Adding Tokens in Flex Report
Abstract

The purpose of this document is to help users understand Token facility available in EventTracker Enterprise that amplifies the clarity of Flex Report. This feature offers flexibility to customize report configurations, data selection, and sort sequences.
# Table of Contents

Abstract ............................................................................................................................................ 1
Introduction ......................................................................................................................................... 3
Customization of Reports .................................................................................................................... 3
EventTracker Enterprise – Adding Tokens in Flex Report in v7.6 ...................................................... 4
  What is a Token? ............................................................................................................................... 4
  What is a Display Name? .................................................................................................................. 5
  What is a Separator? ...................................................................................................................... 5
  What is a Terminator? ..................................................................................................................... 6
Understanding the Token, Separator & Terminator ......................................................................... 8
Example # 1 ...................................................................................................................................... 8
Example # 2 ...................................................................................................................................... 9
Example # 3 ..................................................................................................................................... 10
Example # 4 ..................................................................................................................................... 11
Generating On Demand Flex Report ................................................................................................. 13
Generated Report .............................................................................................................................. 19
EventTracker Enterprise – Adding Tokens in Flex Report in v8.x .................................................... 20
  What is a Token? ............................................................................................................................... 20
  What is a Display Name? .................................................................................................................. 21
  What is a Separator? ...................................................................................................................... 22
  What is a Terminator? ..................................................................................................................... 23
Understanding the Token, Separator & Terminator ......................................................................... 24
  Example # 1 ...................................................................................................................................... 25
  Example # 2 ...................................................................................................................................... 26
  Example # 3 ...................................................................................................................................... 28
  Example # 4 ...................................................................................................................................... 29
Generating On Demand Flex Report ................................................................................................. 31
Generated Report .............................................................................................................................. 37
Introduction

Examining the contents of Log data is a time consuming task.

Data is not information unless it’s understood, associated, and interpreted. Since valuable information is dumped in the log description, there should be a way to break down and analyze the data and turn it into valuable business information.

Furthermore, there is no standardized message format and different conventions are being followed by various vendors of NIX systems, for example, comma-separated values, fixed-width text, or free-form text, it is difficult even for a seasoned administrator to decipher syslog messages.

Customization of Reports

The very purpose of generating reports is defeated if it lacks clarity or cluttered up with superfluous information.

Wouldn’t it be ideal if the information you seek were presented in the format and context in which you want? Wouldn’t it be beneficial if the reports module to have the ability to add tokens when creating reports?

As the saying goes, “devil is always in the detail” there looks like some data worth highlighting in the report.

For instance, the logon/logoff category of the Windows security log gives you the ability to monitor all attempts to access the local computer.

Event IDs 528 and 540 signify a successful logon, event ID 538 a logoff and all the other events in this category identify different reasons for a logon failure. However, just knowing about a successful or failed logon attempt doesn’t fill in the whole picture. Thankfully, logon/logoff events specify the Logon Type code, which reveals the type of logon that prompted the event.

Each Windows service is configured to run as a specified user account. When a service starts, Windows first creates a logon session for the specified user account, which results in a Logon/Logoff event with logon type 5. Failed logon events with logon type 5 usually indicate the password of an account has been changed without updating the service but there’s always the possibility of malicious users at work too.

Windows presents this Logon Type information as a parameter in the Event Description. If only you could strip this information out from the description and highlight in the report, the report does serve the purpose.
EventTracker Enterprise – Adding Tokens in Flex Report in v7.6

Aside from the standard report definition format, EventTracker Enterprise report module provides a simple, yet powerful Flex reporting facility to add and parse dynamic variables. Dynamic variables are special strings that are stripped from Windows event description or NIX syslog messages.

Adding Token feature facilitates you to query and include parts of clogged syslog like messages and Windows event descriptions as columns in reports, thus enhancing the comprehensibility and usefulness of the report.

Being said that, it is expected to have comfortable knowledge and understanding of syslog message formats of different flavors of NIX systems.

What is a Token?

It is the “token” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide Token and can contain:

- Characters (a,b,c…)
- Numbers (1,2,3…)
- Special characters (#,$,%, space character…)
- (or) Combination of all three (a1#)

If there are multiple occurrences of Token in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.

![Figure 1](image-url)
What is a Display Name?

It is a temporarily assumed name (alias) for the queried string. This display name will appear as column title in the report. It is mandatory to provide display name. You can choose any name and can contain:

- Characters
- Numbers
- (or) Combination of characters and numbers
- Special characters are not accepted.
- Display name should be unique throughout the report

![Figure 2](image)

What is a Separator?

It is the “token” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide separator and can contain:

- Characters
- Numbers
- Special characters
- (or) Combination of all three

If there are multiple occurrences of Separator in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.
What is a Terminator?

It is the ‘token’ that concludes the queried string. It is the “token” that reporter engine regards as a reference point and considers the string that precedes for parsing. The queried string is extracted till the first occurrence of the terminator. It is optional to provide terminator and can contain:

- Character
- Numbers
- Special characters
- (or) Combination of all three

If there are multiple occurrences of Terminator in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.
By default, Windows event separator is a colon (:) and terminator is a new line character (\n).

EventTracker Enterprise is shipped with a precisely defined set of columns for your convenience. If you wish to add columns and if these predefined columns do not align with your requirement, EventTracker Enterprise provides adequate facilities to add/modify/delete columns in Admin> Parsing Rules. Otherwise, default columns are sufficient.
Understanding the Token, Separator & Terminator

Following use cases will help you understand the finer nuances of Token, Separator and Terminator.

Sample Syslog description:

```
Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-
time_generated cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved
```

Example # 1

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>src</td>
<td>=</td>
<td>\s</td>
<td>172.18.90.7</td>
</tr>
</tbody>
</table>

Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-
time_generated cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted after the first occurrence of the separator till the first occurrence of the terminator.
Generated Flex Report for Example# 1:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventId</th>
<th>EventTime</th>
<th>Computer</th>
<th>EventSource</th>
<th>EventDescription</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015/02/28 21:00:00 PM</td>
<td>16</td>
<td>NA</td>
<td>MLC009-A-SYSLOG</td>
<td>SYSLOG</td>
<td></td>
<td>172.18.90.7</td>
</tr>
</tbody>
</table>

Example # 2

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>src</td>
<td>=</td>
<td></td>
<td>172.18.90.7 dst=68.232.44.169 sourceTranslatedAddress=210.69.104.254</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>destinationTranslatedAddress=68.232.44.169 cs1Label=Rule cs1=T2U-web-browsing user=app=web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131 destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated cn3=8 cs2Label=URL Category cs2=not-resolved</td>
</tr>
</tbody>
</table>
Adding Tokens in Flex Report

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted till the first occurrence of the terminator. Note that it is optional to provide Token, separator, and terminator.

Generated Flex Report for Example #2:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source</th>
<th>Separator</th>
<th>Computer</th>
<th>Source/Source Description</th>
<th>Source</th>
</tr>
</thead>
</table>

**Example #3**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>src</td>
<td>space</td>
<td>=172.18.90.7</td>
<td></td>
</tr>
</tbody>
</table>
Adding Tokens in Flex Report

Palo Alto Networks | PAN-OS | 4.0.0 | end | TRAFFIC | 1 | rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169
cs1Label=Rule cs1=T2U-web-browsing
duser=app=web-browsing
DeviceTranslatedAddress=210.69.104.254 receive_time
cs4Label=Source Zone cs4=Trust
cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/3
cs6Label=LogProfile
cs6=log
cn1Label=SessionID
cn1=261076
cnt=1
cn2Label=Packets
cn2=10
start=$cefformatted-time_generated
cn3Label=Elapsed time in seconds
cn3=8
cn4Label=Begin

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted after the first occurrence of the separator till the end of the description. Note that it is optional to provide Token, separator, and terminator.

Generated Flex Report for Example#3

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Src=</td>
<td></td>
<td></td>
<td>172.18.90.7 dst=68.232.44.169</td>
</tr>
</tbody>
</table>
sourceTranslatedAddress=210.69.104.254
destinationTranslatedAddress=68.232.44.169
cs1Label=Rule
cs1=T2U-web-browsing
suser= app=web-browsing
cs3Label=Virtual System
cs3=vsys1
cs4Label=Source Zone
cs4=Trust
cs5Label=Destination Zone
cs5=Untrust
deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/3
cs6Label=LogProfile
cs6=log
cn1Label=SessionID
cn1=261076
cnt=1
spt=3701
dpt=80
sourceTranslatedPort=24131
destinationTranslatedPort=80
flexString1Label=Flags
flexString1=0x400000
proto=tcp
act=allow
flexNumber1Label=Totalbytes
flexNumber1=1351
cn2Label=Packets
cn2=10
start=$cefformatted-time_generated
cn3Label=Elapsed time in seconds
cn3=8
cs2Label=URL Category
cs2=not-resolved

Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356
src=172.18.90.7
dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254
destinationTranslatedAddress=68.232.44.169
cs1Label=Rule
cs1=T2U-web-browsing
suser= app=web-browsing
cs3Label=Virtual System
cs3=vsys1
cs4Label=Source Zone
cs4=Trust
cs5Label=Destination Zone
cs5=Untrust
deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/3
cs6Label=LogProfile
cs6=log
cn1Label=SessionID
cn1=261076
cnt=1
spt=3701
dpt=80
sourceTranslatedPort=24131
destinationTranslatedPort=80
flexString1Label=Flags
flexString1=0x400000
proto=tcp
act=allow
flexNumber1Label=Totalbytes
flexNumber1=1351
cn2Label=Packets
cn2=10
start=$cefformatted-time_generated
cn3Label=Elapsed time in seconds
cn3=8
cs2Label=URL Category
cs2=not-resolved

This is the desired output. Since the Token is mentioned, parsing is done starting from the token. The queried string is extracted after the first occurrence of the token till the end of the description. Note that it is optional to provide token, separator, and terminator.
<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventId</th>
<th>EventLayer</th>
<th>Computer</th>
<th>EventSource</th>
<th>EventDescription</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-01-05 00:20:49 PM</td>
<td>16</td>
<td>NA</td>
<td>MOLOONIA-01/BLOG S/SLOG</td>
<td>Adding Tokens in Flex Report</td>
<td></td>
</tr>
</tbody>
</table>

**Generating On Demand Flex Report**

- Log on to EventTracker.
- Click **Report** on the menu bar.
- Click on the **New** button.
- Go to **Flex Reports**.
- Right-click **Logs -> Detail**.
- Select the **On Demand** option from the shortcut menu.
Click Next >>.
Select the Select custom properties option.
Enter / select appropriately in the relevant fields.

NOTE: In the v7.6, even for the Event categories, you will have the options to select either Parsing rules or Token Templates.
• For selecting categories, click the hyperlink ‘Select category’.

![Figure 7]

• Click Next >>.
• Select the systems.
• Select the duration options.
• Enter / select appropriately in the relevant fields.

![Figure 8]
Adding Tokens in Flex Report

- **Click Next >>**

- **For selecting customized parsing rules, click the hyperlink ‘Select Parsing Rule’**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display name</strong></td>
<td>Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.</td>
</tr>
<tr>
<td><strong>Token</strong></td>
<td>Type the name of the column in this field. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td><strong>Tag</strong></td>
<td>Tags are added when we want to bring multiple columns under one single column based on their log formats.</td>
</tr>
<tr>
<td><strong>Separator</strong></td>
<td>Type the separator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td><strong>Terminator</strong></td>
<td>Type the terminator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td><strong>Resolution</strong></td>
<td>This option helps to resolve IP address of the host by doing DNS lookup and view event &amp; port details in the EventTracker Knowledge Base. EventTracker adds hyperlinks in the generated report that enables you to navigate to the EventTracker Knowledge Base Web site to get more information on Events and ports and DNS look up Web site to resolve IP address.</td>
</tr>
</tbody>
</table>
### Summary / Report Columns

Columns that are selected in the Available Columns are listed under Report Columns. By default, these columns are included in both the Summary and Detail sections of the report. Under Summary, clear the check boxes against the columns that you wish not to include in the Summary section and be displayed only in the Detail section. Note that you cannot include Event Description, Event Id, and Log Time in the Summary section of the report. Scroll up/down to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.

### Sort By

Columns that you have selected to display in the report are listed in this drop-down list. Select an appropriate sort by option.

---

**NOTE:** For Creating, Adding and Modifying Parsing rules, go to Admin>Parsing Rules. Also separator and terminator can be added there

- Clicking on ‘Select Parsing Rules’ will display the Search Parsing Rule window.

  ![Search Parsing Rule Window](image)

  **Figure 10**

- Select the rule you want to add by clicking on the check box and click OK.
- Example:
  - Display name: Source
  - Token: src
  - Separator: “=”
  - Terminator: \\s
  - Group: Fortigate
EventTracker adds that rule as shown in the figure below:

- Clear the check boxes against the rules that you do not want to appear in the generated report.
- Select the columns in the Report Column list by scrolling up/down. EventTracker will display the columns in the report same order as you arrange.
- Type appropriate Refine and Filter criteria.
- Type title, header, footer, and description in the relevant fields.
- Review cost details and enter / select publishing options.
- Crosscheck analysis parameters.
- Click **Generate**.
- Click **Open** on the File Download pop-up window.
Generated Report

Report is generated with the newly added columns and the order of the columns that you have arranged.

The Report Summary:

Figure 13

The Report detail:
Aside from the standard report definition format, EventTracker Enterprise report module provides a simple, yet powerful Flex reporting facility to add and parse dynamic variables. Dynamic variables are special strings that are stripped from Windows event description or NIX syslog messages.

Adding Token feature facilitates you to query and include parts of clogged syslog like messages and Windows event descriptions as columns in reports, thus enhancing the comprehensibility and usefulness of the report.

Being said that, it is expected to have comfortable knowledge and understanding of syslog message formats of different flavors of NIX systems.

## What is a Token?

It is the “token” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide Token and can contain:

- Characters (a,b,c,...)
- Numbers (1,2,3,...)
- Special characters (#,$,%, space character...)

![Figure 14](image-url)
(or) Combination of all three (a1#)

If there are multiple occurrences of Token in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.

Figure 15

What is a Display Name?

It is a temporarily assumed name (alias) for the queried string. This display name will appear as column title in the report. It is mandatory to provide display name. You can choose any name and can contain:

- Characters
- Numbers
- (or) Combination of characters and numbers
- Special characters are not accepted.
- Display name should be unique throughout the report
What is a Separator?

It is the “token” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide separator and can contain:

- Characters
- Numbers
- Special characters
- (or) Combination of all three

If there are multiple occurrences of Separator in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.
What is a Terminator?

It is the ‘token’ that concludes the queried string. It is the “token” that reporter engine regards as a reference point and considers the string that precedes for parsing. The queried string is extracted till the first occurrence of the terminator. It is optional to provide terminator and can contain:

- Character
- Numbers
- Special characters
- (or) Combination of all three

If there are multiple occurrences of Terminator in the description, reporter engine considers only the first occurrence as reference point. So be specific while you frame your query.
NOTE

By default, Windows event separator is a colon (:) and terminator is a new line character (\n).

EventTracker Enterprise is shipped with a precisely defined set of columns for your convenience. If you wish to add columns and if these predefined columns do not align with your requirement, EventTracker Enterprise provides adequate facilities to add/modify/delete columns in Admin> Parsing Rules. Otherwise, default columns are sufficient.

Understanding the Token, Separator & Terminator

Following use cases will help you understand the finer nuances of Token, Separator and Terminator.

Sample Syslog description:

Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
**Example # 1**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>src</td>
<td>=</td>
<td>\s</td>
<td>172.18.90.7</td>
</tr>
</tbody>
</table>

Palo Alto Networks| PAN-OS| 4.0.0| end| TRAFFIC| 1| rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=**172.18.90.7** dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated.cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted after the first occurrence of the separator till the first occurrence of the terminator.
### Generated Flex Report for Example #1:

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>src</td>
<td>=</td>
<td></td>
<td>172.18.90.7 dst=68.232.44.169 sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule cs1=T2U-web-browsing ssuser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=42131 destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated cn3=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved</td>
</tr>
</tbody>
</table>
Palo Alto Networks | PAN-OS | 4.0.0 | end | TRAFFIC | 1 | rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= dstuser= suser= web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131
destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated
cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted till the first occurrence of the terminator. Note that it is optional to provide Token, separator, and terminator.

**Generated Flex Report for Example#2:**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogTime</td>
<td>EventId</td>
<td>FlexId</td>
<td>Computer</td>
<td>FlexSource</td>
<td>FlexDescription</td>
<td>Source</td>
</tr>
<tr>
<td>000500015.06.28 26.46 #01</td>
<td>18</td>
<td>SYSTEM</td>
<td>MCOL-08815.08.28</td>
<td>SYSL0G wis</td>
<td>Ap 14:27:20 (Netsuron-Palo Alto Networks)Cn1 (formatted-receive_time) deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169 sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule cs1=T2U-web-browsing suser= dstuser= suser= web-browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131 destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved</td>
<td>172.18.90.7 src=46.232.44.169 dest=68.232.44.169 srcLabel=Rule sLabel=T2U-web-browsing suser= dstuser= suser= web-browsing csLabel=Virtual System csysLabel=vsys1 csLabel=Source Zone csysLabel=Trust csLabel=Destination Zone csysLabel=Untrust deviceLabel=ethernet1/1 deviceLabel=ethernet1/3 deviceLabel=LogProfile deviceLabel=log cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80 sourceTranslatedPort=24131 destinationTranslatedPort=80 flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow flexNumber1Label=Totalbytes flexNumber1=1351 cn2Label=Packets cn2=10 start=$cefformatted-time_generated cn3Label=Elapsed time in seconds cn3=8 cs2Label=URL Category cs2=not-resolved</td>
</tr>
</tbody>
</table>
Example #3

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>src</td>
<td>space</td>
<td></td>
<td>=172.18.90.7</td>
</tr>
</tbody>
</table>

Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169 cs1Label=Rule
cs1=T2U-web-browsing suser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3 cs6Label=LogProfile cs6=log

This is the desired output. Since the Token is mentioned, parsing is done starting from the Token. The queried string is extracted after the first occurrence of the separator till the end of the description. Note that it is optional to provide token, separator, and terminator.

Generated Flex Report for Example#3
### Example # 4

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Token</th>
<th>Separator</th>
<th>Terminator</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Src=</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254
destinationTranslatedAddress=68.232.44.169
cs1Label=Rule cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1
deviceOutboundInterface=ethernet1/3
cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80
sourceTranslatedPort=24131
destinationTranslatedPort=80
flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
cflexNumber1Label=Totalbytes flexNumber1=1351
cn2Label=Packets cn2=10 start=start
flexNumber1Label=Totalbytes flexNumber1=1351
cn2Label=Packets cn2=10 start=start

cn3Label=Elapsed time in seconds cn3=8
```

Palo Alto Networks|PAN-OS|4.0.0|end|TRAFFIC|1|rt=$cefformatted-receive_time
deviceExternalId=0003C105356 src=172.18.90.7 dst=68.232.44.169
sourceTranslatedAddress=210.69.104.254 destinationTranslatedAddress=68.232.44.169
cs1Label=Rule cs1=T2U-web-browsing suser= duser= app=web-browsing cs3Label=Virtual System cs3=vsys1
cs4Label=Source Zone cs4=Trust cs5Label=Destination Zone cs5=Untrust
deviceInboundInterface=ethernet1/1 deviceOutboundInterface=ethernet1/3
cs6Label=LogProfile cs6=log
cn1Label=SessionID cn1=261076 cnt=1 spt=3701 dpt=80
sourceTranslatedPort=24131
destinationTranslatedPort=80
flexString1Label=Flags flexString1=0x400000 proto=tcp act=allow
cflexNumber1Label=Totalbytes flexNumber1=1351
cn2Label=Packets cn2=10 start=start
flexNumber1Label=Totalbytes flexNumber1=1351
cn2Label=Packets cn2=10 start=start

cn3Label=Elapsed time in seconds cn3=8
```

This is the desired output. Since the Token is mentioned, parsing is done starting from the token. The queried string is extracted after the first occurrence of the token till the end of the description. Note that it is optional to provide token, separator, and terminator.
## Generated Flex report for Example#4

<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventId</th>
<th>EventSource</th>
<th>EventDescription</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/24/2015 05:44 PM</td>
<td>16</td>
<td>SISTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/24/2015 05:44 PM</td>
<td>16</td>
<td>SISTEM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generating On Demand Flex Report

- Log on to EventTracker.
- Click **Report** on the menu bar.
- Click on the **New** button.
- Go to **Flex Reports**.
- Right-click **Logs -> Detail**.
- Select the **On Demand** option from the shortcut menu.

![Figure 19](image-url)

- Click **Next >>**.
- Select the **Select custom properties** option.
- Enter / select appropriately in the relevant fields.
NOTE: In v8.0, even for the Event categories, you will have the options to select either Parsing rules or Token Templates.

- For selecting categories, click the hyperlink ‘Select category’.

- Click Next >>.
• Select the systems.
• Select the duration options.
• Enter / select appropriately in the relevant fields.

![Figure 22](image1.png)

• Click Next >>.

![Figure 23](image2.png)

• For selecting customized parsing rules, click the hyperlink ‘Select Parsing Rule’.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.</td>
</tr>
<tr>
<td>Token</td>
<td>Type the name of the column in this field. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Tag</td>
<td>Tags are added when we want to bring multiple columns under one single column based on their log formats.</td>
</tr>
<tr>
<td>Separator</td>
<td>Type the separator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Terminator</td>
<td>Type the terminator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Resolution</td>
<td>This option helps to resolve IP address of the host by doing DNS lookup and view event &amp; port details in the EventTracker Knowledge Base. EventTracker adds hyperlinks in the generated report that enables you to navigate to the EventTracker Knowledge Base Web site to get more information on Events and ports and DNS look up Web site to resolve IP address.</td>
</tr>
<tr>
<td>Summary / Report Columns</td>
<td>Columns that are selected in the Available Columns are listed under Report Columns. By default, these columns are included in both the Summary and Detail sections of the report. Under Summary, clear the check boxes against the columns that you wish not to include in the Summary section and be displayed only in the Detail section. Note that you cannot include Event Description, Event Id, and Log Time in the Summary section of the report. Scroll up/down to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.</td>
</tr>
<tr>
<td>Sort By</td>
<td>Columns that you have selected to display in the report are listed in this drop-down list. Select an appropriate sort by option.</td>
</tr>
</tbody>
</table>

**NOTE:** For Creating, Adding and Modifying Parsing rules, go to Admin>Parsing Rules. Also separator and terminator can be added there

- Clicking on ‘Select Parsing Rules’ will display the Search Parsing Rule window.
Select the rule you want to add by clicking on the check box and click OK.

Example:
- **Display name:** Source
- **Token:** src
- **Separator:** “=”
- **Terminator:** \s
- **Group:** Fortigate
EventTracker adds that rule as shown in the figure below:
Clear the check boxes against the rules that you do not want to appear in the generated report.
Select the columns in the Report Column list by scrolling up/down. EventTracker will display the columns in the report same order as you arrange.
Type appropriate Refine and Filter criteria.
Type title, header, footer, and description in the relevant fields.
Review cost details and enter / select publishing options.
Crosscheck analysis parameters.
Click **Generate**.
Click **Open** on the File Download pop-up window.

**Generated Report**

Report is generated with the newly added columns and the order of the columns that you have arranged.

The Report Summary:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Event User</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEOCON</td>
<td>TOONSSCMOLO B</td>
<td><strong>47,545</strong></td>
</tr>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td>TOONSSCMOLO B</td>
<td><strong>47,545</strong></td>
</tr>
<tr>
<td>TOONSSCMOLO B</td>
<td>TOONSSCMOLO B</td>
<td><strong>47,545</strong></td>
</tr>
</tbody>
</table>

**Logs - Detail**

**User Selection:**
- From Date: 23/2015 4:07:24 PM
- To Date: 24/2015 4:07:24 PM
- Limit Time Range: None
- Refine: None
- Filter: None
- Categories Selected: N/A
- Description: None

**Summary:**

<table>
<thead>
<tr>
<th>Computer</th>
<th>Total Event Occurred</th>
<th>Event Id (Total Count)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEOCON</td>
<td>83,500</td>
<td>4091,0953, 3221,5655, 4699,0569, 4073,00097, 1002,7302, 3400,0766, 5200,0402, 5660,0760, 5400,0691, 5400,0101, 1001,129, 1031,129, 81,781, 4674,096, 3404,049, 3037,043, 3090,025, 4694,013, 4834,011, 4024,013, 3402,055, 250, 3403,025, 564, 560, 9001, 0, 9170, 0, 3302, 3455, 3401, 0, 3202</td>
</tr>
</tbody>
</table>

Figure 27
The Report details:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventId</th>
<th>EventClass</th>
<th>Computer</th>
<th>EventSource</th>
<th>EventDescription</th>
<th>Source</th>
</tr>
</thead>
</table>
| 04/24/2015 05:26:31 PM | 18      | SYSTEM     | NILCOMM-4 SYLOG     | SYLOG-mail | Apr 24 17:26:31 Netsurion-Palo Alto Networks(PAN-0342.01)generateTraffic receive_line_deviceTimestamp:00000:000000 src=172.16.90.7 dst=10.224.244.169 source=10.168.1.104 dst=10.168.104.254 destination=10.168.104.169 dstLabel=Basic dst=1024 web browsing system-down approach-browsing dstLabel=Virtual System cs=any src=Label=Source Zone cs=trust cs=Label=Destination Zone cs=untrust de-remote=country=country=ethernet=11 device=bound interfaces=ethernet=11 cs=LoginHost=cs=Login cs=Login=10.6.120.108 | 102.1.67.108 |}

<table>
<thead>
<tr>
<th>LogTime</th>
<th>EventId</th>
<th>EventClass</th>
<th>Computer</th>
<th>EventSource</th>
<th>EventDescription</th>
<th>Source</th>
</tr>
</thead>
</table>
| 04/24/2015 05:26:31 PM | 18      | system     | NILCOMM-4 SYLOG     | SYLOG-mail | Apr 24 17:26:31 Netsurion-Palo Alto Networks(PAN-0342.01)generateTraffic receive_line_deviceTimestamp:00000:000000 src=172.16.90.7 dst=10.224.244.169 source=10.168.1.104 dst=10.168.104.254 destination=10.168.104.169 dstLabel=Basic dst=1024 web browsing system-down approach-browsing dstLabel=Virtual System cs=any src=Label=Source Zone cs=trust cs=Label=Destination Zone cs=untrust de-remote=country=country=ethernet=11 device=bound interfaces=ethernet=11 cs=LoginHost=cs=Login cs=Login=10.6.120.108 | 102.1.67.108 |}