

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

EventTracker 8815 Centre Park Drive Columbia MD 21045 www.eventtracker.com

Publication Date: Sept. 20, 2016

#### 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

odate: ET82U16-022	
	5



# 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



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

PresentTracker Agent Configuration	x
File Help	
C Select Systems	_
Agent based system	
Apply the following settings to specified Agents	
Appy the following settings to specified Agents	
Manager destinations:	_
Log Backup Performance Network Connections	1
Managers Event Filters System Monitor Monitor Processes Services	İ.
Logfile Monitor   File Transfer   Config Assessment   syslog FTP server	Ì,
I Logfile Monitor	
Search log files (various formats supported) for matching patterns specified	
here. Both individual files as well as folders can be monitored for matching	
entries. Matches cause an event to be generated.	
Logfile Name File Type	
Add File Name View File Details Delete File Name Search Strings	
<u>S</u> ave <u>C</u> lose	
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**.

🕎 Enter File name					×
You can configure the co along with the strings that	mplete path of th need to be sea	he log file o rched.	or folder that need:	s to be monitored	
🔲 Get All Existing Log	Files				
Select <u>L</u> og File Type	CSV			-	]
This is the CSV Extende header line number is dif available on line number Enter File name Enter Header Line Num	MULTILINE CHECKPOINT W3C CSV XML VMWARE LOG4XML JSON				
			ОК	Cancel	
	F	igure: 2			

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





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



For the string of the second s	or folder that needs to be monitored
Get All Existing Log Files Select Log File Type CSV	<b>•</b>
This is the CSV Extended Log File Format. Differer header line number is different. The header line will available on line number one by default.	nt types of CSV files exist, in which, Il start with '#Field' qualifier and mostly
Enter File name C:\\logs1.CSV Enter Header Line Number of the above file:	
	OK Cancel
Figure: 4	

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



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

earch String Search Strings for Use a '*' in any co	: C:\\logs1.CSV olumn to match every entry i	n the file
Column Name	Search String	
Add String	Edit String	Delete String
	0K.	Cancel



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.

Enter Search Str	ing	×
You can configure the st record matching the sea	rrings that need to be searched in the selected log file(s). If any rch string is found, an event will be generated	1
	ion ading to tourid, an orong him be generated.	
Colorek Einled Manner		7
Select Field Name:	File Name	
This is a generic CSV fi comma) in the text file.	le, where the text value is any separate word (separated by	
Enter Search String		
×		
You can select date ar	nd time from the parsing file by Deselecting this checkbox.	
Current DateTime		
No of Fields	1	
Date Field	File Name	
Time Field	File Name	
Select Date and Time	e format value	
Format value	<b>•</b>	
	OK Cancel	

#### 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.



🕎 Enter Search Stri	ingX	
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.		
Select <u>F</u> ield Name:	Alert Time Stamp	
This is a generic CSV fi comma) in the text file.	e, where the text value is any separate word (separated by	
Enter Search String		
×		
You can select date ar	nd time from the parsing file by Deselecting this checkbox.	
Current DateTime		
No of Fields	1	
Date Field	Alert Time Stamp	
Time Field	Alert Time Stamp	
Select Date and Time	e format value	
Format value	YYYY-MM-DDThh:mm	
	YYYY-MM-DDThh:mm	
	YYYY'-MM-DDThh:mm∠	
	YYYY-MM-DDThh:mm:ss	
	YYYY-MM-DDThh:mm:ssZ	
	YYYYMDDThhmm	
	YYYYMMDDThhmmZ	

• Click OK.

Figure: 8

Search String		×	
Search Strings for : C:\\logs1.CSV Use a ' * ' in any column to match every entry in the file			
Column Name	Search String		
Alert Time Stamp	×		
Add String	Edit String	Delete String	
	ОК	Cancel	
	Figure: 9		



The log file gets added and is displayed.

🚰 EventTracker Agent Configuration	×
File Help	
-Select Sustems	
PNPL-TEST4	ent based system
Apply the following settings to specified Agents	
Manager destinations:	
1-2	
Log Backup Performance Netwo	rk Connections
Managers Event Filters System Monitor Monitor Pro	cesses Services
Logfile Monitor   File Transfer   Config Assessment	syslog FTP server
I antila Manitar	
<ul> <li>Search log files (various formats supported) for matching patter here. Both individual files as well as folders can be monitored.</li> </ul>	erns specified
entries. Matches cause an event to be generated.	for matering
Logfile Name	File Type
☑ d:\xml\csv2.CSV	CSV
C:\\logs1.CSV	CSV
Add File Name View File Details Delete File Name	Search Strings
Save Close	
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.

🕎 Enter File name	×
You can configure the co along with the strings that	mplete path of the log file or folder that needs to be monitored : need to be searched.
Get All Existing Log	Files
Select <u>L</u> og File Type	IIS 💌
This is the Microsoft IIS	IIS IISMSID NCSA
Enter File name	URLSCAN HTTPERR EVT TEXTWORD
	Figure: 11
	Figure: 11

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

🚰 Select Folder/File Name	×
Select Drive Name:	
Select Folder Name:	✓ Show all the files.
C:\ inetpub Iogs LogFiles K3SVC2	u_ex150216.log u_ex150217.log u_ex150219.log u_ex150220.log u_ex150223.log u_ex150224.log u_ex150224.log u_ex150226.log u_ex150227.log ▼
OK	Cancel
Figu	re: 12

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



Enter File name     You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type IIS
This is the Microsoft IIS log file format generated by IIS.
Enter File name
C:\inetpub\logs\LogFiles\W3SVC2\u_ex150216.log
OK Cancel



EventTracker Agent configuration displays the below message. Click Yes.



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

Search String		×
Search Strings for C:\inetpub\logs\Lo Use a '*' in any co	: ogFiles\W3SVC2\u_ex15021 olumn to match every entry in	6.log the file
Column Name	Search String	
Add String	Edit String	Delete String
	OK	Cancel
	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.

🚰 Enter Search St	ring 🛛 🗙
You can configure the record matching the se	strings that need to be searched in the selected log file(s). If any arch string is found, an event will be generated.
Select Field Name:	Date
This is the Microsoft II	S log file format generated by IIS.
Enter Search String	
×	
You can select date a	and time from the parsing file by Deselecting this checkbox.
🔲 Current DateTime	
No of Fields	2
Date Field	Date
Time Field	Time
Select Date and Tin	ne format value
Format value	CUSTOM
	YYYY-MM-DD hh:mm:ss
	OK Cancel

Figure: 16

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

Search String	2	×
Search Strings for C:\inetpub\logs\Lu Use a '*' in any co	: ogFiles\W3SVC2\u_ex150216.log olumn to match every entry in the file	
Column Name	Search String	
Date	×	
Add String	Edit String Delete String	
	OK Cancel	
	Figure: 17	



• The logfile gets added and is displayed.

🚰 EventTracker Agent Configuration	×
File Help	
Select Systems	1
PNPL-TEST4   Agent based system	
Apply the following settings to specified Agents	
Manager destinations:	
102.100.1.105, PNPL-TEST4	1
Log Backup   Performance   Network Connections	
Logfile Monitor File Transfer Config Assessment Suslog FTP server	
C Logfile Monitor	
Search log files (various formats supported) for matching patterns specified	
here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated	
Logfile Name File Type	
d:\xml\csv2.CSV CSV	
C:\inetpub\logs\LogFiles\W3SVC2\u_ex150216.log IIS	
I	
Add File Name View File Details Delete File Name Search Strings	
Save Close	
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.

🕎 Enter File name	×
You can configure the co along with the strings tha	emplete path of the log file or folder that needs to be monitored t need to be searched.
Get All Existing Log	Files
Select <u>L</u> og File Type	XML 🔽
This is the XML Log File numeric value is stored only.	MULTILINE CHECKPOINT W3C
Enter File name	XML
	VMWARE LOG4XML JSON
	Figure: 19

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

🚰 Select Folder/File Name	×
Select Drive Name:	_
Select Folder Name:	Show all the files.
trace2     TXT     vas     VMESX3-VM3_20151229-0000     w3c     xml     yuvaraj     yuvaraj	ibook.xml book1.xml book1-epoch.xml log4.xml SampleLog_log4j.xml
ОК	Cancel



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



Enter File name You can configure the complete path of the log file along with the strings that need to be searched.	e or folder that needs to be monitored
Get All Existing Log Files	
Select Log File Type XML	•
This is the XML Log File Format. The field types a numeric value is stored as numeric and an albhat only.	are strongly typed in XML parsing, ie., a betic value is stored as albhabetic
Enter File name	
d:\xml\book.xml	E
	OK Cancel
Figure: 21	

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



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

Search String		×
Search Strings for Use a '*' in any c	: d:\xml\book.xml olumn to match every entry in the file	
Column Name	Search String	וב
Add String	Edit String Delete String	]
	0K. Cancel	
	Figure: 23	



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

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

🚰 Enter Search Stri	ing	×
You can configure the st	rings that need to be searched in the selected log file(s). If any	y
record matching the sea	ch string is round, an event will be generated.	
Select <u>F</u> ield Name:	publish_date	•
This is a generic XML fi	le.	
Enter Search String		
×		
You can select date ar	nd time from the parsing file by Deselecting this checkbox.	
Current DateTime		
No of Fields		
Data Field		
	publish_date	
Time Field	title	
Select Date and Time	e format value	
Format value	<u> </u>	
	-YYYY-MM-DDThh:mmZ	
	Cancel	
	YYYY-MM-DDThh:mm:ssZ	
	YYYY-MM-DDThh:mm:ss(+,-)UTC	

Figure: 24

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



Search String		×
Search Strings for Use a '*' in any cr	: d:\xml\book.xml olumn to match every entry in t	the file
Column Name	Search String	
publish date	×	
Add String	Edit String	Delete String
	OK	Cancel
	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.



EventTrac	ker Age	ent Confi	igurat	ion						
e Help										
Select Syster	ns									
PNPL-TEST	4				1	- A	gent	base	d systen	ı
Applu	Floo Follor	uina oottiv	ara ka k	peoified /	ganta					
	ine tollov	wing setur	igs to s	specified P	gents					
anager destir	hations:									
	, PNPL-	TEST4								
Log Bac	:kup	Í F	Perform	ance	1	Net	work	Conn	ections	
Managers	Event	Filters	Syster	n Monitor	Mor	nitor P	roce	sses	Servi	ces
Logfile Mon	itor	File Trans	sfer	Config A	ssessm	nent	sj	yslog I	FTP ser	ver
✓ Logfile I	Ionitor									
c L	ci z	. ,		1.07					10 I	
Search log	hles Ivar	ious torma	ate eum	nortedi tor	matchi	ng pa	ittern:	s spec	ched	
hara Bathi	ndividua	l filos as u	uall as I	folders ca		mitore	d for	matel	hina	
here. Both i entries. Mal	ndividua ches ca	l files as v use an ev	vell as i vent to	folders car be genera	n be ma ited.	nitore	ed for	matel	hing	
here. Both i entries. Mal	ndividua ches ca	l files as v use an ev	vell as i vent to	folders car be genera	n be mo ited.	nitore	ed for	matel	hing	-
here. Both i entries. Mal	ndividua ches ca ime	l files as v use an ev	vell as i vent to	folders car be genera	n be ma ited.	nitore	ed for	matcl File	hing Type	I
here. Both i entries. Mal Logfile Na I d:\xml	ndividua ches ca ime icsv2.CS	I files as v use an ev	vell as l	folders car be genera	n be ma ted.	onitore	ed for	File CSV	hing Type /	I
here. Both i entries. Mai Logfile Na I d:\xml <sup>1</sup> I d:\xml <sup>1</sup>	ime ches ca me csv2.CS	i files as v use an ev iV	vell as l	folders car be genera	n be ma ted.	nitore	ed for	File CSV XMI	hing Type /	I
here. Both i entries. Mai Logfile Na I d:\xml <sup>*</sup> d:\xml <sup>*</sup>	me ches ca me csv2.CS	i files as v use an ev	vell as l	folders car be genera	n be ma ted.	pnitore	ed for	File CSV XMI	hing Type /	I
here. Both i entries. Mal Logfile Na d:\xml d:\xml	ame webook.xn	l files as v use an ev SV	vent to	folders car be genera	n be mo ted.	pnitore	ed for	File CSV XMI	hing Type /	I
here. Both i entries. Mai Logfile Na Ø d:\xml <sup>*</sup>	ame wesv2.CS wbook.xn	l files as v use an ev	vell as i	folders car be genera	n be mo ted.	pnitore	ed for	File CSV XMI	Type /	I
here. Both i entries. Mal Logfile Na ♥ d:\xml*	individua ches ca ime iscsv2.CS	l files as v use an ev	vell as l	folders car be genera	n be mo ted.	pnitore	ed for	File CSV XMI	hing Type -	I
here. Both i entries. Mal	ndividua ches ca ame .csv2.CS	l files as v use an ev	vell as l	folders car be genera	n be mo ted.	mitore	ed for	File CSV XMI	hing Type /	I
Logfile Na Logfile Na d:\xml <sup>*</sup> d:\xml <sup>*</sup> Add File f	ame Acsv2.CS Abook.xn	View File	e Detai	s Dele	te File N	Vame	ed for	File CSV XMI	hing 7 -	I
Logfile Na C d:\xml <sup>*</sup> d:\xml <sup>*</sup> d:\xml <sup>*</sup>	ame Accsv2.CS Abook.xn	View File	e Detai	s	te File N	Name	ed for	File CSV XMI	hing / -	I
Logfile Na Logfile Na d:\xml d:\xml	ame Acsv2.CS Abook.xn	View File	e Detai	s Dele	te File N	Name	ed for	File CSV XMI	hing / -	I
here. Both i entries. Mal	ame Acesv2.CS Abook.xn	View File	e Detai	s Dele	te File N	Name		File CSV XMI	hing / -	]
here. Both i entries. Mai	ame tesv2.CS	View File	e Detai	s Dele	te File M	Name	d for	File CSV XMI	hing / -	I 5
Logfile Na Logfile Na d:\xml d:\xml	ame Acesv2.CS Abook.xn	View File	e Detai	s Dele	te File N	Name <u>C</u> lo	ed for	File CSV XMI	hing 7 -	I 

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

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



💽 Enter File name		x
You can configure the c along with the strings th	complete path of the log file or folder that needs to be monitored at need to be searched.	
🔽 Get All Existing Log	g Files	
Select <u>L</u> og File Type	XML	]
This is the XML Log Fil numeric value is stored only.	e Format. The field types are strongly typed in XML parsing, ie., I as numeric and an albhabetic value is stored as albhabetic	a
Enter File name		
d:\xml\book.xml	<u></u>	
You can select date a	nd time from the parsing file by Deselecting this checkbox.	
No of Fields	1	
Date Field	publish_date	
Time Field		
Select Date and Tim	e format value	
Format value	EPOCH	
		, mul

Figure: 27

### NOTE:

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

