Splunk Assist FAQ

Get cloud-powered insights for your on-prem deployment.

About Splunk® Assist

What is Splunk Assist?

Splunk Assist inspects Splunk deployments and makes cloud-powered recommendations to help bridge security gaps and reduce admin overhead when managing your environment. With Splunk Assist, you can 1) Detect critical issues, 2) Receive in-product targeted recommendations to fix detected issues, and 3) Stay up-to-date on new insights automatically - no need to manually update Splunk Assist to get continuous improvements.

What version of Splunk Assist is this?

Splunk Assist is comprised of packages that can be continuously updated with improvements like any other cloud-first service. We released the first version of Splunk Assist at .conf on June 14th, 2022, which included two packages - Cert Assist and Config Assist:

- Cert Assist warns users of certificate expiration, helping to prevent lost connectivity between Splunk nodes.
- Config Assist surfaces insecure configurations within your deployment and provides recommendations to fix those configurations.

Since then, we released a third package - App Assist. App Assist highlights apps not running the latest supported version, which could have security or performance improvements.

Although we don't follow the traditional versioning like other Enterprise apps, the latest version of Splunk Assist, released on October 11, 2022, has the following notable improvements:

- This release will make it easier to activate Splunk Assist by no longer requiring customers to log into a separate portal and download an activation code
- The release also addresses a few bugs, which include license quota enforcement.
- It expands the eligibility of customers to include partners and developers.

Once you have upgraded to 9.0 or higher and turned on Splunk Assist, new updates will not require any action from admins. All proceeding updates will be delivered automatically to your deployments.

Why should a Splunk Admin care about Splunk Assist?

Based on research we conducted, we believe that Splunk Assist will reduce ~25% of a Splunk Admin's efforts spent on low-value activities like managing certificates and configurations. This will give admins more time to focus their efforts on high-value activities like use-case discovery and delivery, adoption enablement, and tracking value realization.

Why should a CTO care about Splunk Assist?

Assist reduces the time an admin spends on low-value operational tasks such as cert updates and adjusting configurations. A CTO will care for this since admins can reallocate the saved time into high-value activities such as use-case and business value generation with Splunk.

Getting Started

How can I get started with Splunk Assist?

- Install or Upgrade your Monitoring Console node to at least Splunk® Enterprise 9.0 (optionally upgrade your Indexers to 9.0 as well for additional insights around certificate management)
- Next, enable “Support Usage Data” under Instrumentation settings
- Ensure port 443 is open and allow outbound traffic to *.scs.splunk.com.
- Finally, enable Splunk Assist from the Monitoring Console.

Can I access Splunk Assist insights from Splunk Cloud Platform??

No, Splunk Assist is currently not available in Splunk Cloud Platform.

If I already turned on Splunk Assist can I turn it off?

Yes, you can disable Splunk Assist by disabling the backend app that is processing data. Under “Manage Apps” look for the app “splunk_assist” and disable it.

Pricing

How much does Splunk Assist cost?

This is no additional cost, in-product, hybrid capability. Customers who opt into Splunk 9.0 and higher will not have to pay for Splunk Assist, but they will need to turn it on and be opted in to sharing Support Usage Data telemetry.

Deployment, Configurations, and Data Collection

I don’t want Assist to make any changes to my deployment, even if it’s only updating Splunk Assist-specific packages.

Splunk Assist doesn’t make any changes. It only surfaces any issues and provides steps to fix them. It’s completely under the admin’s control to apply any recommended changes (or not). Being a cloud-native service, one of Splunk Assist’s key value propositions is that it can auto-update itself and keep bringing in net new insights and recommendations and then the admin can decide if and when to take action.

If Splunk Assist knows about the correct configuration, why doesn’t Splunk come with those as the “default” configuration?

Splunk’s default configuration is meant for users to try Splunk out and evaluate it within minutes. Setting up SSL connections and certificates, for any application, be it Splunk or not, takes time.

One size doesn’t fit all. Due to the highly flexible and customizable nature of Splunk, one kind of setup may not be optimal for a different configuration. Hence Splunk Assist provides custom recommendations, based on the specific configuration and setup of the customer.

What type of data does Splunk Assist use to provide the recommendations? Who will have access to such data and for how long?

Splunk Assist is powered by Support Usage Data, which you can read more about, as well as how we use telemetry data, here.

Splunk Assist Versus Other Tools

Does Splunk Assist replace any of the other Splunk management tools?

No, Splunk Assist does not replace any of the other Splunk management tools.

How does Splunk Assist fit into the existing monitoring tools Splunk Enterprise ships today?

Splunk Assist is part of the Monitoring Console. Splunk Assist UI will be powered from the cloud but be accessible when a customer configures and uses the Splunk Enterprise Monitoring Console. The recommendation to include Splunk Assist with the Monitoring Console was influenced by feedback from Splunkers and customers.

Note that customers who do not configure or use the Monitoring Console will not be able to review the cloud-powered recommendations offered by Splunk Assist.

Resources

Where can I learn more about Splunk Assist?

Check out our documentation as well as this blog.

Where can I go if I have more questions?

Please send an email to ssg-splunk-assist@splunk.com and we'll work to respond in 3 to 5 business days.