



Offer Description

Cisco Secure Access

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. Any references to the Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

This Offer Description applies to Cisco Secure Access (Cloud Services) and any Cisco Offers that reference this Offer Description (the “**Cisco Offer**”). For more information on Cisco Secure Access, see the [Secure Access Site](#) and the [Secure Access Datasheet](#).

2. Support and Other Services

Support. You will be required to select [Enhanced or Signature](#) support when You purchase the Cisco Offer. If You purchase Secure Access for Government, You will be required to select [Software Support Enhanced or Premium for Government](#). Support for the Cisco Offer and Secure Access for Government does not include an initial meeting to understand Customer’s desired outcomes to define an IT and Infosec adoption plan.

3. Performance Standards

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

4. Data Handling

The [Disclosure Documents](#) for Cisco Secure Access provide information about data handling practices, security controls, and other features specific to this Cisco Offer.

5. Special Terms

5.1 Covered Users.

You must purchase one Covered User license for each individual protected by the applicable Cisco Secure Access package purchased by You. The quantity of Covered Users You purchase may differ across Secure Access packages (e.g., Secure Internet Access (“**SIA**”), Secure Private Access (“**SPA**”), and Secure Access DNS Defense).

5.2 **Subscription Start Date; Claim Code.** You will receive a subscription claim code via email at the requested start date (“**RSD**”). The claim code enables You to (i) set up Your subscription in Security Cloud Control, and (ii) provision and access the Cisco Offer. 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.

5.3 Usage and Range Limits.

(A) Cisco Secure Access SIA and SPA subscriptions are subject to a total aggregate data transfer limit per month across all packages purchased for such Cisco Offer equal to the quantity of purchased Covered Users multiplied by 20 GB. The data transfer limit applies to the amount of data going through the Cisco Offer (inbound and outbound) whether resulting from Covered Users and/or non-user devices protected by the Cisco Offer. If You purchase an SIA and an SPA package with different quantities, the Covered User quantity used to calculate the total data transfer limit is the higher of the two Covered User quantities purchased.

For example:

- If You purchase an SIA subscription for 1000 Covered Users and do not purchase an SPA package, Your subscription is subject to a monthly data transfer limit of 20,000 GB.
- If You purchase SIA for 5000 Covered Users and SPA for 3000 Covered Users, Your monthly data transfer limit across SPA and SIA is 5000 x 20GB = 100,000 GB.

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

- (B) The DNS Defense Package is subject to a monthly DNS query limit average (whether such queries are generated by individuals, devices, or servers), as further described in the [DNS Defense Documentation](#). You and Cisco agree to work together in good faith to resolve any excessive usage.
 - (C) Remote browser isolation (RBI) is subject to a total aggregate data transfer limit per Covered User per day of 2 GB. If a Covered User exceeds this limit, RBI may bypass the domain having the highest data transfer impact, typically a streaming site such as YouTube, Netflix, TikTok and other video streaming services. If a domain is bypassed, it means that the user's access to the domain is not blocked but that domain will not pass through the RBI service. RBI is also subject to a limit of 25 active concurrent sessions. If a user tries to open a 26th session, the user will receive a message indicating that they will need to close an existing session in order to start a new session.
 - (D) Secure access Multi-org provides You with the ability to manage multiple organizations through a single instance of the console. You are permitted to deploy up to ten (10) Multi-orgs, each with a minimum of fifty (50) Covered Users for each Multi-org. Any deployments exceeding this limit require prior written approval from Cisco. Should You exceed the ten Multi-org limit without Cisco's approval, You may be required to pay for such additional usage.
 - (E) The Cisco Offer is subject to other technical usage and range limitations as set forth in the [Cisco Secure Access Documentation](#). Where there are sudden spikes in data usage or significant excess usage that may cause service degradation, You agree to take prompt action at Cisco's direction to reduce Your usage.
- 5.4 **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 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.
- 5.5 **Unlicensed Feature Usage.** You may have access to certain features that are not included in the Cisco Secure Access subscription package You purchase. If You utilize features not covered by Your subscription, Cisco may require You to upgrade Your subscription to purchase the appropriate package. Prior to the upgrade, You may use such unlicensed features for evaluation purposes 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. Unlicensed feature usage does not apply to ThousandEyes Users Embedded. For details on feature entitlement by subscription packages, see: [SSE Packages](#).
- 5.6 **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.
- 5.7 **Data Centers.** Data center(s) located in mainland China, when and if available, require a separate subscription purchased directly through the applicable service operator in China.
- 5.8 **Cisco Secure Client.** Your subscription to Cisco Secure Access includes the right to use Cisco Secure Client. If you wish to use Cisco Secure Client with other products, You must purchase a separate Cisco Secure Client license.
- 5.9 **ThousandEyes.** Your subscription to Cisco Secure Access includes the ThousandEyes Embedded Endpoint Agent license. See Section 5.1 of the [ThousandEyes Offer Description](#) for information regarding features and restrictions associated with the Embedded Endpoint Agent license. If You deploy ThousandEyes Users Embedded, Your ThousandEyes account will be provisioned by default to ThousandEyes' data center in the United States. You may contact support@thousandeyes.com to make a request to change your data center location to ThousandEyes' EU

data center. Additional information about ThousandEyes' use, storage, and processing of Your data is available in the ThousandEyes [Disclosure Documents](#). If You purchase SIA and SPA packages with different license quantities, Your entitlement to ThousandEyes Embedded Endpoint Agent licenses will be equal to the highest license quantity purchased between the SIA and SPA packages.

- 5.10 **Competitive Testing.** You will not publish or disclose to any third party any Cisco Offer performance information or analysis (including without limitation the results of benchmark or competitive testing) except with Cisco's prior written consent.
- 5.11 **Cisco Secure Access Reserved IP.** If You are entitled in writing to a Cisco Secure Access Reserved IP subscription, please see the [Reserved IP Supplemental Terms](#) for additional terms and conditions applicable to Your subscription. Your Approved Source reserves the right to charge a fee, and You agree to pay, for Your Cisco Secure Access Reserved IP subscription.
- 5.12 **AI Assistant.** AI Assistants are not error free. You are responsible for considering the results and recommendations generated by an AI Assistant and determining what actions to take (if any) based on such results and recommendations.
- 5.13 **Third Party Threat Intelligence Data Feeds.** You can configure the Cisco Offer 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.
- 5.14 **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.**

5.15 **Definitions**

Term	Meaning
Covered User	Each Internet-connected employee, subcontractor, and other authorized individual covered (i.e., protected) by Your deployment of the Cisco Offer.