EventTracker
Secure. Comply. Succeed.

Enhancement in Direct Log Archiver to specify different VCP port for each configuration

EventTracker Enterprise

Publication Date: Oct. 14, 2016

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

Update: ET82U16-028

Abstract: This update will provide an option to assign different VCP port from the each DLA configuration.

Who should read this document?

Customers who use v 8.2 Build 14.

Why to apply the Update?

The existing behavior of the DLA configuration is that it always refers to the single associated virtual collection point. The log parser always picks a single configuration at a time to parse and it only picks other configuration once it completes the earlier one.

After applying this update, the user can now configure a DLA configuration by using different VCP port selection and the log parser will now pick all the configurations to parse at the same time as per the port selected.

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.

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.

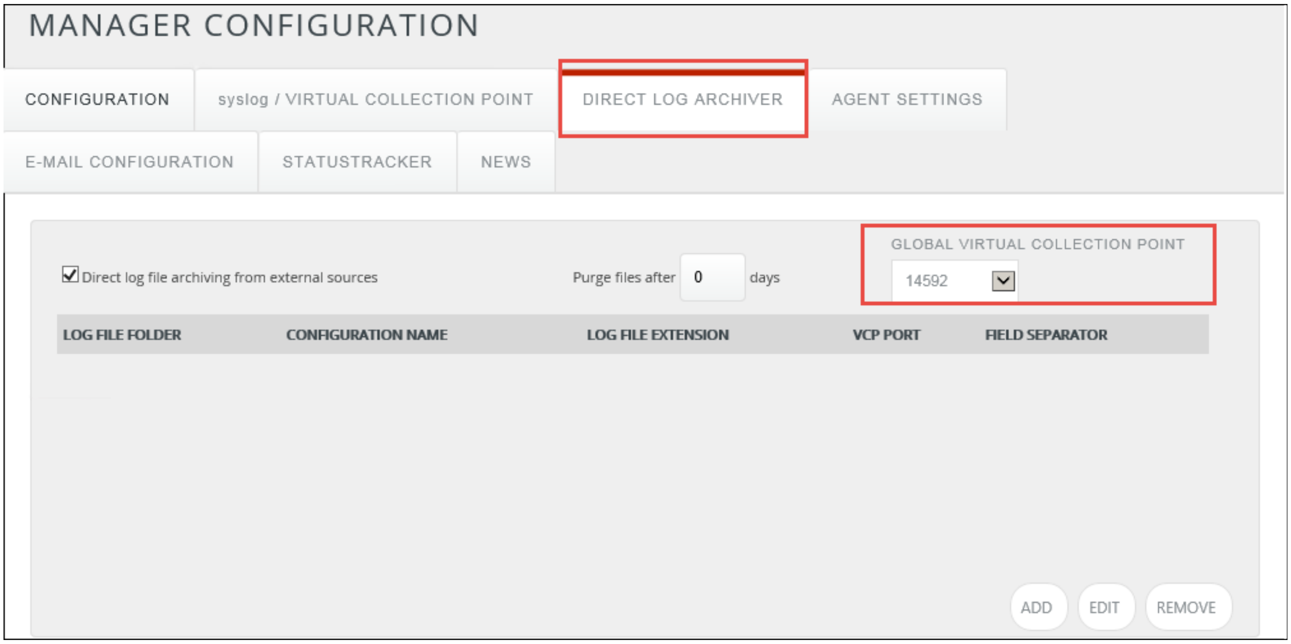
The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Process to be followed after applying the Update

NOTE: The Global Virtual Collection Point configuration option will not be available for '**DLA-Extension**" and '**Vulnerability**" type.

- Login to **EventTracker** web.
- Click **Admin** and select **Manager** from the dropdown list.
- Click the **Direct Log Archiver** tab.



MANAGER CONFIGURATION

☑ Direct log file archiving from external sources

Purge files after 0 days

GLOBAL VIRTUAL COLLECTION POINT 14592

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR

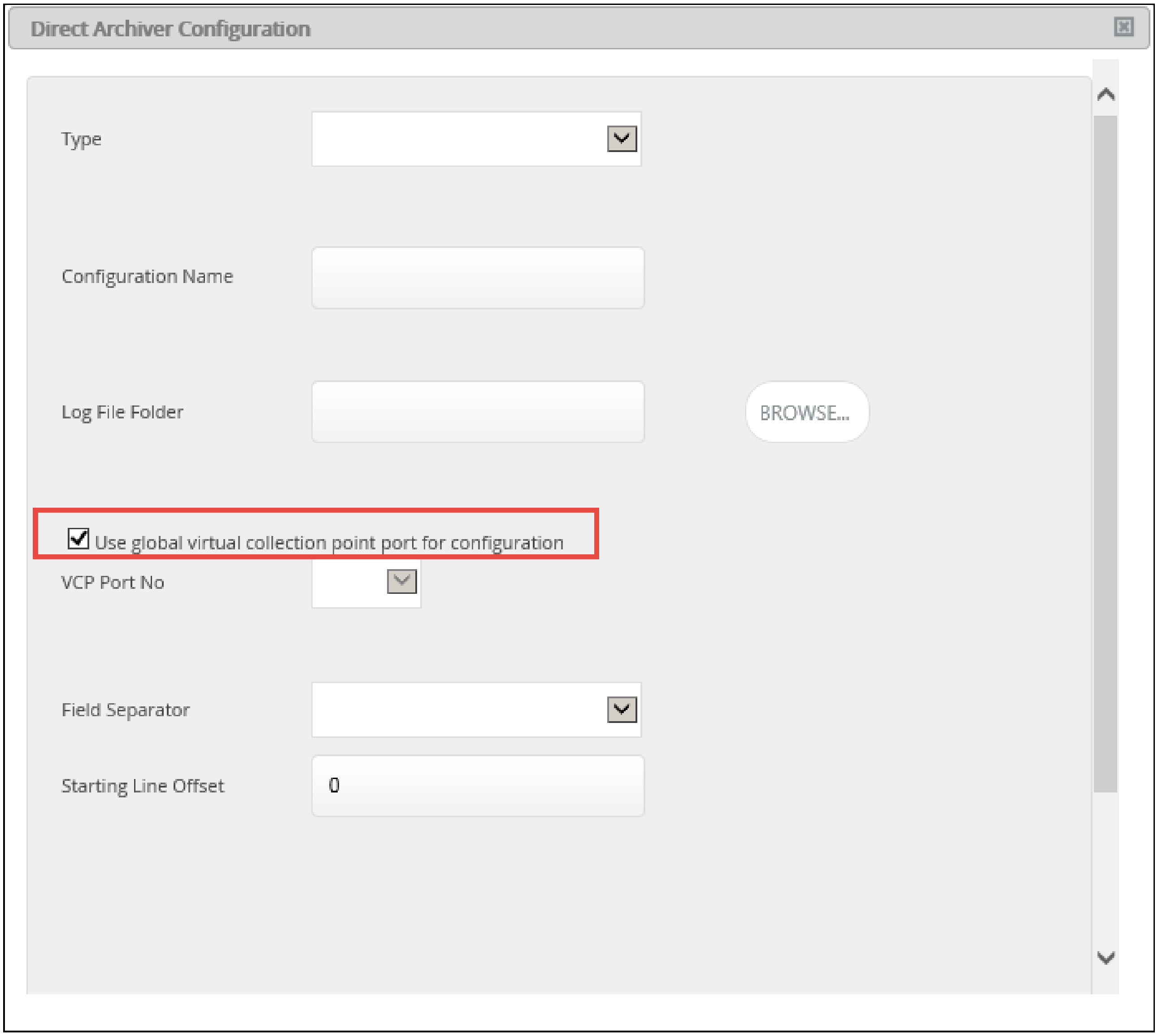
Figure 1

- The configured port will be taken as the Global Virtual Collection Point, which is highlighted in the figure above.

- To configure DLA, click the **ADD** button.

Global VCP Port Configuration

***IMPORTANT:** The earlier DLA Configurations will be listed under '**GLOBAL**" VCP Port Configuration, after applying the product update.



Direct Archiver Configuration

Type

Configuration Name

Log File Folder

☑ Use global virtual collection point port for configuration

VCP Port No

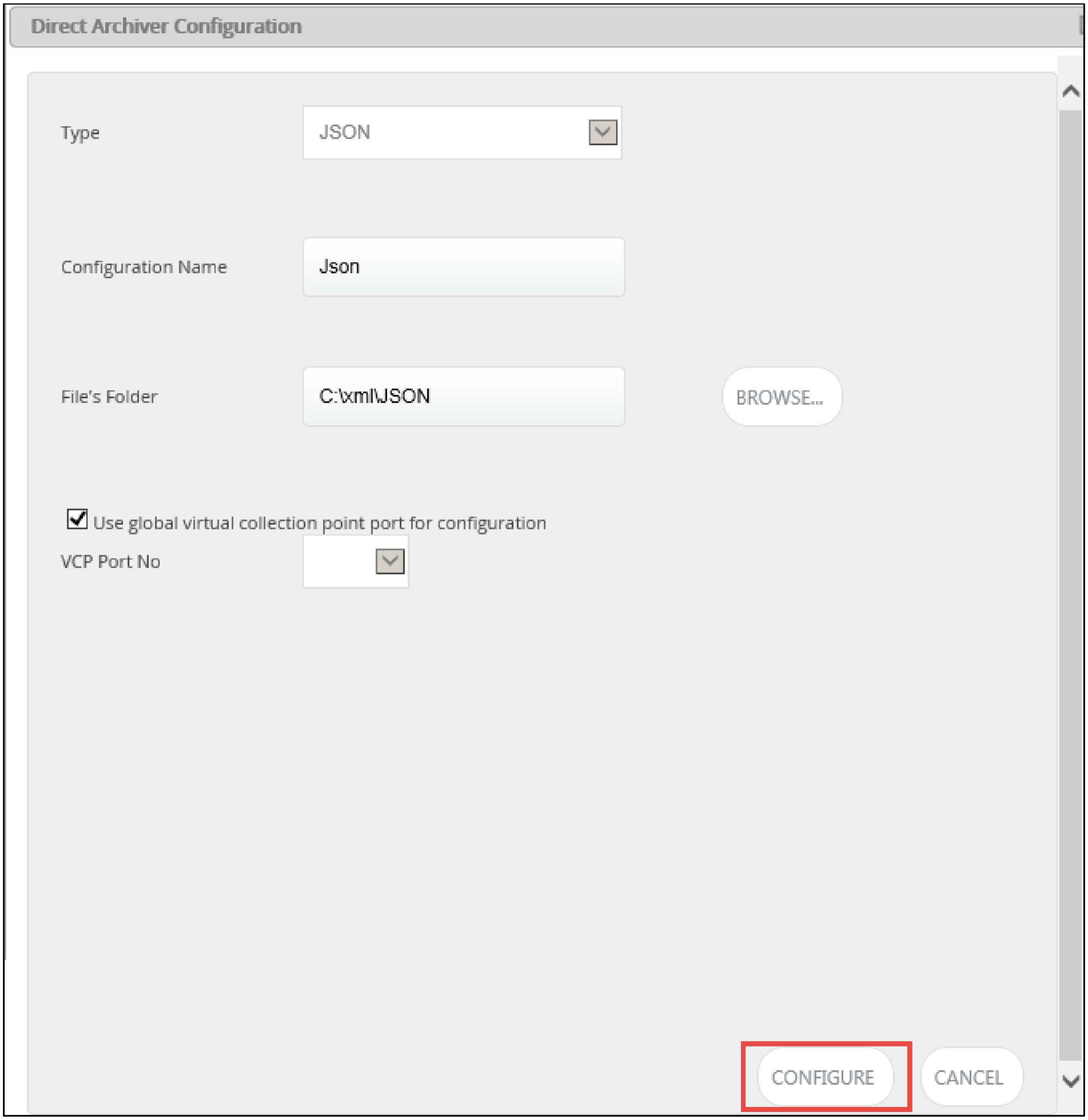
Field Separator

Starting Line Offset: 0

Figure 2

- A new option '**Use global virtual collection point port for configuration**" has been provided, which will be checked, by default. If the user wants to assign global VCP port for configuration, this option can be used while configuring DLA.

- Make the configuration changes and click the **Configure** button.



Direct Archiver Configuration

Type: JSON

Configuration Name: Json

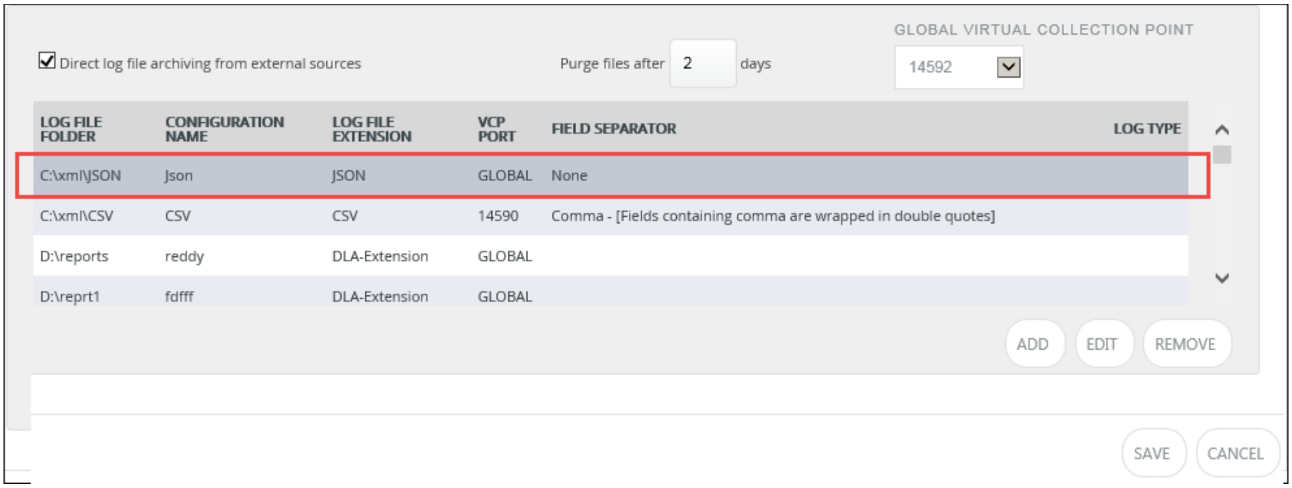
File's Folder: C:\xml\JSON

☑ Use global virtual collection point port for configuration

VCP Port No

Figure 3

- Enter the relevant details and **Save & Close** the configuration. It will be listed as '**Global**" VCP port in the Manager Configuration page.



☑ Direct log file archiving from external sources

Purge files after 2 days

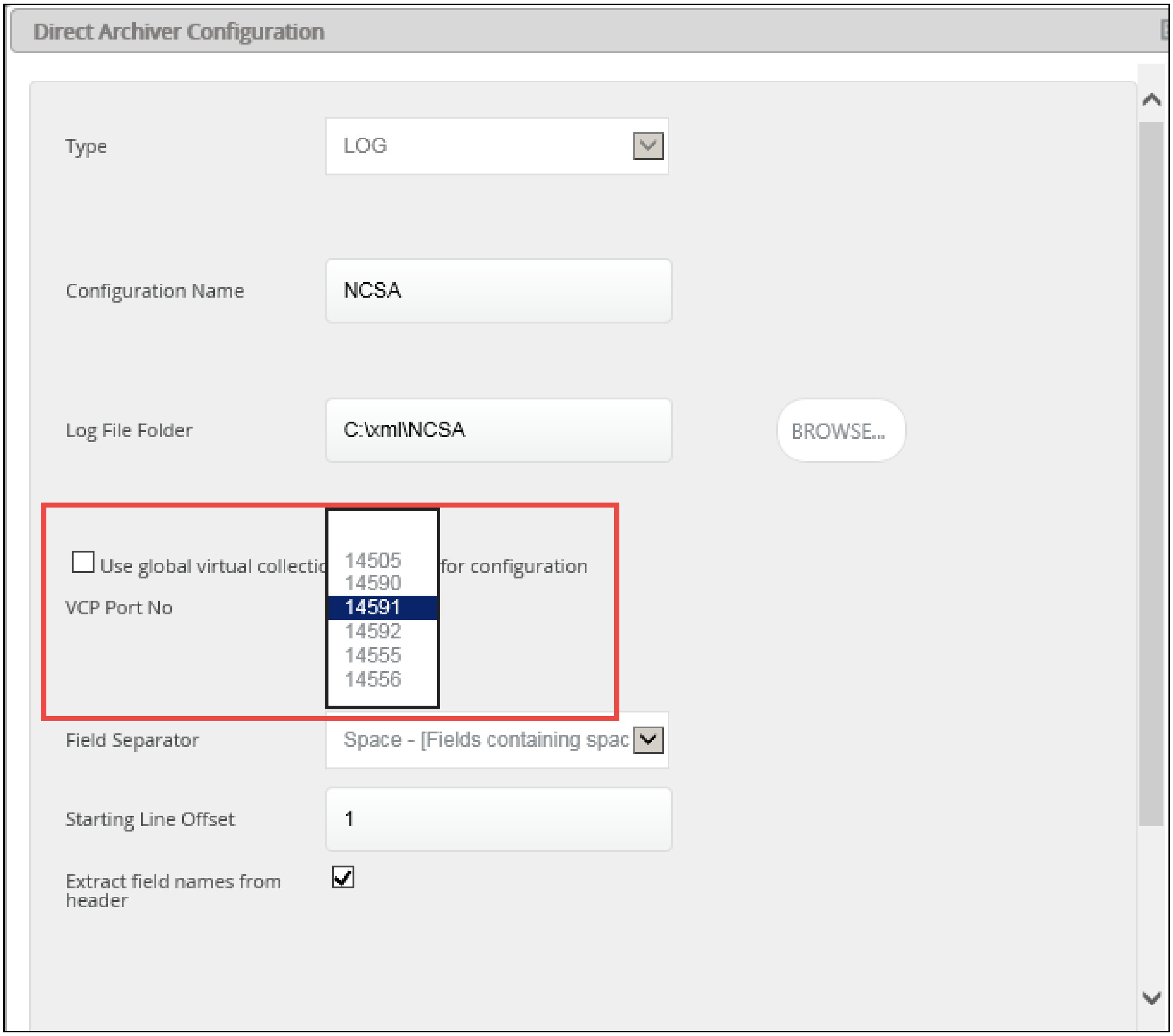
GLOBAL VIRTUAL COLLECTION POINT 14592

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR	LOG TYPE
C:\xml\JSON	Json	JSON	GLOBAL	None	
C:\xml\CSV	CSV	CSV	14590	Comma - [Fields containing comma are wrapped in double quotes]	
D:\reports	reddy	DLA-Extension	GLOBAL		
D:\reprt1	fdfff	DLA-Extension	GLOBAL		

Figure 4

Custom VCP Port Configuration

For custom VCP port configuration, uncheck the ‘**Use global virtual collection point port for configuration”** and select the custom port from the dropdown list.



Direct Archiver Configuration

Type: LOG

Configuration Name: NCSA

Log File Folder: C:\xml\NCSA

□ Use global virtual collectio[n point] for configuration

VCP Port No: 14505, 14590, 14591, 14592, 14555, 14556 (14591 selected)

Field Separator: Space - [Fields containing spac

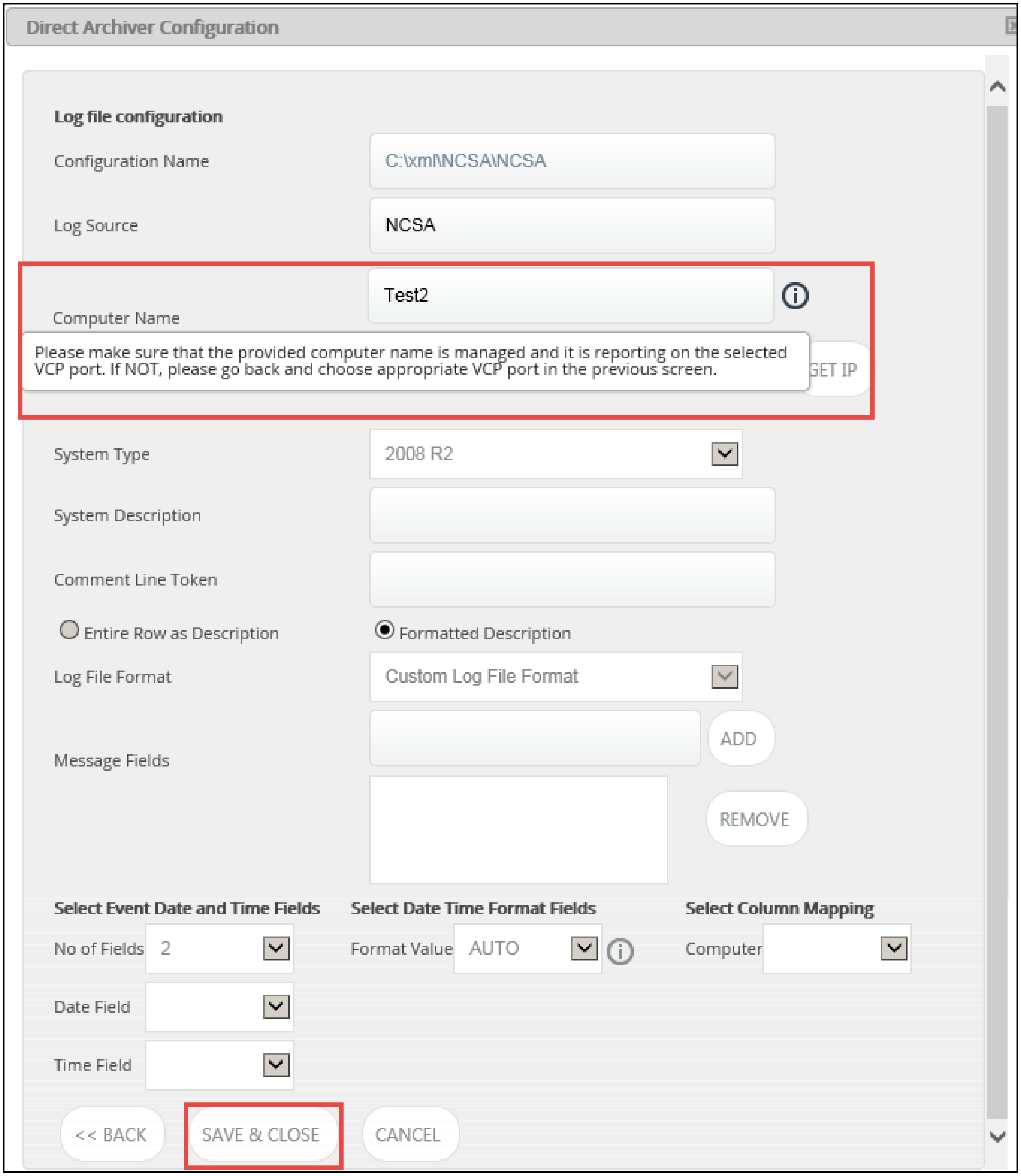
Starting Line Offset: 1

Extract field names from header: ☑

Figure 5

- Click **Configure** and enter the relevant details.

NOTE: An information icon ⓘ has been provided.



Log file configuration

Configuration Name: C:\xml\NCSA\NCSA

Log Source: NCSA

Computer Name: Test2

Please make sure that the provided computer name is managed and it is reporting on the selected VCP port. If NOT, please go back and choose appropriate VCP port in the previous screen.

System Type: 2008 R2

System Description:

Comment Line Token:

○ Entire Row as Description ● Formatted Description

Log File Format: Custom Log File Format

Message Fields:

Select Event Date and Time Fields

No of Fields: 2

Date Field:

Time Field:

Select Date Time Format Fields

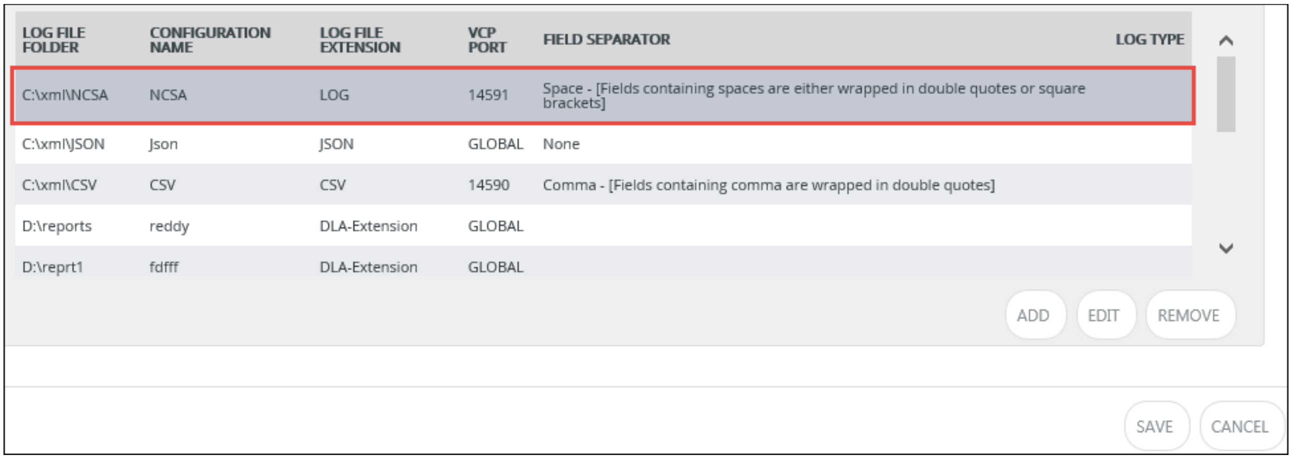
Format Value: AUTO

Select Column Mapping

Computer:

Figure 6

- Save the configuration changes by clicking the **Save & Close**. It will get listed with the user selected port in the Manager Configuration page.



LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR	LOG TYPE
C:\xml\NCSA	NCSA	LOG	14591	Space - [Fields containing spaces are either wrapped in double quotes or square brackets]	
C:\xml\JSON	Json	JSON	GLOBAL	None	
C:\xml\CSV	CSV	CSV	14590	Comma - [Fields containing comma are wrapped in double quotes]	
D:\reports	reddy	DLA-Extension	GLOBAL		
D:\reprt1	fdfff	DLA-Extension	GLOBAL		

Figure 7