Cisco Catalyst SD-WAN (cloud-hosted Cisco Catalyst SD-WAN and cloud-delivered Cisco Catalyst SD-WAN)

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by cloud-hosted Cisco Catalyst SD-WAN and by cloud-delivered Cisco Catalyst SD-WAN. In both situations, the SD-WAN controller software is hosted in the Cisco cloud environment. Cloud-hosted Cisco Catalyst SD-WAN and cloud-delivered Cisco Catalyst SD-WAN are hereinafter referred collectively as "Cisco Catalyst SD-WAN".

Cisco Catalyst SD-WAN is a cloud-based enterprise networking solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco Catalyst SD-WAN 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 SD-WAN in order to provide its functionality.

1. Overview

The Cisco Catalyst SD-WAN solution is a software defined wide area network (SD-WAN) solution that allows customers to (i) orchestrate network policies and manage their network from a centralized console, and (ii) segregate the management, control, and orchestration layers from the device transport layer. This enables network policy, control, and orchestration to be performed across the entire network of compatible Cisco routers (physical or virtual) in a secure and extensible manner.

Cisco Catalyst SD-WAN customer data is stored based on how the solution is deployed. As a result, Cisco only processes customer data from Cisco Catalyst SD-WAN when a customer deploys Cisco Catalyst SD-WAN in a Cisco cloud hosted environment, uses a SaaS feature of the solution such as Cisco Catalyst SD-WAN Analytics, interactive help feature from Walkme, or the Cisco Catalyst SD-WAN Portal, or when customer elects to share data with Cisco. If a customer deploys the Catalyst SD-WAN technology in its own data center or in a third-party cloud controlled by customer (i.e., not hosted or delivered in the Cisco cloud environment), Cisco Catalyst SD-WAN data is not accessible to Cisco, except for the aforementioned exceptions.

Other than the personal data described in this Privacy Data Sheet, the data collected by the Cisco Catalyst SD-WAN cloud-hosted consists of network traffic metadata and non-personal Systems Information (i.e., configuration data, logs, device data, cloud controller health and cloud infrastructure data, application usage data, edge usage data, product usage data). Network traffic remains at the routing transport layer and is not sent to Cisco's cloud environment.

Cisco Catalyst SD-WAN integrates with Cisco ThousandEyes WAN Insights and Cisco Success Tracks, which are optional services that must be enabled by customers. Please see the ThousandEyes Privacy Data Sheet for details regarding processing of personal data by Cisco ThousandEyes WAN Insights receiving personal data from Cisco Catalyst SD-WAN. Although some Systems Information is shared with Cisco Success Tracks, no personal data is shared.

Note, Cisco Catalyst SD-WAN may be integrated with third-party products at customer's election. Cisco is not responsible for customer data once it leaves Cisco Catalyst SD-WAN for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contracts and policies of the applicable third party.

For more information about Cisco Catalyst SD-WAN visit https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html.

For more information about cloud-hosted Cisco Catalyst SD-WAN, see the Cisco Catalyst SD-WAN Getting Started Guide.

For more information about cloud-delivered Cisco Catalyst SD-WAN, see the Cloud-delivered Cisco Catalyst SD-WAN Getting Started Guide.

2. Personal Data Processing

The table below lists the personal data processed by Cisco Catalyst SD-WAN to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
System Administrator Log-in Information	• Sys Admin User ID, Email, and hashed password or • Cisco Single Sign-on (CCO) (i.e., SmartAccount), pursuant to which any personal data is processed through the Smart Account service. For more information, see https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1552559092863129 • Web browser localStorage (Cisco Catalyst SD-WAN Analytics)	• Provision of the service (i.e., authenticate authorized users of the solution), audit logs for Cisco Catalyst SD-WAN Manager (SD-WAN management platform), troubleshooting, support, and product notification. Note: For authentication, customer may elect to use local authentication, Cisco CCO, Okta, or other third-party identity providers (IDP), such as Radius or TACACS. When using local or other third-party authentication (non-Okta), except where required by law or enabled by customer, this data is stored locally or by third party IDP, as applicable, and not accessible by Cisco. • Audit logs for Cisco Catalyst SD-WAN Manager for incident response for certified versions of the SD-WAN solution (e.g., FedRAMP, SOC2), if Customer elects to use those versions. • Audit logs for Cisco Catalyst SD-WAN Portal whereby Customer may view audit logs detailing users who have modified customer's overlay fabric via the portal. • Ensure operation of the Cisco Catalyst SD-WAN Analytics feature by saving selected user roles, user authentication, user preferences.
End User Device Identifiers	• Source IP address • Host IP address • Destination IP address	• Provision of the features such as Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) and Cisco Catalyst SD-WAN Analytics meant to offer insights into and optimization for network and application behavior. • Product usage analytics, product improvement and development, product adoption and sales support Note: End User Device IP address data collected by Cisco Catalyst SD-WAN is dynamic, not fixed, and not associated with End User personal information. As a result, such data is not identifiable by Cisco and cannot be associated with any host/user information unless provided by customer.

Cisco Catalyst SD-WAN collects System information to assist Cisco with understanding product usage, product improvement and development, and product adoption and sales support. Customers have the option of disabling the transmission of some categories of Systems Information, such as SD-WAN telemetry data and Cisco Catalyst SD-WAN Analytics. For more information

about how Cisco uses, shares and protects Systems Information, see the Cisco Trust Center. Any personal data that is processed as part of this Systems Information is protected in accordingly.

3. Data Center Locations

Cisco Catalyst SD-WAN leverages third party cloud hosting providers to provide services globally. The following table shows where the data centers that store customer data are located, for reference purposes only. Please note that specific data center locations where customer data is stored may change over time and this Privacy Data Sheet will be updated to reflect those changes if they occur.

Infrastructure Provider	Description	Location
AWS	Hosting Cisco Catalyst SD-WAN controller software in the Cisco cloud (i.e., Cisco Catalyst SD-WAN Manager, Validator, Controller)	Customer chooses one of the following region-specific data centers to host the software controller and to store their data: Australia, Brazil, Canada, Germany, India, Indonesia, Ireland, Japan, South Africa, Singapore, South Korea, Sweden, UK, USA
AWS	Hosting Cisco Catalyst SD-WAN Analytics	Customer chooses one of the following region-specific data centers to store their data: Australia, Germany, USA
Microsoft Azure	Hosting Cisco Catalyst SD-WAN controller software in the Cisco cloud (i.e., Cisco Catalyst SD-WAN Manager, Validator, Controller)	Customers choose the region-specific data center to host the controller software and to store their data: Australia, Brazil, Canada, France, India, Ireland, Japan, the Netherlands, Singapore, South Africa, UAE, UK, USA

Note: When you purchase a service subscription, Cisco processes, and stores customer contact information for product notification purposes, personal information described in Section 2 (Personal Data Processing), and Systems Information detailed in Section 1 (Overview) in the United States, regardless of the subsequent provisioning of your accounts in a chosen regional cloud. All data are encrypted in transit. As noted above, customers have the option of disabling some categories of Systems Information transmission to Cisco. For SD-WAN controller software after the 20.9 release, Systems Information related to the Cisco Catalyst SD-WAN cloud hosted controllers, such as controller health data, controller connection status and other data related to the cloud infrastructure are necessary for Cisco to monitor the health of the Cisco Catalyst SD-WAN cloud hosted controllers and therefore transmission to Cisco in the United States cannot be disabled.

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

Personal Data Category	Who has Access	Purpose of the Access
System Administrator Log-In Information	Cisco Note: When using local or other, third-party identity providers (IDP), except where required by law, or enabled by customer, this data is stored locally or by third party IDP, as applicable, and not	• Upon customer providing access, provide troubleshooting and technical support for the service • Provision and authentication of the service • Communicate service and product updates to customer

	accessible by Cisco. For Okta Cisco accesses the Sys Admin ID and contact information	
	Customer	• Use the service
End User Device Identifiers	Cisco	• Providing the SAIE and Cisco Catalyst SD-WAN Analytics service (i.e., analytics and insights to network and application performance) • Product usage analytics, product development and improvement, product adoption and sales support
	Customer	• Use of the SAIE and Cisco Catalyst SD-WAN Analytics services (i.e., analytics and insights to network and application performance)

6. Data Portability

Customer (or a managed service provider (MSP) in the MSP context) is able to download and transfer audit logs and network statistic data.

7. Data Retention

The table below lists the personal data used by Cisco Catalyst SD-WAN, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
System Administrator Log-In Information	• During customer's active Cisco Catalyst SD-WAN subscription, plus 3 years thereafter	• Customer's use of the service • Provide troubleshooting and technical support for the service • Insights and analytics for product usage, product improvement and development, product adoption and sales support
End User Device Identifiers	• During customer's active Cisco Catalyst SD-WAN subscription, plus 3 years thereafter Note: Retention period differs from the historical data that is visible on the Cisco Catalyst SD-WAN Analytics dashboard. See Cisco Catalyst SD-WAN Analytics User Guide for more details on dashboard data visibility.	• Customer's use of the services • Insights and analytics for product usage, product improvement and development, product adoption and sales support

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
System Administrator Log-In Information	• Encrypted at rest with AES-256 algorithm. Encrypted in transit with TLS 1.2
End User Device Identifiers	• Encrypted at rest with AES-256 algorithm. Encrypted in transit with TLS 1.2

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
AWS	System Administrator Log-in Information, End User Device Identifiers	Hosting Cisco Catalyst SD-WAN controller software in the Cisco cloud environment (i.e., Cisco Catalyst Manager, Validator, Controller), hosting Catalyst SD-WAN Analytics	See Section 3 (Data Center Locations) above
Microsoft Azure	System Administrator Log-in Information, End User Device Identifiers	Hosting Cisco Catalyst SD-WAN controller software in the Cisco cloud (i.e., Cisco Catalyst Manager, Validator, Controller)	See Section 3 (Data Center Locations) above
Okta	Sys Admin ID, Email and password	Authentication services	USA, Europe
Walkme (interactive help)	User identity (e.g., Sys Admin Username, Hostname, session ID), Geo location/time zone, End user device IP address, User agent (e.g., browser name/version, device type, operating system, page URL/title), User behavior tracking (e.g., clickstream data, input into fields, custom events). See for complete details: https://support.walkme.com/knowledge-base/what-data-does-walkme-collect/	Interactive product help guide for system admins, user interaction with UI, insights and analytics Note: Subprocessor will collect data if customer uses this feature. Walkme is available to customers who use cloud-hosted Cisco Catalyst SD-WAN, hosted on the customer's premise, and cloud-delivered Cisco Catalyst SD-WAN.	USA

10. Information Security Incident Management

Breach and Incident Notification Processes

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

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

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

11. 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 security and privacy in mind and is designed so that it can be used by Cisco customers in a manner consistent with global privacy requirements.

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

12. Exercising Data Subject Rights

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

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 redirected to their employer for a response.

Requests can be made by submitting a request via:

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

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	**APJC Privacy Officer** Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	**EMEA Privacy Officer** Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

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.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy 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.