Security Information Event Management (SIEM): Email Logs

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 Forcepoint Email Security 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 Forcepoint Email Security
- Working with SIEM integration CEF format
- CEF format reference
- CEF key-value table
- Log format reference

Enabling SIEM in Forcepoint Email Security

Access SIEM integration settings on the Settings > General > SIEM Integration page of the Forcepoint Security Manager Email Security 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**

**Applies To:** Forcepoint Email Security v8.4

When the SIEM integration is enabled in Forcepoint Email Security, 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 Forcepoint.
  - 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 Email Security.
  - 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 Forcepoint Email Security.

### CEF key-value table

The following table contains a list of all the key names used to log data from these Forcepoint Email Security logs:

- Connection
- Message
- Policy
- Delivery
- Hybrid

See **Log format reference, page 6**, for each log’s specific format.
<table>
<thead>
<tr>
<th>CEF Key Name</th>
<th>Full Name</th>
<th>Key Value</th>
<th>Forcepoint Email Security Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>act</td>
<td>deviceAction</td>
<td>Policy action result Message delivery status</td>
<td>Policy Delivery, Hybrid</td>
</tr>
<tr>
<td>app</td>
<td>applicationProtocol</td>
<td>Transport protocol</td>
<td>Connection Delivery</td>
</tr>
<tr>
<td>cat</td>
<td>deviceEventCategory</td>
<td>Antispam tool name</td>
<td>Policy</td>
</tr>
<tr>
<td>cc</td>
<td>cc</td>
<td>Message header “Cc”</td>
<td>Message</td>
</tr>
<tr>
<td>cs1</td>
<td>deviceCustomString1</td>
<td>Virus name</td>
<td>Policy</td>
</tr>
<tr>
<td>deliveryCode</td>
<td>n/a</td>
<td>Delivery status code</td>
<td>Delivery</td>
</tr>
<tr>
<td>deliveryCodeInfo</td>
<td>n/a</td>
<td>Delivery status information</td>
<td>Delivery</td>
</tr>
<tr>
<td>deviceDirection</td>
<td>deviceDirection</td>
<td>Email direction: inbound/internal = 0 outbound = 1</td>
<td>Policy</td>
</tr>
<tr>
<td>deviceFacility</td>
<td>deviceFacility</td>
<td>Policy name</td>
<td>Policy</td>
</tr>
<tr>
<td>deviceProcessName</td>
<td>deviceProcessName</td>
<td>Policy rule name</td>
<td>Policy</td>
</tr>
<tr>
<td>dst</td>
<td>destinationAddress</td>
<td>Email destination IP address</td>
<td>Delivery</td>
</tr>
<tr>
<td>duser</td>
<td>destinationUserName</td>
<td>Destination (recipient) user name</td>
<td>Message, Policy, Delivery, Hybrid</td>
</tr>
<tr>
<td>dvc</td>
<td>deviceAddress</td>
<td>Email appliance IP address</td>
<td>Connection, Message, Policy, Delivery, Hybrid</td>
</tr>
<tr>
<td>dvchost</td>
<td>deviceHostName</td>
<td>Email appliance fully qualified domain name (FQDN)</td>
<td>Connection, Message, Delivery, Hybrid</td>
</tr>
<tr>
<td>encryptedDelivery</td>
<td>n/a</td>
<td>Encryption type</td>
<td>Delivery</td>
</tr>
<tr>
<td>exceptionReason</td>
<td>n/a</td>
<td>Reason for exception (e.g., DLP policy, file sandbox, antivirus or antispam analysis)</td>
<td>Policy</td>
</tr>
<tr>
<td>externalID</td>
<td>n/a</td>
<td>Connection ID</td>
<td>Connection, Message, Delivery</td>
</tr>
</tbody>
</table>

SIEM Integration ➤ 4
<table>
<thead>
<tr>
<th>CEF Key Name</th>
<th>Full Name</th>
<th>Key Value</th>
<th>Forcepoint Email Security Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>fname</td>
<td>fileName</td>
<td>Email attachment name</td>
<td>Message</td>
</tr>
<tr>
<td>fnameAndHash</td>
<td></td>
<td>Message attachments in the format: &lt;filename&gt;</td>
<td>&lt;filehash&gt;</td>
</tr>
<tr>
<td>from</td>
<td>from</td>
<td>Message header “from”</td>
<td>Message, Policy</td>
</tr>
<tr>
<td>hybridSpamScore</td>
<td>n/a</td>
<td>Email hybrid service spam score</td>
<td>Policy</td>
</tr>
<tr>
<td>in</td>
<td>bytesIn</td>
<td>Inbound email size</td>
<td>Message, Policy, Hybrid</td>
</tr>
<tr>
<td>localSpamScore</td>
<td>n/a</td>
<td>On-premises email spam score</td>
<td>Policy</td>
</tr>
<tr>
<td>messageID</td>
<td>n/a</td>
<td>Message ID number</td>
<td>Message, Policy, Delivery, Hybrid</td>
</tr>
<tr>
<td>msg</td>
<td>message</td>
<td>Message subject</td>
<td>Message, Hybrid</td>
</tr>
<tr>
<td>reason</td>
<td>reason</td>
<td>Connection status details</td>
<td>Connection, Hybrid</td>
</tr>
<tr>
<td>replyTo</td>
<td>n/a</td>
<td>Message header “replyTo”</td>
<td>Policy</td>
</tr>
<tr>
<td>rt</td>
<td>receiptTime</td>
<td>Time of event receipt (format is MMM dd yyyy HH:mm:ss)</td>
<td>Connection, Message, Policy, Delivery, Hybrid</td>
</tr>
<tr>
<td>spamScore</td>
<td>n/a</td>
<td>Email hybrid service spam score</td>
<td>Hybrid</td>
</tr>
<tr>
<td>spfResult</td>
<td>n/a</td>
<td>Relay control SPF check result</td>
<td>Connection</td>
</tr>
<tr>
<td>src</td>
<td>sourceAddress</td>
<td>Email source IP address</td>
<td>Connection, Delivery, Hybrid</td>
</tr>
<tr>
<td>suser</td>
<td>sourceUserName</td>
<td>Envelope sender</td>
<td>Message Policy, Hybrid</td>
</tr>
<tr>
<td>to</td>
<td>n/a</td>
<td>Message header “to”</td>
<td>Message</td>
</tr>
</tbody>
</table>
The following sections illustrate the format for each email protection system SIEM log record.

### Connection log

```plaintext
<13>%<:%b %_2d %T> %<applianceHostName>
CEF:0|Forcepoint|Email
Security|%<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

```plaintext
<13>%<:%b %_2d %T> %<applianceHostName>
CEF:0|Forcepoint|Email
Security|%<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>
```

### Policy log

```plaintext
<13>%<:%b %_2d %T> %<applianceHostName>
CEF:0|Forcepoint|Email
Security|%<version>|Policy|%<reason>|5|
dvc=%<applianceIP> dvchost=%<=applianceHostName> rt=%<timestamp> messageId=%<messageId> suser=%<=sender> duser=%<=recipient> from=%<=fromAddress> replyTo=%<=replyToAddress> in=%<messageSize> deviceDirection=%<direction>
```

Log format reference

URLs in the format:
```
<url>|<url category>|<triggered/not triggered>
```

<table>
<thead>
<tr>
<th>CEF Key Name</th>
<th>Full Name</th>
<th>Key Value</th>
<th>Forcepoint Email Security Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>n/a</td>
<td>Message embedded URLs in the format: <code>&lt;url&gt;;&lt;url category&gt;;&lt;triggered/not triggered&gt;</code></td>
<td>Message, Policy</td>
</tr>
<tr>
<td>x-mailer</td>
<td>n/a</td>
<td>Email client</td>
<td>Message</td>
</tr>
</tbody>
</table>
Delivery log

<13>%<:%b %_2d %T> %<applianceHostName>
CEF:0|Forcepoint|Email
Security|%<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|Forcepoint|Email Security|%<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
©2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.