



MSLA Product Terms Umbrella MSSP (Insights)

Additional Product Terms

Service Provider's use of Umbrella MSSP (Insights) ("Umbrella Insights") covered by the MSLA Program Terms includes these Product Terms. These terms take precedence over any conflicting terms in the Program Terms. Capitalized terms used but not defined in these Product Terms are defined in the Program Terms or the Master Agreement. Cloud Service will mean Umbrella Insights for the purposes of this document.

Cloud Service Description

Umbrella Insights is a cloud-based security platform at the DNS (domain name system) layer that provides the first line of defense against threats on the Internet by blocking requests to malicious destinations (domains, IPs, URLs) before a connection is established. It provides protection against threats over all ports and protocols, and can protect Internet access across all network devices, office locations, and roaming users. Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

1. Supplemental Terms

- 1.1. Scope of Use/Limitations.** Service Provider shall use the Cloud Service as a Cisco-branded Cloud Service to provide Software Services to End Users and shall not alter or modify the Cloud Services except at Cisco's request or with Cisco's authorization. Service Provider may only use a license to the Cloud Service and any policies, data, or reports derived from the use of such license on behalf of the actual End User who purchased such license from Service Provider. For clarity, Service Provider may not use one license to the Cloud Service or any policies, data, or reports derived from the use of such license for the benefit of multiple End Users.
- 1.2. Eligibility Criteria.** In order to be eligible to purchase the Cloud Service under the MSLA, Service Provider must: (a) provide connectivity, management and/or administrative services along with the Cloud Service such that Service Provider fully manages the Cloud Service for the End User; and (b) Complete the Umbrella MSSP Curriculum. The Umbrella MSSP Curriculum is as follows:
 - 1.2.1.** Completion by a minimum of two Service Provider systems engineers ("SEs") of the Umbrella Systems Engineer Pre-Sales Training and Umbrella Technical Training Assessment COLT Exam provided by Cisco to Service Provider; or completion of the Fire Jumper Stage 4 Cloud and Web Security Training provided by Cisco to Service Provider.
 - 1.2.2.** Completion by a minimum of two Service Provider SEs of the Cisco Umbrella MSSP Training Course provided by Cisco to Service Provider; and completion of the Umbrella MSSP Technical Training COLT Exam provided by Cisco to Service Provider.
 - 1.2.3.** Service Provider is required to complete the Umbrella MSSP Curriculum for each Cisco country group in which Service Provider accesses the MSSP Console.
- 1.3. Support.** The Licenses Fees include the support levels set forth below when Service Provider uses the Cloud Service to provide the Software Services. For clarity, the SSSS set forth in Section 5 of the MSLA does not apply to the Umbrella Insights Cloud Service. Service Provider is responsible for providing front-line support for the Cloud Service to its End Users with respect to their use, maintenance, support, training and technical assistance; provided that Service Provider may escalate support to Cisco as necessary and in compliance with any support guidelines provided by Cisco. In no event shall Cisco have any obligation to provide support directly to, or respond to support requests from, an End User.

Technical Support Level

Gold	<ul style="list-style-type: none"> • Email Access • Access to online tools (e.g. knowledgebase, forums, Documentation, case portal, and notifications) • 24x7 phone support for P1 requests • 24x5 phone support for P2 – P3 requests (Sunday 4pm PST – Friday 5pm PST)
------	---

Priority Levels and Response Targets

Support Priority	Response Target	Description
P1: Outage (An “Outage” means the Cloud Service is completely unreachable when Your Internet connection is working correctly)	30 minutes for phone request 2 hours for email request	Cisco will work on the resolution on a 24x7 basis to either resolve the issue, or develop a reasonable workaround.
P2: Technical Issue	1 business day	An issue occurs if Cloud Service is available but response times are slow while Your Internet connection is working correctly. Issues include technical questions or configuration issues related to Service Provider’s account that moderately impact Service Provider’s ability to use and/or manage the Cloud Service. Cisco will work on the resolution continuously during business hours until either the issue has been resolved, or a plan has been developed and mutually agreed upon between You and Cisco.
P3: Information Request	2 business days	Information requests include account questions, password resets, and feature questions. Cisco personnel will be assigned to work on the resolution at the time of response or as soon as practicable thereafter.

1.4. Cisco Threat Response. Umbrella Insights includes access to Cisco Threat Response. Cisco Threat Response is a cloud-based aggregator of threat intelligence collected or generated by Cisco security products as well as other third-party security products. Cisco Threat Response allows Service Provider to pull together critical threat intelligence and add context from its customers’ organizations so Service Provider knows which systems and devices are infected. Please see the [Cisco Threat Response Privacy Data Sheet](#) regarding any Personal Data processed by Cisco Threat Response.

1.5. Warranties. In addition to the warranties and disclaimers set forth in the Master Agreement, Cisco warrants that it will provide the Cloud Service in a manner consistent with general industry standards reasonably applicable to the provision thereof. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICE WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD-PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SYSTEM OR SERVICE TO WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN “AS IS” BASIS.

1.6. Student Licenses for K-12 and Higher Education End Users.

For End Users that are K-12 and/or higher education customers, the number of licenses of the Cloud Service required for students is based on the following applicable ratio:

- For K-12, one user license is required for every ten students protected by the Cloud Service
- For higher education, one user license is required for every five students protected by the Cloud Service.

For example, if a K-12 End User has 1000 faculty, 500 staff and 30,000 students, the total number of Cloud Service licenses required is $1000 + 500 + (30,000/10) = 4500$ user licenses.

In order to correctly calculate subscription fees due for a month, Service Provider should ensure that it has entered the correct number of user licenses in the MSSP Console using the ratios above for its K-12 and higher education End Users. In the example above, 4500 users should be reflected in the MSSP Console for purposes of reporting and subscription fee calculation under Section 2.2 below. For this example, 4500 users would also count as the quantity of Covered Users for purposes of calculating the Monthly DNS Query Average for the applicable End User under Section 1.4.

1.7. Cisco-Managed S3 Log Storage.

Certain Cisco Umbrella packages include the ability to select Cisco-managed S3 storage or customer-managed storage for DNS, proxy and event logs. Cisco-managed S3 log storage is available with seven, 14 or 30 day retention options. If more than 30 days retention is required, Service Provider should select customer-managed storage or export the data from the Cisco-managed storage to the customer managed storage prior to the expiration of the retention period.

2. Program Requirements

- 2.1. Training.** Prior to using the MSLA Software to provide the Software Services to End Users, any of Service Provider’s employees or Authorized Users engaged in providing the Software Services must complete, at Service Provider’s cost (as applicable), any and all required Cloud Service training courses required by Cisco. In addition, Service Provider must comply with Section 3 of the MSLA related to Authorized Users.
- 2.2. Eligibility.** Service Provider must be able to provide connectivity, management and/or administrative services along with the Cloud Service to provide the Software Services to End Users such that Service Provider fully manages the Cloud Service for the End User.
- 2.3. Reporting and Subscription Fee Calculation.** Service Provider must accurately report the number of licenses to the Cloud Service for that month using the functionality included in the MSLA Software. Except as provided in Section 1.6 for student licensing, one license is required for each individual covered by the Cloud Service. Notwithstanding Section 7.2 of the MSLA, subscription fees are calculated as follows:

Subscription fees are charged based on the quantity of licenses reflected in the Umbrella Insights console as of the last day of the month, pro-rated (based on the Creation Date for the applicable End Users), totalled for all End Users, and then rounded down to the nearest whole number. End-of-month license quantities for End Users with Creation Dates prior to the month covered by the bill are calculated at 100% proration (active full month). End-of-month quantities for End Users with Creation Dates occurring in the month covered by the bill are pro-rated based on the number of days between the Creation Date and the end of the month, inclusive. For example: If three End Users have 100 users each on the last day of December with Creation Dates of 11/20, 12/3 and 12/15, the billed quantity for the month of December would be 248. The “Creation Date” is the date that the Service Provider creates the End User child org within the Umbrella Insights console.

Example:

End User	Creation Date	Users on 12/31	Proration
1	11/20/2019	100	100.00
2	12/3/2019	100	93.55
3	12/15/2019	100	54.84
			248.39
	Round Down Billed Quantity		248

- 2.4. Co-branding.** Any co-branding of the Cloud Service by Service Provider shall be subject to the guidelines located here <https://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf> and any additional trademark guidelines in its Master Agreement.

- 2.5. Security.** When providing the Software Services to End Users, Service Provider and/or its Authorized Users shall implement and maintain appropriate industry standard technical and organizational measures to protect End User data against accidental or unlawful use or destruction, accidental loss, alteration, and unauthorized disclosure of, or access to, any End User data.
- 2.6. Ordering.** Service Provider shall follow the ordering process as instructed by Cisco. Cisco may change or update its ordering process at any time, upon prior written notice to Service Provider.

3. Definitions

“End User” means a commercial business entity that obtains the Cloud Service from Service Provider on a commercial (e.g. non-residential) basis.

“MSSP Console” means the centralized managed security service provider console that Service Provider receives access to in order to manage the Cloud Service.