



# **RSA** | Security Analytics

Versenden von Warnmeldungen mit ESA  
für Version 10.6

## **Marken**

RSA, das RSA Logo und Copyright 2016 EMC Deutschland GmbH sind Marken oder eingetragene Marken der Copyright 2016 EMC Deutschland GmbH Copyright 2016 EMC Deutschland GmbH in den USA und/oder in anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber. Eine Liste der EMC Marken finden Sie unter [germany.emc.com/legal/emc-corporation-trademarks.htm](http://germany.emc.com/legal/emc-corporation-trademarks.htm).

## **Lizenzvereinbarung**

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden. Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

## **Drittanbieterlizenzen**

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, der sich auf Drittanbietersoftware in diesem Produkt bezieht, ist in der Datei „thirdpartylicenses.pdf“ zu finden.

## **Hinweis zu Verschlüsselungstechnologien**

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

## **Verteilung**

Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von EMC ist eine entsprechende Softwarelizenz erforderlich. EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. DIE EMC CORPORATION MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.



# Inhalt

---

<b>Erste Schritte mit ESA</b> .....	<b>11</b>
Best Practices .....	11
Grundlegendes zu Event Stream Analysis-Regeltypen .....	11
Best Practices für das Schreiben von Regeln .....	13
Best Practices zur Verwendung von RSA Live-Regeln .....	14
Best Practices für die Bereitstellung von Regeln .....	15
Best Practices für die Systemintegrität .....	15
Troubleshooting für ESA .....	16
Troubleshooting bei ESA-Services .....	17
Troubleshooting bei ESA-Datenbankproblemen .....	19
Troubleshooting bei RSA Live-Regeln für ESA .....	20
Troubleshooting für Bereitstellungen .....	22
Troubleshooting bei Regeln .....	22
Schritte zur Behebung von Speicherproblemen, wenn ein ESA-Service offline ist .....	23
Anzeigen von Speicherkennzahlen für Regeln .....	30
Voraussetzungen .....	30
Methoden .....	31
<b>So erzeugt ESA Warnmeldungen</b> .....	<b>35</b>
Vertrauliche Daten .....	35
Wie ESA vertrauliche Daten von Security Analytics-Core behandelt .....	36
Erweiterte EPL-Regel .....	36
Erweiterungsquelle .....	36
<b>ESA-Regeltypen</b> .....	<b>39</b>
Starterpaketregeln .....	39
Testregelmodus .....	39
Rollenberechtigungen .....	40
Üben mit Starterpaket-Regeln .....	41
Regelbibliothek .....	42
Verfahren .....	43

<b>Verwenden von Testregeln</b> .....	<b>45</b>
Bereitstellen von Regeln als Testregeln .....	46
Verfahren .....	46
Anzeigen von Speicherkennzahlen für Regeln im Testmodus .....	47
Voraussetzungen .....	49
Methoden .....	49
<b>Hinzufügen von Regeln zur Regelbibliothek</b> .....	<b>51</b>
Herunterladen von konfigurierbaren ESA-Regeln von RSA Live .....	51
Voraussetzungen .....	52
Verfahren .....	52
Anpassen von RSA Live ESA-Regeln .....	54
Hinzufügen einer Regelerstellungsregel .....	55
Schritt 1. Benennen und Beschreiben der Rolle .....	56
Schritt 2. Erstellen einer Regelanweisung .....	57
So fügen Sie eine Whitelist hinzu .....	59
So fügen Sie eine Blacklist hinzu .....	60
Beispiel: Blacklist .....	60
Beispiel: Groß-/Kleinschreibung ignorieren, strenge Musterübereinstimmung und Operator Is Not Null .....	62
Beispielergebnisse .....	66
Beispiel: Gruppieren der Regelergebnisse .....	68
Beispiel: Arbeiten mit numerischen Operatoren .....	69
Schritt 3. Hinzufügen von Bedingungen zu einer Regelanweisung .....	70
Hinzufügen einer erweiterten EPL-Regel .....	72
Voraussetzungen .....	72
Verfahren .....	73
Event Processing Language (EPL) .....	74
ESA-Anmerkungen .....	75
Beispiele für erweiterte EPL-Regeln .....	76
EPL Nr. 1: .....	76
EPL Nr. 2: .....	77

EPL Nr. 3: .....	78
EPL Nr. 4: Verwenden von NamedWindows und match_recognize .....	79
EPL Nr. 5: Verwenden von Every @RSAAlert(oneInSeconds=0, identifiers={user_src}) .....	80
EPL Nr. 6: @RSAAlert(oneInSeconds=0, identifiers={ip_src}) .....	80
EPL Nr. 7: @RSAAlert(oneInSeconds=0, identifiers={"ip_src"}) .....	81
EPL Nr. 8: Verwenden von groupwin , time_length_batch und unique .....	82
EPL Nr. 9: Verwenden von groupwin, time_length und unique .....	83
EPL Nr. 10: Verwenden von groupwin , time_length_batch und unique .....	83
Arbeiten mit Regeln .....	85
Bearbeiten, Duplizieren oder Löschen einer Regel .....	85
Bearbeiten einer Regel .....	85
Duplizieren von Regeln .....	86
Löschen einer Regel .....	86
Filtern oder Suchen von Regeln .....	87
Filter .....	87
Suchen .....	88
Importieren oder Exportieren von Regeln .....	88
Importieren von ESA-Regeln .....	88
Export .....	89
<b>Auswählen von Benachrichtigungsmethoden über Warnmeldungen ....</b>	<b>91</b>
Benachrichtigungsmethoden .....	92
Hinzufügen einer Benachrichtigungsmethode zu einer Regel .....	94
Voraussetzungen .....	94
Verfahren .....	94
<b>Hinzufügen einer Datenerweiterungsquelle .....</b>	<b>97</b>
Beispielregel mit Erweiterung .....	98
Konfigurieren einer Datenbankverbindung .....	100

Verfahren .....	101
Erweiterungsquellen .....	103
Konfigurieren einer Datenbank als Erweiterungsquelle .....	104
Konfigurieren einer In-Memory-Tabelle als Erweiterungsquelle .....	106
Konfigurieren einer Ad-hoc-In-Memory-Tabelle .....	107
Hinzufügen einer wiederkehrenden In-Memory-Tabelle .....	110
Konfigurieren von Warehouse Analytics als Erweiterungsquelle .....	112
Hinzufügen einer Erweiterung zu einer Regel .....	114
Verfahren .....	114
<b>Bereitstellen von Regeln für die Ausführung in ESA .....</b>	<b>117</b>
Funktionsweise der Bereitstellung .....	117
Bereitstellungsschritte .....	118
Schritt 1. Hinzufügen einer Bereitstellung .....	118
Schritt 2. Hinzufügen eines ESA-Services .....	119
Schritt 3. Hinzufügen und Bereitstellen von Regeln .....	121
Zusätzliche Bereitstellungsverfahren .....	122
Löschen eines ESA-Services in einer Bereitstellung .....	123
Bearbeiten oder Löschen einer Regel in einer Bereitstellung .....	123
Bearbeiten einer Regel .....	124
Löschen einer Regel .....	124
Bearbeiten oder Löschen einer Bereitstellung .....	124
Anzeigen der Aktualisierungen an einer Bereitstellung .....	126
<b>Anzeigen von ESA-Statistiken und -Warnmeldungen .....</b>	<b>127</b>
Anzeigen der Statistiken zu einem ESA-Service .....	127
Methoden .....	127
Anzeigen einer Zusammenfassung der Warnmeldungen .....	129
Verfahren .....	129
<b>Automatisierte Bedrohungserkennung .....</b>	<b>133</b>
Verstehen der automatisierten Bedrohungserkennung .....	133
Workflow .....	134
Konfigurieren der automatisierten Bedrohungserkennung .....	136
Voraussetzungen .....	136

Verfahren: Konfigurieren der automatisierten Bedrohungserkennung .....	136
Ergebnis .....	144
Nächste Schritte .....	144
Arbeiten mit Ergebnissen der automatisierten Bedrohungserkennung .....	144
Ergebnisse der Bedrohungserkennung verstehen .....	144
Was als nächstes zu tun ist .....	147
	149
Troubleshooting der automatisierten Bedrohungserkennung .....	149
Mögliche Probleme .....	151
<b>Referenzen .....</b>	<b>155</b>
Registerkarte „Neue erweiterte EPL-Regel“ .....	155
Funktionen .....	156
Ansicht Zusammenfassung der Wammeldungen .....	158
Funktionen .....	159
Dialogfeld „Anweisung erstellen“ .....	163
Funktionen .....	164
Dialogfeld „ESA-Regeln bereitstellen“ .....	167
Funktionen .....	168
Dialogfeld „ESA-Services bereitstellen“ .....	169
Funktionen .....	169
Registerkarte Regelerstellung .....	170
Funktionen .....	170
Registerkarte Regeln .....	175
Funktionen .....	176
Bereich „Optionen“ .....	176
Abschnitt Regeln .....	177
Abschnitt Bereitstellungen .....	177
Bereich „Regelbibliothek“ .....	177
Symbolleiste Regelbibliothek .....	179
Regelbibliotheksliste .....	179
Bereich „Bereitstellung“ .....	181
ESA-Services .....	181



ESA-Regeln .....	182
Dialogfeld Regelsyntax .....	183
Funktionen .....	184
Dialogfeld „ESA-Service auswählen“ .....	185
Funktionen .....	186
Registerkarte Services .....	186
Funktionen .....	187
Bereich „Statistik für bereitgestellte Regeln“ .....	189
	189
Registerkarte „Einstellungen“ .....	190
Funktionen .....	191
Datenbankverbindungen .....	191
Dialogfeld „Aktualisierungen an der Bereitstellung“ .....	192
Funktionen .....	193



## Erste Schritte mit ESA

---

Dieses Thema enthält eine Kurzanleitung zu Event Stream Analysis (ESA), um Ihnen bei den ersten Schritten mit ESA zu helfen. Die folgenden Themen dienen dazu, Sie bei der Arbeit mit ESA zu unterstützen.

- Dieses Thema hilft Ihnen dabei zu verstehen, wie Sie am besten Regeln einrichten, bereitstellen und erstellen. Siehe [Best Practices](#)
- Dieses Thema hilft Ihnen beim Troubleshooting verschiedener Aspekte von ESA, einschließlich dem Erstellen und der Bereitstellung von Regeln: [Troubleshooting für ESA](#)
- Dieses Thema unterstützt Sie beim Arbeiten mit Speicherkennzahlen, um den Gesamtverbrauch an Arbeitsspeicher für ESA-Services zu verstehen. Siehe [Anzeigen von Speicherkennzahlen für Regeln](#)

### Best Practices

In den Best Practices finden Sie Guidelines zum Schreiben, Verwalten und Bereitstellen von Regeln sowie zur Bewahrung der Systemintegrität für die ESA-Services.

### Grundlegendes zu Event Stream Analysis-Regeltypen

Der Security Analytics ESA-Service (Event Stream Analysis) bietet erweiterte Streamanalysen wie beispielsweise Korrelation und komplexe Ereignisverarbeitung bei hohen Durchsätzen und niedriger Latenz. Er ist in der Lage, große Mengen verteilter Ereignisdaten aus den Concentrators zu verarbeiten. Damit Sie effektive Regeln erstellen, sollten Sie bei der Arbeit mit Event Stream Analysis die Faktoren berücksichtigen, die sich auf den Ressourcenverbrauch auswirken.

Jedes von ESA empfangene Ereignis wird bewertet, um festzustellen, ob es möglicherweise eine Regel auslöst. Drei Typen von Regeln können bereitgestellt werden, um zu bestimmen, wie die ESA-Engine mit dem eingehenden Ereignis verfährt. Diese Regeltypen wirken sich jeweils unterschiedlich auf die Systemressourcenauslastung aus. Alle drei Regeltypen können über die Regelerstellung oder erweiterte EPL-Regeln erstellt bzw. über RSA Live heruntergeladen werden. Die Tabelle unten enthält die Regeltypen und deren mögliche Auswirkungen auf die Systemressourcen.

Regeltyp	Beschreibung
Einfache Filterregel	<p>Diese Regel steht nicht in Beziehung zu anderen Ereignissen. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Wenn diese Bedingungen zutreffen, wird eine Warnmeldung erzeugt. Wenn keine Bedingungen zutreffen, wird das Ereignis schnell von der Engine freigegeben, um Arbeitsspeicher zur Verfügung zu stellen. Diese Regeln beanspruchen keinen Speicher, da die Ereignisse nicht über die Erstbewertung hinaus beibehalten werden. Die Bereitstellung von weiteren einfachen Filterregeln führt nicht zu einem Anstieg der Nutzung von Arbeitsspeicherressourcen. Wenn die Filterbedingung allerdings zu allgemein ist, können zu viele Warnmeldungen erzeugt werden. Die Systemressourcen werden dann durch das Speichern und Abrufen dieser Warnmeldungen belastet.</p> <p>Beispiel: Sie können eine Regel schreiben, durch die eine Warnmeldung erzeugt wird, wenn HTTP-Netzwerkaktivitäten über einen Port eingehen, der kein Standard-HTTP-Port ist.</p>
Ereignisfensterregel	<p>Diese Regel bewertet eine Reihe von Ereignissen über einen Zeitraum im Hinblick auf bestimmte Bedingungen. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Treffen diese Bedingungen zu, verbleibt das Ereignis für eine festgelegte Dauer im Speicher. Nach Ablauf der angegebenen Zeit werden die Ereignisse aus dem Zeitfenster entfernt, wenn die Anzahl der erfassten Ereignisse nicht den Schwellenwert erreicht, um eine Warnmeldung auszulösen. Der Arbeitsspeicherverbrauch solcher Regeln hängt stark von der Ereigniseingangsrate (Datenverkehr) ab, der Menge von Daten pro Ereignis und der im Ereignisfenster festgelegten Zeitdauer. Jedes zutreffende Ereignis wird im Arbeitsspeicher behalten, bis das Zeitfenster vergangen ist. Je länger das Zeitfenster dauert, desto größer ist die Menge der Daten. Beispiel: Sie können eine Regel schreiben, die eine Warnmeldung erzeugt, wenn ein Benutzer sich nicht in einem Zeitrahmen von zehn Minuten fünfmal an einem System anmeldet.</p>

Regeltyp	Beschreibung
Gefolgt-von-Regel	<p>Diese Regel bewertet eine Kette von eingehenden Ereignissen, um zu bestimmen, ob die Reihenfolge von Ereignissen einer festgelegten Bedingung entspricht. Zum Zeitpunkt der Aufnahme wird diese Regel anhand einer Reihe von Bedingungen bewertet. Treffen die Bedingungen zu, findet eine von zwei Aktionen statt:</p> <ul style="list-style-type: none"> <li>• Ist dies das erste Ereignis der Sequenz, wird ein neuer Ereignis-Thread gestartet und das Ereignis als Kopf der Sequenz beibehalten.</li> <li>• Gehört das Ereignis zu einem vorhandenen Ereignis-Thread, wird es dieser Sequenz hinzugefügt.</li> </ul> <p>In beiden Fällen verbleibt das Ereignis im Arbeitsspeicher. Der Umfang der Ressourcennutzung hängt bei diesem Regeltyp besonders von der Kundenumgebung ab. Wenn die Filterbedingung viele Ereignis-Threads erzeugt, werden für jeden neuen Thread Ressourcen verbraucht (zusätzlich zum Ereignis). Wenn zudem der Ereignis-Thread nie das Ende erreicht (also keine Warnmeldung erzeugt wird), wird das gesamte Ereignis auf unbestimmte Zeit im Arbeitsspeicher gespeichert. Beispiel: Sie könnten eine Regel schreiben, die eine Warnmeldung erzeugt, wenn die Anmeldung eines Benutzers an einem Server fehlschlägt, der Benutzer sich dann erfolgreich anmeldet und anschließend ein neues Konto erstellt.</p>

Zusätzlich zur oben erörterten Speichernutzung verbraucht die Erzeugung von Warnmeldungen Systemressourcen. Jede erzeugte Warnmeldung muss zum Abrufen gespeichert und zudem in Incident Management verarbeitet werden. Dieser Prozess verwendet Speicherplatz auf dem Datenträger zum Speichern, nutzt Datenbankspeicher und erhöht die CPU-Auslastung durch Ausführung von Abfragen.

Berücksichtigen Sie beim Schreiben und Bereitstellen von Regeln, dass jede dieser Aktionen sich zulasten der Systemressourcen auswirkt. Anhand der Anleitungen in den folgenden Abschnitten können Sie den Verbrauch auf einem ordnungsgemäßen Niveau halten und mögliche Probleme im Falle von Systemüberlastungen entdecken.

### **Best Practices für das Schreiben von Regeln**

Hierbei handelt es sich um allgemeine Richtlinien für das Schreiben von Regeln.

- **Warnmeldungen für Ereignisse mit ausführbaren Aktionen erstellen.** Der Zweck einer Warnmeldung ist, Sie auf ein Ereignis hinzuweisen, das sofort bestimmte Aktionen erfordert. Für Ereignisse, die keine Aktion erfordern oder über die Sie nur informiert sein müssen, können Sie einen Bericht erstellen. Sie vermeiden dadurch eine Überlastung der Datenbank, die die Warnmeldungen speichert.
- **Neue Regeln als Testregeln konfigurieren, um ihre Ausführung in der Umgebung zu beobachten.** Wenn Sie neue Regeln als Testregeln bereitstellen, werden sie bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher deaktiviert. Im Falle der Deaktivierung einer Testregel können Sie mithilfe der Snapshot-Funktion für den Arbeitsspeicher sehen, wie viel Speicher verwendet wurde. Weitere Informationen finden Sie unter [Verwenden von Testregeln](#).
- **Erstellen von Warnmeldungsbenachrichtigungen erst, nachdem die Regel getestet und optimiert wurde.** Auf diese Weise stellen Sie sicher, dass Sie nicht übermäßig viele Warnmeldungen erhalten, falls eine Regel sich anders als erwartet verhält.
- **Regeln müssen spezifisch sein, damit Sie die Ressourcennutzung beschränken können.** Beschränken Sie die Nutzung mithilfe der folgenden Guidelines:
  - Schließen Sie mit den Filtern der Regel alle bis auf die erforderlichen Ereignisse aus, um die Regel korrekt auszulösen.
  - Definieren Sie die Fenster (Zeitfenster für die Korrelation) so kurz wie möglich.
  - Begrenzen Sie die Ereignisse, die Sie dem Fenster hinzufügen. Wenn Sie zum Beispiel nur IDS-Ereignisse anzeigen möchten, fügen Sie dem Zeitfenster nur solche Ereignisse hinzu.
- **Regeln müssen für eine verwaltbare Menge von Warnmeldungen optimiert werden.** Wenn Sie übermäßig viele Warnmeldungen erhalten, geht deren Zweck und Nutzen verloren. Außerdem ist eine Überflutung der zur Speicherung der Warnmeldungen genutzten Datenbank möglich, was zu einer Verlangsamung oder Verhinderung der Verarbeitung von Warnmeldungen durch das System führen kann. Beispiel: Sie möchten Informationen über verschlüsselten Datenverkehr in andere Länder erhalten. Möglicherweise können Sie aber die Liste auf die Länder eingrenzen, die ein bekanntes Risiko darstellen. Sie beschränken dadurch die Warnmeldungen auf eine Menge, die Sie verwalten können.

## Best Practices zur Verwendung von RSA Live-Regeln

Hierbei handelt es sich um Richtlinien für die RSA Live-Regeln.

- **RSA Live-Regeln in kleinen Batches bereitstellen:** Nicht jede Regel ist für jede Umgebung geeignet. Stellen Sie Ihre RSA Live-Regeln in kleinen Batches bereit, damit Sie sie in Ihrer

Umgebung testen können. Dies ist die beste Methode, um sicherzustellen, dass die RSA Live-Regeln erfolgreich funktionieren. Durch die Bereitstellung in kleinen Batches können Sie viel einfacher feststellen, ob eine bestimmte Regel einen Fehler aufweist.

- **Die entsprechenden Beschreibungen der RSA Live-Regeln beachten:** ESA-Regeln passen nicht allgemein. Es werden nicht alle Regeln in Ihrer Umgebung funktionieren. In den Regelbeschreibungen erfahren Sie, welche Parameter geändert werden müssen, um eine Regel in der Umgebung erfolgreich bereitzustellen.
- **Eigene Parameter festlegen:** RSA Live-Regeln haben Parameter, die geändert werden müssen. Wenn Sie die Parameter unverändert beibehalten, funktioniert die Regel vielleicht nicht oder verbraucht zu viel Speicher.
- **Neue Regeln als Testregeln bereitstellen, damit Sie ihre Auswirkung in der Umgebung beobachten können:** Wenn Sie neue Regeln als Testregeln bereitstellen, werden sie bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher deaktiviert. Ausführlichere Informationen finden Sie unter [Verwenden von Testregeln](#).

## Best Practices für die Bereitstellung von Regeln

Hierbei handelt es sich um allgemeine Richtlinien für die Bereitstellung von Regeln.

- **Neue Regeln in kleinen Batches bereitstellen, damit Sie ihre Auswirkung in der Umgebung beobachten können:** Umgebungen sind unterschiedlich. Regeln müssen daher unter Berücksichtigung der Speichernutzung, der Menge an Warnmeldungen und der effektiven Erkennung von Ereignissen optimiert werden.
- **Regeln vor dem Konfigurieren von Warnmeldungsbenachrichtigungen testen:** Erstellen Sie Warnmeldungsbenachrichtigungen erst, nachdem die Regel getestet und optimiert wurde. Auf diese Weise stellen Sie sicher, dass Sie nicht übermäßig viele Warnmeldungen erhalten, falls eine Regel sich anders als erwartet verhält.
- **Systemintegrität während des Bereitstellungsprozesses überwachen:** Überwachen Sie bei der Bereitstellung von Regeln als Teil des Prozesses die Systemintegrität. Die Gesamtspeicherauslastung für ESA können Sie auf der Registerkarte „Integrität und Zustand“ prüfen. Weitere Informationen finden Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ unter [Troubleshooting für ESA](#).

## Best Practices für die Systemintegrität

Hierbei handelt es sich um allgemeine Richtlinien für die Systemintegrität.


- **Die für Warnmeldungen verwendete Datenbank konfigurieren, um eine fehlerfreie Menge von Warnmeldungen beizubehalten:** ESA verwendet MongoDB zum Speichern von Warnmeldungen. Wenn die MongoDB-Datenbank mit Warnmeldungen überflutet wird, kann sie verlangsamt oder angehalten werden. Konfigurieren Sie die Datenbankeinstellungen für die regelmäßige Löschung von Warnmeldungen, um eine fehlerfreie Menge von Warnmeldungen sicherzustellen. Informationen hierzu erhalten Sie unter „Konfigurieren des ESA-Speichers“ im **Konfigurationsleitfaden für Event Stream Analysis (ESA)**.
- **Neue Regeln als Testregeln definieren:** Durch neue Regeln verursachte Speicherprobleme sind weit verbreitet. Legen Sie neue Regeln als Testregeln fest, um dieses Problem zu vermeiden. Bei einer Überschreitung des konfigurierten Schwellenwerts für den Arbeitsspeicher werden alle Testregeln deaktiviert, damit das System weiter über ausreichenden Speicher verfügt. Weitere Informationen über Testregeln finden Sie unter [Verwenden von Testregeln](#).
- **Schwellenwerte im Modul „Integrität und Zustand“ festlegen, um eine Warnmeldung bei zu hoher Speicherauslastung zu erhalten.** Das Modul „Integrität und Zustand“ enthält Metriken zur Nachverfolgung der Speicherauslastung. Sie können für die Warnmeldungen und Benachrichtigungen festlegen, dass Sie eine E-Mail erhalten, wenn die Schwellenwerte überschritten werden. Weitere Informationen über die anzeigbaren Speicherstatistiken erhalten Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ in [Troubleshooting für ESA](#).
- **Überwachen Sie für jede Regel im Modul „Integrität und Zustand“ die Speicherkennzahlen.** Sie können jetzt für jede aktive Regel im Modul „Integrität und Zustand“ den geschätzten Speicherverbrauch anzeigen lassen. Sie können diese Informationen verwenden, um sicherzustellen, dass Regeln nicht zu viel Speicher verbrauchen. Weitere Informationen über die anzeigbaren Speicherstatistiken erhalten Sie unter „Anzeigen von Statistiken zu Integrität und Zustand“ in [Troubleshooting für ESA](#).

## Troubleshooting für ESA

In diesem Abschnitt werden häufig vorkommende Probleme beschrieben, die bei der Verwendung von ESA auftreten können, und generelle Lösungen für diese Probleme vorgeschlagen.



## Troubleshooting bei ESA-Services

Problem	Mögliche Ursachen	Lösungen
<p>Im Security Analytics Dashboard ist der ESA-Service rot markiert, um darauf hinzuweisen, dass er offline ist.</p> <p>Auf der Seite <b>Warnmeldungen &gt; Konfigurieren</b> wird die folgende Meldung angezeigt: „Der Service ist entweder offline oder nicht erreichbar.“</p>	<p>Verschiedene</p>	<p>Wenn ein ESA-Service offline ist, kann dies viele Ursachen haben. Häufig liegt es jedoch daran, dass eine von Ihnen erstellte Regel zu viel Arbeitsspeicher benötigt und der ESA-Service dadurch fehlschlägt. Informationen über die Behebung des Problems finden Sie unter „Schritte zur Behebung von Speicherproblemen, wenn ein ESA-Service offline ist.“</p> <p>Andere häufige Ursachen sind die Blockierung der Verbindung zwischen ESA und Security Analytics durch eine Firewall oder ein Ausfall des Computers mit dem ESA-Service.</p>
		<p>So starten Sie ESA-Services:</p> <p>Klicken Sie in <b>Administration &gt; Services</b> auf das Symbol „Aktionen“  für den ESA-Service und wählen Sie <b>Starten</b> aus.</p> <p>Falls der ESA-Service in einer Dauerschleife angehalten und von Neuem gestartet wird, bitten Sie den Customer Service, die Services wieder zum Starten zu bringen.</p>



Problem	Mögliche Ursachen	Lösungen
<p>Nach einem kürzlich erfolgten Upgrade ist der ESA-Service im Security Analytics Dashboard rot markiert, um darauf hinzuweisen, dass er offline ist.</p> <p>Auf der Seite <b>Warnmeldungen</b> &gt; <b>Konfigurieren</b> wird die folgende Meldung angezeigt: „Der Service ist entweder offline oder nicht erreichbar.“</p>	<p>Konfigurationsprobleme</p>	<p>Falls Sie Ihr System vor Kurzem aktualisiert haben, ist Ihnen vielleicht ein Konfigurationsfehler unterlaufen. Wählen Sie unter <b>Administration</b> &gt; <b>Services</b> Ihren ESA-Service aus und klicken Sie auf <b>Service bearbeiten</b>. Klicken Sie im Feld „Service bearbeiten“ auf „Überprüfen der Verbindung“.</p> <p>Wenn keine Verbindung hergestellt werden kann, liegt wahrscheinlich ein Konfigurationsfehler vor. Versuchen Sie, den Konfigurationsfehler zu beheben, und überprüfen Sie die Verbindung erneut.</p>
<p>Der ESA-Service wird offenbar langsam ausgeführt.</p>	<p>Konfigurationsprobleme</p>	<p>Sie können die Performance möglicherweise steigern, indem Sie den Puffer ändern (der Standardwert ist <i>10485760 Byte</i>) oder die TCP-Einstellung auf „TCPNoDelay“ festlegen, um eine Verzögerung beim Empfang von TPC Acks zu verhindern. Sie können diese Einstellungen ändern (<i>readBufferSize</i> und <i>tcpNoDelay</i>) unter <i>Explorer/Workflow/Source/nextgenAggregation</i>.</p>

## Troubleshooting bei ESA-Datenbankproblemen

Problem	Mögliche Ursachen	Lösungen
<p>Mein ESA-Dashboard wird nicht geladen,</p> <ul style="list-style-type: none"> <li>• beim Abrufen der Daten tritt ein Fehler auf</li> <li>• oder das Laden geschieht sehr langsam.</li> </ul>	<p>Die Datenbank, in der Warnmeldungen gespeichert werden, ist zu groß geworden.</p>	<p>Sie können die Einstellungen für die Warnmeldungsdatenbank so konfigurieren, dass alte Warnmeldungen nach einiger Zeit automatisch gelöscht werden. Informationen über die Konfiguration dieser Einstellungen finden Sie unter „Konfigurieren des ESA-Speichers“ im <b>Konfigurationsleitfaden für Event Stream Analysis (ESA)</b>.</p> <p>Wenn die Datenbank zu groß geworden ist, müssen Warnmeldungen gelöscht werden. Bitte wenden Sie sich dazu an den Customer Service.</p>

## Troubleshooting bei RSA Live-Regeln für ESA

Problem	Mögliche Ursachen	Lösungen
Ich habe eine Gruppe von Regeln aus RSA Live importiert und nun stürzt mein ESA-Service ab. Warum?	Möglicherweise haben Sie die Parameter für die RSA Live-Regeln nicht konfiguriert, um sie auf Ihre Umgebung abzustimmen.	<p>Zu jeder Regel in RSA Live gehört eine Beschreibung, die die zu konfigurierenden Parameter sowie die umgebungsspezifischen Voraussetzungen enthält. Überprüfen Sie in dieser Beschreibung, ob die Regel für Ihre Umgebung korrekt ist.</p> <p>Damit gewährleistet ist, dass sichere Regeln für Ihre Umgebung bereitgestellt werden, konfigurieren Sie neue Regeln zunächst als Testregeln, um sie in Ihrer Umgebung zu testen. Testregeln sind eine Vorsichtsmaßnahme zum Testen neuer Regeln. Weitere Informationen über diese Ansicht finden Sie unter <a href="#">Bereitstellen von Regeln als Testregeln</a>.</p>

Problem	Mögliche Ursachen	Lösungen
<p>Ich habe eine Gruppe von Regeln aus RSA Live importiert. Sie wurden zwar ohne Fehler bereitgestellt, wurden aber später deaktiviert.</p>	<p>Nicht alle RSA Live-Regeln passen in jede Umgebung. Möglicherweise verfügen Sie nicht über die korrekten Metadaten in Ihrer ESA, um die Regel auszuführen.</p>	<p>Sie können überprüfen, ob eine Regel deaktiviert wurde, indem Sie zu „Warnmeldungen &gt; Services &gt; Statistik für bereitgestellte Regeln“ wechseln. Wenn die Regel deaktiviert ist, wird das grüne Symbol neben der Regel nicht angezeigt.</p> <p>Wenn eine Regel korrekt bereitgestellt, jedoch deaktiviert wurde, prüfen Sie die Protokolle auf Ausnahmen in Bezug auf die Regel. Prüfen Sie insbesondere, ob die Regeln aufgrund von fehlenden Metadaten deaktiviert wurden. Gehen Sie dazu zu <b>Administration &gt; Services</b>, wählen Sie den ESA-Service und dann   &gt; <b>Ansicht &gt; Protokolle</b> aus.</p> <p>Suchen Sie dann nach einer Meldung ähnlich der Folgenden:</p> <p>"Property named '&lt;meta_name&gt;' is not valid in any stream"</p> <p>Es könnte z. B. Folgendes angezeigt werden:</p> <pre>Failed to validate filter expression '(medium=1 and streams=2 or medium=3...(238 chars)': Property named 'tcp_flags_seen' is not valid in any stream</pre> <p>Wenn eine ähnliche Meldung angezeigt wird, müssen Sie dem Log Decoder oder Concentrator möglicherweise einen benutzerdefinierten Metaschlüssel hinzufügen. Befolgen Sie dazu die Anweisungen unter „Erstellen benutzerdefinierter Metaschlüssel mithilfe benutzerdefinierter Feeds“ im <b>Konfigurationsleitfaden für Decoder und Log Decoder</b>.</p>

## Troubleshooting für Bereitstellungen

Problem	Mögliche Ursachen	Lösungen
Ich habe die Regel erstellt und die Syntax überprüft. Die Regel sah korrekt aus. Als ich die Regel bereitstellen wollte, trat ein Fehler auf. Warum?	Möglicherweise verfügen Sie nicht über die korrekten Metadaten zur Bereitstellung der Regel.	Überprüfen Sie die Metaschlüsselverweise. Möglicherweise verfügen Sie nicht über die korrekten Metadaten zur Bereitstellung der Regel.

## Troubleshooting bei Regeln

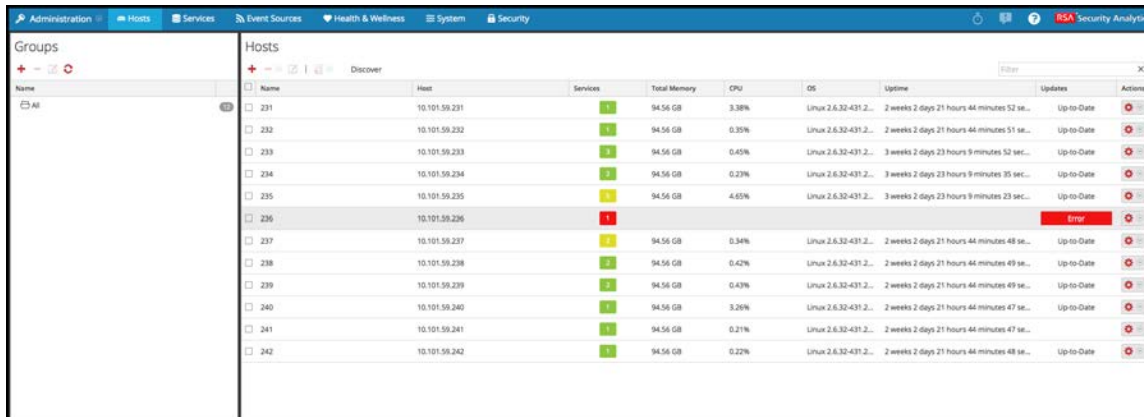
Problem	Mögliche Ursachen	Lösungen
Ich habe (über die Registerkarten Regelerstellung oder Erweiterte EPL-Regel) eine benutzerdefinierte Regel erstellt, die jedoch keine Aktion auslöst. Warum?	Möglicherweise bestehen Verbindungsprobleme.	<p>Überprüfen Sie die Statistik „Angebotene Rate“ auf der Registerkarte <b>Warnmeldungen &gt; Konfigurieren &gt; Services</b>.</p> <p>Ist die angebotene Rate gleich null, empfängt der ESA-Service keine Daten von Concentrators. Überprüfen Sie die Verbindung des Concentrator. Gehen Sie zu <b>Administration &gt; Services</b>, wählen Sie den ESA-Service aus und klicken Sie auf <b>Ansicht &gt; Konfigurieren</b>. Stellen Sie sicher, dass der Concentrator aktiviert ist. Wählen Sie den Concentrator aus und klicken Sie auf <b>Überprüfen der Verbindung</b>.</p> <p>Wenn die angebotene Rate nicht gleich null ist, stimmen wahrscheinlich der in der Regel angegebene Metaschlüsselname und -typ nicht mit dem Metaschlüssel in Ereignissen überein. Überprüfen Sie die Gültigkeit des in der Regel angegebenen Metaschlüsselnamens und -typs, indem Sie auf der Registerkarte <b>Warnmeldungen &gt; Konfigurieren &gt; Einstellungen</b> nach dem Namen des Metaschlüssels suchen (Metaschlüssel-Verweissuche).</p>

Problem	Mögliche Ursachen	Lösungen
	Möglicherweise besteht ein Problem mit der Regel.	<p><b>Falls nur eine bestimmte Regel keine Aktionen auslöst</b>, rufen Sie <b>Warnmeldungen &gt; Konfigurieren &gt; Services</b> auf, um festzustellen, ob die Regel deaktiviert wurde. Bei einer deaktivierten Regel wird im Bereich <b>Statistik für bereitgestellte Regeln</b> eine durchsichtige Schaltfläche „Aktiviert“ anstelle einer grünen Schaltfläche „Aktiviert“ angezeigt.</p> <p>Sie können auch das Feld <b>Übereinstimmende Ereignisse</b> überprüfen. Gehen Sie zu <b>Warnmeldungen &gt; Konfigurieren &gt; Services</b>. Dort wird die Anzahl der übereinstimmenden Ereignisse in der Spalte <b>Übereinstimmende Ereignisse</b> angezeigt.</p> <p>Wenn keine übereinstimmenden Ereignisse angezeigt werden, überprüfen Sie die Logik Ihrer Regel auf Fehler. Beispiel: Überprüfen Sie die Syntax auf Fehler bei der Groß- und Kleinschreibung und überprüfen Sie das Zeitfenster. Wenn die Regel immer noch nicht funktioniert, ziehen Sie eine Vereinfachung der Logik der Regel in Betracht, um herauszufinden ob sie in einer weniger komplexen Version funktioniert.</p>

## Schritte zur Behebung von Speicherproblemen, wenn ein ESA-Service offline ist

### Schritt 1: Überprüfen, ob der Host ausgeführt wird

Vergewissern Sie sich als ersten Schritt zum Troubleshooting, dass der Host ausgeführt wird. Rufen Sie dazu **Administration > Hosts** auf. Wenn der Host nicht verfügbar ist, werden die Systemparameter nicht angezeigt (die Aktualisierung der Hostinformationen kann jedoch manchmal etwas dauern), **Services** wird rot markiert und im Feld **Updates** wird eine Fehlermeldung angezeigt.



Falls der Host nicht ausgeführt wird, bitten Sie den SA-Administrator, ihn von Neuem zu starten. Andernfalls fahren Sie mit Schritt 2 fort.

## Schritt 2: Anzeigen von detaillierten Statistikdaten in „Integrität und Zustand“

Wenn Sie sicher sind, dass der ESA-Service ausgefallen ist, können Sie „Integrität und Zustand“ aufrufen, um festzustellen, wo möglicherweise Probleme aufgetreten sind. Das häufigste Problem ist, dass der ESA-Service Arbeitsspeicher-Schwellenwerte überschreitet, was ein Stoppen oder Fehlschlagen des Services zur Folge hat.

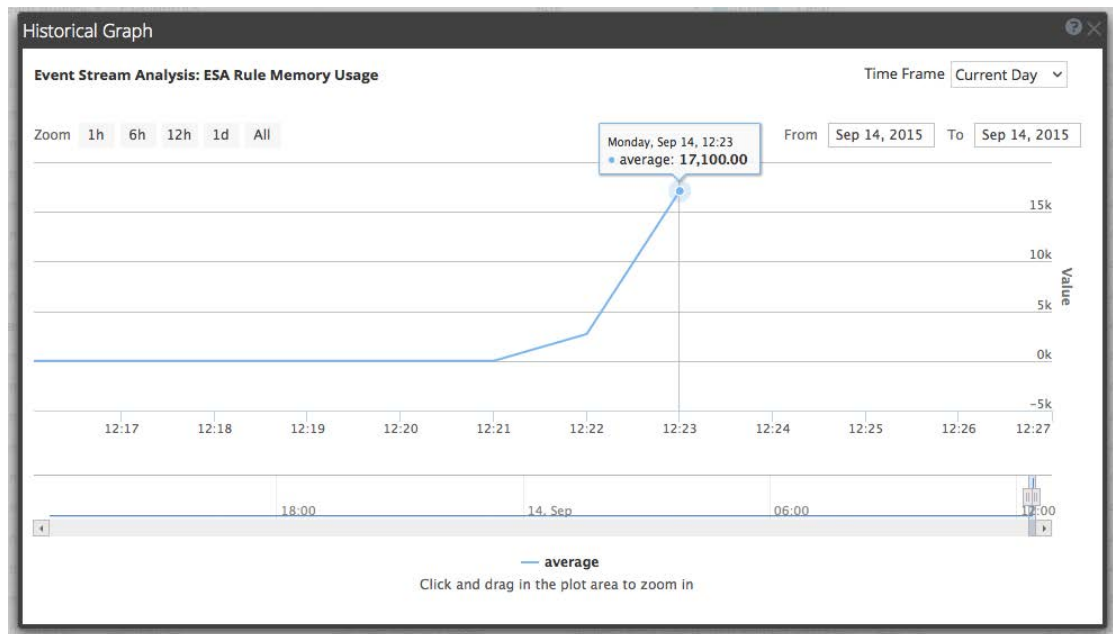
1. Rufen Sie **Integrität und Zustand > Alarme** auf, um festzustellen, ob der ESA-Service Alarme ausgelöst hat. Suchen Sie nach folgenden Alarmen:
  - ESA-Gesamtspeicherauslastung > 85 %
  - ESA-Gesamtspeicherauslastung > 95 %
  - ESA-Service angehalten
2. Gehen Sie zu **Integrität und Zustand > Systemstatistikbrowser**, um die Speichermetriken für die Performance jeder Regel zu sehen. Um die Kennzahlen anzuzeigen, geben Sie Folgendes ein:

Host	Komponente	Kategorie
<Ihr Host>	Event Stream Analysis	ESA-Metriken



Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
New York	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		0,15%	2015-09-24 09:01:23 P...	
New York	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Forwarder	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Cross-site Correlation ...	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Cross-site Correlation ...	184 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Cross-site Correlation ...	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Cross-site Correlation ...	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Forwarder	0%	2015-09-24 08:24:56 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Cross-site Correlation ...	0 bytes	2015-09-24 08:23:47 P...	
Paris	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Forwarder	0 bytes	2015-09-24 08:23:47 P...	

Der Arbeitsspeicher für jede Regel wird in der Spalte **Wert** angezeigt und der Wert wird in Byte angezeigt. Sie können eine Verlaufsansicht des Speicherverbrauchs in der Spalte **Verlaufdiagramm** anzeigen.



3. Navigieren Sie zu **Integrität und Zustand > Systemstatistikbrowser**, um Details zur ESA-Performance anzuzeigen. Wählen Sie Ihren Host aus und verwenden Sie diese Filter zum Anzeigen der folgenden Statistikdaten:


Hos t	Komponen te	Kategorie	Statistik	Beispiel
<Ihr Hos t>	Host	Systeminformatio nen	CPU-Auslastung	1,08 %

Host	Komponente	Kategorie	Statistik	Beispiel
<Ihr Host>	Host	Systeminformationen	Arbeitsspeicherauslastung	45,43 %
<Ihr Host>	Host	Systeminformationen	Belegter Arbeitsspeicher	7,08 GB
<Ihr Host>	Host	Systeminformationen	Gesamtspeicher	15,58 GB
<Ihr Host>	Host	Systeminformationen	Uptime	77758, 1 Woche, 2 Tage
<Ihr Host>	Event Stream Analysis	Prozessinformationen	Arbeitsspeicherauslastung	7,07 GB
<Ihr Host>	Event Stream Analysis	Prozessinformationen	CPU-Auslastung	0,2 %
<Ihr Host>	Event Stream Analysis	JVM.Memory	all	Festgelegte Heap-Arbeitsspeicherauslastung 8,0 GB
<Ihr Host>	Event Stream Analysis	ESA-Metriken	ESA-Gesamtspeichernutzung %	4,64 %

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
ESA_10.4.2_10.5	Host	Systeminfo	CPU Utilization		1.08%	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Current Time		2015-May-29 18:28:58	2015-05-29 06:28:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Hardware Type		VMware Virtual Platfo...	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Hostname		NWAPPLIANCE12202	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Memory Utilization		45.43%	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Running Since		2015-May-20 18:26:20	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	System Info		Linux 2.6.32-431.29.2...	2015-05-29 06:27:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Total Memory		15.58 GB	2015-05-29 06:29:08 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Uptime		777758, 1 week 2 day...	2015-05-29 06:28:58 P...	
ESA_10.4.2_10.5	Host	Systeminfo	Used Memory		7.08 GB	2015-05-29 06:29:08 P...	

Falls ein Problem mit der Arbeitsspeicher- oder CPU-Auslastung besteht, fahren Sie mit Schritt 3 fort.

### Schritt 3: Erneutes Starten der ESA-Services

1. Klicken Sie in **Administration > Services** auf das Symbol  für den ESA-Service und wählen Sie **Starten** aus.
2. Kehren Sie zum ESA-Service zurück, um festzustellen, welche Regeln Speicherprobleme verursacht haben.

Falls der ESA-Service in einer Dauerschleife angehalten und von Neuem gestartet wird, bitten Sie den Customer Service, die Services wieder zum Starten zu bringen.

Wenn Sie den ESA-Service ohne Herunterfahren starten können, fahren Sie mit Schritt 4 fort.

### Schritt 4: Überprüfen der Menge an Warnmeldungen und Ereignissen

Wenn Sie den ESA-Service erneut starten können, ohne dass er sofort wieder heruntergefahren wird, können Sie in den Regelstatistiken überprüfen, welche Regeln zu viele Ressourcen verbrauchen. Gelegentlich schlagen ESA-Services fehl, weil eine Regel zu viele Warnmeldungen erzeugt oder mit zu vielen Ereignissen übereinstimmt. Suchen Sie nach solchen Problemen, wenn Sie ermittelt haben, dass der Ausfall Ihres ESA-Services durch Speicherprobleme verursacht wird.

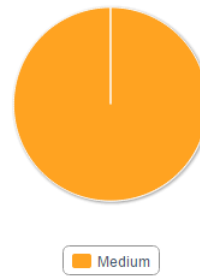
### Anzeigen von Warnmeldungs zusammenfassungen

Regeln, die zu viele Warnmeldungen erzeugen, können das System überfordern und zum Ausfall oder Neustart führen. Um Zusammenfassungen von Warnmeldungen anzuzeigen, rufen Sie **Dashboard > Warnmeldungen > Zusammenfassung** auf. In der unteren Hälfte des Bildschirms wird im Feld **Anzahl** für jede Regel die Anzahl der erzeugten Warnmeldungen angezeigt. Wenn die Anzahl bei einer bestimmten Regel signifikant hoch ist, deaktivieren Sie die Regel und formulieren Sie sie so um, dass sie effizienter funktioniert.

Alerts

Name	Count	Severity	Last Detected
epl_module_no_18	5123	Medium	2015-05-19T00:39:57
epl_module_no_21	12454	Medium	2015-05-19T00:39:57
epl_module_no_48	12454	Medium	2015-05-19T00:39:57
epl_module_no_12	12454	Medium	2015-05-19T00:39:57
epl_module_no_22	12454	Medium	2015-05-19T00:39:57
epl_module_no_49	12454	Medium	2015-05-19T00:39:57
epl_module_no_42	12454	Medium	2015-05-19T00:39:57
epl_module_no_27	12454	Medium	2015-05-19T00:39:57

Alerts by Severity



Anzeigen der übereinstimmenden Ereignisse

Manchmal stimmt eine Regel mit zu vielen Ereignissen überein, wodurch übermäßig viel Speicher verbraucht wird. Dies ist typischerweise der Fall, wenn Sie ein weites Ereigniszeitfenster definieren, in dem sich eine große Anzahl von Ereignissen ansammeln kann, ohne dass eine Warnmeldung ausgelöst wird. Dies ist problematisch, da jedes Ereignis im Arbeitsspeicher gespeichert wird, während die Regel auf die Auslösung der Warnmeldung wartet. Dies können Sie unter **Dashboard > Warnmeldungen > Services** überprüfen. Dort wird in der Spalte **Übereinstimmende Ereignisse** die Anzahl der übereinstimmenden Ereignisse angezeigt. Wenn eine Regel eine hohe Anzahl übereinstimmender Ereignisse aufweist, sollten Sie untersuchen, ob Sie die Regel effizienter formulieren können.

The screenshot shows the 'Services' tab in the ESA dashboard, specifically the '231 - Event Stream Analysis' configuration page. It displays engine and rule statistics, and a table of 'Deployed Rule Stats'. The table has columns for 'Enable', 'Name', 'Trial Rule', 'Last Detected', and 'Events Matched'. The rule 'epl\_module\_no\_43' is highlighted with a red circle around its 'Events Matched' value of 70555.

Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	epl_module_no_43	Yes	2015-05-19 00:39:57	70555
<input type="checkbox"/>	epl_module_no_9	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_19	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_50	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_12	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_3	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_13	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_4	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_1	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_10	Yes	2015-05-19 00:39:57	12454
<input type="checkbox"/>	epl_module_no_11	Yes	2015-05-19 00:39:57	12454


**Schritt 5: Deaktivieren und Reparieren der Regel, die Probleme verursacht**

Nachdem Sie ermittelt haben, welche Regeln überarbeitet werden müssen, deaktivieren Sie diese und formulieren Sie sie so um, dass sie nicht mehr so viele Warnmeldungen oder Ereignisse erzeugen. Tipps zum Formulieren effizienter Regeln finden Sie unter [Best Practices](#).

**Deaktivieren von Regeln**

1. Rufen Sie zum Deaktivieren von Regeln **Warnmeldungen > Services** auf und wählen Sie im Feld **Statistik für bereitgestellte Regeln** die zu deaktivierenden Regeln aus.
2. Wählen Sie **Deaktivieren** aus, um die Regeln zu deaktivieren.

**Bearbeiten von Regeln**

1. Wenn Sie Regeln korrigieren möchten, rufen Sie **Warnmeldungen > Regeln > Regelbibliothek** auf. Wählen Sie die zu bearbeitende Regel aus und klicken Sie auf das Symbol .
2. Wählen Sie **Bearbeiten** aus.
3. Formulieren Sie die Regel effizienter. Anweisungen zur Erstellung von Regeln finden Sie unter [Hinzufügen von Regeln zur Regelbibliothek](#)
4. Wenn Sie mit der Formulierung der Regel zufrieden sind, können Sie sie als Testregel speichern, um sicherzustellen, dass die Performance der ESA-Services nicht durch Speicherprobleme beeinträchtigt wird. Befolgen Sie dazu die Schritte, die aufgelistet sind in [Verwenden von Testregeln](#).

**Aktivieren von Regeln**

1. Rufen Sie zum Aktivieren von Regeln **Warnmeldungen > Services** auf und wählen Sie im Feld **Statistik für bereitgestellte Regeln** die zu aktivierenden Regeln aus.
2. Wählen Sie **Aktivieren** aus, um die Regeln zu aktivieren.

**(Optional) Überprüfen der ESA-Protokolldateien auf weitere Informationen**

Wenn Sie feststellen, dass Services ausfallen, und bereits einige mögliche Ursachen für den Systemausfall untersucht haben, sollten Sie überprüfen, ob der Service in einer Dauerschleife gestoppt und von Neuem gestartet wird. Rufen Sie dazu die ESA-Protokolle auf. Wählen Sie im Modul **Administration > Services** Ihren ESA-Service aus, klicken Sie auf das Symbol

„Aktionen“  und wählen Sie **Ansicht > Protokolle** aus.

Falls Sie über die Security Analytics-Benutzeroberfläche nicht auf die ESA-Protokolle zugreifen können, können Sie sich über SSH im System einloggen und Folgendes eingeben: `opt/rsa/esa/logs/esa.log`

## Anzeigen von Speicherkennzahlen für Regeln

In diesem Thema erfahren Autoren von ESA-Regeln, wie sie Speicherkennzahlen für Regeln anzeigen können. Sie können den geschätzten Speicherverbrauch für jede Regel, die auf einem Server ausgeführt wird, anzeigen und Sie können diese Informationen verwenden, Ihre Regeln und Bedingungen zu ändern, wenn sie zu viel Speicher verbrauchen.

Regeln können manchmal mehr Speicher verbrauchen als erwartet, wodurch Ihre ESA verlangsamt oder sogar gestoppt wird. Um annähernd zu sehen, wie viel Arbeitsspeicher eine Regel verbraucht, können Sie Speicherkennzahlen konfigurieren. Speicherkennzahlen ermöglichen es Ihnen, einen geschätzten Speicherverbrauch für jede Regel im Systemstatistikbrowser von „Integrität und Zustand“ anzuzeigen (Sie benötigen Zugriffsberechtigungen, um auf dieses Modul zuzugreifen). Sie können diese Informationen verwenden, um Ihre Regeln für mehr Effizienz zu ändern.

Allgemein müssen Sie die folgenden Schritte ausführen, um die Speicherkennzahlen für das Troubleshooting der Speichernutzung von Regeln verwenden zu können:

1. Stellen Sie sicher, dass die Funktion „Speicherkennzahlen“ aktiviert ist (über „Explorer > CEP > Kennzahlen > EnableStats“). Die Funktion „Speicherkennzahlen“ ist standardmäßig aktiviert.
2. Vergewissern Sie sich, dass Sie über die korrekten Berechtigungen zum Anzeigen des Moduls „Integrität und Zustand“ verfügen. Informationen über Rollen und Berechtigungen erhalten Sie unter [Rollenberechtigungen](#).
3. Zeigen Sie die Speicherstatistik in „Integrität und Zustand“ an.
4. (Empfohlen) Konfigurieren Sie die ESA-Richtlinien für „Integrität und Zustand“ so, dass eine E-Mail gesendet wird, wenn die Speicherschwelldaten überschritten werden. Anweisungen zum Senden von E-Mail-Benachrichtigungen erhalten Sie unter „Managen von Richtlinien“ im **Leitfaden Systemwartung**.
5. Verwenden Sie die Speicherkennzahlen, um bei Bedarf Regeln für mehr Effizienz zu ändern.

### Voraussetzungen

Im Folgenden sind die Anforderungen für die Verwendung von Speicherkennzahlen aufgeführt:

- Die Funktion „Speicherkennzahlen“ ist aktiviert (über **Explorer > CEP > Kennzahlen > EnableStats**).
- Der Benutzer muss über die entsprechenden Berechtigungen zum Anzeigen der Statistik in „Integrität und Zustand“ verfügen.

- (Empfohlen) Konfigurieren Sie die ESA-Richtlinie für „Integrität und Zustand“ so, dass eine E-Mail gesendet wird, wenn die Speicherschwel­lenwerte überschritten werden.

## Methoden

### Anzeigen der Speicherkennzahlen im Systemüberwachungsmodul „Integrität und Zustand“

1. Navigieren Sie im Menü **Security Analytics** zu **Administration > Integrität und Zustand > ESA > Systemüberwachung**.
2. Zeigen Sie die Details für den ESA-Service an.
3. Wählen Sie **Regeln** aus.
4. Sie können die durchschnittliche Speicherauslastung für jede Regel für die vorherige Stunde anzeigen.

The screenshot shows the RSA Security Analytics interface. The top navigation bar includes 'Administration', 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The main content area is titled 'ESA Details' and shows service information: CPU (1%), Running Since (2015-Sep-03 01:36:11), Build Date (2015-Sep-01 09:08:04), Used Memory (6.70 GB), Max Process Memory (15.58 GB), and Version Information (10.5.1.0). Below this is a 'Details' section with tabs for 'Rules', 'Monitor', and 'JVM'. The 'Rules' tab is active, showing a table of 'Deployed Rule Memory Utilization' with columns for Name, Event Stream Engine, and Total Estimated Memory (last hr).

Name	Event Stream Engine	Total Estimated Memory (last hr)
Rule with MatchRecognize	Local ESA (Default)	<1% 7.32 KB / 64.00 GB
Failed Logins Followed By Successful Login Password Change	Local ESA (Default)	<1% 336 bytes / 64.00 GB
Rule with Pattern	Local ESA (Default)	<1% 150 bytes / 64.00 GB
Brute Force Login To Same Destination	Local ESA (Default)	<1% 53 bytes / 64.00 GB
Brute Force Login From Same Source	Local ESA (Default)	<1% 45 bytes / 64.00 GB
Logins across Multiple Servers	Local ESA (Default)	<1% 45 bytes / 64.00 GB
Multiple Failed Logins from Multiple Diff Sources to Same Dest	Local ESA (Default)	<1% 45 bytes / 64.00 GB

### Anzeigen der Speicherkennzahlen im Systemstatistikbrowser „Integrität und Zustand“

1. Navigieren Sie im Menü **Security Analytics** zu **Administration > Integrität und Zustand > Systemstatistikbrowser**.
2. Wählen Sie als Komponente **Event Stream Analysis** aus. Geben Sie als Kategorie **ESA-Kennzahlen** ein.

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

Der Name der Regel wird im Feld **Unterelement** angezeigt, die Speichernutzung in der Spalte **Wert**.

3. Klicken Sie auf das Symbol **Verlaufdiagramm**, um den Verlauf der Speicherauslastung für die Regel anzuzeigen.

**Hinweis:** Im Feld **Letzte Aktualisierung** ist angegeben, wann ESA von „Integrität und Zustand“ abgefragt wird. Die Speicherkennzahlen werden jedoch nicht mit der Abfrage von „Integrität und Zustand“ synchronisiert. Beispiel: Wenn der Speicherschwel­lenwert am 10.10.15 um 12.00 Uhr überschritten wird, aber „Integrität und Zustand“ am 10.10.15 um 12:10 Uhr abfragt, zeigt das Feld **Letzte Aktualisierung** einen Zeitstempel von 10.10.15 12:10 Uhr an.

### Aktivieren oder Deaktivieren der Funktion „Speicherkennzahlen“

1. Navigieren Sie im Menü **Security Analytics** zu **Administration** > **Services** und wählen Sie Ihren ESA-Service aus.
2. Nachdem Sie die ESA ausgewählt haben, klicken Sie auf **Aktionen** > **Anzeigen** > **Durchsuchen** und navigieren Sie wie unten gezeigt zu **CEP-Kennzahlen** > **Konfiguration**.

Path	Value
/com.rsa.netwitness.esa/CEP/Metrics/configuration	New York - Event Stream Analysis (Event Stream Analysis)
LogLevels	service esper module statement
EnabledMemoryMetric	false
EnabledCaptureSnapshot	false
CurrentLogLevel	module
CollectionIntervalSec	1000
EnableStats	true
LoggingIntervalSec	1000



3. Ändern Sie das Feld „EnabledStats“ in **wahr** oder **falsch**, je nachdem, ob Sie die Speicherkennzahlen-Funktion aktivieren oder deaktivieren möchten.



## So erzeugt ESA Warnmeldungen

---

In diesem Thema wird kurz beschrieben, wie ein ESA (Event Stream Analysis)-Service Regeln ausführt, um Warnmeldungen zu erzeugen. Der Security Analytics Event Stream Analysis (ESA)-Service führt Regeln aus, die Kriterien für Problemverhalten oder bedrohliche Ereignisse in Ihrem Netzwerk bestimmen. Wenn ESA einen Incident entdeckt, der Regelkriterien entspricht, erzeugt er eine Warnmeldung.

ESA führt die folgenden Funktionen aus, um Warnmeldungen zu erzeugen:

1. Sammeln von Daten
2. Führt ESA-Regeln für die Daten aus.
3. Erfassen von Ereignissen, die die Regelkriterien erfüllen
4. Erzeugen von Warnmeldungen für diese erfassten Ereignisse

Mithilfe des Warnmeldungsmoduls können Sie Einsichten in Ihr Netzwerk gewinnen und Probleme darin erkennen.

## Vertrauliche Daten

In diesem Thema wird erläutert, wie ESA vertrauliche Daten behandelt, z. B. Benutzernamen oder IP-Adressen, die von Security Analytics-Core-Services stammen. Die Rolle des Datenschutzbeauftragten (Data Privacy Officer, DPO) kann Metaschlüssel identifizieren, die vertrauliche Daten enthalten und verschleierte Daten anzeigen sollten. ESA zeigt vertrauliche Metadaten weder an noch speichert es sie. Folglich übergibt ESA vertrauliche Daten nicht an Incident Management.

Optional kann ESA eine verschleierte Version der vertraulichen Daten einem Ereignis hinzufügen. Zum Beispiel identifiziert der DPO `user_dst` als vertraulich. ESA kann eine verschleierte Version, wie etwa `user_dst_hash`, zu einem Ereignis hinzufügen. Die verschleierte Metadaten sind nicht vertraulich, sodass ESA sie auf dieselbe Weise anzeigen und speichern kann wie alle anderen nicht vertraulichen Metadaten.

Weitere Informationen über die Strategie und Vorteile der Datenverschleierung finden Sie im **Security Analytics Leitfaden Datenschutzmanagement**.

Dieses Thema erklärt Folgendes:

- Wie ESA vertrauliche Daten behandelt, die von Security Analytics Core stammen
- Wie Lecks vertraulicher Daten in einer erweiterten EPL-Regel vorzubeugen ist

## Wie ESA vertrauliche Daten von Security Analytics-Core behandelt

Wenn ESA vertrauliche Daten von Security Analytics Core empfängt, gibt ESA nur die verschleierte Version der Daten weiter. ESA speichert keine vertraulichen Daten noch zeigt es sie an.

Die folgenden Funktionen sind betroffen:

- Ausgaben: ESA leitet keine vertraulichen Daten an Ausgaben weiter, dazu gehören Warnmeldungen, Benachrichtigungen und MongoDB-Speicher.
- Erweiterte EPL-Regeln: Wenn eine EPL-Aussage einen Alias für einen vertraulichen Metaschlüssel erstellt, kommt es zu einem Leck vertraulicher Daten. Dieses Thema illustriert, wie das passiert, damit Sie es verhindern können.
- Erweiterungen: Wenn ein vertraulicher Metaschlüssel in der Verknüpfungsbedingung verwendet wird, kommt es zu einem Leck vertraulicher Daten. Dieses Thema illustriert, wie das passiert, damit Sie es verhindern können.

### Erweiterte EPL-Regel

Wenn eine EPL-Abfrageaussage einen vertraulichen Metaschlüssel umbenennt, sind die Daten nicht geschützt.

ESA identifiziert einen vertraulichen Metaschlüssel über den Namen:

`ip_src` ist der vertrauliche Metaschlüssel.

`ip_src_hash` ist die nicht vertrauliche, verschleierte Version.

Zur Unterstützung des Datenschutzes darf der vertrauliche Metaschlüssel in einer EPL-Abfrage nicht umbenannt werden. Wenn ein vertraulicher Metaschlüssel umbenannt wird, sind die Daten nicht mehr geschützt.

Beispiel: In einer Regel wie `select ip_src as ip_alias...` enthält `ip_alias` die vertraulichen Daten. Diese sind aber nicht geschützt, weil ESA nur `ip_src` kennt, nicht aber `ip_alias`. In diesem Fall würden die IP-Adressen nicht verschleiert. Echte Werte würden angezeigt.

### Erweiterungsquelle

Wenn ein vertraulicher Metaschlüssel in einer Verknüpfungsbedingung verwendet wird, können vertrauliche Daten nicht angezeigt werden.

Die Erweiterungsdatenbank, der andere Teil der Verknüpfungsdatenbank, hat eine Spalte, die dem vertraulichen Metaschlüssel entspricht. Dieser Querverweis bezieht sich auf tatsächliche Werte, nicht verschleierte Werte. Folglich werden tatsächliche Werte angezeigt.

Im folgenden Beispiel werden beide Teile der Verknüpfungsbedingung hervorgehoben.

Type	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input type="checkbox"/> GeolP	Default GeolP	ip_src	ipv4

- ip\_src enthält vertrauliche Daten.
- ipv4 wird der Warnmeldung hinzugefügt und ist als nicht vertrauliches Datenelement gefährdet

Da der ipv4-Wert derselbe ist wie der ip\_src-Wert, enthält ipv4 vertrauliche Daten und zeigt sie an.



## ESA-Regeltypen

In diesem Thema werden alle Typen von ESA-Regeln beschrieben, wann sie verwendet werden und über welche Berechtigungen die jeweilige Rolle verfügt. Die folgende Tabelle enthält die jeweiligen Typen und ihre Beschreibung sowie die Erläuterung, wann ein Typ verwendet wird.

Regeltyp	Beschreibung	Verwendung
Regelerstellung	Die Regelerstellung bietet eine einfache Benutzeroberfläche zum Definieren von Regelkriterien.	Verwenden Sie die Regelerstellung, um Ihre ersten Regeln zu erstellen. Sie können viele Regelbedingungen aus Listen auswählen.
Erweiterte EPL	Mit EPL (Event Processing Language) definieren Sie Regelkriterien, indem Sie eine Abfrage schreiben.	Verwenden Sie die erweiterten EPL-Regeln, um Regelkriterien in der EPL-Syntax zu definieren.
RSA Live-ESA	RSA Live bietet einen Katalog von ESA-Regeln, die Sie herunterladen und ändern können, um sie in Ihrem Netzwerk auszuführen.	Laden Sie ESA-Regeln von RSA Live herunter, um bereits erstellte Regeln zu nutzen. Ändern Sie die konfigurierbaren Parameter, um die Regeln nach Ihrem Bedarf anzupassen.

### Starterpaketregeln

Security Analytics umfasst einige Regelerstellungsregeln, die in der Regelbibliothek angezeigt werden. Verwenden Sie die Starterpaketregeln, um sich mit der Arbeit mit Regeln vertraut zu machen, bevor Sie eigene Regeln erstellen. Sie können diese Beispielregeln sicher bearbeiten und bereitstellen.

### Testregelmodus

Bei allen Typen von Regeln bietet die Auswahl der Einstellung Testregel zusätzliche Sicherheit. Testregeln werden deaktiviert, wenn sie einen vom Administrator festgelegten Schwellenwert für die Arbeitsspeicherauslastung überschreiten. Führen Sie eine Regel im Testmodus aus, um die Arbeitsspeicherauslastung zu überwachen und die Regel automatisch zu deaktivieren, wenn ihr Speicherverbrauch über dem zulässigen Schwellenwert liegt.

## Rollenberechtigungen

Dieses Thema enthält eine Liste aller ESA-Berechtigungen mit Erläuterung, welche Berechtigungen den einzelnen vorkonfigurierten Security Analytics-Rollen zugewiesen sind. Der Benutzerzugriff wird auf der Grundlage der Rollen und der den Rollen zugewiesenen Berechtigungen eingeschränkt.

- Administratoren
- Operatoren
- Analyst
- Security Operations Center-Manager (SOC-Manager)
- Malware Analysts (MA)
- Datenschutzbeauftragter

Es gibt vier Berechtigungen für ESA:

1. Auf Alerting-Modul zugreifen: Für alle Berechtigungen erforderlich
2. Regeln anzeigen: Die Nur-Lese-Berechtigung für Regeln in der Regelbibliothek
3. Warnmeldungen anzeigen: Nur-Lese-Berechtigung für Warnmeldungen, die ESA erzeugt
4. Regeln managen: Berechtigung zum Anzeigen, Erstellen, Bearbeiten und Löschen von Regeln

In der folgenden Tabelle sind die Berechtigungen für ESA und die Rollen aufgeführt, denen sie zugewiesen sind. Anhand dieser Tabelle können Sie erkennen, wie die einzelnen Rollen mit Regeln und Warnmeldungen arbeiten können.

Berechtig- ung	Admi- nistratoren	Ope- ratoren	Ana- lysten	SOC- Mana- ger	M- A	DP- O
Auf Alerting- Modul zugreifen	Ja	Ja	Ja	Ja		Ja
Regeln anzei- gen	Ja	Ja		Ja		Ja
Warnmeldungen anzeigen	Ja		Ja	Ja		Ja



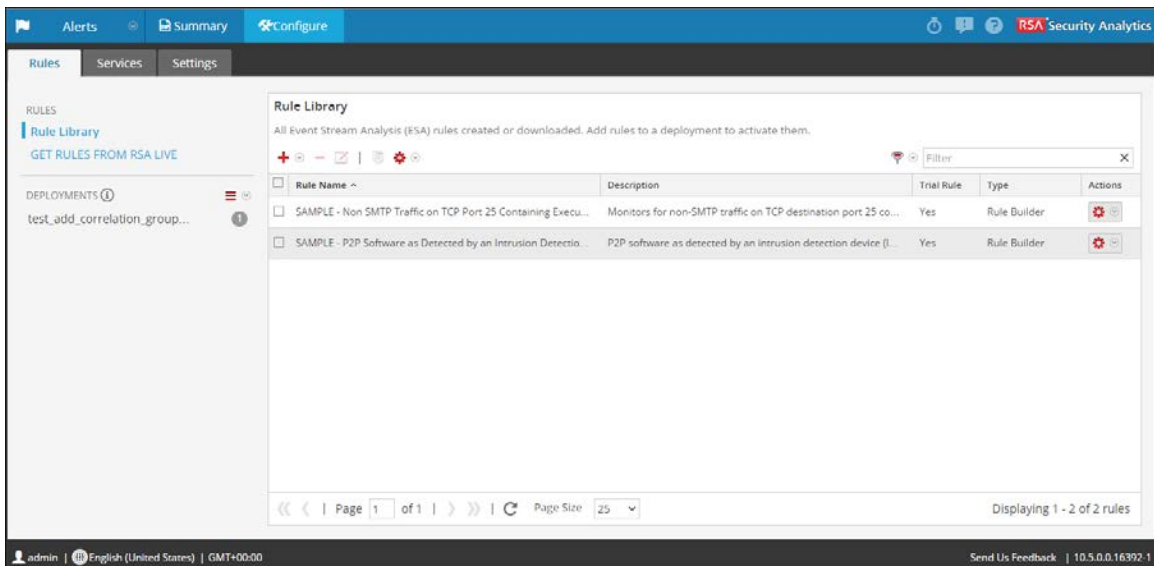
Berechtig- ung	Admi- nistratoren	Ope- ratoren	Ana- lysten	SOC- Mana- ger	M- A	DP- O
Regeln mana- gen	Ja	Ja		Ja		Ja

Weitere Informationen über Rollen und Berechtigungen finden Sie im **Handbuch Systemsicherheit und Benutzerverwaltung**.

## Üben mit Starterpaket-Regeln

Security Analytics enthält zwei Starterpaketregeln, damit Analysten sich mit dem Aussehen von Regeln vertraut machen können, bevor sie ihre eigenen Regeln erstellen. Verwenden Sie die Starterpaket-Regeln, um sich mit der Regelerstellung vertraut zu machen und das Bearbeiten und Bereitstellen von Regeln zu üben.

Die Starterpaket-Regeln sind in der Regelbibliothek installiert, die alle Regeln enthält, die Sie herunterladen oder erstellen. Die folgende Abbildung zeigt die Regelbibliothek nach der Installation.



Dies sind die verfügbaren Starterpaketregeln:

- SAMPLE: P2P Software, wie von einem Meldesystem zur Erkennung von Eindringversuchen erkannt

- **SAMPLE:** Nicht-SMTP-Datenverkehr auf TCP-Port 25, der eine ausführbare Datei enthält
- **SAMPLE: Whitelist:** von außerhalb Deutschlands, P2P-Software, wie von einem Meldesystem zur Erkennung von Eindringversuchen erkannt
- **SAMPLE: Blacklist:** aus Ländern außerhalb der US, Nicht-SMTP-Datenverkehr auf TCP-Port 25, der eine ausführbare Datei enthält
- **SAMPLE:** Benutzer derselben Administratorgruppe hinzugefügt gleicher Benutzer su Sudo

Beide Namen beginnen mit SAMPLE, um die in Security Analytics vorinstallierten Regeln von denen zu unterscheiden, die Sie herunterladen oder erstellen.

## Regelbibliothek

Die Regelbibliothek enthält folgende Informationen zu einer Regel:

- **Name:** fasst die Daten oder Ereignisse zusammen, die die Regel sammelt.
- **Beschreibung:** erklärt die Regel detaillierter. Es wird jedoch nur der Anfang in der Regelbibliothek angezeigt.
- **Testregel:** zeigt an, ob der Testmodus für die Regel aktiviert oder deaktiviert ist.
- **Typ:** zeigt den Ursprung der Regel an (in der Regelerstellung oder erweiterten EPL erstellt oder von RSA Live heruntergeladen).

Rule Name	Description	Trial Rule	Type	Actions
<input type="checkbox"/> SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Execu...	Monitors for non-SMTP traffic on TCP destination port 25 co...	Yes	Rule Builder	
<input type="checkbox"/> SAMPLE - P2P Software as Detected by an Intrusion Detectio...	P2P software as detected by an intrusion detection device (l...	Yes	Rule Builder	

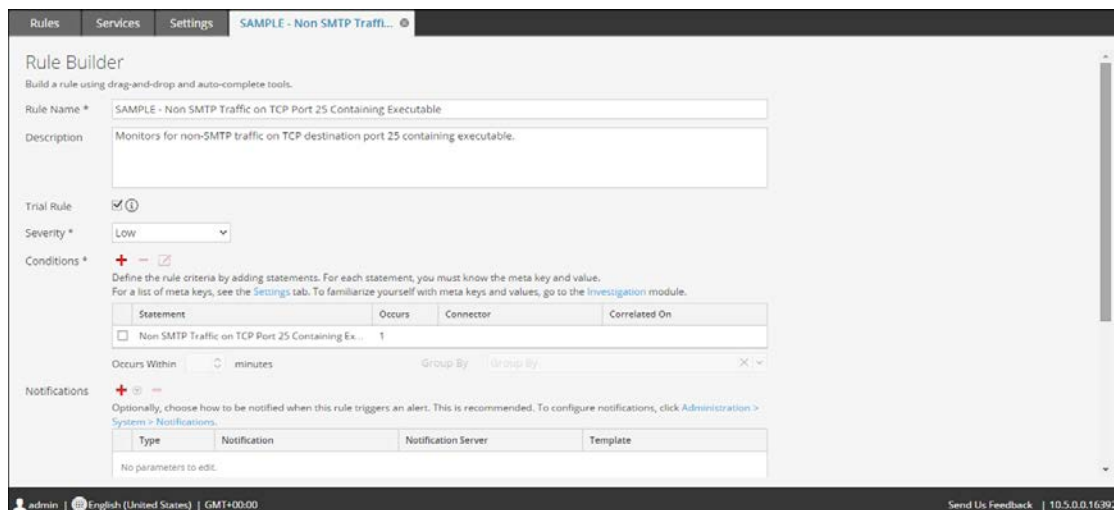
## Verfahren

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.

2. Wählen Sie in der **Regelbibliothek** eine Beispieldatei aus und klicken Sie auf  oder doppelklicken Sie auf eine Regel.

Die Regel wird in der Regelerstellung geöffnet.



3. Lesen Sie zum Üben mit einer Starterpaket-Regel die folgenden Themen für detaillierte Beschreibungen und Verfahren:

- Zum Kennenlernen der Benutzeroberfläche der Regelerstellung finden Sie unter [Registerkarte Regelerstellung](#) eine Beschreibung der einzelnen Felder.
- Wenn Sie erfahren möchten, wie Sie eine Regel bearbeiten, finden Sie unter [Hinzufügen einer Regelerstellungsregel](#) ein Schritt-für-Schritt-Verfahren.
- Wenn Sie ein Starterpaketregel bereitstellen möchten, erfahren Sie unter [Bereitstellen von Regeln für die Ausführung in ESA](#), wie Sie die Regel einem ESA-Service zuweisen können.

Nachdem Sie mit den Starterpaket-Regeln geübt haben, können Sie Ihre eigenen Regeln herunterladen, erstellen und bereitstellen.



## Verwenden von Testregeln

---

Wenn Regeln zu viel Speicher benötigen, kann Ihr ESA-Service langsam werden oder nicht mehr reagieren. Um dafür zu sorgen, dass Regeln nicht übermäßig viel Speicher benötigen, können Sie für jeden Regeltyp Testregeln aktivieren. Wenn Sie eine Testregel erstellen, stellen Sie einen globalen Schwellenwert für den Prozentsatz des Speichers ein, den Regeln verwenden können. Wenn dieser konfigurierte Speicherschwellenwert überschritten wird, werden alle Testregeln deaktiviert.

Der ESA-Service von Security Analytics (Event Stream Analysis) ist in der Lage, große Mengen unterschiedlicher Ereignisdaten von Concentrators zu verarbeiten. Allerdings ist es bei der Arbeit mit Event Stream Analysis möglich, Regeln zu erstellen, die übermäßig viel Speicher verwenden. Dies kann Ihren ESA-Service verlangsamen oder sogar verursachen, dass er unerwartet herunterfährt. Um dafür zu sorgen, dass das nicht passiert, können Sie Ihre Regel als eine Testregel konfigurieren. Wenn Sie eine Testregel konfigurieren, stellen Sie auch einen globalen Schwellenwert für den Prozentsatz des Speichers ein, den Regeln verwenden können. Wenn dieser konfigurierte Speicherschwellenwert überschritten wird, werden alle Testregeln automatisch deaktiviert.

Empfehlungen zur Erstellung effizienterer Regeln finden Sie unter „Best Practices für das Schreiben von Regeln“ in [Best Practices](#)

Eine Best Practice ist es, wenn Sie eine neue Regel hinzufügen oder eine bestehende Regel bearbeiten, die Option Testregel auszuwählen, die Ihnen Folgendes ermöglicht:

- Die Regel mit einer zusätzlichen Sicherung bereitzustellen
- Optional einen Snapshot der Speicherauslastung anzuzeigen, um zu erkennen, ob die Regel Speicherprobleme verursacht
- Zu wissen, ob Sie die Regelkriterien ändern müssen, um die Performance zu verbessern

**Hinweis:** Führen Sie eine Regel lange genug als Testregel aus, um die Performance während des normalen und des höchsten Netzwerkverkehrs zu bewerten.

## Bereitstellen von Regeln als Testregeln

In diesem Thema wird erklärt, wie Administratoren beim Erstellen neuer Regeln oder Bearbeiten von Regeln Testregeln aktivieren können. Testregeln werden automatisch deaktiviert, wenn ein festgelegter Schwellenwert für die JVM-Gesamtspeichernutzung überschritten wird.

### Verfahren

So stellen Sie Regeln als Testregeln bereit:

1. Navigieren Sie im Menü **Security Analytics** zu den Optionen **Warnmeldungen** > **Konfigurieren**.  
Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.
2. Wählen Sie in der Regelbibliothek das Hinzufügen oder Bearbeiten einer Regel aus. Die Regelerstellung wird in einer neuen Registerkarte in Security Analytics angezeigt.

Rule Builder

Build a rule using drag-and-drop and auto-complete tools.

Rule Name \* 5 Failed Login Attempts followed by Successful Login

Description The same user tries to log in and fails. 5 consecutive times. On the next try, the user logs in successfully.

Trial Rule

Severity \* Medium

Conditions \* [Investigation](#)

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> 5 Failed Logons	5	followed by	
<input type="checkbox"/> Successful Logon	1		

Occurs Within 3 minutes Group By user\_dst

Notifications [Global Notifications](#)

Output	Notification	Notification Server	Template
No parameters to edit.			

Output Suppression of every minutes

Enrichments [Settings](#)

Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
No parameters to edit.			

Debug

[Save](#) [Close](#) [Show Syntax](#) \* = required field

admin | English (United States) | GMT+00:00 [Send Us Feedback](#) | 10.5.0.0.17881-1

3. Um eine neue oder bestehende Regel zu einer Testregel zu machen, wählen Sie **Trial Rule**  aus.

4. Fügen Sie bei Bedarf Regelbedingungen hinzu oder ändern Sie die Regel. Anweisungen zum Bearbeiten von Regeln finden Sie unter [Hinzufügen von Regeln zur Regelbibliothek](#).
5. Klicken Sie auf **Save**.
6. Vergewissern Sie sich, dass die Testregeln für Ihre ESA aktiviert sind und dass die für die Testregeln konfigurierten Schwellenwerte Ihren Vorstellungen entsprechen.  
Der Speicherschwellenwert wird in der Konfigurationsdatei festgelegt. Informationen über die Konfiguration des Werts erhalten Sie unter „Ändern des Speicherschwellenwerts für Testregeln“ im **Konfigurationsleitfaden für Event Stream Analysis (ESA)**.  
Der Schwellenwert wird pro ESA konfiguriert und repräsentiert einen Prozentsatz des Java Virtual Memory.  
Der Standardwert für den Konfigurationsparameter, MemoryThresholdforTrialRules, ist 85.
7. Optional können Sie die Richtlinien in Integrität und Zustand so festlegen, dass Sie eine E-Mail-Benachrichtigung erhalten, wenn der Schwellenwert für die Gesamtnutzung des JVM-Speichers überschritten wird.

Wenn Sie die Regel das nächste Mal bereitstellen, wird Sie im Testregelmodus ausgeführt.

**Hinweis:** Wenn eine Testregel deaktiviert wird, müssen Sie zur Registerkarte **Warnmeldungen > Konfigurieren > Services** navigieren, um die Testregeln wieder zu aktivieren. Weitere Anweisungen zum erneuten Aktivieren von Testregeln auf einem Service finden Sie unter [Anzeigen von ESA-Statistiken und -Warnmeldungen](#).

## Anzeigen von Speicherkennzahlen für Regeln im Testmodus

In diesem Thema erfahren Autoren von ESA-Regeln, wie sie Speicherkennzahlen anzeigen können, wenn der für Testregeln konfigurierte Speicherschwellenwert überschritten wird. Wenn der Speicherschwellenwert überschritten wird, können Sie einen Snapshot der Speichernutzung von ESA-Regeln konfigurieren, der zu dem Zeitpunkt erstellt wird, wenn die Testregeln deaktiviert werden. Dies ermöglicht die Untersuchung der Speichernutzung und das Bearbeiten der Regeln für mehr Effizienz.

Wenn Sie Testregeln konfigurieren und die Funktion Speicher-Snapshot aktivieren, werden bei Überschreiten des Speicherschwellenwerts alle Testregeln deaktiviert und es wird ein Snapshot der Speichernutzung für alle ESA-Regeln zum Zeitpunkt der Deaktivierung erstellt. Dies ermöglicht es Ihnen, einzusehen, wie viel Speicher verwendet wurde, damit Sie die ESA-Regeln anpassen können, um sie effizienter zu machen. Der Speicher-Snapshot kann im Systemstatistikbrowser von „Integrität und Zustand“ angezeigt werden. Sie benötigen daher die Berechtigungen zum Zugriff auf dieses Modul. Wenn Sie die Details im Systemstatistikbrowser anzeigen, können Sie die Testregelsyntax ändern und die Testregeln wieder aktivieren.

Allgemein müssen Sie die folgenden Schritte ausführen, um den Speicher-Snapshot für das Troubleshooting der Speichernutzung von Regeln verwenden zu können:

1. Aktivieren Sie Testregeln für jede neue Regel, die Sie bereitstellen. Siehe [Bereitstellen von Regeln als Testregeln](#).
2. Vergewissern Sie sich, dass Sie die ESA-Richtlinien in „Integrität und Zustand“ so konfiguriert haben, dass eine E-Mail gesendet wird, wenn die Speicherschwellenwerte überschritten werden.
3. Vergewissern Sie sich, dass Sie über die korrekten Berechtigungen zum Anzeigen des Moduls „Integrität und Zustand“ verfügen. Informationen über Rollen und Berechtigungen erhalten Sie unter [Rollenberechtigungen](#).
4. Vergewissern Sie sich, dass die Funktion Speicher-Snapshot aktiviert ist (über den Parameter EnabledCaptureSnapshot in SA Explorer). Die Funktion „Speicher-Snapshot“ ist standardmäßig deaktiviert. Siehe „Aktivieren und Deaktivieren der Funktion für Speicher-Snapshots“ unten. RSA empfiehlt, die Funktion zu deaktivieren, nachdem Sie die Test neuer Regeln abgeschlossen haben.
5. Sehen Sie sich die Speicherschwellenwert-Statistiken in „Integrität und Zustand“ an, wenn der Speicherschwellenwert für Testregeln überschritten wird.
6. Ändern Sie die Regel oder Regeln, die die Warnmeldung ausgelöst haben. Best Practices für das Erstellen von Regeln finden Sie unter [Best Practices](#).
7. Aktivieren Sie die Testregeln wieder, die deaktiviert wurden, als der Speicherschwellenwert überschritten wurde. Anweisungen zum erneuten Aktivieren der Testregeln auf einem Service erhalten Sie unter [Anzeigen von ESA-Statistiken und -Warnmeldungen](#).
8. Setzen Sie das Testen der Testregeln fort.

**Hinweis:** Wie bei jedem Debugging-Tool kann ein außergewöhnlicher Overhead mit der Verwendung der Funktion Speicher-Snapshot verbunden sein. Wenn Sie aktiv einen Snapshot erstellen, kann die Funktion Speicher-Snapshot zu Verzögerungen des ESA-Services beitragen. Der ESA-Service erzeugt keine Warnmeldungen, während ein Snapshot erstellt wird. RSA empfiehlt, die Funktion zu deaktivieren, nachdem Sie das Testen neuer Regeln abgeschlossen haben. Wenn Sie die Funktion „Speicher-Snapshot“ deaktivieren, werden Testregeln weiterhin deaktiviert, wenn die Speichernutzung die konfigurierten Schwellenwerte überschreitet, es wird jedoch kein Speicher-Snapshot erstellt und die Statistik wird nicht im Systemstatistikbrowser von „Integrität und Zustand“ angezeigt.



## Voraussetzungen

Hierbei handelt es sich um die Anforderungen für das Anzeigen von Speicherkennzahlen:

- Eine oder mehrere ESA-Regeln müssen als Testregeln konfiguriert sein.
- Speicher-Snapshot muss aktiviert sein (über den Parameter EnabledCaptureSnapshot in SA Explorer).
- Der Benutzer muss über die entsprechenden Berechtigungen zum Anzeigen der Statistik in „Integrität und Zustand“ verfügen.
- Der Benutzer muss die ESA-Richtlinie in „Integrität und Zustand“ so konfiguriert haben, dass eine E-Mail gesendet wird, wenn die Speicherschwelwerte überschritten werden.

## Methoden

### Anzeigen von Speicherkennzahlen

1. Navigieren Sie im Menü **Security Analytics** zu **Administration** > **Integrität und Zustand** > **Systemstatistikbrowser**.
2. Wählen Sie als Komponente **Event Stream Analysis** aus. Geben Sie als Kategorie **ESA-Kennzahlen** ein.

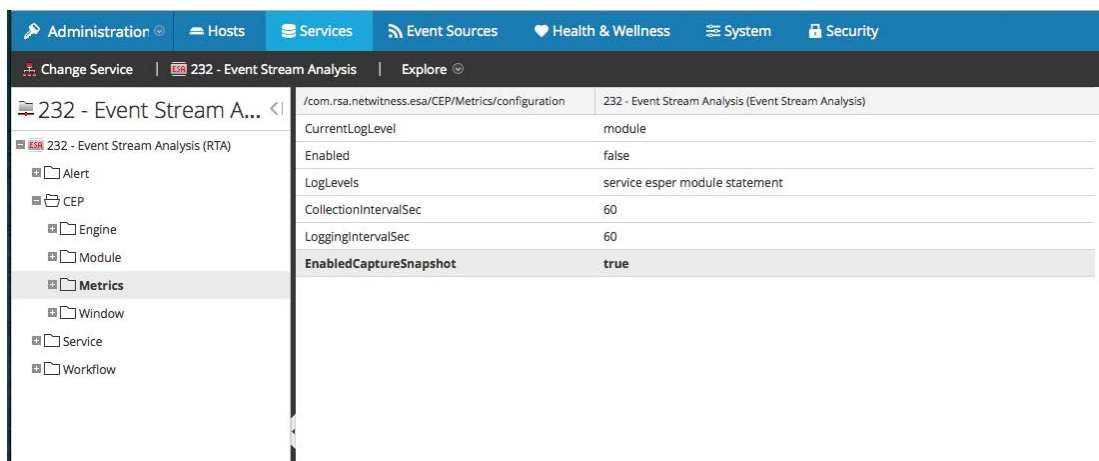
Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Named Window Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Never Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage	Always Fire	0 bytes	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Never Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Rule Total Memory Usage %	Always Fire	0%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Total ESA Memory Usage %		5.27%	2015-05-07 05:20:25 P...	
10.101.217.53	Event Stream Analysis	ESA-Metrics	Trial Rules Status		enabled	2015-05-07 05:20:25 P...	

Der Name der Regel wird im Feld **Unterelement** angezeigt, die Speichernutzung in der Spalte **Wert**.

**Hinweis:** Im Feld **Letzte Aktualisierung** ist angegeben, wann ESA von „Integrität und Zustand“ abgefragt wird. Der Speicher-Snapshot wird jedoch nur erstellt, wenn die Speicherschwelldaten überschritten werden. Das Feld gibt also keine Auskunft darüber, wann der Snapshot erstellt oder aktualisiert wurde. Der Snapshot bleibt unverändert, bis der Speicherschwelldaten wieder überschritten wird. Beispiel: Wenn der Speicherschwelldatenwert am 10.10.15 um 12 Uhr überschritten wird, die Abfrage durch „Integrität und Zustand“ aber am 10.10.15 um 15 Uhr erfolgt, wird im Feld **Letzte Aktualisierung** das Datum 10.10.15 15 Uhr angezeigt.

### Aktivieren oder Deaktivieren der Funktion Speicher-Snapshot

1. Navigieren Sie im Menü **Security Analytics** zu **Administration** > **Services** und wählen Sie Ihren ESA-Service aus.
2. Nachdem Sie die ESA ausgewählt haben, klicken Sie auf **Aktionen** > **Anzeigen** > **Durchsuchen** und navigieren Sie wie unten gezeigt zu den CEP-Kennzahlen.



3. Ändern Sie das Feld **EnabledCaptureSnapshot** in **wahr** oder **falsch**, je nachdem, ob Sie die Speicher-Snapshot-Funktion aktivieren oder deaktivieren möchten.

## Hinzufügen von Regeln zur Regelbibliothek

---

In diesem Thema wird erläutert, wie der jeweilige Regeltyp zur Regelbibliothek hinzugefügt wird. Sie müssen eine Regel zur Regelbibliothek hinzufügen, um sie bereitstellen zu können. Für alle Aufgaben in diesem Abschnitt ist die Berechtigung zum Regelmanagement erforderlich. Wenn Sie Regeln hinzufügen möchten, können Sie sie von Live-ESA herunterladen, eine Regel über die Regelerstellung erstellen oder erweiterte EPL-Regeln schreiben.

Weitere Informationen über die einzelnen Verfahren finden Sie unter:

- [Herunterladen von konfigurierbaren ESA-Regeln von RSA Live](#)
- [Hinzufügen einer Regelerstellungsregel](#)
- [Hinzufügen einer erweiterten EPL-Regel](#)

Neben der Bereitstellung einer Regel können Sie sie in der Regelbibliothek auch bearbeiten, duplizieren, importieren, exportieren und entfernen. Weitere Informationen über diese Verfahren finden Sie unter [Arbeiten mit Regeln](#)

## Herunterladen von konfigurierbaren ESA-Regeln von RSA Live

In diesem Thema wird erläutert, wie Sie konfigurierbare Regeln vom Security Analytics Live-Contentmanagementsystem herunterladen, sodass Sie sie Ihrem Bedarf anpassen können.

RSA Live enthält einen Regelkatalog. Jede Regel hat konfigurierbare Parameter, sodass Sie die Regel an Ihre Umgebung anpassen können. Wenn RSA Live eine Regel zur Erkennung von Ereignissen bietet, die Sie im Netzwerk erkennen möchten, sparen Sie Zeit, indem Sie diese Regel herunterladen. Sie können die konfigurierbaren Parameter bearbeiten und die Regel in Ihrer Regelbibliothek speichern.

Hier sehen Sie ein Beispiel dafür, wie die RSA Live-ESA-Regeln in RSA Live beschrieben werden:

Name der Regel	Beschreibung
Anmeldungen auf mehreren Servern	Erkennt Anmeldungen desselben Benutzers auf 3 oder mehr einzelnen Servern innerhalb von 5 Minuten.  Das Zeitfenster und die Anzahl eindeutiger Ziele sind konfigurierbar.

Wie der Name sagt, sucht die Regel nach Anmeldungen über mehrere Server hinweg. Die Beschreibung bietet eine genauere Erklärung der Regelkriterien und gibt an, welche Parameter Sie ändern können.

**Hinweis:** Wenn eine Regelbeschreibung einen konfigurierbaren Parameter umfasst, wird die Standardeinstellung für diesen verwendet. In der Beispielregelbeschreibung sind 5 Minuten angegeben. Da das Zeitfenster aber konfigurierbar ist, ist 5 die Standardanzahl von Minuten.

## Voraussetzungen

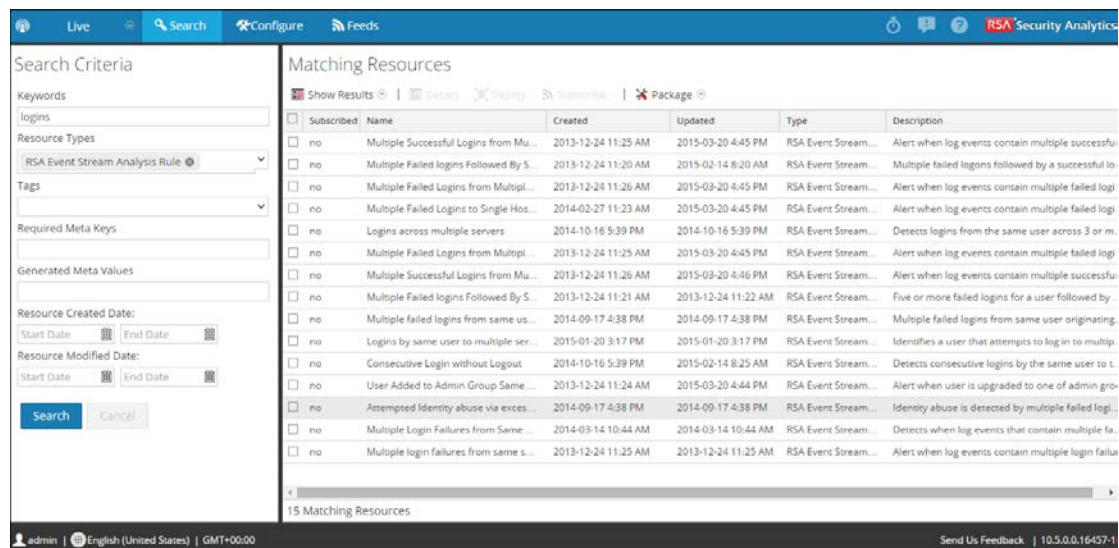
Dies sind die Voraussetzungen für das Herunterladen von konfigurierbaren RSA Live ESA-Regeln.

- Sie müssen zum Regelmanagement berechtigt sein.
- Erstellen eines Live-Kontos. Weitere Informationen finden Sie im **Handbuch Live-Servicemanagement**.
- Einrichten von Live auf Security Analytics. Weitere Informationen finden Sie im **Handbuch Live-Servicemanagement**.

## Verfahren

So laden Sie konfigurierbare ESA-Regeln von RSA Live herunter:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Registerkarte Regeln wird angezeigt.
2. Klicken Sie im Bereich Optionen auf **Regeln von RSA Live abrufen**.  
Die Registerkarte Suche wird angezeigt.



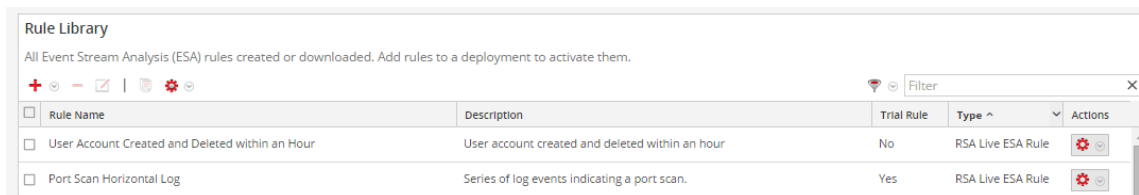
3. Wählen Sie in den **Suchkriterien** als **Ressourcentyp** die Option **RSA Event Stream Analysis-Regel** aus.
4. Legen Sie die folgenden Kriterien nach Bedarf fest, um eine Regel zum Konfigurieren für Ihre Umgebung zu suchen.  
Genauere Beschreibungen der Suchkriterien finden Sie unter „Die Ansicht Live-Suche“ im **Handbuch Live-Servicemanagement**.
  - a. Stichwörter
  - b. Tags
  - c. Erforderliche Metaschlüssel
  - d. Erzeugte Metawerte
  - e. Erstellungsdatum der Ressource
  - f. Änderungsdatum der Ressource
5. Klicken Sie auf **Search**. In Übereinstimmende Ressourcen werden die Regeln angezeigt, die mit den Suchkriterien übereinstimmen.
6. Wählen Sie alle Rollen aus, die Sie herunterladen möchten, und klicken Sie auf **Bereitstellen**.  
Der Bereitstellungsassistent wird angezeigt
7. Befolgen Sie die Schritte im Assistenten. Wenn Sie weitere Informationen benötigen, siehe „Bereitstellen von Ressourcen in Live“ im **Handbuch Live-Servicemanagement**.

Wenn Sie die Schritte im Assistenten abgeschlossen haben, werden die ausgewählten Regeln in der Regelbibliothek angezeigt.

### Anpassen von RSA Live ESA-Regeln

In diesem Thema wird erläutert, wie Parameter in einer RSA Live ESA-Regel konfiguriert werden. Wenn Sie eine RSA Live ESA-Regel konfigurieren, wird die Regel in der Regelbibliothek aufgeführt. Diese enthält folgende Spalten:

- Name
- Beschreibung
- Testregel
- Typ



The screenshot shows the 'Rule Library' interface. At the top, it says 'All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.' Below this is a table with columns: Rule Name, Description, Trial Rule, Type, and Actions. Two rules are listed: 'User Account Created and Deleted within an Hour' and 'Port Scan Horizontal Log'.

Rule Name	Description	Trial Rule	Type	Actions
<input type="checkbox"/> User Account Created and Deleted within an Hour	User account created and deleted within an hour	No	RSA Live ESA Rule	
<input type="checkbox"/> Port Scan Horizontal Log	Series of log events indicating a port scan.	Yes	RSA Live ESA Rule	


Der Typ lautet „RSA Live ESA-Regel“.

### Voraussetzungen

- Als Rollenberechtigungen sind erforderlich: Administrator, Operator, SOC Manager oder DPO.
- Regeln müssen in die Regelbibliothek heruntergeladen werden.

### Verfahren

So passen Sie eine RSA Live ESA-Regel an:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regel** aus.
2. Wählen Sie in der **Regelbibliothek** eine RSA Live ESA-Regel aus und klicken Sie auf .  
Die Registerkarte RSA Live ESA-Regel wird angezeigt.
3. (Optional) Ändern Sie die folgenden Felder:
  - Name der Regel
  - Beschreibung

- Testregel
  - Schweregrad
4. Um die Regel für Ihre Umgebung zu konfigurieren, ersetzen Sie im Abschnitt **Parameter** den Standardwert in der Spalte **Wert**.

Parameters	Name ^	Value
	With this number of events	200
	Within this number of seconds	60

5. Klicken Sie auf **Save**

## Hinzufügen einer Regelerstellungsregel

In diesem Thema wird eine Reihe von umfassenden Verfahren zum Hinzufügen von Regeln des Typs Regelerstellung vorgestellt.

Jede ESA-Regel ist darauf ausgelegt, etwas im Netzwerk zu erkennen und eine Warnmeldung dazu zu erzeugen:

- Unerlaubte Benutzeraktivitäten, wie den Versuch, Software herunterzuladen, die nicht genehmigt wurde
- Verdächtiges Verhalten, wie Massenlöschen von Audits
- Bekannte schädliche Bedrohungen, wie Tools zur Verbreitung von Würmern oder zum von Knacken von Passwörtern

Es gibt zwei Methoden für das Entwerfen von Regeln in ESA:

- Die Regelerstellung ist eine benutzerfreundliche Oberfläche. Sie geben einen Metaschlüssel und einen Wert an und wählen dann Optionen in Listen aus, um die Kriterien zu vervollständigen.
- Erweitertes EPL ermöglicht das Schreiben von Abfragen in der Event Processing Language. Dazu müssen Sie mit der EPL-Syntax vertraut sein.

Wenn Sie mit EPL vertraut sind, können Sie beide Methoden verwenden. Wenn Sie nicht mit EPL vertraut sind, müssen Sie die Regelerstellung verwenden. Diese Themen erläutern die Regelerstellung.

## Schritt 1. Benennen und Beschreiben der Rolle


Dieses Thema enthält Anweisungen zur Identifizierung einer Rolle, zur Kennzeichnung als Testregel und zum Zuweisen eines Schweregrads. Wenn Sie eine neue Regel hinzufügen, müssen Sie als erstes einen eindeutigen Namen und eine Beschreibung dessen eingeben, was die Regeln erkennt. Nach dem Speichern der Regel werden diese Informationen in der Regelbibliothek angezeigt.

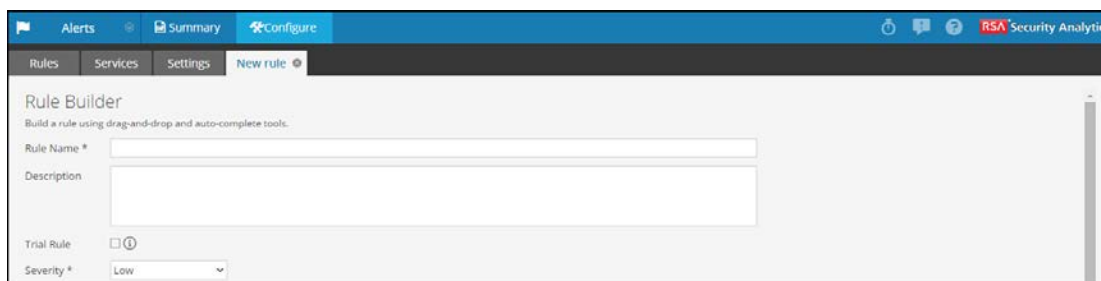
### Voraussetzungen

Sie benötigen die Berechtigung zum Verwalten von Regeln. Siehe [Rollenberechtigungen](#).

### Verfahren

So benennen und beschreiben Sie eine Regel:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regel** aus.
2. Wählen Sie in der **Regelbibliothek** die Option  **> Regelerstellung** aus.  
Die Registerkarte Neue Regel wird angezeigt.



3. Geben Sie im Feld **Name der Regel** einen eindeutigen, deskriptiven Namen ein.  
Dieser Name wird in der Regelbibliothek angezeigt. Wählen Sie ihn spezifisch genug, um die Regel von anderen abzugrenzen.
4. Erläutern Sie im Feld **Beschreibung**, welche Ereignisse von der Regel erkannt werden..  
Der Anfang der Beschreibung wird in der Regelbibliothek angezeigt.
5. Wählen Sie **Testregel** aus, um die Regel automatisch zu deaktivieren, wenn die Summe aller Testregeln den Speicherschwelldwert überschreitet.  
Verwenden Sie den Testregelmodus als Sicherheitsvorkehrung, um zu erkennen, ob eine Regel effizient ausgeführt wird, und um Ausfallzeiten aufgrund von mangelndem Speicherplatz zu vermeiden. Weitere Informationen finden Sie unter [Verwenden von Testregeln](#).



6. Klassifizieren Sie den **Schweregrad** für die Regel als Niedrig, Mittel, Hoch oder Kritisch.

## Schritt 2. Erstellen einer Regelanweisung

In diesem Thema wird erläutert, wie Sie in der Regelerstellung durch Hinzufügen von Anweisungen Regelkriterien definieren. Eine Anweisung ist eine logische Gruppierung von Regelkriterien in der Regelerstellung. Sie fügen Anweisungen hinzu, um zu definieren, was eine Regel erkennen soll.

### Beispiel

Die folgende Grafik zeigt ein Beispiel für eine Anweisung in der Regelerstellung.

Jede Anweisung enthält einen Schlüssel und einen Wert. Dann erstellen Sie Logik um dieses Paar herum. Dazu wählen Sie eine Option in den anderen Feldern aus.

Build a Statement

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name \*

if all conditions are met

Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/> event.medium	is	32	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> event.device_class	is	IDS, Firewall, IPS, Intrusion, Vuln...	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Cancel Save

### Voraussetzungen

Zum Erstellen einer Regelanweisung müssen Sie den Metaschlüssel und den Metawert kennen. Eine vollständige Liste der Metadaten Schlüssel finden Sie unter **Warnmeldungen > Konfiguration > Einstellungen > Metaschlüsselverweise**.

### Verfahren

So erstellen Sie eine Regelanweisung:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

Die Registerkarte „Regeln“ wird standardmäßig angezeigt.

2. Klicken Sie in der **Regelbibliothek** auf **+ >** **Regelerstellung** oder bearbeiten Sie eine

vorhandene Regelerstellungsregel.

Die Ansicht „Regelerstellung“ wird angezeigt.

3. Klicken Sie im Abschnitt **Bedingungen** auf **+**.

Die Ansicht „Anweisung erstellen“ wird angezeigt.

Key	Operator	Value	Ignore Case?	Array?
<input checked="" type="checkbox"/> event.ec_outcome	is	Failure	<input type="checkbox"/>	<input type="checkbox"/>

4. Geben Sie einen eindeutigen und genauen **Namen** für die Anweisung ein. Der Anweisungsname wird in der Regelerstellung angezeigt.
5. Wählen Sie in der Drop-down-Liste die Bedingungen aus, die für die Regel erforderlich sind:
- wenn **alle Bedingungen** erfüllt sind
  - wenn **eine dieser Bedingungen** erfüllt ist
6. Geben Sie die Kriterien für die Anweisung an:
- a. Geben Sie für **Schlüssel** den Namen des **Metaschlüssels** ein.
  - b. Geben Sie als **Operator** die Beziehung zwischen dem Metaschlüssel und dem Wert ein, den Sie für den Schlüssel angeben.  
Die Optionen sind: is, is not, is not null, is greater than (>), is greater than or equal to (>=), is less than (<), is less than or equal to (<=), contains, not contains, begins with, ends with
  - c. Geben Sie den **Wert** für den Metaschlüssel ein.  
Der Wert darf nicht in Anführungszeichen eingeschlossen sein. Trennen Sie mehrere Werte durch Kommata.

- d. Das Kontrollkästchen **Groß-/Kleinschreibung ignorieren?** ist für die Verwendung mit Zeichenfolgewerten und Zeichenfolgearray-Werten vorgesehen. Wenn Sie das Kontrollkästchen **Groß-/Kleinschreibung ignorieren** aktivieren, behandelt die Abfrage den gesamten Zeichenfolgetext als Wert in Kleinbuchstaben. Dadurch wird sichergestellt, dass eine Regel, die nach einem Benutzer namens „Johnson“ sucht, Ereignisse auch dann findet, wenn sie „johnson“, „JOHNSON“ oder „JoHnSoN“ enthalten.
- e. Das Kontrollkästchen **Array?** gibt an, ob der Inhalt des Felds „Wert“ einen oder mehrere Werte darstellt.  
  
Aktivieren Sie das Kontrollkästchen „Array“, wenn Sie mehrere durch Komma getrennte Werte im Feld **Wert** eingegeben haben. Zum Beispiel erfordert „ec\_activity is Logon, Logoff“, dass Sie das Kontrollkästchen „Array“ aktivieren.
7. Wenn Sie andere Metaschlüssel in der Anweisung verwenden möchten, klicken Sie auf **+**, wählen Sie **Metabedingung hinzufügen** aus und wiederholen Sie Schritt 6.
8. Klicken Sie auf **+** und wählen Sie **Whitelist-Bedingung hinzufügen** aus, um eine Whitelist hinzuzufügen.
9. Klicken Sie auf **+** und wählen Sie **Blacklist-Bedingung hinzufügen** aus, um eine Blacklist hinzuzufügen.
10. Klicken Sie zum Speichern der Anweisung auf **Speichern**.

### So fügen Sie eine Whitelist hinzu


Verwenden Sie eine Whitelist, um sicherzustellen, dass angegebene Ereignisse vom Auslösen der Regel ausgeschlossen sind. Whitelists können entweder auf dem geografischen Standort oder auf vom Kunden definierten CSV-Erweiterungsquellen basieren. Beispiel: Wenn Sie eine Regel erstellen möchten, die nur von IP-Adressen außerhalb der USA ausgelöst wird, können Sie eine Whitelist mit US-IP-Adressen erstellen.

1. Nachdem Sie eine Metabedingung hinzugefügt haben, klicken Sie auf **+** und wählen Sie **Whitelist-Bedingung hinzufügen** aus.
2. Wählen Sie im Feld **Namen für Whitelist eingeben** eine Erweiterungsquelle aus. Jede Erweiterungsquelle, die aus einer CSV-Datei oder einem benannten Fenster in Esper geladen wurde, kann als Quelle für eine Whitelist verwendet werden.
3. Wenn Sie eine GeoIP-Quelle für die Whitelist verwendet haben, wird ipv4 automatisch für die Teilbedingung eingegeben. Geben Sie den Metawert für das entsprechende Wertefeld ein. Geben Sie zum Beispiel *ipv4 is ip\_src* ein, um dafür zu sorgen, dass die GeoIP-

Datensätze basierend auf der `ip_src` ausgewählt werden, die in der GeoIP-Abfragedatenbank gefunden werden. Wenn Sie eine GeoIP-Quelle für die Whitelist verwendet haben, sollten Sie gegebenenfalls auch eine Teilbedingung hinzufügen, um die geografische Region anzugeben, die aus den Regelergebnissen ausgeschlossen werden soll. Wenn Sie beispielsweise angeben möchten, dass der Ländercode „USA“ sein muss, geben Sie *CountryCode is US* ein.

### So fügen Sie eine Blacklist hinzu

Sie verwenden eine Blacklist, um sicherzustellen, dass angegebene Ereignisse die Regel auslösen. Blacklists können entweder auf dem geografischen Standort oder auf vom Kunden definierten CSV-Erweiterungsquellen basieren. Zum Beispiel können Sie angeben, dass die Regel nur Ergebnisse aus Deutschland beinhaltet.

1. Nachdem Sie eine Metabedingung hinzugefügt haben, klicken Sie auf  und wählen Sie **Blacklist-Bedingung hinzufügen** aus.
2. Wählen Sie im Feld **Namen für Blacklist eingeben** eine Erweiterungsquelle aus. Jede Erweiterungsquelle, die aus einer CSV-Datei oder einem benannten Fenster in Esper geladen wurde, kann als Quelle für eine Blacklist verwendet werden.
3. Wenn Sie eine GeoIP-Quelle für die Blacklist verwendet haben, wird `ipv4` automatisch für die Teilbedingung eingegeben. Geben Sie den Metawert für das entsprechende Wertefeld ein. Geben Sie zum Beispiel „`ipv4 is ip_src`“ ein, um dafür zu sorgen, dass die GeoIP-Datensätze basierend auf der `ip_src` ausgewählt werden, die in der GeoIP-Abfragedatenbank gefunden werden. Wenn Sie eine GeoIP-Quelle für die Blacklist verwendet haben, sollten Sie gegebenenfalls auch eine Teilbedingung hinzufügen, um die geografische Region anzugeben, die in den Regelergebnissen eingeschlossen werden soll. Um anzugeben, dass die Regel nur Ergebnisse für Deutschland enthält, geben Sie beispielsweise „*CountryCode is DE*“ ein.

### Beispiel: Blacklist

Die folgende Anweisung zeigt eine Blacklist-Anweisung für eine Regel, die Nicht-SMTP-Datenverkehr auf TCP-Zielport 25 daraufhin überwacht, ob er ausführbare Dateien aus Ländern außerhalb der USA enthält.

**Build a Statement**

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name \*

if all conditions are met

<input type="checkbox"/>	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.service	is not	25	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.tcp_dstport	is	25	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.extension	is	exe,com,vb,vbs,vbe,cmd,bat,ws,ws...	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	blacklist.GeoIpLookup				
<input type="checkbox"/>	ipv4	is	event.ip_src	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	countryCode	is not	US	<input type="checkbox"/>	<input type="checkbox"/>

Blacklist conditions can be added to include only those items defined in an enrichment list. Map a list column to an event meta key to join the list to the incoming data stream.

Anweisung	Beschreibung
service is not 25	Der Datenverkehr ist nicht SMTP-Datenverkehr.
tcp_dstport is 25	Der Datenverkehr wird auf TCP-Port 25 ausgeführt.
extension is exe, com,v- b,vbs,vbe,cmd,bat,ws,wsf,src,sh	Die Dateierweiterung weist auf eine ausführbare Datei hin.
GeoIpLookup	Die Blacklist basiert auf einer GeoIPLookup-Quelle.
ipv4 is ip_src	Die GeoIP-Datensätze werden basierend auf der ip_src ausgewählt, die in der GeoIP-Abfragedatenbank gefunden wird.
countryCode is not US	Bei der Abfrage der IP-Adresse „Event.ip_src“ in der GeoIP-Datenbank enthält der zurückgegebene Datensatz nicht „US“ im Feld „countryCode“.

### Beispiel: Groß-/Kleinschreibung ignorieren, strenge Musterübereinstimmung und Operator *Is Not Null*

Im folgenden Beispiel wird die Groß-/Kleinschreibung ignoriert, NULL-Werte werden ausgeschlossen und es gilt eine strenge Musterübereinstimmung, um sicherzustellen, dass die erwarteten Regelergebnisse zurückgegeben werden. Die Regel besteht aus den folgenden Bedingungen:

**Rule Builder**  
Build a rule using drag-and-drop and auto-complete tools.

Rule Name \*

Description

Trial Rule

Severity \*

Conditions \*    Investigation

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Failures	5	followed by	
<input type="checkbox"/> Success	1	AND	
<input type="checkbox"/> ModifyPassword	1		

Group By

Occurs Within  minutes Event Sequence  Strict  Loose

Regelbedingung	Beschreibung
Failures	Diese Bedingung sucht nach 5 fehlgeschlagenen Anmeldungen mit einem „followed by“-Connector. Das bedeutet, dass der Bedingung (Fehler) die nächste Bedingung (Erfolg) folgen muss.
Success	Diese Bedingung sucht nach einer erfolgreichen Anmeldung.
ModifyPassword	Diese Bedingung sucht nach einer Instanz, in der das Passwort geändert wird.

Regelbedingung	Beschreibung
Gruppieren nach: user_dst	Das Feld „Gruppieren nach“ sorgt dafür, dass alle vorherigen Bedingungen nach dem Metawert „user_dst“ (dem Benutzerzielkonto) gruppiert werden. Dies ist wichtig für die Erstellung der Regel, da die Regel versucht, einen Fall zu finden, in dem ein Benutzer mehrere Male versucht hat, sich bei dem gleichen Zielkonto anzumelden, sich dann schließlich erfolgreich angemeldet und dann das Kennwort geändert hat. Die Regel gibt möglicherweise unerwartete Ergebnisse zurück, wenn Sie sie nicht nach dem Benutzerzielkonto gruppieren.
Auftreten innerhalb 5 Minuten	Das Zeitfenster für das Eintreten des Ereignisses beträgt 5 Minuten. Wenn die Ereignisse außerhalb dieses Zeitfensters auftreten, wird die Regel nicht ausgelöst.
Ereignissequenz: Strikt	Die Ereignissequenz wird für eine strenge Musterübereinstimmung konfiguriert. Das bedeutet, dass das Muster genau wie angegeben übereinstimmen muss, ohne dazwischen vorkommende Ereignisse.  Strenge Musterübereinstimmung erlaubt Ihnen sicherzustellen, dass die Esper-Engine nur Warnmeldungen für Regeln erzeugt, die genau dem Muster entsprechen, das Sie suchen. Beispielsweise könnte es eine allgemeine Regel sein, nach 5 fehlgeschlagenen Anmeldungen gefolgt von einer erfolgreichen Anmeldung zu suchen. Wenn Sie eine variable Musterübereinstimmung auswählen, wird diese Regel ausgelöst, wenn es eine beliebige Anzahl erfolgreicher Anmeldungen zwischen den fehlgeschlagenen Anmeldungen gibt. Da es bei der Regel darum geht, häufige <i>und</i> aufeinanderfolgende Anmeldeversuche zu finden, ist eine strenge Übereinstimmung erforderlich, um sicherzustellen, dass Sie die Ergebnisse erhalten, die Sie erwarten.

**Hinweis:** Jede dieser Bedingungen wird in den folgenden Abschnitten ausführlich beschrieben.

Für jede einzelne Bedingung wird eine Anweisung in der Regelerstellung erstellt. Die folgende Anweisung ergibt die Bedingung „Failures“:

**Build a Statement**

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name \* Failures

if all conditions are met

Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/> event.ec_activity	is	Logon	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.ec_outcome	is	Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Regelanweisung	Beschreibung
ec-activity is Logon (Groß-/Kleinschreibung ignorieren)	Identifiziert die Aktivität des Versuchs, sich bei einem System anzumelden  Das Kontrollkästchen <b>Groß-/Kleinschreibung ignorieren?</b> ist für die Verwendung mit Zeichenfolgewerten und Zeichenfolgearray-Werten vorgesehen. Wenn Sie das Kontrollkästchen <b>Groß-/Kleinschreibung ignorieren</b> aktivieren, behandelt die Abfrage den gesamten Zeichenfolgetext als Wert in Kleinbuchstaben. Sie können dieses Kontrollkästchen verwenden, wenn Sie unsicher sind, ob ein bestimmtes Ereignis mit Groß- oder Kleinschreibung protokolliert wird. Da die Groß-/Kleinschreibung ignoriert wird, wird die Regel ausgelöst, wenn die Aktivität als „Logon“, „logon“ oder „LoGoN“ protokolliert wird.
ec_outcome is Failure (Groß-/Kleinschreibung ignorieren)	Identifiziert, dass das Ergebnis der Aktivität als „failure“ protokolliert wird. Da die Groß-/Kleinschreibung ignoriert wird, wird die Regel ausgelöst, wenn die Aktivität als „Failure“, „failure“ oder „FaiLuRe“ protokolliert wird.



Regelanweisung	Beschreibung
user_dst is not null	<p>Sorgt dafür, dass die Bedingung nur wahr ist, wenn user_dst einen Wert besitzt.</p> <p>Mit dem Operator <b>is not null</b> können Sie sicherstellen, dass ein Feld einen Wert zurückgibt. Sie können dieses Feld verwenden, wenn eine Regel davon abhängt, dass ein bestimmtes Feld einen Wert zurückgibt. Beispielsweise möchten Sie eventuell eine Regel erstellen, die denselben Benutzer identifiziert, der mehrmals versucht, sich an demselben Zielkonto anzumelden (möglicherweise also der Versuch, das Passwort zu erraten). Wenn das Feld, das das Benutzerzielkonto repräsentiert, leer ist, möchten Sie nicht, dass die Regel ausgelöst wird. Verwenden Sie den Operator <b>is not null</b>, um sicherzustellen, dass das Feld einen Wert enthält.</p>

Die folgende Anweisung ergibt die Bedingung „Success“:

**Build a Statement** ? X

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name \*

if all conditions are met + -

	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.ec_activity	is	Logon	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.ec_outcome	is	Success	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>

Regelanweisung	Beschreibung
ec_activity is Logon	Identifiziert eine Anmeldeaktivität
ec_outcome is Success	Identifiziert eine Anmeldung, die erfolgreich abgeschlossen wurde
user_dst is not null	Stellt sicher, dass das Feld für das Benutzerzielkonto ausgefüllt ist, damit die Bedingung wahr sein kann

Die folgende Anweisung ergibt die Bedingung „ModifyPassword“:

**Build a Statement** ? X

Define a rule condition by adding one or more statements. For each statement, define the keys, operators, and values that will trigger the rule. If the contents of the value field include more than one value, you must specify that it should be evaluated as an array.

Name \*

if all conditions are met + - =

	Key	Operator	Value	Ignore Case?	Array?
<input type="checkbox"/>	event.user_dst	is not null		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.ec_subject	is	Password	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	event.ec_activity	is	Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Regelanweisung	Beschreibung
user_dst is not null	Stellt sicher, dass das Feld für das Benutzerzielkonto ausgefüllt ist, damit die Bedingung wahr sein kann
ec_subject is Password	Identifiziert ein Element als Passwort.
ec_activity is Modify	Identifiziert die Aktivität, mit der das Passwort geändert wurde

### Beispielergebnisse

Wenn die Warnmeldung für die Beispielregel ausgelöst wird, sehen Sie, dass die Regel für 7 Ereignisse ausgelöst wurde und dass jedes Ereignis einen Benutzer enthält. Sie können auch sehen, dass die Ereignisse einem strengen Muster folgen: 5 fehlgeschlagene Anmeldeereignisse, gefolgt von einer Änderung am Konto.

### 5Fails1Success1Config change - Strict Pattern

Description: 5 failures followed by 1 success and 1 config change  
Strict Match Recognise

Time: 2015-11-18T21:05:59  
Severity: Medium  
# Of Events: 7

**Event Meta** | **Events**

Date	Source	Destination	Username	Alias Host
2015-11-18T21:05:34	[REDACTED]	[REDACTED]	AAA	09:50:11, [REDACTED]
2015-11-18T21:05:34	[REDACTED]	[REDACTED]	AAA	09:50:12, [REDACTED]
2015-11-18T21:05:34	[REDACTED]	[REDACTED]	AAA	09:50:11, [REDACTED]
2015-11-18T21:05:34	[REDACTED]	[REDACTED]	AAA	09:50:10, [REDACTED]
2015-11-18T21:05:34	[REDACTED]	[REDACTED]	AAA	09:50:10, [REDACTED]
2015-11-18T21:05:46	[REDACTED]	[REDACTED]	AAA	09:50:16, [REDACTED]
2015-11-18T21:05:55	[REDACTED]	[REDACTED]	AAA	09:50:16

Wenn Sie einen Drill-down in das Modul Investigation durchführen, indem Sie auf die Quelle für eines der Ereignisse klicken, können Sie die Groß- oder Kleinschreibung bei jedem der Zeichenfolgenwerte sehen. Da Sie **Groß-/Kleinschreibung ignorieren** verwendet haben, wird die Regel ausgelöst, wenn die Zeichenfolgenwerte groß- oder kleingeschrieben wurden.

### Event Reconstruction

service	id	type	service type	service class	event source	event type	event time
[REDACTED]	3213375	Log	winevent_snare	Windows Hosts	Security	Failure Audit	2007-11-16 09:50:08.000

View Meta | View Log | Export Logs

- event.type = "Failure Audit"
- event.computer = "RET7W001"
- category = "Logon/Logoff"
- event.desc = "Logon"
- user.dst = "AAA"
- logon.type = "10"
- process = "User32"
- alias.host = "LNOHPOLBYKDP71"
- ip.src = 10.129.66.126
- parse.error = "Convert Fail: ip.srcport: 0 ,6325212"
- ec.theme = "Authentication"
- ec.subject = "User"**
- ec.activity = "Logon"**
- ec.outcome = "Failure"**

### Beispiel: Gruppieren der Regelergebnisse

Das Feld **Gruppieren nach** erlaubt Ihnen, die Regelergebnisse zu gruppieren und zu filtern. Nehmen Sie zum Beispiel an, es gibt 3 Benutzerkonten – Joe, Jane und John – und Sie verwenden den Metawert **Gruppieren nach**, user\_dst. Das Ergebnis zeigt Ereignisse gruppiert nach den Konten für Joe, Jane und John an.

Sie können auch nach mehreren Schlüsseln gruppieren und so die Regelergebnisse weiter filtern. Sie können zum Beispiel nach Benutzerzielkonto und Computer gruppieren, um festzustellen, ob ein Benutzer, der am selben Zielkonto von demselben Computer aus angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device\_class“ und „user\_dst“ gruppieren.

Das folgende Beispiel zeigt eine Regel, die nach „device\_class“ und „user\_dst“ gruppiert wurde.

The screenshot shows the 'Rule Builder' interface. The rule name is '5F1S with MultipleGroup by' and the description is '5 Failures followed by 1 Success with Group by: Device class, Destination User Account'. The severity is set to 'Low'. The conditions table is as follows:

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Failed Logins	5	followed by	
<input type="checkbox"/> Successful Login	1		

Below the conditions table, the 'Group By' field is highlighted with a red box and contains the values 'user\_dst' and 'device\_class'. At the bottom, the 'Occurs Within' field is set to '5 minutes' and the 'Event Sequence' is set to 'Strict'.

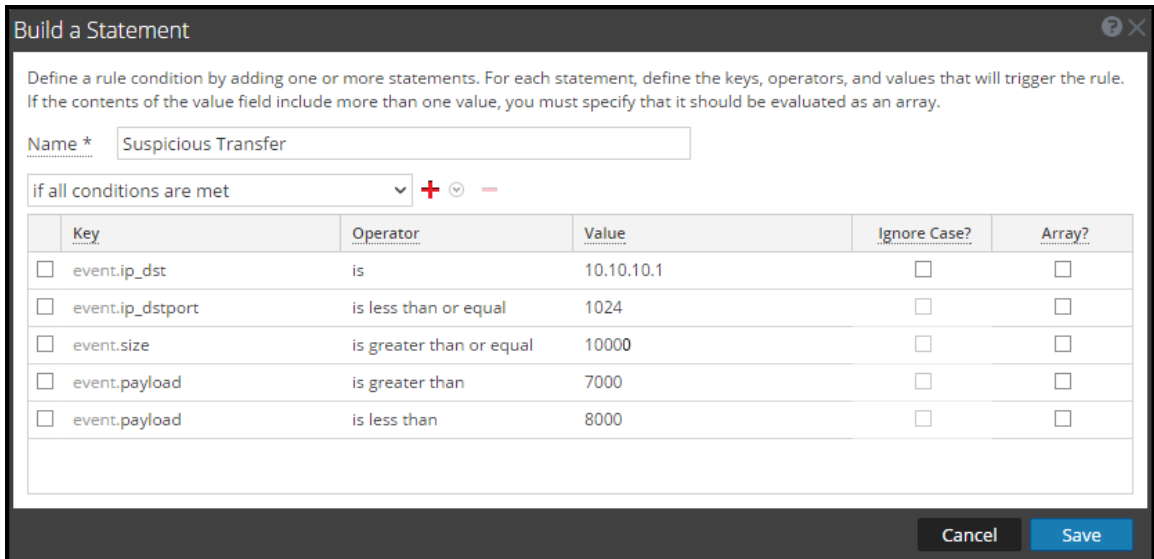
Regelbedingung	Beschreibung
Failed Logins	Identifiziert 5 fehlgeschlagene Anmeldeversuche (darauf muss die nächste Bedingung folgen; d. h. auf die 5 fehlgeschlagenen Anmeldungen muss eine erfolgreiche Anmeldung folgen).
Successful Login	Identifiziert eine erfolgreiche Anmeldung.

Regelbedingung	Beschreibung
Gruppieren nach: user_dst und device_class	Gruppiert die Regelergebnisse nach „user_dst“ (Benutzerzielkonto) und „device_class“ (Typ des Computers, von dem aus sich der Benutzer anmeldet). Dies erlaubt der Regel, nach einem Benutzer zu suchen, der von demselben Computer aus am selben Zielkonto angemeldet ist, und führt damit zu einem weitaus gezielteren Regelergebnis.
Auftreten innerhalb von 5 Minuten mit strikter Musterübereinstimmung	Die Ereignisse müssen innerhalb von 5 Minuten auftreten und die Musterübereinstimmung ist streng, d. h., das Muster muss genau erfüllt sein, damit die Regel auslöst.

**Beispiel: Arbeiten mit numerischen Operatoren**

Mit numerischen Operatoren können Sie Regeln für numerische Werte schreiben, z. B. angeben, dass ein Wert größer als, kleiner als oder gleich einem bestimmten Wert ist. Dies ist insbesondere für Fälle nützlich, in denen Sie einen numerischen Schwellenwert angeben möchten, z. B. *Nutzdaten sind größer als 7000*.

Im folgenden Beispiel wird versucht, eine Datenübertragung an ein bestimmtes Ziel über gängige Ports zu identifizieren, wobei die Übertragungsgröße hoch ist und die Nutzdaten in einem verdächtigen Bereich liegen.



Regelanweisung	Beschreibung
ip_dst is 10.10.10.1	Der Zielport ist 10.10.10.1.
ip_dstport is greater than or equal to 1024	Der Zielport ist im Bereich häufig verwendeter Ports (1024 oder höher).
size is greater than or equal to 10000	Die Größe der Übertragung ist 10000 oder größer, was eine verdächtig große Datenübertragung ist.
payload is greater than 7000	Die Größe der Nutzdaten liegt zwischen 7000 und 8000, was verdächtig groß ist.
payload is less than 8000	Die Größe der Nutzdaten liegt zwischen 7000 und 8000, was verdächtig groß ist.

### Schritt 3. Hinzufügen von Bedingungen zu einer Regelanweisung

Dieses Thema enthält Anweisungen zum Hinzufügen von Bedingungen, z. B. zum Spezifizieren eines bestimmten Zeitraums, zu einer Regelanweisung. Beim Erstellen einer Regelanweisung legen Sie fest, was eine Regel erkennt. Sie fügen Bedingungen hinzu, um weitere Festlegungen zu treffen, z. B. wie oft oder wann die Kriterien erfüllt sein müssen.

#### Beispiel

Die folgende Grafik enthält ein Beispiel mit den Bedingungen von zwei Anweisungen in der Regelerstellung. In Kombination ergeben die Anweisungen und Bedingungen die Regelkriterien.

The screenshot shows the 'Conditions' configuration window. At the top, there are controls for adding (+), removing (-), and refreshing (🔄) conditions. A 'Correlated On' link is visible in the top right. The main area contains a table with the following data:

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Failed Logins	5	followed by	
<input type="checkbox"/> Successful Login	1		

Below the table, the 'Group By' section has two dropdown menus: 'user\_dst' and 'device\_class'. The 'Occurs Within' section is set to '5' minutes. The 'Event Sequence' section has two radio buttons: 'Strict' (selected) and 'Loose'.


Diese Regel erkennt 5 fehlgeschlagene Anmeldeversuche gefolgt von einem erfolgreichen Versuch. Dies könnte ein Zeichen dafür sein, dass ein Benutzerkonto gehackt wurde. Die Kriterien für die Regel sind:

- Es sind 5 fehlgeschlagene Anmeldeversuche hintereinander erforderlich.
- Auf die Fehlschläge muss 1 erfolgreiche Anmeldung folgen.
- Alle Ereignisse müssen innerhalb von 5 Minuten auftreten.

- D. Gruppieren Sie Warnmeldungen nach Benutzer (user\_dst), weil die Schritte A und B auf demselben Benutzerzielkonto durchgeführt werden müssen. Gruppieren Sie auch nach Computer (Device\_class), um sicherzustellen, dass der Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden.
- E. Die Übereinstimmung ist ein strenges Muster, was bedeutet, dass das Muster genau übereinstimmen muss, ohne dazwischenliegende Ereignisse.

### Verfahren

So fügen Sie einer Regelanweisung Bedingungen hinzu:

1. Wählen Sie im Bereich **Bedingungen** eine Anweisung aus und klicken Sie auf .
2. Geben Sie für **Auftreten** einen Wert ein, um anzugeben, wie oft ein Ereignis auftreten muss, um die Regelkriterien zu erfüllen.
3. Wenn mehrere Anweisungen vorhanden sind, wählen Sie im Feld **Verbindungsoperator** einen logischen Operator aus, um die Anweisungen zusammenzufügen:
  - gefolgt von
  - nicht gefolgt von
  - UND
  - ODER
4. **korreliert am** gilt nur für **nicht gefolgt von**.  
Wenn Sie im vorherigen Schritt **nicht gefolgt von** ausgewählt haben, geben Sie den Metaschlüssel ein, der nicht folgen darf.
5. Wenn Ereignisse innerhalb eines bestimmten Zeitraums auftreten müssen, geben Sie im Feld **Auftreten innerhalb** eine Minutenzahl ein.
6. Wählen Sie aus, ob das Muster einer **strengen** oder einer **variablen** Übereinstimmung folgen muss. Wenn Sie eine strenge Übereinstimmung angeben, bedeutet dies, dass das Muster in der genauen Reihenfolge vorkommen muss, die Sie angegeben haben, ohne dass weitere Ereignisse dazwischen vorkommen. Beispiel: Wenn als Sequenz fünf fehlgeschlagene Anmeldungen (F) gefolgt von einer erfolgreichen Anmeldung (S) angegeben ist, wird dieses Muster nur übereinstimmen, wenn der Benutzer die folgende Sequenz ausführt: F, F, F, F, F, S. Wenn Sie eine variable Übereinstimmung angeben, bedeutet dies, dass andere Ereignisse innerhalb der Sequenz auftreten dürfen, aber die Regel wird weiterhin auslösen, wenn alle angegebenen Ereignisse auch auftreten. Beispiel: Fünf fehlgeschlagene Anmeldeversuche (F), gefolgt von einer beliebigen Anzahl dazwischen

liegender erfolgreicher Anmeldeversuche (S), gefolgt von einem erfolgreichen Anmeldeversuch, könnten das folgende Muster erzeugen: F, S, F, S, F, S, F, S, F, S, die die Regel trotz der dazwischenliegenden erfolgreichen Anmeldungen auslösen würden.

7. Wählen Sie die Felder, nach denen gruppiert werden soll, aus der Drop-down-Liste aus. Mit dem Feld **Gruppieren nach** können Sie die eingehenden Ereignisse gruppieren und evaluieren. Beispiel: In der Regel, die fünf fehlgeschlagene Anmeldeversuche gefolgt von einem erfolgreichen Versuch erkennt, muss der Benutzer identisch sein. Daher lautet der unter **Gruppieren nach** aufgeführte Metaschlüssel „user\_dst“. Sie können auch nach mehreren Schlüsseln gruppieren. Mithilfe des vorherigen Beispiels möchten Sie eventuell nach Benutzern und Computern gruppieren, um sicherzustellen, dass derselbe Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device\_class“ und „user\_dst“ gruppieren.

## Hinzufügen einer erweiterten EPL-Regel

In diesem Thema wird erläutert, wie Sie durch Schreiben einer EPL-Abfrage Regelkriterien definieren. EPL ist eine deklarative Sprache zur Bearbeitung von häufig auftretenden, zeitbasierten Ereignisdaten. Sie dient zum Ausdrücken von Filterungen, Aggregationen und Verknüpfungen über mehrere verteilte Ereignisstreams. EPL umfasst außerdem Mustersemantik zum Ausdruck komplexer zeitlicher Zusammenhänge zwischen Ereignissen.

Schreiben Sie eine erweiterte EPL-Regel, wenn die Regelkriterien komplexer sind als die Angaben in der Regelerstellung ermöglichen.

Die EPL-Syntax kann im Rahmen dieses Handbuchs nicht erläutert werden.

- Die EPL-Dokumentation finden Sie unter <http://www.espertech.com/esper/documentation.php>.
- Das EPL-Onlinetool finden Sie unter <http://esper-epl-tryout.appspot.com/epltryout/mainform.htm>.

## Voraussetzungen



Im Folgenden finden Sie die Voraussetzungen für das Hinzufügen einer erweiterten Regel:

- Sie müssen die EPL (Event Processing Language) kennen.
- Sie müssen ESA-Anmerkungen kennen, um markieren zu können, welche EPL-Anweisungen mit erzeugten Warnmeldungen verknüpft sind.



## Verfahren

So fügen Sie eine erweiterte EPL-Regel hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Wählen Sie in der **Regelbibliothek** die Optionen   > **Erweiterte EPL** aus.

3. Geben Sie im Feld **Name der Regel** einen eindeutigen, deskriptiven Namen ein.  
Dieser Name wird in der Regelbibliothek angezeigt. Wählen Sie ihn spezifisch genug, um die Regel von anderen abzugrenzen.
4. Erläutern Sie im Feld **Beschreibung**, welche Ereignisse von der Regel erkannt werden..  
Der Anfang der Beschreibung wird in der Regelbibliothek angezeigt.
5. Wählen Sie **Testregel** aus, um die Regel automatisch zu deaktivieren, wenn die Summe aller Testregeln den Speicherschwelldwert überschreitet.  
Verwenden Sie den Testregelmodus als Sicherheitsvorkehrung, um zu erkennen, ob eine Regel effizient ausgeführt wird, und um Ausfallzeiten aufgrund von mangelndem Speicherplatz zu vermeiden. Weitere Informationen finden Sie unter [Verwenden von Testregeln](#).
6. Klassifizieren Sie den **Schweregrad** für die Regel als Niedrig, Mittel, Hoch oder Kritisch.
7. Schreiben Sie zur Definition der Regelkriterien eine **Abfrage** in EPL.

**Hinweis:** Für alle Metaschlüsselnamen müssen Sie einen Unterstrich anstelle eines Punkts verwenden. Zum Beispiel ist `ec_outcome` korrekt, aber `ec.outcome` nicht.

8. Wenn eine Regel eine Warnmeldung erzeugen soll, fügen Sie diese ESA-Anmerkung in der Syntax ein:

```
@RSAAAlert
```

ESA ermöglicht zwei Anmerkungen. Details finden Sie unter [ESA-Anmerkungen](#).

## Event Processing Language (EPL)

In diesem Thema wird EPL (Event Processing Language, Ereignisverarbeitungssprache) beschrieben, eine deklarative Sprache zur Handhabung hochfrequenter, zeitbasierter Ereignisdaten. ESA verwendet EPL, eine deklarative Sprache zur Handhabung hochfrequenter, zeitbasierter Ereignisdaten. Sie dient zum Ausdruck von Filterung, Aggregation und Verknüpfung über mehrere verteilte Ereignisstreams. EPL umfasst außerdem Mustersemantik zum Ausdruck komplexer zeitlicher Zusammenhänge zwischen Ereignissen. Sie kann unter anderem folgende Funktionen ausführen:

- Ereignisfilterung
- Warnmeldungsunterdrückung
- Berechnung von Prozentwerten oder Verhältnissen
- Durchschnitt, Zähler, Minimum und Maximum für ein angegebenes Zeitfenster
- Korrelation von Ereignissen, die in mehreren Streams eingehen
- Korrelation von Ereignissen, die in falscher Reihenfolge eingehen
- Ein/Aus-Fenster
- Unterstützung von Gefolgt von und Nicht gefolgt von
- Unterstützung von Regex-Filtern

Datenbanken können sinnvolle Daten nur als Antwort auf explizite Abfragen zurückgeben und sind nicht zur Push-Übertragung von Daten bei Änderungen geeignet. Der Entwickler muss die zeitliche Logik und die Aggregationslogik selbst implementieren. Im Gegensatz dazu bietet die EPL-Engine eine höhere Abstraktion und Intelligenz; man kann sie sich als auf dem Kopf stehende Datenbank vorstellen. Anstatt Daten zu speichern und Abfragen an den gespeicherten Daten durchzuführen, ermöglicht EPS es Anwendungen, die Abfragen zu speichern und die Daten kontinuierlich durchlaufen zu lassen. Die Antwort der EPL-Engine wird in Echtzeit gegeben, wenn Bedingungen auftreten, die den vom Benutzer definierten Abfragen entsprechen.

In der Onlinehilfe wird die Einrichtung von ESA anhand von einfachen Anweisungen illustriert; wenn Sie jedoch weitere Informationen über das Verfassen von EPL-Anweisungen benötigen, erhalten Sie auf der Website <http://www.espertech.com> Schulungsmaterial und Beispiele.

**Hinweis:** ESA unterstützt Esper Version 5.1.0.

## ESA-Anmerkungen

In diesem Thema werden zwei Anmerkungen beschrieben, die Security Analytics zur Verwendung in erweiterten EPL-Regeln bietet.

### @RSAAlert-Anmerkung

Mit der @RSAAlert-Anmerkung können die EPL-Anweisungen markiert werden, die mit erzeugten Warnmeldungen verknüpft sind. Die @RSAAlert-Anmerkung ist in erweiterten Regeln optional und nur für Anweisungen hilfreich, die ESA-Warnmeldungen erzeugen.

**Hinweis:** Diese Anmerkung wird nicht in allen EPL-Anweisungen benötigt, z. B. nicht in solchen, die benannte Fenster erstellen usw.

### @RSAPersist-Anmerkung

Mit der @RSAPersist-Anmerkung kann ein benanntes Fenster als von ESA verwaltetes, persistentes Fenster markiert werden. Nachdem ein benanntes Fenster als von ESA verwaltetes Fenster markiert wurde, schreibt ESA die Inhalte des Fensters regelmäßig auf die Festplatte und stellt sie wieder her, wenn die Bereitstellung des Fensters aufgehoben wurde und es wiederhergestellt werden soll. Das System erfasst kurz vor dem Aufheben der Bereitstellung des Moduls und der Entfernung des Fensters einen Snapshot. In ähnlicher Weise stellt es die Fensterinhalte aus dem Snapshot sofort nach dem erneuten Bereitstellen des Moduls wieder her. Damit wird sichergestellt, dass die Inhalte des Fensters nicht verloren gehen, wenn sich der Modulstatus ändert oder der ESA-Service ausfällt.

Beispiel: Das Fenster mit der Bezeichnung `DHCPTracker` enthält eine Zuordnung von IP-Adressen zu dem zuletzt zugewiesenen Hostnamen. Sie können der Anweisung folgende @RSAPersist-Anmerkung hinzufügen:

```
@RSAPersist
  create window DHCPTracker.std:unique(ip_src) as (ip_src string, alias_
host string);
  insert into DHCPTracker select IP as ip_src, HostName as alias_
host from DHCPAssignment(ID=32);
```

**Hinweis:** Nicht alle Fensterdefinitionen eignen sich für die Persistenz. @RSAPersist - Anmerkungen müssen mit Vorsicht verwendet werden. Wenn das Fenster über Datensätze mit Zeitangaben verfügt oder wenn es von zeitbasierten Einschränkungen abhängt, ist es sehr wahrscheinlich, dass das Fenster durch den Snapshot nicht im richtigen Status wiederhergestellt wird. Außerdem machen alle Änderungen an der Fensterdefinition den Snapshot ungültig, sodass das Fenster auf einen leeren Status zurückgesetzt werden würde. Das System führt keine semantische Analyse durch, um zu ermitteln, ob die Änderungen einer Fensterdefinition Konflikte auslösen. Beachten Sie, dass Änderungen an anderen Teilen eines Moduls (d. h. anderen als dem CREATE WINDOW-Aufruf, der das Fenster definiert) die Snapshots nicht ungültig machen.

## Beispiele für erweiterte EPL-Regeln

Im Folgenden sehen Sie die Beispiele für erweiterte ESA-Regeln. Jedes Beispiel bietet mehrere Möglichkeiten zur Implementierung des gleichen Anwendungsbeispiels.

### Beispiel Nr. 1:

Erstellen Sie ein Benutzerkonto und löschen Sie eben dieses Benutzerkonto in 300 Sekunden. Benutzerinformationen werden in der Metadatei user\_src gespeichert.

### EPL Nr. 1:

Regelname	CreateuseraccountFollowedByDeletionof Useraccount1
Regelbeschreibung	Erstellen Sie ein Benutzerkonto, gefolgt von einer Aktion, um eben dieses Benutzerkonto in 300 Sekunden zu löschen.
Regelcode	<pre>SELECT * FROM Event(ec_subject='User'   AND ec_outcome='Success'   AND user_src is NOT NULL   AND ec_activity IN ('Create', 'Delete') ).win:time(300 seconds)  match_recognize (partition by user_src   measures C as c, D as d   pattern (C D)   define     C as C.ec_activity='Create' ,     D as D.ec_activity='Delete');</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Filtern Sie Ereignisse, die für Muster im vorgegebenen Zeitraum erforderlich sind. Aufgrund der Filterbedingungen sollten nur erforderliche Ereignisse an die Funktion match_recognize übergeben werden. In diesem Fall handelt es sich um Erstellen und Löschen von</li> </ul>

	<p>Benutzerkontoereignissen, d. h. Event(ec_subject='User' AND ec_outcome='Success' AND user_src is NOT NULL AND ec_activity IN ('Create', 'Delete')).</p> <ul style="list-style-type: none"> <li>• Partitionieren Sie durch das Erstellen von Buckets. In diesem Fall werden von Esper Buckets pro Wert von user_src erstellt. Und daher weisen beide Ereignisse den gleichen Wert von user_src auf.</li> <li>• Definieren Sie das gewünschte Muster. Gegenwärtig ist es auf Erstellen gefolgt von Löschen eingestellt. Sie können mehrfach Erstellen gefolgt von Löschen (C+ D) einstellen. Ein Muster ist einem regulären Ausdruck sehr ähnlich.</li> <li>• Dies ist das effizienteste Anwendungsbeispiel.</li> </ul>
--	--

**EPL Nr. 2:**

Name der Regel	CreateuseraccountFollowedByDeletionof Useraccount2
Regelbeschreibung	Erstellen Sie ein Benutzerkonto, gefolgt von einer Aktion, um eben dieses Benutzerkonto in 300 Sekunden zu löschen.
Regelcode	<pre>SELECT * from pattern[every (a= Event(ec_ subject='User' AND ec_outcome='Success' AND user_dst is NOT NULL AND ec_activity IN ('Create')) -&gt; ( Event(ec_subject='User' AND ec_ outcome='Success' AND user_dst is NOT NULL AND ec_ activity IN ('Create') AND user_src = a.user_src) ) )where timer:within(300 Sec) ];</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Angenommen, der Benutzer wird zweimal erstellt und einmal gelöscht in dieser Reihenfolge. Dann gibt das oben genannte Muster 2 Warnmeldungen aus.</li> <li>• Für jede Benutzererstellung wird ein Thread erstellt.</li> <li>• Es gibt keine Möglichkeit, um Threads zu steuern. Es ist wichtig, zeitliche Begrenzungen und vorzugsweise kurze Intervalle anzugeben.</li> </ul>

**Beispiel Nr. 2:**

Entdecken eines Musters, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers und der anschließenden Löschung des Benutzerkontos. Im Fall von Windows-Protokollen werden Benutzerinformationen je nach Ereignis entweder in user\_dst oder user\_src gespeichert.

user\_src(create) = user\_dst(Login) = user\_src(Delete)

**EPL Nr. 3:**

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.
Regelcode	<pre>SELECT * FROM Event(ec_subject='User'     and ec_activity in ('Create','Logon','Delete')     and ec_theme in ('UserGroup', 'Authentication')     and ec_outcome='Success'     ).win:time(300 seconds) match_recognize (measures C as c, L as l, D as d     pattern (C L D)     define         C as C.ec_activity = 'Create',         L as L.ec_activity = 'Logon' AND L.user_dst =         C.user_src,         D as D.ec_activity = 'Delete' AND D.user_src =         C.user_src     );</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Da user_src/user_dst nicht allen Ereignissen gemeinsam ist, kann keine Partition verwendet werden. 1 einzelner Bucket führt jeweils 1 Muster aus. Beispiel: Wenn der Ereignisstream für Benutzer 1 und 2 C1C2L1D1, C1L1C2D1 lautet, wird keine Warnmeldung ausgegeben, da der Thread C1 von C2 zurückgesetzt wurde. Eine Warnmeldung wird nur ausgegeben, wenn C1L1D1 in dieser Reihenfolge erfolgen und kein anderes Ereignis weder von selben Benutzer noch einem anderen Benutzer dazwischen auftritt.</li> <li>• Eine weitere Lösung wäre die Verwendung eines benannten Fensters, das Zusammenführen von user_dst und user_src in einer einzelnen Spalte und die anschließende Ausführung von match_</li> </ul>

	<p>recognize. (EPL Nr. 3).</p> <ul style="list-style-type: none"> <li>• Muster können ebenfalls verwendet werden. Möglicherweise erhalten Sie mehr Warnmeldungen als erwartet. (EPL Nr. 4).</li> </ul>
--	--

**EPL Nr. 4: Verwenden von NamedWindows und match\_recognize**

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	<p>Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.</p>
Regelcode	<pre> @Name('NormalizedWindow') create window FilteredEvents.win:time(300 sec) (user String, ecactivity string, sessionid Long);  @Name('UsersrcEvents') Insert into FilteredEvents select user_src as user, ec_activity as ecactivity, sessionid from Event(ec_subject='User' and ec_ activity in ('Create','Delete') and ec_theme in ('UserGroup', 'Authentication') and ec_ outcome='Success' and user_src is not null );  @Name('UsrdstEvents') Insert into FilteredEvents select user_dst as user, ec_activity as ecactivity, sessionid from Event(ec_subject='User' and ec_activity in (Logon') and ec_theme in ('UserGroup', 'Authentication') and ec_ outcome='Success' and user_dst is not null );  @Name('Pattern')  @RSAAalert(oneInSeconds=0, identifiers={"user"})  select * from FilteredEvents     match_recognize ( partition by user measures C as c, L as l, D as d pattern (C L+D) define C as C.ecactivity= 'Create', L as L.ecactivity= 'Logon', D as D.ecactivity='Delete' ); </pre>

**EPL Nr. 5: Verwenden von Every @RSAAlert(oneInSeconds=0, identifiers={user\_src})**

SELECT a.time as time,a.ip\_src as ip\_src,a.user\_dst as user\_dst,a.ip\_dst as ip\_dst,a.alias\_host as alias\_host from pattern[every (a=Event (ec\_subject='User' and ec\_activity='Create' and ec\_theme='UserGroup' and ec\_outcome='Success') -> (Event(ec\_subject='User' and ec\_activity='Logon' and ec\_theme='Authentication' and user\_src=a.user\_dst) -> b=Event (ec\_subject='User' and ec\_activity='Delete' and ec\_theme='UserGroup' and user\_dst=a.user\_dst))) where timer:within(300 sec)];

Name der Regel	CreateUserLoginandDeleteUser
Regelbeschreibung	Entdecken Sie ein Muster, in dem ein Benutzer ein Benutzerkonto erstellt, gefolgt von der Anmeldung dieses Benutzers, gefolgt vom Löschen des Benutzerkontos.

**Beispiel Nr. 3:**

Übermäßige Anmeldefehler von derselben Quell-IP

**EPL Nr. 6: @RSAAlert(oneInSeconds=0, identifiers={ip\_src})**

Name der Regel	ExcessLoginFailure
Regelbeschreibung	Derselbe Benutzer versuchte, sich von derselben Quell-IP anzumelden, und die Anmeldung ist fehlgeschlagen
Regelcode	<pre>SELECT * FROM   Event (     ip_src IS NOT NULL AND ec_activity='Logon'     AND ec_outcome = 'Failure' ).std:groupwin(ip_src).win:time_length_batch(300 sec, 10) GROUP BY ip_src HAVING COUNT(*) = 10;</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Erstellt Fenster gemäß ip_src</li> <li>• Verwendet time_length_batch: Prüft Ereignisse in Batches (Rollierendes Fenster). Jedes Ereignis ist nur Teil eines Fensters. Das Fenster gibt Ereignisse frei, wenn entweder die Zeit abgelaufen oder die Anzahl erreicht ist.</li> <li>• Eines der Probleme mit rollierenden Fenstern ist, dass Ereignisse, die gegen Batch-Ende auftreten, möglicherweise keine Warnmeldung auslösen.</li> </ul>



Obgleich in der folgenden Reihenfolge der Ereignisse bis  $t=301$  10 Anmeldefehler für dieselbe Anmeldung in den letzten 300 Sekunden auftraten, wird keine Warnmeldung ausgegeben, da der Ereignis-Batch bei  $t=300$  verworfen wurde.

Zeit t	Anmeldefehler für bestimmte Benutzer	Warnmeldungen	Zeit-Batch
0	0	0	1
295	6	0	1
299	3	0	1
301	1	0	2
420	6	0	2
550	3	0	2
600	0	0	3
720	6	0	3
850	3	0	3
900	1	1	3 endet und 4 beginnt

- Das oben genannte Problem kann mithilfe von win:time-Fenstern (EPL Nr. 7) anstelle von win:time\_length\_batch-Fenstern gelöst werden.
- Mit dem äußeren Group by werden Ereignisse nach Ablauf der Zeit gesteuert. Angenommen, es liegen 9 Ereignisse nach 60 Sekunden vor, dann werden diese 9 Ereignisse von der Esper-Engine an den Listener übertragen. Group by und Count führen zu einer Einschränkung, da die Anzahl ungleich 10 ist.
- Zeit und Anzahl können nach Bedarf geändert werden.

**EPL Nr. 7: @RSAAAlert(oneInSeconds=0, identifiers={"ip\_src"})**

Name der Regel	ExcessLoginFailure
Regelbeschreibung	Derselbe Benutzer versuchte, sich von derselben Quell-IP anzumelden, und die Anmeldung ist fehlgeschlagen

Regelcode	<pre>SELECT * FROM   Event (     ip_src IS NOT NULL AND ec_activity='Logon' AND ec_ outcome = 'Failure'   ).std:groupwin(ip_src).win:time (300 sec) GROUP BY ip_src HAVING COUNT(*) = 10</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Hierbei handelt es sich um ein Schiebefenster, d. h. nachdem eine Warnmeldung für eine Reihe von Ereignissen ausgegeben wurde, können sie für eine weitere Warnmeldung verwendet werden, bis die Zeit abgelaufen ist.</li> <li>• Wenn 10 Ereignisse an der Auslösung einer Warnmeldung beteiligt waren, wird nur der letzte Ereignisse angezeigt.</li> <li>• Wenn &lt; oder &gt; verwendet wird, werden möglicherweise mehrere Warnmeldungen angezeigt. Sie sollten die Warnmeldungsunterdrückung entsprechend einsetzen.</li> </ul>

**Beispiel Nr. 4:**

Mehrere fehlgeschlagene Anmeldungen von verschiedenen Benutzern von derselben Quelle an dasselbe Ziel, ein einzelner Benutzer von mehreren verschiedenen Quellen an dasselbe Ziel.

**EPL Nr. 8: Verwenden von groupwin , time\_length\_batch und unique**

Name der Regel	MultiplefailedLogins
Regelbeschreibung	<p>Es liegen mehrere fehlgeschlagene Anmeldungen für die folgenden Fälle vor:</p> <ul style="list-style-type: none"> <li>- von mehreren Benutzern von derselben Quelle an dasselbe Ziel.</li> <li>- von einem einzelnen Benutzer von mehreren Quellen an dasselbe Ziel.</li> </ul>
Regelcode	<pre>SELECT * FROM   Event( ec_activity='Logon' AND ec_ outcome='Failure' AND ip_src IS NOT NULL AND ip_ dst IS NOT NULL AND user_dst IS NOT NULL ).std:groupwin(ip_src,ip_dst).win:time_length_batch (300 seconds, 5).std:unique(user_dst) group by ip_ src,ip_dst having count(*) = 5;</pre>
Hinweis	<ul style="list-style-type: none"> <li>• ip.dst und ip.src sind allen Ereignissen gemeinsam.</li> </ul>

	<ul style="list-style-type: none"> <li>• user_dst ist für alle Ereignisse eindeutig.</li> <li>• Eine Warnmeldung wird abgegeben, wenn mindestens 5 verschiedene Benutzer eine Anmeldung von derselben ip.src- und ip.dst-Kombination versuchen.</li> </ul>
--	--

**Beispiel Nr. 5:**

Kein Protokollverkehr von einem Gerät in einem vorgegebenen Zeitraum.

**EPL Nr. 9: Verwenden von groupwin, time\_length und unique**

Name der Regel	NoLogTraffic
Regelbeschreibung	Es wird kein Protokollverkehr von einem Gerät in einem vorgegebenen Zeitraum festgestellt.
Regelcode	<pre>SELECT * FROM pattern [every a = Event(device_ip IN ('10.0.0.0', '10.0.0.1') AND medium = 32) -&gt; (timer:interval (3600 seconds) AND NOT Event(device_ip = a.device_ip AND device_type = a.device_type AND medium = 32))];</pre>
Hinweis	<ul style="list-style-type: none"> <li>• Von der Regel wird nur ein plötzlicher Verkehrsrückgang erkannt. Es wird keine Warnmeldung ausgegeben, wenn es überhaupt keinen Datenverkehr gibt. Es ist mindestens ein Ereignis erforderlich, damit aufgrund der Regel eine Warnmeldung ausgegeben wird.</li> <li>• Liste der Geräte-IP-Adresse oder Gerätehostnamen als Eingabe. Nur diese Systeme werden nachverfolgt.</li> <li>• Eine Zeiteingabe ist erforderlich. Eine Warnmeldung wird ausgegeben, wenn das Zeitintervall zwischen Ereignissen die Eingabezeit überschreitet.</li> </ul>

**Beispiel Nr. 6:**

Mehrere fehlgeschlagene Anmeldungen vom selben Benutzer, auf die KEIN Sperrungsereignis folgt.

**EPL Nr. 10: Verwenden von groupwin , time\_length\_batch und unique**

Name der Regel	FailedloginswoLockout
----------------	-----------------------

<p>Regelbeschreibung</p>	<p>Es gibt mehrere fehlgeschlagene Anmeldungen vom selben Benutzer, auf die KEIN Sperrungsereignis folgt.</p>
<p>Regelcode</p>	<pre>SELECT * FROM pattern [every-distinct(a.user_ dst, a.device_ip, 1 msec) (a= Event(ec_ activity='Logon' and ec_outcome='Failure' and user_dst IS NOT NULL)-&gt; [2]( Event( device_ip =a.device_ip and ec_activity='Logon' and ec_ outcome='Failure' and user_dst=a.user_dst) AND NOT Event( ( ec_activity='Logon' and ec_ outcome='Success' and device_ip = a.device_ip and user_dst=a.user_dst) or (ec_ activity='Lockout' and device_ip = a.device_ip and user_dst=a.user_dst)))] where timer:within(60 seconds) -&gt; (timer:interval(30 seconds) and not Event (device_ip=a.device_ip and user_dst=a.user_dst and ec_activity='Lockout'))];</pre>
<p>Hinweis</p>	<ul style="list-style-type: none"> <li>• Mit der oben genannten Abfrage wird das Fehlen eines Sperrungsereignisses nach 2 fehlgeschlagenen Anmeldungen vom selben Benutzer erkannt.</li> <li>• Der Zeitpunkt des Auftretens der fehlgeschlagenen Anmeldungen wird aufgezeichnet, und es wird davon ausgegangen, dass sie in einem bestimmten Zeitraum auftreten. Außerdem wird in der Praxis davon ausgegangen, dass das Sperrungsereignis kurze Zeit nach der letzten fehlgeschlagenen Anmeldung auftritt, da der Schwellenwert für fehlgeschlagene Anmeldungen pro Benutzer in einer vorgegebenen Domain festgelegt wird.</li> <li>• In der aktuellen Abfrage wird durch every-distinct ein neuer Thread mit einer Kombination aus Benutzer und Gerät für 1 Millisekunde unterdrückt.</li> <li>• Die für 3 fehlgeschlagene Anmeldungen zulässige Zeit nach dem ersten fehlgeschlagenen Versuch beträgt 60 Sekunden. Die Wartezeit für das Auftreten des Sperrungsereignisses beträgt 30 Sekunden.</li> </ul>

**Hinweis:**

1. "." in Metaschlüsseln muss durch ("\_") ersetzt werden.
2. Alle Muster sollten zeitgebunden sein.
3. Verwenden von entsprechenden Tags vor den Aussagen
  - a) @RSAPersist:
  - b) @RSAAlert:

Weitere Informationen finden Sie im:

- EPL-Dokumentation: <http://www.esperitech.com/esper/documentation.php>
- EPL-Onlinetool: <http://esper-epl-tryout.appspot.com/epltryout/mainform.html>

## Arbeiten mit Regeln

In diesem Thema werden zusätzliche Verfahren erläutert, die Sie in Bezug auf Regeln durchführen können. Eventuell möchten Sie eines der folgenden Verfahren durchführen:


- [Bearbeiten, Duplizieren oder Löschen einer Regel](#)
- [Filtern oder Suchen von Regeln](#)
- [Importieren oder Exportieren von Regeln](#)

## Bearbeiten, Duplizieren oder Löschen einer Regel

In diesem Thema erfahren Sie, wie Sie eine Event Stream Analysis-Regel (ESA) bearbeiten, duplizieren oder löschen. Wenn Sie eine Regel bearbeiten, wendet ESA die aktualisierten Kriterien für die zukünftige Verarbeitung an. Es werden keine Änderungen an zuvor erzeugten Warnmeldungen vorgenommen.


### Methoden

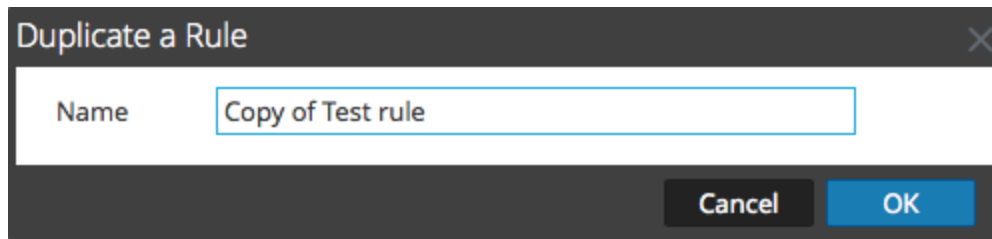
#### Bearbeiten einer Regel

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.  
Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie die zu bearbeitende Regel in der **Regelbibliothek** aus und klicken Sie auf .  
Je nach Regeltyp wird die entsprechende Regelregisterkarte angezeigt.

3. Ändern Sie die erforderlichen Parameter.
4. Klicken Sie auf **Save**.

### Duplizieren von Regeln

1. Wählen Sie die zu duplizierende Regel in der **Regelbibliothek** aus und klicken Sie auf .
2. Das Dialogfeld Regel duplizieren wird angezeigt. Das System fügt vor dem Regelnamen **Kopie von** hinzu.



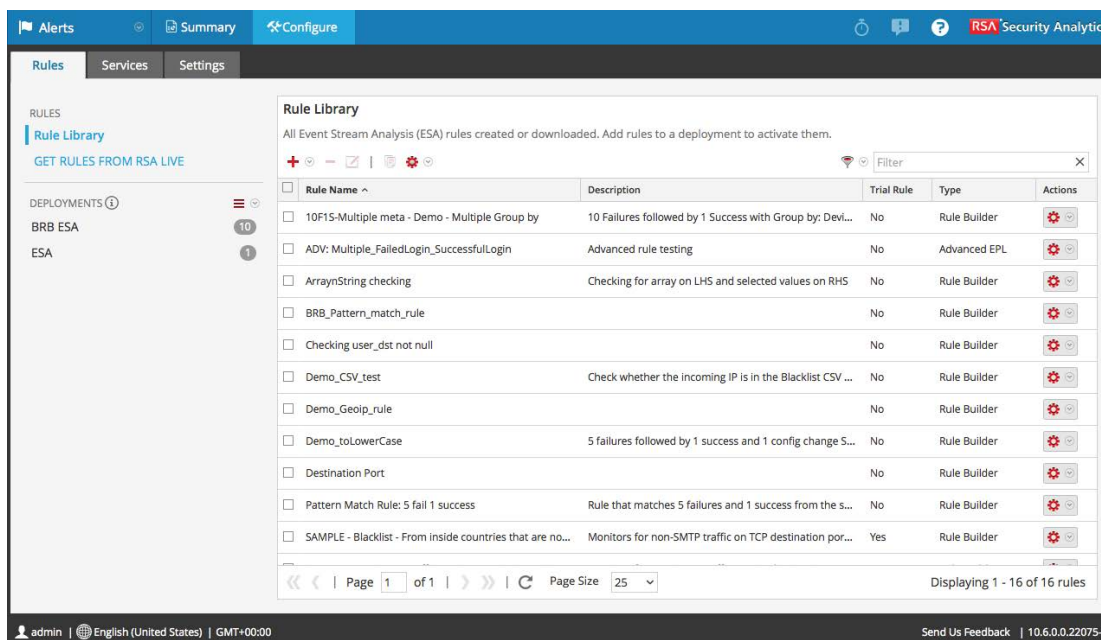
3. Geben Sie im Feld **Name** einen eindeutigen Namen für die duplizierte Regel ein und klicken Sie auf **OK**.


Dem Bereich Regelbibliothek wird eine duplizierte Regel mit dem neuen Namen hinzugefügt.

### Löschen einer Regel

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.

Die Registerkarte Regeln wird angezeigt.



2. Wählen Sie in der Regelbibliothek eine oder mehrere Regeln aus und klicken Sie auf . Ein Warnmeldungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Ja**. Es wird eine Bestätigungsmeldung angezeigt, dass die Regel erfolgreich gelöscht wurde, und die ausgewählte Regel wird aus der Regelbibliothek gelöscht.

## Filtern oder Suchen von Regeln



In diesem Thema erfahren Analysten, wie sie den Typ von Regeln angeben, die in der Regelbibliothek angezeigt werden.

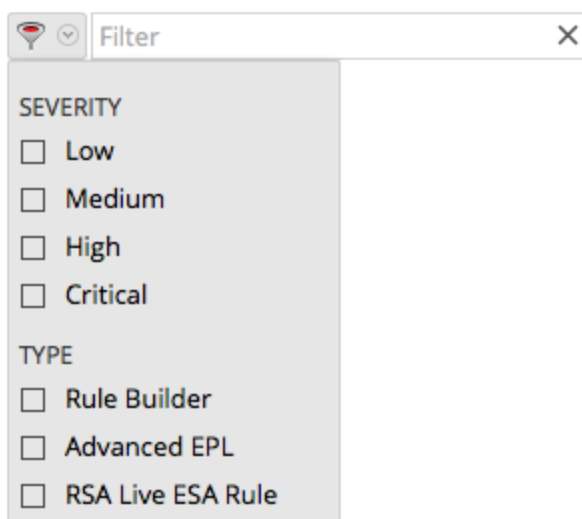
### Voraussetzungen

Stellen Sie sicher, dass Sie mit den Komponenten der Ansicht Regelbibliothek vertraut sind. Weitere Informationen finden Sie unter [Bereich „Regelbibliothek“](#).

### Methoden

#### Filter

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus. Die Registerkarte Regeln wird standardmäßig angezeigt.
2. Klicken Sie in der Symbolleiste des Bereichs **Regelbibliothek** auf   und wählen Sie den Schweregrad und die Regeltypen aus, die in der Liste der Regelbibliothek angezeigt werden sollen. Die folgende Abbildung zeigt die Drop-down-Liste Filter.



Die ausgewählten Regeltypen werden in der Liste angezeigt.

## Suchen

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Registerkarte Regeln wird standardmäßig angezeigt.
2. Geben Sie in der Symbolleiste des Bereichs **Regelbibliothek** im Feld „Filtern“ einen Regelnamen ein.  
Im Bereich Regelbibliothek werden die Regeln aufgelistet, die mit den ins Feld Filter eingegebenen Namen übereinstimmen.

## Importieren oder Exportieren von Regeln

In diesem Thema erfahren Sie, wie Sie ESA-Regeln aus einer Instanz von Security Analytics importieren und wie Sie ESA-Regeln auf Ihre Festplatte exportieren, damit Sie eine lokale Kopie anlegen können.

Wenn Sie eine Regel in einer früheren Version von Security Analytics exportiert haben, gelten beim Import der Regel in Version 10.5 oder später die folgenden Bedingungen:

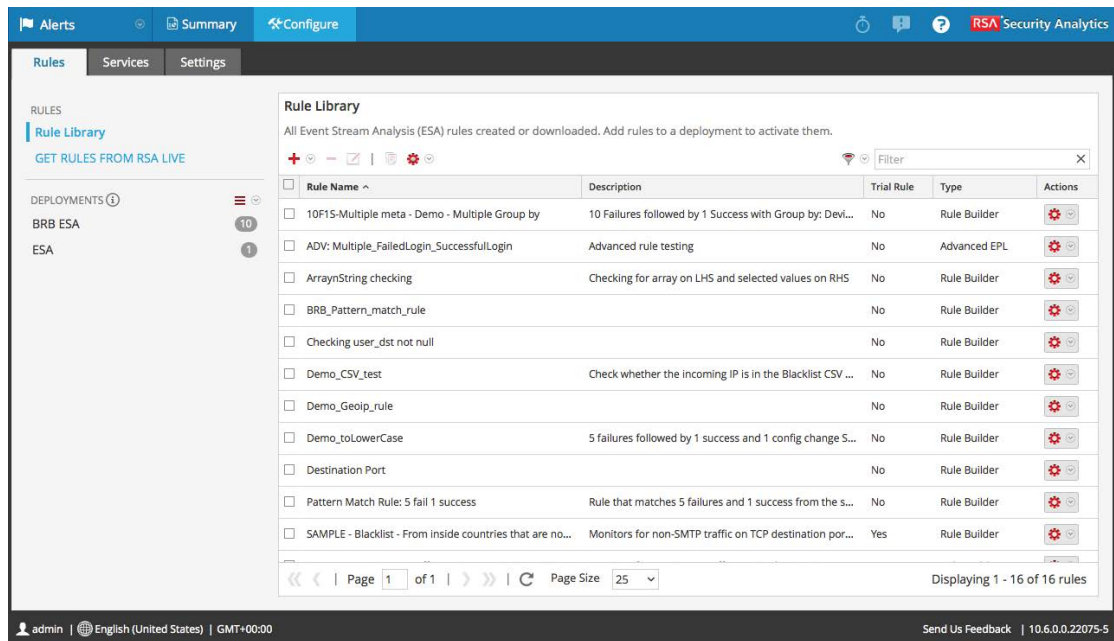
- Exportiert in Version 10.3: Die Regeln können nicht in Version 10.5 importiert werden.
- Exportiert in Version 10.4: Das Regelverhalten hängt davon ab, ob die übergreifende Korrelation deaktiviert (Standardeinstellung) oder aktiviert ist:
  - Deaktiviert: Sie können Regeln in Version 10.5 importieren.
  - Aktiviert: Sie müssen entweder Security Analytics neu starten oder eine kleinere Änderung an der Regel vornehmen, sie speichern, die Änderung wieder entfernen und sie erneut speichern. Mit beiden Verfahren wird die Weiterleitungsregel erstellt, die von der siteübergreifenden Korrelationsfunktion in 10.5 benötigt wird.

## Methoden

### Importieren von ESA-Regeln

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.  
Die Registerkarte Regeln wird angezeigt.






2. Klicken Sie in der Symbolleiste **Regelbibliothek** auf  > **Importieren**.  
Das Dialogfeld ESA-Regeln importieren wird angezeigt.



3. Klicken Sie auf **Durchsuchen**, um die Datei zu suchen und auszuwählen, die die ESA-Regeln enthält.
4. Klicken Sie auf Importieren.

## Export

1. Wählen Sie eine oder mehrere ESA-Regeln aus und klicken Sie in der Symbolleiste „Regelbibliothek“ auf  > **Exportieren**.  
Ein Warnmeldungsdialogfeld wird angezeigt.
2. Klicken Sie auf **Ja**.  
Das Dialogfeld Regeln exportieren wird angezeigt.

3. Geben Sie im Feld **Dateiname**: einen Dateinamen für die Datei mit den ESA-Regeln ein und klicken Sie auf **Exportieren**.

Die Datei wird als Binärdatei auf Ihren Rechner exportiert.

**Hinweis:** Die Binärdatei kann nicht bearbeitet werden.

## Auswählen von Benachrichtigungsmethoden über Warnmeldungen

---

In diesem Thema werden die verschiedenen Benachrichtigungsmethoden beschrieben und wie Sie eine Benachrichtigungsmethode zu einer Regel hinzufügen. Für alle Aufgaben in diesem Abschnitt sind die Berechtigungen der Rollen Administrator, SOC Manager oder DPO erforderlich.

Wenn eine Regel eine Warnmeldung auslöst, kann ESA eine Benachrichtigung auf die folgenden Weisen senden:

- E-Mail
- SNMP
- Syslog
- Skript

Zur Konfiguration einer Benachrichtigung müssen Sie die folgenden Komponenten konfigurieren:

- Benachrichtigungsserver – Nachdem Sie einen Benachrichtigungsserver konfiguriert haben, können Sie ihn einer Regel hinzufügen. Wenn die Regel eine Warnmeldung auslöst, wird die Regel diesen Server verwenden, um Warnmeldungsbenachrichtigungen zu senden.
- Benachrichtigungen – Diese sind die Ausgaben, sie können in den Formaten E-Mail, Skript, SNMP und Syslog erfolgen. Wenn Sie eine Regel konzipieren, können Sie die Benachrichtigung für eine Warnmeldung angeben.
- Vorlagen – Das Format einer Warnmeldungsbenachrichtigung wird in einer Vorlage definiert.

Die Unterdrückung von Warnmeldungen und die Regulierung der Warnmeldungsrate sind zwei Funktionen von Event Stream Analysis. Die Unterdrückung von Warnmeldungen sorgt dafür, dass nicht mehrere E-Mail-Nachrichten zu derselben Warnmeldung gesendet werden. Betrachten Sie zum Beispiel eine Regel, um fehlgeschlagene Benutzeranmeldungen zu erkennen. Wenn Sie die Unterdrückung von Warnmeldungen auf drei Minuten festlegen, werden nur die für diesen Zeitrahmen erzeugten Warnmeldungen angezeigt. Das ist weniger als die Anzahl der Warnmeldungen, die Sie ohne Unterdrückung von Warnmeldungen sehen würden. Einige Warnmeldungen können Duplikate sein. Mit der Unterdrückung von Warnmeldungen werden keine E-Mails für Duplikat-Warnmeldungen gesendet. So sorgen Sie dafür, dass Ihr Posteingang nicht mit redundanten Warnmeldungsbenachrichtigungen überflutet wird.

Die Regulierung der Warnmeldungsrate ist eine vorbeugende Maßnahme, die dafür sorgt, dass Warnmeldungen von fehlgedeuteten Regeln nicht das System überschwemmen. Diese Funktion sorgt dafür, dass ESA nicht mehr als die konfigurierte maximale Anzahl von E-Mail-Nachrichten innerhalb einer Minute sendet.

Benachrichtigungsserver, Benachrichtigungen und Vorlagen werden in der Ansicht Administration > System konfiguriert. Weitere Informationen finden Sie unter „Konfigurieren von Benachrichtigungsservern“, „Konfigurieren von Benachrichtigungstypen“ und „Konfigurieren von Vorlagen für Benachrichtigungen“ im **Systemkonfigurationsleitfaden**.

## Benachrichtigungsmethoden

Wenn eine Regel eine Warnmeldung auslöst, kann ESA eine Benachrichtigung auf die folgenden Weisen senden:

- E-Mail
- SNMP
- Syslog
- Skript

### E-Mail-Benachrichtigungen

Event Stream Analysis kann Benachrichtigungen über verschiedene Systemereignisse per E-Mail an Benutzer senden.

Um diese E-Mail-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie den SMTP-E-Mail-Server als einen Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der E-Mail-Einstellungen als Benachrichtigungsserver“ im **Systemkonfigurationsleitfaden**.
- Richten Sie ein E-Mail-Konto für den Erhalt von Benachrichtigungen ein. Weitere Anweisungen finden Sie unter „Konfigurieren von E-Mail als Benachrichtigung“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie eine Vorlage für die E-Mail-Benachrichtigung. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im **Systemkonfigurationsleitfaden**.

## SNMP

Event Stream Analysis kann Ereignisse als eine SNMP-Trap an einen konfigurierten SNMP-Trap-Host senden.

Um diese SNMP-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie die Einstellungen des SNMP-Trap-Host als Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der SNMP-Einstellungen als Benachrichtigungsserver“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie die Einstellungen der SNMP-Trap als Ausgabeaktion. Weitere Anweisungen finden Sie unter „Konfigurieren von SNMP als eine Benachrichtigung“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie eine Vorlage für SNMP. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im **Systemkonfigurationsleitfaden**.

## Syslog

Event Stream Analysis kann Ereignisse versenden und Protokolle im Syslog-Format auf einem Syslog-Server konsolidieren.

Um diese Syslog-Benachrichtigungen zu konfigurieren, müssen Sie Folgendes tun:

- Konfigurieren Sie die Syslog-Servereinstellungen als Ausgabeprovider. Weitere Anweisungen finden Sie unter „Konfigurieren der Syslog-Einstellungen als Benachrichtigungsserver“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie das Syslog-Nachrichtenformat als eine Ausgabeaktion. Weitere Anweisungen finden Sie unter „Konfigurieren von Syslog als Benachrichtigung“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie eine Vorlage für Syslog. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im **Systemkonfigurationsleitfaden**.

## Script Alerter

Neben den Warnmeldungen ermöglicht ESA den Benutzern auch, als Reaktion auf ESA-Warnmeldungen Skripte auszuführen.

Mithilfe von Skripten können Sie eine benutzerdefinierte Integration mit Anwendungen erreichen, die in Ihrer Umgebung existieren. Beispiel: Wenn Sie ein Incident-Ticket von einer Anwendung öffnen möchten, wenn eine bestimmte Warnmeldung ausgelöst wird, können Sie mit Script Alerter ein Skript erstellen, das die Anwendungs-API aufruft. ESA kann es dann einleiten, wenn die definierte ESA-Regel ausgelöst wird. Sie können eine FreeMarker-Vorlage konfigurieren, um die von der Ausgabe der ESA-Regel zu extrahierenden Details zu definieren und als Befehlszeilenargumente an das Skript weiterzugeben.

Gehen Sie wie folgt vor, um Script Alert zu verwenden:

- Konfigurieren Sie die Benutzeridentität und weitere Details, die für die Ausführung des Skripts notwendig sind. Weitere Anweisungen finden Sie unter „Konfigurieren eines Skripts als Benachrichtigungsserver“ im **Systemkonfigurationsleitfaden**.
- Definieren Sie das Skript. Weitere Anweisungen finden Sie unter „Konfigurieren eines Skripts als eine Benachrichtigung“ im **Systemkonfigurationsleitfaden**.
- Konfigurieren Sie eine Vorlage für das Skript. Weitere Anweisungen finden Sie unter „Konfigurieren einer Vorlage“ im **Systemkonfigurationsleitfaden**.

## Hinzufügen einer Benachrichtigungsmethode zu einer Regel

Dieses Thema erklärt Administratoren, wie sie eine Benachrichtigung, etwa als E-Mail, zu einer Regel hinzufügen können. ESA verwendet die Benachrichtigungsmethode, wenn es eine Warnmeldung für ein Ereignis erzeugt, das die Regelkriterien erfüllt.

Fügen Sie eine Benachrichtigung zu einer Regel hinzu, kann ESA Sie informieren, wenn eine Regel eine Warnmeldung auslöst. Obwohl die Benachrichtigungsfelder nicht erforderlich sind, ist es eine bewährte Vorgehensweise, eine Benachrichtigung zu einer Regel hinzuzufügen.

Wenn Sie eine Benachrichtigungsmethode zu einer Regel hinzufügen, wählen Sie die folgenden Informationen aus:

- Ausgabe
- Benachrichtigung
- Benachrichtigungsserver
- Vorlage




## Voraussetzungen

- Ihre Rolle muss die Berechtigung zum Managen von Regeln haben.
- Die Regel muss vorhanden sein.
- Die Benachrichtigungsmethode muss mit einem unterstützten Server und einer Vorlagekonfiguriert sein:
  - Klicken Sie auf **Administration > System > Globale Benachrichtigungen**.
  - Detaillierte Informationen über die Verfahren finden Sie im **Systemkonfigurationsleitfaden**.

## Verfahren

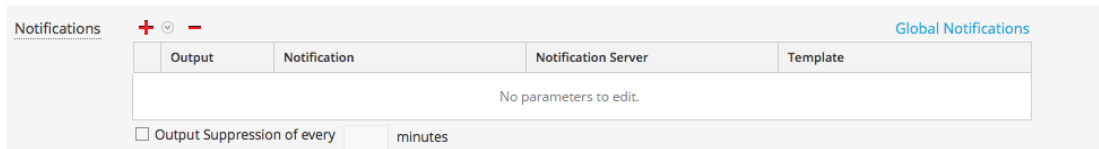
So fügen Sie einer Regel eine Benachrichtigungsmethode hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.

2. Klicken Sie in der **Regelbibliothek** auf  , um eine neue Regel hinzuzufügen, oder wählen Sie eine vorhandene Regel aus und klicken Sie auf .

Je nach Regeltyp wird entweder die Registerkarte **Regelerstellung** oder **Erweiterte EPL** angezeigt.

Der Abschnitt **Benachrichtigungen** ist für beide Registerkarten gleich.



3. Klicken Sie auf   und wählen Sie die **Ausgabe** für die Warnmeldung aus:

- E-Mail
- SNMP
- Syslog
- Skript

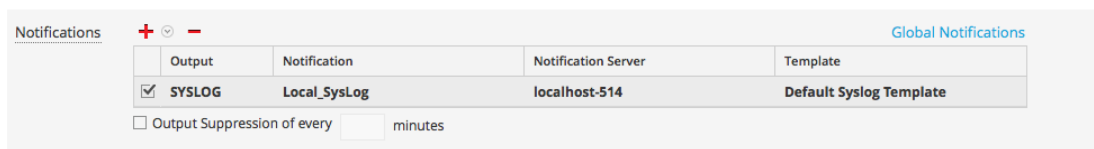
4. Doppelklicken Sie auf das Feld **Benachrichtigung** und wählen Sie den Namen einer vorher konfigurierten Ausgabe.

Zum Beispiel könnte „Level 1 Analyst“ der Name einer E-Mail-Benachrichtigung sein, die an die Verteilergruppe „L1-Analysten“ gesendet wird.

5. Doppelklicken Sie auf das Feld **Benachrichtigungsserver** und wählen Sie den Server aus, der die Benachrichtigung versendet.

6. Doppelklicken Sie auf das Feld **Vorlage** und wählen Sie ein Format für die Warnmeldung aus.

Die folgende Abbildung zeigt die Einstellungen für eine Syslog-Benachrichtigung:



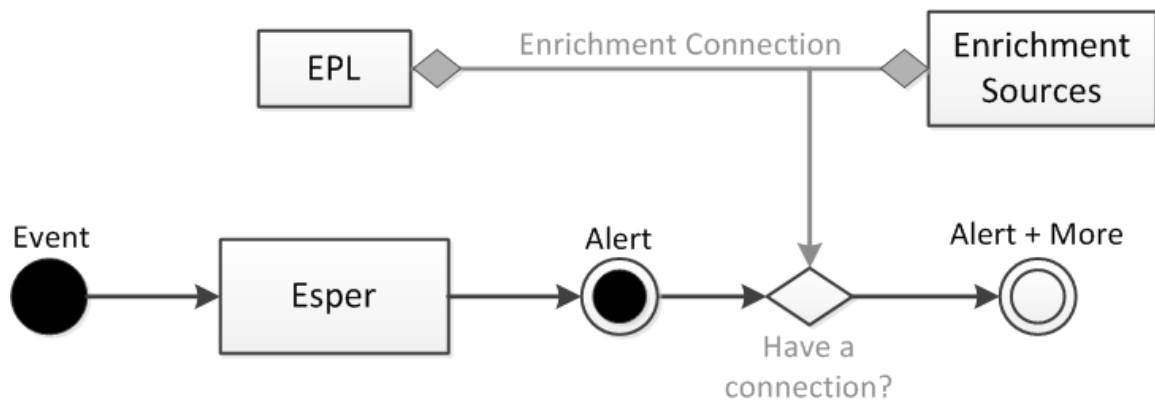
7. Wenn Sie die Frequenz angeben möchten, wählen Sie **Ausgabeunterdrückung** aus und geben Sie dann die Anzahl **Minuten** ein.
8. Wenn Sie eine weitere Benachrichtigung hinzufügen möchten, wiederholen Sie die Schritte 3 bis 7.
9. Klicken Sie auf **Save**.  
Wenn ESA eine Warnmeldung für ein Ereignis erzeugt, das die Regelkriterien erfüllt, werden Sie über die Warnmeldung über jede Benachrichtigungsmethode informiert, die zu der Regel hinzugefügt wurde.



## Hinzufügen einer Datenerweiterungsquelle

In diesem Thema wird erläutert, wie eine zuvor konfigurierte Erweiterungsquelle zu einer Regel hinzugefügt wird. Wenn ESA eine Warnmeldung erstellt, werden die Informationen aus dieser Quelle einbezogen.

Mit Erweiterungen können Kontextinformationen in Korrelationslogiken und Warnmeldungsausgaben integriert werden. Ohne Erweiterungen stammen alle in einer ESA-Warnmeldung enthaltenen Informationen aus einem Security Analytics-Core-Service. Mit Erweiterungen können Sie Suchvorgänge in einer Vielzahl von Quellen anfordern und die Ergebnisse in die ausgehenden Warnmeldungen integrieren. In der folgenden Abbildung ist die Erweiterungsfunktion dargestellt.



Eine Erweiterungskonfiguration besteht aus zwei logischen Einheiten:

- Erweiterungsquellen: Diese Quellen sind Datenspeicher für Kontextinformationen.
- Erweiterungsverbindungen: Diese agieren als Verbindungselemente zwischen den Warnmeldungsmetadaten und den Quellspalten.

In ESA können Sie Verbindungen zwischen EPL-Anweisungen (Event Processing Language, Ereignisverarbeitungssprache) und Erweiterungsquellen herstellen. Sobald die Verbindungen hergestellt wurden, verbindet das System die ausgewählten Felder aus der Warnmeldungsausgabe mit den Informationen der Quellen und füllt die gesendete Warnmeldung mit den übereinstimmenden Daten. ESA kann Verbindungen mit folgenden Quellen herstellen:

- Esper-Named-Windows
- Relationale Datenbanktabellen
- MaxMindGeoIP-Datenbank
- RSA Warehouse Analytics-Watchlisten

**Hinweis:** Die Erweiterungsquelle GeoIP kann weder erstellt noch gelöscht werden. Sie wird dem Benutzer vorkonfiguriert bereitgestellt.

## Beispielregel mit Erweiterung

In der folgenden Beispielregel wird die von ESA bereitgestellte Erweiterungsfunktion illustriert:

```
@RSAAlert @Name("simple") SELECT * FROM CoreEvent(ec_theme='Login Failure')
```

Die Regel erzeugt eine Warnmeldung für jede fehlgeschlagene Anmeldung und meldet somit, ob der folgende (vereinfachte) Ereignisstream von ESA empfangen wird:

sessionid	ec_theme	username	ip_src	ip_dst	host_dst
1	Login Success	dshrute	23.xx.23x.16		
2	Login Failure	jhalpert	23.xx.23x.16	31.1x.x9.1x8	www.facebook.com

Eine Warnmeldung mit dem folgenden Bestandteil `events` wird möglicherweise als Reaktion auf die zweite Sitzung erzeugt:

```
{
  "events": [
    {
      "username": "jhalpert",
      "host_dst": "www.facebook.com",
      "ip_dst": "31.1x.x9.1x8",
      "sessionid": 2,
      "ec_theme": "Login Failure",
      "esa_time": 1406148964130,
      "ip_src": "23.xx.23x.16"
    }
  ]
}
```

Die JSON-Ausgabe zeigt alle verfügbaren Informationen für die Integration in eine ESA-Benachrichtigung mit einer entsprechenden

FreeMarker-Vorlage an. Der Vorlagenausdruck `${events[0].username}` wird beispielsweise mit `jhalpert` erfüllt.

Mit Erweiterungen kann dasselbe Modul mit demselben Ereignisstream die unten stehende Warnmeldung erzeugen. Das System kann mehrere Erweiterungsverbindungen herstellen und Kontextdaten abrufen, damit die Warnmeldung aussagekräftiger wird.

Beispiel:

`${events[0]["RSADataScienceLookup"][0].score}` ergibt eine **Risikobewertung** der Zieldomain, die vom RSA Warehouse Analytics-Modul berechnet wird. `${events[0]["orgchart"][0].supervisor}` ergibt den Namen des Supervisors des Mitarbeiters, auf den sich die Warnmeldung bezieht (aus einer HR-Datenbank abgerufen). `${events[0]["LoginRegister"][0].username}` ergibt den Namen des Benutzers, der sich zuletzt erfolgreich mit derselben `ip_src` (mit einem auf dem benannten Fenster basierenden Stream) angemeldet hat.

```
{
  "events": [
    {
      "username": "jhalpert",
      "host_dst": "www.facebook.com",
      "GeoIpLookup": [
        {
          "city": "Cambridge",
          "longitude": -71,
          "countryCode": "US",
          "areaCode": 617,
          "metroCode": 506,
          "region": "MA",
          "dmaCode": 506,
          "ipv4Obj": "/23.62.236.16",
          "countryName": "United States",
          "postalCode": "02142",
          "ipv4": "23.62.236.16",
          "latitude": 42,
          "organization": "Verizon Business"
        }
      ],
      "RSADataScienceLookup": [
        {
          "model_id": "suspiciousDomains_1",
          "_id": "EXEC_BATCH_1_20140630153740_facebook.com",
          "score": 10,
          "key": "www.facebook.com"
        }
      ],
      "orgchart": [
        {
          "supervisor": "mscott",
          "name": "James Halpert",
          "extension": 3692,
          "location": "Scranton",

```

```
        "department": "Sales",
        "id": "jhalpert"
    }
],
"ip_dst": "31.13.69.128",
"sessionid": 2,
"LoginRegister": [
    {
        "username": "dshrute",
        "ip_src": "23.62.236.16"
    }
],
"ec_theme": "Login Failure",
"esa_time": 1406155218912,
"ip_src": "23.62.236.16"
}
]}
```

## Konfigurieren einer Datenbankverbindung

In diesem Thema wird erläutert, wie eine Verbindung zu einer externen Datenbank konfiguriert wird, in der zusätzliche Informationen für Warnmeldungen bereitgestellt werden können. Sie konfigurieren eine Datenbankverbindung, sodass Sie anschließend die Datenbank als Erweiterungsquelle konfigurieren können, um Warnmeldungen weitere Details hinzuzufügen. Dieser Prozess besteht aus drei Schritten:

1. Konfigurieren Sie eine Verbindung zu einer Datenbank.
2. Konfigurieren Sie die externe Datenbank als Erweiterungsquelle.
3. Fügen Sie die Erweiterungsquelle zu einer Regel hinzu

In diesem Thema wird Schritt 1 erläutert.

### Beispiel

Dieses Beispiel veranschaulicht, wie durch Hinzufügen einer Datenbank als Erweiterungsquelle ein Wert zu Warnmeldungen hinzugefügt wird.

Eine Regel erkennt Benutzer, die versuchen, sich bei einem im Hintergrund aktiven E-Mail-Service anzumelden. Die Regelkriterien treffen auf 25 Benutzer zu. Ohne die Erweiterung enthält die Warnmeldung 25 Benutzer-IDs. Mit der Erweiterung enthält die Warnmeldung auch die folgenden Informationen zu den einzelnen Benutzer-IDs:

- Name
- Title

- Abteilung
- Niederlassung

### Abhängigkeiten

Wenn Sie eine Datenbank konfigurieren, gelten folgende Bedingungen:

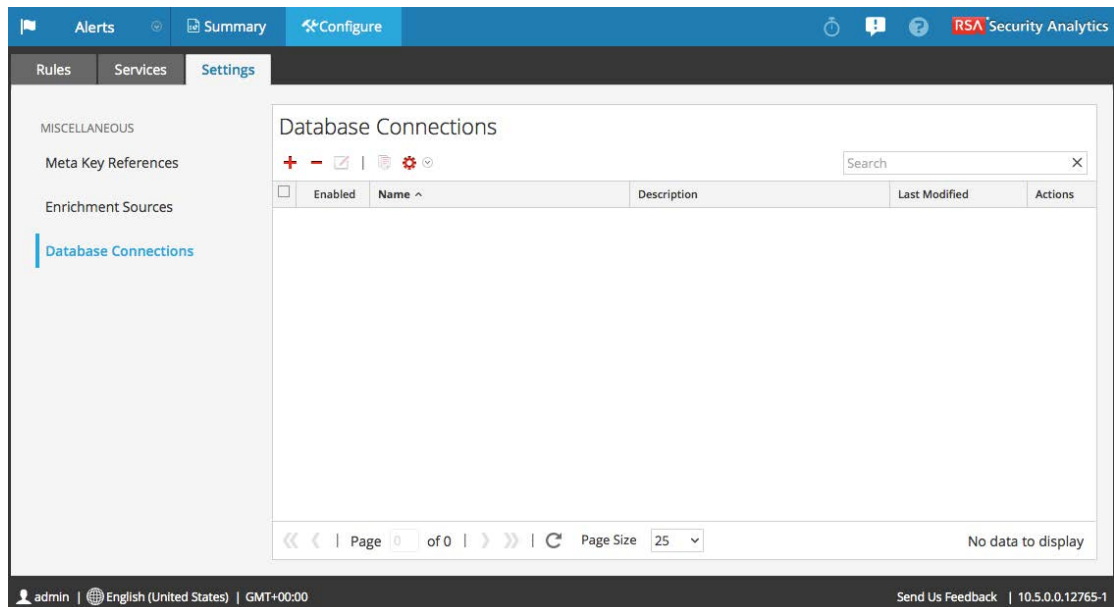
- Auf jedem ESA wird ein Verweis zu der Datenbank bereitgestellt, selbst wenn der ESA keine Regeln bereitstellt, die die Datenbank als Erweiterungsquelle verwenden.
- Wenn der Server, auf dem die Datenbank gehostet wird, ausfällt, hat dies Auswirkungen auf eine Bereitstellung.
  - Eine aktive Bereitstellung erfasst weiterhin Daten und führt Regeln aus, aber in den Warnmeldungen werden keine Erweiterungen angezeigt.
  - Eine neue Bereitstellung schlägt solange fehl, bis Sie den Host neu starten.

### Verfahren

So konfigurieren Sie eine Datenbankverbindung:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Datenbankverbindungen** aus.

Der Bereich Datenbankverbindungen wird angezeigt.



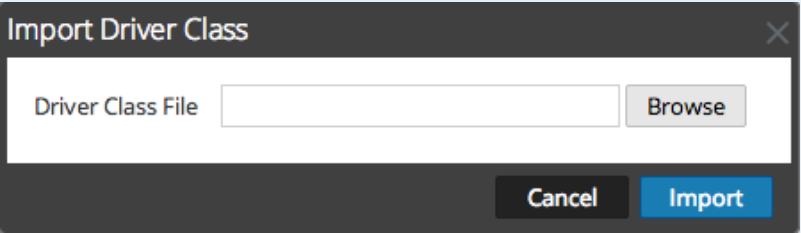
4. Klicken Sie auf **+**, um eine Datenbankverbindung hinzuzufügen.

The screenshot shows a 'Database Connection' dialog box with the following fields and controls:

- Enable:** A checkbox that is checked.
- Connection Name \*:** A text input field.
- Description:** A text input field.
- Driver Class \*:** A dropdown menu with an 'Upload' button to its right.
- Database URL/IP \*:** A text input field.
- Username \*:** A text input field.
- Password \*:** A text input field with asterisks for masking.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

5. Geben Sie im Dialogfeld **Datenbankverbindung** die folgenden Informationen an.

Feld	Beschreibung
Aktivieren	Wählen Sie Aktivieren aus, um die Warnmeldung um zusätzliche Daten zu erweitern. Standardmäßig ist „Aktiviert“ ausgewählt. Deaktivieren Sie „Aktiviert“, um zusätzliche Daten aus der Warnmeldung auszuschließen.
Verbindungsname	Geben Sie einen Namen ein, um die Verbindung zu identifizieren. Wenn Sie eine Datenbank als Erweiterungsquelle hinzufügen, wird dieser Name in der Liste der Datenbankverbindungen angezeigt.
Beschreibung	(Optional) Geben Sie eine kurze Beschreibung der Datenbankverbindung ein.

Feld	Beschreibung
Treiberklasse	<p>Wählen Sie eine geeignete Treiberklasse für die Datenbank aus. In Security Analytics sind zwei Treiber enthalten: MongoDB und Postgres.</p> <p>Wenn Sie einen neuen Treiber importieren möchten, klicken Sie auf <b>Hochladen</b>.</p>  <p>Klicken Sie im Dialogfeld <b>Treiberklasse importieren</b> auf <b>Durchsuchen</b>, wählen Sie einen neuen Treiber aus und klicken Sie auf <b>Importieren</b>.</p>
Datenbank-URL oder IP-Adresse	Geben Sie die URL oder die IP-Adresse der zu konfigurierenden Datenbank ein.
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf die Datenbank ein.
Password	Geben Sie das Passwort für den Zugriff auf die Datenbank ein.

6. Klicken Sie auf **Save**.

Weitere Informationen erhalten Sie unter [Registerkarte „Einstellungen“](#)

## Erweiterungsquellen

In diesem Thema werden Optionen zum Hinzufügen einer externen Datenquelle für zusätzliche Informationen in Warnmeldungen erklärt. Enrichment-Quellen bieten zusätzliche Information in Warnmeldungen. Beispiel: Eine Datenbank kann Informationen zu Name, Abteilung und Bürostandort bereitstellen, wenn ein Benutzer Regelbedingungen erfüllt. Es gibt drei Typen von Enrichment-Quellen:

- Externer DB-Verweis
- In-Memory-Tabelle
- Warehouse Analytics

## Konfigurieren einer Datenbank als Erweiterungsquelle

Sie können eine Datenbank als Erweiterungsquelle konfigurieren, damit Sie sie einer Regel hinzufügen können. Die Esper-Engine, die die Ereignisse analysiert, kann auf die Informationen in der Datenbank zugreifen und in der Warnmeldung zusätzliche Angaben bereitstellen.

Beispiel: Eine Regel erkennt, dass Benutzer versuchen, sich bei einem Tarnkappen-E-Mail-Service anzumelden. Die Regelkriterien treffen auf 25 Benutzer zu. Die Warnmeldung enthält 25 Benutzer-IDs. In diesem Beispiel erweitert eine externe Datenbank die Warnmeldung um die folgenden zusätzlichen Informationen für jede Benutzer-ID:

- Name
- Title
- Abteilung
- Niederlassung
- Vorgesetzte

Sie können eine Datenbankverbindung bearbeiten, duplizieren, importieren oder exportieren.

### Voraussetzungen

Sie müssen eine Datenbankverbindung konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren einer Datenbankverbindung](#).

### Verfahren

So konfigurieren Sie eine Datenbank als Erweiterungsquelle

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Klicken Sie auf die Registerkarte **Einstellungen**.  
Die Registerkarte Einstellungen wird angezeigt.



- Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.  
Der Bereich Erweiterungsquellen wird angezeigt.

Enrichment Sources

Enabled	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	Default GeolIP	GeolIP	Default Geo IP Enrichment Source. This cannot be edited.	2014-08-22 16:13:49	
<input type="checkbox"/>	MySql1	External DB Re...	table - satest1	2014-08-22 16:13:49	
<input type="checkbox"/>	Table1	In-Memory Table	ip_src, hostname and user	2014-08-25 15:06:03	
<input type="checkbox"/>	Table2	In-Memory Table	ip_src, hostname, user, place and id	2014-08-25 15:06:42	
<input type="checkbox"/>	WarehouseAnalytics	Warehouse An...		2014-08-22 16:13:49	

Page 1 of 1 | Page Size 25 | Displaying 1 - 5 of 5

- Wählen Sie aus dem -Drop-down-Menü **Externer DB-Verweis** aus. Sie müssen einen Datenbankverweis hinzufügen, damit die Datenbank aufgelistet werden kann.  
Das Dialogfeld Externer DB-Verweis wird angezeigt.

External DB Reference

Enable

User-Defined Table Name \*

Description

Database Connection \*

Table Name \*

Cancel Save

- Wählen Sie **Aktivieren** aus, um die Warnmeldung um zusätzliche Daten zu erweitern.  
Diese Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, wird die Warnmeldung nicht um zusätzliche Daten erweitert.
- Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen ein, um die Datenbankkonfiguration zu identifizieren oder zu bezeichnen.

7. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der Datenbankkonfiguration ein.
8. Wählen Sie im Drop-down-Menü **Datenbankverbindung** die definierten Datenbankverbindungen aus.
9. Geben Sie in das Feld **Name der Tabelle** den Tabellennamen der Datenbank ein.
10. Klicken Sie auf **Save**.

Weitere Informationen über Parameter und ihre Beschreibung erhalten Sie unter [Registerkarte „Einstellungen“](#).

## Konfigurieren einer In-Memory-Tabelle als Erweiterungsquelle

Dieses Thema bietet Anweisungen zum Konfigurieren einer In-Memory-Tabelle. Wenn Sie eine In-Memory-Tabelle konfigurieren, laden Sie eine CSV-Datei als Eingabe in die Tabelle hoch. Sie können diese Tabelle einer Regel als Erweiterungsquelle zuordnen. Wenn die zugeordnete Regel eine Warnmeldung erzeugt, erweitert ESA die Warnmeldung um relevante Informationen aus der In-Memory-Tabelle.

Beispiel: Eine Regel könnte dazu konfiguriert sein, zu erkennen, wenn ein Benutzer versucht, Freeware herunterzuladen, und die Person anhand der Benutzer-ID in der Warnmeldung zu identifizieren. Die Warnmeldung könnte um zusätzliche Informationen aus einer In-Memory-Tabelle erweitert werden, die Details wie vollständigen Namen, Titel, Bürostandort und Mitarbeiternummer enthält.

Eine In-Memory-Tabelle eignet sich hervorragend für den Umgang mit kleinen Datenmengen. Sie lässt sich leicht einrichten und erfordert weniger Wartungsaufwand als eine Datenbank. Beispiel: Die Firma AllTech ist ein kleines Unternehmen, daher kann der Systemadministrator die Mitarbeiterinformationen in einer .CSV-Datei verwalten. Würde sich AllTech zu einem großen Unternehmen entwickeln, müsste der Administrator eine externe Datenbankreferenz zur Erweiterung konfigurieren und die Datenbank mit einer Regel verknüpfen.

### Voraussetzungen

Der Spaltenname in der CSV-Datei darf keine Leerzeichen enthalten.

Die erste Zeile der CSV-Datei muss für jede Spalte wie folgt formatiert sein:

```
name_of_column_1 type_of_column_1
```

Hier sehen Sie ein Beispiel für drei korrekt formatierte Zeilen:

```
Last_Name string
```

```
First_Name string
```

```
Phone integer
```

## Methoden

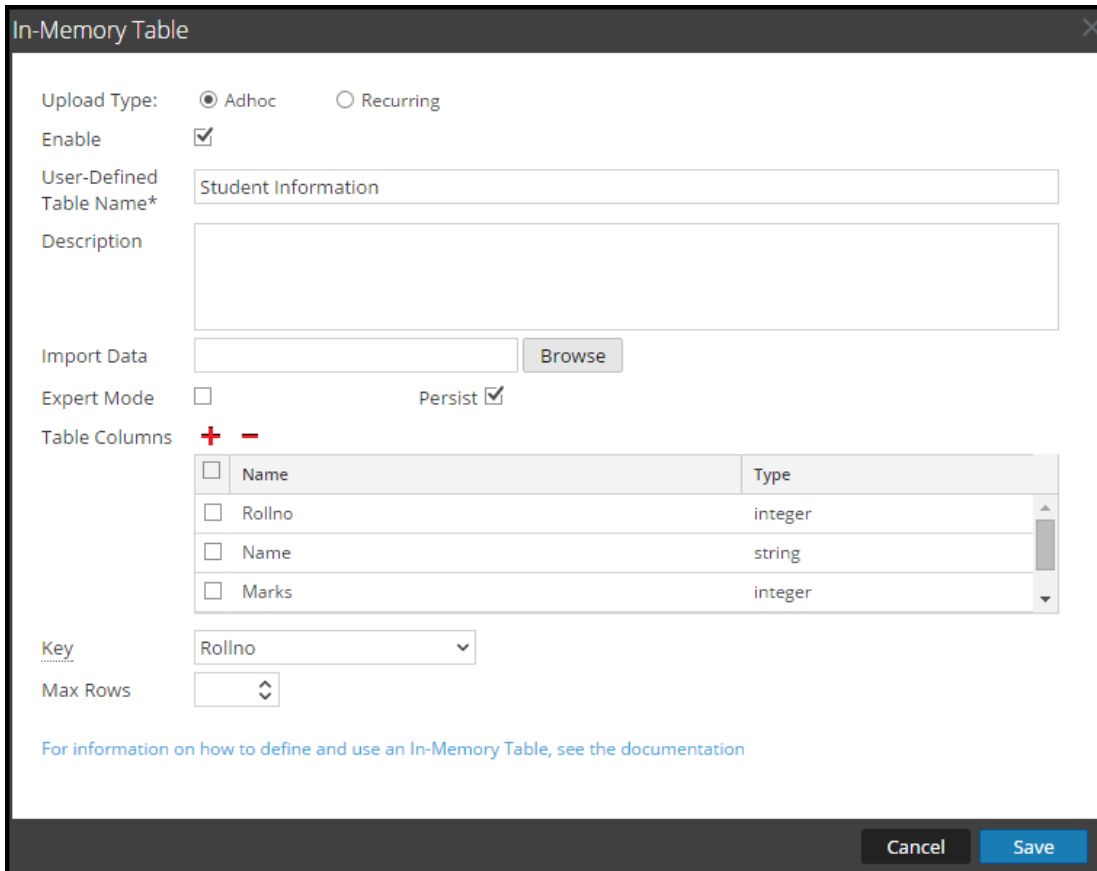
### Konfigurieren einer Ad-hoc-In-Memory-Tabelle

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.

Enrichment Sources						
Enabled	Name ^	Type	Description	Last Modified	Actions	
<input type="checkbox"/>	Default GeoIP	GeoIP	Default Geo IP Enrichment Source. This cannot be edited.	2015-05-13 10:11:34		
<input type="checkbox"/>	HrOrgChart	External DB Reference	Engineering organization in NE region	2015-05-13 10:11:34		
<input type="checkbox"/>	hrcsv	In-Memory Table	Employee information as of end of Q2	2015-05-13 10:13:58		

Page 1 of 1 | Page Size 25 | Displaying 1 - 3 of 3

4. Klicken Sie im Abschnitt **Erweiterungsquellen** auf   > **In-Memory-Tabelle**.



**In-Memory Table**

Upload Type:  Adhoc  Recurring



Enable

User-Defined Table Name\*

Description

Import Data

Expert Mode  Persist

Table Columns  

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Rollno	integer
<input type="checkbox"/>	Name	string
<input type="checkbox"/>	Marks	integer

Key

Max Rows

[For information on how to define and use an In-Memory Table, see the documentation](#)

5. Beschreiben Sie die In-Memory-Tabelle:
- Wählen Sie **Ad-hoc** aus.
  - Standardmäßig ist **Aktiviert** ausgewählt. Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, werden Warnmeldungen mit den Daten aus der Tabelle erweitert.  
Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, die Warnmeldungen aber nicht erweitert werden sollen, deaktivieren Sie das Kontrollkästchen.
  - Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen für die Konfiguration der In-Memory-Tabelle ein, zum Beispiel „Studenteninformationen“.
  - Wenn Sie erläutern möchten, welche Informationen die Erweiterung zu einer Warnmeldung hinzufügt, geben Sie eine **Beschreibung** ein, wie z. B.:  
Wenn eine Warnmeldung nach „Rollno“ gruppiert ist, fügt diese Erweiterung Studenteninformationen hinzu, z. B. Name und Markierungen.
6. Wählen Sie im Feld **Daten importieren** die CSV-Datei aus, aus der Daten in die In-Memory-Tabelle übertragen werden.

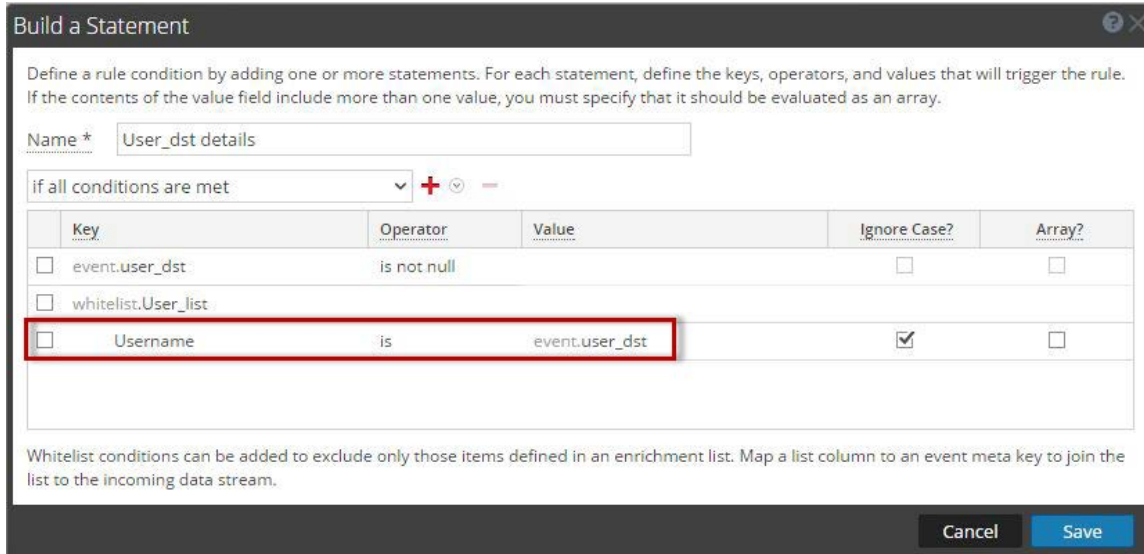
7. Wenn Sie eine EPL-Abfrage schreiben möchten, um eine erweiterte Konfiguration für eine In-Memory-Tabelle zu definieren, wählen Sie Expertenmodus aus.  
Der Abschnitt „Tabellenspalten“ wird durch ein Feld **Abfrage** ersetzt.
8. Wählen Sie „Fortbestehen“ aus, um die In-Memory-Tabelle auf dem Datenträger beizubehalten, wenn der ESA-Service angehalten wird, und um die Tabelle wieder aufzufüllen, wenn der Service wieder gestartet wird.
9. Klicken Sie im Abschnitt **Tabellenspalten** auf **+**, um Spalten zur In-Memory-Tabelle hinzuzufügen.
10. Wenn Sie im Feld „Daten importieren“ eine gültige Datei ausgewählt haben, werden die Spalten automatisch ausgefüllt.

**Hinweis:** Wenn Sie den Expertenmodus ausgewählt haben, wird anstelle des Abschnitts Tabellenspalten das Feld Abfrage angezeigt.

11. Wählen Sie bei Verwendung einer CSV-basierten In-Memory-Tabelle als Erweiterung im Drop-down-Menü **Schlüssel** das Feld aus, das als Standardschlüssel verwendet werden soll, um eingehende Ereignisse mit der In-Memory-Tabelle zu verbinden. Standardmäßig ist die erste Spalte ausgewählt. Sie können den Schlüssel auch später ändern, wenn Sie die In-Memory-Tabelle in Erweiterungsquellen öffnen.
12. Wählen Sie im Drop-down-Menü **Max. Zeilen** die maximale Anzahl der Zeilen aus, die eine bestimmte Instanz der In-Memory-Tabelle enthalten kann.
13. Klicken Sie auf **Save**.  
Die Ad-hoc-In-Memory-Tabelle ist konfiguriert. Sie können sie der Regel als Erweiterung oder als Teil der Regelbedingung hinzufügen. Siehe Hinzufügen einer Erweiterung zu einer Regel.

Wenn Sie eine In-Memory-Tabelle hinzufügen, können Sie sie einer Regel als Erweiterung oder als Teil der Regelbedingung hinzufügen. Zum Beispiel verwendet die folgende Regel eine In-Memory-Tabelle als Teil der Regelbedingung zur Erstellung einer Whitelist und sie verwendet ebenfalls eine In-Memory-Tabelle mit Details in der Datei „user\_dst“, um die Warnmeldung, die angezeigt wird, zu erweitern.

Die Regel zeigt die In-Memory-Tabelle als eine Whitelist-Regelbedingung an:



Als Nächstes wird die Warnmeldung um die In-Memory-Tabelle „User\_list“ erweitert:



Aus diesem Grund wird die In-Memory-Tabelle „user\_dst“ verwendet, um eine Whitelist zu erstellen, und sie wird auch verwendet, um die Daten in der Warnmeldung zu erweitern, wenn die Warnmeldung ausgelöst wird.

### Hinzufügen einer wiederkehrenden In-Memory-Tabelle

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.
4. Klicken Sie auf  +  > **In-Memory-Tabelle**.
5. Beschreiben Sie die In-Memory-Tabelle:
  - a. Klicken Sie auf **Wiederkehrend**.
  - b. Standardmäßig ist **Aktiviert** ausgewählt. Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, werden Warnmeldungen mit den Daten aus der Tabelle erweitert.  
Wenn Sie einer Regel eine In-Memory-Tabelle hinzufügen, die Warnmeldungen aber nicht erweitert werden sollen, deaktivieren Sie das Kontrollkästchen.

- c. Geben Sie im Feld **Benutzerdefinierter Tabellenname** einen Namen für die Konfiguration der In-Memory-Tabelle ein, zum Beispiel „Studenteninformationen“.
- d. Wenn Sie erläutern möchten, welche Informationen die Erweiterung zu einer Warnmeldung hinzufügt, geben Sie eine **Beschreibung** ein, wie z. B.:  
Wenn eine Warnmeldung nach „Rollno“ gruppiert ist, fügt diese Erweiterung Studenteninformationen hinzu, zum Beispiel Name und Markierungen.
6. Geben Sie die URL der CSV-Datei ein, die die In-Memory-Tabelle mit Daten befüllt. Klicken Sie auf „Überprüfen“, um den Link zu validieren und die Spalten in der CSV-Datei zu befüllen. Sie können mithilfe der Plus- und Minus-Schaltflächen Spalten hinzufügen oder entfernen.
7. Wenn der Server hinter einem anderen Server konfiguriert ist, wählen Sie **Proxy verwenden** aus.
8. Wenn Anmeldeinformationen für den Server erforderlich sind, wählen Sie **Authentifiziert** aus.
9. Geben Sie als **Wiederholungsintervall** an, wie oft ESA die letzte CSV-Datei prüfen muss:
  - a. Wählen Sie Minute(n), Stunde(n) , Tag(e) oder Woche aus.
  - b. Wenn Sie „Woche“ auswählen, wählen Sie einen Wochentag aus.
  - c. Klicken Sie auf **Datumsbereich**, um ein **Startdatum** und ein **Enddatum** für den wiederkehrenden Plan auszuwählen.

10. Wählen Sie **Fortbestehen** aus, um die In-Memory-Tabelle auf dem Datenträger beizubehalten, wenn der ESA-Service angehalten wird, und um die Tabelle wieder aufzufüllen, wenn der Service wieder gestartet wird.
11. Wählen Sie bei Verwendung einer CSV-basierten In-Memory-Tabelle als Erweiterung im Drop-down-Menü **Schlüssel** das Feld aus, das als Standardschlüssel verwendet werden soll, um eingehende Ereignisse mit der In-Memory-Tabelle zu verbinden. Standardmäßig ist die erste Spalte ausgewählt. Sie können den Schlüssel auch später ändern, wenn Sie die In-Memory-Tabelle in Erweiterungsquellen öffnen.
12. Wählen Sie im Drop-down-Menü **Max. Zeilen** die Anzahl der Zeilen aus, die die eine bestimmte Instanz der In-Memory-Tabelle enthalten kann.
13. Klicken Sie auf **Save**.  
Die wiederkehrende In-Memory-Tabelle ist konfiguriert. Sie können sie der Regel als

Erweiterung oder als Teil der Regelbedingung hinzufügen. Siehe [Hinzufügen einer Erweiterung zu einer Regel](#).

## Konfigurieren von Warehouse Analytics als Erweiterungsquelle

In diesem Thema werden Anweisungen zur Konfiguration von RSA Warehouse Analytics als Erweiterungsquelle für ESA bereitgestellt. Datenanalysten nutzen RSA Analytics Warehouse-Daten, um Sitzungs- und Protokoll Daten zu analysieren.

So konfigurieren Sie Warehouse Analytics als Erweiterungsquelle:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Klicken Sie auf die Registerkarte **Einstellungen**.

Name ^	Type
OS	string
access_point	string
accesses	string
action	string[]
ad_computer_dst	string
ad_computer_src	string
ad_domain_dst	string
ad_domain_src	string
ad_username_dst	string
ad_username_src	string
alert	string
alert_id	string

3. Wählen Sie im Bereich „Optionen“ die Option **Erweiterungsquellen** aus.  
Der Bereich Erweiterungsquellen wird angezeigt.



Enrichment Sources

Enabled	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	Default GeoIP	GeoIP	Default Geo IP Enrichment Source. This cannot be edited.	2014-08-22 16:13:49	
<input type="checkbox"/>	MySql1	External DB Re...	table - satest1	2014-08-22 16:13:49	
<input type="checkbox"/>	Table1	In-Memory Table	ip_src, hostname and user	2014-08-25 15:06:03	
<input type="checkbox"/>	Table2	In-Memory Table	ip_src, hostname, user, place and id	2014-08-25 15:06:42	
<input type="checkbox"/>	WarehouseAnalytics	Warehouse An...		2014-08-22 16:13:49	

Page 1 of 1 | Page Size 25 | Displaying 1 - 5 of 5

4. Wählen Sie aus dem Drop-down-Menü **Warehouse Analytics** aus.

Warehouse Analytics

Enable

Name \*

Description

Warehouse Analytics Database URL \*

Username

Password

Cancel Save

5. Wählen Sie **Aktivieren** aus, um Warnmeldungen um zusätzliche Daten zu erweitern. Diese Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, werden die Warnmeldungen nicht um zusätzliche Daten erweitert.
6. Geben Sie in das Feld **Name** einen Namen ein, um die Warehouse Analytics-Konfiguration zu identifizieren oder zu bezeichnen.
7. Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung der Warehouse Analytics-Konfiguration ein.

8. Geben Sie in das Feld **Warehouse Analytics-Datenbank-URL** die MongoDB-URL für die Warehouse Analytics-Datenbank ein.
9. Geben Sie in das Feld **Benutzername** den Benutzername ein, um auf die MongoDB zugreifen zu können.
10. Geben Sie in das Feld **Passwort** das Passwort ein, um auf die MongoDB zugreifen zu können.
11. Klicken Sie auf **Save**.

Weitere Informationen finden Sie unter [Registerkarte „Einstellungen“](#).


## Hinzufügen einer Erweiterung zu einer Regel

In diesem Thema wird erläutert, wie eine zuvor konfigurierte Erweiterungsquelle zu einer Regel hinzugefügt wird. Wenn ESA eine Warnmeldung erstellt, werden die Informationen aus dieser Quelle einbezogen.


Durch Hinzufügen einer Erweiterungsquelle können Sie eine Suche in einer Vielzahl von Quellen anfordern und die Ergebnisse in die ausgehenden Warnmeldungen integrieren, um deren Inhalt detaillierter zu gestalten. Für dieses Verfahren sind die Rollenberechtigungen Administrator, DPO und SOC Manager erforderlich.

### Verfahren

So fügen Sie einer Regel eine Erweiterung hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Führen Sie in der Ansicht **Regelbibliothek** einen der folgenden Schritte aus:
  - Doppelklicken Sie auf eine Regel.
  - Wählen Sie eine Regel aus und klicken Sie in der Symbolleiste der **Regelbibliothek** auf .

Der Bereich „Regelerstellung“ wird in einer neuen Security Analytics-Registerkarte angezeigt.

3. Klicken Sie im Bereich **Erweiterungen** auf  und wählen Sie einen der folgenden Erweiterungstypen aus:
  - In-Memory-Tabelle
  - Externer DB-Verweis

- Warehouse Analytics
- GeoIP
- **Hinweis:** Wenn Sie eine GeoIP-Quelle verwenden, wird ipv4 automatisch ausgefüllt und kann nicht bearbeitet werden.

Die von Ihnen ausgewählten Erweiterungstypen werden in der Tabelle angezeigt.

4. Gehen Sie für den hinzugefügten Erweiterungstyp wie folgt vor:
  - Wählen Sie in der Spalte **Ausgabe** den Typ aus, den Sie konfiguriert haben.
  - Wählen Sie in Drop-down-Liste **Erweiterungsquelle** die definierte Erweiterungsquelle aus.
  - Geben Sie im Feld **ESA Ereignis-Stream-Metadaten** den Metaschlüssel des Ereignis-Streams ein, dessen Wert als ein Operand der Verknüpfungsbedingung verwendet wird.

Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/> <b>In-Memory Table</b>	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> Warehouse Analytics	Select Enrichment Source	Enter Meta	key
<input type="checkbox"/> GeoIP	Select Enrichment Source	Enter Meta	ipv4

- Geben Sie im Feld **Spaltenname „Erweiterungsquelle“** den Spaltennamen der Erweiterungsquelle ein, dessen Wert als weiterer Operand der Verknüpfungsbedingung verwendet wird.
5. Wählen Sie **Debuggen** aus. Hierdurch wird eine @Audit(,Stream‘)-Anmerkung zur Regel hinzugefügt. Das ist für das Debuggen der Esper-Regeln von Vorteil.
  6. Klicken Sie auf **Syntax anzeigen**, um zu testen, ob die definierte ESA-Regel gültig ist.
  7. Klicken Sie auf **Save**.

Weitere Informationen über Parameter und ihre Beschreibung erhalten Sie unter [Registerkarte Regelerstellung](#).



## Bereitstellen von Regeln für die Ausführung in ESA

In diesem Thema wird erläutert, wie ein ESA-Service und die darauf anzuwendenden Regeln ausgewählt werden. Für alle Aufgaben in diesem Abschnitt sind die Berechtigungen der Rollen Administrator, SOC Manager oder DPO erforderlich.

Für die Erstellung einer Bereitstellung müssen Sie die Schritte ausführen, die beschrieben sind unter [Bereitstellungsschritte](#)

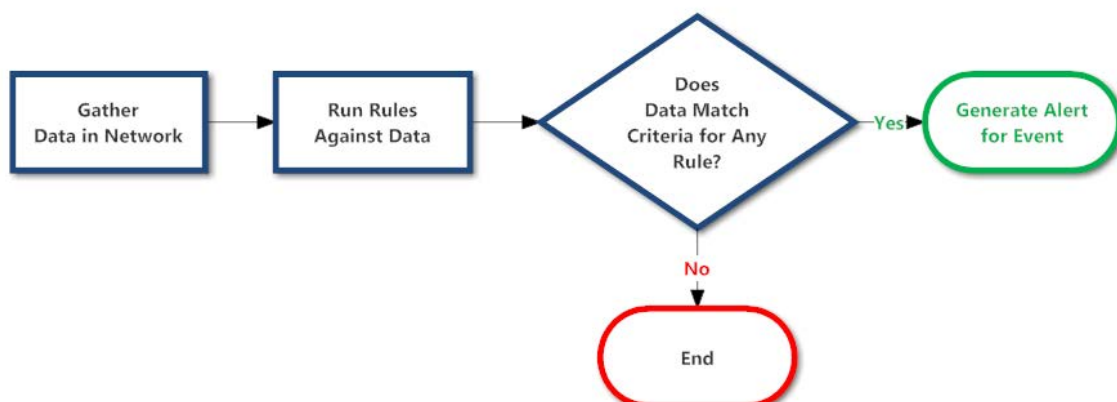
### Funktionsweise der Bereitstellung

Eine Bereitstellung besteht aus einem ESA-Service und einem Satz von ESA-Regeln. Wenn Sie Regeln bereitstellen, führt der ESA-Service diese aus, um verdächtige oder unerwünschte Aktivitäten in Ihrem Netzwerk zu erkennen. Jede ESA-Regel erkennt ein unterschiedliches Ereignis, zum Beispiel den Fall, dass ein Benutzerkonto erstellt und innerhalb einer Stunde gelöscht wird.

Der ESA-Service führt die folgenden Funktionen aus:

1. Sammelt **Daten** im Netzwerk.
2. Führt **ESA-Regeln** für die Daten aus.
3. Wendet **Regelkriterien** auf Daten an.
4. Erzeugt eine **Warnmeldung** für das erfasste Ereignis.

In der folgenden Grafik wird dieser Workflow dargestellt:



Darüber hinaus möchten Sie möglicherweise weitere Schritte für die Bereitstellung durchführen, beispielsweise einen ESA-Service in der Bereitstellung löschen, eine Regel aus der Bereitstellung bearbeiten oder löschen, eine Bereitstellung bearbeiten oder löschen oder Updates für eine Bereitstellung anzeigen. Beschreibungen dieser Verfahren finden Sie unter [Zusätzliche Bereitstellungsverfahren](#)

## Bereitstellungsschritte

In diesem Thema wird das Hinzufügen einer Bereitstellung erläutert, die einen ESA-Service und einen Satz ESA-Regeln enthält. Sie können eine Bereitstellung zum Organisieren und Managen von ESA-Services und -Regeln hinzufügen. Stellen Sie sich die Bereitstellung als Container für beide Komponenten vor:

1. Einen ESA-Service
2. Einen Satz ESA-Regeln

Wenn Sie beispielsweise die Bereitstellung für Spamaktivität hinzufügen, kann sie ESA London und einen Satz ESA-Regeln zur Erkennung von verdächtiger E-Mail-Aktivität enthalten.

Zum Hinzufügen einer Bereitstellung müssen Sie die folgenden Verfahren durchführen:

- [Schritt 1. Hinzufügen einer Bereitstellung](#)
- [Schritt 2. Hinzufügen eines ESA-Services](#)
- [Schritt 3. Hinzufügen und Bereitstellen von Regeln](#)

## Schritt 1. Hinzufügen einer Bereitstellung

### Voraussetzungen


Folgendes ist erforderlich, um eine Bereitstellung hinzuzufügen:

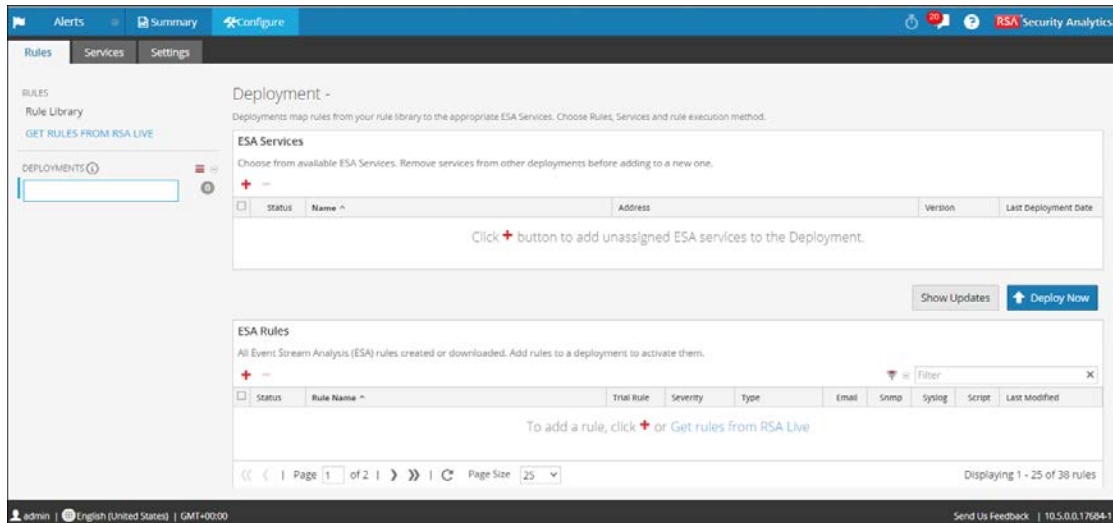
- Der ESA-Service muss auf dem Host konfiguriert werden. Siehe „Konfigurieren von ESA-Services“ im **Konfigurationsleitfaden für Event Stream Analysis (ESA)**.
- Regeln müssen in der Regelbibliothek festgelegt werden. Siehe [Hinzufügen von Regeln zur Regelbibliothek](#).

### Verfahren

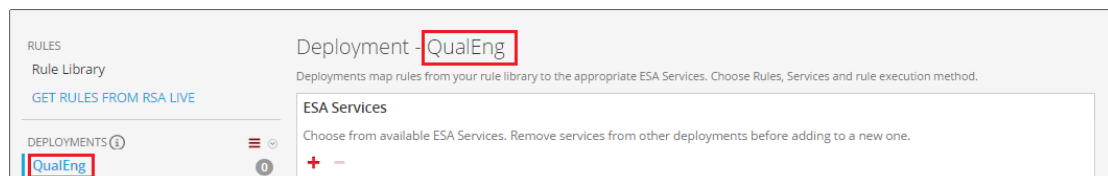
So fügen Sie eine Bereitstellung hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Registerkarte Regeln wird angezeigt.

2. Wählen Sie im Bereich „Optionen“ neben „Bereitstellungen“ die Option  **Hinzufügen** aus.  
Die Ansicht Bereitstellung wird rechts angezeigt.



3. Geben Sie einen **Namen** für die Bereitstellung ein. Sie können die Benennungskonvention beliebig festlegen.  
Sie kann beispielsweise den Verwendungszweck angeben oder einen Eigentümer identifizieren.
4. Drücken Sie die **Eingabetaste**.  
Die Bereitstellung wurde hinzugefügt.



## Schritt 2. Hinzufügen eines ESA-Services

Der ESA-Service in einer Bereitstellung sammelt Daten im Netzwerk und führt ESA-Regeln an den Daten aus. Dies dient dazu, Ereignisse zu erfassen, die den Regelkriterien entsprechen, und dann eine Warnmeldung zu dem erfassten Ereignis zu erzeugen.

Der gleiche ESA-Service kann zu mehreren Bereitstellungen hinzugefügt werden. Beispielsweise kann ESA London gleichzeitig in folgenden Bereitstellungen vorhanden sein:

- Bereitstellung EUR, die einen Satz von ESA-Regeln enthält
- Bereitstellung CORP, die einen anderen Satz von ESA-Regeln enthält

Wenn Sie einen ESA-Service aus einer Bereitstellung entfernen, werden die Regeln ebenfalls aus dem ESA-Service entfernt. Beispielsweise kann die Bereitstellung EUR ESA London sowie 25 Regeln enthalten. Wenn Sie ESA London aus der Bereitstellung EUR entfernen, werden die 25 Regeln ebenfalls aus ESA London entfernt. Folglich enthält ein ESA-Service keine Regeln, wenn er nicht Bestandteil einer Bereitstellung ist.

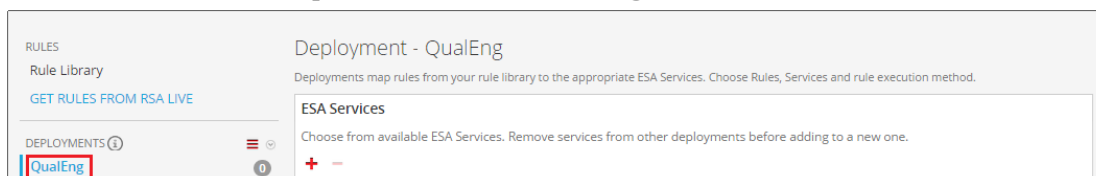
### Verfahren

So fügen Sie einen ESA-Service hinzu:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

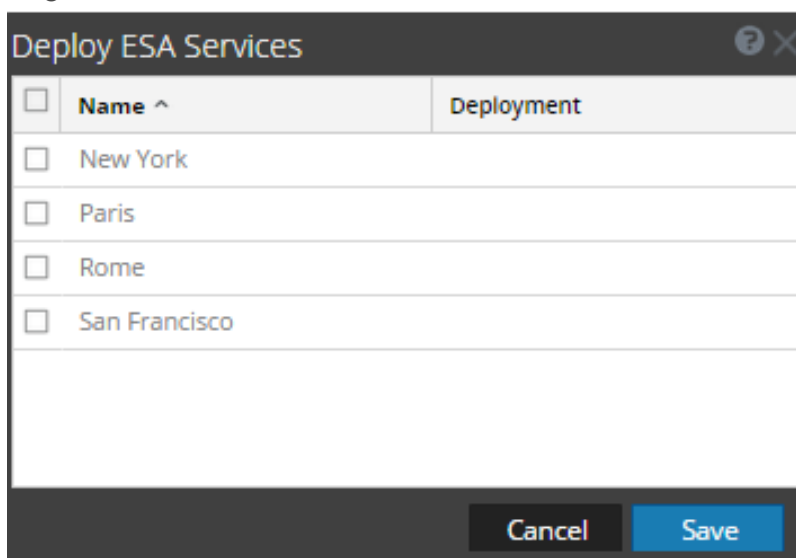
Die Registerkarte Regeln wird angezeigt.

2. Wählen Sie im Bereich Optionen eine **Bereitstellung** aus:



3. Klicken Sie in der Ansicht **Bereitstellung** unter **ESA-Services** auf **+**.

Im Dialogfeld ESA-Services bereitstellen werden alle konfigurierten ESA-Services aufgelistet.





4. Wählen Sie eine ESA aus und klicken Sie auf **Speichern**.

Die Ansicht Bereitstellung wird angezeigt. Der ESA-Service wird im Bereich **ESA-Services** mit dem Status „Hinzugefügt“ aufgeführt.

### **Schritt 3. Hinzufügen und Bereitstellen von Regeln**

In diesem Thema wird erläutert, wie Sie einer Bereitstellung ESA-Regeln hinzufügen und die Regeln dann in ESA bereitstellen. Jede ESA-Regel hat eindeutige Kriterien. Die ESA-Regeln in einer Bereitstellung legen fest, welche Ereignisse von ESA erfasst werden. Damit werden wiederum die Warnmeldungen festgelegt, die Sie erhalten.

Zum Beispiel enthält Bereitstellung A ESA Paris und unter anderem eine Regel, mit der Dateitransfer über einen nicht standardmäßigen Port erfasst wird. Wenn ESA Paris einen Dateitransfer erkennt, der den Regelkriterien entspricht, wird das Ereignis erfasst und eine entsprechende Warnmeldung erzeugt. Wenn Sie diese Regel aus der Bereitstellung A entfernen, erzeugt ESA keine Warnmeldung mehr für ein solches Ereignis.

#### **Verfahren**

So fügen Sie Regeln hinzu und stellen sie bereit:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

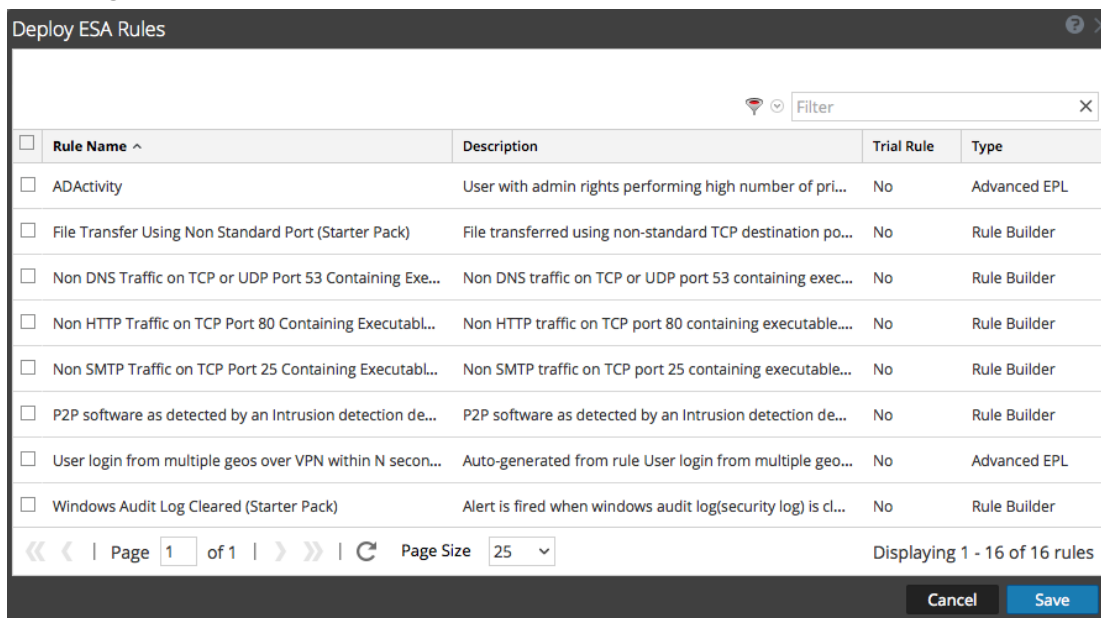
Die Registerkarte Regeln wird angezeigt.

2. Wählen Sie im Bereich Optionen eine Bereitstellung aus.

3. Klicken Sie in der Ansicht **Bereitstellung** auf **+** in **ESA-Regeln**.

Das Dialogfeld ESA-Regeln bereitstellen wird angezeigt. Es enthält die einzelnen Regeln in


Ihrer Regelbibliothek:

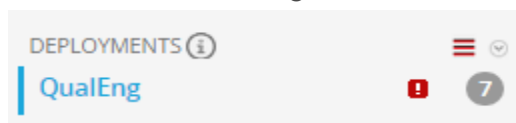


4. Wählen Sie Regeln aus und klicken Sie auf **Speichern**.

Die Ansicht Bereitstellung wird angezeigt.

5. Die Regeln werden im Abschnitt ESA-Regeln aufgelistet.

- In der Spalte „Status“ wird **Hinzugefügt** neben jeder neuen Regel angezeigt.
- Im Abschnitt „Bereitstellung“ zeigt  an, dass Updates für die Bereitstellung vorhanden sind.
- Die Gesamtzahl der Regeln in der Bereitstellung wird auf der rechten Seite angezeigt.



6. Klicken Sie auf **Jetzt bereitstellen**.

Der ESA-Service führt den Regelsatz aus.

## Zusätzliche Bereitstellungsverfahren

Neben der Bereitstellung eines ESA-Services und -Regeln möchten Sie möglicherweise weitere Schritte für die Bereitstellung durchführen, beispielsweise einen ESA-Service in der Bereitstellung löschen, eine Regel aus der Bereitstellung bearbeiten oder löschen, eine Bereitstellung bearbeiten oder löschen oder Updates für eine Bereitstellung anzeigen.

Um diese Verfahren durchführen zu können, gehen Sie zu:

- [Löschen eines ESA-Services in einer Bereitstellung](#)
- [Bearbeiten oder Löschen einer Regel in einer Bereitstellung](#)
- [Bearbeiten oder Löschen einer Bereitstellung](#)
- [Anzeigen der Aktualisierungen an einer Bereitstellung](#)


## Löschen eines ESA-Services in einer Bereitstellung

Dieses Thema bietet Anweisungen zum Löschen eines ESA-Services in einer Bereitstellung. In einer Bereitstellung mit einem Service können Sie die auf den Service angewendeten Regeln bearbeiten und den Service aus der Bereitstellung löschen.

Jedes der folgenden Verfahren beginnt auf der Registerkarte Regeln.

### Verfahren

So löschen Sie einen ESA-Service:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.  
Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.
3. Wählen Sie im Bereich **ESA-Services** einen Service aus und klicken Sie in der Symbolleiste auf .  
Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.  
Der Service wird gelöscht.

## Bearbeiten oder Löschen einer Regel in einer Bereitstellung


In einer Bereitstellung mit Regeln können Sie die Regeln bearbeiten oder löschen, um die Bereitstellung anzupassen. Jedes der folgenden Verfahren beginnt auf der Registerkarte Regeln.

## Methoden

### Bearbeiten einer Regel

1. Wählen Sie im Menü „Security Analytics“ die Optionen „Warnmeldungen > Konfigurieren > Regeln“ aus.  
Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich Optionen unter Bereitstellungen eine Bereitstellung aus.
3. Doppelklicken Sie im Bereich **ESA-Regeln** auf eine Regel, um diese in einer neuen Security Analytics-Registerkarte zu öffnen.
4. Ändern Sie die Regel und klicken sie anschließend auf **Anwenden**.  
Die Regel wird gespeichert.

### Löschen einer Regel

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Regeln** aus.  
Die Registerkarte Regeln wird angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.
3. Wählen Sie im Bereich **ESA-Regeln** eine Regel aus und klicken Sie in der Symbolleiste auf .  
Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Yes**.  
Die Regel wird gelöscht.

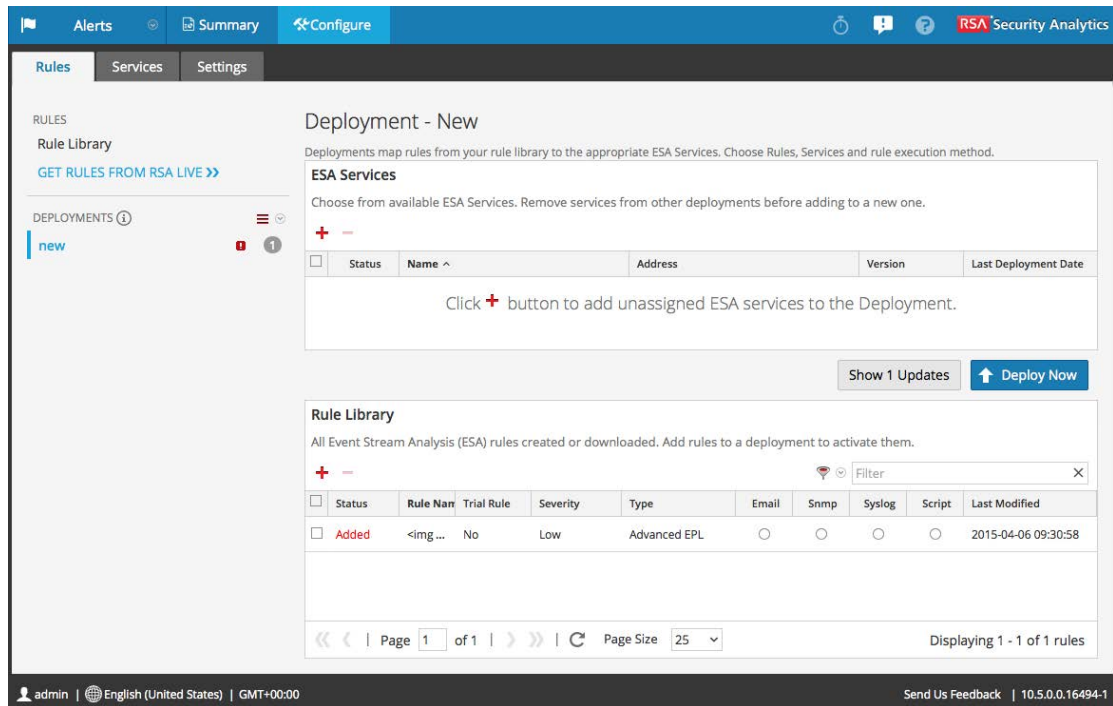
### Bearbeiten oder Löschen einer Bereitstellung

In diesem Thema wird erläutert, wie Security Analytics eine Korrelationsregel an alle ESA-Services in einer Korrelationsgruppe weiterleitet. In einer Korrelationsgruppe muss jeder ESA-Service denselben Satz von Regeln ausführen. Wenn Sie einer Korrelationsgruppe eine Regel hinzufügen, leitet Security Analytics die Regel an jeden ESA-Service in der Gruppe weiter.


So greifen Sie auf die Bereitstellungen zu

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.
2. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.


Die Ansicht Bereitstellung wird angezeigt.




### Bearbeiten einer Bereitstellung

1. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.  
Die Ansicht Bereitstellung wird angezeigt.
2. Wählen Sie  > **Bearbeiten** aus.  
Der Bereitstellungsname kann jetzt bearbeitet werden.

### Löschen einer Bereitstellung

1. Wählen Sie im Bereich „Optionen“ unter **Bereitstellungen** eine Bereitstellung aus.  
Die Ansicht Bereitstellung wird angezeigt.
2. Wählen Sie  > **Löschen** aus.  
Ein Bestätigungsfeld wird angezeigt.
3. Klicken Sie auf **Yes**.  
Die Bereitstellung wird gelöscht.

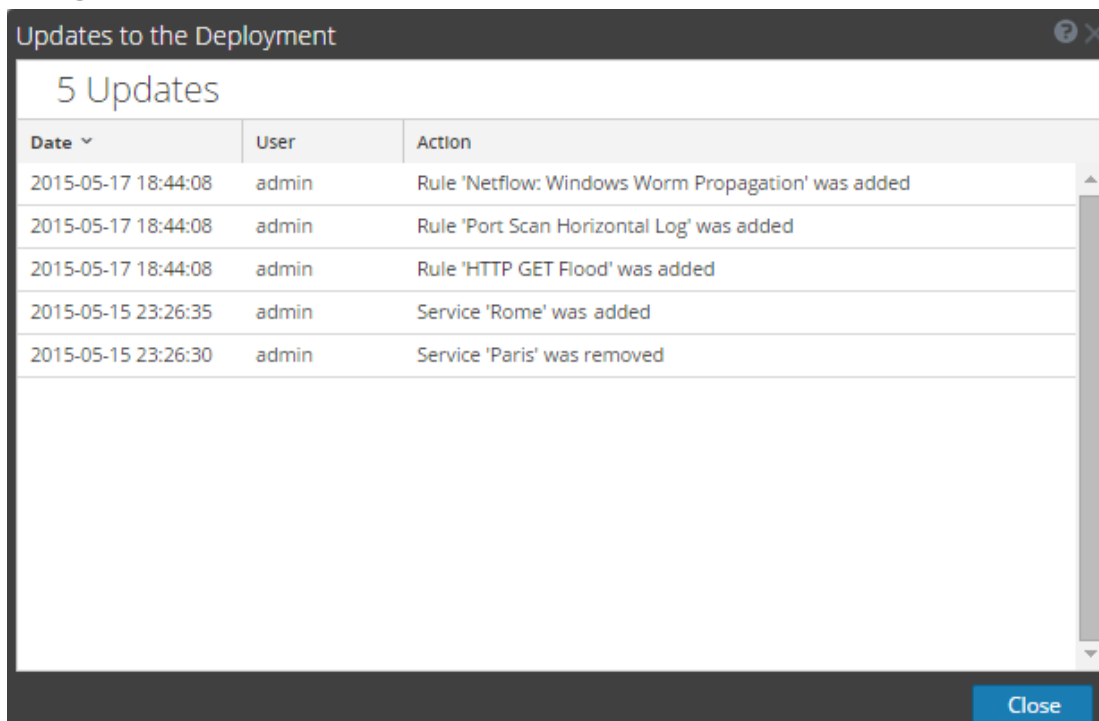
## Anzeigen der Aktualisierungen an einer Bereitstellung

In diesem Thema wird erläutert, wie Aktualisierungen an einer Bereitstellung, beispielsweise das Hinzufügen und Löschen von Regeln, angezeigt werden. Wenn Sie eine Änderung an einer Bereitstellung vornehmen, wird das Aktualisierungssymbol (  ) neben dem Namen der Bereitstellung angezeigt.

### Verfahren

So zeigen Sie die Updates zu einer Bereitstellung:

1. Wählen Sie im Menü Security Analytics die Optionen Warnmeldungen > Konfigurieren aus. Die Registerkarte Regeln wird angezeigt.
2. Klicken Sie im Bereich „Optionen“ unter **Bereitstellungen** ganz rechts auf **Updates anzeigen**.



3. Klicken Sie auf **Close**.

## Anzeigen von ESA-Statistiken und -Warnmeldungen

---

Wenn der ESA-Service Warnmeldungen erzeugt, können Sie Informationen dazu anzeigen, wie die Regeln ausgeführt wurden, wie etwa Statistiken zur Engine, Regel und Warnmeldung, und Sie können auch Informationen dazu anzeigen, welche Regeln aktiviert oder deaktiviert sind. Anweisungen zur Anzeige von ESA-Statistiken finden Sie unter [Anzeigen der Statistiken zu einem ESA-Service](#)

Wenn Ihr ESA-Service Warnmeldungen erzeugt, können Sie die Ergebnisse auf der Seite „Zusammenfassung der Warnmeldungen“ anzeigen. So können Sie Trends sehen und sowohl die Menge als auch die Häufigkeit von Warnmeldungen erkennen. Anweisungen zur Anzeige von Warnmeldungen finden Sie unter [Anzeigen einer Zusammenfassung der Warnmeldungen](#)

### Anzeigen der Statistiken zu einem ESA-Service

In diesem Thema wird beschrieben, wie die Bereitstellungsstatistiken für einen ESA-Service angezeigt werden können. Dieses Verfahren ist nützlich bei dem Versuch, die Effektivität einer Regel oder des Troubleshooting einer Bereitstellung zu ermitteln.

### Methoden

#### Anzeigen der ESA-Statistiken

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren > Services** aus.

- Wählen Sie aus der Liste **ESA-Services** auf der linken Seite einen Service aus.  
Die Bereitstellungsstatistiken für den ausgewählten Service werden angezeigt.

The screenshot shows the RSA Security Analytics interface for the San Francisco service. The left sidebar lists services: New York, Paris, Rome, and San Francisco (selected). The main content area is titled 'San Francisco' and contains the following sections:

- Engine Stats:** Esper Version: 3.1.0, Time: 2015-05-17T23:05:29, Events Offered: 0, Offered Rate: 0 per second / 0 max.
- Rule Stats:** Rules Enabled: 7, Rules Disabled: 0, Events Matched: 0.
- Alert Stats:** Email: 0, SNMP: 0, Syslog: 0, Script: 0, Storage: 0, Message Bus: 0.
- Deployed Rule Stats:** Includes a table with columns: Enable, Name, Trial Rule, Last Detected, and Events Matched. The table shows 4 rules, all with 0 events matched.

Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	SAMPLE - P2P Software as Detected by an Intrusion Detection Device	Yes		0
<input type="checkbox"/>	SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Yes		0
<input type="checkbox"/>	ECAT alerts with audit log cleared	No		0
<input type="checkbox"/>	HTTP GET Flood	Yes		0

- Lesen Sie die folgenden Abschnitte mit ESA-Statistiken.  
Eine vollständige Beschreibung jeder Statistik in den Abschnitten finden Sie unter [Registerkarte Services](#).
  - Engine-Statistiken**
  - Regelstatistiken**
  - Warmmeldungsstatistiken**
- Lesen Sie die detaillierten Informationen zu den auf dem ESA bereitgestellten Regeln unter „Statistik für bereitgestellte Regeln“ nach.  
Eine vollständige Beschreibung jeder Spalte in den Abschnitten finden Sie unter [Registerkarte Services](#).
  - Ob die Regel aktiviert oder deaktiviert ist
  - Der Name der Regel
  - Ob die Regel im Testregelmodus ausgeführt wird
  - Zuletzt erkannt
  - Übereinstimmende Ereignisse
- Klicken Sie zum Erstellen eines Snapshot des Regelspeichers auf **Integrität und Zustand**.



### Aktivieren und Deaktivieren von Regeln

1. Wählen Sie im Bereich **Statistik für bereitgestellte Regeln** eine Regel aus dem Raster aus.
2. Klicken Sie auf  **Enable**, um die Regel zu aktivieren, oder klicken Sie auf  **Disable**, um die Regel zu deaktivieren.

Die Registerkarte Services wird mit den Änderungen aktualisiert, die sofort wirksam sind.

### Aktualisieren der Statistiken

Die Registerkarte Services aktualisiert Statistiken nicht automatisch, es sei denn, Sie aktivieren oder deaktivieren eine Regel. So sorgen Sie dafür, dass die aktuellen Statistiken angezeigt werden:

1. Klicken Sie in der oberen rechten Ecke auf , um die Informationen zu aktualisieren.
2. Zeigen Sie die aktualisierten Kundeninformationen an.

## Anzeigen einer Zusammenfassung der Warnmeldungen

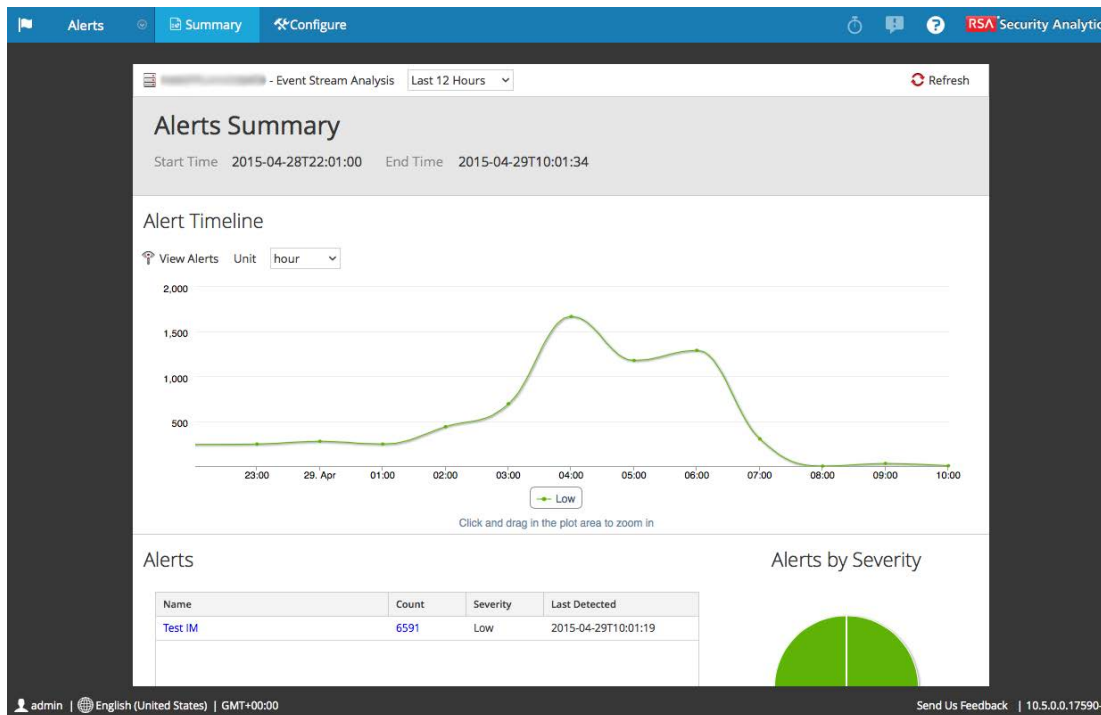
In diesem Thema wird beschrieben, wie Sie eine Zusammenfassung der Warnmeldungen anzeigen. Sie können eine zusammenfassende Ansicht der Warnmeldungen anzeigen, die in einem bestimmten Zeitbereich erzeugt wurden.

### Verfahren



So zeigen Sie eine Zusammenfassung der Warnmeldungen an:


1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Zusammenfassung** aus.

Wenn ein standardmäßiger ESA-Service vorhanden ist, wird die Ansicht Zusammenfassung mit den Informationen für diesen Service angezeigt.



Wenn kein Standardservice ausgewählt wurde, wird das Dialogfeld ESA-Service auswählen angezeigt.

2. Wählen Sie im Dialogfeld **ESA-Service auswählen** einen Service aus und klicken Sie auf **Auswählen**.  
Die Ansicht Zusammenfassung wird angezeigt.
3. So wählen Sie einen neuen Service für die Anzeige aus:
  - a. Klicken Sie auf .  
Das Dialogfeld ESA-Service auswählen wird angezeigt.
  - b. Wählen Sie in der Liste einen Service aus und klicken Sie auf **Auswählen**.  
Die Ansicht Zusammenfassung wird mit den Informationen für den ausgewählten Service angezeigt.
4. Öffnen Sie zum Auswählen des Zeitrahmens das Drop-down-Menü **Zeitbereich** und wählen Sie einen Zeitbereich aus.  
Die Felder Startzeit und Endzeit markieren den neuen Zeitbereich.
5. Öffnen Sie das Drop-down-Menü **Einheit**, um die Zeitachse auszuwählen, und wählen Sie eine Zeiteinheit aus.
6. Klicken Sie zum Aktualisieren der Informationen in der Ansicht „Zusammenfassung“ auf .

7. Klicken Sie zum Anzeigen der Warnmeldungen in einer Liste auf  **View Alerts** .  
Weitere Informationen finden Sie unter [Ansicht Zusammenfassung der Wammeldungen](#).



## Automatisierte Bedrohungserkennung

---

In diesem Thema wird erläutert, wie Sie die automatisierte Bedrohungserkennung konfigurieren und verwenden. Automatisierte Bedrohungserkennung ist ein Service, den Sie auf Ihrer ESA-Installation bereitstellen. Er untersucht Ihren HTTP-Datenverkehr, um die Wahrscheinlichkeit dafür zu ermitteln, dass böswillige Aktivitäten in Ihrer Umgebung stattfinden.

Weitere Informationen über die Arbeit mit der automatisierten Bedrohungserkennung finden Sie in den folgenden Themen:

- [Konfigurieren der automatisierten Bedrohungserkennung](#)
- [Arbeiten mit Ergebnissen der automatisierten Bedrohungserkennung](#)
- [Troubleshooting der automatisierten Bedrohungserkennung](#)

## Verstehen der automatisierten Bedrohungserkennung

Dieses Thema bietet eine Übersicht über die automatisierte Bedrohungserkennung. Bei der automatisierten Bedrohungserkennung handelt es sich um einen Service, den Sie auf Ihrer ESA bereitstellen. Die Verhaltensanalysen: Das Modul „Verdächtige Domains“ untersucht Ihren HTTP-Datenverkehr, um Domains zu erkennen, die wahrscheinlich Schadsoftware-Command-and-Control-Server sind und sich mit Ihrer Umgebung verbinden. Sobald die automatisierte Bedrohungserkennung Ihren Datenverkehr untersucht, erzeugt sie Bewertungen basierend auf verschiedenen Aspekten des Verhaltens Ihres Datenverkehrs (z. B. die Häufigkeit und Regelmäßigkeit, mit der eine bestimmte Domain kontaktiert wird). Wenn diese Bewertungen einen festgelegten Schwellenwert erreichen, wird eine ESA-Warnmeldung erzeugt. Diese ESA-Warnmeldung löst auch eine Warnmeldung im Incident Manager aus. Die Warnmeldung in Incident Manager wird mit Daten erweitert, die Ihnen helfen, die Bewertungen zu interpretieren, um festzustellen, welche Gegenmaßnahmen zu ergreifen sind.

Diese Version der automatisierten Bedrohungserkennung erlaubt Bewertungen, um Command-and-Control-Kommunikation zu erkennen. Command-and-Control-Kommunikation erfolgt, wenn Schadsoftware ein System infiziert hat und Daten zurück zu einer Quelle sendet. Oft kann Command-and-Control-Schadsoftware über Beaconing-Verhalten erkannt werden. Beaconing tritt auf, wenn die Schadsoftware regelmäßig Kommunikation zurück an den Command-and-Control-Server sendet, um ihn zu informieren, dass eine Maschine infiziert wurde und dass die Schadsoftware auf weitere Anweisungen wartet. Die Fähigkeit, die Schadsoftware an diesem Punkt der Infizierung zu ergreifen, kann weiteren Schaden an der infizierten Maschine vermeiden und gilt als kritische Phase in der „Kill Chain“.

Diese Funktion löst einige häufige Probleme, die bei der Suche nach Schadsoftware auftreten:

- **Fähigkeit zur Verwendung von Algorithmen anstatt Signaturen.** Da viele Ersteller von Schadsoftware inzwischen polymorphe oder verschlüsselte Codesegmente verwenden, für die nur sehr schwer eine Signatur erstellt werden kann, kann dieser Ansatz manchmal Schadsoftware nicht entdecken. Da die automatisierte Bedrohungserkennung einen verhaltensbasierten Algorithmus verwendet, kann sie Schadsoftware schneller und effizienter erkennen.
- **Möglichkeit zur Automatisierung der Jagd.** Das manuelle Durchsuchen von Daten ist eine effektive, aber sehr zeitaufwändige Methode zum Auffinden von Schadsoftware. Die Automatisierung dieses Prozesses erlaubt es Analysten, ihre Zeit effizienter zu nutzen.
- **Fähigkeit, einen Angriff schnell zu entdecken.** Anstatt Daten in Batches zu sammeln und dann zu analysieren, analysiert die automatisierte Bedrohungserkennung Daten, während sie von Security Analytics aufgenommen werden, so dass die Angriffe nahezu in Echtzeit gefunden werden können.

## Workflow

Automatisierte Bedrohungserkennung funktioniert ähnlich wie ein Filtersystem. Sie überprüft, ob ein bestimmtes Verhalten auftritt (oder bestimmte Bedingungen bestehen), und wenn dieses Verhalten oder diese Bedingung auftritt, fährt es mit dem nächsten Schritt im Prozess fort. Damit wird das System effizienter und es bleiben Ressourcen frei, da Ereignisse, die als nicht bedrohlich eingestuft werden, nicht im Arbeitsspeicher gehalten werden. Das folgende Diagramm bietet eine vereinfachte Version des Workflows.



- 1.) **HTTP-Pakete werden zum ESA-Service geleitet.** Die HTTP-Pakete werden vom Decoder analysiert und an das ESA-Gerät gesendet.
- 2.) **Die Whitelist wird geprüft.** Wenn Sie eine Whitelist über Context Hub erstellt haben, prüft der ESA-Service diese Liste, um Domains auszuschließen. Wenn eine Domain im Ereignis auf der Whitelist steht, wird das Ereignis ignoriert.
- 3.) **Das Profil der Domain wird geprüft.** Automatisierte Bedrohungserkennung prüft, ob die Domain neu in Erscheinung tritt (ca. drei Tage), über wenige Quell-IP-Verbindungen verfügt, viele Verbindungen ohne einen Referrer oder Verbindungen mit seltenen Benutzeragenten hat. Wenn eine oder mehrere dieser Bedingungen zutrifft, wird die Domain als nächstes auf regelmäßiges Beaconsing geprüft. Eine detaillierte Beschreibung dieser profilbezogenen Bewertungen einer Domain finden Sie unter „Arbeiten mit Bewertungen der automatisierten Bedrohungserkennung“.
- 4.) **Die Domain wird auf regelmäßiges Beaconsing geprüft.** Beaconsing tritt auf, wenn die Schadsoftware regelmäßig Kommunikation zurück an den Command-and-Control-Server sendet, um ihn zu informieren, dass eine Maschine infiziert wurde und dass die Schadsoftware auf weitere Anweisungen wartet. Wenn die Site Beaconsing-Verhalten zeigt, wird die Registrierungsinformation der Domain geprüft.
- 5.) **Registrierungsinformation der Domain wird geprüft.** Der Whois-Service wird verwendet, um festzustellen, ob die Domain vor kurzem registriert wurde oder fast abgelaufen ist. Domains, die eine sehr kurze Lebensdauer haben, sind oft Kennzeichen für Schadsoftware.

6.) **Command and Control (C2) aggregiert Bewertungen.** Jeder der oben genannten Faktoren erzeugt eine separate Bewertung, die gewichtet wird, um verschiedene Niveaus der Wichtigkeit zu kennzeichnen. Die gewichteten Bewertungen bestimmen, ob eine Warnmeldung erzeugt werden sollte. Wenn eine Warnmeldung erzeugt wird, werden die zusammengefassten Warnmeldungen im Incident Manager angezeigt und können von dort aus dann weiter untersucht werden. Sobald die Warnmeldungen im Incident Manager angezeigt werden, werden sie weiter unter dem zugehörigen Incident aggregiert. Dies erleichtert das Durchgehen großer Mengen von Warnmeldungen, die für einen Command-and-Control-Incident generiert werden können.

Wenn Sie Analyst sind, können Sie die im Modul „Zusammenfassung der Warnmeldungen“ oder im Modul „Incident Manager“ generierten Warnmeldungen anzeigen. Wenn Sie SecOps verwenden, können Sie Warnmeldungen in den SecOps-Versionen 1.2 und 1.3 anzeigen.

## Konfigurieren der automatisierten Bedrohungserkennung

Dieses Thema enthält Informationen für Administratoren und Analysten zur Konfiguration von und Arbeit mit der automatisierten Bedrohungserkennung.

Dieses Verfahren enthält die erforderlichen Schritte für die Konfiguration der automatisierten Bedrohungserkennung auf Ihrem ESA-Service. Bevor Sie allerdings die automatisierte Bedrohungserkennung aktivieren, ist es wichtig zu beachten, dass es viele potenzielle Installationskonfigurationen gibt, die auf dem ESA-Service installiert werden können, einschließlich: Automatisierte Bedrohungserkennung, ESA-Regeln und Context Hub. Sie alle binden Ressourcen, daher ist es wichtig, vor dem Aktivieren dieser Funktion auf Ihrem ESA-Service die Dimensionierung zu berücksichtigen.

### Voraussetzungen

Sie müssen einen Decoder für HTTP-Paketdaten konfiguriert haben.

Sie müssen einen HTTP-Lua oder Flex-Parser konfiguriert haben.

Aktivieren Sie für eine optimale Performance den Service „Context Hub“. Damit können Sie eine Whitelist erstellen.

### Verfahren: Konfigurieren der automatisierten Bedrohungserkennung

Dieses Verfahren enthält die erforderlichen Schritte für die Konfiguration der automatisierten Bedrohungserkennung.

Die erforderlichen grundlegenden Schritte sind:



1. **WhoIs-Einstellungen konfigurieren.** Mit dem Service „Whois“ können Sie präzise Daten über Domains erhalten, mit denen Sie sich verbinden. Um eine effektive Bewertung zu ermöglichen, ist es wichtig, dass Sie die Whois-Serviceeinstellungen konfigurieren.



2. **Eine Whitelist (optional) mithilfe des Service „Context Hub“ erstellen.** Durch das Erstellen einer Whitelist können Sie sicherstellen, dass häufig verwendete Websites von der Bewertung der automatisierten Bedrohungserkennung ausgeschlossen sind.
3. **Die automatisierte Bedrohungserkennung für Ihren angegebenen ESA-Service aktivieren.** Sie müssen für jeden ESA-Service, für den der Service ausgeführt werden soll, die automatisierte Bedrohungserkennung aktivieren.
4. **24 Stunden für die Anlaufphase warten und die C2-Incident-Manager-Regel aktivieren.** Wenn Sie die automatisierte Bedrohungserkennung verwenden, dauert es ca. 24 Stunden, bis der Bewertungsalgorithmus angelaufen ist. Aktivieren Sie nach 24 Stunden die C2-Regel auf Incident Manager.

**Schritt 1: Konfigurieren Sie die Whols-Serviceeinstellungen für Ihren ESA-Service.**

Sie konfigurieren Einstellungen, um Ihrem ESA-Service zu ermöglichen, sich mit dem Whois-Service zu verbinden. Dies ermöglicht Ihrem ESA-Service, detaillierte Informationen über die Domäne abzurufen, die die Bewertung der automatisierten Bedrohungserkennung auslöst.

1. Wählen Sie unter „Administration > Services“ Ihren ESA-Service und dann   > „Ansicht > Durchsuchen“ aus.
2. Klicken Sie im Explorer auf **Service > Whois > whoisClient**.
3. Konfigurieren Sie die folgenden Einstellungen (beachten Sie, dass nur die ersten beiden Parameter geändert werden müssen. RSA empfiehlt, dass Sie die Standardeinstellungen für andere Parameter verwenden):

Parameter	Beschreibung
whoisUserId	<b>Erforderlich:</b> Geben Sie die Anmeldeinformationen für die Authentifizierung für den RSA Whois-Server ein. Diese sind identisch mit Ihrer RSA Live-Benutzer-ID. Wenn Sie noch kein RSA Live-Konto konfiguriert haben, müssen Sie dies jetzt tun. Der Standardwert ist „whois“.
whoisPassword	<b>Erforderlich:</b> Geben Sie die Anmeldeinformationen für die Authentifizierung für den RSA Whois-Server ein. Diese sind identisch mit Ihrem RSA Live-Passwort. Wenn Sie noch kein RSA Live-Konto konfiguriert haben, müssen Sie dies jetzt tun. Der Standardwert ist null.

Parameter	Beschreibung
whoisUrl	<p><b>Optional:</b> Geben Sie die URL ein, um Whois-Daten von dem RSA Whois-Service zu erhalten. Beachten Sie, dass der nachgestellte Schrägstrich („/“) erforderlich ist. Andernfalls werden Anfragen fehlschlagen.</p> <p>Der Standardwert ist:  <a href="https://cms.netwitness.com/whois/query/">„https://cms.netwitness.com/whois/query/“</a></p>
whoisAuthUrl	<p><b>Optional:</b> Geben Sie die URL ein, um Authentifizierungstoken von dem RSA Whois-Service zu erhalten.</p> <p>Der Standardwert ist:  <a href="https://cms.netwitness.com/authlive/authenticate/WHOIS">” https://cms.netwitness.com/authlive/authenticate/WHOIS“</a></p>
whoisAuthTokenLifespanSeconds	<p><b>Optional:</b> Geben Sie die Zeit in Sekunden ein, nach der ein Authentifizierungstoken verlängert werden sollte.</p> <p>Der Standardwert ist 3.300.</p>
whoisHttpsProxy	<p><b>Optional:</b> Wenn HTTP-Anforderungen einen Proxy erfordern, legen Sie diesen auf denselben Wert fest, wie er für den RSA Live-Service verwendet wird. Verwenden Sie diesen Parameter nur, wenn <b>insecureConnection</b> auf <b>true</b> festgelegt ist.</p> <p>Der Standardwert ist false.</p> <p>(Erfordert einen Neustart des ESA-Service, um wirksam zu werden.)</p>
insecureConnection	<p><b>Optional:</b> Legen Sie diesen Parameter auf <b>true</b> fest, damit die HTTP-Anforderung an den RSA Whois-Service SSL-Zertifikate ignorieren darf.</p> <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p><b>Hinweis:</b> Wenn auf den RSA Whois-Service über einen Proxy zugegriffen wird, sollte dieser Parameter auf <b>true</b> festgelegt sein.</p> </div> <p>Der Standardwert ist false.</p> <p>(Erfordert einen Neustart des ESA-Service, um wirksam zu werden.)</p>

Parameter	Beschreibung
allowedRequests	<p><b>Optional:</b> Geben Sie ein, wie viele Abfragen Sie zulassen möchten, bevor der Whois-Service gedrosselt werden soll. Dieser Parameter funktioniert mit „allowedRequestsIntervalSeconds“, wo Sie das Intervall für Abfragen festlegen können. Beispiel: Wenn Sie <b>allowedRequests</b> auf 100 und <b>allowedRequestsIntervalSeconds</b> auf 60 festlegen, können Sie 100 Anforderungen in jedem 60-Sekunden-Intervall starten.</p> <p>Der Standardwert ist 100.</p> <p>(Erfordert einen Neustart des ESA-Service, um wirksam zu werden.)</p>
allowedRequestsIntervalSeconds	<p><b>Optional:</b> Wenn Sie den Parameter <b>allowedRequests</b> festlegen, müssen Sie auch diese Einstellung konfigurieren, um das Intervall festzulegen. Dieser Wert sollte für Ihre Umgebung optimiert werden.</p> <p>Die Standardeinstellung beträgt 60 Sekunden.</p> <p>(Erfordert einen Neustart des ESA-Service, um wirksam zu werden.)</p>
queueMaxSize	<p><b>Optional:</b> Geben Sie die maximale Größe der Warteschlange der Domains an, deren Informationen von dem RSA Whois-Service angefordert werden.</p> <p>Die Standardeinstellung ist 100.000.</p>
cacheMaxSize	<p><b>Optional:</b> Geben Sie die maximale Anzahl der zwischengespeicherten Whois-Einträge an. Sobald diese Grenze erreicht ist, wird der am längsten nicht verwendete Eintrag entfernt, um Platz für einen neuen Eintrag freizugeben.</p> <p>Die Standardeinstellung ist 50.000.</p> <p>(Erfordert einen Neustart des ESA-Service, um wirksam zu werden.)</p>




Parameter	Beschreibung
refreshIntervalSeconds	<p><b>Optional:</b> Geben Sie die Anzahl der Sekunden für das Aktualisierungsintervall an. Wenn die angeforderte Whois-Information im Cache gefunden wird und der Cacheeintrag älter ist als die angegebene Anzahl Sekunden, wird der Eintrag aus dem Cache entfernt und die Domain an die Warteschlange zurückgegeben, um abgefragt zu werden. (Der Cache-Eintrag wird für die Anforderung zurückgegeben, die ihn als veraltet gekennzeichnet hat.)</p> <p>Die Standardeinstellung beträgt 2.592.000 Sekunden (30 Tage).</p>
waitForHTTPRequest	<p><b>Optional:</b> Erfordert, dass der ESA-Service wartet, bis der Whois-Service antwortet, bevor die Ausführung von EPL abgeschlossen werden kann. Dadurch wird sichergestellt, dass die Whois-Daten immer in den Suchergebnissen enthalten sind, aber die Performance kann beeinträchtigt werden, da ESA bis zu 30 Sekunden auf die Antwort des Whois-Service wartet.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren und die Antwortzeit langsam ist, schließt ESA die Analyse für ein gegebenes Ereignis ohne die Whois-Daten ab und berechnet die Bewertung ohne die Daten.</p> <p>Die Standardeinstellung ist <b>true</b>.</p>

## Schritt 2: Erstellen Sie eine Domain-Whitelist (Optional)


**Hinweis:** Dieser Schritt ist optional: Wenn Sie den Incident Manager verwenden, um diese Incidents zu managen, können Sie auch eine Whitelist erstellen, indem Sie einen Incident als falsch positiv schließen.

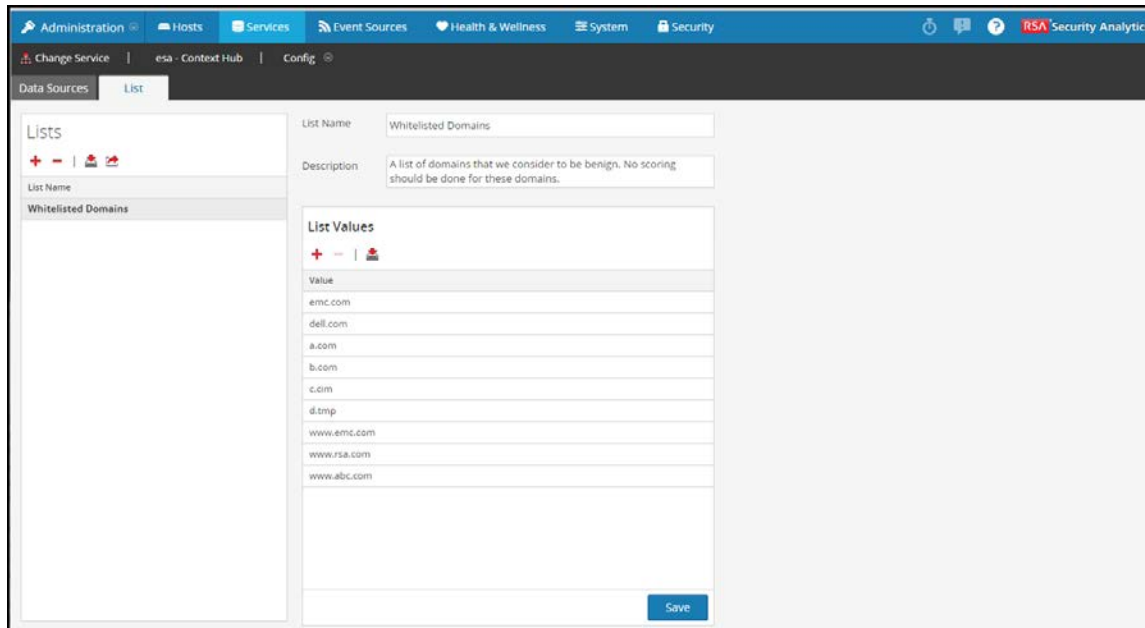
Dieses Verfahren wird bei der Arbeit mit der automatisierten Bedrohungserkennung verwendet, um sicherzustellen, dass bestimmte Domains keine Bedrohungsbewertung auslösen. Manchmal kann eine Domain, auf die Sie regelmäßig zugreifen, eine Bewertung der automatisierten Bedrohungserkennung auslösen. Beispielsweise könnte ein Wetterdienst ein ähnliches Beaconing-Verhalten zeigen wie eine Command-and-Control-Kommunikation und so eine nicht gerechtfertigte negative Bewertung auslösen. Ein solches Ereignis wird als falsch positiv bezeichnet. Um das Auslösen eines falsch positiven Ereignisses zu verhindern, können Sie die Domain einer Whitelist hinzufügen. Die meisten Domains müssen nicht einer Whitelist hinzugefügt werden, da die Lösung nur bei sehr verdächtigem Verhalten eine Warnmeldung auslöst. Die Domains, die Sie möglicherweise einer Whitelist hinzufügen möchten, sind gültige automatisierte Services, mit denen sich wenige Hosts verbinden.




**Hinweis:** Sie können nur eine Context Hub-Instanz in Ihrer Bereitstellung von Security Analytics aktiviert haben. Wenn Ihr Context Hub-Service auf einem anderen ESA-Service ausgeführt wird, müssen Sie ihn so konfigurieren, dass er sich mit dem ESA-Service verbindet, der den Context Hub-Service ausführt. Anweisungen dazu finden Sie unter „Konfigurieren eines ESA-Services zur Herstellung einer Verbindung mit dem Context Hub auf einem anderen ESA-Service“ im **Konfigurationsleitfaden für Event Stream Analysis (ESA)**.

1. Von dem Context Hub-Service können Sie eine Liste erstellen und manuell Domains hinzufügen oder Sie können eine CSV-Datei mit einer Liste von Domains hochladen.
  - a. Wählen Sie unter „Administration > Services“ den Context Hub aus.
  - b. Wählen Sie den Context Hub aus, dann  Ansicht > **Konfigurieren**>.
  - c. Wählen Sie die Registerkarte **Liste** aus, um die zu bearbeitenden Listen zu öffnen.
  - d. Klicken Sie im linken Bereich auf , um eine Liste hinzuzufügen. Geben Sie einen Namen für die Liste ein und fügen Sie manuell Domains hinzu, indem Sie auf  im rechten Bereich klicken.

**Achtung:** Die Whitelist muss den Namen *Domains auf weißer Liste* erhalten. Andernfalls kann Context Hub die Liste nicht als Whitelist verarbeiten.



- e. Um eine CSV-Datei zu importieren, klicken Sie auf  und navigieren Sie im Dialogfeld „Datei importieren“ zu der CSV-Datei. Beachten Sie, dass die Datei den Namen *Domains auf weißer Liste* erhalten muss. Wählen Sie eines der folgenden Trennzeichen aus: Komma, LF (Zeilenvorschub) und CR (Wagenrücklauf), je nachdem, wie Sie die Werte in Ihrer Datei getrennt haben. Klicken Sie dann auf **Hochladen**.
- f. Vom Service „Context Hub“ aus können Sie auch eine vorhandene Whitelist ändern, um eine Domain hinzuzufügen oder zu entfernen.
- g. Im rechten Bereich zeigt **Liste** Ihre vorhandene Domain-Whitelist an.
- h. Klicken Sie auf **Domains auf weißer Liste**. Die Werte für die Whitelist werden im rechten Bereich angezeigt.

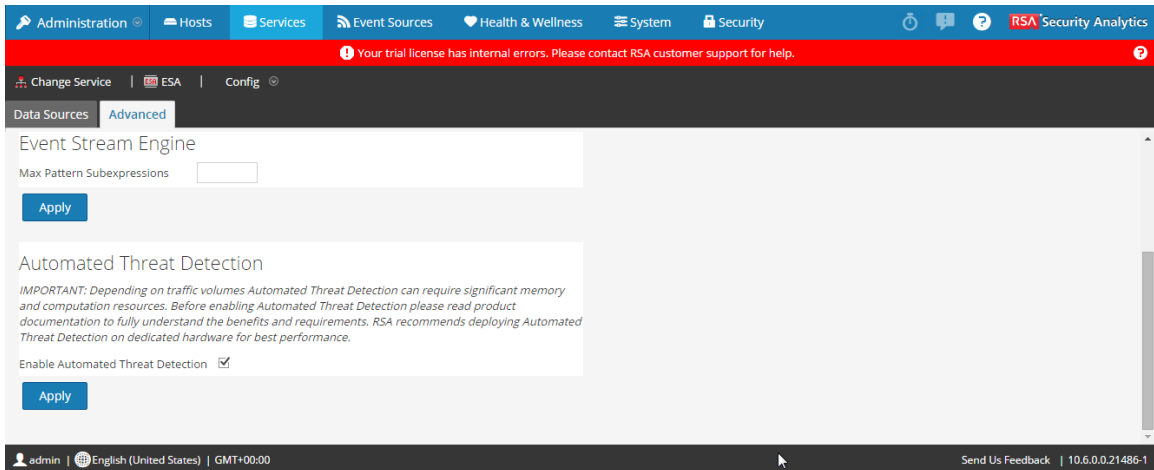


- i. Klicken Sie auf  und geben Sie den Domainnamen ein, um eine Domain hinzuzufügen.
- j. Wählen Sie die Domain aus und klicken Sie auf , um eine Domain zu entfernen.
- k. Um eine CSV-Datei zu importieren, klicken Sie auf  und navigieren Sie im Dialogfeld „Datei importieren“ zu der CSV-Datei. Wählen Sie eines der folgenden Trennzeichen aus: Durch Komma, LF (Zeilenvorschub) und CR (Wagenrücklauf), je nachdem, wie Sie die Werte in Ihrer Datei getrennt haben. Klicken Sie dann auf **Hochladen**.

**Hinweis:** Es ist wichtig, eine Whitelist vor der Aktivierung der automatisierten Bedrohungserkennung zu konfigurieren, um sicherzustellen, dass Domains auf der Whitelist sind, bevor die Bewertung der Bedrohungen beginnen.

### Schritt 3: Aktivieren Sie die automatisierte Bedrohungserkennung

1. Wählen Sie unter „Administration > Services“ Ihren ESA-Service aus und dann   > „Ansicht > Konfigurieren“.
2. Klicken Sie auf die Registerkarte „Erweitert“ und wählen Sie **Automatisierte Bedrohungserkennung aktivieren** aus und klicken Sie auf **Anwenden**.

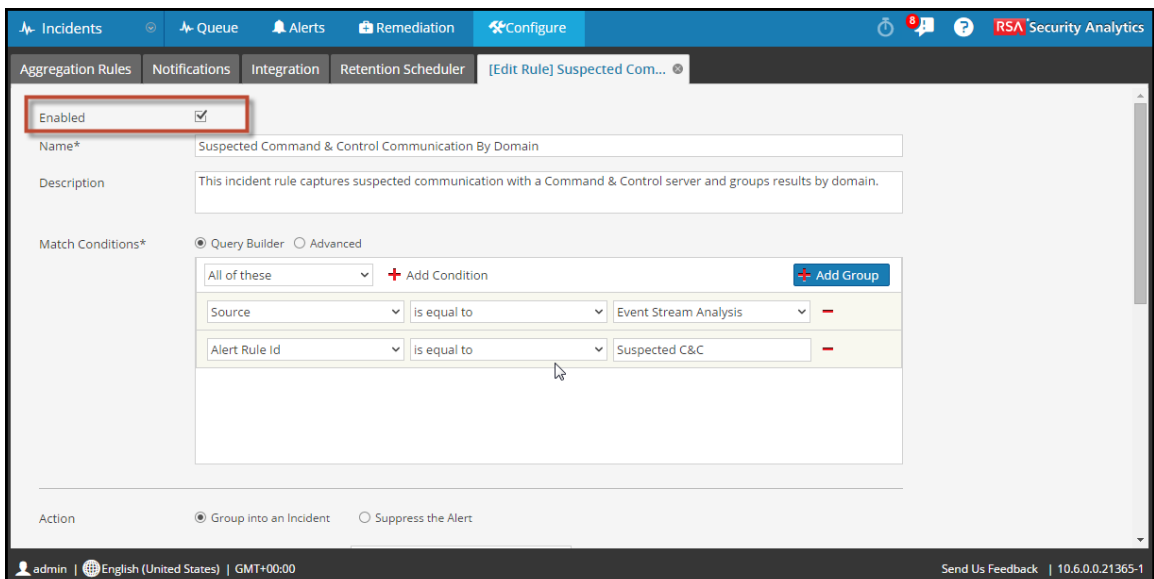


Die automatisierte Bedrohungserkennung ist jetzt auf Ihrem ausgewählten ESA-Service aktiviert.

#### Schritt 4: Aktivieren Sie die Regel für die C2-Erkennung auf dem Incident Manager

Aktivieren Sie die Regel für die C2-Erkennung auf dem **Incident Manager**.

1. Wählen Sie unter **Incidents > Konfigurieren** die Option **Aggregationsregeln** aus.
2. Wählen Sie die Regel **Verdacht auf Command-and-Control-Kommunikation von Domain** aus und doppelklicken Sie darauf, um sie zu öffnen.



3. Klicken Sie auf **Aktiviert** und klicken Sie auf **Speichern**.

Sobald sie aktiviert ist, zeigt die Regel eine grüne Schaltfläche „Aktiviert“ an.

## Ergebnis

Sobald Sie die automatisierte Bedrohungserkennung aktiviert haben, wird Ihr ESA-Service beginnen, den HTTP-Datenverkehr zu analysieren. Sie können detaillierte Informationen für jeden Incident in der Incident Management-Warteschlange anzeigen.

## Nächste Schritte

Nachdem Sie die Regel aktiviert haben, überwachen Sie den Incident Manager, um festzustellen, ob die Regel ausgelöst wird. Wenn die Regel ausgelöst wird, befolgen Sie die Schritte im folgenden Abschnitt, um die mit der ausgelösten Regel verknüpfte Domain zu untersuchen.

[Arbeiten mit Ergebnissen der automatisierten Bedrohungserkennung](#)

## Arbeiten mit Ergebnissen der automatisierten Bedrohungserkennung

In diesem Thema wird erläutert, wie Sie die Ergebnisse der automatisierten Bedrohungserkennung interpretieren und was Sie mit ihnen tun können.

Wenn Sie die Ergebnisse der automatisierten Bedrohungserkennung in Incident Manager anzeigen, gibt es eine Reihe verschiedener Faktoren, die verwendet werden, um die allgemeine Bewertung zu bestimmen. Dieser Abschnitt soll Ihnen helfen, besser zu verstehen, wie diese Bewertungen erzeugt werden und was sie bedeuten.

## Ergebnisse der Bedrohungserkennung verstehen

Wenn Sie mit der automatisierten Bedrohungserkennung arbeiten, werden mehrere Bewertungen zusammen aggregiert, um die Bewertung der Command-and-Control-Erkennung zu bestimmen. Damit Sie besser verstehen können, wie diese Bewertung zustande kommt, ist es empfehlenswert, die Elemente zu verstehen, die die endgültige Bewertung ausmachen.

Wenn Sie eine Warnmeldung über eine Command-and-Control-Erkennung erhalten, können Sie die folgende detaillierte Warnmeldungszusammenfassung im Incident Management-Modul anzeigen:

The screenshot displays the Incident Manager interface for a specific incident. The incident title is "INC-49: Suspected command and control communication with m1.4554mb.ru". The summary states: "SA detected communications with m1.4554mb.ru that may be malware command and control. 1. Evaluate if the domain is legitimate (online radio, news feed, partner, automated testing, etc.). 2. Review domain registration for suspect information (Registrar country, registrar, no)". The priority is "High", there are "147 Alerts", and the "Risk Score" is "50". The incident was created on "2015/12/18 05:12 (4 days ago)" and updated on "2015/12/18 05:12 (4 days ago)". The domain information section shows "Registration data not available". The assignee is "Unassigned" and the status is "New". The sources listed are "Event Stream Analysis". At the bottom, there are six numbered icons representing different factors: 1. Beacon Behavior, 2. Domain Age, 3. Expiring Domain, 4. Rare Domain, 5. No Referrers, and 6. Pure User Agent.



Jedes Symbol steht für eine andere Bewertung, die zusammen das berechnete Gesamtrisiko ausmachen. Beachten Sie, dass die Bewertungen gewichtet werden, so dass jede Bewertung einen anderen Anteil an der endgültigen Bewertung hat. Beispielsweise kann die Bewertung des Beacon-Verhaltens 20 % der endgültigen Bewertung ausmachen, und das Alter der Domain 5 % beitragen:

1. **Beacon-Verhalten.** Command-and-Control-Erkennung versucht, hochgradig regelmäßige periodische Verbindungen zu einer verdächtigen Domain zu finden, daher kommt es bei Beacon-Verhalten darauf an, wie regelmäßig die Quell-IP sich mit dem Domain-Server verbindet. Eine hohe Bewertung bedeutet, dass Verbindungen zwischen dieser Quell-IP und der Domain sehr regelmäßig sind.
2. **Domainalter.** Oft verwendet ein Command-and-Control-Server eine neue Domain, um Verbindungen herzustellen, d. h., wenn eine Domain neu im Netzwerk ist, bedeutet dies, dass es wahrscheinlicher eine Command-and-Control-Domain ist. Eine hohe Bewertung deutet darauf hin, dass die Domain relativ neu in diesem Netzwerk ist. Diese Bewertung wird aus dem Whois-Service abgeleitet. Wenn Ihr Whois-Service nicht funktioniert oder wenn ESA keine Verbindung zu ihm herstellen kann, wird das Symbol grau dargestellt. Wenn es ein Problem mit der Verbindung gibt oder der Whois-Service einen Nullwert oder einen Wert in einem unerwarteten Format zurückgibt, wird ein Standardwert verwendet, um diese Bewertung zu schätzen. Dies sorgt dafür, dass die allgemeine Bewertung genauer ist.
3. **Ablaufende Domain.** Oft verwendet ein Command-and-Control-Server eine ablaufende Domain, um Verbindungen herzustellen, sodass eine Domain, die bald ablaufen wird, mit höherer Wahrscheinlichkeit eine Command-and-Control-Domain ist. Diese Bewertung wird aus dem Whois-Service abgeleitet. Wenn Ihr Whois-Service nicht funktioniert oder wenn ESA keine Verbindung zu ihm herstellen kann, wird das Symbol grau dargestellt. Wenn es ein Problem mit der Verbindung gibt oder der Whois-Service einen Nullwert oder einen Wert in einem unerwarteten Format zurückgibt, wird ein Standardwert verwendet, um diese Bewertung zu schätzen. Dies sorgt dafür, dass die allgemeine Bewertung genauer ist.
4. **Seltene Domain.** Eine seltene Domain ist eine, mit der sich nur relativ wenige Quell-IP-Adressen in einem bestimmten Netzwerk in der letzten Woche verbunden haben. Wenn eine Domain nur selten verwendet wird, ist die Wahrscheinlichkeit höher, dass es eine Command-and-Control-Domain ist, als wenn es eine häufig verwendete legitime Domain ist wie *Google.com*.
5. **Ohne Referrer.** Ein Referrer ist ein HTTP-Feld, das die Adresse der Webseite identifiziert, die auf die angeforderte Ressource verweist. Zum Beispiel, wenn ich auf die Website meiner Bank über die Website meiner Arbeitsstelle zugreife, erscheint die Website meiner Arbeitsstelle als Referrer. Da eine Verbindung zu einer Website häufig über einen Referrer

erfolgt, bedeutet eine hohe Bewertung (d. h. ein geringer Prozentsatz der IP-Adressen, die sich mit dieser Domain verbinden, haben Referrer verwendet), dass eine Command-and-Control-Kommunikation wahrscheinlicher ist.

6. **Seltener User-Agent.** Benutzeragenten identifizieren die Clientsoftware, von der die Anforderung stammt. Eine hohe Bewertung zeigt an, dass der mit der IP-Adresse assoziierte Benutzeragent nicht häufig verwendet wird. Ebenso wie die Bewertung der seltenen Domain bedeutet ein ungewöhnlicher Benutzeragent eine höhere Wahrscheinlichkeit für eine Command-and-Control-Domain.

Die Symbole werden in verschiedenen Farben angezeigt und die Farben helfen bei der Visualisierung der Risikostufe. Details entnehmen Sie der nachfolgenden Tabelle.

Symbol	Bedeutung
Grau 	Es wurde keine Bewertung erzeugt, da keine Daten verfügbar waren. Das kann passieren, wenn der Whois-Service deaktiviert ist oder keine Daten verfügbar sind, um eine bestimmte Bewertung zu erzeugen.
Schwarz 	Der Bewertungsindikator ist schwach.
Orange 	Der Bewertungsindikator ist moderat.
Rot 	Der Bewertungsindikator ist hoch.

## Was als nächstes zu tun ist

Es gibt drei mögliche Aktionspfade, nachdem Sie die Bedrohungsbewertungen gesehen haben:

- **Drill-down für weitere Informationen.** Für jede Bewertung gibt es mehrere Faktoren, die diese Bewertung ausmachen. Sie können diese Details auf der Seite **Ereignisdetails** anzeigen.
- **Untersuchen der Domäne im Modul „Investigation“.** Sie können auf dem Bildschirm „Investigations“ weitere Details über die Domain und die zugehörigen Incidents erfahren.
- **Hinzufügen von Domains zu einer Whitelist.** Wenn Sie sich die Details ansehen und feststellen, dass die betreffende Domain keine Bedrohung darstellt, ist es empfehlenswert, sie zu einer Whitelist hinzuzufügen. Dadurch wird sichergestellt, dass die Domain keine Bewertung der Bedrohungserkennung mehr auslöst, und es hilft dabei, die Genauigkeit der Bewertung zu optimieren.

### Drill-Down in die Bewertungen für weitere Informationen

Jede Ereignisbewertung wird durch Daten erweitert, damit Sie leichter feststellen können, ob die Kommunikation mit der Domain Schadsoftware ist, sowie in einem solchen Fall den Schweregrad des Angriffs. Für jede der oben aufgeführten Bewertungen gibt es weitere Details, die in den Details für jedes Ereignis enthalten sind.

So greifen Sie auf diese Details zu:

1. Doppelklicken Sie in der Warteschlange **Incidents** auf einen Incident, um die **Incident-Details** anzuzeigen.
2. Doppelklicken Sie im Abschnitt **Warnmeldungsdetails** auf eine Warnmeldung.
3. Die Seite **Ereignisdetails** wird geöffnet.

Von dort können Sie Details für das Ereignis anzeigen. Wenn Sie mit der Maus über jedes einzelne Detail fahren, wird Text angezeigt, der Ihnen hilft, die Daten zu interpretieren. Sie können Details anzeigen wie den Bewertungsbereich, die Anzahl der Vorkommnisse für jede Bewertung, den Beaconing-Zeitraum, die aus den Whois-Registrierungsdaten verfügbaren Informationen usw.


Z. B. können Sie aus den folgenden Ereignisdetails ersehen, dass die Bewertung für „Seltene Domain“ 100 war (die höchste Bewertung), aber dass nur eine IP-Adresse dieser Domäne zugeordnet war und dass es 24 Vorkommnisse in der vorherigen Woche gab.

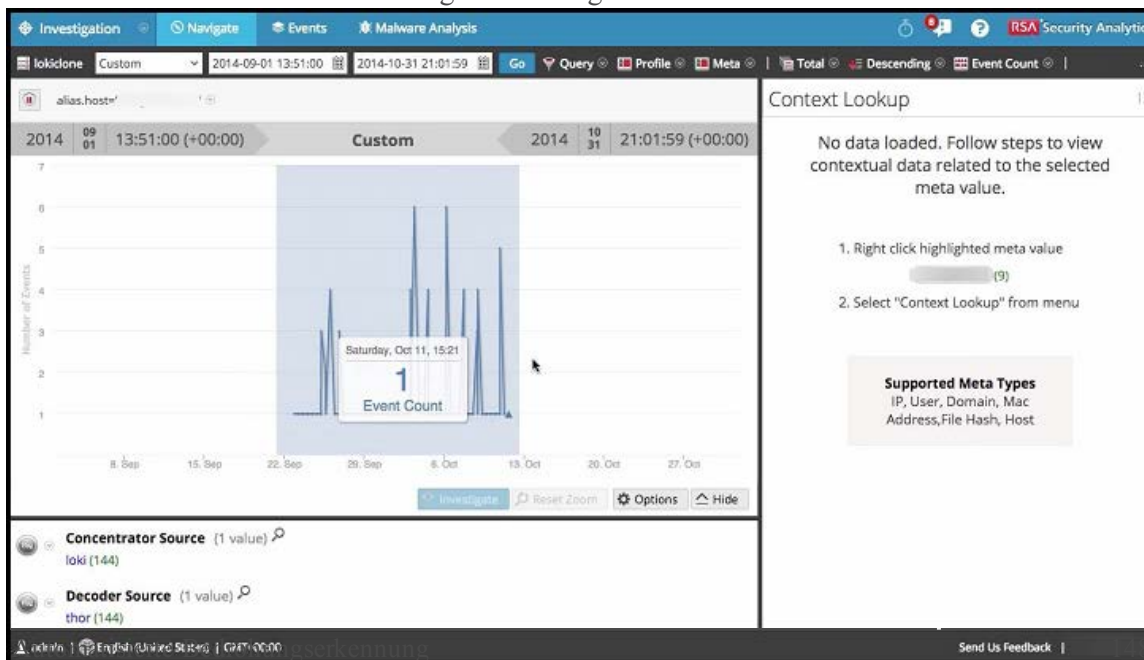
Event Details -- 2015/12/21 00:56

	Contribution of No Domain Referrer Score:	4
	Contribution of Rare User Agent Score:	4
<b>Beacon Behavior Indicator</b>	Beaconing Score:	97.93435439256842
	Beaconing Period:	35350
<b>Domain Age Indicator</b>	Domain Age Score (This Network):	100
	Domain Age (This Network):	564000
<b>Expiring Domain Indicator</b>	No domain registration data available	
<b>Rare Domain Indicator</b>	Rare Domain Score (This Network):	100
	IPs Associated With The Domain:	1
	Occurrences in the last week:	24
<b>No Referers Indicator</b>	No Referers Score:	100
	IPs With No Referrer:	1
	Percentage of IPs With No Referrer:	100
	Occurrences in the last week:	24
<b>Rare User Agent Indicator</b>	Rare User Agent Score:	100
	IPs With Rare User Agent:	1
	Percentage of IPs With Rare User Agent:	100
	Occurrences in the last week:	24

Close

### Untersuchen der Domäne im Modul „Investigation“

Von den Warmmeldungsdetails aus können Sie auch das Modul „Investigation“ öffnen, um einen Drill-down in die Details der Domain durchzuführen. Um dies zu erreichen, klicken Sie in den **Warmmeldungsdetails** auf  > **Zieldomain ermitteln**. Von dort aus können Sie die Tage rund um das Ereignis durchsuchen, um zu sehen, was möglicherweise sonst noch passiert ist, und um andere Details über das Ereignis anzuzeigen.





## Reduzieren falsch positiver Ergebnisse

Manchmal kann eine Domain, auf die Sie regelmäßig zugreifen, eine Bewertung der automatisierten Bedrohungserkennung auslösen. Beispielsweise könnte ein Wetterdienst das gleiche Beaconing-Verhalten zeigen wie eine Command-and-Control-Kommunikation und so eine nicht gerechtfertigte negative Bewertung auslösen. Ein solches Ereignis wird als falsch positiv bezeichnet. Wenn Sie nach der Untersuchung des Ereignisses feststellen, dass es sich um eine falsch positives handelt, können Sie es als falsch positiv kennzeichnen. Dadurch wird die Domain zu einer Whitelist hinzugefügt. Sobald die Domain zu der Whitelist hinzugefügt wurde, wird sie keine Bewertung für die automatisierte Bedrohungserkennung mehr auslösen.

**Hinweis:** Wenn Sie SecOps oder eine andere Ticketing-Lösung verwenden, können Sie mithilfe des Context Hub-Services „Domains“ manuell zur Whitelist hinzufügen. Siehe „Schritt 2: Konfigurieren einer Whitelist“ in [Konfigurieren der automatisierten Bedrohungserkennung](#).

## Verfahren

1. Auf der Seite **Incidents-Detail** können Sie einen bestimmten Incident als falsch positiv markieren, wodurch er automatisch zur Whitelist hinzugefügt wird.
  1. Wählen Sie vom **Incident-Manager** aus den Incident aus, der eine falsch positive Bewertung ausgelöst hat. Klicken Sie auf   > **Incident bearbeiten**.  
Das Dialogfeld **Incident bearbeiten** wird angezeigt.
  2. Klicken Sie im Dialogfeld **Incident bearbeiten** auf das Feld **Status** und wählen Sie *Geschlossen – falsch positives Ergebnis* aus. Dadurch wird die Domain der Whitelist hinzugefügt und der Incident geschlossen. Sobald die Domain zu der Whitelist hinzugefügt wurde, wird sie bei der Bewertung für die automatisierte Bedrohungserkennung ignoriert.


## Troubleshooting der automatisierten Bedrohungserkennung

Die automatisierte Bedrohungserkennung ist eine Analyse-Engine, die Ihre HTTP-Daten untersucht. Sie verwendet auch andere Komponenten, wie etwa die Services „WhoIs“ und „Context Hub“, die Ihre Installation komplexer machen können. Dieses Thema enthält Vorschläge zum Auffinden von Problemen, wenn Ihre Bereitstellung der automatisierten Bedrohungserkennung nicht die Ergebnisse liefert, die Sie erwarten.

Beim Troubleshooting der automatisierten Bedrohungserkennung ist es wichtig, den verwendeten Modus zu berücksichtigen. Wenn der gemischte Modus verwendet wird (automatisierte Bedrohungserkennung auf dem gleichen Rechner aktiviert wie ESA-Regeln oder Context Hub), müssen Sie die Gesamtnutzung von Arbeitsspeicher und I/O dieser Anwendungen beim Troubleshooting berücksichtigen. Im Allgemeinen wird bei der Konfiguration der Installation im gemischten Modus die automatisierte Bedrohungserkennung so eingerichtet, dass sie ca. 50 Prozent des verfügbaren Speichers nutzt, während die Speichernutzung der ESA-Regeln unbegrenzt ist. Sie sollten daher in einem ersten Schritt Ihre ESA-Regeln überprüfen, wenn Sie ein Troubleshooting im gemischten Modus durchführen.

Wenn Sie den gemischten Modus verwenden, sollten Sie auch berücksichtigen, ob der ESA-Service für Speicherpools oder für Ordnen nach Ereigniszeit konfiguriert wurde. Speicherpools können sich auf die Performance auswirken, während das Ordnen nach Ereigniszeit sich auf Performance und Speichernutzung auswirken kann.

## **Mögliche Probleme**

Problem	Mögliche Ursachen	Lösungen
<p>Ich erhalte zu viele Warnmeldungen (falsch positive Ergebnisse).</p>	<p>Verschiedene</p>	<p>Eine mögliche Ursache ist, dass die Whois-Abfrage fehlgeschlagen oder nicht konfiguriert ist. Die Whois-Abfrage ist hilfreich bei der Ermittlung, ob eine URL gültig ist, und wenn die Verbindung fehlschlägt oder nicht ordnungsgemäß konfiguriert ist, kann es zu falsch positiven Ergebnissen kommen.</p> <p>Es gibt eine Reihe von Zählern für den Whois-Abfrageservice, die Sie anzeigen können.</p> <ol style="list-style-type: none"> <li>1. Wählen Sie unter „Administration &gt; Services“ Ihren ESA-Service und dann  &gt; „Ansicht &gt; Durchsuchen“ aus.</li> <li>2. Klicken Sie im Explorer auf <b>Service &gt; Whois &gt; whoisClient</b>.</li> </ol> <p>Nachfolgend finden Sie einige nützliche zu prüfende Zähler:</p> <ul style="list-style-type: none"> <li>• <b>FailedLookupCount:</b> Wann immer eine Anforderung an den RSA Whois-Service für Whois-Daten fehlschlägt, wird dieser Zähler erhöht.</li> <li>• <b>LookupQueueFailureCount:</b> Dieser Zähler zählt jeden fehlgeschlagenen Versuch, einen Eintrag dem Cache hinzuzufügen. Diese Fehler erfolgen aufgrund von internen Fehlern im Cache.</li> <li>• <b>Response401Count:</b> Dieser Zähler zählt die Anforderungen an den RSA Whois-Server, die mit einem Statuscode 401 fehlschlagen. Anfragen mit abgelaufenen Authentifizierungstoken sind in dieser Anzahl enthalten. Diese Anzahl ist enthalten in <b>FailedLookupCount</b>.</li> </ul>



Problem	Mögliche Ursachen	Lösungen
		<p>Sie müssen eventuell URLs zur Whitelist hinzufügen. Manchmal löst das legitime Verhalten für eine URL eine Warnmeldung aus. Eine Möglichkeit, dies zu verhindern, besteht darin, die URL zur Whitelist hinzuzufügen. Weitere Anweisungen finden Sie unter „Reduzieren falsch positiver Ergebnisse“ in <a href="#">Arbeiten mit Ergebnissen der automatisierten Bedrohungserkennung</a>.</p>
<p>Ich sehe keine Warnmeldungen.</p>	<p>Der ESA-Service erfordert eine Aufwärmphase von 24 Stunden, wenn Sie die automatisierte Bedrohungserkennung aktivieren.</p>	<p>Wenn Sie die automatisierte Bedrohungserkennung aktivieren, gibt es eine Aufwärmphase, während der keine Warnmeldungen angezeigt werden. Die Standardzeitdauer beträgt 24 Stunden. Nach dieser Lernphase von 24 Stunden können Warnmeldungen angezeigt werden. Wenn der ESA-Service neu gestartet wird, beginnt diese Lernphase erneut, somit wird die Wartezeit von 24 Stunden zurückgesetzt.</p>
<p>Ich sehe Performanceprobleme (es werden mehr Ressourcen verbraucht oder der Durchsatz geht zurück).</p>	<p>Verschiedene</p>	<p>Wenn Sie Performanceprobleme bei einem ESA-Service haben, der auch ESA-Regeln ausführt, befolgen Sie die Schritte zum Troubleshooting für Regeln. ESA-Regeln sind unbegrenzt, während die automatisierte Bedrohungserkennung so konfiguriert ist, dass eine bestimmte Menge der Ressourcen (gewöhnlich ca. 50 %) genutzt werden. Gehen Sie für diese Troubleshooting-Schritte zu <a href="#">Troubleshooting für ESA</a>.</p>



## Referenzen

---

Das Modul Alerting dient zur Konfiguration und Bereitstellung von ESA-Regeln, die Sie über potenzielle Netzwerkbedrohungen informieren.

In diesen Themen wird die Benutzeroberfläche des Moduls Alerting erläutert.

- [Registerkarte „Neue erweiterte EPL-Regel“](#)
- [Ansicht Zusammenfassung der Warnmeldungen](#)
- [Dialogfeld „Anweisung erstellen“](#)
- [Dialogfeld „ESA-Regeln bereitstellen“](#)
- [Dialogfeld „ESA-Services bereitstellen“](#)
- [Registerkarte Regelerstellung](#)
- [Registerkarte Regeln](#)
- [Dialogfeld Regelsyntax](#)
- [Dialogfeld „ESA-Service auswählen“](#)
- [Registerkarte Services](#)
- [Registerkarte „Einstellungen“](#)
- [Dialogfeld „Aktualisierungen an der Bereitstellung“](#)

### Registerkarte „Neue erweiterte EPL-Regel“

In diesem Thema wird die Registerkarte Erweiterte EPL-Regel beschrieben, die zur Definition von Regelkriterien mit einer EPL-Abfrage (Event Processing Language) verwendet wird.

So greifen Sie auf die Registerkarte Erweiterte EPL-Regel zu:

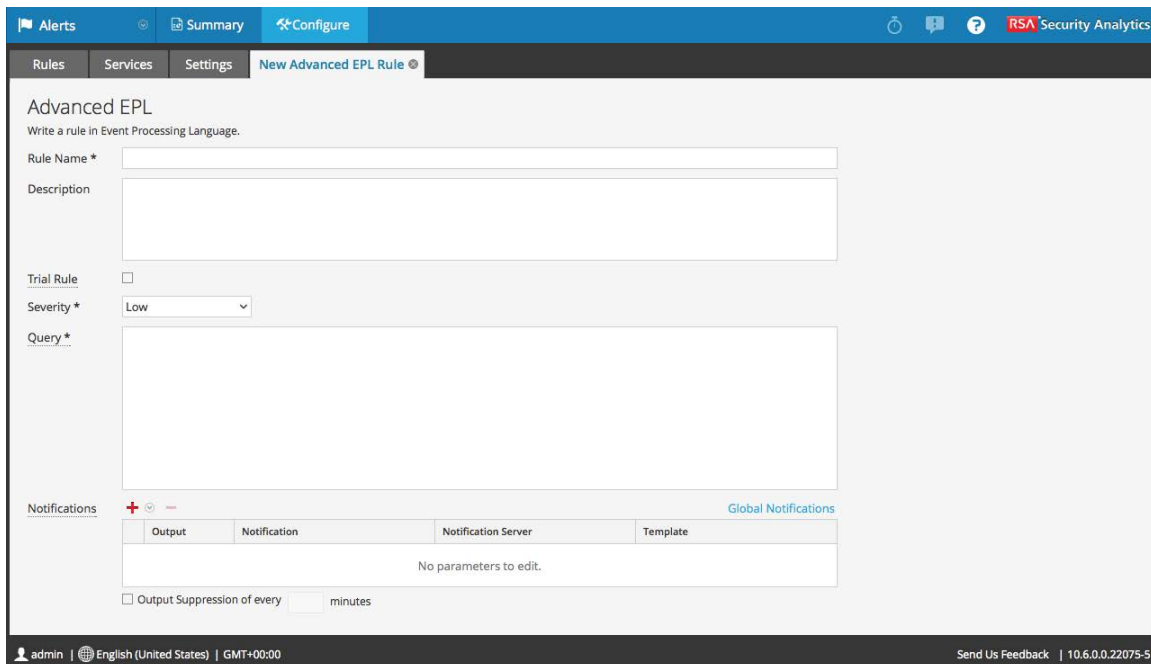
1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

Die Ansicht Konfigurieren wird standardmäßig mit geöffneter Registerkarte Regeln angezeigt.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Option   > **Erweiterte EPL** aus.

Die Registerkarte Erweiterte EPL-Regel wird angezeigt.

Unten sehen Sie einen Screenshot der Registerkarte Erweiterte EPL-Regel.



## Funktionen

In der folgenden Tabelle sind die Parameter der Registerkarte Erweiterte EPL-Regel aufgeführt.

Parameter	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
Abfrage	EPL-Abfrage, die die Regelkriterien definiert

## Benachrichtigungen

Im Abschnitt Benachrichtigungen können Sie auswählen, wie Sie benachrichtigt werden, wenn ESA eine Warnmeldung für die Regel erzeugt.

Weitere Informationen über Warnmeldungsbenachrichtigungen erhalten Sie unter [Hinzufügen einer Benachrichtigungsmethode zu einer Regel](#).

Die folgende Abbildung zeigt den Abschnitt Benachrichtigungen.

Notifications [Global Notifications](#)

Output	Notification	Notification Server	Template
<input checked="" type="checkbox"/> SYSLOG	Local_SysLog	localhost-514	Default Syslog Template

Output Suppression of every  minutes

Parameter	Beschreibung
<b>+</b>	So fügen Sie einen Warnmeldungsbenachrichtigungstyp hinzu.
<b>-</b>	So löschen Sie den ausgewählten Warnmeldungsbenachrichtigungstyp.
Ausgabe	Typ der Warnmeldungsbenachrichtigung Optionen: <ul style="list-style-type: none"> <li>• E-Mail</li> <li>• SNMP</li> <li>• Syslog</li> <li>• Skript</li> </ul>
Benachrichtigung	Name der zuvor konfigurierten Ausgabe, beispielsweise ein E-Mail-Verteiler
Benachrichtigungsserver	Name des die Ausgabe sendenden Servers
Vorlage	Name der Vorlage für die Warnmeldungsbenachrichtigung
Ausgabeunterdrückung alle	Option zur Spezifizierung der Warnmeldungshäufigkeit
Minuten	Warnmeldungshäufigkeit in Minuten

### Erweiterung

Im Abschnitt Erweiterung können Sie einer Regel eine Datenerweiterungsquelle hinzufügen.

Weitere Informationen über Erweiterungen erhalten Sie unter [Hinzufügen einer Erweiterung zu einer Regel](#).

In der folgenden Abbildung wird der Abschnitt Erweiterungen dargestellt.

Enrichments <span style="float: right;">Settings</span>			
Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/> In-Memory Table	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/> Warehouse Analytics	Select Enrichment Source	Enter Meta	key
<input type="checkbox"/> GeoIP	Select Enrichment Source	Enter Meta	ipv4

Parameter	Beschreibung
<b>+</b>	So fügen Sie eine Erweiterung hinzu.
<b>-</b>	So löschen Sie eine ausgewählte Erweiterung.
Ausgabe	Erweiterungsquellentyp Optionen: <ul style="list-style-type: none"> <li>• In-Memory-Tabelle</li> <li>• Externer DB-Verweis</li> <li>• Warehouse Analytics</li> <li>• GeoIP</li> </ul>
Erweiterungsquelle	Name der zuvor konfigurierten Erweiterungsquelle, z. B. ein .CSV-Dateiname einer In-Memory-Tabelle
ESA Ereignis-Stream-Metadaten	ESA-Metaschlüssel, der als ein Operand der Verknüpfungsbedingung verwendet wird
Spaltenname „Erweiterungsquelle“	Erweiterungsquellen-Spaltenname, dessen Wert als ein weiterer Operand der Verknüpfungsbedingung verwendet wird

## Ansicht Zusammenfassung der Warnmeldungen

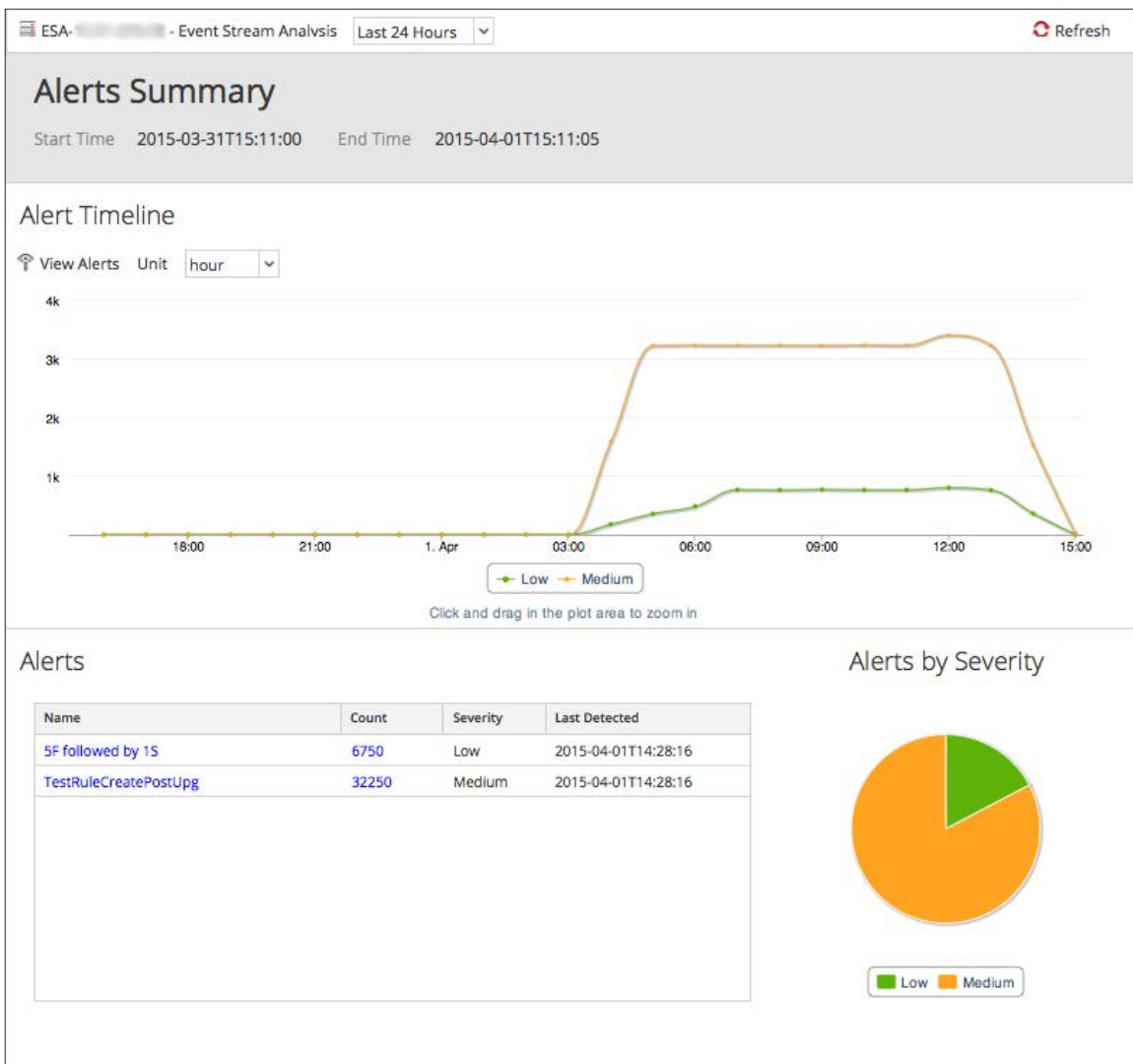
Die Ansicht „Zusammenfassung der Warnmeldungen“ zeigt eine konsolidierte Ansicht aller Warnmeldungen, die in einem bestimmten Zeitraum erzeugt werden. Sie können einen Zeitraum angeben und Warnmeldungen als grafische Darstellung, als Diagramm oder in Tabellenform darstellen. Wenn Sie zum Beispiel anzeigen möchten, wie viele Warnmeldungen mit einem niedrigen, mittleren oder hohen Schweregrad in einem bestimmten Zeitraum erzeugt werden, können Sie für eine deutlichere Darstellung ein Diagramm verwenden. Sie können auch die Anzahl von Warnmeldungen anzeigen, die in einer bestimmten Minute bzw. Stunde oder an einem bestimmten Tag erzeugt werden.

Bei weiteren Drill-downs zeigt die Ansicht auch Ereignismetadaten und Ereignisdetails zu jeder erzeugten Warnmeldung.

**Hinweis:** Die in der Benutzeroberfläche (UI) angezeigte Uhrzeit und das angezeigte Datum hängen vom Zeitzonenprofil ab, das vom Benutzer ausgewählt wurde.

Die Ansicht „Zusammenfassung der Warnmeldungen“ wird in Security Analytics angezeigt, wenn Sie zu **Warnmeldungen > Zusammenfassung** navigieren und einen ESA-Service auswählen.

In der folgenden Abbildung sind die verschiedenen Komponenten der Ansicht „Zusammenfassung der Warnmeldungen“ dargestellt.



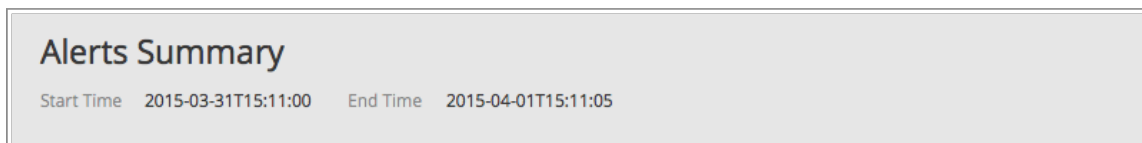
## Funktionen

Die Ansicht „Zusammenfassung der Warnmeldungen“ enthält die folgenden Abschnitte:

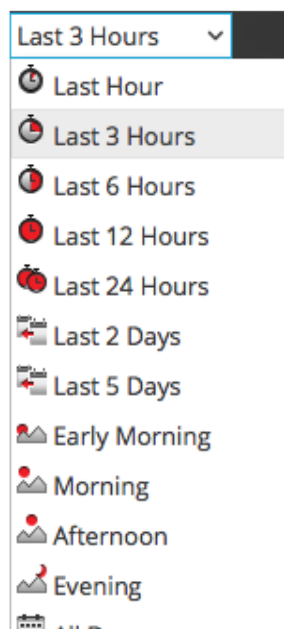
- Zusammenfassung der Warnmeldungen
- Warnmeldungszeitachse
- Warnmeldungen
- Warnmeldungen nach Schweregrad

### Zusammenfassung der Warnmeldungen

Im Abschnitt „Zusammenfassung der Warnmeldungen“ wird der Zeitraum angezeigt, in dem Warnmeldungen erzeugt werden. In der folgenden Abbildung ist der Abschnitt „Zusammenfassung der Warnmeldungen“ dargestellt.



Im oberen linken Bereich des Abschnitts wird der ausgewählte ESA-Service angezeigt. Sie können einen Zeitraum auswählen, für den Warnmeldungen angezeigt werden sollen. In der folgenden Abbildung sind einige der verfügbaren Optionen zu sehen.

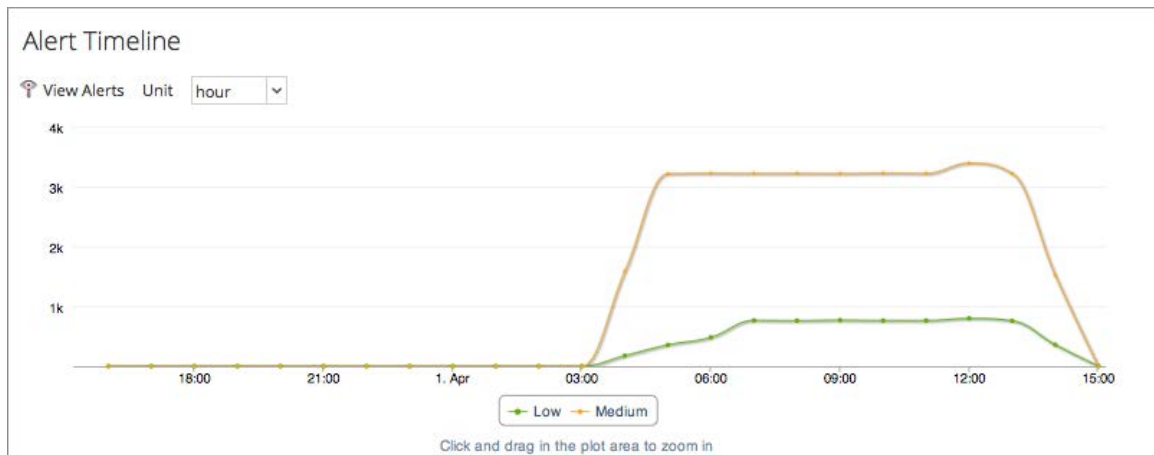


In diesem Abschnitt wird die Start- und Endzeit basierend auf dem ausgewählten Zeitraum angezeigt.

### Warnmeldungszeitachse

Der Abschnitt „Warnmeldungszeitachse“ enthält eine grafische Darstellung der in einem bestimmten Zeitraum erzeugten Warnmeldungen. In der folgenden Abbildung wird der Abschnitt „Warnmeldungszeitachse“ dargestellt.





Im Abschnitt „Warnmeldungszeitachse“ können Sie folgende Aktionen durchführen:

- Anzeigen der in einer bestimmten Minute bzw. Stunde oder an einem bestimmten Tag erzeugten Warnmeldungen durch Auswählen der gewünschten Option in der Drop-down-Liste neben **Einheit**.
- Anzeigen der Details zu jeder erzeugten Warnmeldung durch Klicken auf die Option **Warnmeldungen anzeigen**.
- Anzeigen der Anzahl von erzeugten Warnmeldungen, des Schweregrads und des Zeitpunkts, an dem sie erzeugt wurden, indem die Maus über einen bestimmten Punkt in der grafischen Darstellung bewegt wird.

**Hinweis:** Sie können auch auf die in der Warnmeldungszeitachse angegebene Legende klicken und die Warnmeldungen nach dem **Schweregrad** anzeigen. Des Weiteren können Sie auch in den Zeichenbereich klicken und ihn ziehen, um ihn zu vergrößern und Daten anzuzeigen.

## Warnmeldungen

Im Abschnitt „Warnmeldungen“ werden die in einem bestimmten Zeitraum erzeugten Warnmeldungen in Tabellenform angezeigt. In der folgenden Abbildung wird der Abschnitt „Warnmeldungen“ dargestellt.

Alerts

Name	Count	Severity	Last Detected
<a href="#">test</a>	19057	Low	2015-03-31T13:05:49
<a href="#">User login from multiple geos over VPN wit...</a>	5	Medium	2015-03-30T11:20:12
<a href="#">ADActivity</a>	40	Low	2015-03-31T09:37:00
<a href="#">5F followed by 1S</a>	10994	Low	2015-04-01T14:28:16
<a href="#">TestRuleCreatePostUpg</a>	42544	Medium	2015-04-01T14:28:16

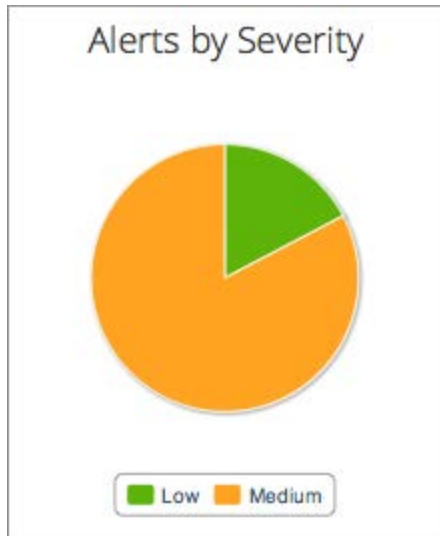
In der folgenden Tabelle werden die verschiedenen Spalten im Abschnitt „Warnmeldungen“ und die zugehörigen Beschreibungen aufgeführt:

Spalte	Beschreibung
Name	Der zur Identifizierung der Warnmeldung verwendete Name
Count	Die Anzahl des Auftretens von Warnmeldungen
Schweregrad	Der Schweregrad für die Warnmeldung
Zuletzt erkannt	Der letzte Zeitpunkt, an dem die Warnmeldung erkannt wurde

Sie können die Details zu jeder erzeugten Warnmeldung durch Klicken auf die gewünschte Warnmeldung einsehen und auch die Protokolle zum jeweiligen Ereignis in der Warnmeldung exportieren.

### Warnmeldungen nach Schweregrad

Der Abschnitt „Warnmeldungen nach Schweregrad“ enthält eine grafische Darstellung der Warnmeldungen nach Schweregrad. In der folgenden Abbildung ist der Abschnitt „Warnmeldungen nach Schweregrad“ dargestellt.



Sie können die Details zu den erzeugten Warnmeldungen durch Klicken in das Diagramm einsehen.

## Dialogfeld „Anweisung erstellen“

Das Dialogfeld Anweisung erstellen ermöglicht das Zusammenstellen einer Bedingungsanweisung, wenn eine neue Regelerstellungsregel erstellt wird.

So greifen Sie auf das Dialogfeld Anweisung erstellen zu:

1. Wählen Sie im Menü Security Analytics die Optionen **Warnmeldungen > Konfigurieren** aus.

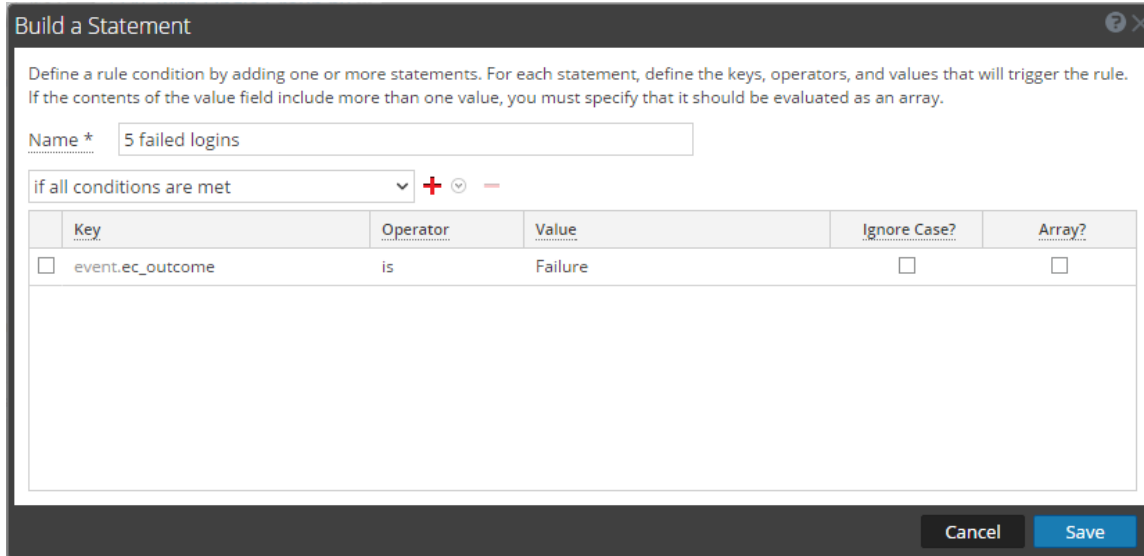
Die Ansicht Konfigurieren wird mit geöffneter Registerkarte Regeln angezeigt.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Optionen   > **Regelerstellung** aus.

Die Registerkarte „Neue Regel“ wird in Security Analytics angezeigt.

3. Klicken Sie im Abschnitt **Bedingungen** auf  .



Die Ansicht Anweisung erstellen wird angezeigt.



## Funktionen

In der folgenden Tabelle werden die Parameter im Dialogfeld Anweisung erstellen beschrieben.

Parameter	Beschreibung
Name	Zweck der Anweisung
Auswählen	Bedingungen, die die Regel erfordert Es gibt zwei Optionen: <ul style="list-style-type: none"> <li>• Alle Bedingungen sind erfüllt</li> <li>• Keine der Bedingungen ist erfüllt</li> </ul>
Schlüssel	Schlüssel, den ESA in der Regelnweisung überprüfen soll

Parameter	Beschreibung
Evaluierungstyp	<p>Beziehung zwischen dem Metaschlüssel und dem Wert für den Schlüssel:</p> <ul style="list-style-type: none"> <li>• is</li> <li>• ist nicht</li> <li>• ist nicht null</li> <li>• ist größer als (&gt;)</li> <li>• ist größer als oder gleich (&gt;=)</li> <li>• ist kleiner als (&lt;)</li> <li>• ist kleiner als oder gleich (&lt;=)</li> <li>• enthält</li> <li>• enthält nicht</li> <li>• beginnt mit</li> <li>• endet in</li> </ul>
Wert	Wert, nach dem ESA in dem Schlüssel sucht
Groß-/Kleinschreibung ignorieren?	<p>Dieses Feld wurde für die Verwendung mit Zeichenfolgen- und Array-von-Zeichenfolgenwerten entworfen. Indem Sie das Feld <b>Groß-/Kleinschreibung ignorieren</b> auswählen, wird die Abfrage den ganzen Text der Zeichenfolge als Wert in Kleinbuchstaben behandeln. Dadurch wird sichergestellt, dass eine Regel, die nach einem Benutzer namens „Johnson“ sucht, Ereignisse auch dann findet, wenn sie „johnson“, „JOHNSON“ oder „JoHnSoN“ enthalten.</p>
Array?	<p>Auswahl zur Angabe, ob die Inhalte des Felds Wert für einen oder mehrere Werte stehen:</p> <ul style="list-style-type: none"> <li>• Aktivieren Sie das Kontrollkästchen, wenn mehrere Werte angegeben werden.</li> <li>• Deaktivieren Sie das Kontrollkästchen, wenn nur ein Wert angegeben wird.</li> </ul>
	Fügt eine Anweisung hinzu Sie können ein Metabedingung, eine Whitelist-Bedingung oder eine Blacklist-Bedingung hinzufügen.
	Löscht die ausgewählte Anweisung

Parameter	Beschreibung
Speichern	Fügt eine Anweisung zum Abschnitt Bedingungen der Registerkarte Regelerstellung hinzu.

Die folgende Tabelle zeigt die Operatoren, die Sie bei der Regelerstellung verwenden können:

Operator	Erforderlicher Wert	Verwendung	Beispiel	Bedeutung
is	Einzelne-Zeichenfolge-Wert	Der Metaschlüssel entspricht dem Feld <i>Wert</i> .	<i>user_dst</i> ist „John Doe“.	<i>user_dst</i> ist gleich der Zeichenfolge „John Doe“.
is	Array-Zeichenfolge-Wert	Der Metaschlüssel ist gleich einem der Elemente des Felds <i>Wert</i> .	<i>user_dst</i> ist „John Doe“, „Smith“.	<i>user_dst</i> ist entweder gleich der Zeichenfolge „John“ oder der Zeichenfolge „Doe“ oder der Zeichenfolge „Smith“ (beachten Sie, dass die Leerzeichen entfernt werden).
ist nicht	Einzelne-Zeichenfolge-Wert	Der Metaschlüssel entspricht dem Feld <i>Wert</i> nicht.	<i>size</i> ist nicht 200.	<i>Größe</i> ist nicht gleich der Anzahl 200 („Größe“ ist ein numerischer Wert).
ist nicht	Array-Zeichenfolge-Wert	Der Metaschlüssel ist nicht gleich einem der Elemente des Felds <i>Wert</i> .	<i>size</i> ist nicht 200, 300, 400.	<i>Größe</i> ist weder gleich 200 noch gleich 300 noch gleich 400.
ist nicht null	– (sucht nach jedem Wert)	Der Metaschlüsselwert ist nicht null.	<i>user_dst</i> ist nicht null.	<i>user_dst</i> ist ein Metadatum, das einen Wert enthält.
ist größer als (>)	Nummer	Der numerische Wert des Metaschlüssels ist größer als die Anzahl im Feld <i>Wert</i> .	<i>payload</i> ist größer als 7000.	<i>payload</i> ist ein numerischer Wert, der größer als 7000 ist.
ist größer als oder gleich (>=)	Nummer	Der numerische Wert des Metaschlüssels ist größer als oder gleich der Anzahl im Feld <i>Wert</i> .	<i>payload</i> ist größer als oder gleich 7000.	<i>payload</i> ist ein numerischer Wert, der größer als oder gleich 7000 ist.
ist kleiner als (<)	Nummer	Der numerische Wert des Metaschlüssels ist kleiner als die Anzahl im Feld <i>Wert</i> .	<i>ip_dstport</i> ist kleiner als 1024.	<i>ip_dstport</i> ist ein numerischer Wert, der kleiner ist als der numerische Wert 1024.


Operator	Erforderlicher Wert	Verwendung	Beispiel	Bedeutung
ist kleiner als oder gleich ( $\leq$ )	Nummer	Der numerische Wert des Metaschlüssels ist kleiner als oder gleich der Anzahl im Feld <i>Wert</i> .	<i>ip_dstport</i> ist kleiner als oder gleich 1024.	<i>ip_dstport</i> ist ein numerischer Wert, der kleiner als oder gleich dem numerischen Wert 1024 ist.
enthält	Zeichenfolge	Das Feld <i>Wert</i> ist eine Teilzeichenfolge des Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	<i>ec_outcome</i> enthält „failure“.	<i>ec_outcome</i> ist eine Zeichenfolge, die die Teilzeichenfolge „failure“ enthält.
enthält nicht	Zeichenfolge	Das Feld <i>Wert</i> ist nicht eine Teilzeichenfolge des Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	<i>ec_outcome</i> enthält nicht „failure“.	<i>ec_outcome</i> ist eine Zeichenfolge, die nicht die Teilzeichenfolge „failure“ enthält.
beginnt mit	Zeichenfolge	Das Feld <i>Wert</i> ist der Anfang eines Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	<i>ip_dst</i> beginnt mit 127.0.	<i>ip_dst</i> ist eine Zeichenfolge, die mit „127.0“ beginnt.
endet in	Zeichenfolge	Das Feld <i>Wert</i> ist das Ende eines Metaschlüssels (dieser Operator ist nur verfügbar für einen Metaschlüssel mit Zeichenfolgenwert).	<i>user_dst</i> endet auf „son“.	<i>user_dst</i> ist eine Zeichenfolge, die auf „son“ endet.

Hinweis: Ausdrücke in *fett kursiv* sind Metadaten, die möglicherweise nicht in allen Kundenumgebungen vorhanden sind.

## Dialogfeld „ESA-Regeln bereitstellen“

Im Dialogfeld ESA-Regeln bereitstellen können Sie Regeln für die Bereitstellung eines ESA-Services filtern und auswählen.

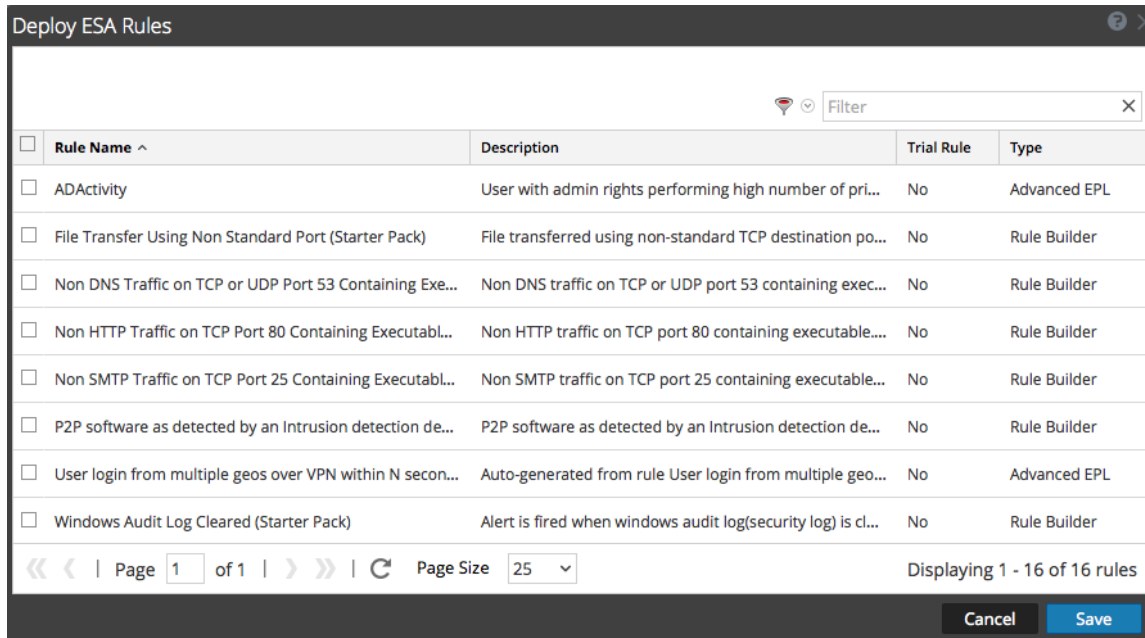
So rufen Sie dieses Dialogfeld auf:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.  
Die Registerkarte Regeln wird standardmäßig angezeigt.
2. Wählen Sie im Bereich „Optionen“ im Abschnitt **Bereitstellung** eine neue Bereitstellung aus, oder fügen Sie eine neue hinzu, indem Sie auf  > **Hinzufügen** klicken.

3. Klicken Sie im Bereich **ESA-Regeln** auf **+**.


Das Dialogfeld ESA-Regeln bereitstellen wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld:



## Funktionen

In der folgenden Tabelle werden die Parameter im Dialogfeld ESA-Regeln bereitstellen beschrieben.

Parameter	Beschreibung
	Filtert die Regelliste nach Schweregrad und Typ. Das Textfeld neben diesem Symbol filtert nach Regelname.
Name der Regel	Zeigt den Namen einer Regel an.
Beschreibung	Beschreibt die Regel.
Testregel	Gibt an, ob die Regel eine Testregel ist.
Typ	Zeigt den Typ der Regel an: RSA Live ESA-Regel, Erweiterte EPL-Regel oder Regelerstellungsregel.



## Dialogfeld „ESA-Services bereitstellen“

Im Dialogfeld ESA-Services bereitstellen werden alle verfügbaren ESA-Services angezeigt, die einer Bereitstellung hinzugefügt werden können.

So rufen Sie dieses Dialogfeld auf:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

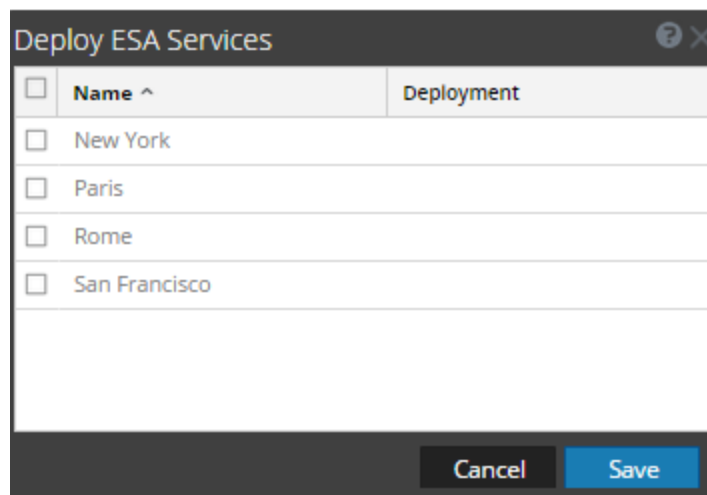
Die Registerkarte Regeln wird standardmäßig angezeigt.

2. Wählen Sie im Bereich „Optionen“ im Abschnitt **Bereitstellungen** eine Bereitstellung aus oder fügen Sie eine hinzu.

3. Klicken Sie im Bereich **ESA-Services** auf **+**.

Das Dialogfeld ESA-Services bereitstellen wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld:



## Funktionen

In der folgenden Tabelle werden die Parameter im Dialogfeld ESA-Services bereitstellen beschrieben.

Parameter	Beschreibung
Name	Zeigt die Namen von konfigurierten ESA-Services an.
Bereitstellung	Zeigt die Bereitstellungen an, für die der Service schon hinzugefügt wurde.

## Registerkarte Regelerstellung

Auf der Registerkarte Regelerstellung können Sie eine Regelerstellungsregel definieren.

So greifen Sie auf die Registerkarte Regelerstellung zu:

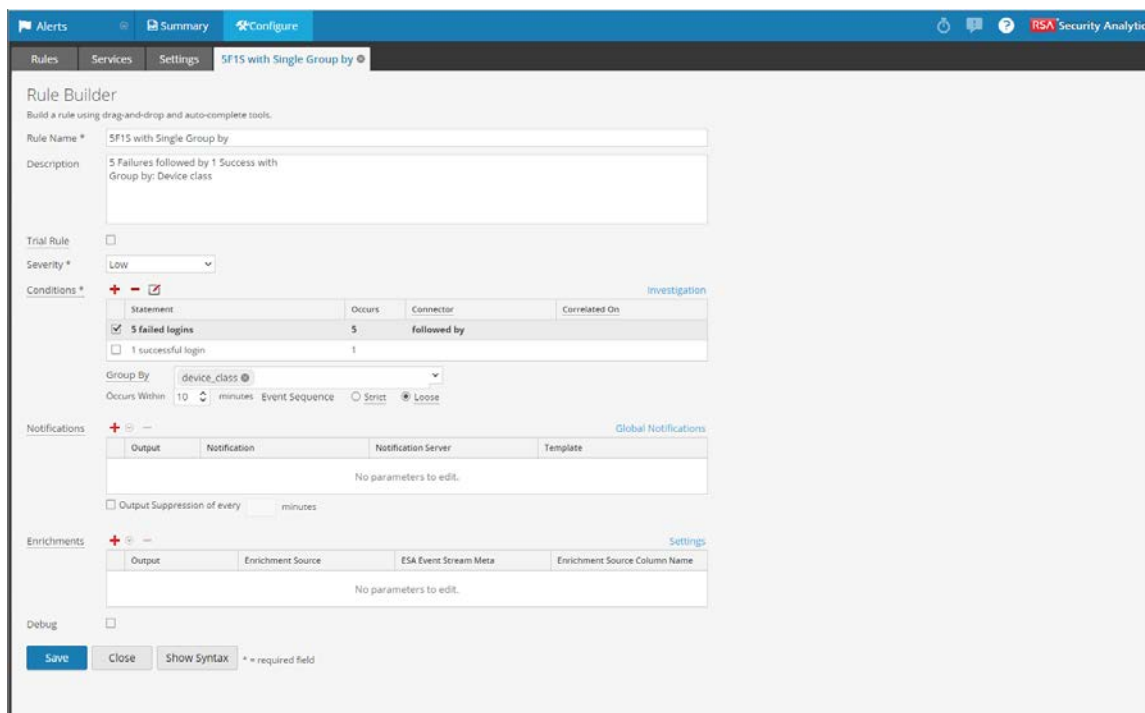
1. Wählen Sie im Menü Security Analytics die Optionen **Warnmeldungen > Konfigurieren** aus.

Die Ansicht Konfigurieren wird standardmäßig mit geöffneter Registerkarte Regeln angezeigt.

2. Wählen Sie in der Symbolleiste **Regelbibliothek** die Optionen   > **Regelerstellung** aus.

Die Registerkarte Regelerstellung wird angezeigt.

Die folgende Abbildung zeigt die Registerkarte Regelerstellung.



## Funktionen

In der folgenden Tabelle sind die Berechtigungen für die Registerkarte Regelerstellung aufgeführt:

Parameter	Beschreibung
-----------	--------------

Parameter	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung

Die „Regelerstellung“ umfasst die folgenden Komponenten:

- Abschnitt Bedingungen
- Abschnitt Meldungen
- Abschnitt Erweiterungen

### Abschnitt Bedingungen

Im Abschnitt Bedingungen der Registerkarte Regelerstellung definieren Sie, was die Regel erkennt.

In der folgenden Abbildung wird der Abschnitt Bedingungen dargestellt.

In der folgenden Tabelle sind die Parameter des Abschnitts Bedingungen angeführt.

Parameter	Beschreibung
<b>+</b>	Fügt eine Anweisung hinzu
<b>-</b>	Ausgewählte Anweisung löschen.
	Ausgewählte Anweisung bearbeiten.
Anweisung	Logische Gruppe von Bedingungen für eine Operation.

Parameter	Beschreibung
Tritt auf	Warnmeldungshäufigkeit bei erfüllter Bedingung. Dies gibt an, dass eine bestimmte Mindestanzahl von Ereignissen vorhanden sein muss, damit die Kriterien zum Auslösen einer Warnmeldung erfüllt sind. Das Minutenzeitfenster bindet den Tritt auf-Zähler.
Connector	<p>Optionen zur Spezifizierung der Beziehung zwischen Anweisungen:</p> <ul style="list-style-type: none"> <li>• gefolgt von</li> <li>• nicht gefolgt von</li> <li>• UND</li> <li>• ODER</li> </ul> <p>Der Connector verbindet zwei Anweisungen mit „UND“, „ODER“, „gefolgt von“ oder „nicht gefolgt von“. Wenn gefolgt von verwendet wird, wird angegeben, dass es eine Sequenz dieser Ereignisse gibt. UND und ODER erstellen ein großes Kriterium. Das Verhältnis gefolgt von erstellt verschiedene Kriterien, die in einer Sequenz auftreten.</p>
Korreliert am	Option für den Connector „Nicht gefolgt von“. Geben Sie den Metaschlüssel für das Feld an, das in der Sequenz nicht folgen soll.
tritt innerhalb von Minuten auf	Zeitfenster, innerhalb dessen die Bedingungen auftreten müssen.

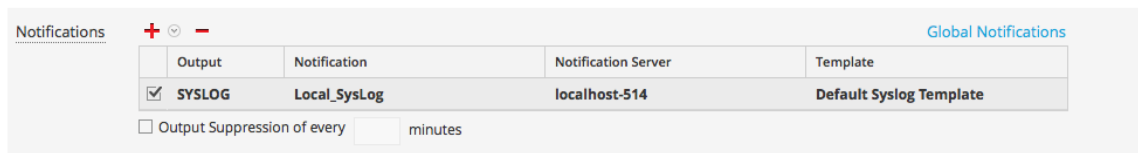
Parameter	Beschreibung
Ereignissequenz	<p>Wählen Sie aus, ob das Muster einer <i>strengen</i> oder einer <i>variablen</i> Übereinstimmung folgen muss. Wenn Sie eine strenge Übereinstimmung angeben, bedeutet dies, dass das Muster in der <i>genauen</i> Reihenfolge vorkommen muss, die Sie angegeben haben, ohne dass weitere Ereignisse dazwischen vorkommen. Beispiel: Wenn als Sequenz fünf fehlgeschlagene Anmeldungen (F) gefolgt von einer erfolgreichen Anmeldung (S) angegeben ist, wird dieses Muster nur übereinstimmen, wenn der Benutzer die folgende Sequenz ausführt: F, F, F, F, F, S. Wenn Sie eine variable Übereinstimmung angeben, bedeutet dies, dass andere Ereignisse innerhalb der Sequenz auftreten dürfen, aber die Regel wird weiterhin auslösen, wenn alle angegebenen Ereignisse auch auftreten. Beispiel: Fünf fehlgeschlagene Anmeldeversuche (F), gefolgt von einer beliebigen Anzahl dazwischen liegender erfolgreicher Anmeldeversuche (S), gefolgt von einem erfolgreichen Anmeldeversuch, könnten das folgende Muster erzeugen: F, S, F, S, F, S, F, S, F, S, die die Regel trotz der dazwischenliegenden erfolgreichen Anmeldungen auslösen würden.</p>
Gruppieren nach	<p>Wählen Sie den Metaschlüssel aus, nach dem die Ergebnisse aus der Dropdown-Liste gruppiert werden sollen. Nehmen Sie zum Beispiel an, es gibt die drei Benutzer Joe, Jane und John und Sie verwenden das Metadatum „Gruppieren nach“, <b>user_dst</b> („user_dst“ ist das Metadatenfeld für das Benutzerzielkonto). Das Ergebnis zeigt Ereignisse gruppiert nach den Benutzerzielkonten, Joe, Jane und John, an.</p> <p>Sie können auch nach mehreren Schlüsseln gruppieren. Beispielsweise möchten Sie eventuell nach Benutzern und Computern gruppieren, um zu sehen, ob ein Benutzer, der an demselben Computer angemeldet ist, mehrmals versucht, sich an einem Konto anzumelden. Um dies zu erreichen, können Sie nach „device_class“ und „user_dst“ gruppieren.</p>

### Benachrichtigungen

Im Abschnitt Benachrichtigungen können Sie auswählen, wie Sie benachrichtigt werden, wenn ESA eine Warnmeldung für die Regel erzeugt.

Weitere Informationen zu Warnmeldungsbenachrichtigungen erhalten Sie unter [Hinzufügen einer Benachrichtigungsmethode zu einer Regel](#).

Die folgende Abbildung zeigt den Abschnitt Benachrichtigungen.



Parameter	Beschreibung
<b>+</b>	So fügen Sie einen Warnmeldungsbenachrichtigungstyp hinzu.
<b>-</b>	So löschen Sie die ausgewählte Warnbenachrichtigung.
Ausgabe	Typ der Warnmeldungsbenachrichtigung Optionen: <ul style="list-style-type: none"> <li>• E-Mail</li> <li>• SNMP</li> <li>• Syslog</li> <li>• Skript</li> </ul>
Benachrichtigung	Name der zuvor konfigurierten Ausgabe, beispielsweise ein E-Mail-Verteiler
Benachrichtigungsserver	Name des die Ausgabe sendenden Servers
Vorlage	Name der Vorlage für die Warnmeldungsbenachrichtigung
Ausgabeunterdrückung alle	Option zur Spezifizierung der Warnmeldungshäufigkeit
Minuten	Warnmeldungshäufigkeit in Minuten



### Erweiterung

Im Abschnitt Erweiterung können Sie einer Regel eine Datenerweiterungsquelle hinzufügen.

Weitere Informationen zu Erweiterungen erhalten Sie unter [Hinzufügen einer Erweiterung zu einer Regel](#).

In der folgenden Abbildung wird der Abschnitt Erweiterungen dargestellt.

Enrichments <span style="float: right;">Settings</span>				
<input type="checkbox"/>	Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
<input checked="" type="checkbox"/>	<b>In-Memory Table</b>	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/>	External DB Reference	Select Enrichment Source	Enter Meta	Enter Column Name
<input type="checkbox"/>	Warehouse Analytics	Select Enrichment Source	Enter Meta	key
<input type="checkbox"/>	GeoIP	Select Enrichment Source	Enter Meta	ipv4

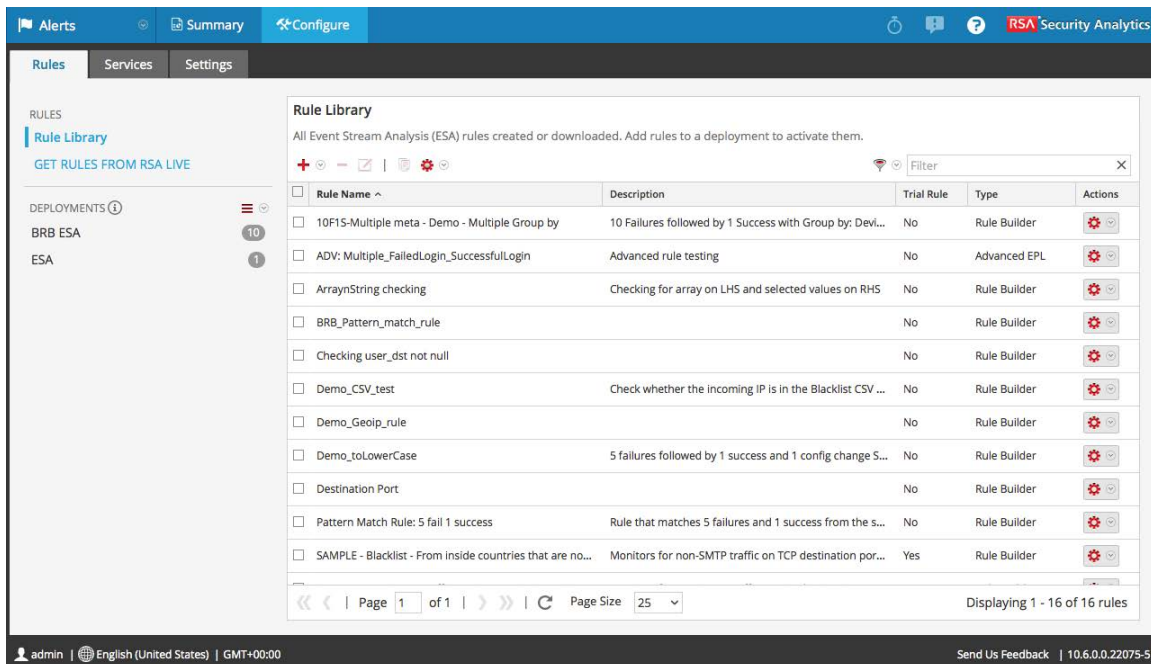
Parameter	Beschreibung
	So fügen Sie eine Erweiterung hinzu.
	So löschen Sie eine ausgewählte Erweiterung.
Ausgabe	Erweiterungsquellentyp Optionen: <ul style="list-style-type: none"> <li>• In-Memory-Tabelle</li> <li>• Externer DB-Verweis</li> <li>• Warehouse Analytics</li> <li>• GeoIP</li> </ul>
Erweiterungsquelle	Name der zuvor konfigurierten Erweiterungsquelle, z. B. ein .CSV-Dateiname einer In-Memory-Tabelle
ESA Ereignis-Stream-Metadaten	ESA-Metaschlüssel, der als ein Operand der Verknüpfungsbedingung verwendet wird
Spaltenname „Erweiterungsquelle“	Erweiterungsquellen-Spaltenname, dessen Wert als ein weiterer Operand der Verknüpfungsbedingung verwendet wird  Für eine In-Memory-Tabelle gilt, wenn Sie beim Erstellen einer CSV-basierten Erweiterung einen Schlüssel konfiguriert haben, wird diese Spalte mit dem ausgewählten Schlüssel automatisch ausgefüllt. Allerdings können Sie es nach Wunsch ändern.  Für eine GeoIP-Erweiterungsquelle wird ipv4 automatisch ausgewählt.

## Registerkarte Regeln

In diesem Thema wird die Registerkarte Regeln beschrieben, mit der Sie ESA-Regeln und Bereitstellungen managen.

Die Registerkarte „Regeln“ wird automatisch angezeigt, wenn Sie **Warnmeldungen > Konfigurieren** im Menü Security Analytics auswählen.

Die folgende Abbildung zeigt die Registerkarte „Regeln“.



## Funktionen

Die Registerkarte Regeln ist in zwei Bereiche unterteilt:

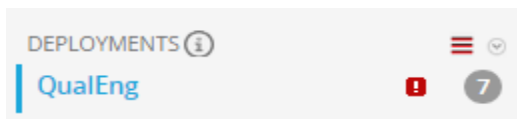
- [Bereich „Optionen“](#)
- [Bereich „Regelbibliothek“](#)
- [Bereich „Bereitstellung“](#)

## Bereich „Optionen“

Im Bereich „Optionen“ der Registerkarte **Regeln** können Sie folgende Aufgaben durchführen:

- Anzeigen von ESA-Regeln in der Regelbibliothek
- Erstellen von Bereitstellungen

In der folgenden Abbildung ist der Bereich „Optionen“ der Registerkarte **Regeln** dargestellt:



## Funktionen

Der Bereich Optionen enthält zwei Abschnitte: Regeln und Bereitstellungen.






## Abschnitt Regeln

Der Abschnitt „Regeln“ enthält zwei Optionen. Die Option **Regelbibliothek** ist standardmäßig aktiviert und wenn sie ausgewählt ist, wird die Ansicht „Regelbibliothek“ auf der Registerkarte angezeigt. Mit der Option **Regeln aus RSA Live abrufen** können Sie zur Ansicht „Live-Suche“ navigieren, in der Sie nach Regeln suchen können.

## Abschnitt Bereitstellungen

Im Abschnitt Bereitstellungen werden Bereitstellungen aufgeführt und hierfür verfügbare Aktualisierungen angezeigt. In diesem Abschnitt können Bereitstellungen hinzugefügt, gelöscht, bearbeitet und aktualisiert werden. Durch Auswahl einer Bereitstellung aus der Liste wird der Bereich Bereitstellung auf der Registerkarte angezeigt. In der folgenden Tabelle werden die Funktionen dieses Abschnitts beschrieben.

Funktion	Beschreibung
	Öffnet ein Drop-down-Menü, mit dem Sie eine Bereitstellung hinzufügen, bearbeiten oder löschen können. Sie können auch die Liste der Bereitstellungen aktualisieren, um festzustellen, ob neue Aktualisierungen für die Liste vorhanden sind.
	Gibt an, ob neue Aktualisierungen für die Bereitstellung vorhanden sind.
	Gibt die Anzahl der Regeln in der Bereitstellung an.

## Bereich „Regelbibliothek“

In diesem Thema werden die Komponenten der Ansicht „Regelbibliothek“ beschrieben. In der Ansicht „Regelbibliothek“ können Sie folgende Aufgaben ausführen:

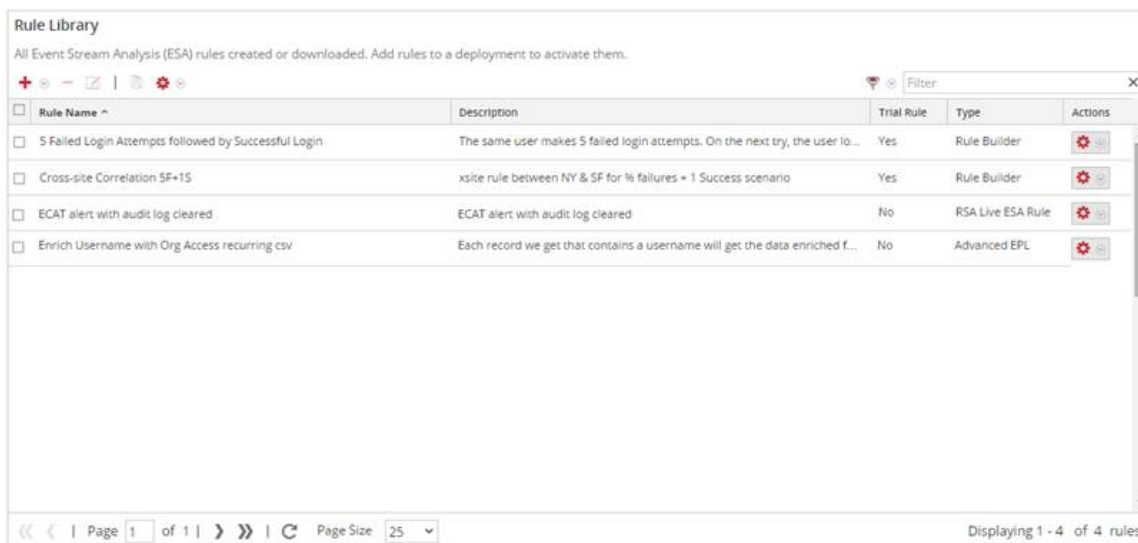
- Hinzufügen einer ESA-Regel
- Löschen einer ESA-Regel
- Bearbeiten einer ESA-Regel

- Duplizieren einer ESA-Regel
- Importieren von ESA-Regeln
- Exportieren einer ESA-Regel
- Filtern der ESA-Regelliste

Um auf diese Ansicht zuzugreifen, wählen Sie im Menü Security Analytics die Optionen **Warnmeldungen > Konfigurieren** aus. Die Registerkarte „Regeln“ wird angezeigt und die Ansicht „Regelbibliothek“ befindet sich auf der rechten Seite.

### Funktionen

Die folgende Abbildung zeigt die Liste „Regelbibliothek“.



The screenshot displays the 'Rule Library' interface. At the top, it states: 'All Event Stream Analysis (ESA) rules created or downloaded. Add rules to a deployment to activate them.' Below this is a toolbar with icons for adding, deleting, and refreshing rules, and a search filter box. The main area contains a table with the following data:

<input type="checkbox"/>	Rule Name ^	Description	Trial Rule	Type	Actions
<input type="checkbox"/>	5 Failed Login Attempts followed by Successful Login	The same user makes 5 failed login attempts. On the next try, the user lo...	Yes	Rule Builder	
<input type="checkbox"/>	Cross-site Correlation SF+15	xsite rule between NY & SF for % failures + 1 Success scenario	Yes	Rule Builder	
<input type="checkbox"/>	ECAT alert with audit log cleared	ECAT alert with audit log cleared	No	RSA Live ESA Rule	
<input type="checkbox"/>	Enrich Username with Org Access recurring csv	Each record we get that contains a username will get the data enriched f...	No	Advanced EPL	

At the bottom of the interface, there is a pagination control showing 'Page 1 of 1' and a 'Page Size' dropdown set to '25'. The status bar at the bottom right indicates 'Displaying 1 - 4 of 4 rules'.

Die Ansicht „Regelbibliothek“ enthält folgende Komponenten:

- Symbolleiste Regelbibliothek
- Regelbibliotheksliste

### Symbolleiste Regelbibliothek

Über die Symbolleiste „Regelbibliothek“ können Sie ESA-Regeln hinzufügen, löschen, bearbeiten, duplizieren, filtern, exportieren und importieren.



### Regelbibliotheksliste

Die folgende Abbildung zeigt die Liste „Regelbibliothek“.

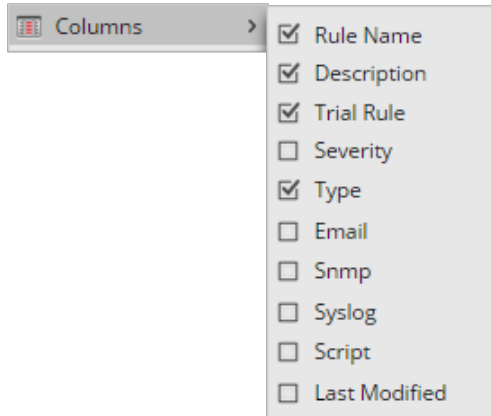


Die Liste „Regelbibliothek“ enthält alle ESA-Regeln, die von RSA Live heruntergeladen oder in den Registerkarten „Erweiterte EPL“ und „Regelerstellung“ erstellt wurden. In der folgenden Tabelle sind die verschiedenen Spalten der Liste „Regelbibliothek“ mit Beschreibung aufgelistet.

Spalte	Beschreibung
Name der Regel	Zweck der ESA-Regel
Beschreibung	Zusammenfassung dessen, was die ESA-Regel erkennt

Spalte	Beschreibung
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Typ	Der Typ der Regel
Aktionen (  )	Menü für das Löschen, Bearbeiten, Duplizieren oder Exportieren der ausgewählten Regel
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
E-Mail	Gibt an, ob eine Warnbenachrichtigung für die Regel per E-Mail gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.
SNMP	Gibt an, ob eine Warnbenachrichtigung für die Regel über SNMP gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.
Syslog	Gibt an, ob eine Warnbenachrichtigung für die Regel über Syslog gesendet werden soll. Diese Spalte wird standardmäßig nicht angezeigt.
Skript	Gibt an, ob eine Warnbenachrichtigung für die Regel ein Skript ausführt. Diese Spalte wird standardmäßig nicht angezeigt.
Zuletzt geändert	Datum und Uhrzeit der letzten Änderung der ESA-Regel Diese Spalte wird standardmäßig nicht angezeigt.

Bewegen Sie die Maus über den Titel einer Spalte und klicken Sie rechts auf das v, um Spalten anzuzeigen, die nicht standardmäßig sichtbar sind. Dadurch wird ein Drop-down-Menü geöffnet, in dem Sie die Inhalte der Spalte sortieren oder wählen können, welche Spalten Sie in der Regelbibliotheksliste sehen möchten.

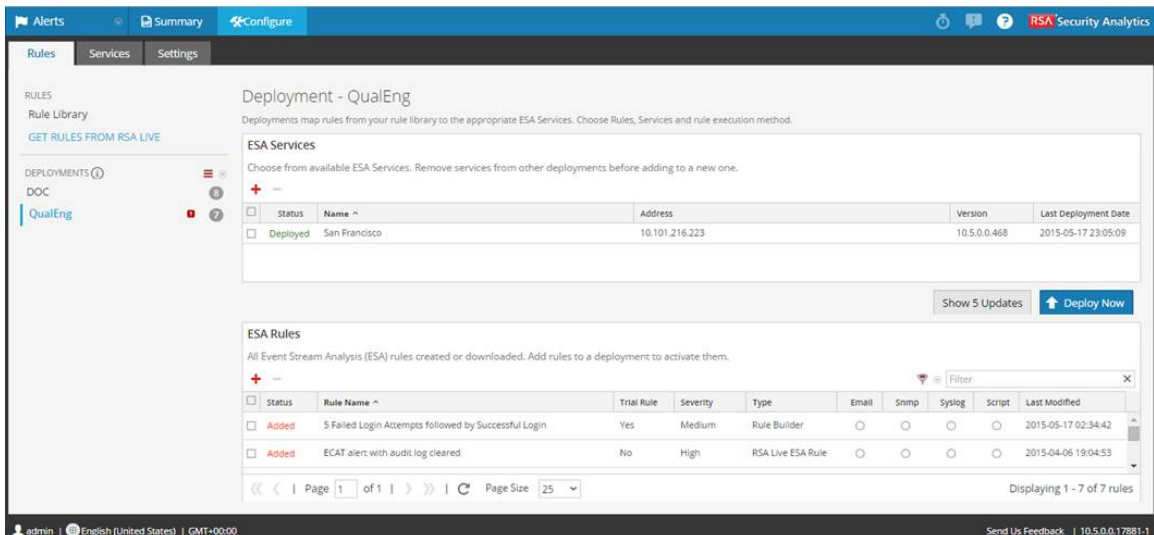


## Bereich „Bereitstellung“

Dieses Thema bietet eine Übersicht über den Bereich „Bereitstellung“. In dem Bereich „Bereitstellung“ können Sie die Bereitstellungen erstellen und konfigurieren. Der Bereich „Bereitstellung“ umfasst folgende Abschnitte:

- ESA-Services
- ESA-Regeln

Die folgende Abbildung zeigt den Bereich „Bereitstellung“.





## Funktionen

### ESA-Services

Im Abschnitt ESA-Services können Sie die ESA-Services in der Bereitstellung managen.

Im Abschnitt ESA-Services können Sie die folgenden Aufgaben ausführen:

Aufgabe	Beschreibung
	Mit diesem Symbol fügen Sie der Bereitstellung einen ESA-Service hinzu.
	Der ausgewählte ESA-Service wird aus der Bereitstellung entfernt.
Updates anzeigen	Das Dialogfeld Aktualisierungen an der Bereitstellung wird geöffnet.
Jetzt bereitstellen	Stellen Sie die aktuellen Regelsätze bereit.



In der folgenden Tabelle sind die Parameter im Abschnitt ESA-Services aufgelistet.


Parameter	Beschreibung
Status	Zeigt an, ob der Bereitstellungsstatus <b>Hinzugefügt</b> , <b>Bereitgestellt</b> , <b>Aktualisiert</b> oder <b>Fehlgeschlagen</b> ist.
Name	Der Name des ESA-Service.
Adresse	Die IP-Adresse des Hosts, auf dem der ESA-Service installiert ist.
Version	Die Version des ESA-Service.
Datum der letzten Bereitstellung	Datum und Uhrzeit der letzten Bereitstellung des ESA-Services.

### ESA-Regeln

Im Abschnitt ESA-Regeln managen Sie die Regeln in der Bereitstellung. In diesem Abschnitt sind alle Regeln aufgeführt, die derzeit in der Bereitstellung vorhanden sind.

Im Abschnitt **ESA-Regeln** können Sie die folgenden Aufgaben ausführen.

Aufgabe	Beschreibung
	Öffnet das Dialogfeld ESA-Regeln bereitstellen, in dem Sie eine Regel auswählen können.
	Mit diesem Symbol werden die ausgewählten ESA-Regeln aus der Bereitstellung entfernt.

Aufgabe	Beschreibung
	Mit diesem Symbol filtern Sie die Regelliste.
<input type="text" value="Filter"/>	In diesem Feld können Sie nach einer Regel suchen.




In der folgenden Tabelle sind die Parameter des Abschnitts ESA-Regeln aufgeführt.

Parameter	Beschreibung
Status	Gibt den Regelstatus an: <ul style="list-style-type: none"> <li>• Bereitgestellt: Die Regel wurde bereitgestellt.</li> <li>• Aktualisiert: Die Regel wurde seit der letzten Bereitstellung aktualisiert.</li> <li>• Hinzugefügt: Die Regel wurde seit der letzten Bereitstellung hinzugefügt.</li> <li>• Fehlgeschlagen: Die Bereitstellung ist fehlgeschlagen.</li> </ul>
Name der Regel	Zweck der ESA-Regel
Testregel	Bereitstellungsmodus zur Bestimmung, ob die Regel effizient ausgeführt wird
Schweregrad	Bedrohungsstufe der von der Regel ausgelösten Warnmeldung
Ausgabe	Der Typ der ESA-Regel.
E-Mail, SNMP, Syslog, Skript	Gibt an, welche Benachrichtigungstypen für durch die Regeln erzeugte Warnmeldungen verwendet werden
Zuletzt geändert	Datum und Uhrzeit der letzten Änderung der ESA-Regel

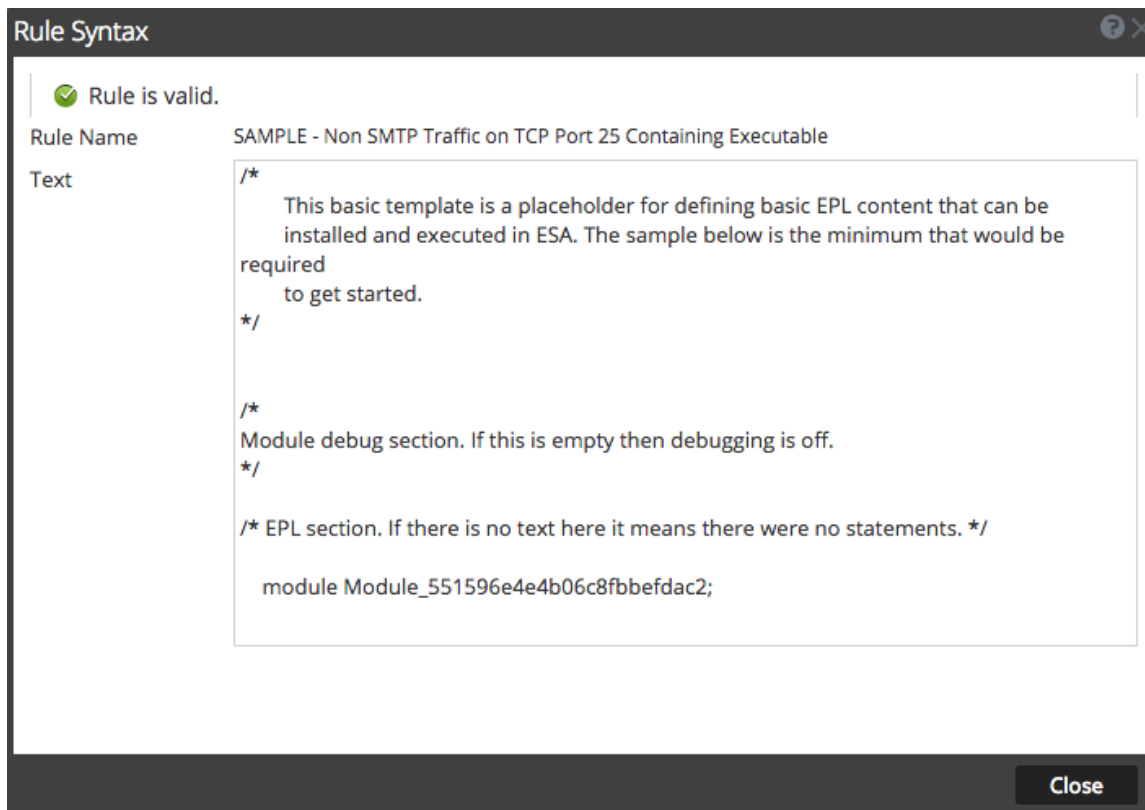
## Dialogfeld Regelsyntax

In diesem Thema werden die Funktionen des Dialogfelds Regelsyntax beschrieben. Im Dialogfeld Regelsyntax wird die EPL-Syntax von Bedingungen, Anweisungen und Debugging-Parametern angezeigt. Wenn die Syntax ungültig ist, erscheint eine Warnmeldung.

So rufen Sie dieses Dialogfeld auf:

1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.
2. Führen Sie in der Ansicht **Regelbibliothek** einen der folgenden Schritte aus:
  - a. Klicken Sie auf  und wählen Sie **Erweiterte EPL** oder **Regelerstellung** aus.
  - b. Doppelklicken Sie auf eine vorhandene Regel.
  - c. Wählen Sie eine vorhandene Regel aus und klicken Sie in der Symbolleiste der **Regelbibliothek** auf .
  - d. Wählen Sie in der Zeile einer vorhandenen Regel  > **Bearbeiten** aus.  
Die neue oder vorhandene Regel wird in einer neuen Registerkarte angezeigt und kann bearbeitet werden.
3. Klicken Sie unten auf der Registerkarte auf **Syntax anzeigen**.

Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld Regelsyntax:



## Funktionen


In der folgenden Tabelle sind die Eigenschaften der Parameter des Dialogfelds Regelsyntax beschrieben:



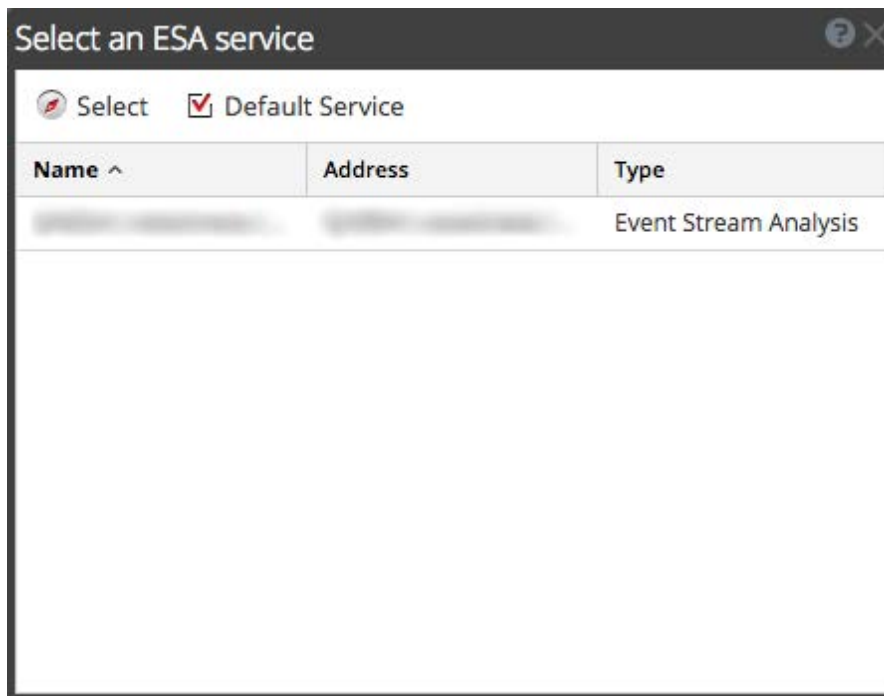
Parameter	Beschreibung
<b>Regel ist gültig oder Validierungsfehler in Regel</b>	Zeigt an, ob die Regelsyntax gültig ist oder geändert werden muss.
Name der Regel	Zeigt den Namen einer Regel an.
Text	Zeigt die EPL-Syntax von Bedingungen, Anweisungen und Debugging-Parametern an, wenn die Regel gültig ist.

### Dialogfeld „ESA-Service auswählen“

In diesem Thema werden die Funktionen des Dialogfelds ESA-Service auswählen beschrieben. Im Dialogfeld ESA-Service auswählen werden alle verfügbaren ESA-Services angezeigt. Das Auswählen eines Services ermöglicht Ihnen das Anzeigen einer Zusammenfassung zu diesem Service in der Ansicht Zusammenfassung.

Wählen Sie für den Zugriff auf dieses Dialogfeld im Menü Security Analytics die Optionen **Warnmeldung > Zusammenfassung** aus. Wenn das Dialogfeld „ESA-Service auswählen“ nicht automatisch angezeigt wird, klicken Sie auf .

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld:



## Funktionen

In der folgenden Tabelle sind die Funktionen des Dialogfelds ESA-Service auswählen beschrieben.

Parameter	Beschreibung
Auswählen	Zeigt die Ansicht Zusammenfassung für den ausgewählte Service an.
Standardservice	Kennzeichnet einen Standardservice. Die Ansicht Zusammenfassung für den Standardservice wird automatisch angezeigt.
Name	Zeigt den Namen dieses ESA-Services an.
Adresse	Zeigt die Adresse des ESA-Services an.
Typ	Zeigt den Typ des -Services an.

## Registerkarte Services

Dieses Thema enthält eine Übersicht über die Registerkarte **Warnmeldungen > Konfigurieren > Services**. Die Registerkarte „Services“ bietet Details zu den ESA-Services, die Security Analytics hinzugefügt wurden.

In der folgenden Abbildung wird die Registerkarte „Services“ dargestellt:

The screenshot shows the 'Services' configuration page in RSA Security Analytics. The page title is 'ESA - Event Stream Analysis'. It features three main sections: 'Engine Stats', 'Rule Stats', and 'Alert Stats'. Below these is a 'Deployed Rule Stats' table with columns for 'Enable', 'Name', 'Trial Rule', 'Last Detected', and 'Events Matched'. The table lists several rules, all of which are currently enabled and have no events matched. The interface also includes navigation controls at the bottom, such as 'Page 1 of 1' and 'Page Size 25'.

Engine Stats	Rule Stats	Alert Stats
Esper Version: 5.3.0	Rules Enabled: 11	Email: 0
Time: 0	Rules Disabled: 0	SNMP: 0
Events Offered: 0	Events Matched: 0	Syslog: 0
Offered Rate: 0 per second / 0 max		Script: 0
		Storage: 0
		Message Bus: 0

Deployed Rule Stats																																			
<table border="1"> <thead> <tr> <th>Enable</th> <th>Name</th> <th>Trial Rule</th> <th>Last Detected</th> <th>Events Matched</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>Demo_toLowerCase</td> <td>No</td> <td></td> <td>0</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Pattern Match Rule: 5 fail 1 success</td> <td>No</td> <td></td> <td>0</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Destination Port</td> <td>No</td> <td></td> <td>0</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>ArrayString checking</td> <td>No</td> <td></td> <td>0</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>ADV: Multiple_failedLogin_SuccessfulLogin</td> <td>No</td> <td></td> <td>0</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>10F15-Multiple meta - Demo - Multiple Group by</td> <td>No</td> <td></td> <td>0</td> </tr> </tbody> </table>	Enable	Name	Trial Rule	Last Detected	Events Matched	<input checked="" type="checkbox"/>	Demo_toLowerCase	No		0	<input checked="" type="checkbox"/>	Pattern Match Rule: 5 fail 1 success	No		0	<input checked="" type="checkbox"/>	Destination Port	No		0	<input checked="" type="checkbox"/>	ArrayString checking	No		0	<input checked="" type="checkbox"/>	ADV: Multiple_failedLogin_SuccessfulLogin	No		0	<input checked="" type="checkbox"/>	10F15-Multiple meta - Demo - Multiple Group by	No		0
Enable	Name	Trial Rule	Last Detected	Events Matched																															
<input checked="" type="checkbox"/>	Demo_toLowerCase	No		0																															
<input checked="" type="checkbox"/>	Pattern Match Rule: 5 fail 1 success	No		0																															
<input checked="" type="checkbox"/>	Destination Port	No		0																															
<input checked="" type="checkbox"/>	ArrayString checking	No		0																															
<input checked="" type="checkbox"/>	ADV: Multiple_failedLogin_SuccessfulLogin	No		0																															
<input checked="" type="checkbox"/>	10F15-Multiple meta - Demo - Multiple Group by	No		0																															

Die Registerkarte Services verfügt über die folgenden Abschnitte:

- Bereich „ESA-Services“
- Bereich „Allgemeine Statistik“
- Bereich „Statistik für bereitgestellte Regeln“

## Funktionen

### Bereich „ESA-Services“

Der Bereich ESA-Services listet die Namen von allen ESA-Services auf, die zu Security Analytics hinzugefügt werden.

### Bereich „Allgemeine Statistik“

Der Bereich Allgemeine Statistik enthält Informationen über die Esper-Engine, Regeln und Warnmeldungen.

Der Bereich Allgemeine Statistik ist in die folgenden Abschnitte unterteilt:

- Engine-Statistiken
- Regelstatistiken
- Warnmeldungsstatistiken

In der folgenden Abbildung wird der Bereich Allgemeine Statistik dargestellt:

San Francisco					
<b>Engine Stats</b>	5.1.0	<b>Rules Enabled</b>	53	<b>Email</b>	0
Esper Version	2015-05-19T00:44:34	<b>Rules Disabled</b>	0	<b>SNMP</b>	0
Time	381973392	<b>Events Matched</b>	622696	<b>Syslog</b>	0
Events Offered				<b>Script</b>	0
Offered Rate	0 per second / 144,360 max			<b>Storage</b>	622696
				<b>Message Bus</b>	0

In der folgenden Tabelle sind die Parameter im jeweiligen Abschnitt beschrieben.

Abschnitte	Parameter	Beschreibung
Engine-Statistiken	Esper-Version	Esper-Version, die im ESA-Service ausgeführt wird
	Zeit	Zeitpunkt, an dem das letzte Ereignis an die Esper-Engine gesendet wurde
	Angebotene Ereignisse	Anzahl an Ereignissen, die vom ESA-Service seit dem letzten Servicestart analysiert wurde
	Angebotene Rate	Aktuelle Rate angebotener Ereignisse im ESA-Service
Regelstatistiken	Regeln aktiviert	Anzahl aktivierter Regeln
	Regeln deaktiviert	Anzahl deaktivierter Regeln
	Übereinstimmende Ereignisse	Gesamtanzahl der Ereignisse, die mit allen Regeln im ESA-Service übereinstimmen
Warnmeldungsstatistiken	E-Mail	Anzahl von E-Mail-Benachrichtigungen, die vom ESA-Service gesendet wurden
	SNMP	Anzahl von SNMP-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Syslog	Anzahl von Syslog-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Skript	Anzahl von Skript-Benachrichtigungen, die vom ESA-Service gesendet wurden
	Speicher	Gesamtanzahl der in der Datenbank gespeicherten Warnmeldungen
	Nachrichtenbus	Gesamtanzahl von Warnmeldungen, die an den Nachrichtenbus gesendet wurden

## Bereich „Statistik für bereitgestellte Regeln“

Der Bereich Statistik für bereitgestellte Regeln liefert Details zu den im ESA-Service bereitgestellten Regeln.

In der folgenden Abbildung wird der Bereich „Statistik für bereitgestellte Regeln“ dargestellt.

Deployed Rule Stats					
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		See <a href="#">Health &amp; Wellness</a> to monitor rule memory usage.			
<input type="checkbox"/>	Enable	Name	Trial Rule	Last Detected	Events Matched
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - P2P Software as Detected by an Intrusion Detection Device	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	SAMPLE - Non SMTP Traffic on TCP Port 25 Containing Executable	Yes		0
<input type="checkbox"/>	<input checked="" type="radio"/>	ECAT alert with audit log cleared	No		0
<input type="checkbox"/>	<input checked="" type="radio"/>	HTTP GET Flood	Yes		0

<< < | Page 1 of 1 | >> | Page Size 25 | Displaying 1 - 7 of 7

In der Tabelle werden die verschiedenen Parameter und deren Beschreibung aufgelistet.

Parameter	Beschreibung
<input checked="" type="radio"/>	Gibt an, dass die Regel aktiviert ist. Aktiviert eine Regel, die deaktiviert war.
<input type="radio"/> Disable	Gibt an, dass die Regel deaktiviert ist. Deaktiviert eine Regel, die aktiviert war.
Integrität und Zustand	Zeigt eine Momentaufnahme des Speichernutzung an, wenn Testregeln deaktiviert werden.
Aktivieren	Zeigt an, ob die Regel aktiviert oder deaktiviert ist Das grüne Symbol gibt an, dass die Regel aktiviert ist. Das weiße Symbol gibt an, dass die Regel deaktiviert ist.
Name	Name der ESA-Regel
Testregel	Zeigt an, ob die Regel im Testregelmodus ausgeführt wird.
Zuletzt erkannt	Zeitpunkt, an dem das letzte Mal eine Warnmeldung für diese Regel ausgelöst wurde

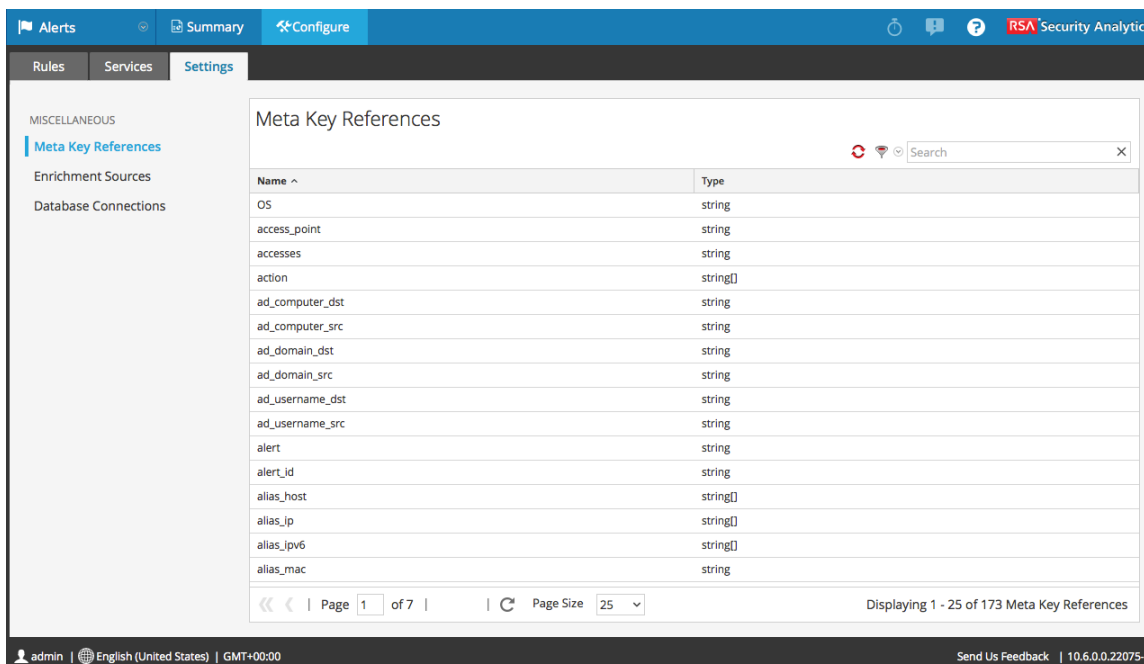
Parameter	Beschreibung
Übereinstimmende Ereignisse	Gesamtanzahl von Ereignissen, die mit der Regel übereinstimmen

## Registerkarte „Einstellungen“

In diesem Thema werden die Komponenten der Registerkarte „Einstellungen“ beschrieben. Auf der Registerkarte „Einstellungen“ können Sie folgende Aufgaben durchführen:

- Eine Liste der Metaschlüssel anzeigen
- Eine Datenerweiterungsquelle konfigurieren
- Eine Verbindung zu einer externen Datenbank hinzufügen

Die folgende Abbildung zeigt den Abschnitt Metaschlüsselverweise der Registerkarte Einstellungen.



## Funktionen

### Metaschlüsselverweise

Im Bereich Metaschlüsselverweise werden die einzelnen Metaschlüssel und die Art des Werts, die für einen Schlüssel erforderlich ist, aufgelistet.

### Erweiterungsquellen

Im Bereich Erweiterungsquellen können Sie die folgenden externen Datenquellen konfigurieren:

- GeoIP
- Externe Datenbankreferenz
- In-Memory-Tabelle
- Warehouse Analytics

Die folgende Abbildung zeigt den Abschnitt Erweiterungsquellen der Registerkarte Einstellungen.

The screenshot shows the 'Enrichment Sources' configuration page in the RSA Security Analytics interface. The page is titled 'Enrichment Sources' and includes a search bar and a table of configured sources. The table has the following data:

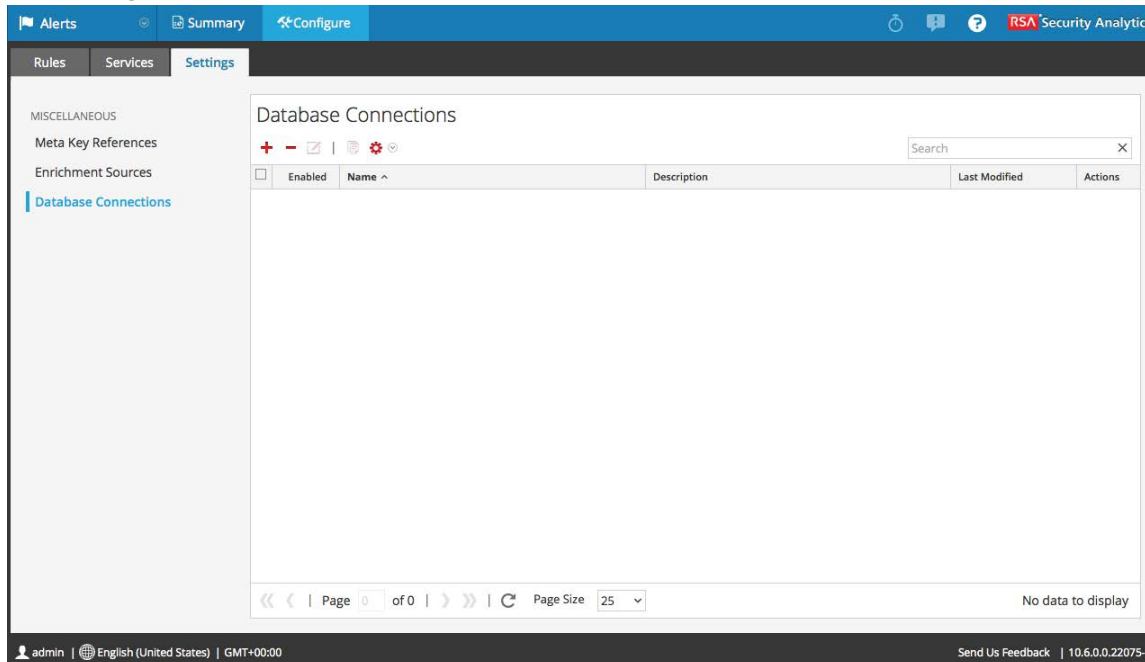
Enabled	Name	Type	Description	Last Modified	Actions
<input type="checkbox"/>	Default GeoIP	GeoIP	Default Geo IP Enrichment Source. This canno...	2016-02-12 06:13:07	
<input type="checkbox"/>	Gold_CSV	In-Memory Table		2016-02-15 04:07:02	
<input type="checkbox"/>	Sunila_CSV	In-Memory Table		2016-02-16 07:06:05	

The interface also shows a sidebar with 'Enrichment Sources' selected under 'Settings', and a footer with user information and system details.

## Datenbankverbindungen

Im Bereich Datenbankverbindungen können Sie eine Verbindung zu einer externen Datenbank konfigurieren, damit ESA auf diese Daten zugreifen kann.

Die folgende Abbildung zeigt den Abschnitt Datenbankverbindungen der Registerkarte Einstellungen.



Im Abschnitt Datenbankverbindungen können Sie folgende Vorgänge ausführen:

- Hinzufügen einer Datenbankverbindung
- Löschen von Datenbankverbindungen
- Bearbeiten von Datenbankverbindungen
- Duplizieren von Datenbankverbindungen
- Importieren von Datenbankverbindungen
- Exportieren von Datenbankverbindungen

## Dialogfeld „Aktualisierungen an der Bereitstellung“

Das Dialogfeld Aktualisierungen an der Bereitstellung zeigt Änderungen an der Bereitstellung an, wie etwa die Hinzufügung einer Regel und eines Services. Aktualisierungen an der Bereitstellung werden durch das Aktualisierungssymbol (🔄) neben dem Namen der Bereitstellung im Bereich „Optionen“ auf der Registerkarte „Regeln“ angezeigt.

So rufen Sie dieses Dialogfeld auf:

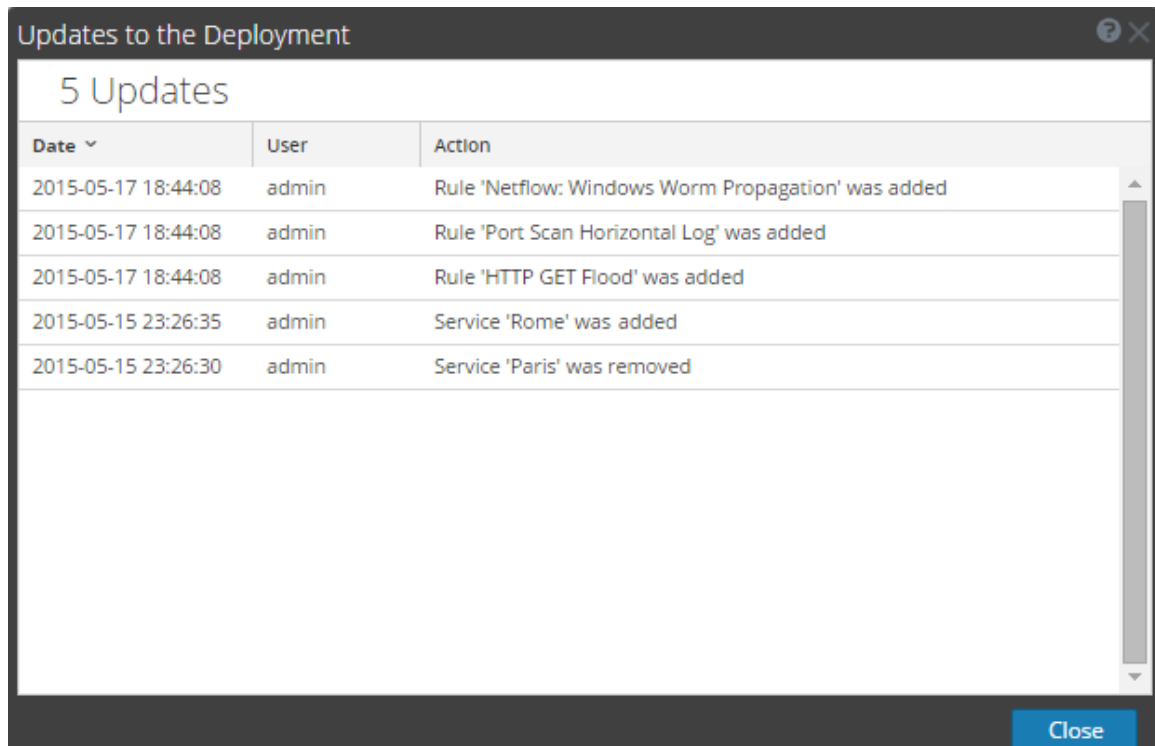
1. Wählen Sie im Menü **Security Analytics** die Optionen **Warnmeldungen > Konfigurieren** aus.

Die Registerkarte Regeln wird standardmäßig angezeigt.



2. Wählen Sie im Bereich „Optionen“ unter dem Abschnitt **Bereitstellungen** eine Bereitstellung aus oder fügen Sie eine hinzu.
3. Klicken Sie im Bereich **Bereitstellung** auf **Updates anzeigen**.  
Das Dialogfeld Aktualisierungen an der Bereitstellung wird angezeigt.

Die folgende Abbildung zeigt ein Beispiel für dieses Dialogfeld:



## Funktionen

Im Dialogfeld „Aktualisierungen an der Bereitstellung“ wird die Anzahl der Aktualisierungen oben im Dialog angezeigt. In der folgende Tabelle werden die Parameter dieses Dialogs beschrieben.

Parameter	Beschreibung
Datum	Zeigt den Tag und die Uhrzeit der Aktualisierung an.
Benutzer	Zeigt den Benutzer an, der die Aktualisierung vorgenommen hat.
Aktion	Beschreibt die Aktualisierung.

