

Create Custom Dashboards and Alerts on Splunk using Syslogs from FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Configure Syslog Settings for the FTD](#)

[Configure a Data Input on the Splunk Enterprise Instance](#)

[Execute SPL Queries and Create Dashboards](#)

[Configure Alerts Based on SPL Queries](#)

[Verify](#)

[View Logs](#)

[View the Real-time Dashboards](#)

[Check if Any Alerts Have Been Triggered](#)

Introduction

This document describes a step-by-step walkthrough for configuring FTD to send syslogs to Splunk and using those logs to build custom dashboards and alerts.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before going through this configuration guide:

- Syslog
- Basic knowledge of Splunk's Search Processing Language (SPL)

This document also assumes that you already have Splunk Enterprise instance installed on a server and have access to the web interface.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firepower Threat Defense (FTD) running on version 7.2.4
- Cisco Firepower Management Center (FMC) running on version 7.2.4

- Splunk Enterprise instance (version 9.4.3) running on a Windows machine

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Background Information

Cisco FTD devices generate detailed syslogs covering intrusion events, access control policies, connection events, and more. Integrating these logs with Splunk enables powerful analysis and real-time alerting for network security operations.

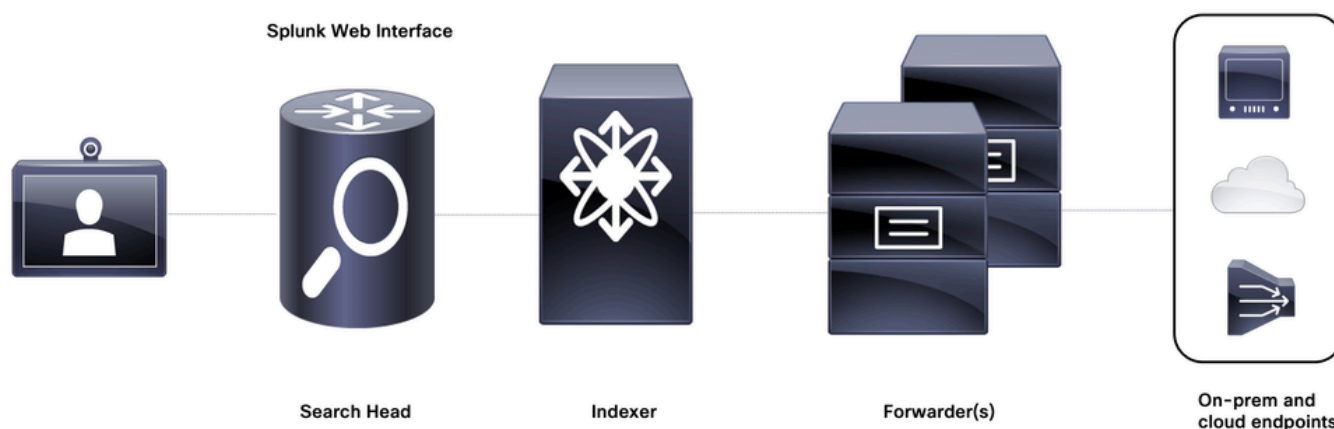
Splunk is a real-time data analytics platform designed to ingest, index, search, and visualize machine-generated data. Splunk is especially effective in cybersecurity environments as a Security Information and Event Management (SIEM) tool due to its ability to:

- Ingest log data at scale
- Perform complex searches with SPL
- Create dashboards and alerts
- Integrate with security orchestration and incident response systems

Splunk processes data through a structured pipeline in order to make unstructured or semi-structured machine data useful and actionable. The key stages of this pipeline are often referred to as **IPIS** which stands for:

- Input
- Parsing
- Indexing
- Searching

The main broad components of the underlying architecture which are used to realize the IPIS pipeline are shown in this diagram:



Splunk underlying architecture

Configure

Network Diagram

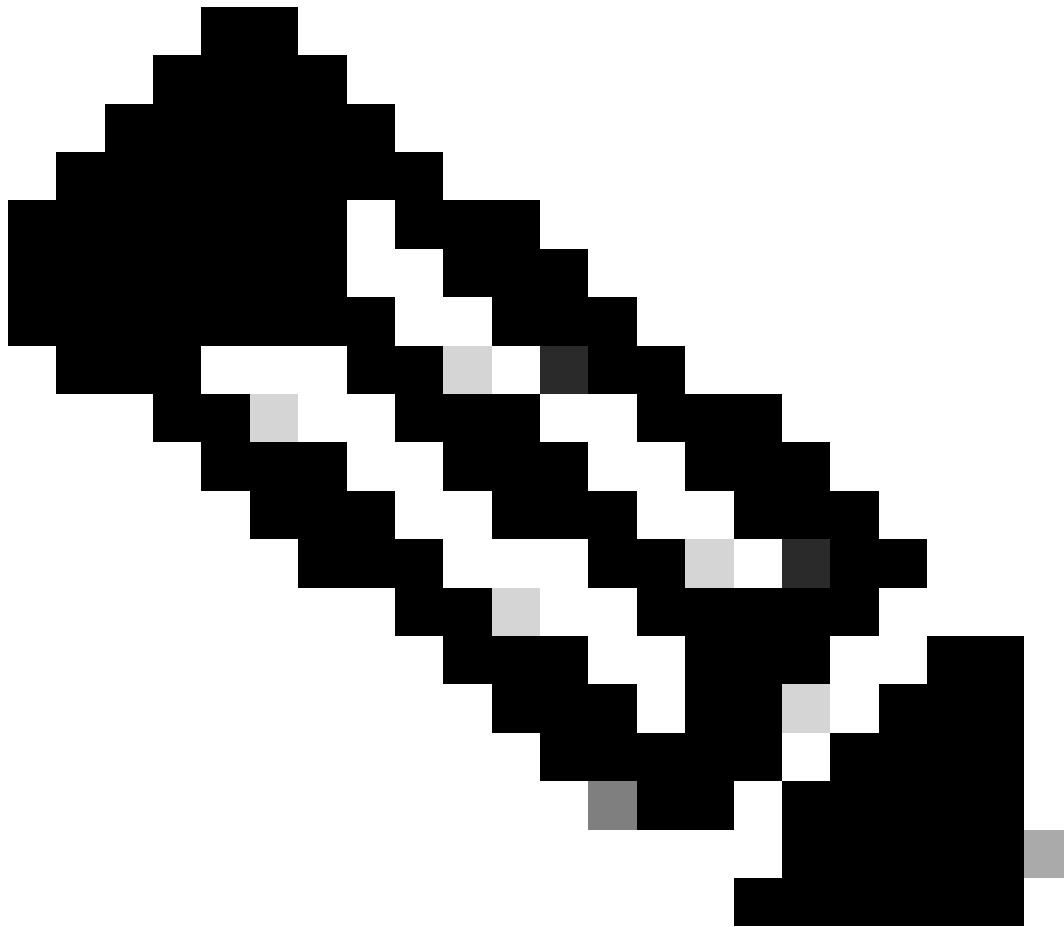


**Firepower Threat
Defense device**



**Syslog server with the
Splunk Search Head**

Network Diagram



Note: The lab environment for this document does not require separate forwarder and indexer instances. The windows machine, that is, the syslog server on which the Splunk Enterprise instance is installed is acting as the indexer and the search head.

Configurations

Configure Syslog Settings for the FTD

Step 1. Configure the preliminary syslog settings on FMC for the FTD under **Devices > Platform Settings** in order to send the logs to the syslog server on which the Splunk instance is running.

FTD-PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

Basic Logging Settings

☒ Enable Logging

☐ Enable Logging on the failover standby unit

☒ Send syslogs in EMBLEM format

☒ Send debug messages as syslogs

Memory Size of the Internal Buffer

52428700

(4096-52428800 Bytes)

VPN Logging Settings

☒ Enable Logging to Firewall Management Center

Logging Level

debugging

Specify FTP Server Information

Platform Settings on FTD - Syslog

Step 2. Configure the IP address of the machine where the Splunk Enterprise instance is installed and running as a **Syslog Server**. Define the fields as mentioned.

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

Add Syslog Server



IP Address* +

Protocol ☐ TCP ☒ UDP

Port (514 or 1025-65535)

Log Messages in Cisco
EMBLEM format(UDP only) ☒

Enable secure syslog. ☐

Reachable By:

- ☐ Device Management Interface (Applicable on FTD v6.3.0 and above)
- ☒ Security Zones or Named Interface

Available Zones



Add

inside
outside

Selected Zones/Interfaces

outside



Interface Name

Add

Cancel

OK

Platform Settings on FTD - Add Syslog Server

Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers

☒ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*

(0 ~ 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

Interface	IP Address	Protocol	Port	EMBLEM	SECURE	
outside	192.168.1.1	UDP	5156	true	false	

Step 3. Add a logging destination for **Syslog Servers**. The logging level can be set according to your choice or use case.

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

+ Add

Logging Destination	Syslog from All Event Class	Syslog from specific Event Class	
No records to display			

Add Logging Filter

?

Logging Destination

Syslog Servers

Event Class

Filter on Severity

debugging

+ Add

Event Class	Syslog Severity	
No records to display		

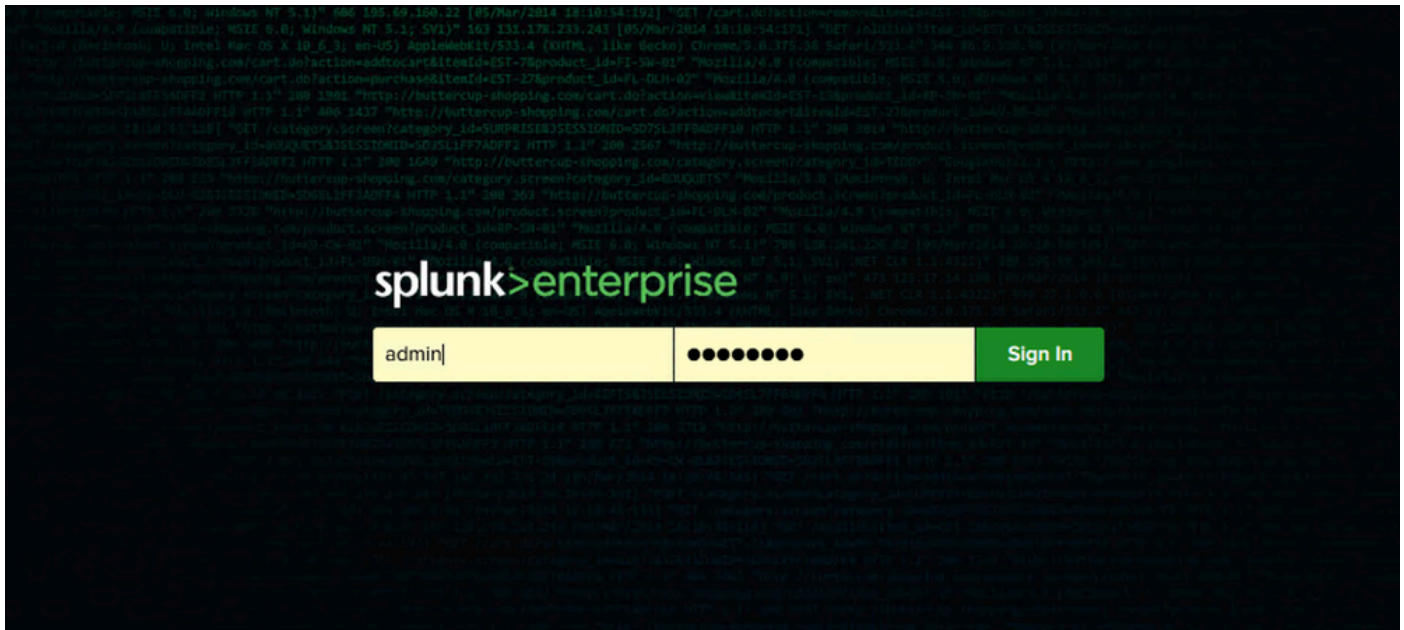
Cancel

OK

Deploy the platform setting changes onto the FTD after completing these steps.

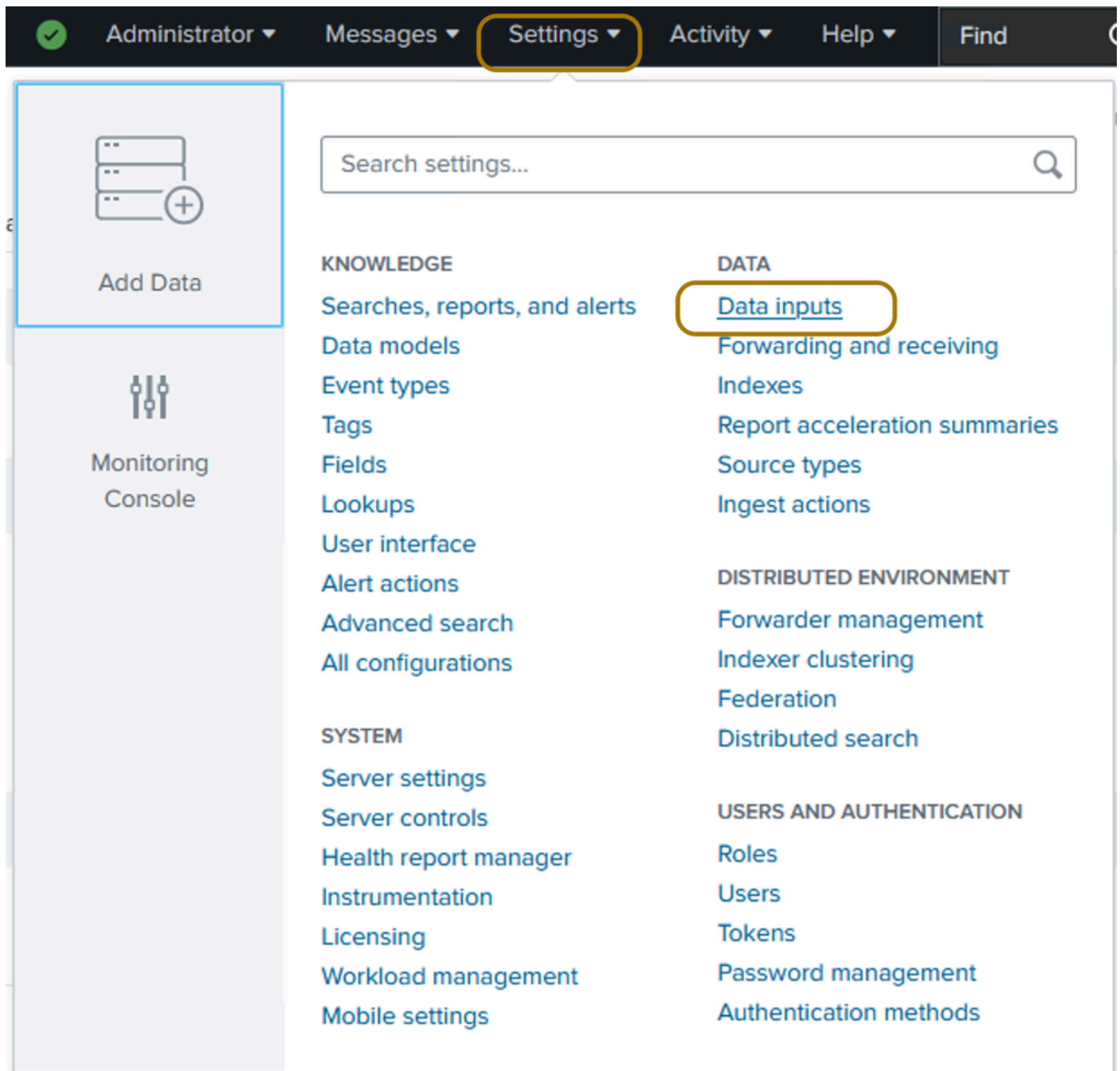
Configure a Data Input on the Splunk Enterprise Instance

Step 1. Login to your Splunk Enterprise instance web interface.



Splunk Web Interface Login Page

Step 2. You must define a **Data Input** so that you can store and index the syslogs on Splunk. Navigate to **Settings > Data > Data Inputs** after logging in.



Navigate to Data Inputs on Splunk

Step 3. Choose UDP and then click on **New Local UDP** on the next page that appears.

Local inputs		
Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	20	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	0	+ Add new

Click on 'UDP' for a UDP Data Input

splunk>enterprise Apps		Administrator Messages Settings Activity Help Find
UDP Data inputs > UDP		New Local UDP
filter		25 per page

Create a 'New Local UDP' Input

Step 4. Enter the port on which the syslogs are being sent. It must be the same as the port configured on the FTD syslog settings, in this case 5156. In order to accept the syslogs only from one source (the FTD), set the **Only Accept Connection From** field to the IP of the interface on the FTD that is communicating with the Splunk server. Click **Next**.

splunk>enterprise Apps		Administrator Messages Settings Activity Help Find
Add Data <div> Select Source Input Settings Review Done </div> < Back Next >		
<div>Local Event Logs</div> <div>Remote Event Logs</div> <div>Files & Directories</div> <div>HTTP Event Collector</div> <div>TCP / UDP</div> <div>Local Performance Monitoring</div> <div>Remote Performance Monitoring</div> <div>Registry monitoring</div>	Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More <div> <div>TCP UDP</div> <div> Port ? 5156 <small>Example: 514</small> </div> <div> Source name override ? optional <small>host:port</small> </div> <div> Only accept connection from ? [] <small>example: 10.1.2.3, !badhost.splunk.com, *splunk.com</small> </div> </div> <div> FAQ <ul style="list-style-type: none"> > How should I configure the Splunk platform for syslog traffic? > What's the difference between receiving data over TCP versus UDP? > Can I collect syslog data from Windows systems? > What is a source type? </div>	

Specify Port and FTD IP address

Step 5. You can search and choose the **source type** and **index** field values from the pre-defined ones on Splunk as highlighted in the next image. The default settings can be used for the remaining fields.

Add Data Select Source **Input Settings** Review Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Source type
Select New
cisco:ftd:syslog

App Context
Apps Browser (appsbrowser)

Method
IP DNS Custom

Index
cisco_sfw_ftd_syslog [Create a new index](#)

Configure Data Input Settings

Step 6. Review the settings and click **Submit**.

Add Data Select Source Input Settings **Review** Done < Back Submit >

Review

Input Type UDP Port
Port Number 5156
Source name override N/A
Restrict to Host [REDACTED]
Source Type cisco:ftd:syslog
App Context launcher
Host (IP address of the remote server)
Index cisco_sfw_ftd_syslog

Review Data Input Settings

Execute SPL Queries and Create Dashboards

Step 1. Navigate to the **Search and Reporting App** on Splunk.

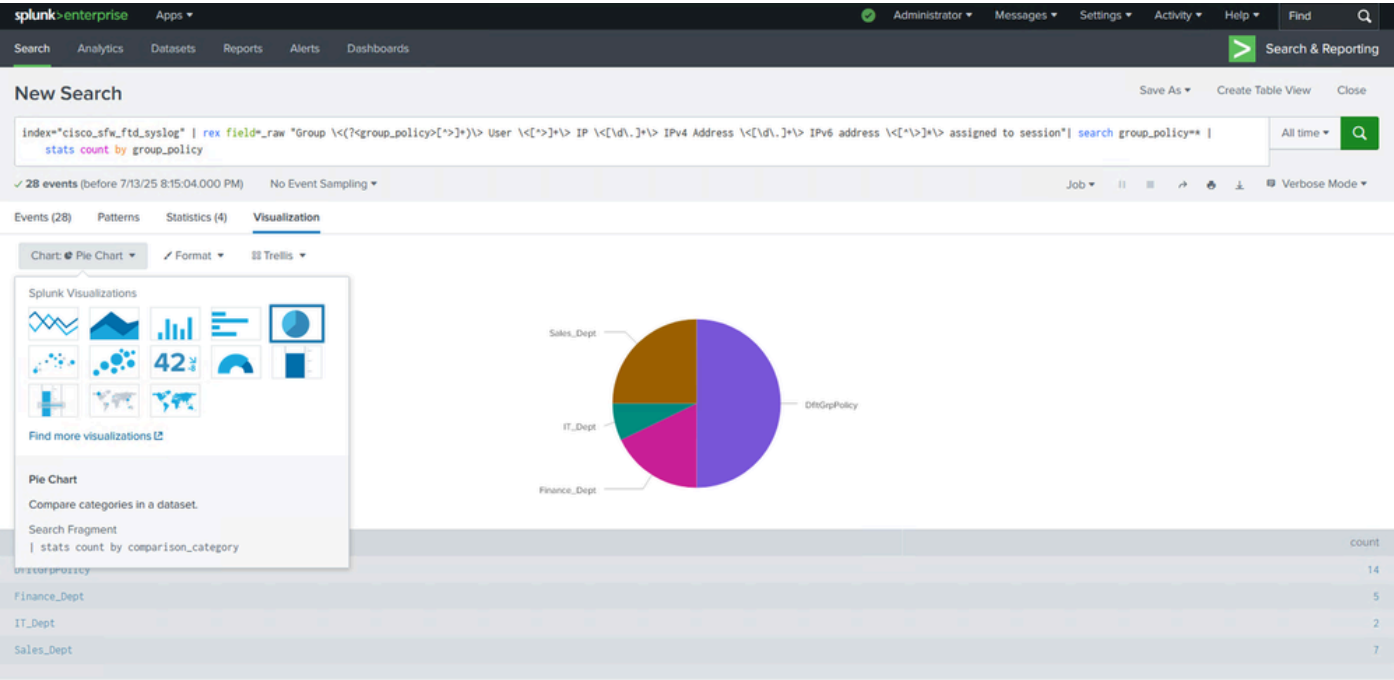
Navigate to the Search and Reporting App

Step 2. Formulate and execute a SPL query according to the data that you want to visualize. You will be able to see each log completely (in the **verbose mode**) under the **Events** tab, the count of connections per group-policy in the **Statistics** tab and visualize this data using these statistics under the **Visualization** tab.

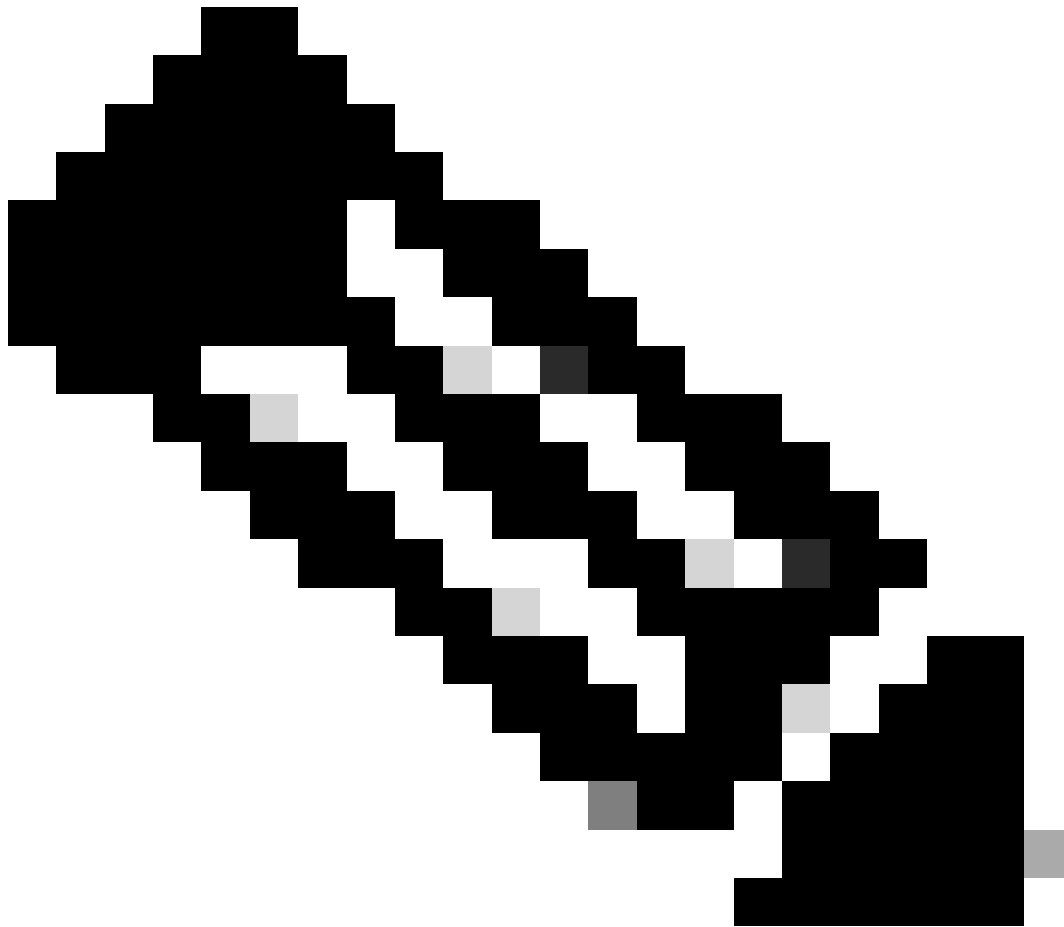
Search for Events using SPL Queries

group.policy	count
Df1t6rPolicy	14
Finance_Dept	5
IT_Dept	2
Sales_Dept	7

Check the Statistics Tab

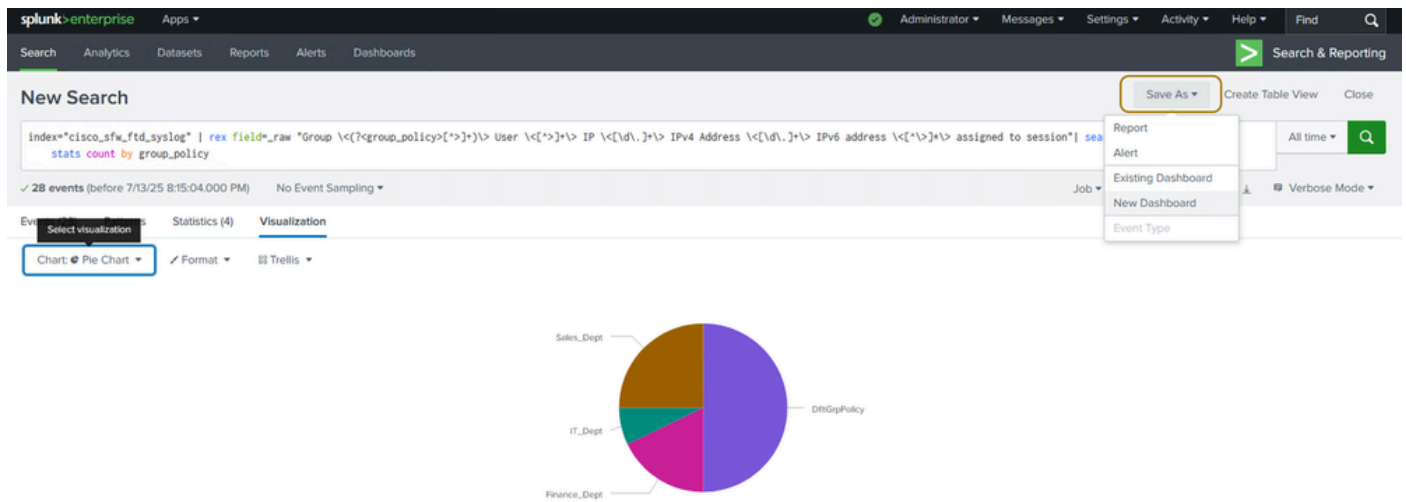


Visualization Tab Will Show the Graph/Chart



Note: In this example, the query is fetching logs for successful remote-access VPN connections across different group-policies. A pie-chart has been used in order to visualize the number and percentage of successful connections per group-policy. Based on your requirements and preferences, you can choose to use a different type of visualization such as a bar graph as well.

Step 3. Click **Save As** and choose **New or Existing dashboard** depending whether you already have a dashboard to which you want to add this panel or you want to create a new one. This examples showcases the latter.



Save the Panel to a Dashboard

Step 4. Give a title to the dashboard you are creating and provide a title for the panel which will contain the pie-chart.

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

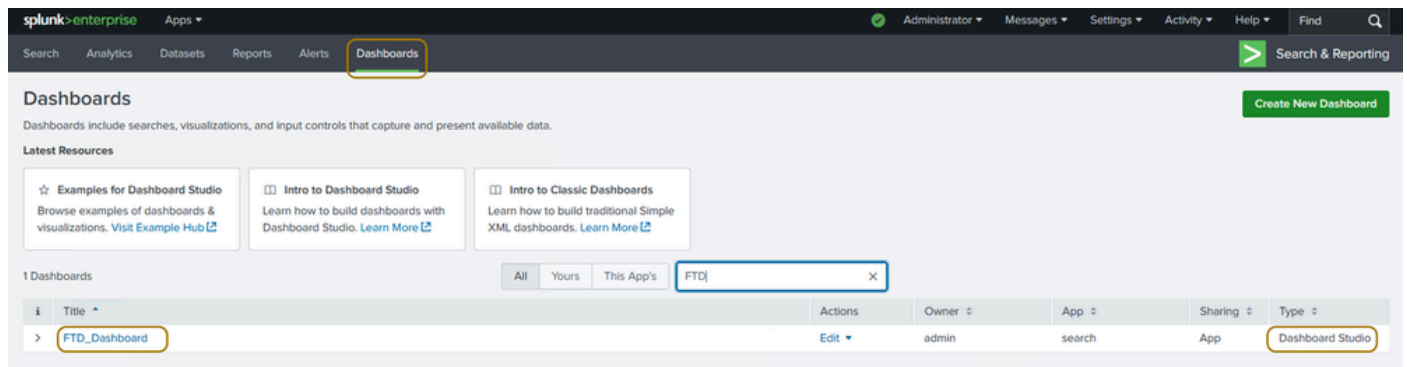
Cancel

Save to Dashboard

: You can set the permissions to Private or Shared in App based on whether only you are supposed to view the dashboard or other users with access to the Splunk instance are allowed too. Furthermore, depending on whether or not you want granular control over panel settings and layout of the dashboard, choose the Classic or Dashboard Studio mode to build your dashboard.

Step 5 (Optional). Execute and save more SPL queries as panels to this dashboard as per your requirement using the earlier mentioned steps.

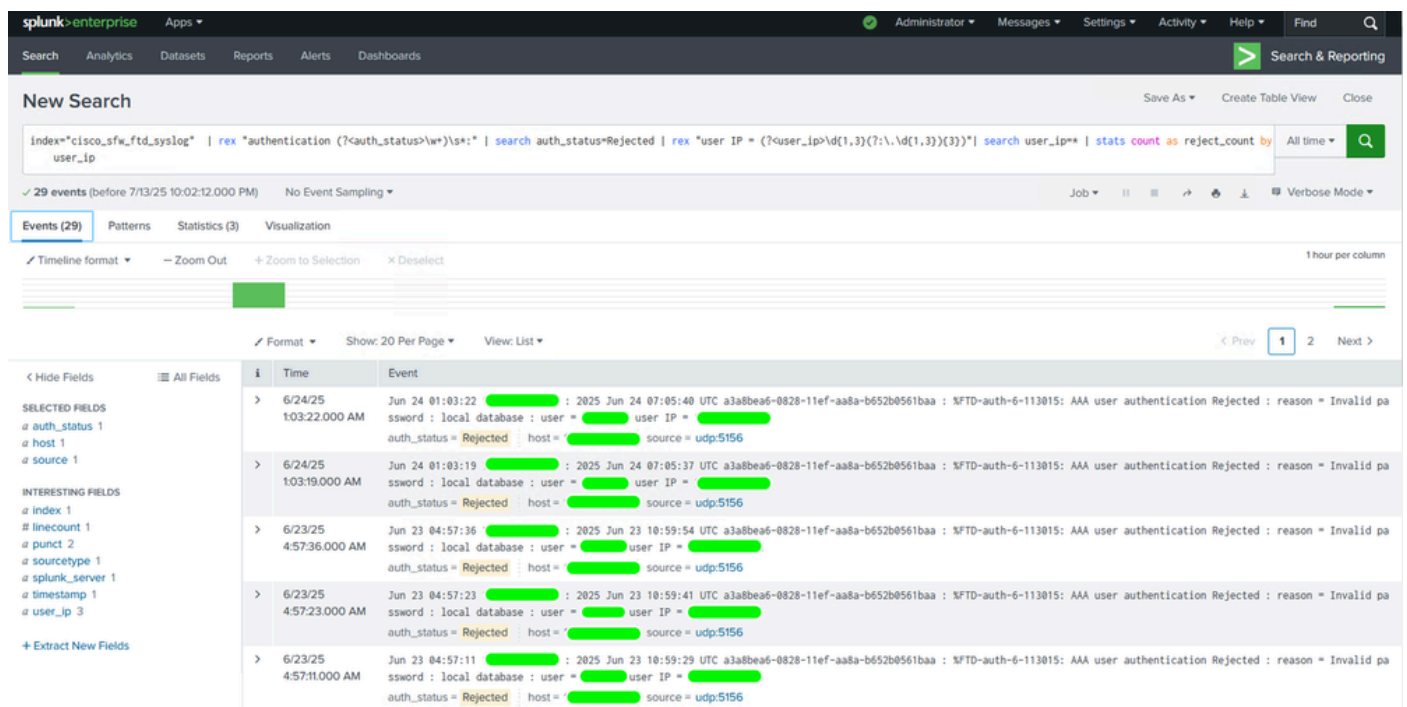
Step 6. Navigate to the **Dashboard** tab in order to search and choose the dashboard that you have created. Click it to view, edit, or rearrange its panels.



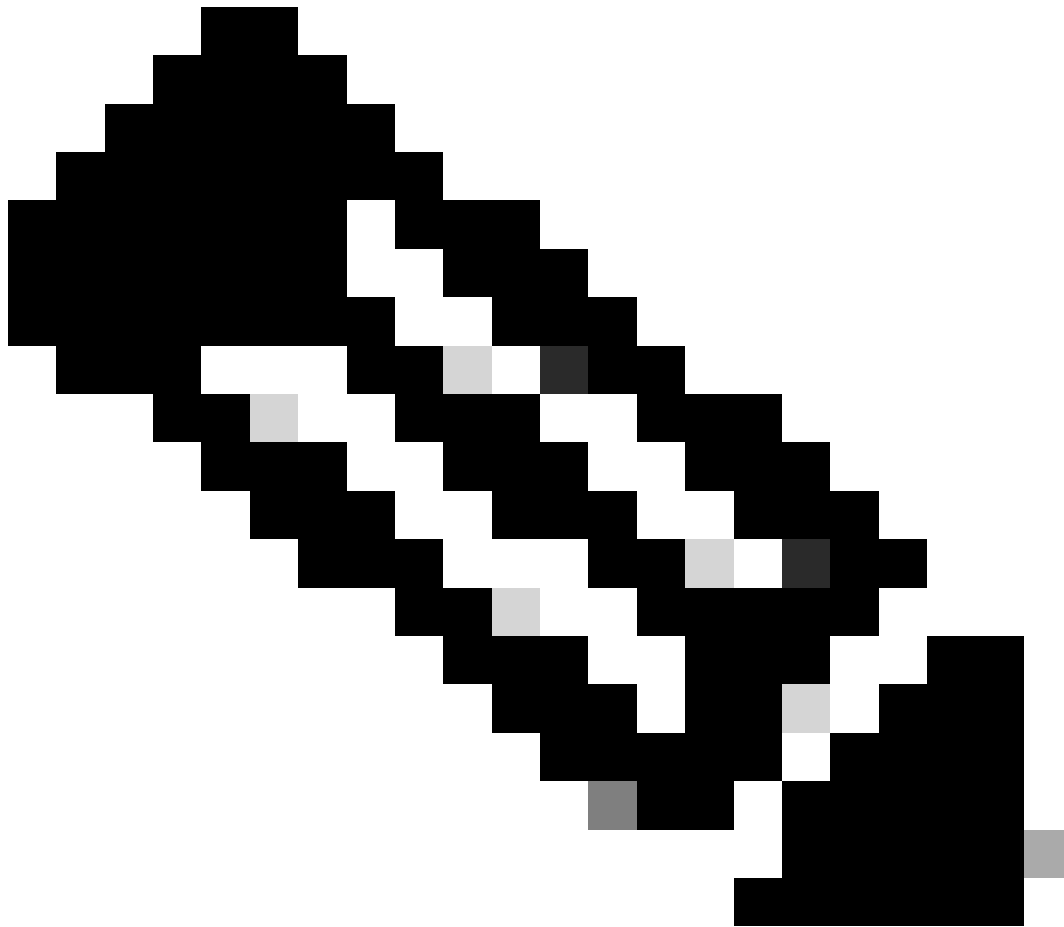
How to View the Dashboard

Configure Alerts Based on SPL Queries

Step 1. Navigate to the Search and Reporting App to construct and run your SPL query in order to verify that it is fetching the correct logs which will be used to trigger the alert.



Run SPL Queries for Creating Respective Alerts



Note: In this example, the query is used to fetch failed authentication logs for remote-access VPN to trigger alerts when the number of failed attempts exceed a certain threshold within a certain amount of time.

Step 3. Click **Save As** and choose **Alert**.



Save the Alert

Step 4. Give a Title to name the Alert. Fill in all the other details and parameters required to configure the alert and click Save. The settings used for this alert have been mentioned here.

<#root>

Permissions: Shared in App.

Alert Type: Real-time (allows failed user authentications in the last 10 minutes can be tracked continuously)

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.

Save As Alert



Settings

Title

Alert to notify more than 10 failed attempts in 10 minutes

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Expires

10

minute(s) ▼

Trigger Conditions

Trigger alert when

Custom ▼

e.g. "search count > 10"

in

Trigger

Throttle ?

☐

Trigger Actions

+ Add Actions ▼

Per-Result

Triggers whenever search returns a result.

Number of Results

Triggers based on a number of search results during a rolling-window of time.

Number of Hosts

Triggers based on a number of hosts during a rolling-window of time.

Number of Sources

Triggers based on a number of sources during a rolling-window of time.



Custom

Triggers based on a custom condition during a rolling-window time.

Save

Trigger Conditions

Trigger alert when

Custom ▼

search reject_count>10

e.g. "search count > 10". Evaluated against the results of the base search.

in

5

minute(s) ▼

Trigger

Once

For each result

Throttle ?

☐

Additional Settings for Alert Creation

Trigger Actions

+ Add Actions ▼

When triggered



Add to Triggered Alerts

Remove

Severity

Medium ▼

Info

Low

✓ Medium

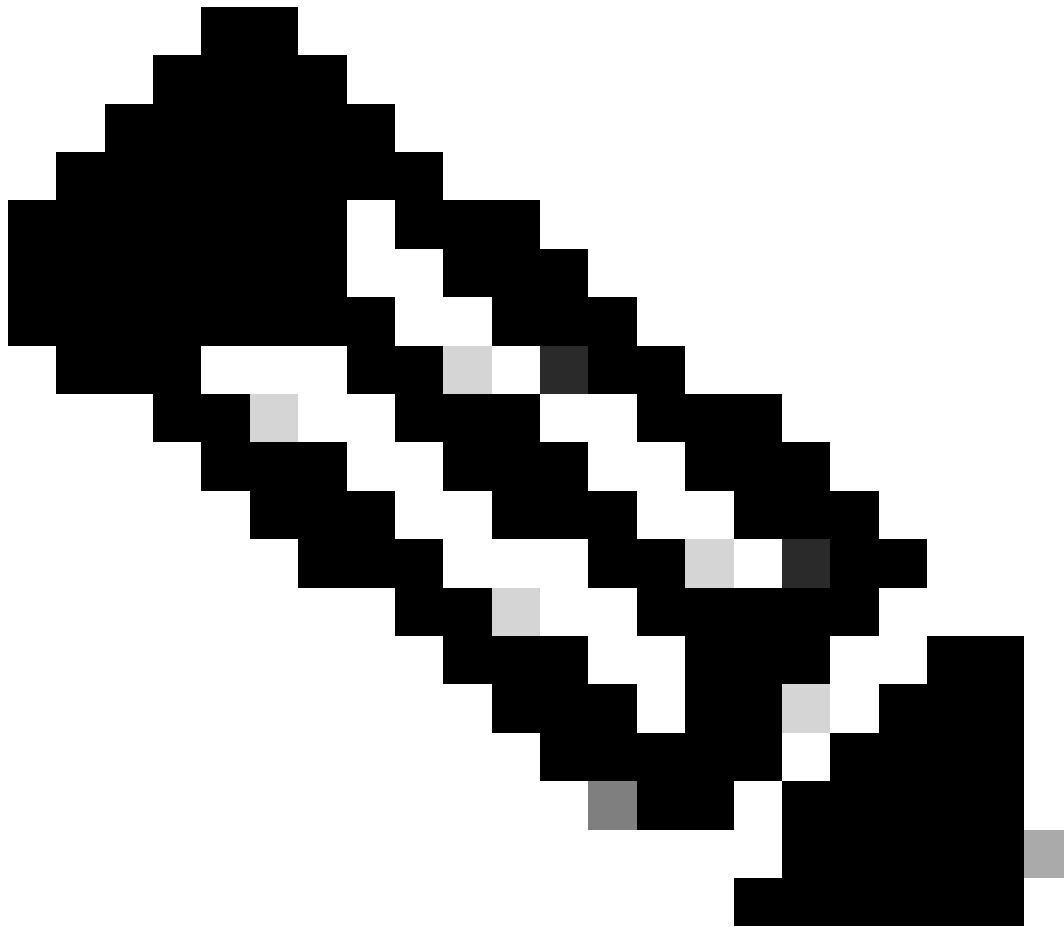
High

Critical

Cancel

Save

Additional Settings for Alert Creation



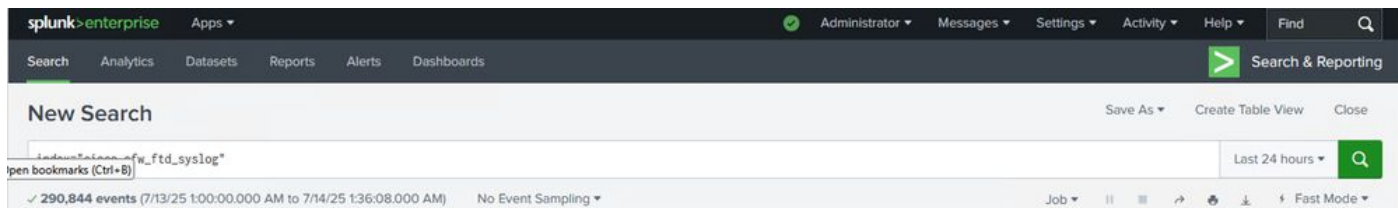
Note: If you want to trigger the alerts for each result, you will have to define the throttling settings accordingly as well.

Verify

Once you have created the dashboards and alerts, you can verify the configurations, data flow, dashboards and real-time alerts using the instructions provided in this section.

View Logs

You can use the search app in order to confirm if the logs sent by the firewall are received and visible to the splunk search head. This can be verified by checking the latest logs indexed (search **index** = "**cisco_sfw_ftd_syslog**") and the time stamp associated with it.



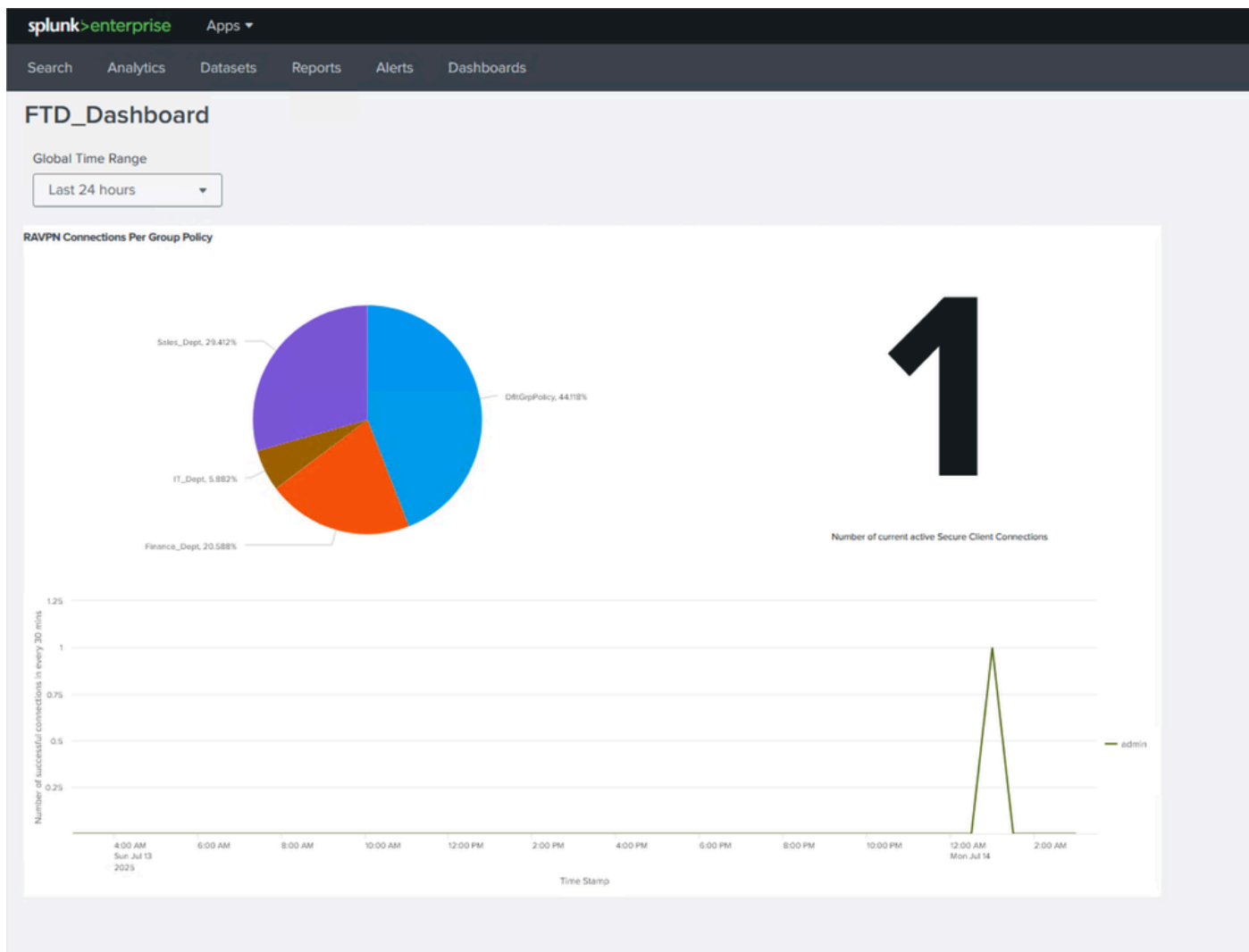
Check and View Logs

i	Time	Event
>	7/14/25 1:36:00.000 AM	Jul 14 01:36:00 : Jul 14 07:36:09 UTC: %FTD-config-7-111009: User 'enable_1' executed cmd: show resource usage resource Routes host = source = udp:5156

Check and View Logs

View the Real-time Dashboards

You can navitage to the custom dashboard which you have created and see the change on each of the panels as new data and logs are generated from the FTD.



View Dashboards

Check if Any Alerts Have Been Triggered

In order to verify the information about the alerts you can navigate to the section searches, reports, and alerts

to see the recent alert information. Click **View Recent** in order to check further about the jobs and searches.

splunk>enterpriseApps

AdministratorMessagesSettings

Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)

2 Searches, Reports, and AlertsType: AllApp: Search & Reporting (search)Owner: Administrator (admin)filter

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App
Alert to notify more than 10 failed attempts in 10 minutes	EditRunView Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search
Exceeding maximum number of failed alerts	EditRunView Recent	Alert	2025-07-14 01:24:00 Pacific Daylight Time	none	admin	search

Check and View Alerts

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Jobs

Manage your jobs. [Learn More](#)

68 JobsApp: Search & Reporting (search)Owner: AllStatus: Alllabel="Alert to notify more than 10 failed attempts in 10 minutes"10 Per Page

Edit Selected

< Prev1234567Next >

i	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	admin	search	11	4.57 MB	Jul 13, 2025 10:56:02 PM	Jul 14, 2025 1:27:30 AM	02:29:27	Running (real-time)	JobViewPauseStopRestartDownload

Alert to notify more than 10 failed attempts in 10 minutes [real-time]

Check and View Alerts

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Alert to notify more than 10 failed attempts in 10 minutesSaveSave AsViewCreate Table ViewClose

index="cisco_sfwd_syslog" | rex "authentication (?<auth_status>\w*)s*:" | search auth_status=Rejected | rex "user IP = (?<user_ip>\d{1,3}(?:\.\d{1,3}){3})" | search user_ip=* | stats count as reject_count by user_ip

Real-time

26 of 33,995 events matchedNo Event Sampling

JobViewPauseStopRestartDownloadFast Mode

EventsPatternsStatistics (1)Visualization

Show: 20 Per PageFormat

user_ip	reject_count
	15

Check Statistics for Triggered Alert