Offer Description

Cisco Unified SASE SKUs

This Offer Description is part of the General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "**Agreement**"). Capitalized terms, unless defined in this document, have the meaning in the Agreement or the Cisco Secure Access Offer Description. Any references to a Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

This Offer Description applies to the Cisco Unified SASE SKUs and any Cisco Offers that reference this Offer Description (collectively, the "**Cisco Offer**"). The Cisco Unified SASE SKUs combine Cloud-Delivered Cisco Catalyst SD-WAN and Cisco Secure Access site-based Secure Internet Access ("**SIA**") within a single subscription. For more information about the Cisco Offer, see the Product Data Sheet here.

2. Support and Other Services

Included Cisco support. Your purchase of the Cisco Offer includes the Standard tier Cisco Software Support Services.

3. Performance Standards

3.1 **Cisco Secure Access.** Cisco Secure Access will use commercially reasonable efforts to deliver its Core Services to meet or exceed 99.999% Availability in accordance with the Secure Access Service Level Agreement (the "**Secure Access SLA**") available from Your Cisco account representative or Cisco authorized partner. Capitalized terms in this subsection 3.1 will have the meaning in the Secure Access SLA.

3.2 **Cloud-Delivered Cisco Catalyst SD-WAN.** The Cloud-delivered Cisco Catalyst SD-WAN Service Level Objective applies.

4. Data Protection

The Disclosure Documents for Cloud-Delivered Cisco Catalyst SD-WAN and Cisco Secure Access provide information about data handling practices, security controls, and other features specific to this Cisco Offer.

5. Special Terms

5.1 **Subscription Start Date; Claim Code.** You will receive a subscription claim code via email at the requested start date ("RSD"). Before using this code to enable the Cisco Unified SASE SKUs in Security Cloud Control, complete Your Cloud-Delivered Cisco Catalyst SD-WAN provisioning through Cisco Catalyst SD-WAN Portal. Then, use the claim code to (i) set up Your subscription in Security Cloud Control, and (ii) provision and access the Cisco Unified SASE SKUs. Your subscription will commence on the RSD whether You elect to provision the Cisco Offer on the RSD or delay provisioning of the Cisco Offer.

5.2 **Cloud-Delivered Cisco Catalyst SD-WAN Subscriptions.** Cloud-Delivered Cisco Catalyst SD-WAN subscriptions purchased as part of this Cisco Offer are also governed by the terms of the Cloud-Delivered Cisco Catalyst Offer Description, provided that such subscriptions are available and operational only on Cisco C81XX-G2 and C82XX-G2 Secure Routers and only as Cisco WAN Essentials subscriptions.

5.3 **Cisco Secure Access Licenses.** You may purchase Cisco Secure Access SIA Covered Site licenses for each Covered Site that routes network traffic to the Cisco Offer. A Covered Site license covers individuals physically present at a Covered Site. However, remote or hybrid workers not physically present at a Covered Site are excluded and require separate Covered User licenses.

5.4 **Cisco Secure Access Usage and Range Limits.**

(A) Cisco Secure Access Covered Site licenses are subject to a total aggregate data transfer limit per month, as specified in the Secure Access Ordering Guide. The data transfer limit applies to the amount of data going through the Cisco Offer (inbound and outbound). If an organization purchases multiple Covered Site licenses, then the applicable data limits are pooled to determine the organization's total aggregate monthly data transfer

limit. For example: Your organization purchases one Small-1 license with a data limit of 100 GB/month, two Medium-2 licenses with a data limit of 2,500 GB/month/license, and one Large-1 license of a data limit of 10,000 GB/month. Your total aggregate data limit per month is 15,100 GB.

(B) Cisco will work with You in good faith to try and resolve any excess usage. If You cannot reduce Your excess usage sufficiently, You may be required to purchase additional licenses to obtain the additional required data transfer capacity.

5.5 **Cisco Secure Access Feature Previews.** Cisco may offer You the ability to participate in a preview of new Cisco Secure Access features before they are generally available ("**Preview**"). Your usage of such features during a Preview is subject to the terms in the Agreement specifically related to beta and evaluation software use, except as follows: (a) You may use Cisco Secure Access features in production during a Preview; and (b) participation in a Preview does not alter Your obligation to pay any fees owed to Your Approved Source during the Use Term.

5.6 **Cisco Secure Access Third Party Threat Intelligence Data Feeds.** You can configure Cisco Secure Access to ingest third party threat intelligence data feeds ("**Third Party Threat Intelligence**"). By enabling data sharing, You (i) warrant that You are authorized to grant the Cisco Offer access to the Third Party Threat Intelligence, (ii) are solely responsible for validating the quality and accuracy of the Third Party Threat Intelligence, (iii) are solely responsible for ensuring that the Third Party Threat Intelligence is fully and correctly ingested by the Cisco Offer, and (iv) agree that Cisco is not responsible for enforcement delays as the Cisco Offer may experience processing delays between Third Party Threat Intelligence ingestion and enforcement. Cisco is not liable for any damages resulting from Your use, sharing or reliance on the Third Party Threat Intelligence.

5.7 **Cisco Secure Access Data Centers.** Cisco Secure Access data center(s) located in mainland China, when and if available, require a separate Cisco Secure Access subscription purchased directly through the applicable service operator in China.

5.8 **Acceptable Use.** The Cisco Acceptable Use Policy applies to the Cisco Offer. In addition, 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 the Cisco Offer (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 the Cisco Offer to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use the Cisco Offer 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 the Cisco Offer 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.

5.9 **Unlicensed Feature Usage.** If You have access to certain features that are not included in the subscription package You purchase, and You utilize those features, Cisco may require You to purchase the appropriate package. Prior to purchasing the appropriate package, if You are using unlicensed Cisco Secure Access SPA package features for evaluation purposes, You may do so for up to 100 Covered Users. Cisco's support and Service Level Agreement obligations do not apply to unlicensed features. Cisco reserves the right to terminate access and/or usage rights to unlicensed features at any time with or without notice.

5.10 **Cisco OpenDNS Service.** If You are a paid customer of the Cisco Offer and nevertheless choose to use the Cisco OpenDNS Service (as defined in the OpenDNS Public DNS Terms of Service), You agree that Your use of Cisco OpenDNS Service is not subject to this Offer Description, including any associated warranties or SLAs. Your use of the OpenDNS Service is governed by the OpenDNS Public DNS Terms of Service.

5.11 **Use of MCP Servers.** By accessing, developing, deploying, integrating with or otherwise using any application, client, or AI Agent that interacts with Cisco Secure Access or Cloud-Delivered Cisco Catalyst SD-WAN through use of an MCP Server, You agree to be bound by the Cisco Security Model Context Protocol Server Terms attached to this Offer Description as Exhibit A.

5.12 **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 the product will guarantee absolute security or that it will protect all your files, network, or endpoints from all malware, viruses, or third-party malicious attacks.

5.13 **Definitions**

Term	Meaning
AI Agent	Any software system that uses a machine learning model or other AI technology to discover, select, or invoke tools exposed by an MCP Server, whether autonomously or in response to user input.
Covered Site	A specific physical location, such as a retail branch, office, corporate campus or headquarters, that sends its network throughput to Cisco Secure Access.
Covered User	Each Internet-connected employee, subcontractor, and other authorized individual covered (i.e., protected) by Your deployment of the Cisco Offer.
MCP Server	a Model Context Protocol Server that Cisco makes available to interoperate with a Cisco Offer, or that You develop or host to interoperate with a Cisco Offer.

Exhibit A
Cisco Security Model Context Protocol (MCP) Server Terms

These Cisco Security Model Context Protocol Server Terms ("**MCP Terms**") constitute Supplemental Terms under the Cisco General Terms applicable to the specific Cisco Offer(s) that reference these MCP Terms. You may only use a Model Context Protocol Server that Cisco makes available to interoperate with a Cisco Offer, or that You develop or host to interoperate with a Cisco Offer (each an "**MCP Server**"), if You are an Authorized User of the Cisco Offer with which an MCP Server interoperates. Collectively, the following terms (the "**Terms**") apply to Your Use (as defined below) of an MCP Server: these MCP Terms, the Cisco General Terms, the applicable Offer Description, the Cisco Baseline API License Terms (the "**API Terms**"), and the Cisco Acceptable Use Policy ("**AUP**"). For clarity, You understand and agree that any references in the API Terms to "API Integration" include Your interaction with an MCP Server, and any references in the API Terms to "Cisco API" include an MCP Server. All capitalized terms, unless defined in these MCP Terms, have the meaning in Cisco's General Terms or the applicable Offer Description.

By accessing, developing, deploying, integrating with or otherwise using any application, client, or AI Agent (defined below) (collectively, Your "**Application(s)**") that interacts with a Cisco Offer through use of an MCP Server (collectively, "**Use**"), You agree to be bound by the Terms. All Use of an MCP Server must be in accordance the Terms, and all rights not expressly granted by the Terms are reserved by Cisco. If You are using an MCP Server on behalf of an entity, You represent and warrant that You have authority to bind that entity to the Terms, and by accepting the Terms, You are doing so on behalf of that entity.

For purposes of these MCP Terms, "**AI Agent**" means any software system that uses a machine learning model or other AI technology to discover, select, or invoke tools exposed by an MCP Server, whether autonomously or in response to user input.

1. **Nature of the Service**. An MCP Server is a probabilistic discovery interface, not a traditional REST API. The tools, schemas, and response formats that the MCP Server exposes may change without notice, and You are responsible for designing Your Application(s) to handle such changes. Any MCP Server made available by Cisco is provided on an "as available" basis and is not subject to any service level agreement, uptime commitment, technical support obligation, or express or implied warranties.
2. **Authentication and Access Control**. You must ensure that Your Application(s) accessing an MCP Server authenticate in accordance with the Documentation and are scoped to the minimum permissions necessary. All requests to an MCP Server are subject to the Cisco Offer's standard role-based access controls. You may access only the accounts, data, and other information for which the authenticated user has been granted permission. You are responsible for the secure issuance, storage, and rotation of credentials.
3. **Human Authorization for State-Changing Actions**. Some tools exposed by an MCP Server may perform actions that may modify or delete Your Cisco Offer's settings, configurations, data, or services (collectively, "**State-Changing Tools**"). Before Your Application(s) invokes a State-Changing tool, You must require affirmative authorization from a human operator who has been shown the proposed permitted action(s) and the affected resources (for clarity, this may include preauthorization of specific state-changing actions by an Authorized User). Blanket or programmatic approvals for State-Changing Tools are prohibited.
4. **Responsibility for Your Application(s).** You are responsible for the configuration, behavior, and outputs of Your Application(s) that interact with a Cisco Offer through use of an MCP Server, including any actions taken based on results returned by an MCP Server. Cisco is not liable for decisions made or actions taken by You or Your Application(s), and You agree to defend, indemnify, and hold harmless Cisco from any claim arising out of those actions and Your Application(s) in accordance with the indemnification provisions of the API Terms.
5. **Data Use; No Model Training.** You may not use any data, telemetry, metadata, schemas, or results obtained from a Cisco Offer through use of an MCP Server to train, fine-tune, evaluate, or otherwise develop any machine learning model or AI

system. You may not retain or aggregate results beyond what is reasonably necessary for the immediate operation of Your Application(s), short-term operational logging, or audit and compliance.

6. **Acceptable Use.** In addition to the conditions set forth in the API Terms and AUP, You may not: (i) rename, alias, or repackage namespaced tools in a way that obscures their origin as Cisco tools; or (ii) circumvent any rate limits, access controls, or other technical restrictions. Your Use of an MCP Server will count toward the applicable Cisco Offer's API rate limits and may be monitored by Cisco. Cisco may throttle, suspend, or limit access that exceeds applicable limits or imposes an undue burden on the applicable Cisco Offer(s).
7. **Downstream Users.** If You make Your Application(s) available to other users or customers, You are responsible for their compliance with the Terms and must impose terms on such additional users that are at least as protective of Cisco as those set out here. You remain responsible for such additional users' actions as if they were Your own.
8. **MCP Terms Changes and Termination.** Cisco may update or terminate these MCP Terms at any time. Material changes to these MCP Terms will be posted to the applicable Cisco Offer's Documentation or Offer Description. Your continued use of an MCP Server after the effective date of any such change(s) constitutes acceptance of the updated terms.
9. **Order of Precedence.** If there is any conflict between the Terms, the order of precedence (from highest to lowest) is: these MCP Terms, the API Terms, the AUP, the applicable Offer Description, and the Cisco General Terms.