

# Security Information Event Management (SIEM): Email Logs

SIEM | TRITON AP-EMAIL | Updated: 02-May-2016

|                    |                      |
|--------------------|----------------------|
| <b>Applies To:</b> | TRITON AP-EMAIL v8.2 |
|--------------------|----------------------|

Third-party security information and event management (SIEM) tools allow the logging and analysis of internal operations and activities generated by network devices and software. Integration of TRITON AP-EMAIL with SIEM technology allows the transfer of message traffic events to a third-party SIEM system for analysis and reporting. The following email protection system logs can send data to a SIEM server:

- Connection
- Message
- Policy
- Delivery
- Hybrid

## Contents:

- [Enabling SIEM in TRITON AP-EMAIL](#)
- [Working with SIEM integration CEF format](#)
- [CEF format reference](#)
- [CEF key-value table](#)
- [Log format reference](#)

## Enabling SIEM in TRITON AP-EMAIL

SIEM | TRITON AP-EMAIL | Updated: 02-May-2016

|                    |                      |
|--------------------|----------------------|
| <b>Applies To:</b> | TRITON AP-EMAIL v8.2 |
|--------------------|----------------------|

Access SIEM integration settings on the **Settings > General > SIEM Integration** page of the TRITON Manager Email module. Mark the **Enable SIEM integration** check box to activate SIEM integration functions.

After you enable SIEM integration, use the following steps to configure the SIEM server and transport protocol:

1. Enter the IP address or hostname for the SIEM integration server in the **IP address or hostname** entry field.
2. Enter the port number for the SIEM integration server in the Port field. Default is 514.
3. Select the protocol used for data transport, either **UDP** or **TCP**. User datagram protocol (UDP) is a transport layer protocol in the Internet protocol suite. UDP is stateless and therefore faster than transmission control protocol (TCP), but it can be unreliable. Like UDP, TCP is a transport layer protocol, but it provides reliable, ordered data delivery at the expense of transport speed.
4. Click **Send Test Message** to confirm that the SIEM product is properly configured and can receive messages from your email software.

## Working with SIEM integration CEF format

SIEM | TRITON AP-EMAIL | Updated: 02-May-2016

|                    |                      |
|--------------------|----------------------|
| <b>Applies To:</b> | TRITON AP-EMAIL v8.2 |
|--------------------|----------------------|

When the SIEM integration is enabled in TRITON AP-EMAIL, log data can be sent to the SIEM server using the predefined syslog/common event format (CEF) (for ArcSight).

Because CEF uses UTF-8 character encoding, you should consider the following issues and character usage:

- Spaces used in header fields or extension values are valid. The encoding <space> is not used.
- A vertical bar, or pipe, (|) used in a CEF header must be escaped with a backslash (\). However, a vertical bar in an extension section does not need an escape character.
- A backslash (\) used in the header or the extension must be escaped with a second backslash (\).
- An equals sign (=) used in an extension must be escaped with a backslash (\). Equals signs in the header do not need an escape character.
- Multi-line fields can be sent by CEF by encoding the newline character \n or \r. Note that multiple lines are allowed only in the value part of the key-value extensions.

## CEF format reference

A SIEM record has the following format, which includes a syslog protocol prefix, a header, and a set of extensions comprising key-value pairs:

PRI SP HEADER SP CEF:Version|Device\_Vendor|Device\_Product  
|Device\_Version|Signature\_ID|Name|Severity|Extension

- **PRI** (priority value) is a combination of (Facility Level value\*8) + Severity Level. The default values are:
  - Facility Level (user-level messages) = 1
  - Severity Level (Notice: Normal but significant condition) = 5
- **Header** includes a timestamp (format MMM-dd hh:mm:ss) and the appliance hostname, separated by a space (SP).
- **CEF** indicates the common event format portion of the data record and contains the following fields:
  - **Version** identifies the current CEF format version.
  - The **Device\_Vendor** field is a unique identifier. Along with **Device\_Product**, it identifies the device. In this case, **Device\_Vendor** is Websense.
  - The **Device\_Product** field is a unique identifier. Along with **Device\_Vendor**, it identifies the device sending the data to SIEM. In this case, **Device\_Product** is ESG (i.e., TRITON AP-EMAIL).
  - The **Device\_Version** field indicates the Device\_Product version.
  - The **Signature\_ID** field is a unique event-type indicator. In this case, the field identifies the type of email protection system log that is generating the record: Connection, Message, Policy, Delivery, or Hybrid (for email hybrid service traffic).
  - The **Name** component is the event description. For the policy log, this field contains the message analysis result. For the other email protection logs, this field contains the log type.
  - **Severity** is a value between 0 and 10 that indicates an event's importance. A higher severity value indicates increased event importance. Default value is 5.
  - The **Extension** field contains a set of pre-defined key-value pairs separated by spaces. See [CEF key-value table, page 3](#), for details about these entries for TRITON AP-EMAIL.

## CEF key-value table

---

The following table contains a list of all the key names used to log data from these TRITON AP-EMAIL logs:

- Connection
- Message
- Policy
- Delivery
- Hybrid

See [Log format reference, page 5](#), for each log's specific format.

| CEF Key Name      | Full Name           | Key Value  | TRITON<br>AP-EMAIL<br>Log                                 |
|-------------------|---------------------|--|---|
| act               | deviceAction        | Policy action result<br>Message delivery status  | Policy<br>Delivery,<br>Hybrid                             |
| app               | applicationProtocol | Transport protocol   | Connection<br>Delivery                                    |
| cat               | deviceEventCategory | Antispam tool name   | Policy  |
| cc                | cc                  | Message header “Cc”  | Message   |
| cs1               | deviceCustomString1 | Virus name   | Policy  |
| deliveryCode      | n/a                 | Delivery status code   | Delivery  |
| deliveryCodeInfo  | n/a                 | Delivery status<br>information   | Delivery  |
| deviceDirection   | deviceDirection     | Email direction: inbound,<br>outbound, internal  | Policy  |
| deviceFacility    | deviceFacility      | Policy name  | Policy  |
| deviceProcessName | deviceProcessName   | Policy rule name   | Policy  |
| dst               | destinationAddress  | Email destination IP<br>address  | Delivery  |
| duser             | destinationUserName | Destination (recipient)<br>user name   | Message,<br>Policy,<br>Delivery,<br>Hybrid                |
| dvc               | deviceAddress       | Email appliance IP<br>address  | Connection,<br>Message,<br>Policy,<br>Delivery,<br>Hybrid |
| dvchost           | deviceHostName      | Email appliance fully<br>qualified domain name<br>(FQDN)                                       | Connection,<br>Message,<br>Delivery,<br>Hybrid            |
| encryptedDelivery | n/a                 | Encryption type  | Delivery  |
| exceptionReason   | n/a                 | Reason for exception<br>(e.g., DLP policy, file<br>sandbox, antivirus or<br>antispam analysis) | Policy  |
| externalID        | n/a                 | Connection ID  | Connection,<br>Message,<br>Delivery                       |
| fname             | fileName            | Email attachment name  | Message   |
| from              | from                | Message header “from”  | Message   |

| CEF Key Name    | Full Name      | Key Value  | TRITON<br>AP-EMAIL<br>Log                                 |
|-----------------|----------------|--|---|
| hybridSpamScore | n/a            | Email hybrid service spam score                              | Policy  |
| in              | bytesIn        | Inbound email size   | Message,<br>Policy,<br>Hybrid                             |
| localSpamScore  | n/a            | On-premises email spam score                                 | Policy  |
| messageID       | n/a            | Message ID number  | Message,<br>Policy,<br>Delivery,<br>Hybrid                |
| msg             | message        | Message subject  | Message,<br>Hybrid  |
| reason          | reason         | Connection status details<br>Hybrid analysis result          | Connection<br>Hybrid                                      |
| rt              | receiptTime    | Time of event receipt<br>(format is MMM dd yyyy<br>HH:mm:ss) | Connection,<br>Message,<br>Policy,<br>Delivery,<br>Hybrid |
| spamScore       | n/a            | Email hybrid service spam score                              | Hybrid  |
| spfResult       | n/a            | Relay control SPF check result                               | Connection  |
| src             | sourceAddress  | Email source IP address                                      | Connection,<br>Delivery,<br>Hybrid                        |
| suser           | sourceUserName | Source (sender) user name                                    | Message<br>Policy,<br>Hybrid                              |
| to              | n/a            | Message header “to”  | Message   |
| url             | n/a            | Message embedded URL   | Message   |
| x-mailer        | n/a            | Email client   | Message   |

## Log format reference

The following sections illustrate the format for each email protection system SIEM log record.

## Connection log

```
<13>%<: %b %_2d %T> %<applianceHostName>  
CEF:0| Websense | ESG | %<version> | "Connection | Connection | 5 |  
dvc=%<applianceIP> dvchost=%<=applianceHostName>  
rt=%<timestamp> externalId=%<connectionID> src=%<sourceIP>  
dst=%<destinationIP> app=%<transportType> reason=%<reason>  
spfResult=%<spfResult>%<\n>
```

## Message log

```
<13>%<: %b %_2d %T> %<applianceHostName>  
CEF:0| Websense | ESG | %<version> | Message | Message | 5 |  
dvc=%<applianceIP> dvchost=%<=applianceHostName>  
rt=%<timestamp> externalId=%<connectionID>  
messageId=%<messageId> suser=%<=sender> duser=%<=recipient>  
msg=%<=subject> in=%<messageSize> trueSrc=%<tsip>  
from=%<=from> to=%<=to> cc=%<=cc> x_mailer=%<=x_mailer>  
url=%<=url> fname=%<=attachment>%<\n>
```

Use the following table to map the ID shown in the **url** field to category classification information. The ID number that precedes the caret character (“^”) indicates whether the URL falls in a category that is classified in the Forcepoint Master Threat Database:

```
url= 0^http://www.example.com
```

| URL ID | Category Classification Information |
|--------|-------------------------------------|
| 0      | Not classified                      |
| 1      | Classified                          |

## Policy log

```
<13>%<: %b %_2d %T> %<applianceHostName>  
CEF:0| Websense | ESG | %<version> | Policy | %<reason> | 5 |  
dvc=%<applianceIP> dvchost=%<=applianceHostName>  
rt=%<timestamp> messageId=%<messageId> suser=%<=sender>  
duser=%<=recipient> in=%<messageSize>  
deviceDirection=%<direction> deviceFacility=%<=policyName>  
deviceProcessName=%<=ruleName> act=%<action>  
cat=%<=spamEngineName> cs1=%<=virusName>  
exceptionReason=%<=exceptionReason>  
hybridSpamScore=%<=hybridSpamScore>  
localSpamScore=%<=localSpamScore>%<\n>
```

## Delivery log

```
<13>%<: %b %_2d %T> %<applianceHostName>  
CEF:0| Websense | ESG | %<version> | Delivery | Delivery | 5 |
```

```
dvc=%<applianceIP> dvchost=%<=applianceHostName>  
rt=%<timestamp> externalId=%<connectionID>  
messageId=%<messageId> duser=%<=recipient> src=%<sourceIP>  
dst=%<destinationIP> encryptedDelivery=%<encryptedDelivery>  
deliveryCode=%<deliveryCode>  
deliveryCodeInfo=%<deliveryCodeInfo> app=%<transportType>  
act=%<action>%<\n>
```

## Hybrid log

```
<13>%<: %b %_2d %T> %<applianceHostName>  
CEF:0| Websense| ESG| %<version>| Hybrid| Hybrid| 5|  
dvc=%<applianceIP> dvchost=%<=applianceHostName>  
rt=%<timestamp> messageId=%<messageId> suser=%<=sender>  
duser=%<=recipient> msg=%<=subject> in=%<messageSize>  
src=%<sourceIP> act=%<=action> reason=%<=reason>  
spamScore=%<=spamScore>%<\n>
```

