ESAでのCEFログエントリとCEFヘッダーの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[CEFログエントリ](#)
[着信/発信コンテンツフィルタの追加](#)
[統合イベントログサブスクリプションへのCEFログエントリの追加](#)
[CEFヘッダー](#)
[ログにCEFヘッダーを追加します。](#)
[統合イベントログサブスクリプションへのCEFログエントリの追加](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Secure Email Gateway(SEG)のCommon Event Format(CEF)ログエントリとヘッダーの設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Eメールゲートウェイ/Eメールセキュリティアプライアンス(SEG/ESA)
- コンテンツフィルタの知識
- サブスクリプションの知識の記録

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Eメールセキュリティアプライアンスバージョン14.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

統合イベント・ログでは、各メッセージ・イベントが1行にまとめられます。このログタイプを使用して、Security Information and Event Management(SIEM)ベンダーまたは分析用アプリケーションに送信されるデータ（ログ情報）のバイト数を減らします。ログは、ほとんどのSIEMベンダーで広く使用されているCEFログメッセージ形式です。

CEFログエントリとCEFヘッダーが追加され、メールイベントを追跡および整理するための追加情報が提供されます。

設定

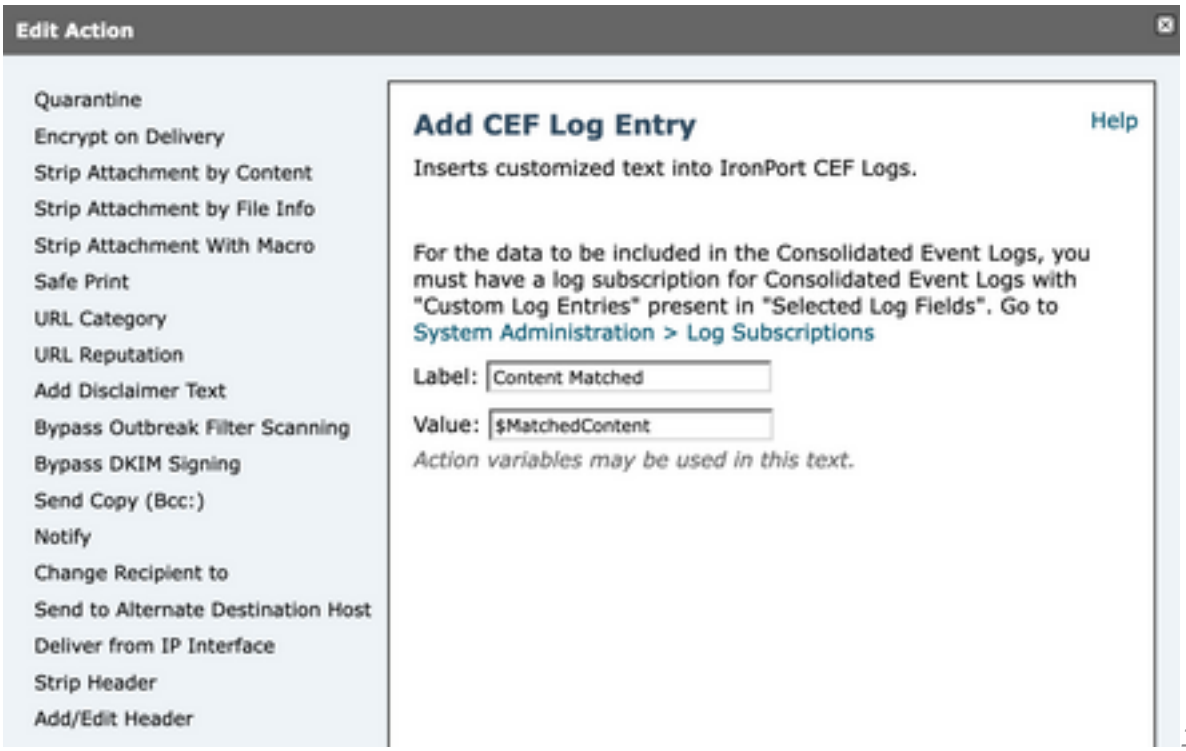
CEFログエントリ

着信/発信コンテンツフィルタの追加

最初に、ESAでコンテンツフィルタを作成します。

1. 次に **Mail Policies > Incoming/Outgoing content filters**
2. クリックする **Add Filter**
3. フィルタに名前を付ける
4. 必要な条件の追加
5. クリックする **Add Action**
6. 選択 **Add CEF Log Entry**
7. ラベルに名前を付け、 **Action Variables** 値ボックスの場合
8. **Submit and Commit**

このドキュメントの例では、 **$MatchedContent** 図に示すアクション変数：

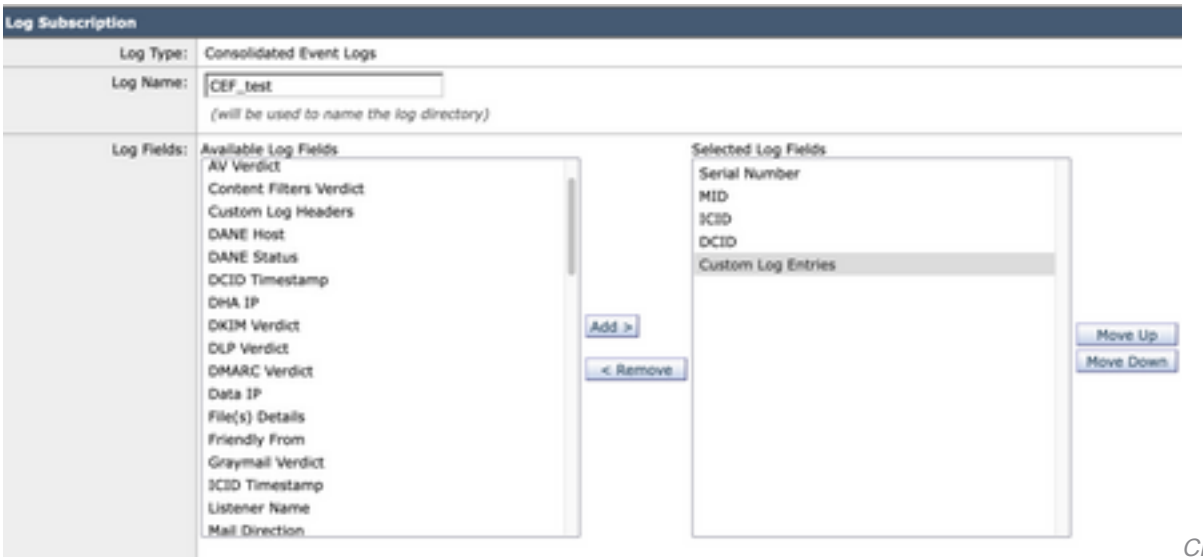


コンテンツフィルタでのCEFログエントリアクション

統合イベントログサブスクリプションへのCEFログエントリの追加

次に、統合イベントログサブスクリプションを作成または変更して、以前に作成したCEFログエントリを追加します。

1. 次に **System Administration > Log Subscriptions**
2. 統合イベント・ログの追加または選択
3. 選択 **Custom Log Entries** をクリックし、 **Add**
4. **Submit and Commit**



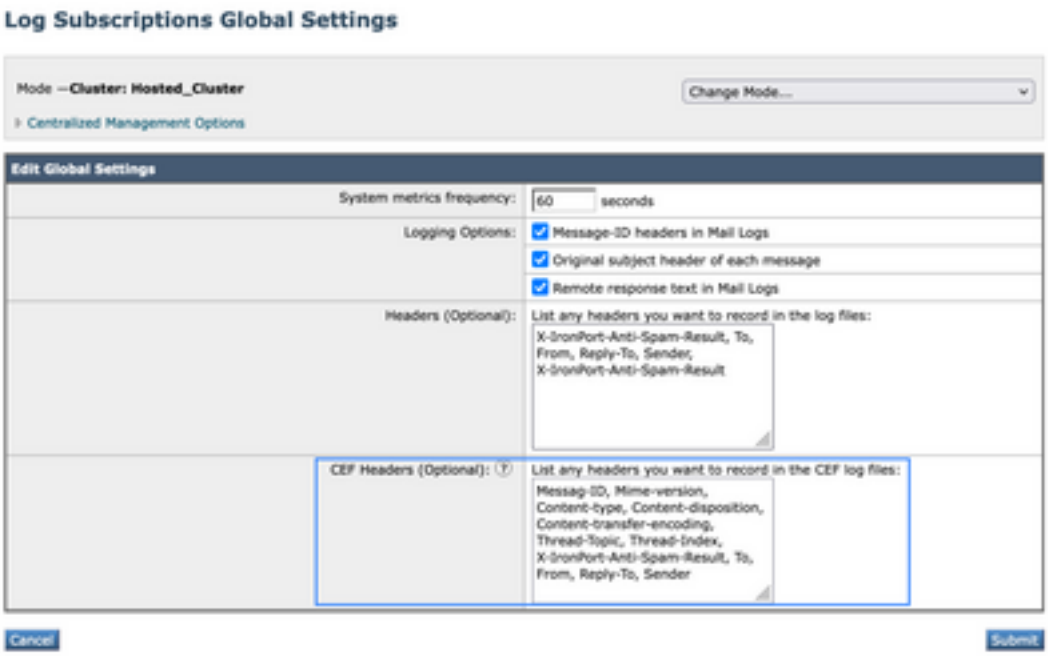
CEFログサブスクリプションのカスタムログエントリ

CEFヘッダー

ログにCEFヘッダーを追加します。

最初にESAにCEFヘッダーを追加します

1. 次に **System Administration > Logs Subscription**
2. クリックする **Edit Settings** [Global Settings]で
3. [CEF Headers]の下で、ログに記録するヘッダーをリストします
4. **Submit and Commit**

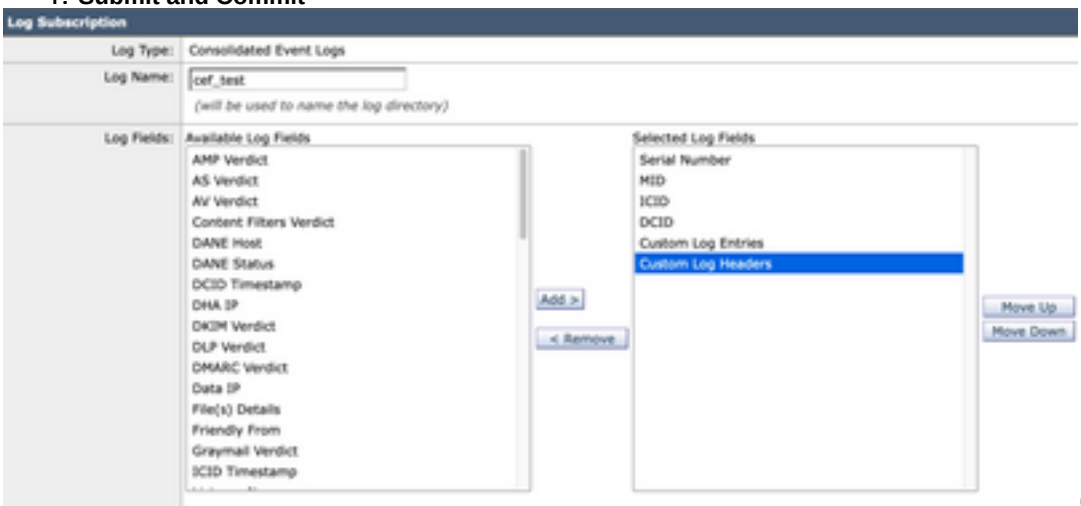


CEFヘッダーの設定

統合イベントログサブスクリプションへのCEFログエントリの追加

次に、統合イベントログサブスクリプションを作成または変更して、以前に記録したCEFヘッダーを追加します。

1. 次に **System Administration > Logs Subscription**
2. 統合イベント・ログの追加または選択
3. 選択 **Custom Log Entries** をクリックし、 **Add**
4. **Submit and Commit**



CEFログサブスクリプションのCEFログヘッダー

関連情報

- エンドユーザガイドESA 14.3
- リリースノートESA 14.3
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。