Configure CEF Log Entry and CEF Headers in ESA

Contents

Introduction

This document describes the configuration for Common Event Format (CEF) Log entry and headers for Cisco Secure Email Gateway (SEG).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco Secure Email Gateway / Email Security Appliance (SEG / ESA)
- Content Filters knowledge
- Log subscription knowledge

Components Used

The information in this document is based on these software and hardware versions:

- Email Security Appliance version 14.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Consolidated Event Logs summarizes each message event in a single log line. Use this log type in order to reduce the number of bytes of data (log information) sent to a Security Information and Event Management (SIEM) vendor or application for analysis. The logs are in the CEF log message format that is widely used by most SIEM vendors.

CEF Log Entry and CEF Headers are added to provide extra information to track and organize the mail events.

Configure

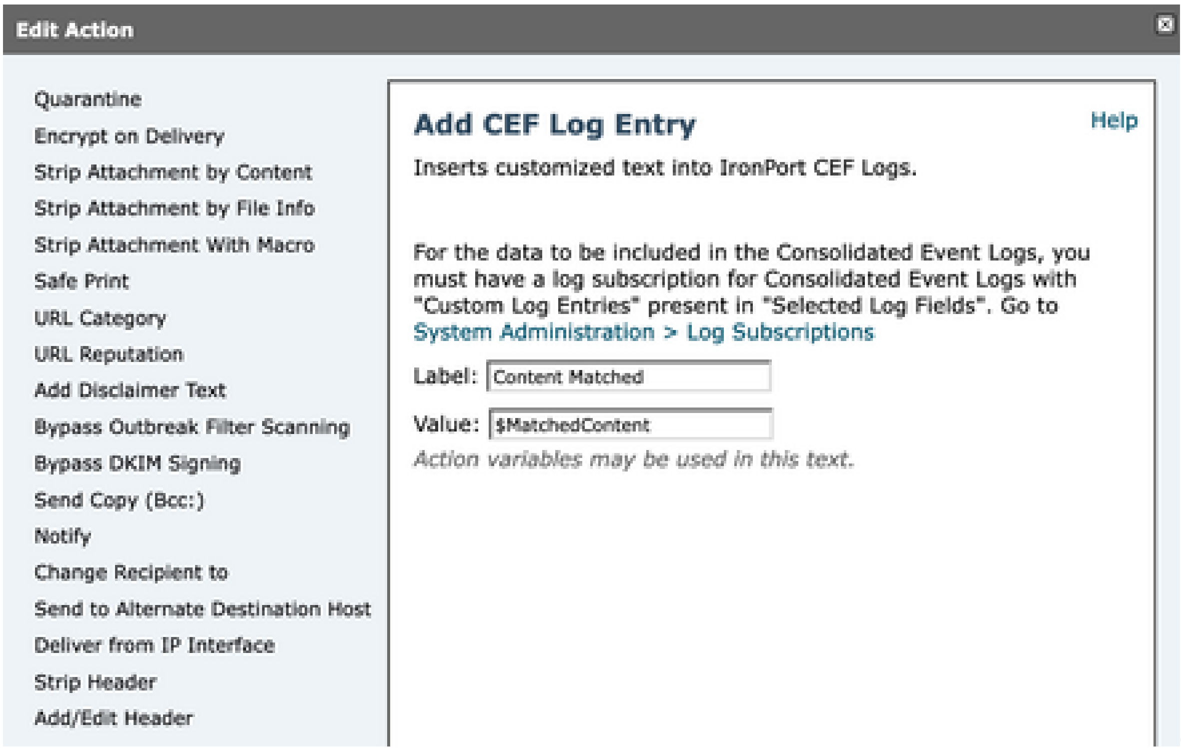
CEF Log Entry

Add the incoming/outgoing content filter

First, create the content filter on the ESA:

1. Go to **Mail Policies > Incoming/Outgoing content filters**
2. Click in **Add Filter**
3. Name the filter
4. Add condition desired
5. Click in **Add Action**
6. Select **Add CEF Log Entry**
7. Name the label and use **Action Variables** for the value box
8. **Submit and Commit**

This documentation example we use **$MatchedContent** Action Variable, as shown in the image:



Inserts customized text into IronPort CEF Logs.

For the data to be included in the Consolidated Event Logs, you must have a log subscription for Consolidated Event Logs with "Custom Log Entries" present in "Selected Log Fields". Go to System Administration > Log Subscriptions

Label: Content Matched

Value: $MatchedContent

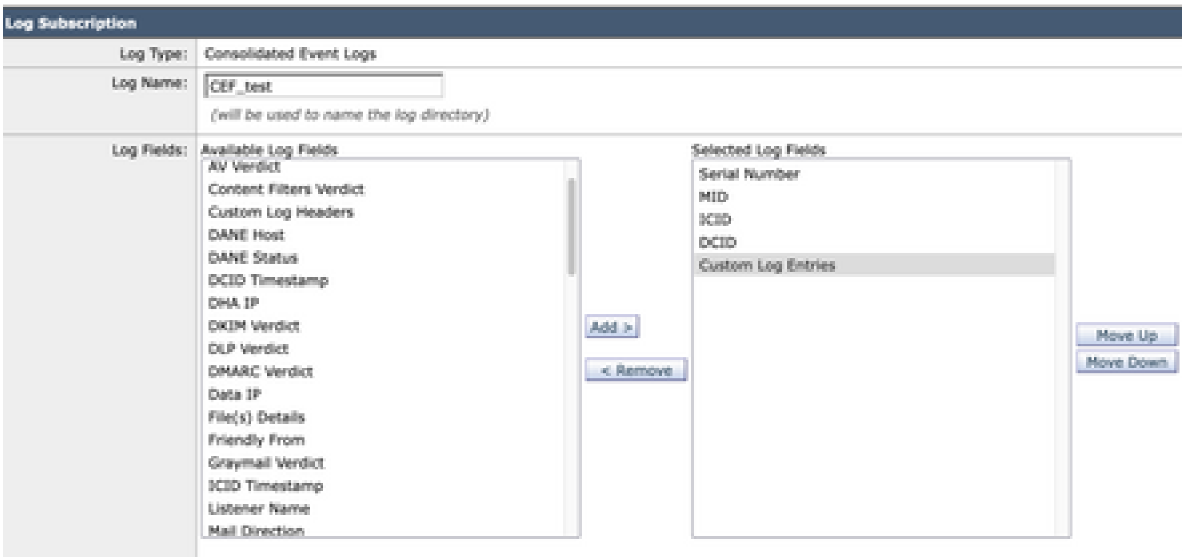
Action variables may be used in this text.

CEF Log entry action in content filters

Add CEF Log Entry in the Consolidated Event Log Subscription

Next, create or modify the Consolidated Event Log Subscription to add the CEF Log Entry previously created:

1. Go to **System Administration > Log Subscriptions**
2. Add or Select the Consolidated Event Logs
3. Select **Custom Log Entries** and click **Add**
4. **Submit and Commit**



Log Subscription

Log Type: Consolidated Event Logs

Log Name: CEF_test
(will be used to name the log directory)

Log Fields:

Available Log Fields:
- AV Verdict
- Content Filters Verdict
- Custom Log Headers
- DANE Host
- DANE Status
- DCID Timestamp
- DHA IP
- DKIM Verdict
- DLP Verdict
- DMARC Verdict
- Data IP
- File(s) Details
- Friendly From
- Graymail Verdict
- ICID Timestamp
- Listener Name
- Mail Direction

Selected Log Fields:
- Serial Number
- MID
- ICID
- DCID
- Custom Log Entries

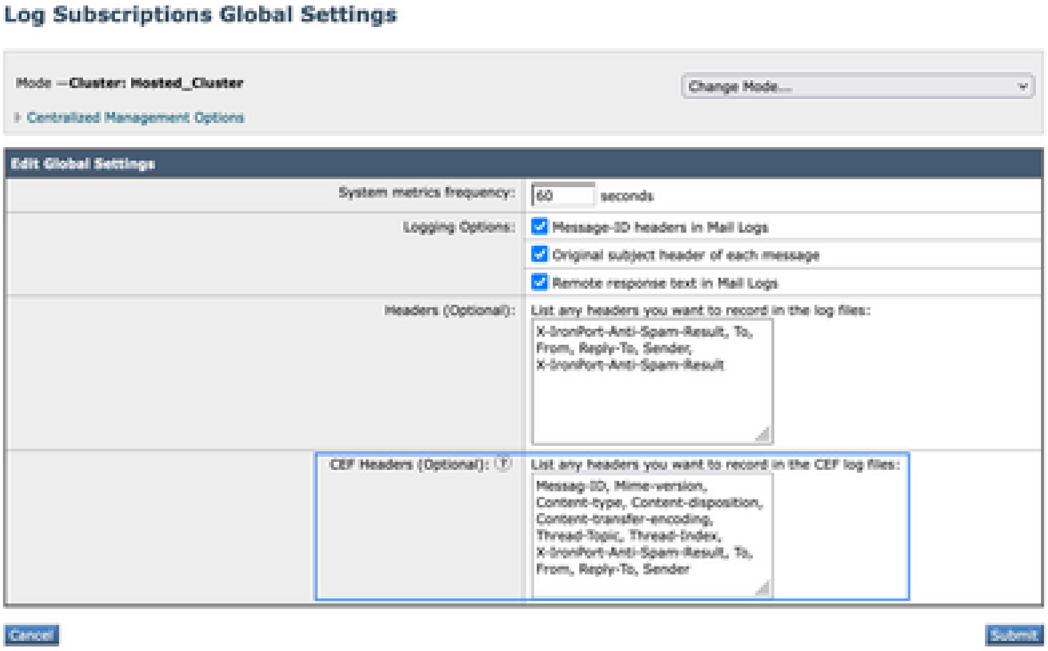
Custom Log Entries in CEF Log Subscription

CEF Headers

Add the CEF Headers to log:

First add the CEF Headers in the ESA

1. Go to **System Administration > Logs Subscription**
2. Click in **Edit Settings** under Global Settings
3. Under CEF Headers, list the headers to log
4. **Submit and Commit**



Log Subscriptions Global Settings

Mode —**Cluster: Hosted_Cluster**

Edit Global Settings

System metrics frequency: 60 seconds

Logging Options:
- ☑ Message-ID headers in Mail Logs
- ☑ Original subject header of each message
- ☑ Remote response text in Mail Logs

Headers (Optional): List any headers you want to record in the log files:
X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender, X-IronPort-Anti-Spam-Result

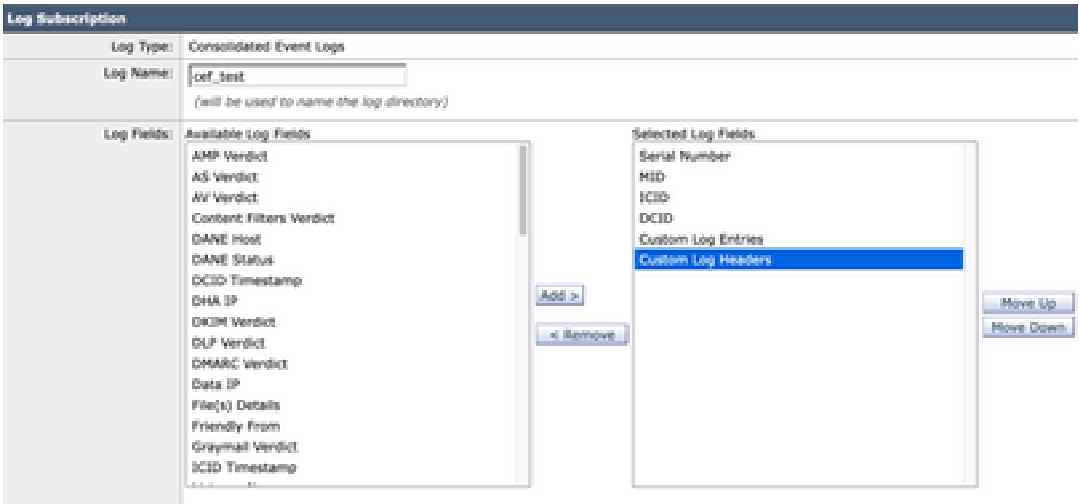
CEF Headers (Optional): List any headers you want to record in the CEF log files:
Messag-ID, Mime-version, Content-type, Content-disposition, Content-transfer-encoding, Thread-Topic, Thread-Index, X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender

CEF Headers Configuration

Add CEF Log Entry in the Consolidated Event Log Subscription

Next, create or modify the Consolidated Event Log Subscription to add the CEF Headers previously recorded:

1. Go to **System Administration > Logs Subscription**
2. Add or Select the Consolidated Event Logs
3. Select **Custom Log Entries** and click **Add**
4. **Submit and Commit**



Log Subscription

Log Type: Consolidated Event Logs

Log Name: cef_test

(will be used to name the log directory)

Log Fields:

Selected Log Fields: Serial Number, MID, ICID, DCID, Custom Log Entries, Custom Log Headers

CEF Log Headers in CEF Log Subscription

Related information

- [End user guide ESA 14.3]
- [Release Notes ESA 14.3]
- [Technical Support - Cisco Systems]