



# InterSight Add-on for Splunk

## An Introduction

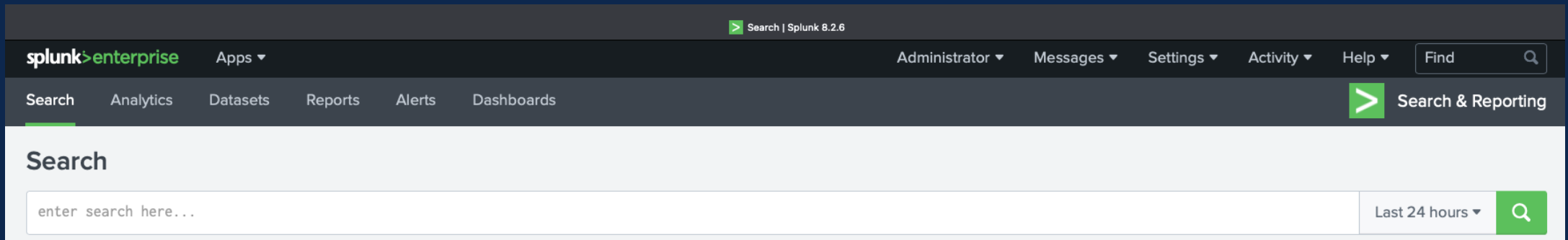
Jeremy Williams, Technical Solutions Architect

August 2022

# What is Splunk?

*Splunk says...*

“The data platform that helps turn data into action for Observability, IT, Security and more.”



# Splunk Architecture

## Data Collection

Handles data inputs such as modular or scripted inputs, network inputs, and HTTP Event Collector. Forwards data to indexers.

Sometimes called a Forwarder or Heavy Forwarder.

## Index Tier

Handles data-manipulation functionality including parsing, indexing, and search. Indexes data, transforming raw data into events and placing results into an index.

Sometimes called an Indexer or Search Peer.

## Search Tier

Handles search-time functionality, and includes dashboards, searches, macros, tags, lookups, data models, and other knowledge objects.

Sometimes called a Search Head.



*Each function can be separated and scaled onto many servers in large environments or all functions can be combined onto a single server for very small environments.*

# Splunk Application Architecture

## Add-On

An add-on is an application that provides specific capabilities to assist in gathering, normalizing, and enriching data sources.



## App

An app is an application that runs on the Splunk platform. Apps are designed to analyze and display knowledge around a specific data source or data set.

*The Add-on gets the data from Intersight into Splunk. That is available now.  
The App provides pre-determined reports and dashboards. That has not been built yet.*

# Splunk Deployment Models

## splunk® > enterprise

Traditional software distribution model.

Deploy the provided packages on your choice of server Operating System either on-premise or in the cloud.

Supports all Apps and Add-Ons.

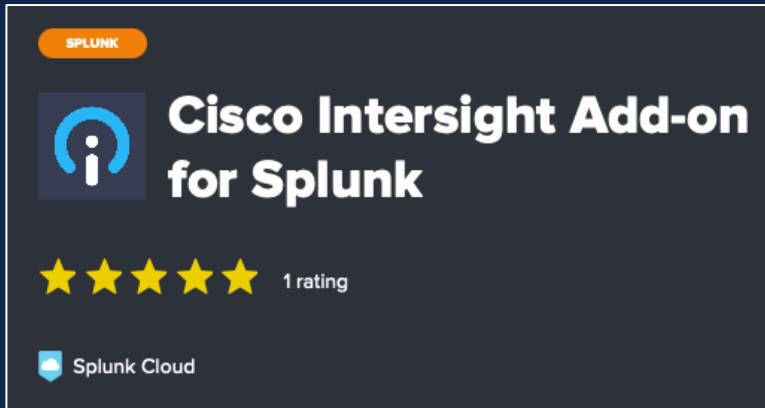
## splunk® > cloud™

As-a-Service model.

Splunk managed and deployed for the customer. Some differences in features and capabilities compared to Splunk Enterprise.

Supports a subset of published Apps and Add-Ons.

# Cisco Intersight Add-on for Splunk

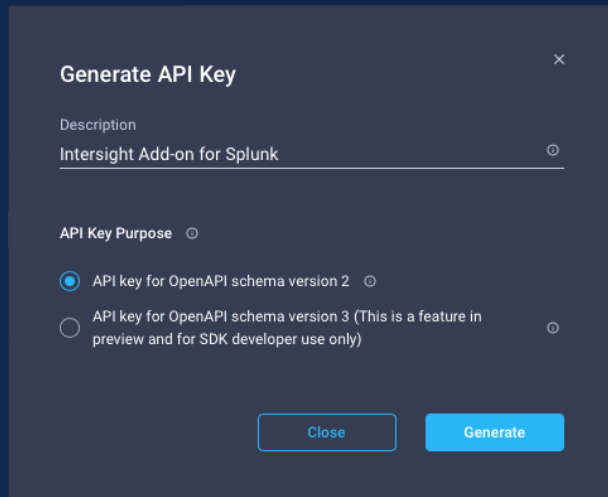


- ✓ Compatible with Splunk Enterprise 8.0 or later
- ✓ Compatible with Splunk Cloud
- ✓ Published on Splunkbase (the Splunk app store)...
  - <https://splunkbase.splunk.com/app/6482/>
- ✓ Also published on GitHub...
  - <https://github.com/jerewill-cisco/intersight-splunk-addon>
- ✓ Documentation, examples, troubleshooting, and more are available at the GitHub repository.
- ✓ Written in Python targeting the 3.7 release

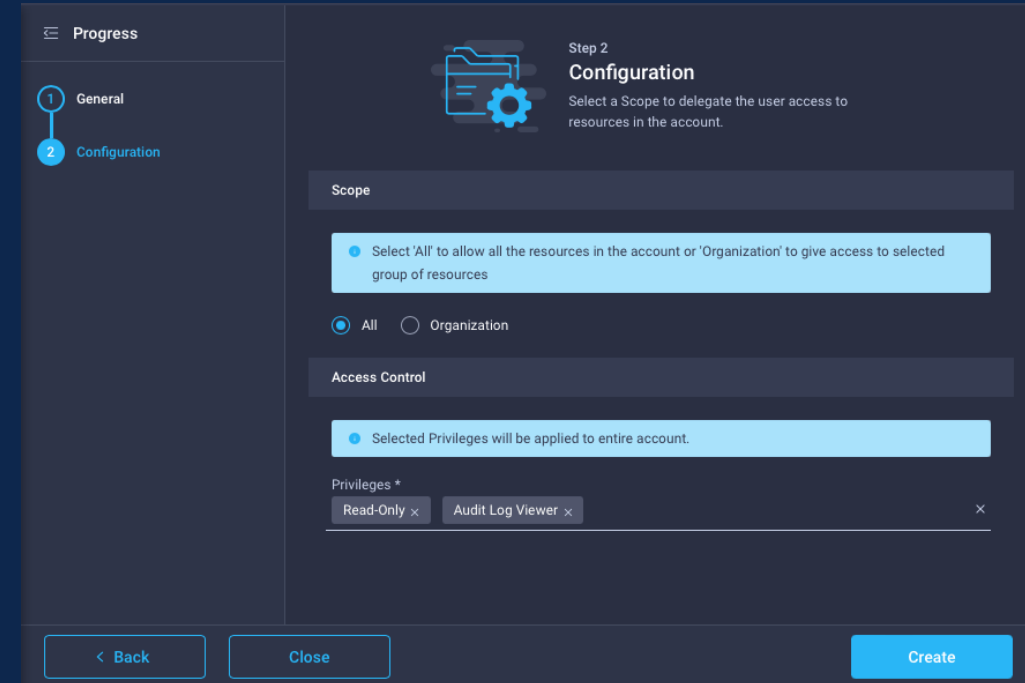


# Cisco Intersight Add-on for Splunk

Data is retrieved from Intersight using the REST API and an Intersight API Key



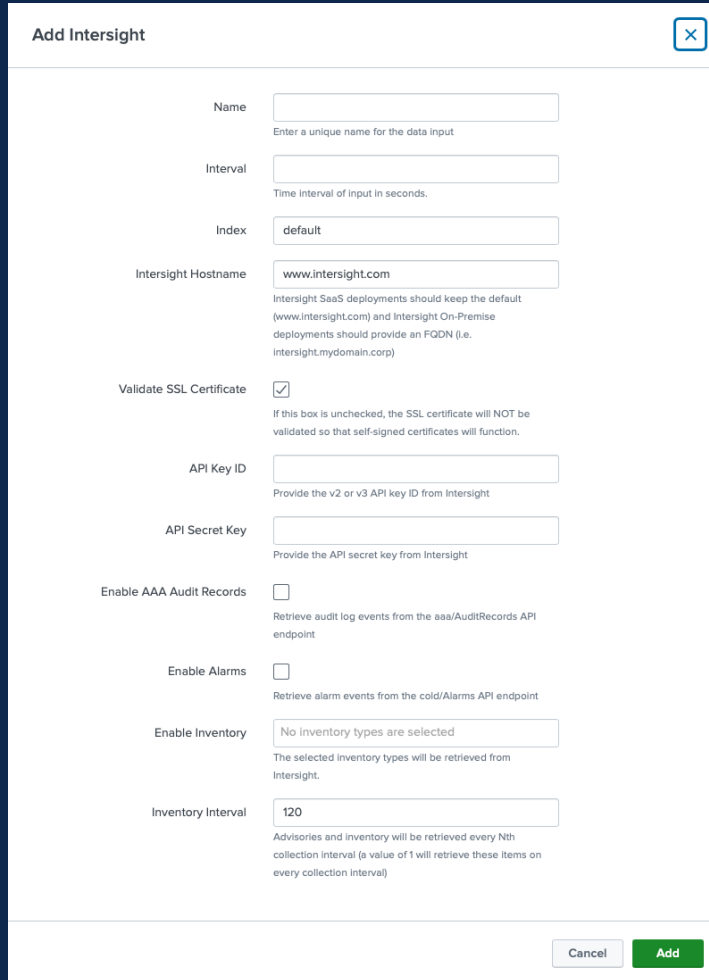
The 'Generate API Key' dialog box is shown with a close button (X) in the top right corner. It contains a 'Description' field with the text 'Intersight Add-on for Splunk'. Below this is the 'API Key Purpose' section with two radio button options: 'API key for OpenAPI schema version 2' (selected) and 'API key for OpenAPI schema version 3 (This is a feature in preview and for SDK developer use only)'. At the bottom are 'Close' and 'Generate' buttons.



The 'Configuration' step is shown in a multi-step progress bar. The 'Scope' section has a blue box with the text 'Select 'All' to allow all the resources in the account or 'Organization' to give access to selected group of resources'. Below this are two radio buttons: 'All' (selected) and 'Organization'. The 'Access Control' section has a blue box with the text 'Selected Privileges will be applied to entire account.'. Below this is a 'Privileges \*' section with two buttons: 'Read-Only' and 'Audit Log Viewer'. At the bottom are '< Back', 'Close', and 'Create' buttons.

Most of the functionality will work with an API key having the system defined Read-Only role. But to get the Audit Logs while maintaining a least privilege access model, I suggest that creating a custom role that includes the Read-Only and Audit Log Viewer privileges.

# Cisco Intersight Add-on for Splunk



The screenshot shows the 'Add Intersight' configuration window. It includes fields for Name, Interval, Index, Intersight Hostname, Validate SSL Certificate (checked), API Key ID, API Secret Key, Enable AAA Audit Records, Enable Alarms, Enable Inventory (with a dropdown showing 'No inventory types are selected'), and Inventory Interval (set to 120). The form has 'Cancel' and 'Add' buttons at the bottom right.

**Add Intersight**

Name   
Enter a unique name for the data input

Interval   
Time Interval of input in seconds.

Index

Intersight Hostname   
Intersight SaaS deployments should keep the default (www.intersight.com) and Intersight On-Premise deployments should provide an FQDN (i.e. intersight.mydomain.corp)

Validate SSL Certificate ☒  
If this box is unchecked, the SSL certificate will NOT be validated so that self-signed certificates will function.

API Key ID   
Provide the v2 or v3 API key ID from Intersight

API Secret Key   
Provide the API secret key from Intersight

Enable AAA Audit Records ☐  
Retrieve audit log events from the aaa/AuditRecords API endpoint

Enable Alarms ☐  
Retrieve alarm events from the cold/Alarms API endpoint

Enable Inventory   
The selected inventory types will be retrieved from Intersight.

Inventory Interval   
Advisories and inventory will be retrieved every Nth collection interval (a value of 1 will retrieve these items on every collection interval)

The Add-on's primary function is to provide a python scripted input that retrieves data from Intersight.

- Either SaaS or On-premise appliance deployments of Intersight are supported
- Various data types are selectable in the input
- Multiple instances of the inputs are supported to gather data from any combination of Intersight SaaS and On-Premise accounts



# Examples

# New Search

Save As

Create Table View

Close

sourcetype="cisco:intersight:licenseAccountLicenseData" source="Richfield-Lab" | dedup Moid

Last 7 days

✓ 1 event (7/27/22 3:00:00.000 PM to 8/3/22 3:13:52.000 PM) No Event Sampling

Job

||

Verbose Mode

Events (1)

Patterns

Statistics

Visualization

Format Timeline

List

Format

20 Per Page

<div>&lt; Hide Fields</div> <div>All Fields</div>		i	Time	Event
<div>SELECTED FIELDS</div> <div>a host 1</div> <div>a source 1</div> <div>a sourcetype 1</div> <div>INTERESTING FIELDS</div> <div>a AccountId 1</div> <div>a AccountMoid 1</div> <div>a AuthExpireTime 1</div> <div>a AuthInitialTime 1</div> <div>a AuthNextTime 1</div> <div>a Category 1</div> <div>a CreateTime 1</div> <div>a DefaultLicenseType 1</div>		>	8/3/22 1:47:49.000 PM	{ [-] <b>AccountId:</b> 5981bd053e95200001fd5632 <b>AccountMoid:</b> 5981bd053e95200001fd5632 <b>AuthExpireTime:</b> 2022-11-01 08:23:06 <b>AuthInitialTime:</b> 2022-08-03 08:28:07 <b>AuthNextTime:</b> 2022-09-02 08:28:07 <b>Category:</b> e <b>CreateTime:</b> 2018-01-24T03:51:55.867Z <b>DefaultLicenseType:</b> Premier <b>ErrorDesc:</b> <b>Group:</b> default <b>HighestCompliantLicenseTier:</b> Premier <b>LastCssmSync:</b> 2022-07-29T19:13:26.614Z <b>LastRenew:</b> 2022-07-28T12:05:35.071Z <b>LastSync:</b> 2022-08-03T08:26:34.973Z



# New Search

Save As ▾







Create Table View

Close

sourcetype=cisco:intersight:aaaAuditRecords MoDisplayNames.Name{}=test102 | [table](#) ModTime, Email, MoType, Event, MoDisplayNames.Name{}

Last 30 days ▾

✓ 6 events (7/4/22 12:00:00.000 AM to 8/3/22 2:42:31.000 PM) No Event Sampling ▾

Job ▾ Verbose Mode ▾

Events (6)

Patterns






Statistics (6)

Visualization

100 Per Page ▾

 Format

Preview ▾

ModTime ▾ 	Email ▾ 	MoType ▾ 	Event ▾ 	MoDisplayNames.Name() ▾ 
2022-07-27T13:41:56.886Z	tkaryano@cisco.com	server.Profile	Modified	test102
2022-07-27T13:41:56.886Z	tkaryano@cisco.com	server.Profile	Modified	test102
2022-07-27T13:41:56.886Z	tkaryano@cisco.com	server.Profile	Created	test102
2022-07-27T12:21:16.273Z	tkaryano@cisco.com	server.Profile	Modified	test102
2022-07-27T12:19:12.275Z	tkaryano@cisco.com	server.Profile	Modified	test102
2022-07-27T12:18:43.026Z	tkaryano@cisco.com	server.Profile	Created	test102


# New Search

Save As ▼







Create Table View

Close

index=\* sourcetype=cisco:intersight:tamAdvisoryInstances source="Richfield-Lab" | dedup Moid | rename AffectedObjectType as type, Advisory .AdvisoryId as Id, Advisory.Severity.Level as Severity | sort Severity | stats count by source, Id, Severity | rename count as Instances

Last 24 hours ▼

✓ 34 events (8/1/22 5:00:00.000 PM to 8/2/22 5:58:16.000 PM) No Event Sampling ▼

Job ▼ ||       Verbose Mode ▼

Events (34)

Patterns




Statistics (4)

Visualization

100 Per Page ▼

 Format

Preview ▼

source ↕ 	Id ↕	Severity ↕ 	Instances ↕ 
Richfield-Lab	INTEL-SA-00601	high	31
Richfield-Lab	cisco-sa-20160927-openssl	medium	1
Richfield-Lab	cisco-sa-20170405-cimc	medium	1
Richfield-Lab	cisco-sa-20180104-cpusidechannel	medium	1

# New Search

Save As

Create Table View

Close

```
sourcetype=cisco:intersight:condAlarms | dedup Moid | search Severity != "Cleared" | table AncestorMoId, Code, Description, Severity, Acknowledge | rename AncestorMoId as Moid | join Moid [search sourcetype=cisco:intersight:computePhysicalSummaries | dedup Moid] | table Name, Model, Serial, UserLabel, Severity, Code, Description, Acknowledge
```

Last 7 days

✓ 10 events (7/27/22 2:00:00.000 PM to 8/3/22 2:58:21.000 PM) No Event Sampling

Job

Verbose Mode

Events (10)

Patterns

Statistics (3)

Visualization

100 Per Page

Format

Preview

Name	Model	Serial	UserLabel	Severity	Code	Description	Acknowledge
UCSM-1-6	UCSB-B200-M3	FCH173974R2		Critical	F0314	Server 1/6 (service profile: ) discovery: failed	None
UCSM-1-6	UCSB-B200-M3	FCH173974R2		Critical	F0868	Motherboard of server 1/6 (service profile: ) power: failed	Acknowledge
UCSM-1-6	UCSB-B200-M3	FCH173974R2		Critical	F0311	Server 1/6 (service profile: ) oper state: inoperable	Acknowledge



# New Search

Save As

Create Table View

Close

```
index=* sourcetype=cisco:intersight:*Summaries source="Richfield-Lab" | dedup Moid | eval version=coalesce(Version,Firmware) | rex field=SourceObjectType "compute\.(?<ComputeType>.*)" | eval Type=coalesce(ComputeType,SwitchType)| rename AlarmSummary.Critical as Criticals | rename AlarmSummary.Warning as Warnings | eval Health=case(Criticals >= 1,"Critical", Warnings >= 1,"Warning", 1=1, "Healthy") | rename RegisteredDevice.ConnectionStatus as Status | table source, Status, Health, Type, Name, Model, Serial, version | sort Name
```

Last 24 hours

✓ 49 events (8/1/22 5:00:00.000 PM to 8/2/22 5:47:46.000 PM) No Event Sampling

Job

Verbose Mode

Events (49)

Patterns

Statistics (49)

Visualization

100 Per Page

Format

Preview

source	Status	Health	Type	Name	Model	Serial	version
Richfield-Lab	Connected	Healthy	RackUnit	ASGARD-APIC01-CIMC	APIC-SERVER-L2	FCH1951V247	4.1(2f)
Richfield-Lab	Connected	Warning	RackUnit	C240-FCH1934V3CR	UCSC-C240-M4SX	FCH1934V3CR	4.1(2g)
Richfield-Lab	Connected	Healthy	RackUnit	R143D-APIC1-cimc	APIC-SERVER-M2	FCH1945V3MR	4.1(2g)
Richfield-Lab	Connected	Critical	RackUnit	R143D-ESX01-cimc	HX240C-M4SX	FCH2042V1N1	4.1(2g)
Richfield-Lab	Connected	Critical	RackUnit	R143D-ESX02-cimc	HX240C-M4SX	FCH2042V1N0	4.1(2g)
Richfield-Lab	Connected	Critical	RackUnit	R143D-ESX03-cimc	HXAF240C-M4SX	FCH2146V37Z	4.1(2g)
Richfield-Lab	Connected	Healthy	FabricInterconnect	heimdall-ucs FI-A	UCS-FI-6454	FD02416171W	9.3(5)I42(1j)
Richfield-Lab	Connected	Healthy	FabricInterconnect	heimdall-ucs FI-B	UCS-FI-6454	FD02416170G	9.3(5)I42(1j)



# New Search

Save As ▾

Create Table View

Close

```
index=* sourcetype=cisco:intersight:hyperflexNodes source="Richfield-Lab" | dedup Moid | chart count by Cluster.Moid, Role | join Cluster.Moid
[search index=* sourcetype=cisco:intersight:hyperflexClusters | dedup Moid | rename Moid as Cluster.Moid, RegisteredDevice.ConnectionStatus
as ConnectionStatus] | join Cluster.Moid [search index=* sourcetype=cisco:intersight:hyperflexStorageContainers | dedup Moid | chart count
by Cluster.Moid, Type] | join Cluster.Moid [search index=* sourcetype=cisco:intersight:hyperflexLicenses | dedup Moid | rename
ComplianceState as LicenseState | table Cluster.Moid, LicenseState, LicenseType]| rename STORAGE as ConvergedNodes, COMPUTE as
ComputeOnlyNodes, Summary.DataReplicationFactor as RF, UtilizationPercentage as Used, Summary.ResiliencyInfo.NodeFailuresTolerable as FTT,
HypervisorType as Hypervisor | eval StorageCapacity.TB=round(StorageCapacity/1024/1024/1024, 1)| eval Used=round(Used, 0).%" | eval
sort=upper(ClusterName) | sort source, sort | fields ClusterName, DeploymentType, LicenseType, LicenseState, DriveType, Hypervisor, RF, FTT
, ConvergedNodes, NFS, iSCSI, StorageCapacity.TB, Used
```

Last 24 hours ▾

🔍

✓ 12 events (8/1/22 6:00:00.000 PM to 8/2/22 6:03:02.000 PM) No Event Sampling ▾

Job ▾

⏸

■

➔

🖨

⬇

🗨 Verbose Mode ▾

Events (12)

Patterns

Statistics (3)

Visualization

100 Per Page ▾

✎ Format

Preview ▾

ClusterName	DeploymentType	LicenseType	LicenseState	DriveType	Hypervisor	RF	FTT	ConvergedNodes	NFS	iSCSI	StorageCapacity.TB	Used
Loki	Datacenter	Evaluation	UNIDENTIFIED	All-Flash	IWE	THREE_COPIES	1	4	0	2	8.6	1%
Panther	Datacenter	Evaluation	UNIDENTIFIED	All-Flash	ESXi	THREE_COPIES	1	4	1	0	17.9	1%





The bridge to possible