Offer Description: Cisco Secure Client

This Offer Description (the “Offer Description”) describes Cisco Secure Client (formerly known as AnyConnect and referred to below as Cisco Secure Client or the Cisco Technology). Your use is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (the “EULA”) (or similar terms existing between you and Cisco) (the “Agreement”). If capitalized terms are not defined in this Offer Description, then they have the meaning given to them in the Agreement or order(s).

1. Description

1.1. Cisco Secure Client

Cisco Secure Client is a unified security endpoint agent that delivers multiple security services to help protect the enterprise. It provides the visibility and control to help identify who and which devices are accessing the extended enterprise. Cisco Secure Client’s range of security services include functions such as remote access, endpoint security, posture enforcement, web security features, and roaming protection.

1.2. Cisco Endpoint Security Analytics- Built on Splunk

The Endpoint Security Analytics- Built on Splunk is used in conjunction with the Cisco Secure Client Network Visibility Module.

2. Supplemental Terms and Conditions

2.1. Required Devices

Each Endpoint must use the Cisco Secure Client Software to connect to a Cisco Network Device. Your use of Cisco Network Devices is subject to separate license entitlements and restrictions that are not covered by this Agreement. Each Cisco Network Device may need to be registered for use with your license. However, a Network Access Manager Module and/or Network Visibility Module may be used by You in conjunction with non-Cisco equipment as described in the Administrator Guide.

2.2. Cisco SecureX

Your Cisco Secure Client licenses include access to certain Cisco SecureX features. For more information on SecureX, please see the SecureX Offer Description at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

2.3. Cisco Endpoint Security Analytics Built on Splunk

Cisco Endpoint Security Analytics Built on Splunk (“CESA”) is sold by Cisco and is licensed and supported by Splunk under the Splunk Software License Agreement available (the “Splunk EULA”) as updated by Splunk from time to time. You may be required to accept the Splunk EULA in connection with the delivery to you of CESA and/or related software license key(s). For more information on CESA, see https://www.cisco.com/c/en/us/products/security/endpoint-security-analytics-built-on-splunk/index.html.

2.4. NVM for Splunk
“NVM for Splunk” means the Cisco Secure Client Network Visibility Module (NVM) App for Splunk and the Cisco NVM Technology Add-On for Splunk, both of which are available for download from Splunkbase. NVM for Splunk is subject to the following license limitations and restrictions in addition to those set forth in the EULA:

a. Except as provided in Sections 2.5 and 2.6, NVM for Splunk is licensed to You solely for use with CESA under Your CESA license (including any trial, proof of concept/proof of value, or paid for license of CESA).

b. You are authorized to use NVM for Splunk with Your Splunk license or subscription for a Splunk version other than CESA (e.g., a Splunk license purchased from Splunk or a Splunk reseller) provided that such use is limited solely to NVM data collected from no more than fifty (50) Endpoints in the aggregate.

c. You are authorized to use NVM for Splunk for evaluation purposes on a one-time basis for up to ninety (90) days from the date of first download.

You are not authorized to use NVM for Splunk and may not download it from Splunkbase unless Your use of NVM is explicitly authorized under Sections 2.4.1, 2.4.2, and/or 2.4.3. If You use NVM for evaluation purposes under Section 2.4.3, You are required to cease use and delete NVM for Splunk from all computing devices on which it was installed upon completion of the ninety (90) day evaluation period, unless You have purchased a CESA license or are using it with up to fifty (50) Endpoints as permitted under Section 2.4.2 of this Offer Description. For clarity, You are not authorized to use NVM for Splunk or any portion of it independently of Your use of Cisco Secure Client/AnyConnect and CESA (or another Splunk offer as permitted under Section 2.4.2 of this Offer Description).

3. Data Protection

The Cisco Secure Client and SecureX Privacy Data Sheet (available [here](#)) describes the Personal Data that Cisco collects and processes as part of the delivery of the Cisco Technology. For further information on how Cisco processes, uses and protects all categories of data, please visit Cisco’s Security and Trust Center.

4. Support & Maintenance

The Cisco Technology Software includes online support and phone support. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email, and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

If you have access to Software, Cisco will provide (i) work-around solutions or patches to reported problems and (ii) major, minor and maintenance releases of the licensed Software version, which can be accessed on Cisco Software Central. You may be required to update to the latest Software release to correct a reported Software problem.
The below table outlines Cisco’s response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions 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 with Phone Support</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 1 hour</td>
<td>Response within next Business Day</td>
</tr>
<tr>
<td>Basic with Online Support</td>
<td>Web</td>
<td>Response to all cases within next Business Day during Standard Business Hours</td>
<td></td>
</tr>
</tbody>
</table>

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

“Severity 1” means the Software is unavailable or down or there is a critical impact to a significant impact to Case Submitter’s business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

“Severity 2” means the Software is degraded or significant aspects of Case Submitter’s business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

“Severity 3” means the Software is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

“Severity 4” means minor intermittent functionality or performance issue, or information is required on the Software. There is little or no impact to Case Submitter’s business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

“Business Day” means the generally accepted days of operation per week within the relevant region where the Software will be performed, excluding local holidays as observed by Cisco.

“Local Time” means Central European Time for support provided in Europe, Middle East and Africa, Australia’s Eastern Standard Time for support provided in Australia, Japan’s Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

“Standard Business Hours” means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Your access to and use of the Software may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.

5. Definitions

“Administrator Guide” means the Cisco Secure Client or Secure Mobility Client Administrator Guide or the Administrator Guide for the applicable Cisco product or service.
“Cisco Network Device” means a Cisco Adaptive Security Appliance (ASA), Cisco head-end termination device or other Cisco product or solution including, but not limited to the Cisco Identity Services Engine, used in conjunction with the Software that is not associated with a specific end user.

“Endpoint” means a computer, smartphone or other mobile device used by an end user in conjunction with any of the Software.

“Network Access Manager Module” means a separate module in the Software with IEEE 802.1X authentication functionality to manage wired and wireless network connections.

“Network Visibility Module” or “NVM” means a separate module in the Software providing networking flow telemetry functionality to enable endpoint and user behavior analysis.