

Splunk for Network Engineers

Catalyst, Meraki, ISE, ThousandEyes and ITSI

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

cisco Live !

Cisco Webex App

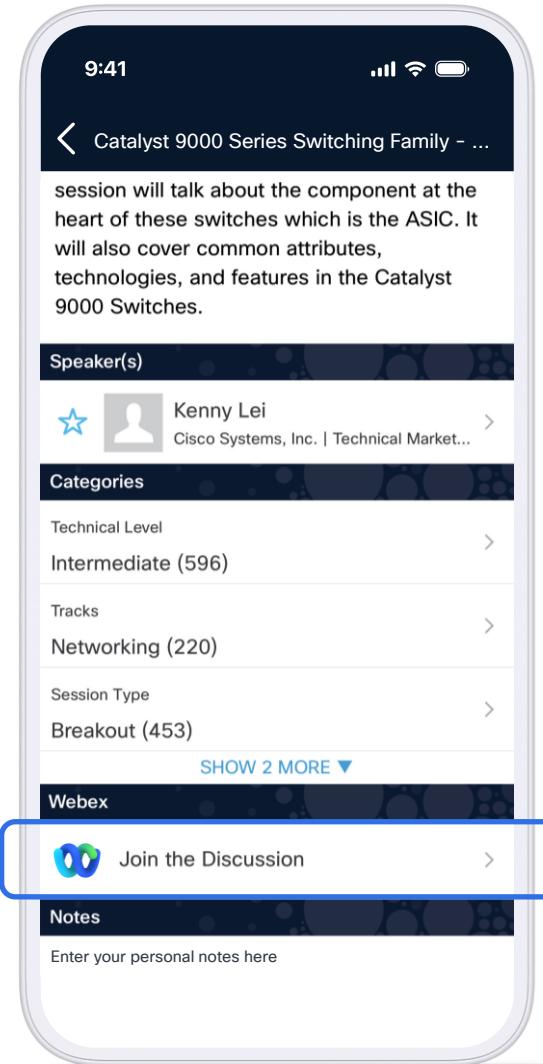
Questions?

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://cislive.ciscoevents.com/>
cislivebot/#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

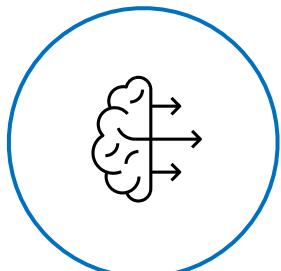
- Network Engineers/Operators
- Generally familiar with Catalyst Center, Identity Services Engine, SD-WAN and Meraki
- Less familiar with Thousand Eyes
- Even less familiar with Splunk
- Probably never heard of ITSI

Why Splunk?



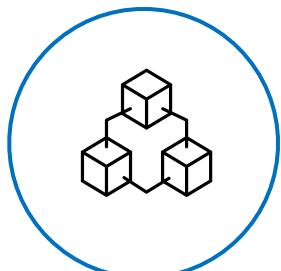
Consolidated Dashboard

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



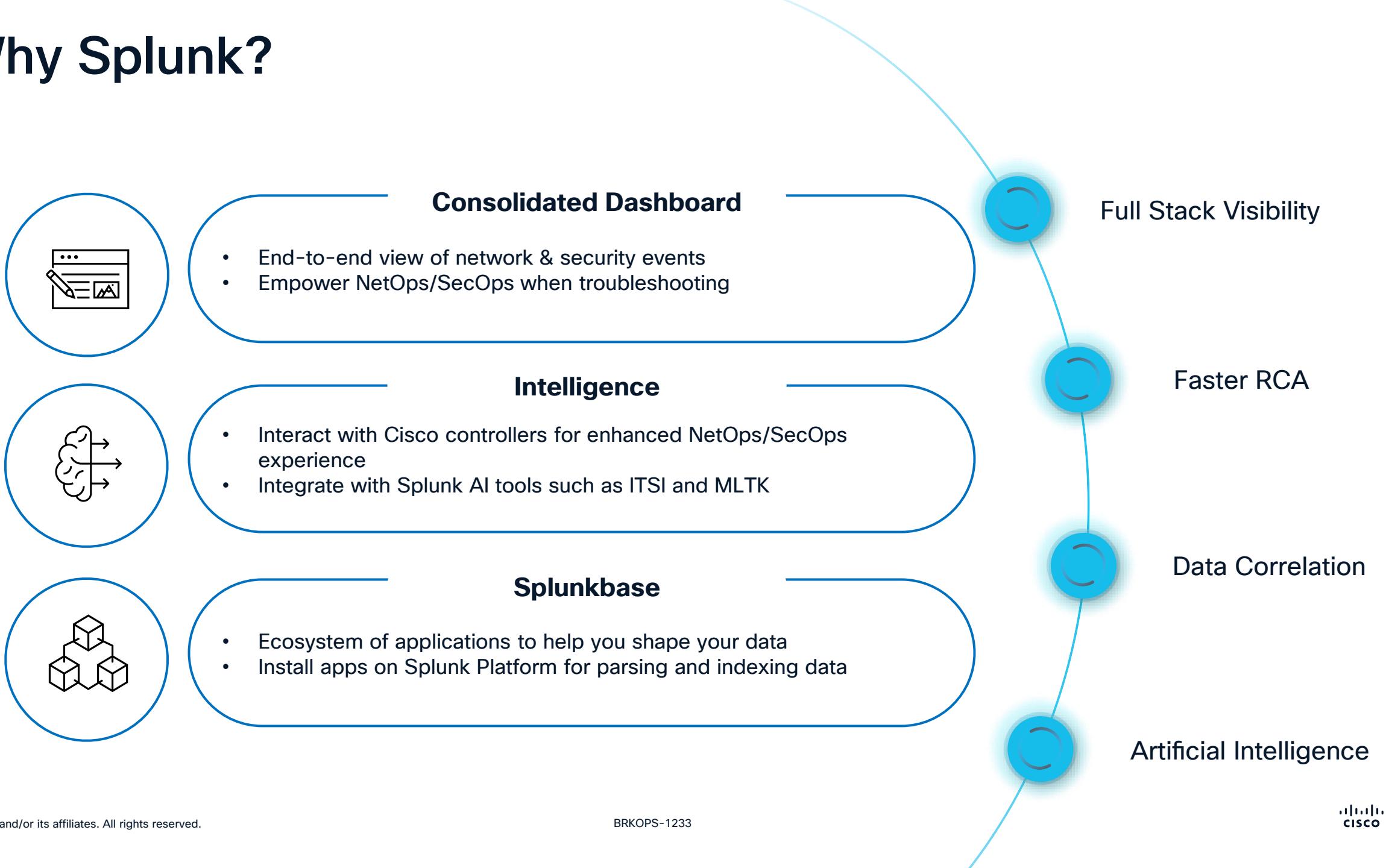
Intelligence

- 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



Getting Data to Splunk

Various Data Structures | Common Repository | Custom Searches

Splunk Platform

Various Data Structures

Custom Searches



Common Data Repository

Cross Domain Correlation

Normalize Metrics, Events, Alerts & Logs Across Multiple Solutions

Data

Data

Data

Data

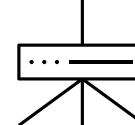
Data



Devices & Users



Wireless



Switching



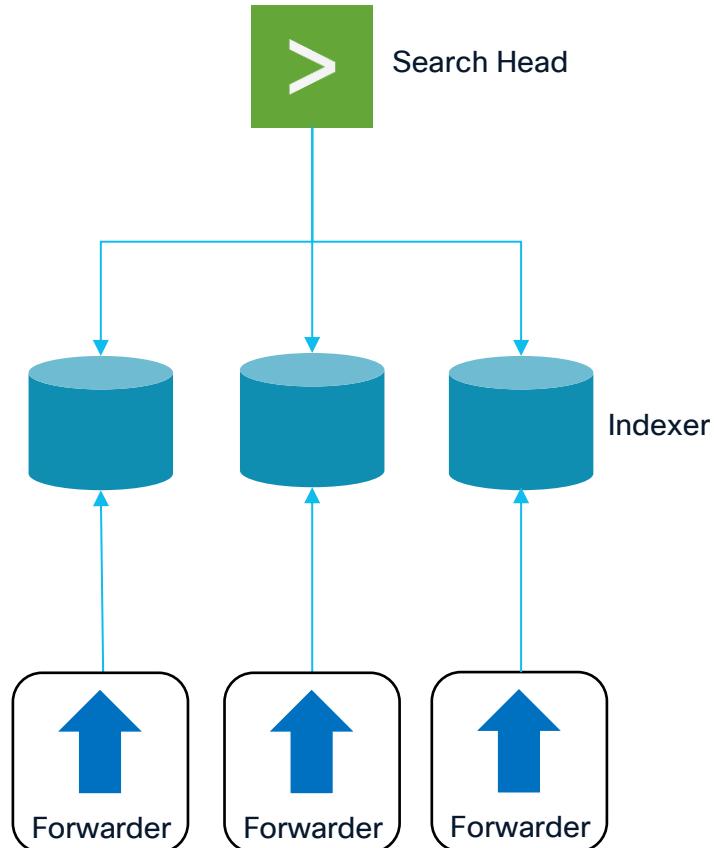
Routing



Security

Get Data In

Splunk - Main Components



Search Head

- Handles search requests and consolidating results back to the user

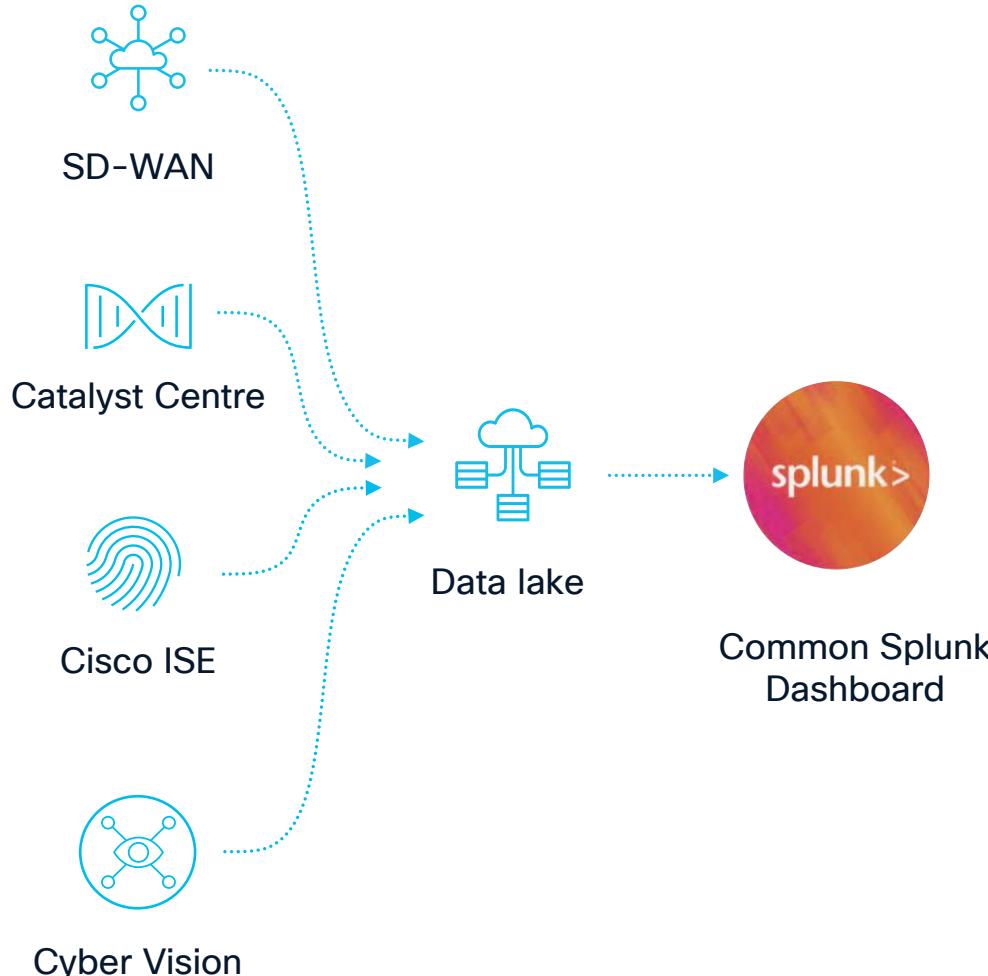
Indexer

- 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



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

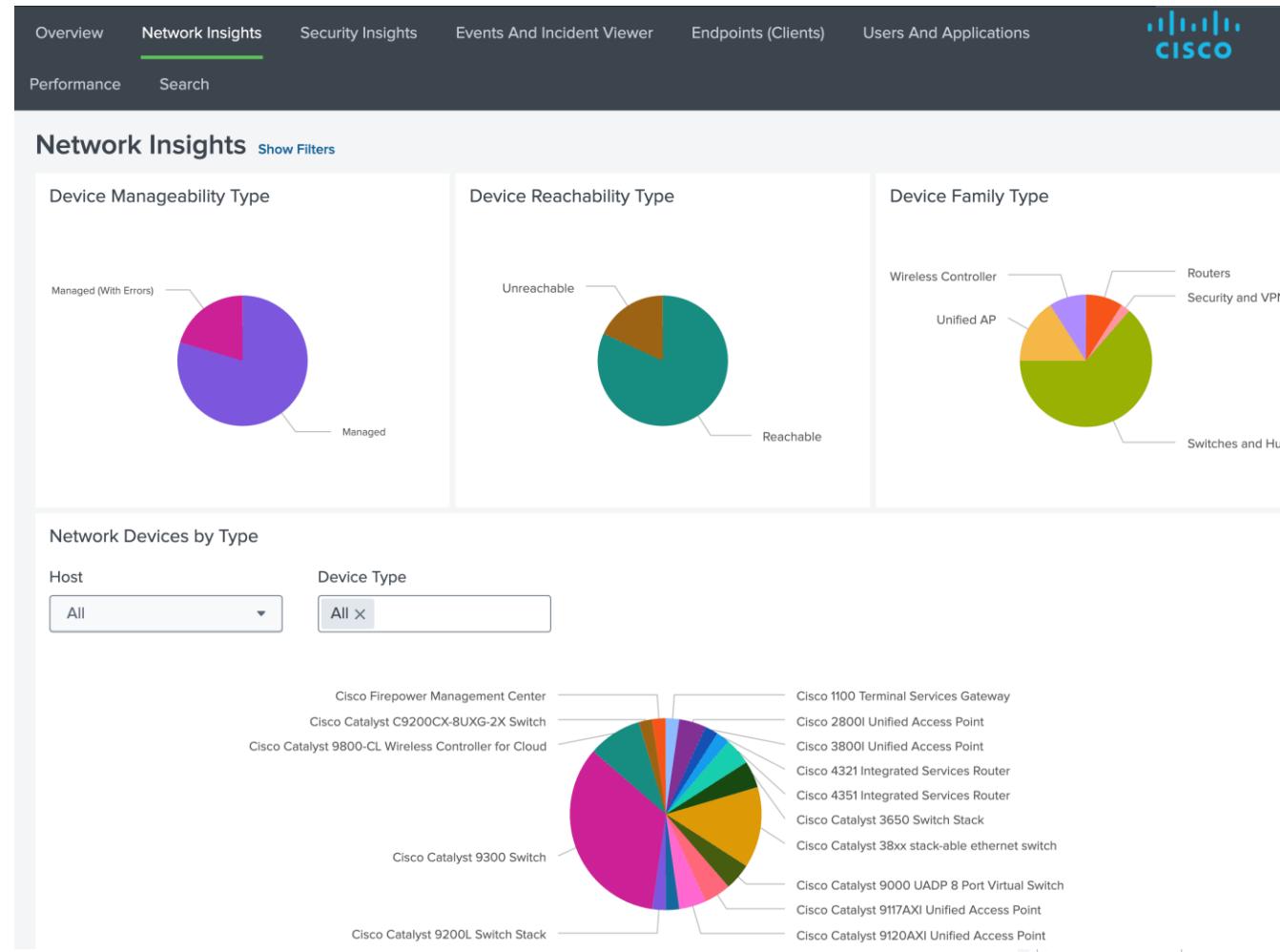
Analytics dashboard* to detect and report on anomalies based on deviation from the baseline (potentially powered by ITSI)

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

Enterprise Networking for Splunk

Network Insights & Endpoints

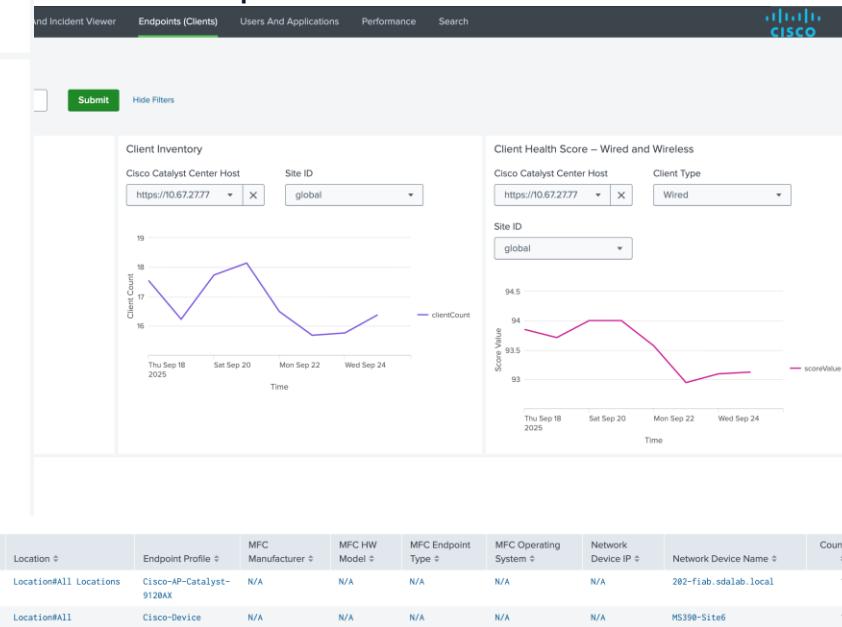


Network Insights

- 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

Device Uplink Addresses

Time Organization Id

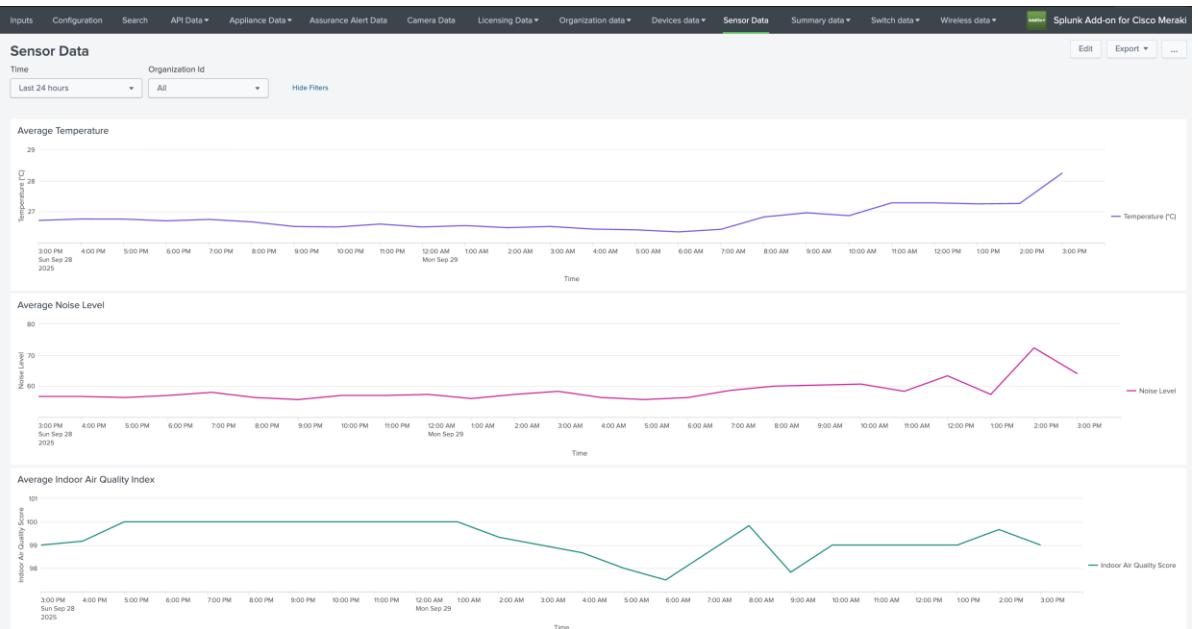
Last 24 hours All Hide Filters

Device Name	Device Serial	Interface	Uplink Address	Assignment Mode	Address Gateway	
MS	Q2JY-3BCC-E3L5	cellular	192.168.11.172	dynamic	192.168.11.254	
		wan1				
		wan2				
MG	Q2SX-4V76-Z6VP	man1	172.31.128.5 2001:8004:5198:20af:fa9e:28ff:fe26:a299	dynamic	172.31.128.1 fe80::2e3f:bf:fe1:397f	
	Q2VY-CKQ6-YT7D	cellular	10.249.56.19 2001:8004:5198:20af:dcad:beff:feef:0	dynamic	10.249.56.20 fe80::43e:db97:79f:da28	
	Q3EA-9228-E85T	man1	192.168.11.158	dynamic	192.168.11.254	
site6-9f:00	Q3EF-AJ99-TV4C	man1	192.168.254.86	static	192.168.254.81	
site7-64:00	Q3EF-D2BK-UL5D	man1	192.168.254.94	static	192.168.254.89	
	Q3LN-P952-96Z5	man1	192.168.60.17	dynamic	192.168.60.1	
	Q5AA-CLQL-6BZJ	man1	192.168.60.151	dynamic	192.168.60.1	
CW	Q5AC-REPL-SLKM	man1	172.31.128.4 2001:8004:5198:20af:ce9c:3eff:fee9:50e0	dynamic	172.31.128.1 fe80::2e3f:bf:fe1:397f	
	802705CSH01_S1	Q5JC-3QFZ-NQ44	man1	192.168.11.187	dynamic	192.168.11.254

Uplink Interface Distribution

Address Assignment Modes

Protocol Distribution



Devices Data

- Summary of Meraki device change history and uplink information

Sensor Data

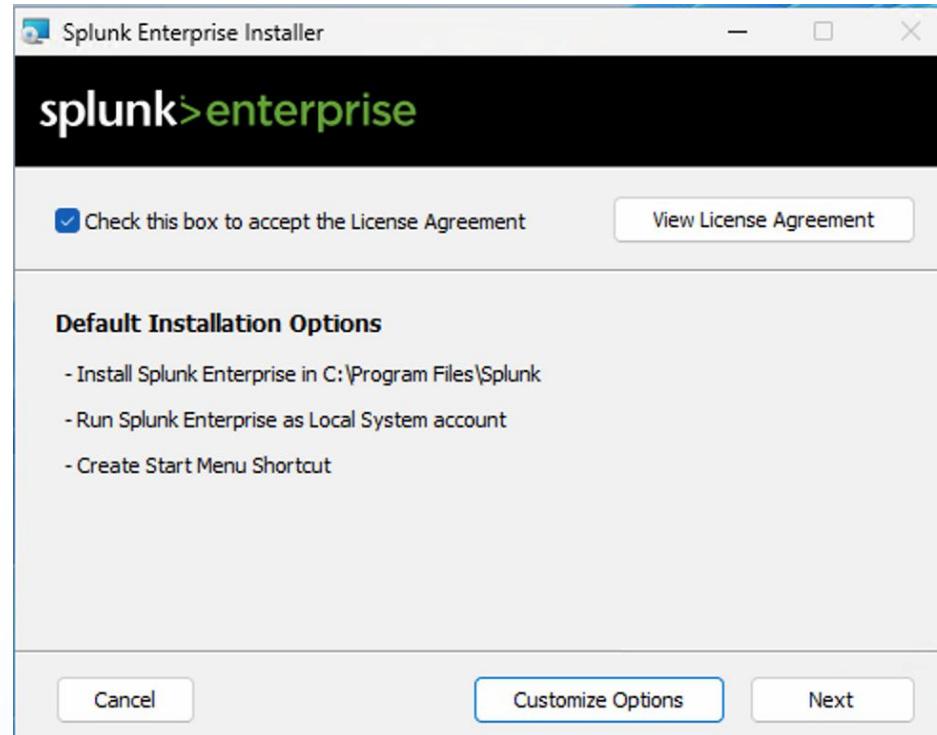
- Provides sensor data from Meraki environmental sensors

Splunk Installation & Getting Started

Splunk Enterprise Installation

Windows, Linux, Mac OS

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



Windows

```
cisco@splunk ~
$ ls
splunk-9.4.4-f627d88b766b.x86_64.rpm
cisco@splunk ~
$ sudo rpm -i splunk-9.4.4-f627d88b766b.x86_64.rpm
warning: splunk-9.4.4-f627d88b766b.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID b3cd4420: NOKEY
no need to run the pre-install check
complete
cisco@splunk ~
$ sudo su - splunk
[splunk@splunk ~]$ pwd
/opt/splunk
[splunk@splunk ~]$ ./bin/splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
```

Linux

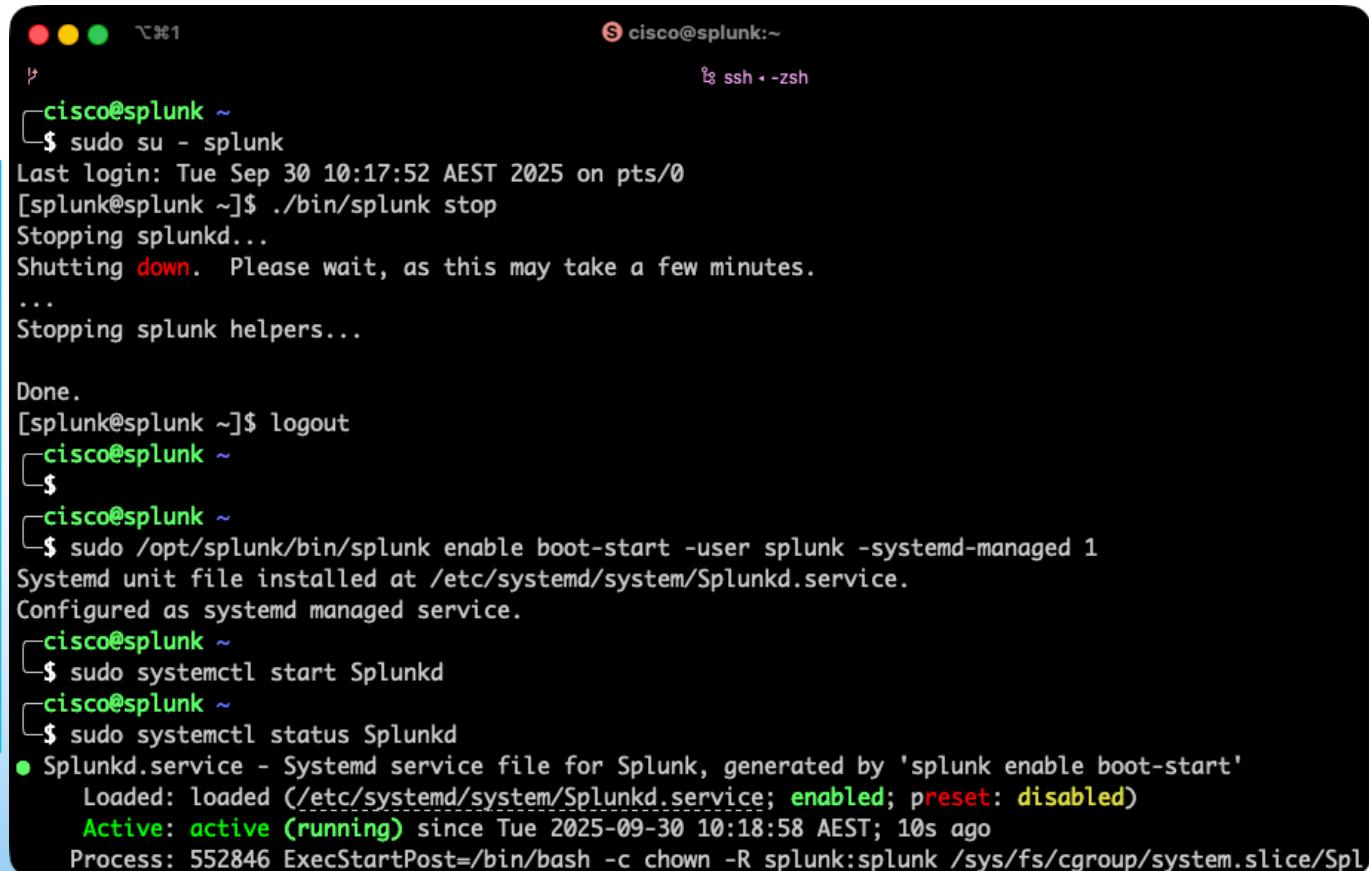
Splunk Enterprise Installation – Automatic Start

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
```

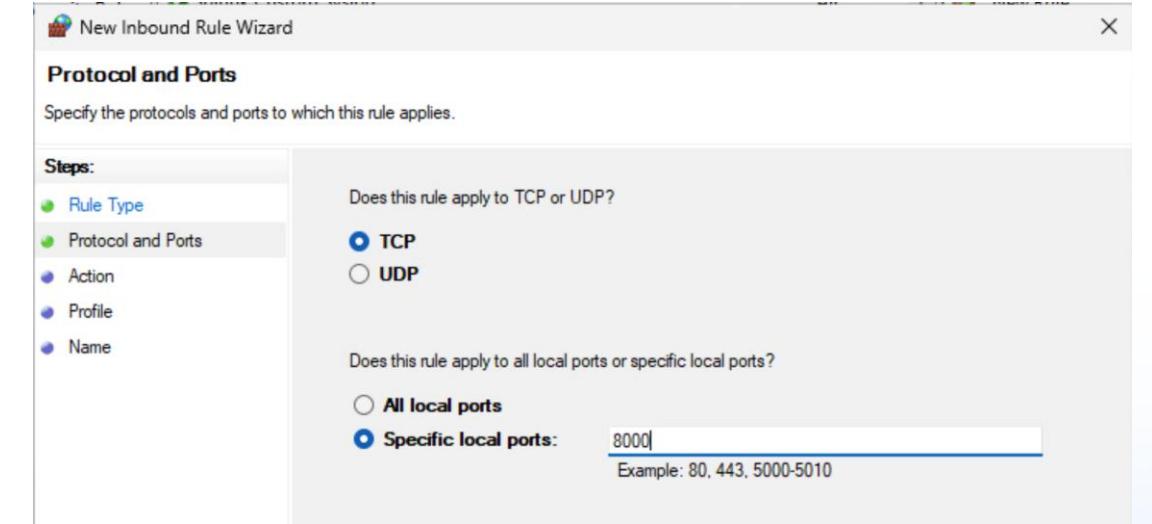


The terminal window shows the following session:

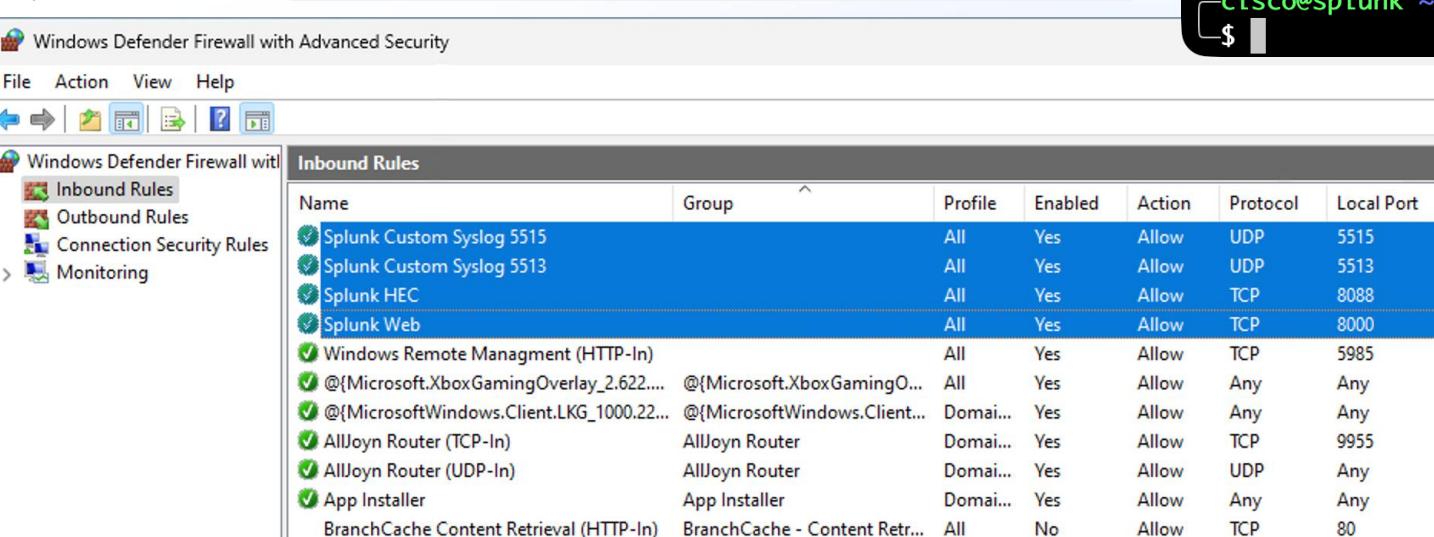
```
cisco@splunk:~$ sudo su - splunk
Last login: Tue Sep 30 10:17:52 AEST 2025 on pts/0
[splunk@splunk:~]$ ./bin/splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
...
Stopping splunk helpers...
Done.
[splunk@splunk:~]$ logout
cisco@splunk:~$ 
cisco@splunk:~$ sudo /opt/splunk/bin/splunk enable boot-start -user splunk -systemd-managed 1
Systemd unit file installed at /etc/systemd/system/Splunkd.service.
Configured as systemd managed service.
cisco@splunk:~$ sudo systemctl start Splunkd
cisco@splunk:~$ sudo systemctl status Splunkd
● Splunkd.service - Systemd service file for Splunk, generated by 'splunk enable boot-start'
    Loaded: loaded (/etc/systemd/system/Splunkd.service; enabled; preset: disabled)
      Active: active (running) since Tue 2025-09-30 10:18:58 AEST; 10s ago
        Process: 552846 ExecStartPost=/bin/bash -c chown -R splunk:splunk /sys/fs/cgroup/system.slice/Splunkd.service
           CPU: 10ms
```

Splunk Enterprise Installation - Firewall

Allow ports for Splunk



The screenshot shows the 'Protocol and Ports' step of the New Inbound Rule Wizard. It asks if the rule applies to TCP or UDP, with TCP selected. It then asks if it applies to all local ports or specific local ports, with 'Specific local ports' selected and the value '8000' entered.



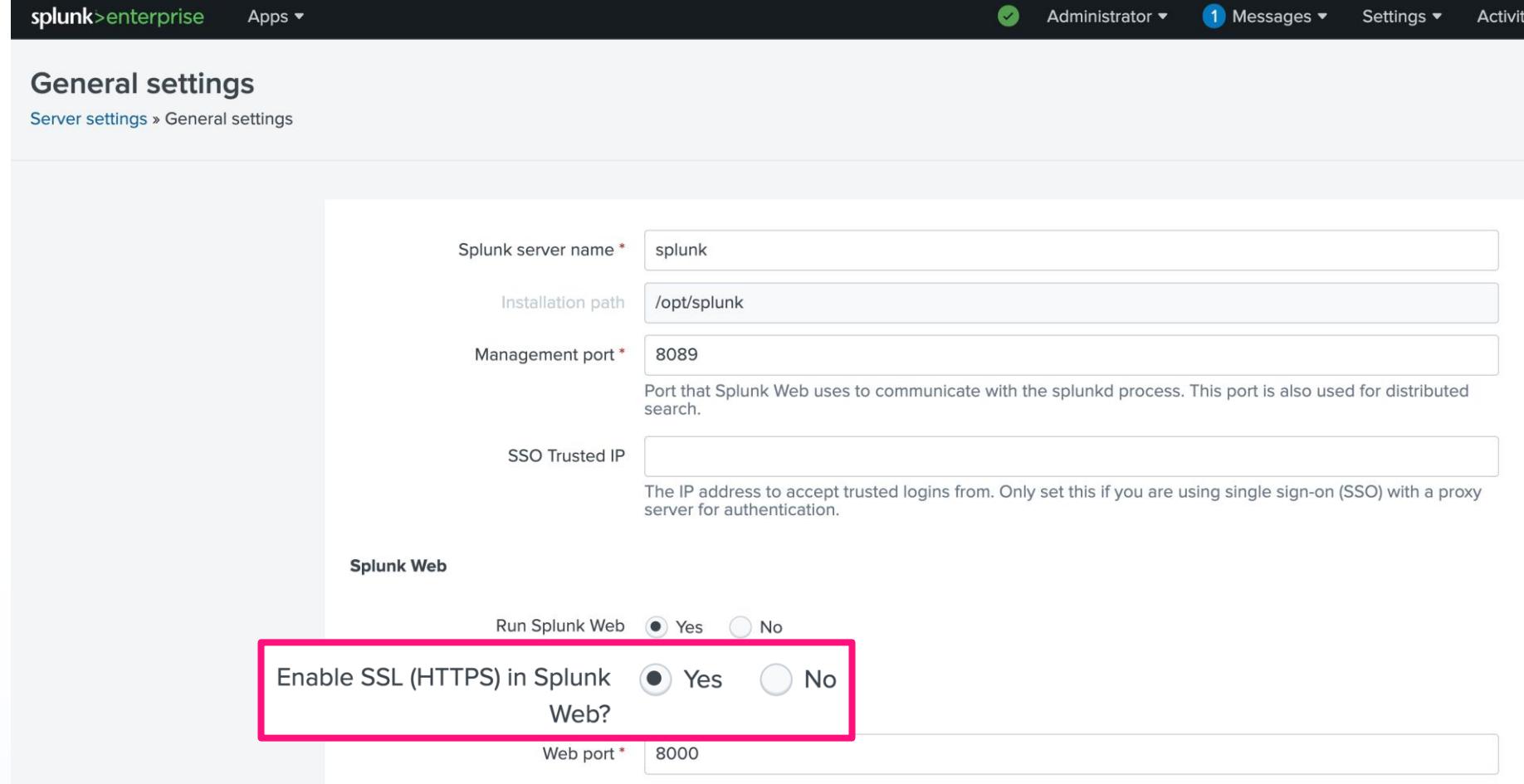
The screenshot shows the Windows Defender Firewall with Advanced Security interface. The 'Inbound Rules' table is displayed, listing various rules. The 'Splunk Web' rule is visible, showing it is an Allow rule for TCP port 8000.

Name	Group	Profile	Enabled	Action	Protocol	Local Port
Splunk Custom Syslog 5515		All	Yes	Allow	UDP	5515
Splunk Custom Syslog 5513		All	Yes	Allow	UDP	5513
Splunk HEC		All	Yes	Allow	TCP	8088
Splunk Web		All	Yes	Allow	TCP	8000
Windows Remote Management (HTTP-In)		All	Yes	Allow	TCP	5985
@{Microsoft.XboxGamingOverlay_2.622.7...}	@{Microsoft.XboxGamingO...	All	Yes	Allow	Any	Any
@{MicrosoftWindows.Client.LKG_1000.22...}	@{MicrosoftWindows.Client...	Domai...	Yes	Allow	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	TCP	9955
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	UDP	Any
App Installer	App Installer	Domai...	Yes	Allow	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	TCP	80

```
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



The screenshot shows the 'General settings' page in the Splunk Web interface. The top navigation bar includes 'splunk>enterprise', 'Apps ▾', 'Administrator', '1 Messages ▾', 'Settings ▾', and 'Activity'. The left sidebar shows 'General settings' under 'Server settings'. The main form contains the following fields:

- Splunk server name ***: splunk
- Installation path**: /opt/splunk
- Management port ***: 8089
- SSO Trusted IP**: (empty input field)
- Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.**: (empty input field)
- Splunk Web** section:
 - Run Splunk Web**: Yes No
 - Enable SSL (HTTPS) in Splunk Web?**: Yes No
 - Web port ***: 8000

Splunk Web

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

Splunk Technology Add-Ons (TAs)

Splunk Apps and Technology Add-Ons



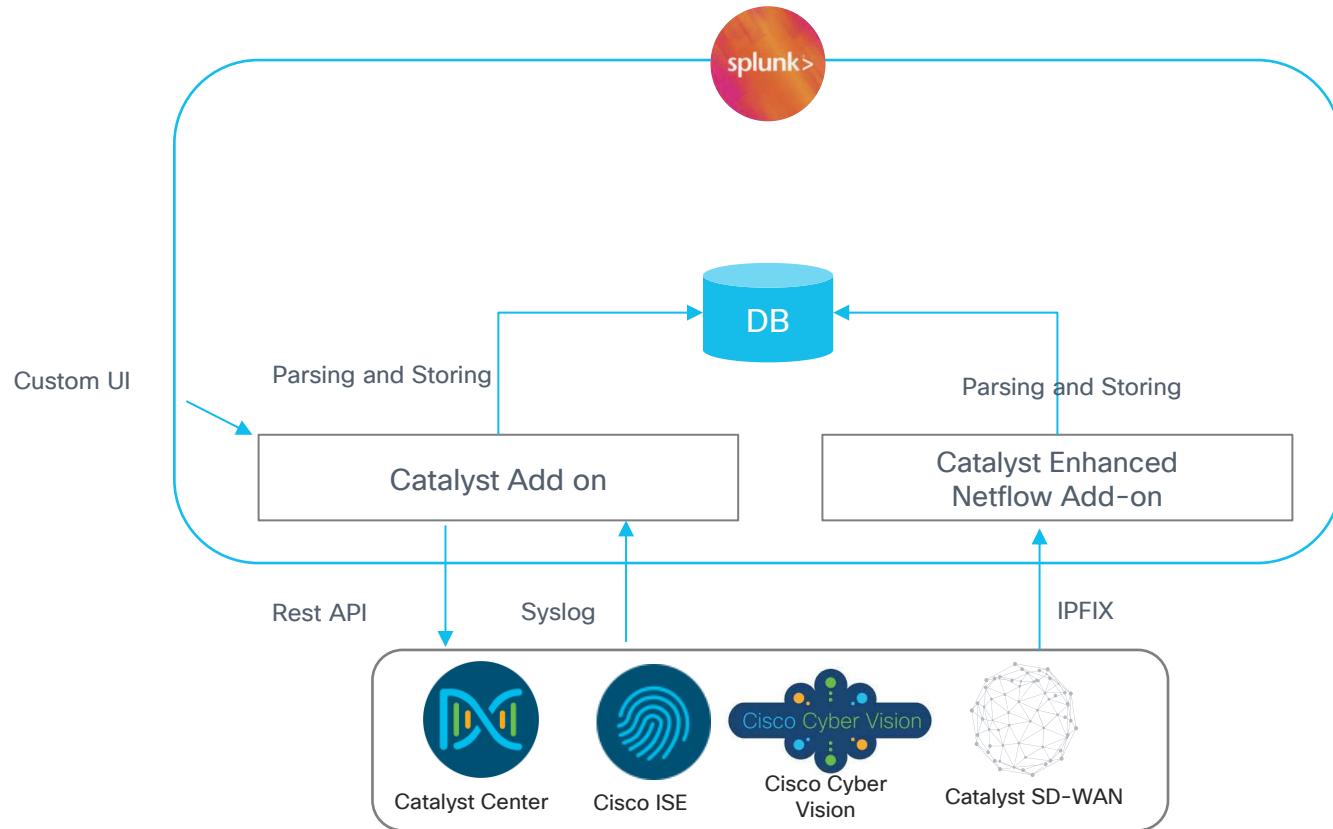
The screenshot shows the Splunkbase website interface. At the top, there is a navigation bar with the 'splunkbase' logo, 'Collections', 'Apps', 'Submit an app', and 'Log In' buttons. The main heading 'Get more out of Splunk with applications' is displayed in large white text. Below it is a search bar with the placeholder 'Search for apps'. To the right, there is a 3D perspective view of a grid of colorful app icons, including AWS, Cisco, Splunk, and others, arranged on a gradient surface.

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

<https://splunkbase.splunk.com>

Catalyst Add-On

Technical Add-On Architecture

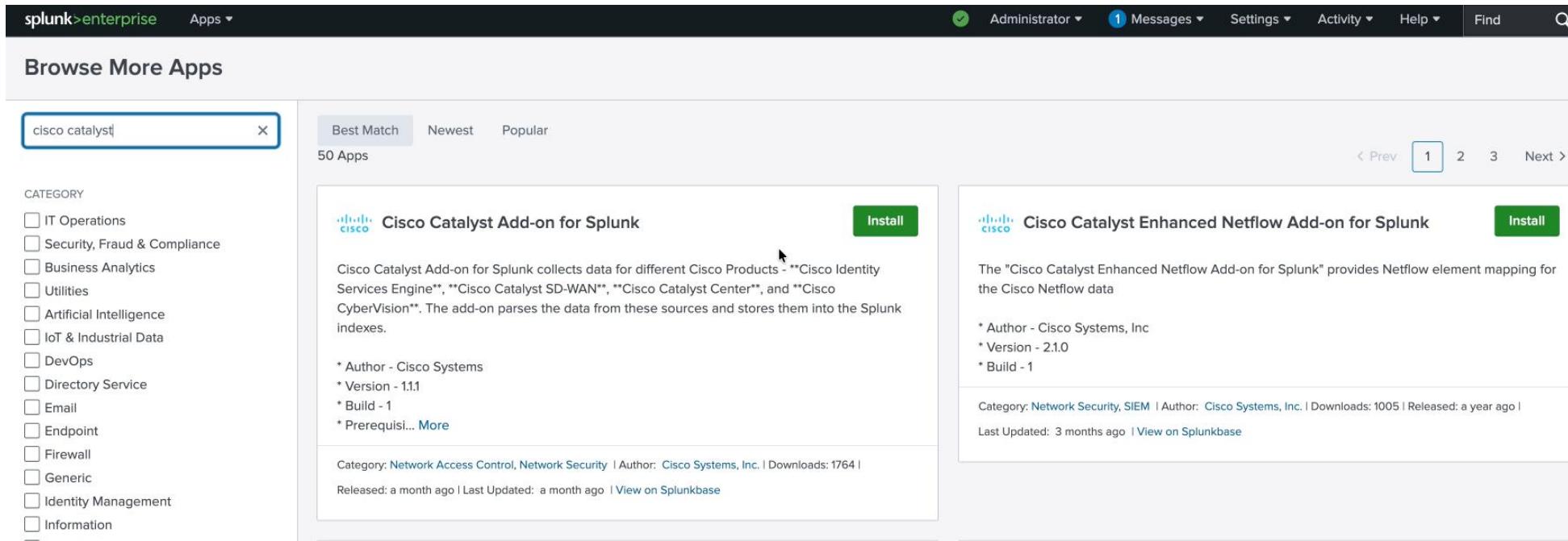


Two TAs used for ingesting telemetry

- [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



The screenshot shows the Splunk App Store interface. The search bar at the top contains the text 'cisco catalyst'. The search results are displayed in a grid format. The first result is 'Cisco Catalyst Add-on for Splunk', which is highlighted with a blue border. The second result is 'Cisco Catalyst Enhanced Netflow Add-on for Splunk'. The sidebar on the left shows various category filters, and the top navigation bar includes links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon.

Cisco Catalyst Add-on for Splunk

Cisco Catalyst Add-on for Splunk collects data for different Cisco Products - **Cisco Identity Services Engine**, **Cisco Catalyst SD-WAN**, **Cisco Catalyst Center**, and **Cisco CyberVision**. The add-on parses the data from these sources and stores them into the Splunk indexes.

* Author - Cisco Systems
* Version - 1.1.1
* Build - 1
* Prerequisi... [More](#)

Category: Network Access Control, Network Security | Author: Cisco Systems, Inc. | Downloads: 1764 | Released: a month ago | Last Updated: a month ago | [View on Splunkbase](#)

Cisco Catalyst Enhanced Netflow Add-on for Splunk

The "Cisco Catalyst Enhanced Netflow Add-on for Splunk" provides Netflow element mapping for the Cisco Netflow data

* Author - Cisco Systems, Inc
* Version - 2.1.0
* Build - 1

Category: Network Security, SIEM | Author: Cisco Systems, Inc. | Downloads: 1005 | Released: a year ago | Last Updated: 3 months ago | [View on Splunkbase](#)

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



Cisco Catalyst Add-on for Splunk

Cisco Catalyst Add-on for Splunk collects data for different Cisco Products - **Cisco Identity Services Engine**, **Cisco Catalyst SD-WAN**, **Cisco Catalyst Center**, and **Cisco CyberVision**. The add-on parses the data from these sources and stores them into the Splunk indexes.

Built by [Cisco Systems, Inc.](#)

[Download](#)

Cisco Catalyst Add-On for Splunk – Stream

Install the pre-requisite apps & add-ons

Splunk App for Stream

Splunk App for Stream is part of the purpose-built wire data collection and analytics solution from Splunk along with Splunk Add-on for Stream Forwarders for data collection and Splunk Add-on for Stream Wire Data for data parsing and formatting.

Built by [Splunk LLC](#)

 [Download](#)

[Main Page](#) / [Apps](#) / [Splunk Add-on for Stream Forwarders](#)

Splunk Add-on for Stream Forwarders

Splunk Add-on for Stream Forwarders is part of the purpose-built wire data collection and analytics solution from Splunk along with Splunk App for Stream for data visualization and forwarder management and Splunk Add-on for Stream Wire Data for data parsing and formatting.

Built by [Splunk LLC](#)

 [Download](#)

[Main Page](#) / [Apps](#) / [Splunk Add-on for Stream Wire Data](#)

Splunk Add-on for Stream Wire Data

Splunk Add-on for Stream Wire Data is part of the purpose-built wire data collection and analytics solution from Splunk along with Splunk App for Stream for data visualization and data capture management and Splunk Add-on for Stream Forwarders for data collection.

Built by [Splunk LLC](#)

 [Download](#)

Cisco Catalyst Enhanced Netflow Add-on for Splunk

The "Cisco Catalyst Enhanced Netflow Add-on for Splunk" provides Netflow element mapping for the Cisco Netflow data

Built by [Cisco Systems, Inc.](#)

 [Download](#)

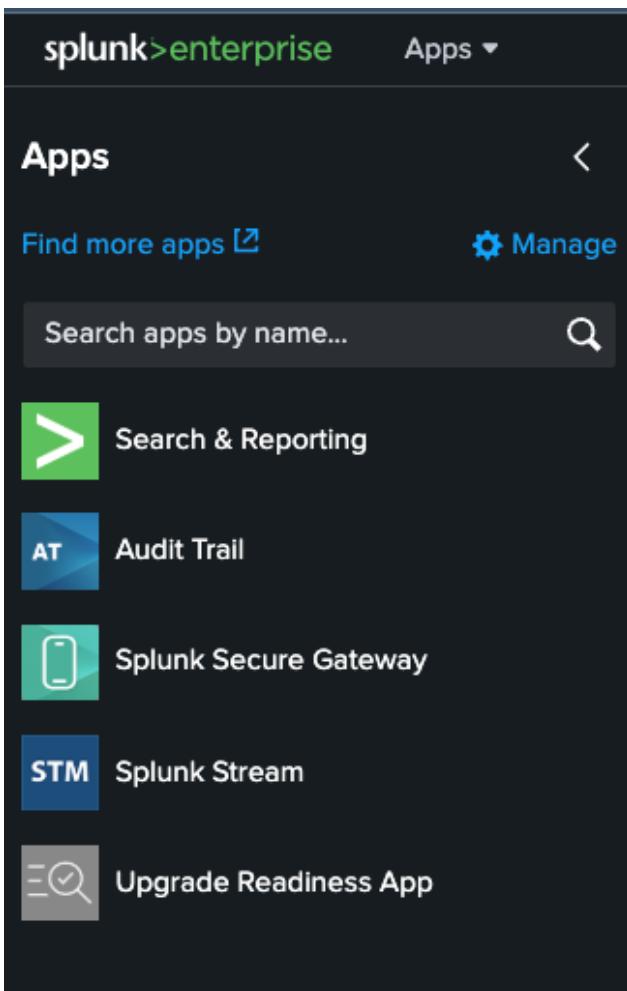
<https://splunkbase.splunk.com/app/1809>

<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



Informational Dashboards ▾ Admin Dashboards ▾ Stream Estimate Configuration ▾ Product Tour

Setup Stream

Run stream for the first time

Collect data from this machine using Wire Data input (Splunk_TA_stream).

⚠ Failed to detect Splunk_TA_stream status. [Please refer to the documentation for installation instructions](#) ↻ Redetect

Collect data from other machines.

[Let's get started](#)

```
cisco@splunk ~
└$ sudo su - splunk
Last login: Thu Oct  2 11:00:05 AEST 2025 on pts/0
[splunk@splunk ~]$ hostname
splunk
[splunk@splunk ~]$ cat /opt/splunk/etc/system/local/inputs.conf
[default]
host = splunk

[splunk@splunk ~]$
logout
[cisco@splunk ~
└$ sudo systemctl restart Splunkd
[cisco@splunk ~
$ ]
```

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

Informational Dashboards ▾ Admin Dashboards ▾ Stream Estimate Configuration ▾ Product Tour

Setup Stream

Run stream for the first time

Collect data from this machine using Wire Data input (Splunk_TA_stream).

⚠ Splunk_TA_stream doesn't have proper permissions to run or not configured properly. [↻ Redetect](#)

Steps to troubleshoot:

1. To ensure that Splunk_TA_Stream has proper permissions on Linux/OSX, run this command from the Splunk_TA_stream directory:

```
sudo ./set_permissions.sh
```

2. Examine Splunk_TA_stream

splunk>enterprise Apps ▾

Learn More ↗

Informational Dashboards ▾ Admin Dashboards ▾ Stream Estimate Configuration ▾ Product Tour

Collect data from other machines.

Let's get started

Setup Stream

Run stream for the first time

Collect data from this machine using Wire Data input (Splunk_TA_stream).

✓ Proper permissions for Splunk_TA_stream have been set. [Learn More ↗](#) [↻ Redetect](#)

Collect data from other machines.

⚠ HTTP Event Collector global token configuration has been disabled. [View configuration ↗](#) [↻ Redetect](#)

Splunk App for Stream auto-configures the token settings only on the search head that it runs on. In a distributed environment, manual replication of the streamfwd token configuration on each indexer is required.

To get data from other machines, run this command on your data source machine:

```
curl -sSL https://splunk:8000/en-us/custom/splunk_app_stream/install_streamfwd | sudo bash
```

Note: Stream Forwarder (streamfwd) independent installation supports data capture on 64-bit Linux (RHEL and Ubuntu) only.

Let's get started

```
cisco@splunk:~$ ssh -zsh
cisco@splunk:~$ sudo chmod +x /opt/splunk/etc/apps/Splunk_TA_stream/set_permissions.sh
cisco@splunk:~$ sudo /opt/splunk/etc/apps/Splunk_TA_stream/set_permissions.sh
setting capabilities
setting setuid for streamfwd-rhel6 - linux 64 bit version
cisco@splunk:~$
```

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

New Index

General Set

Index Name **netflow**

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type **Events**

The type of data to store (event-based or metrics).

Home Path **optional**

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path **optional**

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path **optional**

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check **Enable**

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index **500** **GB**

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket **auto** **GB**

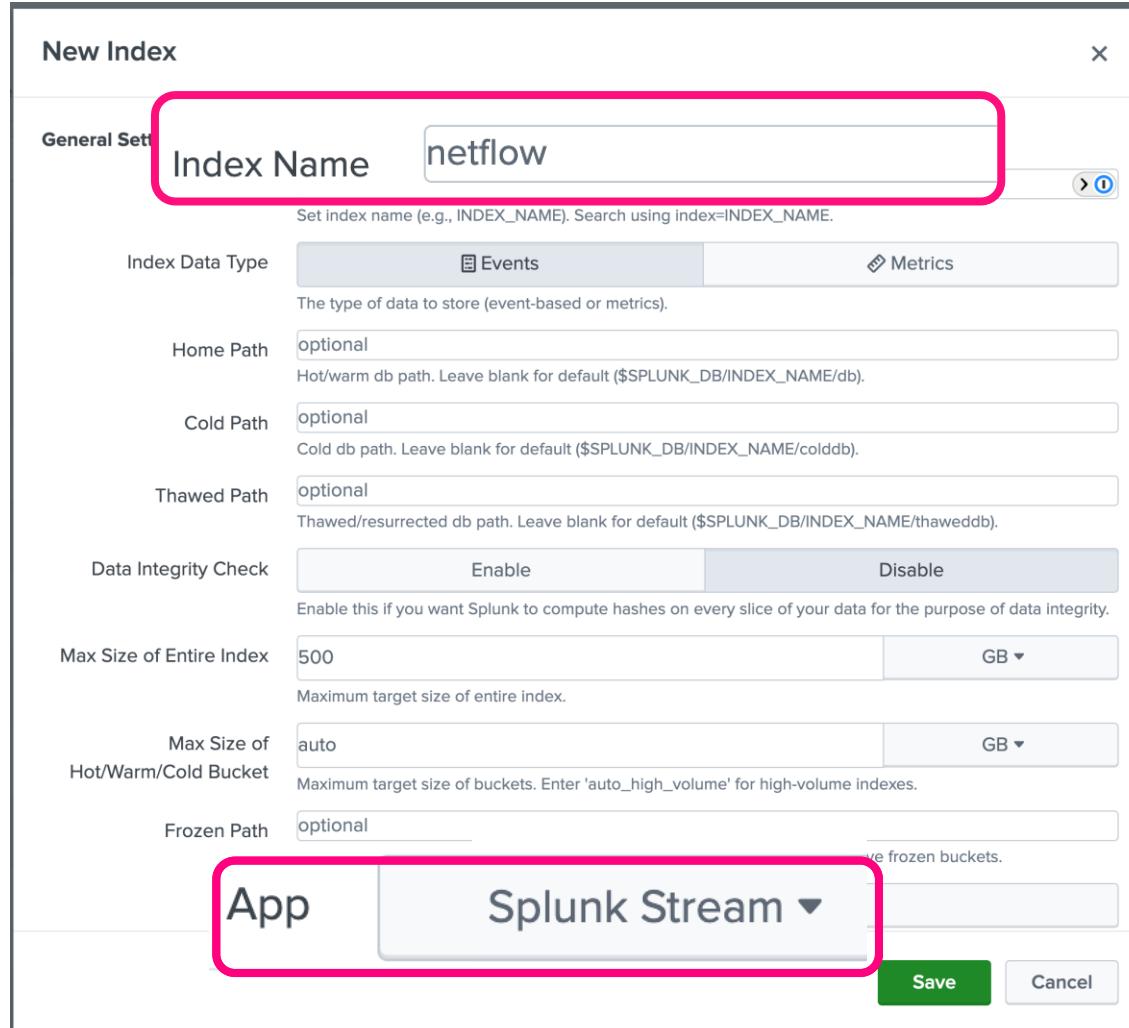
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path **optional**

Leave frozen buckets.

App **Splunk Stream ▾**

Save Cancel



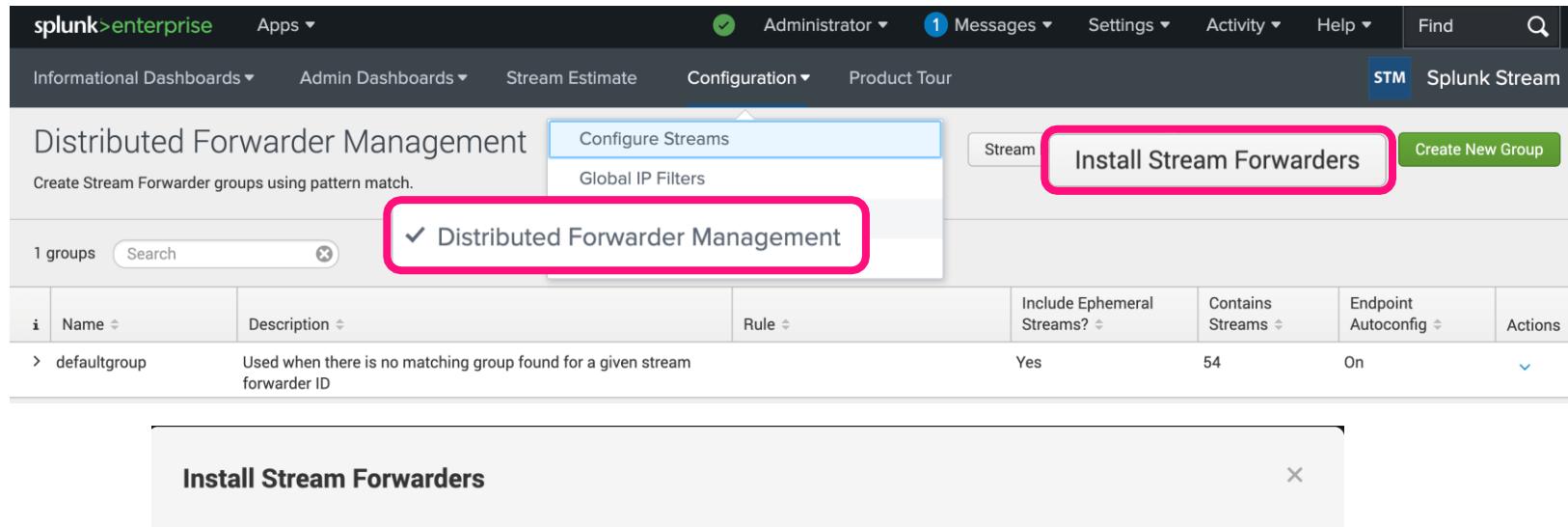
Step 7 – Create an index for NetFlow

Splunk HTTP Event Collector

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
- Page Title:** HTTP Event Collector
- Page Subtitle:** Data Inputs » HTTP Event Collector
- Table:** Shows 1 Token named "streamfwd" with actions: Edit, Disable, Delete, Copy, Show, and Token Value (redacted).
- Buttons:** Global Settings (highlighted with a red box), New Token.
- Modal Dialog:** Edit Global Settings (highlighted with a blue box). It contains the following settings:
 - All Tokens: Enabled (radio button selected)
 - Default Source Type: Select Source Type ▾
 - Default Index: Default ▾
 - Default Output Group: None ▾
 - Use Deployment Server:
 - Enable SSL:
 - HTTP Port Number: 8088
- Callout Box:** Step 8 – Enable HEC globally
Step 9 – Create a HEC for the NetFlow Stream Forwarder

Stream forwarder



The screenshot shows the Splunk Stream interface with the following details:

- Header:** splunk>enterprise, Apps, Administrator, 1 Messages, Settings, Activity, Help, Find, Search.
- Top Navigation:** Informational Dashboards, Admin Dashboards, Stream Estimate, Configuration, Product Tour, STM, Splunk Stream.
- Left Sidebar:** Distributed Forwarder Management (highlighted with a red box), Create Stream Forwarder groups using pattern match.
- Main Content:** A table showing 1 group named 'defaultgroup'. The table columns are: Name, Description, Rule, Include Ephemeral Streams?, Contains Streams, Endpoint Autoconfig, and Actions.
- Actions:** Configure Streams, Global IP Filters, Stream, Create New Group, Install Stream Forwarders (highlighted with a red box).

Install Stream Forwarders

[View configuration](#) [Redetect](#)

Splunk App for Stream auto-configures the token settings only on the search head that it runs on. In a distributed environment, manual replication of the streamfwd token configuration on each indexer is required.

To get data from other machines, run this command on your data source machine:

```
curl -sSL https://splunk:8000/en-us/custom/splunk_app_stream/install_streamfwd | sudo bash
```

Note: Stream Forwarder (streamfwd) independent installation supports data capture on 64-bit Linux (RHEL and Ubuntu) only.

Or install Stream TA on your data source machine. [Learn more](#)

- 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/
Total 45.0M
% 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/
```

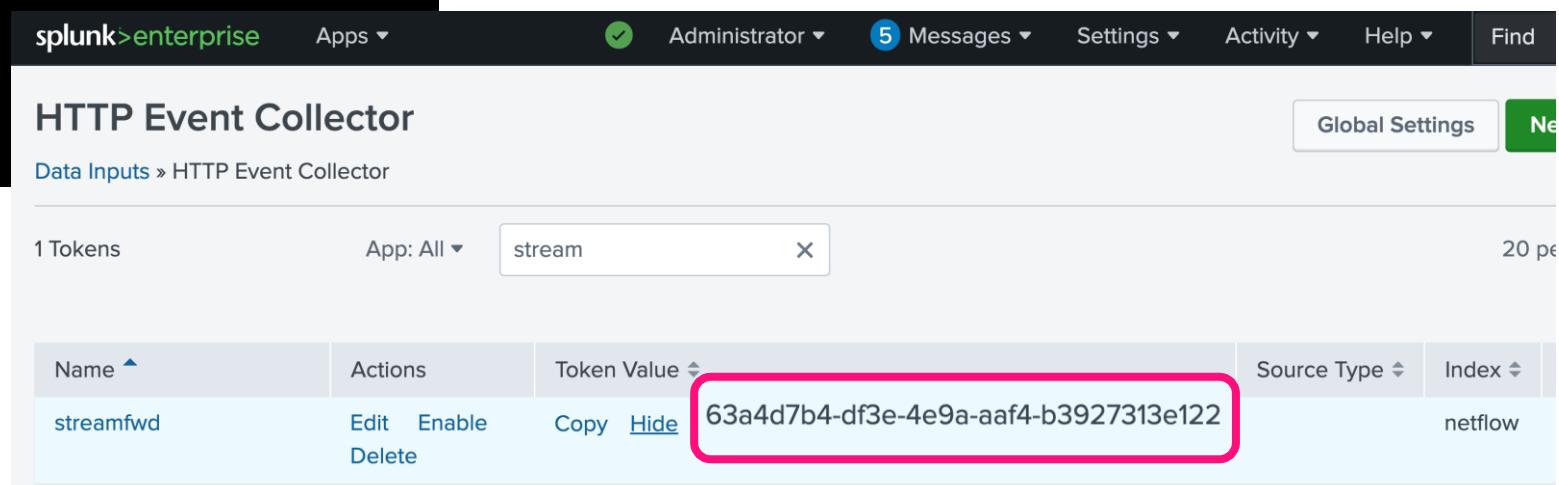
```
● ● ●  ✘ 1  S cisco@streamfwd:~
↳ ssh -zsh
X ~ (ssh)

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  
x ~ (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
```



The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise, Apps ▾, Administrator, 5 Messages, Settings, Activity, Help, Find.
- Page Title:** HTTP Event Collector (Data Inputs > HTTP Event Collector)
- Search Bar:** 1 Tokens, App: All, stream, X, 20 pe.
- Table:** A table showing a single token configuration:

Name	Actions	Token Value	Source Type	Index
streamfwd	Edit, Enable, Delete, Copy, Hide	63a4d7b4-df3e-4e9a-aaf4-b3927313e122	netflow	

- 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

Edit Token: streamfwd

Description: optional

Source: optional

Set Source Type: Entered sourcetype ▾

Source Type: Select Source Type ▾

Select Allowed Indexes (optional): Available indexes: history, main, netflow, summary. Selected indexes: netflow. [add all](#) [remove all](#)

Select indexes that clients will be able to select from.

Default Index (optional): netflow ▾

Output Group (optional): None ▾

Enable indexer acknowledgement:

[Cancel](#) [Save](#)

splunk>enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

HTTP Event Collector

Data Inputs » HTTP Event Collector

1 Tokens App: All ▾ filter 20 per page ▾

Name ▾	Actions	Token Value ▾	Source Type ▾	Index ▾	Status ▾
streamfwd	Edit Disable Copy Show *****		netflow	Enabled	

Informational Dashboards ▾ Admin Dashboards ▾ Stream Estimate Configuration ▾ Product Tour Splunk Stream [New Stream](#) ▾

Configure Streams

Create and configure streams for a variety of network data protocols.

Metadata Streams: 54 Packet Streams: 0 Ephemeral Streams: 0

<input type="checkbox"/>	Name ▾	Actions	Mode ▾	Protocol ▾	Description ▾	App ▾	Created By ▾	Recent Traffic(15m)
<input type="checkbox"/>	amqp	Edit ▾	Enabled	Estimate	Disabled	AMQP	AMQP Protocol Events	Stream
<input type="checkbox"/>	arp	Edit ▾	Enabled	Estimate	Disabled	ARP	ARP protocol events	Stream
<input type="checkbox"/>	cisco_hsl_cisco_hsl_netflow	Edit ▾	Enabled	Estimate	Disabled	Netflow	Netflow Protocol Events	Stream
<input type="checkbox"/>	dhcp	Edit ▾	Enabled	Estimate	Disabled	DHCP	DHCP Protocol Events	Stream

Avg. Traffic(15m) ~ 1.8 Mb/s

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

Cisco Catalyst Add-on for Splunk

Cisco Catalyst Add-on for Splunk collects data for different Cisco Products - **Cisco Identity Services Engine**, **Cisco Catalyst SD-WAN**, **Cisco Catalyst Center**, and **Cisco CyberVision**. The add-on parses the data from these sources and stores them into the Splunk indexes.

Built by [Cisco Systems, Inc.](#)

 [Download](#)

- [Catalyst Add-on](#) – Parses data from specified sources and stores them into Splunk indexes
- [Enterprise Networking](#) – Presents visualizations in dashboards based on the Catalyst Add-on

Cisco Enterprise Networking for Splunk Platform

The **Cisco Enterprise Networking for Splunk Platform** presents visualizations in dashboards for different Cisco Products - **Cisco Identity Services Engine**, **Cisco Catalyst SD-WAN**, and **Cisco Catalyst Center**. The App uses the data collected by "Cisco Catalyst Add-on for..."

Built by [Cisco Systems, Inc.](#)

 [Download](#)

Latest Version 2.0.0
May 30, 2025
[Release notes](#)

Compatibility ⓘ
Splunk Enterprise, Splunk Cloud
Platform Version: 9.4, 9.3, 9.2, 9.1
CIM Version: 5.X

Rating
0  (0)
[Rate this app](#)

Support
 Cisco Supported App
[Learn more](#)

Ranking
#4 In Network Access Control
#18 In Firewall

<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

New Index

General Settings

Index Name **catalyst** (highlighted with a red box)

Index Data Type Events Metrics

Home Path optional

Cold Path optional

Thawed Path optional

Data Integrity Check Enable Disable

Max Size of Entire Index 500 GB ▾

Max Size of Hot/Warm/Cold Bucket auto GB ▾

Frozen Path optional

App Cisco Catalyst Add-on for Splunk (highlighted with a blue box)

Storage Optimization

Tsidx Retention Policy Enable Reduction Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

Save **Cancel**

cisco_catalyst_app_index

Advanced search » Search macros » cisco_catalyst_app_index

Definition* Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

index IN ("catalyst") (highlighted with a red box)

Use eval-based definition?

Arguments Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '-' and '.' characters.

Validation Expression Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message Enter a message to display when the validation expression returns 'false'.

Cancel **Save**

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

Application Setup Search

Catalyst Center

Catalyst Center: A network management solution that leverages AI to connect, secure, and automate network operations for routers, switches and access points. It simplifies IT experiences, enhances business agility, and supports both cloud and on-premises deployments. Manage your entire enterprise network with ease, from routers to wireless access points, all through a single pane of glass.

[Learn More](#) [Configure Application](#)

Cyber Vision

Cisco Cyber Vision is a comprehensive solution designed to ensure the continuity, resilience, and safety of industrial operations by providing continuous visibility into Industrial Control Systems (ICS) and controlling the risks of cyber attacks. It offers full visibility into industrial networks and OT security posture, enabling asset owners to reduce the attack surface, segment the industrial network, and enforce cybersecurity policies.

[Learn More](#) [Configure Application](#)

Cisco Catalyst SD-WAN

Cisco Catalyst™ SD-WAN connects any user to any application with integrated capabilities for multicloud, security, predictive automation, and enhanced network visibility — all on a Secure Access Service Edge (SASE)-enabled architecture. It also simplifies network operations by providing granular network insights, automation, and predictivity that not only heighten network integrity but also deliver an optimal application experience.

[Learn More](#) [Configure Application](#)

Identity Services Engine (ISE)

Cisco Identity Services Engine is the industry's only complete Network Access Control (NAC) solution that provides customers with the ability to see users and devices, control access across wired, wireless VPN, and 5G connections to the corporate network. Cisco ISE works with network devices to create an all-encompassing contextual identity with endpoint users and attributes to apply highly secure access policies through a simple, flexible, and highly consumable platform.

[Learn More](#) [Configure Application](#)

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



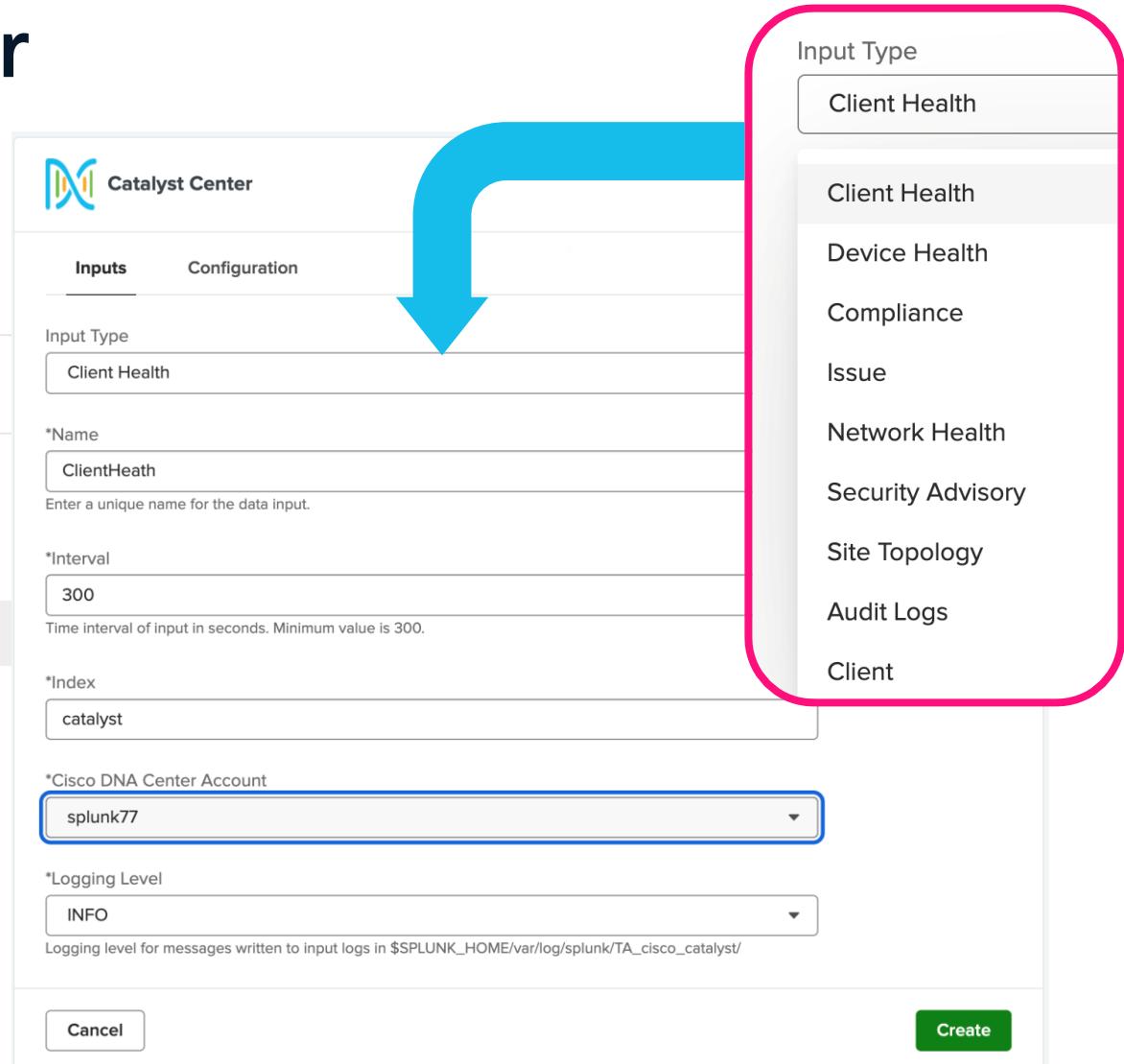
Inputs Configuration

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



Catalyst Center

Inputs Configuration

Input Type

Client Health

Client Health

Device Health

Compliance

Issue

Network Health

Security Advisory

Site Topology

Audit Logs

Client

Name: ClientHeath

Interval: 300

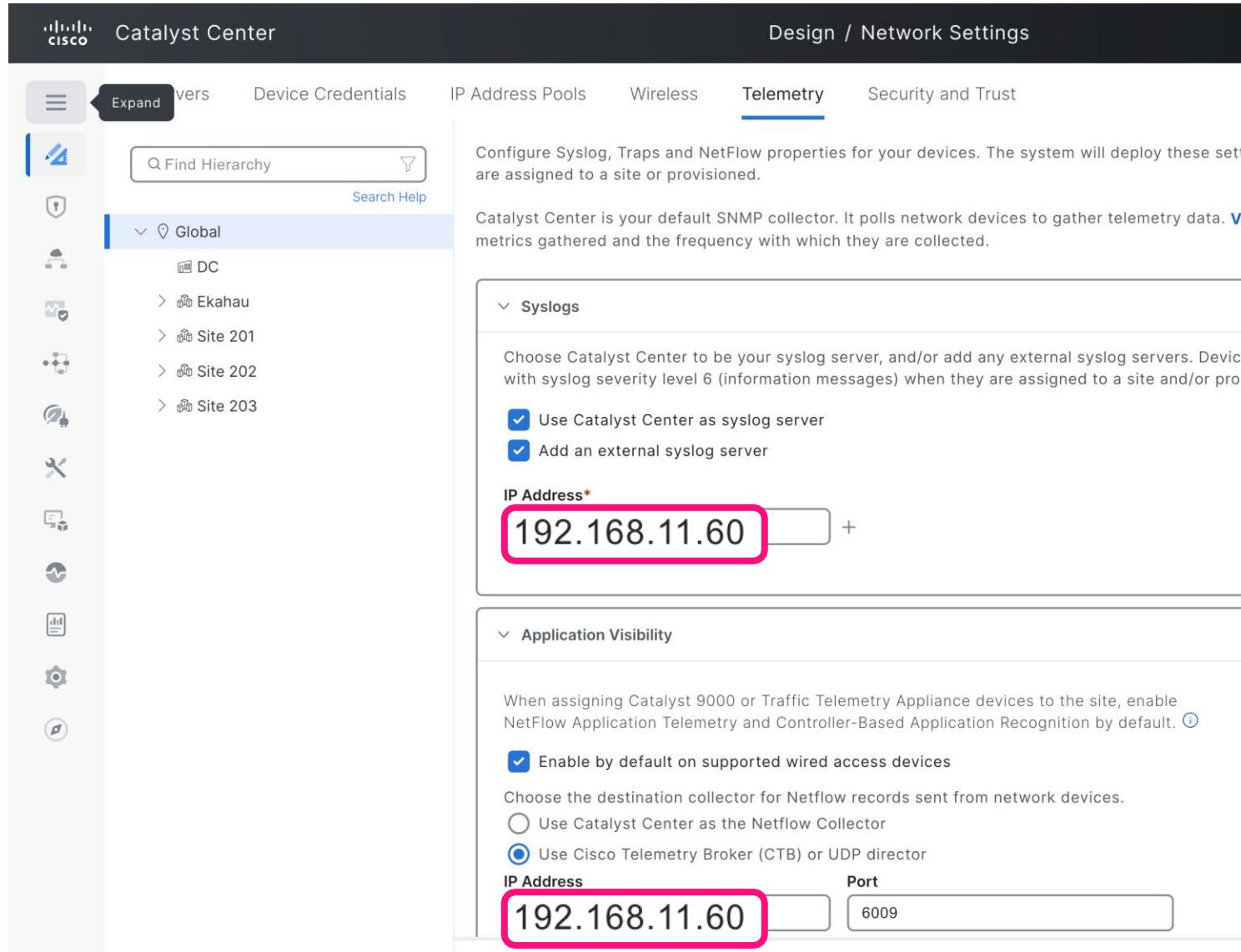
Index: catalyst

Cisco DNA Center Account: splunk77

Logging Level: INFO

Cancel Create

Getting Catalyst Center Telemetry Sent to Splunk



The screenshot shows the Catalyst Center interface with the following details:

- Header:** Catalyst Center, Design / Network Settings, Telemetry (selected).
- Left Sidebar:** Find Hierarchy, Global (selected), DC, Ekahau, Site 201, Site 202, Site 203.
- Telemetry Tab:** Configure Syslog, Traps and NetFlow properties for your devices. Catalyst Center is the default SNMP collector.
- Syslog Section:** Choose Catalyst Center to be your syslog server, and/or add any external syslog servers. IP Address: 192.168.11.60.
- Application Visibility Section:** When assigning Catalyst 9000 or Traffic Telemetry Appliance devices to the site, enable NetFlow Application Telemetry and Controller-Based Application Recognition by default. IP Address: 192.168.11.60, Port: 6009. The "Use Cisco Telemetry Broker (CTB) or UDP director" option is selected.

Syslog

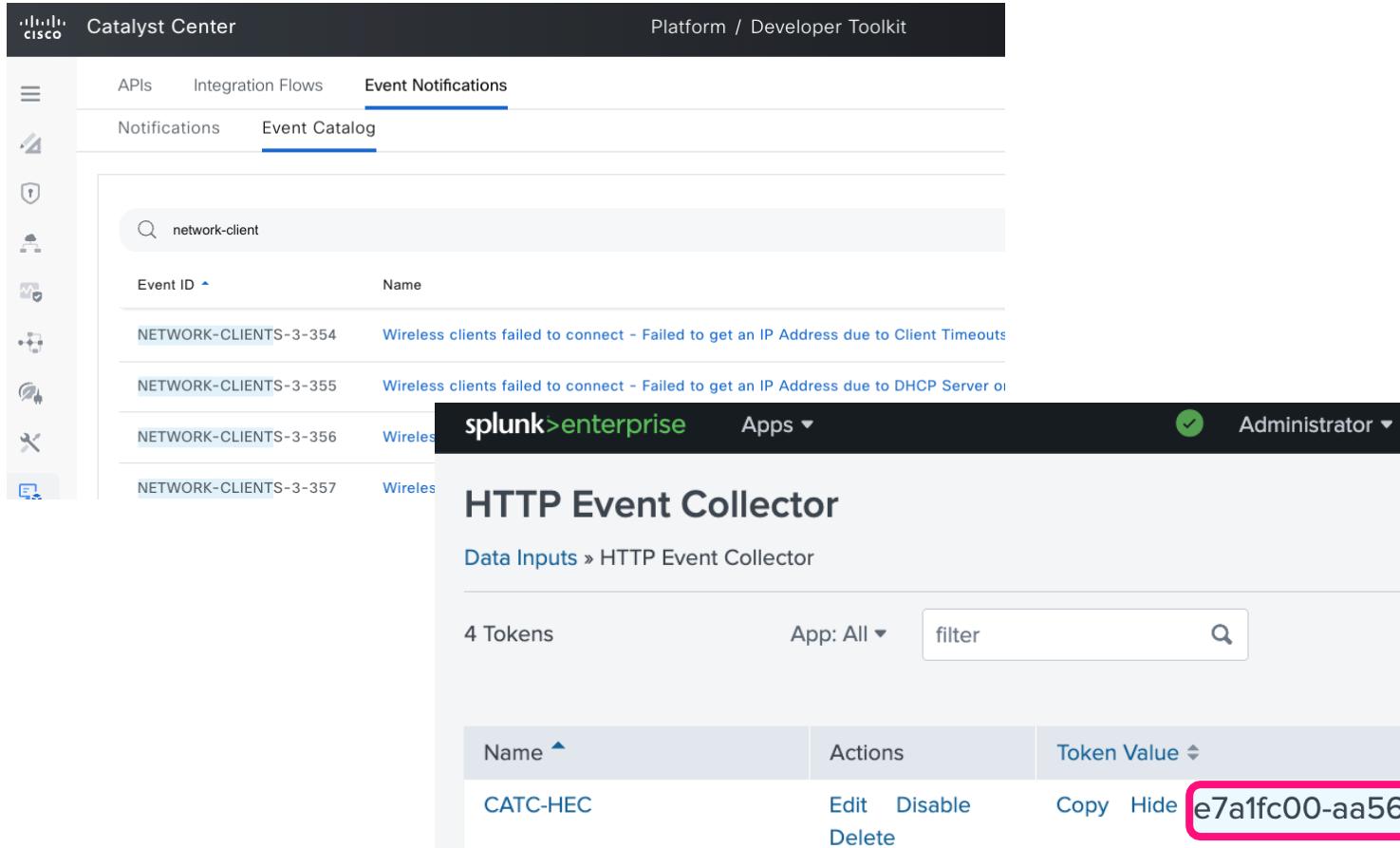
- Add an entry for syslog with Splunk as the destination

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



Catalyst Center

Platform / Developer Toolkit

Event Notifications

Notifications Event Catalog

network-client

Event ID Name

NETWORK-CLIENTS-3-354 Wireless clients failed to connect - Failed to get an IP Address due to Client Timeouts

NETWORK-CLIENTS-3-355 Wireless clients failed to connect - Failed to get an IP Address due to DHCP Server or

NETWORK-CLIENTS-3-356 Wireless

splunk>enterprise Apps ▾ Administrator ▾

HTTP Event Collector

Data Inputs » HTTP Event Collector

4 Tokens App: All filter

Name	Actions	Token Value
CATC-HEC	Edit Disable Copy Hide	e7a1fc00-aa56-4157-ad...

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

Edit Webhook

Name*

CATC-HEC-splunk-raw

Description

Splunk HEC

URL*

https://10.67.27.25:8088/services/collector

Trust Certificate

Yes No

Method*

POST

Authentication

Basic Token No Auth

Proxy

Headers

Header Name

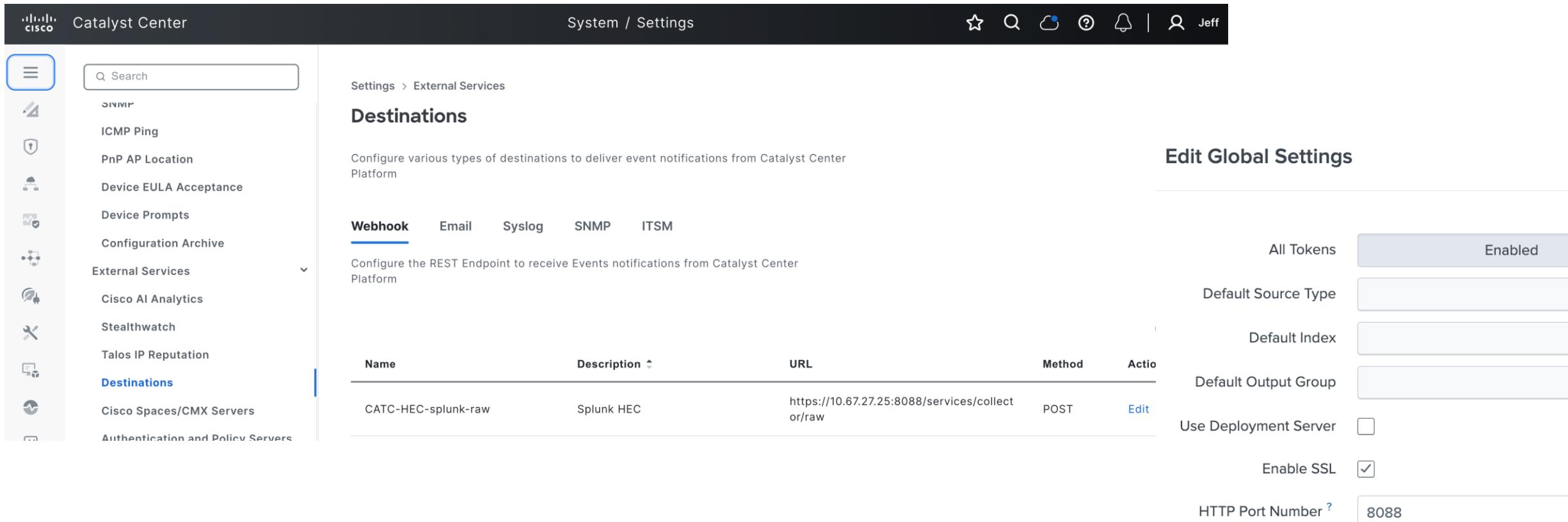
Authorization

Header Value

Splunk e7a1fc00-aa56-4157-ad...

Catalyst Center Event Notifications – Webhook

Send events and notifications from Catalyst Center directly to Splunk



The screenshot shows the Catalyst Center interface. The left sidebar has a 'Destinations' section selected. The main content area is titled 'Destinations' and shows a table for 'Webhook' configurations. One entry is listed: 'CATC-HEC-splunk-raw' with 'Splunk HEC' as the description, 'https://10.67.27.25:8088/services/collect or/raw' as the URL, and 'POST' as the method. To the right, there is a 'Edit Global Settings' panel with various configuration options like 'All Tokens' (Enabled), 'Default Source Type', 'Default Index', 'Default Output Group', 'Use Deployment Server' (unchecked), 'Enable SSL' (checked), and 'HTTP Port Number' (8088).

Name	Description	URL	Method	Action
CATC-HEC-splunk-raw	Splunk HEC	https://10.67.27.25:8088/services/collect or/raw	POST	Edit

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

The screenshot shows the Catalyst Center Event Notifications interface and a Splunk search interface.

Catalyst Center Event Notifications: The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Platform / Developer Tool'. The 'Event Notifications' tab is selected. Below it, the 'Notifications' tab is active, and the 'Event Catalog' tab is visible. A sidebar on the left lists 'CHANNELS' with 'All' selected, and 'REST (2)' and 'WEBEX (2)' options. A 'Create New' button with a plus sign is in the center. To the right, a card for 'P1-Webex-Notifications' is shown, along with a 'Actions' dropdown. A 'Splunk-HEC' card is also visible.

Splunk Search Interface: The bottom part of the screenshot shows a Splunk search interface titled 'New Search'. The search bar contains the query: `index=catalyst_center "details.Category"="OUT OF BAND" | stats count by "details.Device Name"`. The results section shows '10 events' from '03/09/2025 00:00:00.000' to '03/10/2025 12:56:14.000'. A visualization chart titled 'count' is displayed, showing the count of events for various device names. The chart has a legend for 'count' and shows data for devices like 105-flab-1.sdalab.local, 201-core-1.sdalab.local, 201-edge-1.sdalab.local, 202-flab.sdalab.local, 301-leaf-1.sdalab.local, 301-spine-1.sdalab.local, and cl2backbone.sdalab.local.

Identity Services Engine

Catalyst App – Identity Services Engine

Send Identity Services Engine Data to Splunk

Add Identity Services Engine (ISE) Account

*Account Name
splunkise11
Enter a unique name for this account.

*IP Address/Hostname
https://192.168.11.11
Enter the IP Address of the ISE in format https://<ip address> or https://<host-name>

*Username
admin
Enter the username for this account.

*Password

Enter the password for this account.

pxGrid Hostname
https://192.168.11.11
Enter the hostname of the pxGrid in format https://<host-name>

pxGrid Client Username
splunkise
This field is highlighted with a red box.

pxGrid Certificate-Based Authentication

Use Custom CA Certificate

Enable Proxy

Cancel **Add**

Identity Services Engine Administration / pxGrid Services

Summary Client Management Diagnostics Settings

Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

pxGrid Clients

Name	Description	Client Groups	Status
splunkise			Enabled

Identity Services Engine (ISE)

Inputs **Syslog** Configuration Additional Settings

*Input Type
 UDP
 TCP

*Port
5513
Enter the Port for this input.

Only accept connection from
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com (if not set, accepts connections from all hosts).

*Input Source Type
cisco:ise:syslog

Select the relevant source type for your input.

*Index
catalyst
Select the index in which the data should be collected.

Create

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/

Create

Step 3 – Add ISE inputs

Application Setup **Search** 

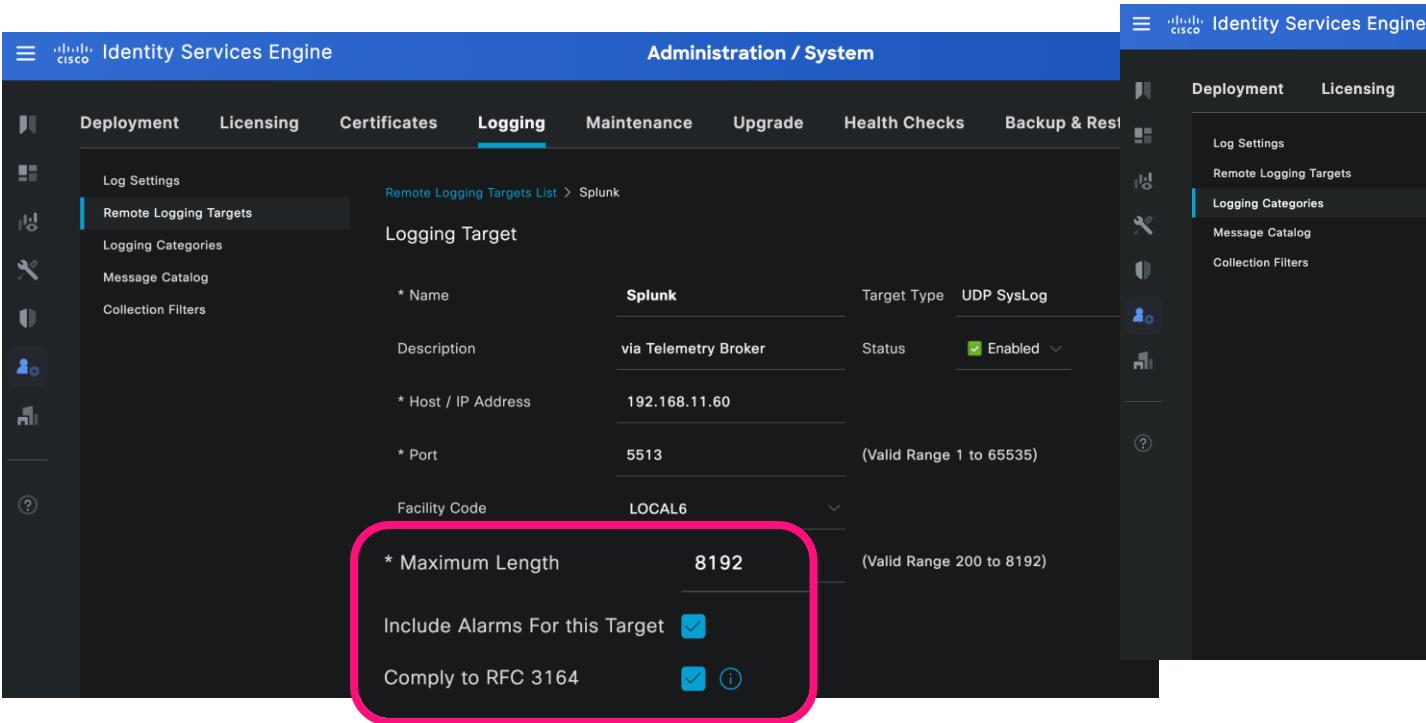
Application Setup

My Apps

	Input Name	Product	Account	Enabled	Status	Source Type	Index	⋮
>	splunkISE	Identity Services Engine (ISE)	splunkise11	<input checked="" type="checkbox"/>	Connected	-	catalyst	<input type="button" value="⋮"/>
>	5513	Identity Services Engine (ISE)	-	<input checked="" type="checkbox"/>	-	cisco:ise:syslog	catalyst	<input type="button" value="⋮"/>

Identity Services Engine Logging to Splunk

Remote Targets and Logging Categories



ISE Administration / System - Logging

Logging Target

- Name:** Splunk
- Description:** via Telemetry Broker
- Status:** Enabled
- Host / IP Address:** 192.168.11.60
- Port:** 5513
- Facility Code:** LOCAL6
- Maximum Length:** 8192
- Include Alarms For this Target:**
- Comply to RFC 3164:** [Info](#)

Targets

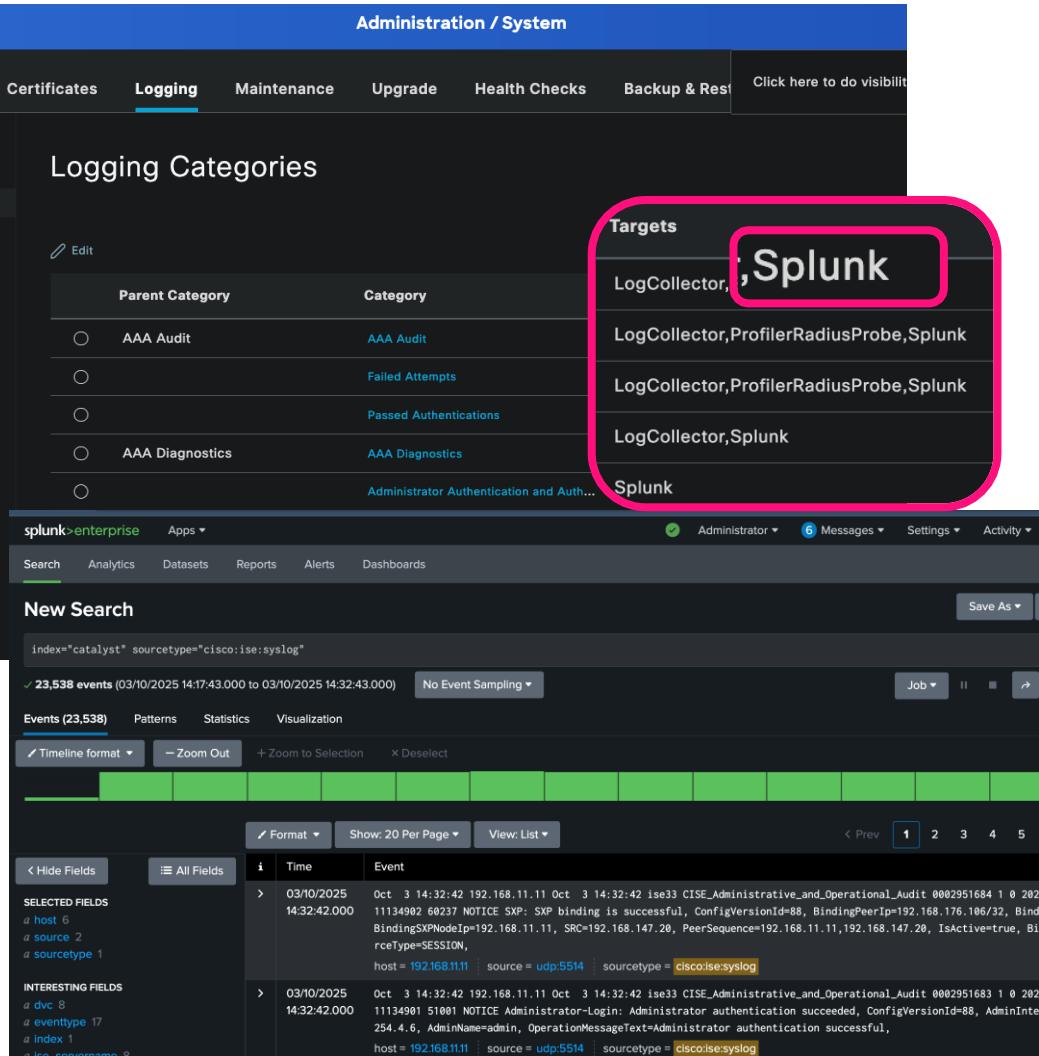
- LogCollector, Splunk
- LogCollector, ProfilerRadiusProbe, Splunk
- LogCollector, ProfilerRadiusProbe, Splunk
- LogCollector, Splunk
- Splunk

Remote Logging Target

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

Logging Category

- Add Splunk Remote Logging Target to Logging Categories



Logging Categories

Parent Category	Category
AAA Audit	AAA Audit
	Failed Attempts
	Passed Authentications
AAA Diagnostics	AAA Diagnostics
	Administrator Authentication and Auth...

New Search

index=catalyst sourcetype=cisco:ise:syslog

23,538 events (03/10/2025 14:17:43.000 to 03/10/2025 14:32:43.000) No Event Sampling

Events (23,538) Patterns Statistics Visualization

Format Show: 20 Per Page View: List

Time	Event
03/10/2025 14:32:42	Oct 3 14:32:42 192.168.11.11 Oct 3 14:32:42 ise33 CISE_Administrative_and_Operational_Audit 0002951683 1 0 202 11134902 60237 NOTICE SXP: SXP binding is successful, ConfigVersionId=88, BindingPeerIp=192.168.176.106/32, BindingSXPNodeIp=192.168.11.11, SRC=192.168.147.20, PeerSequence=192.168.11.11,192.168.147.20, IsActive=true, BrcType=SESSION, host = 192.168.11.11 source = udp:5514 sourcetype = cisco:ise:syslog

Selected Fields: host, source, sourcetype

Interesting Fields: dvc, eventtype, index, ise_servername

SD-WAN

Catalyst App – SD-WAN

Send SD-WAN Data to Splunk

Add Cisco Catalyst SDWAN Account

*Account Name
splunksdwan
Enter a unique name for this account.

*IP Address/Hostname
https://10.67.28.103
Enter the IP Address of the SDWAN in format https://<ip address> or https://<host-name>

*Username
splunk
Enter the username for this account.

*Password
.....
Enter the password for this account.

Use Custom CA Certificate

Enable Proxy

Cancel **Add**

Cisco Catalyst SDWAN

Syslog

*Input Type
 UDP
 TCP

*Port
5515
Enter the Port for this input.

Only accept connection from
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com (if not set, accepts connections from all hosts).

*Input Source Type
cisco:firewall:logs

Select the relevant source type for your input.

*Index
catalyst
Select the index in which the data should be collected.

Cancel **Create**

Catalyst App – SD-WAN

Send SD-WAN Data to Splunk

 **Cisco Catalyst SDWAN**

Inputs **Syslog** **Configuration**

Input Type
Unified Threat Defense/Link Details

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

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

***Index**
catalyst

***Cisco SDWAN Account**
splunksdwan

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

***Health Type**
 Unified Threat Defense Health Link Health

Create

 **Cisco Catalyst SDWAN**

Inputs **Syslog** **Configuration**

Input Type
Site/Tunnel Details

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

***Interval**
3600
Data will be fetched every hour for Sites and Tunnel Details.

***Index**
catalyst

***Cisco SDWAN Account**
splunksdwan

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

***Health Type**
 Site Health Tunnel Health SSE Tunnels

Cancel

Step 3 – Add SD-WAN inputs

 **Application Setup**

My Apps

Input Name	Product	Account	Enabled	Status	Source Type	Index	⋮
UnifiedThreats	SDWAN	splunksdwan	<input checked="" type="checkbox"/>	Connected	-	catalyst	⋮
SiteTunnel	SDWAN	splunksdwan	<input checked="" type="checkbox"/>	Connected	-	catalyst	⋮
5515	SDWAN	-	<input checked="" type="checkbox"/>	-	cisco:firewall:logs	catalyst	⋮



SD-WAN Logging to Splunk

Custom syslog port and NetFlow for Splunk

The screenshot shows the Catalyst SD-WAN interface. A prominent red warning box at the top states: "The network is out of compliance due to licensing, [click here](#) for more a...". The main content area is titled "DC_CLI_Template" and shows the following details:

- Description: Trustsec/logging to SDA Border
- Device solution: SD-WAN
- Updated by: jeff12
- Last updated: Sep 13, 2025

On the left, a sidebar lists various monitoring and configuration tools: Monitor, Configuration, Analytics, Workflows, and Tools. The "Tools" section contains a "CLI Configuration" section with the following configuration:

```
1 logging host 192.168.11.60 vrf 101 transport udp port 5515
2
3 !
```

The screenshot shows the "Global" configuration page in Catalyst SD-WAN. The "Collectors" tab is selected. The "Cflowd" section is active, with a table for "Collector Server (Maximum: 4)". The table shows one entry:

VPN ID	IPv4/IPv6 Address	UDP Port	Export Spreading (optional)	BFD Metrics Exporting (optional)	Exporting Interval (optional)	Action
101	192.168.11.60	9995	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	60	⋮

Syslog

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

NetFlow

- Add Cflowd collector address as Splunk

Enterprise Networking App – SD-WAN Dashboards

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

index=catalyst sourcetype="cisco:sdwan:*"

538 of 538 events matched No Event Sampling ▾

Save As ▾

Events (538) Patterns Statistics Visualization

Timeline format ▾ – Zoom Out + Zoom to Selection × Deselect

Format ▾ Show: 20 Per Page ▾ View: List ▾

◀ Hide Fields ▶ All Fields

SELECTED FIELDS

- a host 5
- a source 3
- a sourcetype 2

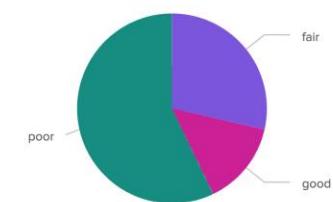
INTERESTING FIELDS

- a af-type 2
- a auto-downstream-bandwidth 1
- a auto-neg 1
- a auto-negotiate 2
- a auto-upstream-bandwidth 1
- a bia-address 46
- # bw-down-util 3
- # bw-up-util 1
- # bytes_in 100+
- # bytes_out 100+
- a duplex 1
- a dvc_ip 13
- a encap-type 1

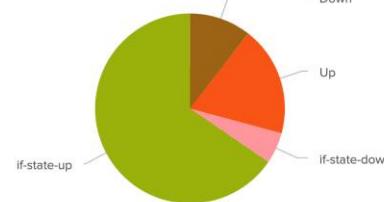
Time Event

> 03/10/2025 16:13:25.000 { [-]
auto-downstream-bandwidth: N/A
auto-upstream-bandwidth: N/A
bia-address: 00:00:00:00:00:00
hwaddr: 58:f3:9c:a7:74:30
if-admin-status: if-state-up
if-oper-status: if-oper-state-ready
ifindex: 17
ifname: vmanage_system
interface-type: iana-iftype-sw-loopback
ip-address: 0.0.0.0
ipv4-subnet-mask: 255.255.255.255
ipv4-tcp-adjust-mss: 0
ipv6-tcp-adjust-mss: 0
lastupdated: 1759470824099
mtu: 0
num-flaps: 0
rx-drops: 0
rx-errors: 0

Cisco SD-WAN Site Health



Cisco SD-WAN Link Health



Cisco SD-WAN Link Health Details

Device Name Search

Data Key	Last Updated	Device Name	Admin Status	IP Address	Received Bytes	Transmit Bytes	Receive Rate(Kbps)	Transmit Rate(Kbps)	Received Packets	Transmit Packets	Count
10.0.0.1-0-GigabitEthernet4-0.0.0.0-52:54:00:9a:d9:53	Oct 03, 2025 04:14:46 PM	10.0.0.1	if-state-up	0.0.0.0	0	0	0	0	0	0	1
10.0.0.1-0-GigabitEthernet5-0.0.0.0-52:54:00:02:e2:7e	Oct 03, 2025 04:14:46 PM	10.0.0.1	if-state-up	0.0.0.0	0	0	0	0	0	0	1
10.0.0.1-0-GigabitEthernet6-0.0.0.0-52:54:00:b7:27:b4	Oct 03, 2025 04:14:46 PM	10.0.0.1	if-state-up	0.0.0.0	0	0	0	0	0	0	1
10.0.0.1-0-GigabitEthernet7-0.0.0.0-52:54:00:1a:3d:58	Oct 03, 2025 04:14:46 PM	10.0.0.1	if-state-up	0.0.0.0	0	0	0	0	0	0	1

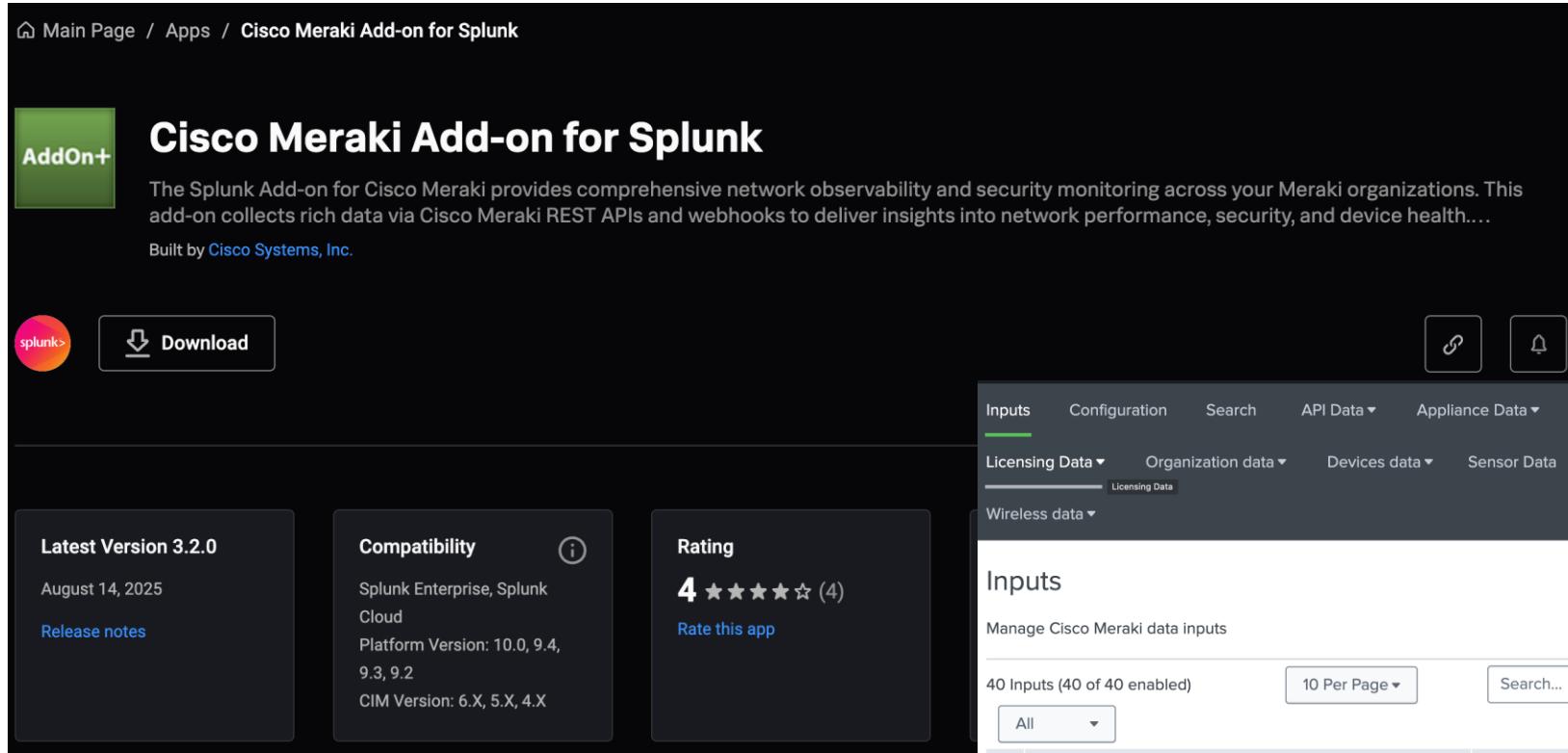
© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOPS-1233

CISCO

Meraki Add-On

Meraki Add-On for Splunk



Main Page / Apps / Cisco Meraki Add-on for Splunk

Cisco Meraki Add-on for Splunk

The Splunk Add-on for Cisco Meraki provides comprehensive network observability and security monitoring across your Meraki organizations. This add-on collects rich data via Cisco Meraki REST APIs and webhooks to deliver insights into network performance, security, and device health....

Built by [Cisco Systems, Inc.](#)

 [Download](#)

[Inputs](#) [Configuration](#) [Search](#) [API Data](#) [Appliance Data](#) [Assurance Alert Data](#) [Camera Data](#)

[Licensing Data](#) [Organization data](#) [Devices data](#) [Sensor Data](#) [Summary data](#) [Switch data](#)

[Wireless data](#)

Inputs

Manage Cisco Meraki data inputs

Name	Organization	Interval	Index	Status	Actions
accesspoints_Meraki	Meraki	86400	meraki	Active	  
airmarshal_Meraki	Meraki	86400	meraki	Active	  
api_request_history_Meraki	Meraki	360	meraki	Active	  
api_request_overview_Meraki	Meraki	86400	meraki	Active	  
api_request_response_code_Meraki	Meraki	86400	meraki	Active	  
appliance_vpn_stats_Meraki	Meraki	86400	meraki	Active	  

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

Meraki Add-On for Splunk – Indexes and Search Macro

Add dedicated Maraki index

New Index

General Settings

Index Name: meraki
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/na...

Data Integrity Check: Enable
Enable this if you want Splunk to compute hashes on every slice of your data for...

Max Size of Entire Index: 500
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume inde...

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive...

App: Splunk Add-on for Cisco Meraki

Save **Cancel**

Step 1 – Create Meraki index

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

splunk>enterprise Apps ▾ Administrator ▾ 6

Search macros

Advanced search » Search macros

Showing 1-1 of 1 item

App	Configuration Source	Owner
Splunk Add-on for Cis...	Visible in the App	Any

Name	Definition	Arguments	Owner	App
meraki_index	index IN(meraki)		No owner	Splunk_TA_cisco_meraki

Meraki Add-On for Splunk – Add Organization

Add Meraki credential information

Add Organization X

*Organization Name Enter a unique name for this Meraki organization.

*Service region Select Service region (Global is preselected)

*Base URL Enter base url for meraki. eg. https://api.meraki.com

*Organization ID Enter Organization ID.

*Organization API Key Enter Organization API Key.

*Max API calls per second Enter maximum api calls per second for the Organization

Create inputs automatically? Selecting this option will automatically create inputs for all input types (except Webhook) in disabled mode. The inputs will follow the default naming convention: <input_type>_<account_name>.

Index An index is a type of data repository. Select the index in which you want to collect the events.

Step 3 – Add Meraki Organization ID and API key

Meraki Add-On for Splunk - Add Inputs

splunk>enterprise Apps ▾

Administrator ▾ 6 Messages ▾ Settings ▾ Activity ▾

Inputs Configuration Search API Data ▾ Appliance Data ▾ Assurance Alert Data Camera Data

Licensing Data ▾ Organization data ▾ Devices data ▾ Sensor Data

Wireless data ▾

Inputs Configuration Search API Data ▾ Appliance Data ▾ Assurance Alert Data Camera Data Licensing Data ▾ Organization data ▾

Splunk Add-on for Cisco Meraki

Sensor Data

Time Organization Id

Last 30 days All Hide Filters

Average Temperature

Temperature (°C)

Wed Sep 3 Fri Sep 5 Sun Sep 7 Tue Sep 9 Thu Sep 11 Sat Sep 13 Mon Sep 15 Wed Sep 17 Fri Sep 19 Sun Sep 21 Tue Sep 23 Thu Sep 25 Sat Sep 27 Mon Sep 29 Wed Oct 1

Average Noise Level

Noise Level

Devices data ▾ Sensor Data ▾ Summary data ▾ Switch data ▾ Wireless data ▾

Device Uplink Addresses

Time Organization Id

Last 24 hours All Hide Filters

Search produced no results.

Devices Uplinks History

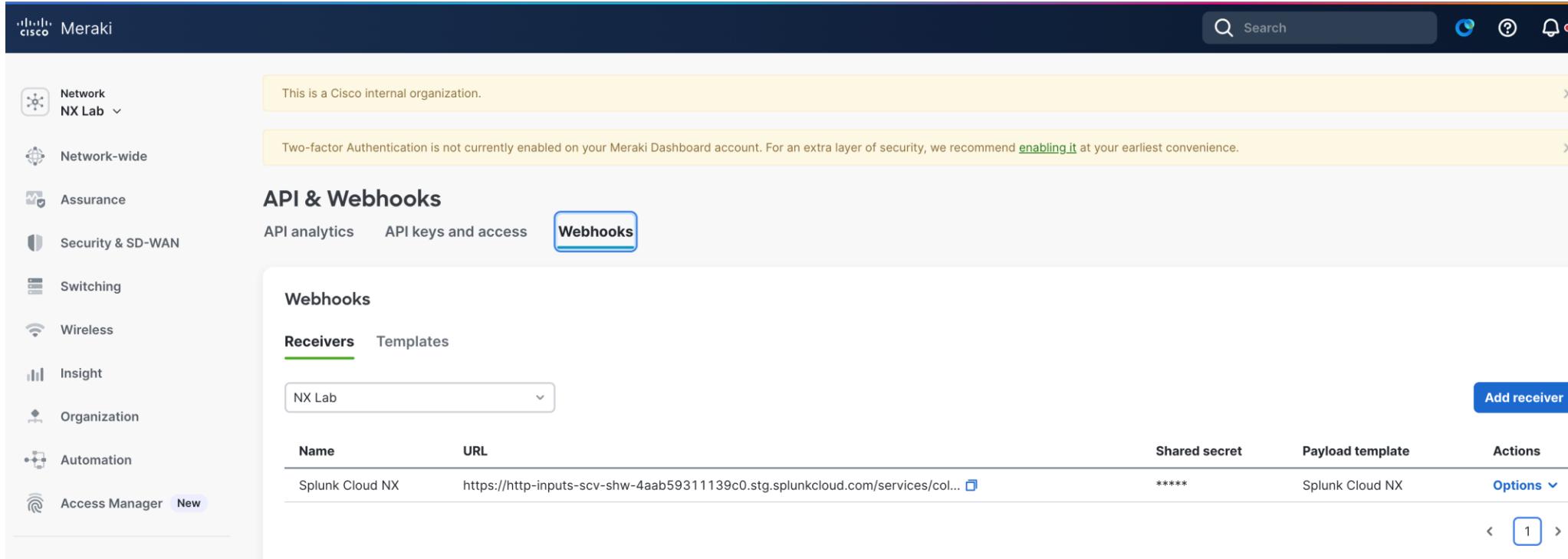
Device Name ▾	Device Serial ▾	Interface ▾	Uplink Address ▾	Assignment Mode ▾	Address Gateway ▾	Address Protocol ▾
site7-64:00	Q3EF-DZBK-UL5D	man1	192.168.254.94	static	192.168.254.89	ipv4
site6-9f:00	Q3EF-AJP9-TV4C	man1	192.168.254.86	static	192.168.254.81	ipv4
MS	Q2SX-4V76-Z6VP	man1	172.31.128.5 2001:8004:15a0:f96:fa9e:28ff:fe26:a299	dynamic dynamic	172.31.128.1 fe80::2e3f:bff:fec1:397f	ipv4 ipv6

BRKOPS-1233

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO

Meraki Add-On for Splunk – Webhooks



The screenshot shows the Meraki Dashboard interface. The left sidebar includes links for Network (selected), Network-wide, Assurance, Security & SD-WAN, Switching, Wireless, Insight, Organization, Automation, and Access Manager (with a 'New' badge). The main content area is titled 'API & Webhooks' with tabs for API analytics, API keys and access, and Webhooks (selected). A yellow banner at the top states 'This is a Cisco internal organization.' and another below it encourages enabling two-factor authentication. The 'Webhooks' section shows a 'Receivers' tab selected, with a dropdown set to 'NX Lab' and a 'Templates' tab. A table lists a single receiver: 'Splunk Cloud NX' with URL 'https://http-inputs-scv-shw-4aab59311139c0.stg.splunkcloud.com/services/col...'. The table includes columns for Name, URL, Shared secret (*****), Payload template (Splunk Cloud NX), and Actions (Options). A page number '1' is shown in the bottom right of the table.

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

The screenshot shows the Splunk Cloud interface. On the left, the 'HTTP Event Collector' page displays a table with one row: 'meraki-webhook' (Actions: Edit, Disable, Copy, Show). On the right, the 'API & Webhooks' page shows a 'Webhooks' section with a 'View Template' form. The 'Template Name' is 'Splunk Cloud NX'. The 'Liquid Body' tab is selected, showing a JSON template with numbered lines. The template content is as follows:

```
1 "sourcetype": "meraki:webhook",
2 "event": {
3     "version": "0.1",
4     "sentAt": "{{sentAt}}",
5     "organizationId": "{{organizationId}}",
6     "organizationName": "{{organizationName}}",
7     "organizationUrl": "{{organizationUrl}}",
8     "networkId": "{{networkId}}",
9     "networkName": "{{networkName}}",
10    "networkUrl": "{{networkUrl}}",
11    "networkTags": {{ networkTags | jsonify }},
12    "deviceSerial": "{{deviceSerial}}",
13    "deviceMac": "{{deviceMac}}",
14    "deviceName": "{{deviceName}}",
15    "deviceUrl": "{{deviceUrl}}",
16    "deviceTags": {{ deviceTags | jsonify }},
17    "deviceModel": "{{deviceModel}}",
18 }
```

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

The screenshot shows the Meraki API & Webhooks interface. In the top navigation bar, 'API & Webhooks' is selected, with 'Webhooks' being the active sub-section. Below this, there are links for 'API analytics', 'API keys and access', and 'Webhooks'. The main content area is titled 'Webhooks' and shows 'Receivers' and 'Templates' tabs. Under 'Templates', a 'Create Template' section is shown with a 'Template Name' field containing 'Splunk Cloud NX'. Below this, there are tabs for 'Liquid Body', 'Liquid Headers' (which is selected), and 'Webhook Data'. The 'Liquid Headers' tab shows a list with an item 'Splunk {{sharedSecret}}' highlighted with a red box. To the right, a 'Generate Preview →' button and a 'Preview' section with a JSON preview of the header are visible. Below the preview, there are tabs for 'access' and 'Webhooks', with 'Webhooks' being the active tab. The 'Webhooks' section shows a 'Receivers' tab selected, with a dropdown menu showing 'NX Lab' and a 'Templates' tab. At the bottom, there is a table with columns 'Name', 'URL', 'Shared secret', 'Payload template', and 'Actions'. A row in the table shows 'Splunk Cloud NX' as the name, the URL 'https://http-inputs-scv-shw-4aab59311139c0.stg.splunkcloud.com/services/collector/event' as the URL, 'HEC TOKEN' as the shared secret, 'Splunk Cloud NX' as the payload template, and 'Save' and 'Cancel' buttons in the actions column.

Step 3 – Create a liquid header template

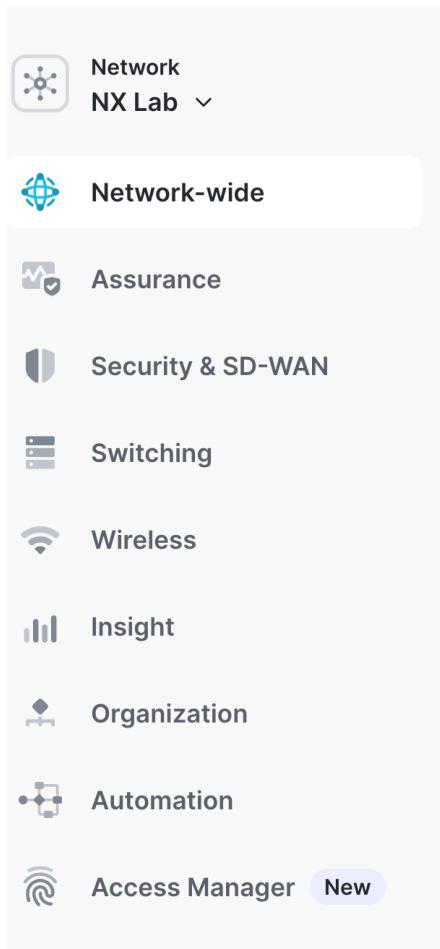
- The Header Value must contain the text **Splunk {{sharedSecret}}**

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



Alerts

Alerts Settings

Default recipients

Webhook: Splunk Cloud NX x

+

Network-wide

Configuration settings are changed

+ Show additional recipients

A VPN connection comes up or goes down ⓘ

+ Show additional recipients

A rogue access point is detected

+ Show additional recipients

Network usage exceeds GB in

+ Show additional recipients

Step 5 – Subscribe to Network-wide Alerts

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

Meraki Webhook Searching

The image displays two side-by-side screenshots of the Splunk Cloud interface, showing search results for Meraki webhook data.

Left Screenshot (Search Results):

- Search Bar:** index=meraki source="http:meraki-webhook" alertLevel=critical networkName!="8*" | stats count by networkName
- Event Count:** 9 events (20/10/2025 01:56:00.000 to 20/10/2025 05:56:55.000)
- Visualization:** A bar chart showing the count of events by networkName. The x-axis is networkName (NX Lab, L14 Lab) and the y-axis is count (0 to 10). The NX Lab bar is large (approx. 8.5) and the L14 Lab bar is small (approx. 1).
- Search Bar (Below Visualization):** index=meraki source="http:meraki-webhook" alertLevel=critical networkName!="8*" | stats count by networkName

Right Screenshot (Event Details):

- Search Bar:** index=meraki source="http:meraki-webhook"
- Event Count:** 6 events (20/10/2025 03:15:00.000 to 20/10/2025 04:15:37.000)
- Event List:** A table showing event details for 6 events. The table has columns: i (Icon), Time, and Event.
- Selected Fields:** host 1, source 1, sourcetype 1
- Interesting Fields:** alertData.changes.globalRecipients.changedBy 1, alertData.changes.globalRecipients.label 1, alertData.changes.globalRecipients.newText 3, alertData.changes.globalRecipients.oldText 1, alertData.changes.globalRecipients.ssid 1, alertData.name 1, alertData.num 1, alertData.url 1, alertData.userId 1

i	Time	Event
>	20/10/2025 04:14:32.000	{ [-] alertData: { [+] } alertId: 683984193453625552 alertLevel: informational alertType: Settings changed alertTypeId: settings_changed deviceMac: deviceModel: deviceName: deviceSerial: deviceTags: [[+]] deviceUrl: networkId: L_683984193406917795 networkName: L14 Lab networkTags: [[+]] networkUrl: https://n215.dashboard.meraki.com/L14-La occurredAt: 2025-10-20T04:04:31.693662Z

ThousandEyes Add-On

ThousandEyes Add-On for Splunk

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

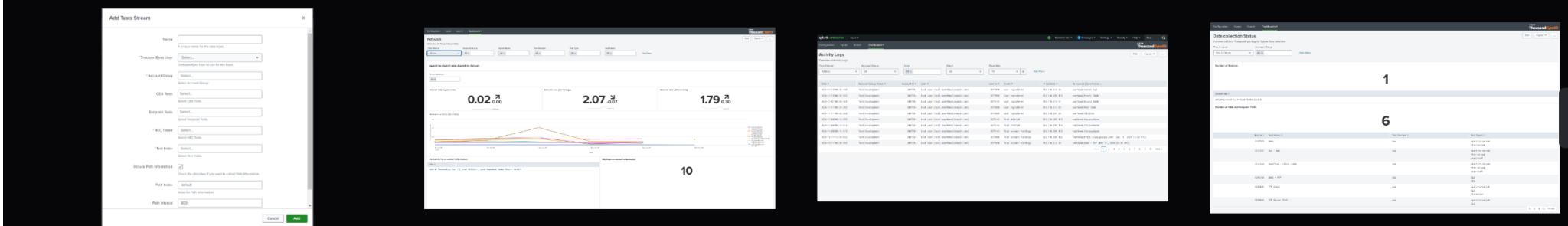
>Main Page / Apps / Cisco ThousandEyes App for Splunk

Cisco ThousandEyes App for Splunk

The ThousandEyes App For Splunk enables organizations to collect and analyze CEA (Cloud and Enterprise Agent) and Endpoint test results data, Event and Activity logs. Integrated with Splunk, it provides visibility into the health and performance of IT systems, applications, and network...

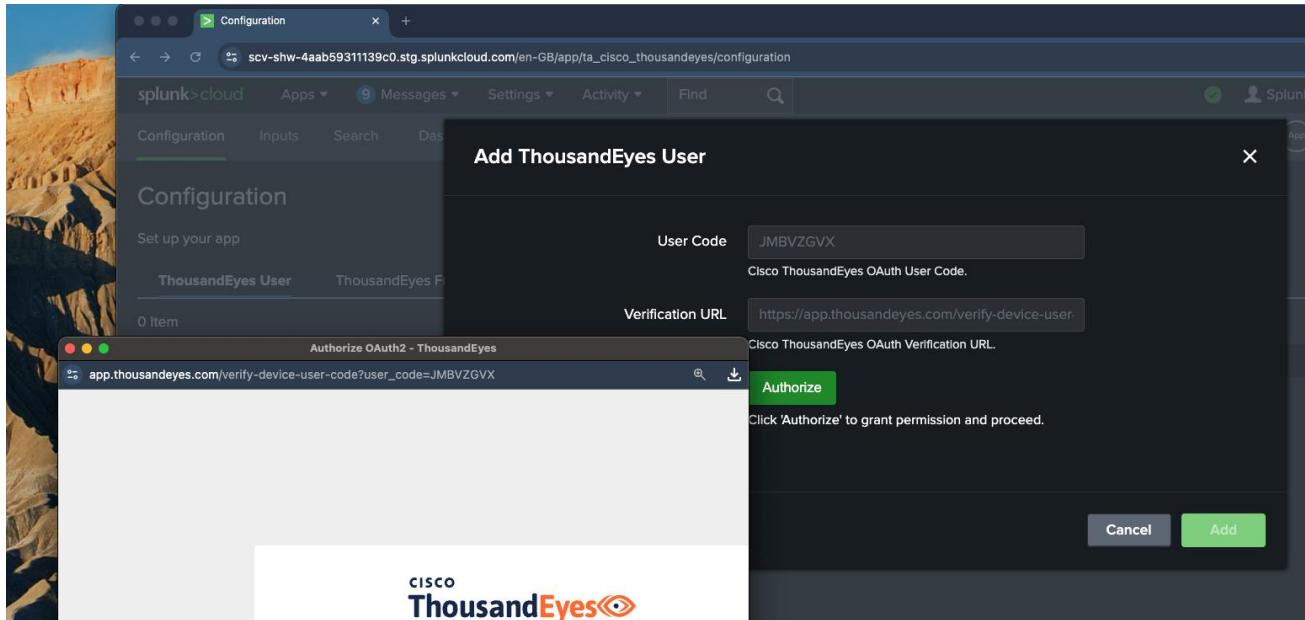
Built by Cisco Systems, Inc.

 [Download](#)  



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

Add ThousandEyes Account

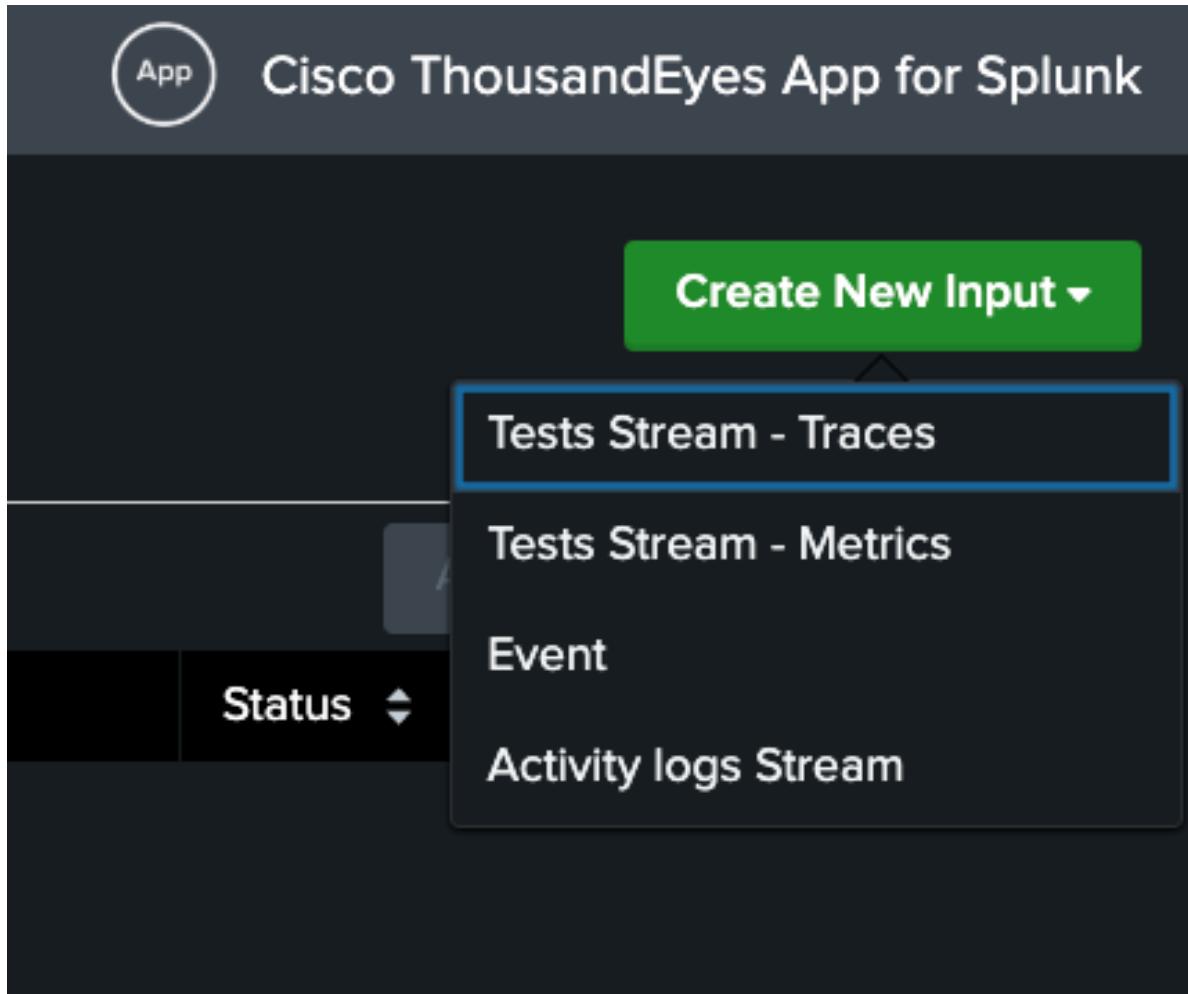


Step 1 – Add ThousandEyes User

Step 2 – Add HTTP Event Collector for ThousandEyes in Splunk

Name	Actions	Token Value	Source Type	Index	Status
victoriahec	Edit Disable Delete Copy Hide	bc77efcf-fc60-494f-b80c-52701d7901d4	main		Enabled

ThousandEyes Add-On for Splunk - Add Inputs



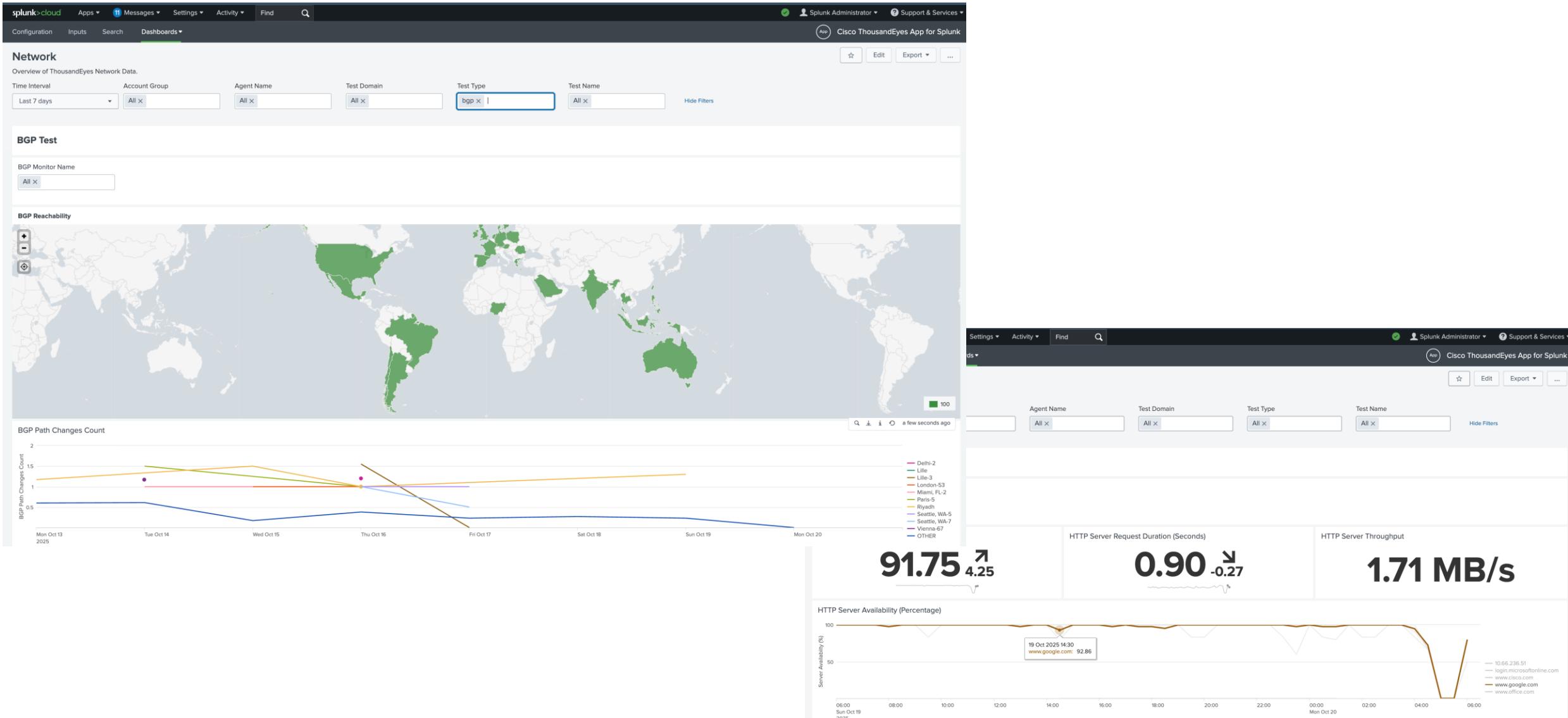
Step 3 - Add ThousandEyes Inputs and select tests

The image shows the 'Update Tests Stream - Traces' configuration dialog. It has a dark background with white text and input fields. The fields are as follows:

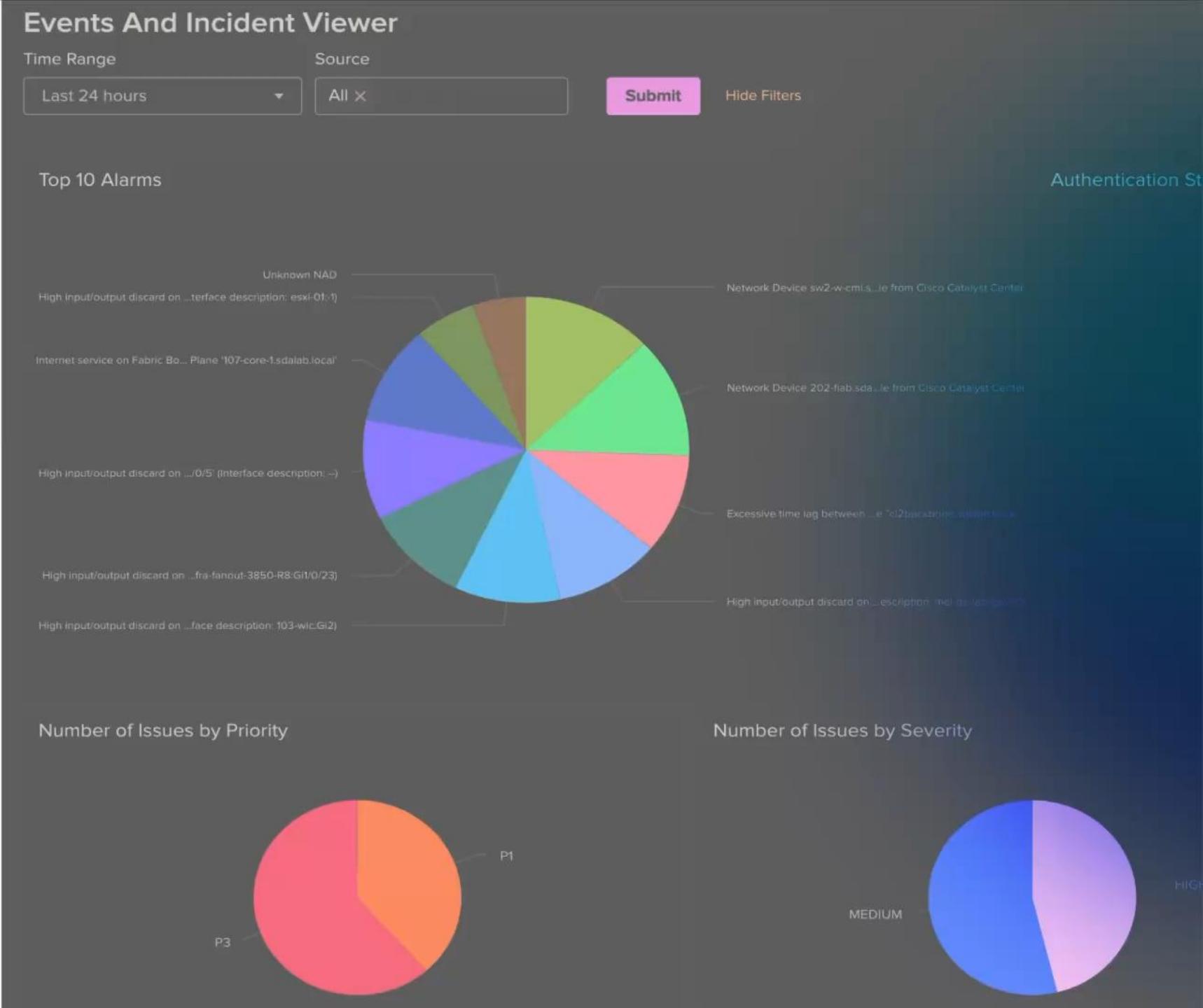
- Name:** traces (highlighted with a blue box)
- ThousandEyes User:** jeffl2@cisco.com
- Account Group:** jeffl2 (217336)
- Tags:** Google:Google, MTeams:MTeams, Zoom:Zoom
- Cloud & Enterprise Agent Tests:** https://www.cisco.com (7749456 | page-load...)
- HEC Target:** https://http-inputs-scv-shw-474714c1af0e16.sp (highlighted with a blue box)
- HEC Token:** victoriahec
- Test Index:** main

At the bottom right, there are 'Cancel' and 'Update' buttons. A blue box highlights the 'Name' field and the 'HEC Target' field.

ThousandEyes Add-On for Splunk - Dashboards



Demo – Splunk Enterprise Networking

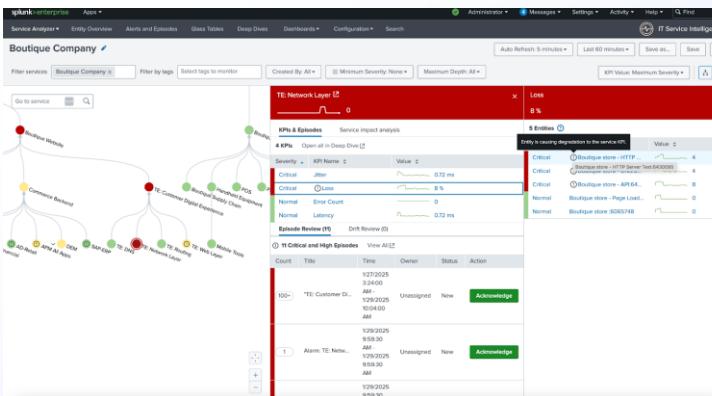


Splunk IT Service Intelligence (ITSI)

Introduce Intelligence with Splunk ITSI

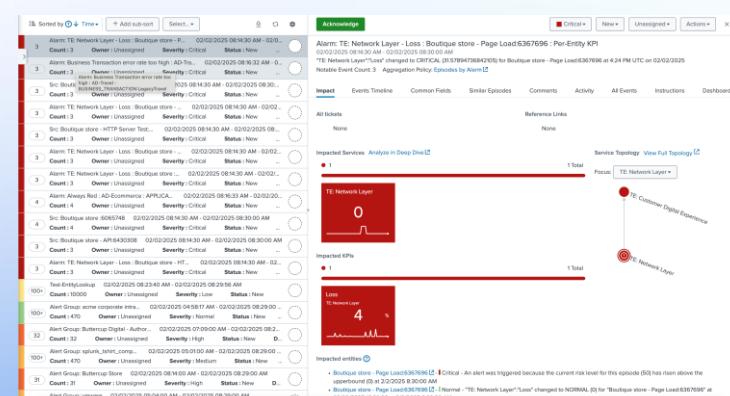
Complete Business Visibility

Eliminate **fragmented visibility** with a single view and accelerate RCA



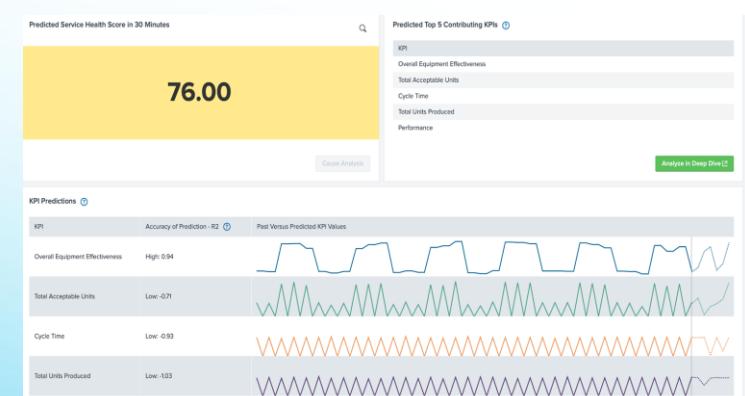
Intelligent Incident Management

Accelerate MTTR using real-time event correlation and automated prioritization



Proactive Incident Prevention

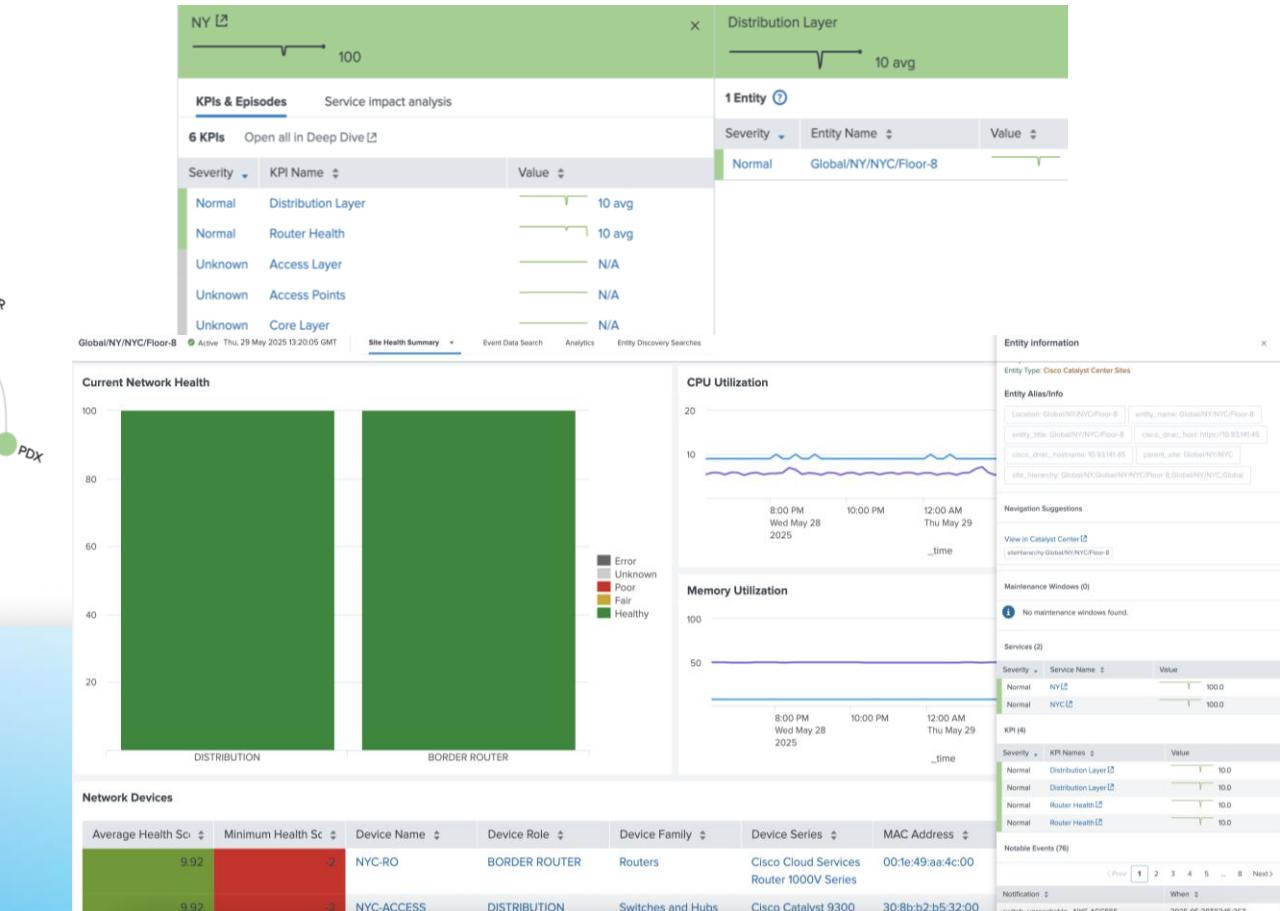
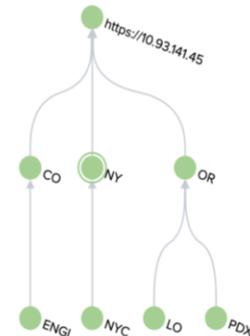
Detect anomalies and **predict** issues **30 mins earlier** for outage prevention



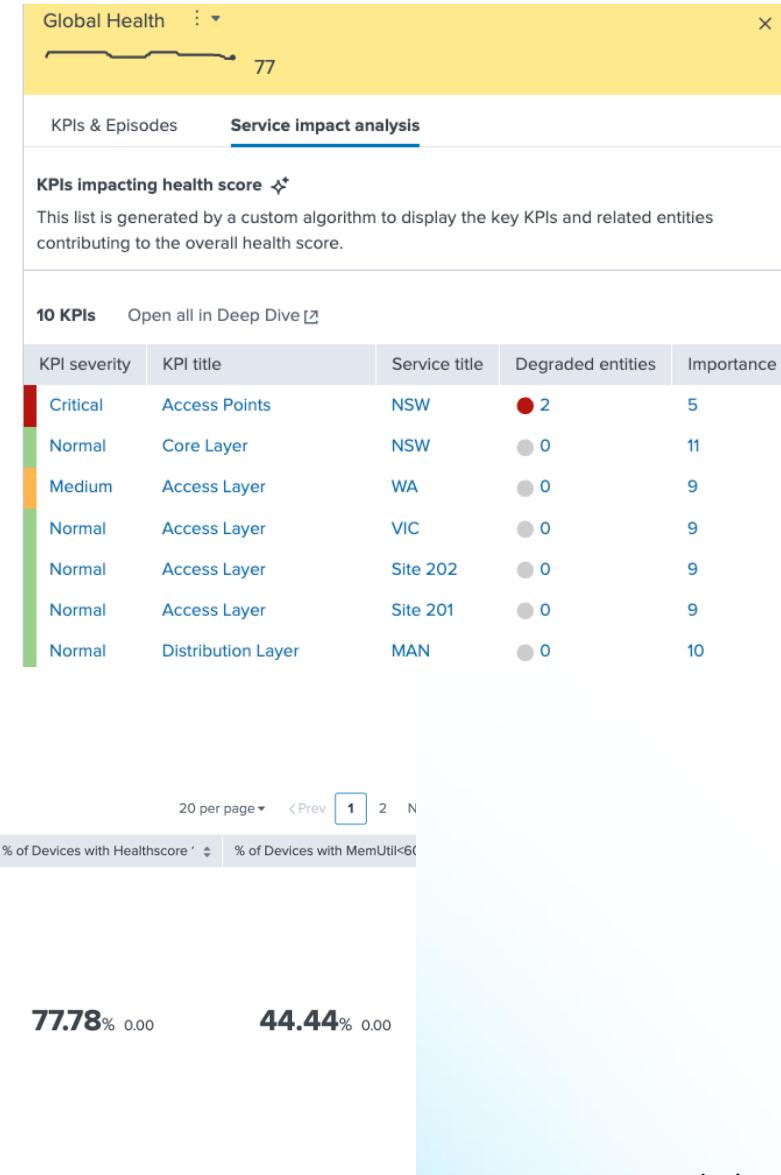
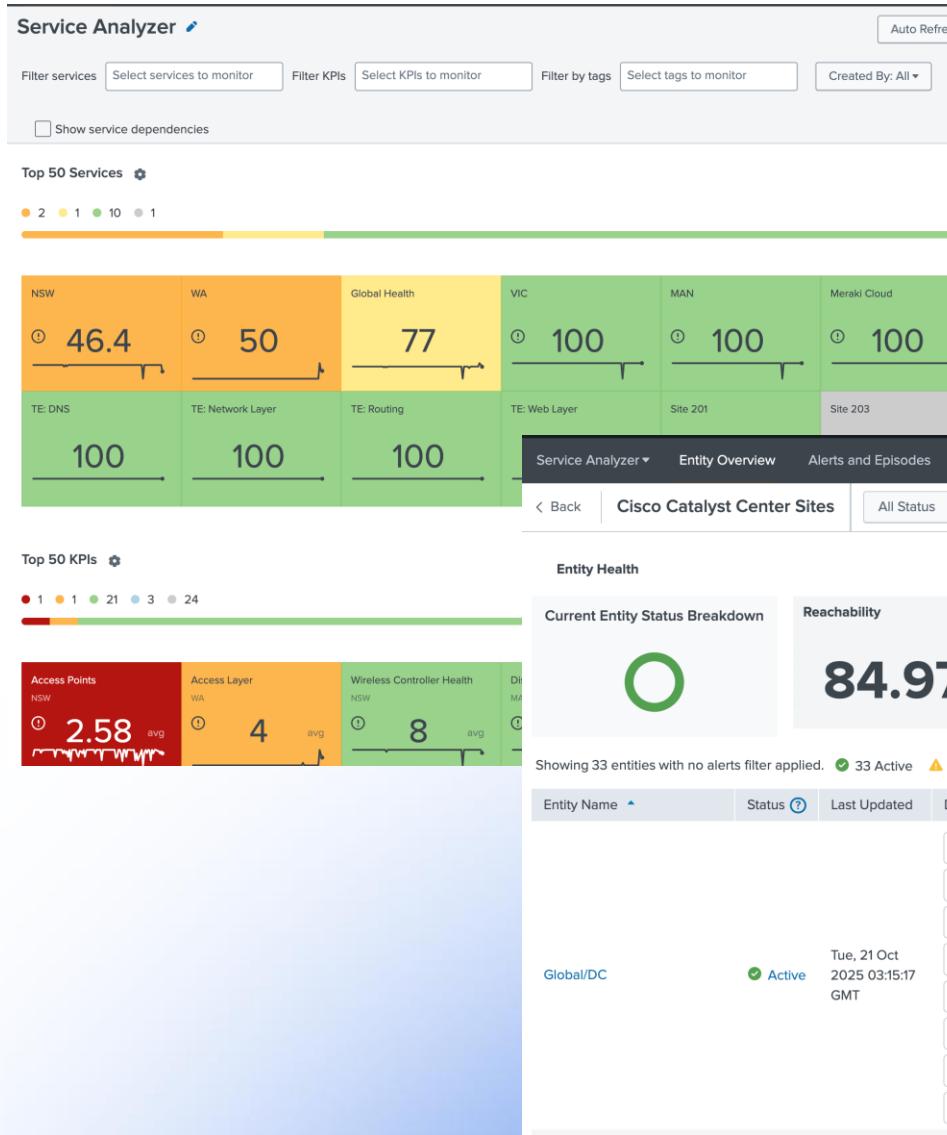
Splunk ITSI and Catalyst Center Integration

Quickly pinpoint site & device issues in the network with:

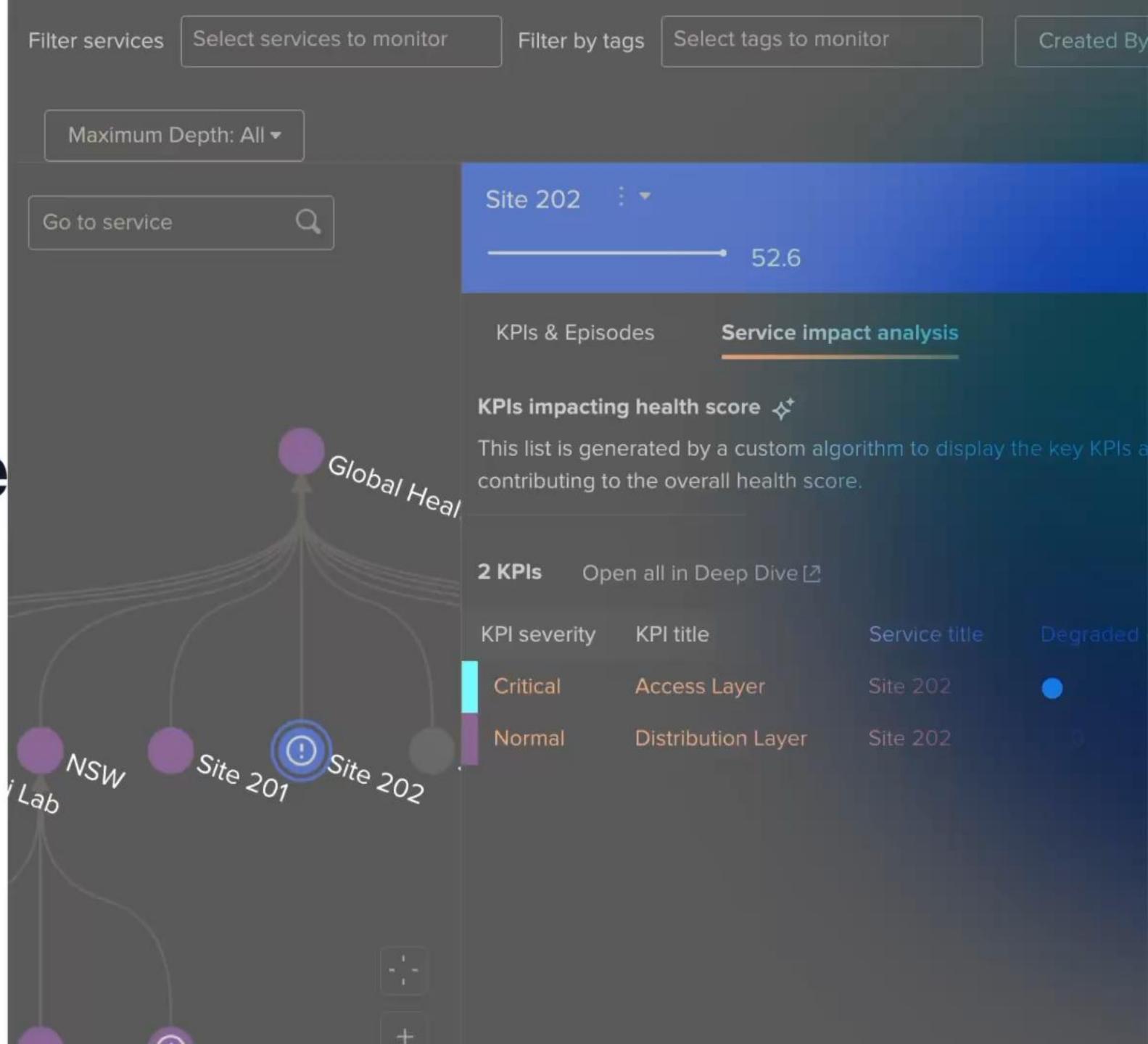
- Site-based dependency mapping for problem isolation
- KPIs and entity models to measure site health incl. core, distribution, and access layers
- Easy alert normalization, deduplication and correlation
- Health visualization of site floors or localized areas to pinpoint unhealthy devices
- In-context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

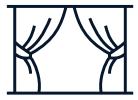


Level up and earn exclusive prizes!



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 Live !

