Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

Dear Customer,

This Supplemental End User License Agreement ("**SEULA**") contains additional terms and conditions for the Software product(s) set forth herein and licensed under the End User License Agreement ("**EULA**") between you and Cisco Systems, Inc. or its Affiliates (collectively, the "**Agreement**"). Please note that there may be terms in this SEULA that do not apply to you. Only those terms related to the specific Software product(s) you purchased apply to you. Except as otherwise set forth in this SEULA, capitalized terms will have the meanings as in the EULA. To the extent that there is a conflict between the EULA and this SEULA, this SEULA will take precedence.

By downloading, installing, or using the Software you agree to comply with the terms of this SEULA.

SUPPLEMENTAL LICENSE TERMS FOR: Cisco Security Management Platform

Table 1. SOFTWARE ENTITLEMENT:

Product	License Metric	License Duration
Cisco Security Management Platform	See Section (1)	Term

DEFINITIONS:

- "Cisco Threat Content" means any Cisco provided threat intelligence, content or data including, but not limited to, rules, signatures, threat data feeds or suspicious URLs and IP address data feeds for use with any Cisco product or service.
- "Cloud Service" means (i) a Cisco hosted software-as-a-service offering or feature, and (ii) the PaaS Service.
- "Integrated Product(s)" means the Software and Cloud Services integrated with the Product and available for use with the Product as indicated on the then current Cisco Global Price List. For example, the Product is available for use with the ESA Inbound Essentials Software Bundle (Anti-Spam, Anti-Virus, Outbreak Filters), the ESA Premium Software Bundle (Anti-Spam, Anti-Virus, Outbreak Filters, Data Loss Prevention, Encryption), and the AMP for Content Security add-on to such bundles, and may be made available for use with other Integrated Products from time to time.
- "PaaS Service" means the optional add-on hosted deployment service for the Product.
- "Personal Data" has the same meaning given to Personal Information in Cisco's Privacy Statement.
- "Product" shall mean the Software product listed in Table 1.
- "Telemetry Data" means information generated by instrumentation and logging systems created through the use and operation of the Products, such as, but not limited to, Tenant entity or division name, address and user quantity and other metadata regarding the usage of the Product and the applicable Integrated.
- "Tenant" means a single instance of the Product and applicable Integrated Products having unique portal access with restricted access to its dataset as configured by the applicable customer.

ADDITIONAL GENERAL LICENSE RIGHTS AND RESTRICTIONS:

(1) Separate License to Integrated Products. The Product is designed to be used as a modular software platform to one or more of the Integrated Products. You must hold a license or subscription to the Integrated Products in order to use the Product. The Product is licensed on the same license unit metric and for the same quantity of licenses as the applicable underlying Integrated Products. For example, if the Integrated Product is licensed based on the quantity of "users" authorized by You to access and use email services, then you must purchase the same quantity of "users" for the Product.

(2) Telemetry Data. Cisco may collect Telemetry Data related to Your use of the Product and Integrated Products in order to deliver, maintain, improve, and/or analyze the effectiveness of such products. You acknowledge that Cisco may freely use any non-personal Telemetry Data that does not identify You or any of Your users specifically. Some Telemetry Data that Cisco collects, or that You provide or make accessible to Cisco as part of Your use of the Product, is necessary for the essential use and functionality of such Product. Telemetry Data is also used by Cisco to provide associated services such as technical support and to continually improve the operation, security efficacy and functionality of the Product and Integrated Products. For those reasons, You may not be able to opt out from some of the Telemetry Data collection other than by uninstalling or disabling the Product or the applicable Integrated Product. Please see the applicable Documentation for information on how to limit some of the Telemetry Data that can be collected.

(3) Data Protection. Personal Data included within Telemetry Data may be shared by Cisco only (x) within Cisco and any of our worldwide subsidiaries and with our authorized contractors for the above authorized purposes; (y) as necessary to comply with law and subject to Cisco's policy on law enforcement requests at http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html; and (z) otherwise with Your written consent. Cisco will use Personal Data only in accordance with the Agreement, this Supplemental End User License Agreement, and Cisco's Privacy Statement. Cisco may process and store Personal Data in the United States or outside of the country where it was collected. You are responsible for providing all required notices to Your users and obtaining all required consents from Your users regarding the processing and transfer of Personal Data including international transfers. Cisco will only transfer Personal Data consistent with applicable law. To the extent Cisco processes any Personal Data from the EEA or Switzerland on behalf of You, we will do so in a manner consistent with the relevant EU-US or Swiss-US Privacy Shield Principles ("Principles") (see www.commerce.gov/privacyshield) or successor frameworks. Where Cisco transfers Personal Data from an APEC Member Economy on behalf of You, Cisco will perform such processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("CBPRs") (see www.cbprs.org) to the extent the requirements are applicable to Cisco's processing of such data. If Cisco is unable to provide at least the same level of protection as required by the Principles or CBPRs, Cisco will promptly notify You and cease processing.

(4) Cisco Threat Content. If Your use of the Product and/or Integrated Products requires or permits You to use any Cisco Threat Content, then You (and Your agents acting on your behalf) may only use such Cisco Threat Content for Your use with such Product and/or Integrated Products and with those third-party products or services offerings that Cisco has identified as being compatible. You agree not to provide Cisco Threat Content to a third party.

(5) Cloud Services. If You elect to enable any Cloud Service included with your subscription or available through an add-on purchase, Your use of such Cloud Service is governed by the Cisco Universal Cloud Agreement and the applicable Offer Description (if one is available) located at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html. For example, the Cisco Universal Cloud Agreement and applicable Offer Description apply if you purchase the Advanced Malware Protection (AMP) – Basic add-on for use with the Integrated Products and/or if you purchase the PaaS Service.