

CEF-logvermeldingen en CEF-koppen in ESA configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[CEF-logingang](#)

[Voeg het filter voor inkomende/uitgaande inhoud toe](#)

[CEF-logboekvermelding toevoegen in het abonnement op geconsolideerd gebeurtenissenlogboek](#)

[CEF-koppen](#)

[Voeg de CEF-koppen toe aan het logbestand:](#)

[CEF-logboekvermelding toevoegen in het abonnement op geconsolideerd gebeurtenissenlogboek](#)

[Gerelateerde informatie](#)

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

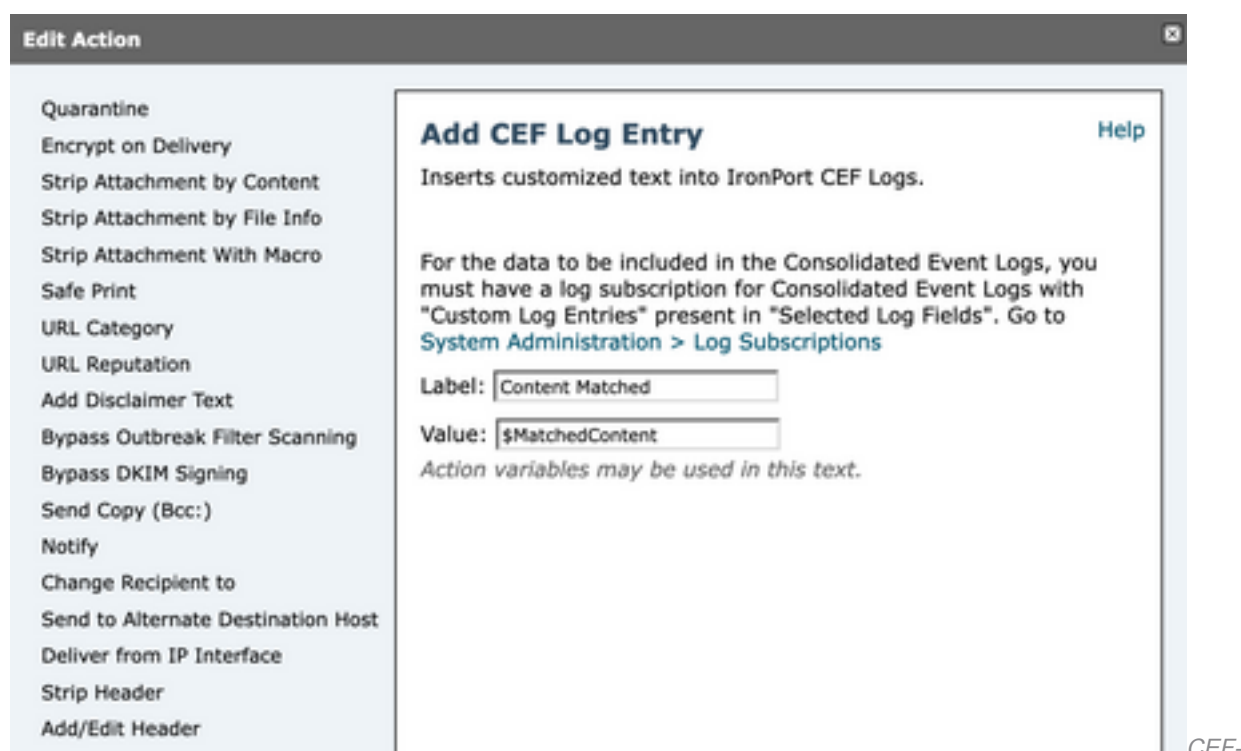
CEF-logingang

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-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**

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

Buttons: Add >, < Remove, Move Up, Move Down

logvermeldingen in CEF-logabonnement

Aangepaste

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**

Log Subscriptions Global Settings

Mode --Cluster: Hosted_Cluster Change Mode...

Centralized Management Options

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:
Message-ID, Mime-version, Content-type, Content-disposition, Content-transfer-encoding, Thread-Topic, Thread-Index, X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender

Cancel Submit

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**

Log Subscription

Log Type: Consolidated Event Logs

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

Log Fields:

Available Log Fields:

- AMP Verdict
- AS Verdict
- AV Verdict
- Content Filters Verdict
- 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

Selected Log Fields:

- Serial Number
- MID
- ICID
- DCID
- Custom Log Entries
- Custom Log Headers

Add > < Remove Move Up Move Down

logabbonnement

CEF-logkopen in CEF-

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.