Configure DLA to transfer
Reports and Files

EventTracker
Version 7.x
Configure DLA to Transfer Reports and Files

ABSTRACT

The purpose of this document is to help users configure EventTracker Direct Log Archiver (DLA) to transfer reports generated by other applications into EventTracker Reports Framework.

TARGET AUDIENCE

- Users of EventTracker v7.x who wish to configure DLA to transfer reports generated by other applications and files into the EventTracker reports framework.
- Technical evaluator of EventTracker who seeks to understand how the feature is implemented.

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.

© 2013 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Configure DLA to Transfer Reports and Files

Table of Contents

Implement transfer of Reports and Files in EventTracker ................................................................. 3
Usage of Direct Log Archiver .................................................................................................................. 6
  Create VCP port for DLA ......................................................................................................................... 6
  Associate VCP port with DLA ............................................................................................................... 6
  Configure DLA ...................................................................................................................................... 7
    Edit DLA Configuration ....................................................................................................................... 15
Search DLA Events ................................................................................................................................. 18
Implement transfer of Reports and Files in EventTracker

LogFileParser.exe,

1. Collects necessary information by reading the *parser.ini* that exists on the system where EventTracker is installed typically,...\Program Files\Prism Microsystems\EventTracker

   **Sample: parser.ini**

   ```
   [DLA]
   logfile_path = C:\ReportsSource
   config_filename = DLA-Extension.ini
   logfile_extension = DLA-Extension
   field_separator =
   log_type =
   [End]
   ```

   2. Reads the *user-defined ini* file in the source folder where reports & files are dumped on the remote or local system.

   **Sample: DLA-Extension.ini**

   ```
   [DLAExtn]
   file_types = *.html
   action = MoveToReports
   folderName = HTML
   sendmail = Yes
   email_type = Notify
   toemail_id = ETUser1@eventtracker.com,ETUser2@eventtracker.com,ETUser3@eventtracker.com
   subject = LogFileParser:- This is a notification mail.
   ```
Configure DLA to Transfer Reports and Files

[End]

[DLAExtn]

file_types = *.log,*.w3c,*.txt

action = MoveToFolder

destination_path = D:\MyDLAFiles\W3ClogFiles

sendmail = Yes

eemail_type = Attach

toemail_id = ETUser1@eventtracker.com,ETUser2@eventtracker.com,ETUser3@eventtracker.com

subject = LogFileParser:- This is an e-mail with file attachment.

[End]

[DLAExtn]

file_types = *.png

action = MoveToFolder

destination_path = D:\MyDLAFiles\PnglogFiles

sendmail = No

eemail_type =
toemail_id =
subject =

[End]

[DLAExtn]

file_types = *.gif

action = MoveToReports

folderName = GIF

sendmail = No
email_type =
toemail_id =
subject =
[End]

3. Searches for .zip, .rar, and .CAB files in the configured source folder. If found, extracts the content.

4. Moves the reports & files to the configured destination. Destination includes, a sub-folder under default Reports folder and a user-defined folder.

**Reports folder:** ...\Program Files\Prism Microsystems\EventTracker\Reports\DlaReports\ESXWEBDOC where ESXWEBDOC is the name of the folder provided during DLA configuration.

**User-defined folder:** Any folder you wish, for example, d:\ESXWEBDOC

**E-mail:** You can attach the files as mail attachment provided the attachment should not exceed the size configured (Admin -> Manager -> Email configuration -> Email attachment maximum size). If the file size exceeds the limit, DLA sends a mail to the receiver with appropriate message. You can also send notification mails to the receiver.

Configure DLA to Transfer Reports and Files

Usage of Direct Log Archiver

On the EventTracker Manager System,

- Create VCP Port for DLA
- Associate the VCP Port with DLA
- Configure DLA
- Run a log search / analysis to view the processed events.

Create VCP port for DLA

1. Log on to EventTracker.
2. Click the Admin hyperlink at the upper-right corner.
3. Click Manager on the Control Panel.
4. Click the Syslog / Virtual Collection Point tab.
5. Click Add under Virtual Collection Points.
   
   EventTracker displays the Receiver Port pop-up window.
6. Type the port number and a brief description, for example, 14515, DLA respectively in the Port Number and Description fields.
7. Click Save.
   
   EventTracker adds the port to the Virtual Collection Points pool.
8. Click Save on the Manager Configuration page.

Associate VCP port with DLA

1. Click the Direct Log Archiver / NetFlow Receiver tab.
2. Select the Direct log file archiving from external sources check box.

   EventTracker enables the Associated virtual collection point drop-down list.
Configure DLA to Transfer Reports and Files

3. Select the port (14515) from the **Associated virtual collection point** drop-down list.

4. Type the number of days in the Purge files after field to automatically delete the files transferred after specified number of days.

5. Click **Save** on the Manager Configuration page.

---

**Configure DLA**

1. Click **Add**.

   EventTracker displays the Direct Archiver Configuration pop-up window.

2. Select the log file extension as **DLA-Extension** from the **Type** drop-down list.

3. Type the name of the configuration file with extension in the **Configuration Name** field. Direct Log Archiver creates an ini file with the name you provide.

4. Type the path of the directory where reports & files are stored in the **Log File Folder** field.
5. Click **Configure**.

EventTracker displays Direct Archiver Configuration window with more configuration options.
Configure DLA to Transfer Reports and Files

Figure 2

<table>
<thead>
<tr>
<th>File Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Pattern:</td>
<td>Action:</td>
</tr>
<tr>
<td>Note: You can enter multiple file patterns separated by comma.</td>
<td></td>
</tr>
</tbody>
</table>

**Field** | **Description**
--- | ---
**File Pattern** | Type the name of file with extension. You can also use wildcard character *, for example, *.pdf, logon*.pdf, etc. Use comma separator for files with different extensions, for example, *.doc, *.chm, *.pdf

**Action** | **Move to Folder:** DLA moves the files to the custom folder. The destination could be on local or remote system. If the folder is on the remote system you should have appropriate privileges on that folder. Type valid path of the destination folder in the **Destination path** field. **Move To Reports:** DLA moves the files to the folder under default EventTracker Reports folder, typically,...\Program Files\Prism
Configure DLA to Transfer Reports and Files

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsystems\EventTracker\Reports\DlaReports</td>
<td>Type the name of the folder in the <strong>Report folder name</strong> field. DLA creates the folder with the name provided and moves available files to that folder.</td>
</tr>
</tbody>
</table>
|                                                                      | For example:                                                                                   
|                                                                      | Report name = ESXWEBDOC                                                                        
|                                                                      | ...\Program Files\Prism                                                                     
|                                                                      | Microsystems\EventTracker\Reports\DlaReports\ESXWEBDOC                                       |
| **Send E-mail:**                                                    | Select this check box to mail attachments or notifications.                                    |
|                                                                      | Type valid receiver mail address and subject of the mail. Use comma separator for multiple mail ids.                                            |
|                                                                      | Select an appropriate email option.                                                           |

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>To add the settings to the configuration pool.</td>
</tr>
<tr>
<td>Back</td>
<td>Go back to the previous screen.</td>
</tr>
<tr>
<td>Save</td>
<td>Save the settings.</td>
</tr>
</tbody>
</table>

6. Enter/select appropriately in the relevant fields.
7. Click **Add**.
8. Click **Save**.

EventTracker adds the DLA settings to the configuration pool.
Configure DLA to Transfer Reports and Files

9. Click **Save**.

10. Open the mail client, for example, Outlook Express and verify if DLA has processed.
If the mail attachment size exceeds the permitted limit, DLA moves the file to configured destination folder and sends e-mail with appropriate message.
Configure DLA to Transfer Reports and Files

Edit DLA Configuration

1. Select a row that you wish to edit, DLA displays the settings associated with the configuration.

   ![Figure 8](image)

   **Figure 8**

2. Enter/type appropriate changes. For example, select the **Send only notification** option.

3. Click **Update**.

   DLA updates the recent changes.
4. Click **Save**.

5. Click **Save** on the Manager Configuration page.

6. Open the mail client, for example, Outlook Express and verify if DLA has processed.
Configure DLA to Transfer Reports and Files

Figure 10

EventTracker DLA Extension

Action: MoveToFolder
Source Path: C:\Reports\Source
Target path: C:\WEB\Doc
Comments: The file has been successfully moved.
Search DLA Events

1. Log on to EventTracker.

2. Click the **Search** hyperlink at the upper-right corner.
   
   EventTracker opens the Log Search browser.

3. Click the **Advanced Search** hyperlink.

4. Set the search criteria. For example, type the source as you have provided in the DLA configuration in the **search in standard and/or custom column(s)** field and select the DLA system.

5. Click **Search**.
   
   Log Search Utility displays the search result.
Configure DLA to Transfer Reports and Files

<table>
<thead>
<tr>
<th>ID</th>
<th>Log Time</th>
<th>Event Properties</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/24/2010 12:29:17 PM</td>
<td>Event ID: 3355</td>
<td>Direct log avhier successfully processed the following files: <code>C:\Reports\SomeTopSecFile.pdf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sources: EventTracker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dismiss: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: SYSTEM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: SYSTEM</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1/24/2010 12:22:09 PM</td>
<td>Event ID: 3359</td>
<td>Direct log avhier successfully processed the following files: <code>C:\Reports\SomeMSQG,ServerSuccessful_logging\421\12903794318[1].pdf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sources: EventTracker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dismiss: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: SYSTEM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: SYSTEM</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1/24/2010 11:41:41 AM</td>
<td>Event ID: 3358</td>
<td>Direct log avhier successfully processed the following files: <code>C:\Reports\SomeMSQG,ServerSuccessful_logging\421\12903794318[1].pdf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sources: EventTracker</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dismiss: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: SYSTEM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: SYSTEM</td>
<td></td>
</tr>
</tbody>
</table>

Figure 12