

CEF-Protokolleintrag und CEF-Header in der ESA konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[CEF-Protokolleintrag](#)

[Hinzufügen des eingehenden/ausgehenden Content-Filters](#)

[Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll](#)

[CEF-Header](#)

[Fügen Sie die zu protokollierenden CEF-Header hinzu:](#)

[Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration für CEF-Protokolleinträge und -Header (Common Event Format) für Cisco Secure Email Gateway (SEG) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Email Gateway/E-Mail Security Appliance (SEG/ESA)
- Kenntnisse zu Content-Filtern
- Kenntnisse zu Protokoll-Abonnements

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Email Security Appliance Version 14.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die konsolidierten Ereignisprotokolle fassen jedes Nachrichtereignis in einer einzigen Protokollzeile zusammen. Verwenden Sie diesen Protokolltyp, um die Anzahl der Byte an Daten (Protokollinformationen) zu reduzieren, die zur Analyse an einen SIEM-Anbieter (Security Information and Event Management) oder eine SIEM-Anwendung gesendet werden. Die Protokolle haben das CEF-Protokollnachrichtenformat, das von den meisten SIEM-Anbietern häufig verwendet wird.

CEF-Protokolleintrag und CEF-Header werden hinzugefügt, um zusätzliche Informationen zum Nachverfolgen und Organisieren von E-Mail-Ereignissen bereitzustellen.

Konfigurieren

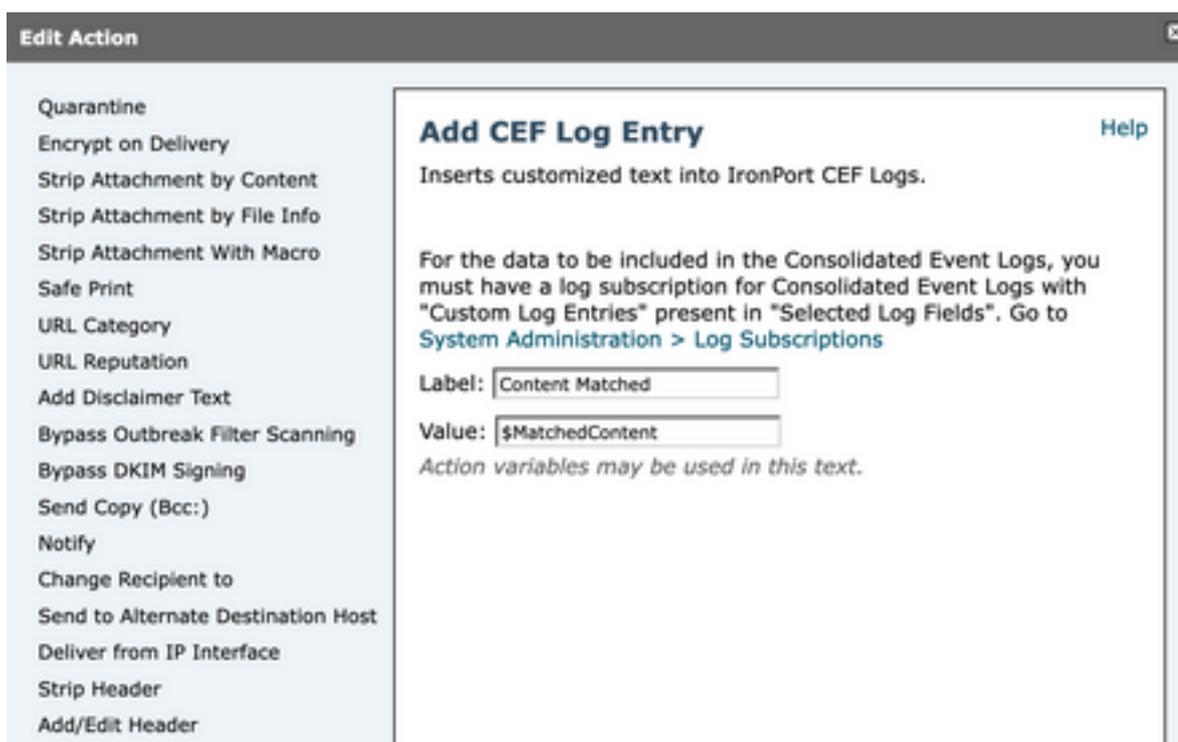
CEF-Protokolleintrag

Hinzufügen des eingehenden/ausgehenden Content-Filters

Erstellen Sie zunächst den Content-Filter auf der ESA:

1. Gehe zu **Mail Policies > Incoming/Outgoing content filters**
2. Klicken Sie in **Add Filter**
3. Filter benennen
4. Bedingung hinzugefügt
5. Klicken Sie in **Add Action**
6. Auswählen **Add CEF Log Entry**
7. Benennen Sie das Label, und verwenden Sie **Action Variables** für das Wertfeld
8. **Submit and Commit**

Dieses Dokumentationsbeispiel verwenden wir `$MatchedContent` Aktionsvariable, wie im Bild gezeigt:



CEF-

Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll

Erstellen oder ändern Sie anschließend das Consolidated Event Log Subscription, um den zuvor erstellten CEF-Protokolleintrag hinzuzufügen:

1. Gehe zu **System Administration > Log Subscriptions**
2. Hinzufügen oder Auswählen der konsolidierten Ereignisprotokolle
3. Auswählen **Custom Log Entries** und klicke auf **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	Selected Log Fields
AV Verdict	Serial Number
Content Filters Verdict	MID
Custom Log Headers	ICID
DANE Host	DCID
DANE Status	Custom Log Entries
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	

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

Benutzerdefinierte

Protokolleinträge in CEF-Protokoll-Subscription

CEF-Header

Fügen Sie die zu protokollierenden CEF-Header hinzu:

Fügen Sie zunächst die CEF-Header in der ESA hinzu.

1. Gehe zu **System Administration > Logs Subscription**
2. Klicken Sie in **Edit Settings** unter Globale Einstellungen
3. Listen Sie unter CEF-Header die zu protokollierenden Header auf.
4. **Submit and Commit**

Log Subscriptions Global Settings

The screenshot shows the 'Log Subscriptions Global Settings' interface. At the top, it indicates 'Mode --Cluster: Hosted_Cluster' and a 'Change Mode...' dropdown. Below this is a 'Centralized Management Options' section. The main area is titled 'Edit Global Settings' and contains several configuration fields:

- System metrics frequency:** Set to 60 seconds.
- Logging Options:** Three checkboxes are checked: 'Message-ID headers in Mail Logs', 'Original subject header of each message', and 'Remote response text in Mail Logs'.
- Headers (Optional):** A text area contains the following headers: 'X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender, X-IronPort-Anti-Spam-Result'.
- CEF Headers (Optional):** A text area contains the following headers: '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'.

Buttons for 'Cancel' and 'Submit' are located at the bottom of the form.

Konfiguration der CEF-Header

Hinzufügen eines CEF-Protokolleintrags im Abonnement für das konsolidierte Ereignisprotokoll

Erstellen oder ändern Sie anschließend das Abonnement für das konsolidierte Ereignisprotokoll, um die zuvor aufgezeichneten CEF-Header hinzuzufügen:

1. Gehe zu **System Administration > Logs Subscription**
2. Hinzufügen oder Auswählen der konsolidierten Ereignisprotokolle
3. Auswählen **Custom Log Entries** und klicke auf **Add**
4. **Submit and Commit**

The screenshot shows the 'Log Subscription' configuration page. It is set to 'Consolidated Event Logs'. The 'Log Name' field contains 'cef_test' with a note '(will be used to name the log directory)'. The 'Log Fields' section is divided into two columns:

- Available Log Fields:** A list of various log fields including 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, and ICID Timestamp.
- Selected Log Fields:** A list of selected fields including Serial Number, MID, ICID, DCID, Custom Log Entries, and Custom Log Headers. The 'Custom Log Headers' field is currently selected and highlighted.

Buttons for 'Add >', '< Remove', 'Move Up', and 'Move Down' are visible between the two columns.

CEF-Protokoll-Subscription

CEF-Protokoll-Header in

Zugehörige Informationen

- [Benutzerhandbuch ESGV 14.3](#)
- [Versionshinweise ESA 14.3](#)
- [Technischer Support – Cisco Systems](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.