

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

EventTracker Enterprise

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

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.

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	3
Global VCP Port Configuration	4
Custom VCP Port Configuration.....	6

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.

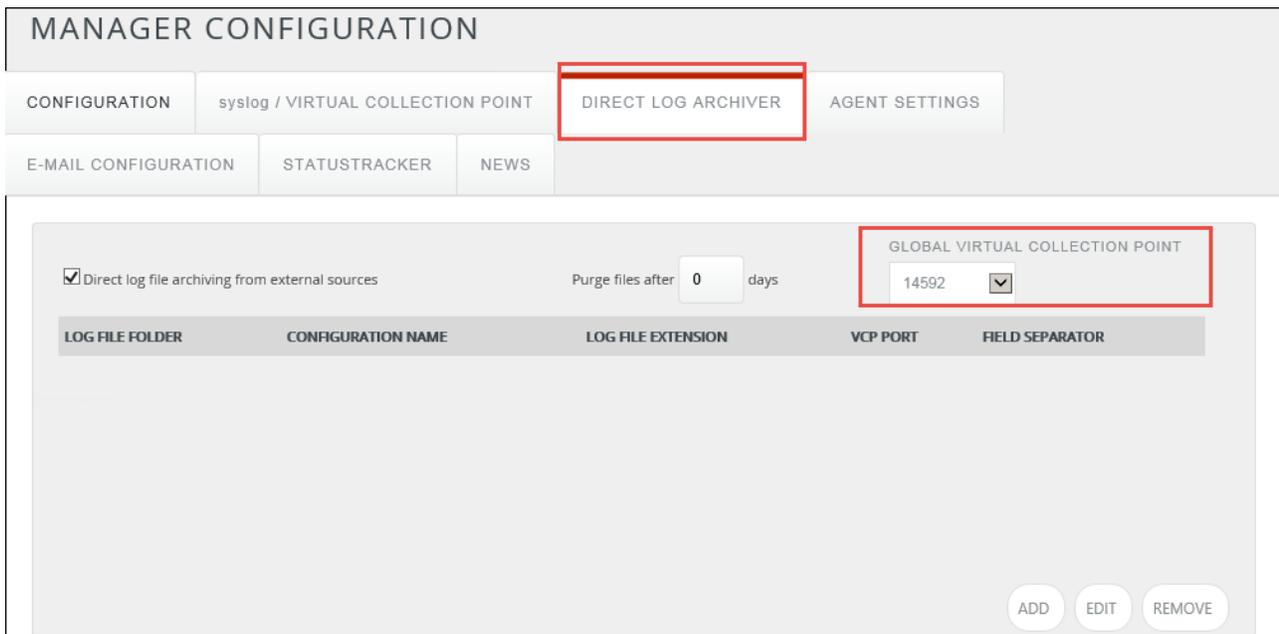
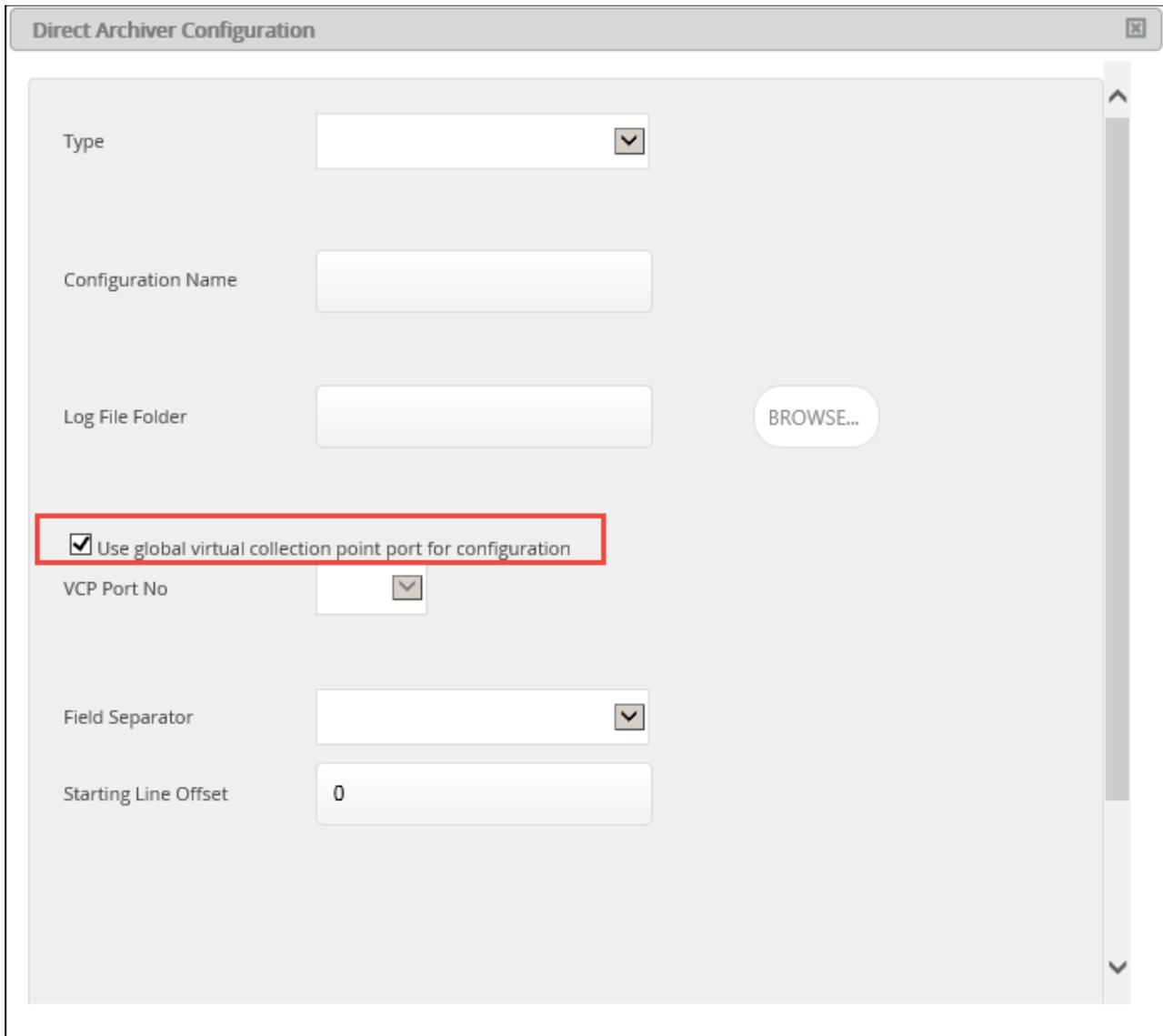


Figure 1

- 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.



The screenshot shows a window titled "Direct Archiver Configuration" with a close button in the top right corner. The window contains several configuration fields: "Type" (a dropdown menu), "Configuration Name" (a text input field), "Log File Folder" (a text input field with a "BROWSE..." button to its right), "Use global virtual collection point port for configuration" (a checked checkbox, highlighted with a red border), "VCP Port No" (a dropdown menu), "Field Separator" (a dropdown menu), and "Starting Line Offset" (a text input field containing the value "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.

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

Direct Archiver Configuration

Type: JSON

Configuration Name: Json

File's Folder: C:\xml\JSON BROWSE...

Use global virtual collection point port for configuration

VCP Port No: [Dropdown]

CONFIGURE CANCEL

Figure 3

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

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

The screenshot shows the configuration interface for Direct Log Archiver. At the top, there is a checkbox for "Direct log file archiving from external sources" which is checked. To its right, there is a "Purge files after" field set to "2" days. Further right is a "GLOBAL VIRTUAL COLLECTION POINT" dropdown menu set to "14592". Below this is a table with the following columns: LOG FILE FOLDER, CONFIGURATION NAME, LOG FILE EXTENSION, VCP PORT, FIELD SEPARATOR, and LOG TYPE. The first row is highlighted with a red box and contains: C:\xml\JSON, Json, JSON, GLOBAL, None. The second row contains: C:\xml\CSV, CSV, CSV, 14590, Comma - [Fields containing comma are wrapped in double quotes]. The third row contains: D:\reports, reddy, DLA-Extension, GLOBAL. The fourth row contains: D:\reprt1, fdfff, DLA-Extension, GLOBAL. At the bottom right of the table area are buttons for "ADD", "EDIT", and "REMOVE". At the very bottom right of the interface are "SAVE" and "CANCEL" buttons.

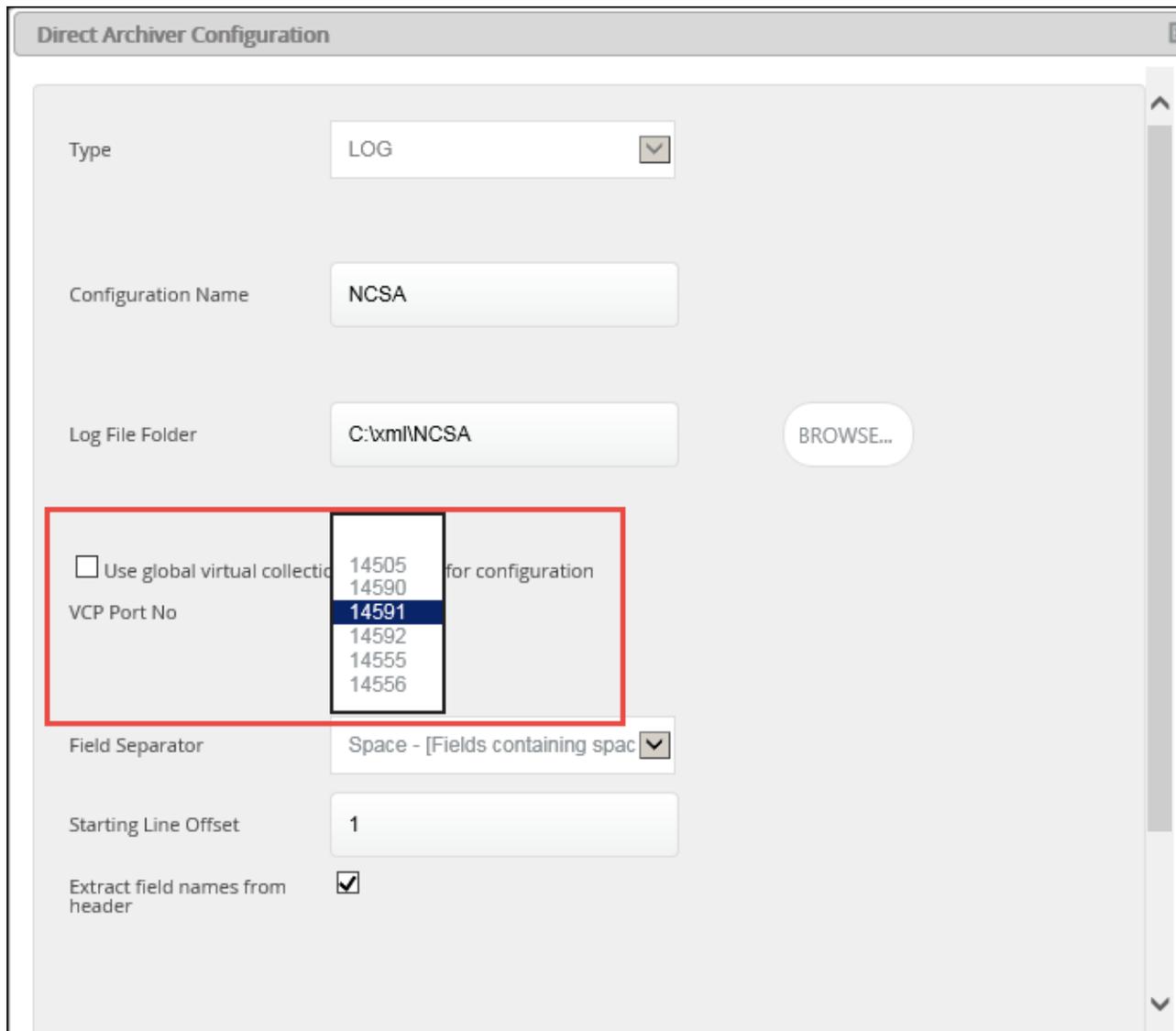
LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR	LOG TYPE
C:\xml\JSON	Json	JSON	GLOBAL	None	
C:\xml\CSV	CSV	CSV	14590	Comma - [Fields containing comma are wrapped in double quotes]	
D:\reports	reddy	DLA-Extension	GLOBAL		
D:\reprt1	fdfff	DLA-Extension	GLOBAL		

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.

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



The screenshot shows the 'Direct Archiver Configuration' window. The configuration details are as follows:

- Type: LOG
- Configuration Name: NCSA
- Log File Folder: C:\xml\NCSA
- Use global virtual collection for configuration:
- VCP Port No: 14591 (selected from a dropdown menu with options: 14505, 14590, 14591, 14592, 14555, 14556)
- Field Separator: Space - [Fields containing space]
- 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.

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

The screenshot shows the 'Direct Archiver Configuration' window. The 'Log file configuration' section includes fields for Configuration Name (C:\xml\NCSA\NCSA), Log Source (NCSA), and Computer Name (Test2). A red box highlights the Computer Name field and an information icon. A tooltip message reads: '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.' Below this, there are fields for System Type (2008 R2), System Description, Comment Line Token, Log File Format (Custom Log File Format), and Message Fields. At the bottom, there are sections for 'Select Event Date and Time Fields', 'Select Date Time Format Fields', and 'Select Column Mapping'. The 'SAVE & CLOSE' button is highlighted with a red box.

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.

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

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

ADD EDIT REMOVE

SAVE CANCEL

Figure 7