



MSLA Product Terms

Umbrella DNS Security

Additional Product Terms

Service Provider's use of Umbrella DNS Essentials and/or Umbrella DNS Advantage (collectively, "Umbrella DNS Security") 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. For purposes of this document, Cloud Service will mean the applicable Umbrella DNS Security package.

Cloud Service Description

Umbrella DNS Security 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 shall not use a single Cisco Umbrella tenant (also known as an Umbrella Org) for multiple End Users.

1.2. 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.

1.3. Monthly DNS Query Average

The following use limitation applies in connection with the use of Umbrella DNS Security. For purposes of this Section 1.3, "End User" includes Service Provider when Service Provider is using the Cloud Service for internal purposes as permitted under Section 2.1.1 of the MSLA.

Umbrella DNS Security is licensed based on the quantity of Covered Users and is subject to a Monthly DNS Query Average (as defined below) per End User of five thousand (5,000) DNS queries per Covered User per day. Cisco will continuously monitor the usage of DNS Security on a monthly basis to determine Service Provider's Monthly DNS Query Average on a per End User basis. If at any time Cisco determines that that the Monthly DNS Query Average for an End User has exceeded five thousand (5,000) DNS queries per Covered User per day, Cisco reserves the right to require Service Provider to purchase additional licenses as required.

Monthly DNS Query Average = (number of DNS queries in applicable month for an End User / number of days in applicable month) / number of licensed Covered Users for that month for such End User.

For example, if an End User has 1,000 Covered Users in a month and its Covered Users submitted a total of 3,000,000 DNS queries in that month, the Monthly DNS Query Average for that End User is as follows:

$$(3,000,000 / 30) / 1,000 = 100$$

1.4. 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 Cisco Umbrella Managed Services 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 Managed Services 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 1.3.

1.5. 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 and Other Program Requirements. Service Provider must complete the complete the training and meet the other requirements set forth in the [program requirements document](#). Service Provider is authorized to have subcontractors serve as SEs and participate in training subject to compliance with Section 3 of the MSLA related to Authorized Third Parties.

2.2. Reporting and Subscription Fee Calculation. Service Provider must ensure the actual quantity of Covered Users for a month is reflected in the Cisco Umbrella Managed Services console at all times (e.g., if additional Covered Users are added to the Cloud Service, the Service Provider should update the quantity within the Managed Services console at that time). Except as provided in Section 1.4 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 Managed Services console as of the last day of the month, pro-rated (based on the Creation Date for the applicable End Users), totaled 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 Managed Services 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
			<u>248.39</u>
	Round Down Billed Quantity	248	

2.3. 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.

2.4. 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.

2.5. 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. Support

The Licenses Fees include the support set forth below. 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 will Cisco have any obligation to provide support directly to, or respond to support requests from, an End User.

Support includes the following:

- Technical support (24x7 access to Cisco Cloud Security Support – phone and online)
- Software updates
- 30 minute response objective for Severity 1 or 2 cases from time of phone call
- Next Business Day response objective for Severity 3 or 4 cases
- Access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums (subject to access restrictions identified by Cisco from time to time).

Service Provider agrees to provide the information requested by the technical support team and understands that a delay in providing the information to Cisco may delay resolution and response time. Cisco may adjust assigned case severity to align with the Severity definitions below.

The following definitions apply to this Section.

“Response time”: Time between case submission in the case management system (or by phone where noted above) to substantive support engineer contact.

“Severity 1” means DNS Security is down. Critical impact on customer’s business operations.

“Severity 2” means DNS Security is degraded. Substantial impact on customer’s business operations.

“Severity 3” means DNS Security is partially degraded. Minimal impact on customer’s business operations.

“Severity 4” means End User or Service Provider requests information about features, implementation, or

configuration for DNS Security. No impact on customer's business operations.

"Business Day" means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

4. Definitions

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

"Managed Services console" means the centralized managed security service provider console that Service Provider receives access to in order to manage the Cloud Service.

"Covered User" means the employees, contractors and other individuals who have online and/or cloud activity (e.g., internet, email, use of cloud applications) protected through use of such Cloud Service.