CEF-logvermeldingen en CEF-koppen in ESA configureren

Inhoud

Inleiding

Dit document beschrijft de configuratie voor het logbestand in Common Event Format (CEF) en de kopregels voor Cisco Secure Email Gateway (SEG).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Cisco Secure Email Gateway/e-mail security applicatie (SEG/ESA)
- Kennis van contentfilters
- Logabonnementskennis

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- E-mail security applicatie versie 14.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Geconsolideerde gebeurtenislogboeken vat elke berichtgebeurtenis in één enkele logregel samen. Gebruik dit logtype om het aantal bytes aan gegevens (loginformatie) te verminderen dat naar een Security Information and Event Management (SIEM)-leverancier of -toepassing voor analyse wordt verzonden. De logboeken zijn in het CEF logboekberichtformaat dat door de meeste SIEM verkopers wijd wordt gebruikt.

CEF Log Entry en CEF Koppen worden toegevoegd om extra informatie te verstrekken om de mail-evenementen te volgen en te organiseren.

Configureren

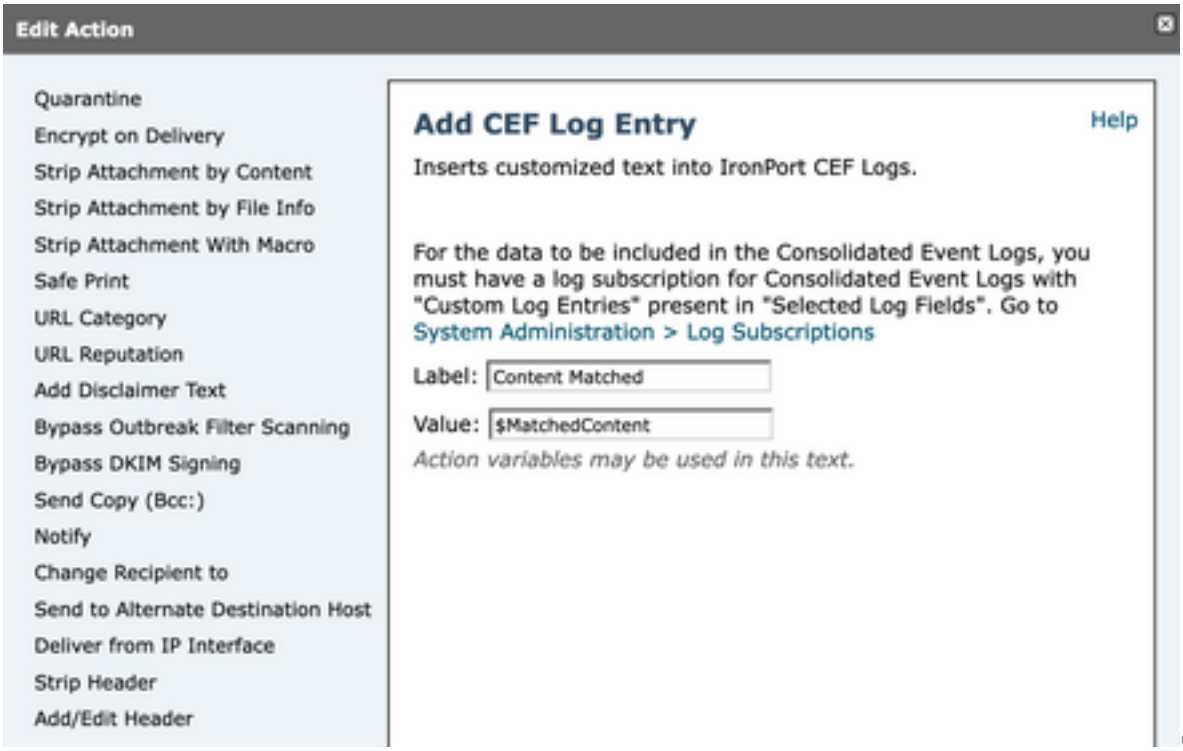
CEF-logingang

Voeg het filter voor inkomende/uitgaande inhoud toe

Maak eerst het inhoudsfilter op de ESA:

1. Ga naar veld **Mail Policies > Incoming/Outgoing content filters**
2. Klik in **Add Filter**
3. Geef het filter een naam
4. Voorwaarde toevoegen
5. Klik in **Add Action**
6. Kiezen **Add CEF Log Entry**
7. Geef het label een naam en gebruik **Action Variables** voor het waardevakje
8. **Submit and Commit**

Dit documentatievoorbeeld gebruiken we **$MatchedContent** Actie Variabele, zoals getoond in de afbeelding:

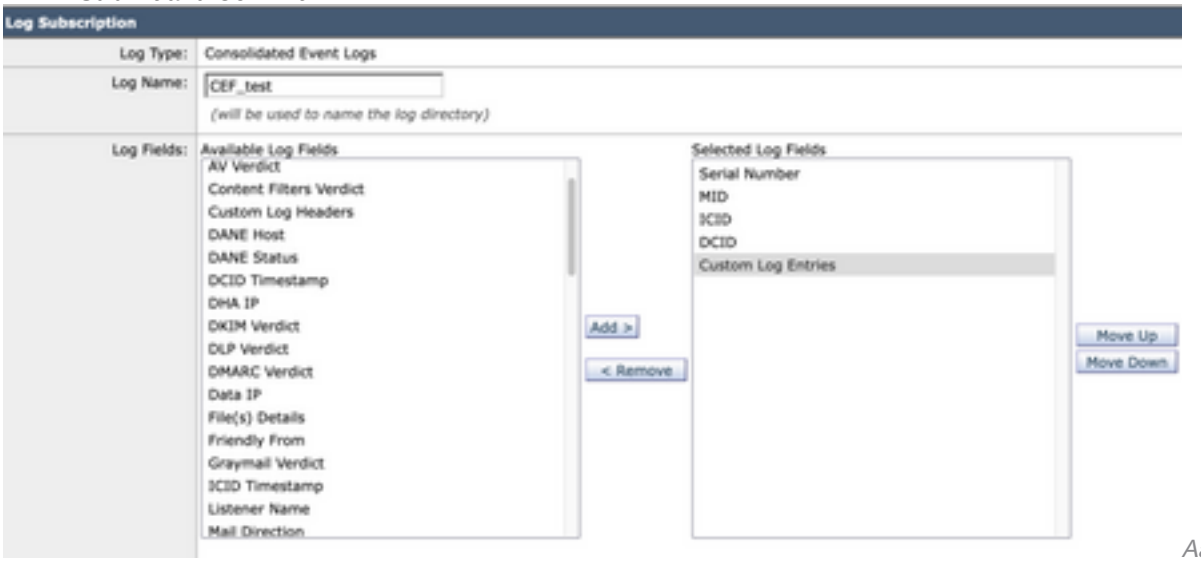


CEF-logboekhandeling in inhoudsfilters

CEF-logboekvermelding toevoegen in het abonnement op geconsolideerd gebeurtenissenlogboek

Maak of wijzig vervolgens het Geconsolideerde Event Log Subscription om de eerder gemaakte CEF-logvermelding toe te voegen:

1. Ga naar veld **System Administration > Log Subscriptions**
2. De geconsolideerde logbestanden voor gebeurtenissen toevoegen of selecteren
3. Kiezen **Custom Log Entries** en klik op **Add**
4. **Submit and Commit**



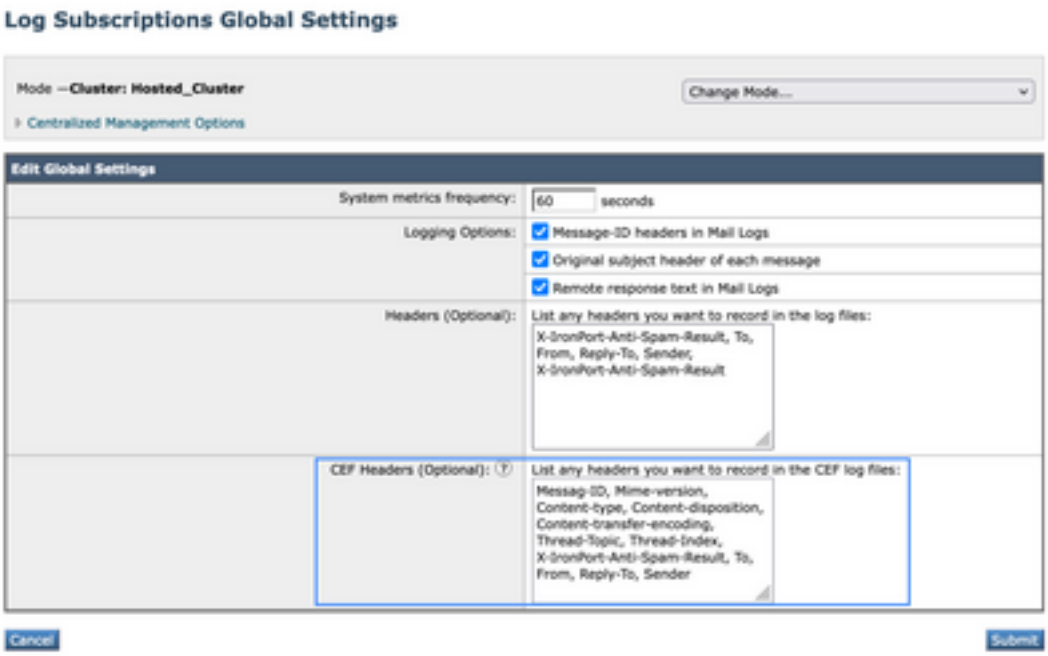
Aangepaste logvermeldingen in CEF-logabonnement

CEF-koppen

Voeg de CEF-koppen toe aan het logbestand:

Voeg eerst de CEF-koppen toe in de ESA

1. Ga naar veld **System Administration > Logs Subscription**
2. Klik in **Edit Settings** onder Globale instellingen
3. Vermeld onder CEF-koppen de kopregels die moeten worden vastgelegd
4. **Submit and Commit**

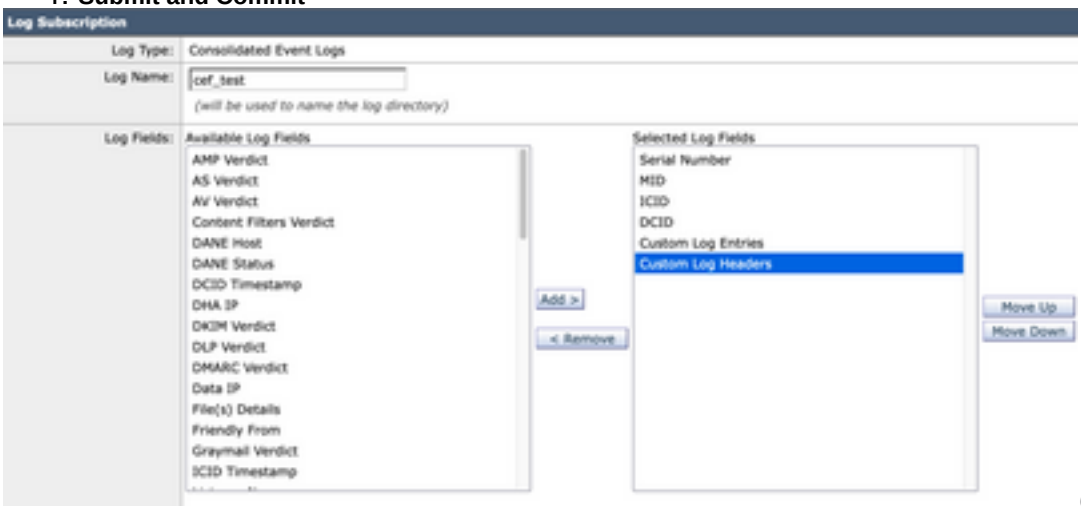


Configuratie van CEF-headers

CEF-logboekvermelding toevoegen in het abonnement op geconsolideerd gebeurtenissenlogboek

Maak of wijzig vervolgens het Geconsolideerde Event Log Subscription om de eerder opgenomen CEF-headers toe te voegen:

1. Ga naar veld **System Administration > Logs Subscription**
2. De geconsolideerde logbestanden voor gebeurtenissen toevoegen of selecteren
3. Kiezen **Custom Log Entries** en klik op **Add**
4. **Submit and Commit**



CEF-logkoppen in CEF-logabonnement

Gerelateerde informatie

- Eindgebruikershandleiding ESR 14.3
- Releaseopmerkingen ESR 14.3
- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.