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 will process personal data from 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 Catalyst Center in order to provide its functionality.

1. Overview of Catalyst Center Capabilities

Catalyst Center is the foundational controller and analytics platform at the heart of Cisco's networking products. Catalyst Center provides a single dashboard for every fundamental management task to simplify running a network, including design, policy, provision, and assurance. With 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.

The Catalyst Center Core Solution contains the back-end software components that support Catalyst Center applications. Customers may also use the following applications 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.
- Group-Based Access Control Policy: Allows you to monitor and manage your scalable group access policies. 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.

Except as provided below, Cisco does not host or operate Cisco Catalyst on the customer's behalf as it is an on-premise solution operated by the customer:

- The optional Cisco Connected Catalyst service, availible as part of some license bundles or purchased seperately, provides enhanced cloud-enabled features and applications in Catalyst Center, including AI Network Analytics, AI Endpoint Analytics, and User Defined Network. Please see each feature's respective section for information on how it processes personal data.
- Personal data may be provided to Cisco in the form of a user credential to associate it with a related Cisco.com account (i.e. CCO) or Smart License account. For more information regarding Smart Licensing and related data collection, please refer to the Smart Software Licensing Privacy Data Sheet.
- For more product information about Catalyst Center, please refer to the Cisco Catalyst Center Product Data Sheet.
- 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 (formerly "Product Usage Telemetry") and Personal Data.

©2023 Cisco and/or its affiliates. All rights reserved.

- If a customer elects to use Catalyst Platform third-party APIs or SDKs, 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 describe how personal data may be processed and stored by a customer when using Catalyst Center.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Device Identifiers	• MAC address • IP address • Hostname (i.e., device host name which could include username or the endpoint's host name) • Device type • Device OS (e.g., MacOS, Windows) • SSID • VLAN ID • VNID (Fabric) • Domain name • Wired access switch port • Access point name and MAC address/location • Timestamp for device connection • LLDP Asset inventory details (e.g. asset name, system name)	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
User Credentials	• CCO / cisco.com userID • Smart Account User Name • Admin UserID • User group • Smart Account • Virtual Account name • ISE username, one-way hashed password, and user details (i.e. first and last name, physical address, email address, phone number, department, organizational unit, job title) • [Only for users enabling the **AppX Connect** feature] MS-Teams email and username	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
Systems Information	• CCO ID for Catalyst Center super admin(s) • Local Username[1] • Customer Name and Address[2]	This data is collected to correlate the Systems Information with the applicable customer and their Cisco account, for product support, customer service, and license verification purposes. Please see the Catalyst Center Product Data Sheet referenced above for more information on the other Systems Information collected by Catalyst Center. 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. Cisco Customer Experience ("CX") may also leverage 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. Note: Although Catalyst Center does not share personal data with CX, please see the CX Cloud for Customers Privacy Data Sheet at the

[1] Determined by customer.
[2] Customer name and address would only be personal data where the customer is an individual person.

©2023 Cisco and/or its affiliates. All rights reserved.

		Cisco Trust Portal for information regarding the processing of personal data by CX.

3. Data Center Locations

Customers have the option of selecting an EU (Germany), APJC (Singapore), or US-based cloud for Cisco Connected Catalyst (the service that provides cloud-enabled features in Catalyst Center). All personal data submitted to a selected regional cloud will remain in that regional cloud. If a customer's Catalyst Center is located in a different country than the selected regional cloud, then a cross-border transfer would occur as data is transferred to the Connected Catalyst environment on Amazon Web Services (AWS). See Section 9 for the specific AWS data center regional locations.

A Catalyst Center instance located outside the U.S. will also incur a cross-border transfer regarding 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 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

5. Access Control

The user of Catalyst Center controls access to the data processed on premise by the product.

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 paragraph below regarding Information Shared by Customer for Support. Only authorized Cisco personnel have access to Systems Information, which is classified by Cisco as Highly Confidential. If the customer elects to use Cisco AI Network Analytics, AI Endpoint Analytics, or User Defined Network with Catalyst Center, please refer to the corresponding Addendum to this document for more information regarding access to personal data used by that feature.

Information Shared by Customer for Support

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from Catalyst Center that is 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 TAC Support Essentials Privacy Data Sheet.

6. Data Portability

Data Portability requirements are not applicable to this product.

7. Data Deletion & Retention

Data collected by the Catalyst Center Core Solution is under control of the customer 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 database may be deleted by the Admin issuing an SQL Query matching the data element desired to be deleted.

The tables below explain in more detail how data is retained and deleted by the different components of Catalyst Center:

©2023 Cisco and/or its affiliates. All rights reserved.

Catalyst Center Core Solution

Personal Data Category	Retention Period	Reason for Retention
User Device Identifiers	4 Weeks Logs may be overwritten at different periods depending on storage capacity of device deployed	Logs are captured for troubleshooting, service and support of the system, improvement of the system.
User Credentials	Customer defined	To associate a user credential with CCO or Smart License account to the system, which is stored by the Catalyst Center License server.
Systems Information	On-Prem: Customer defined Cloud: Upon request	Purpose of retaining CCO ID is to correlate the applicable customer with the customer's Cisco account and license entitlements. Systems Information is retained to provide value to customers by proactively identifying and remediating network issues and understanding product and feature usage to drive product improvements.

Assurance

Personal Data Category	Retention Period	Reason for Retention
User Device Identifiers	30 days	Troubleshooting, service and support of the system, improvement of the system.
User Credentials	On-Prem: 30 days Cloud: 1 Hour	Provision of functionality, troubleshooting, service and support of the system, improvement of the system.

Automation

Personal Data Category	Retention Period	Reason for Retention
User Device Identifiers	60 days	Troubleshooting, service and support of the system, improvement of the system.
User Credentials	Customer defined	Troubleshooting, service and support of the system, improvement of the system.

SD Access - Wireless

Personal Data Category	Retention Period	Reason for Retention
User Device Identifiers	Duration of time the device is connected to a wireless network	Troubleshooting, service and support of the system, improvement of the system

Group-Based Access Control Policy

Personal Data Category	Retention Period	Reason for Retention
User Credentials	Customer defined	Access, troubleshooting, service and support of the system.

Group-Based Policy Analytics

Personal Data Category	Retention Period	Reason for Retention
User Device Identifiers	14 days	Customer can view the visibility of netflow data in the network for last 14 days.

©2023 Cisco and/or its affiliates. All rights reserved.

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.

Catalyst Center Core Solution

Personal Data Category	Security Controls and Measures
User Device Identifiers	None
User Credentials	TLS 1.2, TLS 1.1, TLS 1.0 (if enabled by customer) encryption in transit. Not encrypted at rest.
Systems Information	Encrypted in transit. Not encrypted at rest.

Assurance

Personal Data Category	Security Controls and Measures
User Device Identifiers	Encrypted in transit over TLS 1.2. Not encrypted at rest.
User Credentials	On-Prem: Encrypted in transit over TLS 1.2. Not encrypted at rest. Cloud: Encrypted in transit and at rest.

Automation

Personal Data Category	Security Controls and Measures
User Device Identifiers	Encrypted in transit. Not encrypted at rest.
User Credentials	Encrypted in transit. Not encrypted at rest.

SD Access - Wired

Personal Data Category	Security Controls and Measures
User Device Identifiers	N/A (No handling or storage of User Device Identifiers)
User Credentials	Encryption in transit over TLS 1.2. Data is not stored.

Access - Wireless

Personal Data Category	Security Controls and Measures
User Device Identifiers	Encrypted in transit and at rest.
User Credentials	Encrypted in transit and at rest.

Group-Based Access Control Policy

Personal Data Category	Security Controls and Measures
User Credentials	Encrypted in transit and at rest.

©2023 Cisco and/or its affiliates. All rights reserved.

Group-Based Policy Analytics

Personal Data Category	Security Controls and Measures
User Device Identifiers	Encrypted in transit and at rest.

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

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services	• CCO ID for Catalyst Center super admins	Third party cloud-hosting service	United States	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.
Snowflake Computing	• CCO ID for Catalyst Center super admins	Cloud Data Warehouse Solution	AWS United States	See AWS information. Also see https://www.snowflake.com/product/security-and-trust-center/.
WalkMe	• Sys Admin Username and Hostname, Location, User Behavior Tracking (mousedown, pageChange, keypress, change (input), submit, doubleclick, idle, active)	Provides interactive help for Catalyst Center	AWS United States	See AWS information. Also see https://www.snowflake.com/product/security-and-trust-center/.
Pendo	• Sys Admin Username and Hostname, Location, User Behavior Tracking (mousedown, pageChange, keypress, change (input), submit, doubleclick, idle, active)	Clickstream and user behavior data analytics	Google Cloud App Engine United States	Customers who wish to disable this collection of data, can do so by contacting their Account Managers who can begin the opt-out process.

10. Information Security Incident Management

©2023 Cisco and/or its affiliates. All rights reserved.

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. Please contact your Cisco sales representative with any questions or concerns regarding product or security notifications.

11. Certifications and Compliance with Privacy Requirements

Cisco's Security & Trust and Legal Organizations 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.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

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.

©2023 Cisco and/or its affiliates. All rights reserved.

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.

13. General Information

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

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

©2023 Cisco and/or its affiliates. All rights reserved.

Addendum 1
Cisco AI Network Analytics

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

1. Overview of Cisco AI Network Analytics Cloud Capabilities

Cisco AI Network Analytics ("AI Network Analytics") is a cloud-based machine learning capability within Catalyst Center that is included with Catalyst Center Assurance under the 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 Cisco 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 Catalyst Center, please see the Catalyst Center Privacy Data Sheet to which this Addendum 1 is attached.
- For general information on the Catalyst Center product, please see the 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[3]	• 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.
Personal Data Associated with Network Events	• MAC address4 • IP address2 • Hostname (i.e., device name)2 • End User Username2, 5 • SSID2 • Access point name and MAC address/location2	Use of the product to provide network visibility and insights, network analytics, and remediation.

[3] This data allows Cisco to identify which appliances belong to which customer.
[4] This data is de-identified locally prior to transfer to the AI Network Analytics cloud. See Section 8 "Personal Data Security" for information regarding the de-identification process.
[5] 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.

©2023 Cisco and/or its affiliates. All rights reserved.

	• Application Usage Data2 • Syslog Data Messages6 •	
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 9 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 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 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 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

6. Data Portability

Data Portability requirements are not applicable to this product.

[6] 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.

©2023 Cisco and/or its affiliates. All rights reserved.

7. Data Deletion & Retention

Data collected by the Catalyst Center Core Solution and by the Cisco 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.

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

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.
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.

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 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:

©2023 Cisco and/or its affiliates. All rights reserved.

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". 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 Catalyst Center Privacy Data Sheet to which this Addendum is attached also applies to AI Network Analytics.

©2023 Cisco and/or its affiliates. All rights reserved.

Addendum 2
Cisco AI Endpoint Analytics

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

1. Overview of Cisco AI Endpoint Analytics Cloud Capabilities

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. 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 Catalyst Center, please see the Catalyst Center Privacy Data Sheet to which this Addendum 2 is attached.
- For general information on the Catalyst Center product, please see the 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.

©2023 Cisco and/or its affiliates. All rights reserved.

2. Personal Data Processing

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

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information[7]	• 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 [8]	• 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[9, 10]	• 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 Information11 • Application Usage Data9	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 9 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

[7] This data allows Cisco to identify which appliances belong to which customer.
[8] This section only applies if customer enables CBAR within the settings page.
[9] 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 6 Personal Data Security for information regarding the de-identification process.
[10] This section only applies if customer enables AI Endpoint Analytics Cloud within the settings page.
[11] 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.

©2023 Cisco and/or its affiliates. All rights reserved.

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 Catalyst Center controls access to the data processed by the product including but not limited to use of 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 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 Portability

Data Portability requirements are not applicable to this product.

7. Data Deletion & Retention

Data collected “on-premise” by 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.

©2023 Cisco and/or its affiliates. All rights reserved.

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.
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 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 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 Catalyst Center credential store.

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 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”. 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.
Amazon Web Services	Machine Learning Analytics Data	Third party cloud-hosting service	United States Germany	See above

©2023 Cisco and/or its affiliates. All rights reserved.

10. Other Information

Sections 10 through 13 of the Catalyst Center Privacy Data Sheet to which this Addendum is attached also applies to AI Endpoint Analytics.

©2023 Cisco and/or its affiliates. All rights reserved.

Addendum 3
Cisco User Defined Network

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

1. Overview of Cisco User Defined Network Capabilities

Cisco® User Defined Network (UDN) is a Cisco network solution available through 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 Catalyst Center, please see the Catalyst Center Privacy Data Sheet to which this Addendum 3 is attached.
- For general information on the Catalyst Center product, please see the 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[12]	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[10]	End User data: • First Name • Last Name • Email address • User defined network name	Authenticate the End User's access to UDN.
User Device Identifiers[13]	• MAC Address • User's name • SSID • Device type	For UDN to identify the devices belonging to the End User and perform its functions.

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

©2023 Cisco and/or its affiliates. All rights reserved.

	• Hostname (i.e., device host name which could include username) • Timestamp for device connection	
Personal Data Associated with Network Events[11]	• 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[11]	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	• 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 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 configuration changes are needed. Please refer to the Information Shared by Customers for Support paragraph in Section 5 of the Catalyst Center Privacy Data Sheet to which this Addendum is attached for information regarding technical support.

©2023 Cisco and/or its affiliates. All rights reserved.

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.
System 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 Portability

Data Portability requirements are not applicable to this product.

7. Data Deletion & Retention

Data collected by the 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 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	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.

©2023 Cisco and/or its affiliates. All rights reserved.

	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.	
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.
System Information	Please see the Catalyst Center Product Data Sheet.	Please see the Catalyst Center Product Data Sheet: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/Catalyst-center/nb-06-Catalyst-center-data-sheet-cte-en.html

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.
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 7 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 7 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 Catalyst Center Product Data Sheet.

©2023 Cisco and/or its affiliates. All rights reserved.

9. Sub-processor

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." 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 Catalyst Center Privacy Data Sheet to which this Addendum is attached also apply to Cisco User Defined Network.

©2023 Cisco and/or its affiliates. All rights reserved.