Product Description for Cisco Umbrella

This Product Description is for Cisco Umbrella (the “Product”) and is a part of the End User License Agreement or General Terms (as applicable) located at www.cisco.com/go/eula. Capitalized terms, unless defined in this document, have the meaning in the applicable agreement above. For clarity, this Product Description has historically been referred to as an Offer Description or Supplemental End User License Agreement. References to those documents should be interpreted as a reference to this Product Description.

1. Summary

Umbrella is a cloud security platform that unifies multiple security services in a single cloud-delivered platform to secure internet access and control cloud app usage from your network, branch offices, and roaming users. Your Umbrella subscription includes access to Cisco SecureX, Cisco’s integrated security platform that aggregates threat intelligence, unifies visibility across various Cisco and third-party security products, enables automated workflows, and more.


The Package Comparison (found here: https://umbrella.cisco.com/products/umbrella-enterprise-security-packages) provides information about the various Umbrella packages.

2. Support and Other Services

2.1 Except as provided in Section 2.2, Cisco will provide Support for Umbrella as described here:


2.2 Support for Cisco Umbrella is subject to the following:

a. All references in the Standard Support Description and the Solution Support Description to TAC should be interpreted as references to the Umbrella Technical Support center.

b. Notwithstanding anything to the contrary in the Standard Support Description or the Solution Support Description, the response time objectives for substantive response (i.e., response more than “ticket received”) from Umbrella Support are as set forth below:

<table>
<thead>
<tr>
<th>Software Support Service</th>
<th>Technical Support Coverage</th>
<th>Response Time Objective for Case Severity 1 or 2</th>
<th>Response Time Objective for Case Severity 3 or 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Email access only for Severity 3 or 4 Email and phone for Severity 1 and 2 Access to online tools (e.g., knowledgebase, forums, Documentation, case portal, and notifications)</td>
<td>Response within 1 hour of receipt of phone call</td>
<td>Response next Business Day</td>
</tr>
<tr>
<td>Enhanced (previously “Gold”)</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 30 minutes of receipt of phone call</td>
<td>Response next Business Day</td>
</tr>
<tr>
<td>Premium</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 15 minutes of receipt of phone call</td>
<td>Response next Business Day</td>
</tr>
</tbody>
</table>
3. Performance Standards

This Product comes with Cisco’s standard warranties for Cloud Services as set out in the General Terms/EULA. In addition, Cisco provides the following Service Level Objectives:

3.1 DNS Service

Cisco will use commercially reasonable efforts to maintain DNS Service availability of 99.999% of each calendar month. “DNS Service” means the Umbrella recursive DNS service, excluding web-based user interfaces, dashboards, reporting or other services available to Your Umbrella administrators. Availability will be calculated using the availability calculation below.

3.2 SIG Service

Cisco will use commercially reasonable efforts to maintain SIG Service availability of 99.99% of each calendar month. “SIG Service” means the Umbrella SIG service, excluding web-based user interfaces, dashboards, add-ons, reporting or other services available to Your Umbrella administrators. Availability for the SIG Service means the service is available to accept end user Internet traffic from You when properly configured to allow You to leverage the Umbrella redundant global infrastructure. If You are using an IPSec tunnel(s), proper configuration means the SIG Service is configured with a primary and secondary tunnel with failover behavior. Availability will be calculated using the availability calculation below.

3.3 Availability

Availability will be calculated by dividing the total number of minutes of Uptime during the applicable calendar month by the total number of minutes in such month less minutes of Outages occurring due to scheduled maintenance and/or Third-Party Actions and multiplying the result by 100. The formula for this calculation is as follows:

\[
\text{Availability} = \left( \frac{X}{Y} \right) \times 100, \quad \text{where:}
\]

\[
X = \text{Total # of minutes of Uptime during calendar month; and}
\]

\[
Y = (\text{Total # of minutes in such calendar month}) - (\text{Total # of minutes of Outages from scheduled maintenance and/or Third-Party Actions}).
\]

4. Data Protection

The Cisco Umbrella and Cisco SecureX Privacy Data Sheets describe the Personal Data that Cisco collects and processes as part of the delivery of Umbrella. Additionally, some Umbrella packages leverage Cisco Secure Malware Analytics (formerly, AMP Ecosystem and Threat Grid). Please see the applicable Privacy Data Sheets available here: [https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet](https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet). For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco’s Security and Trust Center: [https://trustportal.cisco.com/c/r/ctp/home.html](https://trustportal.cisco.com/c/r/ctp/home.html)

5. Special Terms
5.1 Definitions

“Covered User” means each Internet-connected employee, subcontractor, and any other authorized individual covered (i.e., protected) by Your deployment of Umbrella.

“Outage” means (i) the DNS Service is completely unreachable when Your Internet connection is working correctly; or (ii) the SIG Service is not available to accept end user Internet traffic from You when properly configured; excluding Outages due to scheduled maintenance and/or Third-Party Actions.

“Third-Party Action” means any action beyond Cisco’s reasonable control including, without limitation, the failure of Your network to forward Internet traffic to Cisco, the performance of Internet networks controlled by other companies (e.g., ISP) or traffic exchange points that are controlled by other companies, local regulations or practices that prevent or limit Cisco from processing Internet traffic in certain regions, events of force majeure (e.g., labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, war, terrorism, governmental action, labor conditions, earthquakes, global pandemics and material shortages), and Your failure to purchase adequate licenses to meet the volume or capacity at which You use Umbrella, if the service level objective would have been met if not for such failure.

“Uptime” means the number of minutes where there were no Outages, excluding Outages for scheduled maintenance and/or Third-Party Actions.

5.2 Covered Users

For packages with user-based pricing, You must purchase one user license for each Covered User unless a published Umbrella data sheet states otherwise.

5.3 Usage and Range Limits

Umbrella is subject to limitations and range limits set forth in the SIG Documentation found here: https://docs.umbrella.com/umbrella-user-guide/docs/limitations-and-range-limits and the DNS Documentation found here: https://docs.umbrella.com/deployment-umbrella/docs/limitations-and-range-limits. Umbrella SIG packages are subject to an average bandwidth limit of up to 50 kilobits per second (“kbps”) per Covered User, based on a 95th Percentile Calculation (whether such traffic is generated by individuals, devices, or servers). The 95th Percentile Calculation allows peaks in usage that exceed the limit for brief periods of time. “95th Percentile Calculation” means Cisco: (a) takes traffic samples over the course of 30 days at each Cisco Umbrella data center handling Your traffic, (b) discards the top 5% of the traffic samples at each such data center and takes the next highest traffic sample value (this next highest traffic sample value is called the “Peak Value”), and (3) adds together the Peak Value for each data center. This limit is further described in the SIG Documentation referenced above. Umbrella DNS Security packages are also subject to a monthly DNS query limit average (whether such queries are generated by individuals, devices, or servers). This limit is further described in the DNS Documentation referenced above. You and Cisco agree to work together in good faith to resolve any excessive usage.

5.4 Cisco Umbrella Reserved IP

If You have purchased a subscription to Cisco Umbrella Reserved IP, please see Reserved IP Supplemental Terms found here: https://docs.umbrella.com/umbrella-user-guide/docs/reserved-ip-terms for additional terms and conditions applicable to Your subscription.

5.5 Cisco-Managed S3 Log Storage

Certain Umbrella packages include the ability to select Cisco-managed S3 storage or Your own storage for DNS, proxy, and event logs. Cisco-managed S3 log storage is available with 7-day, 14-day or 30-day retention options. Please see the Cisco-managed S3 Bucket documentation (found here: https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket) for related requirements and best practices.

5.6 Data Centers

Your Cisco Umbrella subscription includes access to Cisco Umbrella global data centers found here: https://umbrella.cisco.com/why-umbrella/global-network-and-traffic. Data centers not included at this link may require a separate subscription. And any data center(s) located in mainland China, when and if available, require a separate subscription purchased directly through the applicable service operator in China.
5.7 Acceptable Use

You will not (and will not allow any third party to): (i) establish regular and frequent automated queries to an external site, such as port scanning of a third-party entity not in Your control, or use offensive security technologies against a third party through the use of Umbrella (because these actions could reasonably be viewed by the external site as a denial of service attack or a violation of the third party’s terms and could lead to Cisco being blacklisted); (ii) use Umbrella to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use Umbrella for the purpose of intentionally masking Your identity in connection with the commission of unlawful activities or to otherwise avoid legal process. If Cisco receives a third-party request for information, demand letter, or other similar inquiry in connection with Your use of Umbrella relating to alleged unlawful activity on Your network, Cisco may disclose Your name to such third party as necessary to comply with legal process or meet national security requirements; protect the rights, property, or safety of Cisco, its business partners, You, or others; or as otherwise required by applicable law.

5.8 Disclaimers

WHILE CISCO HAS USED COMMERCIALLY REASONABLE EFFORTS TO CREATE EFFECTIVE SECURITY TECHNOLOGIES, DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS, AND ENDPOINTS, CISCO DOES NOT REPRESENT OR WARRANT THAT UMBRELLA WILL GUARANTEE ABSOLUTE SECURITY OR THAT IT WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES, OR THIRD-PARTY MALICIOUS ATTACKS.