

Migrating to Splunk Cloud

Adopting a cloud strategy enables organizations of all sizes to increase agility, reduce costs, decrease time to market and empower innovation. As you embark on your migration journey with Splunk, we'd like to equip you with the right resources and tools.

The Splunk Cloud Advantage

Splunk® Cloud™ delivers the capabilities of Splunk as Software-as-a-Service (SaaS), enabling you to make confident decisions and take decisive action on insights from your data without the need to purchase, manage and deploy additional infrastructure. Ensure fast time to value, security and reliability by outsourcing your infrastructure management and admin tasks to Splunk, so your employees can focus on core, high-priority activities.

- **Service excellence:** With your IT backend managed by our Splunk experts, you can focus on acting on your data
- **Fewer infrastructure requirements:** Splunk-provisioned and -managed infrastructure delivers a turnkey, cloud-based data analytics solution
- **Certified: FedRAMP Authorized at the Moderate Impact Level** by GSA FedRAMP PMO; FedRAMP offering meets U.S. persons requirements under ITAR; **SOC 2 Type 2, ISO 27001, PCI and HIPAA compliant.**



Getting Started

First, download the free [Splunk Migration Assessment App](#), which helps you analyze your on-premises Splunk installation and understand the configuration to move your deployment into Splunk Cloud.

Should I reconfigure my Splunk environment or migrate existing settings?

There are two options to consider when moving to Splunk Cloud:

1. You may wish to start with a brand new Splunk Cloud stack and re-install your apps and re-create your dashboards manually. This is often appropriate for simple environments, and appropriate if you are planning to address new use cases or tidy up historic configurations.
2. Alternatively, if you want your new Splunk Cloud environment to be configured like your existing on-premises Splunk Enterprise environment you can copy your old configurations and settings. Optionally, you can also copy your existing ingested data to allow seamless historic searching. This option requires [engaging with Splunk Professional Services](#). Reach out to your account team or to ps-sales@splunk.com for more information.

Whichever option you choose, please consider that you need to maintain your existing environment to accurately transfer and validate anything moved from the existing environment to Splunk Cloud.

Key Things to Remember Prior to Your Migration

1. Understand the service and differences between on-premises Splunk deployments and Splunk Cloud

- Splunk Cloud and Splunk Enterprise have significant feature overlap (>95%). However, some features are implemented differently. Detailed differentiation is documented [here](#).
- Splunk Cloud is a standardized service (SaaS) offering. When moving a Splunk on-premises/ hosted configuration, it may require modification to ensure compatibility with the standardized service (SaaS) offering.

- It is the same service no matter which underlying cloud service provider you choose: AWS or Google Cloud. Note that FedRAMP is only supported on AWS.
- The [Cloud Migration Assessment App](#) helps you understand the tasks that will need to be carried out to perform a migration and provides an optional export that can be sent for additional review and scoping.
- Hybrid deployments have additional considerations. See the table in the [search section in the Service Description](#) for details.

	Responsibility	Splunk Enterprise Deployed On-Premises	Splunk Cloud	
Admin Tasks: One-time Setup	Purchase/rent HW	Customer	Splunk	Managing a Splunk deployment involves 12 ongoing admin tasks, 6 of which are conducted by Splunk for a Cloud-based deployment
	Rack and stack, cable, network all HW	Customer	Splunk	
	Install Splunk	Customer	Splunk	
	Install OS	Customer	Splunk	
	Configure Splunk (create users, load apps, configure)	Customer	Splunk	
	Configure indexes	Customer	Splunk	
	Setup HA/clustering	Customer	Splunk	
	Setup disaster and recovery	Customer	Splunk	
	Configure forwarders	Customer	Customer	
	Onboard data	Customer	Customer	
	Integrate with LDAP/AD	Customer	Joint	
Admin Tasks: Ongoing	Scale up HW	Customer	Splunk	
	Install Splunk patches/upgrades	Customer	Splunk	
	Install OS patches/upgrades	Customer	Splunk	
	Monitor deployment/health checks	Customer	Splunk	
	Manage forwarders	Customer	Customer	
	Create users/roles	Customer	Customer	
	Manage indexes	Customer	Customer	
	Onboard additional data	Customer	Customer	
	Load search head only apps	Customer	Joint	
	Load distributed apps	Customer	Joint	
	Load premium apps	Customer	Splunk	
	Export data	Customer	Customer	
User Tasks	Search, alerts, reports, dashboards	Customer	Customer	

2. Understand the shared responsibility between you and Splunk

Both Splunk and you are responsible for supporting your Splunk Cloud environment.

The focus is on making the user experience as self-serviced as possible, while Splunk helps administer the rest as indicated in the table on the previous page. Updates that need to be made by Splunk are requested by logging a support ticket, and the changes will be addressed per SLO's associated with your [Support Plan](#) — see [“Support Offerings” for the overview and the estimated](#) response times for P3 tickets.

3. Understand service capability (Apps and add-ons)

Splunk Cloud environments meet strict security and compliance standards as described in the [service description](#). In order to guarantee secure, compliant and reliable service, any Splunk Apps or Add-ons that are deployed into Splunk Cloud must be approved for Splunk Cloud.

Many standard Splunk Apps and Add-ons have already been approved for Splunk Cloud, and these are indicated in Splunkbase as Splunk Cloud

compatible. These apps and add-ons can either be deployed directly by the user Splunk Cloud admin via the UI or by a member of Splunk Support when you raise a request.

You can determine if an app or an add-on has been Splunk Cloud approved by checking its corresponding page on [Splunkbase](#). The app or add-on will indicate “Splunk Cloud” the list of compatible products.

If the app or add-on has not been Splunk Cloud approved, which includes all Custom Apps, then the user Splunk Cloud Admin can submit the app or add-on online for vetting. If the app passes vetting, then the user Splunk Cloud admin can follow instructions for installing the app. If the app does not pass vetting, then the app will need to be updated until it does. Splunk Professional Services can assist with understanding app vetting requirements and provide guidance on paths forward.

Criteria for passing app vetting are shown on [Splunk Dev](#). The checks performed are indicated with an “x” in the Cloud column. You can also validate apps in advance using Splunk’s [AppInspect API or CLI Tool](#), although additional manual checks may be required. Splunk Dev also outlines the [app vetting process](#).

Overview
Details

The Cisco Networks App for Splunk Enterprise includes dashboards, data models and logic for analyzing data from Cisco IOS, IOS XE, IOS XR and NX-OS devices using Splunk® Enterprise.

Install this App on your search head. Install the Cisco Networks Add-on (TA-cisco_ios) on your search head AND indexers/heavy forwarders.

Supported Cisco Devices:

- * Cisco Catalyst series switches (2960, 3650, 3750, 4500, 6500, 6800, 7600 etc.)
- * Cisco ASR - Aggregation Services Routers (900, 1000, 5000, 9000 etc.)
- * Cisco ISR - Integrated Services Routers (800, 1900, 2900, 3900, 4451 etc.)
- * Cisco Nexus Data Center switches (1000V, 2000, 3000, 4000, 5000, 6000, 7000, 9000 etc.)
- * Cisco Carrier Routing System
- * Other Cisco IOS based devices (Metro Ethernet, Industrial Ethernet, Blade Switches, Connected Grid etc.)
- * Cisco WLC - WLAN Controller

Release Notes

Version 2.5.8 May 28, 2019

Fixed issues

Version 2.5.8 of the Cisco Networks app fixes the following Issues:

- Overview dashboard not showing due to bug with index filter (this release actually fixes it)
- Some fields have been renamed to align with field names in TA-cisco_ios because FIELDALIAS behaviour has changed in Splunk 7.2

4,506

Installs

50,937

Downloads

LOGIN TO DOWNLOAD

VERSION

2.5.8 ▾

BUILT BY

Mikael Bjerkeland

SUPPORT ⓘ

Not Supported

[Questions on Splunk Answers](#)

[Flag as inappropriate](#)

Technologies: [Cisco](#)

COMPATIBILITY

Products: [Splunk Enterprise](#) [Splunk Cloud](#)

Splunk Versions: [8.0](#), [7.3](#), [7.2](#), [7.1](#), [7.0](#)

Platform: Platform Independent

CIM Versions: [4.x](#)

Documentation, Education and Getting Help

- Read the [Splunk Cloud Service Description](#) thoroughly, which gives details about the service
- Read the Splunk Cloud [Admin Manual](#) for an overview of working in Splunk Cloud
- If you are, or will be a Splunk Cloud Admin (sc admin), take the [Splunk Cloud Administration course](#) and refer to documentation on the [Cloud Monitoring Console](#) for continuous monitoring of the health and usage of your Splunk Cloud stacks
- If you need help as a Splunk Cloud customer, based on your support contract, you can check [Splunk Answers](#) and [Splunk Docs](#) for guidance, contact [Splunk Support](#) or log a request on the [Splunk Support Portal](#) for change requests and other issues

Service Level Agreement and Maintenance Policy

Splunk's commitment to the customer regarding Splunk Cloud maintenance policy and service availability are defined by two documents:

1. [Splunk Cloud Service Maintenance Policy](#): Outlines what to expect for scheduled maintenance or upgrade events in Splunk Cloud.

2. [Splunk Cloud Service Level Schedule](#): Outlines Splunk Cloud's Service Level Commitment, including our uptime and availability commitment, exclusions to what is considered downtime and the customer's recourse in the event the service is unavailable. This is also referenced as our Service Level Agreement or SLA.

Make Your Migration Seamless

Splunk Cloud allows you to take advantage of the industry-leading capabilities of Splunk® Enterprise as a cloud-based service without architecting, procuring and administering the infrastructure. Splunk Cloud allows you to flexibly, easily and quickly scale the system to your needs, and the experts running Splunk Cloud provide a reliable and compliant system.

We're committed to making the migration experience from Splunk on-premises to Splunk Cloud as seamless as possible for you. Make sure to use the [Splunk Migration Assessment app](#) for guidance and read the [Splunk Cloud Service Description](#); Splunk Professional Services provides [Migration Success Offerings](#) to assist you through the process as well.



Reach out to your sales contact, customer success manager (CSM) or renewal representative today to get up and running in Splunk Cloud.



Learn more: www.splunk.com/asksales

www.splunk.com