



CISCO UMBRELLA DNS SECURITY OFFER TERMS (SECURE MSP CENTER)

MSP's use of Cisco Umbrella DNS Security purchased on and covered by the Cisco Cloud Services Terms of Use (Secure MSP Center) ("Cloud Terms"), which includes the use of Umbrella DNS Security Essentials and/or Umbrella DNS Security Advantage ("Umbrella DNS Security" or "Cloud Service"), also includes these Offer Terms. Capitalized terms used but not defined in these Offer Terms are defined in the Cloud Terms.

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.

Supplemental Terms

- 1. Scope of Use and Limitations.** You will use the Cloud Service as a Cisco-branded Cloud Service (subject to co-branding as described below) to provide Software Services to MSP End Users and You will not alter or modify the Cloud Service except at Cisco's request or with Cisco's authorization. You will not use a single Cisco Umbrella tenant (also known as an Umbrella Org) for multiple MSP End Users.
- 2. Monthly DNS Query Average.** The following use limitation applies to Your use of Umbrella DNS Security. "MSP End User" includes You when You are using the Cloud Service for internal purposes as permitted under Section 1.2 of the Cloud Terms. "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.

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 MSP End User of up to 5,000 DNS queries per Covered User per day. Cisco will continuously monitor the usage of Umbrella DNS Security on a monthly basis to determine Your Monthly DNS Query Average on a per MSP End User basis. If at any time Cisco determines that the Monthly DNS Query Average for an MSP End User has exceeded 5,000 DNS queries per Covered User per day, Cisco reserves the right to require You to purchase additional licenses.

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

For example, if an MSP 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 MSP End User is as follows:

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

- 3. Cisco-Managed S3 Log Storage.** Certain Cisco Umbrella packages include the ability to select Cisco-managed S3 storage or Company-managed storage (i.e., Your own storage) for DNS, proxy and event logs. Cisco-managed S3 log storage is available with 7, 14 or 30 day retention options. If You require more than 30 days retention, You should select Company-managed storage or export the data from the Cisco-managed storage to Your Company-managed storage prior to the expiration of the retention period. If logging to a Cisco-managed S3 bucket is enabled, the download/synchronization of files from that bucket must be configured so each log file

is downloaded only once. Cisco reserves the right to suspend the downloading of logs from an S3 bucket (through the rotation of keys or other methods) if log files are downloaded multiple times instead of once. Please see the Cisco-managed S3 Bucket documentation available here: <https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket>.

4. **Co-branding.** Any co-branding of the Cloud Service by You is 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 the Cloud Terms.
5. **Service Level Objective.** For purposes of this Service Level Objective, “Service” is defined as Cisco’s recursive DNS service and does not include web-based user interfaces, configuration systems or other data access or manipulation methods. Cisco will use commercially reasonable efforts to maintain Service availability of 99.999% of each calendar month. Availability will be calculated by dividing the total number of minutes of Uptime (defined below) during the applicable calendar month by the total number of minutes in such month, minus minutes of Cisco Umbrella Service Outages (defined below) occurring due to scheduled maintenance and attributable to Third-party Actions (defined below) and multiplying that amount by 100. The formula for this calculation is as follows:

$$\text{Availability} = (X \div Y) \times 100$$

X= Total # of minutes of Uptime during calendar month

Y= (Total # of minutes in such calendar month) - (Total # of minutes of Outages from scheduled maintenance and Third-Party Actions)

For the purposes of this calculation, (i) An “Outage” means the Service is completely unreachable when Your Internet connection is working correctly; (ii) “Uptime” means the number of minutes where there were no Outages, excluding Outages for scheduled maintenance and Third-party Actions, and (iii) “Third-party Action” means any action beyond Cisco’s reasonable control including, without limitation, the performance of Internet networks controlled by other companies or traffic exchange points that are controlled by other companies, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortages. If a dispute arises about whether or not an Outage occurred, Cisco will make a determination in good faith based on its system logs, monitoring reports and configuration records, and as between customer records and Cisco records, Cisco records shall control. Cisco is not responsible for any Outages arising out of Third-Party Actions.

6. **Data Protection.** For information on the personal data processed by Umbrella DNS Security, please see the Umbrella Privacy Data Sheet on [Cisco’s Security and Trust Center](#).
7. **Security.** When providing the Software Services to MSP End Users, You will implement and maintain appropriate industry standard technical and organizational measures to protect MSP End User data against accidental or unlawful use or destruction, accidental loss, alteration, and unauthorized disclosure of, or access to, any MSP End User data.