EventTracker
Secure. Comply. Succeed.

Configure NetApp Device Exported EVTX file in DLA without Metadata

ET76U15-040

Publication Date: March 12, 2015

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

Update: ET76U15-040

Abstract: This update will fix the issue where NetApp Device exported EVTX files are not processed without metadata file in Direct Log Archiver.

Who should read this document?

Customers who use v 7.6 and above.

NOTE: Process to be followed after applying the Update.

For users who have already configured Direct Log Archiver from external source for EVTX file, follow the steps:

Step 1: Create manually .ini file under the DLA configured file folder.
Step 2: Name it as NetApp (or you can give a friendly name)
Step 3: Copy the below added data to the newly created .ini file.

NetApp.ini

[DLA]

log_source =

computer = Name of the Computer ----------→ Event will be generated with this computer name.

computer_ip = Computer IP Address ----→ Optional

computer_systype = 17 ------→ Optional

system_description =

comment_line_token =

formatted_description = True

log_file_format =

[End]

[DLA_DateTimeField]

no_of_fields = 0

date =

time =

[End]

[DLA_MessageFields]

[End]

[DLA_FieldEventMap]

Computer =

[End]

Step 4: Open the Parser.ini under the EventTracker folder and change the Config filename to NetApp.ini (or the name that is configured).

Parser.ini

[DLA]

logfile_path = C:\Application\NetAppEvt

config_filename = NetApp.ini ----------→ Provide the name of the .INI after GUI configuration.

logfile_extension = EVTX

field_separator =

log_type = Security

recursive_path = False

StartingLine_Offset = 0

Parsing_Type =

Record_separator =

StringOrExpression =

LineCount = 0

[End]

Step 5: Place the new EVTX files in the DLA configured folder for processing or cut and paste the already processed files outside the 'completed' folder.

For new users who have not configured the DLA, follow the below mentioned steps:

Step 1: Log in to **EventTracker Web.**

Step 2: Go to **Admin** and select **Manager** from the drop down list.

Step 3: Select **Direct Log Archiver/Netflow Receiver** from the external source tab and click on the **Add** button.

EventTracker displays the Direct Archiver Configuration pop-up window.

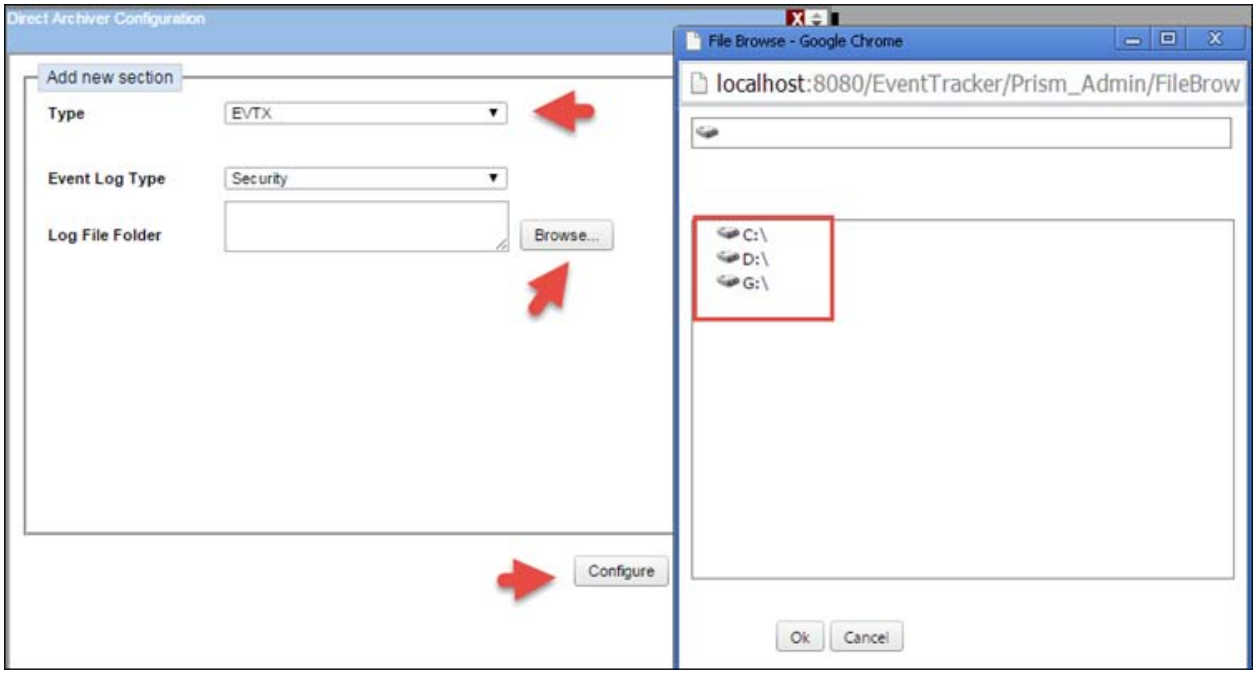

Figure: 1

Step 4: Select EVTX from **Type** drop down and Security (for example) from the **Event Log Type** drop down.

Step 5: Browse the folder where the files are to be processed as shown in the figure above.

NOTE: Do not keep the files that are to be processed, under the configured folder.

Step 6: Click on **Configure** and select the **Save** button.

Step 7: Now, stop and disable the schedule service from the Windows Service Control Manager.

Step 8: Open the Parser.ini under the EventTracker folder and change the Config filename to NetApp.ini (or the name that is configured).

Parser.ini

[DLA]

logfile_path = C:\Application\NetAppEvt

config_filename = NetApp.ini ----------→ Provide the name of the .INI after GUI configuration.

logfile_extension = EVTX

field_separator =

log_type = Security

recursive_path = False

StartingLine_Offset = 0

Parsing_Type =

Record_separator =

StringOrExpression =

LineCount = 0

[End]

Step 9: Enable and Start the scheduler service from the Windows Service Control Manager.

Step 10: Finally, place the files to be processed under the DLA configured file folder.

NOTE: The user needs to change the fields that are marked in red.