Splunk Terms for Splunk Offerings

Published: February 2023

Additional terms apply to certain Splunk Offerings. The below terms apply to your Purchased Offerings as applicable and are incorporated into the Splunk General Terms.

Splunk Cloud Platform

1. **Service Description**
   https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice

2. **Security and Protection of Customer Content on Splunk Cloud Platform.**
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk Cloud Platform as set forth in the Splunk Cloud Security Addendum located at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html ("**Cloud Security Addendum**").

   Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Cloud Security Addendum), and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

3. **Service Level Schedule – Splunk Cloud Platform**
   Splunk's Splunk Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html, will apply to the availability and uptime of the Splunk Cloud Platform, subject to planned downtime and any unscheduled emergency maintenance according to Splunk's Maintenance Policy referenced in the Splunk Service Level Schedule. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.

4. **Data Usage Policy for Splunk Cloud Platform**
   For Subscriptions based on Maximum Daily Indexing Volume, Customer is entitled to periodically exceed the daily volume purchased by Customer in accordance with Splunk's data ingestion and daily license usage policy set forth at http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data_ingestion_and_daily_license_usage

5. **FedRAMP or StateRAMP for Splunk Cloud Platform**
   If you access or use any Hosted Services in the specially isolated Amazon Web Services ("**AWS**") GovCloud (US) region that are provisioned in a FedRAMP or StateRAMP authorized environment ("Government Cloud"), you acknowledge the Government Cloud is a more restricted environment. As a more restricted environment, Administrative Access to the Government Cloud must be restricted to individuals that are US Persons, as defined under 22 CFR part 120.62 ("Approved Personnel"). Administrative Access is defined as Customer's users in roles with capabilities that are exclusive to the "Admin" and/or "Sc admin" roles set forth in the "Table of Splunk platform capabilities" page here: https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Rolesandcapabilities#Table_of_Splunk_platform_capabilities.

   Customer acknowledges that FedRAMP or StateRAMP authorized offerings will only meet the standards of an authorized FedRAMP or StateRAMP Hosted Service, respectively, if Customer performs its obligations as set forth in both the "FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet" and the "FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet" available from Splunk upon request. To maintain the security of the FedRAMP or StateRAMP authorized offerings, Customer agrees to cooperate with Splunk to remediate any security vulnerabilities upon Splunk's request.

Splunk On-Call

1. **Service Description**
   The Splunk On-Call service includes the online software service via https://www.splunk.com/en_us/investor-relations/acquisitions/splunk-on-call.html (or at such other URL as may be designated from time to time), including related application programming interfaces, interactive discussion areas, Customer accounts and profiles, mobile applications, and other related components thereof, on an individual and collective basis.

2. **Additional Users**
If Customer wants to add additional permitted users, Customer can do so through the Offering administrative portal, and either (i) Splunk will immediately charge Customer's credit card for the prorated amount for the current term, or (ii) if Customer does not have a credit card on file, then Splunk will invoice Customer for the additional permitted users in accordance with the Terms.

3. **Necessary Integrations**
Customer acknowledges and agrees that in order to provide certain features and functionalities of the Splunk On-Call service to Customer, Customer must allow the Splunk On-Call service communication with or access to Customer's account(s) with other third party service providers to retrieve, manipulate, process, and modify data ("**Process**"), and you expressly consent to the Splunk On-Call service accessing those accounts to Process that data solely as is necessary to provide the Splunk On-Call service. If the Splunk On-Call service cannot for any reason access your third-party accounts or Process that data, Splunk may not be able to provide Customer those features or functionalities, and Splunk will be excused from any nonperformance. Certain features and functionalities of the Splunk On-Call service require interaction with Customer's other third-party service providers, for instance, through APIs belonging to those third parties. Customer consents to Splunk interacting with Customer's other third party service providers in order to provide Customer requested features and functionality, and Customer acknowledges that Splunk is not responsible or liable for the accuracy, content, appropriateness, or completeness of data or content Splunk receives from those third parties.

4. **Support**
Splunk On-Call support is provided via the following portal: https://www.splunk.com/en_us/investor-relations/acquisitions/splunk-on-call.html.

Splunk Observability Cloud
Splunk Observability Cloud includes the following services (as part of a suite or as individual services): Splunk Infrastructure Monitoring, Splunk Application Performance Monitoring (Splunk APM), Splunk Real User Monitoring (Splunk RUM), and Splunk Log Observer, and Splunk Intelligence.

1. **Service Descriptions**
https://docs.splunk.com/Observability

2. **Usage, Subscription Limits Enforcement, and Entitlements**
https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.html

3. **Security and Protection of Customer Content**
   a. Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content as set forth in the Security Addendum located at https://www.splunk.com/en_us/legal/splunk-observability-security-addendum.html ("**Observability Security Addendum**"). Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations.
   b. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Observability Security Addendum), and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

4. **Service Level Schedule – Splunk Observability Cloud**
Splunk's Splunk Observability Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/observability-service-level-schedule.html, will apply to the availability and uptime of the Splunk Observability Cloud. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.

5. **Definitions.** The following definitions are applicable to Orders for Splunk Observability Cloud services.

"Analyzed Trace" means a trace that was sent to and processed by Splunk APM.

"APM Identities" means the count of all unique spans and initiating operations across all service endpoints for metricization. Additional dimensions on these, specified as select span tags, create further APM Identities based on the count of values of those tags.

"Container" means a stand-alone, executable package of software that includes application software and sufficient operating system libraries to run in isolation but shares the underlying operating system with other Containers.

"Custom Metric" means any Metric that is not automatically collected and reported as part of Splunk's standard Host-based integrations.

"High Resolution Metric" means any Metric reported to Splunk that is specifically identified as a High-Resolution Metric

by Customer in a manner specified by Splunk in the service documentation. Any Metric with such designation shall be processed by Splunk at a resolution no coarser than the native reporting resolution or 1-second, whichever is coarser, and shall be retained according to the Metric retention policy of the service edition purchased.

"Host" means a virtual machine or physical server with a dedicated operating system up to 64GB of memory.

"Metric" means any unique combination of a metric name and dimension value reporting data to Splunk within the last hour.

"Monitoring MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to alert on changes in application performance. A Monitoring MetricSet includes metrics such as request rate, error rate, and latency percentiles.

"MTS" means Metric Time Series.

"**Profiled Container**" means a Container that is instrumented to send Profiling data to Splunk APM.

"**Profiling**" means automated collection and analysis of code behavior data from runtime environments.

"**Profiling Volume**" means the amount of Profiling data that customers pay for to be ingested by Splunk APM.

"**Serverless Function**" means a stand-alone, executable package of single-purpose software that runs in serverless environments and is triggered by an event or message.

"**Session Volume**" means the amount of Session data that customers pay for to be ingested by Splunk RUM.

"Span" means an area of code instrumented to be captured as part of a recorded transaction (eg. rpc, function). Each service can have many spans. At a minimum, there will be 2 spans - inbound and outbound to the service.

"TAPM" means Trace Analyzed Per Minute.

"Trace" means an array of spans represented as a Directed Acyclic Graph.

"Trace Volume" means amount of trace data per minute that customers pay for to be ingested by Splunk APM.

"Troubleshooting MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to enable detailed analysis and troubleshooting of an application. A Troubleshooting MetricSet includes metrics such as the request rate, error rate, root-cause error rate and latency percentiles.

Splunk Synthetic Monitoring

1. **Service Description**
   https://help.rigor.com/hc/en-us

2. **Security**
   Customer hereby acknowledges and agrees that Splunk Synthetic Monitoring has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification. **The security terms in Splunk's Cloud Security Addendum and the Observability Security Addendum do NOT apply.** Customer may not upload or transmit to this environment any regulated data, such as financial information (including PCI-DSS data), protected health information, ITAR data or classified information.

3. **Splunk Web Optimization Usage and Subscription Limits Enforcement**
   a. For each pack of 1000 Enterprise Browser Test Runs purchased, Customer receives 1 Web Optimization Scan per month. Unused Web Optimization Scans do not carry over and will be lost at the end of each month, with the number of allowed Web Optimization Scans resetting at the beginning of the next month.
   b. Technical measures within Splunk Web Optimization will prevent Customers from exceeding their licensed monthly limits of Web Optimization Scans.

4. **Splunk Synthetic Monitoring Usage and Subscription Limits Enforcement**.
   a. Splunk measures Customer's usage as the total number of Browser Test Runs, API Test Runs, and Uptime Test Runs during each monthly billing cycle (the "**Synthetic Monthly Usage Level**").
   b. If Customer's Synthetic Monthly Usage Level exceeds the contractual allowable Subscription Limits, Customer agrees to pay Splunk an overage fee (the "**Overage Fee**") calculated as 150% of the prices specified in the table below (prorated as needed), or Splunk may, at its sole discretion, limit Customer's ability to add new monitors until it conforms to the contractual Subscription Limits. Provided, however, that to help Customer avoid improperly incurring fees, if Customer's usage at any time during the term of the General Terms significantly exceeds the Customer's contractual

Subscription Limits (as determined by Splunk at its sole discretion), Splunk may limit Customer's ability to add new monitors, irrespective of Customer's Synthetic Monthly Usage Level.

Product	SKU	Metric	Standard Edition	Enterprise Edition
Splunk Synthetic Monitoring	Splunk Synthetic Monitoring - Browser Tests, 1k Runs per month	Runs per Month	$12	$20
	Splunk Synthetic Monitoring - API Tests, 10k Runs per month	Runs per Month	$4	$6
	Splunk Synthetic Monitoring - Uptime Tests, 10k Runs per month	Runs per Month	$1	$2

For Offerings with Capacity based on monthly metrics, the metrics will be based on billing month measurements.

Splunk Secure Gateway
Splunk Secure Gateway app facilitates communication between mobile devices and Splunk instances with an end-to-end encrypted free cloud service called Spacebridge. Spacebridge cloud service environment, and the service itself, is separate from the Splunk Enterprise and Splunk Cloud offering. Spacebridge is a free Hosted Service and use is subject to Splunk General Terms available at: https://www.splunk.com/en_us/legal/splunk-general-terms.html. See here to learn more about the Spacebridge offering. Learn more

You may not transmit regulated data, including PHI data of PCI data, to Spacebridge unless you are using Spacebridge with a managed Splunk Cloud deployment and have specifically purchased the applicable regulated environment for that managed Splunk Cloud deployment. Spacebridge does not leverage the FIPS 140-2 validated Splunk Cryptographic Module and may not be used in environments that require this standard.

You must agree to use Spacebridge to use Splunk Secure Gateway. If you want to permanently disable the use of Spacebridge, you must disable Splunk Secure Gateway. Disable Splunk Secure Gateway in **Apps > Manage Apps.** If you're using a managed Splunk Cloud deployment, file a support ticket to disable Splunk Secure Gateway.

Splunk Intelligence Management (TruSTAR legacy service)

1. **Service Description**
   https://docs.splunk.com/Documentation/SIM/current/User/Intelligenceoverview

2. **Security**
   Customer hereby acknowledges and agrees that Splunk Intelligence Management no longer has SOC2 attestation as audited by an independent third party. Customer may not upload or transmit to this environment any regulated data, such as financial information (including PCI-DSS data), protected health information, ITAR data or classified information.

Prior Versions of SPLUNK TERMS FOR OFFERINGS

- Published November 2022
- Published July 2022
- Published May 2022
- Published January 2022
- Published November 2021