Erstellen benutzerdefinierter Dashboards und Warnungen für Splunk mithilfe von Syslogs aus FTD

Inhalt

Einleitung

Dieses Dokument beschreibt eine schrittweise Anleitung für die Konfiguration von FTD zum Senden von Syslogs an Splunk und die Verwendung dieser Protokolle zum Erstellen benutzerdefinierter Dashboards und Warnungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor dem Durchgehen des Konfigurationsleitfadens Kenntnis von diesen Themen zu haben:

- Syslog
- Grundkenntnisse der Suchprozesssprache (SPL) von Splunk

In diesem Dokument wird außerdem davon ausgegangen, dass Sie bereits eine Splunk Enterprise-Instanz auf einem Server installiert haben und auf die Webschnittstelle zugreifen können.

Verwendete Komponenten

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

- Cisco Firepower Threat Defense (FTD) mit Version 7.2.4
- Cisco FirePOWER Management Center (FMC) mit Version 7.2.4
- Splunk Enterprise-Instanz (Version 9.4.3), die auf einem Windows-Computer ausgeführt wird

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration.

Hintergrundinformationen

Cisco FTD-Geräte generieren detaillierte Syslogs zu Zugriffsversuchen, Zugriffskontrollrichtlinien und Verbindungsereignissen. Die Integration dieser Protokolle mit Splunk ermöglicht leistungsstarke Analysen und Echtzeitwarnungen für Netzwerksicherheitsvorgänge.

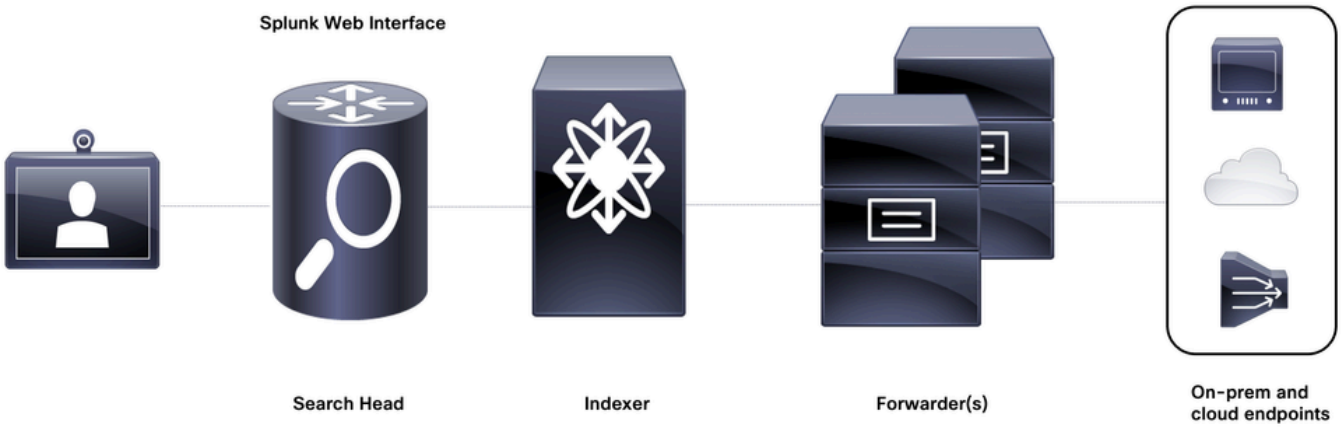
Splunk ist eine Echtzeit-Datenanalyseplattform, die entwickelt wurde, um maschinengenerierte Daten zu erfassen, zu indizieren, zu durchsuchen und zu visualisieren. Splunk ist besonders effektiv in Cybersicherheitsumgebungen als ein Security Information and Event Management (SIEM) Tool aufgrund seiner Fähigkeit,:

- Aufnahme von Protokolldaten skaliert
- Komplexe Suchvorgänge mit SPL durchführen
- Erstellen von Dashboards und Warnungen
- Integration mit Sicherheits-Orchestrierungs- und Reaktionssystemen

Splunk verarbeitet Daten über eine strukturierte Pipeline, um unstrukturierte oder halbstrukturierte Maschinendaten nützlich und umsetzbar zu machen. Die wichtigsten Phasen dieser Pipeline werden häufig als IPIS bezeichnet, das für Folgendes steht:

- Eingabe
- Parsing
- Indizierung
- Suche

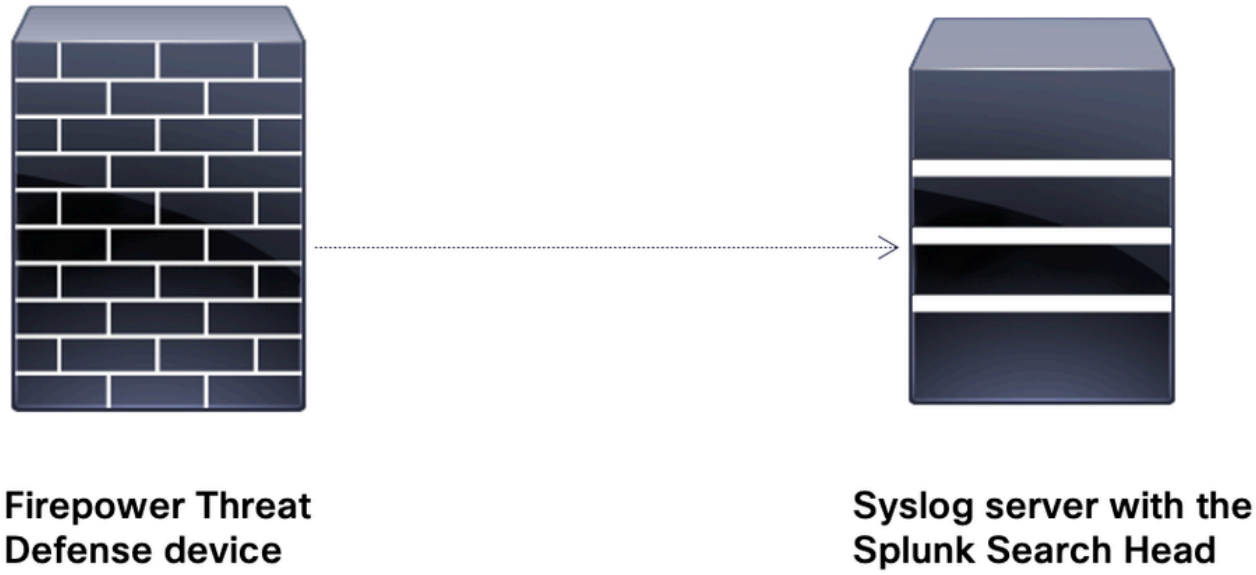
Das folgende Diagramm zeigt die wichtigsten Komponenten der zugrunde liegenden Architektur, die zur Realisierung der IPIS-Pipeline verwendet werden:



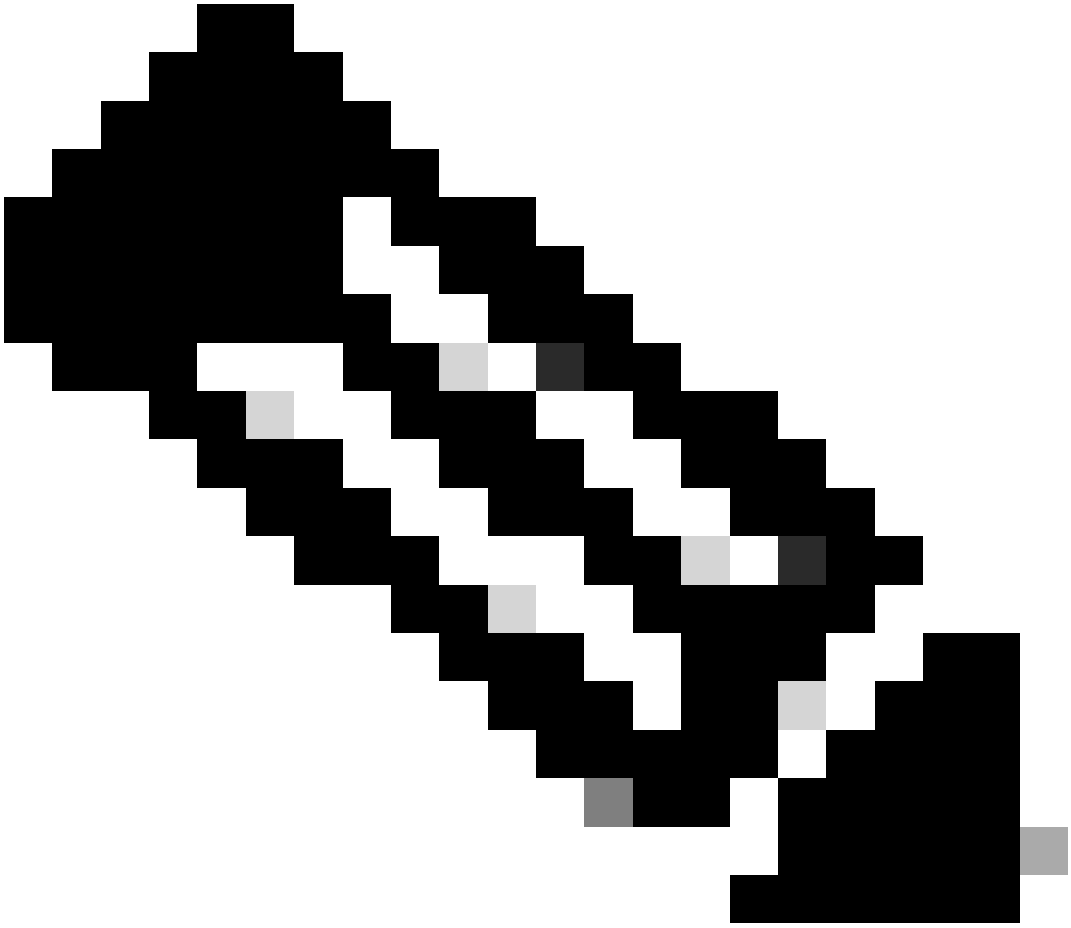
Splunk-Basisarchitektur

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

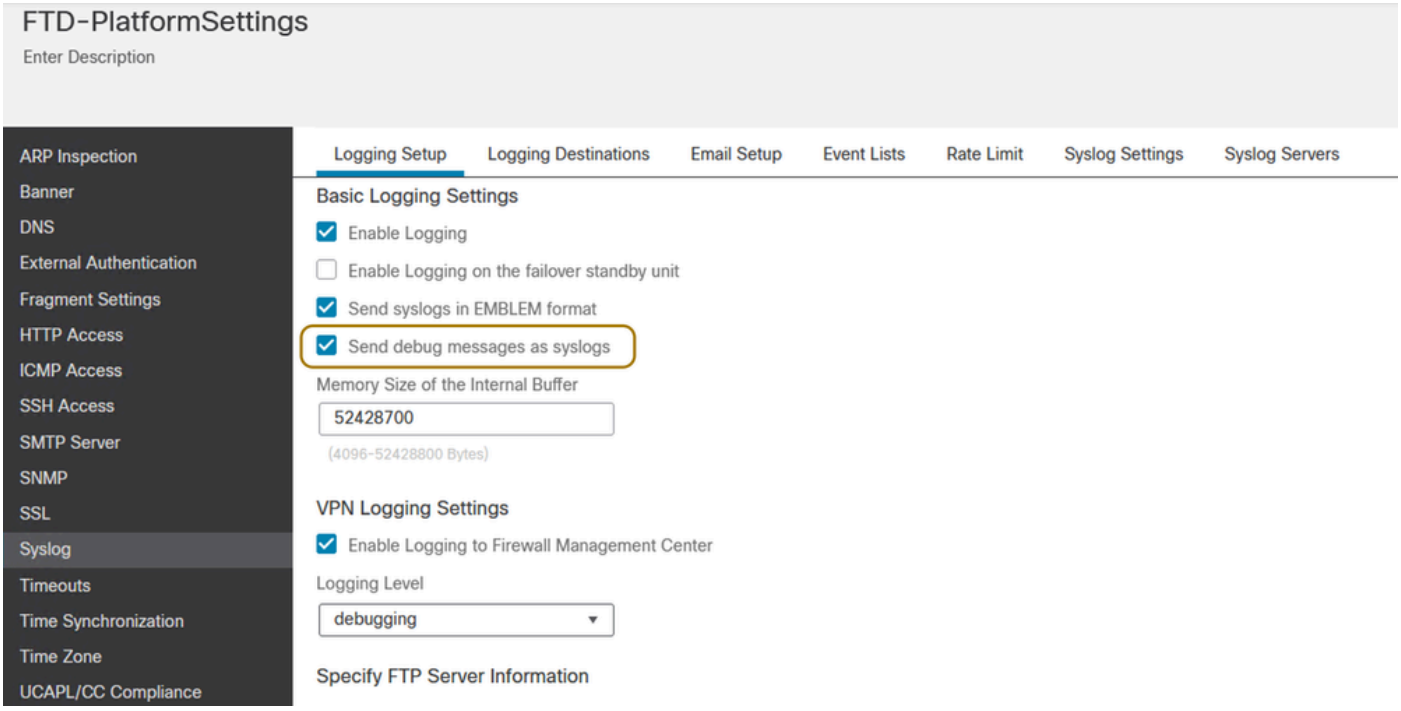


Anmerkung: Für die Laborumgebung für dieses Dokument sind keine separaten Forwarder- und Indexerinstanzen erforderlich. Der Windows-Computer, d. h. der Syslog-Server, auf dem die Splunk Enterprise-Instanz installiert ist, fungiert als Indexer und Suchkopf.

Konfigurationen

Syslog-Einstellungen für FTD konfigurieren

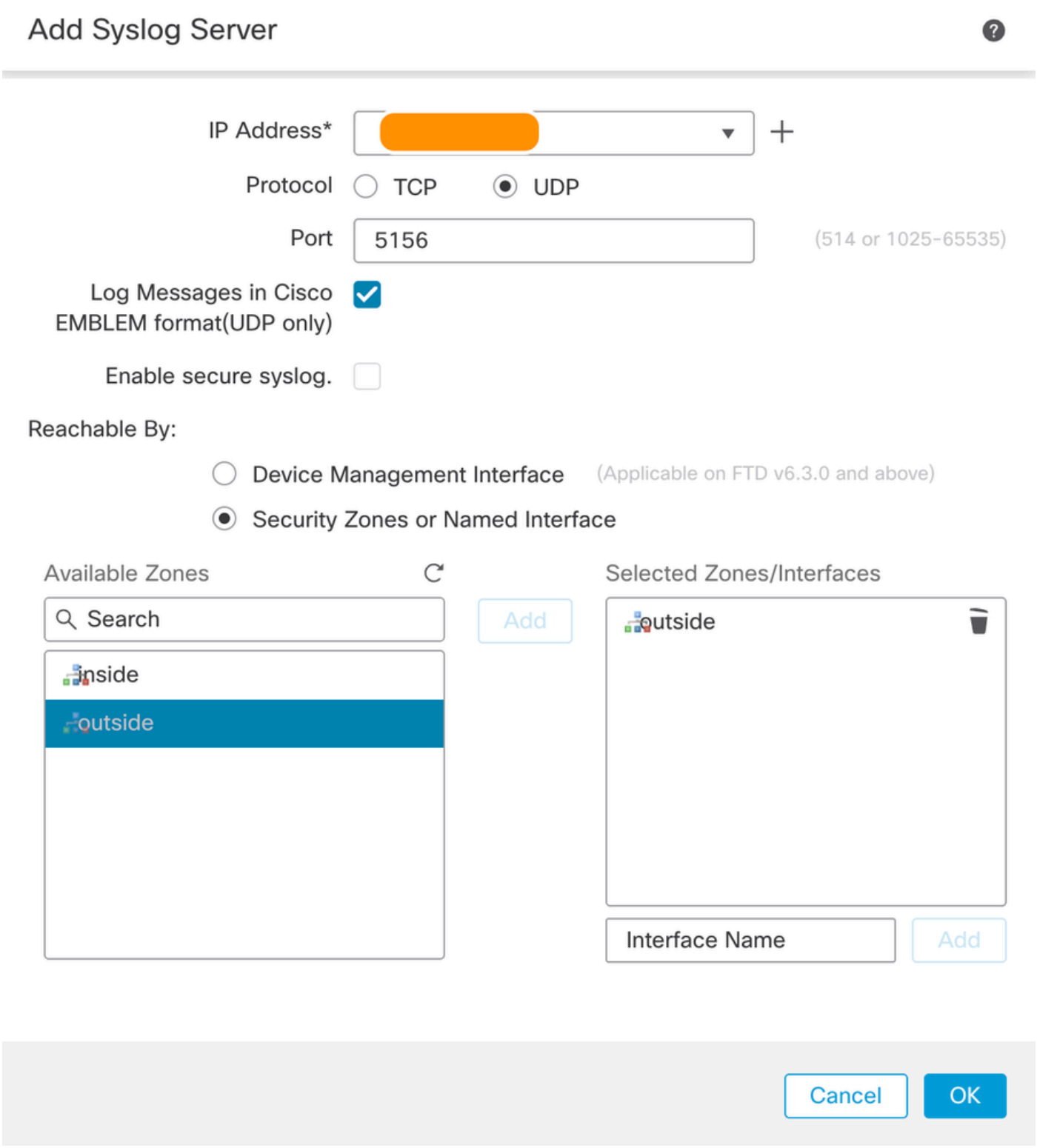
Schritt 1: Konfigurieren Sie die vorläufigen Syslog-Einstellungen auf dem FMC für das FTD unter Geräte > Plattformeinstellungen, um die Protokolle an den Syslog-Server zu senden, auf dem die Splunk-Instanz ausgeführt wird.



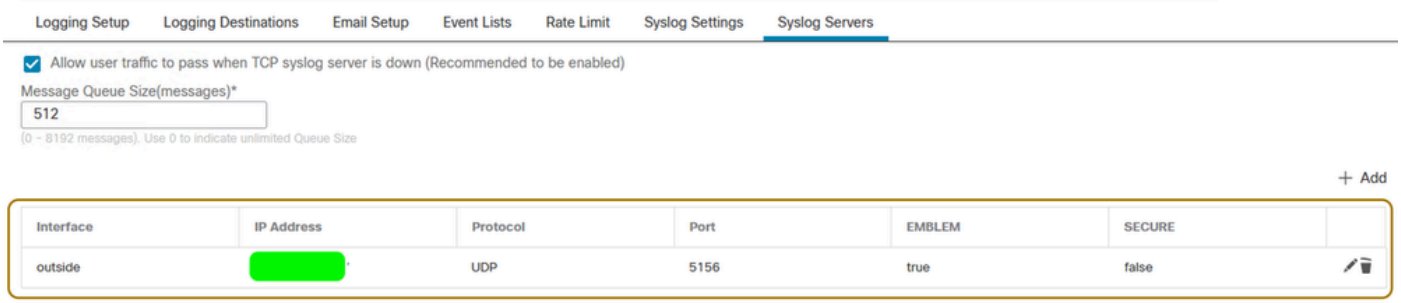
Plattformeinstellungen auf FTD - Syslog

Schritt 2: Konfigurieren Sie die IP-Adresse des Computers, auf dem die Splunk Enterprise-Instanz installiert ist und als Syslog-Server ausgeführt wird. Definieren Sie die Felder wie erwähnt.

```
IP Address: Fill in the IP address of the host acting as the syslog server
Protocol: TCP/UDP (usually UDP is preferred)
Port: You can choose any random high port. In this case 5156 is being used
Interface: Add the interface(s) through which you have connectivity to the server
```

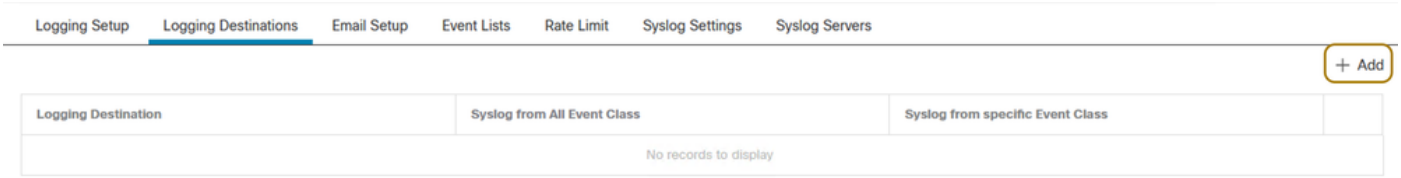


Plattformeinstellungen auf FTD - Syslog-Server hinzufügen

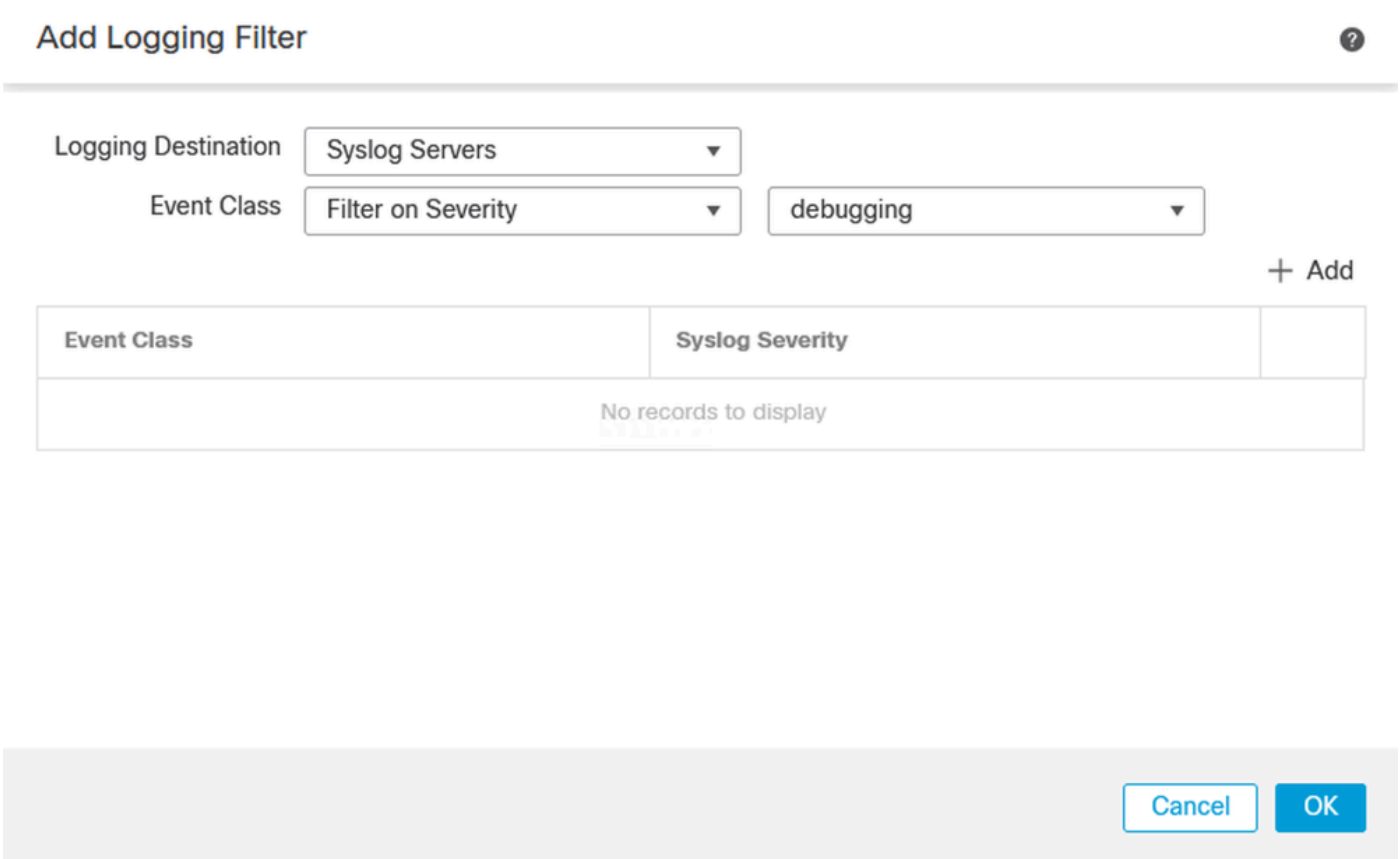


Plattformeinstellungen auf FTD - Syslog-Server hinzugefügt

Schritt 3: Fügen Sie ein Protokollierungsziel für Syslog-Server hinzu. Die Protokollierungsebene kann entsprechend Ihrer Auswahl oder Ihrem Anwendungsfall festgelegt werden.



Plattformeinstellungen auf FTD - Protokollziel hinzufügen



Plattformeinstellungen auf FTD - Schweregrad für Protokollierungsziel festlegen

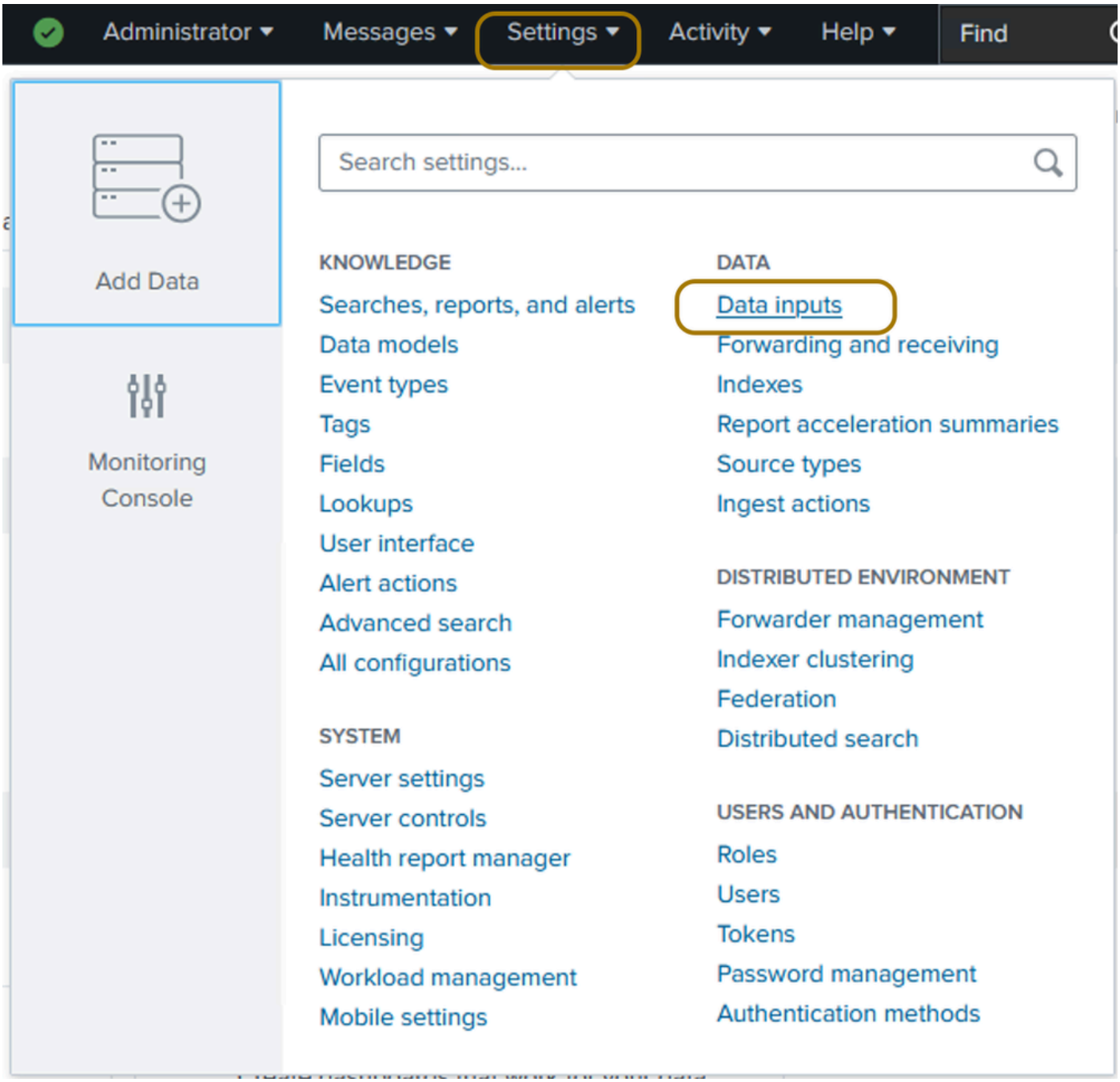
Stellen Sie die Änderungen der Plattformeinstellungen nach Abschluss dieser Schritte auf dem FTD bereit.

Konfigurieren einer Dateneingabe in der Splunk-Enterprise-Instanz

Schritt 1: Melden Sie sich bei der Webschnittstelle Ihrer Splunk Enterprise-Instanz an.

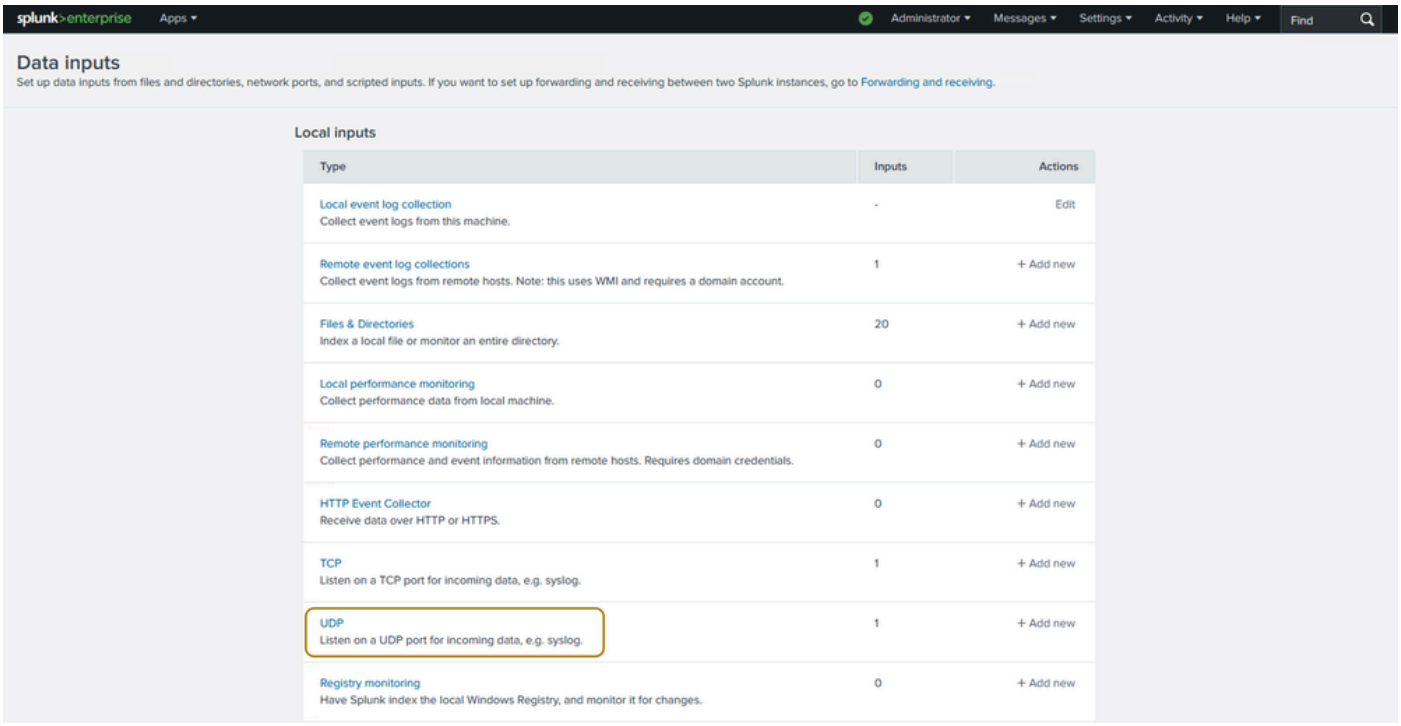
Splunk-Webschnittstelle - Anmeldeseite

Schritt 2: Definieren Sie eine Dateneingabe, damit Sie die Syslogs auf Splunk speichern und indizieren können. Navigieren Sie nach der Anmeldung zu Einstellungen > Daten > Dateneingaben.

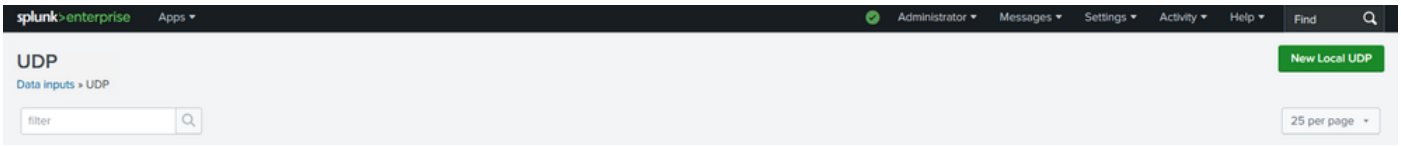


Navigieren zu Dateneingaben auf Splunk

Schritt 3. Wählen Sie UDP und klicken Sie auf der nächsten Seite auf New Local UDP.

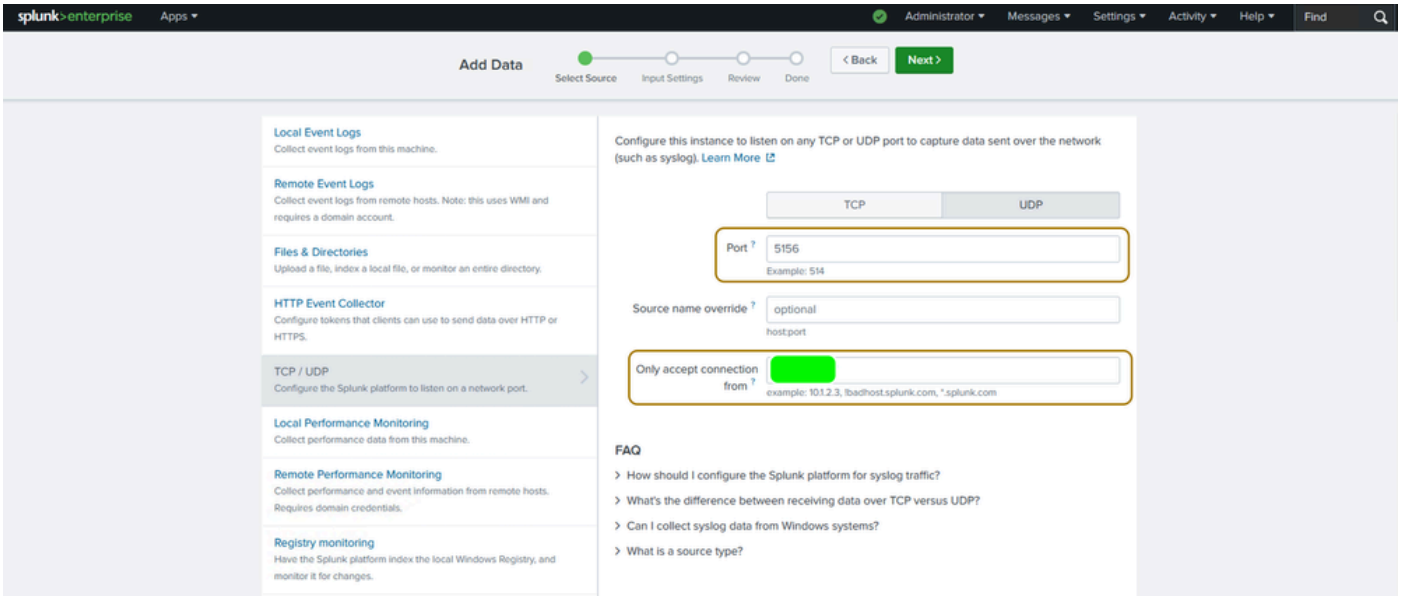


Klicken Sie auf "UDP" für eine UDP-Dateneingabe.



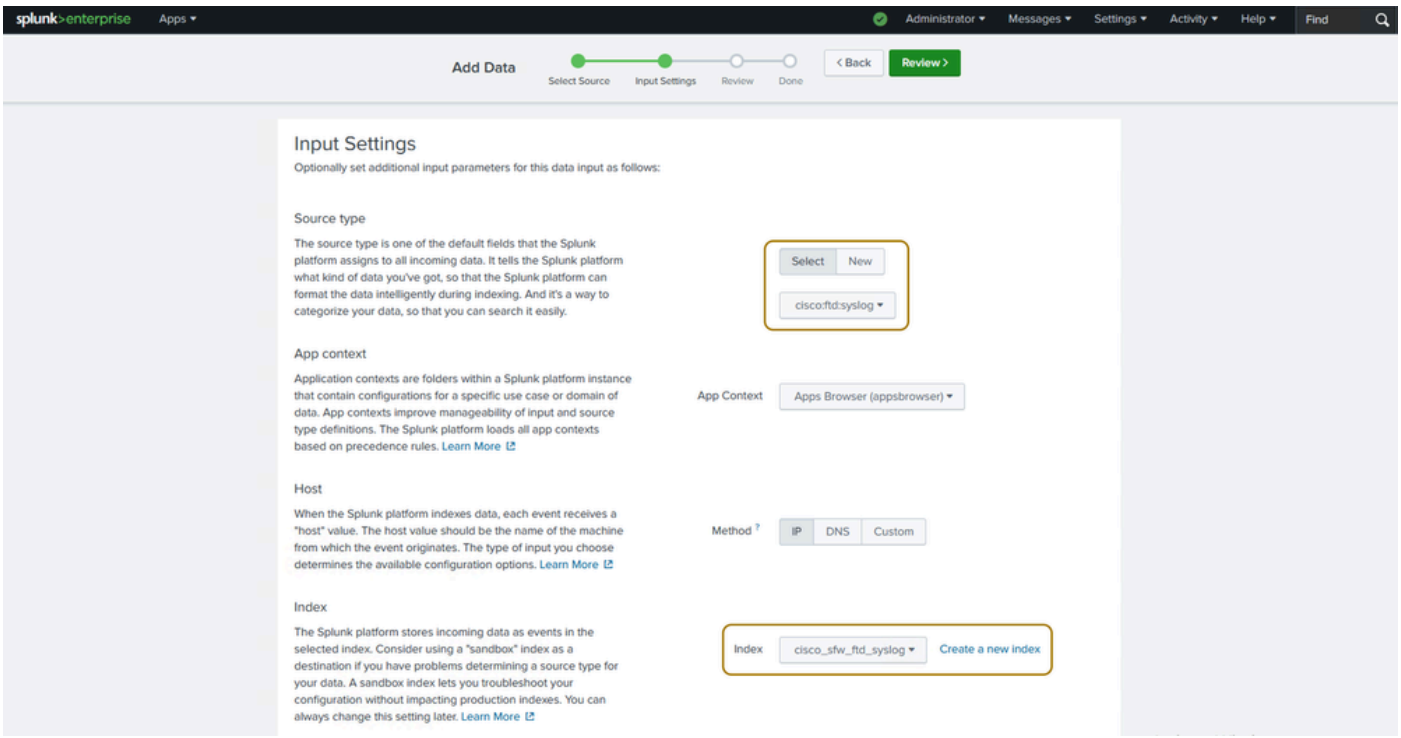
Neue lokale UDP-Eingabe erstellen

Schritt 4: Geben Sie den Port ein, an den die Syslogs gesendet werden. Dieser muss mit dem in den FTD-Syslog-Einstellungen konfigurierten Port übereinstimmen, in diesem Fall mit dem Port 5156. Um die Syslogs nur von einer Quelle (dem FTD) zu akzeptieren, setzen Sie das Feld Nur Verbindung akzeptieren von auf die IP-Adresse der Schnittstelle auf dem FTD, die mit dem Splunk-Server kommuniziert. Klicken Sie auf Next (Weiter).



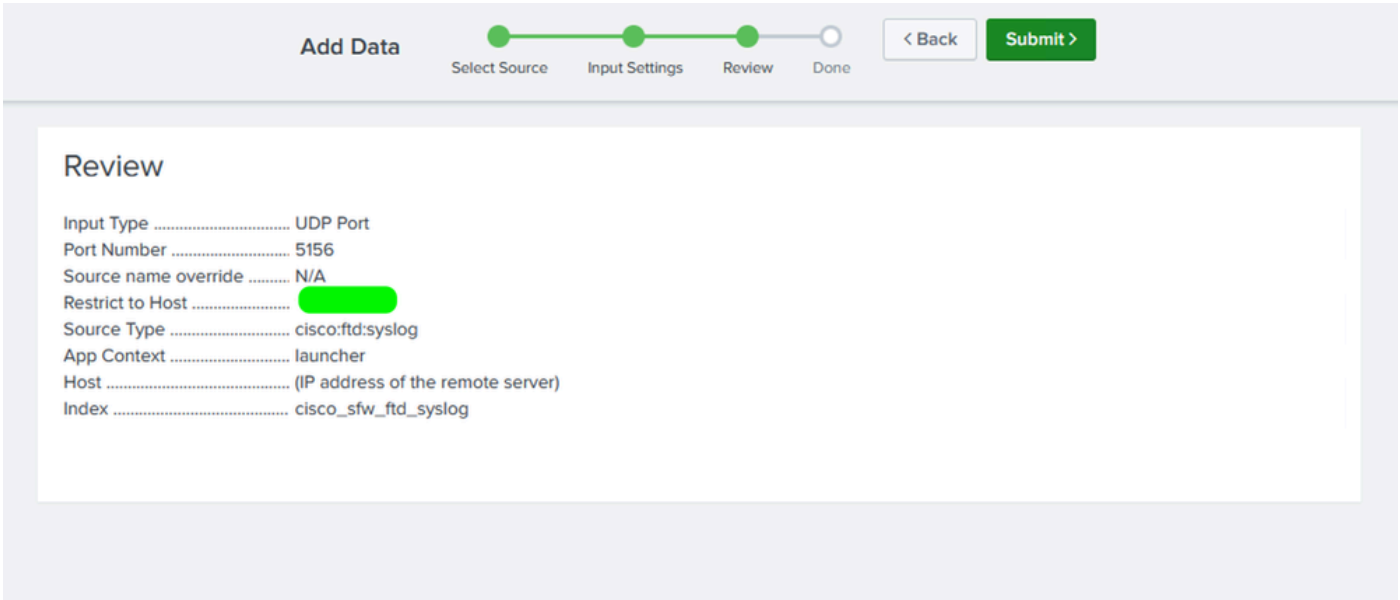
Port- und FTD-IP-Adresse angeben

Schritt 5: Sie können den Quelltyp und die Indexfeldwerte aus den vordefinierten Werten auf Splunk suchen und auswählen, wie im nächsten Bild hervorgehoben. Die Standardeinstellungen können für die übrigen Felder verwendet werden.



Einstellungen für die Dateneingabe konfigurieren

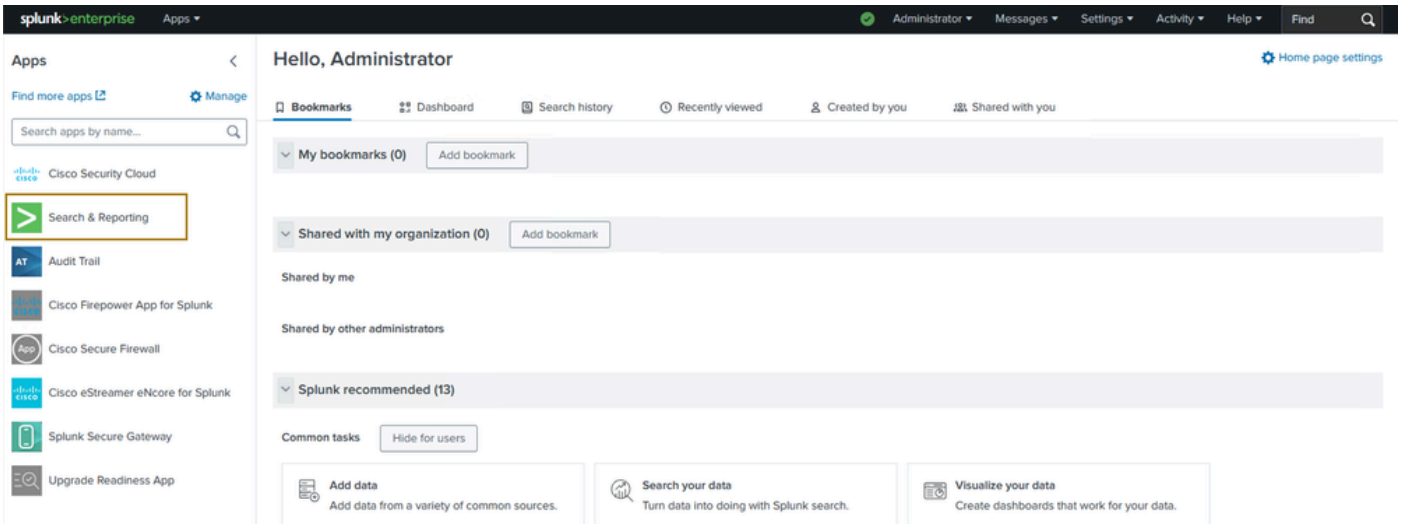
Schritt 6: Überprüfen Sie die Einstellungen, und klicken Sie auf Senden.



Einstellungen zur Dateneingabe überprüfen

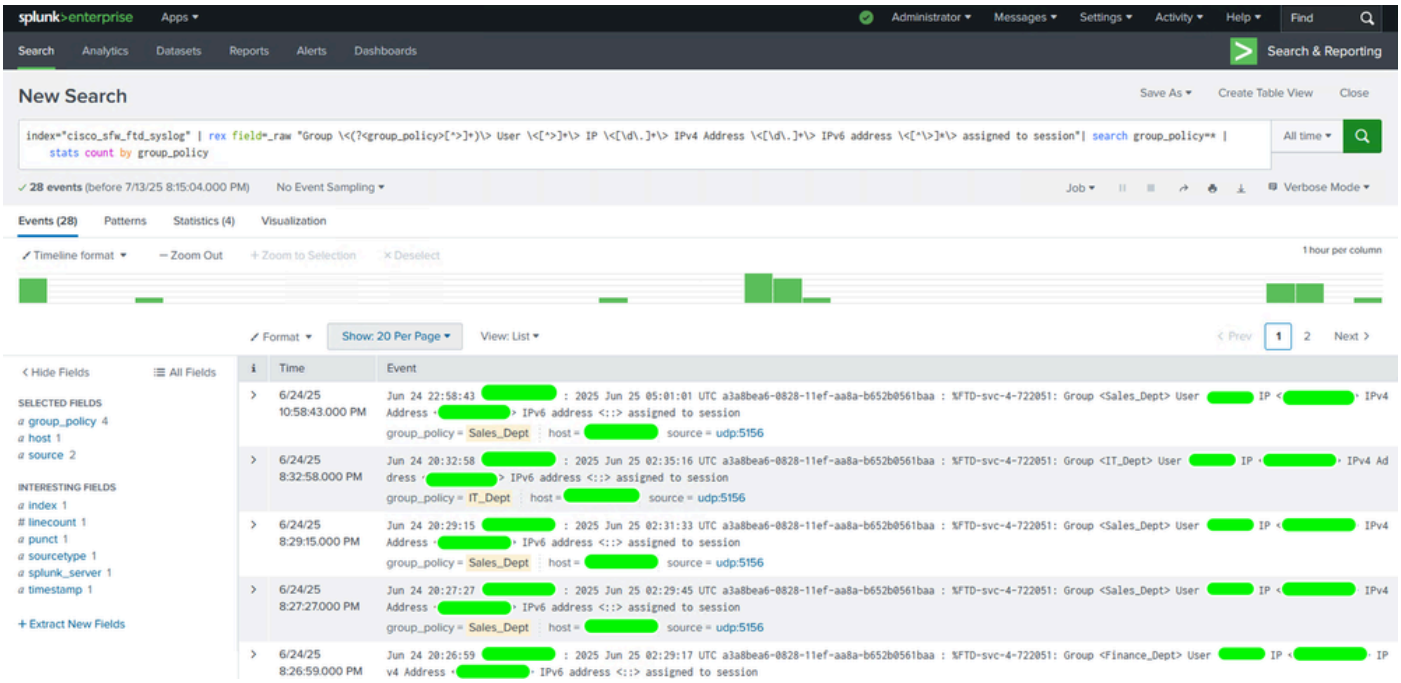
SPL-Abfragen ausführen und Dashboards erstellen

Schritt 1: Navigieren Sie zur App "Search and Reporting on Splunk".

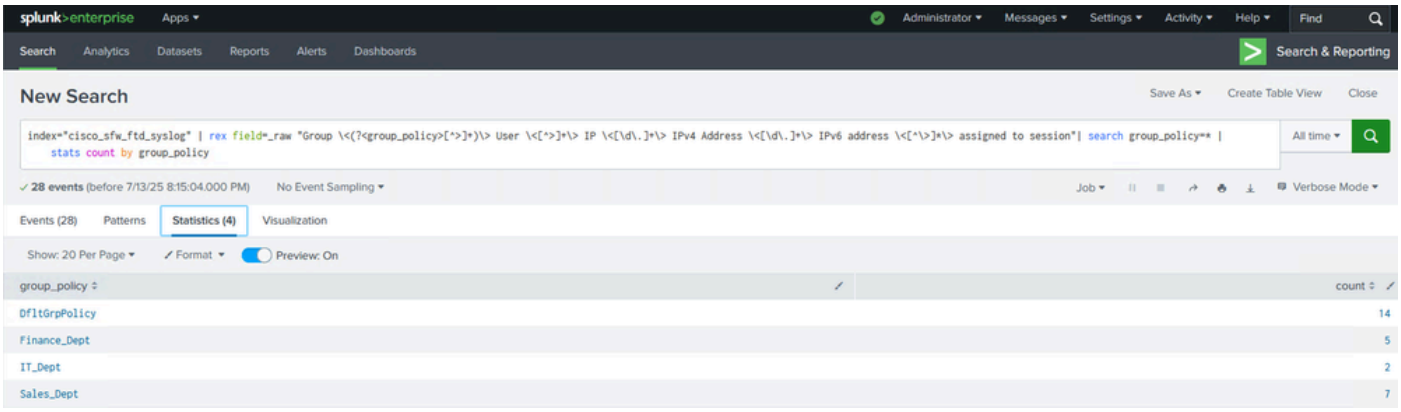


Navigieren Sie zur App "Suchen und Reporting".

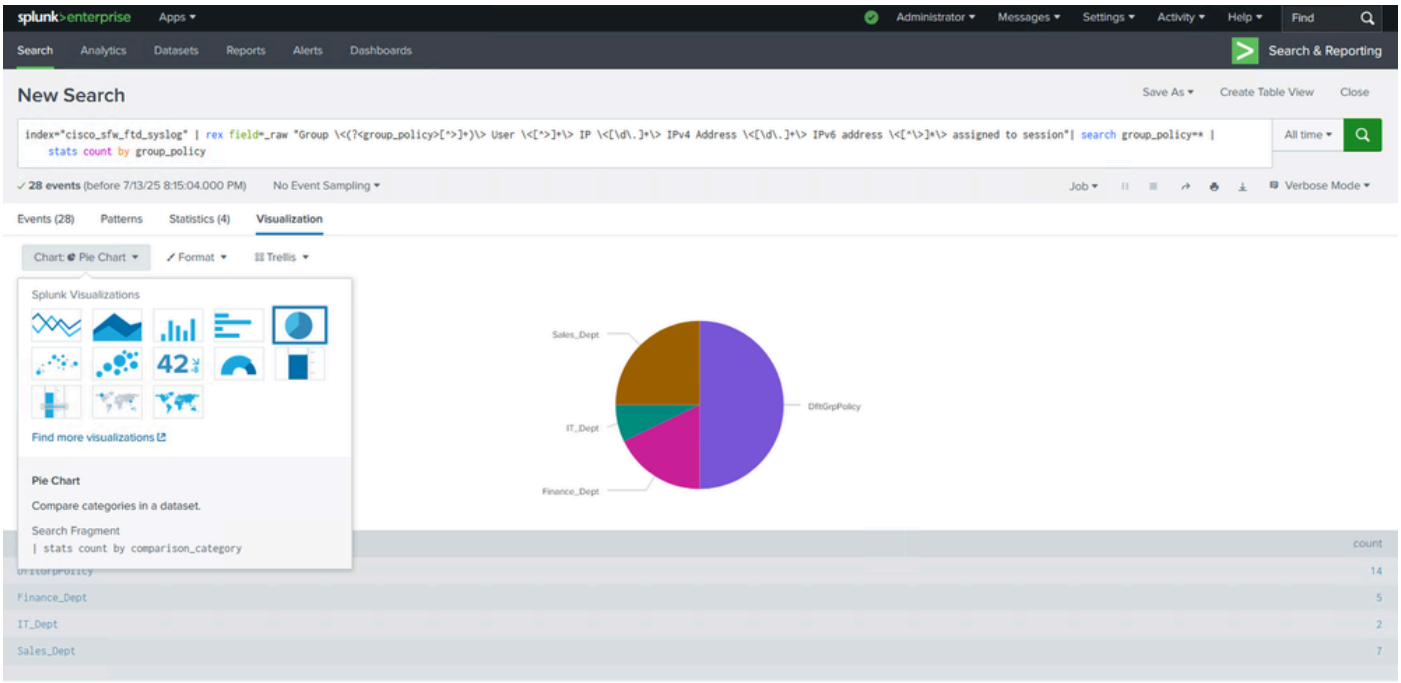
Schritt 2. Formulieren und führen Sie eine SPL-Abfrage entsprechend den Daten aus, die Sie visualisieren möchten. Sie können jedes Protokoll vollständig (im ausführlichen Modus) unter der Registerkarte Ereignisse sehen, die Anzahl der Verbindungen pro Gruppenrichtlinie in der Registerkarte Statistik und diese Daten mit diesen Statistiken unter der Registerkarte Visualisierung visualisieren.



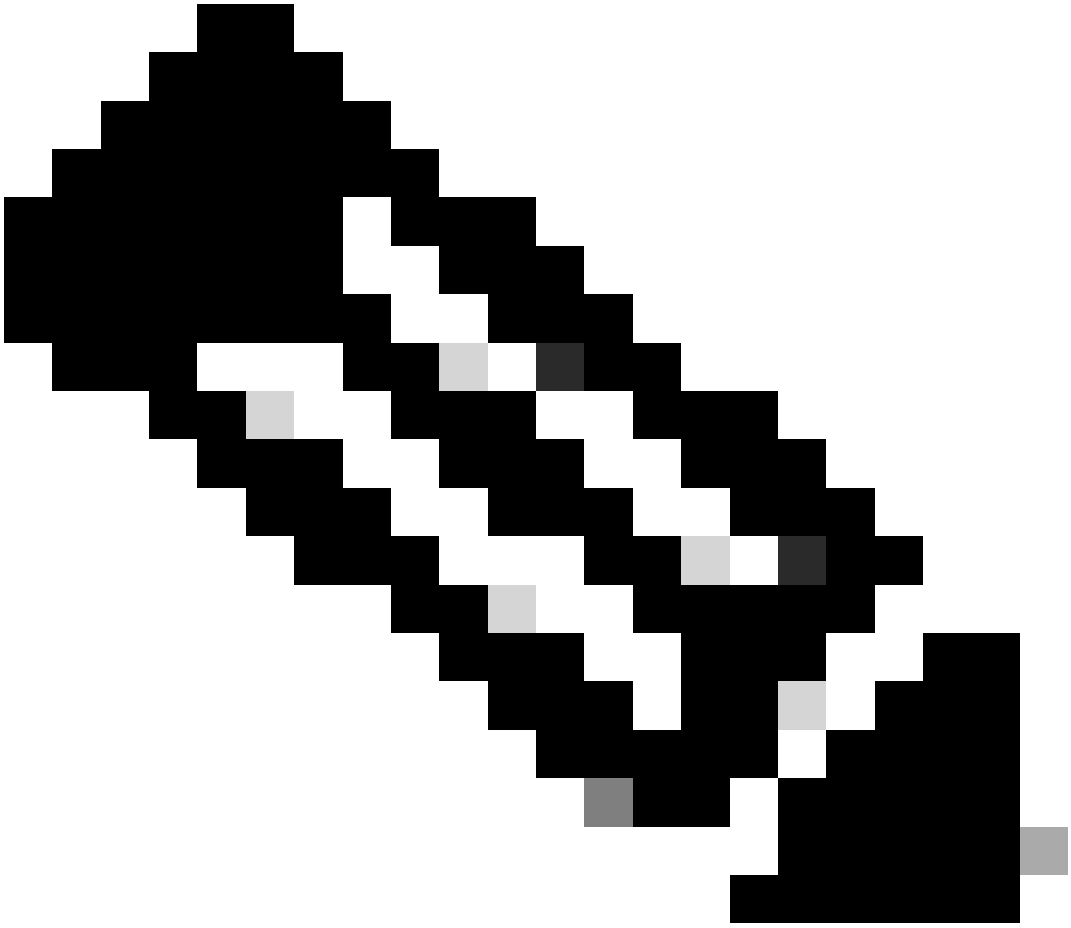
Suchen nach Ereignissen mithilfe von SPL-Abfragen



Registerkarte "Statistik" überprüfen

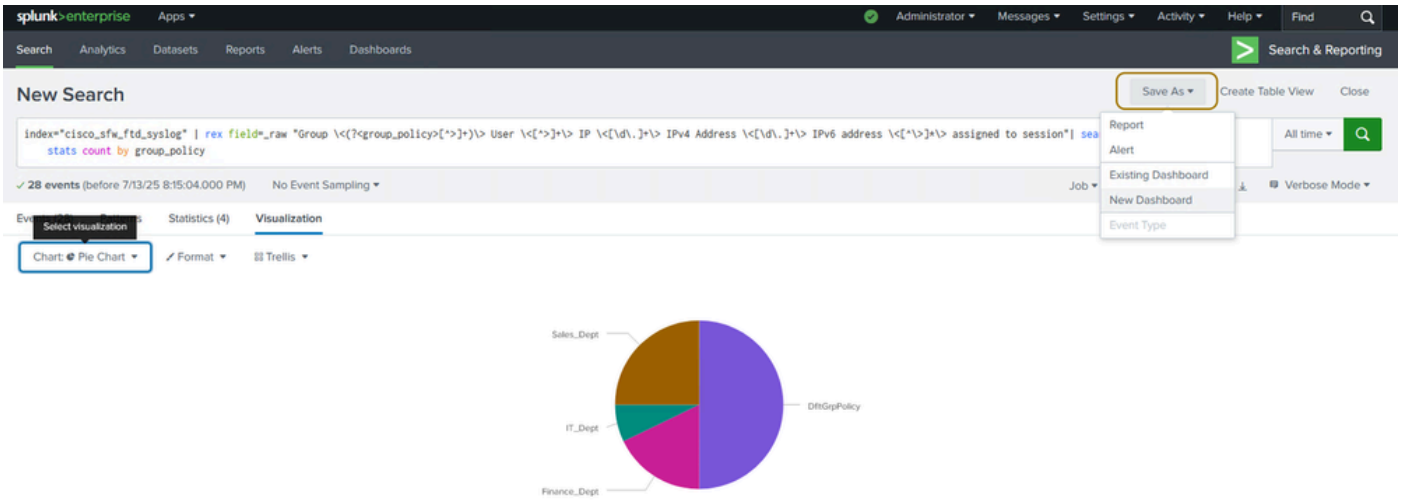


Auf der Registerkarte Visualisierung wird das Diagramm angezeigt.



Anmerkung: In diesem Beispiel werden durch die Abfrage Protokolle für erfolgreiche Remotezugriff-VPN-Verbindungen über verschiedene Gruppenrichtlinien abgerufen. Ein Tortendiagramm wurde verwendet, um die Anzahl und den Prozentsatz erfolgreicher Verbindungen pro Gruppenrichtlinie darzustellen. Je nach Ihren Anforderungen und Vorlieben können Sie auch eine andere Art der Visualisierung verwenden, z. B. einen Balkendiagramm.

Schritt 3. Klicken Sie auf Speichern unter und wählen Sie Neu oder Bestehendes Dashboard, je nachdem, ob Sie bereits ein Dashboard haben, dem Sie diesen Bereich hinzufügen möchten, oder ob Sie ein neues erstellen möchten. In diesem Beispiel wird das letzte Dashboard veranschaulicht.



Speichern des Panels in einem Dashboard

Schritt 4: Geben Sie einen Titel für das Dashboard, das Sie erstellen, und geben Sie einen Titel für das Bedienfeld ein, das das Tortendiagramm enthält.

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard — Edit ID

Description: Optional

Permissions: Private

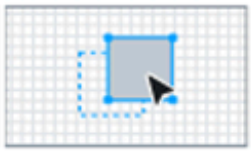
How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control



Grid
Quick organization

Panel Title: Successful RAVPN Connections Per Group Policy

Visualization Type: Pie Chart | Statistics Table

> Advanced Panel Settings

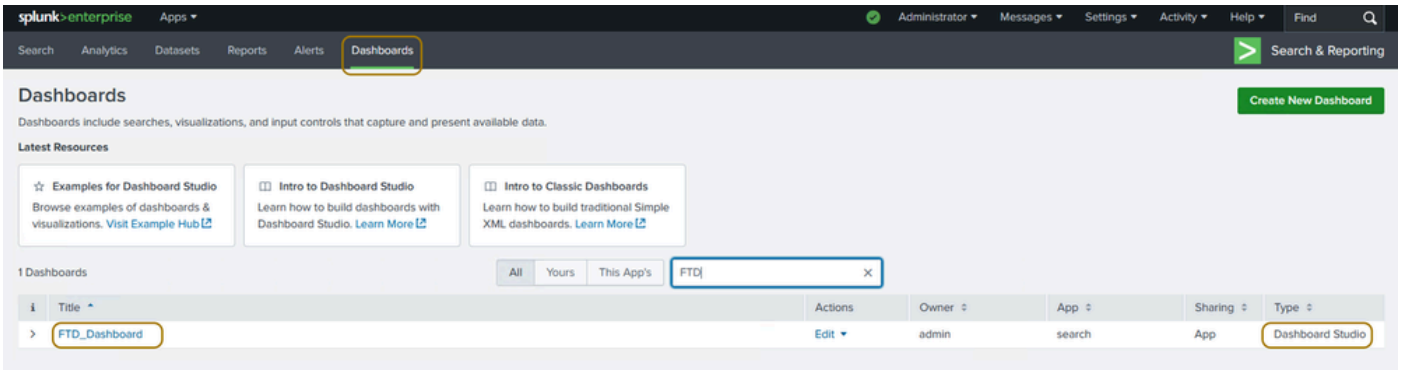
Cancel | Save to Dashboard

Einstellungen für das neue Dashboard

Sie können die Berechtigungen in App auf Privat oder Freigegeben festlegen, je nachdem, ob nur Sie das Dashboard anzeigen sollen oder andere Benutzer mit Zugriff auf die Splunk-Instanz ebenfalls zugelassen sind. Wählen Sie außerdem je nachdem, ob Sie eine präzise Kontrolle über die Panel-Einstellungen und das Layout des Dashboards wünschen oder nicht, den Modus Classic oder Dashboard Studio aus, um Ihr Dashboard zu erstellen.

Schritt 5 (optional). Führen Sie weitere SPL-Abfragen in diesem Dashboard als Bedienfelder aus, und speichern Sie sie entsprechend Ihren Anforderungen. Gehen Sie dazu wie zuvor beschrieben vor.

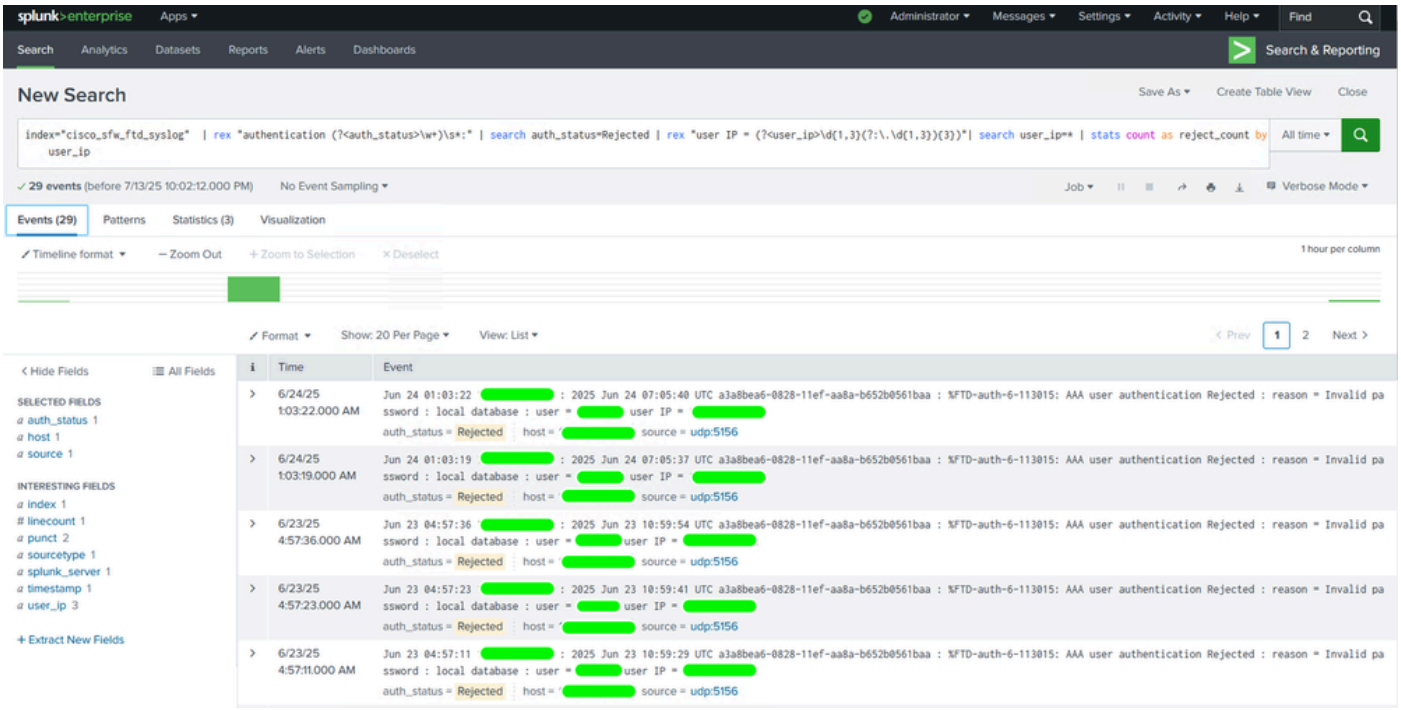
Schritt 6: Navigieren Sie zur Registerkarte Dashboard, um das erstellte Dashboard zu suchen und auszuwählen. Klicken Sie darauf, um die zugehörigen Bereiche anzuzeigen, zu bearbeiten oder neu anzuordnen.



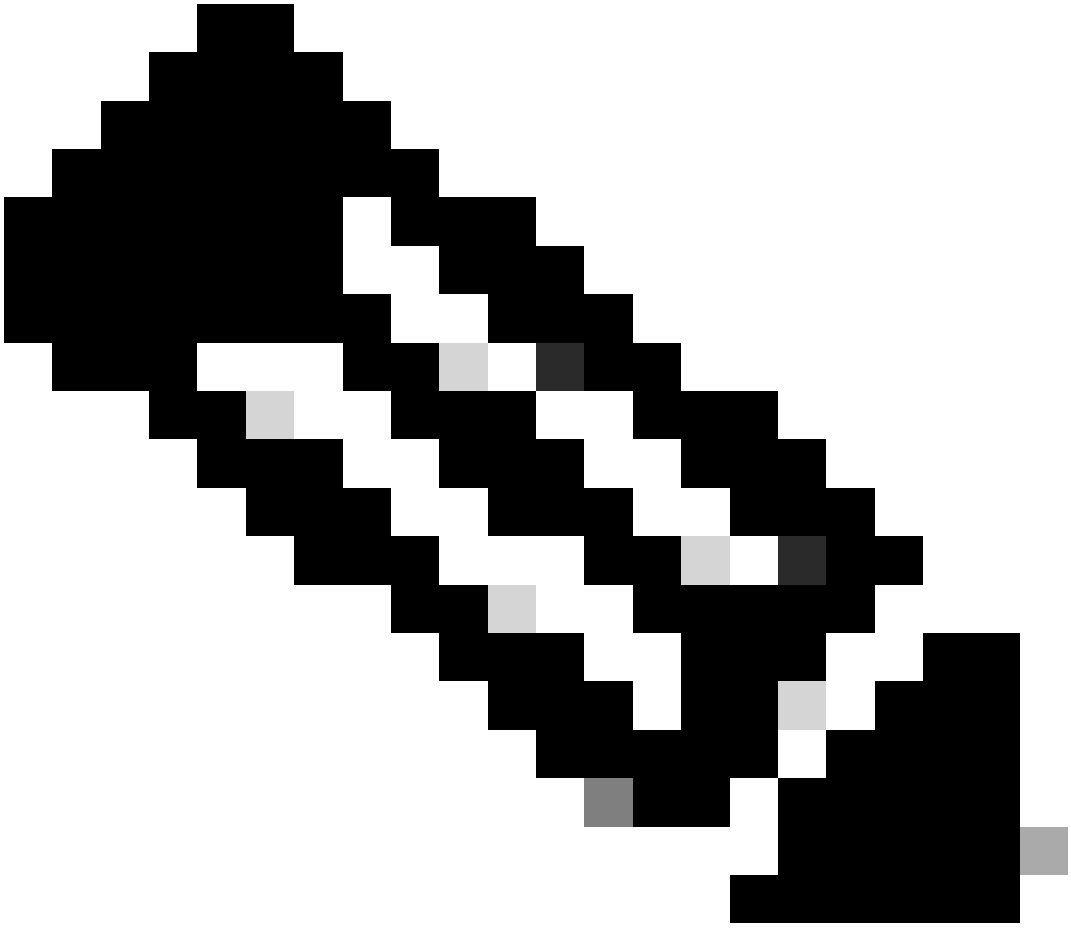
Anzeigen des Dashboard

Warnmeldungen auf Basis von SPL-Abfragen konfigurieren

Schritt 1: Navigieren Sie zur Such- und Reporting-App, um Ihre SPL-Abfrage zu erstellen und auszuführen, damit sichergestellt ist, dass die richtigen Protokolle abgerufen werden, die zum Auslösen der Warnung verwendet werden.



Ausführen von SPL-Abfragen zum Erstellen entsprechender Warnungen



Anmerkung: In diesem Beispiel wird die Abfrage verwendet, um fehlgeschlagene Authentifizierungsprotokolle für das Remotezugriffs-VPN abzurufen, um Warnungen auszulösen, wenn die Anzahl der fehlgeschlagenen Versuche innerhalb eines bestimmten Zeitraums einen bestimmten Schwellenwert überschreitet.

Schritt 3: Klicken Sie auf Speichern unter und wählen Sie Warnmeldung.

Warnmeldung speichern

Schritt 4: Geben Sie einen Titel für die Warnmeldung ein. Geben Sie alle weiteren Details und Parameter ein, die für die Konfiguration der Warnmeldung erforderlich sind, und klicken Sie auf

Speichern. Die für diese Warnung verwendeten Einstellungen wurden hier erwähnt.

<#root>

Permissions: Shared in App.
Alert Type: Real-time (allows failed user authentications in the last 10 minutes can be tracked continu
Trigger Conditions: A

custom

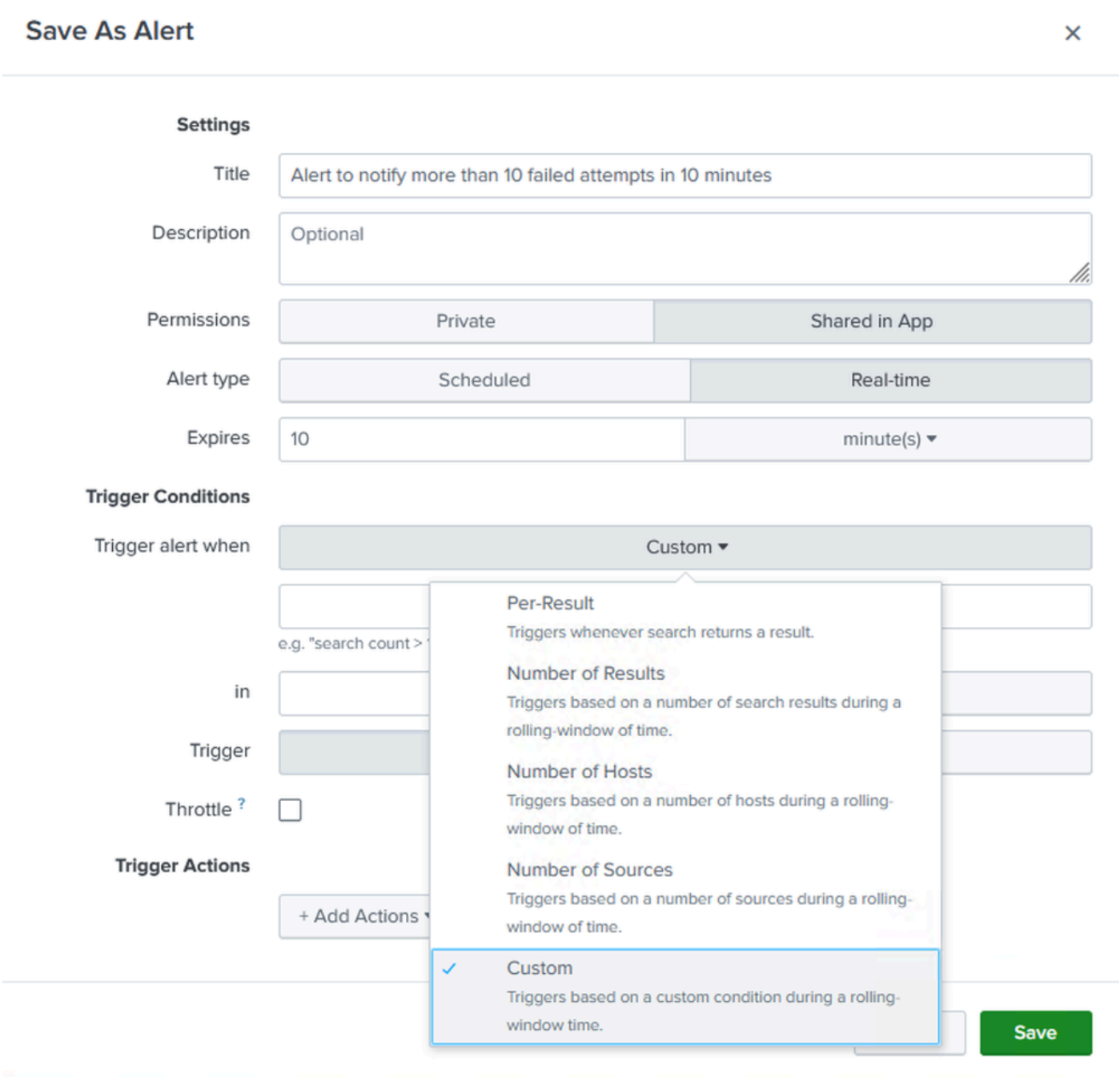
condition is used to search if the

reject_count

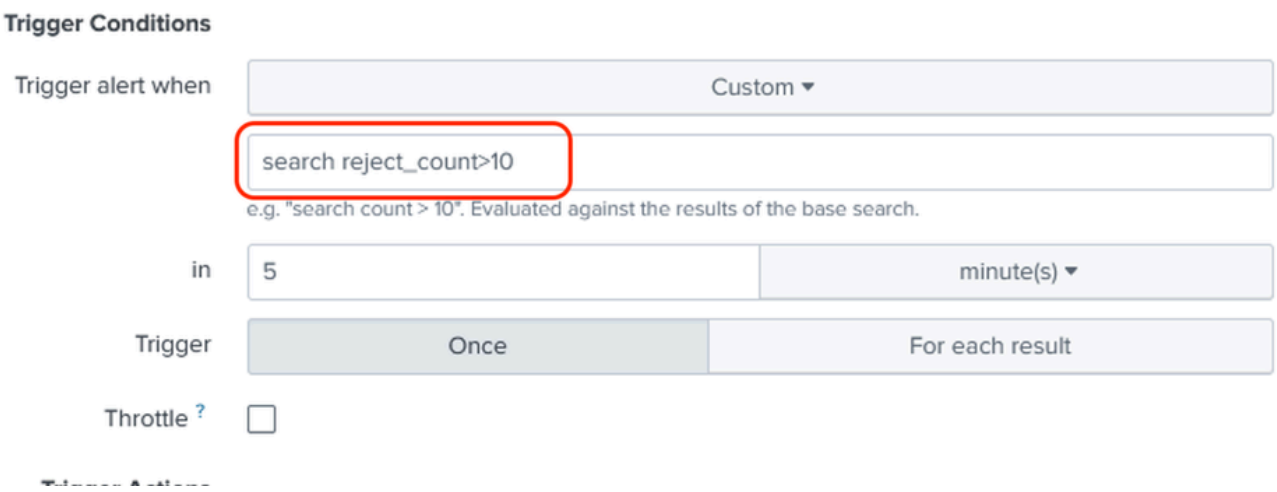
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

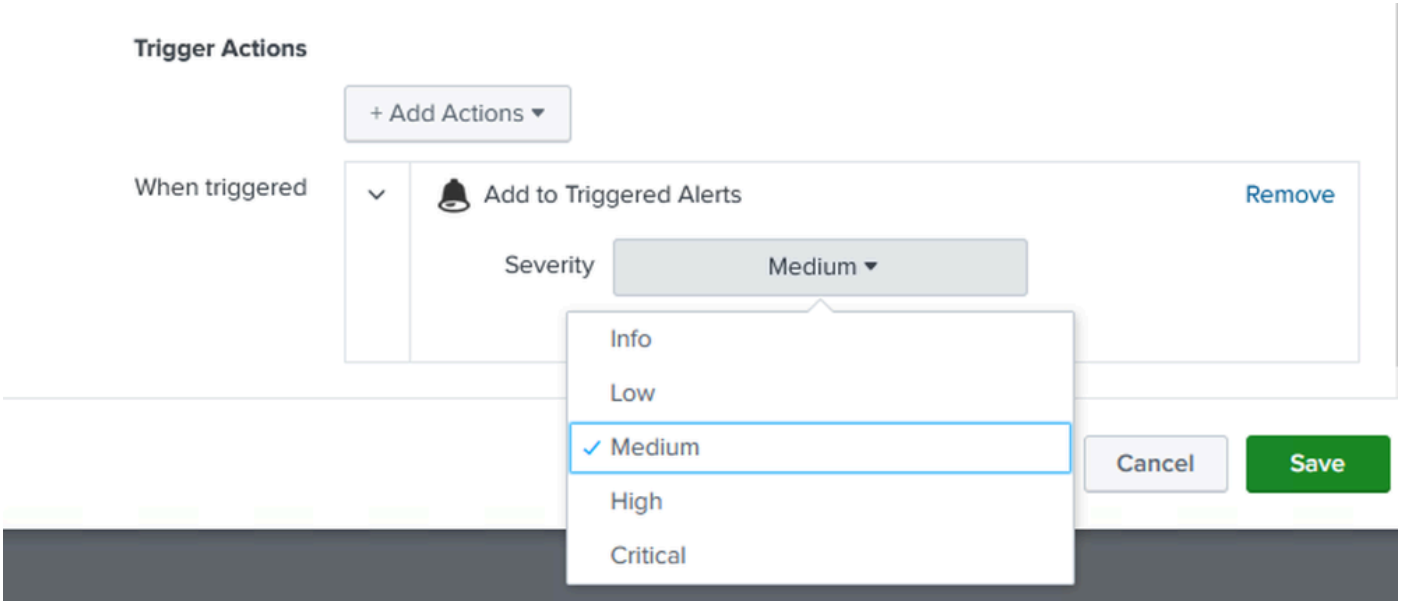
and set the alert severity as per your requirement.



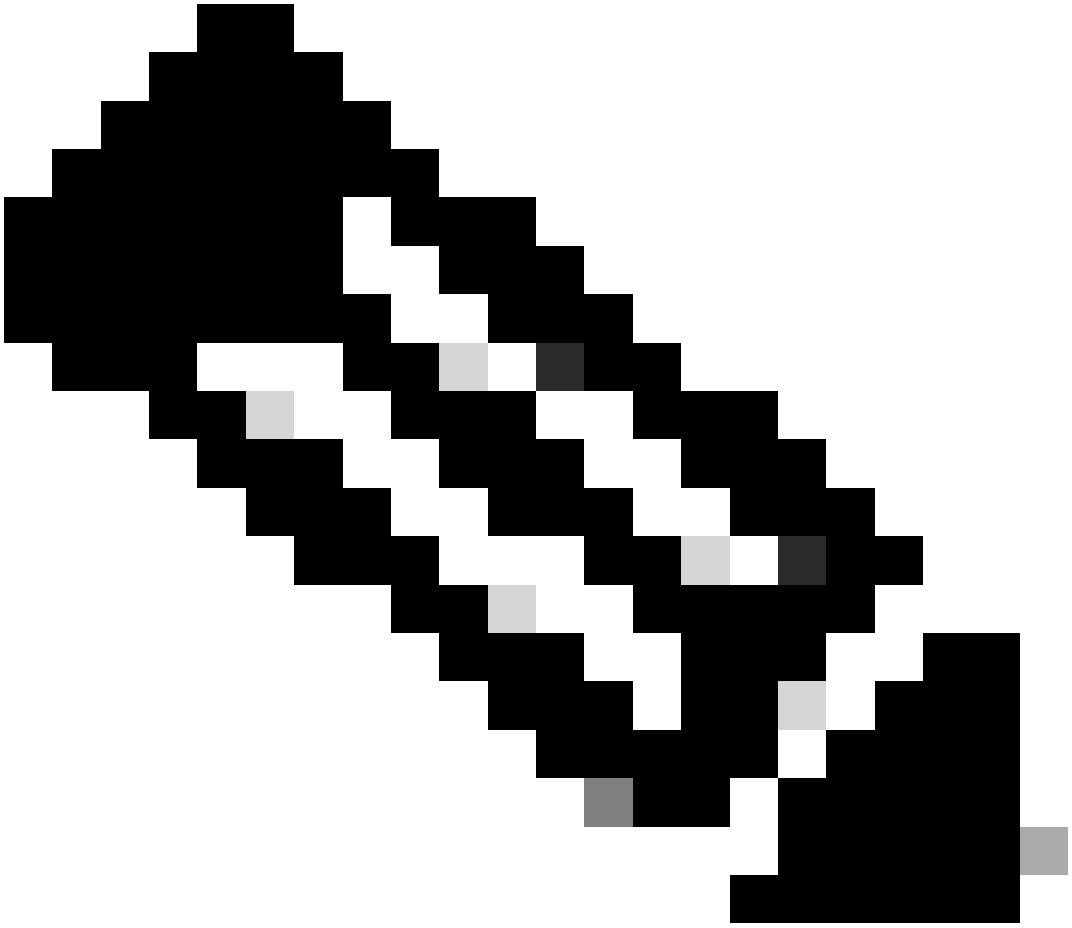
Zusätzliche Einstellungen für die Warnungserstellung



Zusätzliche Einstellungen für die Warnungserstellung



Zusätzliche Einstellungen für die Warnungserstellung



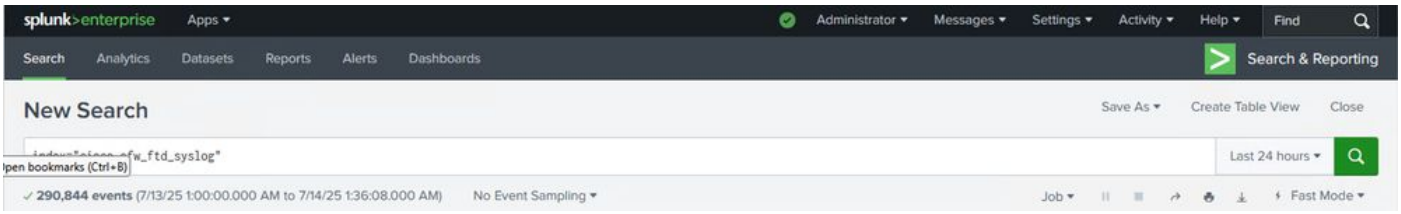
Anmerkung: Wenn Sie die Warnungen für jedes Ergebnis auslösen möchten, müssen Sie auch die Drosselungseinstellungen entsprechend definieren.

Überprüfung

Nachdem Sie die Dashboard- und Warnmeldungen erstellt haben, können Sie die Konfigurationen, den Datenfluss, die Dashboards und die Echtzeit-Warnmeldungen anhand der Anweisungen in diesem Abschnitt überprüfen.

Protokolle anzeigen

Mit der Such-App können Sie überprüfen, ob die von der Firewall gesendeten Protokolle empfangen und für den Splunk-Suchkopf sichtbar sind. Dies kann überprüft werden, indem die neuesten indizierten Protokolle (Suchindex = "cisco_sfw_ftd_syslog") und der zugehörige Zeitstempel überprüft werden.

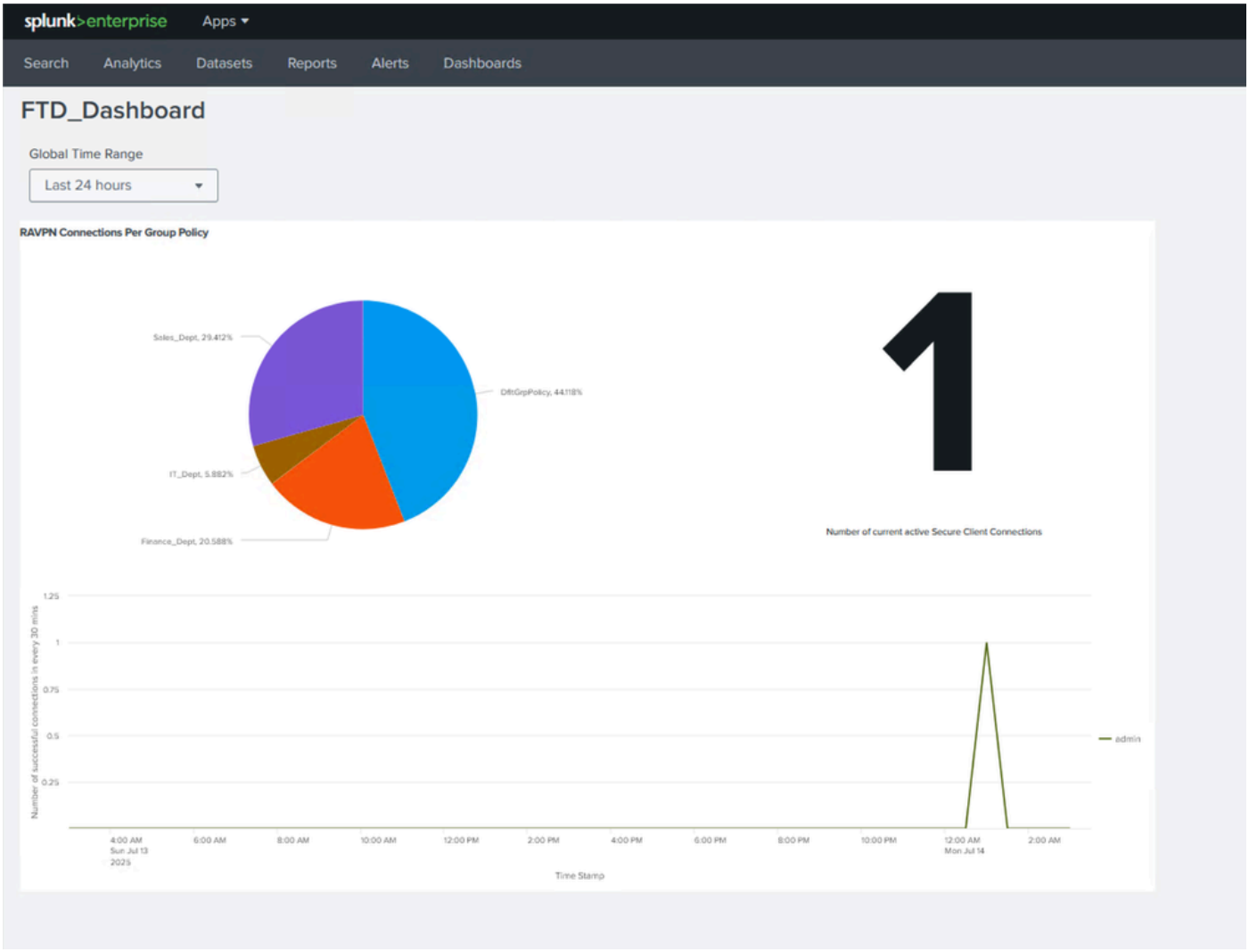


Protokolle überprüfen und anzeigen

Protokolle überprüfen und anzeigen

Anzeigen der Echtzeit-Dashboards

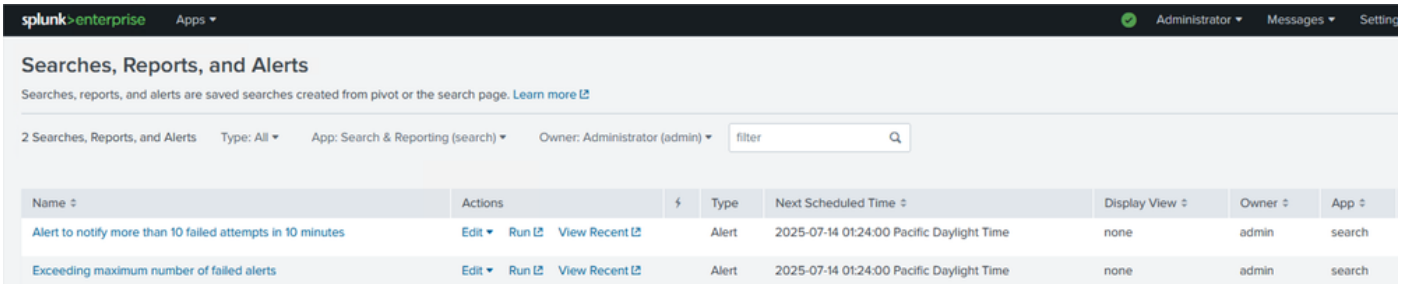
Sie können zum benutzerdefinierten Dashboard navigieren, das Sie erstellt haben, und die Änderungen in jedem der Bereiche anzeigen, wenn neue Daten und Protokolle aus dem FTD generiert werden.



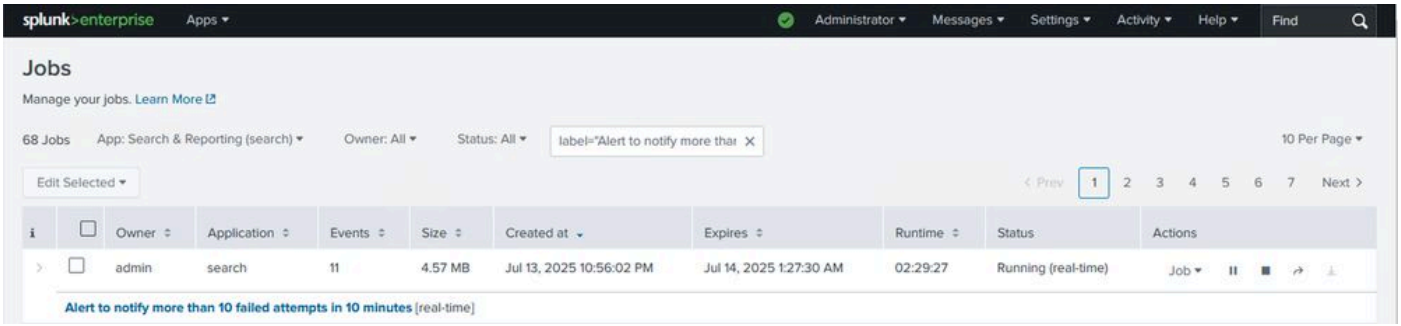
Dashboards anzeigen

Prüfen, ob Warnungen ausgelöst wurden

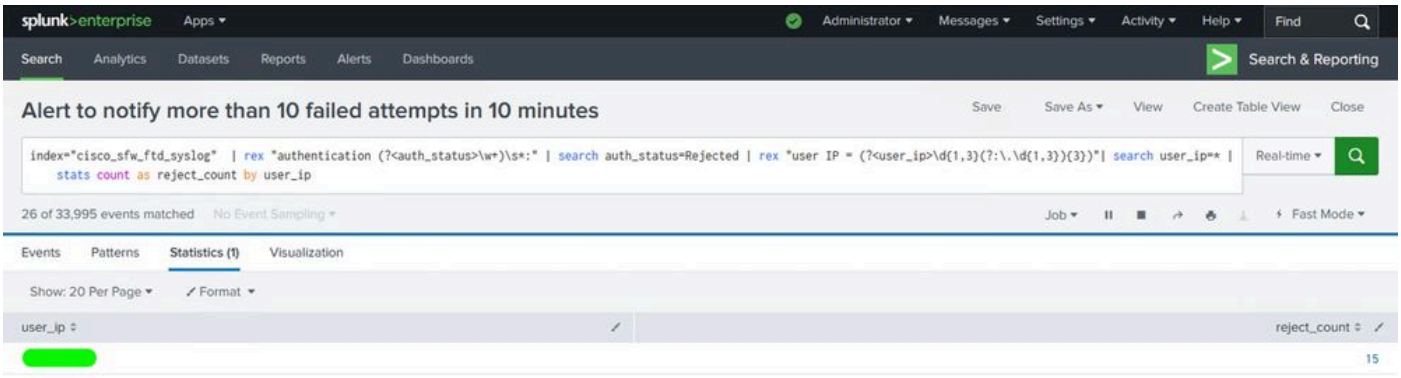
Um die Informationen zu den Warnungen zu überprüfen, können Sie zum Abschnitt Suchen, Berichte und Warnungen navigieren, um die letzten Warnungsinformationen anzuzeigen. Klicken Sie auf Letzte anzeigen, um weitere Informationen zu den Jobs und Suchen zu erhalten.



Warnungen prüfen und anzeigen



Warnungen prüfen und anzeigen



Statistiken für ausgelöste Warnmeldungen überprüfen

Informationen zu dieser Übersetzung

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