Splunk for Network Engineers

Catalyst, Meraki, ISE, ThousandEyes and ITSI

Jeff Lee
Solutions Engineer, CCIE#25598 (R&S)

Session ID: BRKOPS-1233

Cisco Webex App

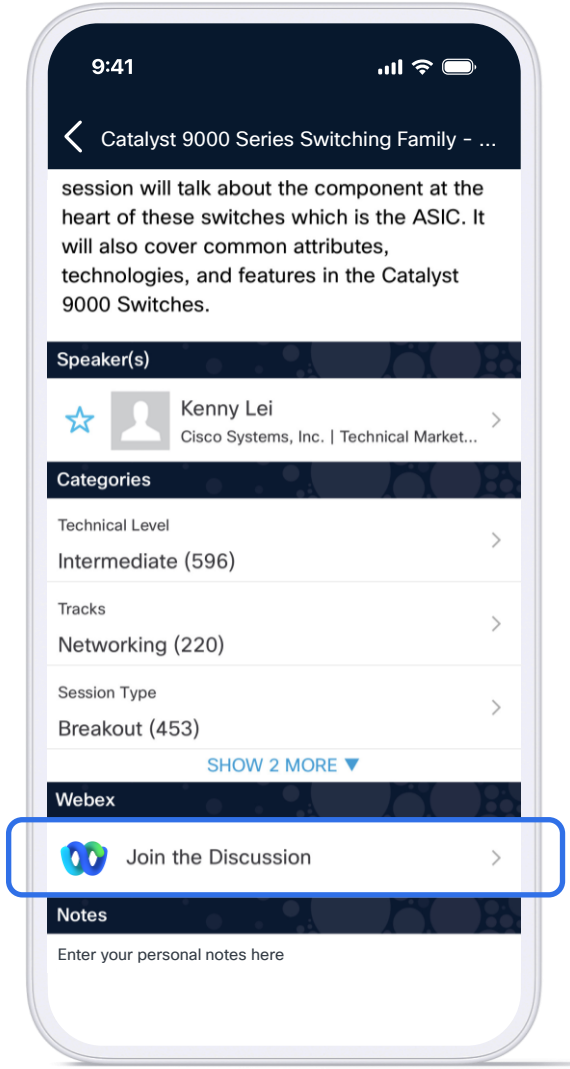
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKOPS-1233**

Who am I?

- Over 20 years networking experience
- 6+ years in Cisco as Enterprise Networking Specialist

- Avid cyclist (used to be good)
- Keen (if not very good) skier

Agenda

01 Splunk Overview

02 Splunk Installation

03 Splunk Technology Add-Ons

04 Catalyst Add-On

05 Meraki App

06 ThousandEyes App

07 Splunk ITSI

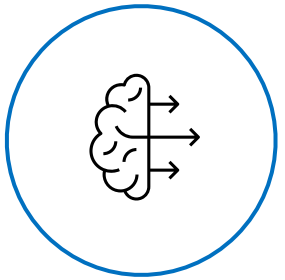
Session Assumptions

- Network Engineers/Operators
- Generally familiar with Catalyst Center, Identity Services Engine, SD-WAN and Meraki
- Less familiar with Thousand Eyes
- Even less familiar with Splunk
- Probably never heard of ITSI

Why Splunk?

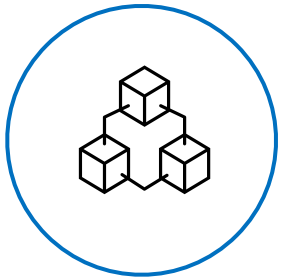
Consolidated Dashboard

- End-to-end view of network & security events
- Empower NetOps/SecOps when troubleshooting



Intelligence

- Interact with Cisco controllers for enhanced NetOps/SecOps experience
- Integrate with Splunk AI tools such as ITSI and MLTK



Splunkbase

- Ecosystem of applications to help you shape your data
- Install apps on Splunk Platform for parsing and indexing data

Full Stack Visibility

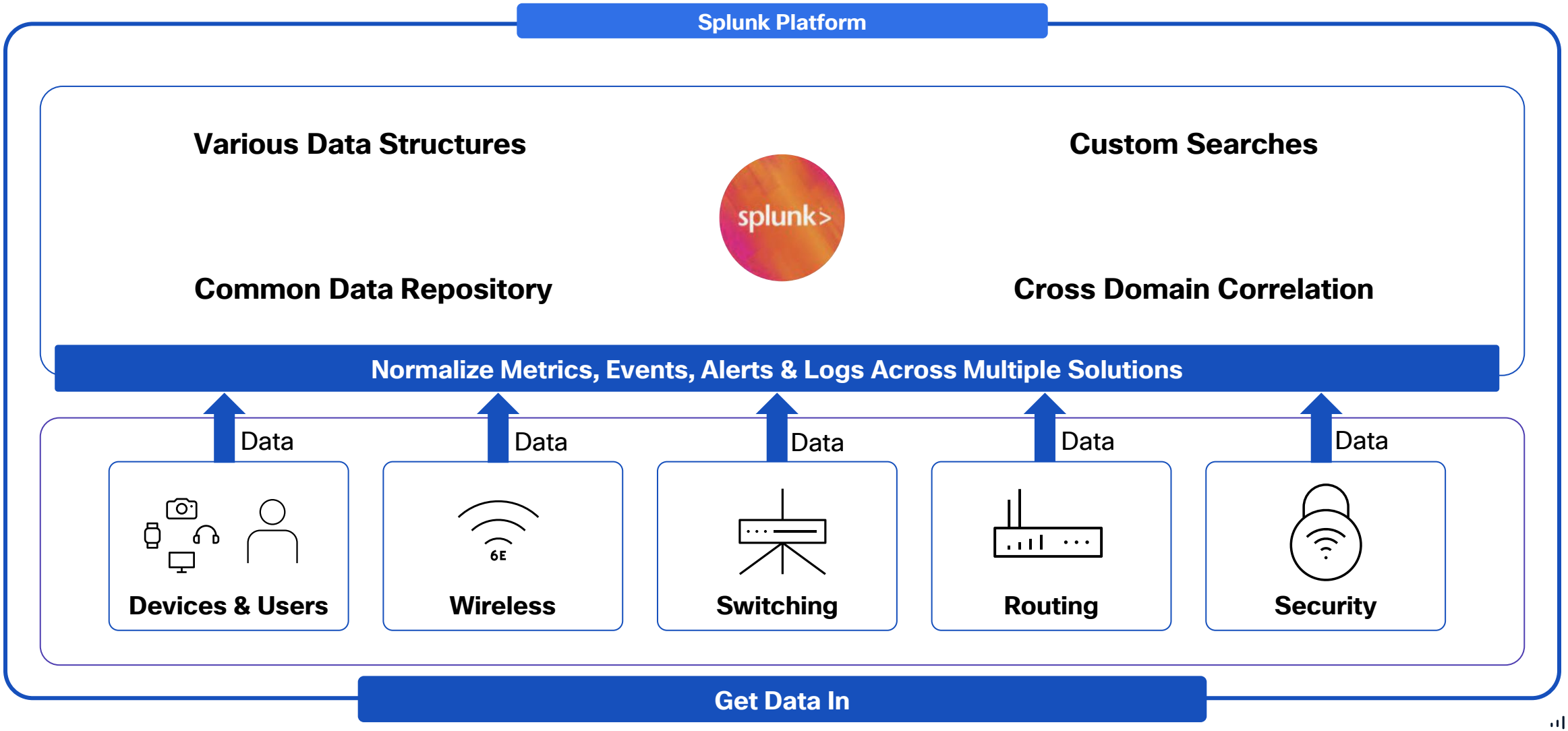
Faster RCA

Data Correlation

Artificial Intelligence

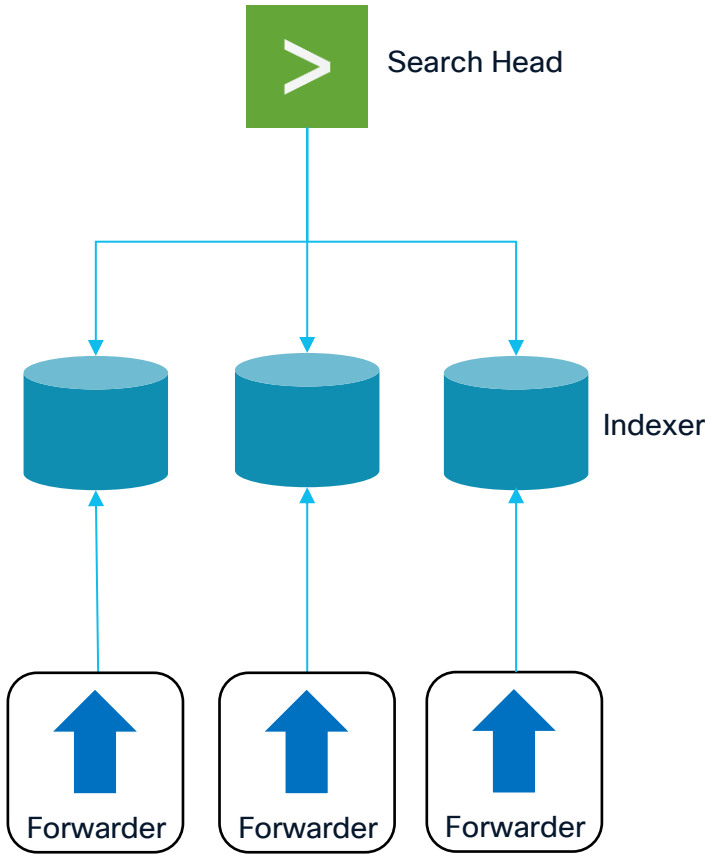
Getting Data to Splunk

Various Data Structures | Common Repository | Custom Searches



cisco

Splunk – Main Components



Search Head

- Handles search requests and consolidating results back to the user

Indexer

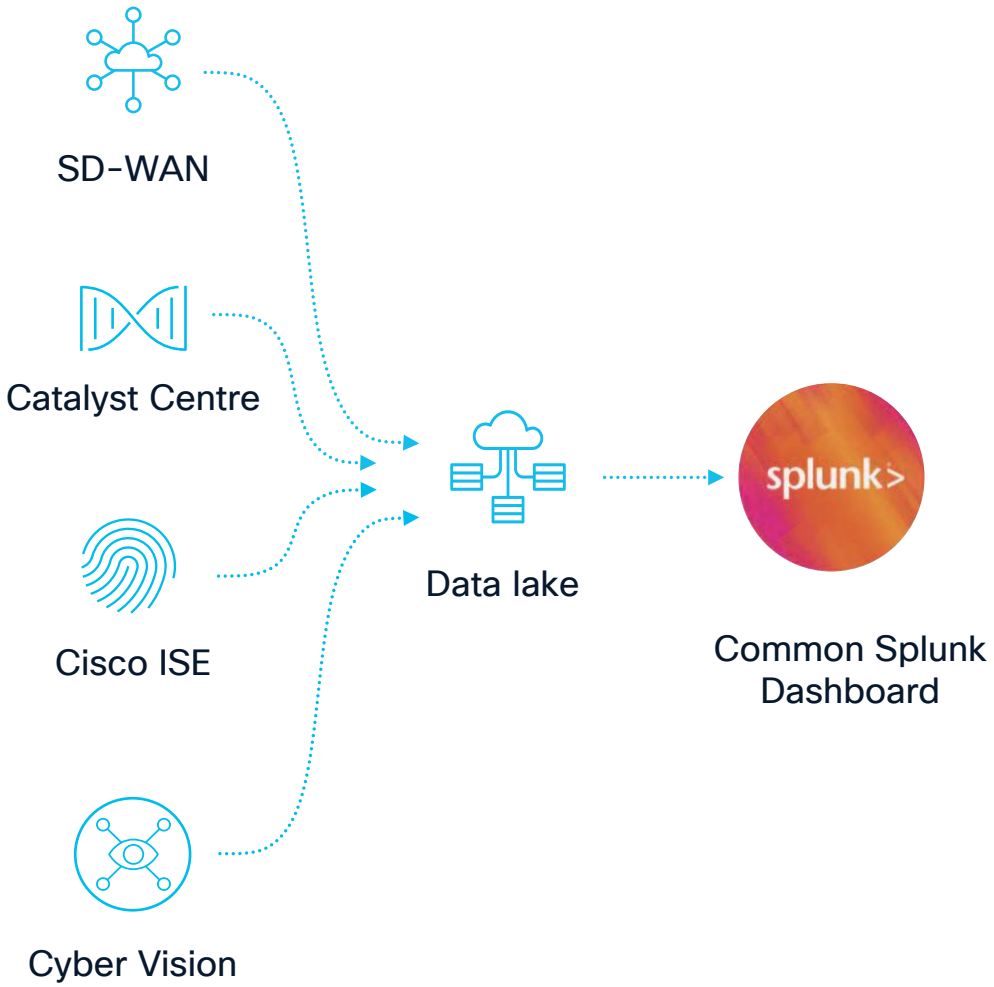
- Takes raw data from forwarders
- Converts the data into events and places the results into an index (bucket)

Forwarder

- Forwards raw data to indexer (or search head + indexer)
- 2 Types
  - **Universal Forwarder** – lightweight, streamlined data collection agent
  - **Heavy forwarder** – Full Splunk Enterprise instance with advanced data processing capabilities

Master Complexity with Observability

*Future Looking



Consolidated visibility (Shipping) on a common dashboard for real-time monitoring, history insights, security insights, and compliance advisory

Analytics dashboard* to detect and report on anomalies based on deviation from the baseline (potentially powered by ITSI)

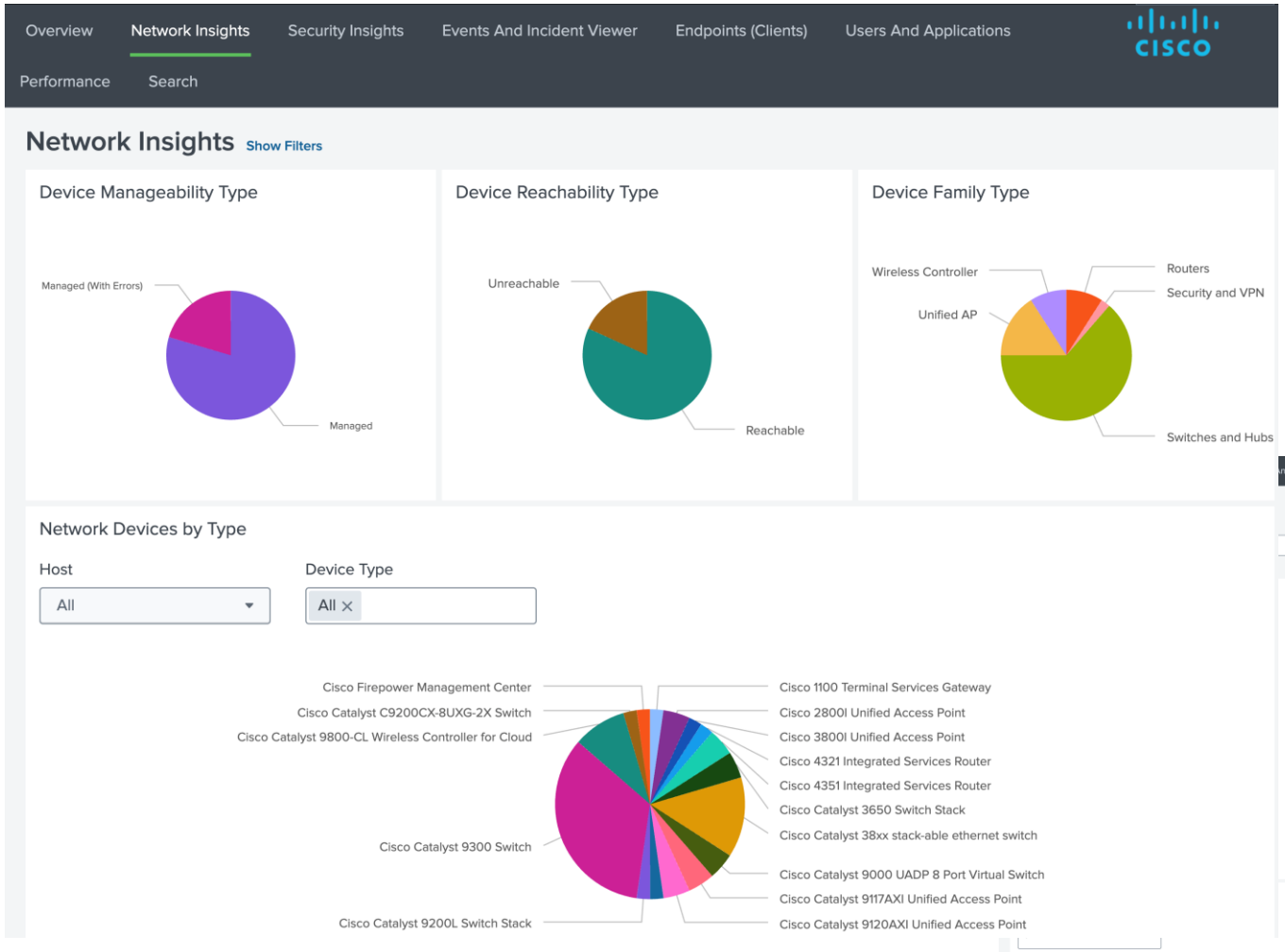
Playbook driven response* based on certain event triggers to generate API calls back to the appropriate domain

Splunk ecosystem partner* trigger notifications to 1,000+ 3rd party applications

cisco

Enterprise Networking for Splunk

Network Insights & Endpoints

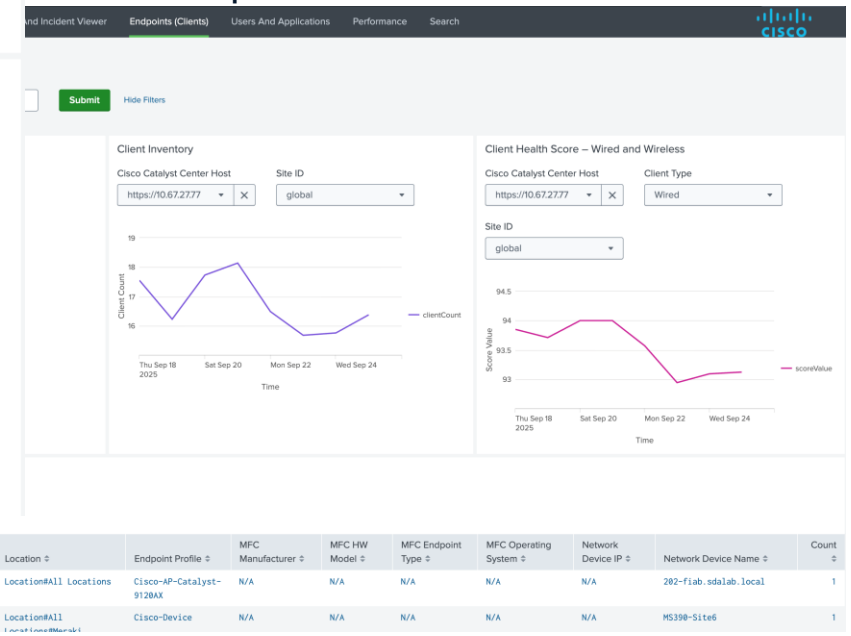


Network Insights

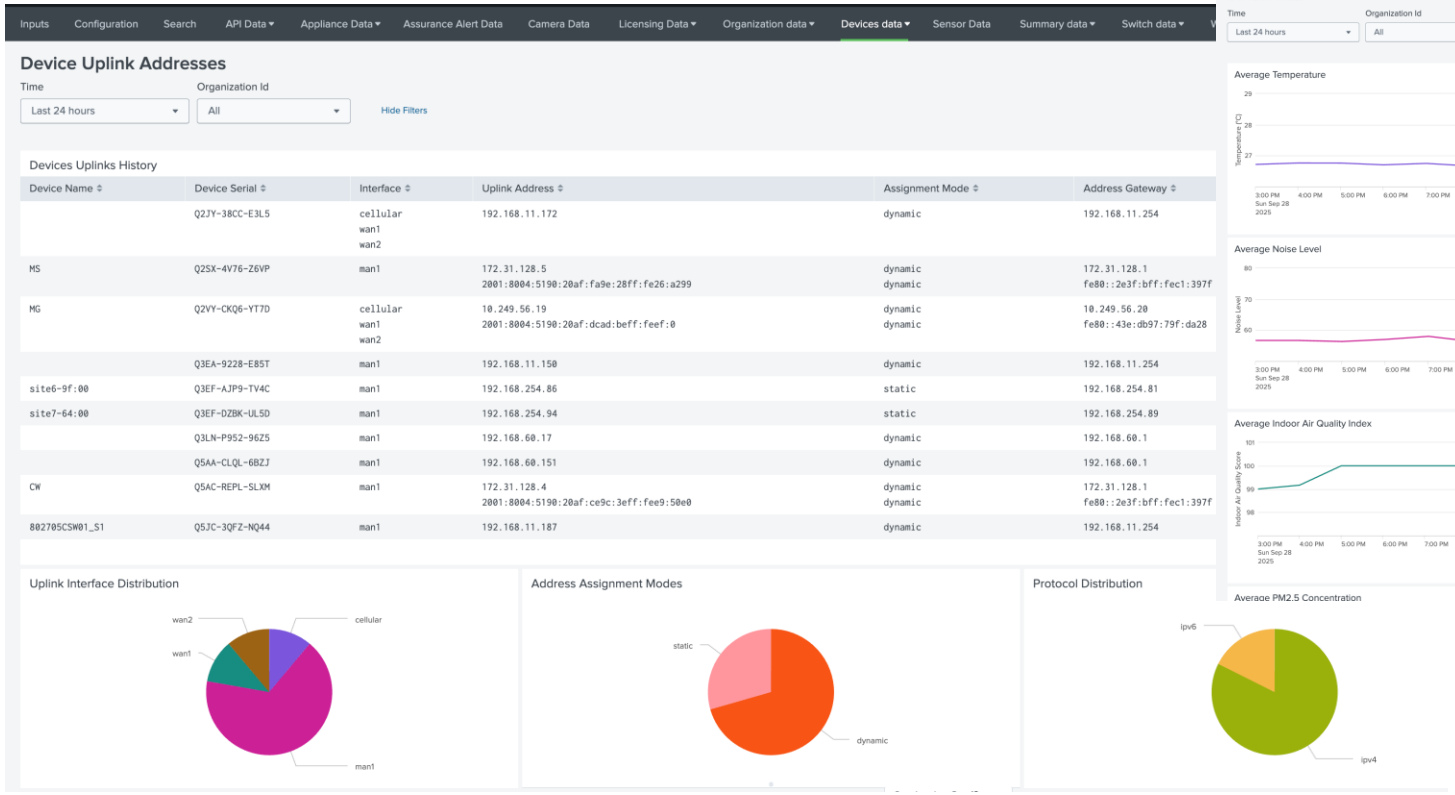
- Provides high-level summary of most pressing issues in the network
- Contains a mix of network and security events across Catalyst Center, ISE and SD-WAN

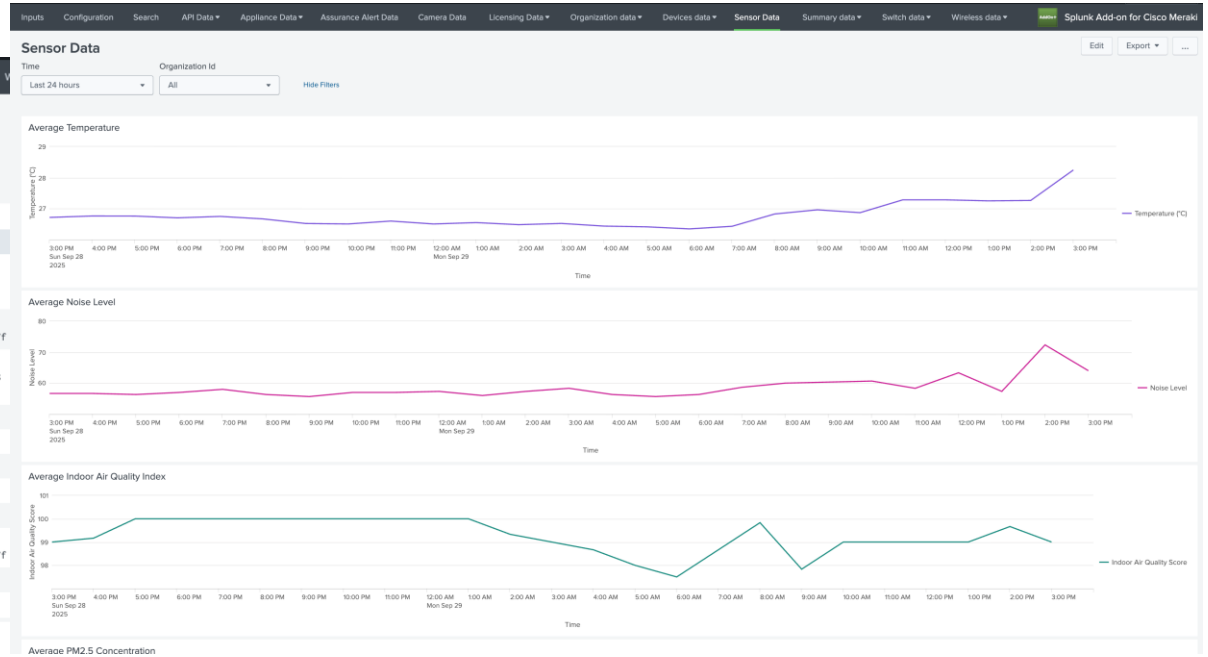
Endpoints

- Health score metrics, endpoint identity summary and endpoint authentication status



Meraki Insights





Devices Data

- Summary of Meraki device change history and uplink information

Sensor Data

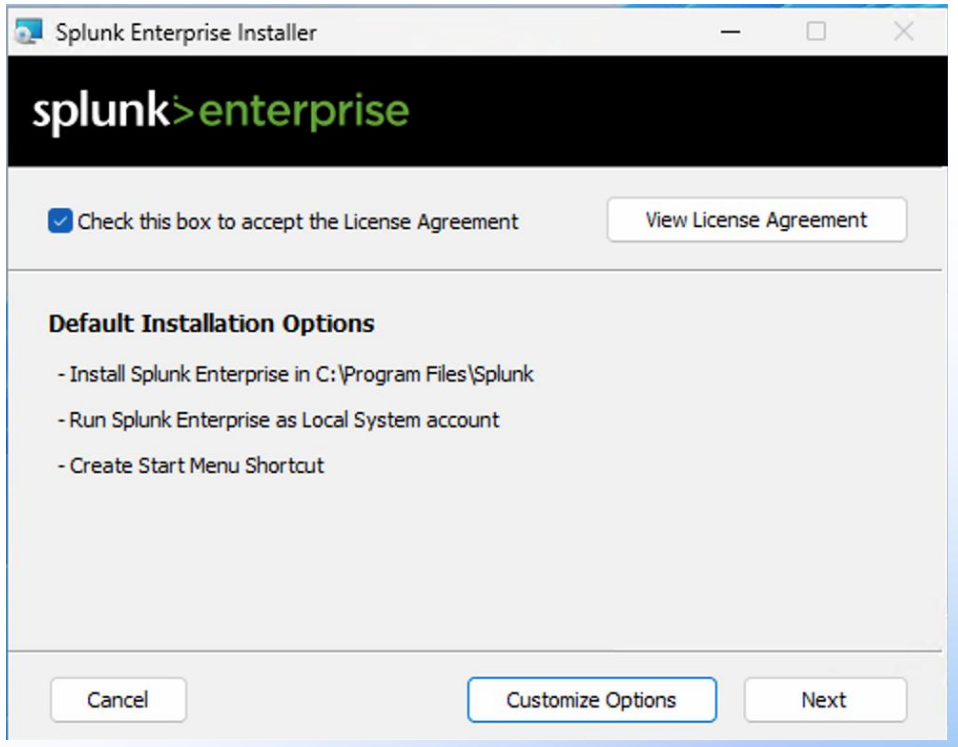
- Provides sensor data from Meraki environmental sensors

Splunk Installation & Getting Started

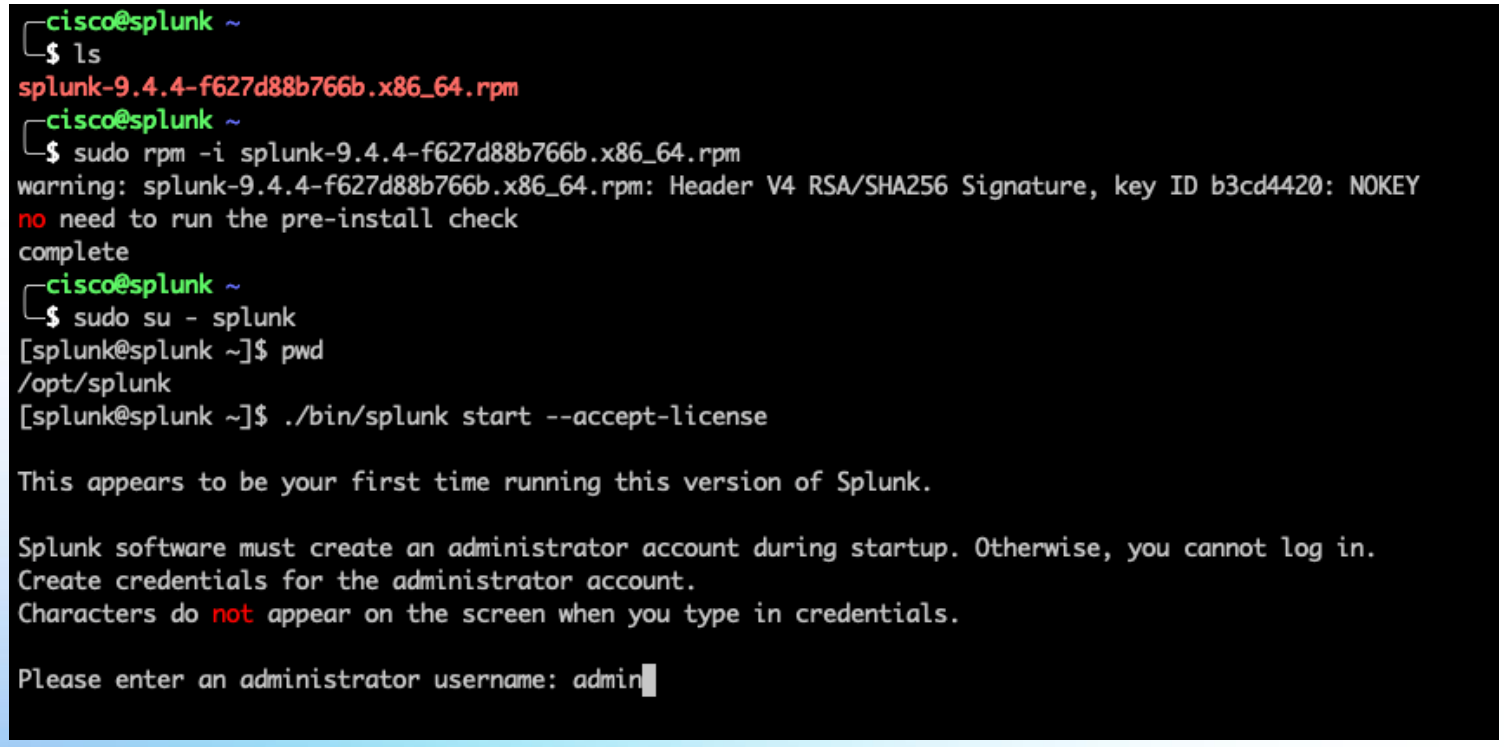
Splunk Enterprise Installation

Windows, Linux, Mac OS

https://www.splunk.com/en_us/download/splunk-enterprise.html



Windows

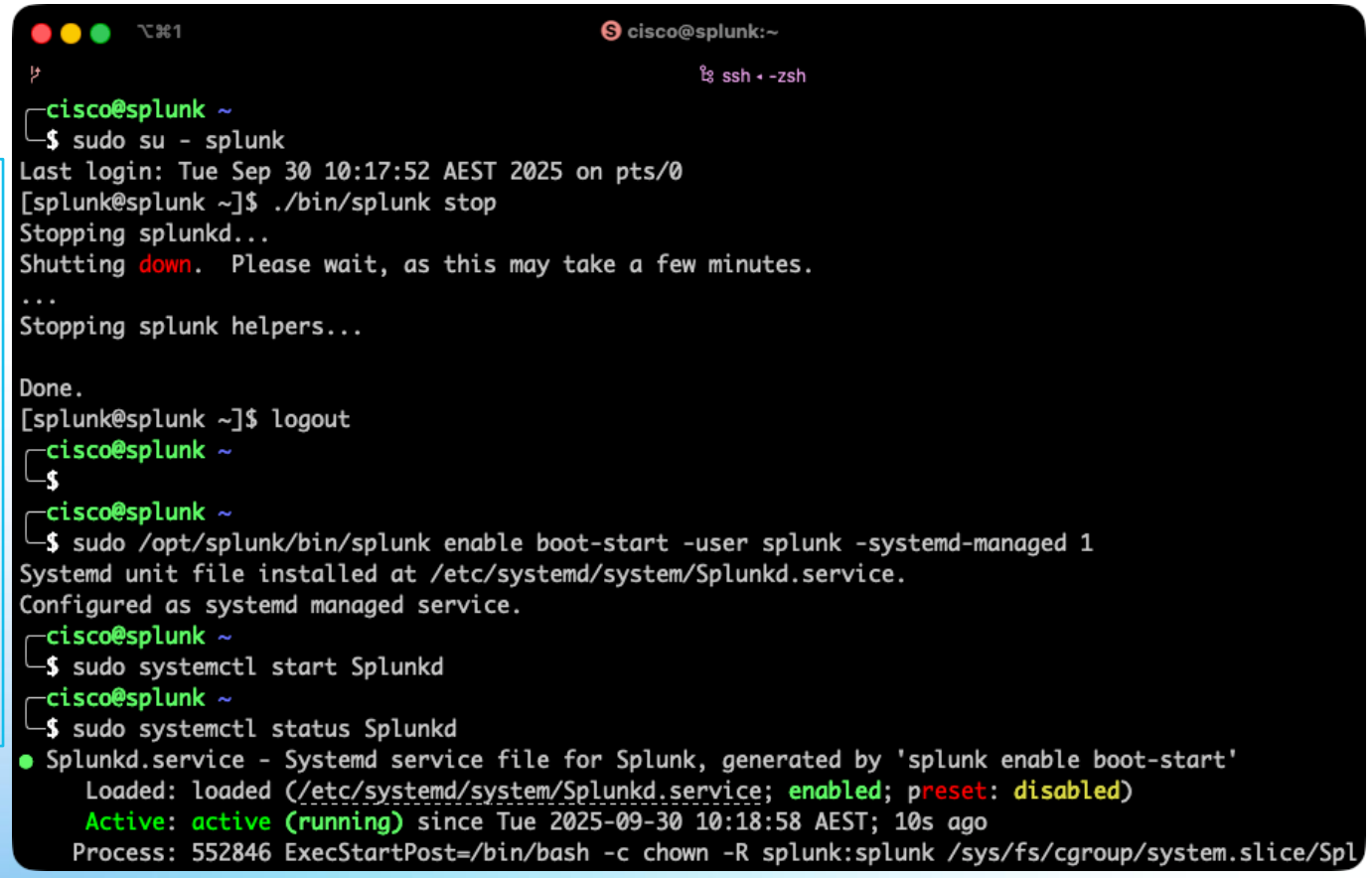


Linux

Splunk Enterprise Installation – Automatic Start

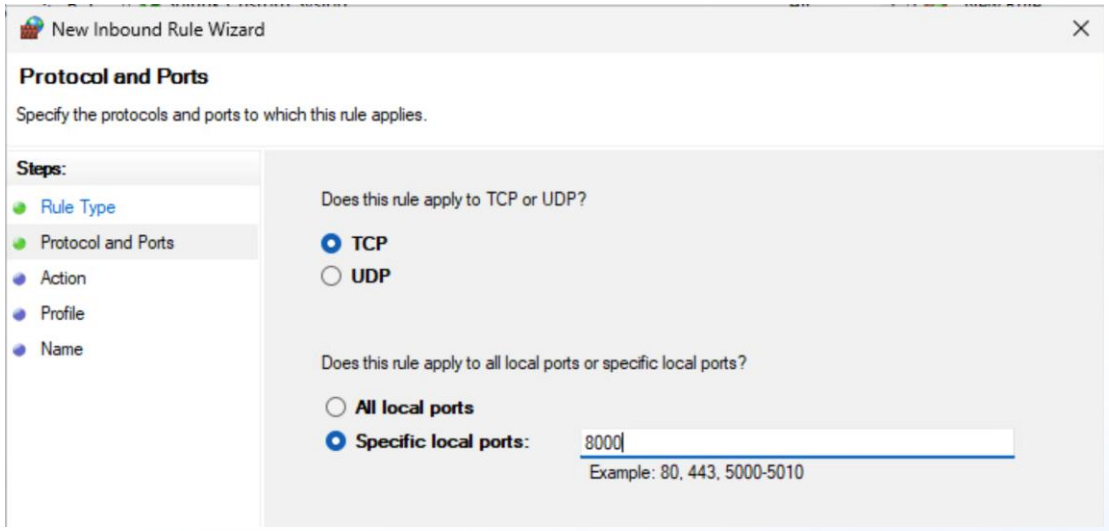
Linux Start on Boot

```
[cisco@splunk ~]$ sudo su – splunk
[splunk@splunk ~]$ ./bin/splunk stop
[splunk@splunk ~]$ logout

[cisco@splunk ~]$ sudo /opt/splunk/bin/splunk
enable boot-start -user splunk -systemd-managed 1

[cisco@splunk ~]$ sudo /systemctl start SplunkD
```

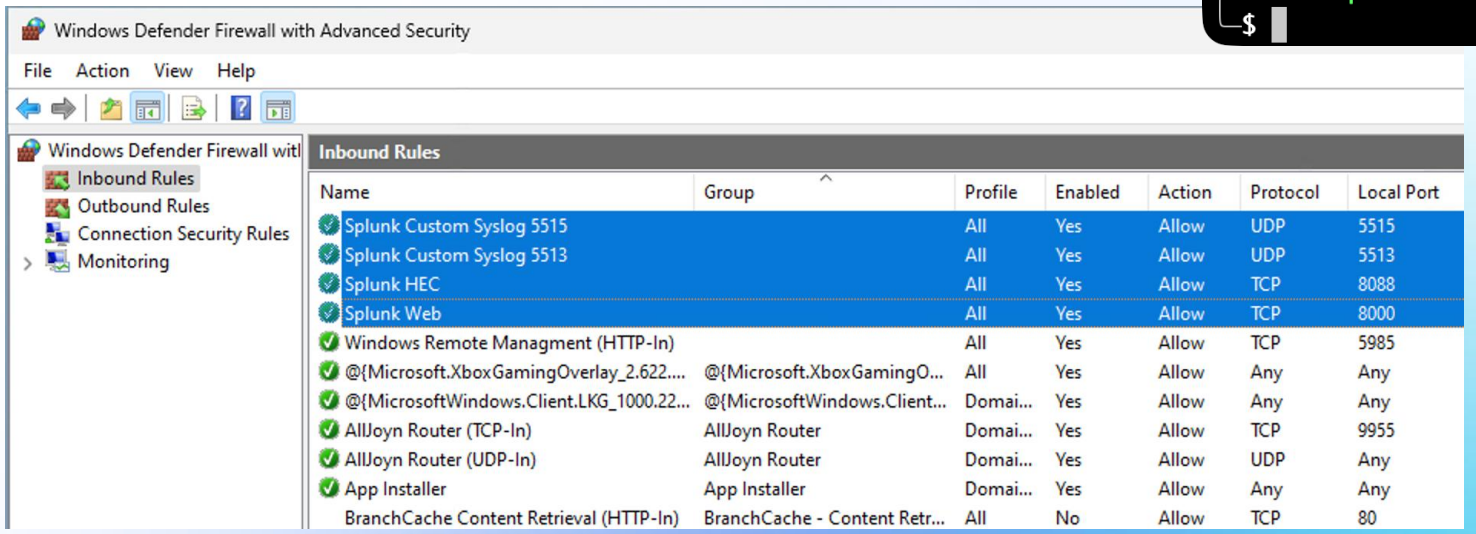


Splunk Enterprise Installation – Firewall

Allow ports for Splunk

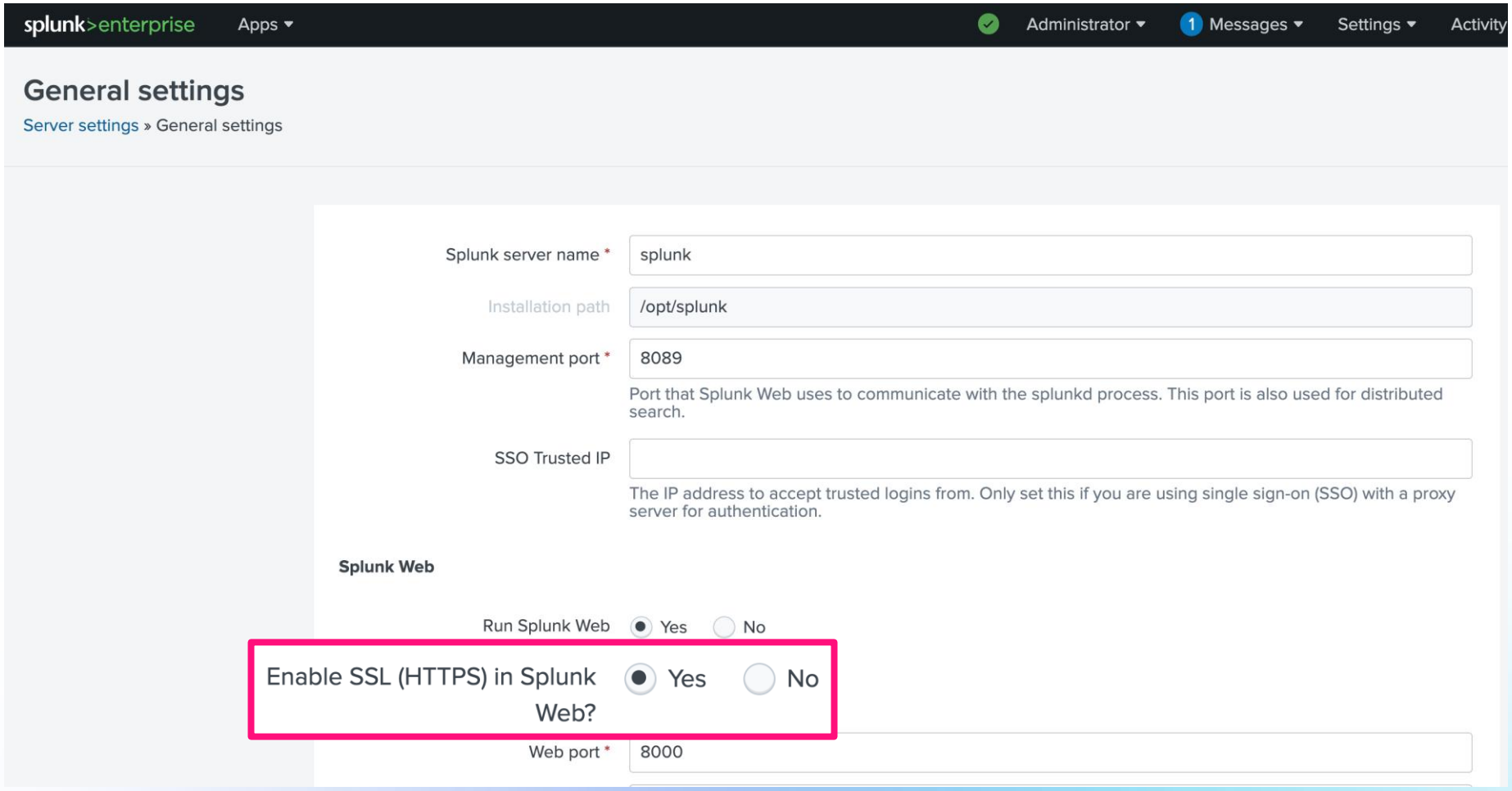



```
cisco@splunk:~
ssh ◂ -zsh
cisco@splunk ~
$ # Splunk Web and HTTP Event Collector
cisco@splunk ~
$ sudo firewall-cmd --zone=public --add-port=8000/tcp --add-port=8088/tcp --permanent
success
cisco@splunk ~
$ # Custom syslogs
cisco@splunk ~
$ sudo firewall-cmd --zone=public --add-port=5513/udp --add-port=5515/udp --permanent
success
cisco@splunk ~
$ sudo firewall-cmd --reload
success
cisco@splunk ~
$
```



- Splunk Web default port 8000
- HTTP Event Collector
- Custom ports as required

Splunk Enterprise Installation – Enable HTTPS



Splunk Web

- HTTP is enabled by default – enable **HTTPS** for added security

Splunk Technology Add-Ons (TAs)

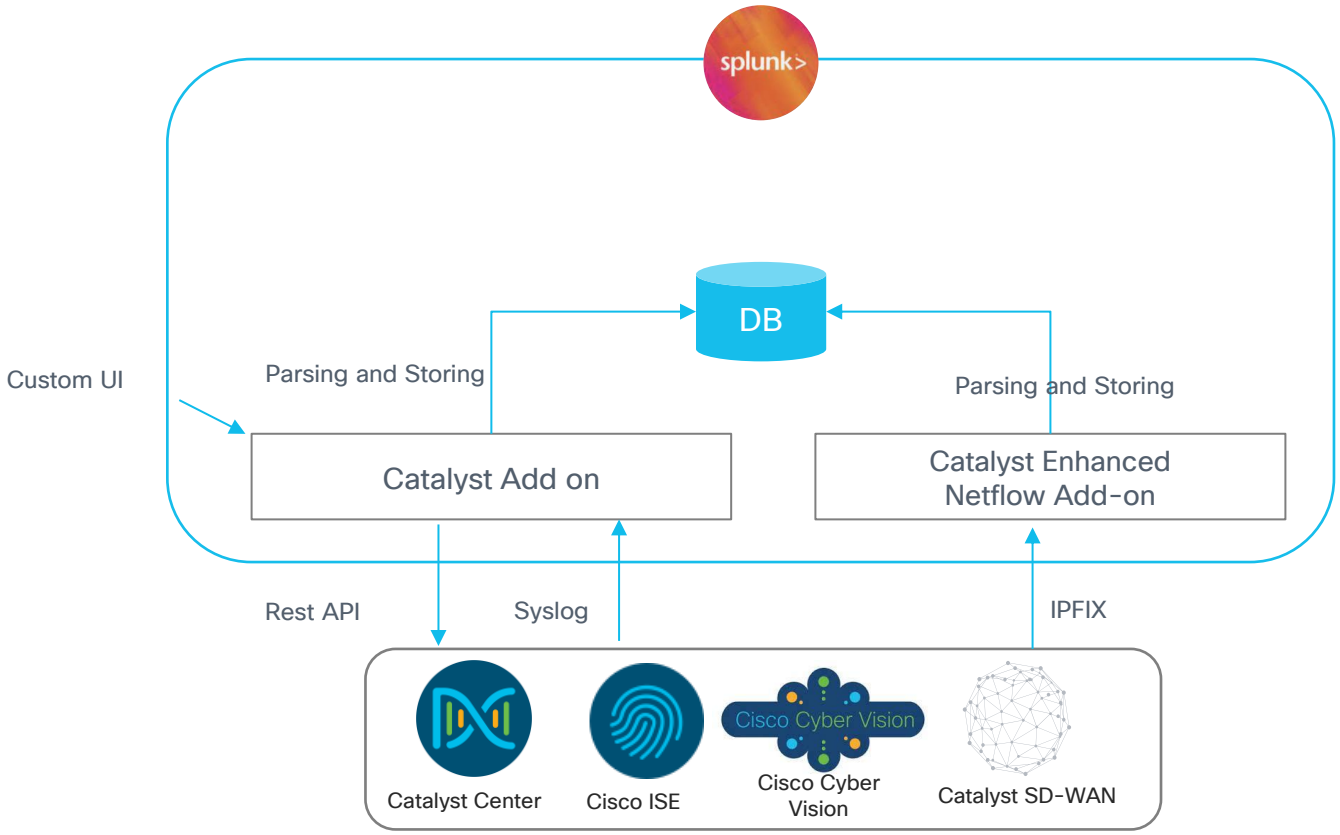
Splunk Apps and Technology Add-Ons

Collects, formats, and normalizes data from a specific technology source

https://splunkbase.splunk.com

Catalyst Add-On

Technical Add-On Architecture

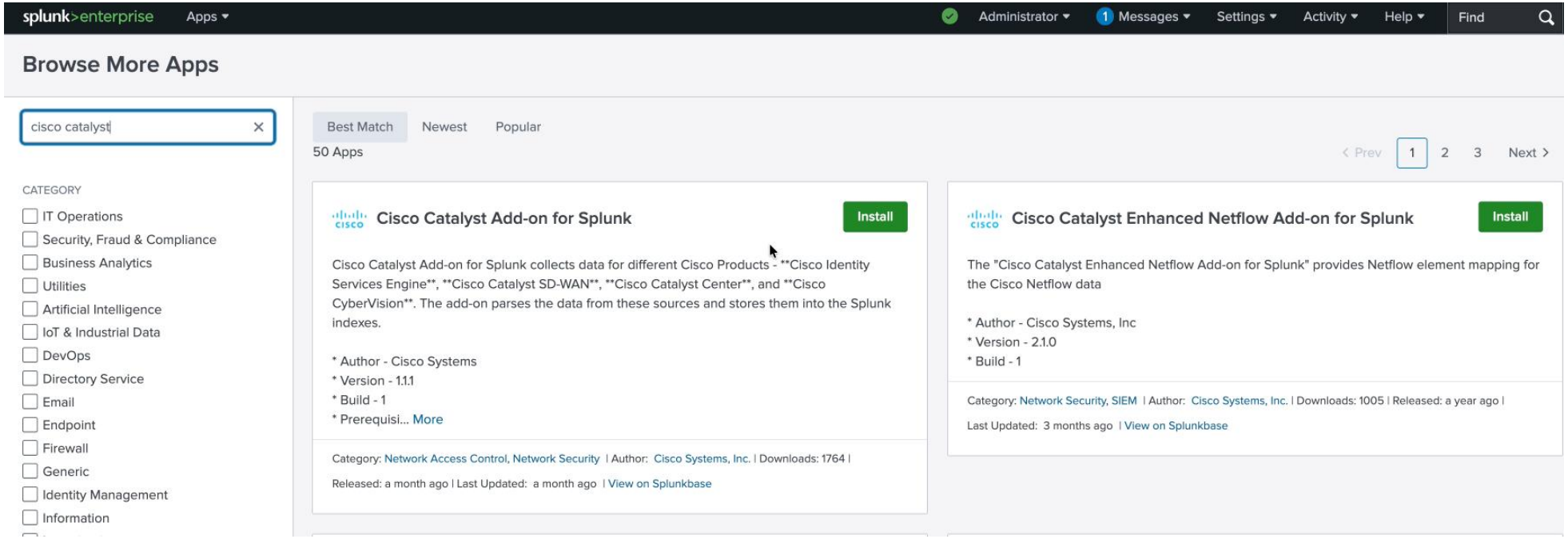


Two TAs used for ingesting telemetry

- Catalyst Add on – Processes API, Syslog and Netflow v10
- Enhanced Netflow Add on – Processes Netflow v9
- TAs adhere to the Splunk gold standard
- Conforms to CIM (common information model) for many of the data ingested
- Catalyst App
- Dashboard with preconfigured charts to visualize data
- Help monitor notifications, events and logs from multiple enterprise networking products on a single pane of glass – covers both the network infrastructure and controllers

Cisco Catalyst Add-On for Splunk

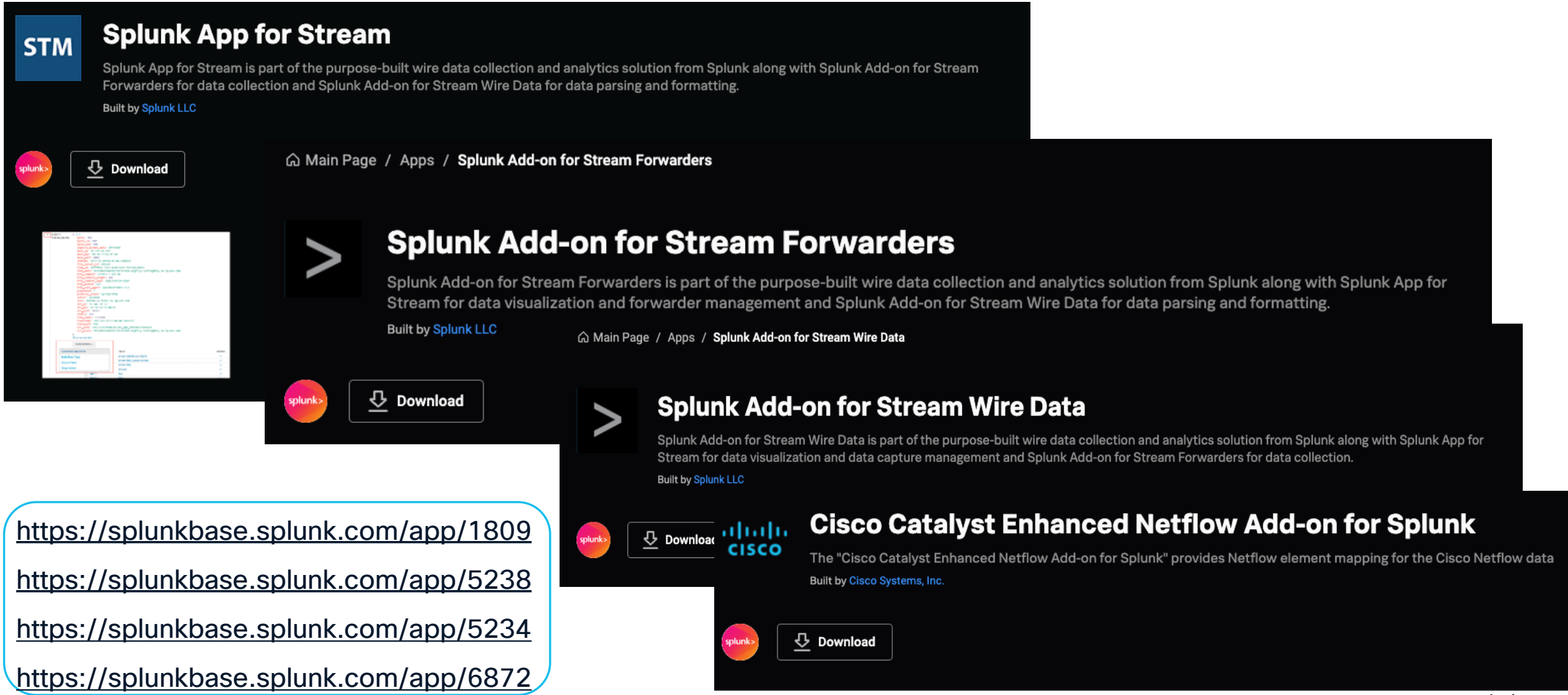
Parses the data from specified sources and stores them into the Splunk indexes



- Cisco Catalyst Center
- Cisco Identity Services Engine
- Cisco Catalyst SD-WAN
- Cisco Cyber Vision

Cisco Catalyst Add-On for Splunk – Stream

Install the pre-requisite apps & add-ons



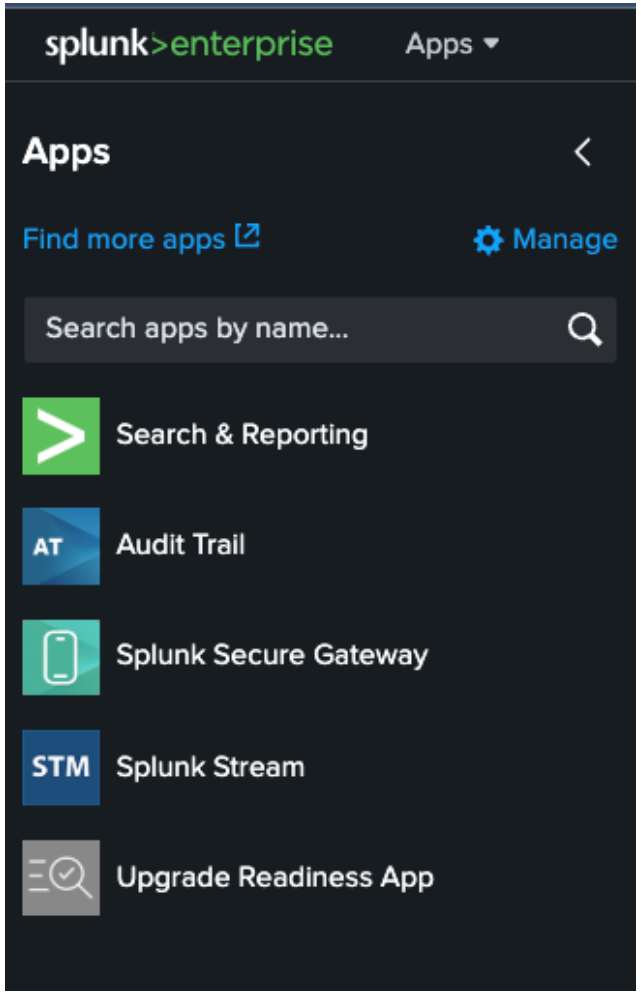
https://splunkbase.splunk.com/app/1809

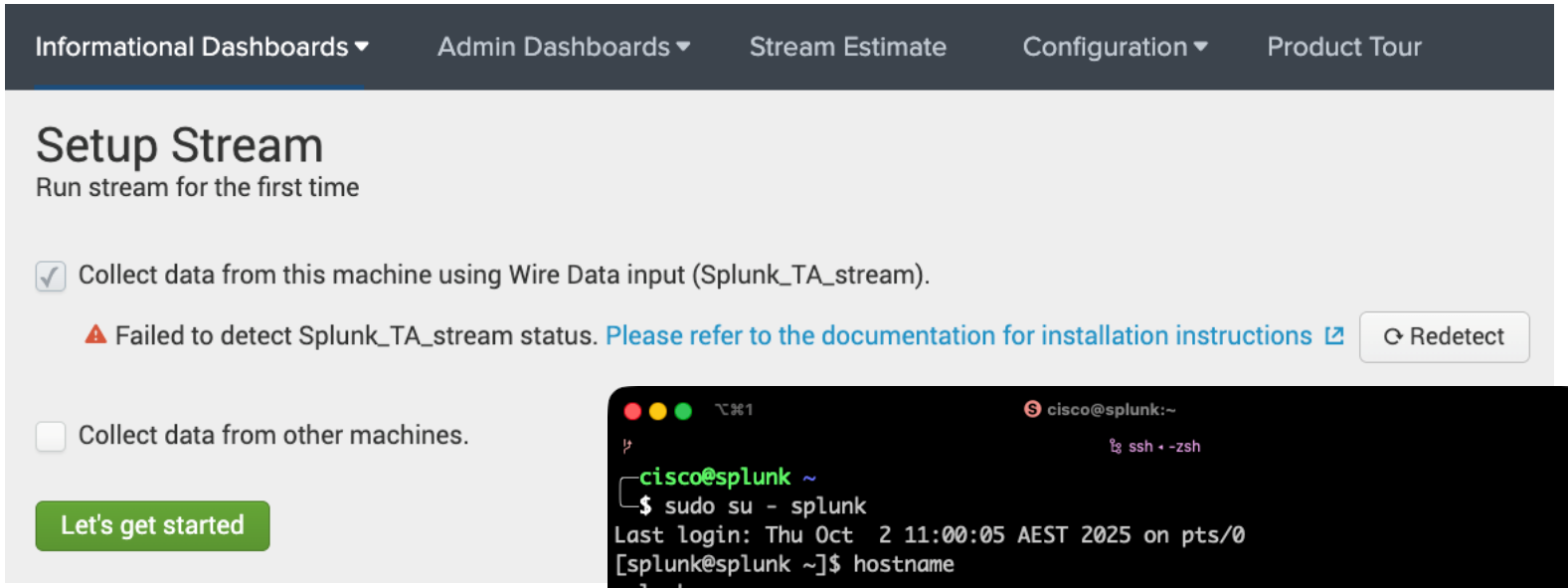
https://splunkbase.splunk.com/app/5238

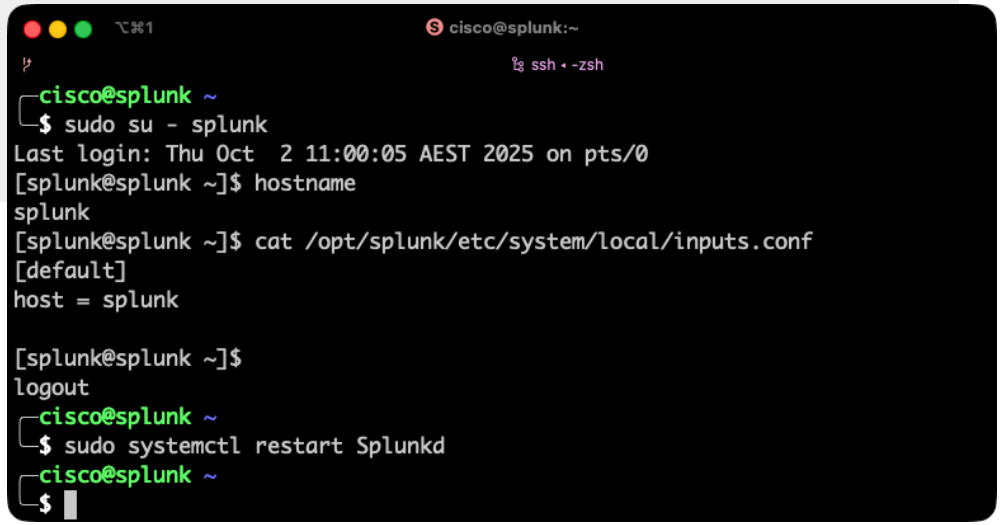
https://splunkbase.splunk.com/app/5234

https://splunkbase.splunk.com/app/6872

Cisco Catalyst Add-On for Splunk – Stream





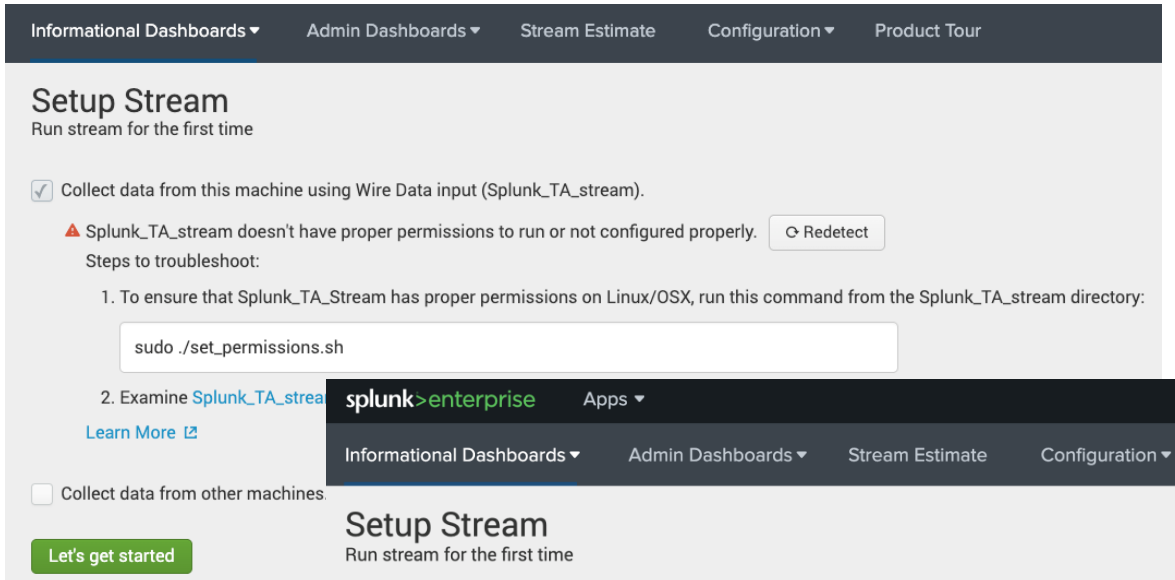


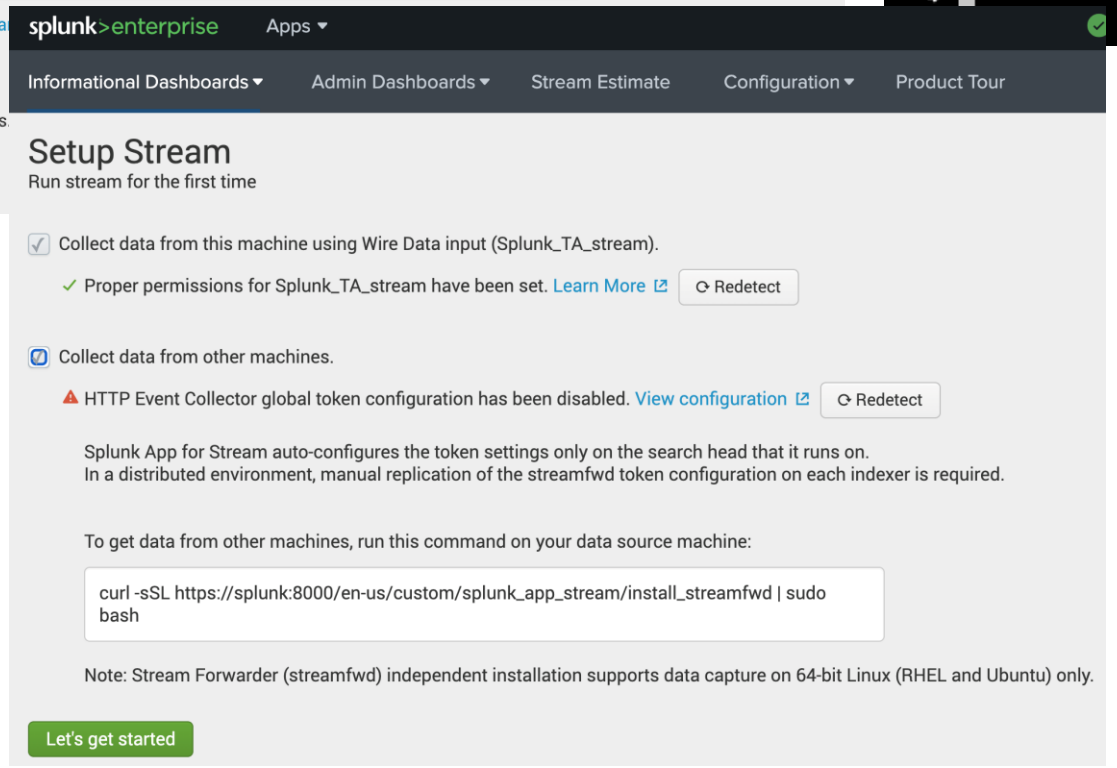
Step 1 – Install Splunk Stream TAs

Step 2 – Add hostname to /opt/splunk/etc/system/local/inputs.conf

Step 3 – Restart Splunk

Cisco Catalyst Add-On for Splunk – Stream



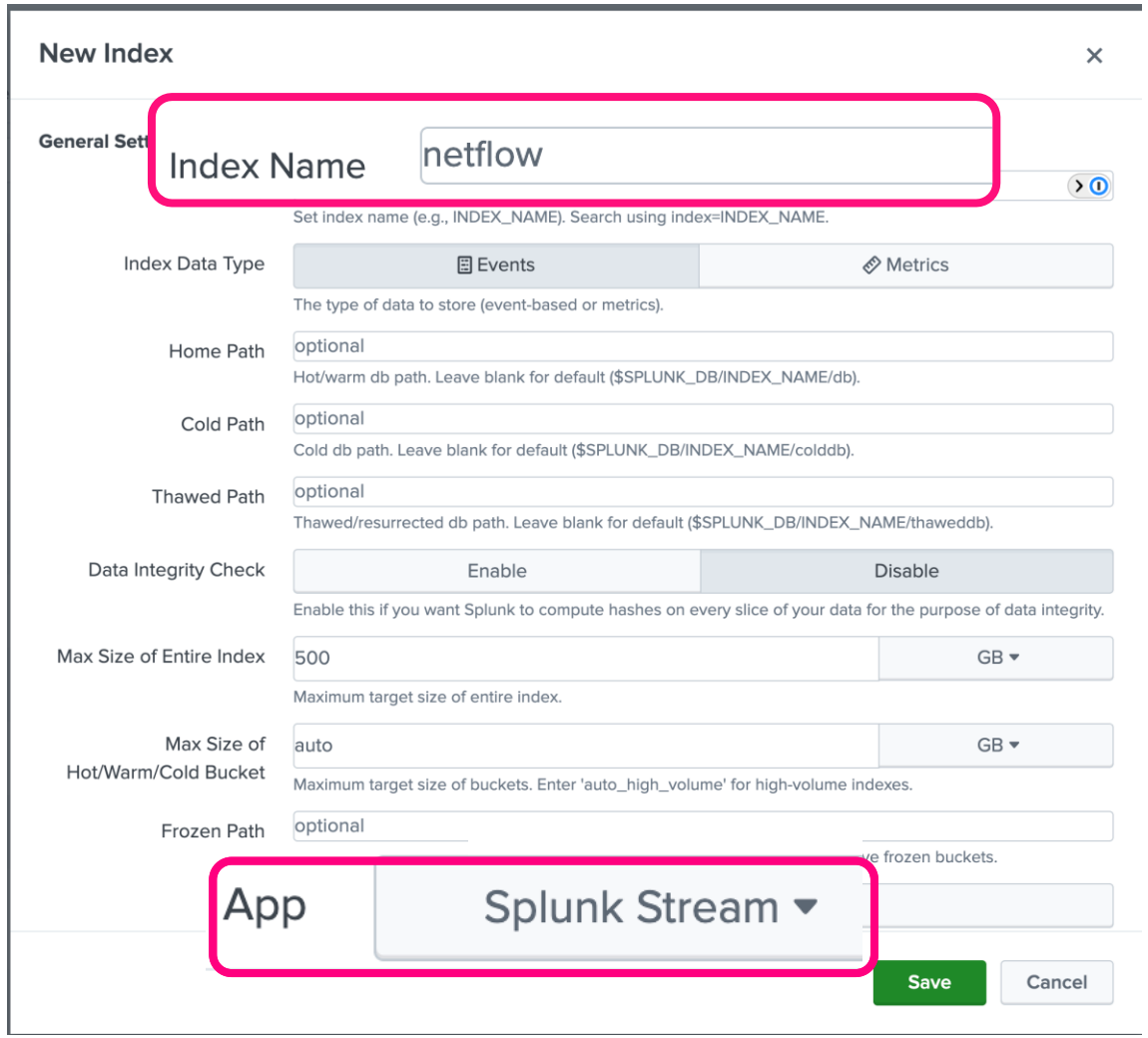


Step 4 – Make set_permissions.sh executable

Step 5 – Run set_permissions.sh

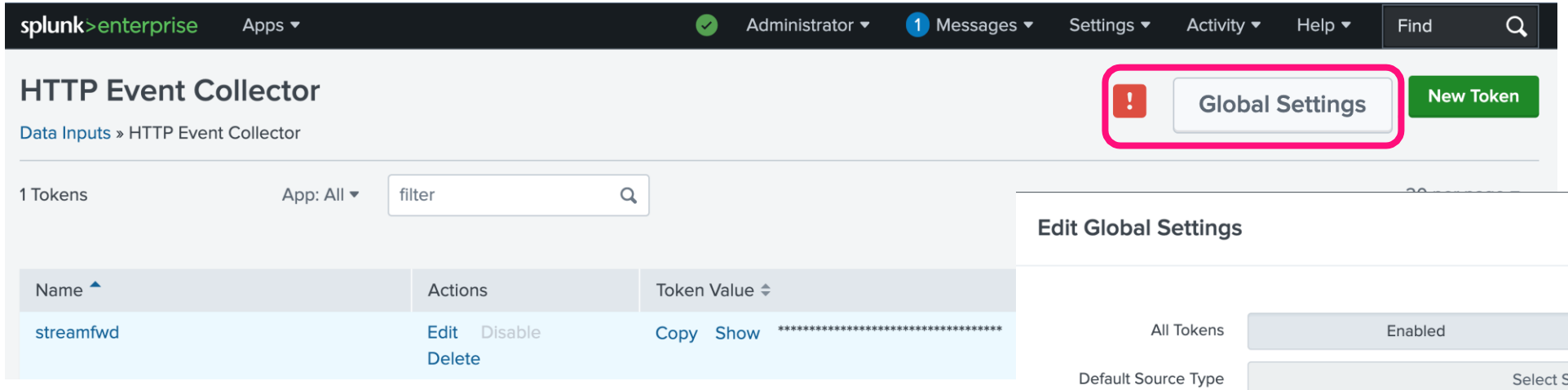
Step 6 – Setup stream forwarder (hidden slides)

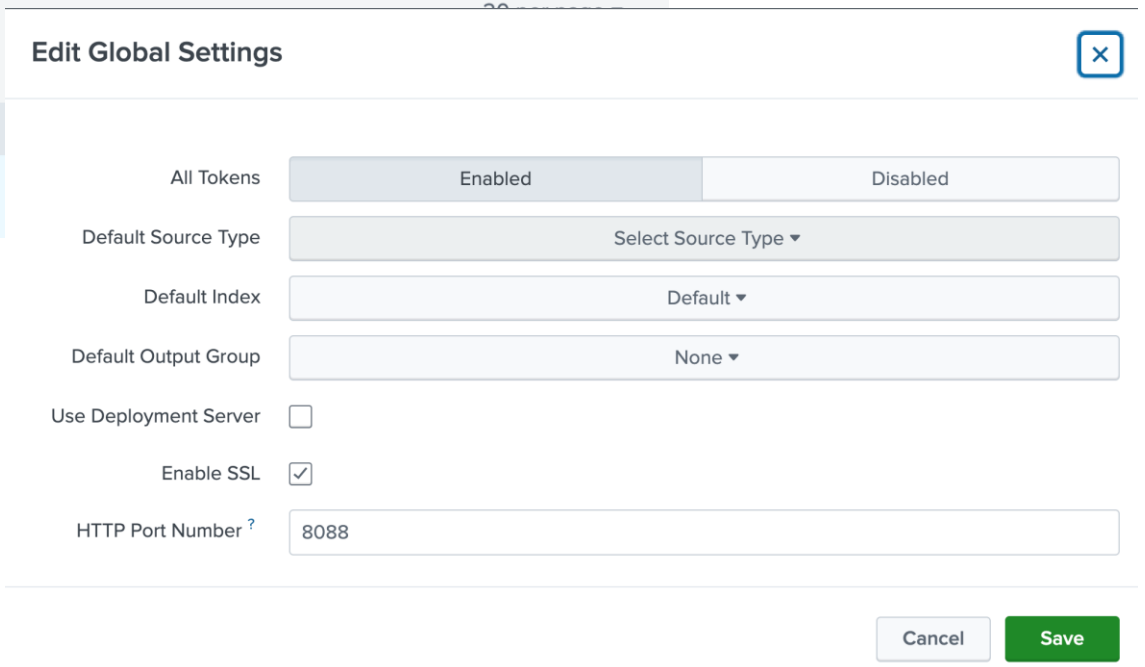
Cisco Catalyst Add-On for Splunk – Indexes



Step 7 – Create an index for NetFlow

Splunk HTTP Event Collector

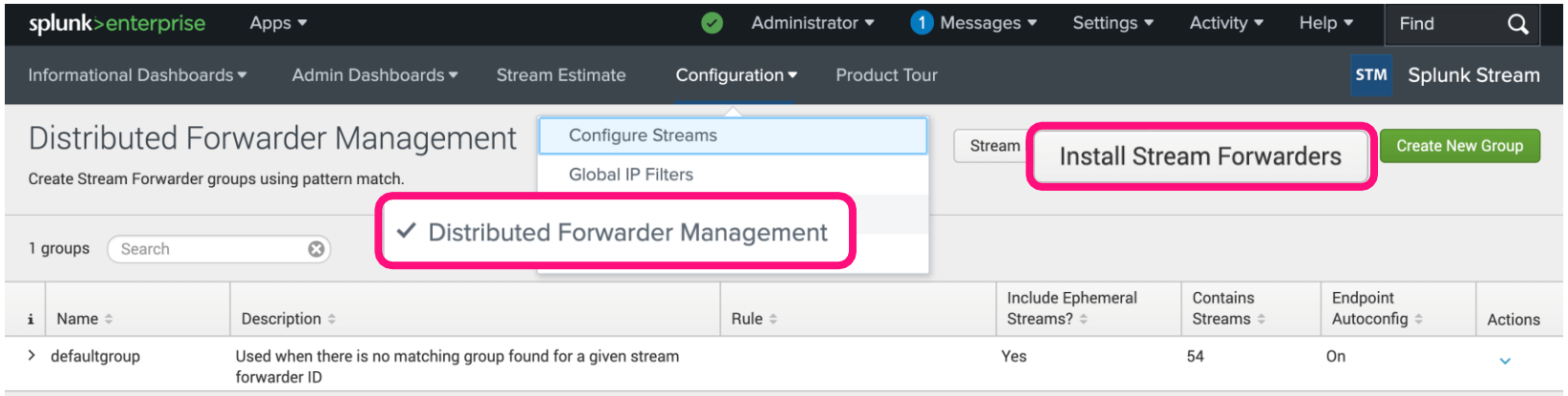


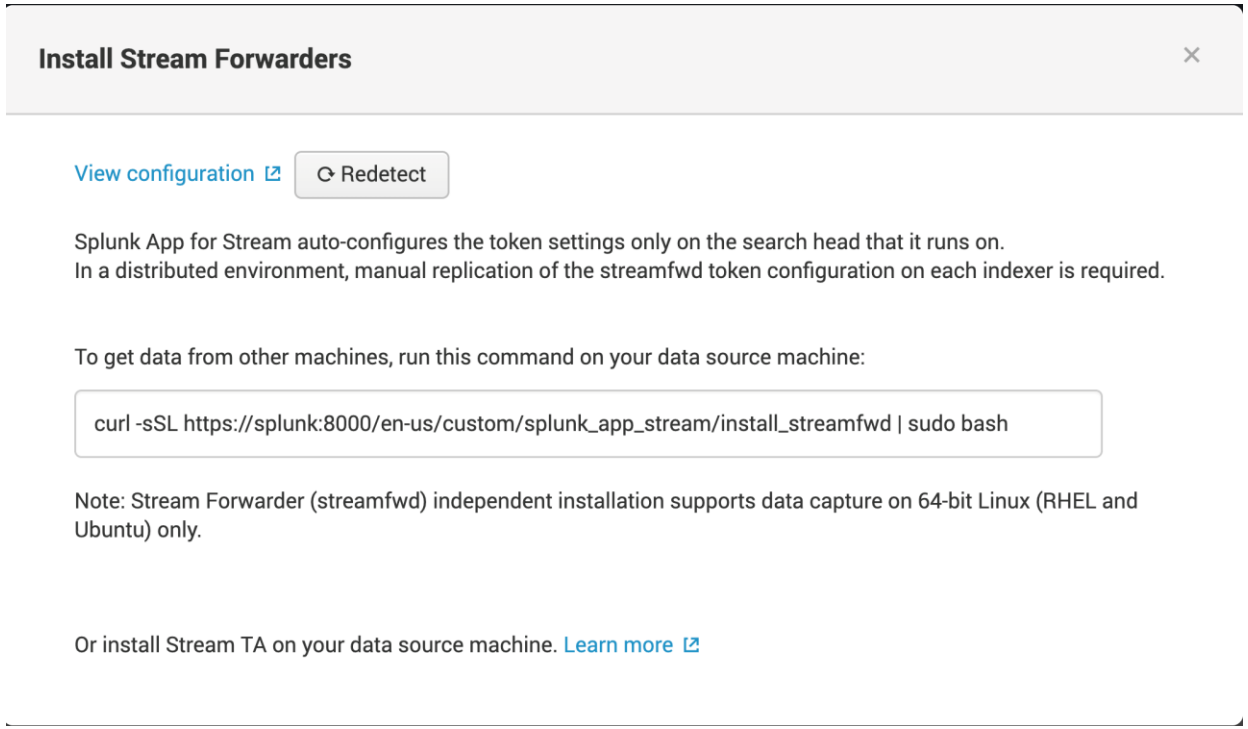


Step 8 – Enable HEC globally

Step 9 – Create a HEC for the NetFlow Stream Forwarder

Stream forwarder





- Copy the setup script text from ‘Install Stream Forwarders’ and install on a dedicated Linux machine

Stream forwarder

```
cisco@streamfwd ~
$ curl -ksSL https://splunk:8000/en-us/custom/splunk_app_stream/install_streamfwd | sudo bash
This script will download and install Splunk Stream Forwarder 8.1.5; do you want to continue (yes/no)? [yes]
downloading splunkstreamfwd-8.1.5-0a64891e.linux64.tar.bz2 package from https://splunk:8000/en-us/custom/splunk_app
_stream/install_streamfwd/linux64 ..
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 45.0M  100 45.0M    0     0   121M      0 --:--:-- --:--:-- --:--:--  121M
splunkstreamfwd-8.1.5/
```

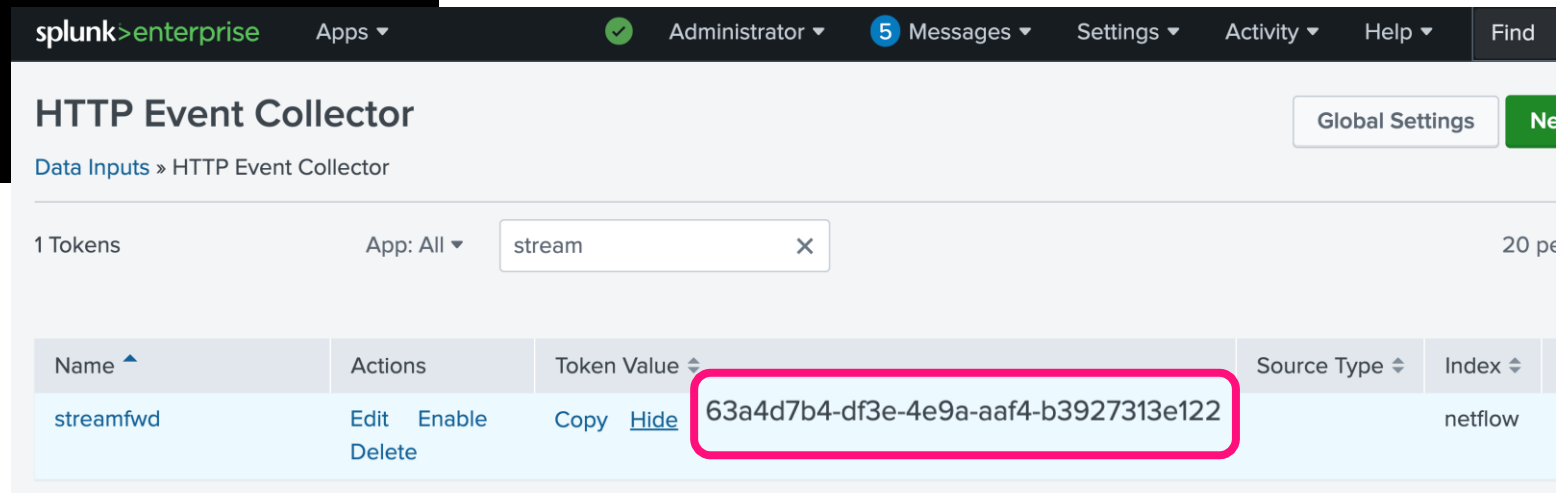
```
⌥⌘1  cisco@streamfwd:~
                                                    ssh ◂ -zsh
~ (ssh)
cisco@streamfwd ~
$ sudo firewall-cmd --zone=public --add-port=9997/udp --permanent
success
cisco@streamfwd ~
$ sudo firewall-cmd --reload
success
cisco@streamfwd ~
$ sudo firewall-cmd --list-ports
9997/udp
cisco@streamfwd ~
$
```

- Run the installer script on the stream forwarder
- Allow the NetFlow port through the firewall on Linux if required

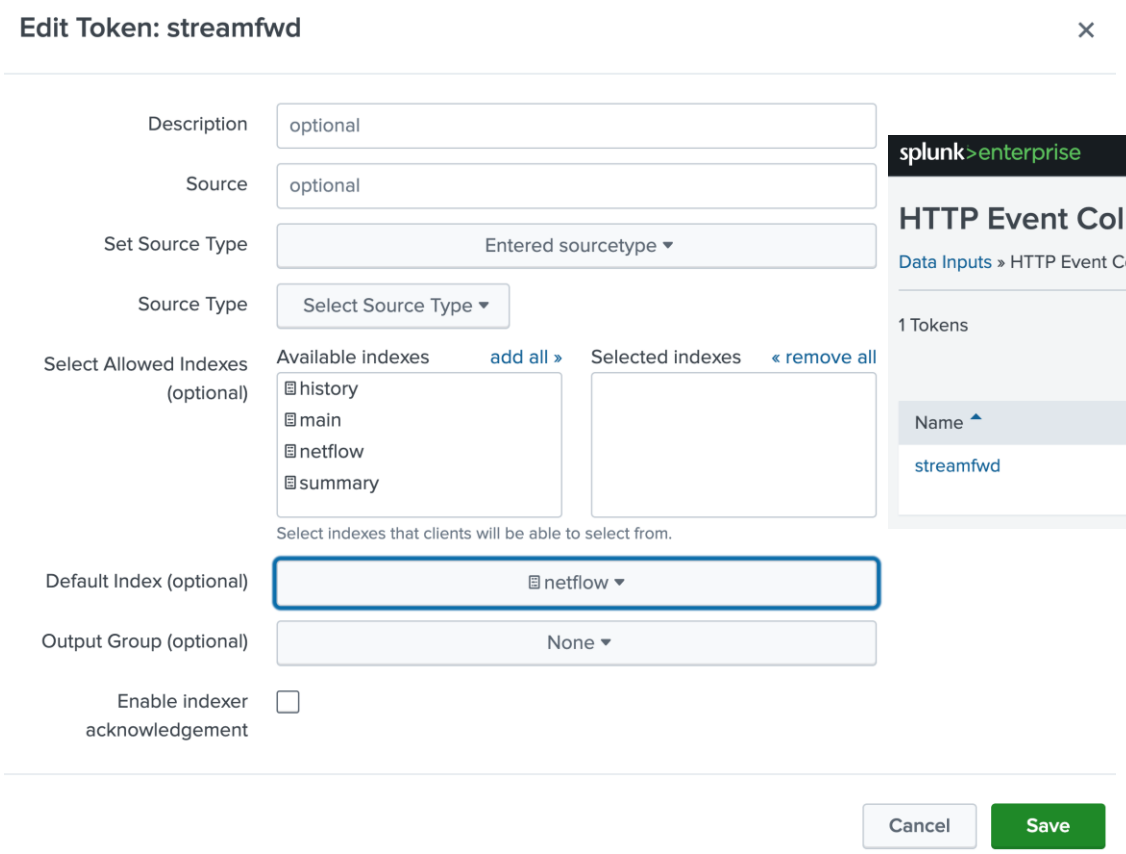
Stream forwarder

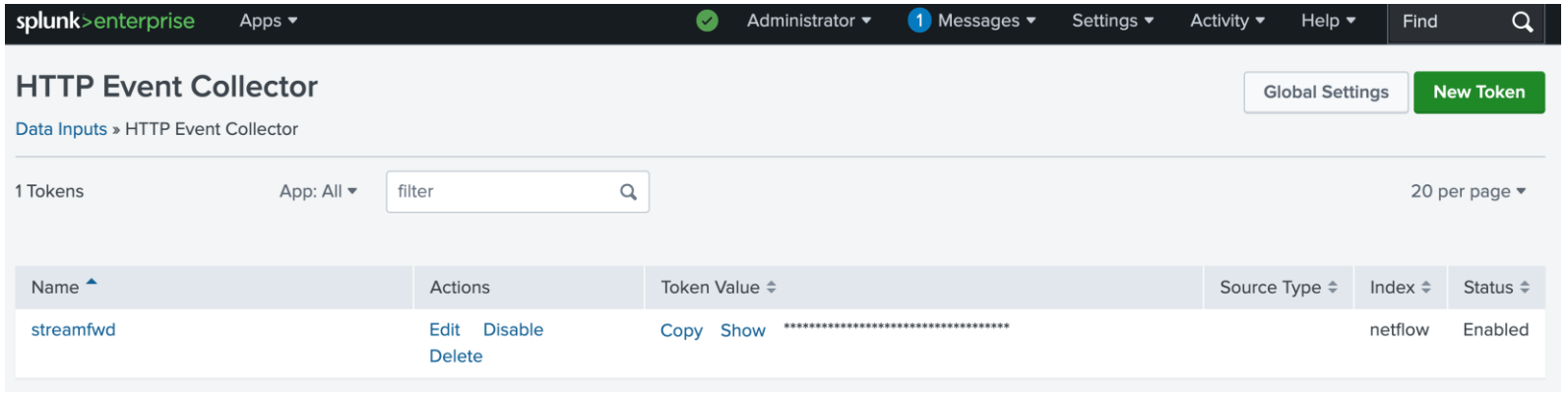
```
⌥⌘1  cisco@streamfwd:~
                                                    ssh ◂ -zsh
~ (ssh)
cisco@streamfwd ~
$ sudo cat /opt/streamfwd/local/streamfwd.conf
[streamfwd]
# My local IP address
ipAddr = 10.67.27.69

httpEventCollectorToken = 63a4d7b4-df3e-4e9a-aaf4-b3927313e122
indexer.0.uri = https://10.67.27.231:8088

netflowReceiver.0.ip = 10.67.27.69
netflowReceiver.0.port = 9997
netflowReceiver.0.decoder = netflow

cisco@streamfwd ~
$ ping splunk
PING splunk (10.67.27.231) 56(84) bytes of data.
64 bytes from splunk (10.67.27.231): icmp_seq=1 ttl=64
^C
```

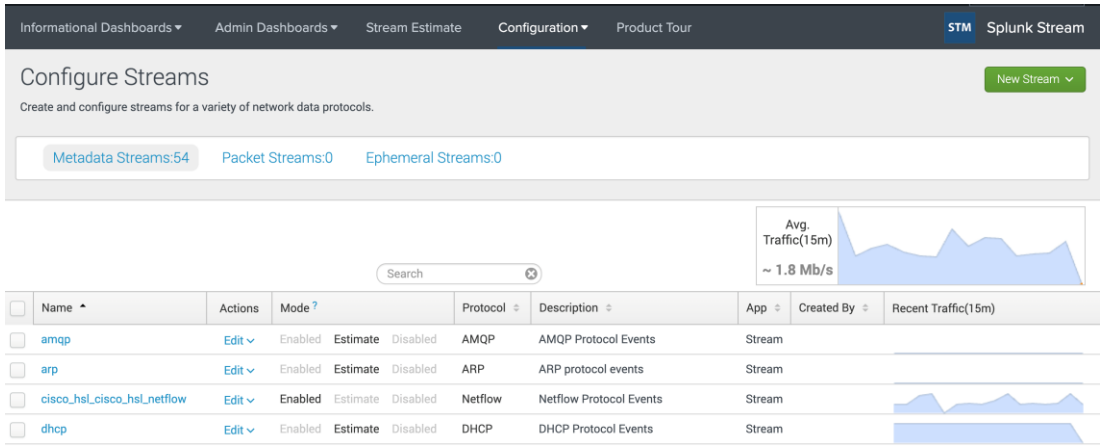
- Create a local streamfwd.conf file
- Specify the HEC token on Splunk for the stream forwarder in the stream forwarder configuration file
- Restart the stream forwarder



Splunk HTTP Event Collector



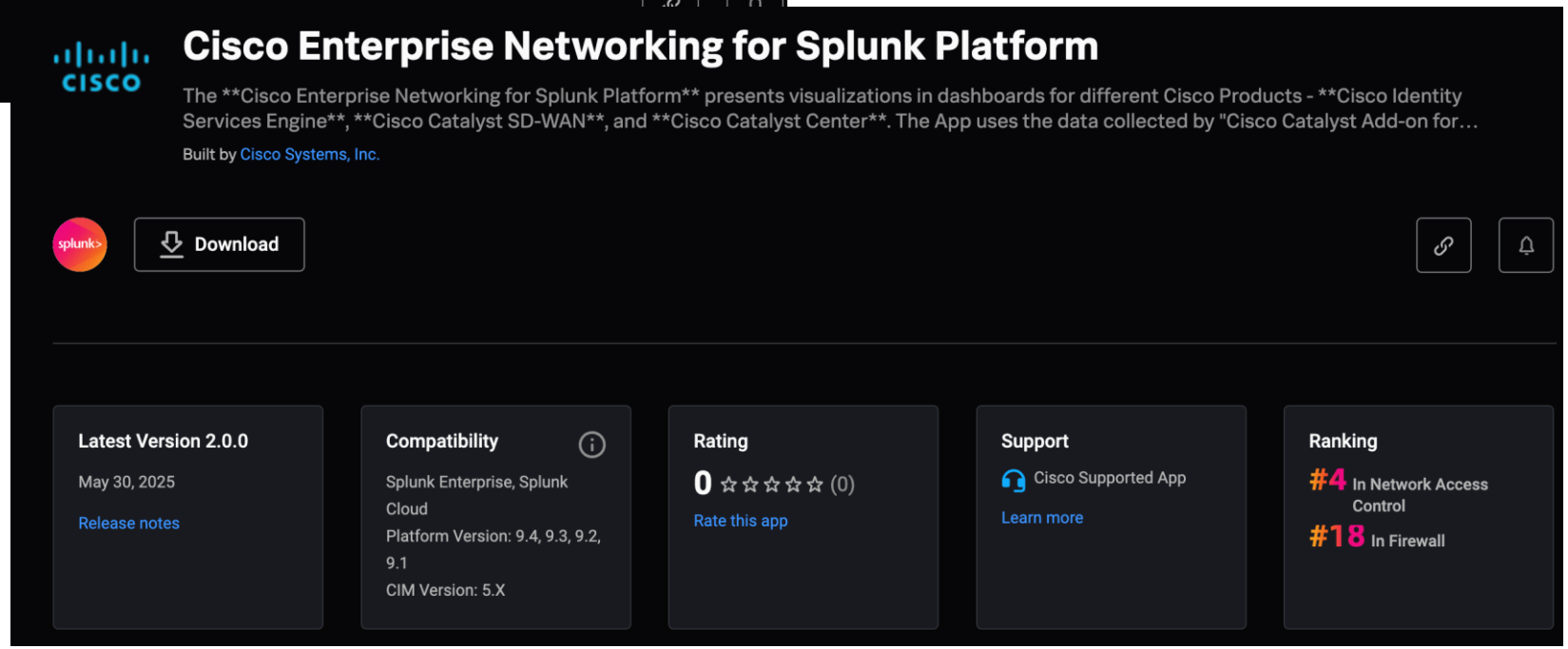




Step 10 – Set the streamfwd HEC to use the netflow index

Enterprise Networking App & Catalyst Add-On

Cisco Catalyst & Enterprise Networking Add-Ons for Splunk



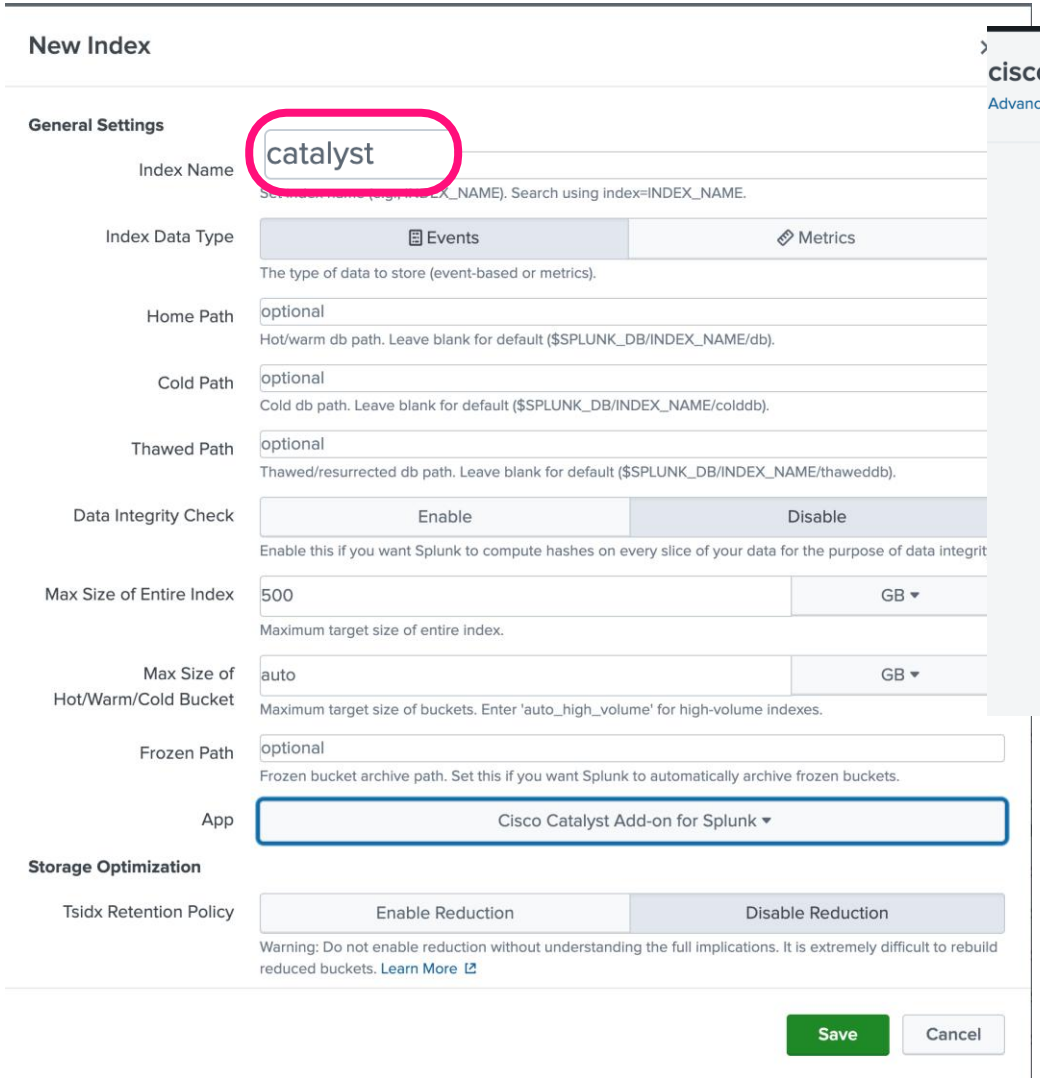
- Catalyst Add-on – Parses data from from specified sources and stores then into Splunk indexes
- Enterprise Networking – Presents visualizations in dashboards based on the Catalyst Add-on

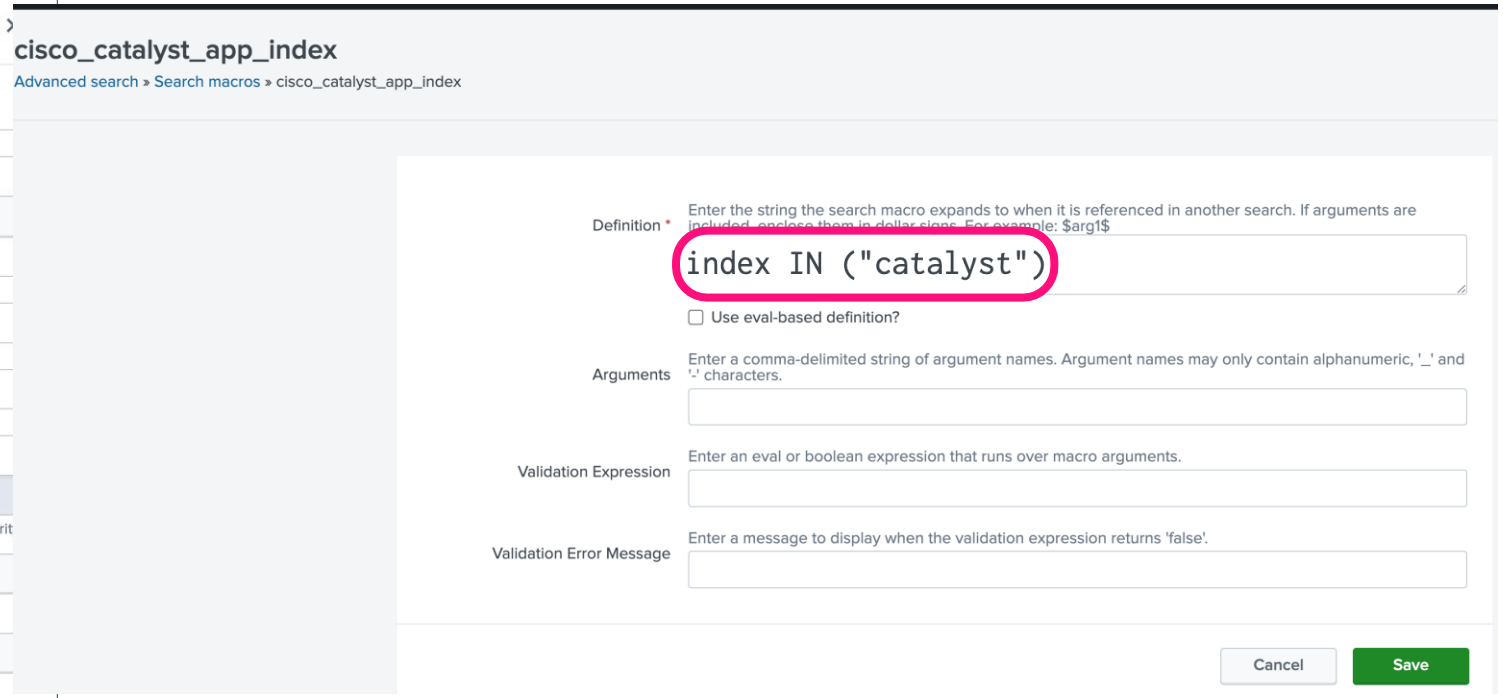
https://splunkbase.splunk.com/app/7538

https://splunkbase.splunk.com/app/7539

Cisco Catalyst Add-On for Splunk – Indexes

Store data from Catalyst Add-on to a dedicated Splunk index





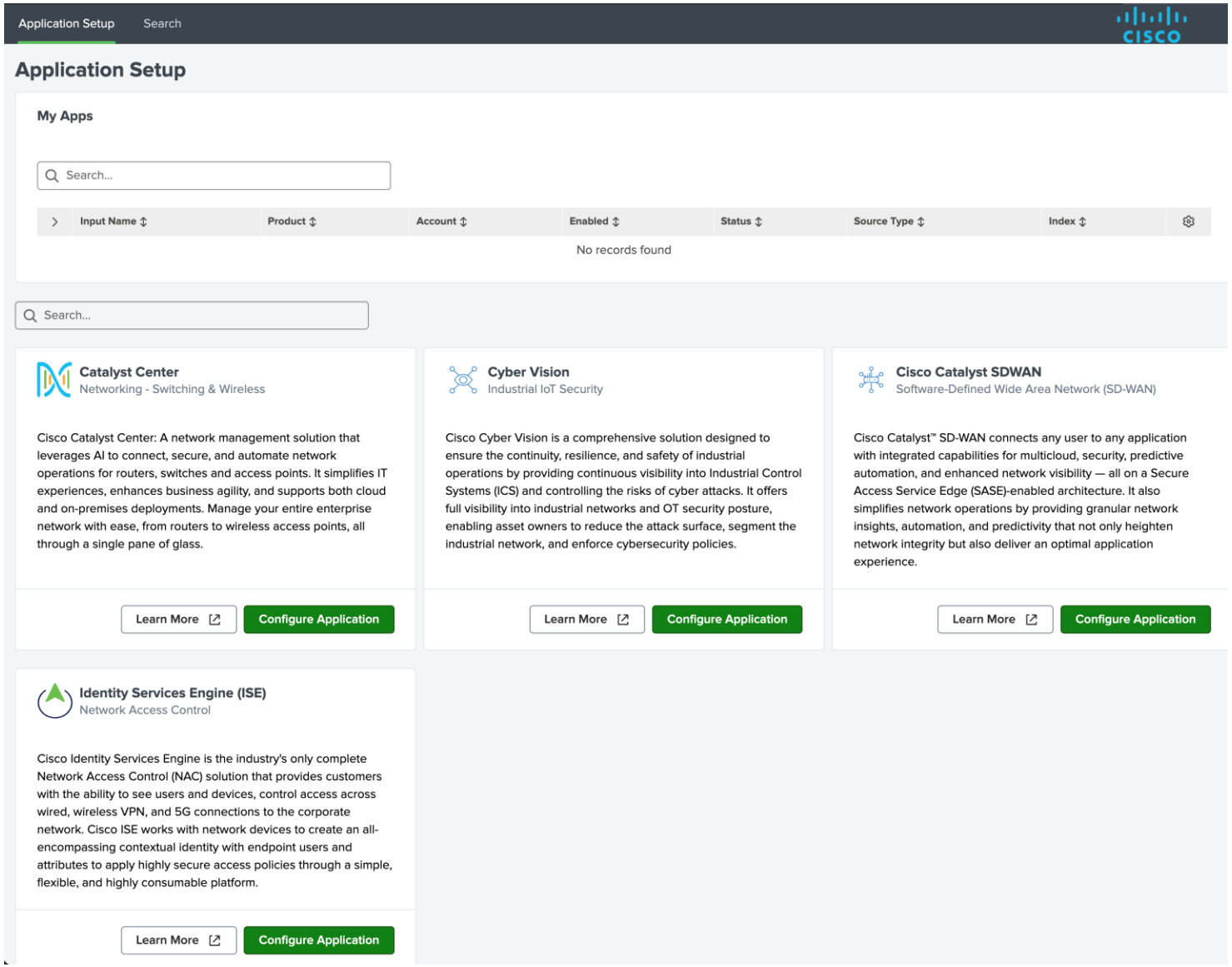
Splunk Index

- It is recommended to have a dedicated Splunk index for an application. A Splunk index is a repository where Splunk stores data.

Search Macro

- Adjust the cisco_catalyst_app_index to use the dedicated Splunk index.

Cisco Catalyst Add-On for Splunk



Catalyst Center

- Facilitates the collection of network inventory, assurance data, event notifications, and audit logs from Catalyst Center

Catalyst SD-WAN

- Collects various types of Cisco SD-WAN log and NetFlow data

Identity Service Engine

- Collects and normalizes ISE data for ingestion into Splunk

Cyber Vision

- Enables integration by pulling device, events, activities, flows, and vulnerability information from Cisco Cyber Vision via REST API

Catalyst Center

Catalyst App – Catalyst Center

Send Catalyst Center Data to Splunk

Catalyst Center

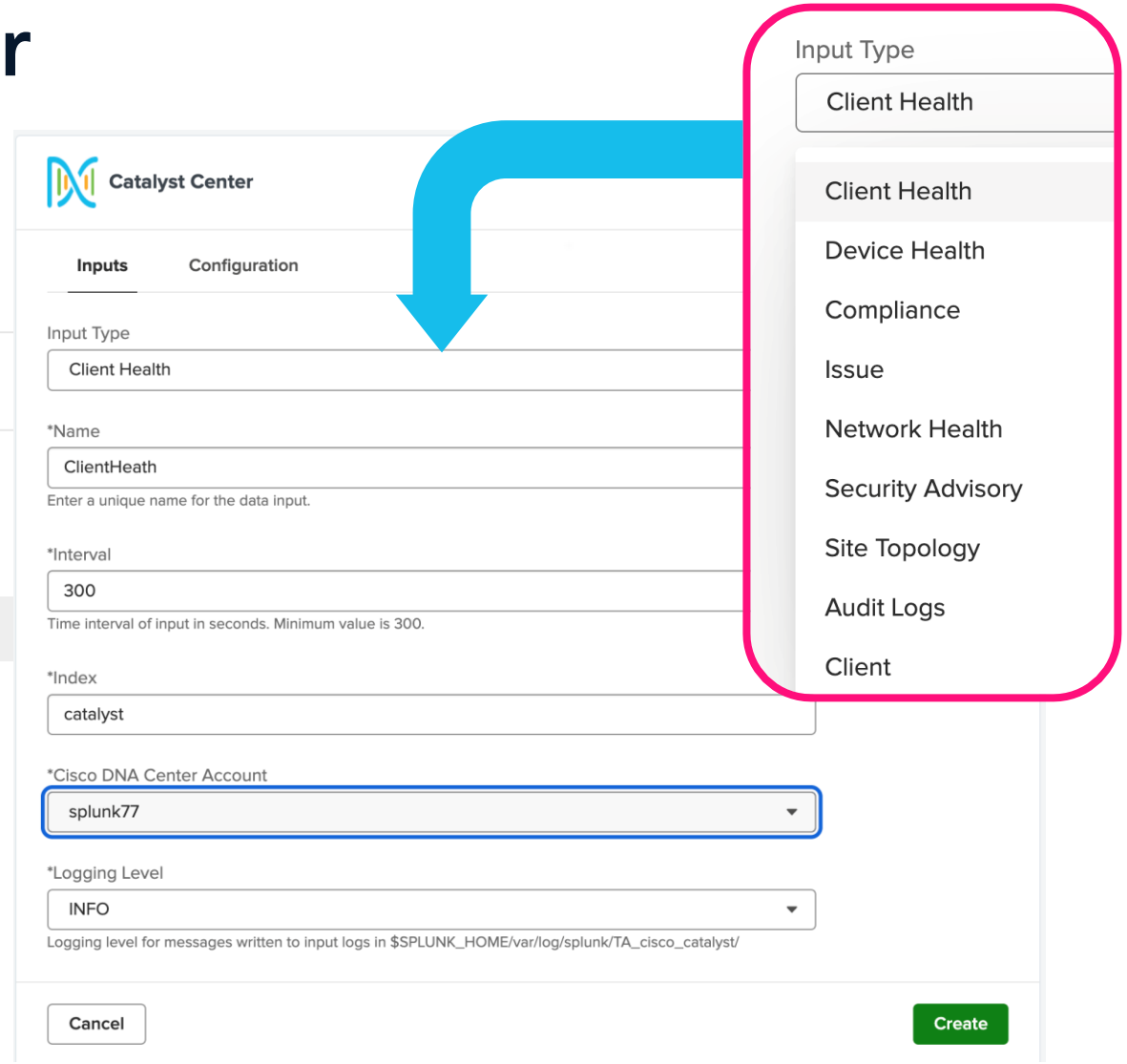
Inputs | **Configuration**

Search...

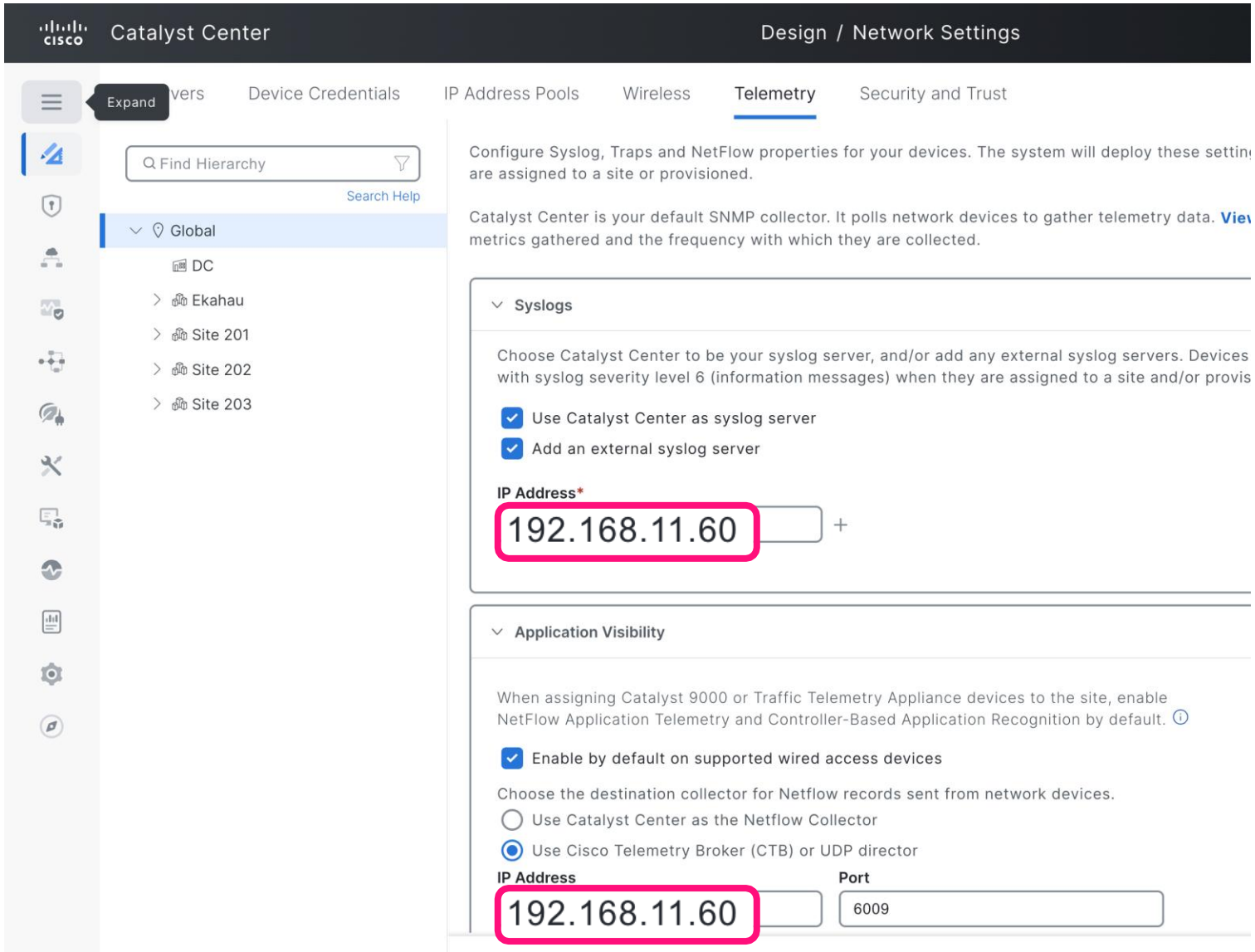
Account Name	Username	Hostname
splunk77	splunk	https://10.67.27.77
splunk79	splunk	https://10.67.27.79

Step 1 – Add Catalyst Center(s) user account

Step 2 – Add Inputs



Getting Catalyst Center Telemetry Sent to Splunk



Syslog

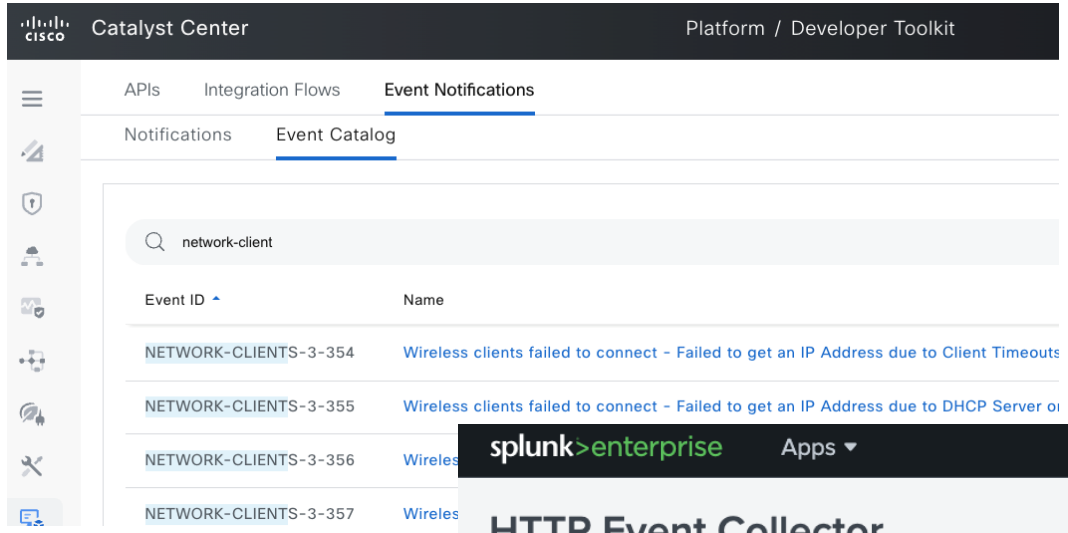
- Add an entry for syslog with Splunk as the destination

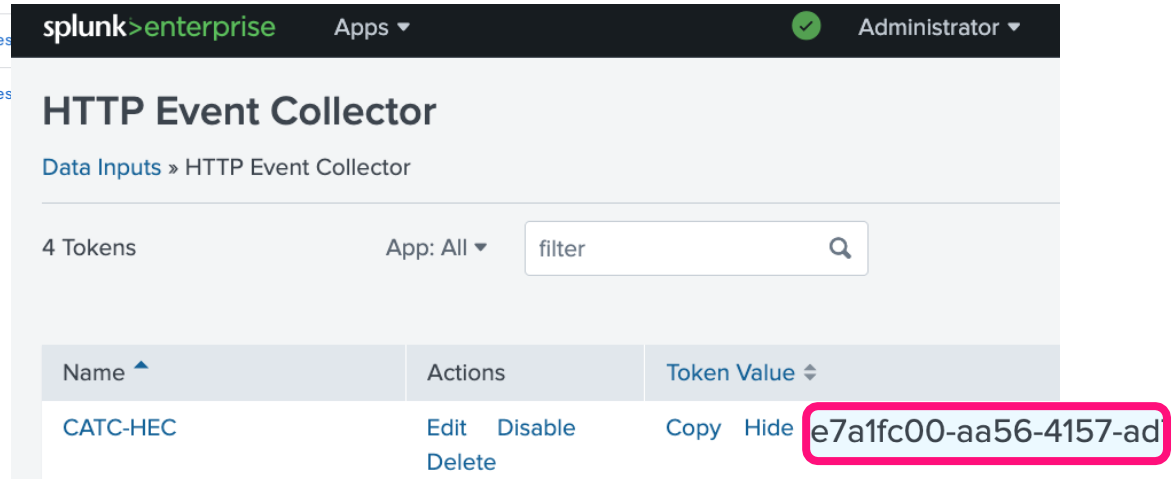
Application Visibility

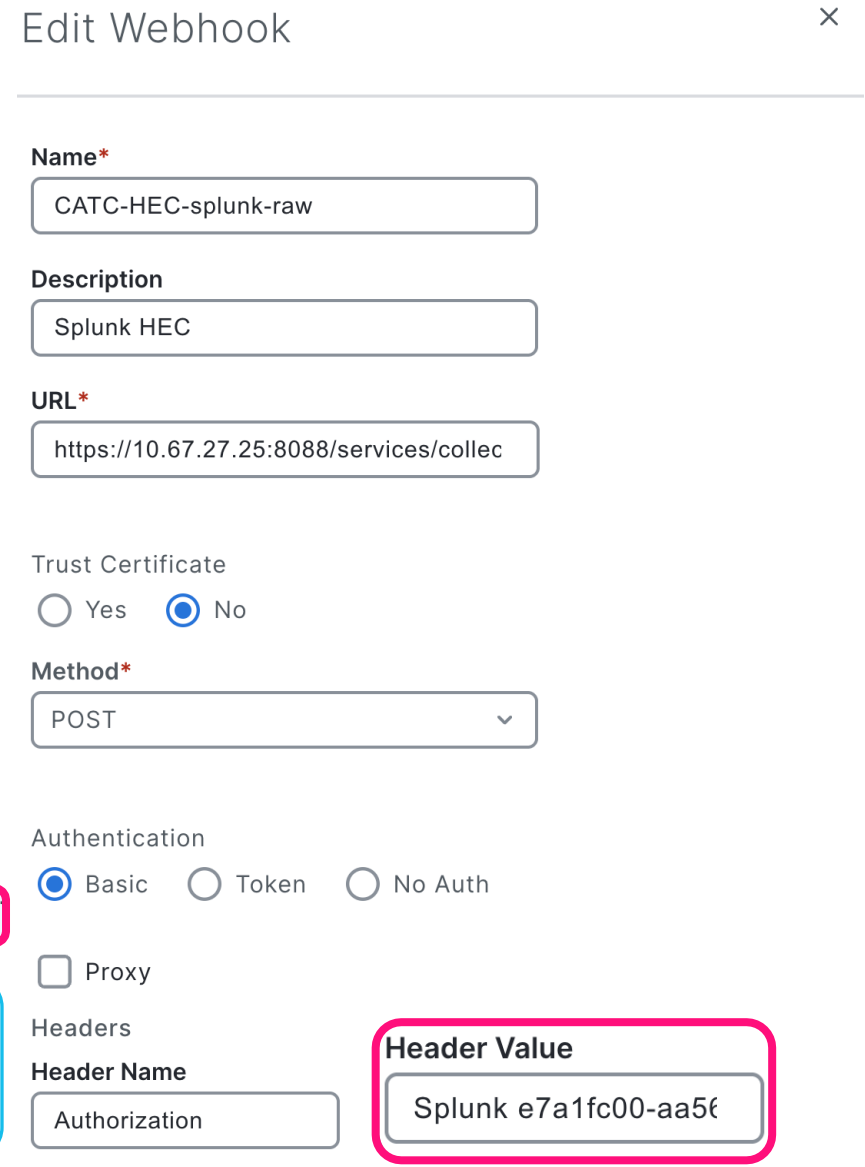
- Use a Telemetry Broker (shown) or add a NetFlow exporter using Catalyst Center Templates

Catalyst Center Event Notifications – Webhook

Send events and notifications from Catalyst Center directly to Splunk







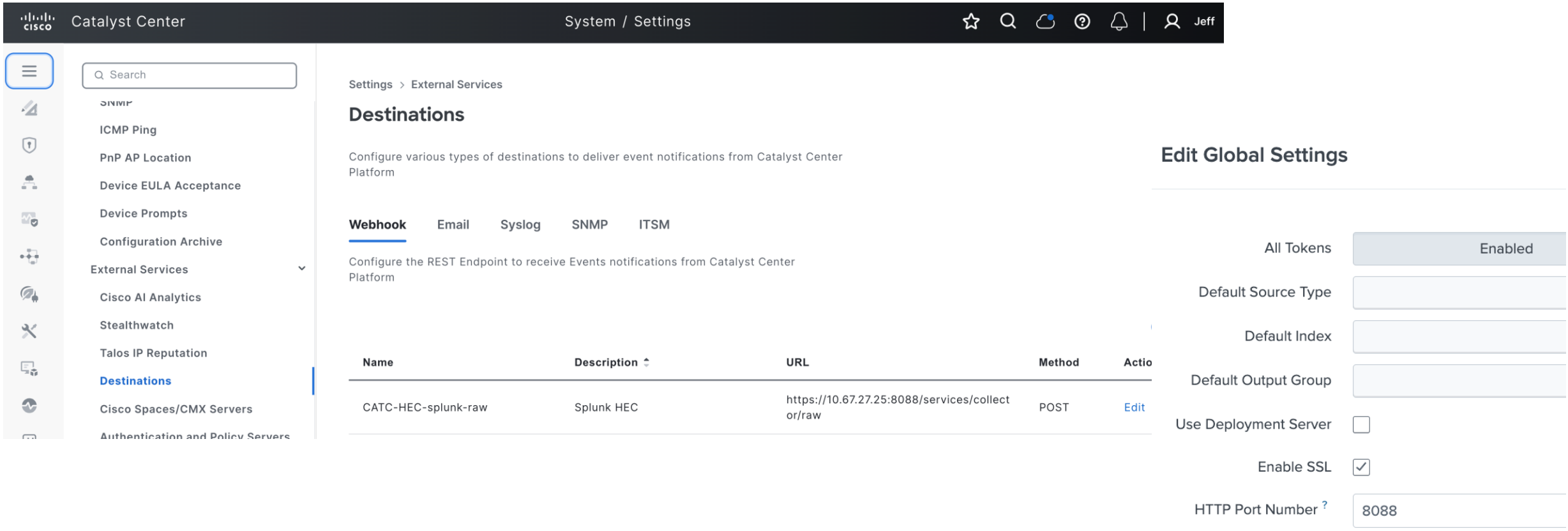
Step 1 – Create a destination webhook in Catalyst Center Settings → External Services

- Header Value must contain the text Splunk, followed by the Splunk HEC token

cisco

Catalyst Center Event Notifications – Webhook

Send events and notifications from Catalyst Center directly to Splunk



Step 1 (cont)– Create a destination webhook in Catalyst Center Settings → External Services

- URL is the Splunk HEC listener on https://<splunk-svr>:8088/services/collector/raw

Catalyst Center Event Notifications – Webhook

Step 3 - REST Settings

Configure the REST channel settings for this notification

Select a REST Webhook setting. Or Click here to create a new

Select Instance

CATC-HEC-splunk-raw

URL

https://10.67.27.25:8088/services/collector/raw

Trust Certificate

Yes No

Method

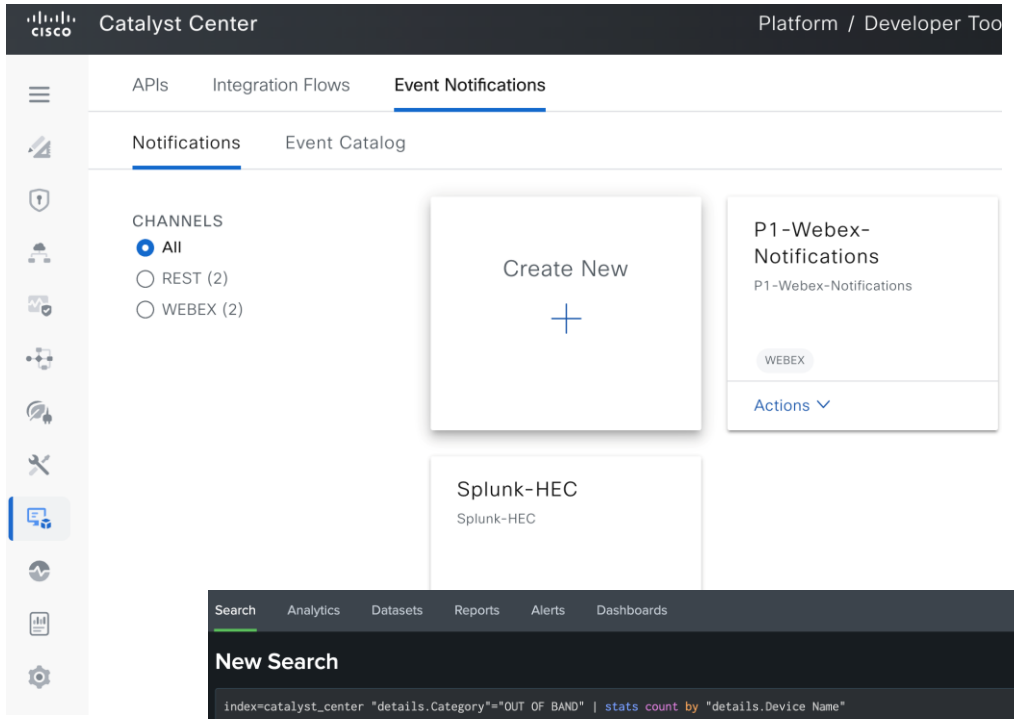
POST

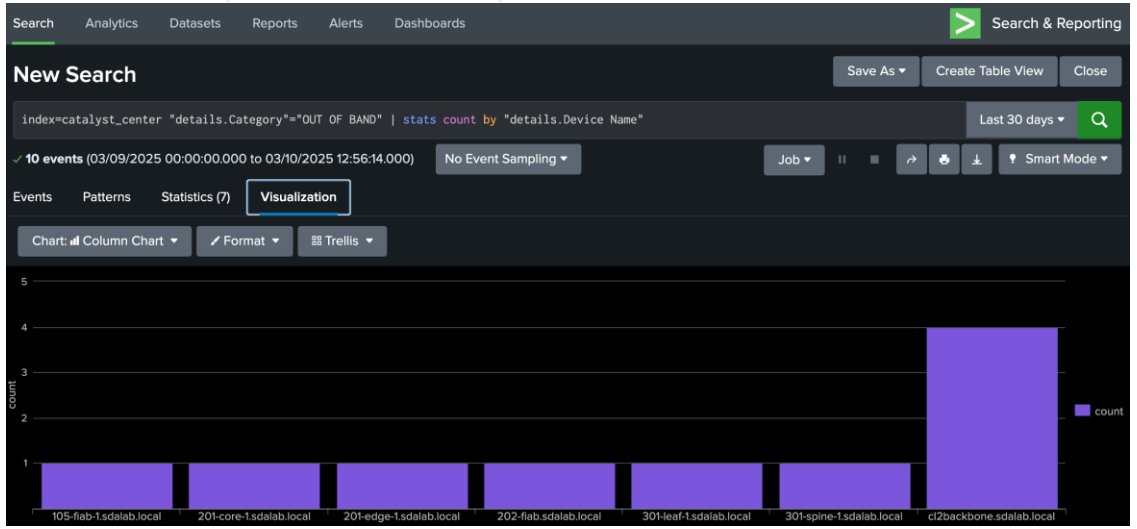
Authentication

Basic Token No Auth

Headers

Header Key	Header Value
Authorization	Splunk e7a1fc00-aa56-4157-ad



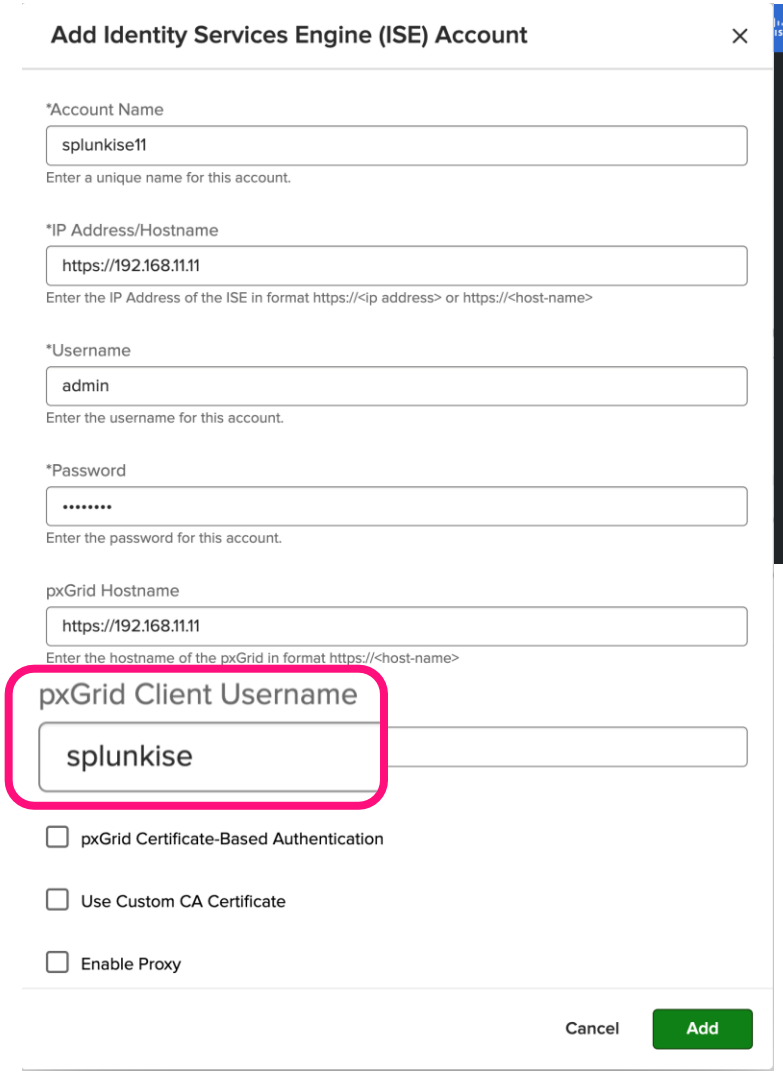


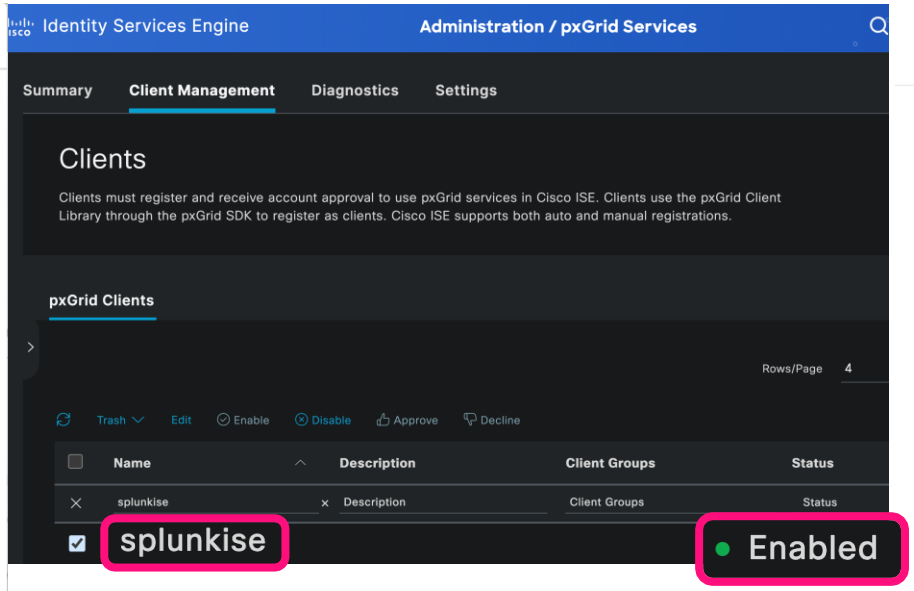
Step 2 – Subscribe to Events in Catalyst Center Platform → Developer Toolkit → Event Notifications

Identity Services Engine

Catalyst App – Identity Services Engine

Send Identity Services Engine Data to Splunk



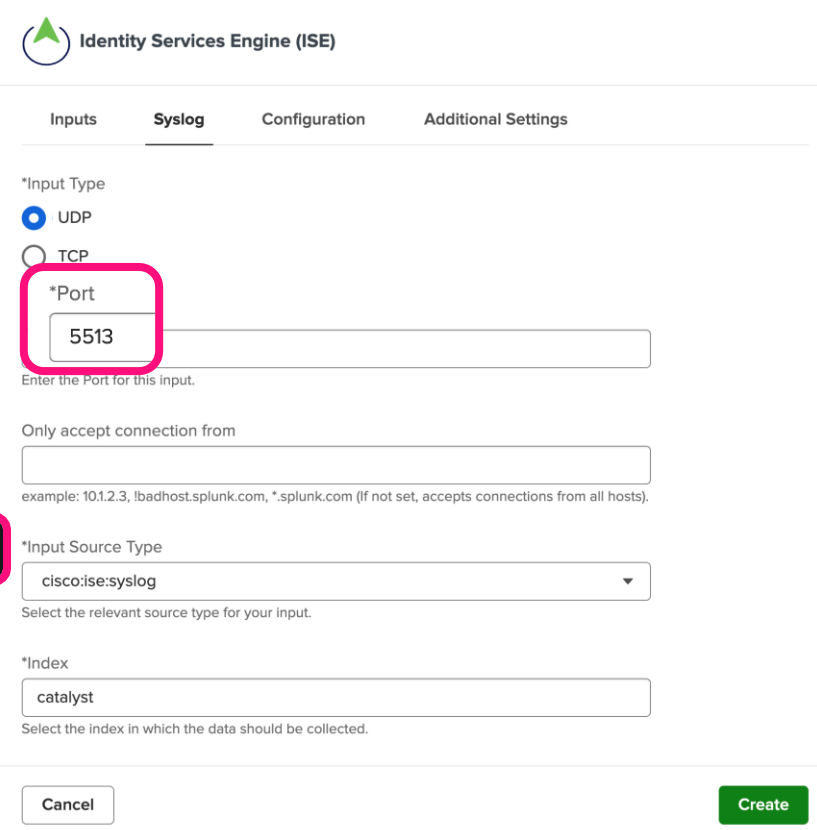


Step 1 – Add ISE user account

- Creates a pxGrid client on ISE
- Enable pxGrid client on ISE

Step 2 – Add Syslog

- Creates a listener port on Splunk automatically



Catalyst App – Identity Services Engine Inputs

Send Identity Services Engine Data to Splunk

Identity Services Engine (ISE)

Inputs | Syslog | Configuration | Additional Settings

*Name
splunkISE
Enter a unique name for the data input.

*Interval
300
Time interval of input in seconds. Minimum value is 60.

*Index
catalyst

*Cisco ISE Account
splunkise11

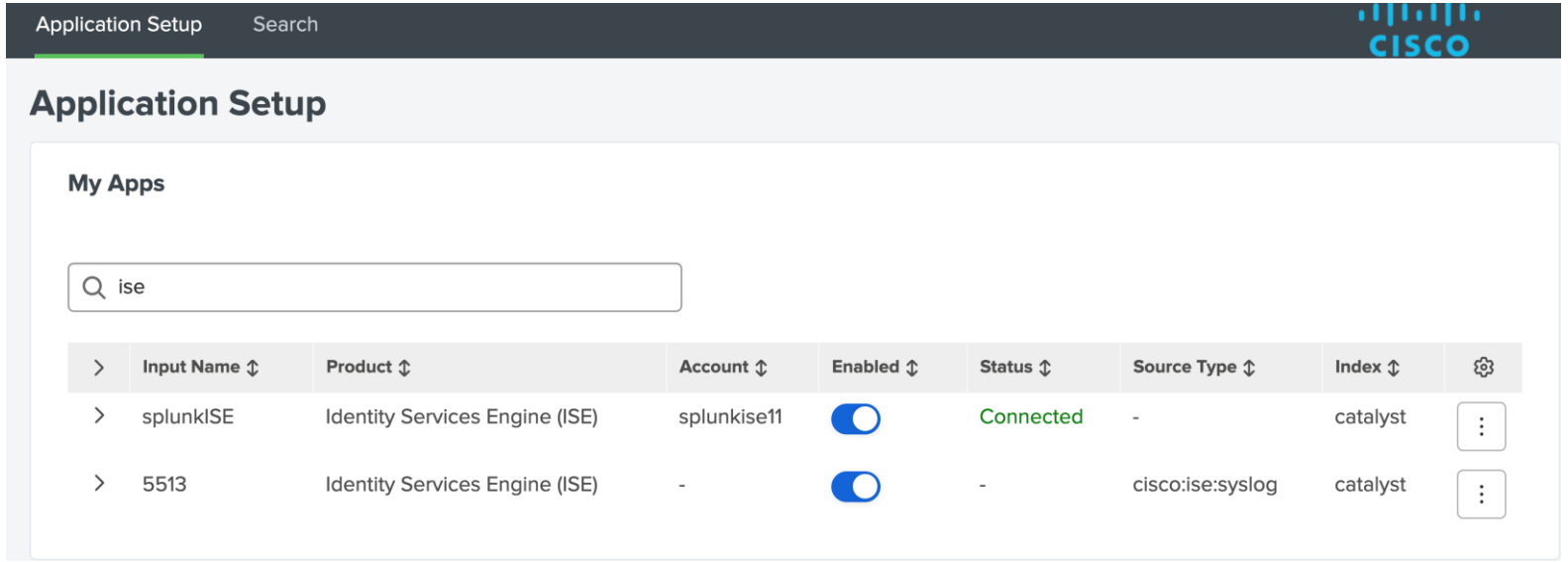
*Fetch Cisco ISE Environment Data
Security Group Tags | Authz Policy Hit | ISE TACACS Rule Hit

IP-SGT Bindings
Configure the settings in the Additional Settings Tab if you want to fetch the Security Group Tags from Cisco ISE server.

*Logging Level
INFO
Logging level for messages written to input logs in $SPLUNK_HOME/var/log/splunk/TA_cisco_catalyst/

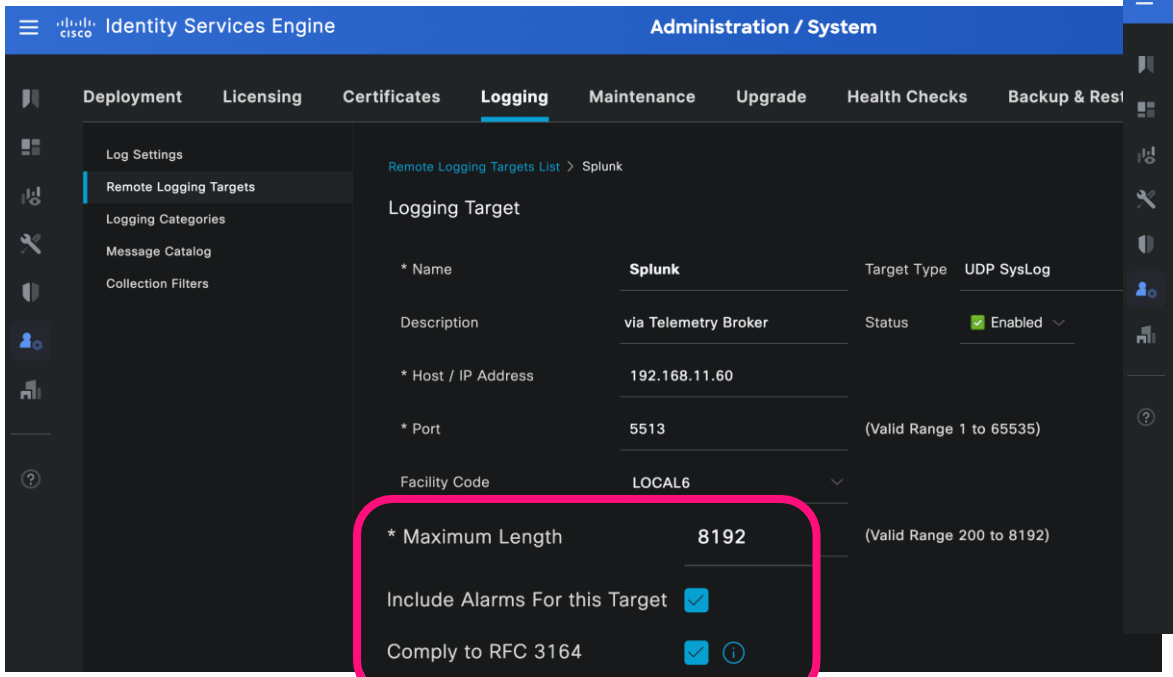
Cancel | Create

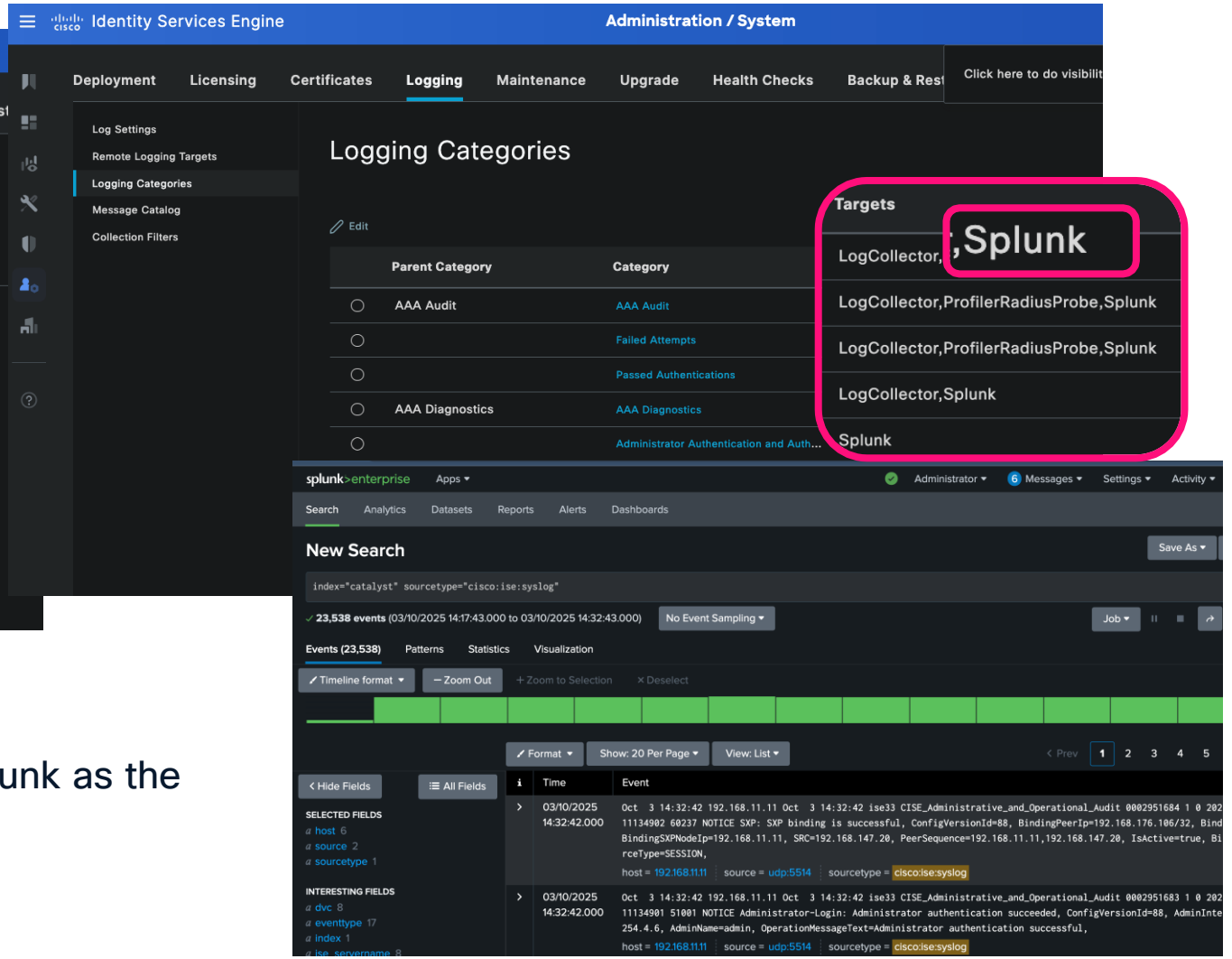
Step 3 – Add ISE inputs



Identity Services Engine Logging to Splunk

Remote Targets and Logging Categories





Remote Logging Target

- Configure an ISE Remote Logging Target using Splunk as the destination

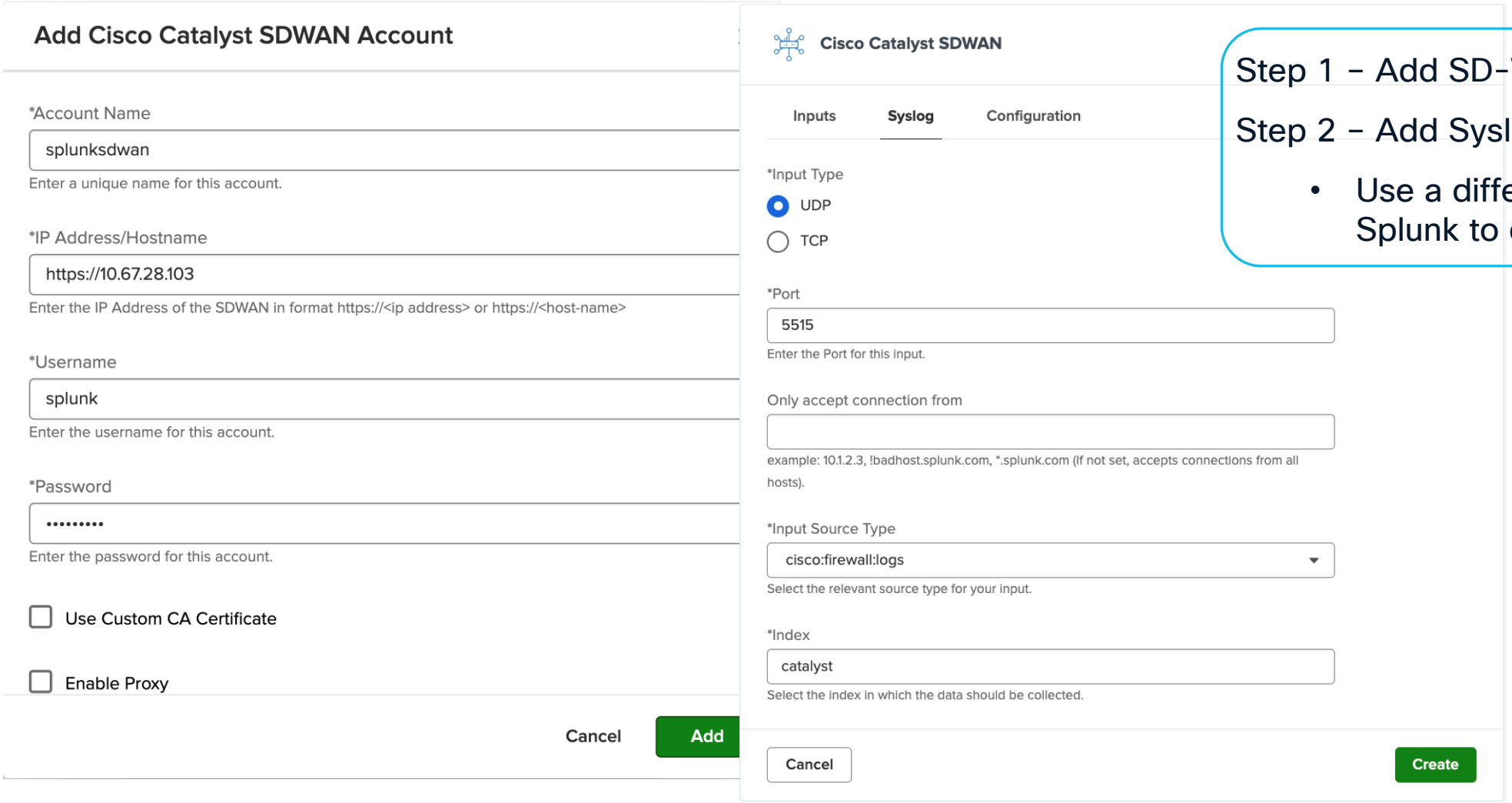
Logging Category

- Add Splunk Remote Logging Target to Logging Categories

SD-WAN

Catalyst App – SD-WAN

Send SD-WAN Data to Splunk



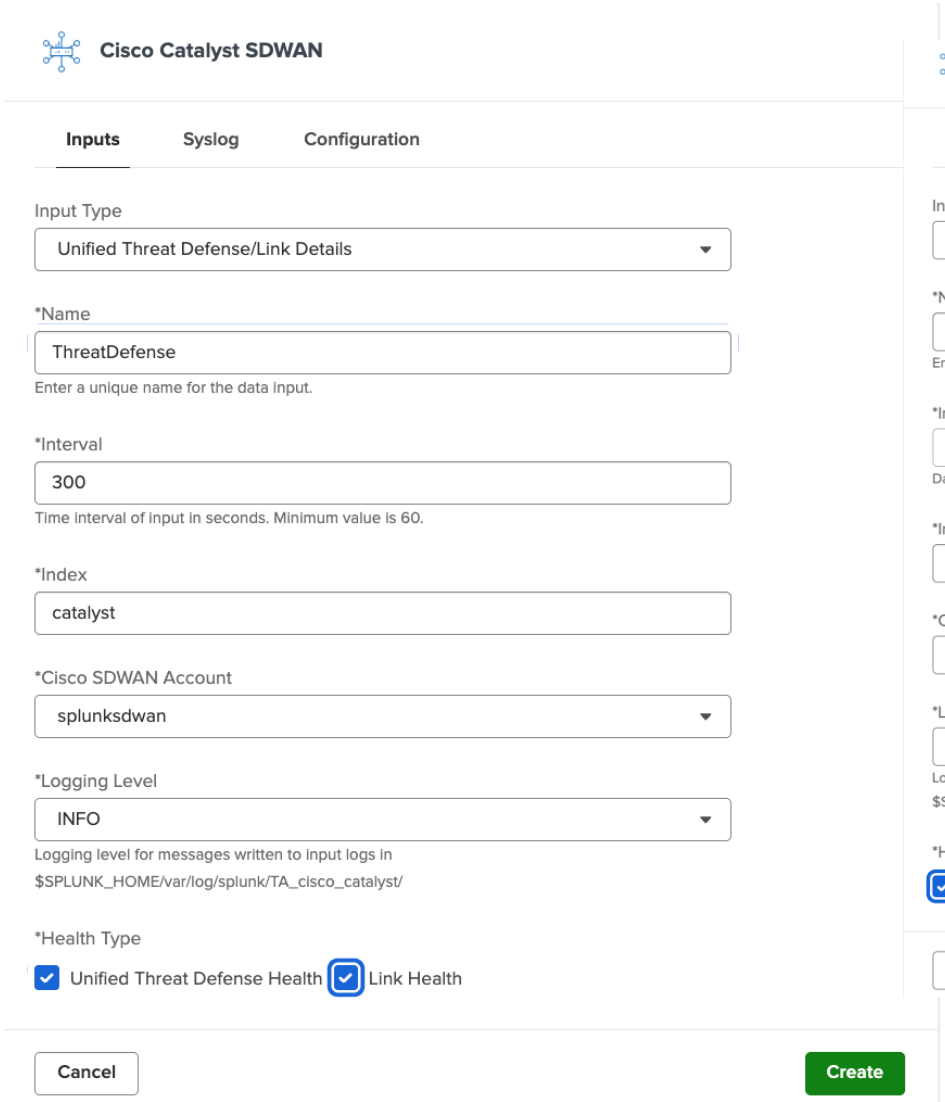
Step 1 – Add SD-WAN user account

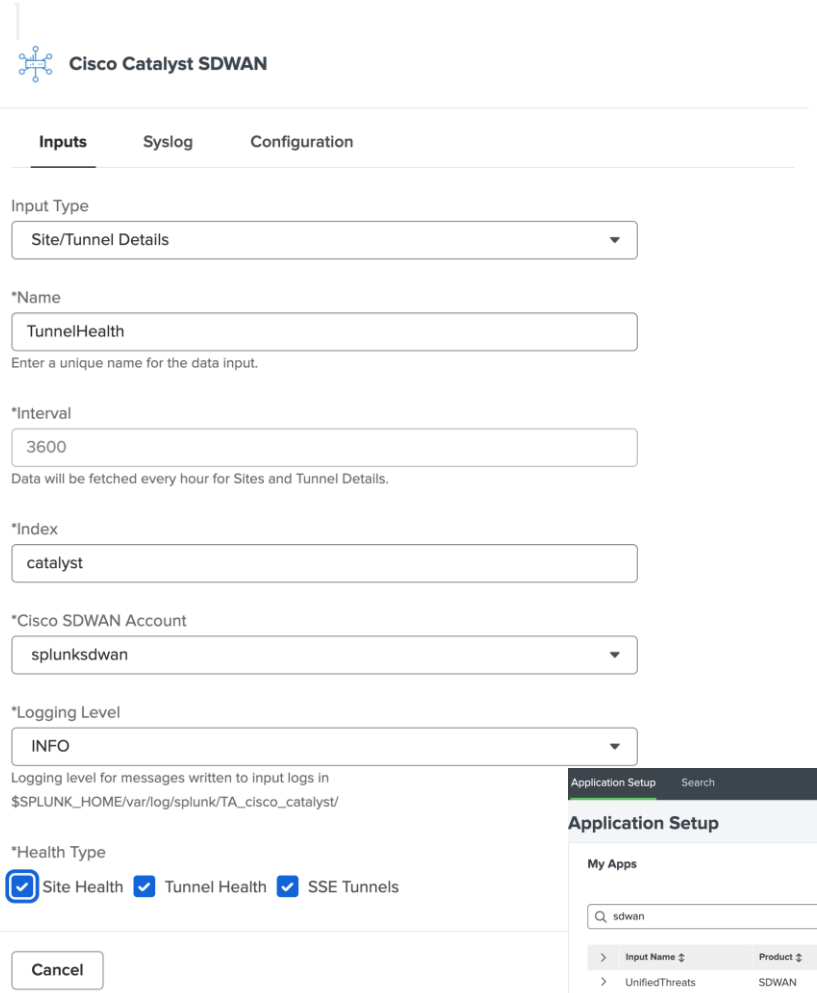
Step 2 – Add Syslog

- Use a different listener port on Splunk to easily search data

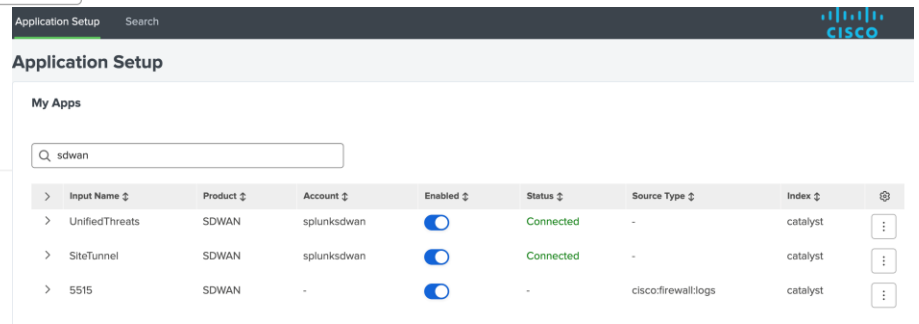
Catalyst App – SD-WAN

Send SD-WAN Data to Splunk



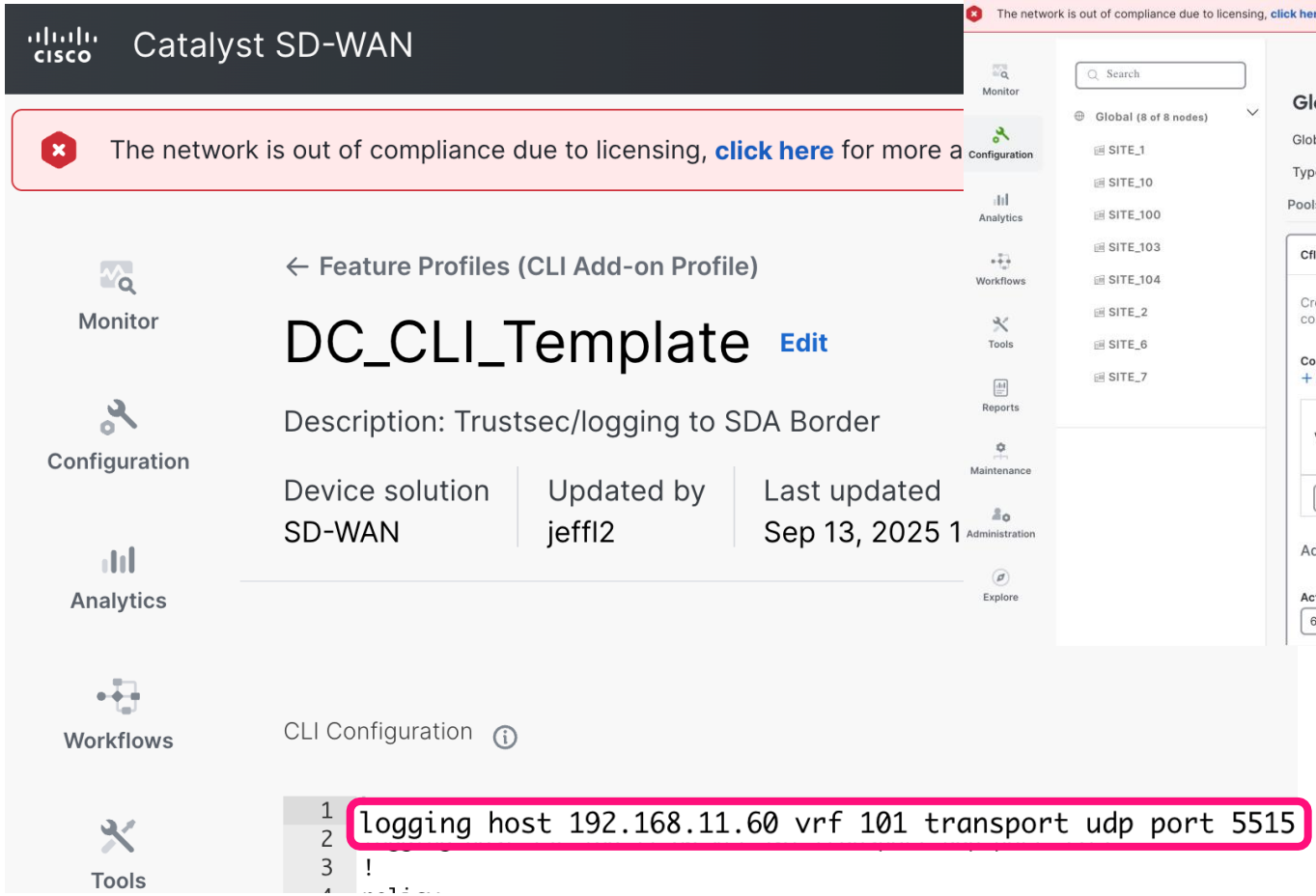


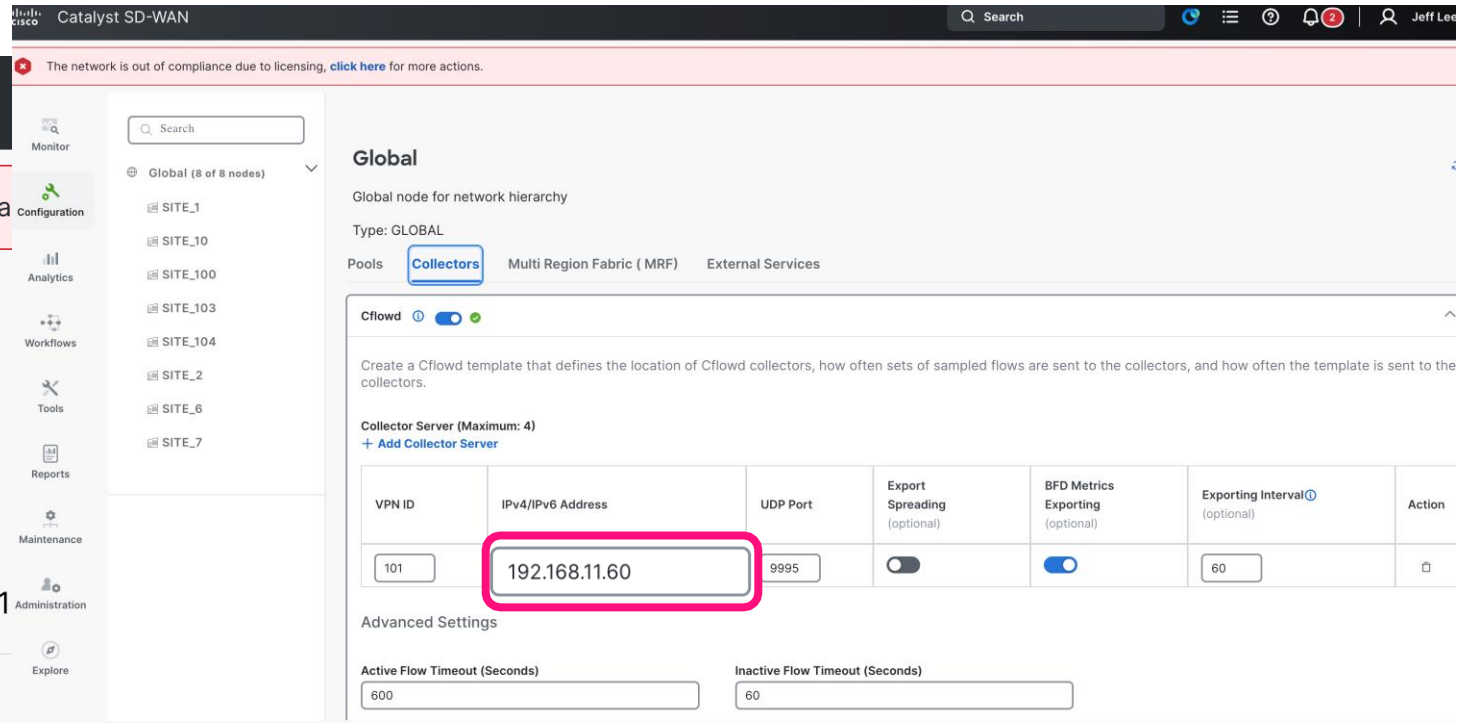
Step 3 – Add SD-WAN inputs



SD-WAN Logging to Splunk

Custom syslog port and NetFlow for Splunk





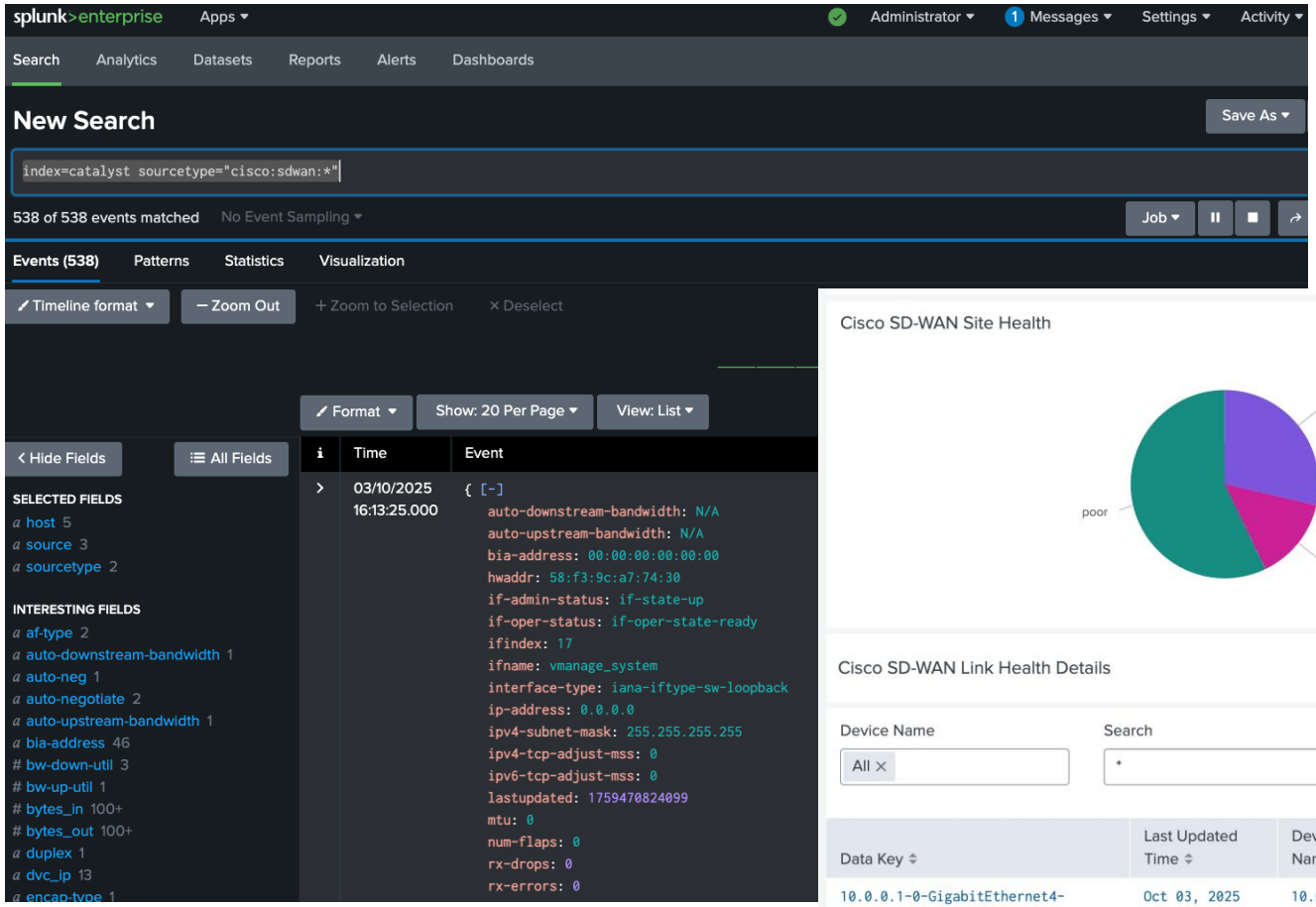
Syslog

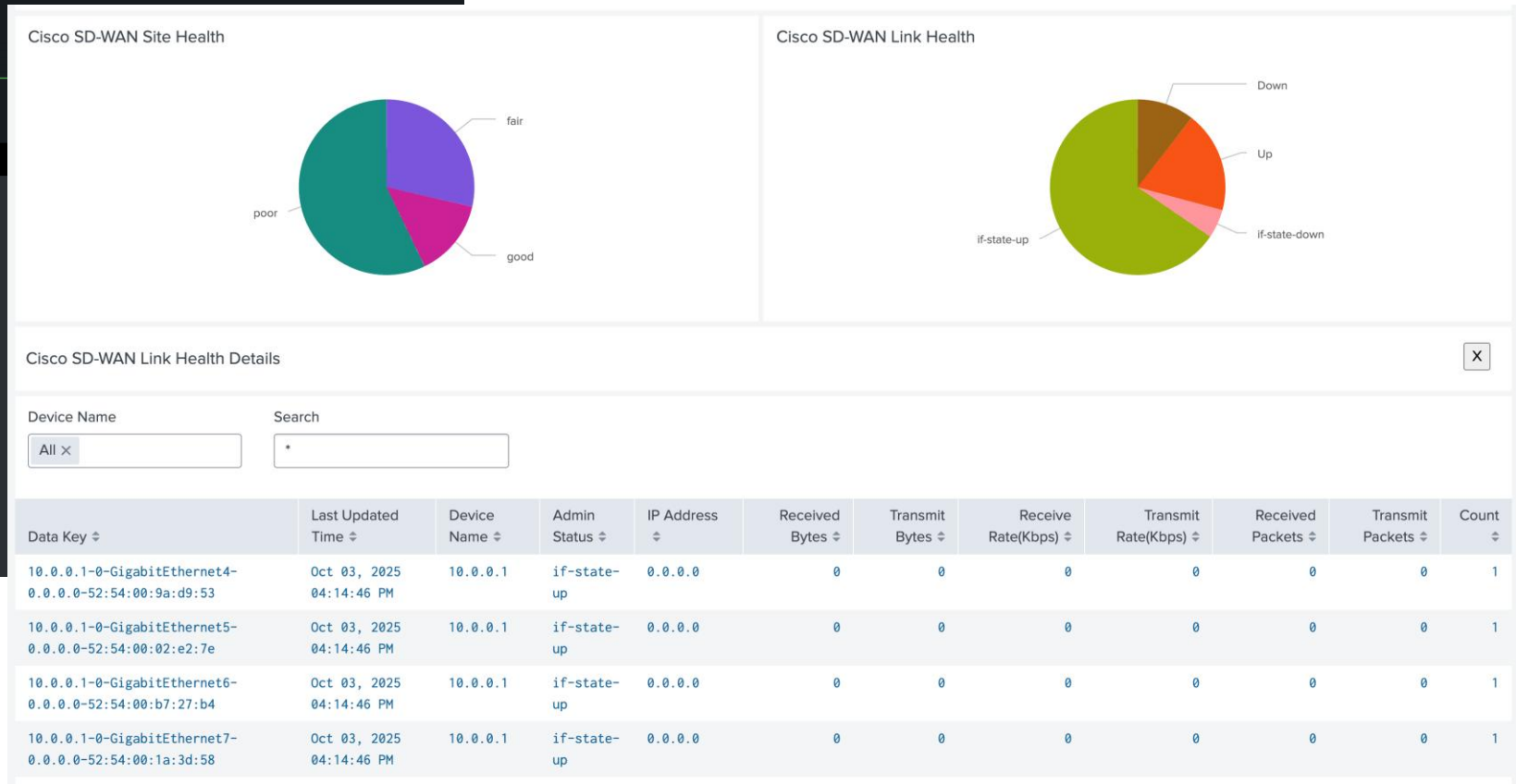
- CLI-Add-on profile specifying custom syslog for Splunk

NetFlow

- Add Cflowd collector address as Splunk

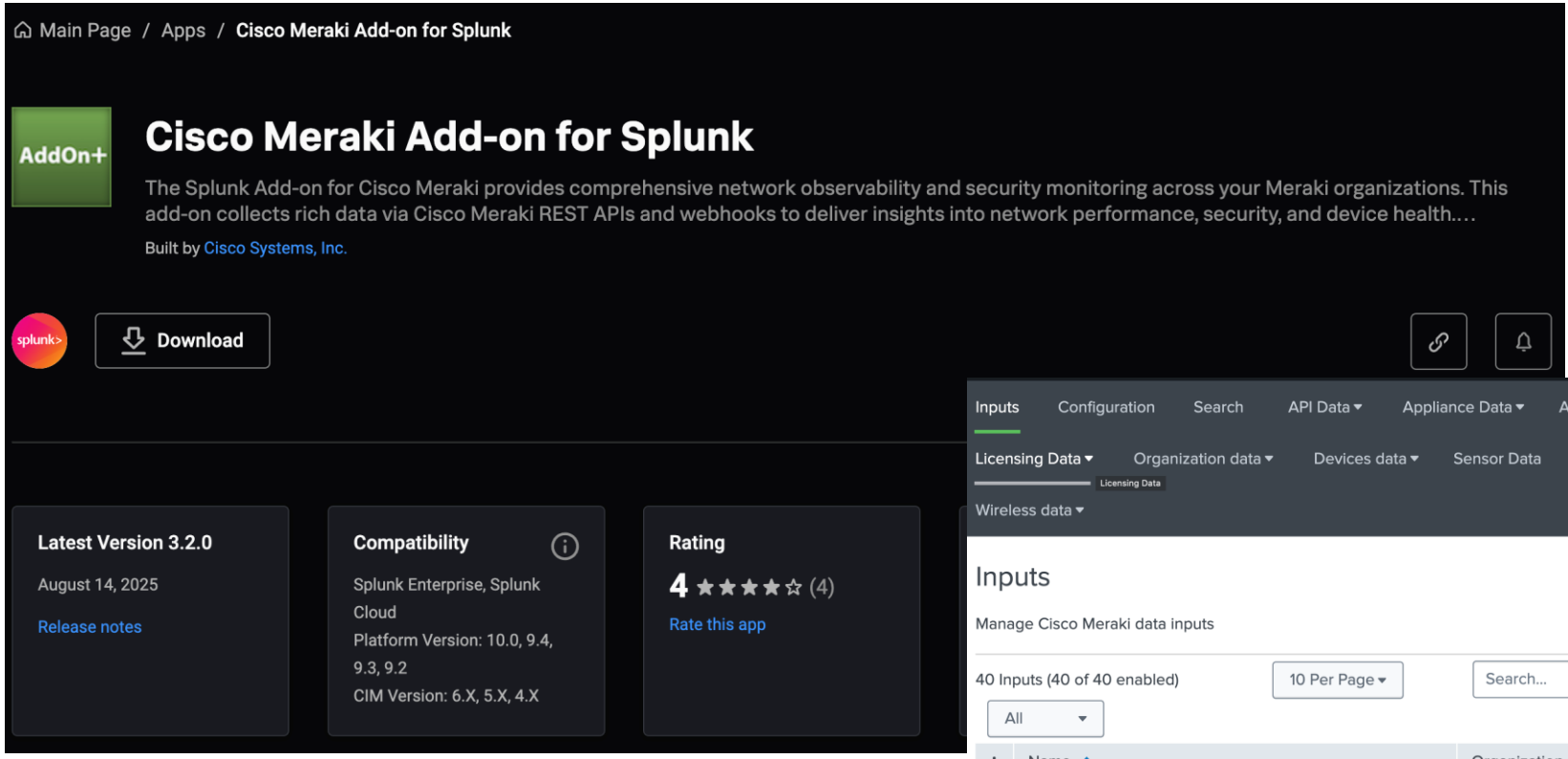
Enterprise Networking App – SD-WAN Dashboards

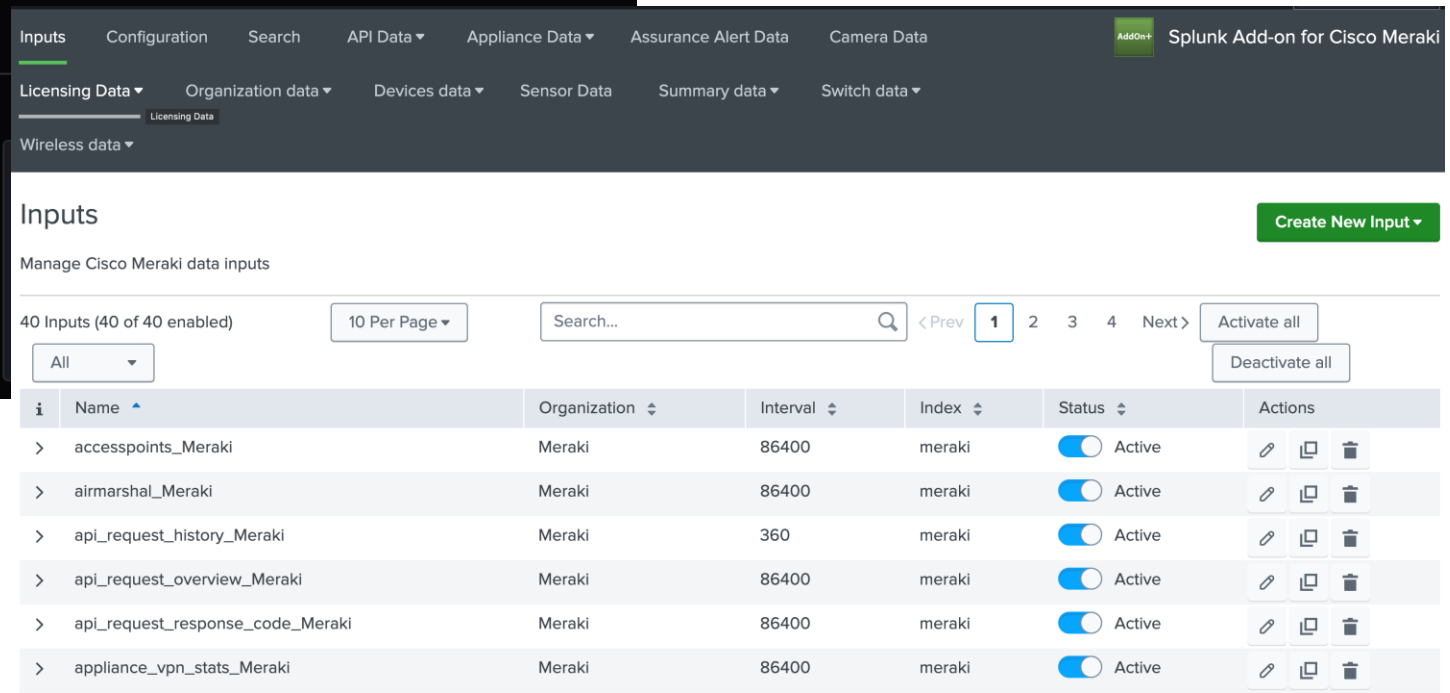




Meraki Add-On

Meraki Add-On for Splunk

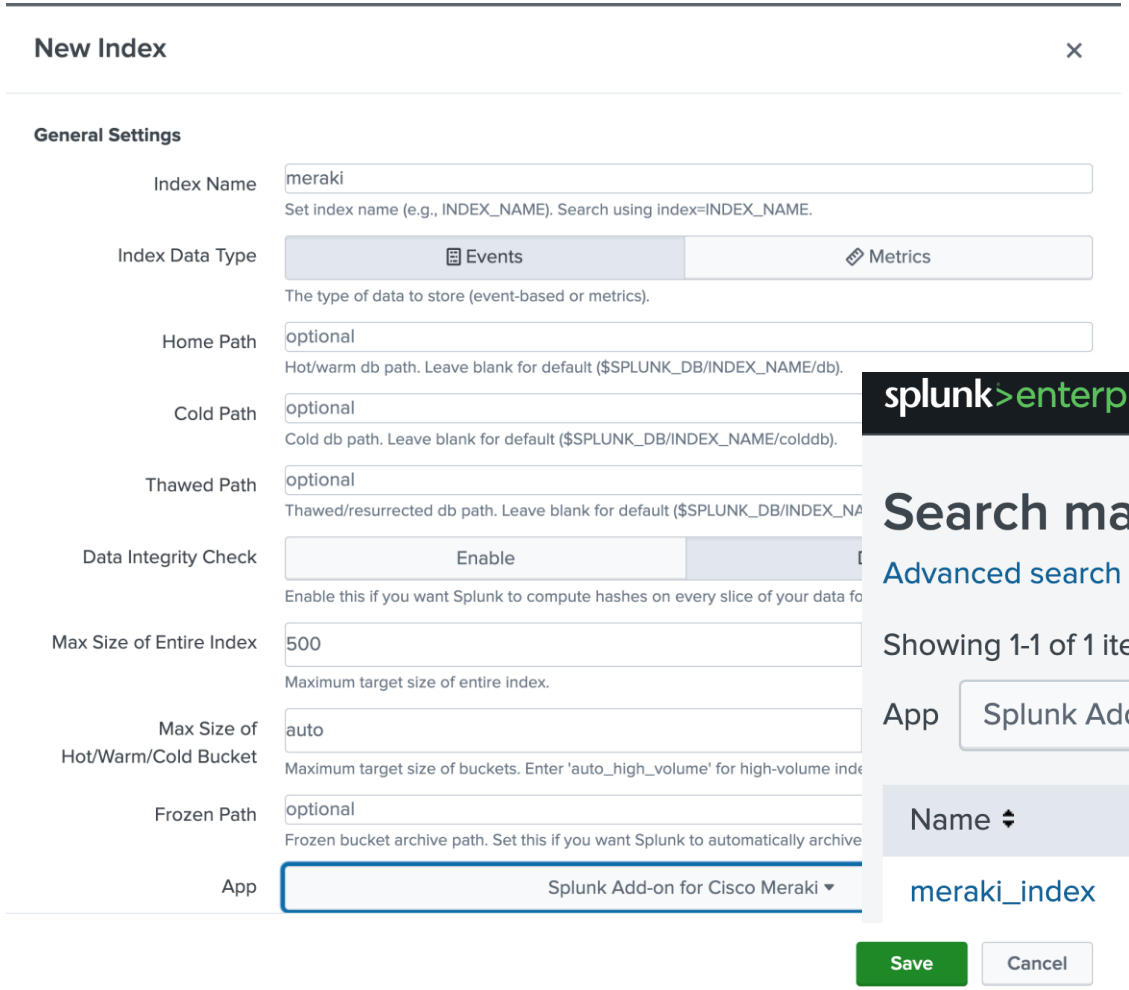




https://splunkbase.splunk.com/app/5580

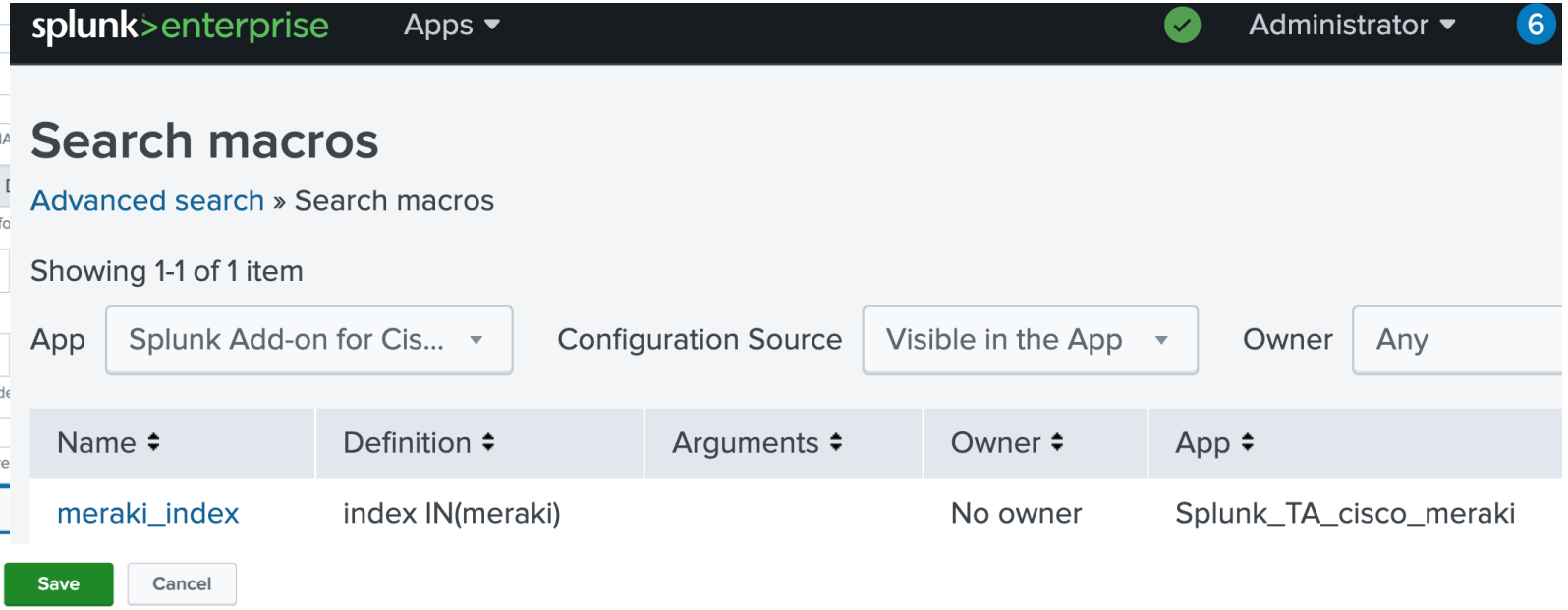
Meraki Add-On for Splunk – Indexes and Search Macro

Add dedicated Maraki index



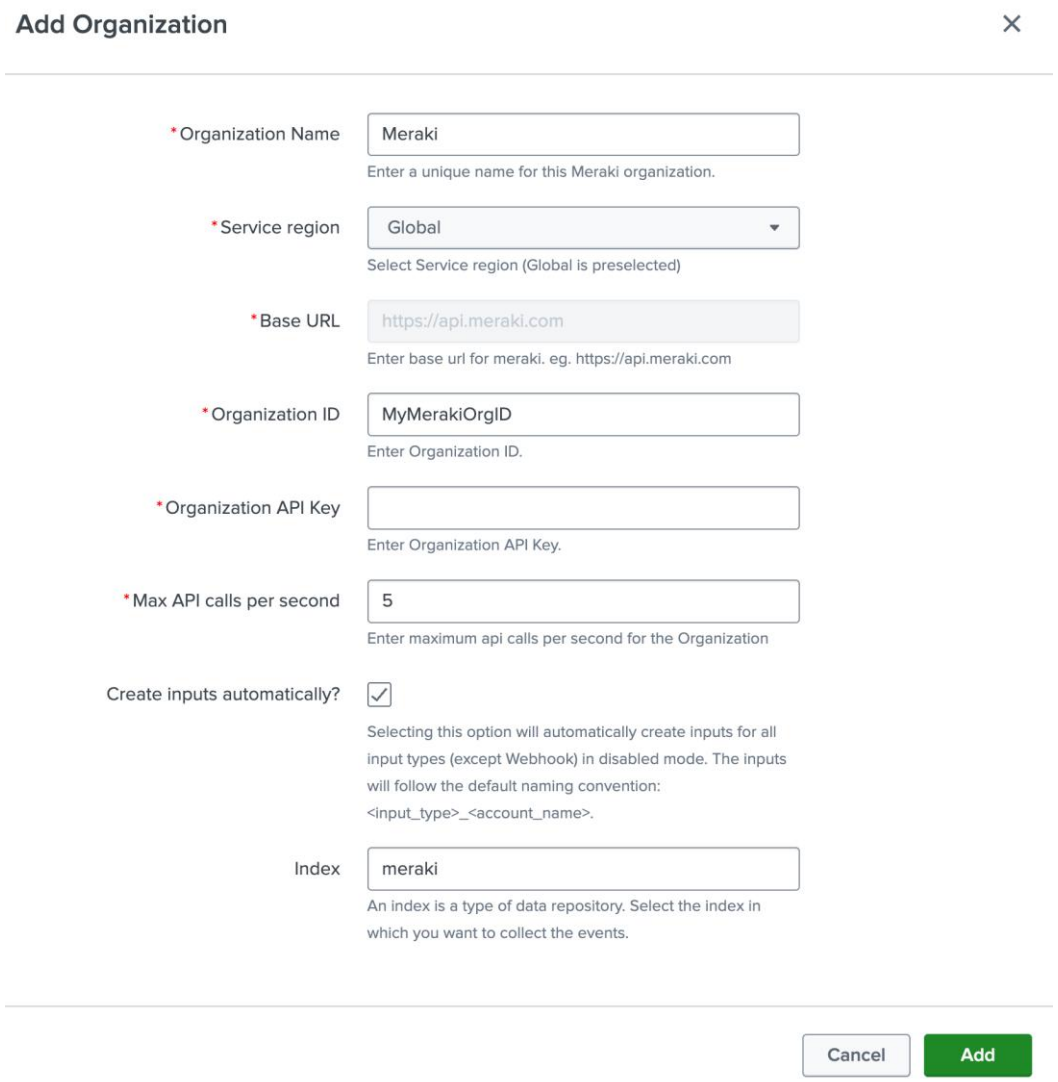
Step 1 – Create Meraki index

Step 2 – Adjust the search macro to use the new index



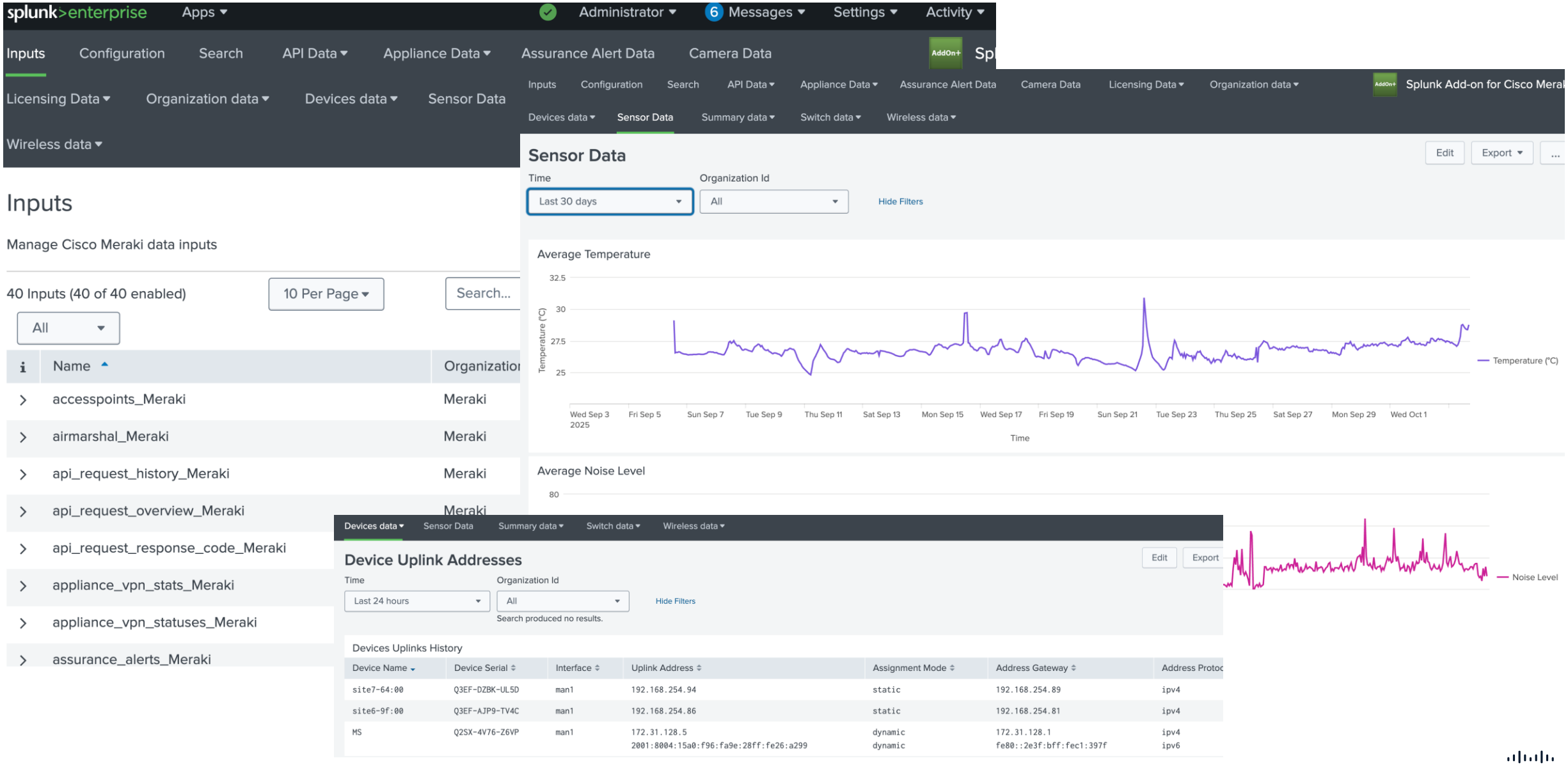
Meraki Add-On for Splunk – Add Organization

Add Meraki credential information

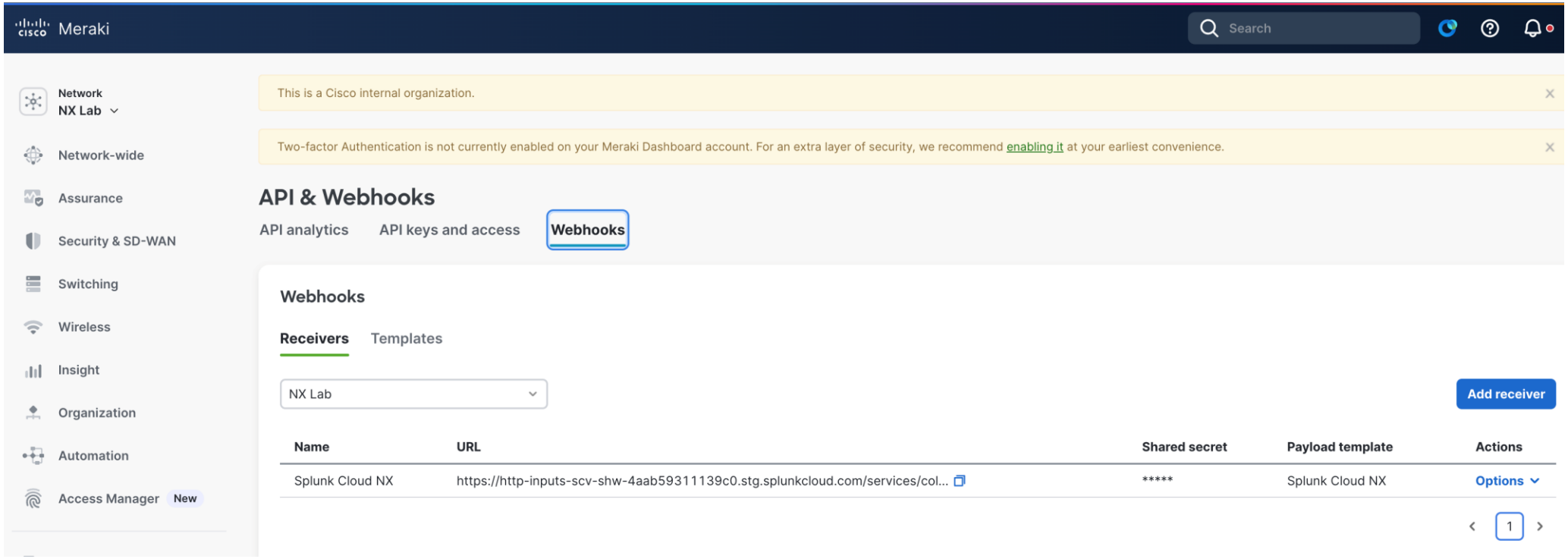


Step 3 – Add Meraki Organization ID and API key

Meraki Add-On for Splunk – Add Inputs



Meraki Add-On for Splunk – Webhooks

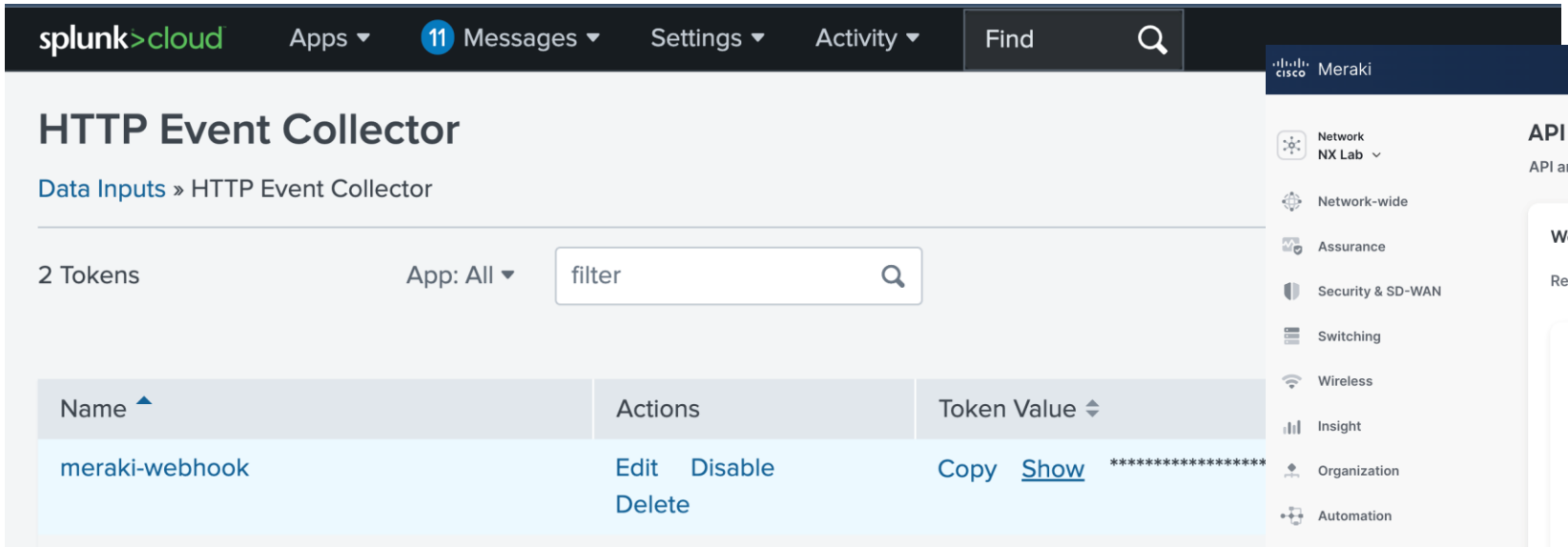


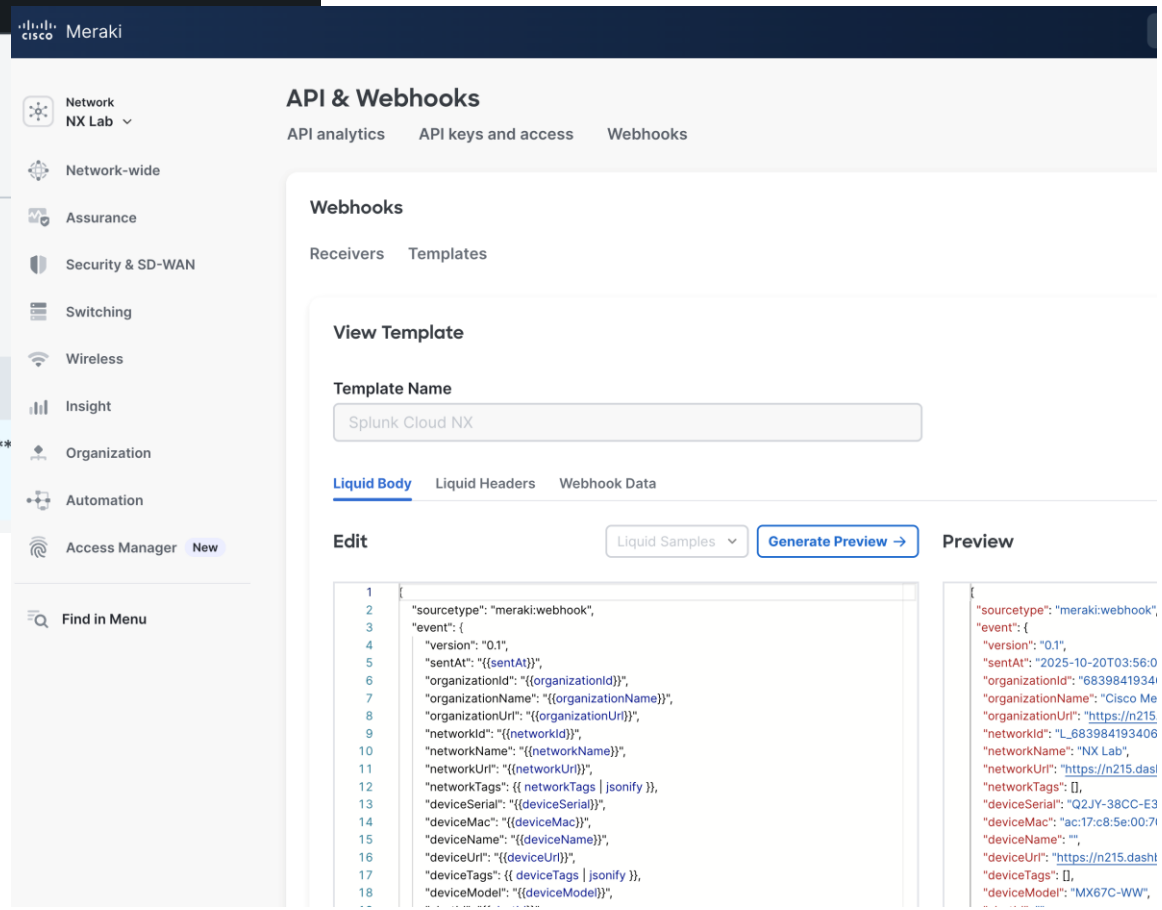
Webhooks

- Subscribe to network alerts from Meraki Dashboard and send directly to Splunk for indexing
- Allows for real-time monitoring
- Format is in JSON format

Meraki Add-On for Splunk – Webhooks

Create Splunk HEC and Meraki liquid body webhook template





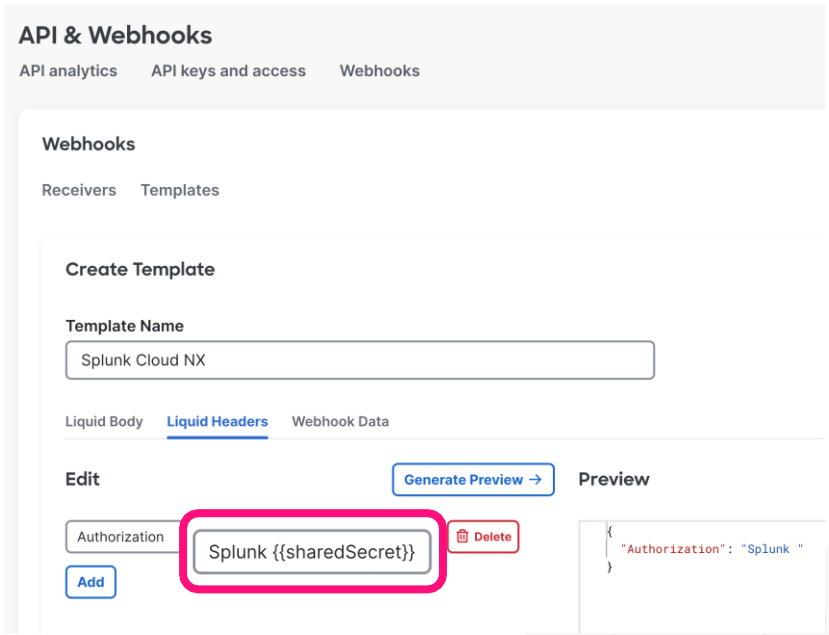
Step 1 – HTTP Event Collector for Meraki webhooks

Step 2 – Create a Meraki liquid body template that is used to format the alert sent to Splunk

https://github.com/meraki/webhook-payload-templates/tree/main/splunk

Meraki Add-On for Splunk – Webhooks

Create a liquid header webhook template



Step 3 – Create a liquid header template

- The Header Value must contain the text **Splunk {{sharedSecret}}**

Step 4 – Add the webhook receiver

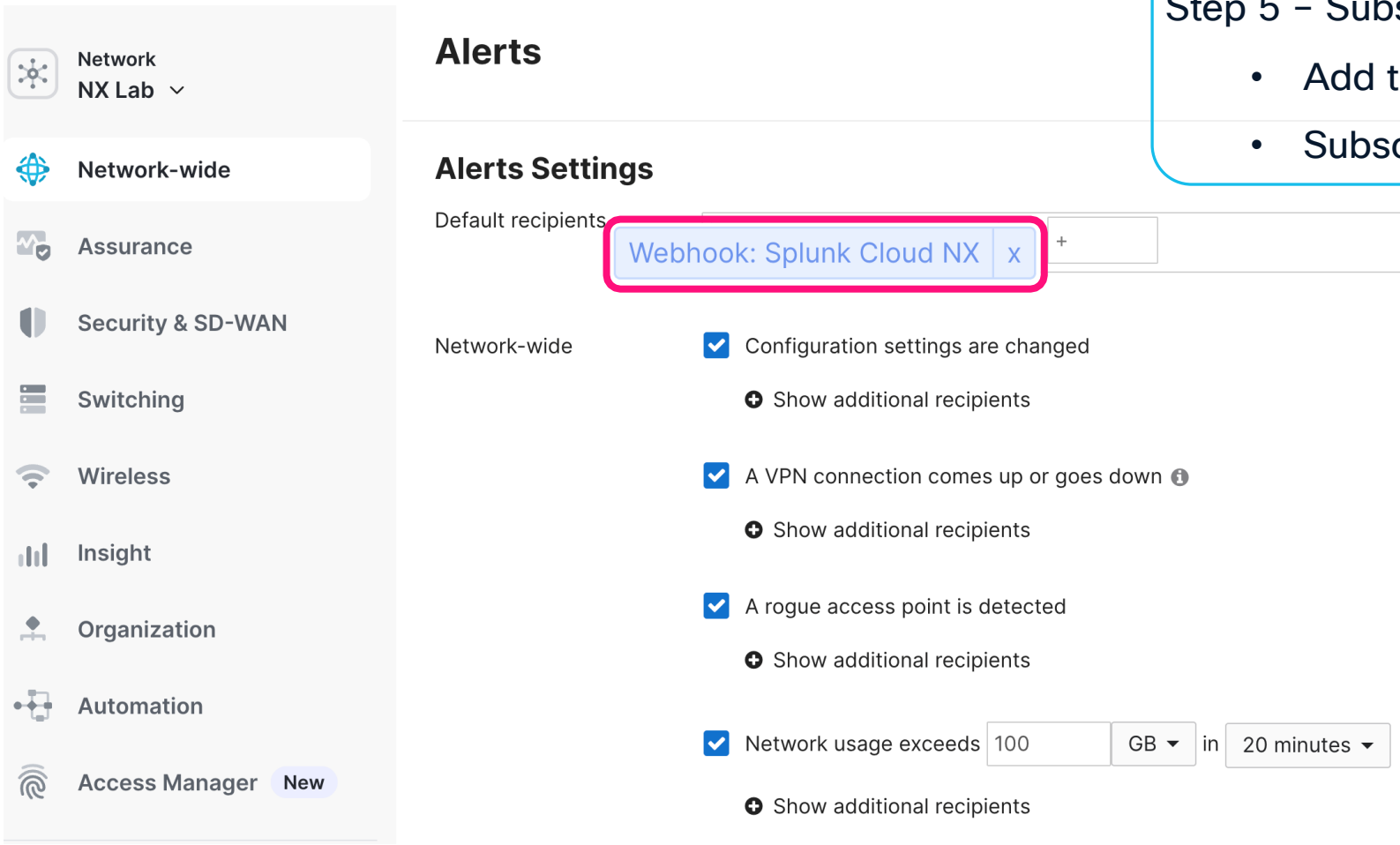
- Specify the Splunk **HEC token** as the shared secret
- Splunk Cloud **URL** – https://http-inputs.<splunkcloudinstance>/services/collector/event

Meraki Add-On for Splunk – Webhooks

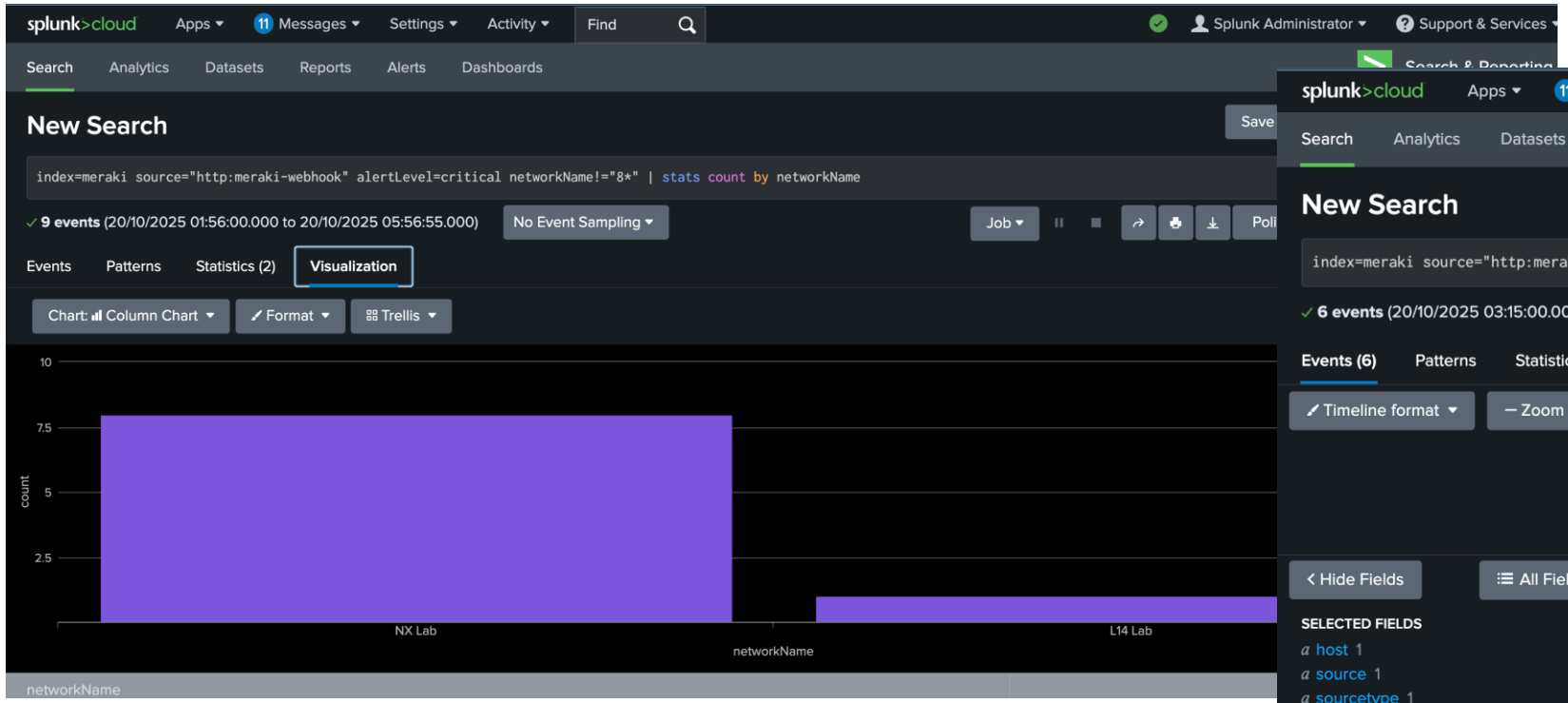
Create a liquid header webhook template

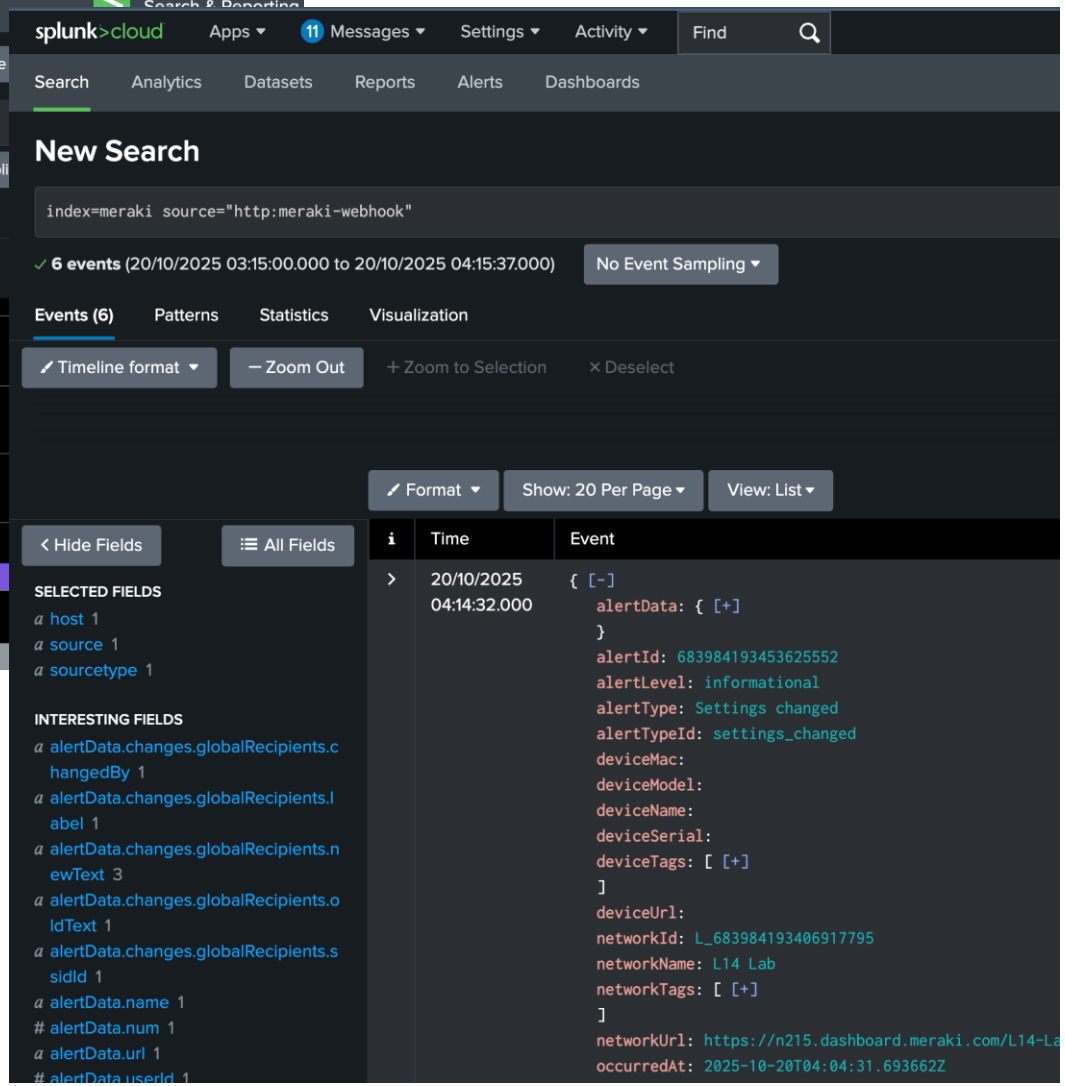
Step 5 – Subscribe to Network-wide Alerts

- Add the recipient as the webhook for the alert
- Subscribe to alerts



Meraki Webhook Searching



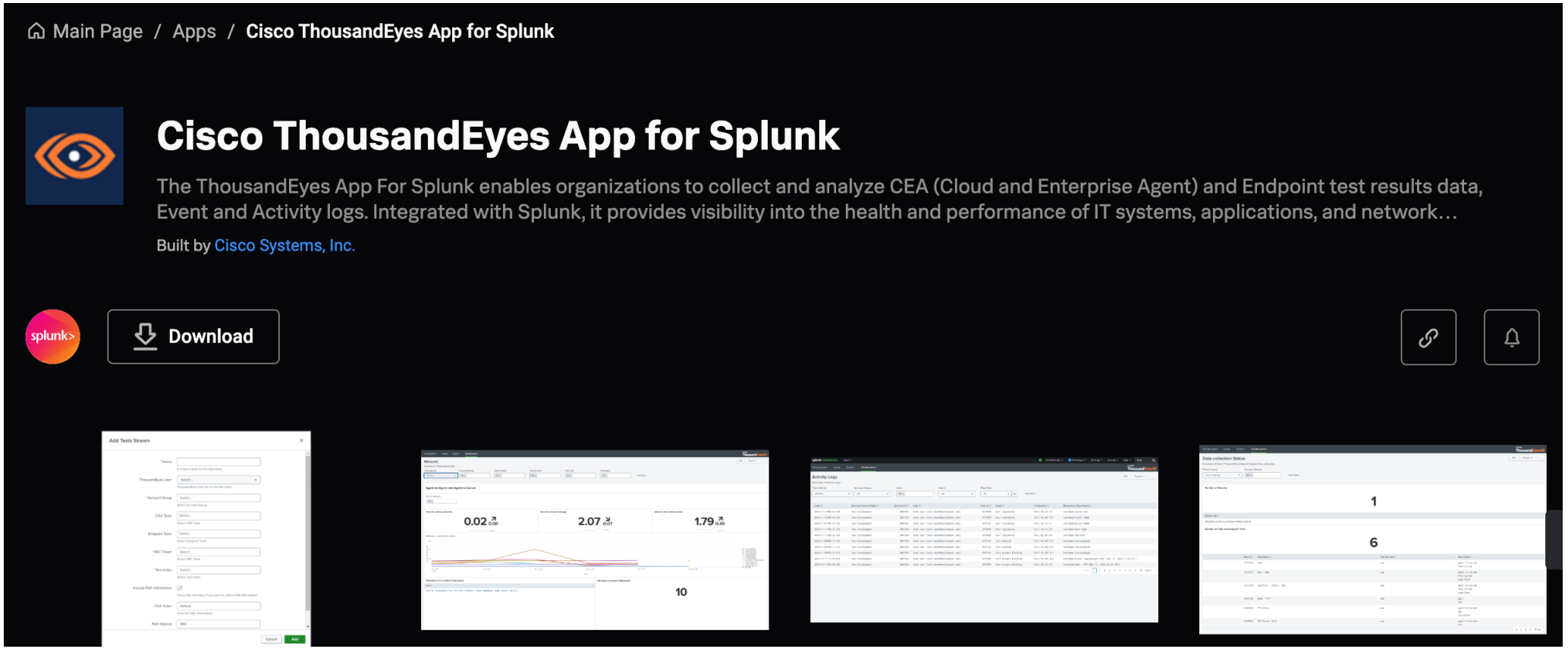



```
index=meraki source="http:meraki-webhook"
```

ThousandEyes Add-On

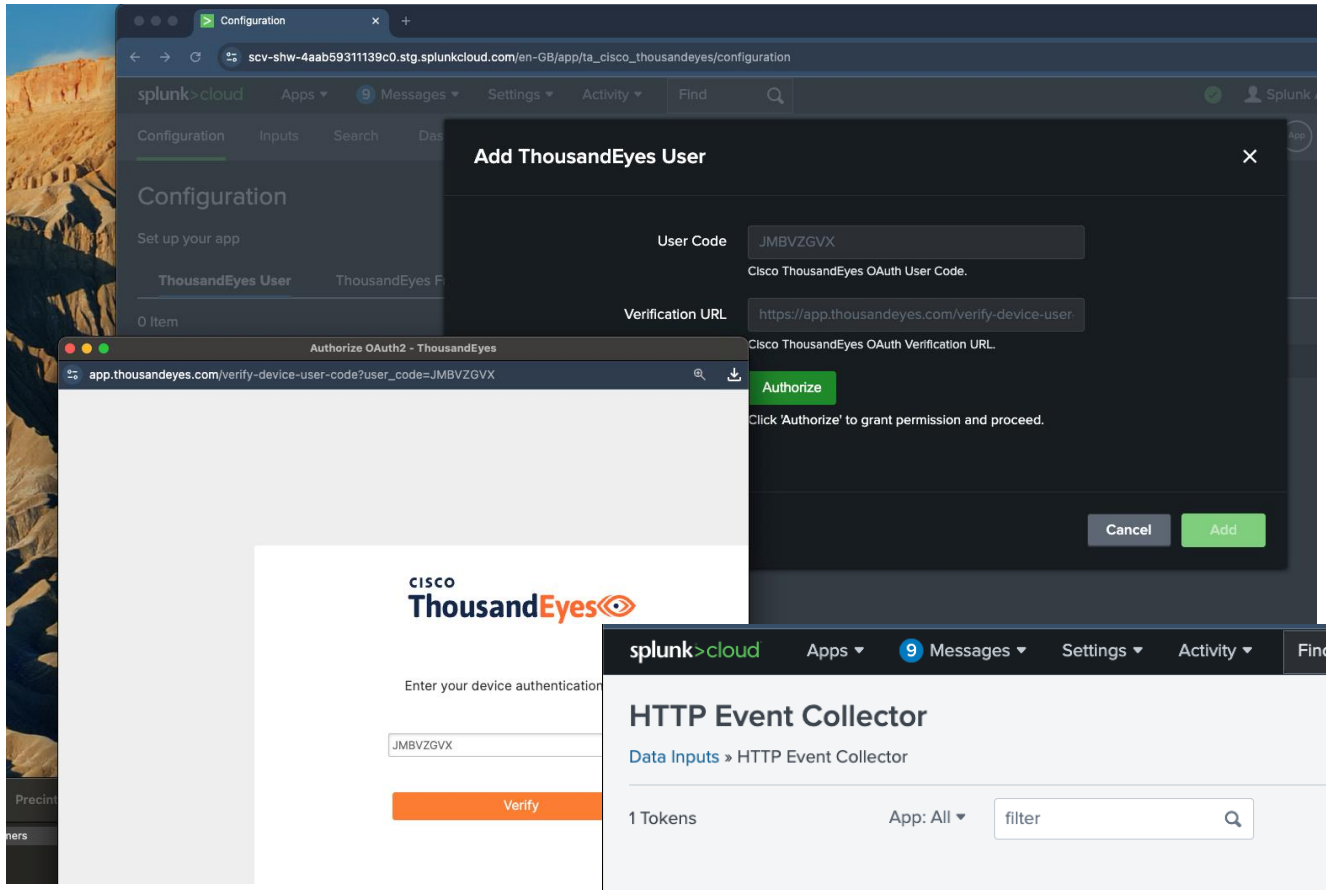
ThousandEyes Add-On for Splunk

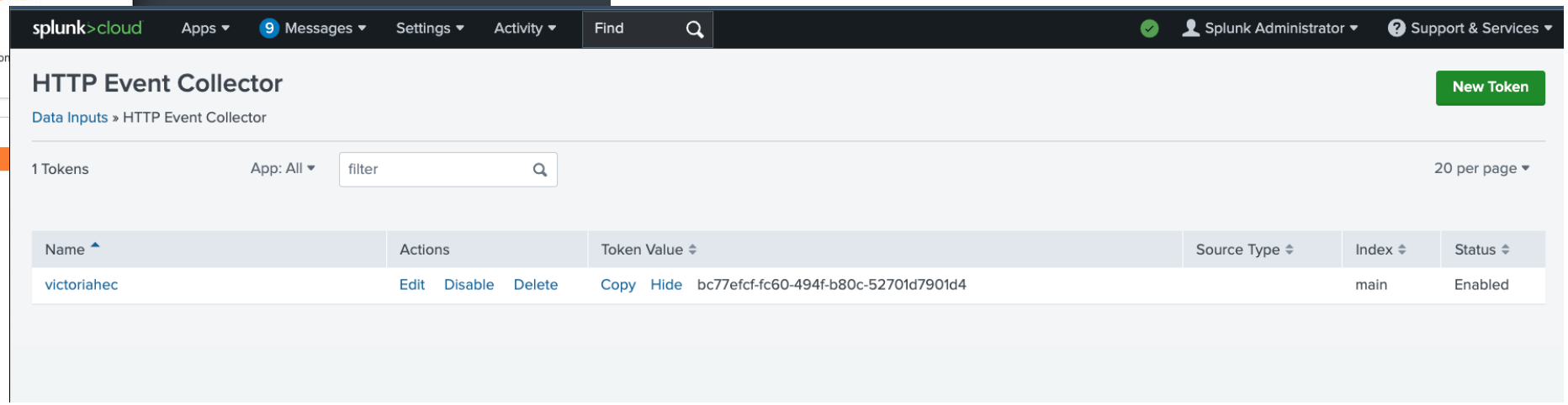
Parses the data from specified sources and stores them into the Splunk indexes



https://splunkbase.splunk.com/app/7719

Add ThousandEyes Account

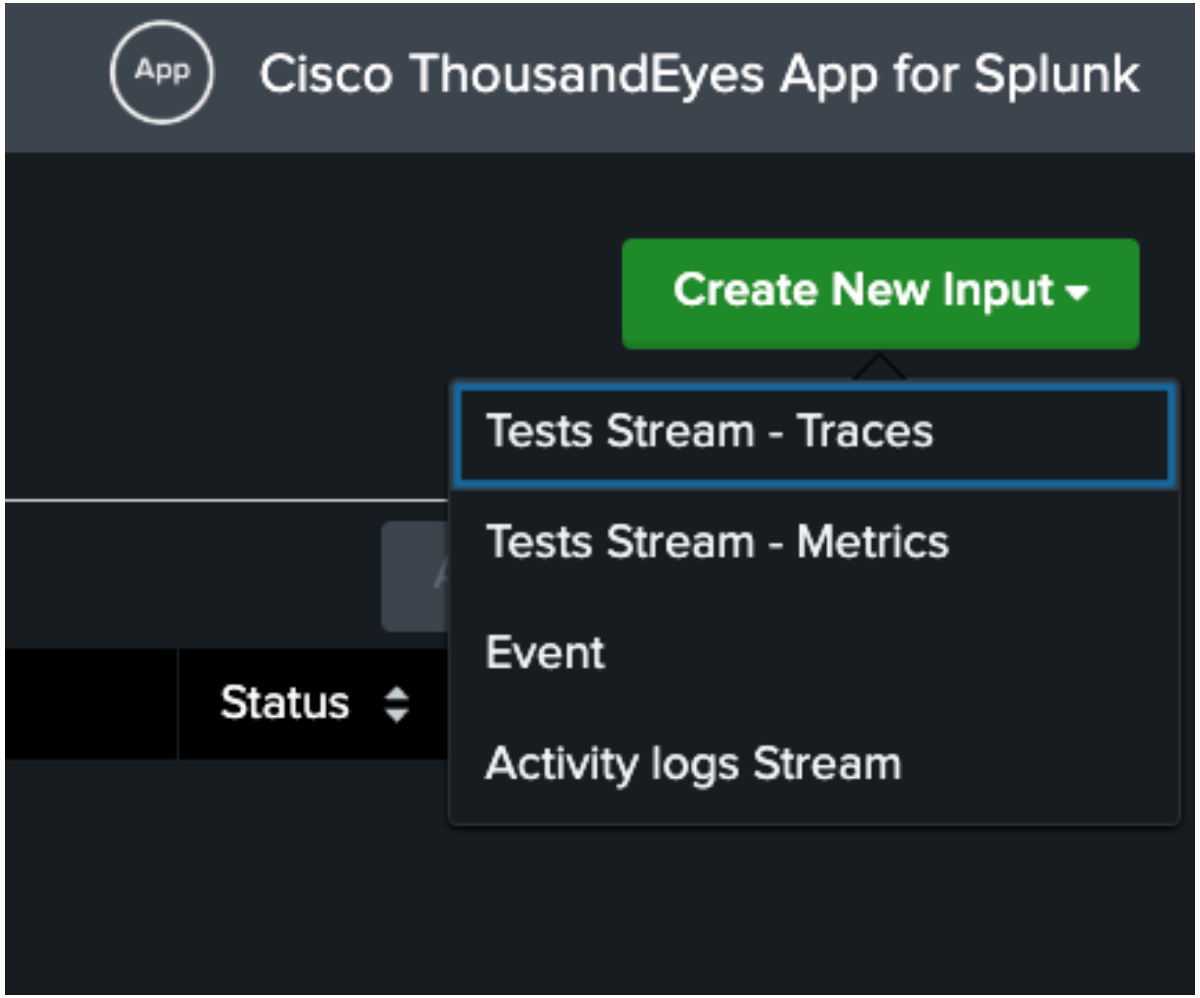




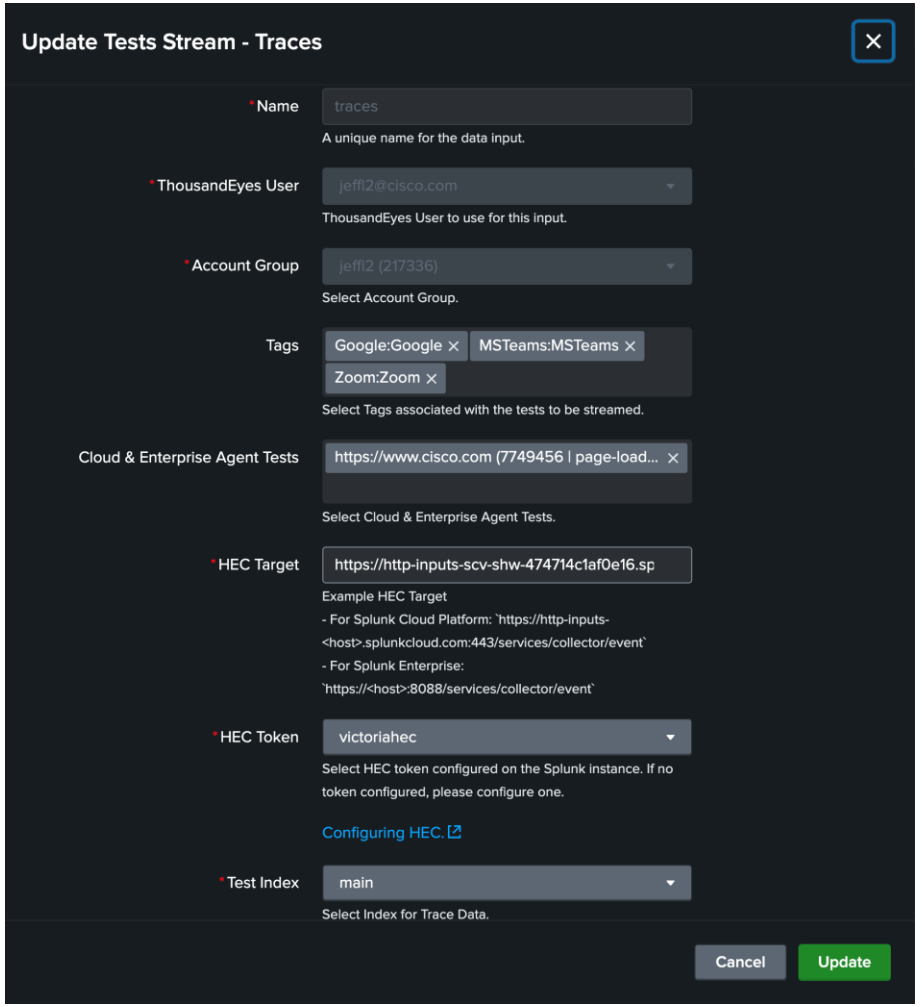
Step 1 – Add ThousandEyes User

Step 2 – Add HTTP Event Collector for ThousandEyes in Splunk

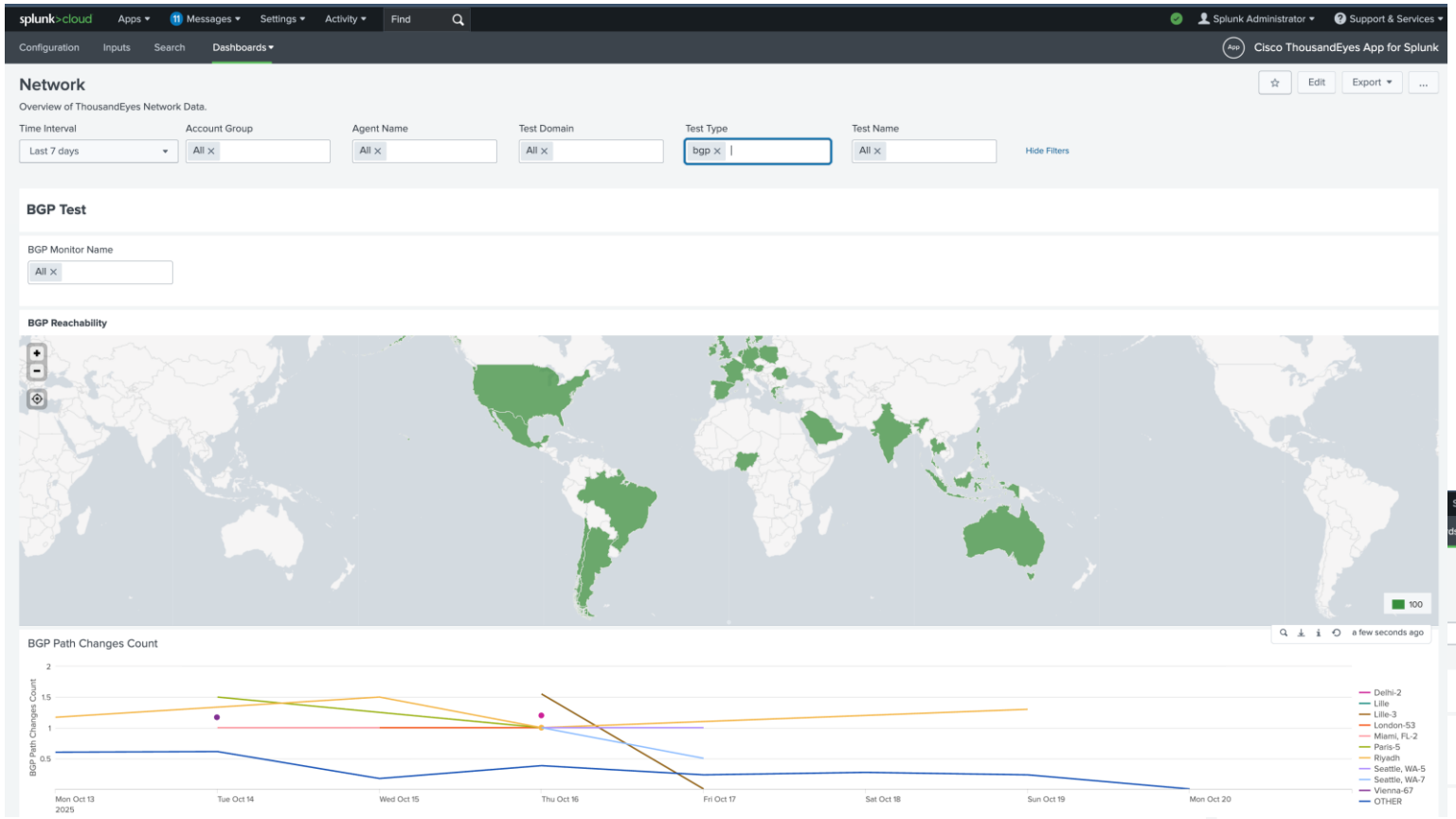
ThousandEyes Add-On for Splunk – Add Inputs

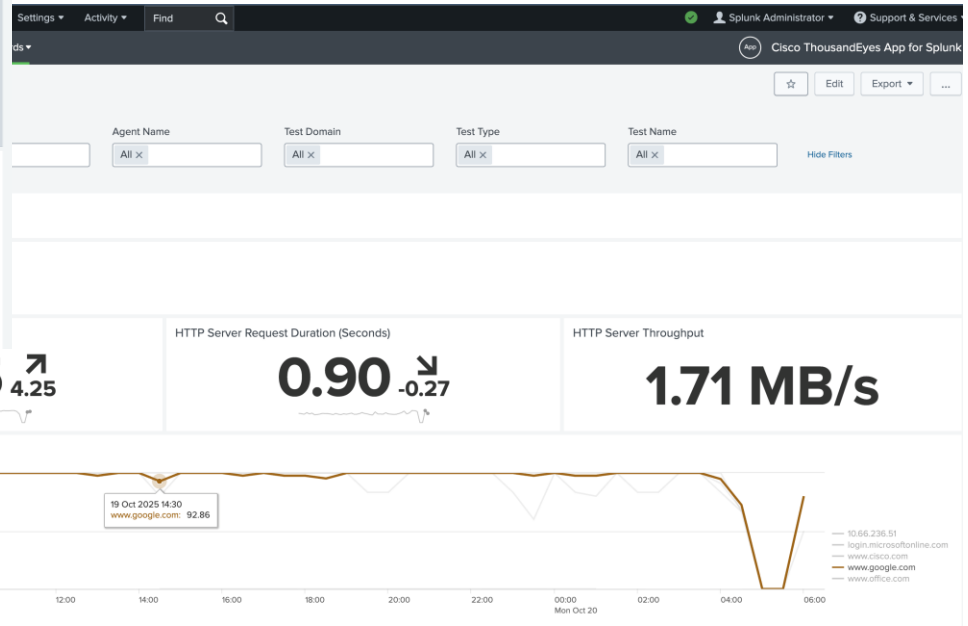


Step 3 – Add ThousandEyes Inputs and select tests

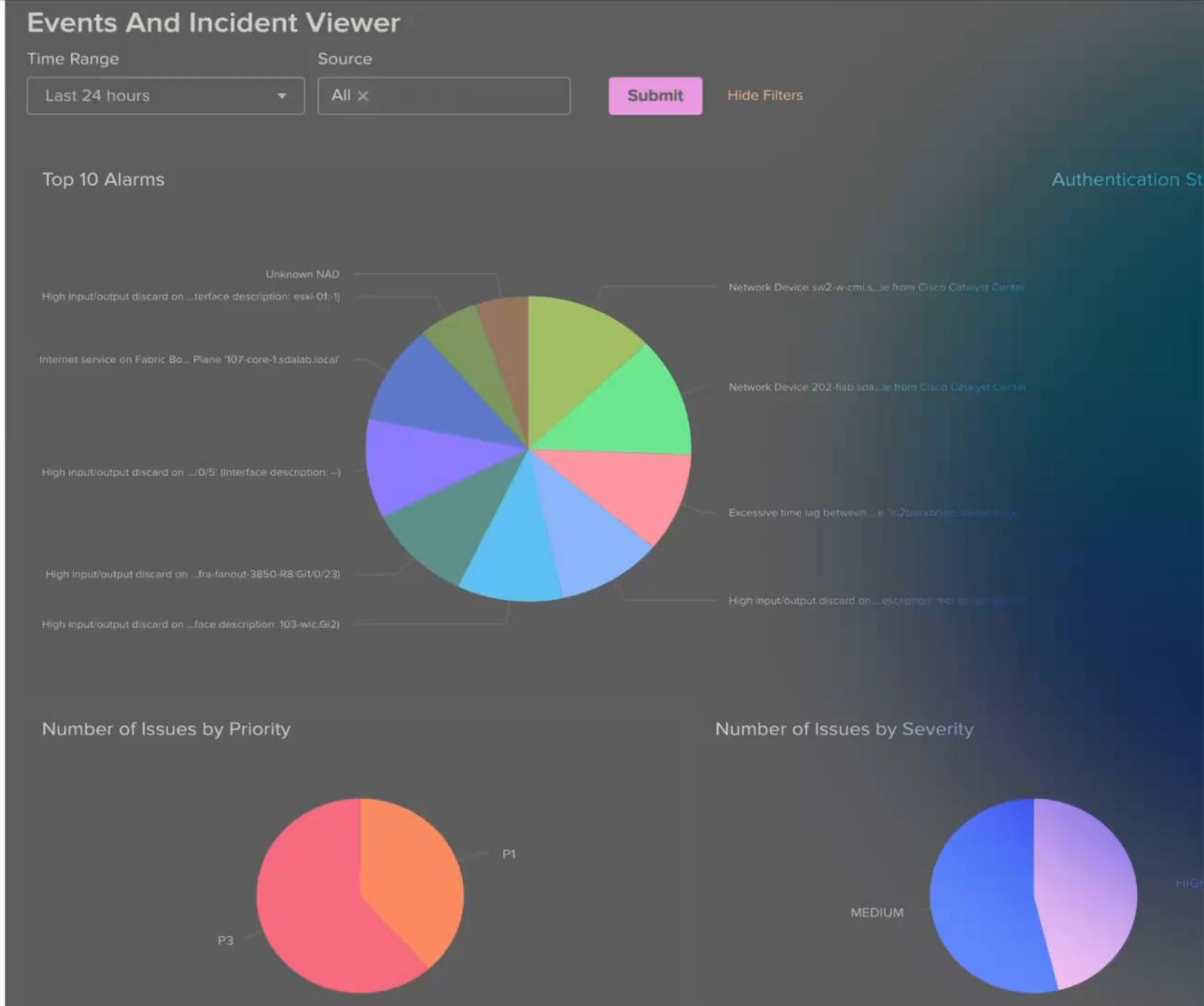


ThousandEyes Add-On for Splunk – Dashboards





Demo – Splunk Enterprise Networking



Splunk IT Service Intelligence (ITSI)

Introduce Intelligence with Splunk ITSI

Complete Business Visibility

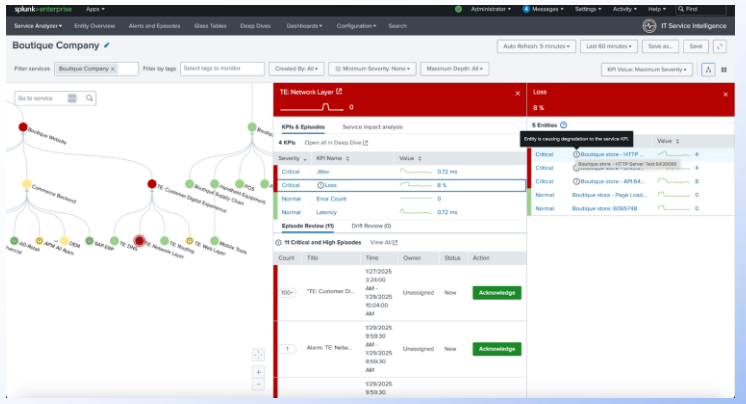
Eliminate fragmented visibility with a single view and accelerate RCA

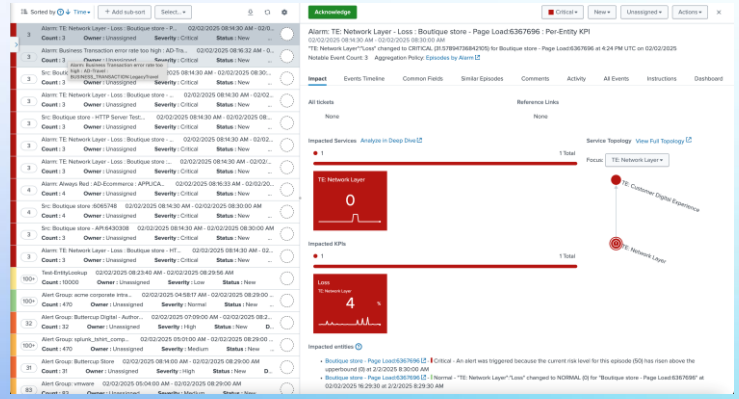
Intelligent Incident Management

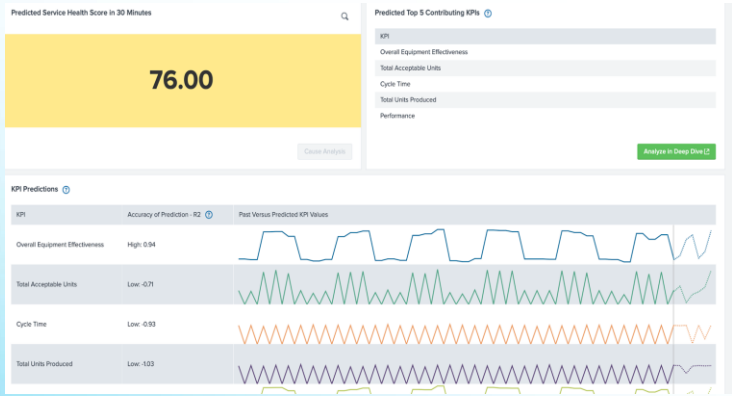
Accelerate MTTR using real-time event correlation and automated prioritization

Proactive Incident Prevention

Detect anomalies and predict issues 30 mins earlier for outage prevention



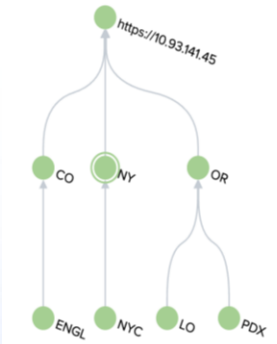


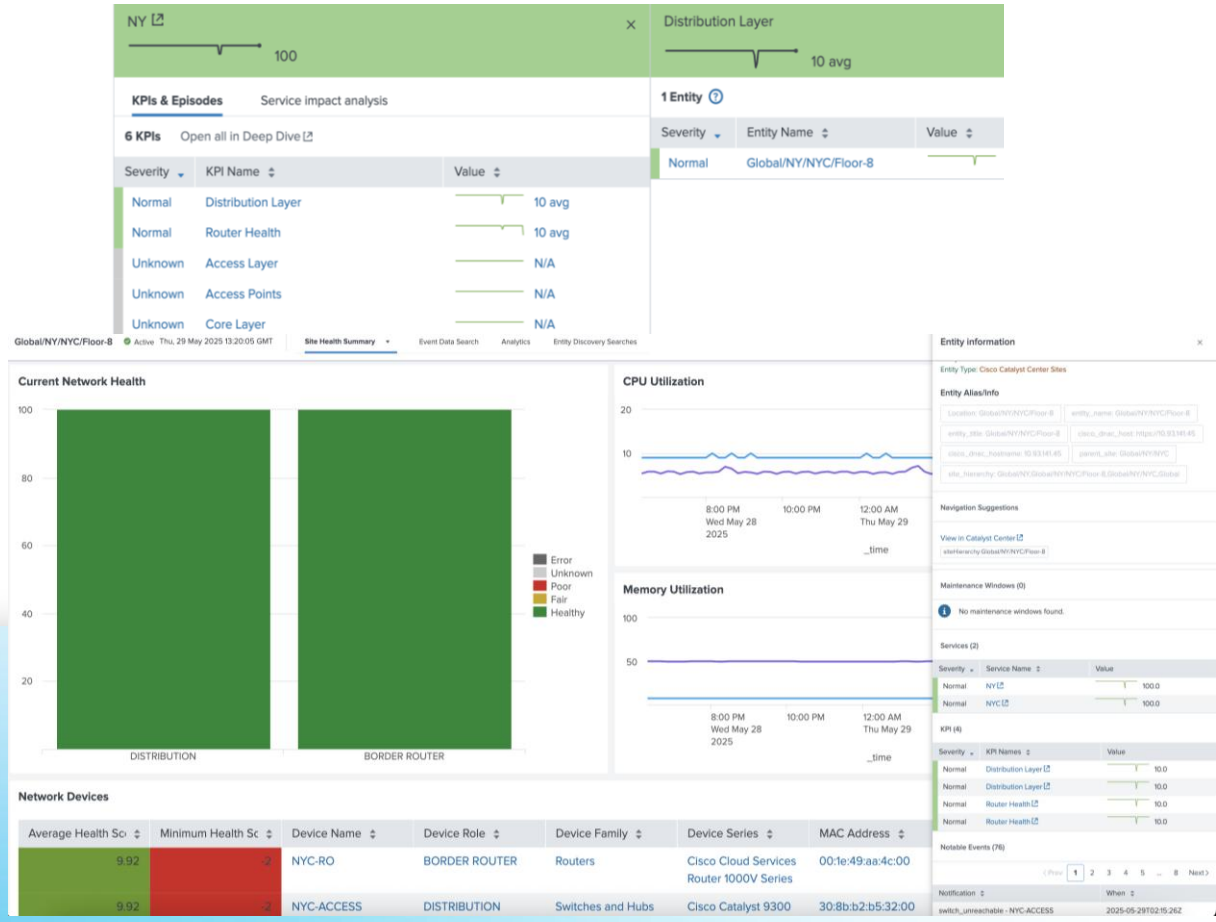


Splunk ITSI and Catalyst Center Integration

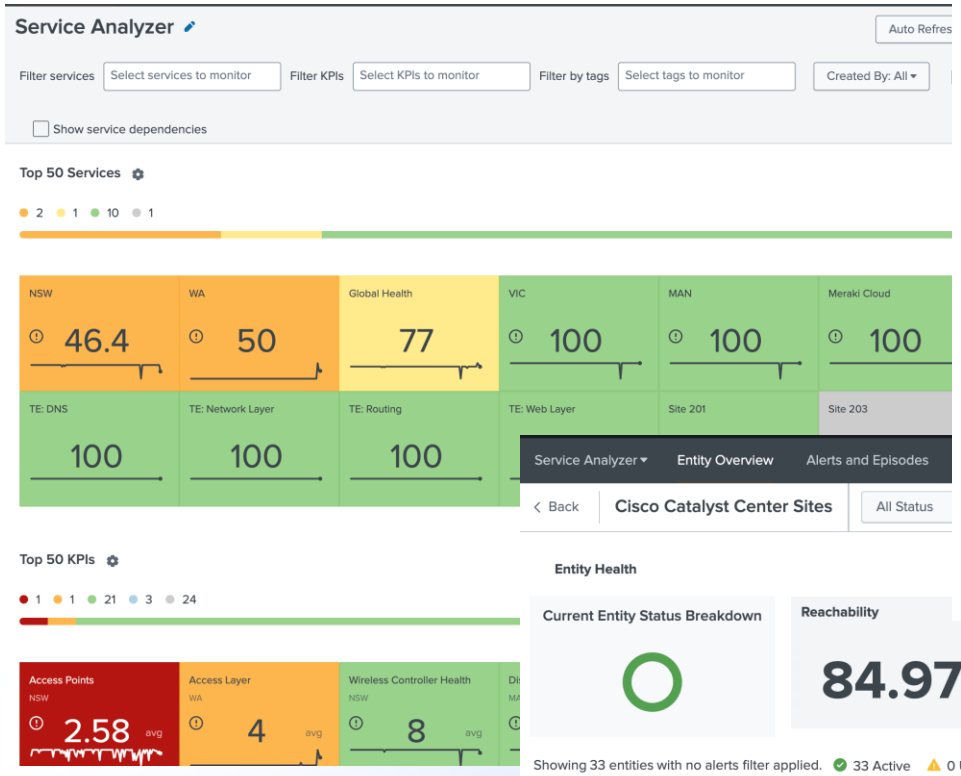
Quickly pinpoint site & device issues in the network with:

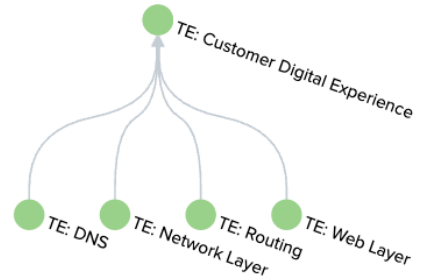
- Site-based dependency mapping for problem isolation
- KPIs and entity models to measure site health incl. core, distribution, and access layers
- Easy alert normalization, deduplication and correlation
- Health visualization of site floors or localized areas to pinpoint unhealthy devices
- In-context drill-downs into Catalyst Center Assurance to perform RCA

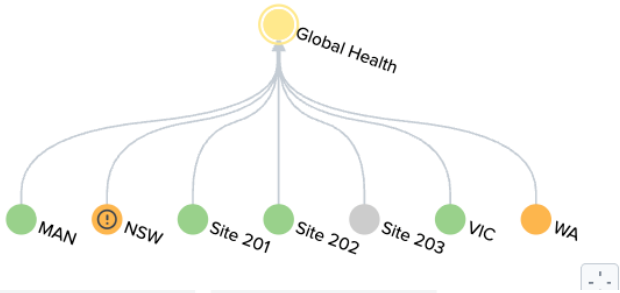


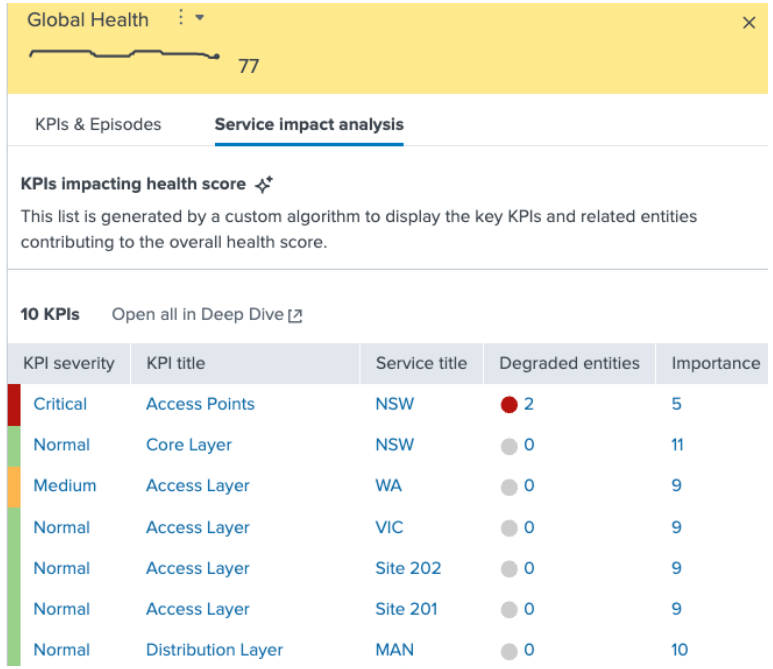


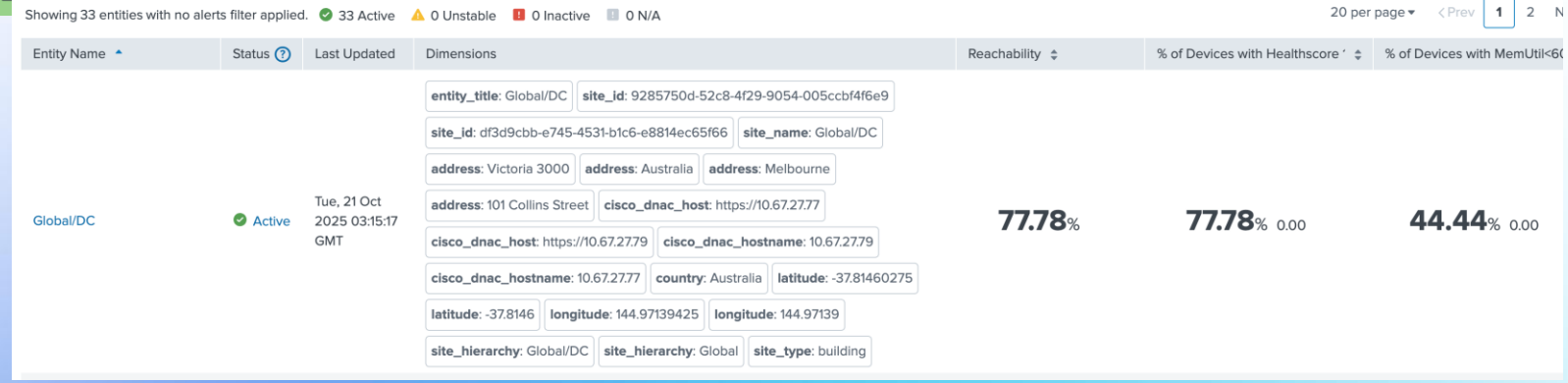
Splunk ITSI Service Analyzer



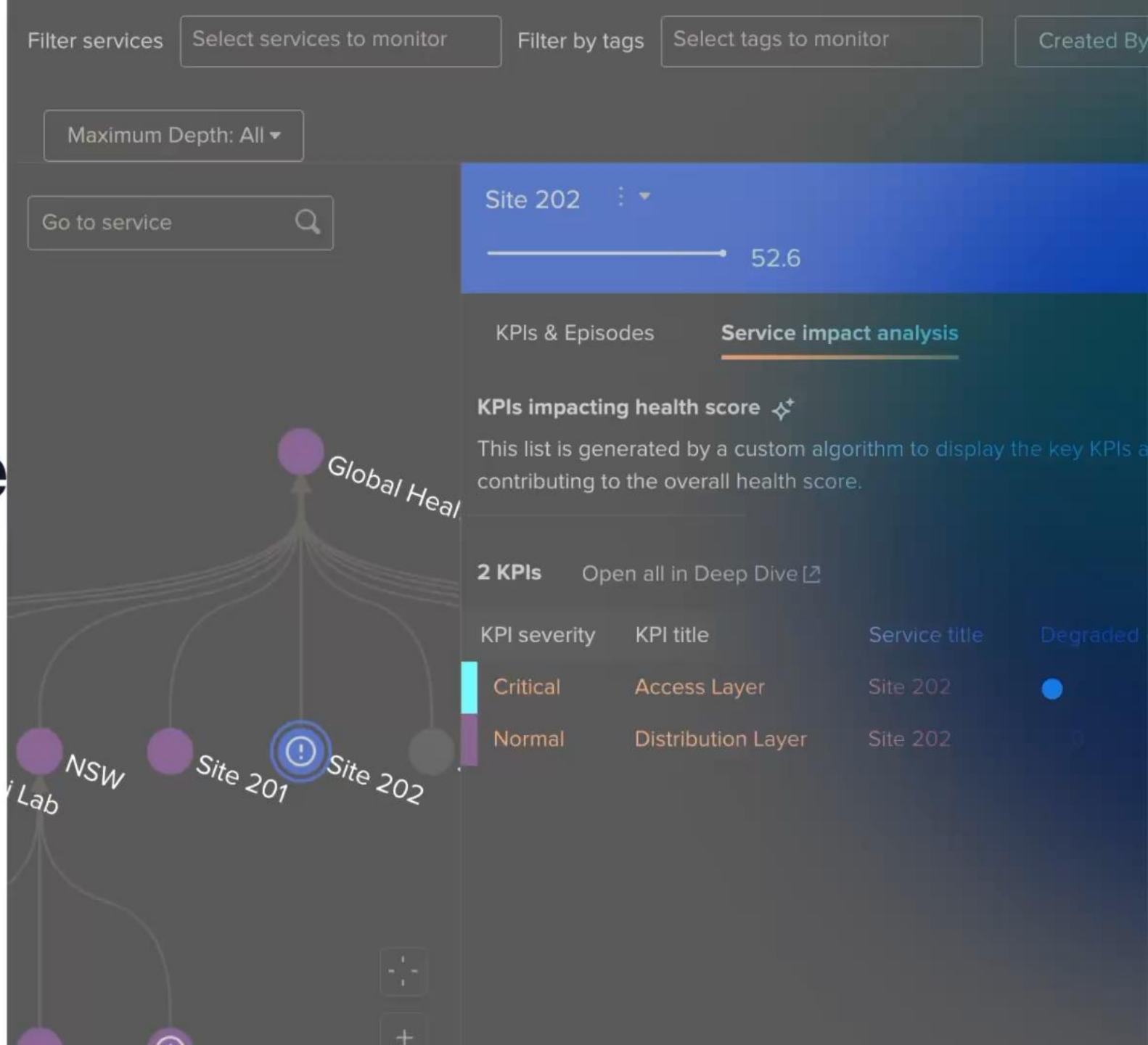








Demo – IT Service Intelligence



Complete your session evaluations

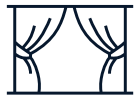
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you


CISCO