Security Information Event Management (SIEM): Email Logs

SIEM | Forcepoint Email Security | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.x

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
- Audit
- Console

Third-party SIEM providers may not support FIPS 140-2 Level 1 certified cryptography. Contact your SIEM provider for more information if FIPS-certified cryptography is required.

Contents:

Enabling SIEM in Forcepoint Email Security

SIEM | Forcepoint Email Security | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.x

Access SIEM integration settings on the SIEM Integration page of the Forcepoint Security Manager Email Security module to enable SIEM integration and configure the SIEM server and transport protocol.

Enable SIEM integration

1. From the Forcepoint Security Manager, navigate to the page **Settings > General > SIEM Integration**.

   The SIEM Integration page displays.
2. Mark the check box **Enable SIEM integration for all email appliances**.

   SIEM configuration settings are enabled for editing.
3. Configure SIEM settings and click **OK**.

   SIEM integration functions are activated. Following activation, configure SIEM settings as detailed below.

Configure SIEM integration

1. In the entry field **IP address or hostname**, enter the IP address or hostname for the SIEM integration server.
2. In the entry field **Port**, enter the port number for the SIEM integration server.

   The default is 514.
3. From the section Transport protocol, 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.

   

   Tip

   When using TCP, it is recommended to end all logs with `%<\n>`.

   From the pull-down menu **SIEM format**, select the format to be used in SIEM logs.

   The format determines the syntax of the string used to pass log data to the integration.

   - The available formats are syslog/CEF (ArcSight), syslog/key-value pairs (Splunk and others), syslog/LEEF (QRadar), and Custom.

- The text boxes populate with CEF format when Custom is selected, and can be edited as needed. The maximum size for each format is 2048 characters. Logs are not saved to the SIEM server for any log fields left blank. Selection of a new template returns any edited custom format to the default.
- Sample formats display for non-custom options.

4. Confirm that the SIEM product is properly configured and can receive messages from the email software; click **Send Test Message**.
5. Configure additional SIEM settings and click **OK**.

   The SIEM configuration settings are saved.

SIEM integration formats

SIEM | Forcepoint Email Security | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.x

Enabling SIEM integration in Forcepoint Email Security allows log data to be saved to the SIEM server using several predefined formats: syslog/common event format (CEF) (for ArcSight), syslog/key-value pairs (Splunk), and syslog log event extended format (LEEF) (QRadar).

The following should be considered when working with CEF and LEEF formats, which use UTF-8 character encoding:

- 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. Multiple lines are allowed only in the value part of the key-value extensions.

SIEM log format reference

The following details the basic syntax of a SIEM record in CEF, LEEF, and Splunk formats.

CEF:

- Header

```
<13>%<:%b %_2d %T> %<applianceHostName> CEF:0|Device
Vendor|Device Product|Product Version|Log Type|LogReason|5|
```

- Data

  ```
  key1=value1 key2=value2
  ```

  Key value pairs are separated by a space.

LEEF:

- Header

  ```
  <13>%<:%b %_2d %T> %<applianceHostName> LEEF:1.0|Device
  Vendor|Device Product|Product Version|Log Type|Log Reason|5|
  ```

- Data

  ```
  key1=value1%<\t>key2=value2
  ```

  Key value pairs are separated by a tab.

Splunk:

- Header

  ```
  <13>%<:%b %_2d %T> %<applianceHostName>
  ```

- Data

  ```
  key1=value1 key2=value2 key3="value 3"
  ```

Splunk format includes a syslog protocol prefix, a header, and a set of extensions comprising key-value pairs. CEF and LEEF formats include 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** or **LEEF** indicates the common event or long event extended format portion of the data record and contains the following fields:
  - **Version** identifies the current CEF or LEEF 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, Audit, Console, 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 the importance of an event. 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 5, for details about these entries for Forcepoint Email Security.

CEF key-value table

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

- Connection
- Message
- Policy
- Delivery
- Hybrid
- Audit
- Console

See *Log format reference*, page 12, for details about the specific format of each log.

CEF Key Name	Full Name	Key Value	Forcepoint Email Security Log
act	deviceAction	Policy action result Message delivery status	Policy Delivery, Hybrid, Audit
app	applicationProtocol	Transport protocol	Connection, Delivery
cat	deviceEventCategory	Antispam tool name	Policy
cc	cc	Message header “Cc”	Message
cs1	deviceCustomString1	Virus name	Policy

CEF Key Name	Full Name	Key Value	Forcepoint Email Security Log
deliveryCode	n/a	Delivery status code	Delivery
deliveryCodeInfo	n/a	Delivery status information	Delivery
deviceDirection	deviceDirection	Email direction: inbound/internal = 0 outbound = 1	Policy
deviceFacility	deviceFacility	Policy name	Policy
deviceProcessName	deviceProcessName	Policy rule name	Policy
dst	destinationAddress	Email destination IP address	Delivery
duser	destinationUserName	Destination (recipient) user name	Message, Policy, Delivery, Hybrid
dvc	deviceAddress	Email appliance IP address	Connection, Message, Policy, Delivery, Hybrid, Audit
dvchost	deviceHostName	Email appliance fully qualified domain name (FQDN)	Connection, Message, Policy, Delivery, Hybrid
element	n/a	Element on the page to which the change was applied	Audit
encryptedDelivery	n/a	Encryption type	Delivery
exceptionReason	n/a	Reason for exception (e.g., DLP policy, file sandbox, antivirus or antispam analysis)	Policy
externalID	externalID	Connection ID	Connection, Message, Delivery
fnameAndHash	n/a	Message attachments in the format: <filename>|<filehash>|<triggered/clean/malicious>	Policy
from	from	Message header “from”	Message, Policy

CEF Key Name	Full Name	Key Value	Forcepoint Email Security Log
hybridSpamScore	n/a	Email hybrid service spam score	Policy
in	bytesIn	Inbound email size	Message, Policy, Hybrid
localSpamScore	n/a	On-premises email spam score	Policy
messageID	n/a	Message ID number	Message, Policy, Delivery, Hybrid
msg	message	Message subject	Audit
page	n/a	Page to which a change was made	Audit
reason	reason	Connection status details Hybrid analysis result	Connection Hybrid
replyTo	n/a	Message header “replyTo”	Policy
rt	deviceReceiptTime	Time of event receipt (format is MMM dd yyyy HH:mm:ss)	Connection, Message, Policy, Delivery, Hybrid, Audit
spamScore	n/a	Email hybrid service spam score	Hybrid
spfResult	n/a	Relay control SPF check result	Connection
spriv	n/a	Role of the user that made a change	Audit
src	sourceAddress	Email source IP address	Connection, Delivery, Hybrid, Audit
suser	sourceUserName	User that made a change	Audit
suser	sourceUserName	Envelope sender	Message Policy, Hybrid
to	n/a	Message header “to”	Message
trueSrc	n/a	True source IP address	Message, Policy

CEF Key Name	Full Name	Key Value	Forcepoint Email Security Log
url	n/a	Message embedded URLs in the format: <url>|<url category>|<triggered/not triggered>	Message, Policy
x-mailer	n/a	Email client	Message

LEEF key-value table

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

- Connection
- Message
- Policy
- Delivery
- Hybrid
- Audit
- Console

See *Log format reference*, page 12, for details about the specific format of each log.

LEEF Key Name	Key Value	Forcepoint Email Security Log
accountName	User that made a change	Audit
act	Policy action result Message delivery status	Policy Delivery, Hybrid, Audit
cat	Antispam tool name	Policy
cc	Message header “Cc”	Message
connectionID	Connection ID	Connection, Message, Delivery
deliveryCode	Delivery status code	Delivery
deliveryCodeInfo	Delivery status information	Delivery
devTime	Time of event receipt (format is MMM dd yyyy HH:mm:ss)	Connection, Message, Policy, Delivery, Hybrid, Audit

LEEF Key Name	Key Value	Forcepoint Email Security Log
deviceDirection	Email direction: inbound/internal = 0 outbound = 1	Policy
deviceFacility	Policy name	Policy
deviceProcessName	Policy rule name	Policy
dst	Email destination IP address	Delivery
dvc	Email appliance IP address	Connection, Message, Policy, Delivery, Hybrid, Audit
element	Element on the page to which the change was applied	Audit
encryptedDelivery	Encryption type	Delivery
exceptionReason	Reason for exception (e.g., DLP policy, file sandbox, antivirus or antispam analysis)	Policy
fnameAndHash	Message attachments in the format: <filename>|<filehash>|<triggered/clean/malicious>	Policy
from	Message header “from”	Message, Policy
hybridSpamScore	Email hybrid service spam score	Policy
identHostName	Email appliance fully qualified domain name (FQDN)	Connection, Message, Policy, Delivery, Hybrid
localSpamScore	On-premises email spam score	Policy
messageID	Message ID number	Message, Policy, Delivery, Hybrid
page	Page to which a change was made	Audit
reason	Connection status details Hybrid analysis result	Connection Hybrid
recipient	Destination (recipient) user name	Message, Policy, Delivery, Hybrid
replyTo	Message header “replyTo”	Policy
role	Role of the user that made a change	Audit
sender	Envelope sender	Message, Policy, Hybrid
spamScore	Email hybrid service spam score	Hybrid
spfResult	Relay control SPF check result	Connection
src	Email source IP address	Connection, Delivery, Hybrid, Audit

LEEF Key Name	Key Value	Forcepoint Email Security Log
srcBytes	Inbound email size	Message, Policy, Hybrid
subject	Message subject	Message Policy, Hybrid
to	Message header “to”	Message
transport	Transport protocol	Connection, Delivery
trueSrc	True source IP address	Message, Policy
url	Message embedded URLs in the format: <url>|<url category>|<triggered/not triggered>	Message, Policy
virus	Virus name	Policy
x-mailer	Email client	Message

Splunk key-value table

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

- Connection
- Message
- Policy
- Delivery
- Hybrid
- Audit
- Console

See *Log format reference*, page 12, for details about the specific format of each log.

Splunk Key Name	Key Value	Forcepoint Email Security Log
act	Policy action result Message delivery status	Policy Delivery, Hybrid, Audit
app	Transport protocol	Connection, Delivery
cat	Antispam tool name	Policy
cc	Message header “Cc”	Message

Splunk Key Name	Key Value	Forcepoint Email Security Log
cs1	Virus name	Policy
deliveryCode	Delivery status code	Delivery
deliveryCodeInfo	Delivery status information	Delivery
deviceDirection	Email direction: inbound/internal = 0 outbound = 1	Policy
deviceFacility	Policy name	Policy
deviceProcessName	Policy rule name	Policy
dst	Email destination IP address	Delivery
duser	Destination (recipient) user name	Message, Policy, Delivery, Hybrid
dvc	Email appliance IP address	Connection, Message, Policy, Delivery, Hybrid, Audit
dvchost	Email appliance fully qualified domain name (FQDN)	Connection, Message, Policy, Delivery, Hybrid
element	Element on the page to which the change was applied	Audit
encryptedDelivery	Encryption type	Delivery
exceptionReason	Reason for exception (e.g., DLP policy, file sandbox, antivirus or antispam analysis)	Policy
externalID	Connection ID	Connection, Message, Delivery
fnameAndHash	Message attachments in the format: <filename>|<filehash>|<triggered/clean/malicious>	Policy
from	Message header “from”	Message, Policy
hybridSpamScore	Email hybrid service spam score	Policy
in	Inbound email size	Message, Policy, Hybrid
localSpamScore	On-premises email spam score	Policy
messageID	Message ID number	Message, Policy, Delivery, Hybrid
msg	Message subject	Audit
page	Page to which a change was made	Audit
reason	Connection status details Hybrid analysis result	Connection Hybrid
replyTo	Message header “replyTo”	Policy

Splunk Key Name	Key Value	Forcepoint Email Security Log
rt	Time of event receipt (format is MMM dd yyyy HH:mm:ss)	Connection, Message, Policy, Delivery, Hybrid, Audit
spamScore	Email hybrid service spam score	Hybrid
spfResult	Relay control SPF check result	Connection
src	Email source IP address	Connection, Delivery, Hybrid, Audit
suser	Envelope sender	Message, Policy, Hybrid
to	Message header “to”	Message
trueSrc	True source IP address	Message, Policy
url	Message embedded URLs in the format: <url>|<url category>|<triggered/not triggered>	Message, Policy
x-mailer	Email client	Message

Log format reference

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

CEF

Policy log

```
<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> to=%<=to>
cc=%<=cc> in=%<messageSize> deviceDirection=%<direction>
deviceFacility=%<=policyName> deviceProcessName=%<=ruleName>
act=%<action> url=%<=urlDetail> cat=%<=spamEngineName>
cs1=%<=virusName> fnameAndfileHash=%<=fileResult>
exceptionReason=%<=exceptionReason>
hybridSpamScore=%<=hybridSpamScore>
localSpamScore=%<=localSpamScore> msg=%<=subject>
trueSrc=%<tsip> x-mailer=%<=x_mailer> %<\\n>
```

Connection log

```
<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

```
<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> %<\\n>
```

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>
```

Audit Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
CEF:0|Forcepoint|Email Security|%<version>|Audit Log|Audit
Log|5| rt=%<timestamp> dvc=%<applianceIP> src=%<clientIP>
suser=%<=user> spriv=%<=role> page=%<page>
element=%<element> act=%<action> msg=%<=details> %<\\n>
```

LEEF

Policy Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email
Security|%<version>|Policy|%<reason>%<\\t>identSrc=%<applian
ceIP>%<\\t>identHostName=%<=applianceHostName>%<\\t>devTime=
%<timestamp>%<\\t>messageId=%<messageId>%<\\t>sender=%<=send
er>%<\\t>recipient=%<=recipient>%<\\t>from=%<=fromAddress>%<
\\t>replyTo=%<=replyToAddress><\\t>to=%<=to>%<\\t>cc=%<=cc>%
<\\t>srcBytes=%<messageSize>%<\\t>deviceDirection=%<directio
n>%<\\t>deviceFacility=%<=policyName>%<\\t>deviceProcessName
=%<=ruleName>%<\\t>act=%<action>%<\\t>url=%<=urlDetail>%<\\t
>cat=%<=spamEngineName>%<\\t>virus=%<=virusName>%<\\t>fnameA
ndfileHash=%<=fileResult>%<\\t>exceptionReason=%<=exceptionR
eason>%<\\t>hybridSpamScore=%<=hybridSpamScore>%<\\t>localSp
amScore=%<=localSpamScore><%\\t>subject=%<=subject>%<\\t>tru
eSrc=%<tsip>% <\\t>x-mailer=%<=x_mailer>%<\\n>
```

Connection Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email
Security|%<version>|Connection|Connection%<\\t>identSrc=%<ap
plianceIP>%<\\t>identHostName=%<=applianceHostName>%<\\t>dev
Time=%<timestamp>%<\\t>connectionId=%<connectionID>%<\\t>src
=%<sourceIP>%<\\t>dst=%<destinationIP>%<\\t>transport=%<tran
sportType>%<\\t>reason=%<reason>%<\\t>spfResult=%<spfResult>
%<\\t>%<\\n>
```

Message Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email
Security|%<version>|Message|Message%<\\t>identSrc=%<applianc
eIP>%<\\t>identHostName=%<=applianceHostName>%<\\t>devTime=%
<timestamp>%<\\t>connectionId=%<connectionID>%<\\t>messageId
=%<messageId>%<\\t>sender=%<=sender>%<\\t>recipients=%<=reci
pient>%<\\t>subject=%<=subject>%<\\t>srcBytes=%<messageSize>
%<\\t>trueSrc=%<tsip>%<\\t>from=%<=from>%<\\t>to=%<=to>%<\\t
>cc=%<=cc>%<\\t>x-mailer=%<=x_mailer>%<\\t>%<\\n>
```

Delivery Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email
Security|%<version>|Delivery|Delivery%<\\t>identSrc=%<applia
nceIP>%<\\t>identHostName=%<=applianceHostName>%<\\t>devTime
=%<timestamp>%<\\t>connectionId=%<connectionID>%<\\t>message
Id=%<messageId>%<\\t>recipient=%<=recipient>%<\\t>src=%<sour
```

```
ceIP>%<\\t>dst=%<destinationIP>%<\\t>encryptedDelivery=%<enc
ryptedDelivery>%<\\t>deliveryCode=%<deliveryCode>%<\\t>deliv
eryCodeInfo=%<deliveryCodeInfo>%<\\t>transport=%<transportTy
pe>%<\\t>act=%<action>%<\\t><%\\n>
```

Hybrid Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email
Security|%<version>|Hybrid|Hybrid%<\\t>identSrc=%<applianceI
P>%<\\t>identHostName=%<=applianceHostName>%<\\t>devTime=%<t
imestamp>%<\\t>messageId=%<messageId>%<\\t>sender=%<=sender>
%<\\t>recipieints=%<=recipient>%<\\t>subject=%<=subject>%<\\
t>srcBytes=%<messageSize>%<\\t>src=%<sourceIP>%<\\t>act=%<=a
ction>%<\\t>reason=%<=reason>%<\\t>spamScore=%<=spamScore>%<
\\t>%<\\n>
```

Audit Log

```
<13>%<:%b %_2d %T> %<applianceHostName>
LEEF:1.0|Forcepoint|Email Security|%<version>|Audit
Log|Audit
Log%<\\t>devTime=%<timestamp>%<\\t>identSrc=%<applianceIP>%<
\\t>src=%<clientIP>%<\\t>accountName=%<=user>%<\\t>role=%<=r
ole>%<\\t>page=%<page>%<\\t>element=%<element>%<\\t>act=%<ac
tion>%<\\t>details=%<=details>%<\\t>%<\\n>
```

Splunk

Policy Log

```
<13>%<:%b %_2d %T> %<applianceHostName> vendor=Forcepoint
product="Email Security" version=%<version>event=Policy
reason=%<reason> dvc=%<applianceIP>
dvchost=%<=applianceHostName> rt=%<timestamp>
messageId=%<messageId> suser="%<=sender>"
duser="%<=recipient>" from="%<=fromAddress>"
replyTo="%<=replyToAddress>" to="%<=to>" cc="%<=cc>"
in=%<messageSize> deviceDirection=%<direction>
deviceFacility=%<=policyName> deviceProcessName=%<=ruleName>
act=%<action> url="%<=urlDetail>" cat=%<=spamEngineName>
cs1=%<=virusName> fnameAndfileHash="%<=fileResult>"
exceptionReason=%<=exceptionReason>
hybridSpamScore=%<=hybridSpamScore>
localSpamScore=%<=localSpamScore> msg="%<=subject>"
trueSrc=%<tsip> x-mailer="%<=x_mailer>" %<\\n>
```

Connection Log

```
<13>%<:%b %_2d %T> %<applianceHostName> vendor=Forcepoint
product="Email Security" version=%<version> event=Connection
```

```
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> vendor=Forcepoint
product="Email Security" version=%<version> event=Message
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>" %<\\n>
```

Delivery Log

```
<13>%<:%b %_2d %T> %<applianceHostName> vendor=Forcepoint
product="Email Security" version=%<version> event=Delivery
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> vendor=Forcepoint
product="Email Security" version=%<version>
event=Hybriddvc=%<applianceIP> dvchost=%<=applianceHostName>
rt=%<timestamp> messageId=%<messageId> suser=%<=sender>
duser=%<=recipient> msg="%<=subject>" in=%<messageSize>
src=%<sourceIP> act=%<=action> reason=%<=reason>
spamScore=%<=spamScore> %<\\n>
```

Audit Log

```
<13>%<:%b %_2d %T> %<applianceHostName> vendor=Forcepoint
product="Email Security" version=%<version>event="Audit Log"
rt=%<timestamp> dvc=%<applianceIP> src=%<clientIP>
suser=%<=user> spriv=%<=role> page=%<page>
element=%<element> act=%<action> msg=%<=details> %<\\n>
```