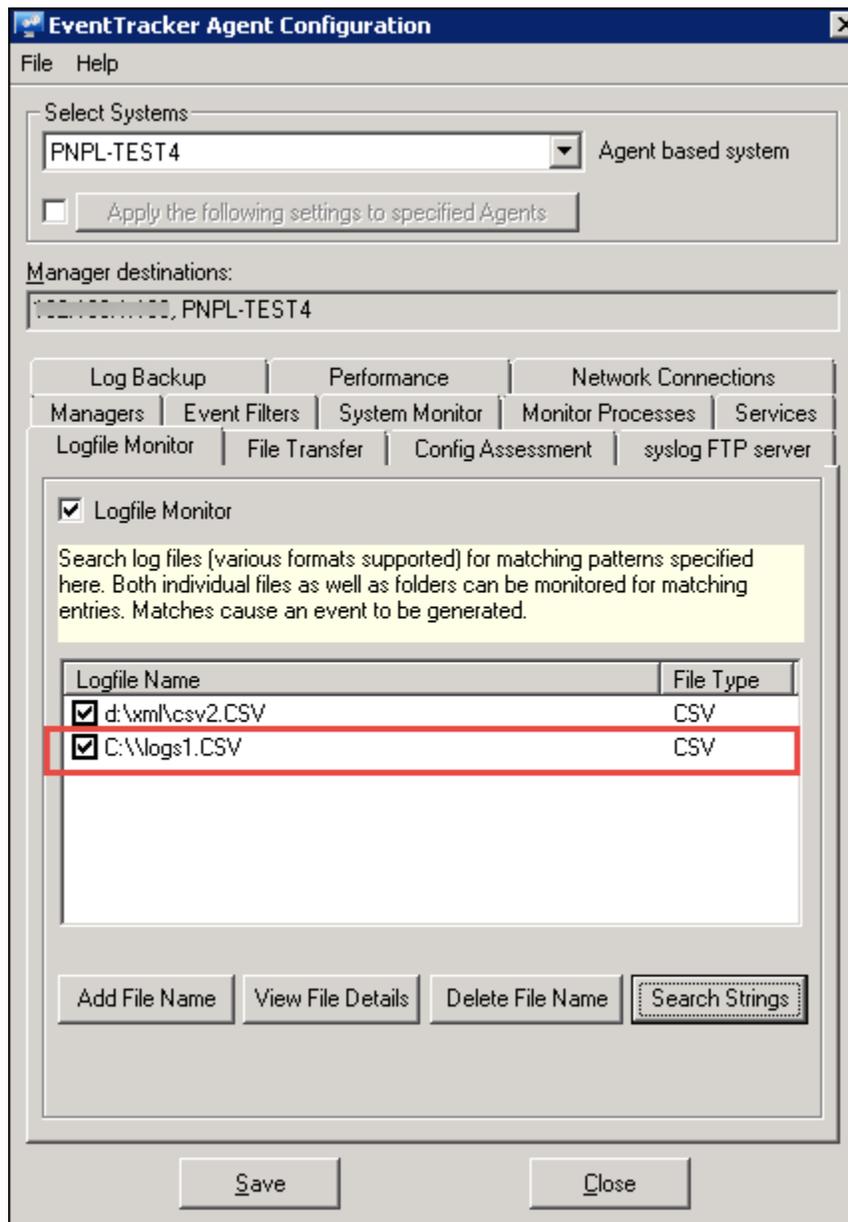


Figure: 10

- To save the changes click **Save** and then close the EventTracker Agent configuration window.

## For Custom Date & Time format

The below example will provide details of how to configure custom date and time formats for **IIS** type. For log types **IISW3C**, **NCSA**, **BIN**, **URLSCAN**, **HTTPERR**, **W3C** also the same custom date and time format will apply.

- Select the **IIS** option from the dropdown list.

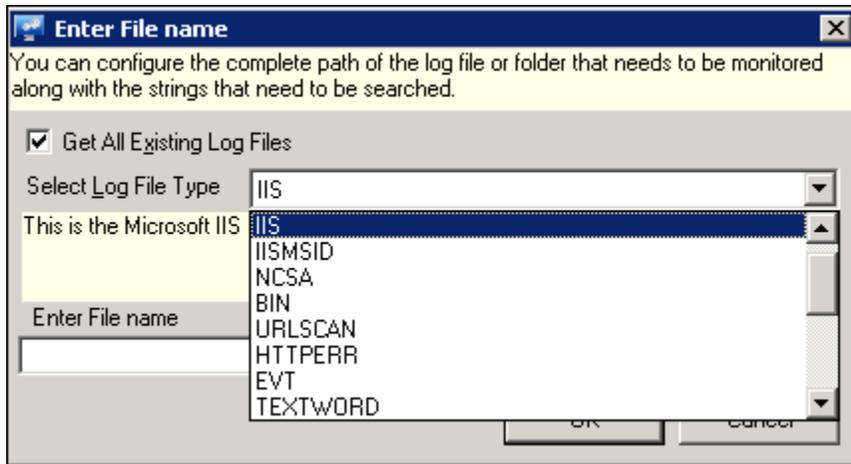


Figure: 11

- Browse the file path, select the file and click **OK**.

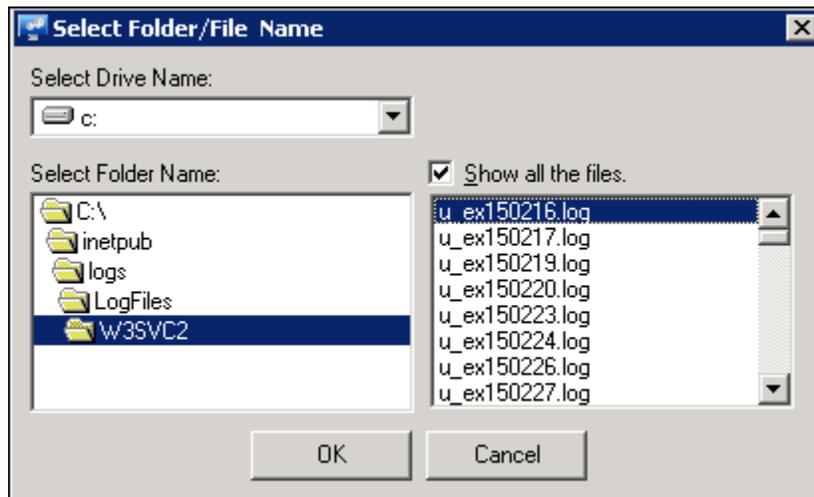


Figure: 12

- The file path gets displayed. Click **OK**.

Enhancement in LFM to consider the date and time mentioned in the log file

---

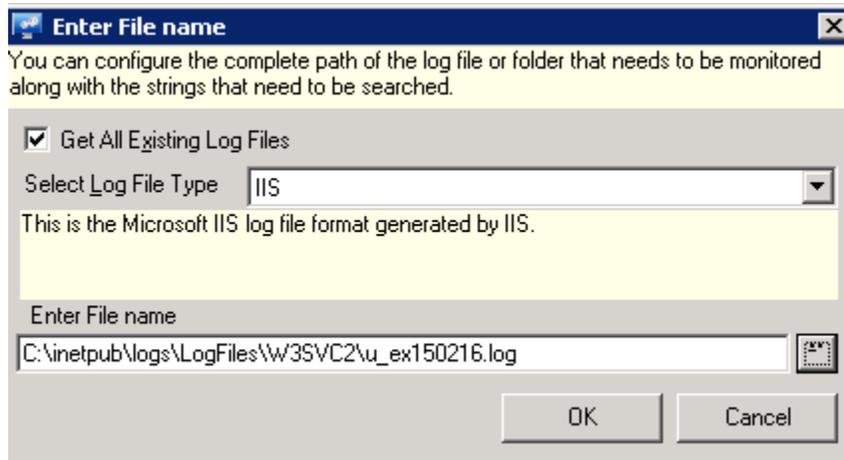


Figure: 13

EventTracker Agent configuration displays the below message. Click **Yes**.

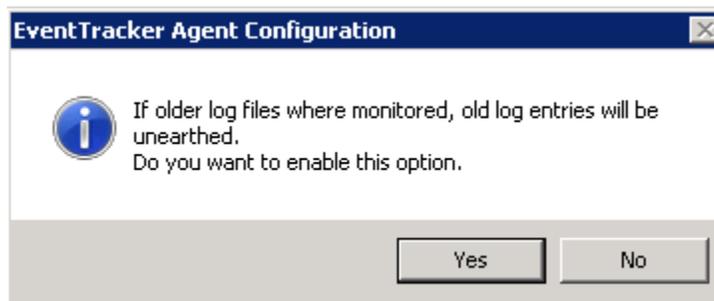


Figure: 14

The search string window displays. Click **Add String** button.

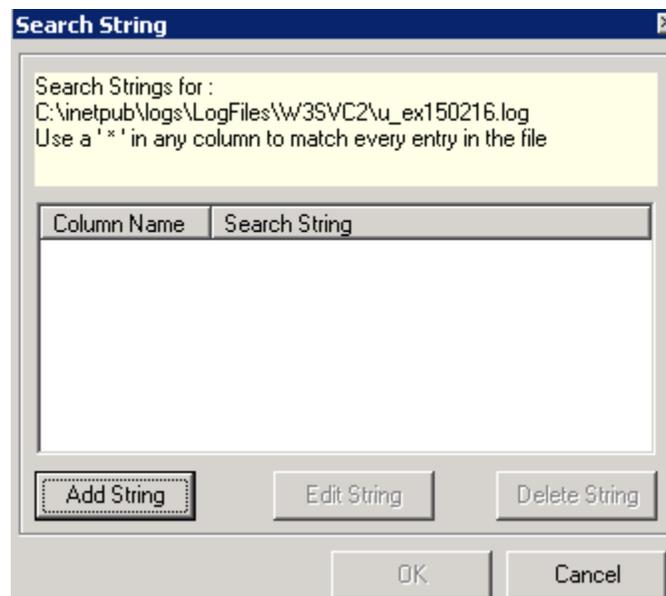


Figure: 15

The **Enter Search String** window gets displayed.

- Select the number of fields.
- Select the Format Value '**Custom** 'from the available options and enter the custom format value which matches the configured file date and time format.

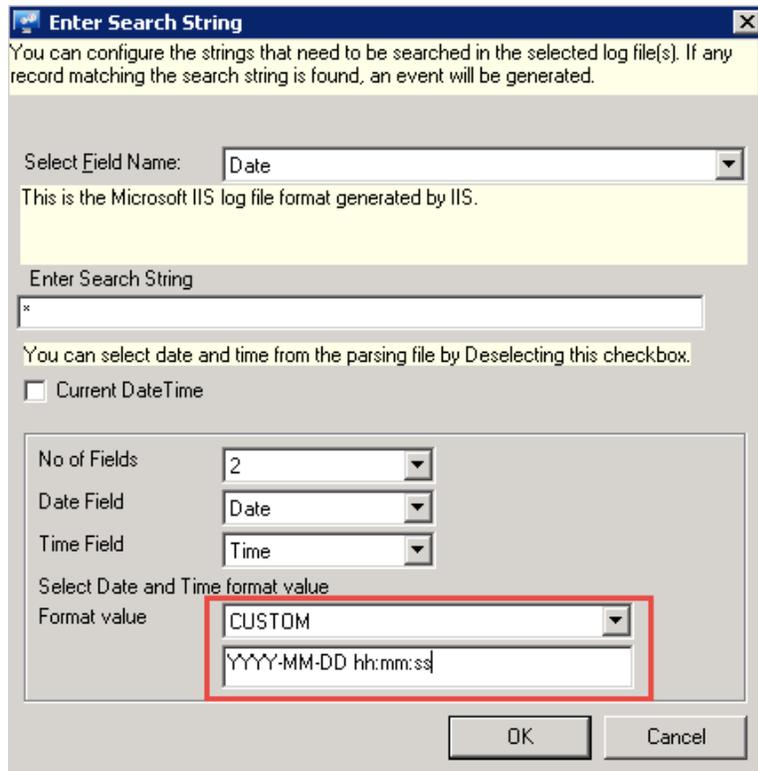


Figure: 16

- Click **OK**.
- Select the search string and click the **OK** button.

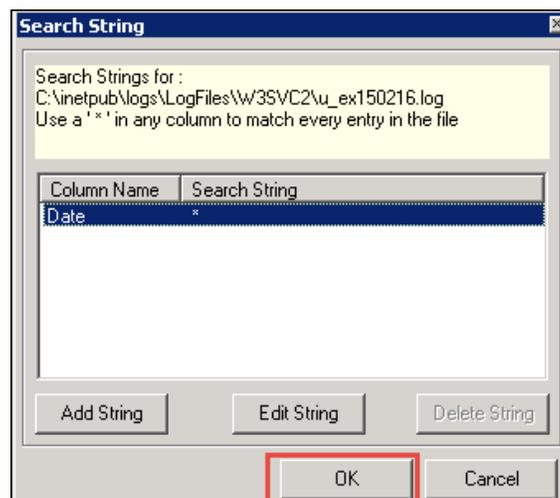


Figure: 17

- The logfile gets added and is displayed.

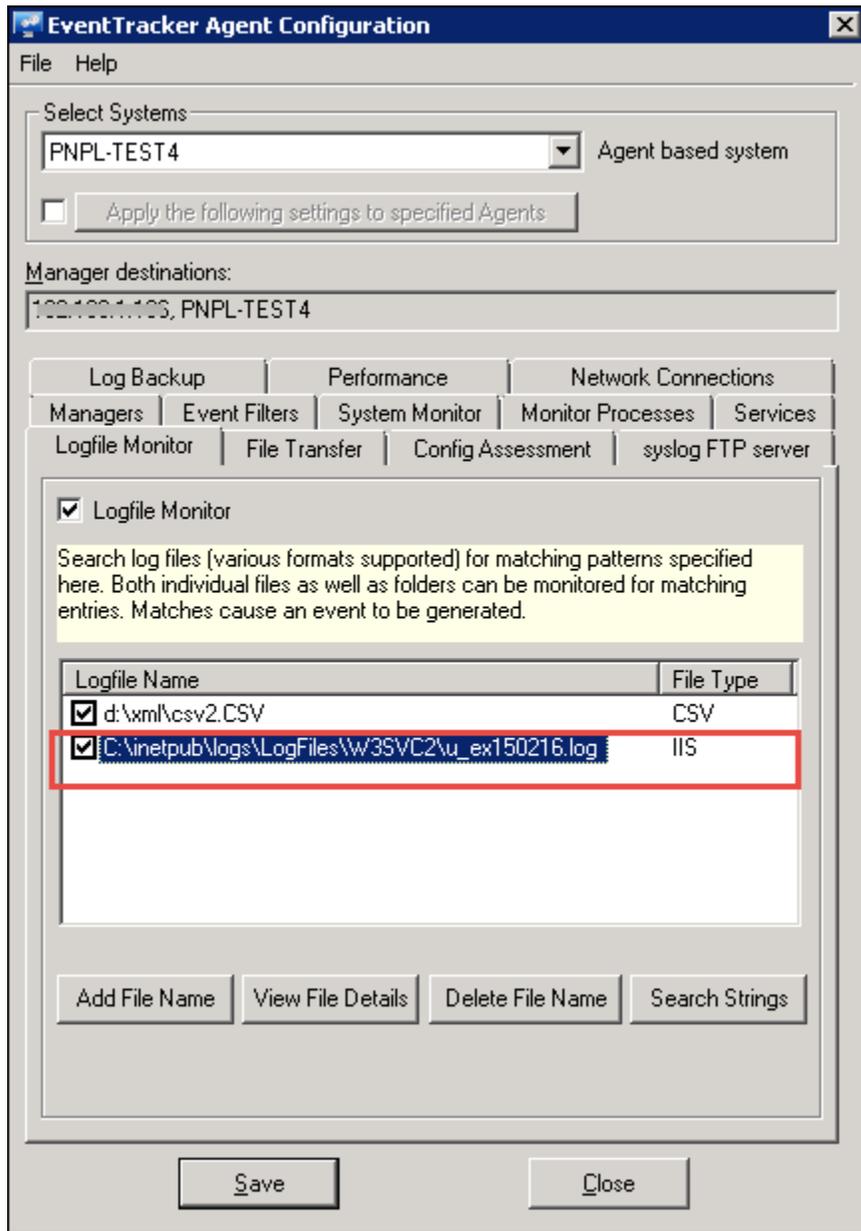


Figure: 18

- **Save** the changes and **Close** the EventTracker Configuration window.

## For EPOCH Date & Time format

The below example will provide details of how to configure EPOCH date and time formats for XML type. The **EPOCH** format will apply only for **CSV, XML, LOG4XML, JSON** logfile type.

- Select the **XML** option from the dropdown list.

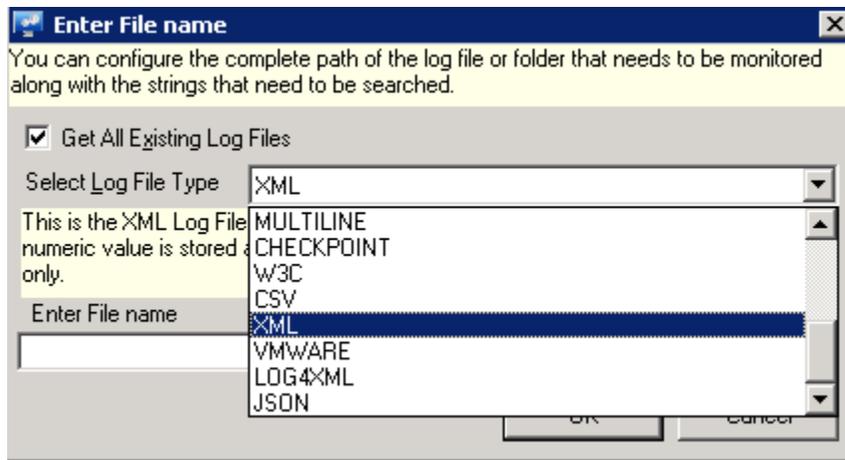


Figure: 19

- Browse the file path, select the file and click **OK**.

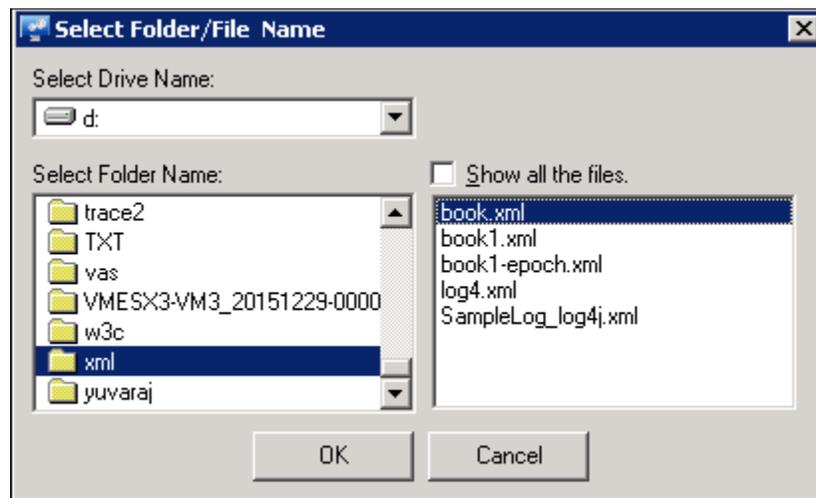


Figure: 20

- The file path gets displayed. Click **OK**.

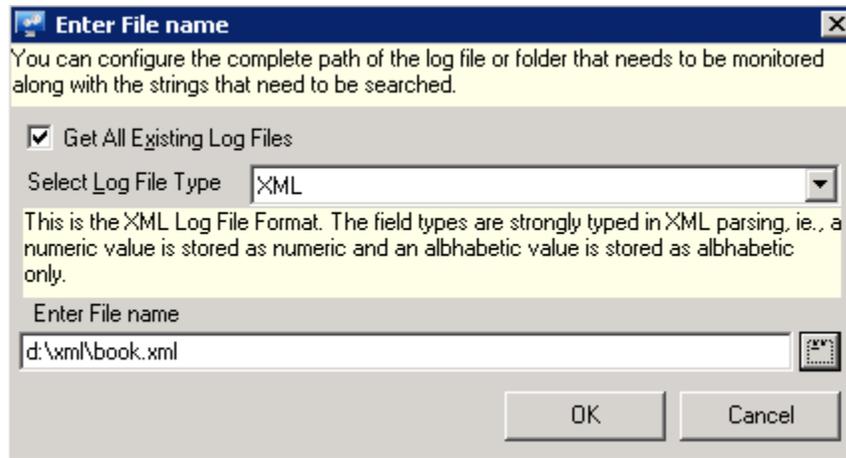


Figure: 21

EventTracker Agent configuration displays the below message. Click **Yes**.

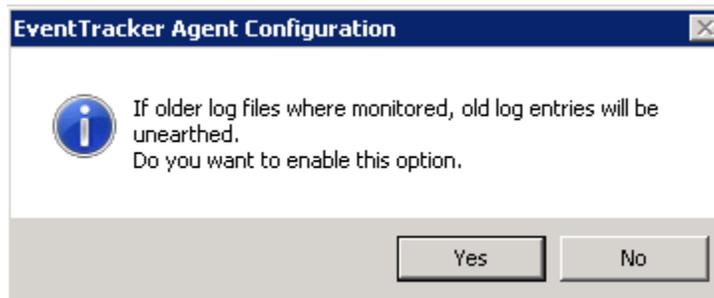


Figure: 22

The search string window displays. Click **Add String** button.

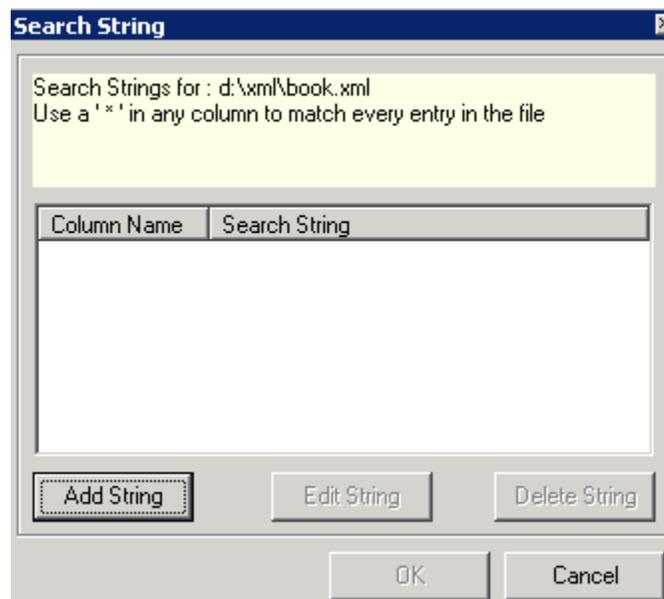


Figure: 23

The **Enter Search String** window gets displayed.

- Select the number of fields.
- Select the Format Value 'EPOCH' format from the available options.

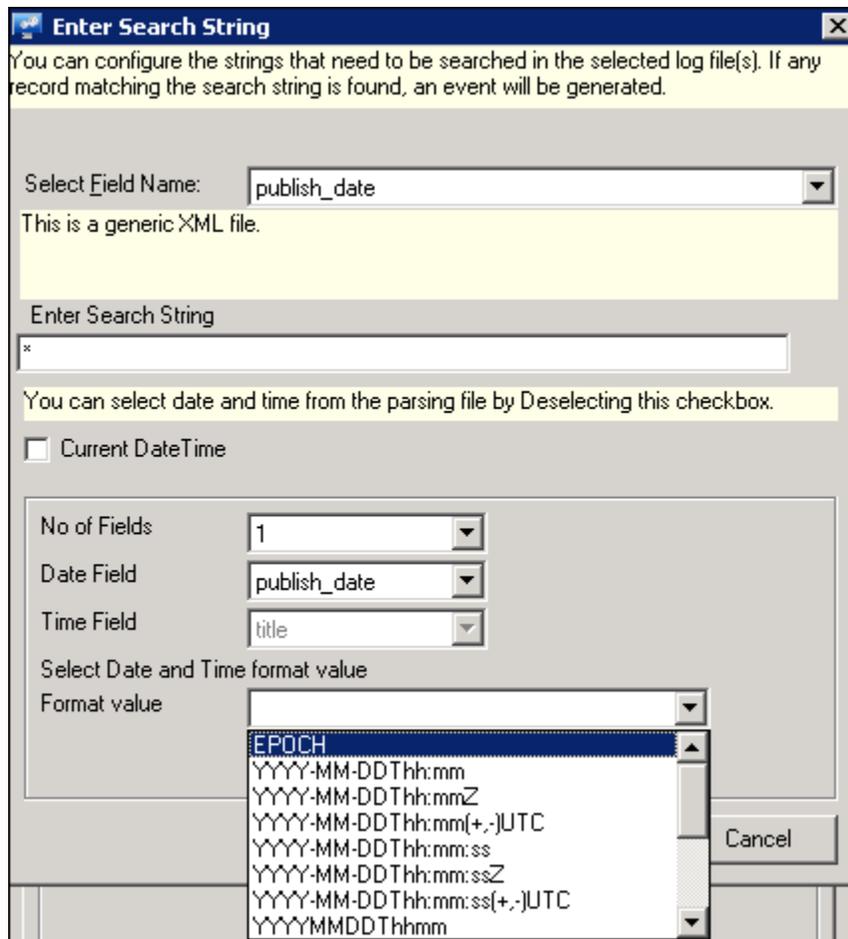


Figure: 24

- Click **OK**.
- Select the search string.

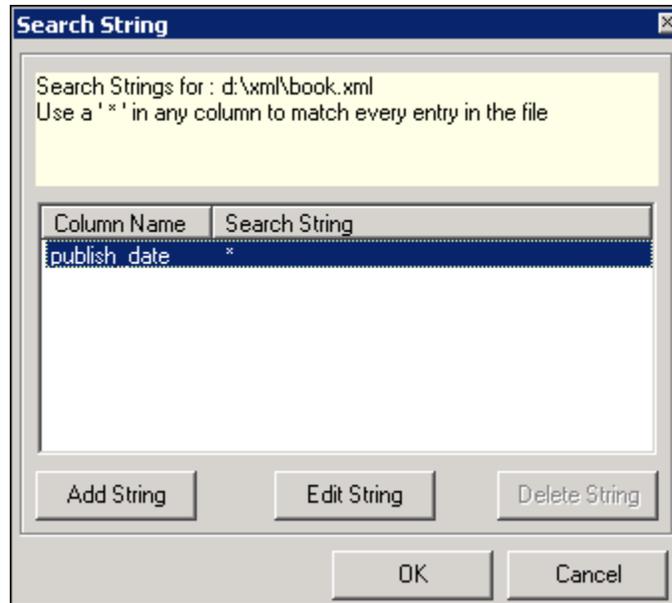


Figure: 25

- To **'Edit'** the search string, click the **Edit String** button.
- To **'Delete'** the search string, click the **Delete String** button.
- Click the **OK** button.

The logfile gets added and is displayed.

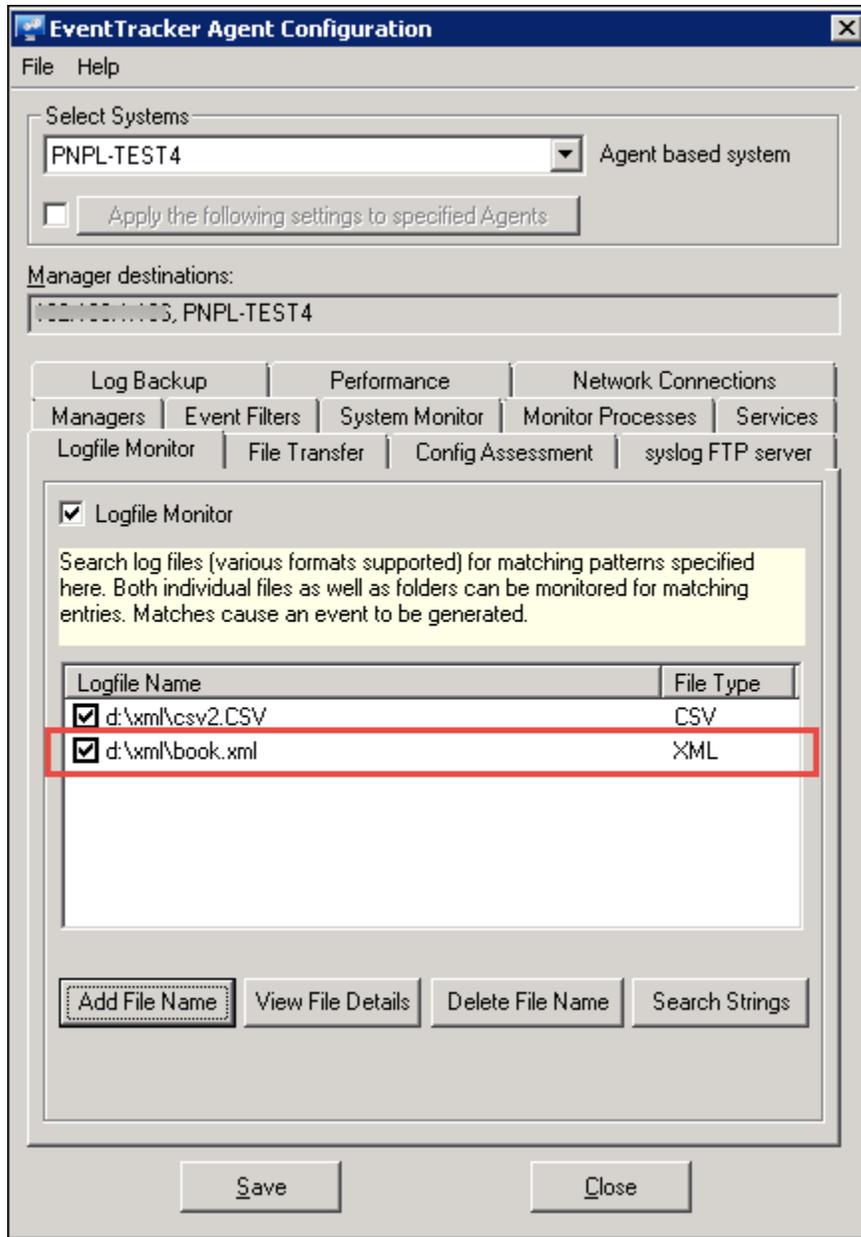


Figure: 26

- **Save** the changes and **Close** the EventTracker Configuration window.

To view the file details, click the **View File Details** button.

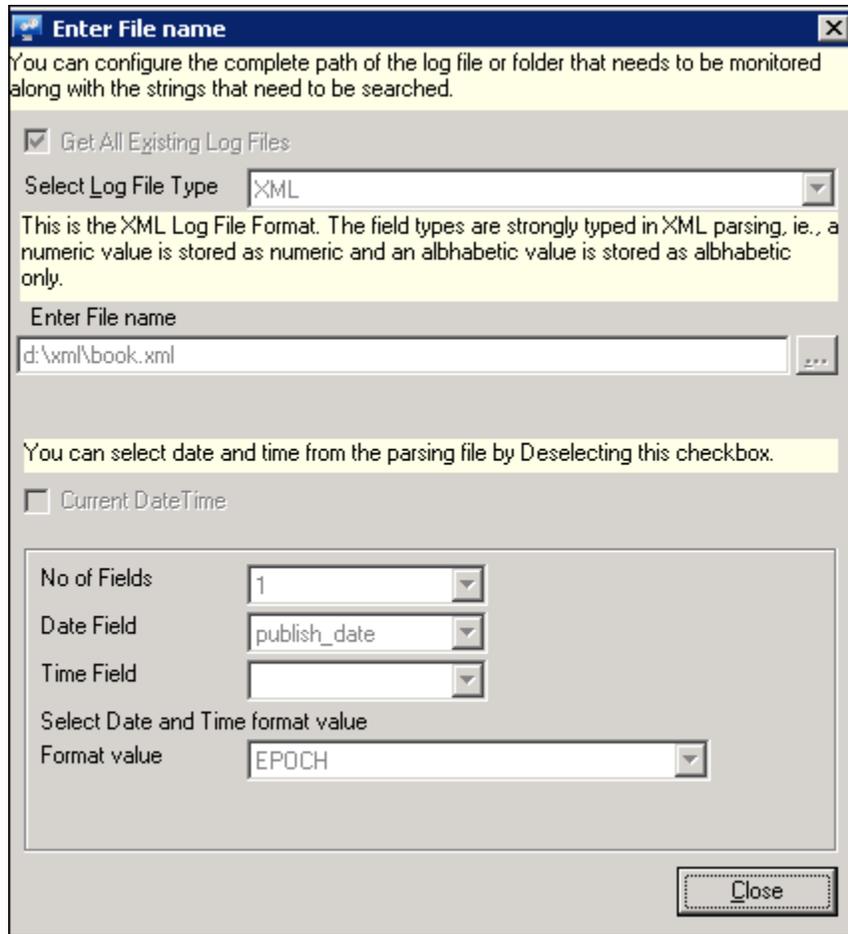


Figure: 27

**NOTE:**

- Please apply the Update **ET82UA16-022** in the agent machine.
- **IISMSID** will always consider current date and time format.