

Splunk for Network Engineers

cisco Live !

Catalyst, Meraki, ISE, ThousandEyes and ITSI

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

Session ID: BRKOPS-1233

Cisco Webex App

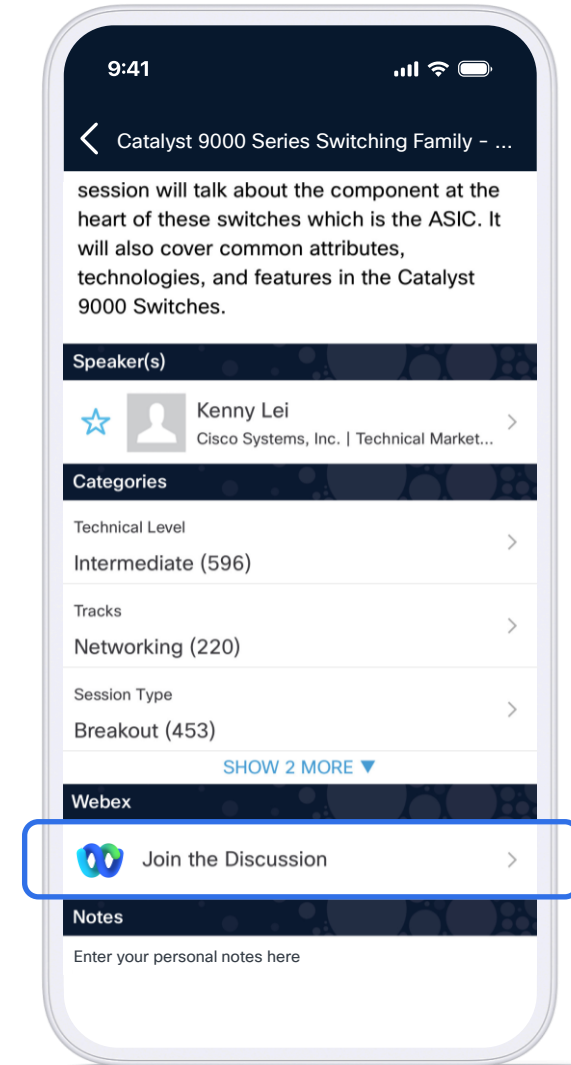
Questions?

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

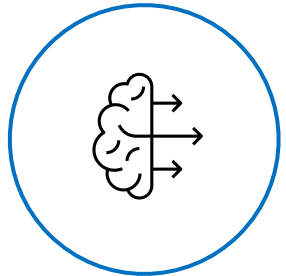
- Network Engineers/Operators
- Generally familiar with Catalyst Center, Identity Services Engine, SD-WAN and Meraki
- Less familiar with Thousand Eyes
- Even less familiar with Splunk
- Probably never heard of ITSI

Why Splunk?



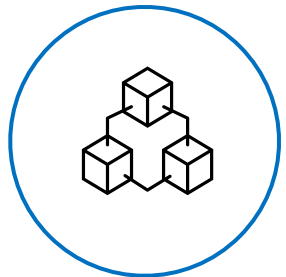
Consolidated Dashboard

- 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

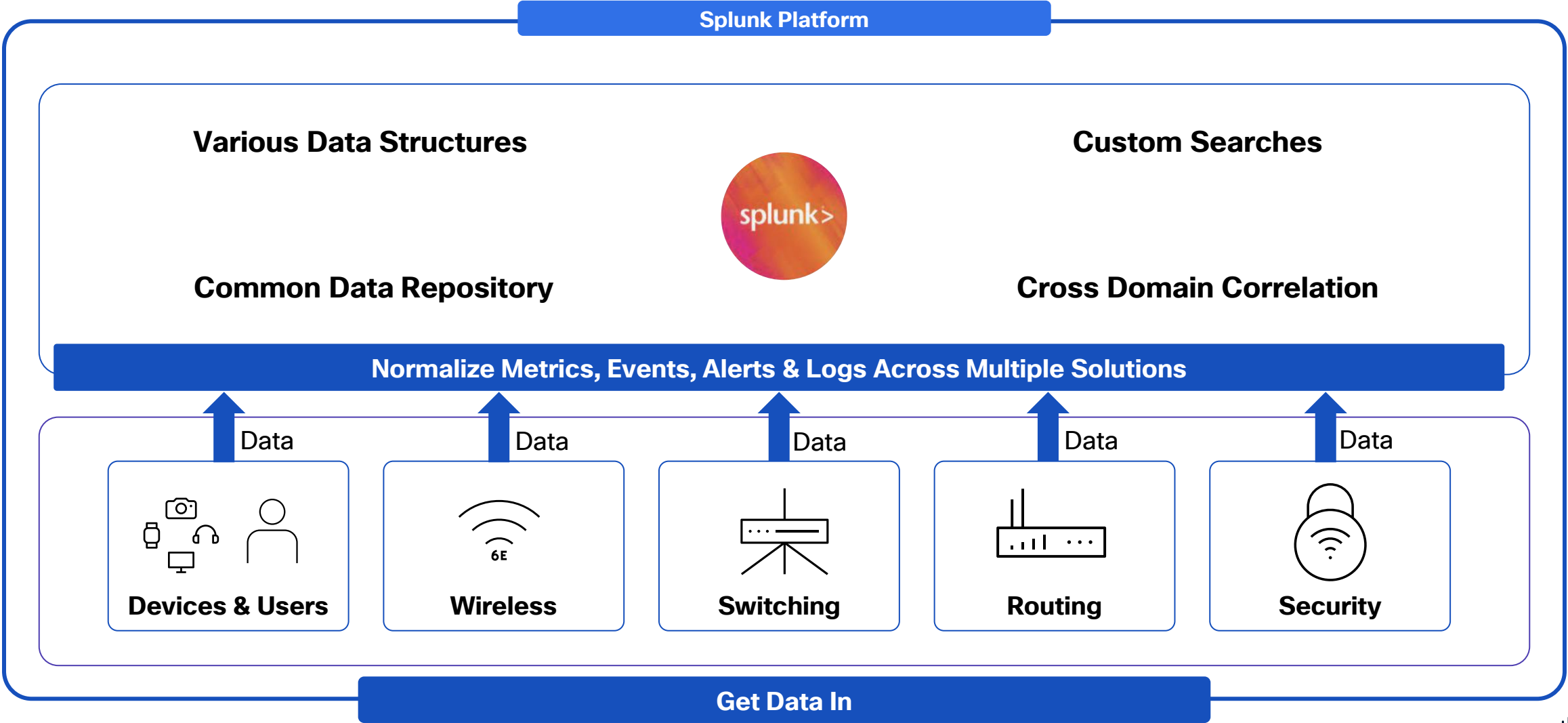
Faster RCA

Data Correlation

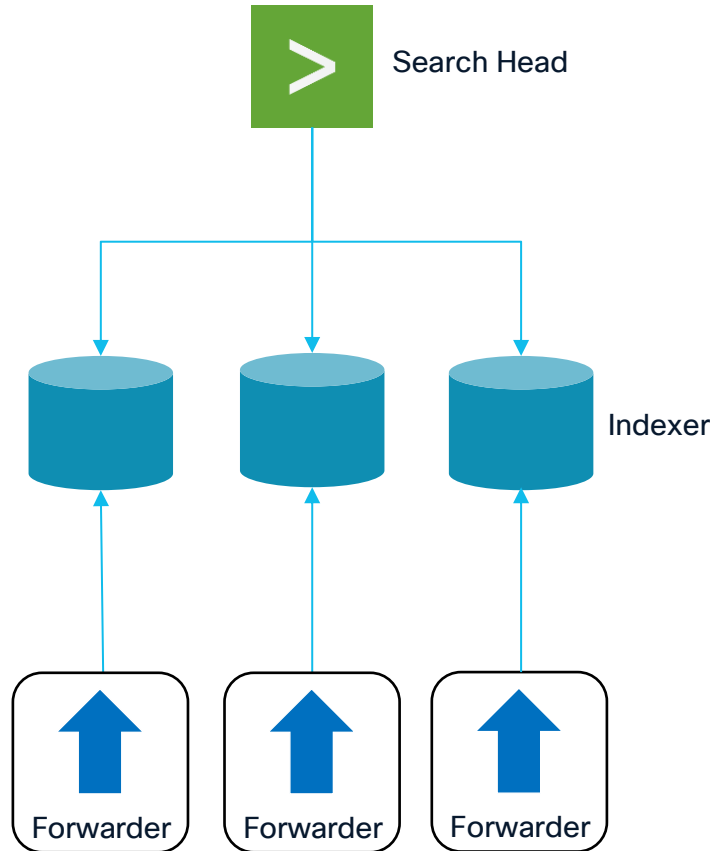
Artificial Intelligence

Getting Data to Splunk

Various Data Structures | Common Repository | Custom Searches



Splunk – Main Components



Search Head

- Handles search requests and consolidating results back to the user

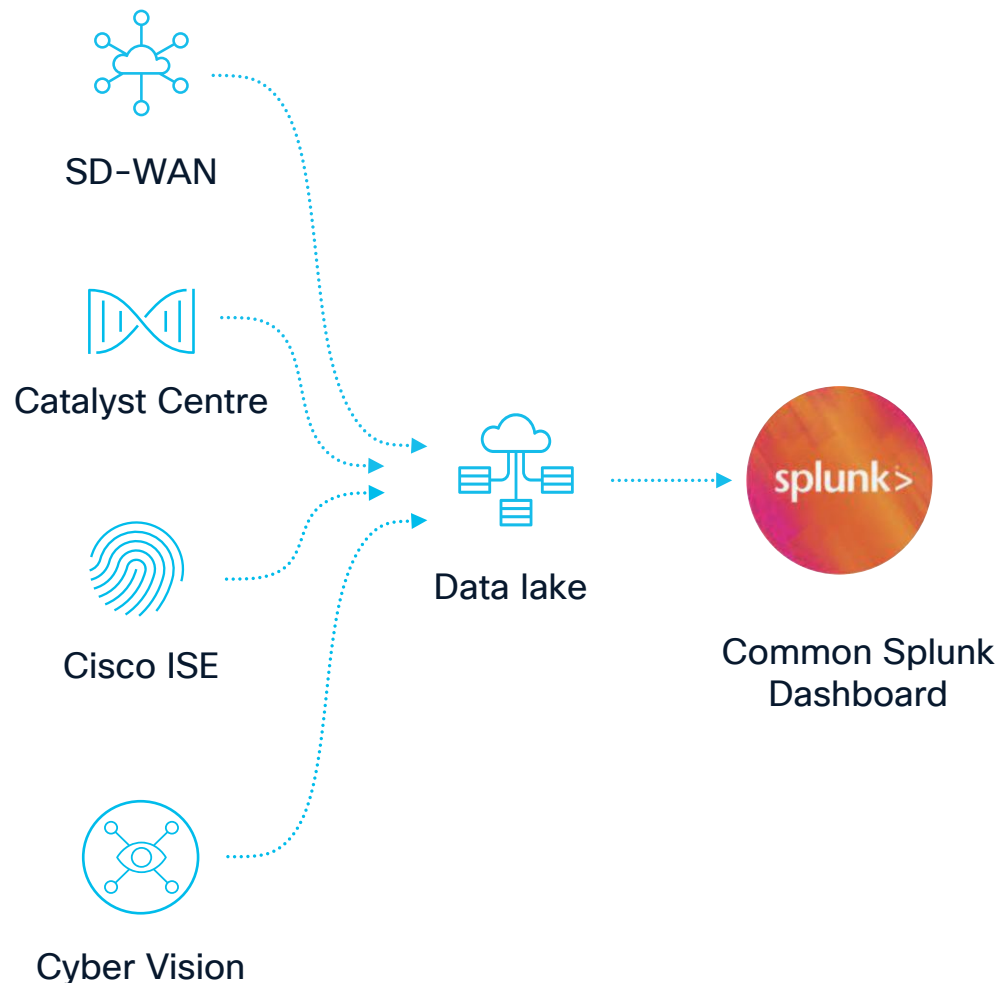
Indexer

- 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

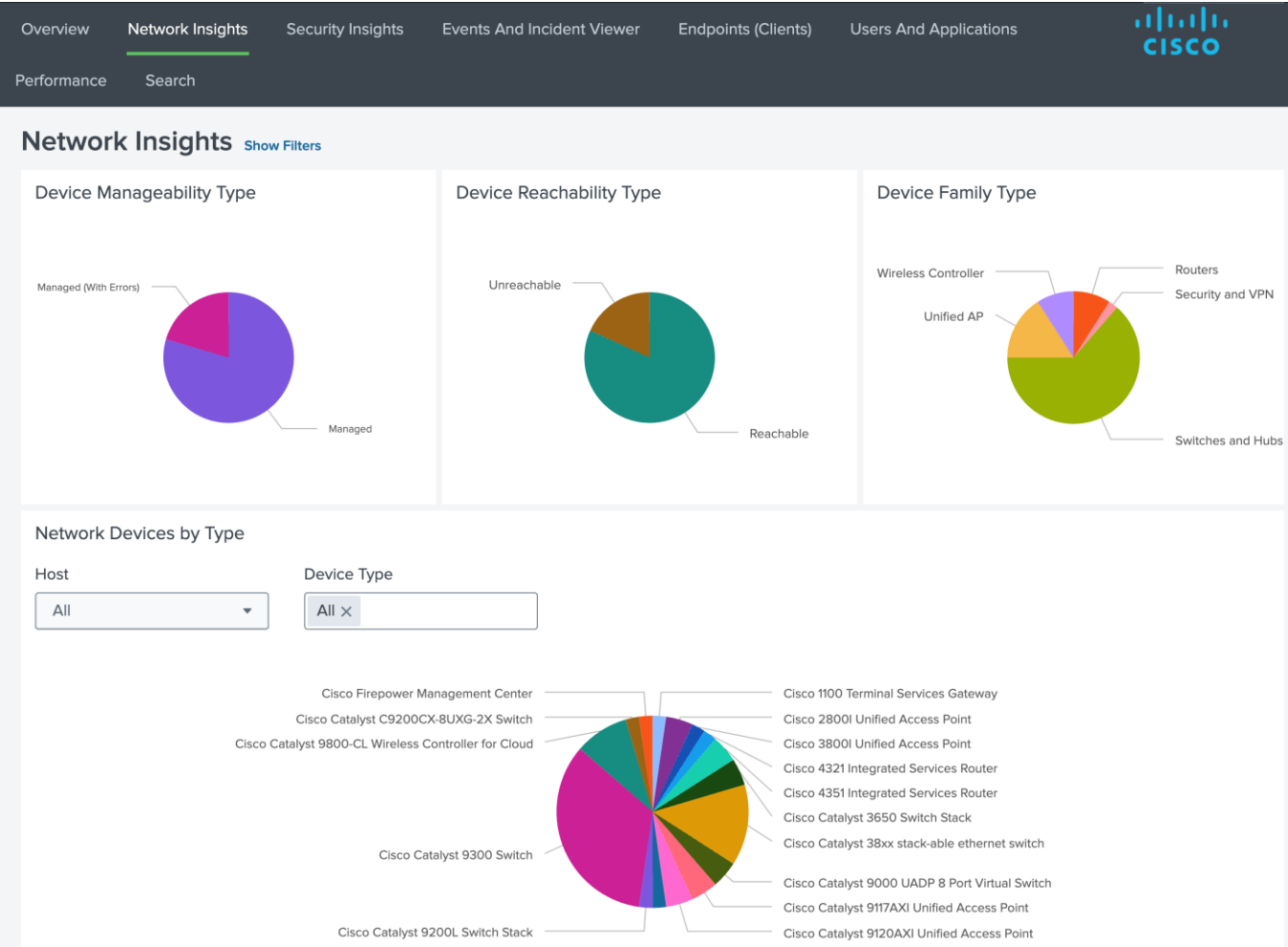
Analytics dashboard* to detect and report on anomalies based on deviation from the baseline (potentially powered by ITSI)

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

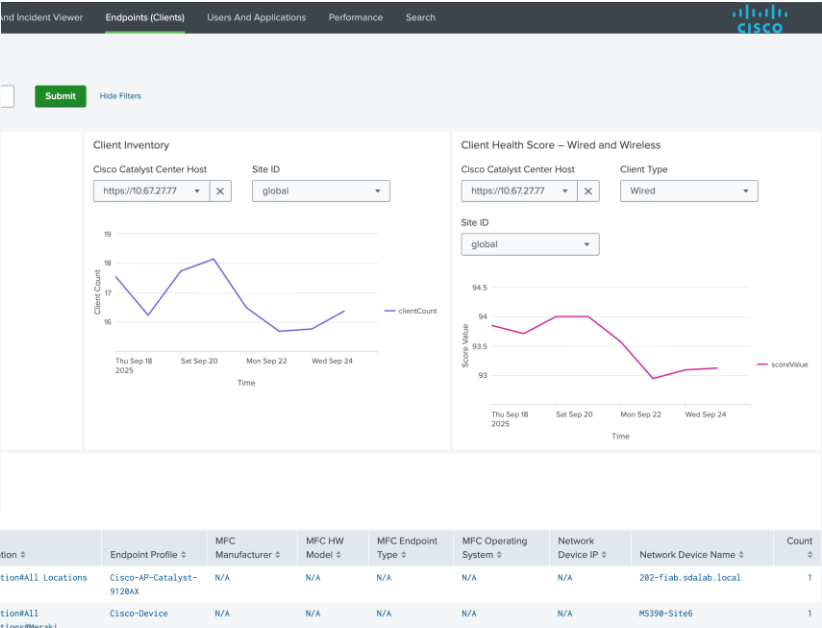


Network Insights

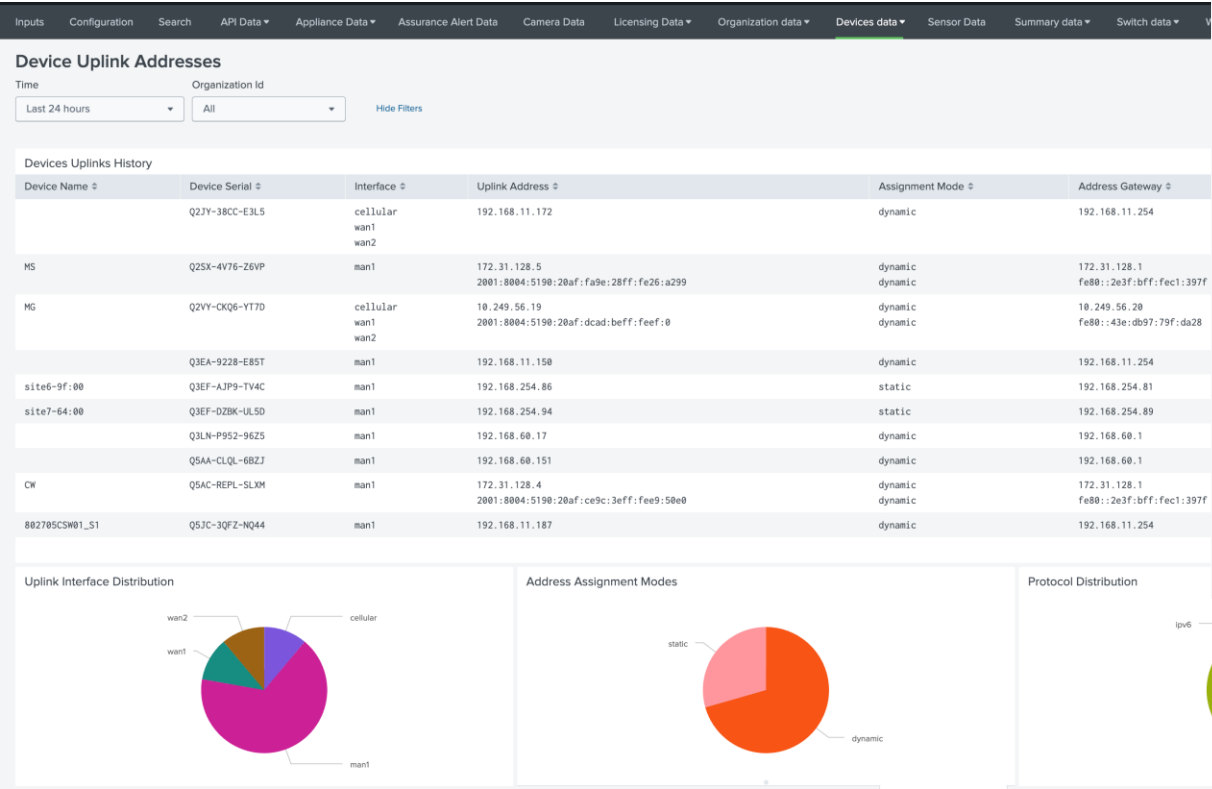
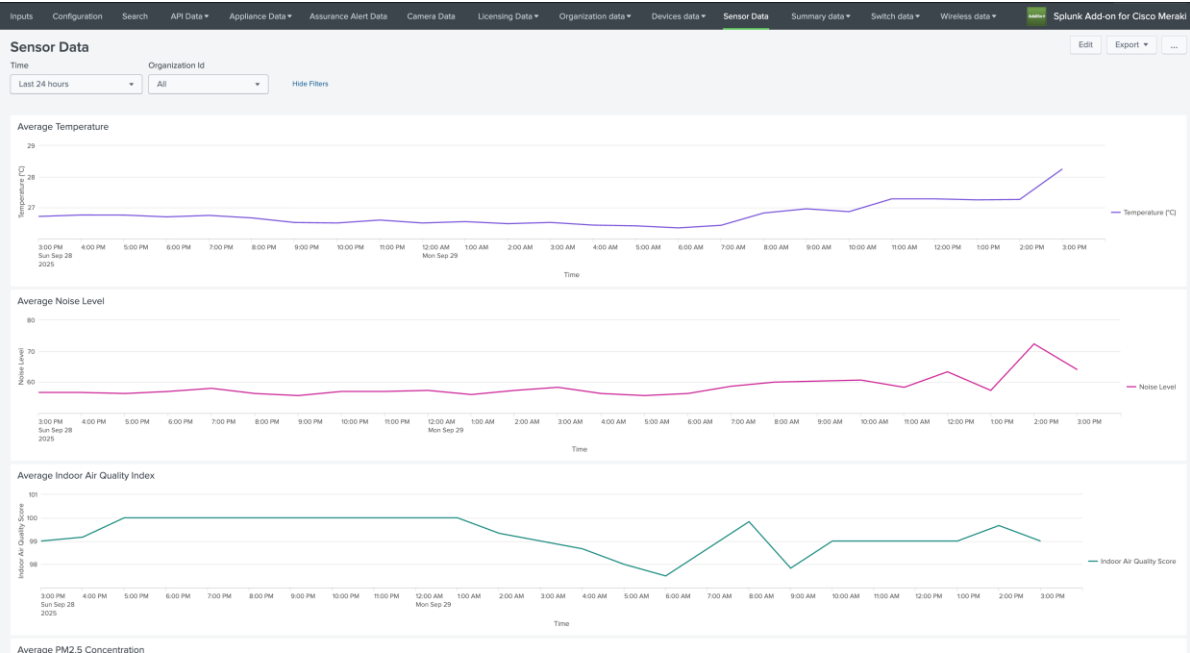
- Provides high-level summary of most pressing issues in the network
- Contains a mix of network and security events across Catalyst Center, ISE and SD-WAN

Endpoints

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



Meraki Insights



Devices Data

- Summary of Meraki device change history and uplink information

Sensor Data

- Provides sensor data from Meraki environmental sensors

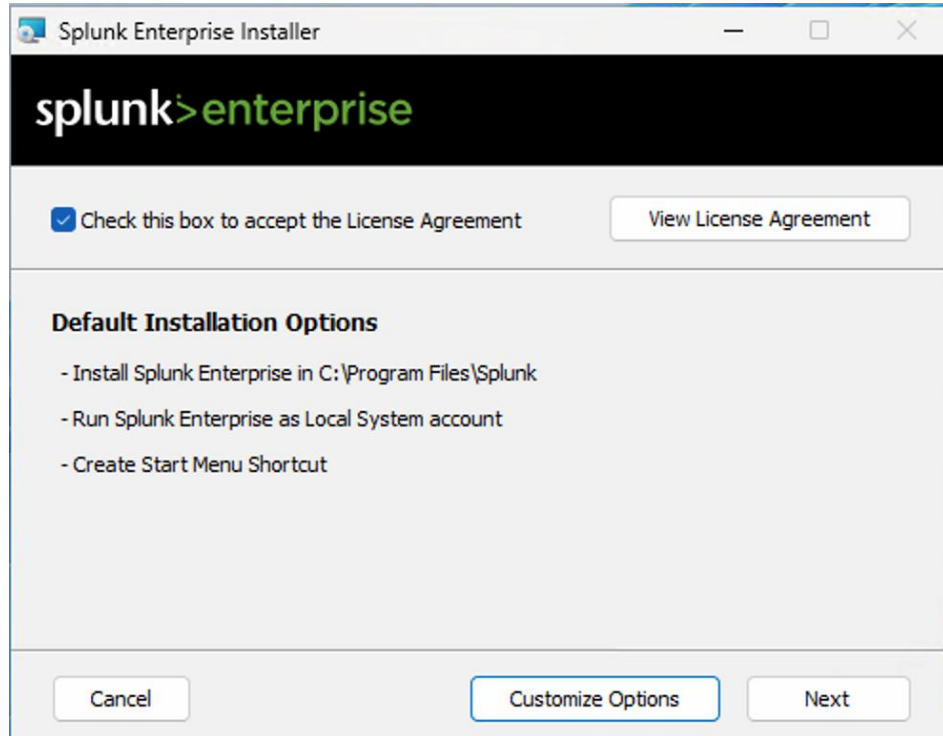


Splunk Installation & Getting Started

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

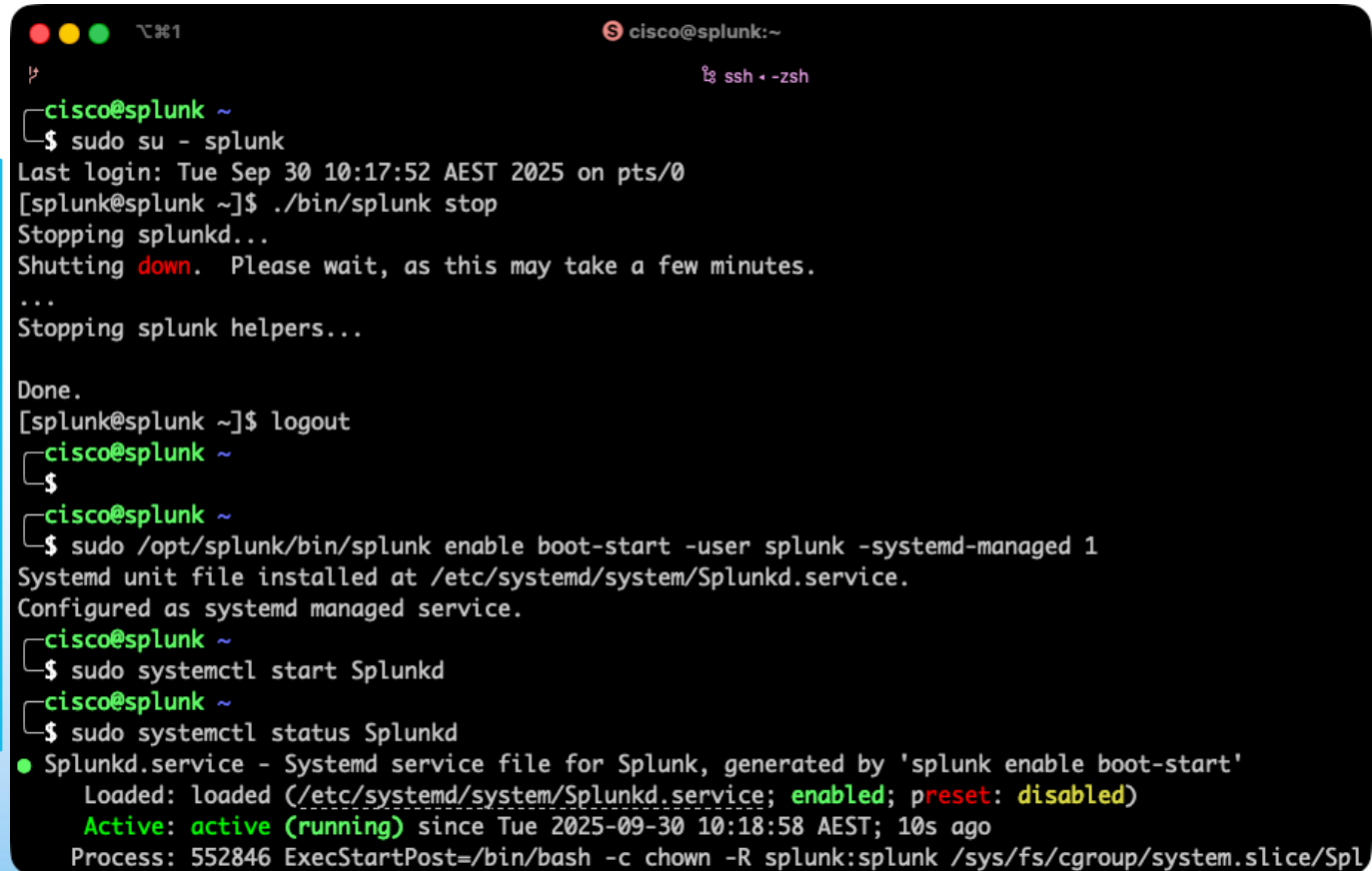
Splunk Enterprise Installation – Automatic Start

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
```

A terminal window with a dark background and light-colored text. The window title is 'cisco@splunk:~'. The terminal shows a sequence of commands and their outputs. The user 'cisco' switches to 'splunk' using 'sudo su - splunk'. The 'splunk' user runs './bin/splunk stop', which outputs 'Stopping splunkd...' and 'Shutting down. Please wait, as this may take a few minutes.' followed by 'Stopping splunk helpers...' and 'Done.'. The user then runs 'logout'. Back at the 'cisco' prompt, the user runs 'sudo /opt/splunk/bin/splunk enable boot-start -user splunk -systemd-managed 1', which outputs 'Systemd unit file installed at /etc/systemd/system/Splunkd.service. Configured as systemd managed service.'. Finally, the user runs 'sudo systemctl start Splunkd' and 'sudo systemctl status Splunkd'. The status output shows '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', and 'Process: 552846 ExecStartPost=/bin/bash -c chown -R splunk:splunk /sys/fs/cgroup/system.slice/Splunkd.service'.

Splunk Enterprise Installation - Firewall

Allow ports for Splunk

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

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

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

Inbound Rules

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....}	@{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

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

Splunk Enterprise Installation – Enable HTTPS

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. On the right, there's a status bar with a green checkmark, 'Administrator', '1 Messages', 'Settings', and 'Activity'. The main content area is titled 'General settings' with a breadcrumb 'Server settings » General settings'. Below this, there's a form for 'Splunk Web' settings. The 'Run Splunk Web' section has two radio buttons: 'Yes' (selected) and 'No'. Below this, the 'Enable SSL (HTTPS) in Splunk Web?' section has two radio buttons: 'Yes' (selected) and 'No'. This section is highlighted with a red rectangular box. Other settings visible include 'Splunk server name' (splunk), 'Installation path' (/opt/splunk), 'Management port' (8089), and 'Web port' (8000). A description for 'Management port' states: 'Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.' A description for 'SSO Trusted IP' states: 'The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.'

Splunk Web

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

Splunk Technology Add-Ons (TAs)

Splunk Apps and Technology Add-Ons

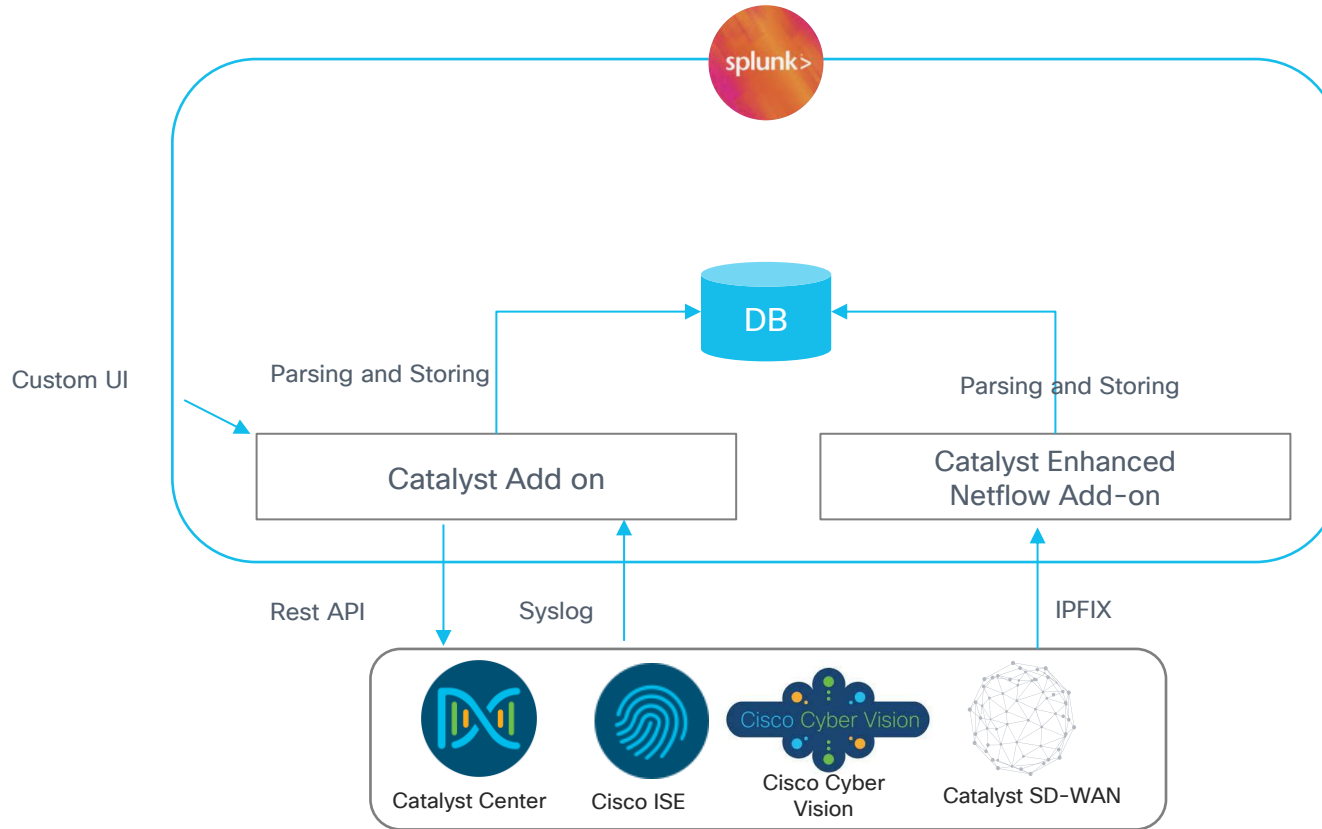


Collects, formats, and normalizes data from a specific technology source

<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

The screenshot shows the Splunk App Store interface. At the top, there's a navigation bar with 'splunk>enterprise', 'Apps', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below this is a 'Browse More Apps' section. A search bar on the left contains 'cisco catalyst'. To the left of the main results is a 'CATEGORY' sidebar with checkboxes for various categories like IT Operations, Security, Fraud & Compliance, Business Analytics, Utilities, Artificial Intelligence, IoT & Industrial Data, DevOps, Directory Service, Email, Endpoint, Firewall, Generic, Identity Management, and Information. The main results area shows two app cards. The first card is for 'Cisco Catalyst Add-on for Splunk' with an 'Install' button. The description states it collects data from Cisco Identity Services Engine, Cisco Catalyst SD-WAN, Cisco Catalyst Center, and Cisco CyberVision. It lists the author as Cisco Systems, version 1.1.1, build 1, and provides a link to prerequisites. The second card is for 'Cisco Catalyst Enhanced Netflow Add-on for Splunk' with an 'Install' button. It describes its function in providing Netflow element mapping and lists its author, version 2.1.0, build 1, and category as Network Security, SIEM. Both cards show download counts and release dates.

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

This is a dark-themed card for the 'Cisco Catalyst Add-on for Splunk'. It features the Cisco logo on the left. The title 'Cisco Catalyst Add-on for Splunk' is prominently displayed. Below the title, the description states: '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.' It also mentions 'Built by Cisco Systems, Inc.' At the bottom left is the Splunk logo. In the center is a 'Download' button with a download icon. On the bottom right are two icons: a link icon and a bell icon.

Cisco Catalyst Add-On for Splunk – Stream

Install the pre-requisite apps & add-ons



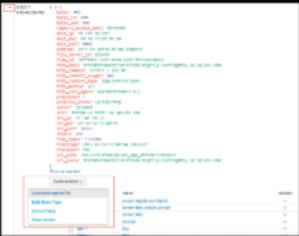
Splunk App for Stream

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](#)



[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](#)



[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](#)





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.](#)



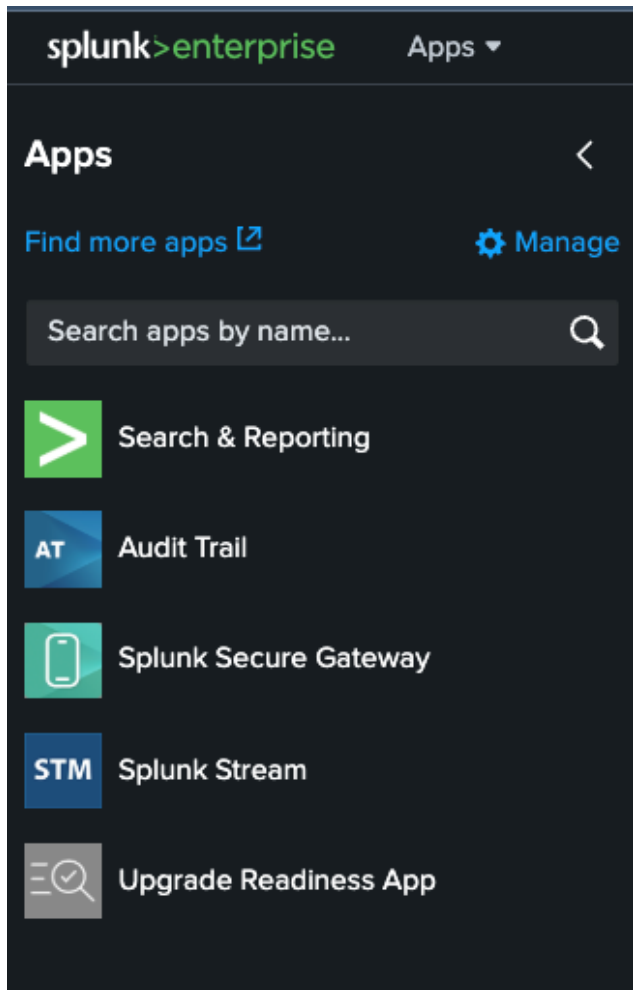
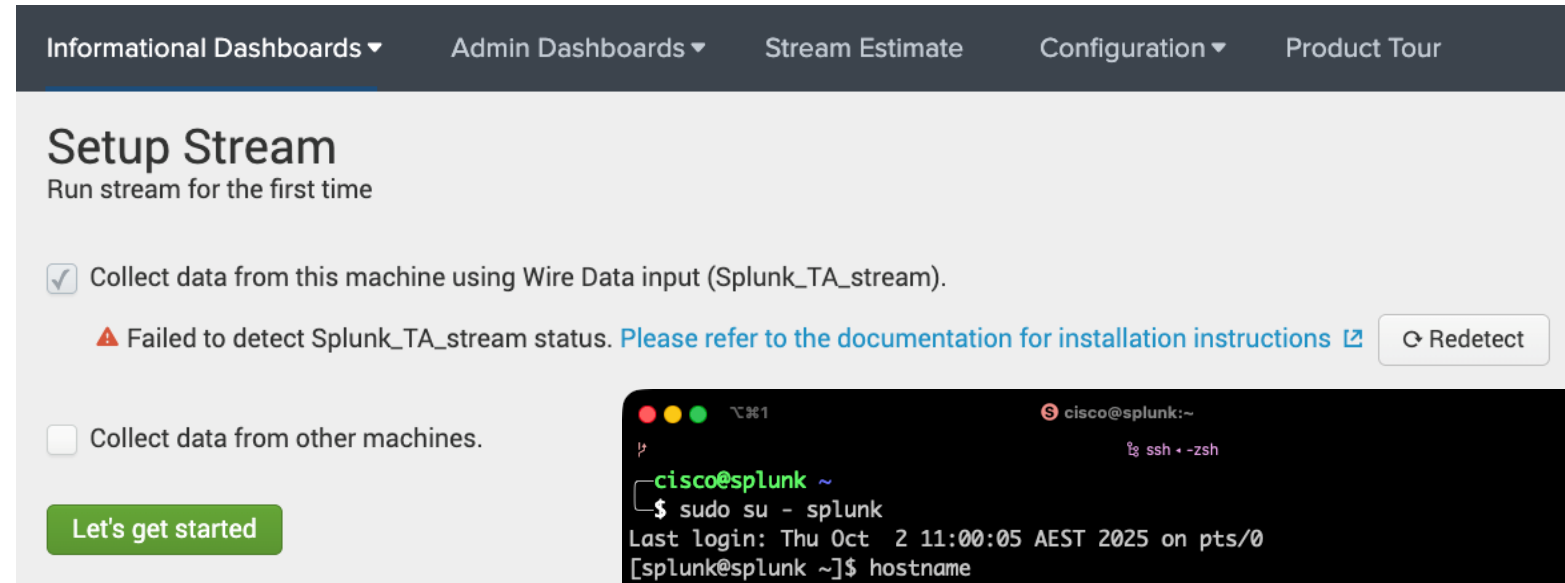
<https://splunkbase.splunk.com/app/1809>

<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



```
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

The image shows the Splunk 'Setup Stream' interface. The top navigation bar includes 'Informational Dashboards', 'Admin Dashboards', 'Stream Estimate', 'Configuration', and 'Product Tour'. The main heading is 'Setup Stream' with the subtitle 'Run stream for the first time'. A checkbox 'Collect data from this machine using Wire Data input (Splunk_TA_stream)' is checked. A warning message states: 'Splunk_TA_stream doesn't have proper permissions to run or not configured properly.' with a 'Redetect' button. Below this, 'Steps to troubleshoot:' are listed, with step 1: 'To ensure that Splunk_TA_Stream has proper permissions on Linux/OSX, run this command from the Splunk_TA_stream directory:' followed by a text box containing 'sudo ./set_permissions.sh'. Step 2 is 'Examine Splunk_TA_stream' with a 'Learn More' link. A checkbox 'Collect data from other machines' is unchecked. A green 'Let's get started' button is at the bottom.

Overlaid on the right is a terminal window showing the execution of the script:

```
cisco@splunk:~  
$ ssh -t -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 ~  
$
```

Below the terminal, a smaller version of the 'Setup Stream' interface is shown, indicating successful completion. The warning message is gone, and a green checkmark is present. The 'Collect data from other machines' checkbox is now checked. A new warning message appears: 'HTTP Event Collector global token configuration has been disabled.' with a 'View configuration' link and a 'Redetect' button. Below this, a note states: '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.' followed by instructions to run a command on the data source machine: 'curl -sSL https://splunk:8000/en-us/custom/splunk_app_stream/install_streamfwd | sudo bash'. A final note states: 'Note: Stream Forwarder (streamfwd) independent installation supports data capture on 64-bit Linux (RHEL and Ubuntu) only.' A green 'Let's get started' button is at the bottom.

- 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 Settings

Index Name

netflow

> ⓘ

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/thaweddb).

Data Integrity Check

Enable

Disable

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

Give frozen buckets.

App

Splunk Stream ▾

Save

Cancel

Step 7 – Create an index for NetFlow

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

BRKOPS-1233

 CISCO

Splunk HTTP Event Collector

splunk>enterprise

Apps

✓

Administrator

1 Messages

Settings

Activity

Help

Find

HTTP Event Collector

Data Inputs » HTTP Event Collector

1 Tokens

App: All

filter

Name	Actions	Token Value
streamfwd	<div>Edit</div> <div>Disable</div> <div>Delete</div>	<div>Copy</div> <div>Show</div> <div>*****</div>

!

Global Settings

New Token

Step 8 – Enable HEC globally

Step 9 – Create a HEC for the NetFlow Stream Forwarder

Edit Global Settings

All Tokens

Enabled

Disabled

Default Source Type

Select Source Type

Default Index

Default

Default Output Group

None

Use Deployment Server

☐

Enable SSL

☒

HTTP Port Number

8088

Cancel

Save

Stream forwarder

splunk>enterprise Apps ▾

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

Distributed Forwarder Management

Create Stream Forwarder groups using pattern match.

1 groups Search

Configure Streams

Global IP Filters

Install Stream Forwarders

Create New Group

✓ Distributed Forwarder Management

i	Name ▾	Description ▾	Rule ▾	Include Ephemeral Streams? ▾	Contains Streams ▾	Endpoint Autoconfig ▾	Actions
>	defaultgroup	Used when there is no matching group found for a given stream forwarder ID		Yes	54	On	⌵

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/
```

```
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

```
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>enterprise Apps Administrator 5 Messages Settings Activity Help Find

HTTP Event Collector

Data Inputs » HTTP Event Collector

1 Tokens App: All stream 20 per page

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

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

add all >

history

main

netflow

summary

Selected indexes

« remove all

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

Global Settings

New Token

Data Inputs > HTTP Event Collector

1 Tokens

App: All ▾

filter

20 per page ▾

Name	Actions	Token Value	Source Type	Index	Status
streamfwd	<div>Edit</div> <div>Disable</div> <div>Delete</div>	<div>Copy</div> <div>Show</div> <div>*****</div>	netflow	netflow	Enabled

Informational Dashboards ▾

Admin Dashboards ▾

Stream Estimate

Configuration ▾

Product Tour

STM

Splunk Stream

Configure Streams

New Stream

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

Metadata Streams:54

Packet Streams:0

Ephemeral Streams:0

Avg. Traffic(15m)

~ 1.8 Mb/s

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

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



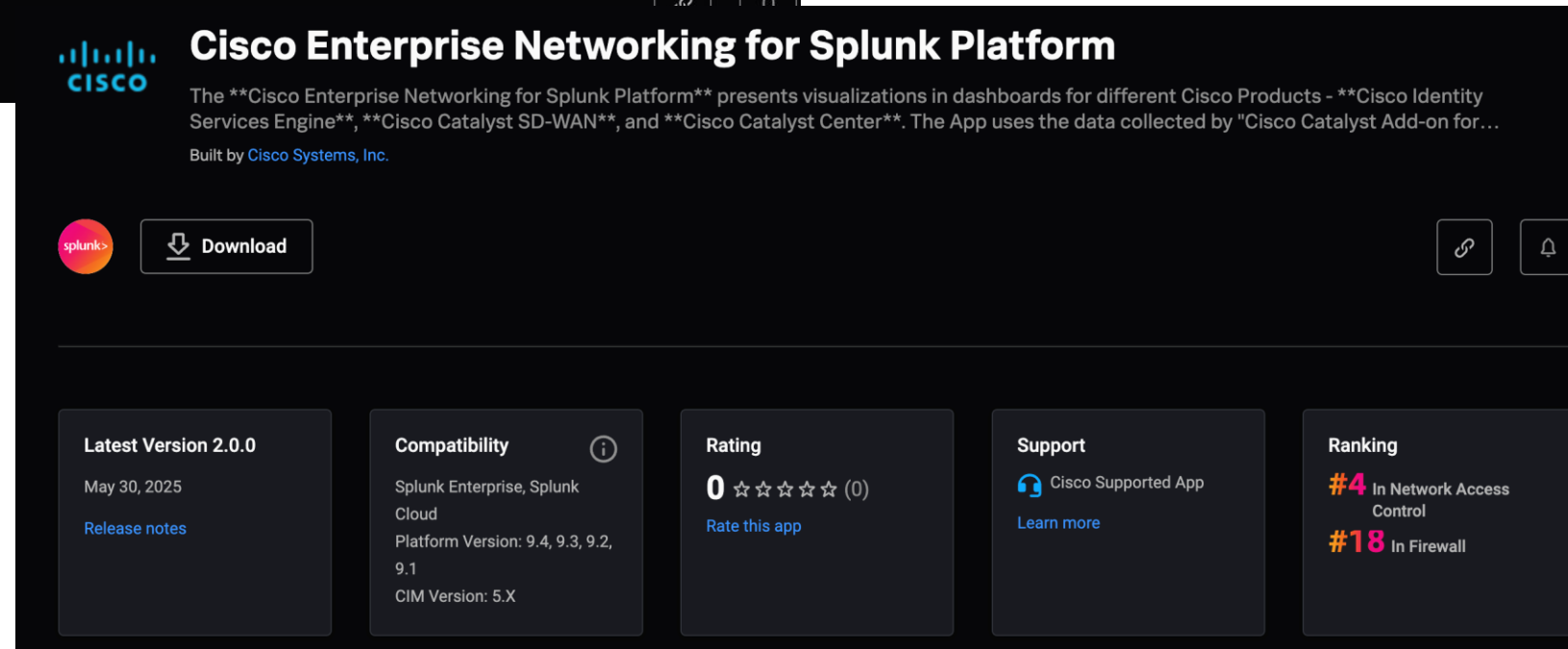
Cisco Catalyst Add-on for Splunk

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 from specified sources and stores then 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](#)

[Link](#) [Alert](#)

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**
Search macros (using 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/thaweddb).

Data Integrity Check ☒ Enable ☐ Disable
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
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Cisco Catalyst Add-on for Splunk

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")
☐ 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

Application Setup

My Apps

Q Search...

>	Input Name ↓	Product ↓	Account ↓	Enabled ↓	Status ↓	Source Type ↓	Index ↓	⚙
No records found								

Q Search...

**Catalyst Center**
Networking - Switching & Wireless

Cisco 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**
Industrial IoT Security

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 SDWAN**
Software-Defined Wide Area Network (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)**
Network Access Control

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		
<div>Q Search...</div>		
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

InputsConfiguration

Input Type

Client Health

*Name

ClientHeath

Enter a unique name for the data input.

*Interval

300

Time interval of input in seconds. Minimum value is 300.

*Index

catalyst

*Cisco DNA Center Account

splunk77

*Logging Level

INFO

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

Cancel

Create

Input Type

Client Health

Client Health

Device Health

Compliance

Issue

Network Health

Security Advisory

Site Topology

Audit Logs

Client

Getting Catalyst Center Telemetry Sent to Splunk

Cisco Catalyst Center Design / Network Settings

Expand | Vers | Device Credentials | IP Address Pools | Wireless | **Telemetry** | Security and Trust

Q Find Hierarchy Search Help

Global

- DC
 - Ekahau
 - Site 201
 - Site 202
 - Site 203

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings to the devices assigned to a site or provisioned.

Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. View metrics gathered and the frequency with which they are collected.

Syslogs

Choose Catalyst Center to be your syslog server, and/or add any external syslog servers. Devices with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned.

- ☒ Use Catalyst Center as syslog server
- ☒ Add an external syslog server

IP Address* 192.168.11.60 +

Application Visibility

When assigning Catalyst 9000 or Traffic Telemetry Appliance devices to the site, enable NetFlow Application Telemetry and Controller-Based Application Recognition by default. ⓘ

- ☒ Enable by default on supported wired access devices

Choose the destination collector for Netflow records sent from network devices.

- ☐ Use Catalyst Center as the Netflow Collector
- ☒ Use Cisco Telemetry Broker (CTB) or UDP director

IP Address 192.168.11.60 Port 6009

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 CenterPlatform / Developer Toolkit

APIsIntegration FlowsEvent Notifications

NotificationsEvent 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 o
NETWORK-CLIENTS-3-356	Wireles
NETWORK-CLIENTS-3-357	Wireles

splunk>enterpriseAppsAdministrator

HTTP Event Collector

Data Inputs » HTTP Event Collector

4 TokensApp: Allfilter

Name	Actions	Token Value
CATC-HEC	EditDisableDelete	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/collec

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

Catalyst Center

System / Settings

☆ 🔍 🔄 ⓘ 🔔 | 👤 Jeff

☰

Q Search

SNMP

ICMP Ping

PnP AP Location

Device EULA Acceptance

Device Prompts

Configuration Archive

External Services

Cisco AI Analytics

Stealthwatch

Talos IP Reputation

Destinations

Cisco Spaces/CMX Servers

Authentication and Policy Servers

Settings > External Services

Destinations

Configure various types of destinations to deliver event notifications from Catalyst Center Platform

Webhook Email Syslog SNMP ITSM

Configure the REST Endpoint to receive Events notifications from Catalyst Center Platform

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

Edit Global Settings

All Tokens Enabled

Default Source Type

Default Index

Default Output Group

Use Deployment Server

Enable SSL

HTTP Port Number 8088

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

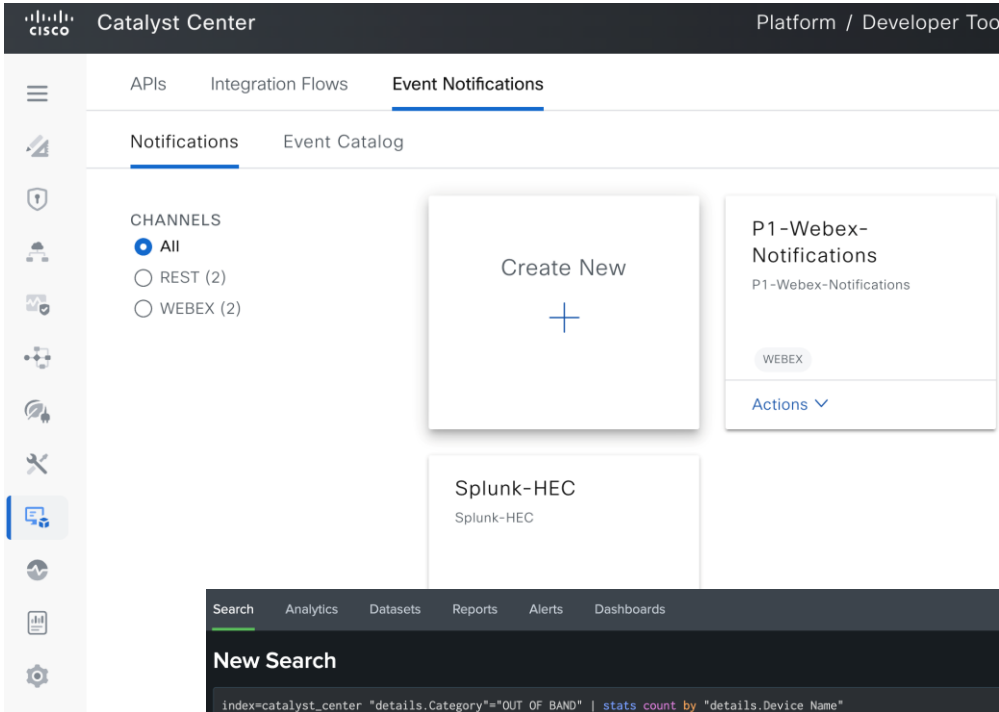
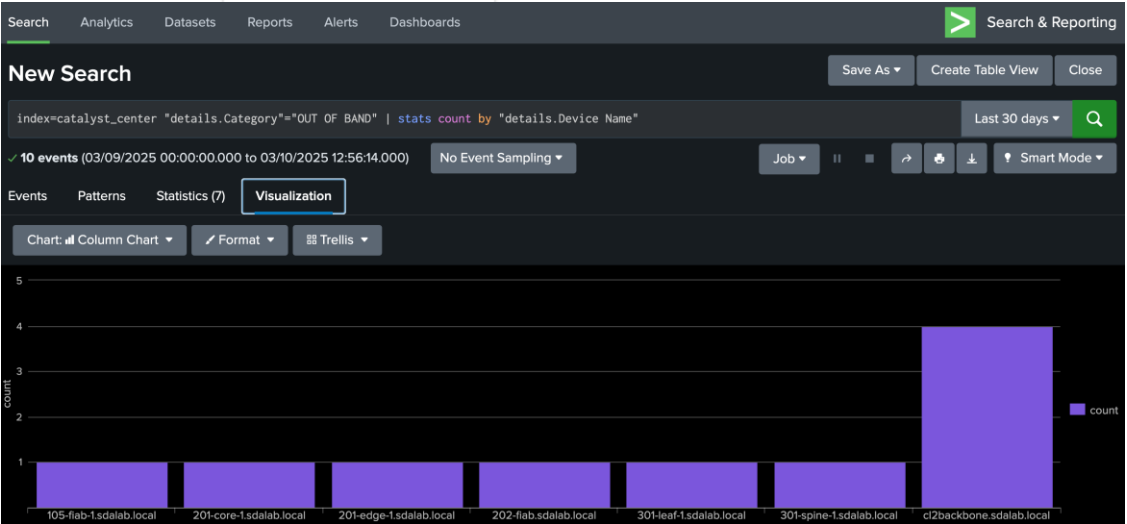
Header Key

Authorization

Header Value

Splunk e7a1fc00-aa56-4157-ad

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



Identity Services Engine

Send Identity Services Engine Data to Splunk

Cisco ISE

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

>

Rows/Page 4

Refresh

Trash

Edit

Enable

Disable

Approve

Decline

☐	Name	Description	Client Groups	Status
☒	splunkise	x Description	Client Groups	Enabled

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



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

Application Setup

Search

CISCO

Application Setup

My Apps

Q ise

>	Input Name ↕	Product ↕	Account ↕	Enabled ↕	Status ↕	Source Type ↕	Index ↕	⚙
>	splunkISE	Identity Services Engine (ISE)	splunkise11	☒	Connected	-	catalyst	⋮
>	5513	Identity Services Engine (ISE)	-	☒	-	cisco:ise:syslog	catalyst	⋮



Identity Services Engine Logging to Splunk

Remote Targets and Logging Categories

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & Res...

Log SettingsRemote Logging TargetsLogging CategoriesMessage CatalogCollection Filters

Remote Logging Targets List > Splunk

Logging Target

* NameSplunk

Descriptionvia Telemetry Broker

* Host / IP Address192.168.11.60

* Port5513

Facility CodeLOCAL6

Target TypeUDP SysLog

StatusEnabled

* Maximum Length8192

Include Alarms For this Target

Comply to RFC 3164

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & Res...

Log SettingsRemote Logging TargetsLogging CategoriesMessage CatalogCollection Filters

Logging Categories

Parent CategoryCategory

AAA AuditAAA Audit

Failed AttemptsFailed Attempts

Passed AuthenticationsPassed Authentications

AAA DiagnosticsAAA Diagnostics

Administrator Authentication and Auth...Administrator Authentication and Auth...

Targets

Splunk

LogCollector,Splunk

LogCollector,ProfilerRadiusProbe,Splunk

LogCollector,ProfilerRadiusProbe,Splunk

LogCollector,Splunk

Splunk

splunk>enterprise

Apps

Administrator6 MessagesSettingsActivity

SearchAnalyticsDatasetsReportsAlertsDashboards

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)

Events (23,538)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect

FormatShow: 20 Per PageView: List

TimeEvent

03/10/2025 14:32:42.000Oct 3 14:32:42 192.168.11.11 Oct 3 14:32:42 ise33 CISE_Administrative_and_Operational_Audit 0002951684 1 0 202 11134902 60237 NOTICE SXP: SXP binding is successful, ConfigVersionId=88, BindingPeerIp=192.168.176.106/32, Bind BindingSXPNodeIp=192.168.11.11, SRC=192.168.147.20, PeerSequence=192.168.11.11,192.168.147.20, IsActive=true, Bi rceType=SESSION, host = 192.168.1111 source = udp:5514 sourcetype = cisco:ise:syslog

03/10/2025 14:32:42.000Oct 3 14:32:42 192.168.11.11 Oct 3 14:32:42 ise33 CISE_Administrative_and_Operational_Audit 0002951683 1 0 202 11134901 51001 NOTICE Administrator-Login: Administrator authentication succeeded, ConfigVersionId=88, AdminInte 254.4.6, AdminName=admin, OperationMessageText=Administrator authentication successful, host = 192.168.1111 source = udp:5514 sourcetype = cisco:ise:syslog

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

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

Inputs

Syslog

Configuration

*Input Type

☒ UDP

☐ TCP

*Port

5515

Enter the Port for this input.

Only accept connection from

example: 10.1.2.3, lbadhost.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

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

 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

Cancel

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

Search

Application Setup

My Apps

Q sdwan

>	Input Name ↕	Product ↕	Account ↕	Enabled ↕	Status ↕	Source Type ↕	Index ↕	⚙
>	UnifiedThreats	SDWAN	splunksdwan	☒	Connected	-	catalyst	⋮
>	SiteTunnel	SDWAN	splunksdwan	☒	Connected	-	catalyst	⋮
>	5515	SDWAN	-	☒	-	cisco:firewall:logs	catalyst	⋮



SD-WAN Logging to Splunk

Custom syslog port and NetFlow for Splunk

 Catalyst SD-WAN



The network is out of compliance due to licensing, [click here](#) for more a



Configuration



Analytics



Workflows



Tools

← Feature Profiles (CLI Add-on Profile)

DC_CLI_Template

Edit

Description: Trustsec/logging to SDA Border

Device solution

SD-WAN

Updated by

jeffl2

Last updated

Sep 13, 2025 1

CLI Configuration ⓘ

1 logging host 192.168.11.60 vrf 101 transport udp port 5515

2

3 !

4

Monitor

Configuration

Analytics

Workflows

Tools

Global (8 of 8 nodes)

SITE_1

SITE_10

SITE_100

SITE_103

SITE_104

SITE_2

SITE_6

SITE_7

Catalyst SD-WAN

Search

The network is out of compliance due to licensing, [click here](#) for more actions.

Global

Global node for network hierarchy

Type: GLOBAL

Pools

Collectors

Multi Region Fabric (MRF)

External Services

Cflowd ⓘ

Create a Cflowd template that defines the location of Cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors.

Collector Server (Maximum: 4)

+ Add Collector Server

VPN ID	IPv4/IPv6 Address	UDP Port	Export Spreading (optional)	BFD Metrics Exporting (optional)	Exporting Interval (optional)	Action
101	192.168.11.60	9995	☐	☒	60	

Advanced Settings

Active Flow Timeout (Seconds)

600

Inactive Flow Timeout (Seconds)

60

Syslog

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

NetFlow

- Add Cflowd collector address as Splunk

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

BRKOPS-1233



Enterprise Networking App – SD-WAN Dashboards

splunk>enterprise

Apps

Administrator

1 Messages

Settings

Activity

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

Save As

index=catalyst sourcetype="cisco:sdwan:*

538 of 538 events matchedNo Event Sampling

Job

II

Events (538)PatternsStatisticsVisualization

Timeline format

Zoom Out

+ Zoom to Selection

x 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 bla-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

i

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

All x

*

Data Key	Last Updated Time	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



Meraki Add-On

Meraki Add-On for Splunk

[Main Page](#) / [Apps](#) / Cisco Meraki Add-on for Splunk

AddOn+

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

Latest Version 3.2.0

August 14, 2025

[Release notes](#)

Compatibility

Splunk Enterprise, Splunk Cloud

Platform Version: 10.0, 9.4, 9.3, 9.2

CIM Version: 6.X, 5.X, 4.X

Rating

4 ★★★★★ (4)

[Rate this app](#)

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

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

40 Inputs (40 of 40 enabled) 10 Per Page ▼ Search... < Prev 1 2 3 4 Next > Activate all Deactivate all

i	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	  

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/...

Data Integrity Check

Enable

Enable this if you want Splunk to compute hashes on every slice of your data fo

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

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

Splunk Add-on for Cis...

Configuration Source

Visible in the App

Owner

Any

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

Save

Cancel

Meraki Add-On for Splunk – Add Organization

Add Meraki credential information

Add Organization

×

*Organization Name

Meraki

Enter a unique name for this Meraki organization.

*Service region

Global

Select Service region (Global is preselected)

*Base URL

https://api.meraki.com

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

*Organization ID

MyMerakiOrgID

Enter Organization ID.

*Organization API Key

Enter Organization API Key.

*Max API calls per second

5

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

meraki

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

Cancel

Add

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

AddOn+

Sp

Licensing Data

Organization data

Devices data

Sensor Data

Inputs

Configuration

Search

API Data

Appliance Data

Assurance Alert Data

Camera Data

Licensing Data

Organization data

AddOn+

Splunk Add-on for Cisco Meraki

Wireless data

Devices data

Sensor Data

Summary data

Switch data

Wireless data

Inputs

Manage Cisco Meraki data inputs

40 Inputs (40 of 40 enabled)

10 Per Page

Search...

All

i	Name	Organization
>	accesspoints_Meraki	Meraki
>	airmarshal_Meraki	Meraki
>	api_request_history_Meraki	Meraki
>	api_request_overview_Meraki	Meraki
>	api_request_response_code_Meraki	
>	appliance_vpn_stats_Meraki	
>	appliance_vpn_statuses_Meraki	
>	assurance_alerts_Meraki	

Sensor Data

Time: Last 30 days

Organization Id: All

Hide Filters

Average Temperature

Average Noise Level

Device Uplink Addresses

Time: Last 24 hours

Organization Id: All

Hide Filters

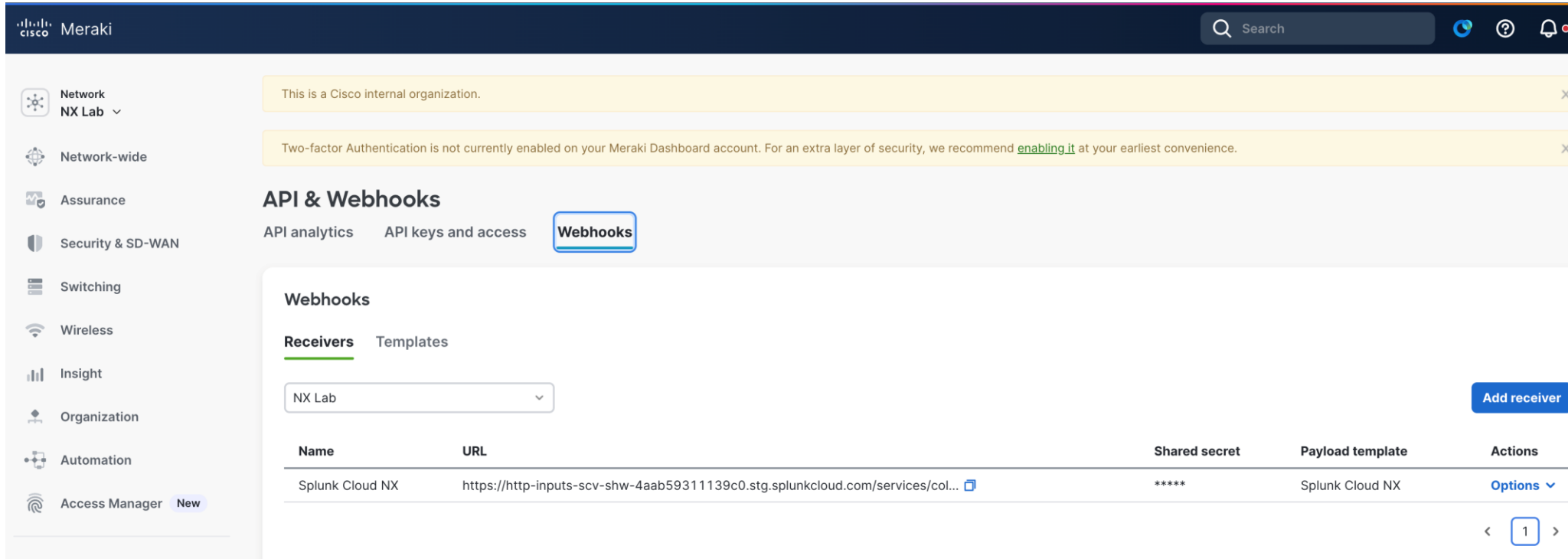
Search produced no results.

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



Meraki Add-On for Splunk – Webhooks



The screenshot shows the Meraki dashboard interface. The left sidebar contains navigation links for Network, Network-wide, Assurance, Security & SD-WAN, Switching, Wireless, Insight, Organization, Automation, and Access Manager. The main content area is titled 'API & Webhooks' and includes tabs for 'API analytics', 'API keys and access', and 'Webhooks'. The 'Webhooks' tab is active, showing a 'Webhooks' section with 'Receivers' and 'Templates' sub-tabs. A dropdown menu shows 'NX Lab' as the selected organization. A table lists the configured webhooks, with one entry for 'Splunk Cloud NX'.

Name	URL	Shared secret	Payload template	Actions
Splunk Cloud NX	https://http-inputs-scv-shw-4aab59311139c0.stg.splunkcloud.com/services/col...	*****	Splunk Cloud NX	Options

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 displays the Splunk Cloud interface. On the left, the 'HTTP Event Collector' configuration page is visible, showing a table with one entry: 'meraki-webhook'. The table has columns for Name, Actions, and Token Value. The Actions column contains 'Edit', 'Disable', and 'Delete' links. The Token Value column contains 'Copy' and 'Show' links, followed by a masked token '*****'. On the right, the 'Meraki' Add-On configuration page is shown, specifically the 'API & Webhooks' section. The 'Webhooks' tab is selected, and the 'View Template' page is displayed. The 'Template Name' field is set to 'Splunk Cloud NX'. The 'Liquid Body' tab is selected, and the 'Edit' page is shown. The 'Liquid Samples' dropdown is set to 'Liquid Samples'. The 'Generate Preview' button is visible. The preview shows a JSON payload for a Meraki webhook event, including fields like 'sourcetype', 'event', 'version', 'sentAt', 'organizationId', 'organizationName', 'organizationUri', 'networkId', 'networkName', 'networkUri', 'networkTags', 'deviceSerial', 'deviceMac', 'deviceName', 'deviceUri', 'deviceTags', and 'deviceModel'.

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

API & Webhooks

API analytics API keys and access Webhooks

Webhooks

Receivers Templates

Create Template

Template Name
Splunk Cloud NX

Liquid Body **Liquid Headers** Webhook Data

Edit [Generate Preview →](#) **Preview**

Authorization [Delete](#)

[Add](#)

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`

Webhooks

Receivers Templates

 [Add receiver](#)

Name	URL	Shared secret	Payload template	Actions
<input type="text" value="Splunk Cloud NX"/>	<input type="text" value="https://http-inputs-scv-shw-4aab59311139c0.stg.splunkcloud.com/services/collec"/>	<input type="text" value="<HEC TOKEN>"/>	<input type="text" value="Splunk Cloud NX"/>	Save Cancel

Meraki Add-On for Splunk – Webhooks

Create a liquid header webhook template

 Network
NX Lab ▾

 Network-wide

 Assurance

 Security & SD-WAN

 Switching

 Wireless

 Insight

 Organization

 Automation

 Access Manager New

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

100

GB ▾

in

20 minutes ▾

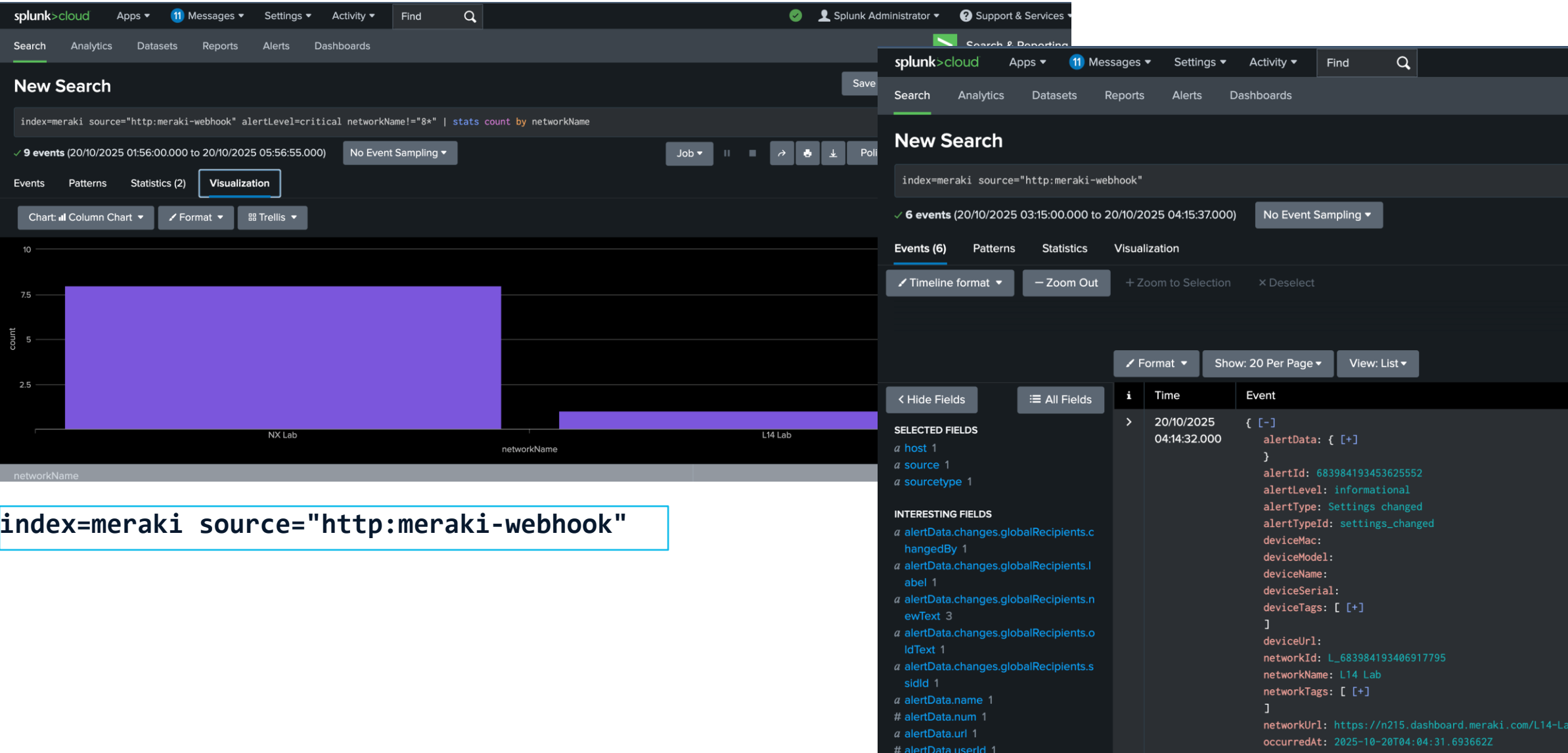


Show additional recipients

Step 5 – Subscribe to Network-wide Alerts

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

Meraki Webhook Searching



`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

[Main Page](#) / [Apps](#) / **Cisco ThousandEyes App for Splunk**



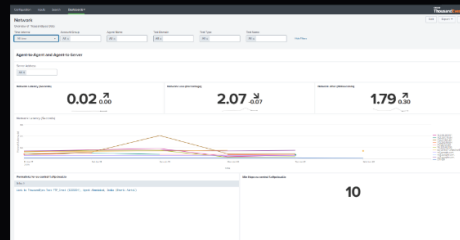
Cisco ThousandEyes App for Splunk

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

Configuration

scv-shw-4aab59311139c0.stg.splunkcloud.com/en-GB/app/ta_cisco_thousandeyes/configuration

splunk>cloud Apps Messages Settings Activity Find

Configuration Inputs Search Dashboards

Add ThousandEyes User

Set up your app

ThousandEyes User ThousandEyes F

0 Item

User Code JMBVZGVX

Cisco ThousandEyes OAuth User Code.

Verification URL https://app.thousandeyes.com/verify-device-user

Cisco ThousandEyes OAuth Verification URL.

Authorize

Click 'Authorize' to grant permission and proceed.

Cancel Add

Authorize OAuth2 - ThousandEyes

app.thousandeyes.com/verify-device-user-code?user_code=JMBVZGVX

cisco ThousandEyes

Enter your device authentication

JMBVZGVX

Verify

splunk>cloud Apps Messages Settings Activity Find

Splunk Administrator Support & Services

HTTP Event Collector

Data Inputs HTTP Event Collector

1 Tokens App: All filter

20 per page

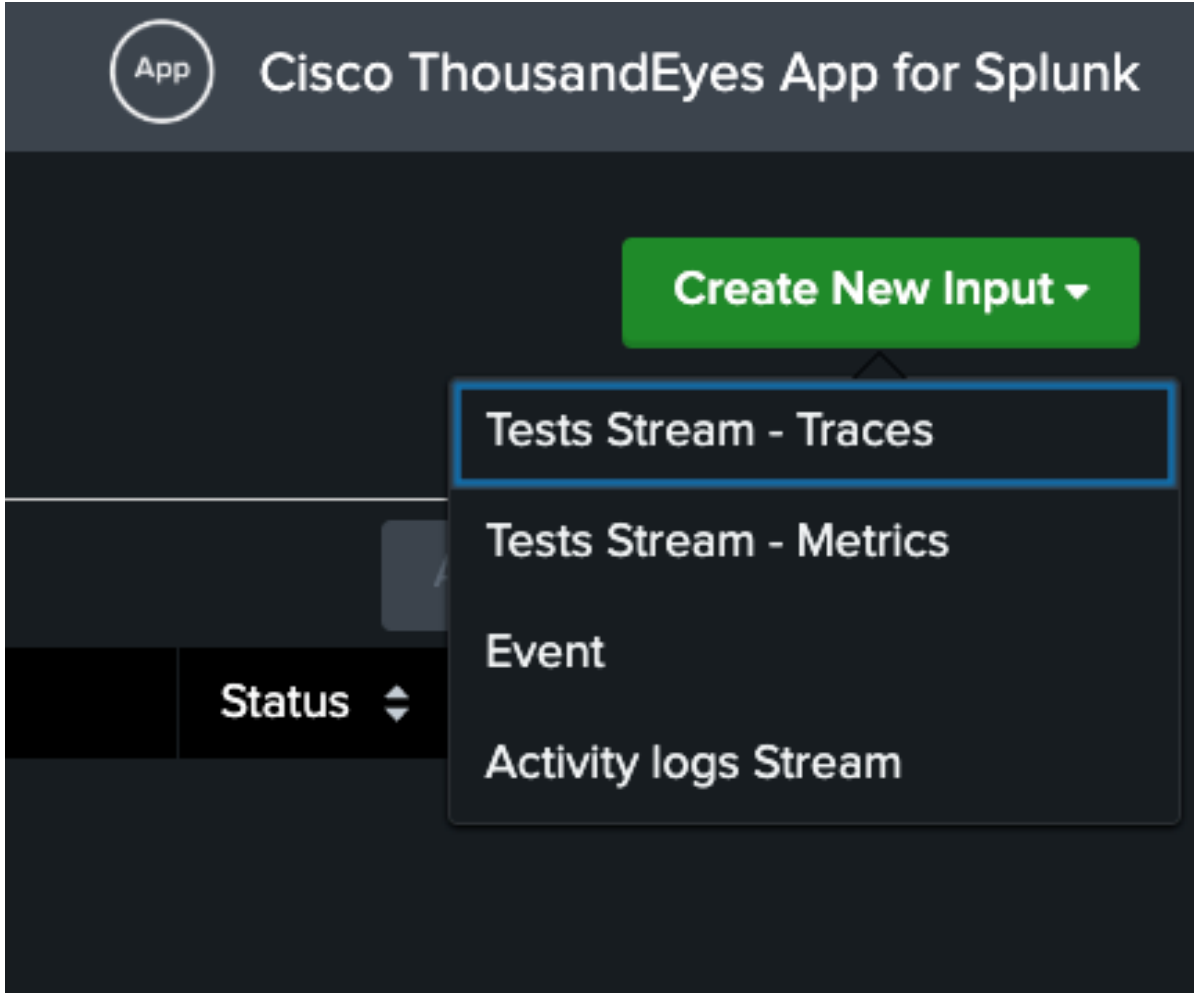
Name	Actions	Token Value	Source Type	Index	Status
victoriahec	Edit Disable Delete	Copy Hide bc77efcf-fc60-494f-b80c-52701d7901d4		main	Enabled

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



Update Tests Stream - Traces

Name: traces
A unique name for the data input.

ThousandEyes User: jeff12@cisco.com
ThousandEyes User to use for this input.

Account Group: jeff12 (217336)
Select Account Group.

Tags: Google:Google X MSTEams:MSTEams X Zoom:Zoom X
Select Tags associated with the tests to be streamed.

Cloud & Enterprise Agent Tests: https://www.cisco.com (7749456 | page-load... X
Select Cloud & Enterprise Agent Tests.

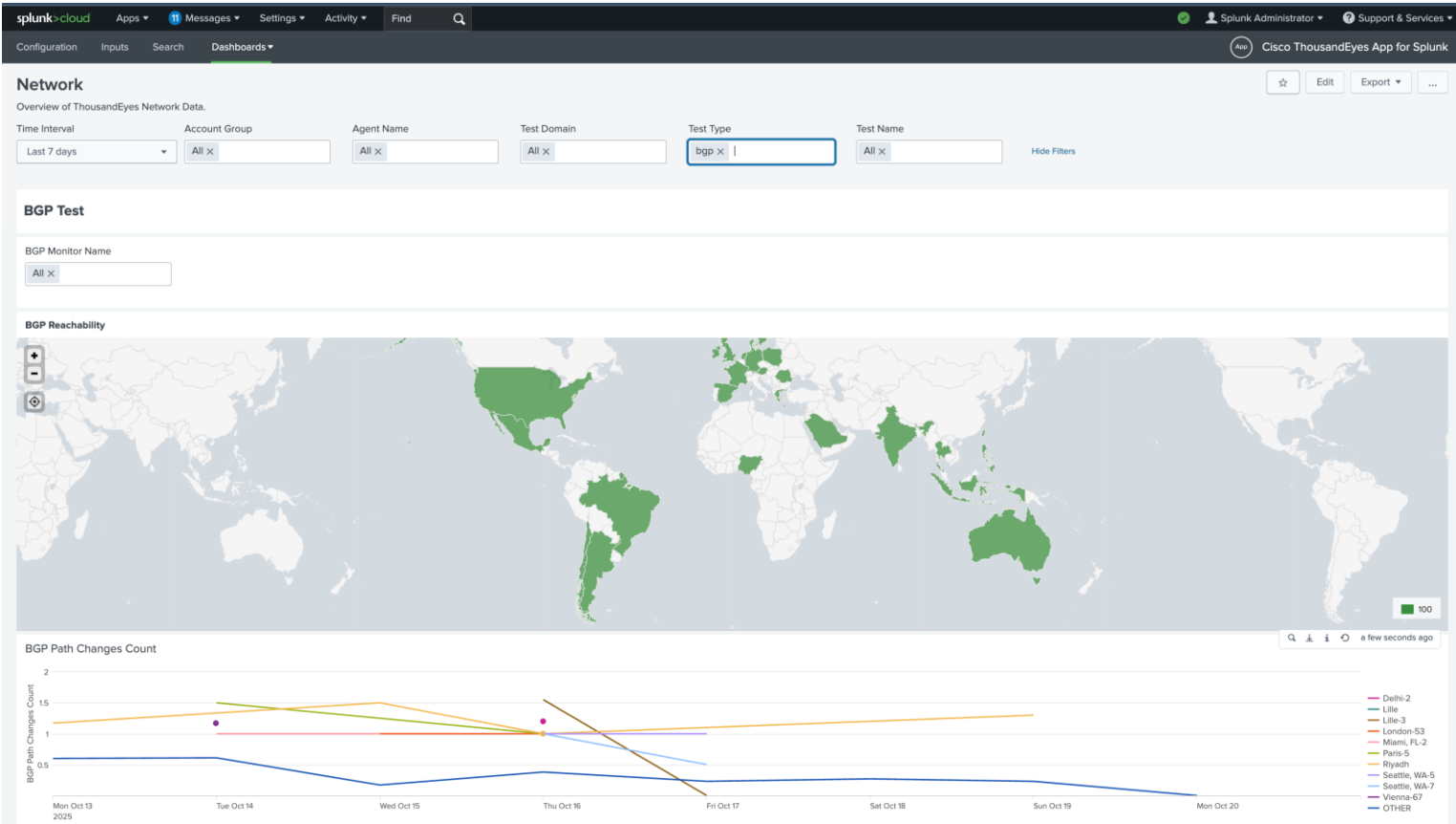
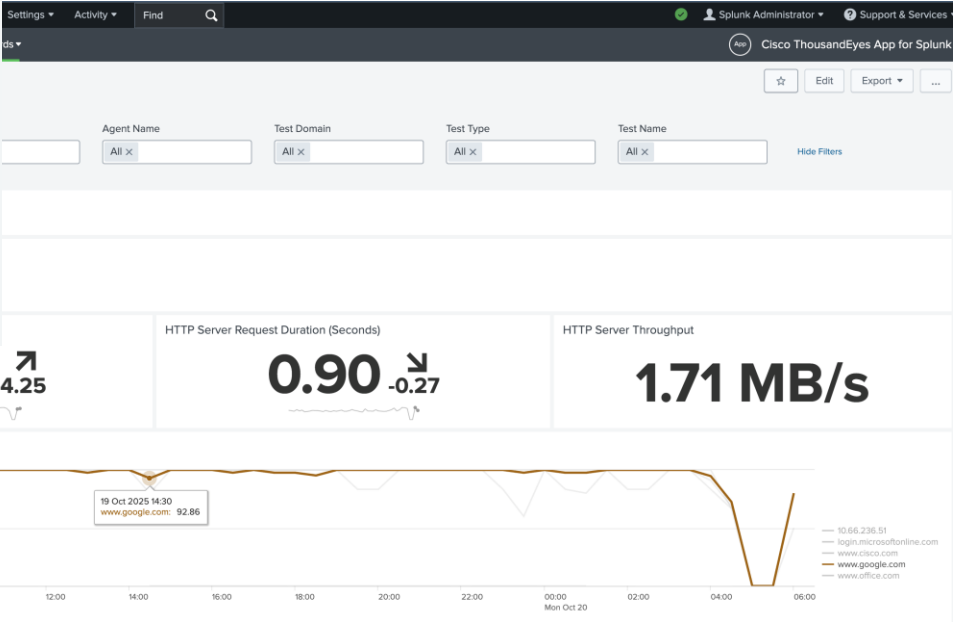
HEC Target: https://http-inputs-scv-shw-474714c1af0e16.sp
Example HEC Target
- For Splunk Cloud Platform: 'https://http-inputs-<host>-splunkcloud.com:443/services/collector/event'
- For Splunk Enterprise: 'https://<host>:8088/services/collector/event'

HEC Token: victoriahec
Select HEC token configured on the Splunk instance. If no token configured, please configure one.
[Configuring HEC.](#)

Test Index: main
Select Index for Trace Data.

Cancel Update

ThousandEyes Add-On for Splunk – Dashboards



Demo – Splunk Enterprise Networking

Events And Incident Viewer

Time Range

Last 24 hours

Source

All X

Submit

Hide Filters

Top 10 Alarms



Number of Issues by Priority



Number of Issues by Severity



Splunk IT Service Intelligence (ITSI)

Introduce Intelligence with Splunk ITSI

Complete Business Visibility

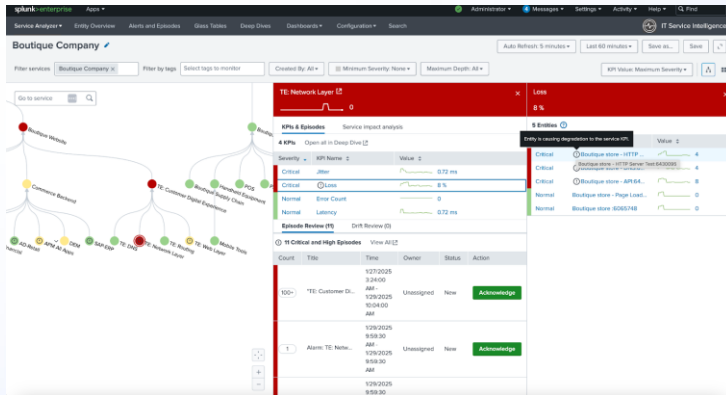
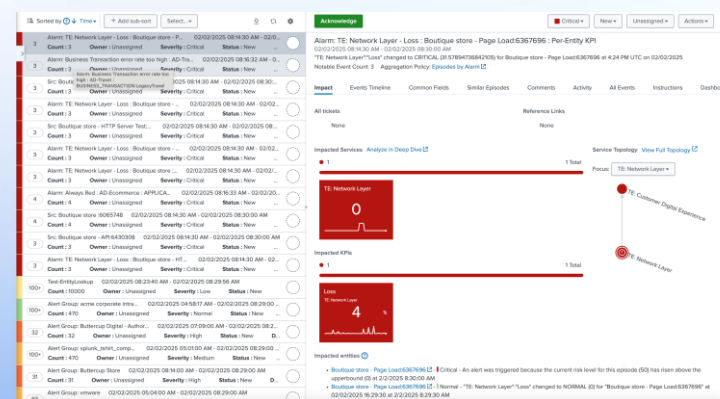
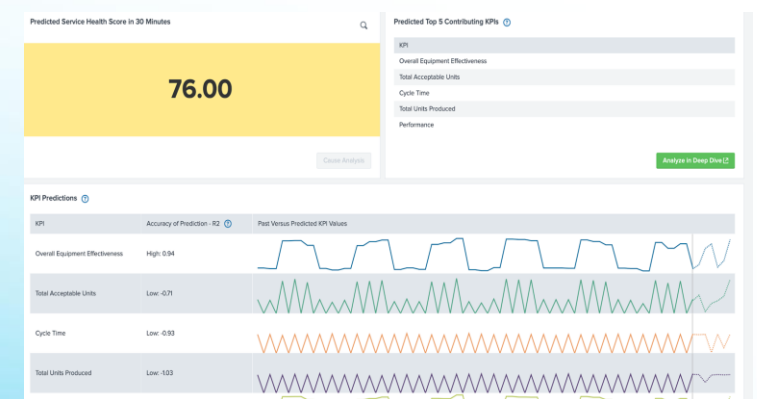
Eliminate **fragmented visibility** with a single view and **accelerate RCA**

Intelligent Incident Management

Accelerate MTTR using real-time event correlation and automated prioritization

Proactive Incident Prevention

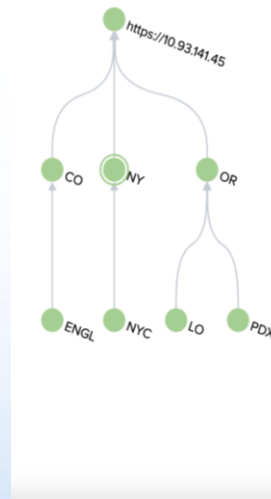
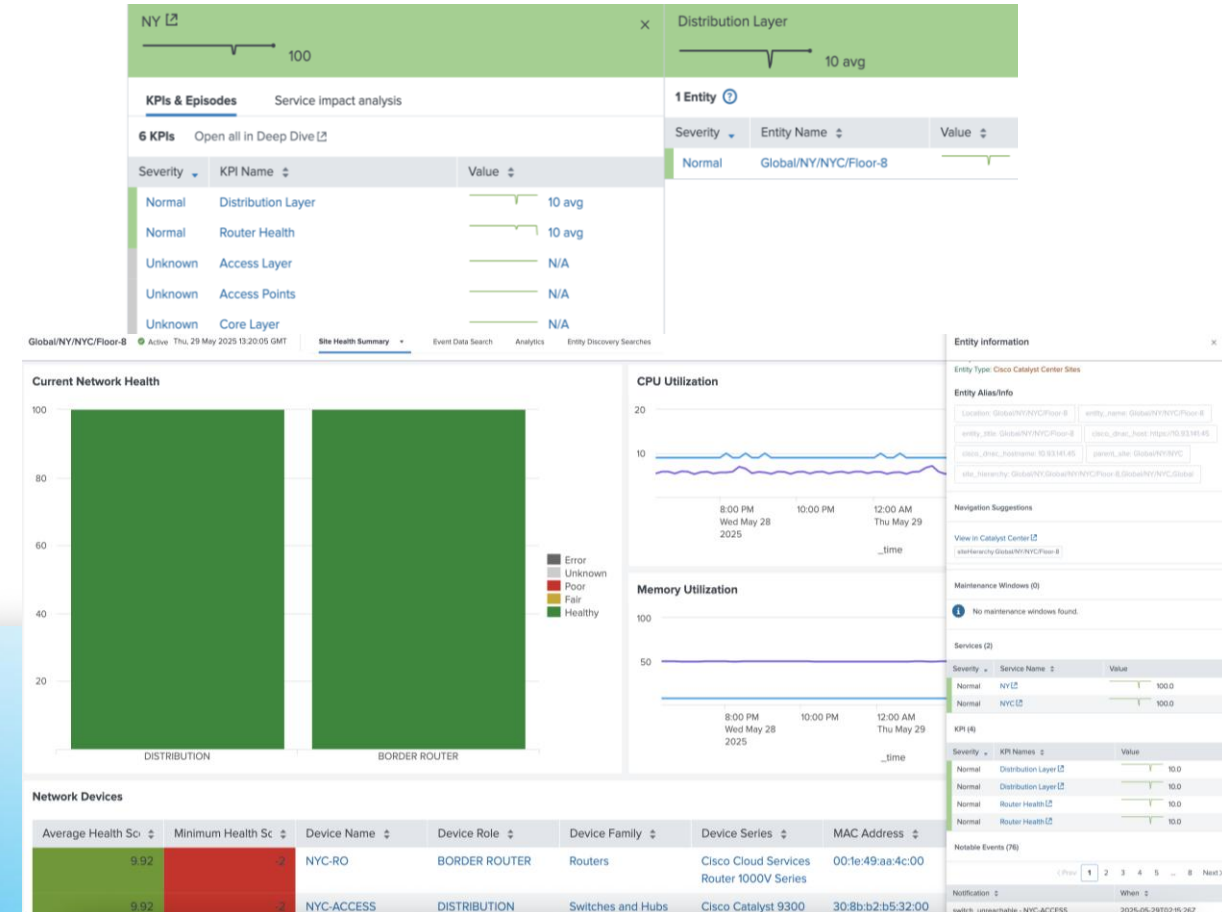
Detect anomalies and **predict issues 30 mins earlier** for **outage prevention**



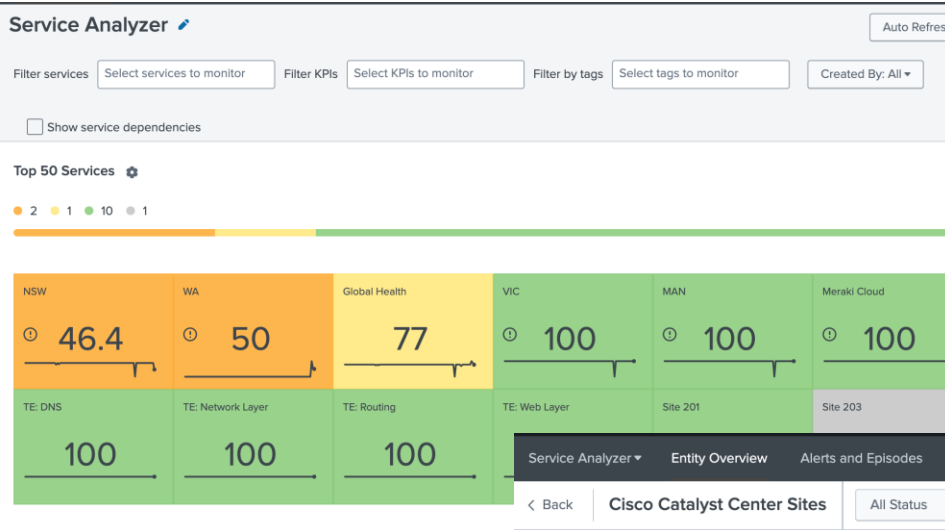
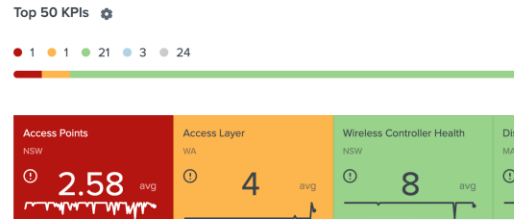
Splunk ITSI and Catalyst Center Integration

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



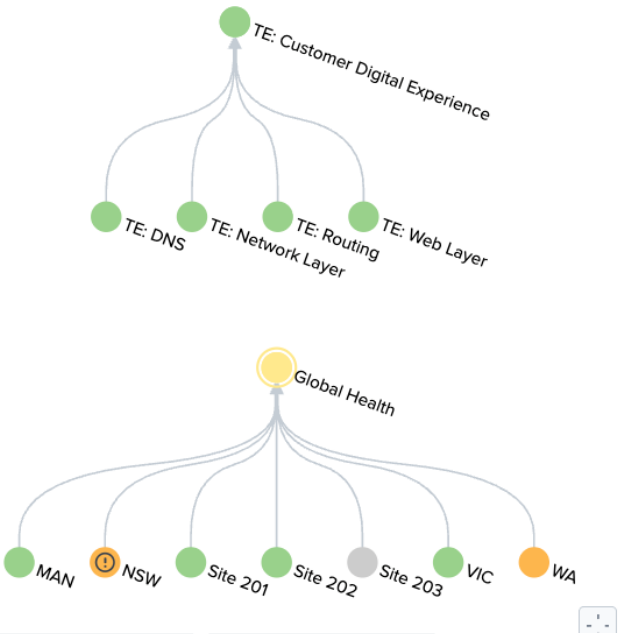
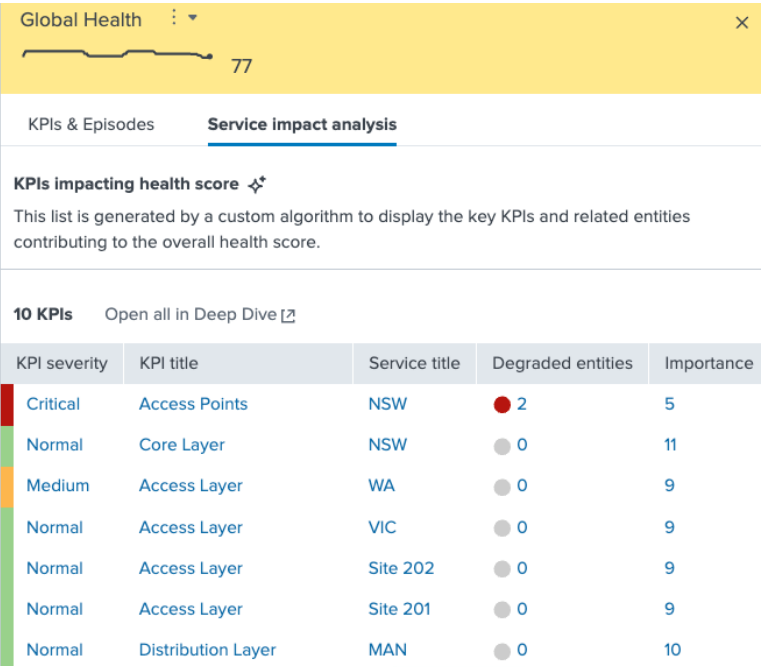
Splunk ITSI Service Analyzer



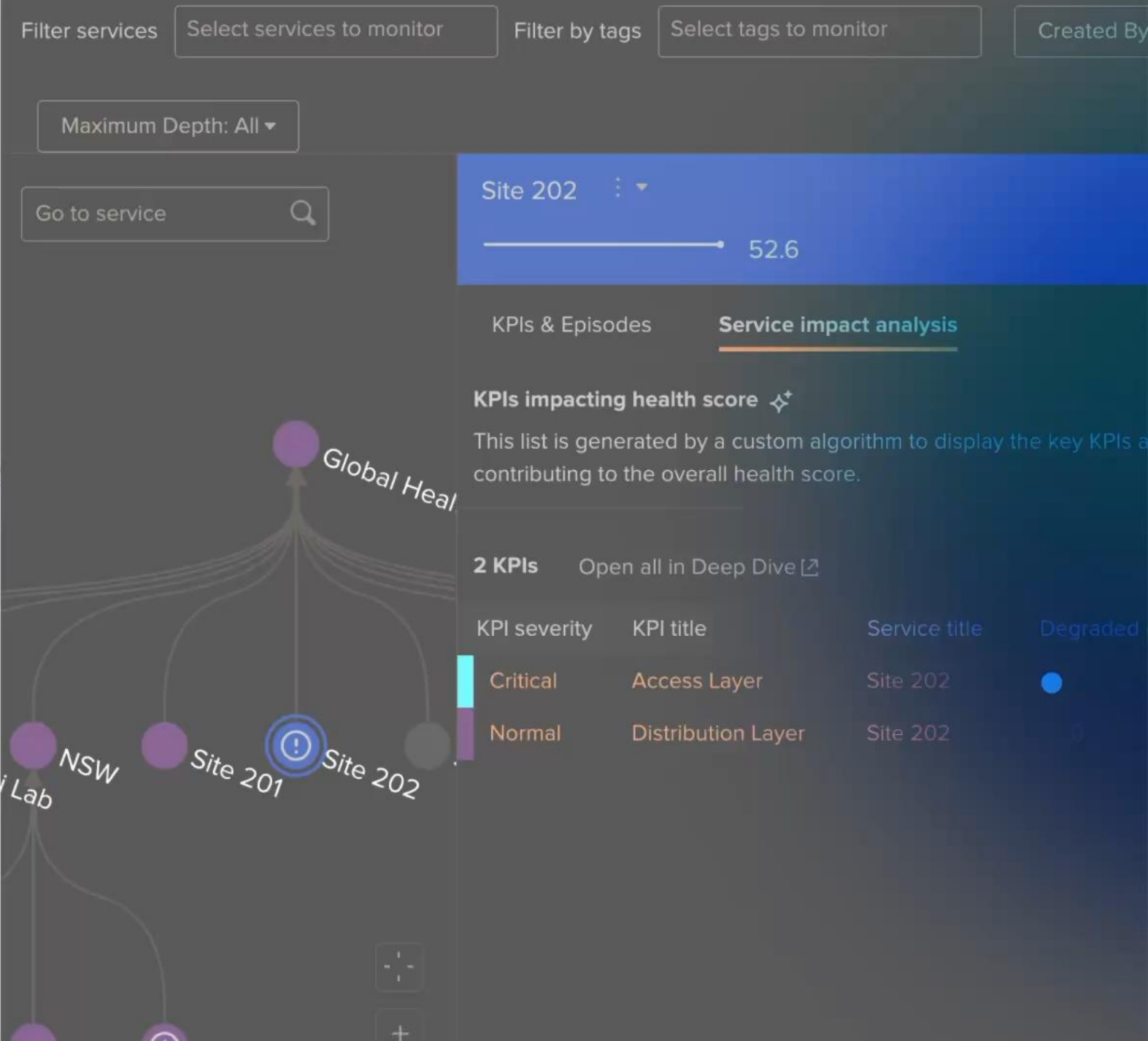
77.78%

77.78% 0.00

44.44% 0.00



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 !

