MSLA Product Terms
Umbrella Mobile Protect

Additional Product Terms

Service Provider's use of Umbrella Mobile Protect under the MSLA Program Terms is subject to these Product Terms. In the event of a conflict, the order of precedence will be (a) these Umbrella Mobile Protect Product Terms; and (b) the Program Terms. Capitalized terms used but not defined in these Program Terms are defined in the Program Terms or the Master Agreement. Cloud Service will mean Umbrella Mobile Protect for the purposes of these Product Terms.

Cloud Service Description

Umbrella Mobile Protect 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 mobile devices that are subscribed to the Cloud Service. 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 may sell the Cloud Service to Enterprise End Users and Commercial End Users. In no event will Service Provider provide to Cisco, or allow Cisco to access, any End User data. Service Provider further agrees to promptly implement any updates, modifications and/or changes to the Software as requested by Cisco. Service Provider will use the Cloud Service as a Cisco-branded Cloud Service to provide Software Services to End Users and will not alter or modify the Cloud Services except at Cisco's request or with Cisco's authorization. Additionally, Umbrella Mobile Protect cannot be used for Consumer End Users in Russia.

1.2. Support. The Licenses Fees include the support levels set forth below. For clarity, the SSSS set forth in Section 6 of the Program Terms does not apply to the Umbrella Mobile Protect 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 will Cisco have any obligation to provide support directly to, or respond to support requests from, an End User.

Technical Support Level

Gold	• 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	30 minutes for phone request 2 hours for email request	Cisco will work on the resolution on a 24×7 basis to either resolve the issue, or develop a reasonable workaround.

Support Priority	Response Target	Description
unreachable when Your Internet connection is working correctly)		
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. "Business Hours" means 8am to 5pm local time at the location of the respective Cisco support personnel, Monday through Friday. "Business Day" means Monday through Friday, excluding local holidays as observed by 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.

1.3. 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.

2. Program Requirements

2.1. Training. Prior to using the MSLA Software to provide the Software Services, any of Service Provider's employees or Authorized Third Parties engaged in providing the Software Services must complete, at Service Provider's cost (as applicable), all Cloud Service training courses required by Cisco. In addition, Service Provider must comply with Section 2.2 of the Program Terms related to Authorized Third Parties.

2.2. Eligibility. Service Provider must be able to provide connectivity, management and/or administrative services along with the Cloud Service in order to provide the Software Services to End Users, such that Service Provider fully manages the Cloud Service for the End User.

2.3. Reporting. Service Provider must provide an accurate monthly report of the number of Devices deployed with the Cloud Service for that month **("Monthly Report")**. Service Provider will provide such Monthly Report in the Cloud Service dashboard by the last day of each month. Notwithstanding Section 4.3.2 of the Program Terms, all Device Licenses deployed in a given month will be charged for the entire month even if the Licenses were used for 15 days or less.

2.4. De-identification Obligation. Service Provider must de-identify and anonymize each APN provisioned with the Cloud Service such that Cisco is unable to determine the name or identity of an End User or an End User's employee. Additionally, Service Provider will not submit any SIMs to the Cloud Service.

2.5. Co-branding. Any co-branding of the Cloud Service will 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.

2.6. **Security**. When providing the Software Services to End Users, Service Provider and/or its Authorized Third Parties will 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.

2.7. **Ordering.** Service Provider will 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

"APN" is an access point name issued to provide a common set of services to a group of Devices that are allocated to that APN.

"Consumer End User" means an individual that obtains the Cloud Service from Service Provider on a home-use (e.g. non-business) basis.

"Device" means a mobile device with a provisioned SIM that is supported by Service Provider to one unique End User.

"End User" means either an Enterprise end User and/or a Commercial End User.

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

"SIM" is a subscriber identity module which is used to identify and authenticate mobile subscribers.