Configuración de entradas de registro CEF y encabezados CEF en ESA

Contenido

Introducción

En este documento se describe la configuración de la entrada de registro y los encabezados de Common Event Format (CEF) para Cisco Secure Email Gateway (SEG).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Cisco Secure Email Gateway/Email Security Appliance (SEG/ESA)
- Conocimiento de filtros de contenido
- Conocimiento de suscripción de registro

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Email Security Appliance versión 14.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los registros de eventos consolidados resumen cada evento de mensaje en una única línea de registro. Utilice este tipo de registro para reducir el número de bytes de datos (información de registro) enviados a un proveedor de información de seguridad y administración de eventos (SIEM) o a una aplicación para su análisis. Los registros están en el formato de mensaje de registro CEF que es ampliamente utilizado por la mayoría de los proveedores de SIEM.

La entrada de registro CEF y los encabezados CEF se agregan para proporcionar información adicional para realizar un seguimiento y organizar los eventos de correo.

Configurar

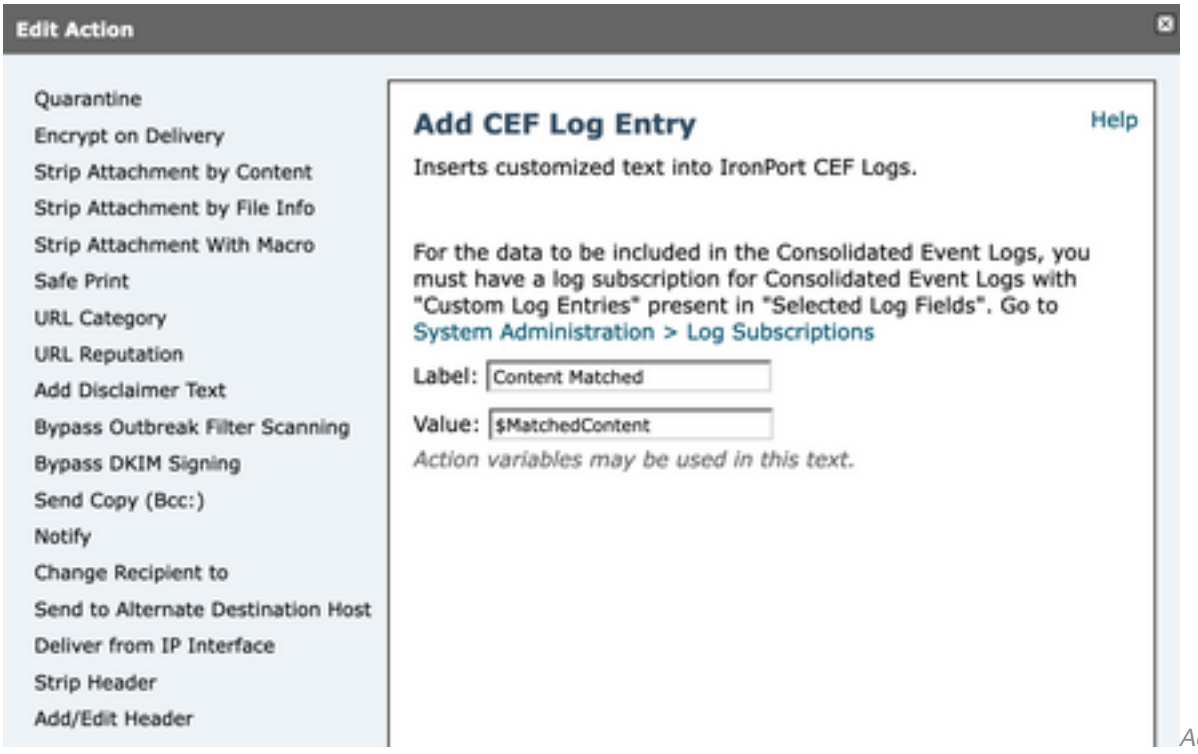
Entrada de registro CEF

Agregar el filtro de contenido entrante/saliente

En primer lugar, cree el filtro de contenido en el ESA:

1. Vaya a **Mail Policies > Incoming/Outgoing content filters**
2. Haga clic en **Add Filter**
3. Asignar nombre al filtro
4. Agregar condición deseada
5. Haga clic en **Add Action**
6. Seleccionar **Add CEF Log Entry**
7. Nombre la etiqueta y uso **Action Variables** para el cuadro de valor
8. **Submit and Commit**

Este ejemplo de documentación que utilizamos **$MatchedContent** Variable de acción, como se muestra en la imagen:



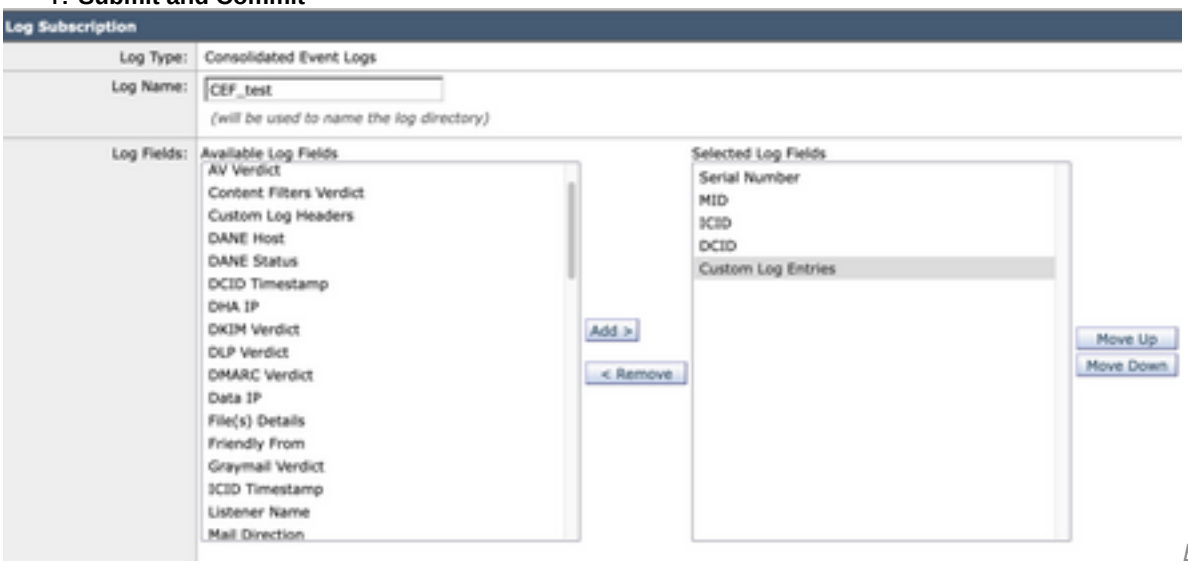
Acción de entrada

de registro CEF en filtros de contenido

Agregar entrada de registro CEF en la suscripción a registro de eventos consolidado

A continuación, cree o modifique la suscripción al registro de eventos consolidado para agregar la entrada de registro de CEF creada anteriormente:

1. Vaya a **System Administration > Log Subscriptions**
2. Agregar o seleccionar los registros de eventos consolidados
3. Seleccionar **Custom Log Entries** y haga clic en **Add**
4. **Submit and Commit**



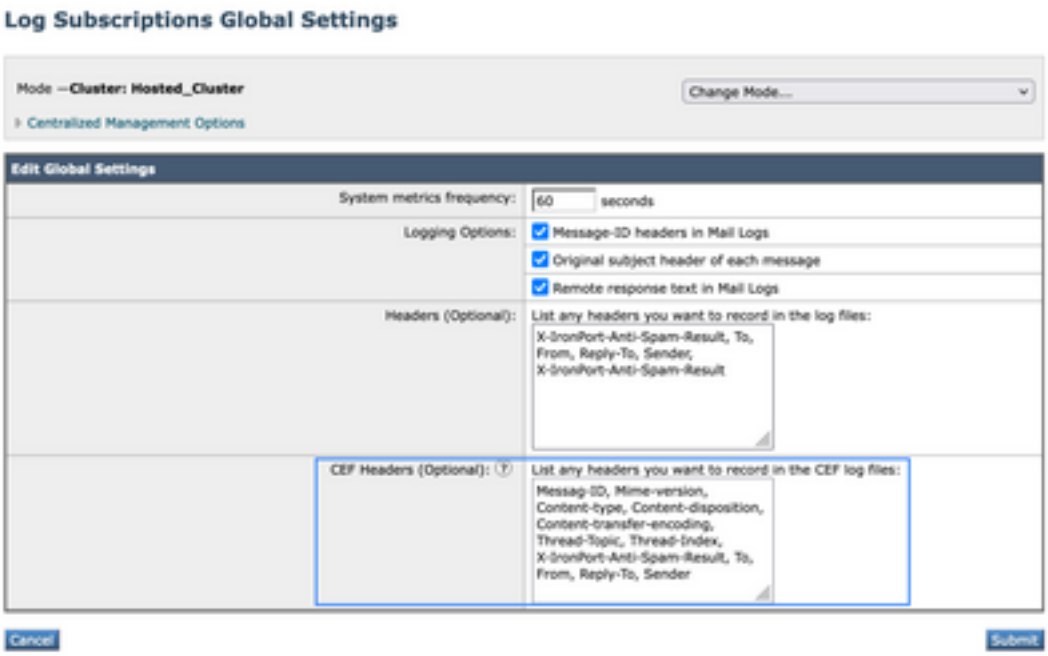
Entradas de registro personalizadas en la suscripción al registro CEF

Encabezados CEF

Agregue los encabezados CEF al registro:

Primero agregue los encabezados CEF en el ESA

1. Vaya a **System Administration > Logs Subscription**
2. Haga clic en **Edit Settings** en Configuración global
3. En Encabezados CEF, indique los encabezados que desea registrar
4. **Submit and Commit**

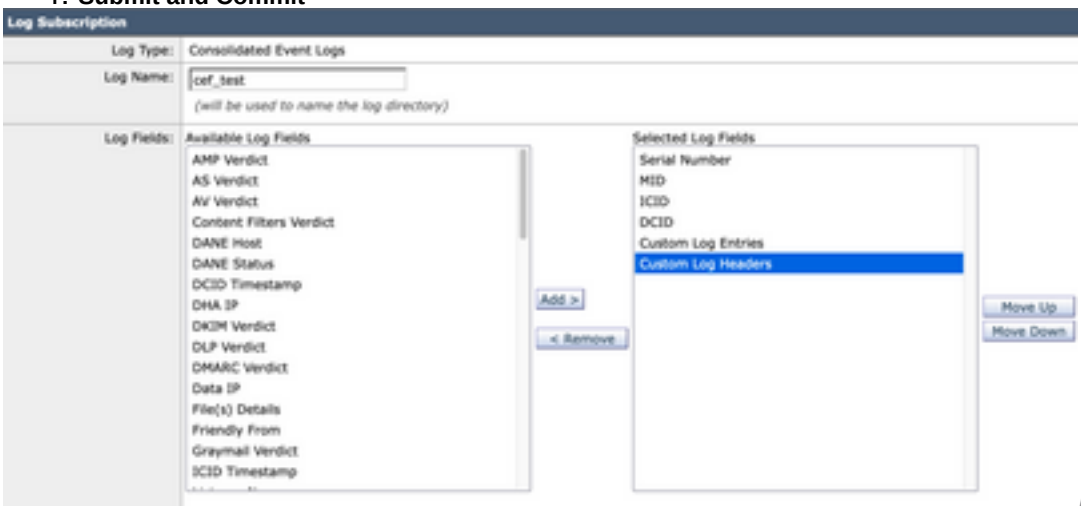


Configuración de encabezados CEF

Agregar entrada de registro CEF en la suscripción a registro de eventos consolidado

A continuación, cree o modifique la suscripción al registro de eventos consolidado para agregar los encabezados CEF previamente registrados:

1. Vaya a **System Administration > Logs Subscription**
2. Agregar o seleccionar los registros de eventos consolidados
3. Seleccionar **Custom Log Entries** y haga clic en **Add**
4. **Submit and Commit**



Encabezados de registro CEF en la suscripción a registro CEF

Información Relacionada

- Guía del usuario final ESA 14.3
- Notas de la versión SEC 14.3
- Soporte Técnico - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).