Cisco Catalyst Center

(formerly DNA Center)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Catalyst Center (formerly called DNA Center).

Cisco Catalyst Center is an on-premise solution and is not hosted or operated by Cisco, and therefore, Cisco does not access or process any personal data from it except as described in this Privacy Data Sheet or unless it is provided to Cisco by the customer.

Cisco will process personal data from Cisco Catalyst Center in a manner that is consistent with this Privacy Data Sheet. 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 processed by Cisco Catalyst Center and sent to Cisco in order to provide Cisco Catalyst Center functionality.

1. Overview

Cisco Catalyst Center is the foundational controller and analytics platform at the heart of Cisco's networking products. Cisco Catalyst Center provides a single dashboard for fundamental management tasks to simplify running a network, including design, policy, provision, and assurance. With Cisco Catalyst Center, IT can respond to changes and challenges faster and more intelligently, with rapid provision and configuration capabilities, and advanced analytics in order to proactively monitor, troubleshoot, and optimize networks.

Cisco Catalyst Center is composed of the Core Solution, which contains the back-end infrastructure, and the Applications. The following Applications are available to customers based on the license subscription obtained:

- Assurance: Provides rich contextual visibility into the user application experience with historical, real-time, and predictive insights across users, devices, applications, and the network. Includes real-time telemetry capability that provides notifications of network conditions that require attention.
- Automation: Simplifies the design, provision, and configuration management of your entire network from a centralized policy-based dashboard, to simplify operations and accelerate policy enforcement consistently and reliably across all devices in access, campus, and WAN network.
- SD Access: Secures end-to-end segmentation, automated user policy access and a single network fabric across wired, wireless, and IoT environments.
- ISE-Bridge: Allows you to monitor and manage your scalable group access policies through integration with Cisco Identity Services Engine (ISE). These policies provide rich identity-based access control functionality with network automation and assurance benefits.
- Group-Based Policy Analytics: Enables you with insights, to create group-based policies by visualizing communications between assets, to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies.

Cisco does not host or operate Cisco Catalyst Center, as it is an on-premise solution operated by the customer; however, unless the customer chooses to deploy Cisco Catalyst Center in air gap mode, some components of Cisco Catalyst Center connect to the Cisco cloud and transmit Personal Data to Cisco as follows:

- As described in this document, to provide the functionality of the product.
- When the optional AI Cloud service, available as part of some license bundles or purchased separately, provides enhanced cloud-enabled features and applications in Cisco Catalyst Center, including AI Network Analytics, AI Endpoint Analytics, and User Defined Network, is enabled. Please see each AI Cloud application Addendum attached to this document for information on how it processes personal data.

- When Systems Information, used to improve your product experience is sent to Cisco. Systems Information provides value to customers by proactively identifying and remediating network issues and understanding product and feature usage to drive product improvements.

  Cisco Customer Experience ("CX") may also leverage this Systems Information for CX purposes, including but not limited to, customer awareness and adoption activities (e.g. deployment guidance, digital journeys, etc.) and providing the CX Cloud for Customers to eligible customers. The Cisco Trust Center provides information about data protection, privacy, and product security, including Data Briefs that describe how we use and share Systems Information. For more information on the full Systems Information collected by Cisco Catalyst Center, please see here. Please see the CX Cloud Privacy Data Sheet for information regarding the processing of personal data by CX.

- When the Cisco Catalyst Center Advanced Features powered by CX Cloud has been enabled by customers with an active Cisco CX subscription (purchased separately or included in some license bundles) or on a trial basis. The Advanced Features provide valuable insights and alerts direct to Catalyst Center in real-time, including Security Advisories, Network Bugs, EoX, and Field Notices. Enabling Advanced Features requires qualifying customers to enable the CX Cloud link through the Catalyst Center UI and consent to the secure sharing of operational data and device configurations with Cisco's US-hosted CX Cloud. For more information about how Advanced Features processes data, please see here in addition to the "Systems Information" sections of this document.

- In the form of Smart License or Virtual account information as part of the onboarding process. For more information regarding Smart Licensing and related data collection, please refer to the Cisco Smart Software Licensing & Smart Accounts Privacy Data Sheet.

For more product information about Cisco Catalyst Center, please refer to the Cisco Catalyst Center Product Data Sheet. Please note that if a customer elects to use third-party APIs or SDKs with Catalyst Center, such usage may result in data being transferred to third-party applications. Before using, please consult the applicable third-party documentation for such third-party APIs and SDKs to understand how they impact personal data.

2. Personal Data Processing

The tables below lists the personal data processed by Cisco Catalyst Center to provide its services and describes why the data is processed. For more information on data management and the purpose of processing, please see our Trust Center on How We Manage Data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Managed Device Information	• MAC address • IP address • Device Hostname • Catalyst Center Hostname[1] • Configurations[2] • Device type and OS • Domain name • Timestamp for device connection • Routing protocol password	Use of the solution, troubleshooting, service and support of the system, improvement of the system, security, tracking changes made to the network, audit logging, and Systems Information.

[1] This data is only collected if Pendo is enabled. Pendo is optional and can be turned off. For more information on Pendo, please see Section 8 "Subprocessors."
[2] Only applicable if using the Advanced Features.

Catalyst Center Operational Information	• Runtime status • Component versions • Log files • Events • Troubleshooting data	Use of the solution, troubleshooting, service and support of the system, improvement of the system, security, tracking changes made to the network, and audit logging.
Cisco Account/Catalyst Center User Information	• Admin CCO / cisco.com userID • Customer name and address[3] • Smart Account username • Virtual Account username • Admin UserID • User role • ISE credentials • MS-Teams email and username[4] • Local username and email[5] • Browser Information[6] • Catalyst Center UI Navigation[7] (mousedown on button, hyperlink, clickable element, page change, dwell time) • CLI credentials • SNMP credentials	Verification and correlation of applicable customer and their Cisco account, for product support, customer service, license verification, and Systems Information.

3. Data Center Locations

Non-air gap deployments of Cisco Catalyst Center have the option of selecting an EU (Frankfurt, Germany), APJC (Singapore), or a US-based regional cloud.

With the exception of Systems Information and Cisco Account / Catalyst Center User Information, which are sent to Cisco's datacenter in the United States, all personal data submitted to a selected regional cloud will remain in that regional cloud.

If a customer deploys Cisco Catalyst Center in a different country than the selected regional cloud, then a cross-border transfer would occur as data is exchanged between the customer's Cisco Catalyst Center instance and the Cisco Catalyst Center cloud environment on Amazon Web Services (AWS). See Section 8 for the specific AWS data center regional locations. Non-air gap deployments of Cisco Catalyst Center located outside the U.S. will also incur a cross-border transfer for Systems Information, which goes to the Cisco data warehouse within the Cisco network in the United States.

If the customer elects to use Cisco AI Network Analytics, AI Endpoint Analytics, or User Defined Network with Cisco Catalyst Center, please refer to the corresponding Addendum to this document for more information regarding data center locations used by those features.

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

[3] Only personal data where the customer is an individual person.
[4] Only for users enabling the AppX Connect feature.
[5] Determined by customer.
[6] This data is only collected if Pendo is enabled. Pendo is optional and can be turned off.
[7] This data is only collected if Pendo is enabled. Pendo is optional and can be turned off.

5. Access Control

Data processed on-premise by Cisco Catalyst Center is under the control of the customer and is not accessed by Cisco.

Managed Device Information and Cisco Account /Catalyst Center User Information that is sent to Cisco's cloud as part of the basic operation of the product is not accessed by Cisco personnel unless for support reasons initiated by the customer. For technical support purposes, a user may also 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 paragraph below for more information on Data Shared by Customers for Support.

Catalyst Center Operational Information may be send to Cisco TAC if granted access by customer for troubleshooting reasons.

All Managed Device Information and Cisco Account / Catalyst Center User Information that is included as part of Systems Information is classified by Cisco as Highly Confidential, and is only accessible by authorized Cisco personnel.

For AI Network Analytics, AI Endpoint Analytics, or User Defined Network, please refer to the corresponding Addendum to this document for more information regarding access to personal data used by that feature.

Data Shared by Customers for Support
If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process Cisco Catalyst Center Operational Data provided by the customer. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to resolve issues. For more information, please refer to the Cisco Technical Assistance (TAC) Service Delivery Privacy Data Sheet.

6. Data Retention

Data collected by Cisco Catalyst Center and stored on-prem is under the control of the customer and may be deleted at any time using the appropriate system-level commands.

The tables below lists the personal data sent to Cisco by the components of Cisco Catalyst Center, the length of time that data needs to be retained, and why we retain it.

Catalyst Center Core Solution

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	7 years or upon request	Use of product, troubleshooting, service and support, auditing, and product improvement.
Catalyst Center Operational Information	Stored on-prem. Customer determines retention period	Determined by Customer
Cisco Account/Catalyst Center User Information	7 years or upon request	Correlation and connection of customer/user accounts, authentication, license and entitlement verification, auditing, and product improvement.

Assurance

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	5 years	Use of product, troubleshooting, service and support, auditing, and product improvement.
Catalyst Center Operational Information	Stored on-prem. Customer determines retention period.	Determined by Customer
Cisco Account/Catalyst Center User Information	Not collected	Not applicable.

Automation

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information[2]	Stored on-prem only unless using Advanced Features.	Necessary for Advanced Features. Please see the CX Cloud Privacy Data Sheet for CX's data retention policy.
Catalyst Center Operational Information	Stored on-prem only. Customer determines retention period.	Determined by Customer
Cisco Account/Catalyst Center User Information	Stored on-prem only. Customer determines retention period.	Determined by Customer

SD Access

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	Stored on-prem only unless using ISE.	Necessary for ISE integration. Please see the ISE Privacy Data Sheet for ISE's data retention policy.
Catalyst Center Operational Information	Stored on-prem. Customer determines retention period.	Determined by Customer
Cisco Account/Catalyst Center User Information	Stored on-prem only unless using ISE.	Necessary for ISE integration. Please see the ISE Privacy Data Sheet for ISE's data retention policy.

ISE-Bridge

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	Not collected	Not applicable.
Catalyst Center Operational Information	Not collected	Not applicable.
Cisco Account/Catalyst Center User Information	Stored on-prem. Customer determines retention period.	Determined by Customer

Group-Based Policy Analytics

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	Stored on-prem. Customer determines retention period.	Determined by Customer
Catalyst Center Operational Information	Stored on-prem. Customer determines retention period. only	Determined by Customer
Cisco Account/Catalyst Center User Information	Not collected	Determined by Customer

Systems Information

Personal Data Category	Retention Period	Reason for Retention
Managed Device Information	7 years or upon request	Product improvement and customer adoption.
Catalyst Center Operational Information	Not collected	Not applicable.

Cisco Account/Catalyst Center User Information	7 years or upon request	Product improvement, customer adoption, and account association.

7. 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. These technical and organizational measures include the following:

Catalyst Center Core Solution

Personal Data Category	Security Controls and Measures
Managed Device Information	Encrypted over TLS 1.3/1.2 in transit and at rest.
Catalyst Center Operational Information	Stored on-prem. Security controls and measures determined by Customer.
Cisco Account/Catalyst Center User Information	Encrypted over TLS 1.3/1.2 in transit and at rest.

Assurance

Personal Data Category	Security Controls and Measures
Managed Device Information	Encrypted over TLS 1.3/1.2 in transit and at rest.
Catalyst Center Operational Information	Stored on-prem. Security controls and measures determined by Customer.
Cisco Account/Catalyst Center User Information	Not collected.

Automation

Personal Data Category	Security Controls and Measures
Managed Device Information	Encrypted over TLS 1.3/1.2 in transit and at rest.
Catalyst Center Operational Information	Stored on-prem. Security controls and measures determined by Customer.
Cisco Account/Catalyst Center User Information	Stored on-prem. Security controls and measures determined by Customer.

SD Access

Personal Data Category	Security Controls and Measures
Managed Device Information	Encrypted over TLS 1.2 in transit and at rest when using ISE, otherwise stored on-prem only and security controls and measures are determined by Customer.

Catalyst Center Operational Information	Stored on-prem. Security controls and measures determined by Customer.
Cisco Account/Catalyst Center User Information	Encrypted over TLS 1.2 in transit and at rest when using ISE, otherwise stored on-prem and security controls and measures are determined by Customer. .

ISE-Bridge

Personal Data Category	Security Controls and Measures
Managed Device Information	Not collected or stored.
Catalyst Center Operational Information	Not collected or stored.
Cisco Account/Catalyst Center User Information	Stored on-prem. Security controls and measures determined by Customer.

Group-Based Policy Analytics

Personal Data Category	Security Controls and Measures
Managed Device Information	Stored on-prem. Security controls and measures determined by Customer.
Catalyst Center Operational Information	Stored on-prem. Security controls and measures determined by Customer.
Cisco Account/Catalyst Center User Information	Not collected.

Systems Information

Personal Data Category	Security Controls and Measures
Managed Device Information	Encrypted over TLS 1.3/1.2 in transit and at rest.
Catalyst Center Operational Information	Not collected.
Cisco Account/Catalyst Center User Information	Encrypted over TLS 1.3/1.2 in transit and at rest.

8. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and 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 service is below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	• Managed Device Information	Third party cloud-hosting service	United States	For information regarding AWS compliance/certification

	• Cisco Account / Catalyst Center User Information			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".
Snowflake Computing	• Managed Device Information • Cisco Account / Catalyst Center User Information	Cloud Data Warehouse Solution	AWS United States	Data is only sent to Snowflake as part of Systems Information. See AWS information. Also see https://www.snowflake.com/product/security-and-trust-center/.
WalkMe	• Browser Information	Provides interactive help for Catalyst Center	AWS United States	https://www.walkme.com/walkme-security/ https://www.walkme.com/privacy-policy/
Pendo	• Hostname, Browser Information, Catalyst Center UI Navigation (mousedown on button, hyperlink, clickable element, page change, dwell time)	Clickstream and user behavior data analytics	Google Cloud App Engine United States	Data sent to Pendo is also sent to Snowflake as part of Systems Information. Customers who wish to disable this collection of data, can do so by contacting their Account Managers who can begin the opt-out process. https://pendo.trust.page
UserVoice	• Customer Name, Email Address	User Feedback	United States	See AWS information. Also see: https://www.uservoice.com/security-compliance

9. 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), and the Advanced Security Initiatives Group (ASIG).

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 you have questions or concerns regarding product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Requirements

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. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

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

11. Exercising Data Subject Rights

Users whose personal data is processed by the Service 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. Data portability requirements are not applicable to this product.

We will confirm 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 redirect 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">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
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, you can contact the data protection supervisory authority in your 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.

12. General Information

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

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. 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 AI Network Analytics

This Privacy Data Sheet Addendum 1 describes how Cisco AI Network Analytics processes personal data.

1. Overview

Cisco AI Network Analytics ("AI Network Analytics") is a cloud-based machine learning capability within Cisco Catalyst Center that is included with Cisco Catalyst Center Assurance under the Cisco Catalyst Advantage license bundle. AI Network Analytics deploys machine learning technology to provide network visibility and insights that drive network analytics and accelerated remediation. Through the use of machine learning technology, AI Network Analytics is capable of dynamically defining the expected behavior of a network and identifying issues in the network. At the same time, it enables customers to more rapidly identify root causes and more quickly remediate and resolve network issues.

This Privacy Data Sheet Addendum 1 only addresses the optional AI Network Analytics cloud-based feature:

- For more information regarding AI Network Analytics, please see here.
- For information regarding the processing of personal data by Cisco Catalyst Center, please see the Cisco Catalyst Center Privacy Data Sheet to which this Addendum 1 is attached.
- For general information on the Cisco Catalyst Center product, please see the Cisco Catalyst Center Product Data Sheet.
- For general information on how Cisco collects and uses Systems Information (formerly "Product Usage Telemetry"), please see the Systems Information Data Brief.

2. Personal Data Processing

The tables below describe how personal data may be processed and stored by Cisco when a customer is using AI Network Analytics.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Customer ID generated by AI Network Analytics • Catalyst Center appliance membership ID if available • Catalyst Center appliance serial number(s) • Customer CCO ID if available	Creating a cloud account, product enablement, product use notifications, training, support, and associating appliances with applicable customer.
Network Event Data[8]	• MAC address • IP address • Hostname (i.e., device name) • End User Username[9] • SSID • Access point name and MAC address/location • Application Usage Data	Use of the product to provide network visibility and insights, network analytics, and remediation.

[8] This data is de-identified locally prior to transfer to the AI Network Analytics cloud. See Section 7 "Personal Data Security" for information regarding the de-identification process.

[9] End User Usernames refer only to the end users clients connecting to the network using Authentication, Authorization, & Accounting (AAA); system administrator management usernames and session information are not processed or exported.

	• Syslog Data Messages[10]	
Comments	• Catalyst Center User ID for admins submitting comments • Open text field for user to submit comments regarding the service. It is possible, but not recommended, that a user could include personal data in the comments.	Comment field is used to obtain feedback from users in order to Improve the system.

3. Data Center Locations

Customers have the option of selecting an EU or U.S. AI Network Analytics cloud. All personal data submitted to the cloud will remain in the selected regional cloud. See Section 8 for the AWS data center regional locations. For troubleshooting and development purposes, the data may be processed by the product development teams in the EU and US as well.

4. Cross-Border Data Transfer Mechanisms

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

- 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 Catalyst Center controls access to the data processed by the product including but not limited to use of AI Network 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 of the Cisco Catalyst Center Privacy Data Sheet to which this Addendum is attached for information regarding technical support.

The table below lists the personal data used by Cisco Catalyst Center to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Cisco	Creating an account and validating license entitlements and general product operations.
Personal Data Associated with Network Events	Cisco	Providing the service features including network analytics and visibility.
Comments	Cisco	Product improvement and auditing.

6. Data Retention

Data collected by the Cisco Catalyst Center Core Solution and by the AI Network Analytics agent is under control of the user Admin. The Admin may delete the log files by issuing the appropriate system level commands. End user data elements such as IP/MAC address stored in the inventory/topology data base may be deleted by the Admin issuing a SQL Query matching the data element desired to be deleted.

[10] Exporting Syslog Messages is an optional Opt-In feature only and is not turned on by default. Please note that Syslog Messages may contain other data types listed in this section and that footnotes 4 and 5 do not apply to the data contained in Syslog Messages.

The tables below explain in more detail how data is retained and deleted by the different components of AI Network 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.
Personal Data Associated with Network Events	Five years. Customer can request earlier deletion by submitting deletion request to Cisco TAC.	Deliver product functionality (network event analytics).
Comments	Five years. Customer can request earlier deletion by submitting deletion request to Cisco TAC.	Product improvement and auditing.

7. 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.
Personal Data Associated with Network Events	Encrypted in transit and at rest.
Comments	Encrypted in transit and at rest.

De-identification Process:
Where noted, personal data is de-identified prior to transfer to the AI Network Analytics cloud. De-identification is completed 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 AI Network Analytics 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 Cisco Catalyst Center credential store.

8. 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 you can expect from Cisco. A current list of sub-processors for the service is below: A current list of sub-processors for the AI Network Analytics service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	• Registration Information • Personal Data Associated with Network Events • Comments	Third party cloud-hosting service	United States – East Europe - Frankfurt	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”.

9. Other Information

Sections 9 through 12 of the Cisco Catalyst Center Privacy Data Sheet to which this Addendum is attached also applies to AI Network Analytics.

Addendum 2
Cisco AI Endpoint Analytics

This Privacy Data Sheet Addendum 2 describes how Cisco AI Endpoint Analytics processes personal data.

1. Overview

Cisco AI Endpoint Analytics is an endpoint visibility tool that aims to provide device visibility by aggregating various sources of device data including network telemetry probes, deep packet inspection (DPI) and configuration management database (CMDB) integration. A robust set of device fingerprints, including ISE and DPI based, are used to automatically classify and assign a trust score to endpoints.

The Application Visibility service, hosted as an application stack within Cisco Catalyst Center, lets you enable the Controller-Based Application Recognition (CBAR) function on a specific device to classify thousands of network and home-grown applications, network traffic and endpoint profiling data.

Crowd-sourced, machine learning (ML) driven analytics automate clustering of unknown endpoints to classify endpoints beyond the capabilities of the device fingerprints. Cisco AI Endpoint Analytics includes on-premise software and cloud-enabled analytics.

This Addendum 2 only addresses the optional Cisco AI Endpoint Analytics cloud-based feature:

- For information on how Cisco Identity Services Engine (ISE) processes personal data, please see here.
- For more information regarding AI Endpoint Analytics, please see here.
- For information regarding the processing of personal data by Cisco Catalyst Center, please see the Cisco Catalyst Center Privacy Data Sheet to which this Addendum 2 is attached.
- For general information on the Cisco Catalyst Center product, please see the Cisco Catalyst Center Product Data Sheet.
- For general information on how Cisco collects and uses Systems Information (formerly “Product Usage Telemetry”), please see the Systems Information Data Brief.

2. Personal Data Processing

The tables below describe how personal data may be processed and stored by Cisco when a customer is using Cisco AI Endpoint Analytics.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information[11]	• Customer ID generated by AI Endpoint Analytics cloud • Catalyst Center appliance membership ID if available • Catalyst Center appliance serial number(s) • Customer CCO ID if available	Creating a cloud account, product enablement, product use notifications, training, support, and associating appliances with applicable customer.
Endpoint Profiling Data[12]	• MAC Address • Hostname (i.e., device host name which could include username) • IP Address • LLDP Asset inventory details (e.g. asset name, system name)	Use of the product to provide endpoint visibility, classification and insights.
Machine Learning Analytics Data[13, 14]	• 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 • Network Connection Information[15] • Application Usage Data	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, and an EU, US, Asia, or Canada based cloud for Endpoint Profiling Data. All personal data submitted to the cloud will remain in the selected regional cloud. See Section 8 for the AWS data center regional locations. For troubleshooting and development purposes, the data may be processed by the development teams in the EU and US as well.

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)

[11] This data allows Cisco to identify which appliances belong to which customer.
[12] This section only applies if customer enables CBAR within the settings page.
[13] The personal data included in Machine Learning Analytics Data is de-identified locally on the Catalyst Center appliance prior to transfer to the AI Endpoint Analytics cloud. See Section 7 Personal Data Security for information regarding the de-identification process.
[14] This section only applies if customer enables AI Endpoint Analytics Cloud within the settings page.
[15] These data elements only apply if customer additionally enables *both* NetFlow AI Spoofing Detection and the option to "Send data to help Cisco improve the model" in the AI Spoofing Detection section of the AI Analytics settings page.

- 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 Catalyst Center controls access to the data processed by the product including but not limited to use of Cisco AI Endpoint 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 Catalyst Center 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.
Endpoint Profiling Data	Cisco	Providing the service features including endpoint visibility and insights.
Machine Learning Analytics Data	Cisco	Providing the service features including machine learning analytics.

6. Data Retention

Data collected “on-premise” by Cisco Catalyst Center and by the Cisco AI Endpoint Analytics agent is under control of the user Admin. The Admin may delete the log files by issuing the appropriate system level commands. End user data elements such as IP/MAC address stored in the inventory/topology data base may be deleted by the Admin.

The tables below explain in more detail how data is retained and deleted by the different cloud-based components of AI Endpoint 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.
Endpoint Profiling Data	6 Months. Customer can request earlier deletion by submitting deletion request to Cisco TAC.	Deliver product functionality for endpoint visibility and insights.
Machine Learning Analytics Data	Five Years. Customer can request earlier deletion by submitting deletion request to Cisco TAC.	Deliver product functionality for machine learning analytics.

7. 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.
Endpoint Profiling Data	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 Cisco AI Endpoint Analytics machine-learning cloud. De-identification is completed 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 Cisco AI Endpoint Analytics 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 in the Cisco Catalyst Center credential store.

8. 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 Cisco AI Endpoint Analytics service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	Endpoint Profiling Data	Third party cloud-hosting service	United States Germany Canada Japan	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”.
Amazon Web Services	Machine Learning Analytics Data	Third party cloud-hosting service	United States Germany	See above for AWS information.

9. Other Information

Sections 9 through 12 of the Cisco Catalyst Center Privacy Data Sheet to which this Addendum is attached also applies to Cisco AI Endpoint Analytics.

Addendum 3
Cisco User Defined Network

This Privacy Data Sheet Addendum 3 describes how Cisco User Defined Network processes personal data.

1. Overview

Cisco® User Defined Network (UDN) is a Cisco network solution available through Cisco Catalyst Center that provides users with a personal network experience in the shared network environment. Cisco UDN enables secure and remote onboarding of client devices and allows IT staff to give each user oversight of their own network partition. Users can register their personal devices on their own from anywhere using the intuitive Cisco UDN mobile app. Once the devices have been registered and the user arrives at the shared network location, their wireless devices will connect to the shared network as usual with their devices placed into their personal network. Cisco UDN also allows users to securely control who can connect to their network for sharing and collaboration, providing the ability to invite trusted users such as friends to their personal network through the mobile app. Cisco UDN is available with Catalyst Advantage and certain ala carte licenses.

This Addendum 3 only addresses the optional Cisco User Defined Network cloud-based feature:

- For more information on Cisco User Defined Network, please visit here.
- For information regarding the processing of personal data by Cisco Catalyst Center, please see the Cisco Catalyst Center Privacy Data Sheet to which this Addendum 3 is attached.
- For general information on the Cisco Catalyst Center product, please see the Cisco Catalyst Center Product Data Sheet.
- For general information on how Cisco collects and uses Systems Information (formerly "Product Usage Telemetry"), please see the Systems Information Data Brief.

2. Personal Data Processing

The table below describes how personal data is processed and stored when a customer is using Cisco UDN:

Personal Data Category	Types of Personal Data	Purpose of Processing
CCO Account Registration Information for Tenant Admin[16]	Admin User data: • First name • Last name • Email	Creating a Customer Cloud Admin account is required for product registration, enablement, use, notifications, training, and support.
User Credentials[18]	End User data: • First Name • Last Name • Email address • User defined network name	Authenticate the End User's access to UDN.

[16] Stored in the Cloud.

User Device Identifiers[17]	• MAC Address • User's name • SSID • Device type • Hostname (i.e., device host name which could include username) • Timestamp for device connection	For UDN to identify the devices belonging to the End User and perform its functions.
Personal Data Associated with Network Events[19]	• MAC address • Hostname (i.e., device name) • User Name • SSID • Timestamp for device connection	For UDN to identify the devices belonging to the End User and perform its functions.
Mobile App: User Credentials & User Device Identifiers[19]	End User data: • First name • Last name • Email User Device data: • MAC Address • User's name • SSID • Device type • Hostname (i.e., device host name which could include username) • Timestamp for device connection	Authenticate End User's access to Mobile App and register End User devices.
Systems Information[19] .	• CCO ID for Catalyst Center super admin(s)	Systems Information is collected to provide value to customers by proactively identifying and remediating network issues and understanding product and feature usage to drive product improvements. CCO ID is used to correlate the applicable customer with the customer's account and license entitlements. Please see the Catalyst Center Product Data Sheet referenced above for more information on Catalyst Center and Systems Information.

3. Data Center Locations

Cisco UDN runs on AWS in the United States.

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 Catalyst Center controls access to the data processed by the product including UDN. 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

[17] Stored in the Cloud and on customer's device.

configuration changes are needed. Please refer to the Information Shared by Customers for Support paragraph in Section 5 of the Cisco Catalyst Center 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.
	Customer Admin	Configuration and use of the product, tracking End User access, and auditing.
User Credentials	Cisco	Allow End User to access UDN and for the product to perform its functions.
	Customer End User	To access UDN.
User Device Identifiers	Cisco	UDN needs information about the devices belonging to the End User to perform its functions.
	Customer End User	End User must input their device identifiers to use the product.
Personal Data Associated with Network Events	Cisco	For the product to perform its functions.
	Customer End User	Provide network visibility and insights.
Mobile App: User Credentials & User Device Identifiers	Cisco	Authenticate End User's access to Mobile App and perform its functions.
	Customer End User	To access and use the Mobile App.
Systems Information	Catalyst Center Admin	System Information is collected to provide value to customers by proactively identifying and remediating network issues and understanding product and feature usage to drive product improvements.

6. Data Retention

Data collected by the Cisco Catalyst Center Core Solution and by the Cisco UDN application are under the control of the Admin User. End User data elements such as IP/MAC address and device information stored in the Cisco UDN application database can be controlled by the Admin or the End User via APIs. The Cisco Catalyst Center Admin may delete 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 components of UDN:

Personal Data Category	Retention Period	Reason for Retention
Registration Information	Until the End User unsubscribes or upon customer's request to Cisco TAC.	Associate offer event data, access audit and administrative purposes.
User Credentials	Until the End User unsubscribes or upon customer's request to Cisco TAC.	Associate network event data, analytics results and insights with the applicable devices and similar administrative purposes. Troubleshooting and enabling customer to do network utilization reporting and capacity planning.
User Device Identifiers	UDN provides a mechanism for the Admin or End User to delete its UDN application data via API at any time during the service or at the time the End User wants to unsubscribe. With this mechanism, the application data will be removed from the primary running	Associate network event data, analytics results and insights with the applicable devices and similar administrative purposes. Troubleshooting and enabling customer to do network utilization reporting and capacity planning.

	database immediately and the copied backup data will automatically delete within 7 days.	
Personal Data Associated with Network Events	UDN provides a mechanism for the Admin or End User to delete its UDN application data via API at any time during the service or at the time the End User wants to unsubscribe. With this mechanism, the application data will be removed from the primary running database immediately and the copied backup data will automatically delete within 7 days.	Associate network event data, analytics results and insights with the applicable devices and similar administrative purposes. Troubleshooting and enabling customer to do network utilization reporting and capacity planning.
Mobile App: User Credentials & User Device Identifiers	When the End User logs out from the Mobile App, their personal data is deleted from the mobile device. If the End User leaves the customer organization and has the Mobile App installed, that End User's access is invalidated.	The offer needs this information to perform its functions.
Systems Information	Please see the Catalyst Center Product Data Sheet.	Please see the Catalyst Center Product Data Sheet: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html?dtid=osscdc000283

7. 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.
User Credentials	Encrypted in transit and at rest.
User Device Identifiers	• Data in transit within UDN, which is hosted in AWS, is not encrypted. Please see Section 8 below for details on AWS's Security Assurances. • Data in transit to and from UDN is encrypted. • Data at rest is encrypted.
Personal Data Associated with Network Events	• Data in transit within UDN, which is hosted in AWS, is not encrypted. Please see Section 8 below for details on AWS's Security Assurances. • Data in transit to and from UDN is encrypted. Data at rest is encrypted.
Mobile App: User Credentials & User Device Identifiers	• Data at rest is encrypted. • Data in transit to and from UDN is encrypted.
Systems Information	Please see the Cisco Catalyst Center Product Data Sheet.

8. 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 UDN are below:

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	• Registration Information	Third party cloud-hosting service	U.S West (Oregon)	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."

9. Other Information

Sections 9 through 12 of the Cisco Catalyst Center Privacy Data Sheet to which this Addendum is attached also apply to Cisco User Defined Network.