# Fehlerbehebung bei Problemen zwischen dem FireSIGHT-System und dem eStreamer-Client (SIEM)

## Inhalt



## Einleitung

Mit dem Event Streamer (eStreamer) können Sie mehrere Arten von Ereignisdaten von einem FireSIGHT-System zu einer benutzerdefinierten Clientanwendung streamen. Nachdem Sie eine Client-Anwendung erstellt haben, können Sie sie mit einem eStreamer-Server (z. B. einem FireSIGHT Management Center) verbinden, den eStreamer-Dienst starten und mit dem Datenaustausch beginnen. Für die eStreamer-Integration ist eine benutzerdefinierte Programmierung erforderlich, Sie können jedoch bestimmte Daten von einer Appliance anfordern. In diesem Dokument wird die Kommunikation eines eStreamer-Clients und die Fehlerbehebung bei einem Client beschrieben.

# Kommunikationsmethode zwischen eStreamer-Client und -Server

Die Kommunikation zwischen einem Client und dem eStreamer-Service erfolgt in vier wichtigen Phasen:

## Schritt 1: Client stellt Verbindung mit eStreamer-Server her

Zunächst stellt ein Client eine Verbindung mit dem eStreamer-Server her und die Verbindung wird von beiden Seiten authentifiziert. Bevor ein Client Daten von eStreamer anfordern kann, muss er eine SSL-fähige TCP-Verbindung mit dem eStreamer-Dienst initiieren. Wenn der Client die Verbindung initiiert, antwortet der eStreamer-Server und initiiert einen SSL-Handshake mit dem Client. Als Teil des SSL-Handshakes fordert der eStreamer-Server das Authentifizierungszertifikat des Clients an und überprüft, ob das Zertifikat gültig ist.

Nachdem die SSL-Sitzung hergestellt wurde, führt der eStreamer-Server eine zusätzliche Überprüfung des Zertifikats nach der Verbindung durch. Nach Abschluss der Verbindungsüberprüfung wartet der eStreamer-Server auf eine Datenanfrage vom Client.

## Phase 2: Client fordert Daten vom eStreamer-Dienst an

In diesem Schritt fordert der Client Daten vom eStreamer-Dienst an und gibt die zu streamenden Datentypen an. Eine einzelne Ereignisanforderungsmeldung kann eine beliebige Kombination verfügbarer Ereignisdaten angeben, einschließlich Ereignismetadaten. Bei einer Anfrage für ein einzelnes Hostprofil kann ein einzelner Host oder mehrere Hosts angegeben werden. Es stehen zwei Anforderungsmodi zum Anfordern von Ereignisdaten &colon zur Verfügung.

- **Event Stream-Anforderung:** Der Client sendet eine Nachricht mit Anforderungsflags, die die angeforderten Ereignistypen und die Version jedes Typs angeben. Der eStreamer-Server antwortet, indem er die angeforderten Daten streamt.
- **Erweiterte Anforderung:** Der Client sendet eine Anforderung mit demselben Nachrichtenformat wie für Event Stream-Anforderungen, legt jedoch ein Flag für eine erweiterte Anforderung fest. Dadurch wird eine Nachrichteninteraktion zwischen Client und eStreamer-Server initiiert, über die der Client zusätzliche Informationen und Versionskombinationen anfordert, die über Event Stream-Anforderungen nicht verfügbar sind.

## Schritt 3: eStreamer richtet den angeforderten Datenstrom ein

In dieser Phase richtet eStreamer den angeforderten Datenstrom zum Client ein. In Zeiten der Inaktivität sendet eStreamer regelmäßig Nullmeldungen an den Client, um die Verbindung offen

zu halten. Wenn er eine Fehlermeldung vom Client oder einem Zwischenhost erhält, wird die Verbindung geschlossen.

### Schritt 4: Die Verbindung wird beendet

Der eStreamer-Server kann eine Client-Verbindung auch aus folgenden Gründen schließen:

- Bei jedem Senden einer Nachricht tritt ein Fehler auf. Dies umfasst sowohl Ereignisdatennachrichten als auch die Null-Keep-Alive-Nachricht, die eStreamer in Inaktivitätszeiträumen sendet.
- Beim Verarbeiten einer Clientanforderung tritt ein Fehler auf.
- Die Client-Authentifizierung schlägt fehl (es wird keine Fehlermeldung gesendet).
- Der eStreamer-Dienst wird heruntergefahren (es wird keine Fehlermeldung gesendet).

## Client zeigt kein Ereignis an

Wenn in Ihrer eStreamer-Client-Anwendung keine Ereignisse angezeigt werden, befolgen Sie die folgenden Schritte, um dieses Problem zu beheben:

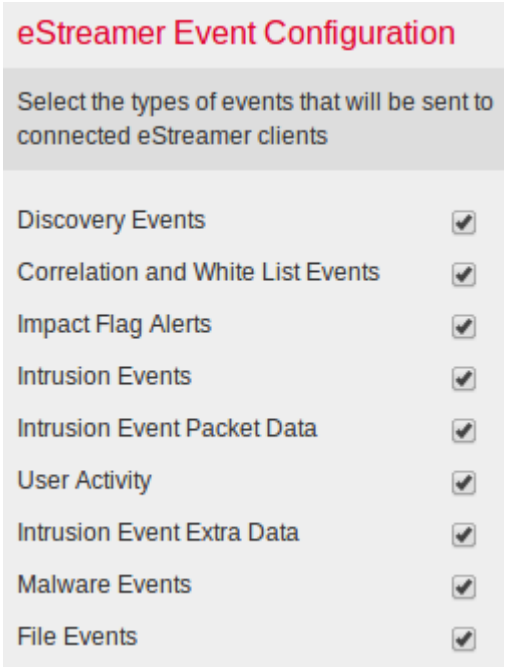
### Schritt 1: Überprüfen der Konfiguration

Sie können steuern, welche Arten von Ereignissen der eStreamer-Server an Clientanwendungen übertragen kann, die sie anfordern. Führen Sie zum Konfigurieren der von eStreamer übertragenen Ereignistypen die folgenden Schritte aus:

1. Navigieren Sie zu **System > Local > Registration**.

2. Klicken Sie auf die Registerkarte **eStreamer**.

3. Aktivieren Sie im Menü **eStreamer Event Configuration** die Kontrollkästchen neben den Ereignistypen, die eStreamer an anfordernde Clients senden soll.




> **Anmerkung:** Stellen Sie sicher, dass die Clientanwendung die Ereignistypen anfordert, die sie empfangen soll. Die Anforderungsnachricht muss an den eStreamer-Server (FireSIGHT Management Center oder verwaltetes Gerät) gesendet werden.

4. Klicken Sie auf **Speichern**.

## Phase 2: Zertifikat überprüfen

Stellen Sie sicher, dass die erforderlichen Zertifikate hinzugefügt wurden. Bevor eStreamer eStreamer-Ereignisse an einen Client senden kann, muss der Client über die eStreamer-Konfigurationsseite zur Peers-Datenbank des eStreamer-Servers hinzugefügt werden. Das vom eStreamer-Server generierte Authentifizierungszertifikat muss ebenfalls auf den Client kopiert werden.

## Schritt 3: Fehlermeldungen überprüfen

Identifizieren Sie offensichtliche eStreamer-bezogene Fehler in /var/log/messages mit dem folgenden Befehl:

```
admin@FireSIGHT:~$ grep -i estreamer /var/log/messages | grep -i error
```

## Schritt 4: Überprüfen der Verbindung

Überprüfen Sie, ob der Server eingehende Verbindungen akzeptiert.

```
admin@FireSIGHT:~$ netstat -an | grep 8302
```

Die Ausgabe sollte wie folgt aussehen. Andernfalls wird der Dienst möglicherweise nicht

ausgeführt.

```
tcp 0 0 <local_ip>:8302 0.0.0.0:* LISTEN
```

### Schritt 5: Überprüfen des Status des Prozesses

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob ein sfestreamer-Prozess ausgeführt wird:

```
admin@FireSIGHT:~$ pstree -a | grep -i sfestreamer
```

## Client zeigt doppelte Ereignisse an

### Behandeln doppelter Ereignisse, die in einem Client angezeigt werden

Der eStreamer-Server speichert keinen Verlauf der von ihm gesendeten Ereignisse, daher muss die Client-Anwendung auf doppelte Ereignisse überprüfen. Doppelte Ereignisse können aus verschiedenen Gründen auftreten.  Wenn Sie beispielsweise eine neue Streaming-Sitzung starten, kann die vom Client als Startpunkt für die neue Sitzung angegebene Zeit mehrere Nachrichten enthalten, von denen einige in der vorherigen Sitzung gesendet wurden, andere jedoch nicht. eStreamer sendet alle Nachrichten, die die angegebenen Anforderungskriterien erfüllen. EStreamer-Client-Anwendungen sollten so konzipiert sein, dass daraus resultierende Duplikate erkannt und dedupliziert werden können.

### Doppelte Datenanforderungen verwalten

Wenn Sie mehrere Versionen derselben Daten anfordern, entweder durch mehrere Flags oder mehrere erweiterte Anforderungen, wird die höchste Version verwendet. Wenn eStreamer beispielsweise Flags-Anforderungen für die Erkennungsereignisse Version 1 und 6 und eine erweiterte Anforderung für Version 3 empfängt, sendet er Version 6.

## Client zeigt falsche Snort Rule ID (SID) an

Dies geschieht in der Regel aufgrund eines SID-Konflikts, wenn eine Regel in das System importiert wird und die SID intern neu zugeordnet wird.

Um die eingegebene SID anstelle der neu zugeordneten SID zu verwenden, müssen Sie den *erweiterten Header* aktivieren. Bit 23 fordert erweiterte Ereignisheader an. Wenn dieses Feld auf 0 gesetzt ist, werden Ereignisse mit einem Standard-Ereignisheader gesendet, der nur den Datensatztyp und die Datensatzlänge enthält.

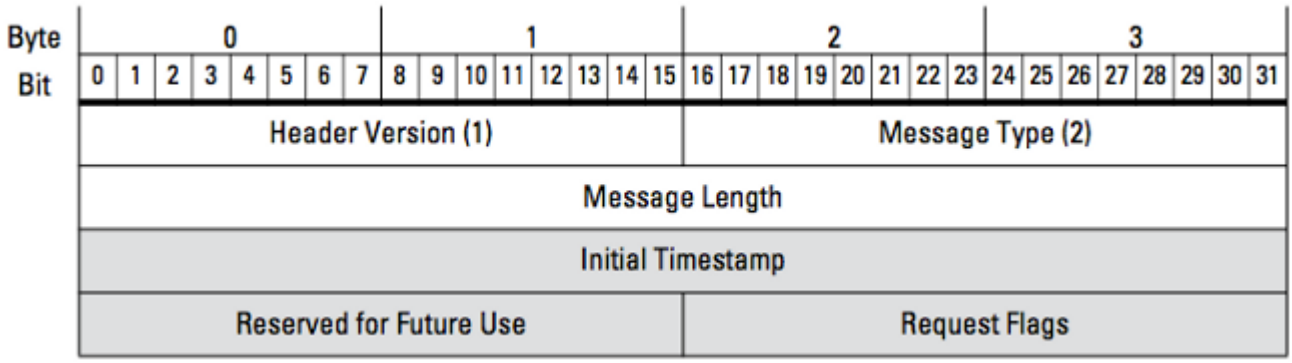



*Abbildung: Das Diagramm zeigt das Nachrichtenformat, das zum Anfordern von Daten von eStreamer verwendet wird. Die Felder für das Format der Anforderungsnachricht sind grau hervorgehoben.*

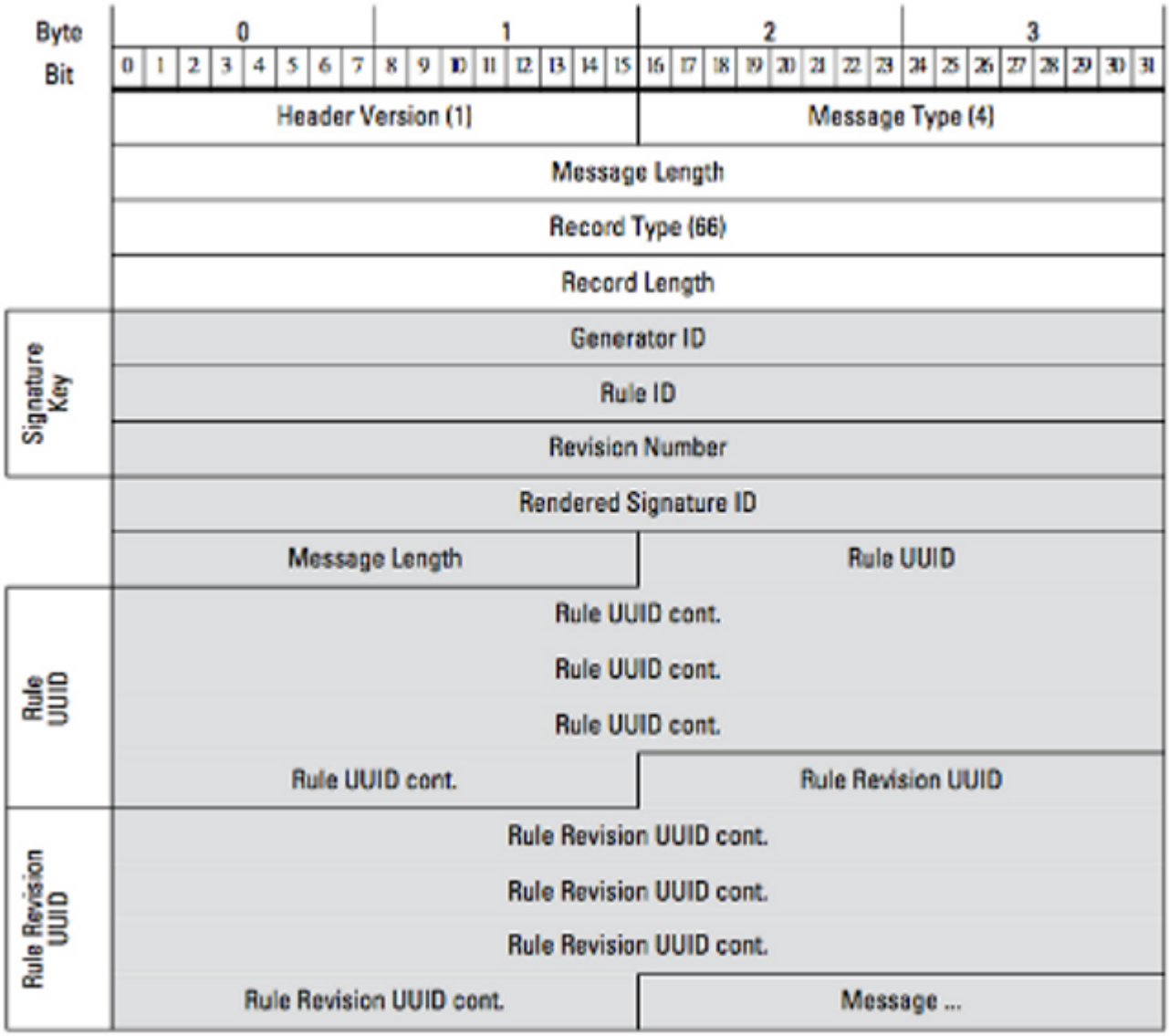



*Abbildung: Das Diagramm veranschaulicht das Format der Regelmeldungsinformationen für ein Ereignis, das innerhalb eines Regelmeldungsdatensatzes übertragen wird. Es zeigt die **RuleID** (die Sie jetzt verwenden) und die **Rendered Signature ID** (die Nummer, die Sie erwarten).*

**Tipp:** Eine detaillierte Beschreibung der einzelnen Bits und Nachrichten finden Sie im

*eStreamer Integration Guide*.

# Erfassung und Analyse zusätzlicher Daten zur Fehlerbehebung

## Testen mit dem Skript ssl_test.pl

Verwenden Sie das Skript ssl_test.pl im *Event Streamer Software Development Kit (SDK)* zur Problemermittlung. Das SDK ist in einer ZIP-Datei auf der Support-Website verfügbar. Anweisungen für das Skript finden Sie in der Datei README.txt, die in dieser ZIP-Datei enthalten ist.

## Erfassungspaket (PCAP)

Erfassen und analysieren Sie Pakete auf der Management-Schnittstelle des eStreamer-Servers. Stellen Sie sicher, dass der Datenverkehr in Ihrem Netzwerk nicht blockiert oder abgelehnt wird.

## Fehlerbehebungsdatei generieren

Wenn Sie die obigen Schritte zur Fehlerbehebung durchgeführt haben und das Problem weiterhin nicht identifizieren können, erstellen Sie eine Problembehebungsdatei in FireSIGHT Management Center. Liefern Sie alle zusätzlichen Daten zur Fehlerbehebung zur weiteren Analyse an den technischen Support von Cisco.

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.