Cisco Identity Services Engine (ISE)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Identity Services Engine (ISE). Although this document is accurate for ISE version 3.3, specific features not available in earlier versions of ISE are noted where relevant throughout the document.

Cisco ISE collects, uses, and processes Customer data as described in the Cisco Privacy Statement and this Privacy Data Sheet, an ISE-specific supplement to the Cisco Privacy Statement.

In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data sent to Cisco to process to provide ISE's functionality.

1. Overview of Cisco Identity Services Engine Capabilities

Cisco Identity Services Engine (ISE) is an on-premise software product that allows Customers to provide highly secure network access to specific users and devices. Cisco ISE helps Customers gain visibility into what is happening in their networks, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so that Customers can identify, contain, and remediate threats faster.

Customers have complete control over the ISE application deployed and managed on their premise. Cisco cannot access an on-premise application without our customer's permission.

Cisco ISE provides the following features, depending on the ISE license installed. See the ISE Licensing Guide for information about which features are available with which license.

- Asset visibility
- Guest and secure wireless access
- BYOD
- Secure wired access
- Authorization for network device administration
- Segmentation
- Compliance and posture
- Security ecosystem engagements
- Threat containment

Some of the capabilities and components discussed in this Privacy Data Sheet are parts of solutions that cover multiple products and are covered in greater details in other Privacy Data Sheets. For information related to each of those capabilities, please refer to the relevant documents listed below:

- User Defined Network: please refer to Addendum 3 of the Cisco DNA Center Privacy Data Sheet.
- Licensing: please refer to the Smart Software Licensing Tools and Smart Account Management Privacy Data Sheet.
- Support Diagnostics: please refer to the Cisco Technical Assistance (TAC) Service Delivery Privacy Data Sheet.

Asset visibility relies on profiling endpoints. Starting from ISE 3.3 ISE can optionally upload certain endpoint data to the Cisco cloud for the purposes of machine learning and profiling improvements. Please see the Addendum for information on this capability and how it processes personal data.

For more information about Cisco ISE please refer to the Cisco ISE Product Data Sheet.

2. Personal Data Processing

The tables below list the personal data processed by ISE to provide its services and describes why the data is processed. The Table 1 lists components whose data gets uploaded to the Cisco cloud or other clouds accessible by Cisco. Except for Licensing & Deployment to a certain extent, which is required for proper operation of the product, all of the capabilities provided by the components in Table 1 can be enabled or disabled by the customer. When disabled, no corresponding data is uploaded to the cloud.

The second table lists components and whose data, which, process data on-premise only, and data is only potentially uploaded to the cloud in case of troubleshooting via a support case.

Table 1

ISE Component	Types of Personal Data	Personal Data Category	Purpose of Processing
Interactive Help (enabled by default)	• IP Address • Username	• Registration Information • Host and Usage Information	• Context based Online Help guides • Product Improvement Services • Enable product operations and functionality
Licensing & Deployment (enabled by default)	• Host Name • MAC Address • Serial Number • Virtual Account ID • Smart Account ID • Email (Optional) • Device Unique ID	• Registration Information • Host and usage information • Customer identification	• Enable product operations and functionality • Authenticate and authorize access to the service • Understanding adoption • Enforcing usage as per licenses purchased
pxGrid Cloud[1] (disabled by default)	• Client name • Client Description The following data is also uploaded to the Cisco Cloud and made available to other pxGrid Cloud supported products used by the customer • adNormalizedUser • assetConnectedLinks • assetCustomAttributes • assetDeviceType • assetHwRevision • assetIpAddress • assetMacAddress • assetName • assetProductId • assetSerialNumber • assetSwRevision • assetVendor • calledStationId • callingStationId • destinationIpAddress • deviceType • endpointOperatingSystem • fullname • identityGroup • imei • ipAddresses • jailBroken • location • macAddress • manufacturer • mdmImei • mdmJailBroken • mdmLocation • mdmManufacturer • mdmMeid • mdmModel	• Registration information • Host information • Endpoint information	• Enable product operations and functionality • Enhance operation of Cisco eco-system partner products through context sharing

[1] pxGrid Cloud is not relevant in ISE versions prior to 3.2.

	• mdmPinLocked • mdmSerialNumber • mdmServerName • mdmUdid • meid • model • mseServerName • name • osVersion • pinLocked • serialNumber • serverName • udid • username		
Support Diagnostics[2] (enabled by default, but only relevant when initiated by a customer action)	• Serial Number • Hostname • IP Address • GUID	• Host information	• Troubleshooting & technical support
Telemetry (enabled by default)	• CCO ID • Other various telemetry items being reported on as referenced in elsewhere in this table	• Registration information • Endpoint information • Usage information	• Product improvements & roadmap development • Analysis of feature usage / success
User Defined Network (disabled by default)	• MAC Address • First name • Last name • Email Address	• Registration Information • Host and Usage Information	• Provision and enroll Customer in the service • Authenticate and authorize access to the service • Enable product operations and functionality

The following table lists components where data is only uploaded to a cloud if initiated by the customer when troubleshooting a support case.

Table 2

ISE Component	Types of Personal Data	Personal Data Category	Purpose of Processing

[2] If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process, at the customer's discretion, some or all of the personal data used or stored by other components of ISE as described in this document. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

Internal Identity Store: **RADIUS** **TACACS+**	- Username - Email Address - First name - Last name - User groups * - Last Successful Login IP address - Last Failed Login IP address - Request login name - IP Address - MAC Address - Certificate - External Identity Attributes - External Identity Groups* - Guest email (logged in NA)* * Only applicable to RADIUS	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality
External Identity Store (i.e., Active Directory, Azure Active Directory[3] Facebook, Security Assertion Markup Language (SAML), Open Database Connectivity (ODBC), RSA Token, RADIUS Token, Passive ID, Lightweight Directory Access Protocol (LDAP))[4]	- Username - Email Address - User groups - Last Successful Login IP address - Last Failed Login IP address - Request login name - IP Address - MAC Address - Certificate - External Identity Attributes - External Identity Groups - Guest email (logged in NA) - First name - Last name - SAM-Account-Name* - Distinguished Name* - User-Principal-Name* - Country** - OnPremises-DistinguishedName** - preferredLanguage** - mySite** - isResourceAccount** - mail** - city** - displayName** - companyName** - jobTitle** - postalCode** - LegalAgeGroup-Classification** - preferredDataLocation** - accountEnabled** - aboutMe** - externalUserState** - onPremisesSyncEnabled** - OnPremisesUserPrincipal-Name** - officeLocation** - surname** - deviceEnrollmentLimit**	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality

[3] Azure AD is not relevant in ISE versions prior to 3.2.

[4] Customer determines which External ID store(s) to use.

	• OnPremisesSamAccount-Name** • passwordPolicies** • state** • preferredName** * Only applicable to Active Directory ** Only applicable to Azure Active Directory **Note:** ISE allows the synchronization of arbitrary fields from an external identity store to ISE. Therefore, other potential Personal Data may be collected depending on the customer's configuration of ISE's integration with the identity store.		
5GaaS[5]	• IMSI • KI (Subscription Key) • OPC (Subscriber Operator Code) • IMEI	• Registration Information • Host and Usage Information	• Authenticate and authorize access to the service • Enable product operations and functionality
Application Programming Interface: **Pxgrid** **External RESTful Service**	Pxgrid: • IP Address • MAC Address • Username • IP Address (of DNA-Center) • Fully Qualified Domain Name (FQDN) (of DNA-Center) • Device Unique ID (of DNA-Center) External RESTful Service: • Username • Email Address • First name • Last name • User groups • Last Successful Login IP address • Last Failed Login IP address • Request login name • IP Address • MAC Address • Certificate • External Identity Attributes • External Identity Groups	• Registration Information • Host and Usage Information	• Provision and enroll Customer in the service • Authenticate and authorize access to the service • Enable product operations and functionality • Integrate with Cisco Eco System Partners
Data Connect[6]	• Username • MAC Address • IP Address • Password	• Registration Information	• Authenticate and authorize access to the service

[5] 5GaaS is not relevant in ISE versions prior to 3.2.

[6] Data Connect is not relevant in ISE versions prior to 3.2.

Posture	- IP Address - MAC Address - Workstation - Network Device - Installed Applications - Other Personal Data, depending on the Customer's configuration[7]	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality
Guest Access	- Username - First Name - Last Name - Email Address - Company - Phone number - Last Login Pass IP Address - Last Login Fail IP Address	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality - Enable Guest Access Service
Context Visibility	- Country Name - Department - Email Address - First Name - Last Name - Job Title - Locality Name - Organizational Unit - State Or Province Name - Street Address - Telephone - Username - Endpoint Attributes	- Registration Information - Host and Usage Information	- Provide network visibility - Authenticate and authorize access to the service - Enable product operations and functionality
Mobile device Management	- International Mobile Equipment Identity (IMEI) - Model - Operating System Version - Serial Number - MAC Address - GUID - UDID - Pin Lock Set - Jail Broken	- Registration Information - Host and Usage Information	- Authenticate and authorize access to the service - Enable network access to mobile devices - Enable product operations and functionality
Profiling	- Endpoint Attributes related to RADIUS Probe (Username,hostname) - Endpoint Attributes related to DHCP Probe (Hostname and dhcp-classidentifier) - Endpoint Attributes related to NMAP Probe (OS) - Endpoint Attributes related to HTTP Probe (UserAgent) - Endpoint Attributes related to DNS Probe (FQDN) - Endpoint Attributes related to AD Probe (Username, hostname)	- Registration Information - Host and Usage Information	- Authenticate and authorize access to the service - Enable product operations and functionality

[7] Registry settings, filenames, and hardware attributes may contain Personal Data, and this data may be collected by ISE if so configured using ISE's flexible posture conditions.

Role Based Access Control (RBAC)	- Name - Password - First Name - Last Name - Description - User Groups - Email address	- Registration Information	- Enable product operations and functionality
Bring Your Own Devices (BYOD)	- Guest/Employee: Username - Endpoint: MAC	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality. Specifically, enable BYOD service
My Devices Portal	- Username - Endpoint MAC	- Registration Information - Host and Usage Information	- Provision and enroll Customer in the service - Authenticate and authorize access to the service - Enable product operations and functionality
Threat Centric NAC	- Device Unique ID - IP Address	- Host Information	- Authenticate and authorize access to the service - Enable product operations and functionality
Trustsec	- Last Successful Login IP address - Last Failed Login IP address - Request login name - IP Address - MAC Address - Certificate - External Identity Attributes	- Registration Information - Host and Usage Information	- Authenticate and authorize access to the service - Enable product operations and functionality

3. Data Center Locations

Cisco ISE is primarily managed and hosted by Customers, and except for Interactive Help, Licensing & Deployment, pxGrid Cloud, Support Diagnostics, Telemetry, and User Defined Network, no Cisco ISE data is sent to Cisco or third parties, unless sent to Cisco by the Customer for troubleshooting. As a result, other than for the data from the components (or data sent to Cisco by the Customer for troubleshooting), Cisco ISE does not make or access cross-border transfers of personal data.

For the personal data sent to Cisco by Cisco ISE, Cisco uses third-party cloud hosting providers and business partners to deliver certain services globally. These Cisco and partner data center locations may change from time to time, and this Privacy Data Sheet will be updated to reflect those changes.

Data Center Location	Data Center	Description
United States	Amazon Web Services (AWS)	Used for providing Interactive Help, pxGrid Cloud, and Telemetry
Europe	Amazon Web Services (AWS)	Used for providing Interactive Help, pxGrid Cloud, and Telemetry
Asia	Amazon Web Services (AWS)	Used for providing Interactive Help, pxGrid Cloud, and Telemetry
United States	Snowflake Computing	Used for providing interactive help functionality and storing telemetry data

For data center locations related to Licensing & Deployment, Support Diagnostics and User Defined Network, refer to their Privacy Data Sheets referenced in section 1 of this document.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

5. Access Control

The Customer determines and maintains access control for all data processed by Cisco ISE with the exception of the data from the components listed in the table below. This table lists the personal data used by Cisco ISE that can be accessed by Cisco, who can access such data, and why:

ISE Component	Who has Access	Purpose of the Access
Interactive Help	**Cisco Engineering, WalkMe (Third Party)**	• **Context-based online help guides for ISE Admins** • **Product improvement services** • **Enable product operations and functionality**
Licensing & Deployment	**Cisco**	• **Ensure operation of the product in line with purchased licenses.**
pxGrid Cloud	**Cisco**	• **Maintain separate cloud tenants per customer** • **Integrate with Cisco Eco System Partners**
Telemetry	**Cisco Engineering**	• **Product improvement services** • **Enable product operations and functionality**

6. Data Portability

Data Portability Requirements are not applicable to this product.

7. Data Retention

Customer determines and maintains the deletion schedule for all data processed by Cisco ISE, with the exception of the data identified in Section 5 above, which Cisco retains as follows:

ISE Component	Retention Period	Reason for Retention
Interactive Help	**Deletion upon customer request or immediately upon termination of ISE license**	• **Context-based online help guides** • **Product improvement services**
Licensing & Deployment	**Deletion upon customer request**	• **Product improvement services** • **Enable product operations and functionality**
pxGrid Cloud	**Transient – no more than 24 hours.**	• **Buffer contextual data for third parties receiving data from ISE to ensure continuity**
Telemetry	**Deletion upon customer request**	• **Product improvement services**

8. Personal Data Security

Cisco has implemented the following appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

ISE Component	Security Controls and Measures
Interactive Help	**TLS Encryption**
Licensing & Deployment	**TLS Encryption**
pxGrid Cloud	**TLS Encryption**
Support Diagnostics	**TLS Encryption**
Telemetry	**TLS Encryption**
User Defined Network	**TLS Encryption**

9. Sub-Processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that Customers can expect from Cisco. A current list of sub-processors for the services for Cisco ISE sends personal data to Cisco is below:

Sub-Processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	pxGrid Cloud	Third party cloud-hosting service	United States
Amazon Web Services	pxGrid Cloud	Third party cloud-hosting service	Europe
Amazon Web Services	pxGrid Cloud	Third party cloud-hosting service	Asia
Snowflake Computing	ISE telemetry, interactive help	Third party cloud-hosting service	United States
WalkMe	Usage Data	Interactive help guide for ISE Admins	United States

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco’s Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco’s response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If a Customer has questions or concerns about any product or security notifications, contact the Cisco sales representative.

11. Certifications and Compliance with Privacy Laws

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. ISE is built with security and privacy in mind and is designed so that it can be used by Cisco customers in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations and certifications to demonstrate our commitment to information security and privacy.

12. Exercising Data Subject Rights

Users whose personal data is processed by ISE have the right to request access, rectification, suspension of processing, and / or deletion of the personal data processed by the Service as well as object to processing.

We will ask for identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirected to their employer for a response.
Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3"><b>Chief Privacy Officer</b>
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td><b>Americas Privacy Officer</b>
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td><b>APJC Privacy Officer</b>
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td><b>EMEA Privacy Officer</b>
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, Customers can contact the data protection supervisory authority in their jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.

Addendum 1
Cisco ISE ML Profiling

This Privacy Data Sheet Addendum 1 describes how Cisco ISE Machine Learning (ML) Profiling processes personal data.

1. Overview of ISE ML Profiling Capabilities

The Cisco ML Profiling Cloud aims to provide endpoint visibility by aggregating various sources of endpoint data including network telemetry probes. ML Profiling is a capability in Cisco Identity Services Engine (ISE) available starting in ISE 3.3 that will enhance ISE profiling capabilities by using Crowd-sourced, Machine Learning (ML) driven analytics in cloud to provide automated grouping of unknown endpoints which assists in endpoint classification at scale. ML Profiling will include on-premise software and cloud-enabled analytics. The successful deployment of the ML profiling feature requires large data sets for the machine learning algorithms to operate on. From ISE 3.2, this capability operates purely in 'collection' mode in order to furnish the large data sets required such that ML profiling will be optimal in the future. Starting from ISE 3.3, delivery of the results of this analysis will be via traditional profile updates to ISE. From ISE 3.3 the benefits of the ML Profiling Cloud will be seen directly in ISE through the ML Profiling capability.

This Addendum 1 only addresses the optional Cisco ML Profiling cloud-based feature for Cisco Identity Services Engine (ISE). This capability is configurable during installation and may be turned off at any time, in which case none of the data mentioned in this addendum is stored nor processed by Cisco or third parties. For information regarding the processing of personal data by Cisco Identity Services Engine (ISE), please see the Cisco Identity Services Engine (ISE) Privacy Data Sheet to which this Addendum 1 is attached.
All personal data included in Machine Learning Analytics Data is de-identified locally on the Cisco ISE appliance prior to transfer to the ML Profiling cloud. See Section 8 of this addendum for information regarding the de-identification process.

2. Personal Data Processing

The table below describes how personal data may be processed and stored by Cisco when a customer is using ML Profiling and only applies if the customer enables ML Profiling in ISE.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Customer ID generated by ML Profiling cloud • ISE appliance Deployment ID • Customer CCO ID if available	• Creating a cloud account, product enablement, product use notifications, training, and support. • Associating appliances with applicable customer
Machine Learning Analytics Data	• Dynamic host configuration protocol (DHCP) client identifier • DHCP requested address • DHCP v6 server identifier • Domain name • IP Address • MAC Address • Asset name • Asset serial number • Hostname (i.e., device host name which could include username or the endpoints' host name) • LLDP system name • Calling station ID • Username • System name • Device information (device type, model, vendor, firmware version, manufacturer and operating system with version) [starting from ISE 3.3]	• Use of the product to provide endpoint analytics and remediation.

3. Data Center Locations

Customers have the option of selecting an EU or U.S. cloud for machine learning analytics. All personal data submitted to the cloud will remain in the selected regional cloud. See Section 9 of this Addendum for the AWS data center regional locations.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

5. Access Control

The user of Cisco ISE controls access to the data processed by the product including but not limited to use of AI Analytics. For technical support purposes, a user may provide logs or other files to Cisco when needed to isolate issues in the product or determine if configuration changes are needed. Please refer to the Information Shared by Customers for Support paragraph in Section 5 in the Cisco Identity Services Engine (ISE) Privacy Data Sheet to which this Addendum is attached for information regarding technical support.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Cisco	Creating an account and validating license entitlements and general product operations.
Machine Learning Analytics Data	Cisco	Providing the service features including machine learning analytics

6. Data Portability

Data Portability requirements are not applicable to this product.

7. Data Retention

In addition to the data uploaded to the cloud, all of the data collected and stored “on-premise” by the ML Profiling agent running on Cisco ISE is under control of the Administrator. The Administrator may delete the log files by issuing the appropriate system level commands.

The tables below explain in more detail how data is retained and deleted by the different cloud-based components of AI Analytics:

Personal Data Category	Retention Period	Reason for Retention
Registration Information	Customer can request deletion by submitting deletion request to Cisco TAC	Associate network event data, analytics results and insights with the applicable customer. Associate customer with applicable selected regional cloud and similar administrative purposes.
Machine Learning Analytics Data	Five years. Customer can request deletion by submitting deletion request to Cisco TAC	Deliver product functionality for machine learning analytics

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
Registration Information	Encrypted in transit and at rest.
Machine Learning Analytics Data	Encrypted in transit and at rest.

De-identification Process:
Where noted, personal data is de-identified prior to transfer to the ML Profiling cloud. De-identification is achieved through the use of a deterministic AES encryption process. The encryption key is 32 bytes long and is randomly generated during each tenant registration. The same key is also used by the on-premise agent to decrypt the data received from the cloud, in order to visualize the clear- text information on the user interface. Cisco does not have access to the encryption key, which is retained locally by the customer. For additional security, the network event data is then encrypted in transit to the cloud and is encrypted at rest on AWS by storage of such data within encrypted databases and S3 buckets.

Cloud Authentication:
The communication with the ML Profiling cloud is secured using TLS 1.2 with strong encryption. Mutual authentication between the on-premise agent and the cloud services is ensured through the use of X.509 certificates. The client certificate used by the on-premise agent is issued during the tenant registration process and securely stored on the ISE internal persistent storage.

9. Sub-processors

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the AI Analytics service is below:

Sub-processor	Personal Data Category	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	Machine Learning Analytics Data	Third party cloud-hosting service	United States Germany	For information regarding AWS compliance/certification please refer to documentation online at https://aws.amazon.com/compliance/. Certifications and SOC reports are listed on this webpage and corresponding links under “Assurance Programs”. An AWS SOC 1 or SOC 2 Report can be requested through a Business Development representative. Cisco cannot provide these reports on behalf of AWS, since they are confidential between AWS and the requesting party. A Business Development representative can make the request at this link. The AWS SOC 3 report is publicly available at this link. The AWS SOC 3 report is a summary of the AWS SOC 2 report. It outlines that AWS meets the AICPA’s Trust Security Principles in SOC 2 and includes the external auditor’s opinion of the operation of controls.

10. Other Information

Sections 10 through 13 of the Cisco Identity Services Engine (ISE) Privacy Data Sheet to which this Addendum is attached also apply to ML Profiling.