Configurar entrada de log CEF e cabeçalhos CEF no ESA

Contents

Introduction

Este documento descreve a configuração da entrada de Log do CEF (Common Event Format) e cabeçalhos do SEG (Secure Email Gateway) da Cisco.

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Cisco Secure Email Gateway / Dispositivo de segurança de e-mail (SEG / ESA)
- conhecimento de Filtros de conteúdo
- Conhecimento de inscrição de log

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Email Security Appliance versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os Logs de Eventos Consolidados resumem cada evento de mensagem em uma única linha de log. Use esse tipo de log para reduzir o número de bytes de dados (informações de log) enviados a um fornecedor ou aplicativo de SIEM (Security Information and Event Management) para análise. Os logs estão no formato de mensagem de log CEF amplamente usado pela maioria dos fornecedores de SIEM.

A Entrada de Log CEF e os Cabeçalhos CEF são adicionados para fornecer informações adicionais para rastrear e organizar os eventos de e-mail.

Configurar

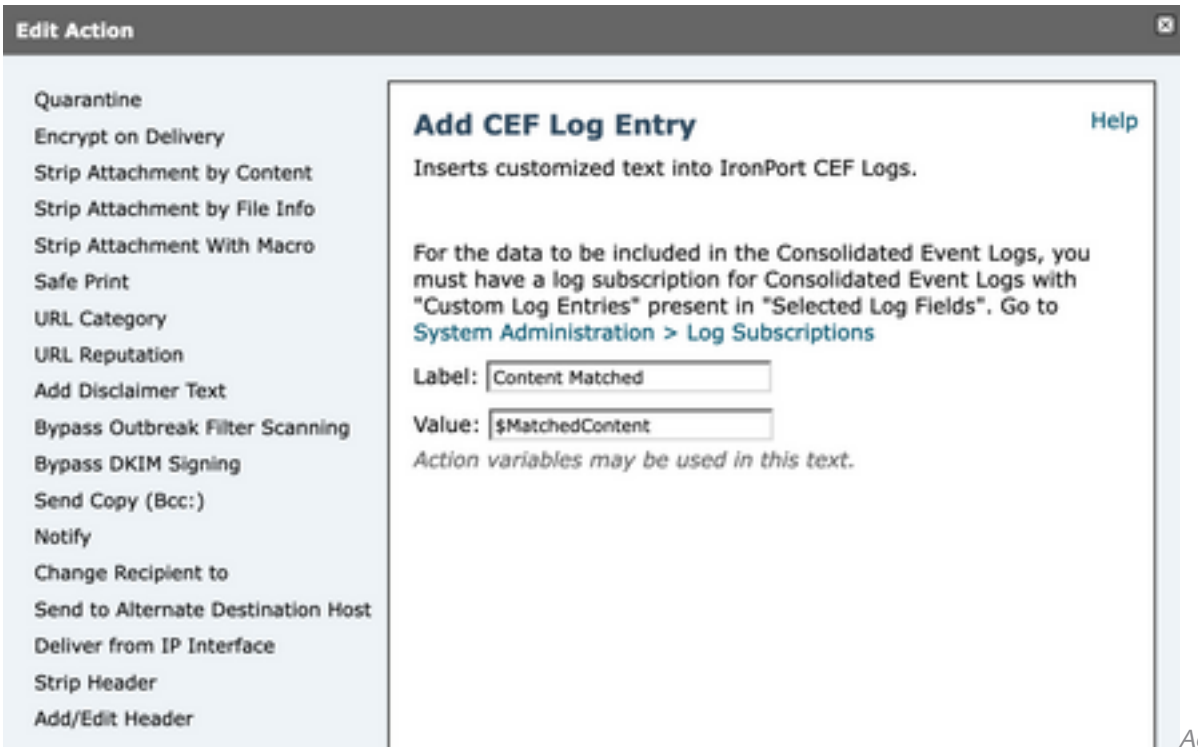
Entrada de Log de CEF

Adicionar o filtro de conteúdo de entrada/saída

Primeiro, crie o filtro de conteúdo no ESA:

1. Ir para **Mail Policies > Incoming/Outgoing content filters**
2. Clique em **Add Filter**
3. Nomear o filtro
4. Adicione a condição desejada
5. Clique em **Add Action**
6. Selecionar **Add CEF Log Entry**
7. Nomear o rótulo e usar **Action Variables** para a caixa de valor
8. **Submit and Commit**

Este exemplo de documentação que usamos **$MatchedContent** Variável de ação, conforme mostrado na imagem:

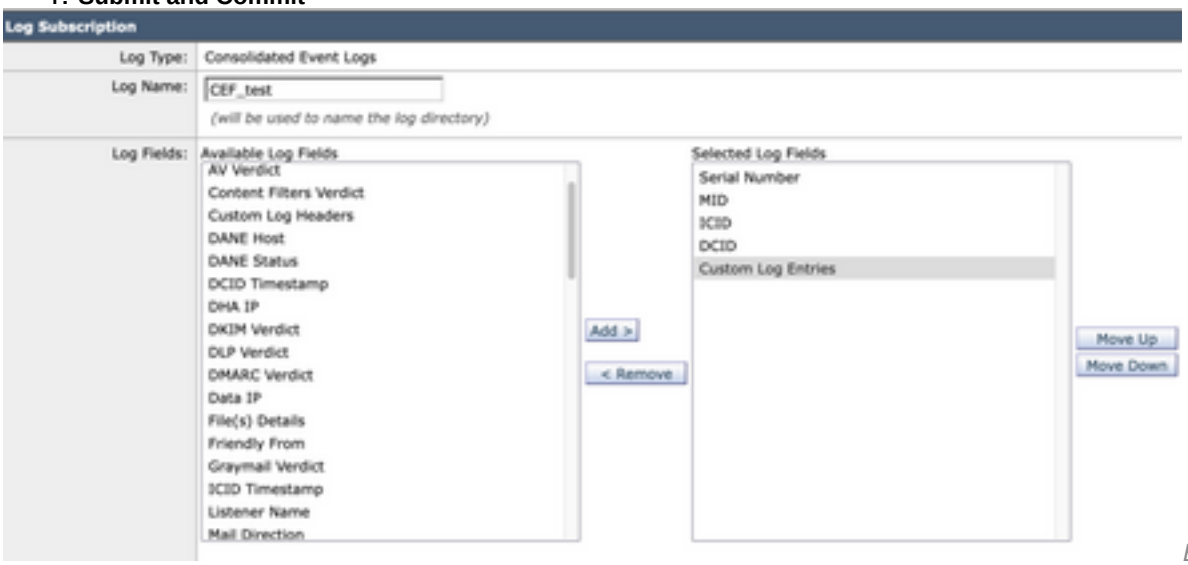


Ação de entrada de Log CEF em filtros de conteúdo

Adicionar Entrada de Log CEF na Assinatura de Log de Eventos Consolidados

Em seguida, crie ou modifique a Inscrição no Log de Eventos Consolidados para adicionar a Entrada de Log CEF criada anteriormente:

1. Ir para **System Administration > Log Subscriptions**
2. Adicionar ou Selecionar os Logs de Eventos Consolidados
3. Selecionar **Custom Log Entries** e clique em **Add**
4. **Submit and Commit**



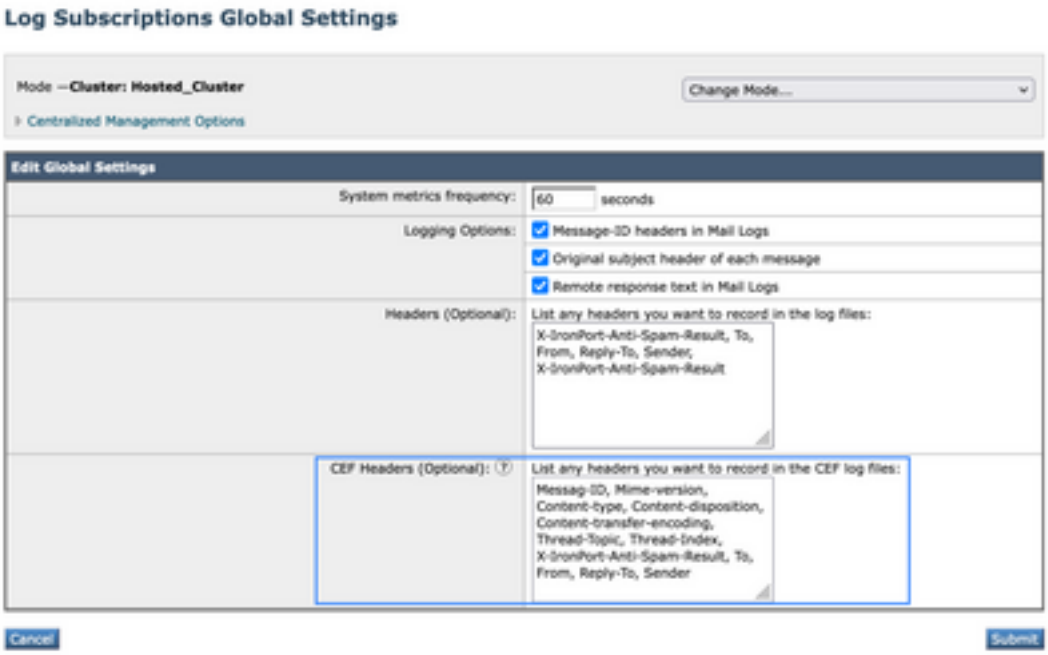
Entradas de log personalizadas na assinatura de log do CEF

Cabeçalhos CEF

Adicione os Cabeçalhos CEF ao log:

Primeiro adicione os cabeçalhos CEF no ESA

1. Ir para **System Administration > Logs Subscription**
2. Clique em **Edit Settings** em Configurações globais
3. Em Cabeçalhos CEF, liste os cabeçalhos a serem registrados
4. **Submit and Commit**

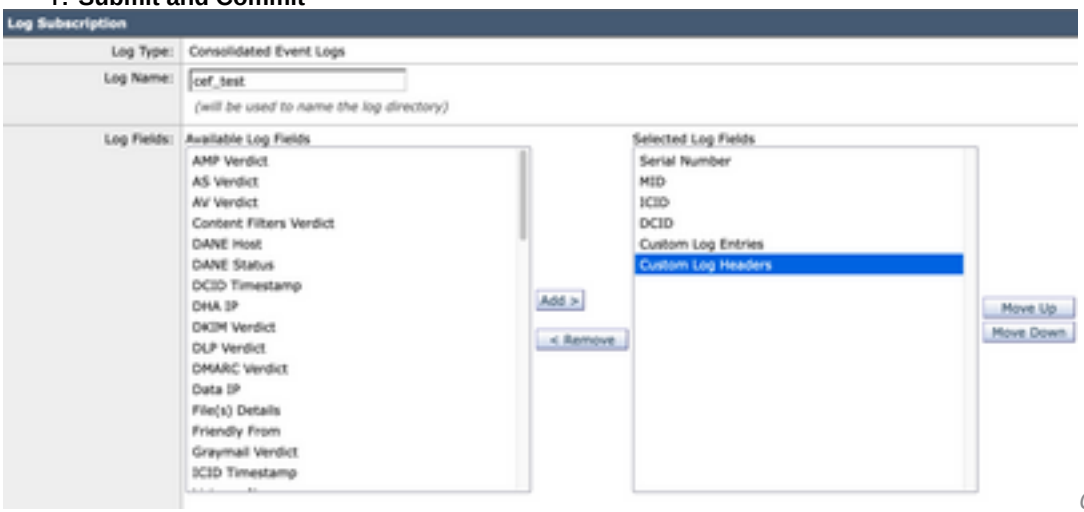


Configuração de Cabeçalhos CEF

Adicionar Entrada de Log CEF na Assinatura de Log de Eventos Consolidados

Em seguida, crie ou modifique a Assinatura do Log de Eventos Consolidados para adicionar os Cabeçalhos CEF previamente gravados:

1. Ir para **System Administration > Logs Subscription**
2. Adicionar ou Selecionar os Logs de Eventos Consolidados
3. Selecionar **Custom Log Entries** e clique em **Add**
4. **Submit and Commit**



Cabeçalhos de Log CEF na Assinatura de Log CEF

Informações Relacionadas

- Guia do usuário final ESA 14.3
- Notas de versão ESA 14.3
- Suporte Técnico - Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.